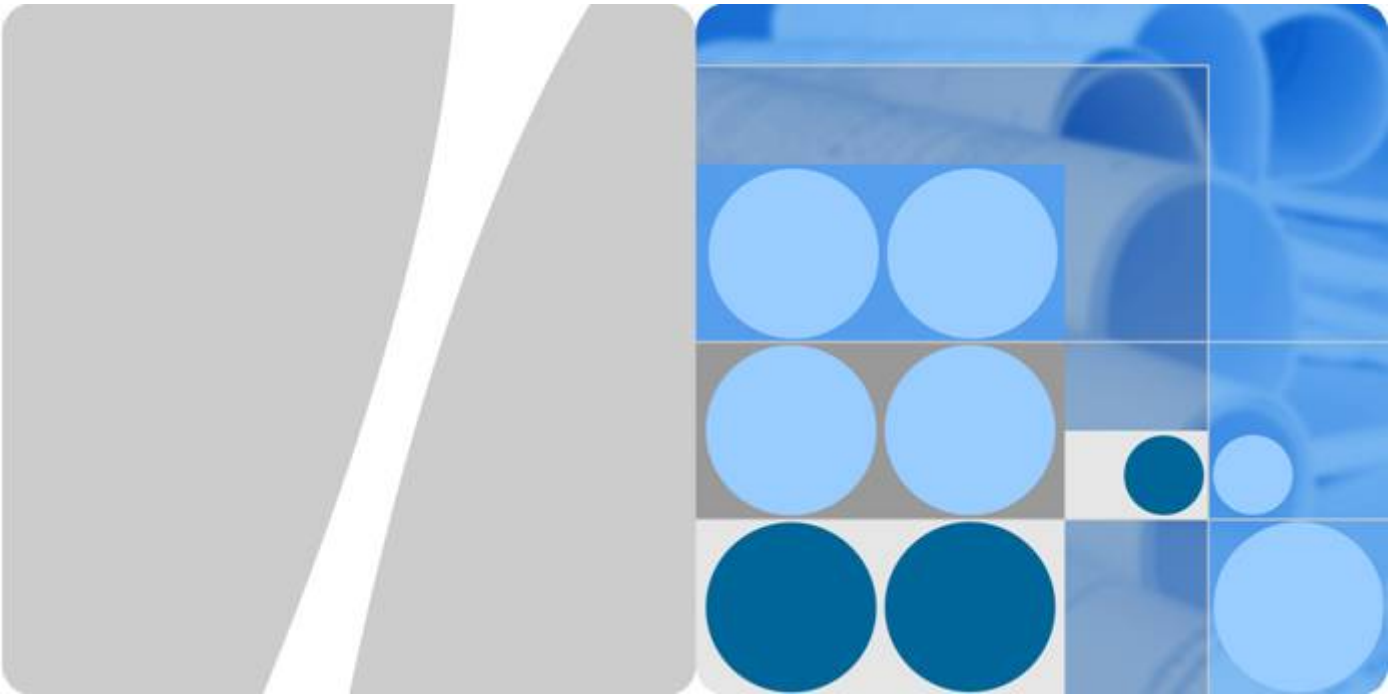


AC6605 无线接入控制器

V200R001C00

故障处理

文档版本　01

发布日期　2012-05-30

华为技术有限公司

HUAWEI

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

本文档介绍了 AC6605 支持特性的告警和常见故障的处理方法、故障案例。

本文档主要适用于以下工程师：

- 网络规划工程师
- 硬件安装工程师
- 调测工程师
- 数据配置工程师
- 现场维护工程师
- 网络监控工程师
- 系统维护工程师

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。

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 (2012-05-30)

第一次正式发布。

目 录

1 设备故障常用信息收集

故障信息收集

故障处理的初期阶段做好与故障相关的各种信息的收集工作，可以帮助维护人员缩小定位故障的范围，提高故障定位的准确性。常用的故障信息搜集的命令如下：

信息项	使用命令	使用说明
基本信息	**display diagnostic-information**	这条命令主要用于系统的基本信息的收集，它包含了 **display current-configuration**、**display device** 等的基本信息，任何网上问题发生时必须提供该信息。使用时请注意，最好在 TELNET 上使用这条命令，如果在 Console 上使用这条命令将需要很长时间且不能够终止。
版本信息	**display version**	-
热补丁信息	**display patch-information**	-
显示系统整体信息	**display device**	-
显示系统温度	**display environment**	-
显示当前配置信息	**display current-configuration**	显示当前设备上所有配置信息。可使用正则表达式对配置信息过滤，以便查找当前所需要的信息。
显示当前时间	**display clock**	-
显示日志信息	**display logbuffer**	-
显示告警信息	**display trapbuffer**	-

信息项	使用命令	使用说明
显示接口信息	**display interface**	与 **display current-configuration interface** *interface-type* [*interface-number*] 命令不同的是：**display interface** 显示的为所有接口的状态信息，而 **display current-configuration** 显示的为当前所有接口下的配置信息。
显示当前系统内存情况	**display memory-usage**	-
显示当前系统 CPU 占有率情况	**display cpu-usage**	-

故障排除

故障定位后，排除故障的典型方法包括以下几种：

- 线路检修或者更换
- 配置数据修改
- 设备重启
- 更换设备

故障排除后，需要在用户视图下执行 **save** 命令，保存系统当前的配置信息。否则设备下次启动时，所做的配置会丢失。

2 硬件类

关于本章

2.1 PoE 故障处理
介绍了 PoE（Power over Ethernet）常见故障的定位思路和案例。

2.1 PoE 故障处理

介绍了 PoE（Power over Ethernet）常见故障的定位思路和案例。

2.1.1 设备的 PoE 功能不可用的定位思路

介绍 PoE 功能不可用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：

- PoE 电源未插入
- PoE 电源工作不正常

故障诊断流程

无

故障处理步骤

执行 **display poe device** 时，显示如下信息：

```
Error: No current active POE board.
```

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 PoE 电源模块是否在位。

只有命名中包含了“PWR”字段的交换机在配置了 PoE 电源模块之后，才能使用 PoE 功能。AC6605 支持的 PoE 电源为交流电源，电源模块上集成有风扇。使用 PoE 功能前请确保 PoE 电源模块已经安装。

- 如果设备上没有安装 PoE 电源模块，请正确安装电源模块。
- 如果设备上已经安装 PoE 电源模块，请执行步骤 2。

步骤 2 检查 PoE 电源模块是否正常。

执行 **display power** 命令，检查 PoE 电源模块的状态。

- 如果“State”显示为“Abnormal”，说明 PoE 电源不能正常供电，请更换 PoE 电源模块。
- 如果“State”显示为“Normal”,说明 PoE 电源模块已经正常上电，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

2.1.2 PSE 检测不到 PD 设备的定位思路

介绍 PSE 检测不到 PD 设备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：

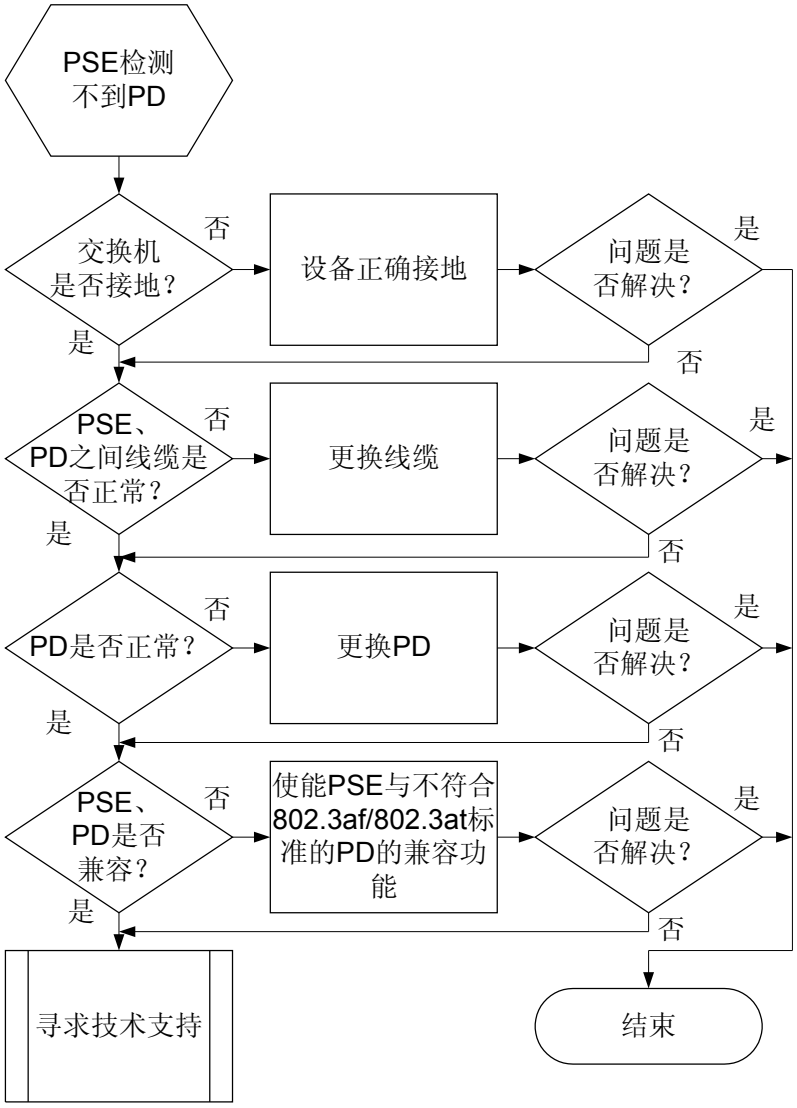
- 交换机没有接地
- PSE（Power Source Equipment）与 PD（Powered Device）之间网线故障
- PD 故障
- PSE 设备与 PD 设备不兼容

故障诊断流程

PD 通过网线接入交换机端口后，执行 **display poe power-state slot** *slot-id* 查看端口的 PoE 供电信息时，发现端口对应的状态 Status 为“Detecting”检测状态。

详细处理流程如图 2-1 所示。

图 2-1 PSE 检测不到 PD 设备故障诊断流程图



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 检查交换机接地是否良好。

由于网线的布线不可控，所以从网线上很容易引入很强的干扰信号，如大功率基站干扰等。在交换机不做接地处理的情况下，干扰很可能影响到网线中的检测信号，从而导致交换机无法发现 PD 设备并对其供电。

- 如果交换机未接地，请将交换机接地。

- 如果交换机已经接地，请执行步骤 2。

步骤 2 检查 PSE 与 PD 之间的网线是否故障。

- 如果网线故障，请更换网线。
- 如果网线没有故障，请执行步骤 3。

步骤 3 检查 PD 是否故障。

将该 PD 连接到可以正常给其他 PD 设备供电的接口上，然后使用 **display poe power-state slot** *slot-id* 命令查看端口状态，如果“Status”显示是，说明是原来的那个端口供电故障。如果仍然不能检测到，说明 PD 故障。

- 如果 PD 故障，请更换 PD 设备。
- 如果 PD 正常，请执行步骤 4。

步骤 4 检查 PSE 是否开启兼容性功能检测。

在接口下执行 **display this** 检查是否开启了兼容性检测。

- 如果没有开启兼容性检测，请在接口视图下执行 **poe legacy enable**。
- 如果已经开启兼容性检测，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

2.1.3 PSE 无法对 PD 供电的定位思路

介绍 PSE 无法对 PD 供电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：

- 关闭了设备的自动供电功能，且未手工配置端口供电功能。
- 接口下未使能 PoE 功能。
- 设备的剩余功率小于 PD 的参考功率。
- 用户预留了过多的 PoE 电源功率，导致无法对外供电。

- PD 可以消耗的总功率已经用完。

故障诊断流程

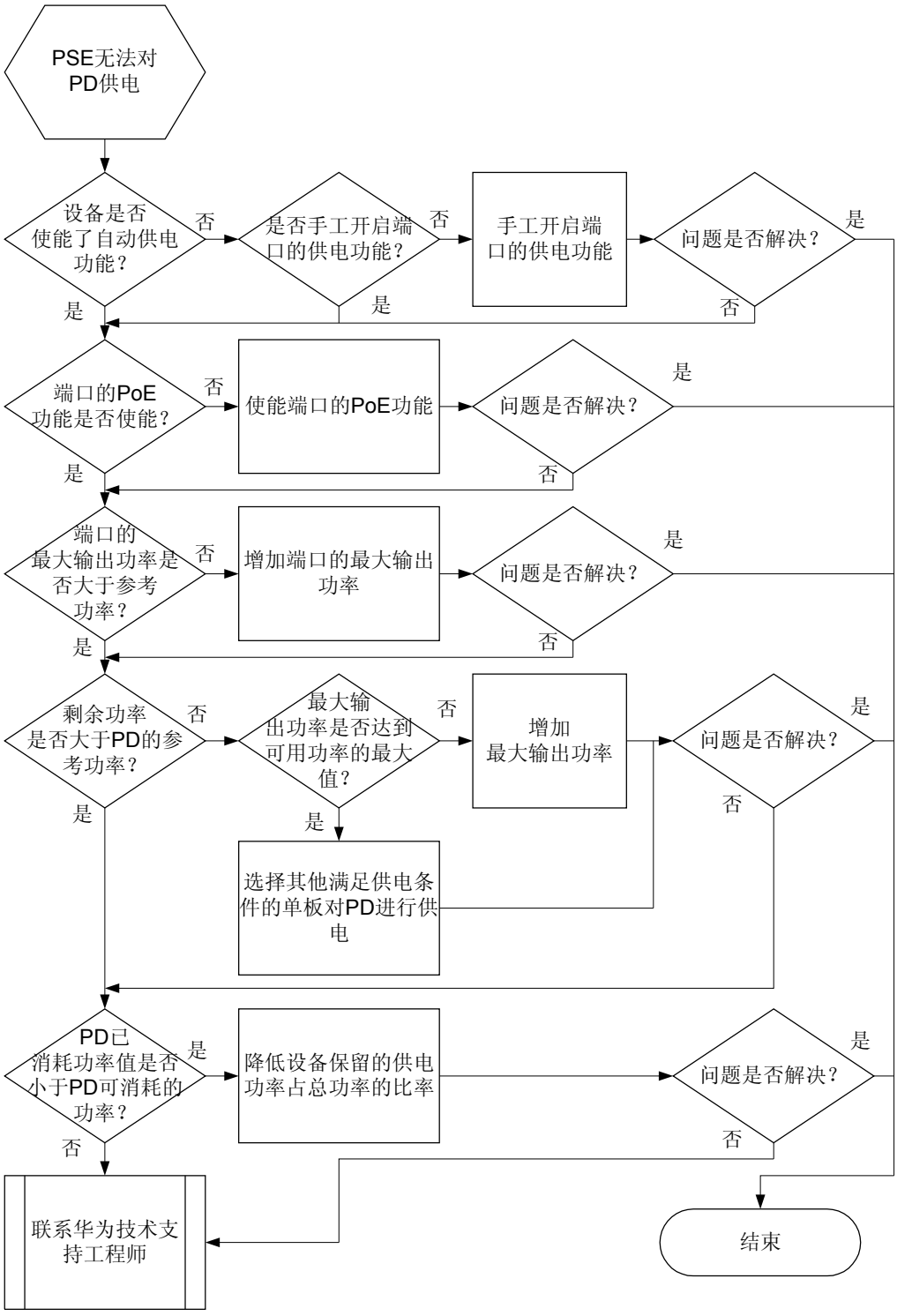
PD 通过网线接入交换机端口后，PSE 能检测到 PD 设备但是无法自动供电。

故障的定位思路如下：

- 是否关闭了自动供电功能，且未手工配置端口供电功能
- 端口的 PoE 功能是否使能
- 用户配置的端口的最大功率是否小于端口的参考功率
- 设备的剩余功率是否小于端口的参考功率
- PoE 电源的可用供电功率是否都已经被消耗

详细处理流程如图 2-2 所示。

图 2-2 PSE 无法对 PD 供电故障诊断流程图



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 检查设备是否已经使能自动供电功能。

交换机的供电方式可以为自动方式或者手工方式，缺省情况下，交换机的供电管理方式为自动方式。当检查到下挂的设备属于合法的 PD 设备，且 PSE 完成对 PD 的分类后，PSE 即开始对该设备进行供电。可以通过执行命令 **display poe information** 查看“Power-Management mode”是否为“auto”，如果为“auto”，说明当前设备使能了自动供电功能，如果为“manual”说明设备的供电方式为手工开启设备供电功能。

- 如果供电方式为手工方式，检查端口下是否手工开启端口的供电功能。

  可以通过执行 **display poe power-state slot** *slot-id* 检查端口的供电功能是否开启。显示信息中字段可用于判断端口的供电功能是否开启。

  - 如果未手工开启端口的供电功能，请在系统视图下执行命令 **poe power-on interface** *interface-type interface-number* 使能端口的供电功能。
  - 如果端口的供电功能已经手工开启，请执行步骤 2。
- 如果供电方式为自动供电方式，请执行步骤 2。

步骤 2 检查端口的 PoE 功能是否开启。

执行 **display poe power-state slot** *slot-id* 检查端口的 PoE 功能是否使能。如果显示信息中端口对应的字段的值为“enable”说明端口的 PoE 功能已经使能。

- 如果端口的 PoE 功能没有使能，请在端口视图下执行 **poe enable** 使能端口的 PoE 功能。
- 如果端口的 PoE 功能已经是使能，请执行步骤 3。

步骤 3 检查配置的端口的最大输出功率是否大于 PD 的参考功率。

系统会自动识别端口连接的 PD 设备的最大功率，并给 PD 设备分成 5 类，定义各类型 PD 的参考功率。可以通过执行命令 **display poe power-state interface** *interface-type interface-number* 检查用户配置的端口最大输出功率“Port max power(mW)”和端口下挂 PD 的参考功率“Port reference power(mW)”。

- 如果端口的最大输出功率小于 PD 的参考功率，请在端口视图下执行 **undo poe power** 命令恢复端口最大输出功率，或者在恢复缺省值以后重新执行命令 **poe power** 配置端口最大输出功率大于 PD 的参考功率值，
- 如果端口的最大输出功率大于 PD 的参考功率，请执行步骤 4。

步骤 4 检查设备的剩余可用功率是否大于 PD 的参考功率。

执行 **display poe information** 可以查看设备的剩余可用功率“Available Total Power”。

- 如果设备上的剩余功率小于 PD 的参考功率，请根据实际情况选择执行。
  - 用户配置的设备最大输出功率未达到设备能够提供的功率（系统自动获取）

    请执行 **poe max-power** *slot_max_power* **slot** *slot-id* 调整设备的最大输出功率，使得设备的剩余功率大于 PD 的参考功率。如果调整设备的最大输出功率后，剩余功率大于 PD 的参考功率，但是 PSE 仍然无法给 PD 供电，请执行步骤 5。
  - 设备的最大输出功率已经达到设备能够提供的 PoE 功率的最大值，说明该设备已经无法再对该 PD 供电。
- 如果当前设备的剩余功率大于 PD 的参考功率，执行步骤 5。

步骤 5 检查 PoE 电源的剩余 PoE 供电功率是否大于 PD 的参考功率。

为了预留功率可以支撑突发需求，设备上可能配置 PoE 电源预留一部分功率（缺省情况下，设备预留 20%的 PoE 电源功率），PD 实际可消耗的功率为 PoE 电源总功率减去预留的供电功率。

执行命令 **display poe-power** 检查 PoE 电源的输出信息，“Available power value(mW)”表示 PoE 电源的供电总功率，“Reserved power percent”表示系统预留的 PoE 电源功率占总供电功率的百分比。如果预留百分比为 100%，说明用户配置预留了所有的 PoE 功率，设备无法对 PD 供电。

执行命令 **display poe information**，显示信息中“Total Power Consumption(mW)”即为设备上已经消耗的功率。

- 如果 PD 已消耗的功率总值已经接近 PD 可以消耗的功率，可用的供电功率小于 PD 的参考功率，此时 PSE 无法对 PD 设备供电。执行命令 **poe power-reserved** *power-reserved* 降低设备保留的供电功率占总功率的比率，使得 PD 可以消耗的总功率变大。
- 如果 PD 已经消耗的功率小于 PD 可以消耗的功率，可用的供电功率大于 PD 的参考功率，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

3 系统类

关于本章

3.1 CPU 故障处理

3.1.1 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%。但是在网络运行中 CPU 高常常会导致其他业务异常，如设备无法登录。业务异常的故障，请根据具体表现查看相应的故障处理章节。以下讨论的原因及步骤基于 CPU 占用率高这个现象。

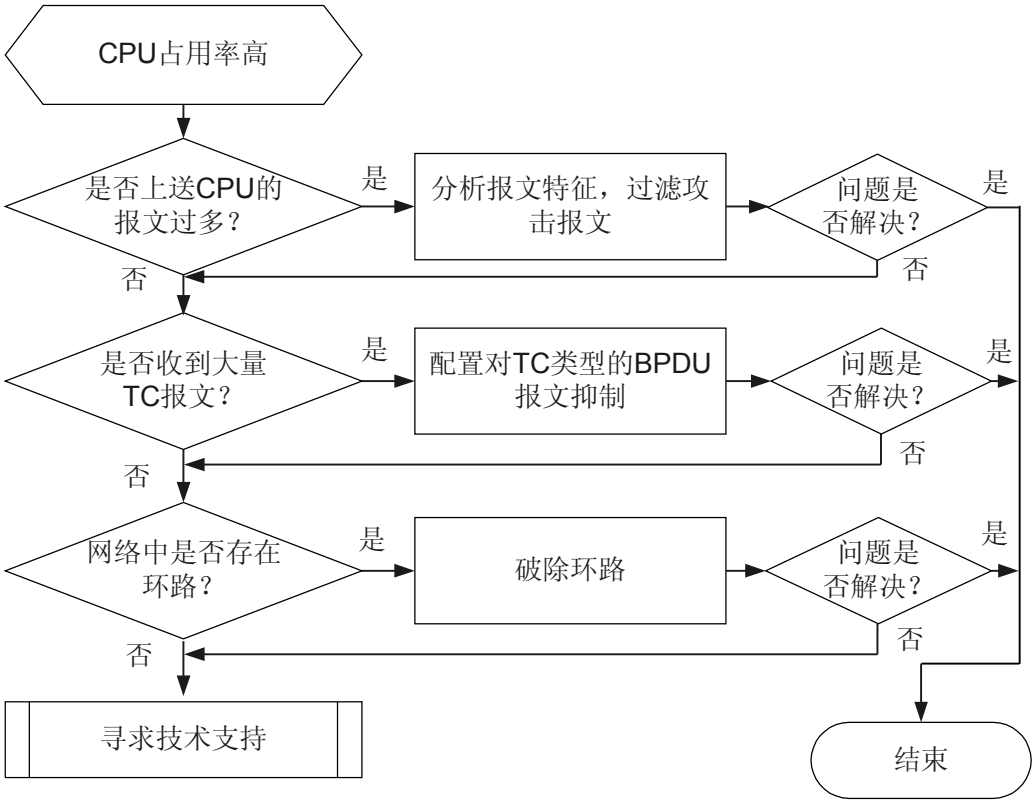
通常，整机 CPU 占用率过高，是由于某些任务的 CPU 占用率居高不下导致的。具体导致某任务 CPU 占用率高的可能原因：

- 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

故障诊断流程

详细处理流程如图 3-1 所示。

图 3-1 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。

常见的任务说明如下表所示。

任务名	描述
VIDL	空闲任务。该任务对应的取值越大，CPU 越空闲。
SOCK	收包处理任务。该任务占用率高，说明 CPU 收到大量协议报文并进行处理，可能是 IP 报文攻击导致。
RPCQ	板间通讯任务。该任务和 SOCK 任务可以结合在一起分析，如果收到大量报文且需要响应，该任务占用率会比较高，可能是受到报文攻击导致。
ROUT	路由模块处理任务。大量路由学习或者路由震荡时，该任务占用率较高，此时需要查看相关路由信息确定路由模块是否存在问题。
bcmRX	底层收包任务。该任务占用率高，说明 CPU 收到大量报文。

步骤 2 检查是否上送 CPU 的报文太多

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 tc-bpdu statistics**，查看接口下收到的 TC 报文和 TCN 报文计数。

- 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。
  ```
  [Quidway] stp tc-protection
  [Quidway] stp tc-protection threshold 5
  [Quidway] stp timer hello 120
  ```
- 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。

根据组网，在 VLAN 视图下执行 **display this** 命令查看是否配置了 MAC 地址漂移告警功能。

```
[Quidway-vlan7] display this
#
vlan 7
 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：
  ```
  Jan 17 2011 19:40:16 L2_SRV_78 L2IFPPI/4/MFLPVLANALARM:OID 1.3.6.1.4.1.2011.5.25.160.3.7 Loop exists in vlan 7, for flapping mac-address 0000-0000-0004 between port GE0/0/2 and port GE0/0/3
  ```
  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 MAC FLAPPING 告警功能，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 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

- VOSCPU/4/CPU_USAGE_HIGH

3.2 ALS 故障处理

3.2.1 光纤链路出现故障时，发光状态未出现周期性变化的定位思路

常见原因

本类故障的常见原因主要包括：

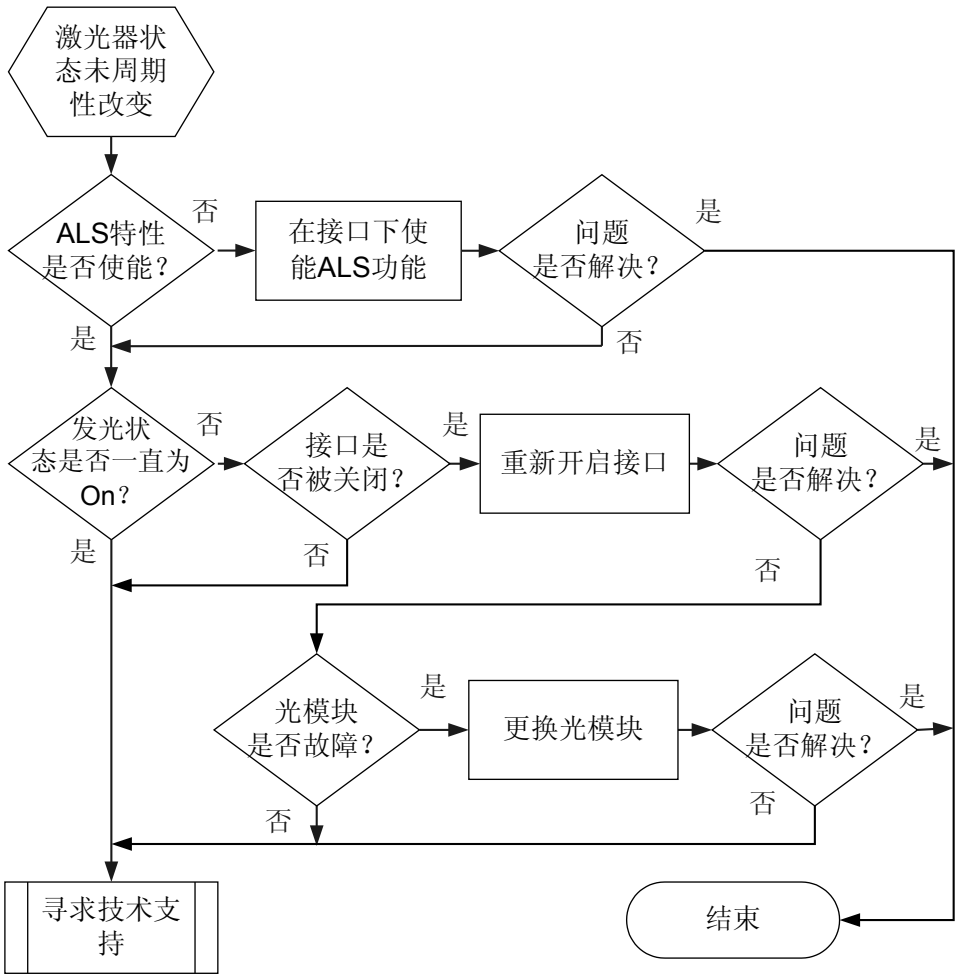
- 端口没有使能 ALS
- 端口被 shutdown
- 光模块故障

故障诊断流程

接口的激光器在自动重启模式的情况下，如果当光纤链路出现故障时，激光器的发光状态未出现周期性的变化，请参考以下步骤解决故障。

详细处理流程如图 3-2 所示。

图 3-2 激光器的发光状态未出现周期性变化的故障诊断流程图



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 ALS 特性是否使能

执行 **display als configuration** 命令检查端口下是否使能 ALS。如果“AlS Status”的值为“Enable”说明 ALS 功能已经使能，值为“Disable”说明 ALS 功能未使能。

- 如果未使能 ALS 功能，请在端口视图下执行 **als enable** 命令，使能 ALS 功能。
- 如果 ALS 功能已经使能，请执行步骤 2。

步骤 2 检查激光器的状态是否一直为 On 或者一直为 Off

使能 ALS 功能后，缺省情况下，如果光纤链路出现故障，激光器将按照缺省的发光间隔和发光时长周期性打开发光器件。重复执行 **display als configuration** 查看激光器的状态，可以看到“Laser status”的值在“On”和“Off”之间变化。

说明

缺省情况下，激光器的重启模式为自动重启，发光间隔为 100s，发光时长为 2s，即激光器每隔 100s 发光 2s。由于发光时长较短，通过 **display als configuration** 查看激光器的状态时，可能一直显示为“Off”。用户可以适当的延长发光时长，观察激光器的状态是否发生变化。

- 如果“Laser status”的值一直为“Off”，说明激光器一直处于关闭状态，请执行步骤 3。
- 如果“Laser status”的值一直为“On”，说明激光器一直处于发光状态，请执行步骤 5。

步骤 3 检查端口是否被 shutdown

- 如果端口被 shutdown。请在端口视图下执行 **undo shutdown** 重启端口。
- 如果端口未被 shutdown，请执行步骤 4。

步骤 4 检查是否出现光模块故障

- 如果设备光模块故障，请更换光模块。
- 如果设备光模块无故障，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

3.2.2 光纤链路恢复正常后，端口无法 Up 的定位思路

常见原因

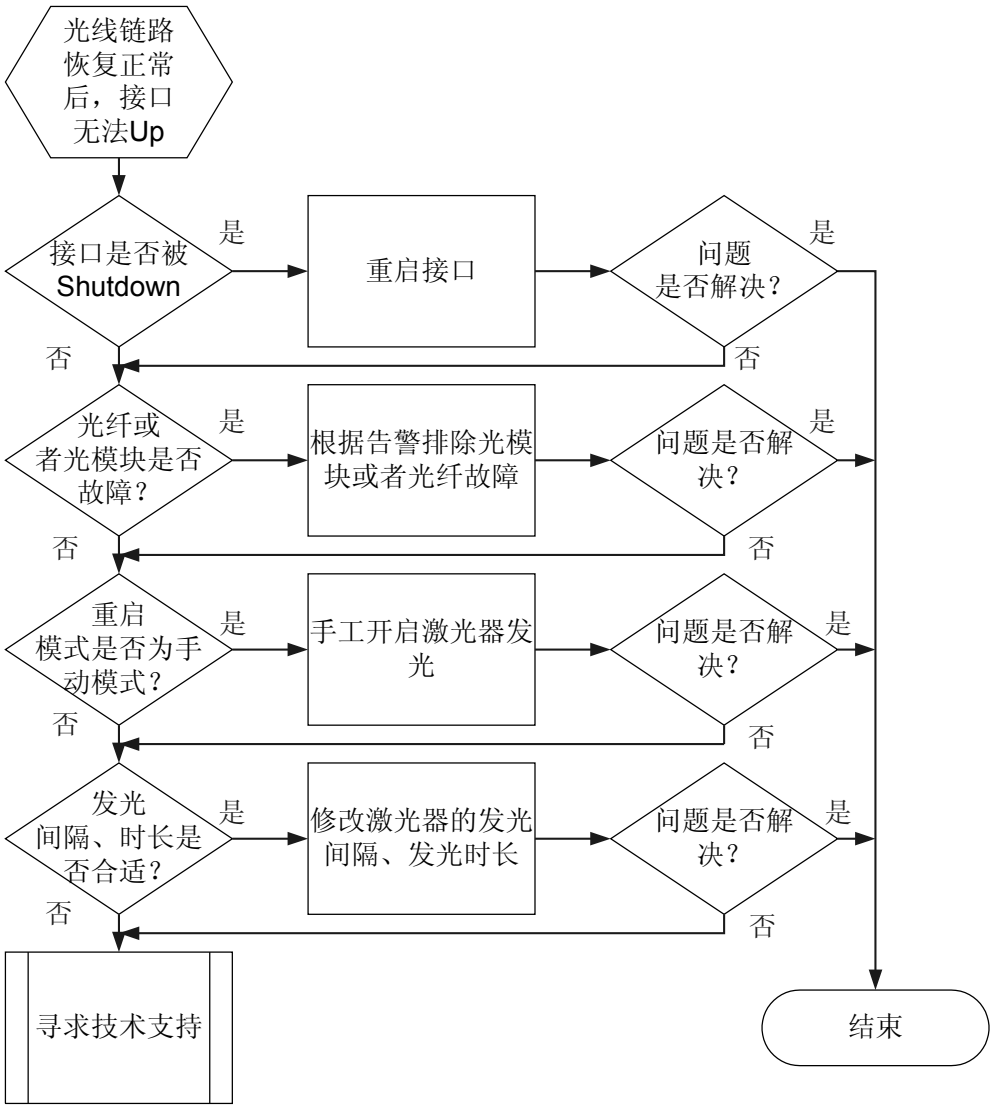
本类故障的常见原因主要包括：

- 端口被 Shutdown 或者光模块损坏
- 激光器的重启模式为手动重启的情况下，未手工打开光模块的激光器。
- 激光器的重启模式为自动重启的情况下，发光间隔配置过长或者发光时长过短。

故障诊断流程

详细处理流程如图 3-3 所示。

图 3-3 光纤链路恢复正常后，端口无法 Up 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 检查端口是否被 Shutdown

- 如果端口被 shutdown。请在端口视图下执行 **undo shutdown** 或者 **restart** 重启端口。
- 如果端口未被 shutdown，请执行步骤 2。

步骤 2 检查是否出现光模块或者光纤故障

- 如果设备光模块故障，请更换光模块。
- 如果设备光纤故障，请更换光纤。
- 如果设备光模块或者光纤无故障，请执行步骤 3。

步骤 3 检查端口的激光器的重启模式是否为手动模式

执行 **display als configuration** 命令检查激光器的重启模式。如果显示信息中“Restart Mode”为“Manual”说明激光器的重启模式为手动模式，如果为“Auto”说明重启模式为自动模式。

- 如果链路两端的激光器重启模式为手动模式，请在任意一端设备上执行 **als restart** 命令手工开启激光器发光。如果链路仍然不能 Up，请执行步骤 5。
- 如果链路两端的激光器的重启模式为一端手动，另一端自动或者两端均为自动，请执行步骤 4。

步骤 4 检查发光器的发光间隔是否配置过长或者发光时长过短

在激光器重启模式为自动模式的一端，执行 **display als configuration** 命令检查配置的发光间隔和发光时长。

显示信息中“Interval(s)”为发光间隔，“Width(s)”为发光时长。缺省情况下，发光间隔为 100s，发光时长为 2s，即每隔 100 秒，设备持续发光 2 秒。发光间隔越长，对端设备接收到本端发送的光脉冲的等待时间越长，这期间端口的 LOS 信号一直存在，从而引起端口无法 Up。

如果需要修改发光间隔，请在端口视图下执行 **als restart pulse-interval** 命令。

如果需要修改发光时长，请在端口视图下执行 **als restart pulse-width** 命令。

如果减小发光间隔或增加发光时长后，端口仍然不能 Up，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

3.3 Telnet 故障处理

3.3.1 Telnet 登录失败的定位思路

常见原因

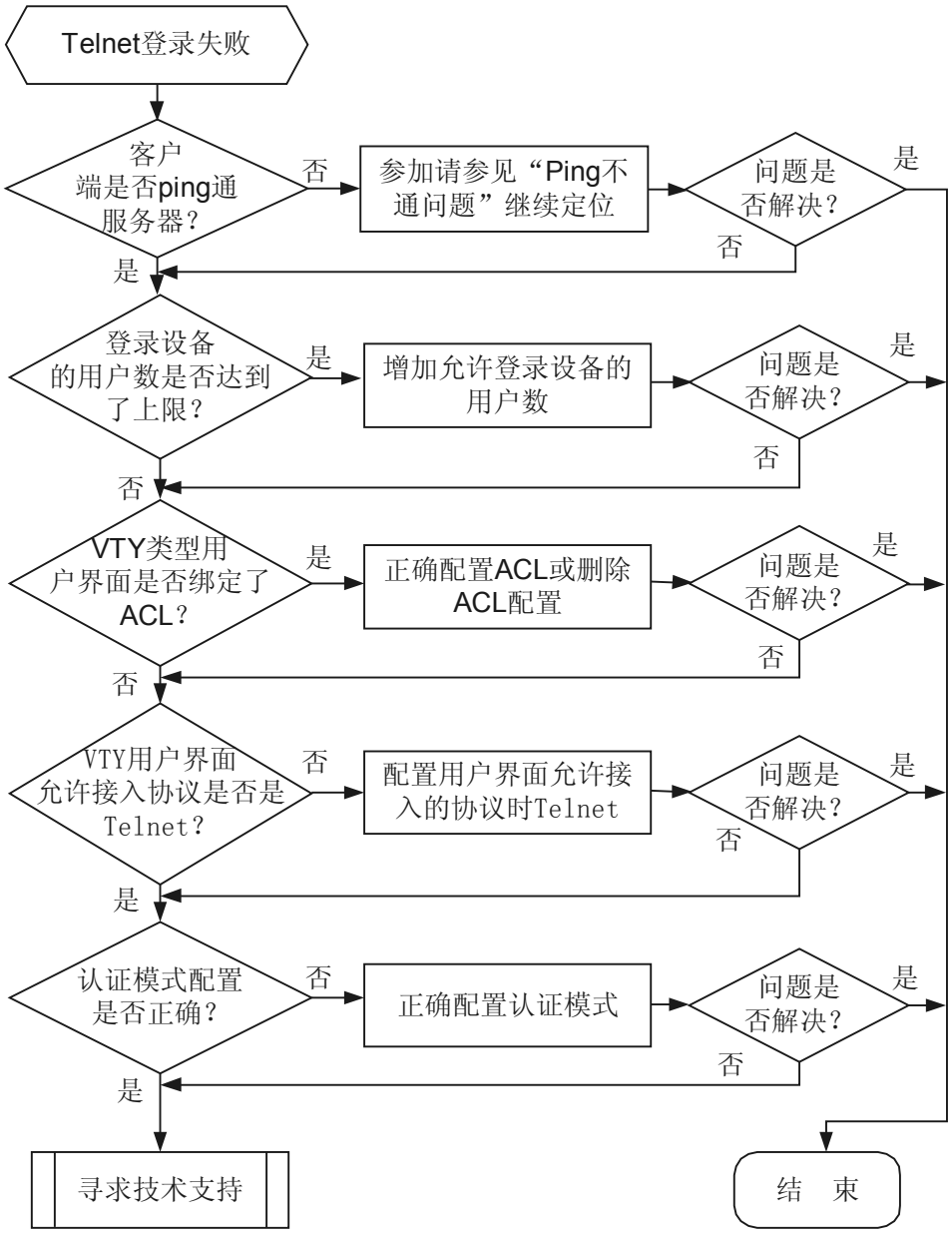
本类故障的常见原因主要包括：

- 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 3-4 所示。

图 3-4 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 **7.2.1 PING 不通故障处理思路**继续定位，使 Telnet 客户端能 Ping 通服务器端。

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。

```
<Quidway> display user-interface maximum-vty
 Maximum of VTY user:5
<Quidway> 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。

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

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

```
[Quidway] user-interface vty 0 4
[Quidway-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。

```
[Quidway] user-interface vty 0 4
[Quidway-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。
- 如果使用命令 **authentication-mode none** 设置认证方式为不认证 **none**，则认证方式不影响用户登录。

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

SHELL/4/TELNETFAILED:Failed to login through telnet. (Ip=[STRING], UserName=[STRING], Times=[ULONG])

3.4 FTP 故障处理

3.4.1 FTP 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：

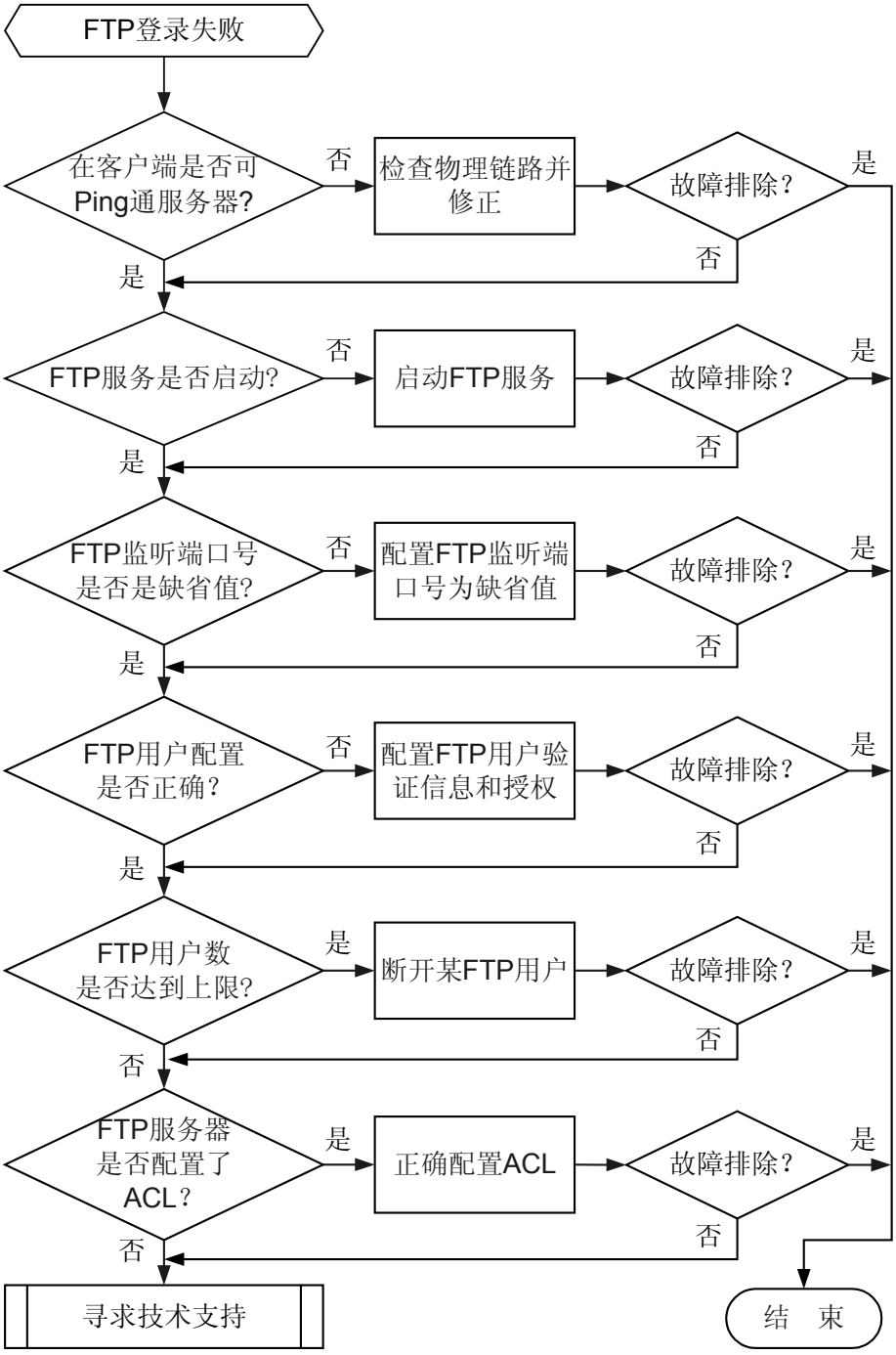
- 客户端与服务器之间的路由不可达。
- FTP 服务器功能没有启动。
- FTP 服务器指定监听端口号不是缺省端口号，且 FTP 客户端登录时没有指定端口号。
- 未配置 FTP 用户的验证信息和工作目录。
- 登录 FTP 服务器的用户数达到上限。
- FTP 服务器配置了 ACL 规则限制客户端登录。

故障诊断流程

从客户端登录 FTP 服务器时发现登录失败。

详细处理流程如图 3-5 所示。

图 3-5 FTP 登录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 检查客户端与服务器之间是否可以 ping 通。

在客户端执行命令 **ping**，查看是否可以 ping 通服务器端。

```
<Quidway> ping 10.164.39.218
  PING 10.164.39.218: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.164.39.218 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

- 如果不能 ping 通，FTP 连接也不能建立。请参见 **7.2.1 PING 不通故障处理思路**继续定位，使 FTP 客户端能 ping 通 FTP 服务器端。
- 如果可以 ping 通，请执行**步骤 2**。

步骤 2 检查 FTP 服务器功能是否启动。

在任意视图下执行命令 **display ftp-server** 查看 FTP 服务器的状态。

- 如果 FTP 服务器没有启动，显示信息如下。

  ```
  <Quidway> display ftp-server
  Info: The FTP server is already disabled.
  ```

  在系统视图下执行命令 **ftp server enable**，使能 FTP 服务器功能。

  ```
  <Quidway> system-view
  [Quidway] ftp server enable
  Info: Succeeded in starting the FTP server.
  ```

- 如果 FTP 服务器功能启动，显示信息如下。请执行**步骤 3**。

  ```
  <Quidway> display ftp-server
    FTP server is running
    Max user number                5
    User count                     0
    Timeout value(in minute)       30
    Listening port                 21
    Acl number                     0
    FTP server's source address    0.0.0.0
  ```

步骤 3 检查 FTP 服务器的监听端口号是否是缺省端口号。

1. 在任意视图下执行命令 **display tcp status** 查看当前 TCP 端口监听状态，是否有 FTP 的缺省监听端口号 21。

   ```
   <Quidway> display tcp status
   TCPCB    Tid/Soid Local Add:port        Foreign Add:port      VPNID  State
   2a67f47c  6  /1    0.0.0.0:21           0.0.0.0:0               23553 Listening
   2b72e6b8  115/4    0.0.0.0:22           0.0.0.0:0               23553 Listening
   3265e270  115/1    0.0.0.0:23           0.0.0.0:0               23553 Listening
   2a6886ec  115/23   10.137.129.27:23     10.138.77.43:4053       0     Establish
   ed
   2a680aac  115/14   10.137.129.27:23     10.138.80.193:1525      0     Establish
   ed
   2a68799c  115/20   10.137.129.27:23     10.138.80.202:3589      0     Establish
   ed
   ```

2. 在任意视图下执行命令 **display ftp-server** 查看 FTP 服务器的监听端口号。

   ```
   <Quidway> display ftp-server
     FTP server is running
     Max user number                5
     User count                     0
     Timeout value(in minute)       30
   ```

```
Listening port                  21
Acl number                      0
FTP server's source address     0.0.0.0
```

- 如果当前 FTP 服务器的监听端口号不是 21，执行命令 **ftp server port**，设置 FTP 服务器的监听端口号为 21。

```
<Quidway> system-view
[Quidway] undo ftp server
[Quidway] ftp server port 21
```

- 如果当前 FTP 服务器的监听端口号是 21，请执行步骤 4。

步骤 4 检查是否配置 FTP 用户的验证信息和授权目录。

- FTP 用户名、密码和工作目录是必配置项。因为没有指定 FTP 工作目录而登录失败是常见故障。
  1. 执行命令 **aaa**，进入 AAA 视图。
  2. 执行命令 **local-user** *user-name* **password** { **simple** | **cipher** } *password*，配置本地用户名和密码。
  3. 执行命令 **local-user** *user-name* **ftp-directory** *directory*，配置 FTP 用户的授权目录。
- 接入类型是可选项。缺省情况下，系统支持所有接入类型。如果配置了其中一项或者几项服务，那么只为该用户提供配置的这几项服务。

  执行命令 **local-user** *user-name* **service-type ftp**，配置 FTP 服务类型。
- 如果已经配置 FTP 用户的验证信息和授权目录，请执行步骤 5。

步骤 5 检查登录 FTP 服务器的用户数是否达到上限。

执行命令 **display ftp-users**，查看 FTP 用户数是否达到 5 个。

- 如果 FTP 用户数达到 5 个，在 FTP 客户端视图下执行命令 **quit** 来断开某 FTP 用户。
- 如果 FTP 用户数没有达到 5 个，请执行步骤 6。

步骤 6 检查 FTP 服务器端是否配置了 ACL。

执行命令 **display** [**ipv6**] **ftp-server**，查看 FTP 服务器端是否配置了 ACL。

- 如果配置了 ACL 规则，系统仅允许在 ACL 规则列表中指定的 IP 地址登录 FTP 服务器。
- 如果没有配置 ACL，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

FTPS/3/LOGIN_FAIL:The user failed to log in. (UserName="[string]", IpAddress=[string], VpnInstanceName="[string]")

FTPS/5/LOGIN_OK:The user succeeded in login. (UserName="[string]", IpAddress=[string], VpnInstanceName="[string]")

FTPS/5/REQUEST:The user had a request. (UserName="[string]", IpAddress=[string], VpnInstanceName="[string]", Request=[string])

3.4.2 FTP 传输失败的定位思路

常见原因

本类故障的常见原因主要包括：

- FTP 源、目的路径中含有空格等设备不支持的字符。
- FTP 服务器根目录下的文件数达到上限。
- FTP 服务器根目录存储空间不足。

故障诊断流程

略。

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 FTP 源、目的路径中含有空格等设备不支持的字符。

- 如果路径中含有空格等设备不支持的字符，请修改路径。
- 如果路径中没有，请执行**步骤 2**。

步骤 2 检查 FTP 服务器根目录下的文件数是否达到上限。

当前文件系统支持的最大文件数是 40。如不及时清理文件，将导致写文件失败。

在 FTP 服务器端执行命令 **dir**，查看 FTP 服务器根目录下的文件数。

- 如果文件数达到 40，在用户视图下执行命令 **delete** 删除某文件。
- 如果文件数没有达到 40，请执行**步骤 3**。

步骤 3 检查 FTP 服务器根目录存储空间是否不足。

在 FTP 服务器端执行命令 **dir**，查看 FTP 服务器根目录下的空闲空间。

- 如果存储空间已满，在用户视图下执行命令 **delete /unreserved** 删除不需要的文件。
- 如果存储空间未满，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

FTPS/3/TRS_FAIL:The user failed to transfer data. (UserName="[string]", IpAddress=[string], VpnInstanceName="[string]")

FTPS/5/SENDDATA:The FTP server sent [ULONG] bytes to the client [STRING]. (IpAddress=[STRING], VpnInstanceName="[string]")

FTPS/5/RECVDATA:The FTP server received [ULONG] bytes from the client [STRING]. (IpAddress=[STRING], VpnInstanceName="[string]")

3.4.3 FTP 传输速度慢的定位思路

常见原因

本类故障的常见原因主要包括：

- 使用 Flash 作为存储介质。
- 网络不稳定造成报文重传。

故障诊断流程

略。

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 AC6605 使用 Flash 作为存储介质。

Flash 的特点是读取速度快，但是写速度慢。**表 3-1** 是 FTP 传输中做的实验数据，可以看出，对 Flash 的写操作是最慢的。

表 3-1 FTP 传输速度列表

测试对象	get	put
Flash—Flash	**0.55 k/s**	**0.51 k/s**
Flash—hda	**0.51 k/s**	16.05 k/s
Flash—CFcard	**1.63 k/s**	58.66 k/s
hda—Flash	32.19 k/s	**1.51 k/s**
hda—hda	32.91 k/s	25.70 k/s
hda—CFcard	21.33 k/s	54.69 k/s
CFcard—Flash	51.23 k/s	**0.55 k/s**
CFcard—hda	40.19 k/s	14.23 k/s
CFcard—CFcard	33.21 k/s	59.14 k/s

步骤 2 检查是否有报文重传。

在客户端 PC 上使用网络抓包工具进行获取、分析报文内容，检查是否有 TCP 重传。一般的原因是网络不稳定。

图 3-6 是通过 Ethereal 抓包工具获取到的样例，表现为收到很多“TCP Retransmission”报文。

图 3-6 Ethereal 抓包图

Time	Source	Destination	Protocol	Info
21 0.076377	192.168.2.1	192.168.2.5	TCP	[TCP Dup ACK 14#4] 4
22 0.509676	192.168.2.5	192.168.2.1	TCP	[TCP Retransmission]
23 0.516849	192.168.2.1	192.168.2.5	TCP	49772 > 2712 [ACK] S
24 0.516886	192.168.2.5	192.168.2.1	TCP	[TCP Retransmission]
25 0.516899	192.168.2.5	192.168.2.1	TCP	[TCP Retransmission]
26 0.516910	192.168.2.5	192.168.2.1	TCP	[TCP Retransmission]
27 0.516952	192.168.2.5	192.168.2.1	TCP	2712 > 49772 [ACK] S

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

3.5 SNMP 故障处理

3.5.1 SNMP 无法连接的定位思路

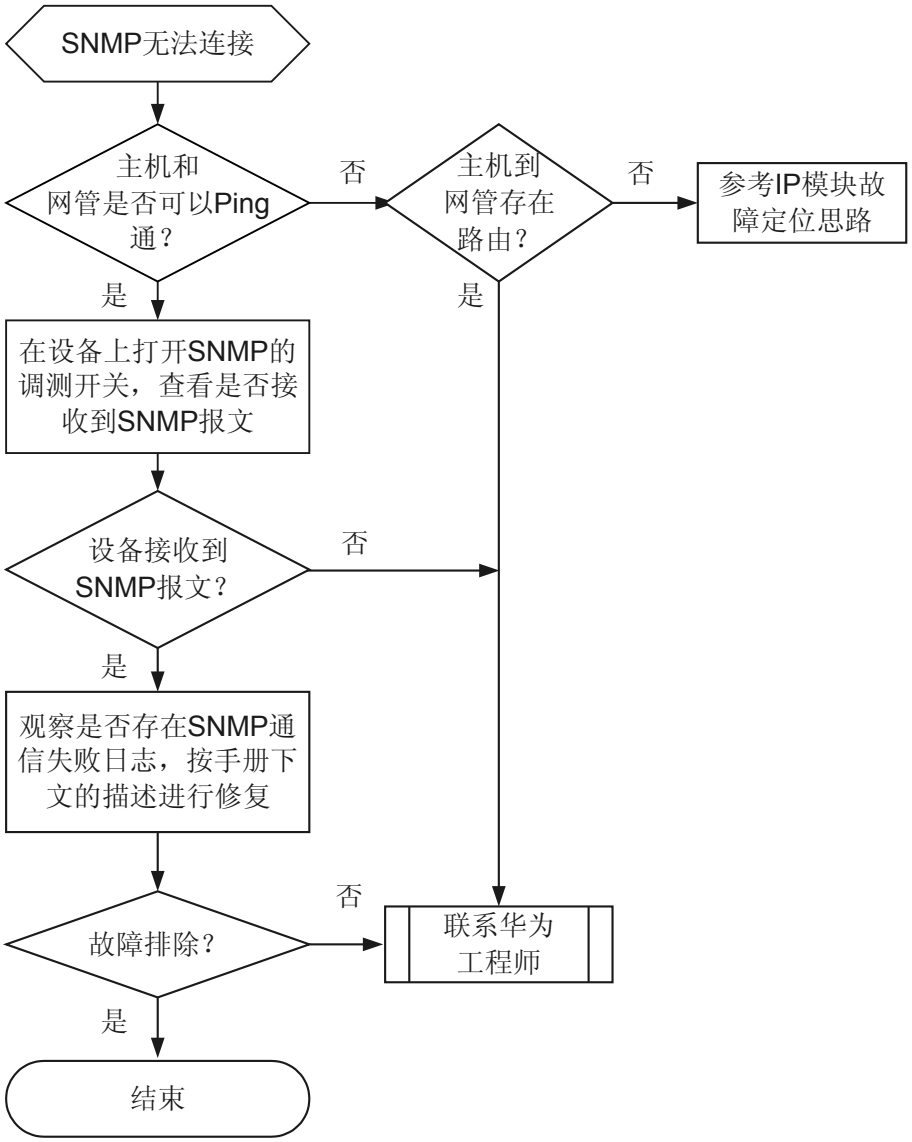
常见原因

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 3-7 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。

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。

- 如果无法 Ping 通，请参见 **7.2.1 PING 不通故障处理思路**继续定位，使主机和网管之间可以 Ping 通。

步骤 2 执行 **display logbuffer** 命令查看主机上是否有提示登录失败的日志。

- 如果没有 SNMP 登录失败日志，则执行步骤 3。
- 否则，将主机的日志取出进行进一步分析：

表 3-2 日志解释及处理建议

日志	日志解释	处理建议
Failed to login through SNMP, because the version was incorrect. (Ip=[STRING], Times=[ULONG])	主机不支持网管发送登录请求所使用的 SNMP 协议版本。	1. 执行 **display snmp-agent sys-info version** 命令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。 ● 是，则=>c。 ● 否则=>b。 2. 执行 **snmp-agent sys-info version** 命令配置主机所支持的 SNMP 协议版本。 ● 问题解决，则=>d。 ● 否则=>c。 3. 请联系华为技术支持工程师。 4. 结束。
Failed to login through SNMP, because the packet was too large. (Ip=[STRING], Times=[ULONG])	设备接收到的报文超过设备所设置的阈值。	1. 执行 **snmp-agent packet max-size** 命令增大报文阈值。 ● 如果日志继续打印，则=>b。 ● 否则=>c。 2. 请联系华为技术支持工程师。 3. 结束。
Failed to login through SNMP,because messages was failed to be added to the message list. (Ip=[STRING], Times=[ULONG])	消息列表积压。	请联系华为技术支持工程师。

日志	日志解释	处理建议
Failed to login through SNMP, because of the decoded PDU error. (Ip=[STRING], Times=[ULONG])	报文解码出现未知错误。	请联系华为技术支持工程师。
Failed to login through SNMP, because the community was incorrect. (Ip=[STRING], Times=[ULONG])	团体字配置错误。	1. 执行 **display snmp-agent community** 命令查看主机配置的团体字。 ● 如果网管发起请求时使用的团体字和主机配置的团体字相同，则=>c。 ● 否则=>b。 2. 执行 **snmp-agent community** 命令配置读写团体名，使之与网管端配置一致。 ● 问题解决，则=>d。 ● 否则=>c。 3. 请联系华为技术支持工程师。 4. 结束。
Failed to login through SNMP, because of the ACL filter function. (Ip=[STRING], Times=[ULONG])	该 IP 被 ACL 禁止。	1. 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，则=>b。 ● 否则=>c。 2. 执行 **rule** 命令配置允许网管端 IP 访问主机。 ● 问题解决，则=>d。 ● 否则=>c。 3. 请联系华为技术支持工程师。 4. 结束。
Failed to login through SNMP, because of the contextname was incorrect. (Ip=[STRING], Times=[ULONG])	登录请求所使用的 contextname 错误。	请联系华为技术支持工程师。

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

SNMP/4/ACL_FAILED
SNMP/4/AR_PAF_FAILED
SNMP/6/CNFM_VERSION_DISABLE
SNMP/4/COMMUNITY_ERR
SNMP/4/CONTEXTNAME_ERR
SNMP/4/DECODE_ERR
SNMP/4/INVAILDVERSION
SNMP/4/MSGTBL_ERR
SNMP/4/PACKET_TOOBIG
SNMP/4/PARSE_ERR
SNMP/4/SNMP_SET
SNMP/4/TRAP_SEND_ERR
SNMP/4/SHORT_VB

3.5.2 网管无法收到主机发送的告警的定位思路

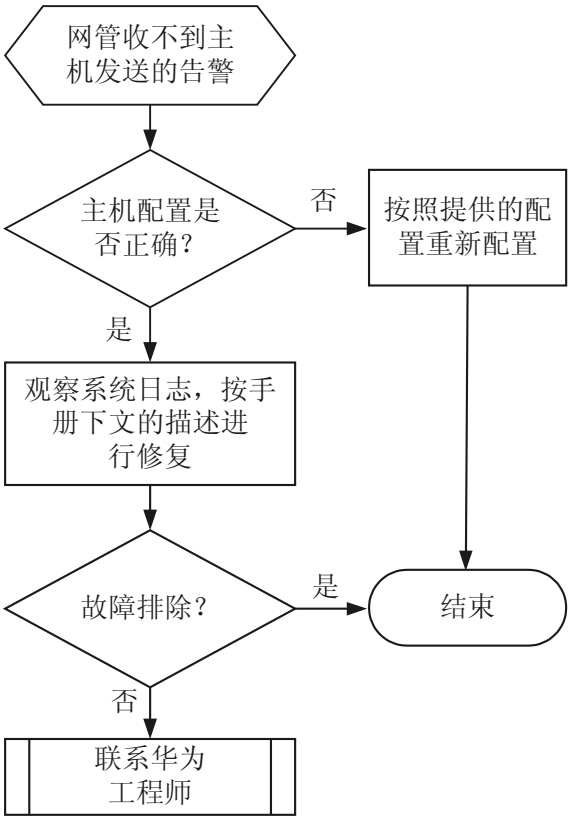
常见原因

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 3-8 网管收不到主机告警的诊断流程图



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 检查设备上告警主机的配置是否正确。

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

表 3-3 告警主机典型配置

配置例	命令行
配置一个版本为 SNMPv2c 的告警主机，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）	<Quidway> system-view [Quidway] snmp-agent target-host trap address udp-domain 192.168.1.1 params securityname huawei v2c
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（huawei 必须是一个确实存在的用户）	# 配置 MIB 视图。 <Quidway> system-view [Quidway] snmp-agent mib-view included Huawei_view iso # 配置用户组。 [Quidway] snmp-agent group v3 huawei_group read-view Huawei_view write-view Huawei_view notify-view Huawei_view # 配置用户。 [Quidway] snmp-agent usm-user v3 huawei huawei_group
配置一个版本为 V3 的告警主机，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）	<Quidway> system-view [Quidway] snmp-agent target-host trap address udp-domain 192.168.1.1 params securityname huawei v3

步骤 2 执行 **display snmp-agent trap all** 命令可以查看到所有特性下的告警的使能情况。

- 如果特性告警没有使能，则执行步骤 3。
- 如果特性告警已经使能，则执行步骤 4。

步骤 3 执行 **snmp-agent trap enable feature-name trap-name** 命令使能设备发送 Trap 报文，并设置 Trap 的相关参数。

- 如果网管能够收到主机发送的告警，则执行步骤 7。
- 否则执行步骤 4。

步骤 4 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，则执行步骤 6。
- 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，则执行步骤 5。

  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 Int erface 109 turned into DOWN state.

步骤 5 配置以 Inform 方式发送告警。

说明

由于 Trap 报文采用 UDP 报文承载发送，本身是一种不可靠的报文，所以可能在链路上丢失。华为提供 Inform 机制可以解决这个问题。具体的配置请参见《AC6605 配置指南-网络管理》的“SNMP 配置”。

- 如果网管能够收到主机发送的告警，则执行步骤 7。
- 否则执行步骤 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

相关告警与日志

相关告警

无

相关日志

无

3.6 RMON 故障处理

3.6.1 网管无法接收 RMON 告警信息的定位思路

常见原因

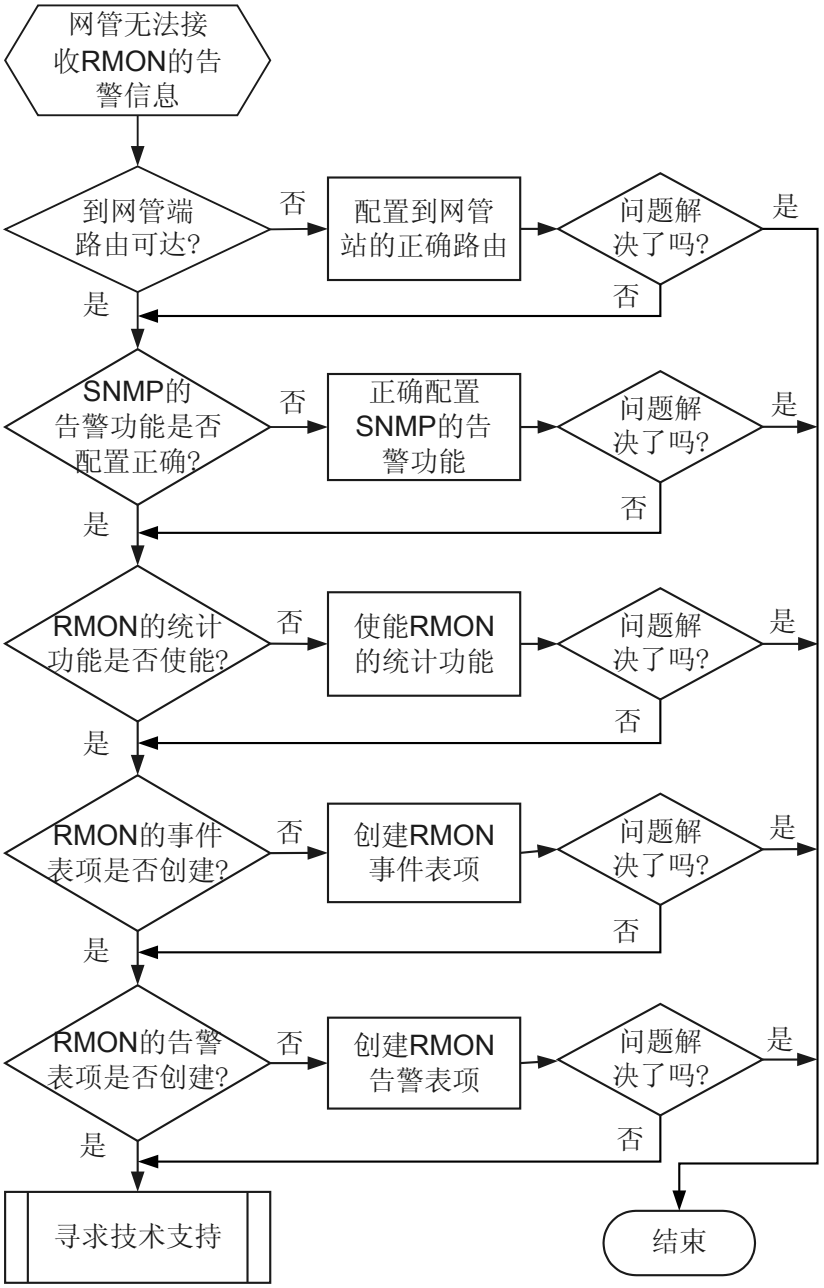
本类故障的常见原因主要包括：

- 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 3-9 所示。

图 3-9 网管无法接收 RMON 告警信息故障诊断流程图



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 检查交换机到网管端是否路由可达

在交换机端 Ping 网管端是否可以 Ping 通。

- 如果可以 Ping 通说明交换机和网管端的路由可达，则执行步骤 2。
- 如果 Ping 不通，请检测交换机和网管端的路由，请参见 **7.2.1 PING 不通故障处理思路**。

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 feature-name rmon all**，检查交换机的告警功能是否已经使能。
- 执行命令 **display snmp-agent target-host**，检查交换机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

在交换机端执行命令 **display rmon statistics** [**gigabitethernet** *interface-number*]，查看 RMON 进行监控的接口的统计功能是否使能。如果表中没有统计到任何的内容，请使用命令 **rmon-statistics enable** 在 RMON 监控的接口上使能 RMON 的统计功能。

步骤 4 检查是否配置了 RMON 统计表

在交换机端执行命令 **display rmon statistics** [**gigabitethernet** *interface-number*]，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

在交换机端执行命令 **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

在交换机端执行命令 **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

在交换机端执行命令 **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交换机端配置的一致，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交换机 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

相关告警与日志

相关告警

无

相关日志

无

3.7 NQA 故障处理

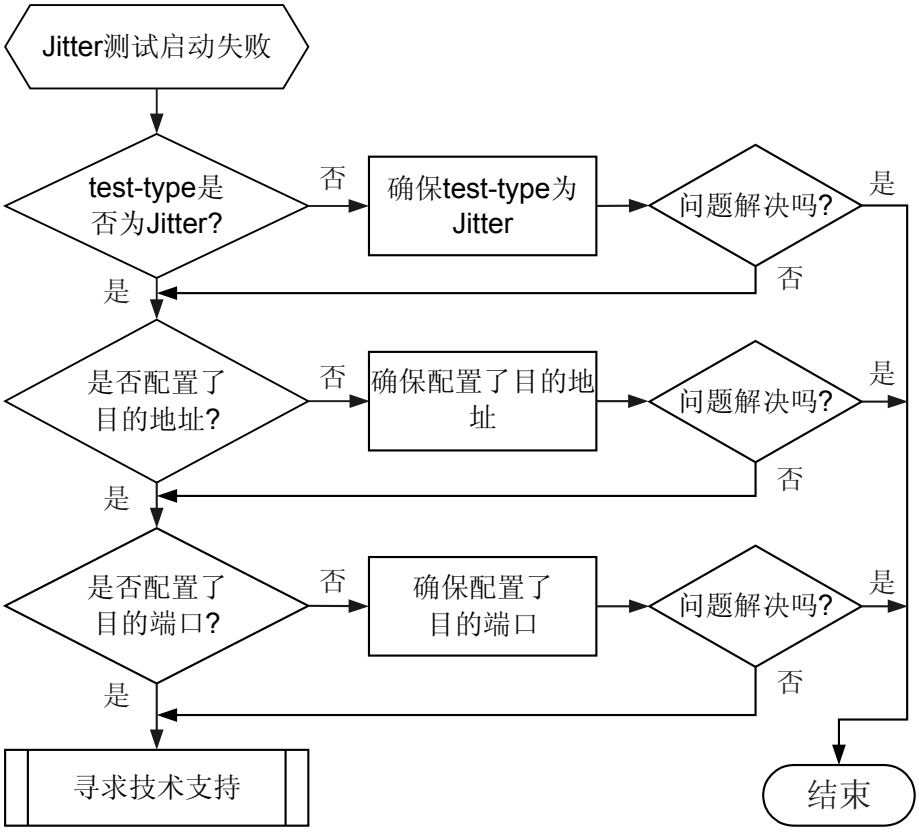
3.7.1 无法启动 UDP Jitter 测试的定位思路

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 3-10 UDP Jitter 测试无法启动故障诊断流程图



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，请执行步骤 5。
  - 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，请执行步骤 5。
  - 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，请执行步骤 5。
  - 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

3.7.2 UDP Jitter 测试结果有 drop 记录的定位思路

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。

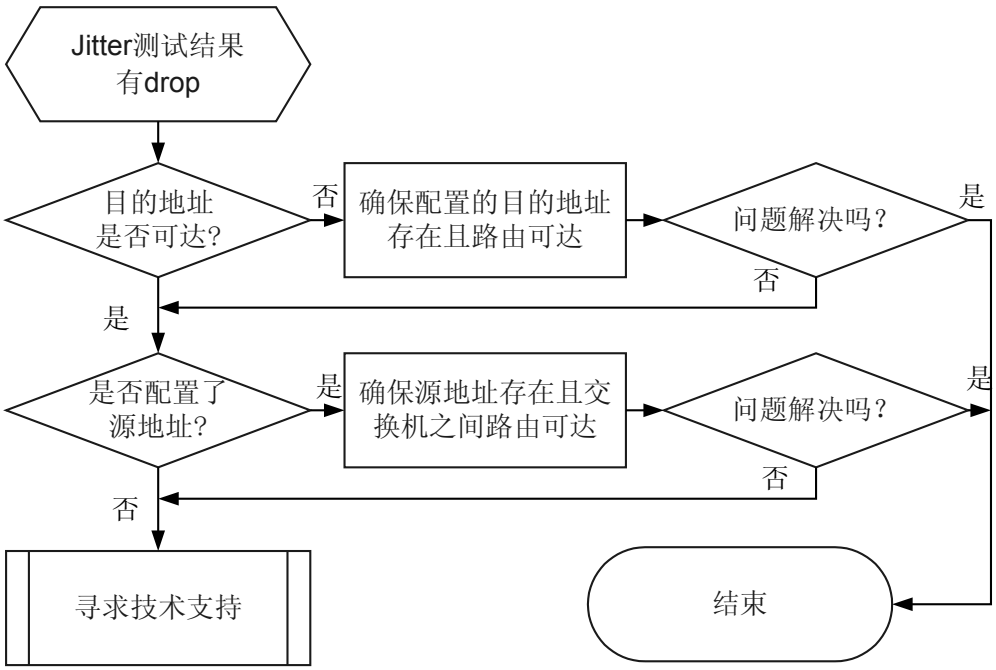
本类故障的常见原因是：

- 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 3-11 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 **7.2.1 PING 不通故障处理思路**。
- 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。

- 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 **7.2.1 PING 不通故障处理思路**。

- 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

3.7.3 UDP Jitter 测试结果有 busy 记录的定位思路

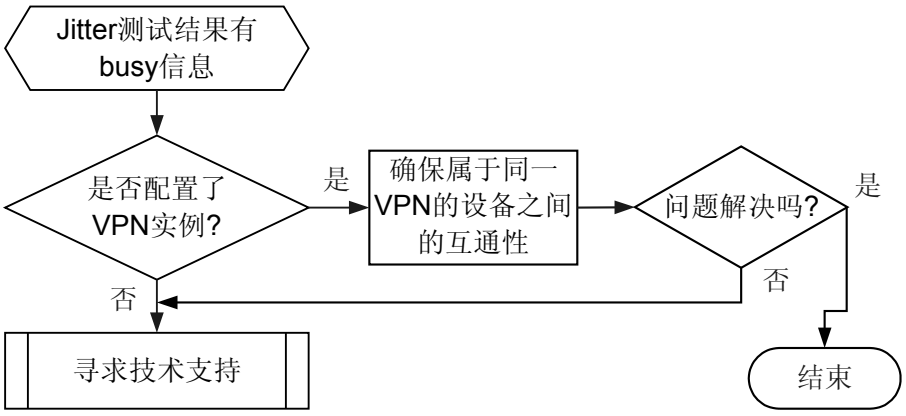
常见原因

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 3-12 UDP Jitter 测试结果有 busy 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 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 **7.2.1 PING 不通故障处理思路**。

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

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

常见原因

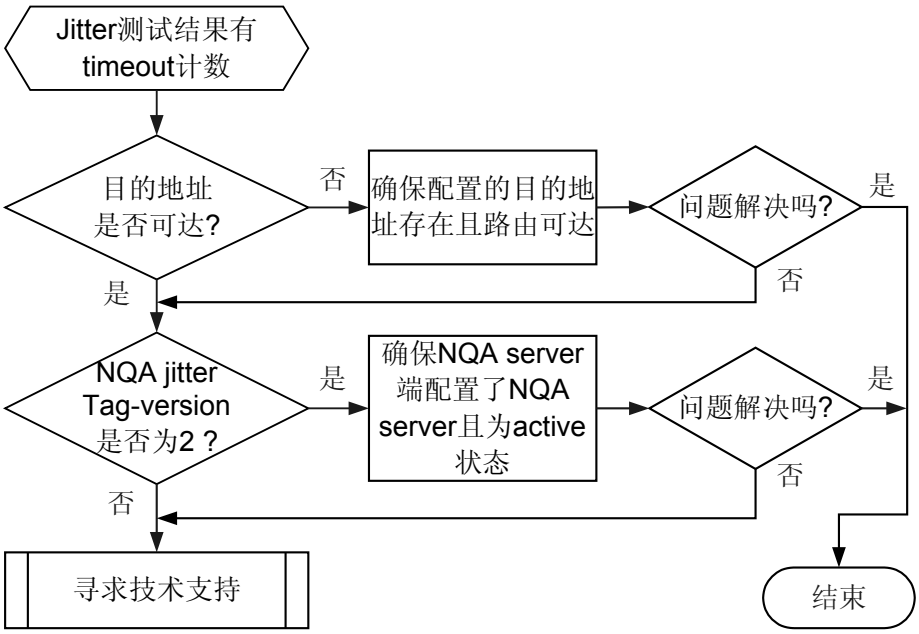
UDP Jitter 测试结果有 timeout 记录是指使用 **display nqa results** 命令查看 NQA 测试的结果统计时，显示信息中“Operation timeout number”字段的值不是 0。

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

故障诊断流程

图 3-13 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 **7.2.1 PING 不通故障处理思路**。

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。

- 如果问题解决，请执行步骤 5。
- 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

3.7.5 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：

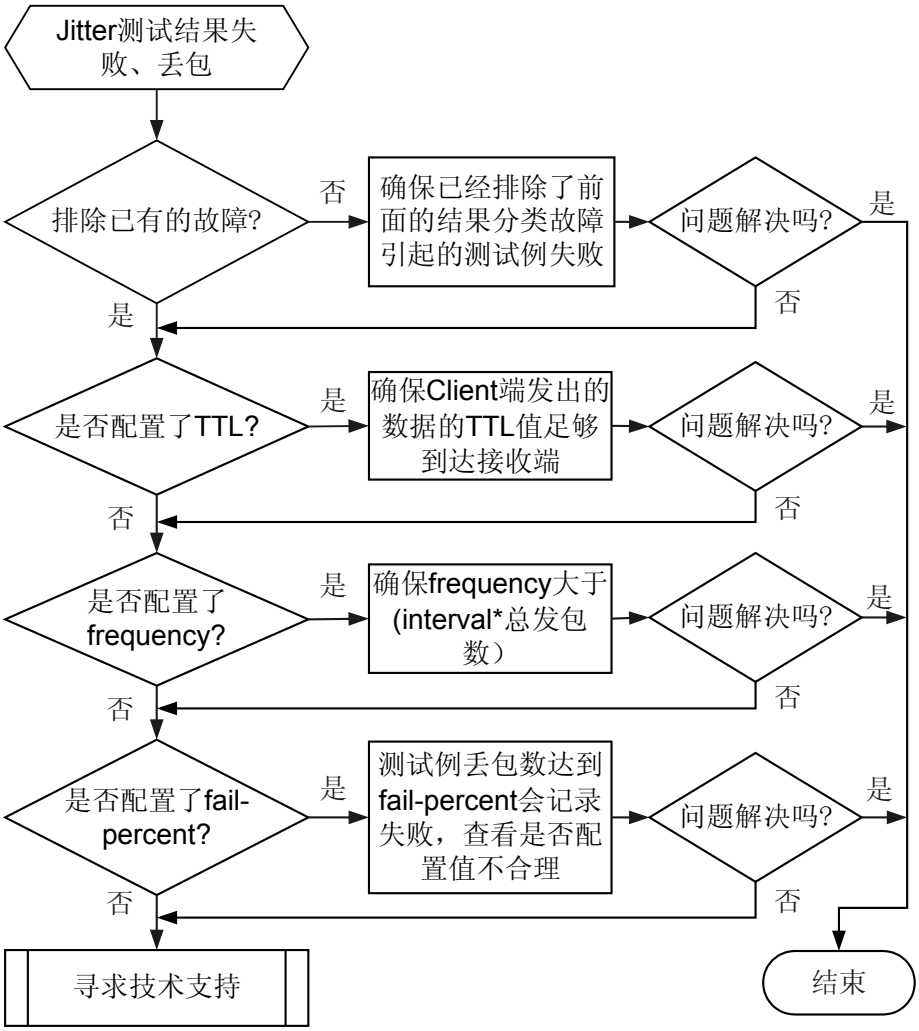
- 如果显示信息中“Completion”字段的值为“failed”，说明测试结果失败。
- 显示信息中“Completion”字段的值为“no result”，说明测试没有得到结果。
- 显示信息中“Lost packet ratio”字段的值不是 0%，说明有丢包。

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 timeout 计数
- TTL 超时
- frequency 配置错误
- fail-percent 配置错误

故障诊断流程

图 3-14 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** *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

3.8 NTP 故障诊断思路

3.8.1 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。

```
<Quidway> 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
 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。

```
<Quidway> display ntp-service sessions
        source          reference       stra reach poll  now offset delay disper
******************************************************************************
     [5] 20.1.14.1       0.0.0.0          16     0   64    -      -    0.0     0.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured,
      6 vpn-instance
```

“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：

```
<Quidway> 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 **7.2.1 PING 不通故障处理思路**继续定位问题。
- 如果不是 100.00%，说明链路震荡，请参见 **7.2.1 PING 不通故障处理思路**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

3.9 HGMP 故障处理

3.9.1 直连链路下 HGMP 成员无法加入集群的定位思路

常见原因

两台交换机直连，在其中一台交换机上建立集群，将另外一台交换机加入该集群时，加入不成功，在命令交换机上没有任何提示信息。

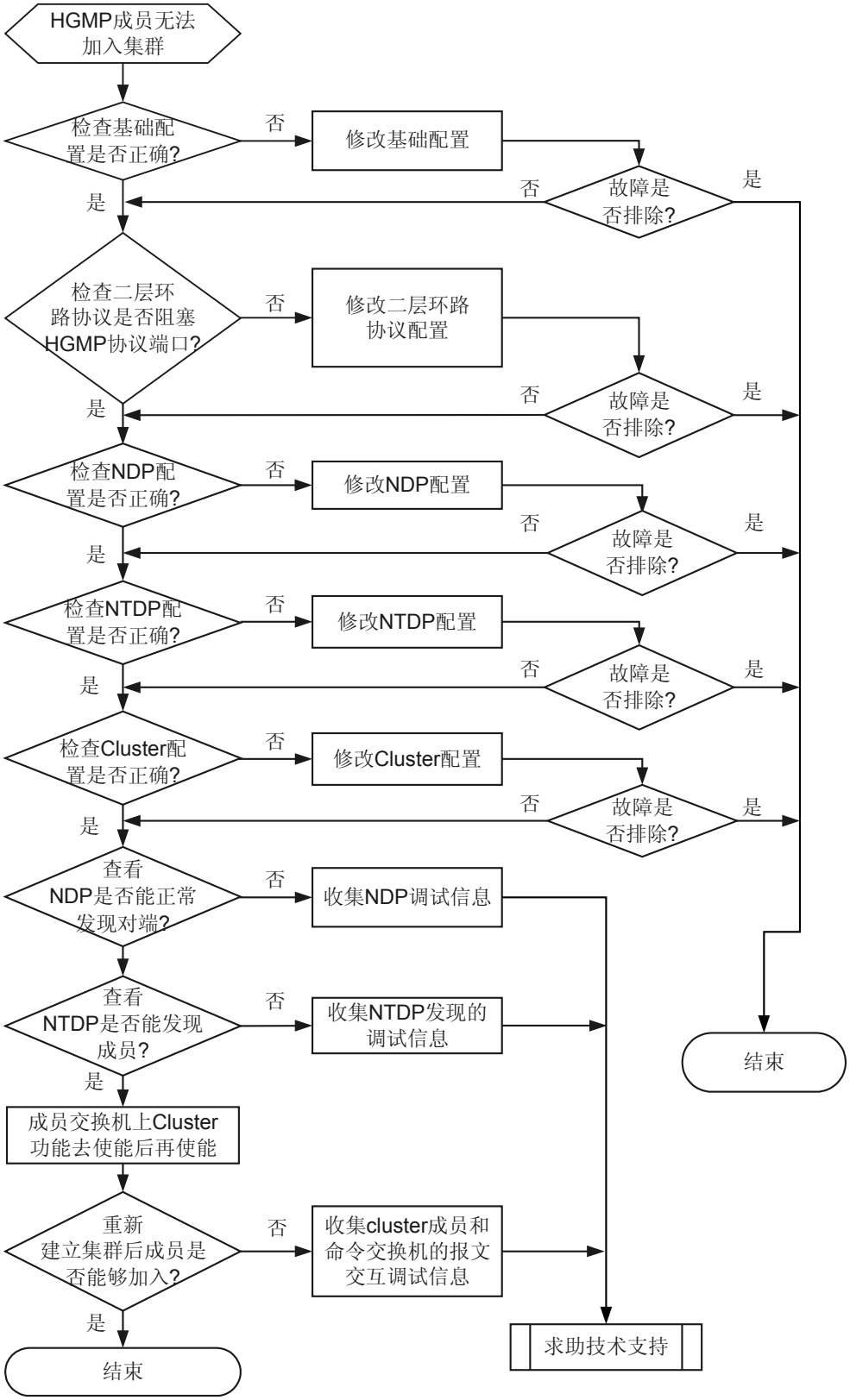
本类故障的常见原因主要包括：

- 接口 Down 导致集群命令交换机和候选交换机之间的报文不通。
- 网络二层转发的基本配置不正确。
- 二层报文转发、透明传输故障。
- 报文经过的接口被环路协议阻塞，导致命令和成员之间的集群报文不通。
- Cluster/NDP/NTDP 配置不正确。
- 成员交换机之前已经加入过集群，且没有退出，并且新的集群名称和原集群名称不同。
- 集群成员和命令交换机的 Super Password 不一致，导致认证失败。

故障诊断流程

可按照图 3-15 排除此类故障。

图 3-15 直连链路下 HGMP 成员无法加入集群故障诊断流程图



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 检查命令交换机和候选交换机基础配置。

HGMP 集群报文交互是建立在二层网络互通的基础上，所以必须采用正确的配置来保证交换机的二层报文能够正常收发。

请确认两交换机已经按照如下方法配置：

- 直连的两个端口都加入了相同的 VLAN。
- 该 VLAN 同时也是集群的管理 VLAN，即 Cluster 视图下配置的命令 **mngvlanid** *vlan-id*，并且该 *vlan-id* 是在端口加入的 VLAN 范围内。
- 端口都以相同的方式加入 VLAN（例如两端都配置为 **port trunk allow-pass vlan** *vlan-id*）。

如果该部分配置正确，请分别在命令交换机和候选交换机上执行命令 **display vlan** *vlan-id* 查看 VLAN 中直连的端口状态是否为 Up。示例如下：

```
[Quidway] display vlan 1000
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------
1000   common  TG:GE0/0/1(U)

VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
1000   enable  default       enable  disable    VLAN 01000
```

- 如果端口没有 Up，则物理链路可能有问题，请排除物理链路故障。
- 如果端口已经 Up，则二层网络正常，可能是集群配置或报文上层处理存在问题。请执行**步骤 2**。

步骤 2 检查命令交换机和候选交换机端口的二层环路协议状态是否正常。

- 若命令交换机和候选交换机上配置了 STP 协议，需检查运行 HGMP 协议端口是否被 STP 阻塞。执行命令 **display stp brief** 查看端口状态，例如：

```
[Quidway] display stp brief
 MSTID      Port                Role  STP State     Protection
   0        GigabitEthernet0/0/1  ROOT  FORWARDING     NONE
   0        GigabitEthernet0/0/2  DESI  FORWARDING     NONE
   0        GigabitEthernet0/0/3  DESI  FORWARDING     NONE
```

转发正常情况下，运行 HGMP 协议的直连端口的 STP state 字段为 **FORWARDING**。若该字段为 **DISCARDING**，则说明 NTDP 协议报文被 STP 阻塞。此时需要修改 STP 配置使该端口不处在 **DISCARDING** 状态，可修改 STP 的优先级使本交换机的选举为根桥，使端口不被阻塞。全局视图下使用命令 **stp priority** *priority-level*，*priority-level* 范围是 0-61440，取值越小则优先级越高，选择较低的优先级可使本设备成为环路的根桥。

若运行 HGMP 协议的端口显示的状态都为 **FORWARDING** 状态，说明端口的 STP 状态正常。

- 若命令交换机和候选交换机上配置了 RRPP 协议，需检查运行 HGMP 协议的直连端口是否被 RRPP 阻塞。执行命令 **display rrpp verbose domain** *domain-index* 查看端口状态，例如：

```
[Quidway] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 1000    sub 1001
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring      : 1
Ring Level     : 0
Node Mode      : Master
Ring State     : Failed
Is Enabled     : Enable         Is Actived : Yes
Primary port   : GigabitEthernet0/0/3         Port status: UP
Secondary port : GigabitEthernet0/0/4         Port status: DOWN
```

  若运行 HGMP 协议的直连的端口的 Port status 字段为 **BLOCK**，则说明该端口上的集群协议报文已被 RRPP 阻塞。此时需要修改 RRPP 配置使该端口不处在 BLOCK 状态。RRPP 协议阻塞的是副端口（Secondary port），所以需要重新规划修改配置，不要将该端口配置成 RRPP 协议的副端口。

  若运行 HGMP 协议的直连的端口的 Port status 字段都为 **Up**，则说明端口的 RRPP 状态正常，请执行**步骤 3**。

  说明

  一般在同一端口上不会配置两种环路协议，所以先看端口目前配置了哪种协议类型，再查看对应的端口状态。

步骤 3 检查 NDP 基本功能是否正常。

分别在命令交换机和候选交换机上执行 **display ndp** 命令，查看 NDP 协议是否能够成功发现邻居。正常情况会在 NDP 显示信息里看到直连的邻居信息，例如：

```
<Quidway> display ndp
 Neighbor discovery protocol is enabled.
 Neighbor Discovery Protocol Ver: 1, Hello Timer: 60(s), Aging Timer: 180(s)
 Interface: GigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 114, Packets Received: 108, Packets Error: 0
    Neighbor 1:  Aging Time: 174(s)
       MAC Address : 0018-8203-39d8
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.70 V100R005C00SPC001
       Device Name : Quidway
       Port Duplex : FULL
       Product Ver : AC6605
```

如果 NDP 不能发现邻居信息，请检查 NDP 已按照如下方法配置：

- 两交换机上 NDP 都已全局使能，即全局视图下出现 **ndp enable** 配置。
- 两直连端口的接口下 NDP 都已经使能，即接口视图下出现 **ndp enable** 配置。

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。

如果配置正确，但 NDP 还无法发现邻居，则需要采集下面调试信息，联系华为技术支持工程师，请执行**步骤 6**。

- 打开监视开关，在用户视图下执行命令 **terminal monitor** 和 **terminal debugging**。
- 打开 NDP 调试开关，在用户视图下执行命令 **debugging ndp packet interface** *interface-type interface-number*，等待 3 分钟，获取屏幕信息。

如果 NDP 能正常发现邻居信息，请执行**步骤 4**。

步骤 4 检查 NTDP 基本功能是否正常。

请检查 NTDP 是否已按照如下方法配置：

- 两交换机上 NTDP 都已全局使能，即全局视图下出现 **ntdp enable** 配置。
- 两直连端口的接口下 NTDP 都已经使能，即接口视图下出现 **ntdp enable** 配置。
- Cluster 视图下配置了集群管理 VLAN，即 Cluster 视图下出现 **mngvlanid** *vlan-id* 配置，且 *vlan-id* 在接口加入的 VLAN 范围内。

如果配置不正确，请修改成正确配置。

如果配置正确，分别在命令交换机和候选交换机上，在用户视图下执行命令 **ntdp explore** 进行拓扑发现，等待 5 秒，然后执行命令 **display ntdp device-list** 命令查看 NTDP 协议是否能够发现网络拓扑。正常情况会在 NTDP 显示信息里可以看到直连的邻居信息，例如：

```
[Quidway] display ntdp device-list
The device-list of NTDP:
--------------------------------------------------------------------------------
 MAC             HOP  IP                  PLATFORM

--------------------------------------------------------------------------------
 001c-2334-2312  1    1.1.1.2/24          AC6605
 0018-82af-fc38  0    1.1.1.1/24          AC6605
```

如果 NTDP 没有显示出网络拓扑信息，则需要分别采集两台交换机的调试信息，联系华为技术支持工程师，请执行**步骤 6**。

- 打开监视开关，在用户视图下执行命令 **terminal monitor** 和 **terminal debugging**。
- 打开 NTDP 调试开关，在用户视图下执行命令 **debugging ntdp all**
- 再次发起拓扑发现功能，执行命令 **ntdp explore** 和 **display ntdp device-list**，采集打印的信息。

如果 NTDP 显示了正常的网络拓扑信息，则执行**步骤 5**。

说明

- 集群成员加入依赖于命令交换机 NTDP 搜集到的网络拓扑信息，NTDP 成功发现成员是成员加入集群的必要不充分条件。
- 因 NDP 报文接收后不会继续在网络上转发，NDP 报文不会被环路协议阻塞。而 NTDP 报文可以在网络上转发，所以可以被阻塞。

步骤 5 检查 Cluster 基本功能是否正常。

请检查 Cluster 是否已按照如下方法配置：

- 两交换机上 Cluster 功能都已全局使能，即全局视图下出现 **cluster enable** 配置。
- 两交换机上都已创建了管理 VLAN 的 Vlanif 接口，即全局视图下出现 **interface Vlanif** *vlan-id* 配置，*vlan-id* 和 Cluster 视图下的 **mngvlanid** 配置中的 *vlan-id* 一致。
- 命令交换机上配置可用的 ip-pool，即 Cluster 视图下出现 **ip-pool** *administrator-ip-address mask* 配置。
- 管理 Vlanif 接口手动配置的 IP 地址不能在 **ip-pool** 网段内。

- 命令交换机和候选交换机都没有配置 Super Password 或配置相同。

如果配置不正确，请修改成正确配置。

如果配置正确，则先在候选交换机上去使能 Cluster 功能，执行命令 **undo cluster enable**，再执行命令 **cluster enable**，排除成员曾经加入过集群遗留的影响。再在命令交换机上清除原有的集群，再重新创建集群，看是否能够成功加入成员：

- 撤销原来的集群，Cluster 视图下执行命令 **undo build**。
- 重新创建集群，执行命令 **auto-build**。

如果此时还不能成功搜集到成员信息，则需要分别采集两台交换机的调试信息，联系华为技术支持工程师，请执行**步骤 6**。

- 打开监视开关，在用户视图下执行命令 **terminal monitor** 和 **terminal debugging**。
- 打开 Cluster 调试开关，在用户视图下执行命令 **debugging cluster all**
- 手动将集群成员加入，即在 Cluster 视图下执行命令 **add-member mac-address** *mac-address*。等待 10 秒钟后获取两设备的屏幕信息，并联系华为技术支持工程师。

如果能够成功搜集到成员信息，则可加入集群，问题解决。

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

HGMP/4/ClstMemStusChg:OID:[oid],DeviceID:[string], Role:[integer].

相关日志

无

3.10 LLDP 故障处理

介绍了 LLDP 常见故障的定位思路。

3.10.1 端口不能发现邻居的定位思路

介绍端口不能发现邻居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：

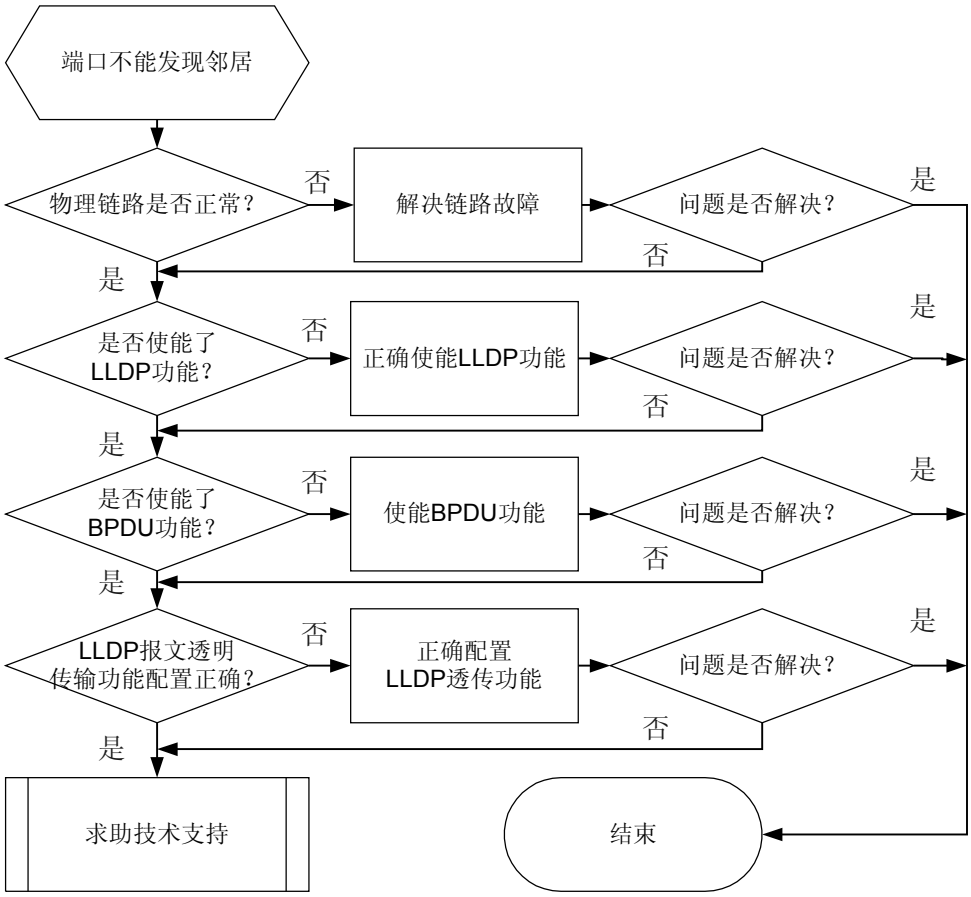
- 物理链路故障
- 未正确使能 LLDP 功能

- 端口下 LLDP 报文透明传输功能配置错误

故障诊断流程

详细处理流程如图 3-16 所示。

图 3-16 端口不能发现邻居故障诊断流程图



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。

在设备上执行命令 **display lldp neighbor brief** 发现没有邻居，请参照以下的步骤进行处理。

操作步骤

步骤 1 检查设备间物理链路是否故障。

执行 **display interface** *interface-type interface-number* 命令查看 **current state** 字段值。

- 如果为 DOWN，说明链路故障，请先解决链路故障。
- 如果为 UP，说明链路正常，请执行步骤 2。

步骤 2 检查 LLDP 功能是否使能。

缺省情况下，在使能全局 LLDP 功能的情况下，所有端口都处于使能 LLDP 功能的状态。当部分端口需要禁用 LLDP 功能时，执行 **undo lldp enable** 命令。

1. 检查是否全局使能了 LLDP 功能。

   执行 **display current-configuration** 命令查看显示信息中是否存在 **lldp enable**。

   - 如果否，请在系统视图下执行 **lldp enable** 使能全局 LLDP 功能。
   - 如果是，请执行步骤 b。

2. 检查端口下是否禁用了 LLDP 功能。

   在接口视图下执行 **display this**，查看显示信息中是否存在 **undo lldp enable**。

   - 如果是，请在接口视图下执行 **lldp enable** 使能 LLDP 功能。
   - 如果否，请执行步骤 3。

步骤 3 检查端口下 LLDP 透明传输功能配置是否正确。

缺省情况下，端口的 LLDP 透明传输功能是禁止的。可以在接口视图下执行 **display this** 查看是否配置了 LLDP 透明传输。如果显示信息中存在 **l2protocol-tunnel lldp enable**，则表示端口下配置了 LLDP 透明传输功能。

- 单邻居组网中，使能 LLDP 功能的设备上必须禁用 LLDP 的透明传输功能，否则端口将不能发现邻居。
- 多邻居组网中，使能 LLDP 功能的设备上需要禁用 LLDP 的透明传输功能，但中间网络的设备上必须使能 LLDP 的透明传输功能，否则端口也不能发现邻居。
  - 在接口视图下执行命令 **l2protocol-tunnel lldp enable** 配置 LLDP 透明传输。
  - 在接口视图下执行命令 **l2protocol-tunnel lldp disable** 取消 LLDP 透明传输。
- 如果配置不正确，请修改配置。
- 如果配置正确，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

相关告警与日志

相关告警

无

相关日志

无

3.11 NAP 远程开局故障处理

3.11.1 无法使用 NAP 功能登录到新开局的设备

常见原因

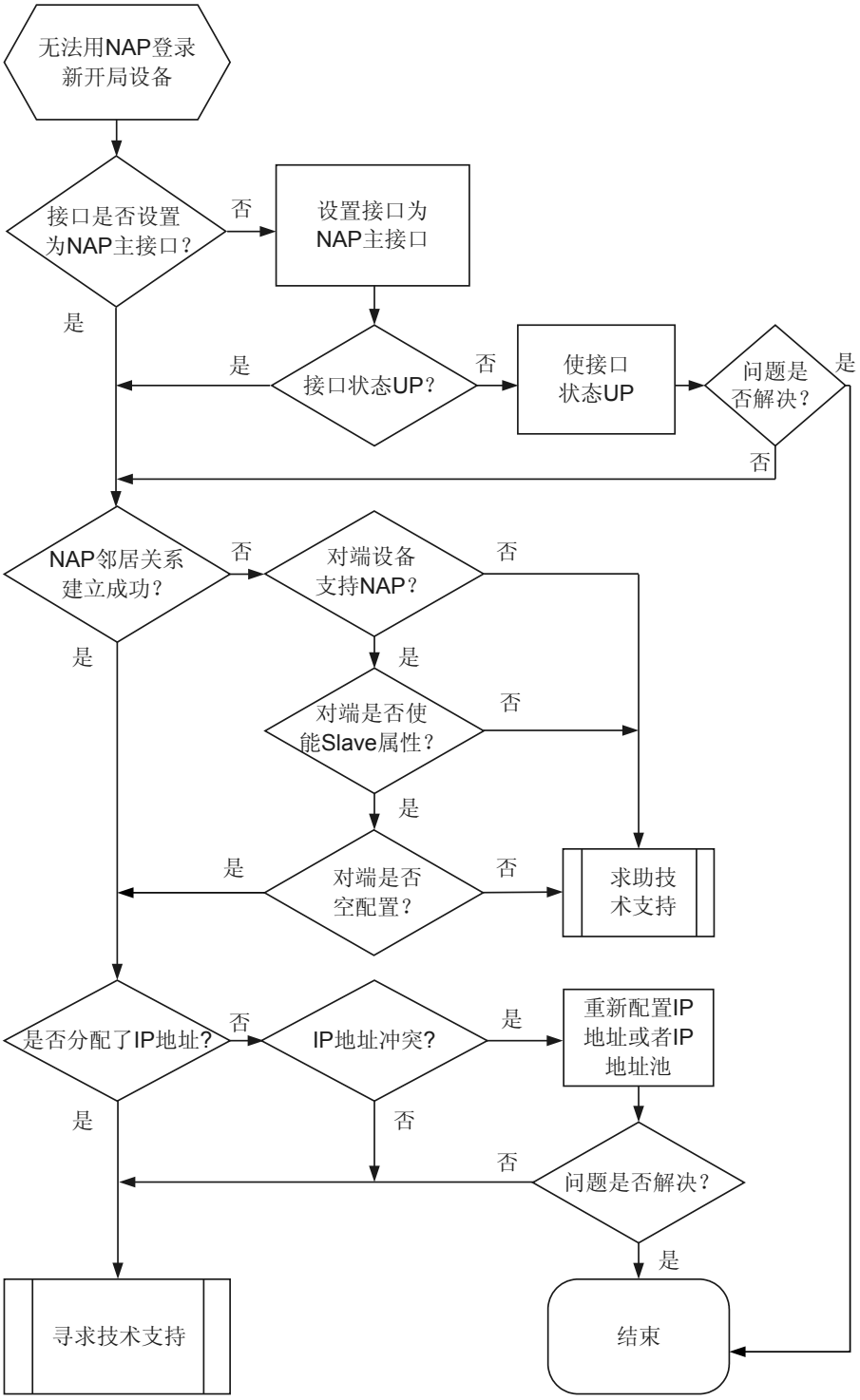
本类故障的常见原因主要包括：

- 本地设备 NAP 配置不正确。
- 主设备与从设备物理连接未建立或者连接不稳定

故障诊断流程

详细的处理流程如图 3-17 所示。

图 3-17 无法通过现网设备 NAP 登录到对端新开局设备的故障诊断流程图



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。
- 处理本故障时，请确保登录的新设备支持 NAP 协议且是空配置设备。

  如果无法确定登录的设备是否是空配置设备，请本地技术支持工程师先检查设备以确保是空配置设备。

操作步骤

步骤 1 检查当前接口是否为 NAP 主接口。

在任意视图下执行命令 **display nap interface**，查看 **Port property** 字段。

- 如果 **Port property** 字段显示是 Master，请执行步骤 2。
- 如果 **Port property** 字段显示不是 Master，请在需要设置为 NAP 主接口对应的接口视图下执行命令 **nap port master**，设置当前接口为 NAP 主接口。

  如果当前接口无法配置 **nap port master** 命令，表示当前接口不支持 NAP，请选择其它类型的接口作为 NAP 主接口。

  说明

  NAP 当前支持 GigabitEthernet 接口。

步骤 2 检查主接口的当前状态是否是 DETECTING 状态。

在任意视图下执行命令 **display nap interface**，查看 **Current status** 字段。

- 如果 **Current status** 字段显示是 DETECTING，请执行命令 **display interface** 查看主接口的当前状态。
  - 如果主接口的当前状态是 Down，请确认是否已经完成与新开局设备的物理连接，以及确认是否使用当前主接口进行 NAP 连接。
  - 如果主接口的当前状态是 Up，请执行步骤 4。
- 如果 **Current status** 字段显示不是 DETECTING，请执行步骤 3。

步骤 3 检查 NAP 邻居是否已经协商到 IP 地址

在任意视图下执行命令 **display nap interface**，查看 **Current status** 字段。

- 如果 **Current status** 字段显示是 Established，且主从接口的 IP 地址不断变化，则说明 IP 地址池中分配的 IP 地址冲突。请执行如下步骤：
  - 如果没有其他主接口，请在系统视图下执行命令 **nap ip-pool**，手工配置 IP 地址池。
  - 如果有其他主接口，请在当前主接口视图下执行命令 **nap local-ip** *mast-inter-mast-ip* **sub-ip** *mast-inter-sub-ip* **peer-ip** *sub-inter-mast-ip* **sub-ip** *sub-inter-sub-ip mask-length*，手工配置 NAP 主从接口的主从 IP 地址。
- 如果 **Current status** 字段显示是 IP-ASSIGNED，说明 IP 地址已分配，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

NAP/4/NAP_STATUSCHANGE:OID 1.3.6.1.4.1.2011.5.25.206.3.1 Index [integer], the status of the nap port [octet] has changed to [integer], and the AbnormalReason is [integer].

相关日志

NAP/6/GOTONEIGHBOR:Connected to the device on the slave interface end through the main interface[STRING].

4 物理对接及接口类

关于本章

4.1 以太网接口故障处理
介绍了以太网接口常见故障的定位思路和案例。

4.2 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。

4.1 以太网接口故障处理

介绍了以太网接口常见故障的定位思路和案例。

4.1.1 以太网接口物理 Down 的定位思路

介绍当两端设备的以太网接口连接好之后物理层状态不能 Up 时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：

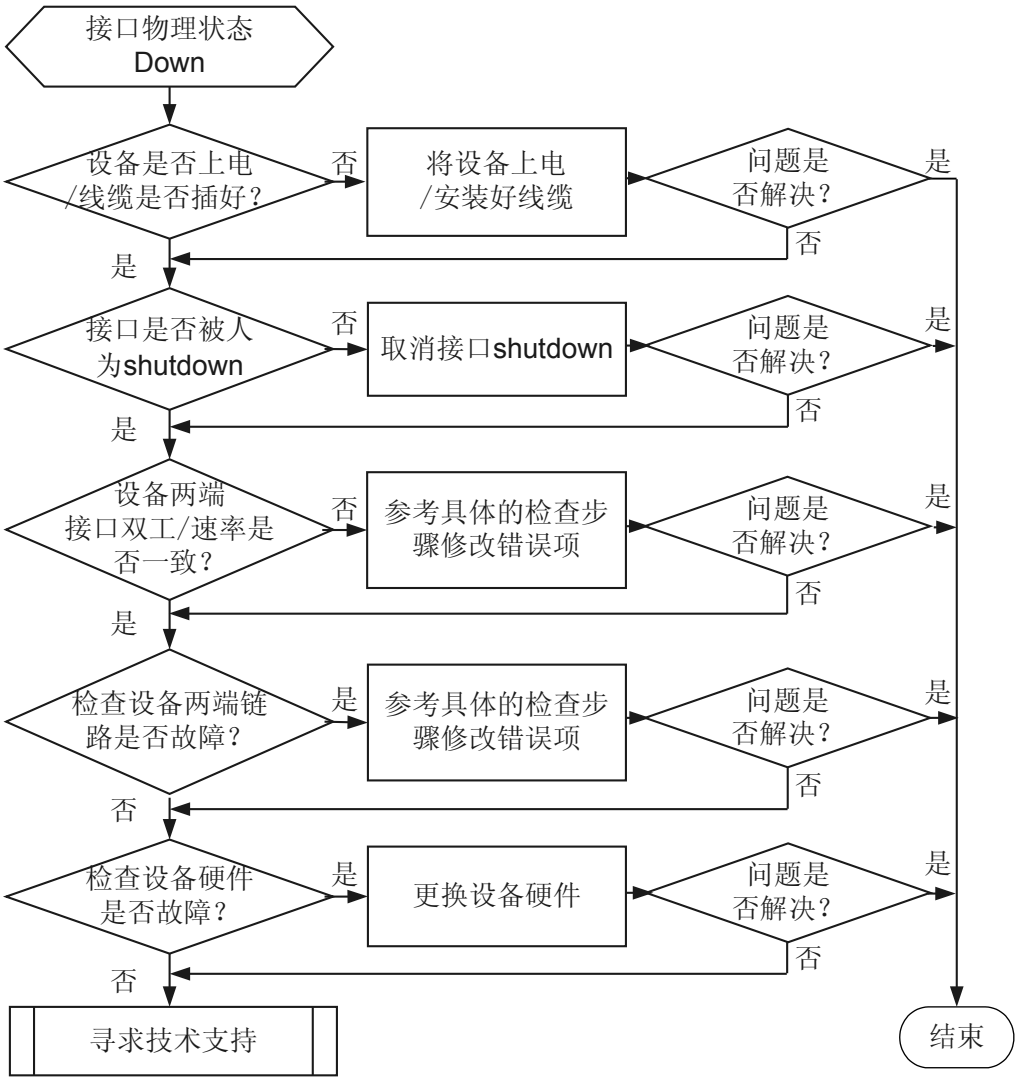
- 设备没有上电、线缆没有连接好。
- 接口被人为的 shutdown。
- 双绞线、光纤过长或链路损耗太大。
- 接口双工、速率协商模式不一致。
- 接口、接口模块或设备故障。

故障诊断流程

在线缆和设备连接好之后接口物理状态处于 Down。

详细处理流程如图 4-1 所示。

图 4-1 以太网接口物理 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 检查本端和对端设备是否上电，设备线缆、模块是否插好。

设备上电并且线缆连接好之后，如果接口的状态仍然 Down，请执行步骤 2。

步骤 2 检查本端和对端设备接口是否被人为 **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。

说明

如果设备上部署了 Monitor Link，若从 Monitor Link 组中删除上行接口或者组中已存在 Up 状态的上行接口变为 Down 状态，则所有下行接口均被 shutdown，如果是上行接口变为 Down 状态导致下行接口 Down，请先排除上行接口 Down 故障。

如果接口的状态仍然 Down，请执行步骤 3。

步骤 3 检查设备两端接口双工、速率、协商模式是否一致。

分别在设备两端执行 **display interface** 命令查看接口的双工、速率、协商模式信息。

检查项	显示信息解释说明	后续操作
Negotiation:	接口自协商状态。 ● 显示信息是“ENABLE”表示接口工作在自协商状态下。 ● 显示信息是“DISABLE”表示接口工作在非自协商状态下。	保持两边的协商模式一致，要么都工作在自协商模式下，要么都工作在非自协商模式下。在接口视图下可以使用 **negotiation auto** 命令调整接口的自协商模式。如果自协商模式下接口仍然频繁 Down，可以尝试将接口改成非自协商模式，强制两边速率、双工一致。
Speed :	接口当前速度。	在非自协商模式下如果设备两端接口速率不一致，请在接口视图下执行 **speed** 命令调整接口速率一致。
Duplex:	接口双工状态。	在非自协商模式下如果设备两端接口双工不一致，请在接口视图下执行 **duplex** 命令调整接口速率一致。
Mdi:	接口的网线适应方式。 ● across：表示接口的网线适应方式为交叉网线。 ● auto：表示接口的网线适应方式为自动识别网线。即与该接口实际连接的网线类型既可以使用直通网线也可以使用交叉网线。 ● normal：表示接口的网线适应方式为直通网线。	保证两端设备接口的网线适应方式和网线类型一致，缺省情况下网线适应方式为 auto 模式，如果接口网线适应方式为非 auto 模式建议使用 **mdi** 命令更改为 auto 模式。

执行上述步骤后，如果接口的状态仍然 Down，请执行步骤 4。

步骤 4 检查设备两端链路、接口模块是否故障。

设备之间是通过双绞线连接，需要做如下检查：

检查项	检查标准	后续操作
用测试仪测试双绞线是否故障。	测试仪显示双绞线正常。	如果检查出线缆故障，请更换线缆。
设备间双绞线长度是否满足要求。	设备间线缆长度<100m。 **说明** 10/100/1000M 电接口采用 RJ-45 连接器，接口线缆为 5 类或 5 类以上双绞线，传输距离 100m。	如果线缆长度大于 100m 可以采用如下方式： ● 缩短设备间距离，以缩短双绞线长度。 ● 如果不能改变设备间的距离，设备之间可以通过中继器、HUB 或交换机串联。
检查双绞线线序类型是否正确。	直通网线用来连接以下设备之间的以太网接口： ● 路由器和集线器 ● 路由器和以太网交换机 ● 计算机和以太网交换机 ● 计算机和集线器 交叉网线用来连接以下设备之间的以太网接口： ● 路由器和路由器 ● 路由器和计算机 ● 集线器和集线器 ● 集线器和交换机 ● 交换机和交换机 ● 计算机和计算机	如果双绞线类型选择错误请选择正确类型的双绞线。
检查两边的电口模块是否正常。	电口模块正常。	尝试更换两端电口模块。

如果设备之间是通过光纤连接，需要做如下检查：

检查项	检查标准	后续操作
检查光模块和光纤的对应关系。	检查光纤类型是否正确，光模类型和光纤类型对应关系请参见硬件描述手册“光模块属性速查表”。	如果对应关系不正确，请根据实际情况选择更换光模块或光纤。
设备间光纤的长度和光模块支持的传输距离是否匹配。	光纤的长度小于光模块支持的传输距离。光模块支持光纤的传输距离请参见硬件描述手册“光模块属性速查表”。	根据现网实际情况缩短光纤长度或者更换支持更大传输距离的光模块。
用测试仪测试信号的衰减在允许的范围内。	光信号的衰减范围请参见硬件描述手册“光模块属性速查表”。	如果衰减过大请更换光纤，如果更换光纤仍不符合衰减要求，或缩短光纤的长度。

检查项	检查标准	后续操作
用测试仪或物理环回方法检查链路光纤链路两端是否故障。	使用测试仪测试时，测试仪显示收发正常。 使用物理环回时，可以看到接口 Up。	如果检查出线缆故障，请尝试更换线缆，如果更换线缆故障依然存在请尝试更换两端接口光模块。

执行上述步骤后，如果接口的状态仍然 Down，请执行步骤 5。

步骤 5 检查本端和对端设备硬件是否故障。

尝试将线缆连接到其他接口，如果故障仍然存在请执行步骤 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

4.1.2 以太网接口频繁 Up/Down 的故障定位思路

介绍以太网接口频繁 Up/Down 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：

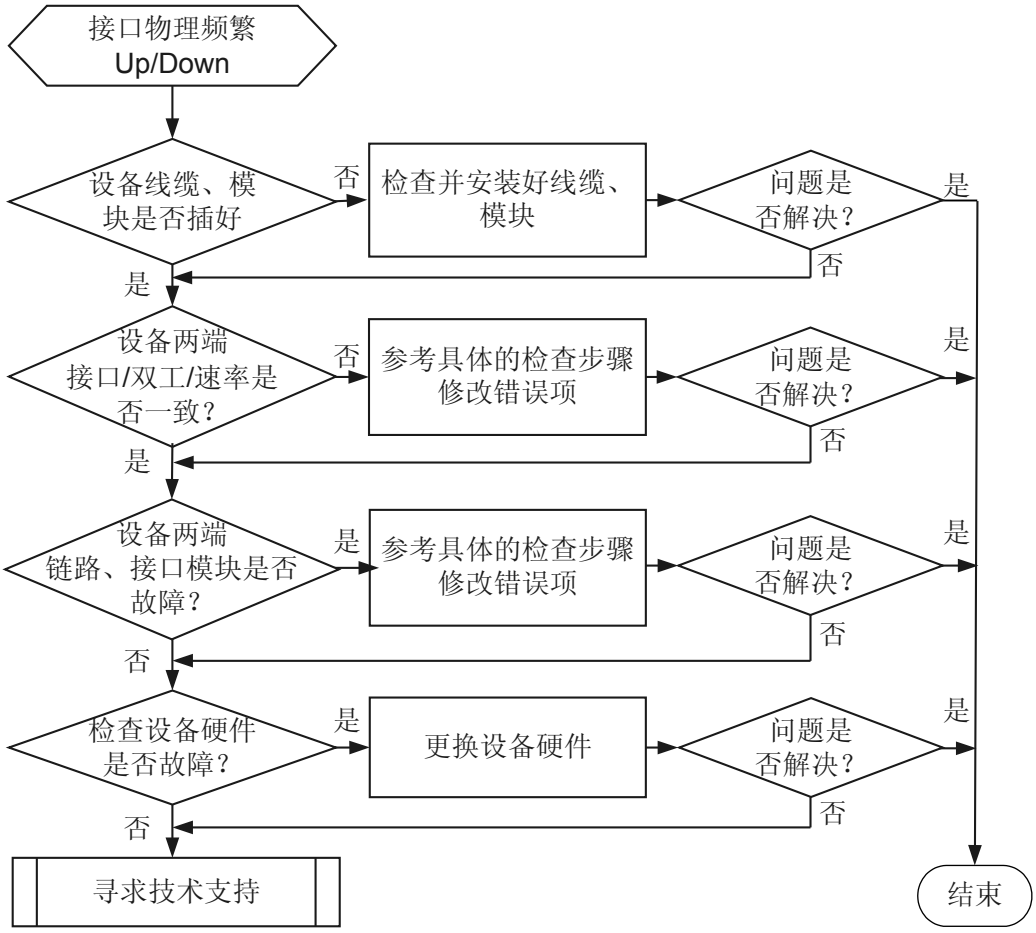
- 线缆没有连接好。
- 双绞线过长、光纤超长或链路损耗太大。
- 接口双工、速率协商模式不一致。
- 接口、接口模块或设备故障。

故障诊断流程

在线缆和设备连接好之后，在设备上看到接口频繁 Up/Down 的告警信息。

详细处理流程如图 4-2 所示。

图 4-2 以太网接口频繁 Up/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 检查本端和对端设备线缆、模块是否插好。

线缆、模块都安装好之后如果接口的仍然频繁 Up/Down，请执行**步骤 2**。

步骤 2 检查设备两端接口双工、速率、协商模式是否一致。

分别在设备两端执行 **display interface** 命令查看接口的双工、速率、协商模式信息。

检查项	显示信息解释说明	后续操作
Negotiation:	表示接口自协商状态。 ● 显示信息是“ENABLE”表示接口工作在自协商状态下。 ● 显示信息是“DISABLE”表示接口工作在非自协商状态下。	保持两边的协商模式一致，要么都工作在自协商模式下，要么都工作在非自协商模式下。在接口视图下可以使用 **negotiation auto** 命令调整接口的自协商模式。如果自协商模式下接口仍然频繁 Up/Down，可以尝试将接口改成非自协商模式，强制两边速率、双工一致。
Speed :	表示接口当前速度。	在非自协商模式下如果设备两端接口速率不一致，请在接口视图下执行 **speed** 命令调整接口速率一致。
Duplex:	接口双工状态。	在非自协商模式下如果设备两端接口双工不一致，请在接口视图下执行 **duplex** 命令调整接口速率一致。

执行上述步骤后，如果接口的状态仍然频繁 Up/Down，请执行步骤 3。

步骤 3 检查设备两端链路、接口模块是否故障。

设备之间是通过双绞线连接，需要做如下检查：

检查项	检查标准	后续操作
用测试仪测试双绞线是否故障。	测试仪显示双绞线正常。	如果检查出线缆故障，请更换线缆。
设备间双绞线长度是否满足要求。	设备间线缆长度<100m。 **说明** 10/100/1000M 电接口采用 RJ-45 连接器，接口线缆为 5 类或 5 类以上双绞线，传输距离 100m。	如果线缆长度大于 100m 可以采用如下方式： ● 缩短设备间距离，以缩短双绞线长度。 ● 如果不能改变设备间的距离，设备之间可以通过中继器、HUB 或交换机串联。
如果设备两端使用的电口模块，请检查电口模块是否故障。	电口模块正常。	尝试更换两端电口模块。

如果设备之间是通过光纤连接，需要做如下检查：

检查项	检查标准	后续操作
用测试仪或物理环回方法检查链路光纤链路两端是否故障。	使用测试仪测试时，测试仪显示收发正常。 使用物理环回时，可以看到接口 Up。	如果检查出线缆故障，请尝试更换线缆，如果更换线缆故障依然存在请尝试更换两端接口光模块。
检查光模块和光纤的对应关系。	检查光纤类型是否正确，光模类型和光纤类型对应关系请参见硬件描述“光模块属性速查表”。	如果对应关系不正确，请根据实际情况选择更换光模块或光纤。
设备间光纤的长度和光模块支持的传输距离是否匹配。	光纤的长度小于光模块支持的传输距离。光模块支持光纤的传输距离请参见硬件描述“光模块属性速查表”。	根据现网实际情况缩短光纤长度或者更换支持更大传输距离的光模块。
用测试仪测试信号的衰减在允许的范围内。	光信号的衰减范围请参见硬件描述“光模块属性速查表”。	如果衰减过大请更换光纤，如果更换光纤仍不符合衰减要求，或缩短光纤的长度。

执行上述步骤后，如果接口的状态仍然频繁 Up/Down，请执行步骤 4。

步骤 4 检查本端和对端设备硬件是否故障。

- 尝试将线缆连接到其他接口。
- 如果对端是 PD(Powered Device)设备，请检查对端 PD 设备的正常工作的功率是否超过了接口能提供的最大供电功率。

  说明

  PD 消耗瞬间功率超过了接口提供的额度功率，会导致设备将连接到该接口的 PD 下电，一段时间后设备重新开始检测发现 PD 设备又开始供电，当发现 PD 消耗瞬间功率超过了接口提供的额度功率时又对连接到该接口的 PD 下电，这样频繁上下电会导致接口频繁 Up/Down。

执行完上述操作后，如果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

相关告警与日志

相关告警

无

相关日志

无

4.2 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。

4.2.1 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。

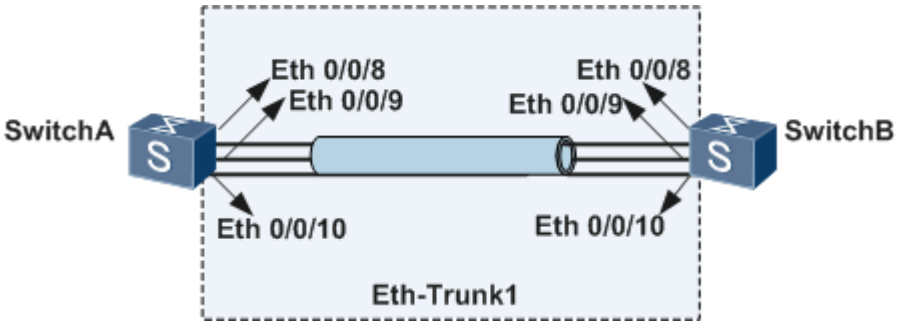
本类故障的常见原因有：

- 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 4-3 所示，Eth-Trunk 接口转发不通的故障处理将基于该网络。

图 4-3 Eth-Trunk 接口组网图

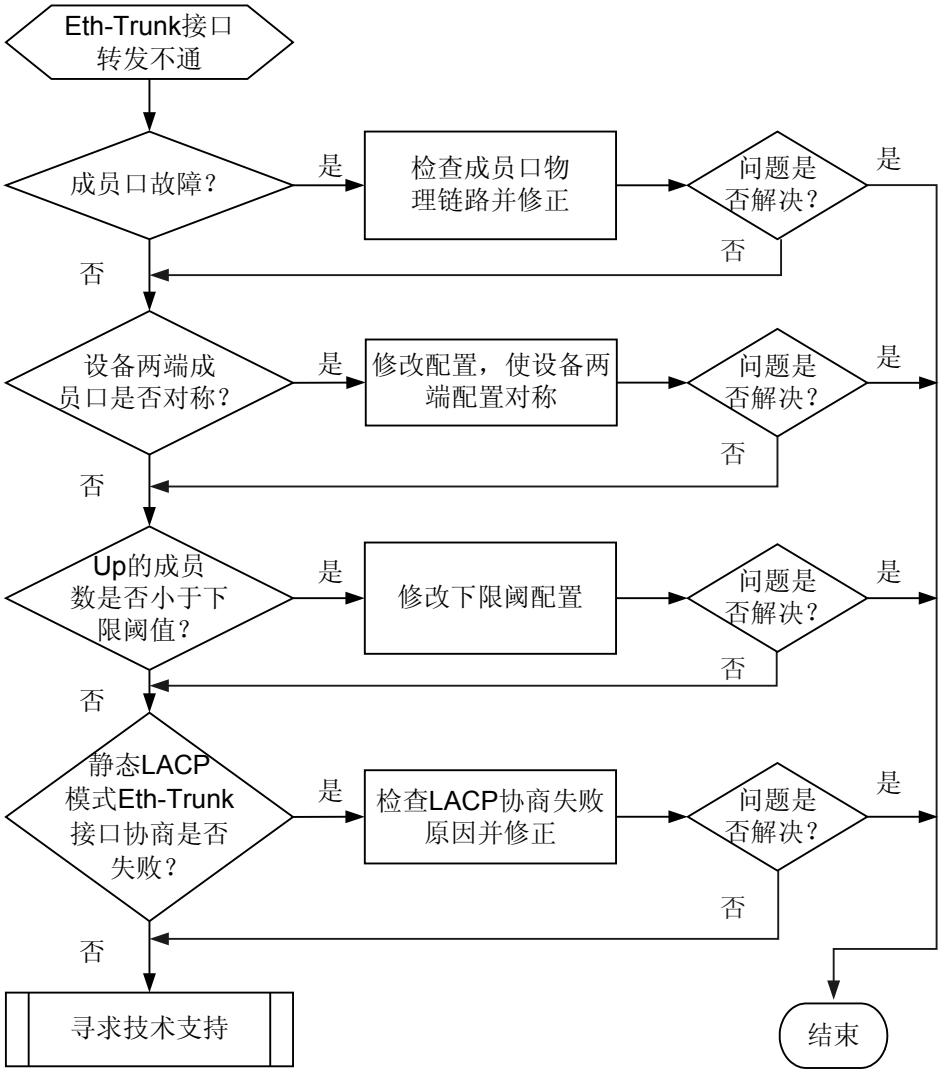


故障诊断思路：

- 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 4-4 排除此类故障。

图 4-4 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。

```
[Quidway] 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: 4
```

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

PortName         Status      Weight
GigabitEthernet0/0/8    Down        1
GigabitEthernet0/0/9    Down        1
GigabitEthernet0/0/10   Down        1
```

- 如果 Eth-Trunk 接口中成员口的状态为 Down，请先根据**以太网接口 Down 的定位思路**排除接口 Down 的故障。
- 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 SwitchA 和 SwitchB 上 Eth-Trunk 接口包含的成员口信息。

```
[SwitchA] 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: 4
Operate status: up            Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------

PortName         Status      Weight
GigabitEthernet0/0/8    up          1
GigabitEthernet0/0/9    up          1
GigabitEthernet0/0/10   up          1
[SwitchB] 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: 4
Operate status: up            Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
PortName         Status      Weight
GigabitEthernet0/0/8    up          1
GigabitEthernet0/0/9    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 SwitchA、SwitchB 上执行命令 **display eth-trunk 1** 查看 Eth-Trunk 接口配置信息。

```
[SwitchA] 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: 4
Operate status: down          Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------

PortName         Status      Weight
GigabitEthernet0/0/8    up          1
GigabitEthernet0/0/9    up          1
GigabitEthernet0/0/10   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 SwitchA、SwitchB 上执行命令 **display eth-trunk 1** 查看 Eth-Trunk 接口配置信息。

```
[SwitchA] 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: 4
Operate status: down        Number Of Up Port In Trunk: 0
--------------------------------------------------------------------------------
ActorPortName         Status     PortType  PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/8  UnSelected 100M      32768   264    305     11100010  1
GigabitEthernet0/0/9  UnSelected 100M      32768   265    305     11100010  1
GigabitEthernet0/0/10 UnSelected 100M      32768   266    305     11100010  1
Partner:
--------------------------------------------------------------------------------
ActorPortName          SysPri SystemID        PortPri PortNo  PortKey   PortState
GigabitEthernet0/0/8   32768  0018-823c-c473  32768   2056    305       11100010
GigabitEthernet0/0/9   32768  0018-823c-c473  32768   2057    305       11100010
GigabitEthernet0/0/10  32768  0018-823c-c473  32768   2058    305       11100010
```

- 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。

    请将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：

```
[SwitchB] 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: 4
Operate status: up          Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------
ActorPortName         Status   PortType  PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/8  Selected 100M      32768   264    305     11111100  1
GigabitEthernet0/0/9  Selected 100M      32768   265    305     11111100  1
GigabitEthernet0/0/10 Selected 100M      32768   266    305     11111100  1
Partner:
--------------------------------------------------------------------------------
ActorPortName          SysPri SystemID        PortPri PortNo  PortKey   PortState
GigabitEthernet0/0/8   32768  0018-823c-c473  32768   2056    305       11111100
GigabitEthernet0/0/9   32768  0018-823c-c473  32768   2057    305       11111100
GigabitEthernet0/0/10  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

4.2.2 故障案例

负载分担模式不合理导致 Eth-Trunk 流量不均衡

网络环境

如图 4-5 所示，SwitchA 和 SwitchB 之间通过 Eth-Trunk 接口互联，SwitchA 和 SwitchB 上所有的接口都属于一个 VLAN。在 SwitchA 上执行 **display interface** 命令发现 GE0/0/1 和 GE0/0/2 两条链路的 outbound 方向流量不均衡；其中 GE0/0/1 outbound 方向约 800M，而 GE0/0/2 outbound 方向约 200M。

图 4-5 负载分担模式不合理导致 Eth-Trunk 流量不均衡的组网图

故障分析

1. 在 Switch 上执行 **display current-configuration** 命令查看 **Eth-Trunk1** 链路相关配置。发现 **Eth-Trunk1** 接口的负载分担模式为 **src-dst-ip**（基于源 IP 地址与目的 IP 地址的异或进行负载分担）。因为 SwitchA 和 SwitchB 之间使用 Eth-Trunk 接口做二层互联。这个负载分担的方式并不适合此处的二层互联场景。

   因此是负载分担模式配置不合理导致链路负载分担不均衡。

操作步骤

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

步骤 2 执行命令 **interface** *interface-type interface-number*，进入 **Eth-Trunk1** 接口视图。

步骤 3 执行命令 **load-balance src-dst-mac**，配置负载分担模式为 **src-dst-mac**。

完成上述操作后，在 SwitchA 上执行 **display interface** [*interface-type* [*number*]]命令查看 GE0/0/1 和 GE0/0/2 两条链路的 outbound 方向流量相当。

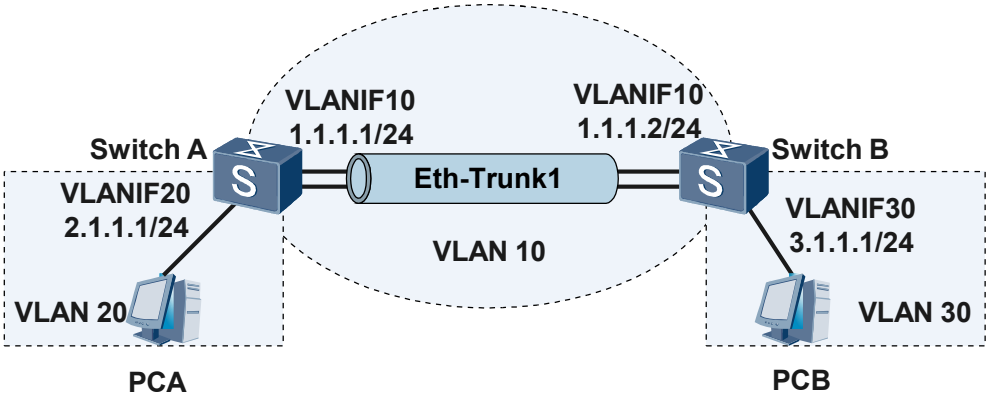
----结束

案例总结

Switch 通过 Eth-Trunk1 接口互联的两种典型场景：

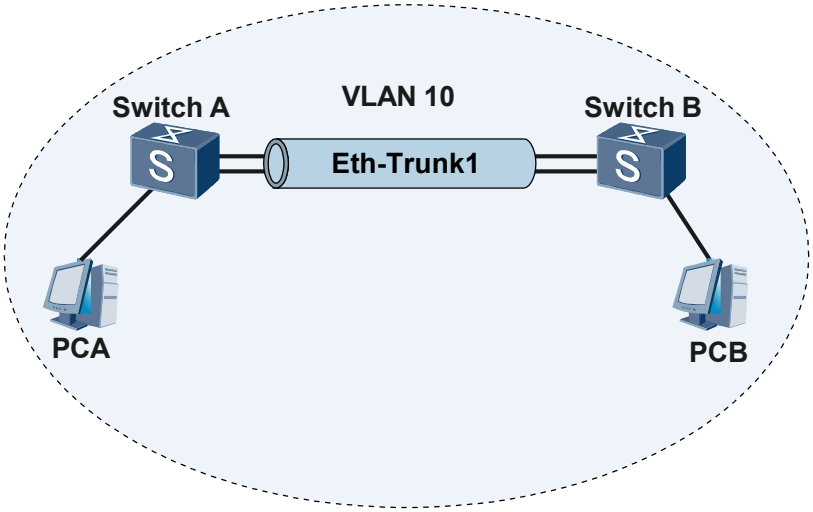
- 三层互联场景如图 4-6 所示。Eth-Trunk1 接口属于 VLAN10，PCA 和 PCB 的网关分别在 SwitchA 和 SwitchB 上，并且 PCA 和 PCB 分别属于不同的网段。PCA 如果要访问 PCB，SwitchA 上必须配置目的网段是 3.1.1.0 下一跳是 1.1.1.2 的路由，同时 SwitchB 上必须配置目的网段是 2.1.1.0 下一跳是 1.1.1.1 的路由。类似这样 SwitchA 和 SwitchB 互相访问需要路由参与的场景为三层互联场景。

图 4-6 Eth-Trunk1 接口互联的三层场景



- 二层互联场景如图 4-7 所示。SwitchA 和 SwitchB 上所有接口都属于 VLAN10。类似这样 PCA 和 PCB 不需要路由参与可以直接访问的场景为二层互联场景。

图 4-7 Eth-Trunk1 接口互联的二层场景



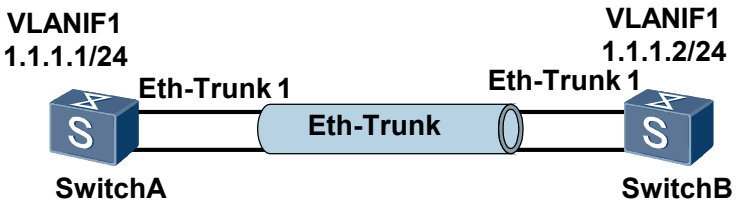
两台 Switch 通过 **Eth-Trunk1** 接口互联时，如果是二层互联负载分担方式选择基于 MAC 方式负载分担，三层互联负载分担方式选择基于 IP 方式负载分担。

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 4-8 的网络中，SwitchA 为 AC6605，SwitchB 为其他厂商设备。两设备之间做链路聚合，将两条 FE 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 4-8 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 SwitchA 上执行 **display current-configuration interface eth-trunk** 命令，检查 SwitchA 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 SwitchA、SwitchB 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. 在 SwitchA 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 SwitchA 和 SwitchB 上执行 **display trunkmembership eth-trunk** 命令检查 Eth-Trunk 的成员接口数目，发现 SwitchA 和 SwitchB 的 Eth-Trunk 成员接口数目相同。
5. 在 SwitchA 上执行 **display mac-address** 命令查看 MAC 地址学习情况，发现 SwitchA 已经学习到了对端的 MAC 地址，但在 SwitchB 上查看 MAC 地址表，发现 SwitchB 并没有学习到 SwitchA 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 AC6605 采用手工聚合方式不进行 LACP 协商，所以 SwitchB 发送的 LACP 协商请求 SwitchA 并未做应答导致链路聚合没有建立成功。

   说明

   - 因为 SwitchA 收到 SwitchB 的 LACP 协商报文，所以 SwitchA 能够学习到 SwitchB 的 MAC 地址。
   - 因为 SwitchA 上并未开启 LACP 协商，所以 SwitchA 收到 SwitchB 的协商报文后直接将其丢弃，SwitchB 收不到应答报文所以 SwitchB 未学习到 SwitchA 的 MAC 地址。
   - SwitchA 没有对 SwitchB 发送的 LACP 协商报文进行应答导致 SwitchB 的 LACP 协商不成功，协商失败后 SwitchB 的 Eth-Truck 处于 Block 状态，因此设备两端不能进行正常的 ARP 学习。

操作步骤

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

----结束

案例总结

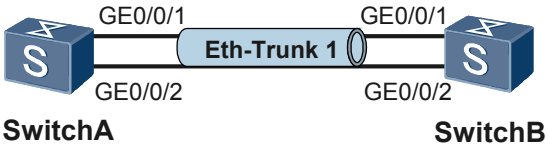
在与其他厂商设备做链路聚合对接时，一定要确保双方采用的聚合方式一致。

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 4-9 的网络中配置 Eth-Trunk。

图 4-9 Eth-Trunk 组网图



配置完成后，发现两台 Switch 之间的数据不能正常转发。

故障分析

1. 依次在 SwitchA、SwitchB 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 SwitchA、SwitchB 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 SwitchA、SwitchB 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 SwitchA、SwitchB 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 SwitchA 的 Eth-Trunk 成员接口数目为 2，SwitchB 的 Eth-Trunk 成员接口数目为 1(即接口 GE0/0/1)。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 SwitchA 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 GE0/0/2 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。

5 局域网类

关于本章

5.1 VLAN 故障处理
介绍了 VLAN 常见故障原因的定位思路和案例。

5.2 MAC 表故障处理
介绍 MAC 表常见故障的定位思路。

5.3 QinQ 故障处理
介绍了 QinQ 常见故障的定位思路和案例。

5.4 MSTP 故障处理

5.5 GVRP 故障处理
介绍了 GVRP 常见故障的定位思路和案例。

5.6 MAC SWAP 环回故障处理
介绍 MAC SWAP 环回常见故障的定位思路。

5.7 VLAN Mapping 故障处理
介绍 VLAN Mapping 故障的定位思路。

5.8 环路故障处理
介绍了环路常见故障的定位思路和案例。

5.9 Loopback Detection 故障处理
介绍 Loopback Detection 故障的定位思路。

5.1 VLAN 故障处理

介绍了 VLAN 常见故障原因的定位思路和案例。

5.1.1 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。
- 交换机 MAC 地址学习错误。
- 交换机上配置了端口隔离。
- 主机配置了错误的静态 ARP。
- 交换机上配置了错误的端口和 MAC 地址绑定。

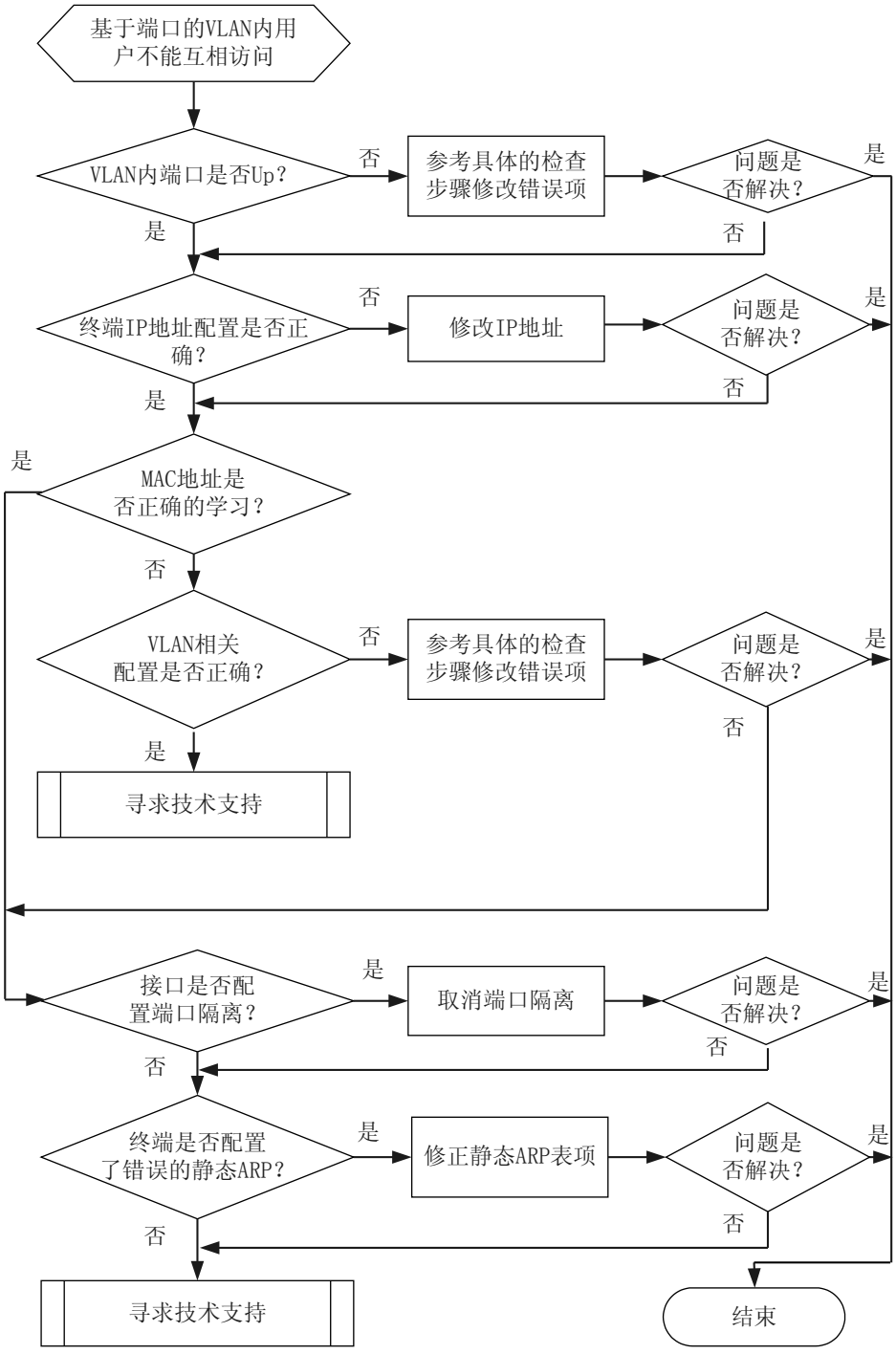
说明

VLAN 间的故障处理请参考 IP 转发故障处理。

故障诊断流程

可按照图 5-1 排除此类故障。

图 5-1 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。

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，请先根据**以太网接口 DOWN 的定位思路**排除接口 Down 的故障。
- 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 Switch 上 MAC 地址表项是否正确。

在 Switch 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 Switch 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。

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交换机，还需要考虑交换机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，Switch 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 Access 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，Switch 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，Switch 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：

- 如果未配置了端口隔离请执行**步骤 6**。

- 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

5.2 MAC 表故障处理

介绍 MAC 表常见故障的定位思路。

5.2.1 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。

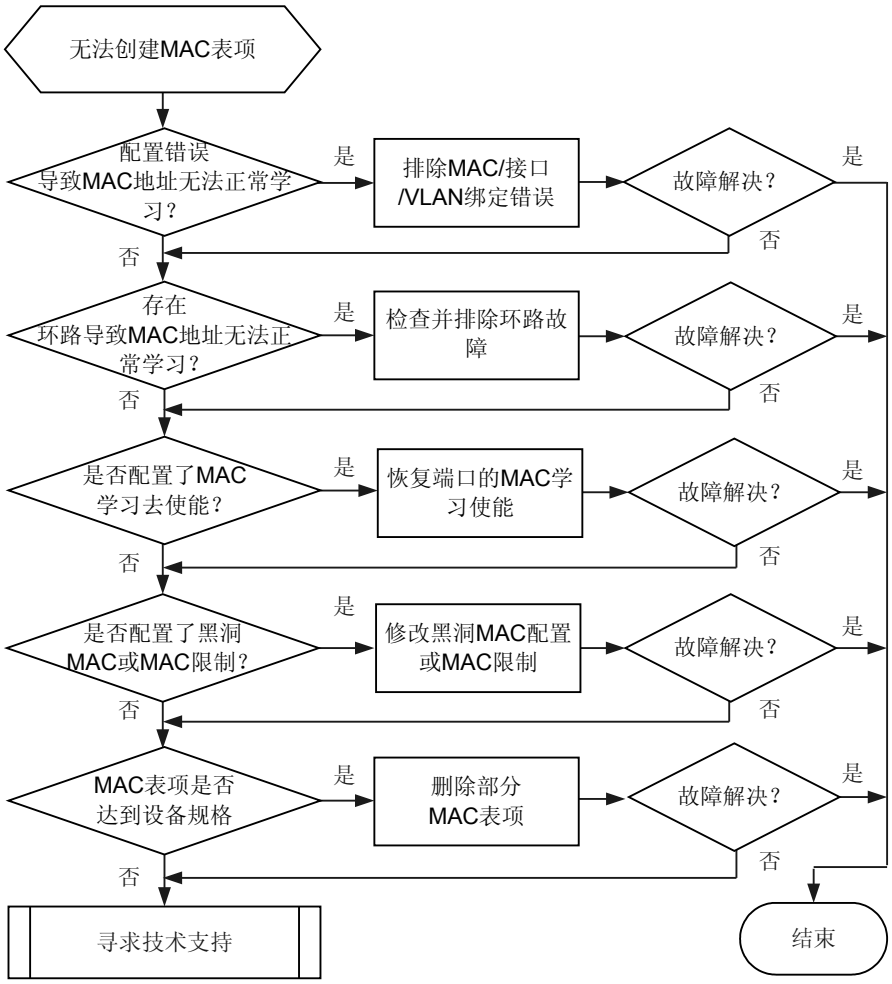
故障的定位思路如下：

- 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

- 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 5-2 所示。

图 5-2 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。

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

```
MAC Address    VLAN/VSI                                Learned-From        Type
------------------------------------------------------------------------------
0025-9e80-2494 1/-                                     GE0/0/1             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。

```
[Quidway-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 mac-address learning disable
 port hybrid tagged vlan 10
 undo negotiation auto
#
return
[Quidway-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。

```
[Quidway] display mac-address blackhole
M------------------------------------------------------------------------------
MAC Address    VLAN/VSI                                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。

- 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交换机，则在该接口连接的交换机上执行命令 **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交换机，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

相关告警与日志

相关告警

无

相关日志

无

5.3 QinQ 故障处理

介绍了 QinQ 常见故障的定位思路和案例。

5.3.1 配置 QinQ 功能后业务不通的定位思路

介绍在 AC6605 上配置 QinQ 功能后出现业务不通时的故障处理流程和详细的故障处理步骤。

常见原因

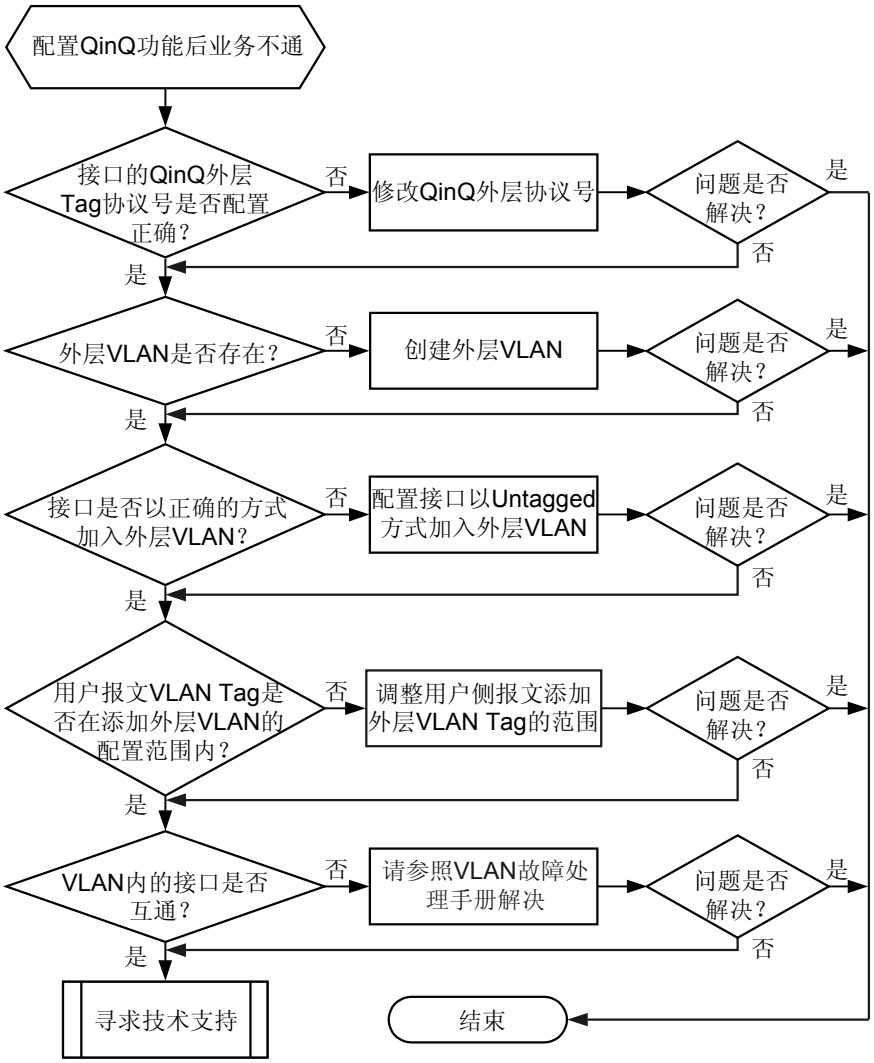
本类故障的常见原因主要包括：

- AC6605 接口的 QinQ 外层 Tag 协议号不能被和该接口直接相连的设备所识别。
- 没有创建外层 VLAN，导致接口无法加入该 VLAN。
- AC6605 接口没有以 Untagged 的方式加入外层 VLAN。
- AC6605 配置了对某一个 VLAN Tag 范围内上行的报文添加双层 VLAN Tag，但上来的用户报文 VLAN Tag 不在此范围内，AC6605 无法识别。
- VLAN 内的接口不能互通。

故障诊断流程

详细处理流程如图 5-3 所示。

图 5-3 配置 QinQ 功能后业务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。

操作步骤

步骤 1 检查 AC6605 接口的 QinQ 外层 Tag 协议号是否能被和该接口直接相连的设备所识别。

说明

- AC6605 接口的 QinQ 外层协议号的缺省值为 0x8100。
- 如果 AC6605 接口的 QinQ 外层 Tag 协议号不能被和该接口直接相连的设备所识别，则该设备无法识别 AC6605 发送过来的 QinQ 报文。

在 AC6605 上执行命令 **display current-configuration interface** *interface-type interface-number*，查找 AC6605 连接对端设备所使用的接口的 QinQ 外层协议号值。

- 如果该接口下显示 **qinq protocol** *protocol-id*，说明 AC6605 接口的 QinQ 外层协议号已经被修改为 *protocol-id*。
- 如果该接口下没有显示 **qinq protocol** *protocol-id*，说明 AC6605 接口的 QinQ 外层协议号仍然是缺省值 **0x8100**。

检查 AC6605 对端设备接口的 QinQ 外层协议号值。

- 如果该设备接口的 QinQ 外层协议号值跟 AC6605 接口的 QinQ 外层协议号值一样，执行步骤 2。
- 如果该设备接口的 QinQ 外层协议号值跟 AC6605 接口的 QinQ 外层协议号值不一样，在 AC6605 的接口视图下，执行命令 **qinq protocol** *protocol-id*，将 AC6605 接口的 QinQ 外层协议号值修改为跟对端设备接口的 QinQ 外层协议号值一致。

步骤 2 检查外层 VLAN 是否存在。

说明

如果要添加的外层 VLAN 没有创建，则 AC6605 无法添加的外层 VLAN Tag。

执行命令 **display vlan** *vlan-id*，检查 **VLAN** *vlan-id* 是否已经存在。

- 如果显示 **Error: The VLAN does not exist.**，说明 **VLAN** *vlan-id* 不存在，执行命令 **vlan** *vlan-id*，创建 VLAN。
- 如果显示了 **VLAN** *vlan-id* 的详细信息，说明 **VLAN** *vlan-id* 已经存在，执行步骤 3。

步骤 3 检查 AC6605 接口是否以正确的方式加入外层 VLAN。

说明

- 缺省情况下，接口的类型为 Hybrid。
- 推荐接口的类型配置为 Hybrid，且以 Untagged 的方式加入外层 VLAN，不推荐接口的类型配置为 Trunk。

在 AC6605 上执行命令 **display current-configuration interface**，查找 AC6605 连接下行设备所使用的接口是否以正确的方式加入外层 VLAN。

显示信息	显示信息解释说明	后续操作
port hybrid untagged vlan *vlan-id*	该接口的类型已经配置为 Hybrid，且以 Untagged 的方式加入外层 VLAN	执行步骤 4
port hybrid tagged vlan *vlan-id*	该接口没有以 Untagged 的方式加入外层 VLAN，而是配置成 Tagged 方式	执行命令 **port hybrid untagged vlan** *vlan-id*，配置接口以 Untagged 的方式加入外层 VLAN。
无上述显示信息	该接口没有加入外层 VLAN	

步骤 4 检查用户侧报文 VLAN Tag 是否在需要添加外层 VLAN 的配置范围内。

在 AC6605 上执行命令 **display current-configuration interface**，查找 AC6605 连接下行设备所使用的接口下的配置。

查找关键字 **port vlan-stacking vlan** *vlan-id1* **to** *vlan-id2* **stack-vlan** *vlan-id3*，得到结论：用户 VLAN Tag 在 *vlan-id1~vlan-id2* 之间，添加外层 VLAN Tag 为 *vlan-id3*。

- 如果用户侧报文 VLAN Tag 在 *vlan-id1~vlan-id2* 之间，执行步骤 5。
- 如果用户侧报文 VLAN Tag 不在 *vlan-id1~vlan-id2* 之间，根据实际情况执行命令 **port vlan-stacking vlan** *vlan-id1* **to** *vlan-id2* **stack-vlan** *vlan-id3*，调整用户侧报文添加外层 VLAN Tag 的范围。

步骤 5 检查 VLAN 内的接口是否互通。

在同一个 VLAN 内，不能互通的两个接口互相 **Ping** 对端。

- 如果不能 **Ping** 通，说明 VLAN 内的接口发生故障，请参考 **5.1 VLAN 故障处理**解决。
- 如果能够 **Ping** 通，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

5.4 MSTP 故障处理

5.4.1 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。

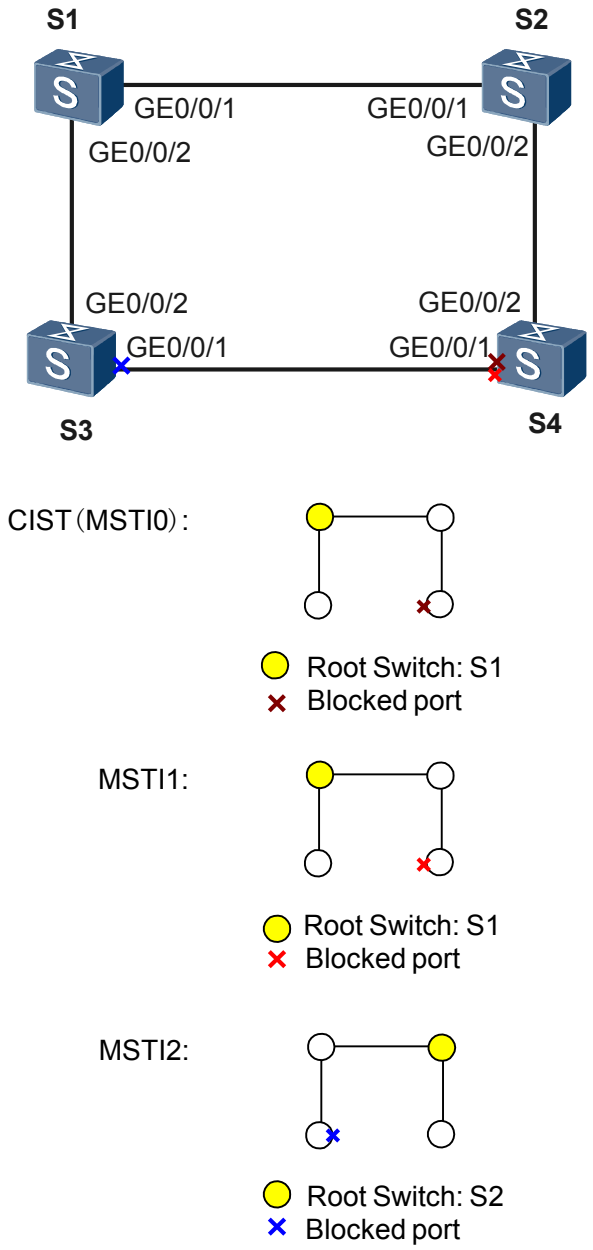
本类故障的常见原因有：

- 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 5-4 所示，MSTP 拓扑变化导致业务中断的故障处理将基于该网络。

图 5-4 MSTP 功能组网图

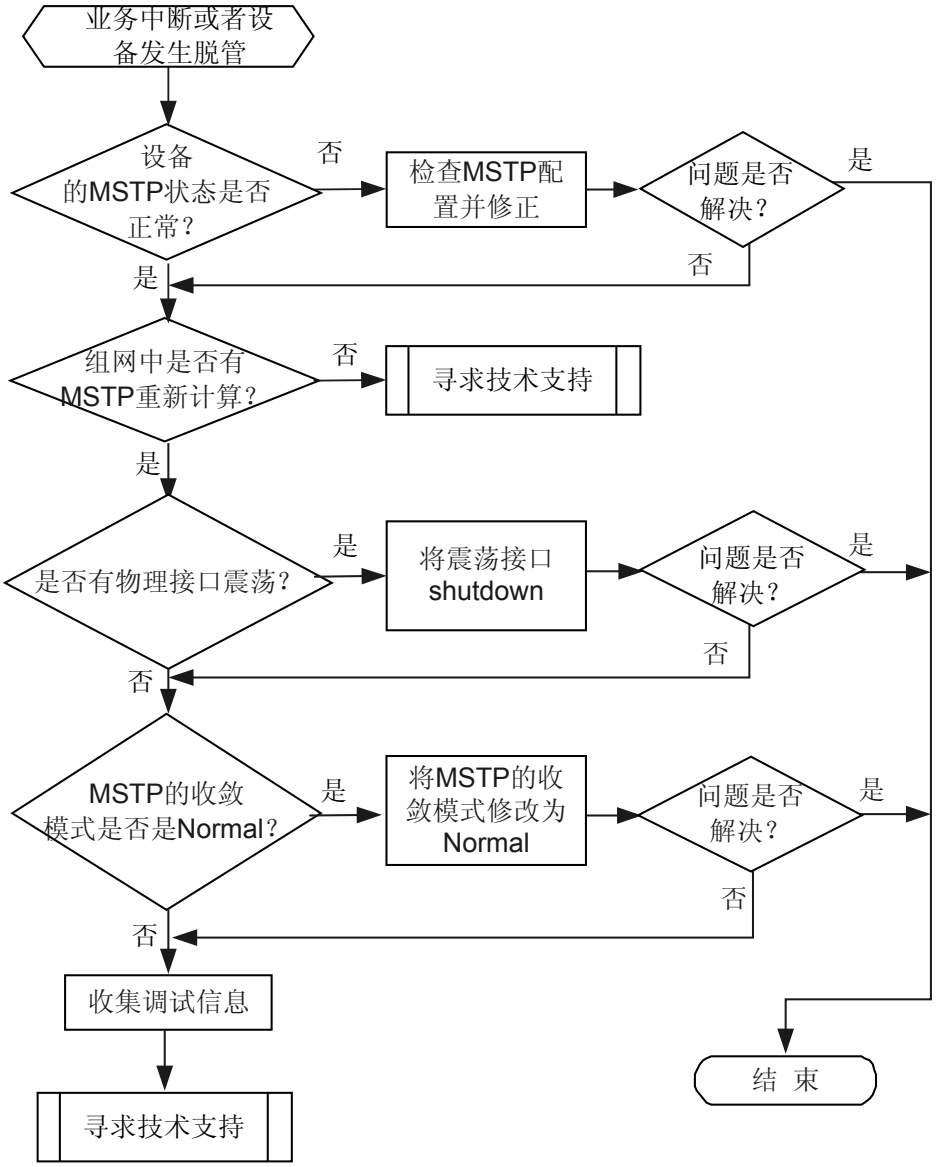


故障诊断思路：

- 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 5-5 排除此类故障。

图 5-5 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。

如图 5-4 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 S1 的 MSTP 状态信息。如**图 5-4** 所示，设备 S1 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 S1 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。

```
[S1] display stp brief
 MSTID      Port                  Role  STP State     Protection
   0        GigabitEthernet0/0/1  DESI  FORWARDING      NONE
   0        GigabitEthernet0/0/2  DESI  FORWARDING      NONE
   1        GigabitEthernet0/0/1  DESI  FORWARDING      NONE
   1        GigabitEthernet0/0/2  DESI  FORWARDING      NONE
   2        GigabitEthernet0/0/1  ROOT  FORWARDING      NONE
   2        GigabitEthernet0/0/2  DESI  FORWARDING      NONE
```

在任意视图下执行命令 **display stp brief** 查看设备 S2 的 MSTP 状态信息。如**图 5-4** 所示，设备 S2 在实例 2 中是根桥，所有端口角色应该都是指定端口。设备 S2 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。

```
[S2] display stp brief
 MSTID      Port                  Role  STP State     Protection
   0        GigabitEthernet0/0/1  ROOT  FORWARDING      NONE
   0        GigabitEthernet0/0/2  DESI  FORWARDING      NONE
   1        GigabitEthernet0/0/1  ROOT  FORWARDING      NONE
   1        GigabitEthernet0/0/2  DESI  FORWARDING      NONE
   2        GigabitEthernet0/0/1  DESI  FORWARDING      NONE
   2        GigabitEthernet0/0/2  DESI  FORWARDING      NONE
```

在任意视图下执行命令 **display stp brief** 查看设备 S3 的 MSTP 状态信息。如**图 5-4** 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 S3 的端口角色分别是指定端口和根端口，转发状态是 FORWARDING。

```
[S3] display stp brief
 MSTID      Port                  Role  STP State     Protection
   0        GigabitEthernet0/0/1  DEST  FORWARDING      NONE
   0        GigabitEthernet0/0/2  ROOT  FORWARDING      NONE
   1        GigabitEthernet0/0/1  DEST  FORWARDING      NONE
   1        GigabitEthernet0/0/2  ROOT  FORWARDING      NONE
   2        GigabitEthernet0/0/1  ALTE  DISCARDING      NONE
   2        GigabitEthernet0/0/2  ROOT  FORWARDING      NONE
```

在任意视图下执行命令 **display stp brief** 查看设备 S4 的 MSTP 状态信息。如**图 5-4** 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 S4 的端口角色分别是指定端口和根端口，转发状态是 FORWARDING。

```
[S4] display stp brief
 MSTID      Port                  Role  STP State     Protection
   0        GigabitEthernet0/0/1  ALTE  DISCARDING      NONE
   0        GigabitEthernet0/0/2  ROOT  FORWARDING      NONE
   1        GigabitEthernet0/0/1  ALTE  DISCARDING      NONE
   1        GigabitEthernet0/0/2  ROOT  FORWARDING      NONE
   2        GigabitEthernet0/0/1  DESI  FORWARDING      NONE
   2        GigabitEthernet0/0/2  ROOT  FORWARDING      NONE
```

- 对于如**图 5-4** 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。

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

```
[S1] 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。

- 查看端口配置，确认使能 MSTP 的端口是否使能了协议报文上送命令。如：**bpdu enable**。
- 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。
- 如果使能 MSTP 的设备上配置了 BPDU Tunnel，请确认 BPDU Tunnel 配置是否正确。正确的 BPDU Tunnel 配置请参见《AC6605 配置指南-以太网》的 BPDU Tunnel 配置一节。
- 查看设备端口是否加入正确的 VLAN。正确的 VLAN 配置请参见《AC6605 配置指南-以太网》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。

```
[S1] 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**。

说明

如果设备创建了多进程并在该进程中配置了 TC 通告，当该进程发生拓扑变化时，该进程会将 TC 消息通知给进程 0，从而 进程 0 内的设备刷新 MAC 地址表和 ARP 地址表，使网络中的设备重新选择链路进行转发，保证流量不中断。

- 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。

- 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。

```
[S1] 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

5.5 GVRP 故障处理

介绍了 GVRP 常见故障的定位思路和案例。

5.5.1 动态 VLAN 无法生成的定位思路

介绍动态 VLAN 无法生成的故障处理流程和详细的故障处理步骤。

常见原因

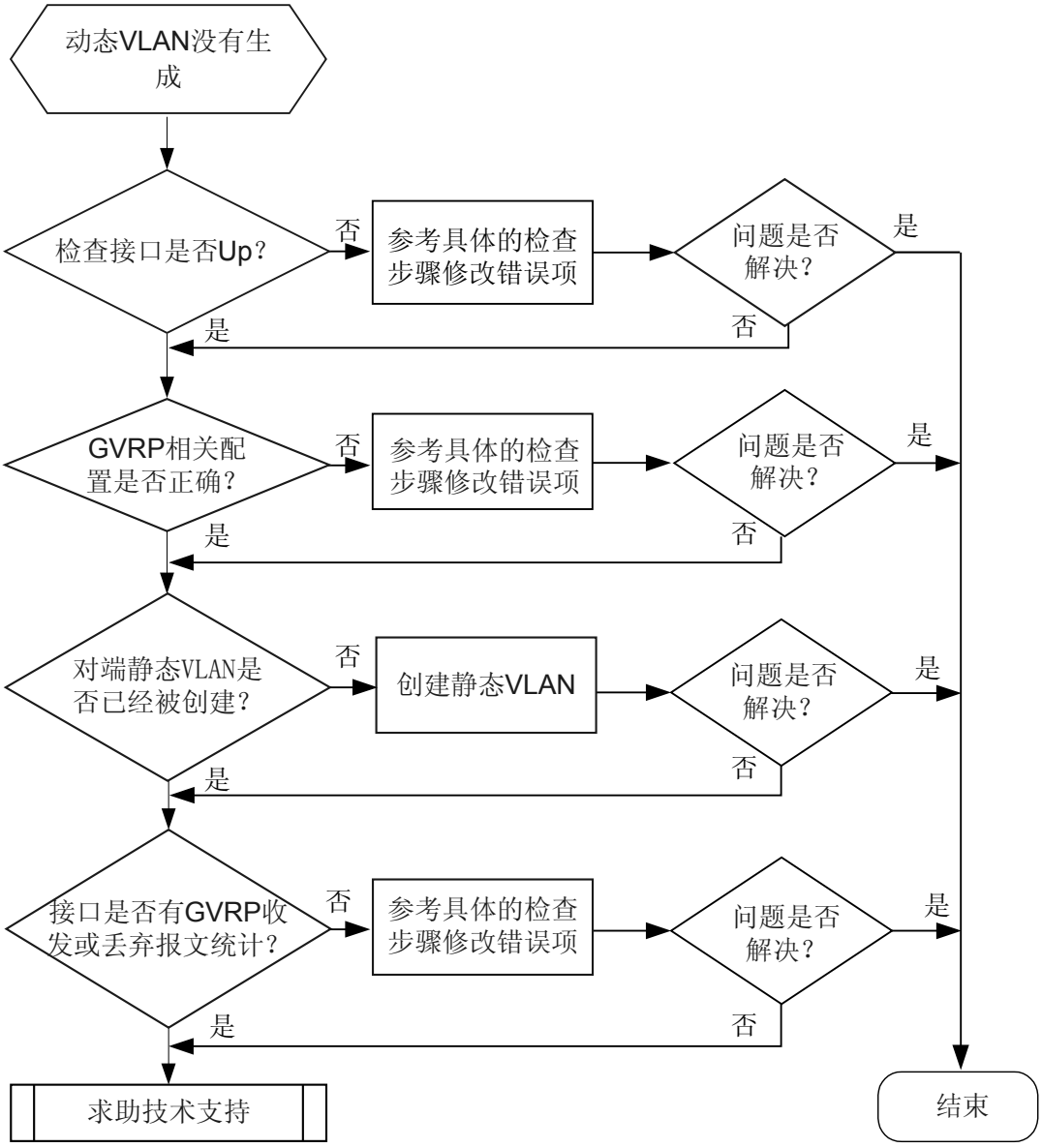
本类故障的常见原因主要包括：

- 部署 GVRP 业务的设备之间的链路故障。
- 接口注册模式配置错误。

故障诊断流程

在配置 GVRP 后发现动态 VLAN 无法生成。可按照如下的故障诊断流程图排除故障。

图 5-6 动态 VLAN 无法生成故障诊断流程图



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 检查使能 GVRP 功能的接口是否 Up。

在任意视图下执行 **display interface** *interface-type interface-number* 命令查看使能 GVRP 功能的接口运行状态。

- 如果接口的状态为 Down，请先根据**以太网接口 DOWN 的定位思路**排除接口 Down 的故障。

  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，请执行**步骤 2**。

步骤 2 检查 GVRP 相关配置是否正确。

请执行如下操作检查 GVRP 相关配置是否正确。

检查项	检查方法及处理建议
查看是否使能了 BPDU。	在接口视图下使用命令 **display this** 查看接口 BPDU 是否被使能。 [Quidway-GigabitEthernet1/0/10/0/1] **display this** # interface GigabitEthernet1/0/10/0/1 bpdu enable # 如果未使能请在接口视图下执行**bpdu enable**命令使能BPDU。
检查是否使能 GVRP	● 检查系统全局是否使能 GVRP 默认情况下全局 GVRP 是被禁用的，可以在系统视图下使用命令 **display gvrp status** 查看全局 GVRP 是否被使能。 <Quidway> **display gvrp status** GVRP is enabled 如果全局 GVRP 没有使能，请在系统视图下执行 **gvrp** 命令使能全局 GVRP 功能。 ● 检查接口视图下是否使能 GVRP 在接口视图下使用命令 **display this** 查看接口 GVRP 是否被使能。 [Quidway-GigabitEthernet0/0/1] **display this** # interface GigabitEthernet0/0/1 gvrp # 如果接口 GVRP 没有使能，请在接口视图下执行 **gvrp** 命令使能接口 GVRP 功能。
检查接口是否以 **port trunk allow-pass vlan** 形式加入了 VLAN。	在接口视图下使用命令 **display this** 查看接口加入的 VLAN。 [Quidway-GigabitEthernet0/0/1] **display this** # interface GigabitEthernet0/0/1 port link-type trunk port trunk allow-pass vlan 20 100 gvrp # **说明** 缺省情况下，Switch 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。 如果未使用 Trunk 方式加入 VLAN，请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。

检查项	检查方法及处理建议
检查接口注册模式是否配置正确。	在接口视图下使用命令 **display this** 查看接口的注册模式，检查接口是否被设置成了 fixed 或 forbidden。 **说明** GVRP 的接口注册模式有三种: ● Normal 模式：允许该接口动态注册、注销 VLAN，传播动态 VLAN 以及静态 VLAN 信息。 ● Fixed 模式：禁止该接口动态注册、注销 VLAN，只传播静态 VLAN 信息，不传播动态 VLAN 信息。也就是说被设置为 Fixed 模式的 Trunk 接口，即使允许所有 VLAN 通过，实际通过的 VLAN 也只能是手动配置的那部分。 ● Forbidden 模式：禁止该接口动态注册、注销 VLAN，不传播除 VLAN1 以外的任何的 VLAN 信息。也就是说被配置为 Forbidden 模式的 Trunk 接口，即使允许所有 VLAN 通过，实际通过的 VLAN 也只能是 VLAN1。 缺省情况下接口接口注册模式是 normal，如果接口注册模式不是 normal，请执行 **gvrp registration** 修改为 normal 模式。 [Quidway-GigabitEthernet0/0/1] **display this** # interface GigabitEthernet0/0/1 port link-type trunk port trunk allow-pass vlan 20 100 gvrp gvrp registration forbidden #

执行完上述操作后，如果故障仍然存在请执行**步骤 3**。

步骤 3 检查静态 VLAN 是否被创建。

在系统视图下使用命令 **display this** 查看静态 VLAN 是否被创建，如果没有创建静态 VLAN 则不会生成动态 VLAN。

```
[Quidway] display this
#
vlan batch 1 to 10
#
```

- 如果静态 VLAN 没有被创建，请创建静态 VLAN。
- 如果静态 VLAN 已经被创建，请执行**步骤 4**。

步骤 4 检查接口是否有 GVRP 收、发报文或丢弃报文统计。

在用户视图下使用命令 **display garp statistics** 查看接口是否有收、发包或报文丢弃统计。

通过反复执行 **display garp statistics** 命令查看各个统计值的变化。

说明

正常情况下收发包应该正常，且不会有丢弃报文计数的。

```
<Quidway> display garp statistics
  GARP statistics on port GigabitEthernet0/0/1
    Number of GVRP frames received       : 0
    Number of GVRP frames transmitted    : 0
    Number of frames discarded           : 0
```

- 如果 GVRP 收、发报文或丢弃报文正常，请执行**步骤 5**。

- 如果 GVRP 收、发报文或丢弃报文异常，请按照下表检查项检查：

检查项	检查方法及处理建议
检查接口是否是 block 接口。	在用户视图下使用命令 **display stp brief** 查看是否存在 STP 协议的 block 接口，检查显示信息中的 STP State 是否为 DISCARDING，如果是 DISCARDING 表明接口被 block，此时设备无法生成动态 VLAN。此时可以使用 **stp port priority** 命令更改接口优先级，生成树重新生成后接口状态由 block 变为 Active。
检查设备上是否配置了 GVRP 报文过滤。	在对端和本端设备上检查是否配置了过滤 GVRP 报文的 ACL 策略，如果配置了请根据需要取消限制 GVRP 报文的 ACL 相关配置。

如果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

5.5.2 动态 VLAN 振荡故障定位思路

介绍动态 VLAN 振荡的故障处理流程和详细的故障处理步骤。

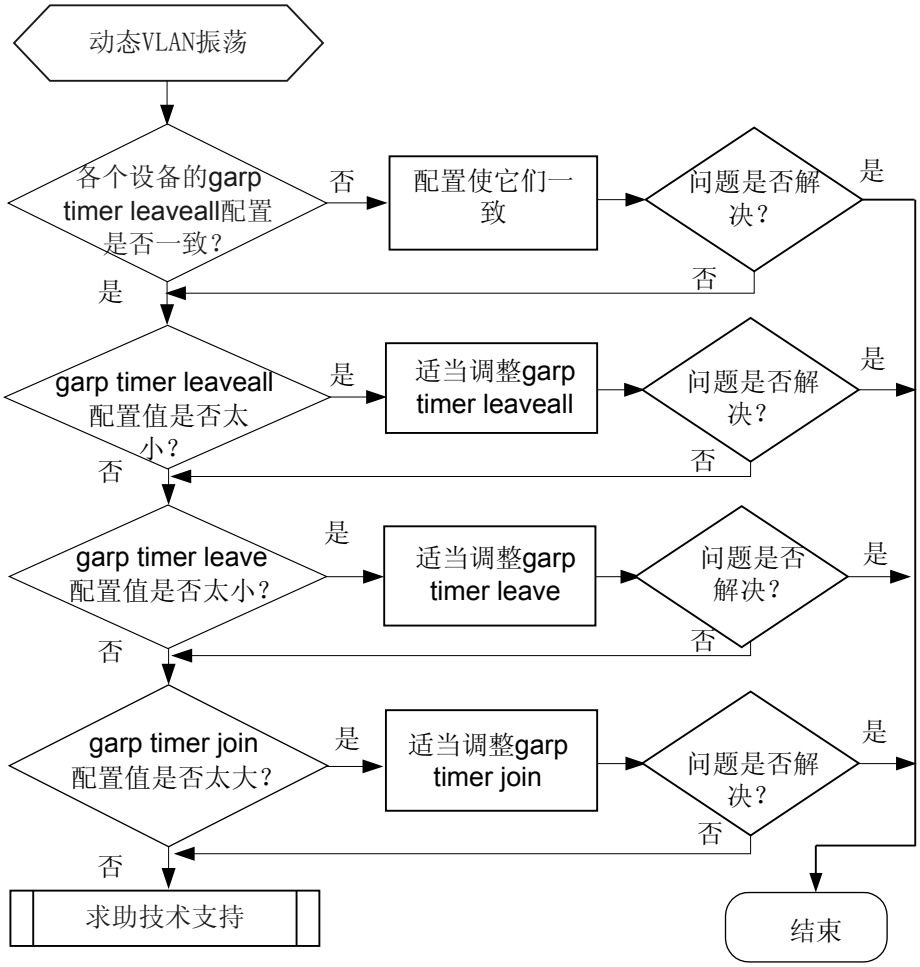
常见原因

本类故障的常见原因是 timer 值得设置不合理。

故障诊断流程

在配置 GVRP 后发现二层流量不通，可按照如下的故障诊断流程图排除故障。

图 5-7 VLAN 振荡故障诊断流程图



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 GARP 的各个 timer 值得设置得是否合理。

如果开启了 GVRP，默认情况下设备会给每一个 timer 设置一个默认值。如果各个时间值的设置不恰当很有可能会引起动态 VLAN 的振荡。现网中的多台设备的 timer 值也要协调合理设置才会保证动态 VLAN 不发生振荡。

因为每个厂家的设备性能不一样，如果配置的静态 vlan 过多，Leave All Period 配置过小有可能产生振荡现象。

在用户视图下使用命令 **display garp timer** 查看交换机上配置的 Timer 值

```
<Quidway> display garp timer
  GARP timers on port GigabitEthernet0/0/1
```

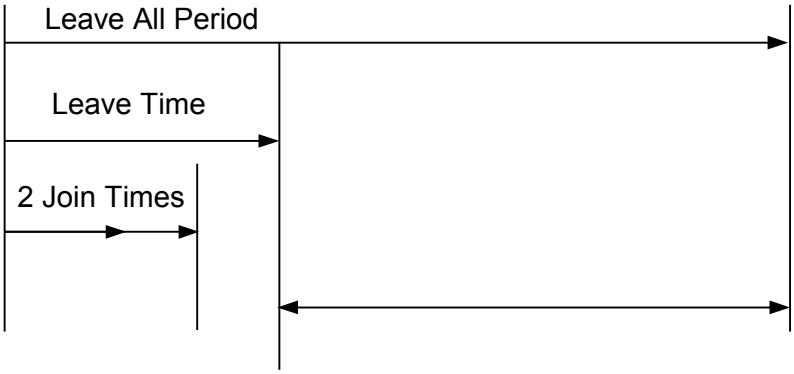
```
GARP JoinTime               : 20 centiseconds
GARP LeaveTime              : 60 centiseconds
GARP LeaveAllTime           : 1000 centiseconds
GARP HoldTime               : 10 centiseconds
```

建议将 GVRP 定时器配置为以下的推荐值：

- GARP Join 定时器：600 厘秒（6 秒钟）
- GARP Leave 定时器：3000 厘秒（30 秒钟）
- GARP LeaveAll 定时器：12000 厘秒（2 分钟）
- GARP Hold 定时器：100 厘秒（1 秒钟）

如果 timer 值设置不合理，请根据以下规律调整。各个 timer 值得设置要满足如下关系：

图 5-8 GARP 定时器



步骤 2 使用命令 **garp timer leaveall** 调整全局 leaveall 值，使交换机上的 leaveall timer 值与网络中其他设备一致。

步骤 3 使用命令 **garp timer** 调整接口的 Leave timer、Join timer 值。

步骤 4 如果问题还没解决，请联系华为技术支持工程师。

----结束

相关告警与日志

相关告警

无

相关日志

无

5.6 MAC SWAP 环回故障处理

介绍 MAC SWAP 环回常见故障的定位思路。

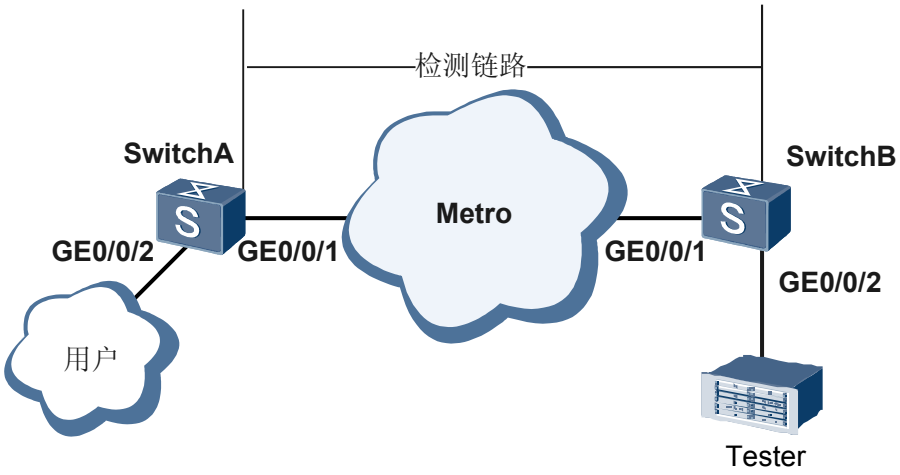
5.6.1 测试仪未收到远端环回流量的定位思路

介绍测试仪未收到环回流量的故障原因、处理流程和详细的故障处理步骤。

常见原因

如图 5-9 所示，在 SwitchA 上的 GE0/0/1 上配置了远端环回，在 SwitchB 上通过测试仪打流，检测 SwitchB 的 GE0/0/2 到 SwitchA 的 GE0/0/1 之间连通性，其中 SwitchA 的接口 GE0/0/1 和 SwitchB 的接口 GE0/0/1、GE0/0/2 被划分在同一个 VLAN。

图 5-9 远端环回的典型组网图



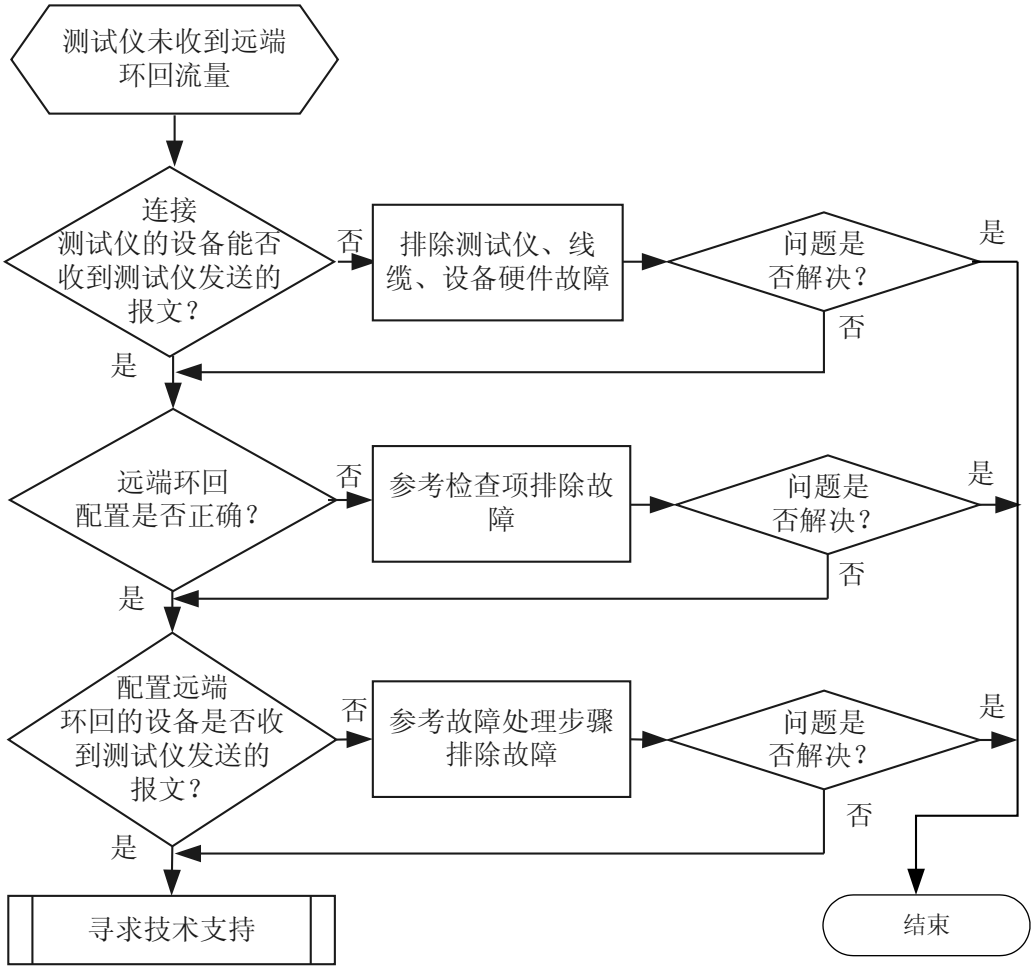
如图 5-9 所示，如果测试仪没有收到 SwitchA 环回的流量，可能有如下原因：

- 远端环回未启动
- 配置远端环回的报文的 VLAN ID 和远端环回的接口所在 VLAN 的 VLAN ID 不一致
- 测试仪配置构造的报文的源和目的 MAC 地址和远端环回接口上配置的不一致
- 测试仪故障
- 测试仪构造的报文不是 IP 报文
- SwitchA 和 SwitchB 之间的链路存在故障
- SwitchA 或 SwitchB 的设备或接口模块故障

故障诊断流程

详细处理流程如图 5-10 所示。

图 5-10 测试仪未收到远端环回流量的故障诊断流程图



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 SwitchB 上是否收到测试仪发的构造报文。

在 SwitchB 上执行 **display mac-address** 命令，查看显示信息中“MAC Address”字段显示的 MAC 地址是否有测试仪构造报文的源 MAC 地址，并且 MAC 地址学习到的接口为测试仪所连接的接口。

- 如果 SwitchB 未学到测试仪构造报文的源 MAC 地址，请做如下检查：

  1. 确保测试仪配置正确，测试仪构造的报文必须是 IP 报文。
  2. 确保测试仪和设备之间线缆无故障。

  完成上述确认后，如果 SwitchB 仍然未学到测试仪构造报文的源 MAC 地址，请尝试将连接测试仪的线缆连接到其他空闲端口，如果完成后 SwitchB 仍然未学到测试仪构造报文的源 MAC 地址，请执行步骤 4。

- 如果 SwitchB 学习到了测试仪构造报文的源 MAC 地址，并且 MAC 地址学习到的接口为测试仪所连接的接口，请执行步骤 2。

步骤 2 检查远端环回配置是否正确。

在 SwitchA 上执行命令 **display loopback swap-mac information**，查看对应端口配置的远端环回的运行状态。

显示信息	显示信息解释说明	后续操作
“Loopback state”	“Loopback state”字段表示远端环回的状态： ● “running”表示环回检测已经运行 ● “stop”表示环回检测未运行	● 如果“Loopback state”字段对应的显示信息为“running”表环回检测已经在运行。 ● 如果“Loopback state”字段对应的显示信息为“stop”表环回检测未运行，请在运行远端环回的接口上执行 **Loopback swap-mac start** 启动远端环回。
“Loopback source MAC ”	环回报文的源 MAC 地址。	● 如果“Loopback source MAC ”字段对应的 MAC 地址和测试仪构造的源地址不相同，请在运行远端环回的接口上执行 **loopback remote swap-mac** 重新配置源 MAC 地址或者更改测试仪构造的源地址。
“Loopback destination MAC”	环回报文的目的 MAC 地址。	● 如果“Loopback destination MAC”字段对应的 MAC 地址和测试仪构造的目的地址不相同，请在运行远端环回的接口上执行 **loopback_remote_swap-mac.**重新配置目的 MAC 地址或者更改测试仪构造的目的地址。
“Loopback vlan”	远端环回报文所在 VLAN。	● 如果“Loopback vlan”字段对应的 VLAN ID 和远端环回接口所属 VLAN 不同，请在运行远端环回的接口上执行 **loopback remote swap-mac** 重新配环回报文所在的 VLAN。

执行完上述检查后，如果故障依然存在请执行步骤 3。

步骤 3 检查 SwitchA 上是否收到测试仪构造的报文。

在 SwitchA 上执行 **display mac-address** 查看 SwitchA 上是否学习到了测试仪构造的报文的 MAC 地址，查看显示信息中“MAC Address”字段显示的 MAC 地址是否有测试仪构造报文的源 MAC 地址，并且 MAC 地址学习到的接口为配置远端环回的接口。

- 如果 SwitchA 未学到测试仪构造报文的源 MAC 地址，请确保 SwitchA 和 SwitchB 链路正常。完成上述确认后，如果 SwitchA 仍然未学到测试仪构造报文的源 MAC 地址，请确认 SwitchA 和 SwitchB 之间其他业务的连通情况：
  - 如果 SwitchA 和 SwitchB 其他业务也不通，有可能是 SwitchA 和 SwitchB 两端的接口存在故障，请尝试更换线缆连接到其他空闲端口，并将端口加入到指定的 VLAN，完成后 SwitchA 仍然未学到测试仪构造报文的源 MAC 地址，请执行步骤 4。
  - 如果 SwitchA 和 SwitchB 其他业务正常，请执行步骤 4。
- 如果 SwitchA 学习到了测试仪构造报文的源 MAC 地址，并且 MAC 地址学习到的接口为测试仪所连接的接口，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

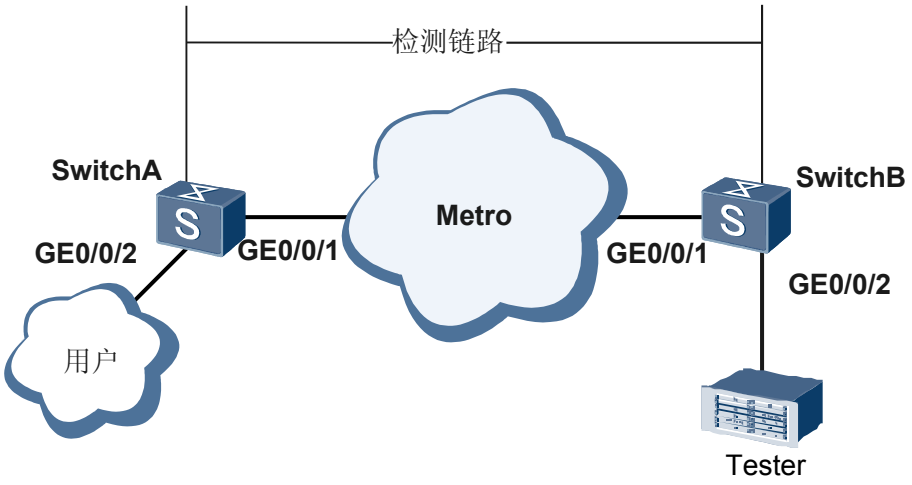
5.6.2 测试仪未收到本端环回流量的定位思路

介绍配置本端环回后未收到环回流量的故障原因、处理流程和详细的故障处理步骤。

常见原因

如图 5-11 所示，在 SwitchA 上的 GE0/0/2 上配置了本端环回，在 SwitchB 上通过测试仪打流，检测 SwitchB 的 GE0/0/2 到 SwitchA 的 GE0/0/2 之间连通性，其中 SwitchA 的接口 GE0/0/1、GE0/0/2 和 SwitchB 的接口 GE0/0/1、GE0/0/2 被划分在同一个 VLAN。

图 5-11 本端环回的典型组网图



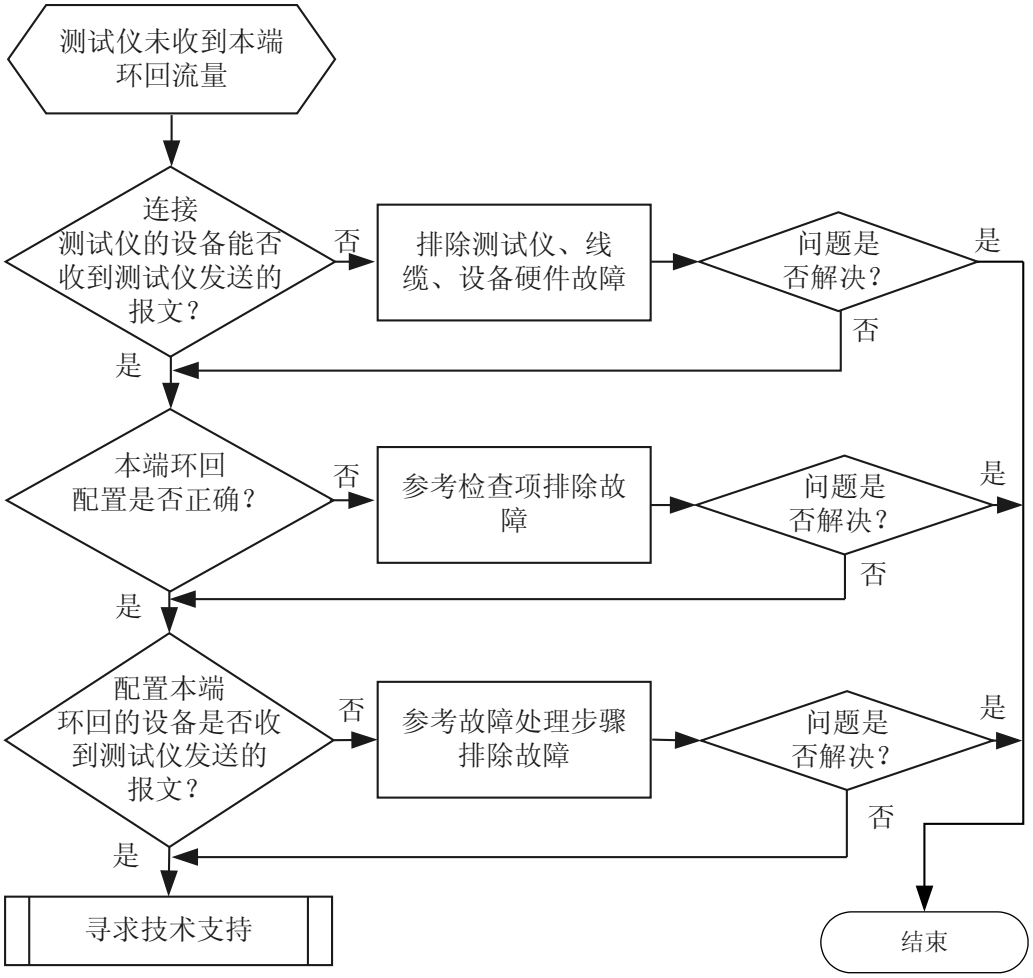
如图 5-11 所示，测试仪没有收到 SwitchA 环回的流量，可能有如下原因：

- 本端环回未启动
- 配置本端环回的报文的 VLAN ID 和本地环回的接口所在 VLAN 的 VLAN ID 不一致
- 测试仪配置构造的报文的源和目的 MAC 地址和本地环回接口上配置的不一致
- 测试仪故障
- 测试仪构造的报文不是 IP 报文
- SwitchA 和 SwitchB 之间的链路存在故障
- SwitchA 或 SwitchB 设备、接口模块故障

故障诊断流程

详细处理流程如图 5-12 所示。

图 5-12 测试仪未收到本端环回流量的故障诊断流程图



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 SwitchB 上是否收到测试仪发的构造报文。

在 SwitchB 上执行 **display mac-address** 查看显示信息中“MAC Address”字段显示的 MAC 地址是否有测试仪构造报文的源 MAC 地址，并且 MAC 地址学习到的接口为测试仪所连接的接口。

- 如果 SwitchB 未学到测试仪构造报文的源 MAC 地址，请做如下检查：

  1. 确保测试仪配置正确。
  2. 确保测试仪和设备之间线缆无故障。

  完成上述确认后，如果 SwitchB 仍然未学到测试仪构造报文的源 MAC 地址，请尝试将连接测试仪的线缆连接到其他空闲端口，如果完成后 SwitchB 仍然未学到测试仪构造报文的源 MAC 地址，请执行步骤 4。

- 如果 SwitchB 学习到了测试仪构造报文的源 MAC 地址，并且 MAC 地址学习到的接口为测试仪所连接的接口，请执行步骤 2。

步骤 2 检查本端环回配置是否正确。

在 SwitchA 上执行命令 **display loopback swap-mac information**，查看对应端口配置的本端环回的运行状态。

显示信息	显示信息解释说明	后续操作
“Loopback state”	“Loopback state”字段表示本端环回的状态： - “running”表示环回检测已经运行 - “stop”表示回检测未运行	- 如果“Loopback state”字段对应的显示信息为“running”表环回检测已经在运行。 - 如果“Loopback state”字段对应的显示信息为“stop”表环回检测未运行，请在运行本端环回的接口上执行 **loopback swap-mac start** 启动本端环回。
“Loopback source MAC ”	环回报文的源 MAC 地址。	- 如果“Loopback source MAC ”字段对应的 MAC 地址和测试仪构造的源地址不相同，请在运行本端环回的接口上执行 **loopback local swap-mac** 重新配置源 MAC 地址或者更改测试仪构造的源地址。
“Loopback destination MAC”	环回报文的目的 MAC 地址。	- 如果“Loopback destination MAC”字段对应的 MAC 地址和测试仪构造的目的地址不相同，请在运行本端环回的接口上执行 **loopback local swap-mac** 重新配置目的 MAC 地址或者更改测试仪构造的目的 MAC 地址。
“Loopback vlan”	本端环回报文所在 VLAN。	- 如果“Loopback vlan”字段对应的 VLAN ID 和本端环回接口所属 VLAN 不同，请在运行本端环回的接口上执行 **loopback local swap-mac** 重新配环回报文所在的 VLAN。

执行完上述检查后，如果故障依然存在请执行步骤 3。

步骤 3 检查 SwitchA 上是否收到测试仪发的构造报文。

在 SwitchA 上执行 **display mac-address** 查看 SwitchA 上是否学习到了测试仪构造的报文的 MAC 地址，查看显示信息中“MAC Address”字段显示的 MAC 地址是否有测试仪构造报文的源 MAC 地址，并且 MAC 地址学习到的接口为配置本端环回的接口。

- 如果 SwitchA 未学到测试仪构造报文的源 MAC 地址，请确保 SwitchA 和 SwitchB 链路正常。完成上述确认后，如果 SwitchA 仍然未学到测试仪构造报文的源 MAC 地址，请确认 SwitchA 和 SwitchB 之间其他业务的连通情况：
  - 如果 SwitchA 和 SwitchB 其他业务也不通，有可能是 SwitchA 和 SwitchB 两端的接口存在故障，请尝试更换线缆连接到其他空闲端口，并将的端口加入到指定的 VLAN，完成后 SwitchA 仍然未学到测试仪构造报文的源 MAC 地址，请执行步骤 4。
  - 如果 SwitchA 和 SwitchB 其他业务正常，请执行步骤 4。
- 如果 SwitchA 学习到了测试仪构造报文的源 MAC 地址，并且 MAC 地址学习到的接口为测试仪所连接的接口，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

5.7 VLAN Mapping 故障处理

介绍 VLAN Mapping 故障的定位思路。

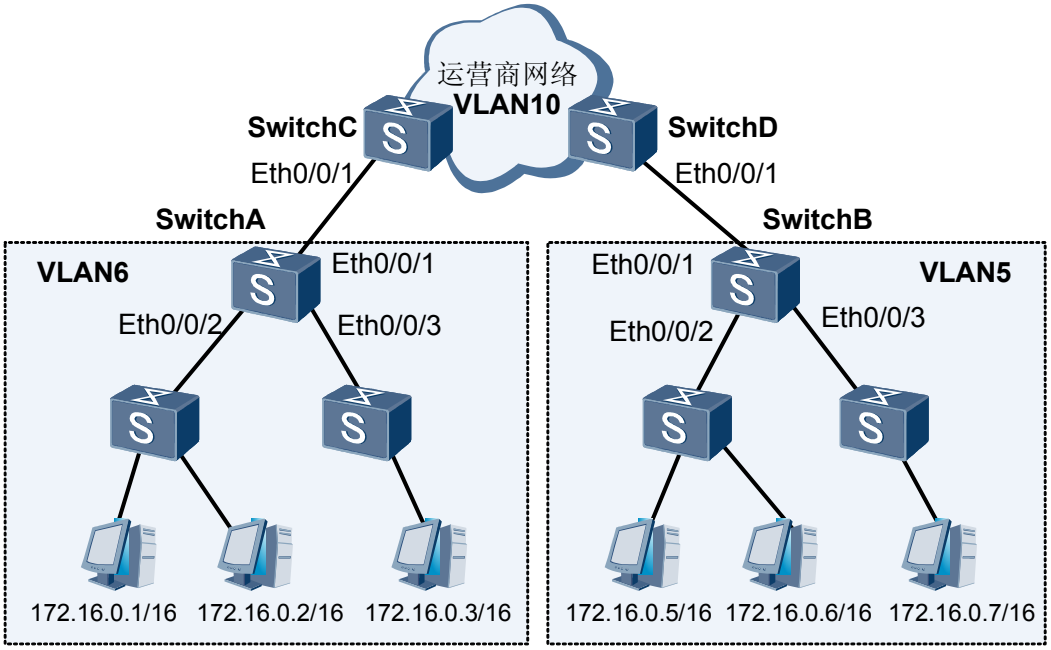
5.7.1 配置 VLAN Mapping 后用户无法通信的定位思路

介绍配置 VLAN Mapping 后用户无法通信的故障原因、处理流程和详细的故障处理步骤。

常见原因

在如图 5-13 所示的网络中，VLAN6 内的用户需要通过运营商网络 VLAN10 与 VLAN5 内的用户通信，在 SwitchC 和 SwitchD 的 GE0/0/1 上分别部署了单层 Tag 的 VLAN Mapping，分别将用户的 VLAN 映射成运营商的 VLAN，其中 VLAN5、VLAN6 为用户 VLAN，VLAN10 为 map-vlan。

图 5-13 VLAN Mapping 组网图



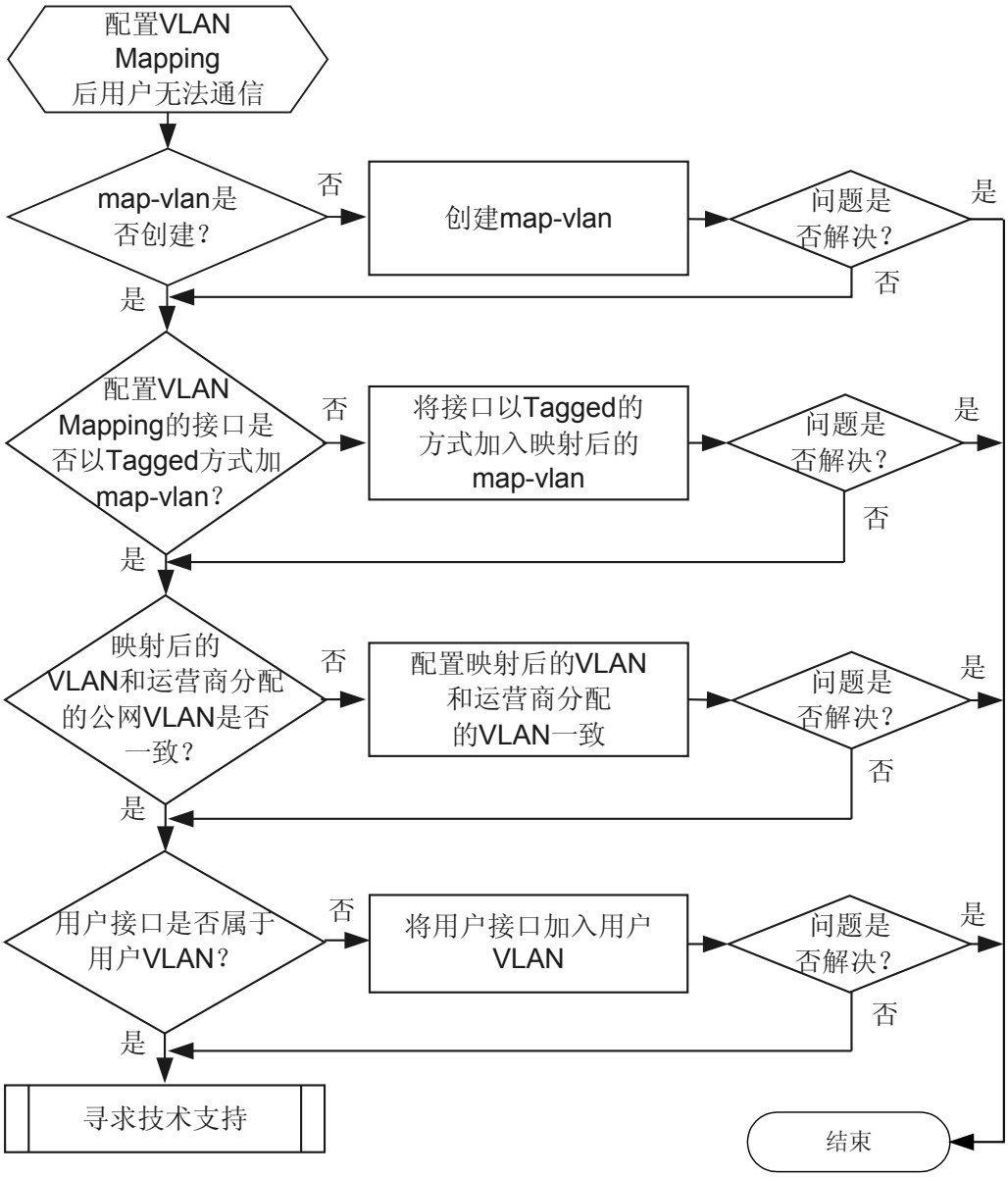
配置 VLAN Mapping 后用户无法正常通信，可能有如下原因：

- map-vlan 未创建
- 配置 VLAN Mapping 的接口未加入 map-vlan
- SwitchC 和 SwitchD 配置的映射后的 VLAN 和运营商分配的公网 VLAN 不一致
- 配置 VLAN Mapping 的接口故障

故障诊断流程

详细处理流程如图 5-14 所示。

图 5-14 配置 VLAN Mapping 后用户无法通信的故障诊断流程图



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 map-vlan 在交换机上是否创建。

分别在 SwitchC 和 SwitchD 上执行 **display vlan** 命令查看 map-vlan 是否被创建。

- 如果未创建请在系统视图下执行 **vlan** 命令创建 VLAN。
- 如果 map-vlan 已经创建，请执行步骤 2。

步骤 2 检查配置 VLAN Mapping 接口是否以 Tagged 的方式加入映射后的 map-vlan。

分别在 SwitchC 和 SwitchD 配置 VLAN Mapping 的接口上执行 **display this** 命令查看接口是否以 Tagged 的方式加入映射后的 map-vlan。

说明

- 配置 VLAN Mapping 功能的接口类型必须为 Trunk 或 Hybrid，接口必须以 Tagged 的方式加入映射后的 map-vlan。
- 当 VLAN 的取值为 *vlan-id1* to *vlan-id2* 时，接口还需要以 Tagged 的方式加入映射前的 vlan，并且 map-vlan 不允许配置成 VLANIF 接口。
- MAC 地址学习限制可能会影响 N：1 的 VLAN Mapping 功能正常使用。
- 如果未以 Tagged 的方式加入映射后的 map-vlan，请在接口视图下执行 **port trunk allow-pass vlan** 或 **port hybrid tagged vlan** 命令将接口以 Tagged 方式加入创建 map-vlan。
- 如果以 Tagged 的方式加入映射后的 map-vlan，请执行步骤 3。

步骤 3 检查 SwitchC 和 SwitchD 配置的映射后的 VLAN 和运营商分配的公网 VLAN 是否一致。

分别在 SwitchC 和 SwitchD 配置 VLAN Mapping 的接口上执行 **display this** 查看接口上配置的映射后的 VLAN 和运营商分配的公网 VLAN 是否一致。

- 如果接口上配置的映射后的 VLAN 和运营商分配的公网 VLAN 不一致，请在配置 VLAN Mapping 的接口上执行 **undo port vlan-mapping vlan** 删除当前配置，然后再使用 **port vlan-mapping vlan** 命令配置 Mapping 后的 VLAN 和运营商分配的公网 VLAN 一致。
- 如果接口上配置的映射后的 VLAN 和运营商分配的公网 VLAN 一致，请执行步骤 4。

步骤 4 检查连接用户的接口是否属于用户 VLAN。

分别在 SwitchA 和 SwitchB 上执行 **display vlan** *vlan-id* 命令查看用户 VLAN 中是否包括用户接口。

- 如果未包括用户接口，请使用命令 **port trunk allow-pass vlan**、**port hybrid tagged vlan** 或 **port default vlan** 将接口加入用户 VLAN。
- 如果包括用户接口，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

5.8 环路故障处理

介绍了环路常见故障的定位思路和案例。

5.8.1 环路导致设备产生广播风暴的定位思路

介绍环路导致设备产生广播风暴的故障处理流程和详细的故障处理步骤。

常见原因

网络出现环路后会导致广播风暴，同时可能会有如下现象产生：

- 设备无法远程登录。
- 在设备上使用 **display interface** 命令查看接口统计信息时发现接口收到大量广播报文。
- 使用串口登录设备进行操作时，操作比较慢。
- CPU 占用率超过 70%。
- 通过 **ping** 命令进行网络测试时丢包严重。
- 设备上发生环路的 VLAN 的接口指示灯频繁闪烁。
- PC 机上通过抓包软件获得大量的广播报文。
- 设备部署环路检测后，设备出现环路告警。

本类故障的常见原因主要包括：

- 设备线缆连接错误导致环路。

  错误连接线缆导致环路典型场景如图 5-15、图 5-16 所示。其中：

  - 图 5-15 中用户将 SwitchB 中相同 VLAN 的两个接口用线缆连接起来导致设备产生环路。

    对于图 5-15 组网的场景，可以采用如下方式检测环路：

    - 在 SwitchA 上部署 Loopback Detection，并且 Loopback Detection 的处理动作配置为发现环路后产生告警，根据告警信息确认环路产生的设备、接口和 VLAN，如果告警信息中发生环路的接口为连接 SwitchB 的接口，证明环路发生在 SwitchB 上，如果未产生告警证明环路发生在 SwitchA 上。确认发生广播风暴的设备之后，再根据接口广播风暴的统计信息或者接口指示灯的状态判断环路可能产生的接口，在环路可能产生的接口上执行 **shutdown** 命令或拔出线缆，如果广播风暴消失证明该接口产生环路。
    - 在 SwitchA 连接 SwitchB 的接口执行 **shutdown** 命令或拔出线缆，此时广播风暴仍然存在证明环路发生在 SwitchA，如果广播风暴消失证明环路发生在 SwitchB。确认发生广播风暴的设备之后，再根据接口广播风暴的统计信息或者接口指示灯的状态判断环路可能产生的接口，在环路可能产生的接口上执行 **shutdown** 命令或拔出线缆，如果广播风暴消失证明该接口产生环路。

  - 图 5-16 中用户错误的将 SwitchE 和 SwitchF 连接起来，由于 SwitchD、SwitchE、SwitchF 之间互联的接口属于同一个 VLAN，SwitchE 和 SwitchF 连接后网络便产生环路。

    对于图 5-16 组网的场景，可以采用如下方式判断环路产生的设备：

    - 在 SwitchC 上配置 Loopback Detection，并且 Loopback Detection 的处理动作配置为发现环路后产生告警，根据告警信息的中的接口判断环路产生的设

备，如果告警信息中发生环路的接口为连接 SwitchD 的接口，证明环路可能发生在 SwitchD、SwitchE、SwitchF 上。如果没有告警，证明环路发生在 SwitchC。确认发生广播风暴的设备之后，再根据接口广播风暴的统计信息或者接口指示灯的状态判断环路可能产生的接口，在环路可能产生的接口上执行 **shutdown** 命令或拔出线缆，如果广播风暴消失证明该接口产生环路。

图 5-15 错误线缆连接导致环路典型场景

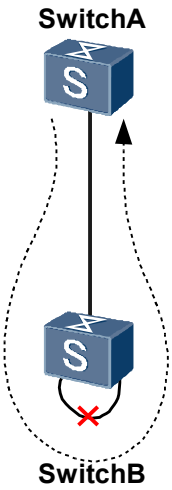
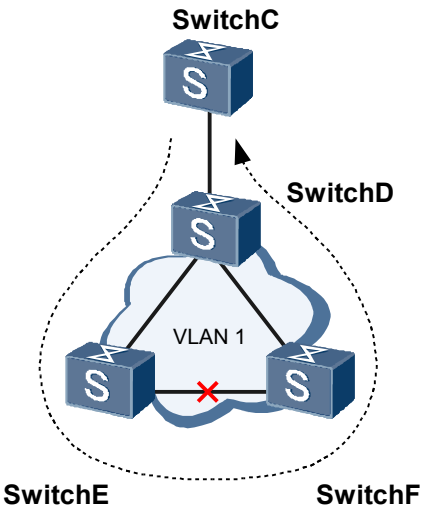


图 5-16 错误线缆连接导致环路典型场景



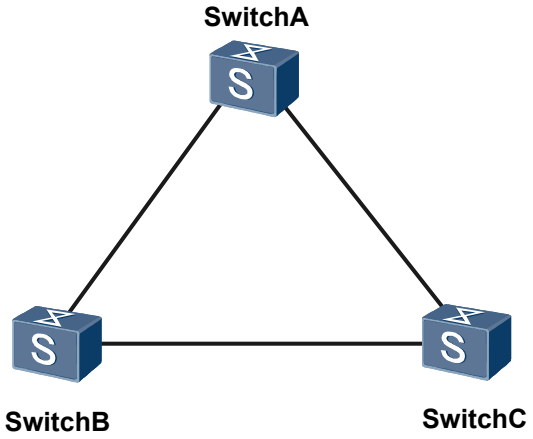
- 网络未规划环路，由于用户的错误配置导致环路。

  错误配置导致环路典型场景如图 5-17 所示。其中 SwitchA 和 SwitchB 互联接口、SwitchA 和 SwitchC 互联接口都允许 VLAN X 通过，按照规划 SwitchB 和 SwitchC 之间互联的接口不允许 VLAN X 通过，但实际用户配置时 SwitchB 和 SwitchC 之间接口错误配置允许 VLAN X 通过从而导致网络出现环路。

  对于图 5-17 组网的场景，可以在采用如下方式进行环路检测：

  - 根据接口广播风暴的统计信息或者接口指示灯的状态判断环路可能产生的接口，在环路可能产生的接口上执行 **shutdown** 命令或拔出线缆，如果广播风暴消失证明该接口产生环路，确认了存在环路的接口后，检查接口配置的允许通过的 VLAN 配置是否正确。

图 5-17 错误配置导致环路典型场景



设备线缆连接错误导致环路故障处理步骤

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 确认存在广播风暴的接口。

可以采用如下方式确认存在广播风暴的接口。

- 通过观察接口指示灯状态，如果接口指示灯频繁闪烁，可以判断该接口可能存在广播风暴。
- 在设备上执行 **display interface brief** 命令查看接口接收方向和发送方向最近一段时间的带宽利用率。

  显示信息中“InUti”字段表示入方向上的带宽利用率，“OutUti”字段表示出方向上的带宽利用率。接口接收方向和发送方向最近一段时间的带宽利用率接近 100%的接口可能是存在广播风暴的接口。

步骤 2 判断环路产生的设备。

说明

在使用通过在接口上执行 **shutdown** 命令或拔出线缆方式关闭当前接口来判断本设备是否存在环路时，因为此操作会导致通过该接口的业务中断，在执行此操作前，请先和管理员确认。环路排除后请及时执行 **undo shutdown** 命令开启当前接口。

- 如果存在广播风暴的接口没有下连其他 Switch，此时可以判断环路发生在该 Switch 上，请执行步骤 3。
- 如果存在广播风暴的接口下连其他 Switch，此时环路可能发生在该 Switch 上也可能发生在下连 Switch 上，此时可以选择如下方式进行环路检测：
  - 采用环路检测协议进行环路检测：

    说明

    在部署环路检测协议之前，可以通过如下方式获取可能发生环路的 VLAN 信息：

    - 查找广播风暴所在的接口所属 VLAN。
    - 用户反馈的故障主机所在的 VLAN。

    - 在 Switch 上针对指定 VLAN 部署 Loopback Detection 协议，检测存在环路的接口，并且 Loopback Detection 的处理动作配置为发现环路后产生告警。

Loopback Detection 的配置方法请参见《AC6605 无线接入控制器 配置指南-以太网》中“Loopback Detection 配置”。如果 Switch 产生 **LDT 1.3.6.1.4.1.2011.5.25.174.3.3 hwLdtPortLoopDetect** 告警，请根据告警中提示的接口信息确认产生环路的接口。如果产生环路的接口是下连其他 Switch 的接口，证明环路发生在下连 Switch。如果未产生告警，证明环路产生在本 Switch。

执行完上述操作后如果本 Switch 还下连其他 Switch，并且发生环路的设备为下连 Switch，请重复执行上述操作。确认发生环路的设备后请执行步骤 3。

- 如果存在多个接口下连其他 Switch，并且该接口产生广播风暴，说明环路可能发生在设备与设备之间，请执行步骤 3。

- 在下连接口上执行 **shutdown** 命令，观察本设备和整个网络是否存在广播风暴。
  - 执行上述操作后如果本设备存在广播风暴，下连 Switch 不存在广播风暴，证明环路发生在本 Switch，请执行步骤 3。
  - 执行上述操作后如果存在广播风暴的接口没有下连其他 Switch，此时可以判断环路发生在该 Switch 上。请执行步骤 3。
  - 执行上述操作后如果本 Switch 和整个网络中广播风暴消失，证明环路发生在设备和设备之间，请执行步骤 3。

  如果下连其他 Switch，并且下游设备仍存在广播风暴，请继续在下连 Switch 上重复执行上述操作。

步骤 3 判断产生环路的接口并破环。

- 如果环路发生在单个设备上，说明环路是因为本设备两个属于相同 VLAN 的接口直接连接导致，可以采用如下方式进行环路排除：
  - 根据广播风暴产生的接口逐个排查该接口连接的线缆对端是不是本设备的其他接口，如果是请拔出线缆。
  - 在产生广播风暴的接口执行 **shutdown** 命令，如果此时广播风暴消失，并且在执行 **shutdown** 命令时设备上另外一个接口变成 Down 状态，此时证明这两个接口为产生环路的接口，此时请和管理员确认后拔出接口线缆。
- 执行步骤 3 操作时，如果确认环路发生在设备之间，此时参考网络规划，排查和本设备相连的其他设备之间是否存在错误的连接导致网络形成环路。根据广播风暴产生的接口逐个排查该接口连接的线缆对端设备是不是和规划中的一样，查找出错误连接并拔出线缆。

执行完上述步骤后故障仍然存在请执行步骤 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

由于用户的错误配置导致环路故障处理步骤

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 确认存在广播风暴的接口。

在网络中所有发生广播风暴的设备上确认产生广播风暴的接口，可以采用如下方式确认存在广播风暴的接口。

- 通过观察接口指示灯状态，如果接口指示灯频繁闪烁，可以判断该接口可能存在广播风暴。
- 在设备上执行 **display interface brief** 命令查看接口接收方向和发送方向最近一段时间的带宽利用率。

  显示信息中“InUti”字段表示入方向上的带宽利用率，“OutUti”字段表示出方向上的带宽利用率。接口接收方向和发送方向最近一段时间的带宽利用率接近 100%的接口可能是存在广播风暴的接口。

步骤 2 确认并修改错误配置。

根据发生广播风暴的接口所属的 VLAN，和网络管理员确认哪些设备之间不允许发生环路的 VLAN 通过，确认完成之后在设备两端修改允许通过 VLAN 的配置。执行完上述操作后如果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。

- 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

LDT_1.3.6.1.4.1.2011.5.25.174.3.3 hwLdtPortLoopDetect

相关日志

无

5.9 Loopback Detection 故障处理

介绍 Loopback Detection 故障的定位思路。

5.9.1 配置 Loopback Detection 后设备仍然存在广播风暴的定位思路

介绍配置 Loopback Detection 后设备仍然存广播风暴的故障原因、处理流程和详细的故障处理步骤。

常见原因

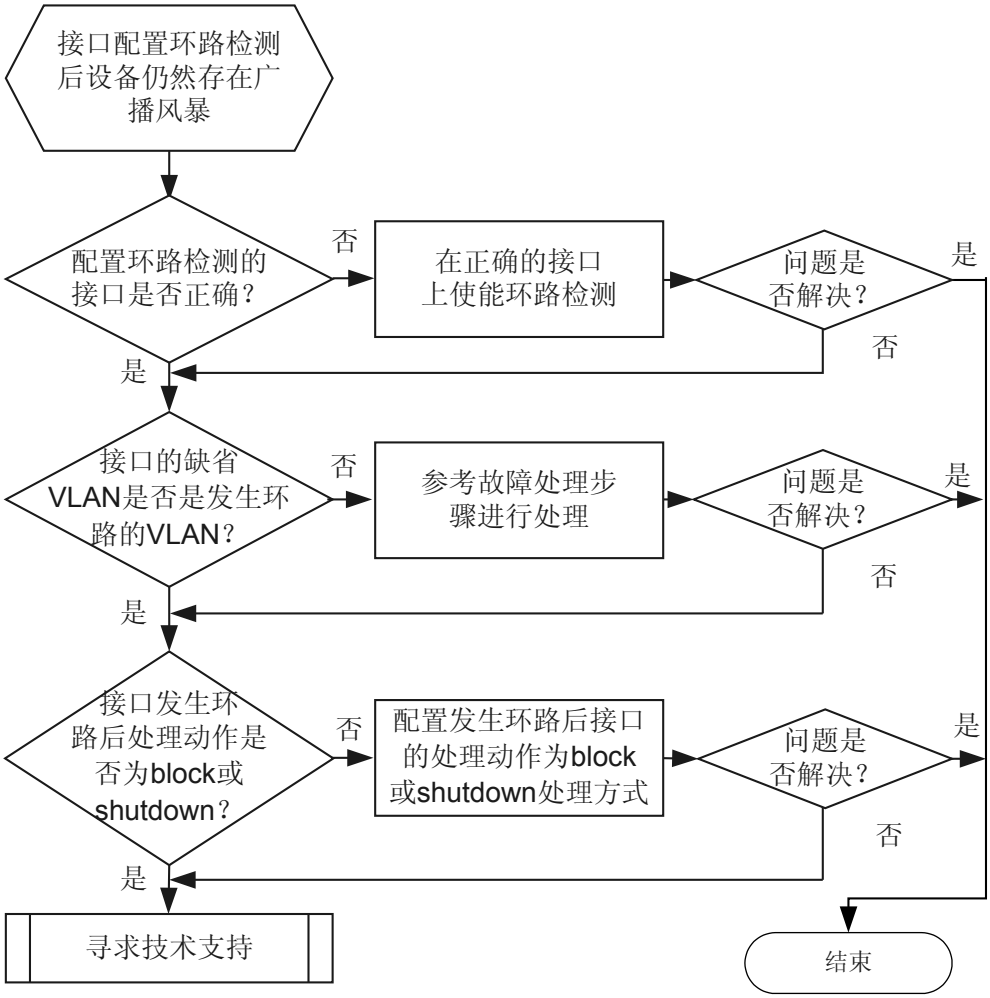
部署环路检测后设备仍然存在广播风暴可能有如下原因：

- 配置环路检测的接口错误
- 环路检测接口缺省 VLAN 和发生环路接口所在的 VLAN 不是一个 VLAN
- 检测出环路后设备没有 block 或 shutdown 接口

故障诊断流程

详细处理流程如图 5-18 所示。

图 5-18 配置环路检测后设备依然存在广播风暴的故障诊断流程图



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 检查配置环路检测的接口是否正确。

在 Switch 连接发生环路网络的接口上执行 **display this** 命令，如果有“loopback-detect enable”信息表示环路检测已经使能。

- 如果没有“loopback-detect enable”信息，请在接口或系统视图下执行 **loopback-detect enable** 使能环路检测。
- 如果有“loopback-detect enable”信息，请执行步骤 2。

步骤 2 检查接口的缺省 VLAN 是否是发生环路的 VLAN。

- 接口的缺省 VLAN 不是发生环路的 VLAN 时，请执行如下操作：
  - 如果接口允许多个 VLAN 以 untagged 方式通过，请在本端和对端执行 **port trunk allow-pass vlan** 或 **port hybrid tagged vlan** 命令将允许通过的 VLAN 以 tagged 方式加入，完成后执行 **loopback-detect packet vlan***vlan-id* 命令配置对指定 VLAN 的报文进行环路检测。
  - 如果接口允许多个 VLAN 以 Tagged 方式通过，请在接口上执行 **loopback-detect packet vlan***vlan-id* 命令配置对指定 VLAN 的报文进行环路检测。
- 接口的缺省 VLAN 是发生环路的 VLAN 时，请执行步骤 3。

步骤 3 检查接口的 Loopback Detection 处理动作是否为 block 或 shutdown。

在系统视图下执行 **display loopback-detect** 命令查看环路检测的配置信息，查看显示信息中“Action”对应的字段是否为 block 或 shutdown。

说明

接口的环路检测处理动作为 block 时，当环路消失后会自动恢复。接口的环路检测处理动作为 shutdown 时，当环路消失后接口不能自动恢复。

- 如果接口的环路检测处理动作不是 block 或 shutdown 时，请执行 **loopback-detect action** 命令配置接口的环路检测处理动作为 block 或 shutdown。
- 如果接口的环路检测处理动作是 block 或 shutdown 时，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

6 IP 业务类

关于本章

6.1 IP 地址故障处理

6.1.1 接口下配置 IP 地址不成功的定位思路

常见原因

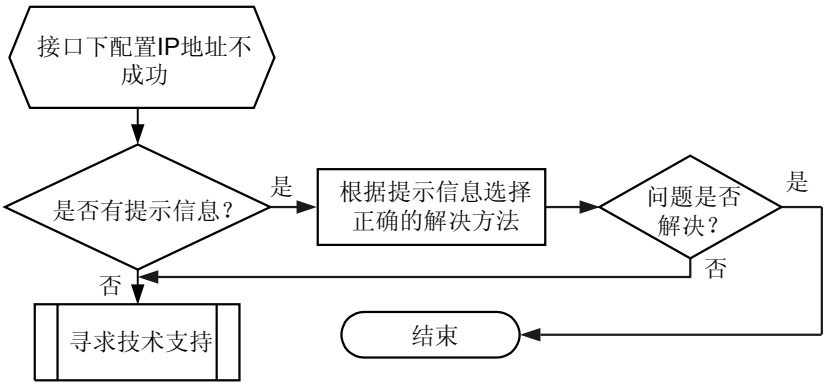
本类故障的常见原因主要包括：

- 接口下配置的 IP 地址或子网掩码错误，为无效的 IP 地址。
- 接口下配置的 IP 地址冲突。
- 在接口下配置的从 IP 地址超过最大数目，无法继续配置从 IP 地址。
- 因为配置了地址借用，接口下无法配置从 IP 地址。
- 接口下已经有相同的从 IP 地址了，应该配置其他的从 IP 地址。

故障诊断流程

详细处理流程如图 6-1 所示。

图 6-1 接口下配置 IP 地址不成功的故障诊断流程图



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 根据表 6-1 检查错误提示信息，并对照采取故障排除方法。

表 6-1 错误提示信息及对应的故障排除方法

错误提示信息	错误提示信息解释	故障排除方法
Error: The specified IP address is invalid.	无效的 IP 地址，IP 地址或子网掩码错误。	请检查后重新配置。 ● IP 地址是否属于常用的 A、B、C 三类 IP 地址中的一种。 ● 子网掩码是否正确。
Error: The specified address conflicts with another address.	IP 地址冲突，本设备的其他接口已使用了该 IP 地址。	请使用其他 IP 地址进行配置。
Error: The specified primary address does not exist.	删除的主地址不存在。 **说明** 一个接口只能有一个主 IP 地址，当配置主 IP 地址时，如果接口上已经有主 IP 地址，则原主 IP 地址被删除，新配置的地址成为主 IP 地址。	无需执行删除操作。
Error: Please configure the primary address in the interface view first.	无法配置从 IP 地址。 **说明** 在配置地址借用的情况下，不能配置从 IP 地址。	先配置主 IP 地址
Error: The number of addresses of the specified interface reached the upper limit (9).	在接口上配置的从 IP 地址超过最大数目，无法继续配置从 IP 地址。 **说明** 默认情况下，每个接口下最多可以配置 8 个从 IP 地址。	-
Error: Please delete the sub address in the interface view first.	无法删除主 IP 地址。	请先删除接口下所有的从 IP 地址，再删除主 IP 地址。
Error: The specified address cannot be deleted because it is not the primary address of this interface.	无法删除从 IP 地址，无法使用删除主 IP 地址的命令删除从 IP 地址。	请执行删除从 IP 地址的命令 **undo ip address** *ip-address* { *mask* | *mask-length* } **sub**。
Error: The specified sub address does not exist.	删除的从 IP 地址不存在。	无需执行删除操作。
Error: The address already exists.	接口下已经有相同的从 IP 地址了，应该配置其他的从 IP 地址。	请使用其他的从 IP 地址进行配置。

步骤 2 如果没有上述提示信息，但是接口 IP 地址没有配置成功，请联系华为技术支持工程师。

----结束

相关告警与日志

相关告警

无

相关日志

无

6.1.2 接口下配置借用 IP 地址后无法通讯的定位思路

常见原因

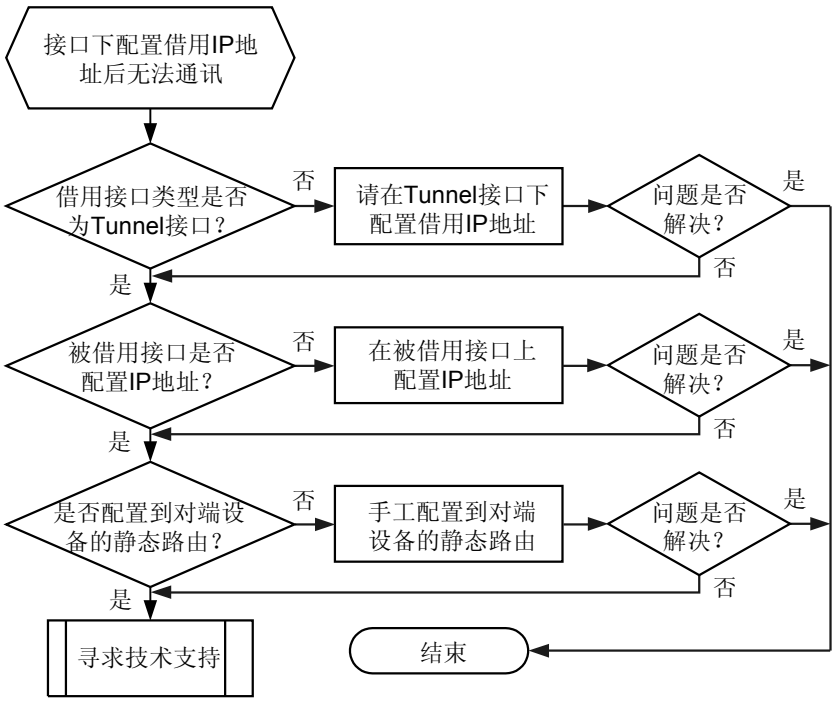
本类故障的常见原因主要包括：

- 借用接口类型不是 Tunnel 接口。
- 被借用接口本身没有配置 IP 地址。
- AC6605 上借用接口没有配置到对端设备的静态路由。

故障诊断流程

详细处理流程如图 6-2 所示。

图 6-2 接口下配置借用 IP 地址后无法通讯的故障诊断流程图



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 检查借用接口类型是否为 Tunnel 接口。

说明

目前 AC6605 仅支持 Tunnel 接口借用 Loopback 接口的 IP 地址，以太网接口不能借用其他接口的 IP 地址。

查看配置借用 IP 地址的接口类型。

- 如果是 GigabitEthernet 等接口视图，请进入 Tunnel 接口视图下，执行命令 **ip address unnumbered interface** *interface-type interface-number* 配置借用 IP 地址。
- 如果是 Tunnel 接口视图，请执行步骤 2。

步骤 2 检查被借用接口是否已经配置了 IP 地址。

在被借用接口视图下执行命令 **display this**，检查该接口下是否已经配置了 IP 地址。

- 如果没有 **ip address x.x.x.x** 字段，请在该被借用接口视图下执行命令 **ip address** *ip-address* { *mask* | *mask-length* }配置 IP 地址。
- 如果有 **ip address x.x.x.x** 字段，请执行步骤 3。

步骤 3 检查 AC6605 上是否配置了到对端设备的静态路由。

说明

由于借用接口本身没有 IP 地址，无法在此接口上启用动态路由协议，所以必须手工配置一条到对端设备的静态路由，才能实现 AC6605 与对端设备之间的连通。

执行命令 **display ip routing-table**，检查 **Proto** 值等于 **Static** 的路由中是否有到对端设备的静态路由。

- 如果在这些静态路由中，没有 **Destination/Mask** 值等于对端设备的目的 IP 地址，说明没有配置静态路由，请执行命令 **ip route-static** *ip-address* { *mask* | *mask-length* } { *nexthop-address* | *interface-type interface-number* [*nexthop-address*] }，配置静态路由。
- 如果在这些静态路由中，有 **Destination/Mask** 值等于对端设备的目的 IP 地址，说明已经正确配置了静态路由，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

6.2 DHCP 故障处理

6.2.1 客户端无法获取 IP 地址的定位思路（AC6605 作为 DHCP Server）

常见原因

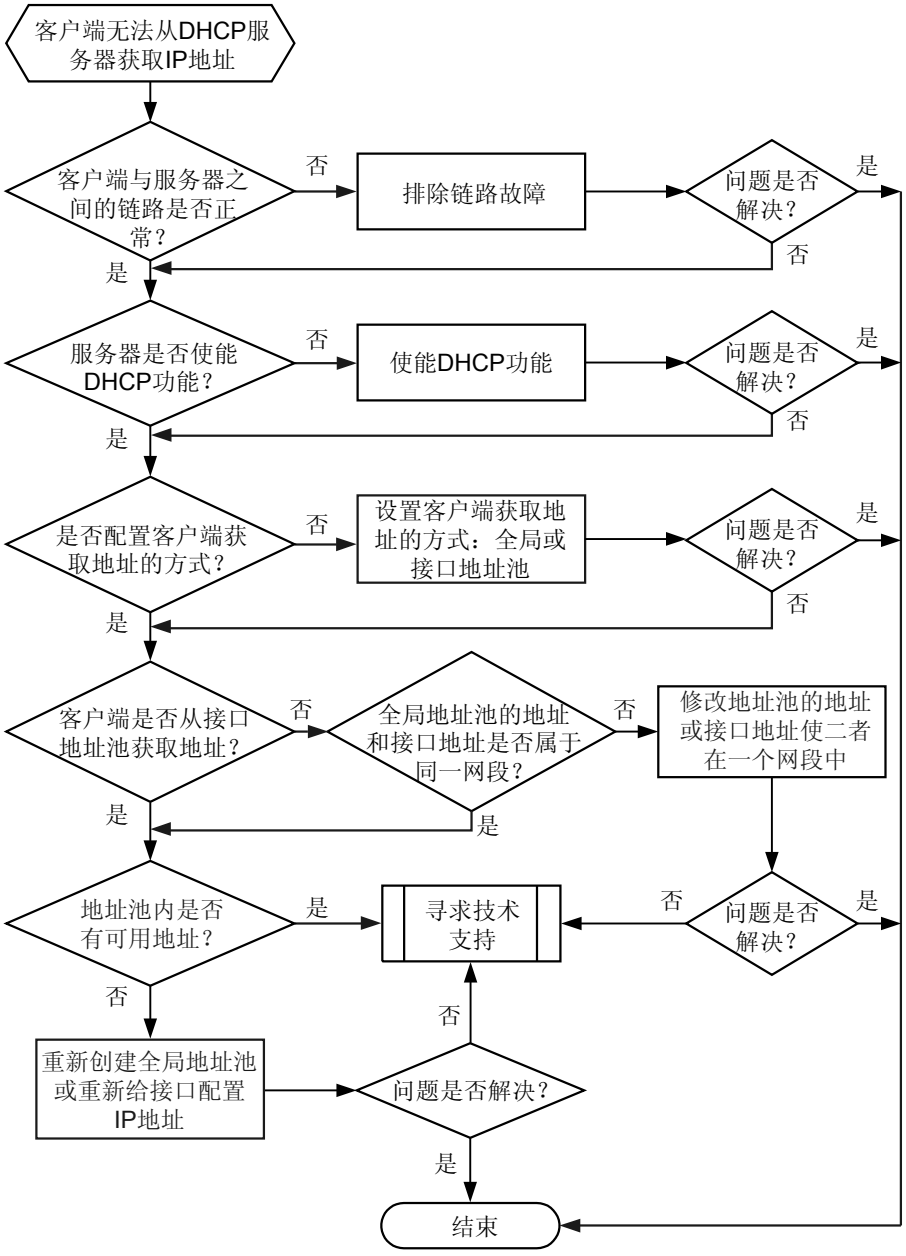
本类故障的常见原因主要包括：

- 客户端与服务器之间的链路有故障。
- AC6605 未使能 DHCP 功能。
- AC6605 VLANIF 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，中间没有中继设备时，全局地址池中的 IP 地址与 AC6605 VLANIF 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 地址与中继设备的 VLANIF 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 6-3 所示。

图 6-3 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，中间没有中继设备时，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 VLANIF 接口的 IP 地址在同一网段，从客户端 Ping VLANIF 接口的 IP 地址。

- 如果 Ping 不通，请先根据 **7.2.1 PING 不通故障处理思路**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 **7.2.1 PING 不通故障处理思路**排除链路的故障。
  - 如果能 Ping 通，请执行步骤 2。

步骤 2 检查 DHCP 功能是否处于使能状态。

说明

如果未使能 DHCP 功能，则 AC6605 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 AC6605 VLANIF 接口下是否选择 DHCP 分配地址的方式。

说明

如果 AC6605 VLANIF 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 VLANIF 接口以 DHCP 的方式来获取 IP 地址。

在 AC6605 VLANIF 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	VLANIF 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	VLANIF 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	VLANIF 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 VLANIF 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 VLANIF 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，中间没有中继设备时：
  - 如果全局地址池中的 IP 地址与 AC6605 VLANIF 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 VLANIF 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 AC6605 VLANIF 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 VLANIF 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 VLANIF 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 VLANIF 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 VLANIF 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 VLANIF 接口选择接口地址池为 DHCP 客户端分配 IP 地址，可以重新为 VLANIF 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

6.2.2 客户端无法获取 IP 地址的定位思路（AC6605 作为 DHCP Relay）

常见原因

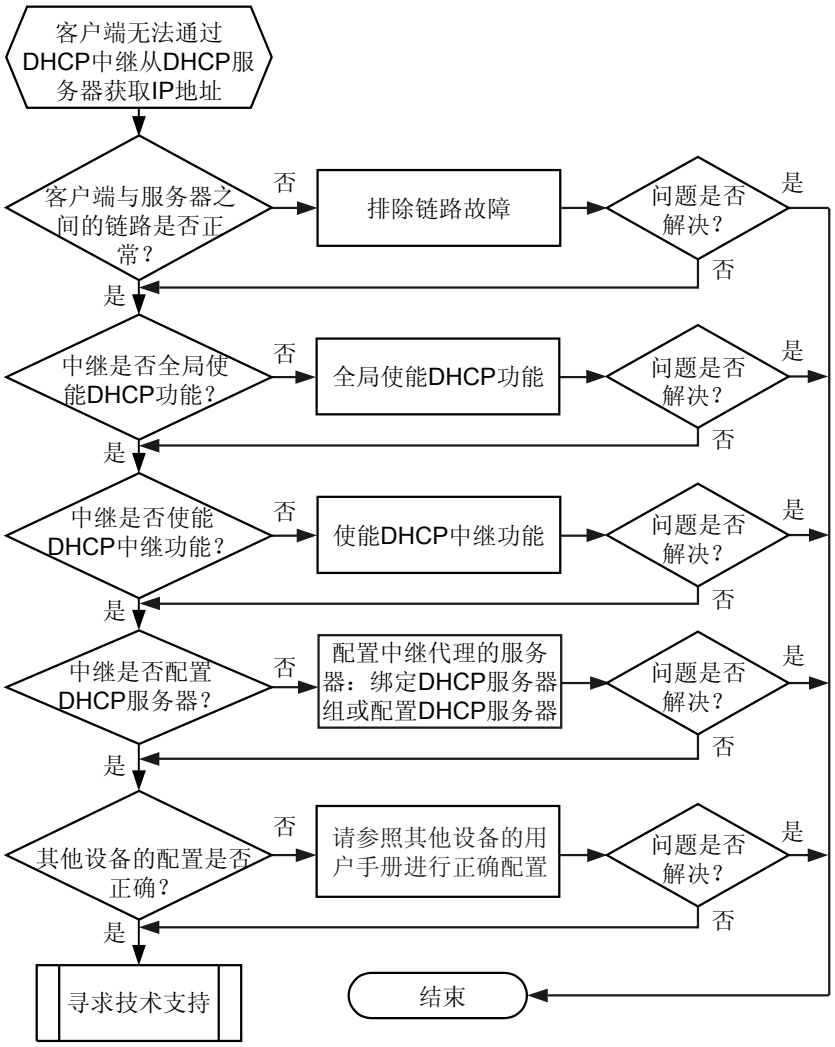
本类故障的常见原因主要包括：

- 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。
- AC6605 未全局使能 DHCP 功能，导致 DHCP 功能没有生效。
- AC6605 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 VLANIF 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 6-4 所示。

图 6-4 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



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 VLANIF 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 **7.2.1 PING 不通故障处理思路**排除链路的故障。
   - 如果能 Ping 通，请执行步骤 b。

2. 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 **7.2.1 PING 不通故障处理思路**排除链路的故障。
   - 如果能 Ping 通，请执行步骤 2。

步骤 2 检查 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 AC6605 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 AC6605 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 AC6605 VLANIF 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。

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 AC6605 VLANIF 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 VLANIF 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 VLANIF 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 检查链路上其他设备的配置是否正确，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 **6.2.1 客户端无法获取 IP 地址的定位思路（AC6605 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

相关日志

无

6.3 DHCPv6 故障处理

6.3.1 客户端无法获取 IPv6 地址的定位思路（AC6605 作为 DHCPv6 Relay）

常见原因

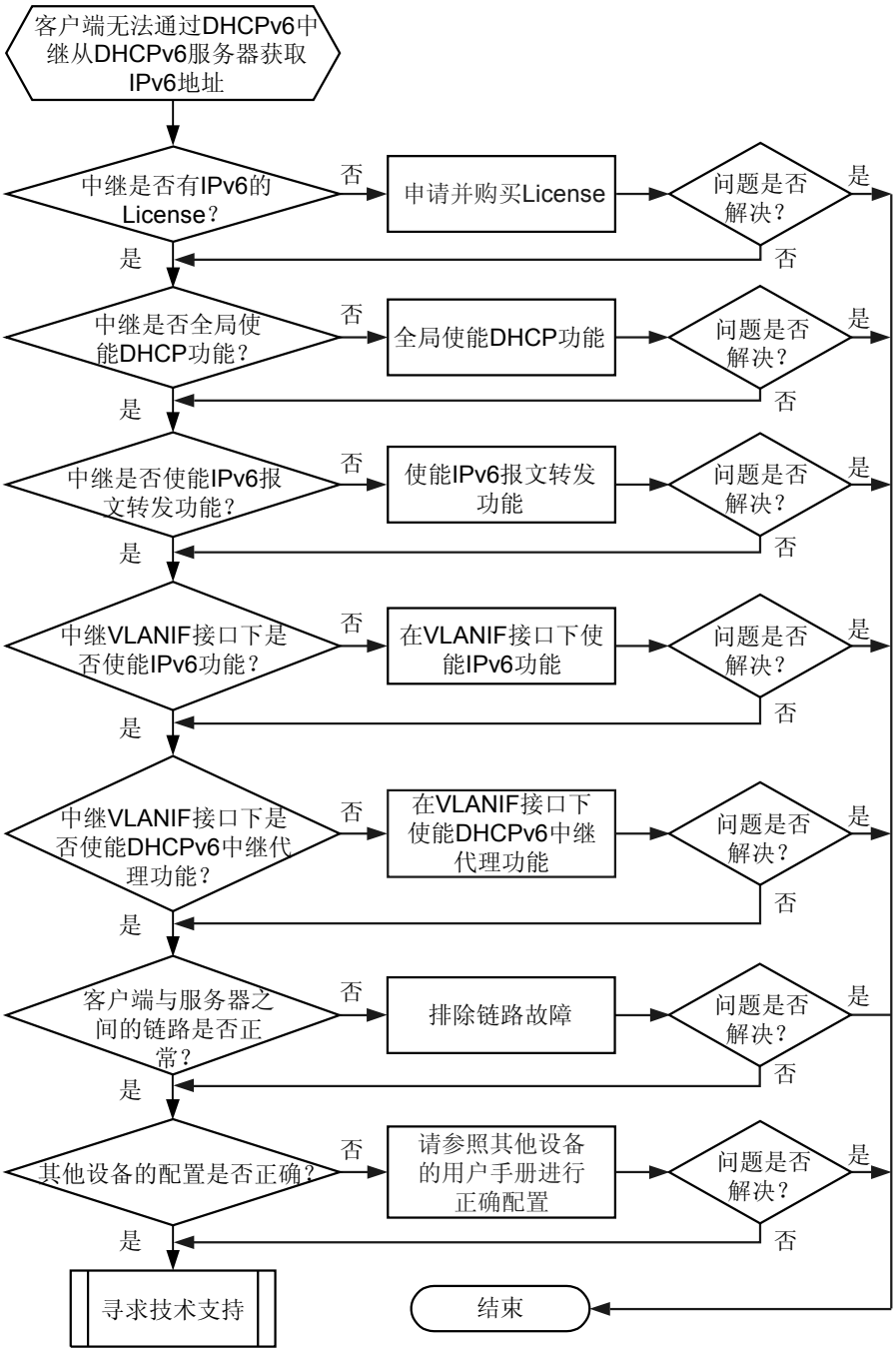
本类故障的常见原因主要包括：

- AC6605 没有 IPv6 的 License。
- AC6605 未全局使能 DHCP 功能。
- AC6605 未使能 IPv6 报文转发功能。
- AC6605 VLANIF 接口下未使能 IPv6 功能。
- AC6605 VLANIF 接口下未使能 DHCPv6 中继代理功能。
- 客户端与 DHCPv6 服务器之间的链路有故障。
  - 客户端与 DHCPv6 中继之间的链路有故障。
  - DHCPv6 中继与 DHCPv6 服务器之间的链路有故障。
- 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 6-5 所示。

图 6-5 客户端无法通过 DHCPv6 中继从 DHCPv6 服务器获取 IPv6 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 DHCPv6 中继是否具有 IPv6 的 License。

说明

一般情况下，新购买的设备 IPv6 功能相关命令可以在设备上配置，但是 IPv6 相关功能并不实现。如果需要实现 AC6605 的 IPv6 功能，请联系华为办事处申请并且购买 License。

执行命令 **display license**，检查是否具有 IPv6 的 License，AC6605 的 IPv6 功能使用 License 控制。

- 如果显示有 IPv6 的 License，请执行步骤 2。
- 如果无 IPv6 的 License，请联系华为办事处申请并且购买 License。

步骤 2 检查 DHCPv6 中继是否全局使能 DHCP 功能。

说明

如果未全局使能 DHCP 功能，则 AC6605 不会处理客户端上送的 DHCPv6 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 DHCPv6 中继是否使能 IPv6 报文转发功能。

执行命令 **display current-configuration | include ipv6**，检查 IPv6 报文转发功能是否已经使能。缺省情况下，IPv6 报文转发功能未使能。

- 如果显示 **ipv6**，说明 IPv6 报文转发功能已经处于使能状态，请执行步骤 4。
- 如果无上述显示信息，说明 IPv6 报文转发功能处于未使能状态，请执行命令 **ipv6**，使能 IPv6 报文转发功能。

步骤 4 检查 DHCPv6 中继 VLANIF 接口下是否使能 IPv6 功能。

在连接客户端侧的 VLANIF 接口视图下，执行命令 **display this**，检查 IPv6 功能是否已经使能。缺省情况下，IPv6 功能未使能。

- 如果显示 **ipv6 enable** 字段，说明 IPv6 功能已经处于使能状态，请执行步骤 5。
- 如果无上述显示字段，说明 IPv6 功能处于未使能状态，请在 VLANIF 接口视图下执行命令 **ipv6 enable**，使能 IPv6 功能。

步骤 5 检查 DHCPv6 中继 VLANIF 接口下是否使能 DHCPv6 中继代理功能。

说明

如果 DHCPv6 中继未使能，则客户端无法跨网段来获取 IPv6 地址。

在连接客户端侧的 VLANIF 接口视图下，执行命令 **display this**，检查 DHCPv6 中继代理功能是否已经使能。缺省情况下，DHCPv6 中继代理功能未使能。

- 如果显示 **dhcpv6 relay destination** *ipv6-address* 字段，说明 DHCPv6 中继代理功能已经处于使能状态，请执行步骤 6。
- 如果无上述显示字段，说明 DHCPv6 中继代理功能处于未使能状态，请在 VLANIF 接口视图下执行命令 **dhcpv6 relay destination** *ipv6-address*，使能 DHCPv6 中继代理功能。

步骤 6 检查客户端与 DHCPv6 服务器之间的链路是否有故障。

1. 检查客户端与 DHCPv6 中继之间的链路是否有故障。

   在客户端手工配置与 DHCPv6 中继用户侧接口位于同一网段的 IPv6 地址（不能与已经分配的 IPv6 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 **7.2.1 PING 不通故障处理思路**排除链路的故障。
   - 如果能 Ping 通，请执行步骤 b。

2. 检查 DHCPv6 中继与 DHCPv6 服务器之间的链路是否有故障。

   在 DHCPv6 中继上执行命令 **ping ipv6 -a** *source-ip-address destination-ip-address*，*source-ip-address* 为 DHCPv6 中继 VLANIF 接口的 IPv6 地址，*destination-ip-address* 为 DHCPv6 服务器的 IPv6 地址。

   - 如果 Ping 不通，请先根据 **7.2.1 PING 不通故障处理思路**排除链路的故障。
   - 如果能 Ping 通，请执行步骤 7。

步骤 7 检查链路上其他设备的配置是否正确，主要包括 DHCPv6 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 IPv6 地址，请执行步骤 8。

步骤 8 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

6.4 IPv6 基础故障处理

6.4.1 IPv6 业务流量转发异常的定位思路

常见原因

本类故障的常见原因主要包括：

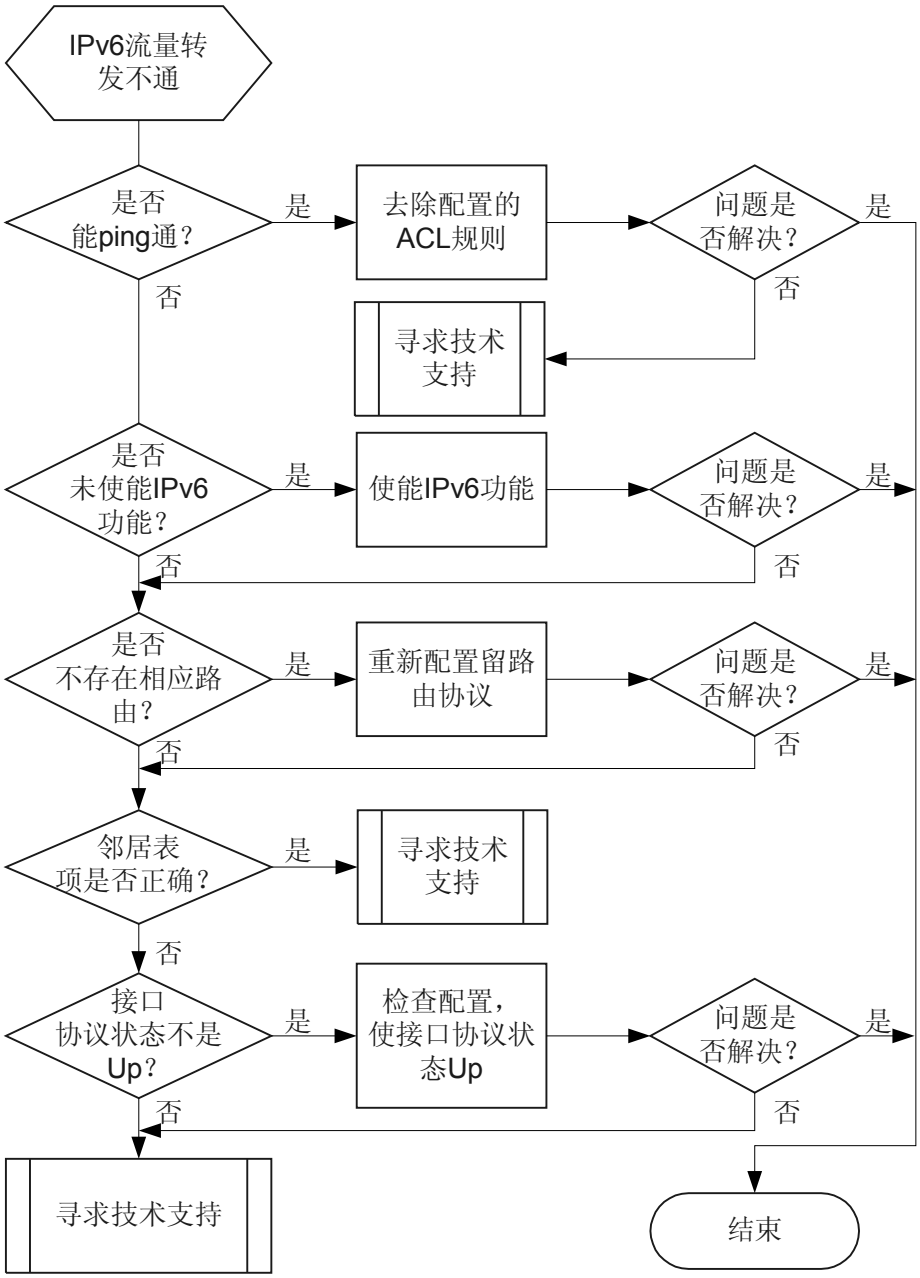
- IPv6 路由配置不正确

- 无法获取下一跳的邻居表项
- 链路问题
- 接口协议不 Up

故障诊断流程

详细处理流程如图 6-6 所示。

图 6-6 IPv6 业务流量转发异常的故障诊断流程图



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 在交换机上检查是否能 ping 通目的地址。

执行 **ping ipv6** 命令，查看目的地址是否可达。

- 如果不能 ping 通，请执行步骤 3。
- 如果能够 ping 通，请执行步骤 2。

步骤 2 查看交换机上是否配置了 ACL 规则。

执行 **display acl ipv6 all** 命令，查看是否存在用户自定义的 ACL 规则与转发的业务流量匹配。检查方法如下：抓包查看报文，分析报文中的信息（如 IP 地址、MAC 地址、DSCP 值、VLAN ID、802.1p 值等）是否与用户自定义 ACL 中的规则匹配。

- 如果匹配，执行 **rule** 命令修改用户自定义 ACL 中的规则。
- 如果不匹配，请执行步骤 7。

步骤 3 检查交换机上是否使能了 IPv6 功能。

分别在全局视图和接口视图下查看是否使能了 IPv6 功能。缺省情况下，全局和接口视图均不使能 IPv6 功能。

- 具体查看办法如下：
  - 在系统视图下，执行 **display current-configuration** | *include ipv6* 命令，查看是否存在“**ipv6**”字段，如果不存在，请执行 **ipv6** 命令。
  - 执行 **display ipv6 interface** *interface-type interface-number* 命令，查看是否存在“**IPv6 is enabled**”字段，如果不存在，请在逻辑接口视图下执行 **ipv6 enable** 命令。
- 如果已经使能了 IPv6 功能，请执行步骤 4。

步骤 4 检查交换机上是否有到目的地址的路由。

执行 **display ipv6 routing-table** 命令查询交换机上的 IPv6 路由表的信息，查看是否存在到达目的地址的路由。如果存在路由信息则应显示如下：

```
Routing Table : Public
       Destinations : 1        Routes : 1

 Destination  : ::1                          PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Static
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : Vlanif10                     Flags        : D
```

- 如果不存在相应的路由表项，请检查路由配置是否正确，如果不正确请参见《Quidway AC6605 无线接入控制器 配置指南-IP 路由》。
- 如果存在对应的路由表项，请执行步骤 5。

步骤 5 检查交换机学到的邻居表项是否正确。

执行 **display ipv6 neighbors** 命令查看邻居表项。

- 如果没有对应的邻居表项，说明未获取到下一跳的邻居信息，请执行步骤 6。
- 如果有下一跳对应的邻居表项，说明下一跳是可达的，请执行步骤 7。

步骤 6 检查交换机上的对应的 VLANIF 接口的 IPv6 的协议状态是否 Up。

- 如果 VLANIF 接口的协议状态是 Down，请执行下表中的检查项。

检查项	判断标准及后续处理步骤
物理状态是否 Up	VLANIF 接口的状态为 Down 可能由于对应的物理接口 Down，具体处理办法请参见**以太网接口物理 Down 的定位思路**。
加入 VLAN 的方式是否相同	执行 **display vlan** *vlan-id* 命令，查看链路两端加入 VLAN 的方式是否相同，即两端接口加入 VLAN 的方式均为 untagged 或是 tagged，如果不相同，请修改配置使其相同。
地址状态是否冲突	执行 **display ipv6 interface brief** 命令，查看 IPv6 地址的状态信息。如果 IPv6 地址的状态是 **DUPLICATE**，说明地址产生了冲突，请找出发生地址冲突的设备，重新配置。 **说明** 在 IPv6 地址刚配置时，IPv6 地址的状态会产生短暂的 **TENTATIVE** 状态，此时地址并未产生冲突。

- 如果协议状态是 Up 的，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

7 IP 转发及路由类

关于本章

7.1 二三层报文转发故障处理

7.1.1 总体定位思路

二三层流量转发不通是极为常见的故障，典型表现为丢包。定位此类问题的总体思路如下：确认丢包的设备—>确认具体原因—>求助华为技术支持工程师。

- 步骤一：确认丢包的设备

  1. 缩小故障范围，定位出可能存在丢包的设备。

     在接口视图下执行 **display interface** *interface-type interface-number* 命令查看接口收发报文计数，初步判断本设备有没有丢包。

```
<Quidway> display interface GigabitEthernet 0/0/1
GigabitEthernet 0/0/1 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, GigabitEthernet 0/0/1 Interface
Switch Port,PVID :   10,The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-2000-0140
Last physical up time   : 2010-02-02 13:00:36 UTC+08:00
Last physical down time : 2010-02-02 10:48:49 UTC+08:00
Port Mode: COMMON FIBER
Speed : 1000,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
Mdi   : NORMAL
Last 300 seconds input rate 200 bits/sec, 0 packets/sec
Last 300 seconds output rate 192 bits/sec, 0 packets/sec
Input peak rate 9488 bits/sec,Record time: 2010-02-02 13:00:39
Output peak rate 161305720 bits/sec,Record time: 2010-02-03 19:27:42

Input:  23446 packets, 6585114 bytes
  Unicast:               8506,  Multicast:               14931
  Broadcast:                9,  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:  307349487 packets, 22131770338 bytes
  Unicast:              16808,  Multicast:            307332535
  Broadcast:              144,  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%
```

     一般情况下，如果收发正常（即没有持续的 Discard，Error 计数增加），表示本设备不存在问题。需要沿转发路径，以同样的方法定位下一台设备是否存在问题。

  2. 在可能存在丢包的设备的入接口和出接口上部署流策略，分别统计入接口的 Inbound 方向和出接口的 outbound 方向的特定报文，以进一步确认该类报文是否在本设备被丢弃。

例如：统计从 GigabitEthernet0/0/2 接口发送的源 IP 为 10.142.132.248 目的 IP 为 10.142.132.81 的 ICMP 报文计数。

```
<Quidway> system-view
[Quidway] acl 3009
[Quidway-acl-adv-3009] rule 5 permit icmp source 10.142.132.248 0 destination
10.142.132.81 0
[Quidway] quit
[Quidway]traffic classifier icmp
[Quidway-classifier-icmp] if-match acl 3009
[Quidway-classifier-icmp] quit
[Quidway] traffic behavior icmp
[Quidway-behavior-icmp]statistic enable
[Quidway-behavior-icmp] quit
[Quidway] traffic policy icmp
[Quidway-trafficpolicy-icmp] classifier icmp behavior icmp
[Quidway-trafficpolicy-icmp] quit
[Quidway] interface GigabitEthernet 0/0/2
[Quidway-GigabitEthernet0/0/2] traffic-policy icmp outbound
[Quidway] display traffic policy statistics interface GigabitEthernet 0/0/2 outbound
 Interface: GigabitEthernet0/0/2
 Traffic policy outbound: icmp
 Rule number: 1
 Current status: OK!
 Board : 2
Item                                Packets                     Bytes
------------------------------------------------------------------------------
------
Matched                                   0                         0
 +--Passed                                0                         0
 +--Dropped                               0                         0
 +--Filter                                0                         0
 +--URPF                                  -                         -
 +--CAR                                   0                         0
```

- 如果入接口的 Inbound 方向有 Dropped 计数，可能是本设备的问题，也可能是上游设备的问题，请一并排查。
- 如果出接口的 outbound 方向有 Dropped 计数，说明是本设备发生了丢包。
- 如果入接口的 Inbound 方向的 Passed 计数=出接口 outbound 的 Passed 计数，说明本设备没有丢包，请排查下游设备是否有丢包。

说明

- 通过在流分类中配置不同的匹配规则来统计特定要求的报文，例如可以执行 **if-match cvlan-id** 配置基于 QinQ 报文内外两层 VLAN ID 的匹配规则，统计特定 QinQ 报文。
- 可以执行命令 **reset traffic policy statistics**{ **global** [**slot** *slot-id*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } **inbound** 清除统计信息。

- 步骤二：根据丢包的类型，确认具体的原因。
  - 二层报文转发丢包请参见 **7.1.2 二层报文转发丢包的故障定位思路**。
  - 三层报文转发丢包请参见 **7.1.3 三层报文转发丢包的故障定位思路**。
- 步骤三：搜集相关信息，求助华为技术支持工程师。

7.1.2 二层报文转发丢包的故障定位思路

常见原因

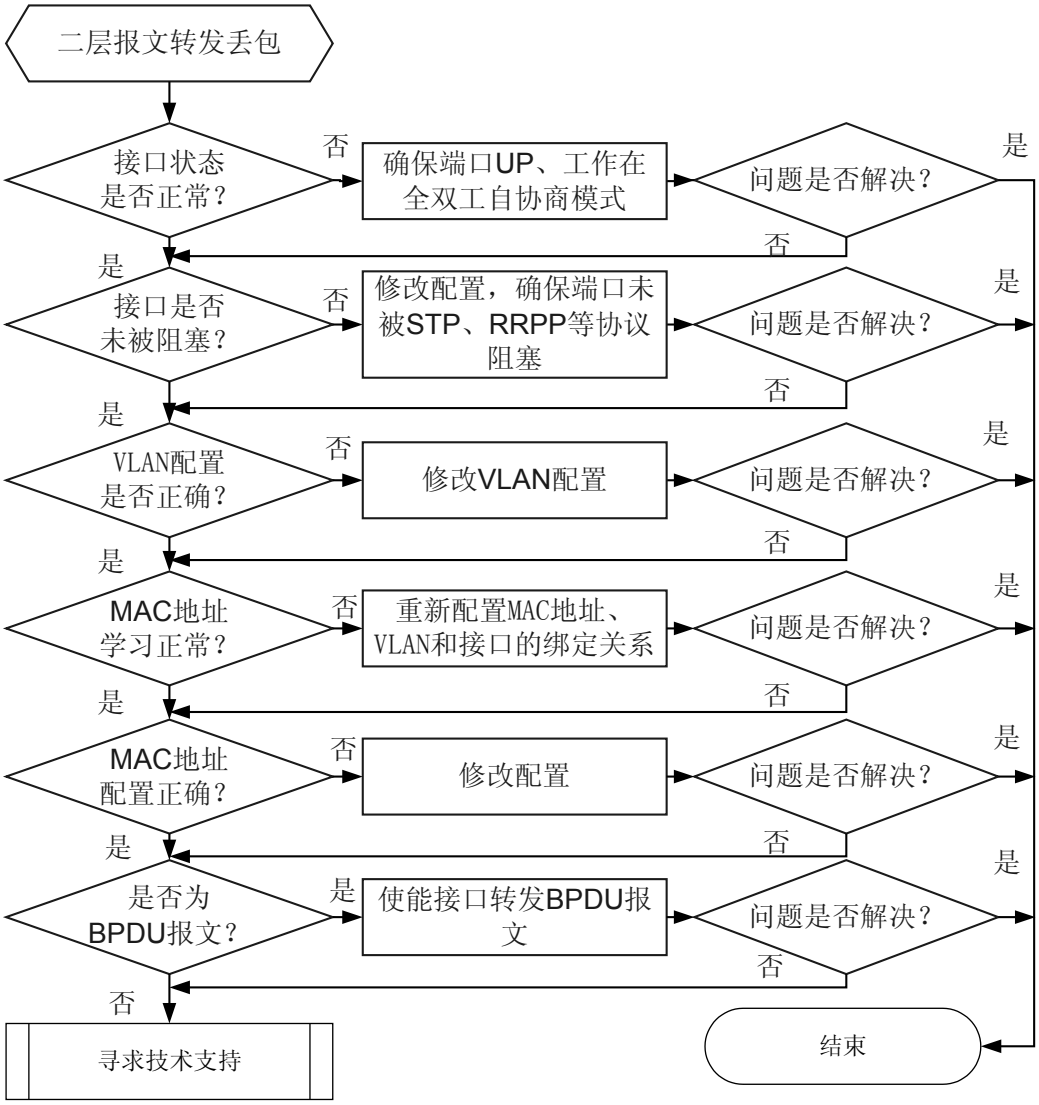
二层报文丢包常见原因主要包括：

- 接口的状态异常（如物理状态 Down，工作模式为半双工、和对端自协商不一致）
- 接口被 STP、RRPP、Smartlink、LDT 等协议阻塞
- 接口没有加入相应的 VLAN，导致接口不允许报文通过
- 设备 MAC 地址学习异常
- MAC 地址配置中存在导致丢包的一些配置，例如：
  - 关闭了 MAC 地址学习，并且指定丢弃动作
  - 配置 MAC 地址学习限制规则，对超过 MAC 地址学习数量限制的报文采取丢弃的动作
  - 配置了静态 MAC
  - 配置黑洞 MAC
  - 配置了端口安全
- 接口下配置了丢弃没有匹配灵活 QinQ 和 VLAN Mapping 的报文
- 接口下配置了丢弃入方向带 VLAN Tag 的报文
- 接口下未使能 BPDU 功能，导致无法透传 BPDU 报文

故障诊断流程

详细处理流程如图 7-1 所示。

图 7-1 二层报文转发丢包的故障诊断流程图



故障处理步骤

操作步骤

步骤 1 检查接口的运行状态。

在本端和对端设备上执行 **display interface** *interface-type interface-number* 命令查看接口运行状态。

```
<Quidway> display interface GigabitEthernet 0/0/1
GigabitEthernet0/0/1 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, GigabitEthernet0/0/1 Interface
Switch Port,PVID :   10,The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-2000-0140
Last physical up time   : 2010-02-02 13:00:36 UTC+08:00
Last physical down time : 2010-02-02 10:48:49 UTC+08:00
Port Mode: COMMON FIBER
```

```
Speed : 1000,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
 ---- More ----
```

如果接口的物理状态 Down，请参见 **4.1.1 以太网接口物理 Down 的定位思路**解决接口 Down 的故障。

- 如果工作模式不是全双工，请在接口视图下执行 **duplex full** 命令将接口设置为全双工模式。
- 如果自协商模式不一致，请在接口视图下执行 **negotiation auto** 命令调整接口的自协商模式。
- 对于电口，当出现协商成 10M/100M 工作正常，而协商成 1000M 工作异常时，请检测网线是否正常，如果有问题请更换网线。

如果接口物理状态为 UP、工作在全双工模式，并且自协商状态和对端一致，表明接口状态正常。请执行步骤 2。

步骤 2 查看接口是否被 STP、RRPP、LDT、SmartLink 等协议阻塞。

以 STP、RRPP 为例说明。

- 若交换机上配置了 STP 协议，需检查接口是否被 STP 阻塞。执行命令 **display stp brief** 查看接口状态，例如：

```
[Quidway] display stp brief
 MSTID      Port                  Role  STP State     Protection
   0        GigabitEthernet0/0/1  ROOT  FORWARDING     NONE
   0        GigabitEthernet0/0/2  DESI  FORWARDING     NONE
   0        GigabitEthernet0/0/3  DESI  FORWARDING     NONE
```

  转发正常情况下，接口的 STP state 字段为 **FORWARDING**。若该字段为 **DISCARDING**，则说明该接口上报文被 STP 阻塞。此时需要修改 STP 配置使该接口不处在 **DISCARDING** 状态，可修改 STP 的优先级使本交换机选举为根桥，使接口不被阻塞。方法如下：

  在系统视图下执行 **stp priority** *priority-level* 命令修改 STP 的优先级。其中，*priority-level* 的取值是 0 ～ 61440，取值越小则优先级越高，设置较低的优先级可使本交换机成为环路的根桥。

  若接口显示的状态都为 **FORWARDING** 状态，说明接口的 STP 状态正常。

- 若交换机上配置了 RRPP 协议，需检查接口是否被 RRPP 阻塞。执行命令 **display rrpp verbose domain** *domain-index* 查看接口状态，例如：

```
[Quidway] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 1000    sub 1001
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring      : 1
Ring Level     : 0
Node Mode      : Master
Ring State     : Failed
Is Enabled     : Enable         Is Actived : Yes
Primary port   : GigabitEthernet0/0/3        Port status: UP
Secondary port : GigabitEthernet0/0/4        Port status: DOWN
```

  若接口的 Port status 字段为 **BLOCK**，则说明该接口上报文被 RRPP 阻塞。此时需要修改 RRPP 配置使该接口不处在 BLOCK 状态。RRPP 协议阻塞的是副接口（Secondary port），所以需要重新规划修改配置，不要将该接口配置成 RRPP 协议的副接口。

  若接口的 Port status 字段都为 **Up**，则说明接口的 RRPP 状态正常。

说明

一般在同一接口上不会配置多种环路协议，所以先看接口目前配置了哪种协议类型，再查看对应的接口状态。

- 如果接口被阻塞，请修改相关配置，具体配置请参见《AC6605 无线接入控制器 配置指南》。
- 如果接口未被阻塞，请执行步骤 3。

步骤 3 检查接口的 VLAN 配置是否正确。

执行 **display vlan** *vlan-id* 命令查看接口是否以 Untagged 或 Tagged 方式加入到指定的 VLAN 中。

说明

- 如果接口配置了 PVID，对于 Untagged 的报文在入接口会被打上 PVID tag，此时需要将入接口加入 PVID VLAN。
- 对于配置灵活 QinQ 的接口，注意要将接口加入替换后的 VLAN。

```
<Quidway> display vlan 10
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------
10   common  UT:GE0/0/1(D)
             TG:GE0/0/2(U)

VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
10   enable  default       enable  disable    VLAN 0010
```

- 如果接口未加入到指定的 VLAN，表明配置不正确，请修改接口的 VLAN 配置。具体配置请参见《AC6605 无线接入控制器 配置指南-以太网配置》中的“VLAN 配置”。
- 如果接口已加入到指定的 VLAN，表明配置正确，请执行步骤 4。

步骤 4 检查源 MAC 地址学习是否正常。

在系统视图下执行 **display mac-address** 命令，检查源 MAC 地址和 VLAN、接口的绑定关系是否正确。对于配置了灵活 QinQ 的接口，源 MAC 是学习在替换后的外层 VLAN 上的。

```
<Quidway> display mac-address 0000-0000-0033
--------------------------------------------------------------------------------
MAC Address          VLAN/VSI                    Learned-From        Type
--------------------------------------------------------------------------------
0000-0000-0033         100/-                     GE0/0/2             dynamic
--------------------------------------------------------------------------------
Total items displayed = 1
```

- 如果源 MAC 没有学习到，请重新配置 MAC 地址、VLAN 和设备端口的绑定关系。
- 如果源 MAC 地址学习正常，请执行步骤 5。

步骤 5 检查 MAC 地址配置中是否有导致丢包的配置项。

检查项	检查命令	说明
是否关闭了 MAC 地址学习，并且指定丢弃动作	在接口视图下执行 **display this** 命令查看配置，显示信息有“ mac-address learning disable action discard ”。	配置此项时，接口不再进行 MAC 地址学习，当接收到的报文的源 MAC 与 MAC 地址表项不匹配时，则丢弃该报文。
是否配置了静态 MAC	执行 **display mac-address static** 命令查看静态 MAC 地址表项信息。	如果配置了静态 MAC，只有绑定了静态 MAC 的接口才会处理该 MAC 的报文，其他接口收到该 MAC 的报文直接丢弃。
是否配置了黑洞 MAC	执行 **display mac-address blackhole** 命令查看黑洞 MAC 地址表项信息。	如果配置了黑洞 MAC，当某个报文的源 MAC 地址或目的 MAC 地址等于黑洞 MAC 地址表项的 MAC 地址，该报文会被丢弃。
是否配置了接口安全	执行 **display this** 查看接口的配置，显示信息有“port-security enable ”。	配置此项时，接口会将学习到的 MAC 地址转换为安全动态 MAC 地址。当接口学习的安全动态 MAC 数量达到上限后（缺省上限为 1），不再学习新的 MAC 地址，对超过 MAC 地址学习数量限制的报文采取直接丢弃的动作。

- 如果因配置错误导致丢包，请修改配置，详细配置请参见《AC6605 无线接入控制器 配置指南-以太网配置》中的“MAC 表配置”。
- 如果配置正确，请执行步骤 6。

步骤 6 检查接口下是否有其他特殊配置。

在接口视图下执行 **display this** 查看接口的配置。

```
[Quidway-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 qinq vlan-translation miss-drop
 port discard tagged-packet
#
return
```

- **qinq vlan-translation miss-drop**:灵活 QinQ 和 VLAN Mapping 接口下配置该命令后，接口会对没有匹配叠加前或映射前的 VLAN 的入报文进行丢弃。
- **port discard tagged-packet**:配置该命令的接口将丢弃入方向带 VLAN Tag 的报文。
- 如果因配置错误导致丢包，请修改配置，通过执行 **undo port discard tagged-packet**、**undo qinq vlan-translation miss-drop** 取消配置。
- 如果配置正确，请执行步骤 7。

步骤 7 检查报文是否为 BPDU 报文。

BPDU 报文的目的 MAC 一般为：01:80:C2:00:00:xx。默认情况下，入端口会对接收到的 BPDU 报文进行丢弃。如果需要透传 BPDU 报文，请配置二层协议透明传输功能，具体

配置请参见《AC6605 无线接入控制器 配置指南-以太网配置》中的“二层协议透明传输配置”。

如果故障仍然存在，请执行步骤 8。

步骤 8 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

7.1.3 三层报文转发丢包的故障定位思路

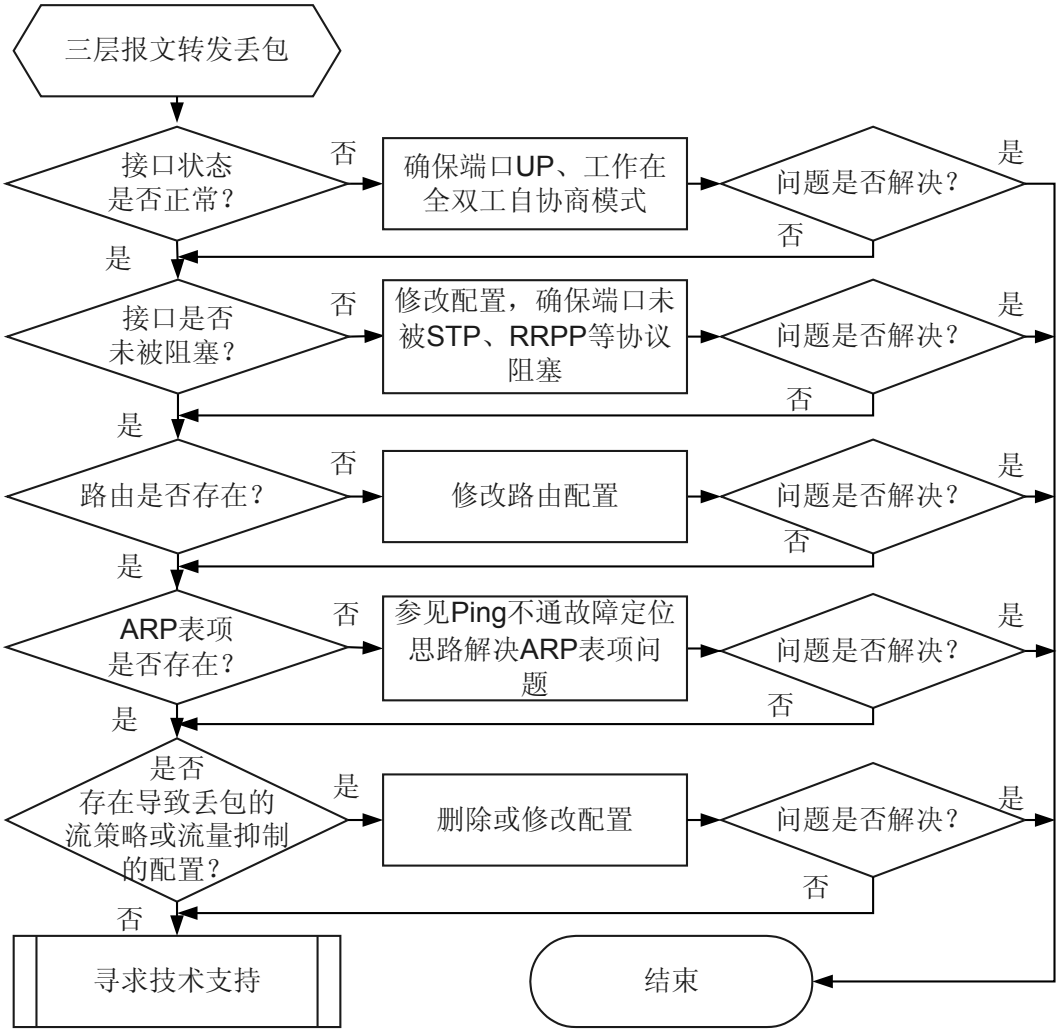
常见原因

- 接口状态异常（如物理状态 Down，工作模式为半双工、和对端自协商不一致）
- 接口被 STP、RRPP、LDT 等协议阻塞
- 路由不通
- 本端没有学习到对端 ARP 表项
- 接口、VLAN、VLANIF 或全局下应用的流策略中包含 deny 动作
- 接口或 VLAN 下配置了流量抑制功能

故障诊断流程

详细处理流程如图 7-2 所示。

图 7-2 三层报文转发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。

操作步骤

步骤 1 检查接口的运行状态。

在本端和对端设备上执行 **display interface** *interface-type interface-number* 命令查看接口运行状态。

```
<Quidway> display interface GigabitEthernet 0/0/1
GigabitEthernet0/0/1 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, GigabitEthernet0/0/1 Interface
Switch Port,PVID :   10,The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-2000-0140
Last physical up time   : 2010-02-02 13:00:36 UTC+08:00
Last physical down time : 2010-02-02 10:48:49 UTC+08:00
```

```
Port Mode: COMMON FIBER
Speed : 1000,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
 ---- More ----
```

如果接口的物理状态 Down，请参见 **4.1.1 以太网接口物理 Down 的定位思路**解决接口 Down 的故障。

- 如果工作模式不是全双工，请在接口视图下执行 **duplex full** 命令将接口设置为全双工模式。
- 如果自协商模式不一致，请在接口视图下执行 **negotiation auto** 命令调整接口的自协商模式。
- 对于电口，当出现协商成 10M/100M 工作正常，而协商成 1000M 工作异常时，请检测网线是否正常，如果有问题请更换网线。

如果接口物理状态为 UP、工作在全双工模式，并且自协商状态和对端一致，表明接口状态正常。请执行步骤 2。

步骤 2 查看接口是否被 STP、RRPP、LDT、SmartLink 等协议阻塞。

以 STP、RRPP 为例说明。

- 若交换机上配置了 STP 协议，需检查接口是否被 STP 阻塞。执行命令 **display stp brief** 查看接口状态，例如：

```
[Quidway] display stp brief
 MSTID      Port                  Role  STP State     Protection
   0        GigabitEthernet0/0/1  ROOT  FORWARDING     NONE
   0        GigabitEthernet0/0/2  DESI  FORWARDING     NONE
   0        GigabitEthernet0/0/3  DESI  FORWARDING     NONE
```

  转发正常情况下，接口的 STP state 字段为 **FORWARDING**。若该字段为 **DISCARDING**，则说明该接口上报文被 STP 阻塞。此时需要修改 STP 配置使该接口不处在 **DISCARDING** 状态，可修改 STP 的优先级使本交换机选举为根桥，使接口不被阻塞。方法如下：

  在系统视图下执行 **stp priority** *priority-level* 命令修改 STP 的优先级。其中，*priority-level* 的取值是 0 ～ 61440，取值越小则优先级越高，设置较低的优先级可使本交换机成为环路的根桥。

  若接口显示的状态都为 **FORWARDING** 状态，说明接口的 STP 状态正常。

- 若交换机上配置了 RRPP 协议，需检查接口是否被 RRPP 阻塞。执行命令 **display rrpp verbose domain** *domain-index* 查看接口状态，例如：

```
[Quidway] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 1000    sub 1001
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring      : 1
Ring Level     : 0
Node Mode      : Master
Ring State     : Failed
Is Enabled     : Enable         Is Actived : Yes
Primary port   : GigabitEthernet0/0/3        Port status: UP
Secondary port : GigabitEthernet0/0/4        Port status: DOWN
```

  若接口的 Port status 字段为 **BLOCK**，则说明该接口上报文被 RRPP 阻塞。此时需要修改 RRPP 配置使该接口不处在 BLOCK 状态。RRPP 协议阻塞的是副接口（Secondary port），所以需要重新规划修改配置，不要将该接口配置成 RRPP 协议的副接口。

  若接口的 Port status 字段都为 **Up**，则说明接口的 RRPP 状态正常。

说明

一般在同一接口上不会配置多种环路协议，所以先看接口目前配置了哪种协议类型，再查看对应的接口状态。

- 如果接口被阻塞，请修改相关配置。具体配置请参见《AC6605 无线接入控制器 配置指南》相关章节。
- 如果接口未被阻塞，请执行步骤 3。

步骤 3 检查路由

请沿转发路径逐跳查看路由，检查本端是否有可达对端的路由，对端是否有回程路由。

- 在本端执行命令 **display ip routing-table** *ip-address* 检查有无到对端的路由。 如有路由则显示如下信息：

```
<Quidway> display ip routing-table 10.1.1.2
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface
       10.1.1.0/24  Direct 0    0           D  10.1.1.2        Vlanif10
```

  如果没有路由，则输入上述命令后无任何信息显示。

- 执行命令 **display fib** *ip-address* 查看 FIB 表。

```
<Quidway> display fib 10.10.1.0
Destination/Mask   Nexthop         Flag TimeStamp     Interface       TunnelID
 10.1.1.0/24       10.1.1.2         U     t[198452]     Vlanif10        0x0
```

- 如果执行上述命令无法查找到路由表项信息，请参见《AC6605 无线接入控制器配置指南-IP 路由配置》检查路由协议配置是否正确。
- 如果执行上述命令可以查找到路由表项信息，请执行步骤 4。

步骤 4 检查是否学习到 ARP 表项。

执行命令 **display arp all** 检查本端是否学习到对端 IP 地址的 ARP 表项。

```
<Quidway> display arp all
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN
------------------------------------------------------------------------------
112.112.112.3       00d0-d0c7-ec21            S--         GE0/0/1
                                                12/-
8.1.1.1             00d0-d0c7-ec21            I -         Vlanif8         vpna
112.112.112.1       00e0-fc17-004a    14      D-0         GE0/0/1
                                                12/-
7.8.60.10           00d0-d0c7-ec21            I -         Vlanif60
4.1.1.1             00d0-d0c7-ec21            I -         Vlanif4
------------------------------------------------------------------------------
Total:5         Dynamic:1       Static:1     Interface:3
```

说明

示例中，EXPIRE 列有数值 TYPE 列记号为 D 的 ARP 表项为动态 ARP，如 112.112.112.1。TYPE 列记号为 S 的为静态 ARP，如 112.112.112.3。TYPE 列记号为 I 的为本设备接口地址的 ARP。

- 如果本端学习不到对端的 ARP 表项，请参见 **7.2.1 PING 不通故障处理思路**解决此故障，使本端能够正确学习到对端的 ARP 表项。
- 如果本端学习到了对端的 ARP 表项，请执行步骤 5。

步骤 5 查看接口、VLAN、VLANIF 以及全局的配置，是否有对某类报文采取丢弃的流策略配置。

主要检查是否正确应用了流策略，流策略中定义的流行为动作和流分类中匹配的规则是否有导致报文被丢弃的配置。

- 执行 **display traffic-policy applied-record** *policy-name* 命令查看指定流策略的应用记录。

```
<Quidway>  display traffic-policy applied-record p1
-----------------------------------------------
  Policy Name:   p1
  Policy Index:  3
     Classifier:c1     Behavior:b1
-----------------------------------------------
 *interface GigabitEthernet0/0/3
    traffic-policy p1 inbound
      slot 3    :  success
 *interface GigabitEthernet0/0/1
    traffic-policy p1 inbound
      slot 1    :  success
 *vlan 100
    traffic-policy p1 inbound
      slot 1    :  fail
      slot 3    :  fail
 *system
    traffic-policy p1 global inbound
      slot 1    :  success
      slot 3    :  success
-----------------------------------------------
  Policy total applied times: 4.
```

- 执行 **display traffic policy user-defined** 命令查看配置的流策略信息。

```
<Quidway> display traffic policy user-defined
User Defined Traffic Policy Information:
  Policy: p1
   Classifier: default-class
     Behavior: be
      -none-
   Classifier: c1
     Behavior: b1
      Committed Access Rate:
        CIR 1000 (Kbps), PIR 2000 (Kbps), CBS 125000 (byte), PBS 250000 (byte)
        Color Mode: color Blind
        Conform Action: pass
        Yellow  Action: pass
        Exceed  Action: discard
```

- 执行命令 **display traffic behavior user-defined** *behavior-name* 命令查看配置的流行为信息，是否有导致报文被丢弃的配置。比如：

```
<Quidway> display traffic behavior user-defined b1
  User Defined Behavior Information:
    Behavior: b1
      Deny
```

- 执行命令 **display traffic classifier user-defined** [*classifier-name*] 查看配置的流分类信息。

```
<Quidway> display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c1
    Precedence: 5
    Operator: OR
    Rule(s) : if-match acl 3000
```

- 执行命令 **display acl** { *acl-number* | **all** } 查看流分类中匹配的 ACL 是否包含 deny 内容。

```
<Quidway> display acl 3000
Advanced ACL 3000, 1 rule
Acl's step is 5
 rule 5 deny ip source 10.10.10.1 0
```

- 如果配置不正确，请修改配置，请参见《AC6605 无线接入控制器 配置指南-QoS 配置》。
- 如果配置正确，请执行步骤 6。

步骤 6 检查接口、VLAN 下是否有流量抑制功能的配置导致丢包。

- 在接口视图下执行 **display this** 查看接口的相关配置。

```
[Quidway-GigabitEthernet0/0/2] display this
#
interface GigabitEthernet0/0/2
 traffic-policy p1 inbound
 unicast-suppression cir 100 cbs 18800
 broadcast-suppression cir 100 cbs 18800
#
return
```

- 在 VLAN 视图下执行 **display this** 查看 VLAN 的相关配置。

```
[Quidway-vlan2] display this
#
vlan 2
 broadcast-suppression qoscar1
 unicast-suppression qoscar1
#
return
```

- 如果配置不正确，请修改配置。
- 如果配置正确，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

7.2 PING 故障处理

介绍 Ping 不通故障的定位思路和典型案例。

7.2.1 PING 不通故障处理思路

介绍 PING 不通的常见原因、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：

- PING 操作错误
- 链路问题

- 路由问题
- ARP 表项无法正常学习
- PING 发起或接收端的 ICMP 报文被丢弃

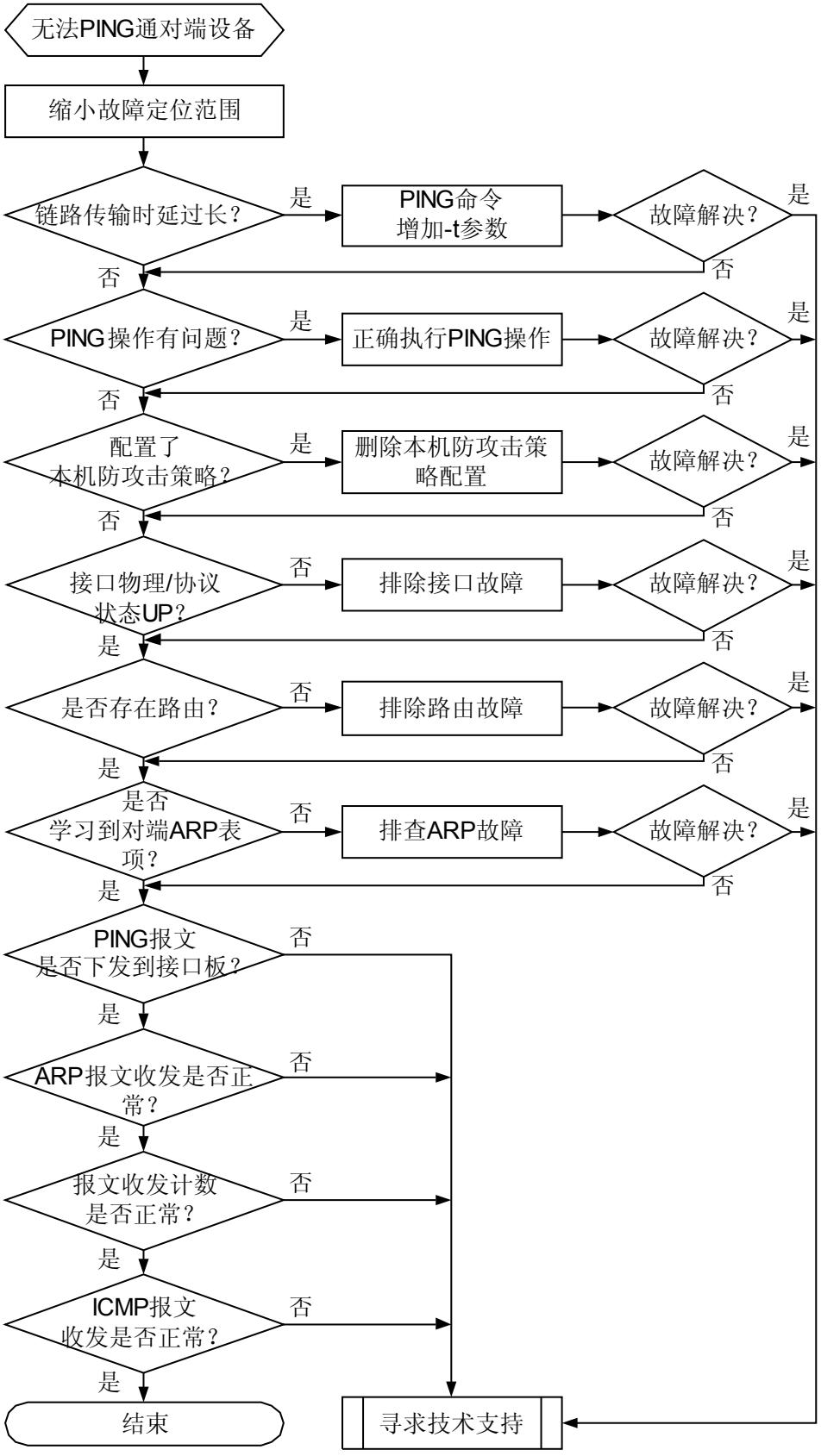
故障诊断流程

故障的定位思路如下：

- 检查路由是否存在问题
- 检查学习到对端 ARP 表项
- 检查 ICMP 报文是否被丢弃
- 检查物理链路/接口是否存在问题

详细处理流程如图 7-3 所示。

图 7-3 PING 不通 故障诊断流程图



故障处理步骤

说明

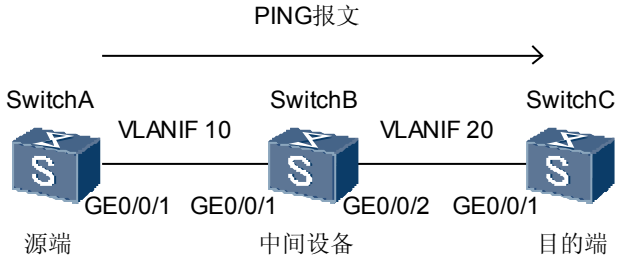
请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

操作步骤

步骤 1 缩小故障定位范围

PING 操作涉及三个角色：PING 报文发起端 SwitchA（源端）、中间设备 SwitchB 和 PING 报文接收端 SwitchC（目的端）。可采用逐段排查法缩小故障定位范围，确定故障所在设备。PING 的应用场景如图 7-4 所示。如果中间设备 SwitchB 无法登录，先在 SwitchA 上执行命令 **ping -a 10.1.1.1 10.1.1.4**，带源地址 PING 目的端 SwitchC。如果 SwitchA 无法 PING 通 SwitchC，则再执行命令 **ping -a 10.1.1.1 10.1.1.2** 从 SwitchA 带源地址 PING 中间设备 SwitchB。由此判断出故障发生在哪 2 台直连设备之间，请执行步骤 2（假设故障发生在 SwitchA 和 SwitchB 之间）。

图 7-4 Network diagram



设备	物理接口	VLANIF 接口	IP 地址
SwitchA	GE0/0/1	VLANIF 10	10.1.1.1
SwitchB	GE0/0/1	VLANIF 10	10.1.1.2
SwitchB	GE0/0/2	VLANIF 20	10.1.2.3
SwitchC	GE0/0/1	VLANIF 20	10.1.1.4

步骤 2 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 流程的原理是在特定时间内收到回应报文就显示能 PING 通，否则就显示 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。如果是传输时延时延较长导致的丢包会打印如下信息：

```
<SwitchA> ping -v -t 1 10.1.1.2
  PING 10.1.1.2: 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，通过设置**-t** 参数的值来增加时延消除故障。如果增加时延故障仍存在请执行步骤 3。

说明

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 3 检查是否 PING 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 报文大小为小于 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：

   ```
   <SwitchA> display interface gigabitethernet 0/0/1
   gigabitethernet 0/0/1 current state : UP
   Line protocol current state : UP
   Last line protocol up time: 2008-08-30 10:56:22
   Description:HUAWEI, Quidway Series, gigabitethernet 0/0/1 Interface
   Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
   ```

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 4。

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 地址作为下一跳地址进行处理。

步骤 4 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* 和 **display cpu-defend car** 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 5。
- 如果没有配置 CPU 防攻击策略，请执行步骤 5。

步骤 5 检查接口的物理状态是否为 UP

在接口视图下执行 **display this interface** 命令，查看接口的物理状态。

```
[SwitchA-gigabitethernet 0/0/1] display this interface
gigabitethernet 0/0/1 current state : UP
```

- 如果物理状态为 UP，请执行步骤 6。

- 如果物理状态为 DOWN，请进行以下检查：
  - 接口是否被 shutdown
  - 接口是否正确连接

  如果接口被 shutdown，请在接口视图下执行 **undo shutdown** 命令；

  如果接口没有正确连接，请参考 **4 物理对接及接口类**排除物理连接问题。

  执行以上操作后，如果故障没有解决，请执行步骤 6。

步骤 6 检查接口的协议状态是否为 UP

在接口视图下执行 **display this interface** 命令，查看接口的协议状态。

```
[SwitchA-gigabitethernet 0/0/1] display this interface
gigabitethernet 0/0/1 current state : UP
Line protocol current state : UP
```

- 如果接口的协议状态为 DOWN，则进行以下处理：

  检查接口是否是以太类型接口、对应 VLANIF 接口是否配置 IP 地址以及两端直连接口的 IP 地址是否处于同一网段。

  说明

  直连接口必须经过网络掩码运算后处于同一网段。

- 当接口的协议状态为 UP 时，再次检查直连接口之间是否能 PING 通，如果不能，请执行步骤 7。

步骤 7 检查路由

查看 SwitchA 是否有可达 SwitchB 的路由，SwitchB 是否有回程路由。

- 在源端执行命令 **display ip routing-table** *ip-address* 检查有无到对端的路由。 如有路由则显示如下信息：

```
<SwitchA>display ip routing-table 10.1.1.2
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

        10.1.1.0/24  Direct 0    0           D  10.1.1.1        Vlanif10
```

  如果没有路由，则输入上述命令后无任何信息显示。

- 执行命令 **display fib** *ip-address* 查看 FIB 表。
- 如果执行上述命令无法查找到路由表项信息，请检查路由协议配置是否正确。
- 如果执行上述命令可以查找到路由表项信息，请执行步骤 8。

步骤 8 检查是否学习到 ARP 表项。

执行命令 **display arp all** 检查是否学习到对端 IP 地址的 ARP 表项。

```
<SwitchA> display arp all
IP ADDRESS      MAC ADDRESS    EXPIRE(M) TYPE   INTERFACE               VPN-INSTANCE
                                         VLAN/CEVLAN
------------------------------------------------------------------------------
--------------------------------
192.168.100.114 00aa-004d-b045  20        D-1   gigabitethernet 0/0/1
10.1.1.1        0000-0000-1122            I -   Vlanif10
```

说明

示例中，EXPIRE 列有数值 TYPE 列记号为 D 的 arp 表项为动态 arp，如 112.112.112.1 和 10.164.44.1。TYPE 列记号为 S 的为静态 arp，如 112.112.112.3。TYPE 列记号为 I 的为本设备接口地址的 arp。

- 如果 SwitchA 学习到了对端的 ARP 表项，则故障消除。

- 如果 SwitchA 学习不到对端的 ARP 表项，请检查 PING 报文是否下发到接口板。请执行步骤 9。

步骤 9 检查 PING 报文是否下发到接口板。

如果接口发送的报文过多，可先配置 ACL。配置的高级 ACL 指定显示报文的目的地址为对端 IP 地址。

```
[SwitchA] acl 3000
[SwitchA-acl-adv-3000] rule permit ip destination 100.1.1.2 0
```

在设备上执行 PING 命令。

```
<SwitchA> ping -c 1000 10.1.1.2
  PING 10.1.1.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
```

打开调试开关，查看发送的 IP 报文。

```
<SwitchA> debugging ip packet acl 3000
<SwitchA> terminal monitor
Info:Current terminal monitor is on
<SwitchA> terminal debugging
Info:Current terminal debugging is on
```

如果设备上显示如下信息：

```
*0.3438047 Quidway IP/8/debug_case:
Sending, interface = OURSENDPKT, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 0, offset = 0, ttl = 255, protocol = 1,
checksum = 0, s = 0.0.0.0, d = 10.1.1.2
prompt: Transfering the packet from slot 0
```

表明 PING 报文从主控板下发，请进一步检查 ARP 报文收发是否正常，执行步骤 10。

步骤 10 检查 ARP 报文收发是否正常。

执行 **debugging arp packet interface** gigabitethernet 0/0/1 命令检查链路层报文是否收发正常。命令。

```
<SwitchA> debugging arp packet
<SwitchA> terminal monitor
Info:Current terminal monitor is on
<SwitchA> teminal debugging
Info:Current terminal debugging is on
```

如果正确收发了 ARP 报文，将输出如下信息。

```
*0.781949290 SwitchA ARP/8/arp_send:Slot=1;Send an ARP Packet, operation : 1, sender_eth_addr :
0000-5ec4-1602,sender_ip_addr : 10.1.1.1, target_eth_addr : 0000-0000-0000, target_ip_addr :
100.1.1.2
*0.781949540 SwitchA ARP/8/arp_rcv:Slot=5;Receive an ARP Packet, operation : 2,sender_eth_addr :
0000-5ec4-1603, sender_ip_addr : 10.1.1.2, target_eth_addr : 00e0-fc70-824f, target_ip_addr :
100.1.1.1
```

正常能够 ping 通的环境，请求和应答报文都应该显示。如果配置环境有问题，可能会只有请求而没有应答，或者请求报文和应答报文都没有。

如果上层收发正常，执行 **debugging ethernet packet arp interface gigabitethernet 0/0/1** 命令检查链路层报文是否收发正常。

```
<SwitchA> debugging ethernet packet arp interface gigabitethernet 0/0/1
<SwitchA> terminal monitor
Info:Current terminal monitor is on
<SwitchA> teminal debugging
```

```
Info:Current terminal debugging is on
Info:Current terminal debugging is on
*0.11763937 SwitchA ETH/8/eth_send:Slot=1;Send an Eth Packet, interface : gigabitethernet 0/0/1,
ethformat: 0, length: 42, prototype: 0806 arp, src_eth_addr : 0000-5ec4-1602, dst_eth_addr : ffff-
ffffffff
*0.11763937 SwitchA ETH/8/eth_rcv:Slot=1;Receive an Eth Packet, interface : gigabitethernet
0/0/1,eth format: 0, length: 42, prototype: 0806 arp, src_eth_addr: 0000-5ec4-1603, dst_eth_addr:
0000-5ec4-1602
```

以上信息表明链路层收发 ARP 请求报文正常，可用检查报文收发计数是否正确，执行步骤 11。

步骤 11 检查报文收发计数是否正确。

在接口视图下执行 **display this interface** 命令，或执行 **display interface** *interface-type interface-number* 命令查看报文计数。

对于 ARP 请求报文，请查看广播报文发计数是否有变化；对于 ARP 应答报文，请查看单播报文收计数情况。

```
[SwitchA-gigabitethernet 0/0/1] display this interface
gigabitethernet 0/0/1 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, gigabitethernet 0/0/1 Interface
Switch Port, PVID :  412, TPID : 8100(Hex), The Maximum Frame Length is 1600
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0025-9e80-2494
Port Mode: COMMON COPPER
Speed :  100,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
Mdi   : AUTO
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 1584 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec,Record time: -
Output peak rate 7072 bits/sec,Record time: 2011-03-28 05:41:20
Input:  89 packets, 19315 bytes
Unicast        :                  0,Multicast          :                  0
Broadcast      :                  0,Jumbo              :                  0
CRC            :                 35,Giants             :                  0
Jabbers        :                  0,Fragments          :                 13
Runts          :                  0,DropEvents         :                  0
Alignments     :                 54,Symbols            :                 89
Ignoreds       :                  0,Frames             :                  0
Discard        :                  0,Total Error        :                191
Output:  182544 packets, 43262236 bytes
Unicast        :                  0,Multicast          :             182544
Broadcast      :                  0,Jumbo              :                  0
Collisions     :                  0,Deferreds          :                  0
Late Collisions:                  0,ExcessiveCollisions:                  0
Buffers Purged :                  0
Discard        :                  0,Total Error        :                  0
    Input bandwidth utilization threshold : 100.00%
    Output bandwidth utilization threshold: 100.00%
    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.01%
```

如果出现以下情况，请记录定位过程和显示的调试信息以及接口计数，并联系华为技术支持工程师。

- 没有显示发送 ARP 报文的 debug 信息，即上层没有发送、或没有正确发送 ARP 请求或者应答报文；
- 显示发送 ARP 报文的 debug 信息，但广播报文发送计数没有增加，即上层正确发送了 ARP 请求或者应答报文，但是链路层没有发送或者发送错误；
- 显示发送 ARP 报文的 debug 信息，广播报文发送计数有增加，但单播报文接收计数没有增加，即上层正确发送了 ARP 请求或者应答报文。链路层也收发正常，但是对应接口没有收发计数。

步骤 12 检查 ICMP 报文收发是否正常。

如果 ARP 表项都正常，并且 VLANIF 逻辑口也正确更新了路由表，仍出现其他异常，可进行下述操作。

- 在用户视图下执行 **debugging ip packet acl acl-number** 命令，检查 IP 报文收发情况
- 使用命令 **debugging ip icmp [verbose]**，收集更多的故障信息以定位问题。如果问题仍然无法定位或无法解决，请联系华为技术工程师。

步骤 13 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

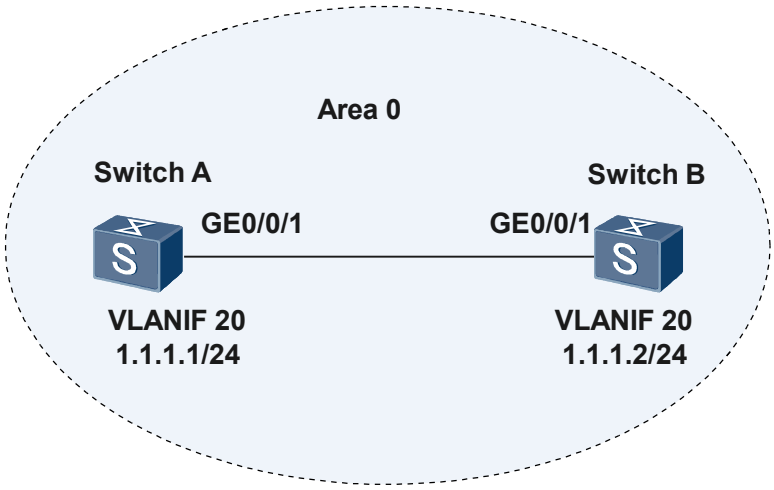
7.2.2 故障案例

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 SwitchA 替换现网中设备,替换完成后组网图如图 7-5，替换完成后发现 SwitchA 和 SwitchB 无法正常 Ping 通。同时在 SwitchA 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 7-5 错误的静态 ARP 表项导致直连设备两端不能 ping 通的组网图



故障分析

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

```
<SwitchA> display arp all
IP ADDRESS      MAC ADDRESS  EXPIRE(M) TYPE INTERFACE      VPN-INSTANCE
                                       VLAN
------------------------------------------------------------------------------
1.1.1.1         0025-9e80-2494         I -  Vlanif20
1.1.1.2         0025-9e80-248e  18     D-0  GE0/0/1
                                       33
------------------------------------------------------------------------------
Total:2        Dynamic:1       Static:0     Interface:1
```

发现 ARP 表项已经正常建立。

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

```
<SwitchA> display arp all
IP ADDRESS      MAC ADDRESS  EXPIRE(M) TYPE INTERFACE      VPN-INSTANCE
                                       VLAN
------------------------------------------------------------------------------
1.1.1.2         0025-9e80-248e         I -  Vlanif20
1.1.1.1         0016-ecb9-0eb2         S--  GE0/0/1
                                       33
------------------------------------------------------------------------------
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 SwitchA 上的 ARP 表项发现，在 SwitchB 上 **1.1.1.1** 对应的 MAC 地址的 MAC 地址并非 SwitchA 上 **1.1.1.1** 地址对应的 MAC 地址。

因此，问题可能是 SwitchB 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 SwitchB 上并未同步刷新 IP+MAC+端口号的静态 ARP，从而导致 SwitchA 和 SwitchB 无法正常 Ping 通。

操作步骤

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

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

说明

此时删除前错误的静态 ARP 表项后 SwitchA 和 SwitchB 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的发生。

步骤 3 执行命令 **arp static** *ip-address mac-address* **vid** *vlan-id* **interface** *interface-type interface-number*，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 SwitchA 和 SwitchB 可以正常 ping 通。同时使用 **display ospf peer** 查看 OSPF 的邻居状态为“FULL”。

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

 Area 0.0.0.0 interface 1.1.1.1(Vlanif33)'s neighbors
```

```
Router ID: 2.1.1.1.168.10.2      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 34  sec
  Retrans timer interval: 8
  Neighbor is up for 00:28:17
  Authentication Sequence: [ 0 ]
```

----结束

案例总结

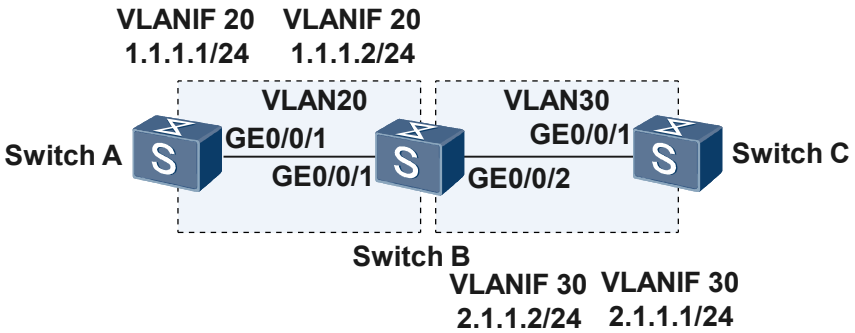
如果某设备上配置了 IP 和 MAC 地址的静态绑定，一旦该 MAC 地址对应设备被替换，则需要同步刷新静态绑定表项。此案例中如果 SwitchB 的对端设备为其他厂商设备，在出现故障时无法正常登录设备查看对端设备配置，此时可以在 SwitchA 上 PingSwitchB，同时通过镜像抓包获取 SwitchA 和 SwitchB 之间的报文，然后对报文进行分析，从而判断报文中的目的 MAC 是否正确。

能 Ping 通但是不能远程登录 Switch

网络环境

在图 7-6 的网络中，在 SwitchC 上可以 Ping 通 SwitchA 的 VLANIF 20 的地址，但是在 SwitchC 上不能 telnet 登录到 SwitchA。

图 7-6 能 Ping 通但是不能远程登录 Switch 的组网图



故障分析

1. 因为 Switch 支持 Ping 快回功能，它可以对收到的目的地址是自己的 ICMP Echo 报文做快速应答。在 SwitchC 上可以 Ping 通 SwitchA 但不能远程登录，有可能是 SwitchA 上开启 Ping 快回功能导致（缺省情况下 Switch 的 Ping 快回功能是使能的），如果 SwitchA 上开启 Ping 快回功能即使 SwitchA 上未配置到目的地址是 **2.1.1.1** 的路由，SwitchA 也能快速应答 ICMP Echo 报文，此时 SwitchC 能 Ping 通 SwitchA 证明 SwitchC 和 SwitchA 之间的链路没有问题，但不能排除路由没有问题，因此要先判断 SwitchC 到 SwitchA 之间网络是否可达。
2. 在 SwitchC 上执行 **tracert 1.1.1.1** 检查 SwitchC 到 SwitchA 之间网络是否可达。

```
traceroute to  1.1.1.1(1.1.1.1), max hops: 30 ,packet length: 40
 1 2.1.1.2 10 ms  1 ms  1 ms
 2  *  *  *
```

```
 3  *  *  *
 4  *  *  *
 5  *  *  *
 6  *  *  *
 7  *  *  *
 8  *  *  *
 9  *  *  *
10  *  *  *
11  *  *  *
12  *  *  *
13  *  *  *
14  *  *  *
15  *  *  *
16  *  *  *
17  *  *  *
18  *  *  *
19  *  *  *
20  *  *  *
21  *  *  *
22  *  *  *
23  *  *  *
24  *  *  *
25  *  *  *
26  *  *  *
27  *  *  *
28  *  *  *
29  *  *  *
30  *  *  *
```

输出信息显示 SwitchC 到 SwitchB 之间网络层是可达的，SwitchC 到 SwitchA 之间网络不可达。怀疑是 SwitchA 上未配置或配置错误的到目地址是 **2.1.1.1** 的路由。

3. 在 SwitchC 上执行 **telnet 2.1.1.2** 命令先登录到 SwitchB，然后再在 SwitchB 上执行 **telnet 1.1.1.1** 命令登录到 SwitchA，此时证明 SwitchA 的 Telnet 相关配置没有问题。
4. 在 SwitchA 上执行 **display ip routing-table 2.1.1.1** 命令，显示到目的地址为 **2.1.1.1** 最长匹配的路由表项发现为空。此时在 SwitchA 上执行 **undo icmp-reply fast** 命令关闭 Ping 快回功能。然后在 SwitchC 上 PingSwitchA 发现不能 Ping 通。

   以上分析可以得出在 SwitchC 上能 Ping 通 SwitchA 是因为 SwitchA 上开启了 Ping 快回功能。从 SwitchC 上不能远程登录到 SwitchA 是因为 SwitchA 上没有配置到目的地址是 **2.1.1.1** 的路由。

操作步骤

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

步骤 2 执行命令 **ip route-static 2.1.1.0 255.255.255.0 1.1.1.2**，配置到目的网段为 **1.1.1.2** 的静态路由。

完成上述步骤后从 SwitchC 上可以远程登录到 SwitchA。

----结束

案例总结

在实际处理故障时，如果是因为路由问题不能直接登录到故障设备，在设备之间链路正常的情况下可以一跳一跳逐跳登录到故障设备，然后进行故障排除。

由于 Switch 支持 Ping 快回功能，为不影响故障判断请先关闭 Switch 的 Ping 快回功能。

能 Ping 通不能远程登录可能还有如下原因：

- SwitchA 上未配置或配置了错误的 Telnet 登录相关配置，例如：

- 配置了错误的用户认证方式、VTY 下只绑定了 SSH 登录。
- 配置了 RADIUS/HWTACAS 认证，但认证服务器上未正确配置用户信息。

- SwitchA 或中间设备上配置了过滤 Telnet 协议 ACL 策略。

  说明

  Telnet 缺省的端口号为 23。

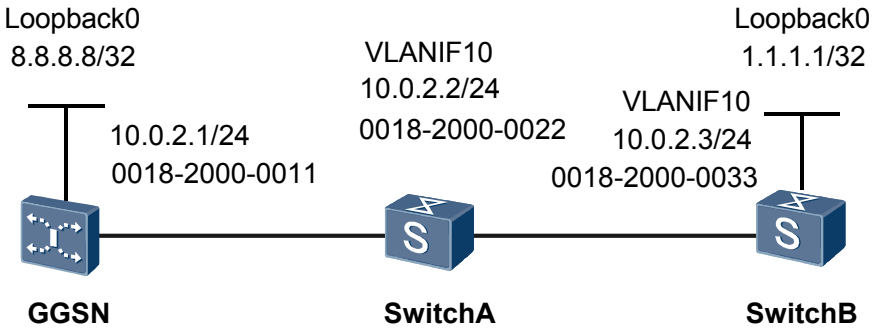
- 实际登录的用户数已经达到允许登录的最大用户数。可以通过串口登录设备，使用 **display current-configuration** 命令查看 Switch 配置的允许登录的最大用户数。使用 **display users** 查看登录类型是 Telnet 的实际登录用户数量，并和实际配置的最大登录信息比较看是否超过了用户配置的最大登录用户数。

Ping 快回功能导致单向 Ping 通

网络环境

在图 7-7 的网络中，SwitchA 连接 GGSN（Gateway GPRS Support Node）和 SwitchB。GGSN 带 Loopback 源地址 Ping 不通 SwitchB 的 Loopback 地址，但是 SwitchB 带 Loopback 源地址可以 Ping 通 GGSN 的 Loopback 地址。

图 7-7 Ping 快回功能导致单向 Ping 通组网图



网络中的路由配置如下：

- GGSN 配置静态路由，目的地址是 1.1.1.1，下一跳是 10.0.2.2。
- SwitchA 配置静态路由，目的地址是 1.1.1.1，下一跳是 10.0.2.3。
- SwitchB 配置静态路由，目的地址是 8.8.8.8，下一跳是 10.0.2.1（GGSN 的接口）。

故障分析

1. 单向可以 Ping 通，可以排除链路的问题。使用测试仪抓包发现，SwitchB 在 Ping 不通的时候收到了 SwitchA 的 10.0.2.2 发过来的目的不可达的消息。初步判断是相关转发表项有错误。
2. 在 SwitchB 上抓包，发现其回应的 Reply 报文目的 IP 地址是 8.8.8.8，目的 MAC 地址是 0018-2000-0022，这样报文到了 SwitchA 上，但是由于 SwitchA 没有到 8.8.8.8 的路由，所以出现了端口不可达，而 Ping 不通。

   原因分析如下：从 GGSN 到 SwitchB 的报文经过 SwitchA 时，由于配置了静态路由（目的地址是 1.1.1.1，下一跳是 10.0.2.3），报文会选择静态路由进行转发，而转发

时根据 ARP 表替换报文 Ethernet 头的源 MAC 和目的 MAC，因此报文从 SwitchA 出来时源 MAC 就是 SwitchA 的设备 MAC，目的 MAC 就是 SwitchB 的设备 MAC。

```
<SwitchA> display arp
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE    VPN-INSTANCE
                                          VLAN/CEVLAN
--------------------------------------------------------------------------------
10.0.2.3        0018-2000-0033  20        D-0         Eth-Trunk3
                                          10/-
```

在 SwitchB 上执行命令 **display current-configuration**，发现有 **icmp-reply fast**。使能了 Ping 快回功能。

Ping 快回是为了提高响应 Ping 的速度，AC6605 的 Ping 快回实现方式是接口板通过交换 Request 报文的源 MAC 和目的 MAC 地址，作为 Reply 报文的目的和源 MAC。当 Request 报文到达 SwitchB 后，交换 Ethernet 报文头的 MAC 地址，源 MAC 为 SwitchB 的设备 MAC，目的 MAC 为 SwitchA 的设备 MAC，这样 Reply 报文发至 SwitchA，在 SwitchA 上面需要经过路由转发，但是此时在 SwitchA 上面并没有到 GGSN 的路由，所以会出现路由不可达的情况，而无法 Ping 通。

3. 从 SwitchB 带源 1.1.1.1 的时候可以 Ping 通 8.8.8.8。

   这是因为从 SwitchB 往 GGSN ping 时报文处理流程和 Ping 快回不一样，报文发出时在 SwitchB 上 ARP 已经学到 GGSN 的 IP 地址。

   ```
   <SwitchB> display arp
   IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE    VPN-INSTANCE
                                             VLAN/CEVLAN
   --------------------------------------------------------------------------------
   10.0.2.3        0018-2000-0033  20        I -         Vlanif10
   10.0.2.1        0018-2000-0011  12        D-0         Eth-Trunk3
                                             10/-
   ```

   报文从 SwitchB 发送出去时，源 MAC 是 SwitchA 的设备 MAC，目的 MAC 是 GGSN 的设备 MAC，ICMP 报文在经过 SwitchA 时完全是二层透传，不需要改换 Ethernet 头的 MAC 地址。

   因此出现了 GGSN 带 Loopback 原地址 Ping 不通 SwitchB 的 Loopback 地址，但是 SwitchB 带 Loopback 原地址可以 Ping 通 GGSN 的 Loopback 地址。

可以通过去使能 SwitchB 上的 Ping 快回功能或修改 GGSN 的静态路由下一跳地址来恢复故障。

操作步骤

- 去使能 SwitchB 上的 Ping 快回功能。
  - 在 SwitchB 上执行命令 **system-view**，进入系统视图。
  - 执行命令 **undo icmp-reply fast**，去使能 Ping 快回功能。
- 修改 GGSN 的静态路由下一跳地址为 SwitchB 的 VLANIF10 接口地址。

  执行以上操作后，GGSN 带 Loopback 地址可以 ping 通 SwitchB 的 Loopback 地址。

----结束

案例总结

AC6605 使能 Ping 快回功能时，为了提高响应 Ping 的速度，接口板通过交换 ICMP Request 报文的源 MAC 和目的 MAC 地址，作为 Reply 报文的目的和源 MAC。Reply 报文在转发过程中可能出现路由不可达的情况。

配置路由时，尽量使来回路径的路由对称。

7.3 Tracert 故障处理

介绍 Tracert 故障的定位思路和典型案例。

7.3.1 Tracert 不通问题的定位思路

常见原因

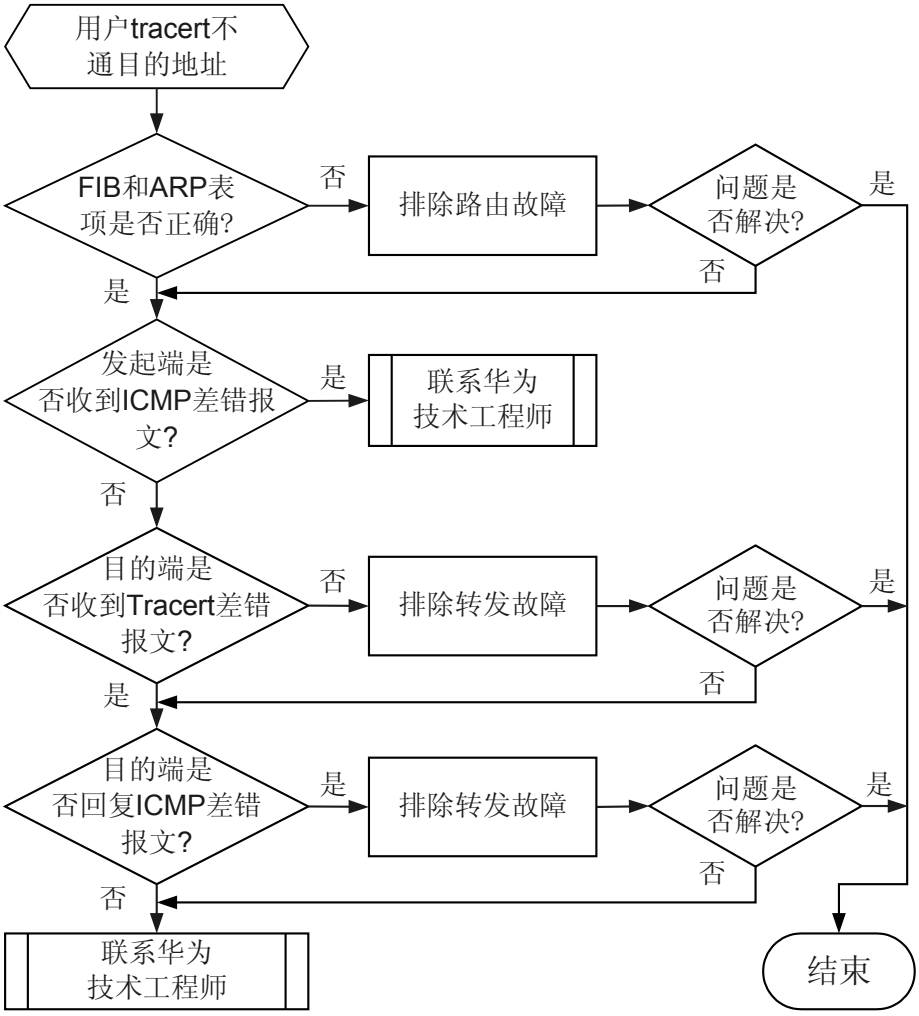
本类故障的常见原因主要包括：

- 路由或者 ARP 表项有问题。
- Tracert 报文被改写导致 IP 层面进行合法性检查失败，丢弃报文。

故障诊断流程

可按照故障诊断流程图 7-8 排除此类故障。

图 7-8 tracert 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 FIB 表项和 ARP 表项是否正确

在不能回应 ICMP 差错报文的设备上面执行 **display fib**，检查是否存在到目的地址的路由。

- 如果路由不存在请参考 **7.4 OSPF 故障处理**或者 **7.5 IS-IS 故障处理**，排除路由问题。
- 如果路由存在并且报文所经链路是以太链路，请执行 **display arp all**，查看 Tracert 的下一跳地址对应的 ARP 表项是否存在，如果不存在请执行步骤 3，否则请执行步骤 2。

步骤 2 检查 Tracert 发起端是否收到 ICMP 差错报文

在 Tracert 发起端执行 **display icmp statistics** 命令查看发起端是否收到 ICMP 差错报文，如下显示：

```
<Quidway> display icmp statistics
  Input: bad formats            0     bad checksum                  0
         echo                  13     destination unreachable      18
         source quench          0     redirects                    43
         echo reply           697      parameter problem            0
         timestamp              0     information request          0
         mask requests          0     mask replies                 0
         time exceeded         12
         Mping request          0     Mping reply                  0
  Output:echo                 704      destination unreachable   93326
         source quench          0     redirects                    0
         echo reply            13     parameter problem            0
         timestamp              0     information reply            0
         mask requests          0     mask replies                 0
         time exceeded          0
         Mping request          0     Mping reply                  0
```

在 Tracert 过程中多次执行该命令并查看结果，如果 Input 项目里面的 destination unreachable 和 time exceeded 两项的计数增加的个数和发起的 Tracert 报文的个数相等则表明 Tracert 发起端收到了 ICMP 差错报文，该回复报文在本机转发时被丢弃，请联系华为技术支持工程师排除转发故障。否则，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

7.4 OSPF 故障处理

7.4.1 OSPF 邻居 Down 的定位思路

常见原因

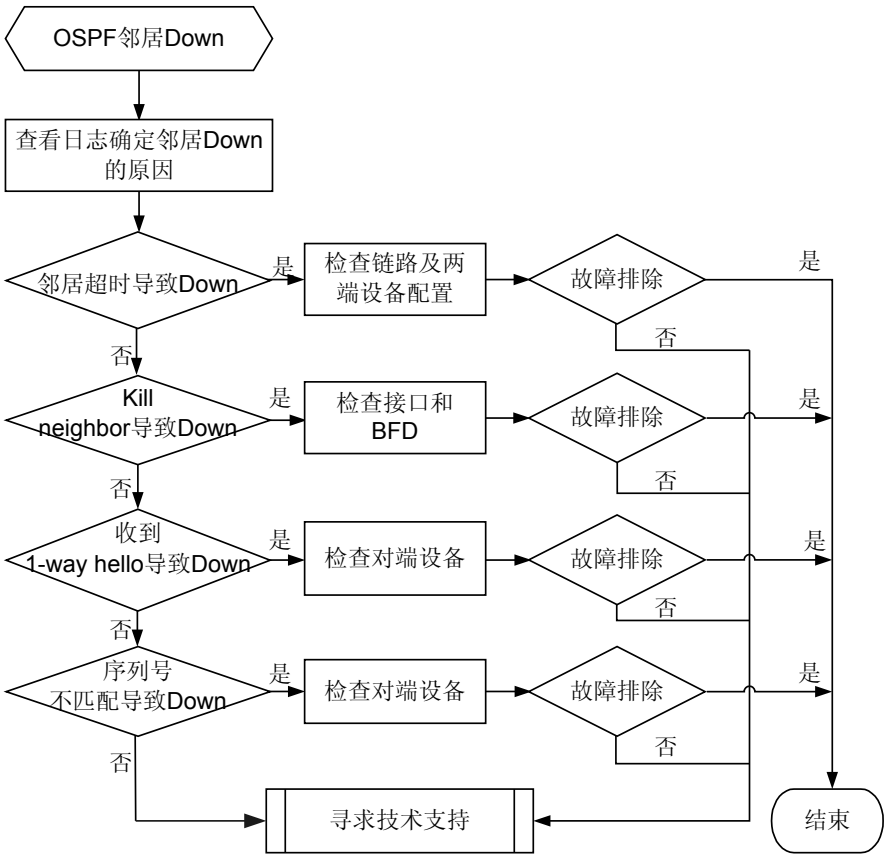
本类故障的常见原因主要包括：

- 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 7-9 排除故障。

图 7-9 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

  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。详细的故障处理方法请参见 **4.1 以太网接口故障处理**的定位。
- 如果是 BFD Session Down，则表示 BFD 会话状态变成 Down，请排查 BFD 故障，详细步骤请参见 **BFD 会话无法 Up 的定位思路**。
- 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。详细的故障处理方法请参见 **4.1 以太网接口故障处理**的定位。

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。

```
<Quidway> 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。

```
<Quidway> 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
```

- 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。

```
<Quidway> 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

   ```
   <Quidway> 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

   ```
   <Quidway> 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。

   ```
   <Quidway> 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
 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：

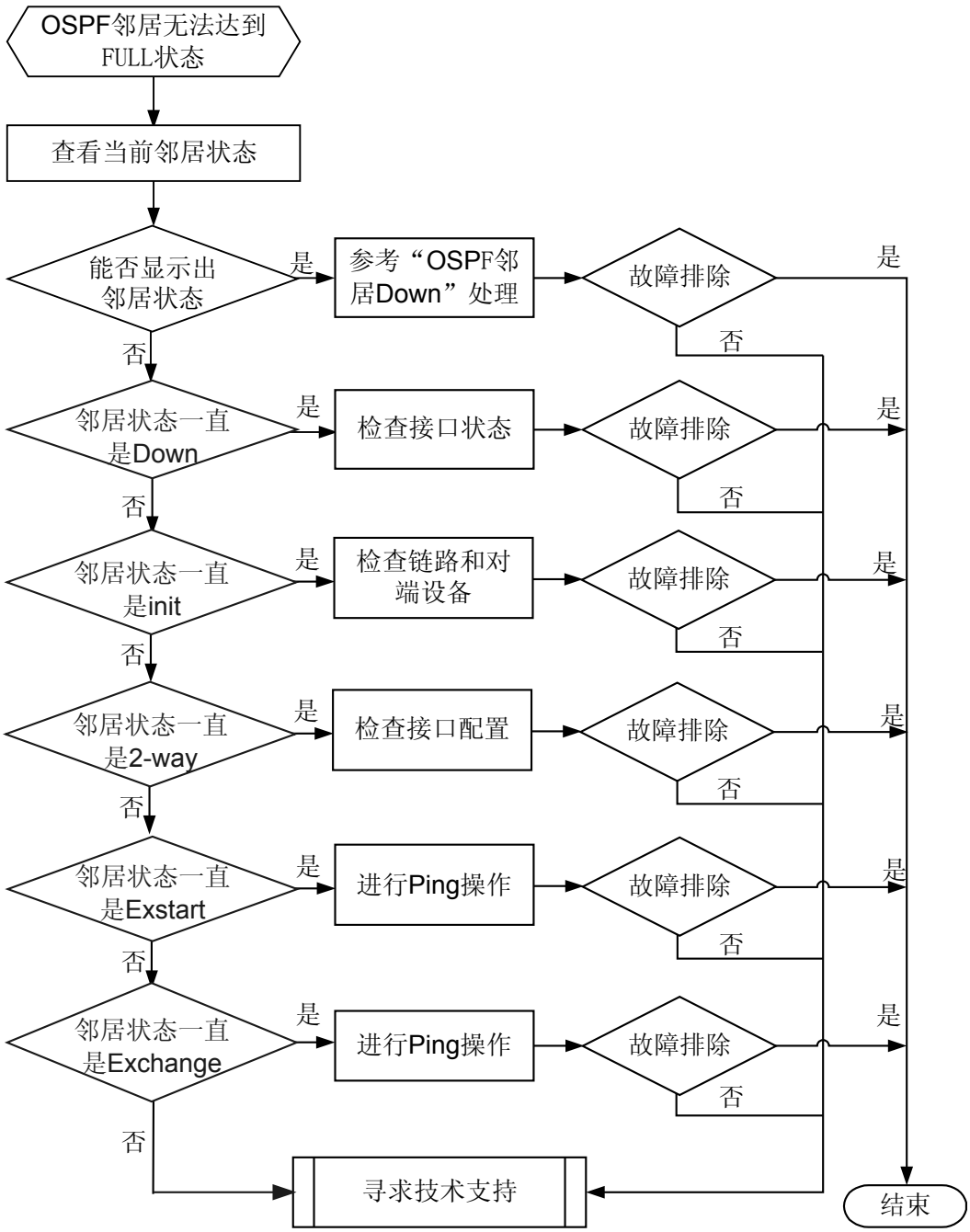
- 链路故障，OSPF 报文被丢弃。
- 接口的 dr-priority 配置不合理。

- 两端配置的 OSPF MTU 值不相等。

故障诊断流程

可按照故障诊断流程图 7-10 排除故障。

图 7-10 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。

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）。

  ```
  <Quidway> 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。

    ```
    <Quidway> 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。

```
<Quidway> 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
```

- 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

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 7-11 的网络中，SwitchC 是其他厂商设备，SwitchA 和 SwitchB 两台交换机上各有两个上行的接口，并分别配置两条静态路由，如下：

- SwitchA

```
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 192.168.0.69
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 192.168.0.65
```

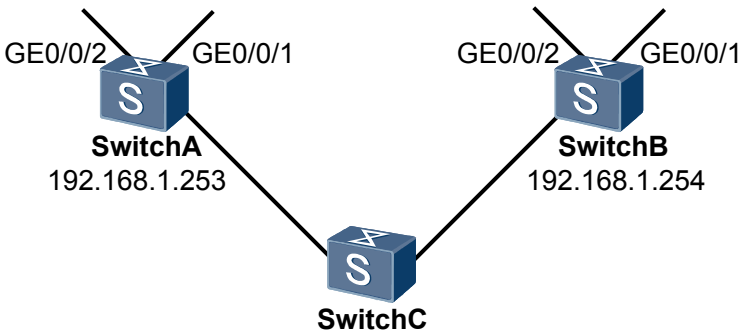
- SwitchB

```
[SwitchB] ip route-static 0.0.0.0 0.0.0.0 192.168.0.5
[SwitchB] ip route-static 0.0.0.0 0.0.0.0 192.168.0.1
```

两台交换机都在 OSPF 进程中非强制发布默认路由给 SwitchC，测试中发现 SwitchC 上故障现象如下：正常时 SwitchC 有两条 OSPF 默认外部路由指向两台交换机，但是如下两种情况时，SwitchC 上只有一条 OSPF 默认路由指向两台交换机中的一台。

- 在 SwitchA 上删除 192.168.0.65 的静态路由，其他保持不变。此时，在 SwitchC 上只有一条 OSPF 默认路由指向 SwitchB；
- 在 SwitchB 上删除 192.168.0.1 的静态路由，其他保持不变。此时，SwitchC 上只有一条 OSPF 默认路由指向 SwitchA。

图 7-11 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 SwitchA 上执行 **undo ip route-static** *0.0.0.0 0.0.0.0 192.168.0.65*，然后在 SwitchC 上查看对应 LSA 详细信息时，发现 FA 地址被 SwitchA 置错，此时 SwitchC 上只有一条 OSPF 默认路由指向 SwitchB，因为 SwitchC 上 OSPF 的 SPF 计算时发现 192.168.0.69 地址不可达。
2. 在 SwitchB 上执行 **undo ip route-static** *0.0.0.0 0.0.0.0 192.168.0.1*，然后在 SwitchC 上查看对应 LSA 详细信息时，发现 FA 地址被 SwitchB 置错，此时 SwitchC 上只有

一条 OSPF 默认路由指向 SwitchA，因为 SwitchC 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 SwitchC 上出现 OSPF 路由学习不是预期的结果，根本的原因是上面 SwitchA 和 SwitchB 将 Forwarding Address（FA）设置错误。

   交换机填写 5 类 LSA 的 FA 地址及其路由计算的规则如下：

   - 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 SwitchA 和 SwitchB 的数据配置发现：
  - SwitchA 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*；
  - SwitchB 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 SwitchA 和 SwitchB 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 SwitchA 和 SwitchB 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 SwitchA 和 SwitchB 上将对应接口设置为 slience 接口，或者让 SwitchA 和 SwitchB 的所有静态路由的下一跳 IP 地址在 SwitchC 上都是路由可达，都可以解决此问题。

----结束

案例总结

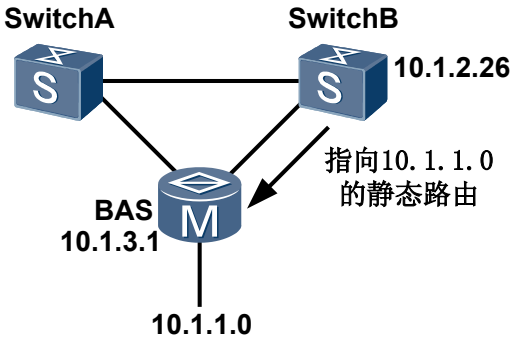
通过正确指定运行 OSPF 协议的接口的 IP 地址位于的网段和配置接口类型，使交换机必须按照规则填写 5 类 LSA 的 FA 地址及其路由计算。

交换机收到两条相同 LSID 的 LSA 但其中一条不能计算出路由

网络环境

在图 7-12 的网络中，由于到 BAS 下的流量不均匀，需要让 SwitchA 到 BAS 下目的网段的路由通过“SwitchA--BAS--目的”和“SwitchA--SwitchB--BAS--目的”来形成负载分担均衡流量。

图 7-12 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 SwitchB 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，SwitchA 上收到 SwitchB 发来的 LS ID 为 10.1.1.0 的 ASE LSA，同时 SwitchA 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，SwitchB 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. SwitchB 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：

```
<SwitchA> 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
<SwitchA> 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
                  O_ASE   150  1           D   10.1.2.49
<SwitchA> 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

    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
<SwitchA> display ip routing-table 10.1.2.26

    10.1.2.24/30  OSPF    10    101          D   10.1.2.45

                  OSPF    10    101          D   10.1.2.49
```

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 SwitchA 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

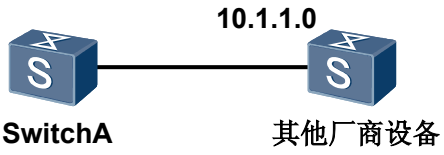
配置 OSPF 形成负载分担，需要正确配置带相同 FA 的 LSA，且配置 LSA 的相同 cost 值。

OSPF 邻居因链路问题无法建立

网络环境

在图 7-13 的组网中，SwitchA 上 OSPF 邻居无法建立，状态为 State:Exchange。

图 7-13 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：

- 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 SwitchA 的 OSPF 配置，确认 SwitchA 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 SwitchB 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 SwitchB 收到的 MTU 值为“0”，即没有收到 SwitchA 的 MTU 值。说明链路方面存在不畅通的情况。

在 SwitchA 上 PING 对端设备直连接口地址，发现有丢包：

```
<SwitchA> 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 SwitchA 上做流量统计，发现数据包是在 SwitchA 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 SwitchB 单板问题。

操作步骤

步骤 1 更换 SwitchB 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。

7.5 IS-IS 故障处理

7.5.1 IS-IS 邻居无法建立的定位思路

常见原因

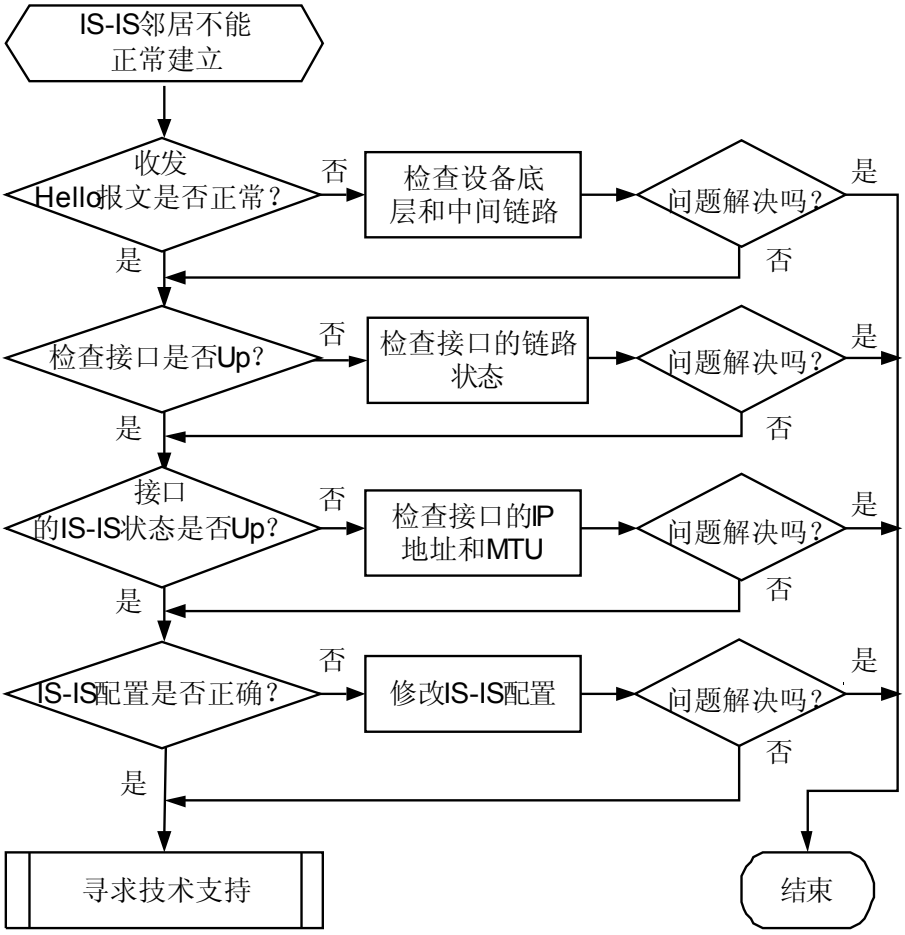
本类故障的常见原因主要包括：

- 设备底层故障或者链路故障导致 IS-IS 无法正常的收发 Hello 报文；
- 链路两端的设备配置的 System ID 相同；
- 链路两端的接口的 MTU 设置不一致或者接口的 MTU 小于发送的 Hello 报文的长度；
- 链路两端的接口的 IP 地址不在同一网段；
- 链路两端的 IS-IS 接口认证方式不匹配；
- 链路两端的 IS-IS Level 不匹配；
- 建立 IS-IS Level-1 邻居时，链路两端设备的区域地址不匹配；

故障诊断流程

可按照故障诊断流程图 7-14 排除故障。

图 7-14 IS-IS 邻居无法建立故障诊断流程图



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 IS-IS 接口的状态

执行 **display isis interface** 命令，检查使能了 IS-IS 的接口的状态（“IPv4.State”字段）。

- 如果状态为 **Mtu:Up/Lnk:Dn/IP:Dn**，请执行**步骤 2**。
- 如果状态为 **Mtu:Dn/Lnk:Up/IP:Up**，执行 **display current-configuration interface** *interface-type* [*interface-number*]，检查两端接口的 MTU 的设置。执行 **display current-configuration configuration isis** 命令，检查 IS-IS 进程的 LSP 的长度设置。

  对于 P2P 接口，需要保证 LSP 的长度不大于接口的 MTU 值；对于广播网接口，需要保证 MTU 值减 LSP 的长度大于等于 3。如果不满足该条件，请在 IS-IS 视图下执行 **lsp-length** 命令修改 LSP 的长度，或者修改 MTU 值。如果两端接口 MTU 值不同，请在对应接口视图下将其修改为相同值。

  如果故障仍未排除，请执行**步骤 4**。
- 如果状态为 **Down**，执行 **display current-configuration configuration isis** 检查是否配置了 NET，如果没有配置，请执行 **network-entity** 命令配置 NET。

  如果故障仍未排除，请执行**步骤 2**。
- 如果状态是 **Up**，请执行**步骤 4**。

步骤 2 检查接口是否 Up

执行 **display ip interface** [*interface-type* [*interface-number*]]命令，查看指定接口的状态。

- 如果接口链路层协议状态（**Line protocol current state** 字段）不是 Up，请处理接口故障，使接口链路层协议状态为 Up。

  如果故障仍未排除，请执行**步骤 3**。
- 如果接口状态是 Up，请执行**步骤 3**。

步骤 3 检查链路两端接口的 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，保证两端的 IP 地址在同一网段。如果故障仍未排除，请执行**步骤 4**。
- 如果 IP 地址在同一网段，请执行**步骤 4**。

步骤 4 检查 IS-IS 收发 Hello 报文是否正常

执行 **display isis statistics packet** [**interface** *interface-type interface-number*]命令，检查 IS-IS 收发报文是否正常。

说明

IS-IS 发送 Hello 报文的缺省间隔是 10 秒，每隔 10 秒执行一次上述命令，查看对应的报文计数是否增长。

对于广播网接口，IS-IS 的 Hello 报文区分 Level，可以根据建立邻居的 Level 查看对应的 Hello 报文计数（**L1 IIH** 或者 **L2 IIH**）；对于 P2P 类型的接口，IS-IS 的 Hello 报文不区分 Level，都记录在 **L2 IIH** 中。

- 如果接收 Hello 报文的计数一直没有增长，请检查 IS-IS 报文是否被丢弃。

- 对于广播网类型接口，执行 **debugging Ethernet packet isis** *interface-type interface-number* 命令。如果有类似如下的信息，表示接口能正常收发 IS-IS 报文。

```
*0.75124950 HUAWEI ETH/7/eth_rcv:Receive an Eth Packet, interface : Vlanif10, eth format: 3, length: 60, protoctype: 8000 isis, src_eth_addr: 00e0-fc37-08c1, dst_eth_addr: 0180-c200-0015
*0.75124950 HUAWEI ETH/7/eth_send:Send an Eth Packet, interface : Vlanif10, eth format: 3, length: 112, protoctype: 8000 isis, src_eth_addr: 00e0-fc26-f9d9, dst_eth_addr : 0180-c200-0015
```

如果接口无法正常收发 IS-IS 报文，请执行**步骤 9**。

- 如果设备能够正常接收 Hello 报文，则执行**步骤 5**。

步骤 5 检查链路两端的设备配置的 System ID 是否相同

执行 **display current-configuration configuration isis** 查看链路两端设备的 IS-IS 配置的 System ID 是否相同。

- 如果两端 System ID 相同，请修改配置，使两端的 System ID 不同。
- 如果两端 System ID 不相同，请执行**步骤 6**。

步骤 6 检查链路两端的设备的 IS-IS Level 是否匹配

执行 **display current-configuration configuration isis | include is-level** 命令查看两端 IS-IS 进程的 Level，执行 **display current-configuration interface** *interface-type interface-number* **| include isis circuit-level** 命令，查看接口的 IS-IS Level 的配置，需要保证链路两端的 Level 匹配才能建立起 IS-IS 邻居。

- 如果链路两端 Level 不匹配，请在 IS-IS 视图下使用命令 **is-level** 修改设备的 IS-IS 级别，或者在接口视图下使用命令 **isis circuit-level** 修改接口的 Level 级别。
- 如果链路两端 Level 匹配，请执行**步骤 7**。

步骤 7 检查链路两端设备的区域地址是否匹配

区域地址不匹配时，会出现 IS-IS 区域地址不匹配的告警 ISIS_1.3.6.1.3.37.2.0.12 isisAreaMismatch。

说明

如果链路两端建立 Level-1 邻居，需要保证链路两端设备在同一个区域内。

一个 IS-IS 进程最多可以配置 3 个区域地址，两端只要有一个区域地址相同，即可建立 Level-1 邻居。

建立 IS-IS Level-2 邻居时，不需要判断区域地址是否匹配。

- 如果链路两端无相同区域地址，请在 IS-IS 视图下使用命令 **network-entity** 修改设备的区域地址。
- 如果链路两端区域地址匹配，请执行**步骤 8**。

步骤 8 检查链路两端设备的认证方式是否匹配

认证方式不匹配时，会出现 ISIS 认证类型不匹配的告警 ISIS_1.3.6.1.3.37.2.0.9 isisAuthenticationTypeFailure 或者认证失败的告警 ISIS_1.3.6.1.3.37.2.0.10 isisAuthenticationFailure。

执行 **display current-configuration interface** *interface-type interface-number* **| include isis authentication-mode** 命令查看两端接口的 IS-IS 认证配置。

- 如果两端认证类型不匹配，请在链路两端的 VLANIF 接口视图下执行命令 **isis authentication-mode**，将链路两端设置为相同的认证类型。
- 如果两端认证密码不匹配，请在链路两端的 VLANIF 接口视图下执行命令 **isis authentication-mode**，将链路两端设置为相同的认证密码。

- 如果两端认证匹配，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

ISIS_1.3.6.1.3.37.2.0.12 isisAreaMismatch

ISIS_1.3.6.1.3.37.2.0.9 isisAuthenticationTypeFailure

ISIS_1.3.6.1.3.37.2.0.10 isisAuthenticationFailure

相关日志

无

7.5.2 设备学习不到 IS-IS 路由的定位思路

常见原因

本类故障的常见原因主要包括：

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

故障诊断流程

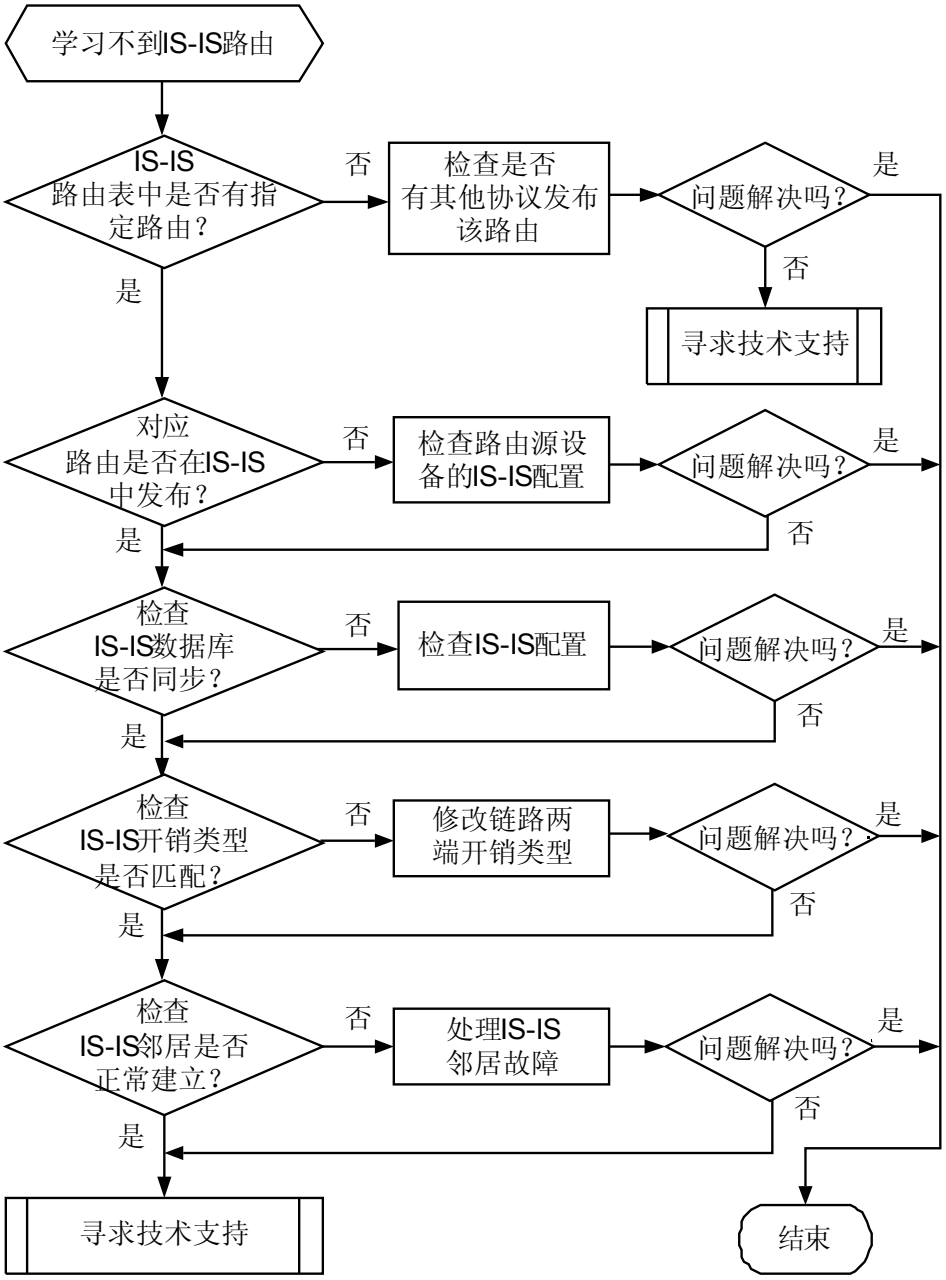
在配置 IS-IS 后发现设备学习不到 IS-IS 路由。

故障诊断思路：

- 检查是否有其它协议也学到了指定路由。
- 检查 IS-IS 是否计算出路由。
- 检查 IS-IS 的 LSDB 数据库是否同步。
- 检查 IS-IS 的配置是否正确。

可按照故障诊断流程**图 7-15** 排除故障。

图 7-15 设备学习不到 IS-IS 路由的故障诊断流程图



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 IS-IS 路由表是否正确

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

- 如果 IS-IS 路由表中存在指定的路由，执行 **display ip routing-table** *ip-address* [*mask* | *mask-length*] **verbose** 命令查看 IP 路由表中是否存在协议优先级比 IS-IS 高的路由。

  说明

  State 字段为 **Active Adv** 表示该路由为活跃的路由，如果存在相同前缀的多个协议的路由，协议优先级高的路由优选为活跃的路由。

  - 如果存在，请根据网络规划调整配置。
  - 如果不存在，请执行**步骤 6**。
- 如果 IS-IS 路由表中不存在指定的路由，请执行**步骤 2**。

步骤 2 检查指定的 IS-IS 路由是否发布

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

- 如果 LSP 报文中没有携带指定的路由，请检查配置是否正确，例如接口是否使能 IS-IS。

  说明

  如果是引入的外部路由，执行 **display ip routing-table protocol** *protocol* **verbose** 命令查看外部路由是否是活跃的。
- 如果 LSP 报文中携带了指定的路由，请执行**步骤 3**。

步骤 3 检查 IS-IS 的数据库是否同步

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

说明

其中，**LSPID** 是一条 LSP 的标识，**Seq Num** 是报文的序列号，序列号越大表示报文越新。

- 如果 LSDB 数据库中不存在指定的 LSP 报文。
  - 如果产生告警信息 ISIS_1.3.6.1.3.37.2.0.9 isisAuthenticationTypeFailure 或 ISIS_1.3.6.1.3.37.2.0.10 isisAuthenticationFailure，则表示配置的 LSP 报文认证的认证类型或认证密码不匹配，请修改配置。
  - 如果未产生以上告警信息，请排查设备底层和中间链路是否存在故障。
- 如果 LSDB 数据库中存在指定的 LSP 报文，但 **Seq Num** 与 **display isis lsdb local verbose** 命令显示的不一致，并且 **Seq Num** 不停的增长，则网络中存在其他设备与发布指定路由的设备的 System ID 配置相同，这种情况下会产生告警信息 ISIS_1.3.6.1.3.37.2.0.8 isisSequenceNumberSkip，请排查并网络中设备的 IS-IS 配置。
- 如果 LSDB 数据库中存在指定的 LSP 报文，但 **Seq Num** 不一致，并且一直保持不变，可能是 LSP 报文在传输过程中被丢弃，请排查设备底层和中间链路是否存在故障。
- 如果 LSDB 数据库中存在指定的 LSP 报文，并且 **Seq Num** 一致，请执行**步骤 4**。

步骤 4 检查 IS-IS 开销类型是否匹配

分别在发布路由的设备和学习不到路由的设备上，执行 **display current-configuration configuration isis** 命令，查看 IS-IS 的开销类型配置（**cost-style** 命令）。

说明

只有开销类型相同，才能学到路由。

IS-IS 的开销类型可以配置为以下 5 种模式:

- narrow：接收和发送开销值类型为 narrow 的报文。
- narrow-compatible：可以接收开销值类型为 narrow 和 wide 的报文，但却只发送 narrow 的报文。
- compatible：可以接收或发送开销值类型为 narrow 和 wide 的报文。
- wide-compatible：可以接收开销值类型为 narrow 和 wide 的报文，但却只发送 wide 的报文。
- wide：接收或发送开销值类型为 wide 的报文。

如果一端配置是 narrow，另一端配置为 wide 或者 wide-compatible，则两端不能互通。

如果一端配置是 narrow-compatible，另一端配置为 wide，则两端不能互通。

- 如果链路两端的设备的 IS-IS 开销类型不匹配，请执行 **cost-style** 命令修改配置。
- 如果两端的设备的 IS-IS 开销类型匹配，请执行**步骤 5**。

步骤 5 检查 IS-IS 邻居是否正常建立

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

- 如果 State 字段不是 Up，请参见 **IS-IS 邻居无法建立的定位思路**。
- 如果 State 字段是 Up，请执行**步骤 6**。

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

ISIS_1.3.6.1.3.37.2.0.8 isisSequenceNumberSkip

ISIS_1.3.6.1.3.37.2.0.9 isisAuthenticationTypeFailure

ISIS_1.3.6.1.3.37.2.0.10 isisAuthenticationFailure

相关日志

无

7.5.3 IS-IS 邻居震荡的定位思路

常见原因

本类故障的常见原因主要包括：

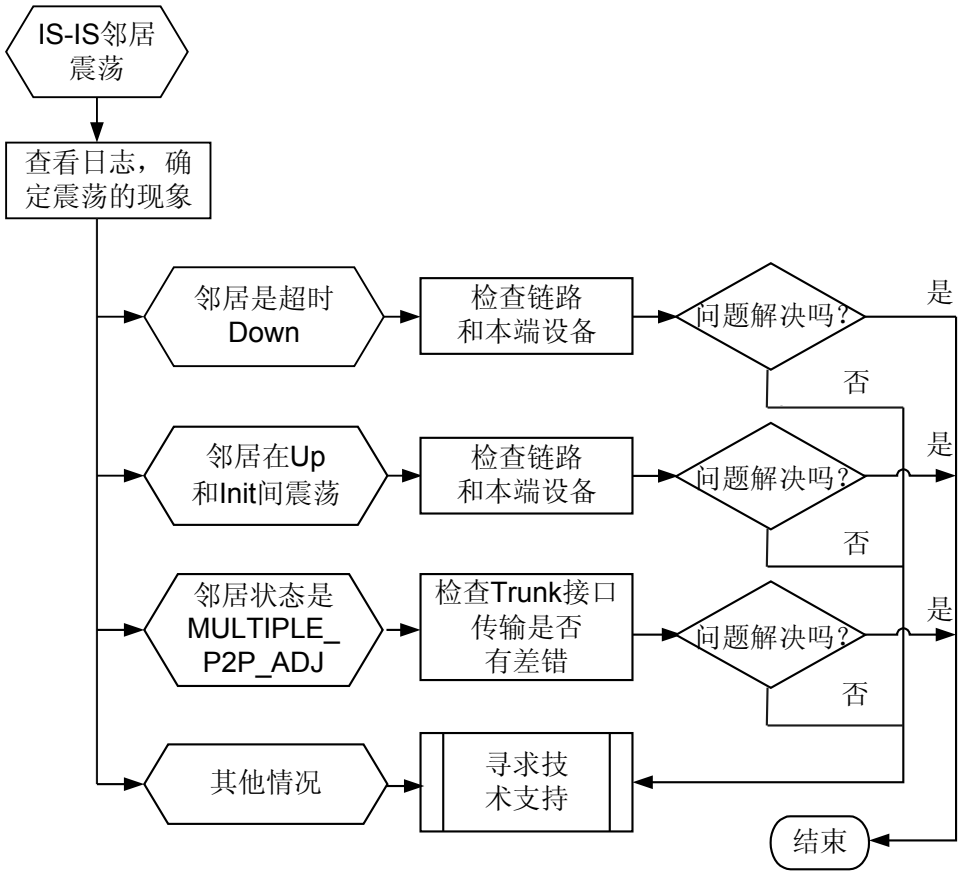
- 链路不稳定或者设备异常，造成丢失报文；
- Trunk 接口的成员口的传输线插错位置。

故障诊断流程

在配置 IS-IS 后发现 IS-IS 邻居震荡。

可按照故障诊断流程图 7-16 排除故障。

图 7-16 IS-IS 邻居震荡的故障诊断流程图



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 IS-IS 邻居变化的情况

如果 IS-IS 邻居状态发生变化，就会出现 IS-IS 邻居变化的告警 ISIS_1.3.6.1.3.37.2.0.17 isisAdjacencyChange 和日志 ISIS/4/ADJ_CHANGE。

说明

只有在 ISIS 进程下配置了 **log-peer-change** 命令后，才会记录 ISIS/4/ADJ_CHANGE 的日志信息。

- 如果在 IS-IS 进程下配置了 **log-peer-change** 命令，可以查看日志信息中 **ChangeType** 字段的值。
  - 如果 **ChangeType** 是 HOLDTIMER_EXPIRED，说明是本端设备不能稳定的收到对端设备的 Hello 报文，请排查中间链路和本端设备底层是否存在丢包问题。
  - 如果 **ChangeType** 在 3_WAY_INIT 和 3_WAY_UP 之间震荡（针对 P2P 类型接口），或者 **ChangeType** 都是 NEW_L1_ADJ 或者 NEW_L2_ADJ（针对广播网类型接口），表明邻居状态是在 Up 和 Init 之间震荡，这是对端设备不能稳定的收到本端设备的 Hello 报文导致的，请排查中间链路和对端设备底层是否存在丢包问题。
  - 如果 **ChangeType** 是 MULTIPLE_P2P_ADJ，并且接口是 IP-Trunk 接口，请检查 Trunk 接口下绑定的接口是否插错线。
  - 其他情况，请执行**步骤 2**。
- 如果没有配置 **log-peer-change**，可以连续执行 **display isis peer** 命令，观察 **State** 和 **HoldTime** 字段的值，确定 IS-IS 邻居变化的情况。
  - 如果邻居震荡时，**State** 字段值不变，**HoldTime** 字段值一直减小，直到减小到 0 后邻居关系被删除，说明是本端设备不能稳定的收到对端设备的 Hello 报文，请排查中间链路和本端设备底层是否存在丢包问题。
  - 如果邻居震荡时，**State** 在 Up 和 Init 之间变化，这是对端设备不能稳定的收到本端设备的 Hello 报文导致的，请排查中间链路和对端设备底层是否存在丢包问题。
  - 其他情况，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

ISIS_1.3.6.1.3.37.2.0.17 isisAdjacencyChange

相关日志

ISIS/4/ADJ_CHANGE

7.5.4 IS-IS 路由震荡的定位思路

常见原因

本类故障的常见原因主要包括：

- IS-IS 邻居震荡；

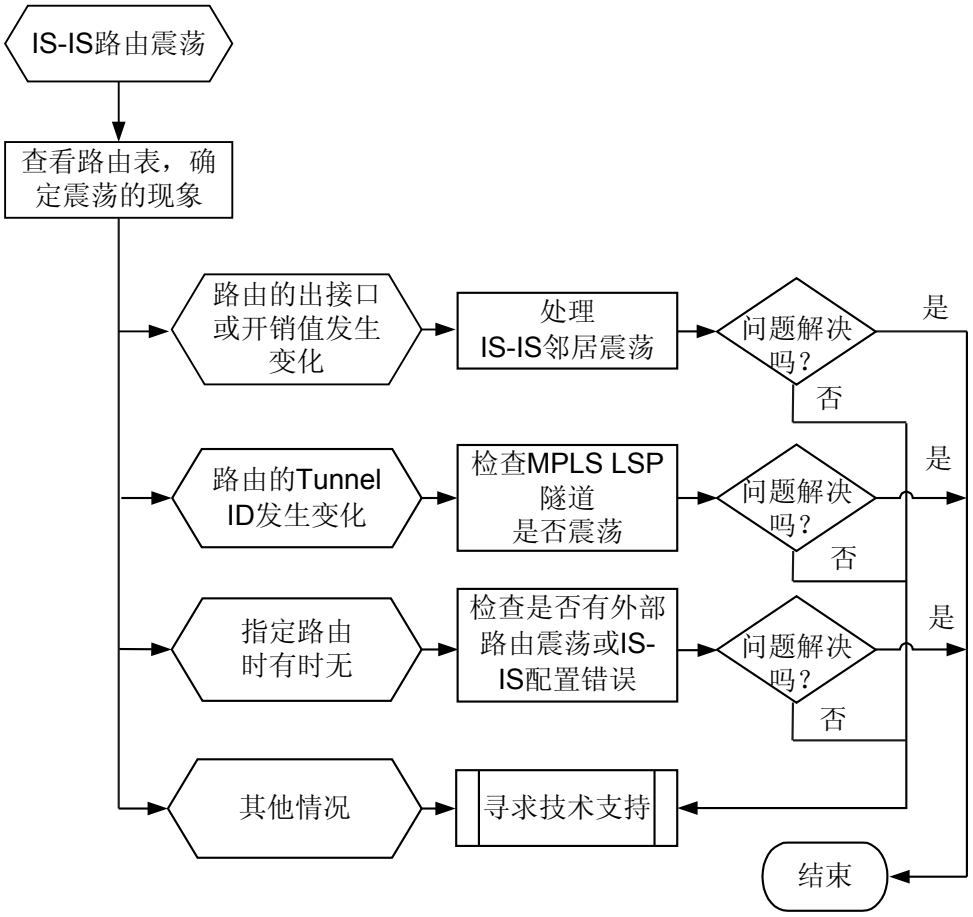
- 两台设备的 IS-IS 引入了相同的外部路由，并且外部路由的优先级比 IS-IS 协议的优先级低；
- 网络上两台设备的 System ID 配置相同。

故障诊断流程

在配置 IS-IS 后发现 IS-IS 路由震荡。

可按照故障诊断流程图 7-17 排除故障。

图 7-17 IS-IS 路由震荡的故障诊断流程图



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 检查路由震荡的情况

执行 **display ip routing-table** *ip-address* **verbose** 命令，查看路由震荡的具体情况，例如路由表中 **Active** 的路由是从哪个协议学到的，路由震荡的时候，哪些属性发生了变化。

- 如果路由震荡的前后，**TunnelID** 字段发生了变化，请检查 MPLS LSP 隧道是否存在震荡。如果 MPLS LSP 隧道振荡，请参考 LDP LSP 振荡的定位思路排查 LSP 振荡问题。
- 如果路由的 **Cost** 或者 **Interface** 字段发生变化，请检查该路由路径上的 IS-IS 邻居是否在震荡，详细的故障处理方法请参考 **IS-IS 邻居震荡故障处理**。
- 如果路由在路由表中时有时无（**Age** 字段在震荡），执行 **display isis lsdb verbose** 命令，确定路由是由哪条 LSP 报文携带的，并且根据查看到的 LSP 报文，执行 **display isis lsdb** *lsp-id* **verbose** 查看这条 LSP 的更新情况。
  - 如果 LSP 中一直携带指定的路由，请检查该路由路径上是否存在 IS-IS 邻居震荡，详细的故障处理方法请参考 **IS-IS 邻居震荡故障处理**。
  - 如果 LSP 的 **Seq Num** 字段值在不停的增加，请检查网络中是否有两台设备配置了相同的 System ID。
  - 如果 LSP 的 **Seq Num** 字段值在不停的增加，并且 LSP 更新前后，指定的路由时有时无，请在产生该 LSP 的设备上执行**步骤 2**。

    说明

    display isis lsdb*lsp-id* **verbose** 命令的显示信息中，IP-Internal 字段或+IP-Internal 字段对应的 IP 地址所在的设备就是产生该 LSP 的设备。
- 如果路由的 **Protocol** 字段发生变化，请执行**步骤 2**。

步骤 2 检查 IS-IS 引入外部路由的配置

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

- 如果路由表中 **Active** 的路由是 IS-IS 路由，而不是 IS-IS 要引入的外部路由，说明网络中还存在其它设备的 IS-IS 也发布了相同的路由，请根据网络规划修改路由协议的优先级，或者在 IS-IS 下配置路由过滤策略，控制下发到 IP 路由表的路由。
- 其它情况，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

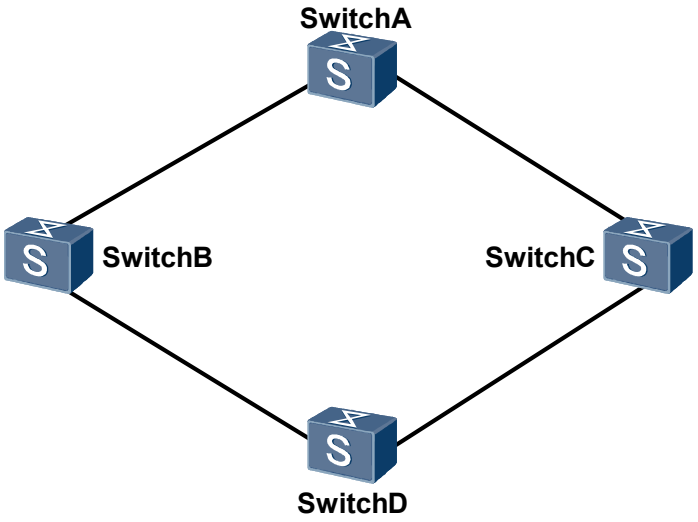
7.5.5 故障案例

由于 IS-IS 路由引入类型与其他厂商设备不一致导致上层设备无法学习 IS-IS 路由

网络环境

在图 7-18 的网络中，SwitchB 和 SwitchC 两台设备位于核心层，下挂两台 SR 设备 SwitchA 和 SwitchD，其中，SwitchD 为其他厂商设备。所有设备部署 IS-IS，都为 Level-2 设备。为实现负载分担，在 SwitchA 和 SwitchD 连接了相同的网络，并在 IS-IS 进程下引入直连路由和静态路由到 IS-IS。配置后发现核心层两台设备 SwitchB 和 SwitchC 上只能从 SwitchD 学习到路由。

图 7-18 设备无法学习 IS-IS 路由



故障分析

由于 SwitchD 引入静态路由到 IS-IS 时，缺省引入类型为 **internal**，**cost** 为路由的原有开销值，而 SwitchA 引入静态路由到 IS-IS 时缺省为 **external**，**cost** 为路由的原有开销值+64。由于开销值不一样，SwitchB 和 SwitchC 两台设备优选从 SwitchD 学到路由。

说明

此问题只有 cost-style 为 narrow 才可能出现。

操作步骤

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

步骤 2 执行命令 **isis** *process-id*，进入 IS-IS 视图。

步骤 3 执行命令 **import-route direct cost-type internal**, 引入直连路由，设定 **cost-type** 为 **internal**。

步骤 4 执行命令 **import-route static cost-type internal**，引入静态路由，设定 **cost-type** 为 **internal**。

说明

将 **cost-type** 由 **external** 改为 **internal** 后，路由的 **cost** 为原有开销值而不是原有开销值+64。

完成上述操作后，在 SwitchB 和 SwitchC 设备上使用命令 **display isis route** 查看路由信息，可以看到有两条到相同 IP 网段的 IS-IS 路由，SwitchA 和 SwitchD 进行负载分担。

----结束

案例总结

在多厂商设备的组网环境中，要注意各厂商设备之间的实现差异。

7.6 BGP 故障处理

7.6.1 BGP 邻居无法建立的定位思路

常见原因

BGP 邻居无法建立是指 BGP 邻居状态无法到达 Established 状态。

本类故障的常见原因主要包括：

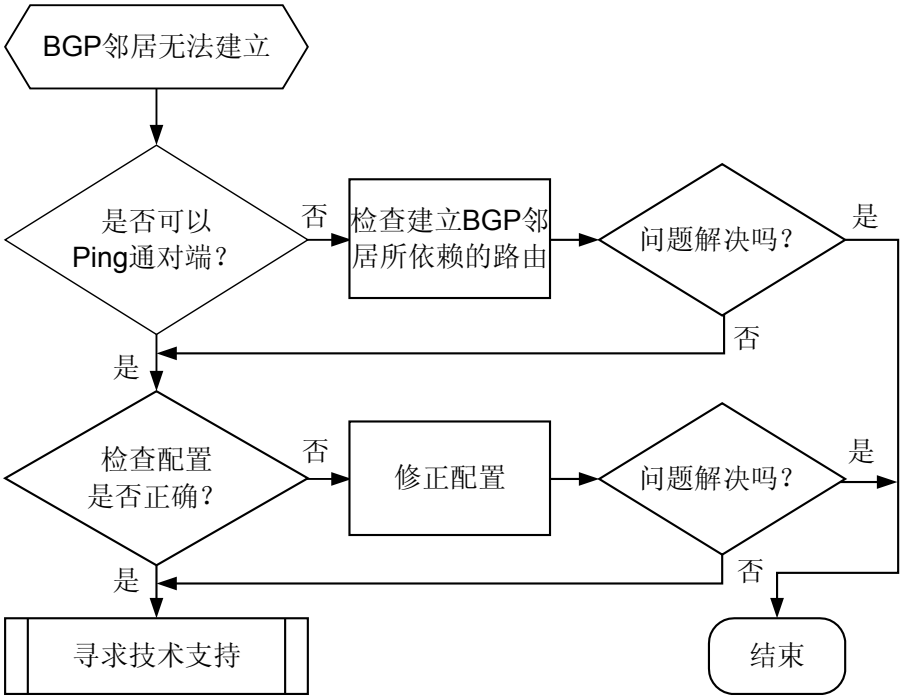
- BGP 报文转发不通
- ACL 过滤了 TCP 的 179 端口
- 邻居的 Router ID 冲突
- 配置的邻居的 AS 号错误
- 用 Loopback 口建立邻居时没有配置 **peer connect-interface**
- 用 Loopback 口建立 EBGP 邻居未配置 **peer ebgp-max-hop**
- 对端发送的路由数量是否超过 **peer route-limit** 命令设定的值。
- 对端配置了 **peer ignore**
- 两端的地址族不匹配

故障诊断流程

在配置 BGP 协议后发现 BGP 邻居无法建立。

可按照故障诊断流程图 **7-19** 排除故障。

图 7-19 BGP 邻居无法建立故障诊断流程图



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 使用 **ping** 命令检测 BGP 邻居之间是否可以 Ping 通

- 如果可以 Ping 通，则说明 BGP 邻居之间有可达的路由并且链路传输也没有问题，请执行**步骤 2**。

  说明

  请使用命令 **ping -a** *source-ip-address* **-s** *packetsize host* 来检测两端的互通性，因为带源地址可以同时检测两端路由是否正常，指定 ping 的字节可以检查大包在链路上传输是否正常。

- 如果不能 Ping 通，请参见 **PING 不通故障处理思路**检查两端的路由表中是否存在对端路由。

步骤 2 检查是否配置 ACL 禁止 TCP 的 179 端口

在两端执行 **display acl all** 命令查看是否禁止 TCP 的 179 端口。

```
<Quidway> display acl all
 Total nonempty ACL number is 1

Advanced ACL 3001, 2 rules
Acl's step is 5
```

```
rule 5 deny tcp source-port eq bgp
rule 10 deny tcp destination-port eq bgp
```

- 如果有禁止 TCP 的 179 端口的 ACL，请执行 **undo rule** *rule-id* **destination-port** 和 **undo rule** *rule-id* **source-port** 命令取消配置。
- 如果没有禁止 TCP 的 179 端口的 ACL，请执行步骤 3。

步骤 3 检查邻居的 Router ID 是否冲突

在两端分别查看无法建立的 BGP 邻居的情况，例如 ipv4 单播邻居无法建立可以执行 **display bgp peer** 命令，查看 Router ID 是否冲突。显示 Router ID 信息的命令行示例如下，该例中本端的 Router ID 是 **223.5.0.109**。

```
<Quidway> display bgp peer
 BGP local router ID : 223.5.0.109
 Local AS number : 41976
 Total number of peers : 12                 Peers in established state : 4

  Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv
  8.9.0.8         4         100     1601     1443     0 23:21:56 Established   10000
  9.10.0.10       4         200     1565     1799     0 23:15:30 Established    9999
```

- 如果 Router ID 冲突，请在 BGP 视图下运行命令 **router id** 将 Router ID 修改为不同（一般会用 Loopback 口的地址作为本端的 Router ID）。
- 如果 Router ID 没有冲突，请执行步骤 4。

步骤 4 检查邻居 AS 号配置是否正确

在两端分别执行 **display bgp peer**，检查邻居的 AS 号是否是对端的 AS 号。

```
<Quidway> display bgp peer
 BGP local router ID : 223.5.0.109
 Local AS number : 41976
 Total number of peers : 12                 Peers in established state : 4

  Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv
  8.9.0.8         4         100     1601     1443     0 23:21:56 Established   10000
  9.10.0.10       4         200     1565     1799     0 23:15:30 Established    9999
```

- 如果 AS 号配置错误，请将 AS 号配置为对端的 AS。
- 如果 AS 号配置没有错误，请执行步骤 5。

步骤 5 检查 BGP 配置是否影响邻居建立

通过 **display current-configuration configuration bgp** 查看 BGP 的配置，进行如下检查。

检查项	说明
peer connect-interface *interface-type interface-number*	如果邻居两端使用 Loopback 口建立邻居，则需要使用命令 **peer connect-interface** 指定相应的 Loopback 口为发送 BGP 报文的源接口。
peer ebgp-max-hop *hop-count*	如果直连设备用 Loopback 口建立 EBGP 邻居，或者非直连多跳设备建立 EBGP 邻居，则需要配置命令 **peer ebgp-max-hop** 指定允许的最大跳数 *hop-count*。 ● 直连设备使用 Loopback 口建立连接时，*hop-count* 只要大于 1 即可。 ● 非直连设备建立连接时需要指定 *hop-count* 为相应的跳数。

检查项	说明
peer route-limit *limit*	如果有该配置时，请确认对端发送的路由数量是否超过 **peer route-limit** *limit*，其中 *limit* 表示限制的路由数量。如果是，则需要降低对端发送过来的路由数量，并在本端使用 **reset bgp** *ip-address* 命令复位相应的 BGP 连接来触发 BGP 重新建立连接。
peer ignore	如果对端配置了 **peer ignore**，说明由于某种原因对端暂时不想和本端建立邻居。如果想建立邻居时，执行 **undo peer ignore** 命令去使能对端的配置即可。
地址族能力	请检查 BGP 会话两端的地址族能力是否匹配。例如，建立 BGP VPNv4 邻居时，需要两端都要在 BGP-VPNv4 地址族下配置命令 **peer enable**。如果一端已配置而另一端没有配置时，没有配置的一端 BGP 邻居状态为“No neg”。

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

BGP_1.3.6.1.2.1.15.7.2 bgpBackwardTransition

相关日志

BGP/3/STATE_CHG_UPDOWN

BGP/3/WRONG_ROUTERID

BGP/3/WRONG_AS

7.6.2 BGP 公网流量中断的定位思路

常见原因

BGP 公网流量中断是指在 BGP 邻居关系正常的情况下，依赖 BGP 公网路由建立起来的流量的中断。

本类故障的常见原因主要包括：

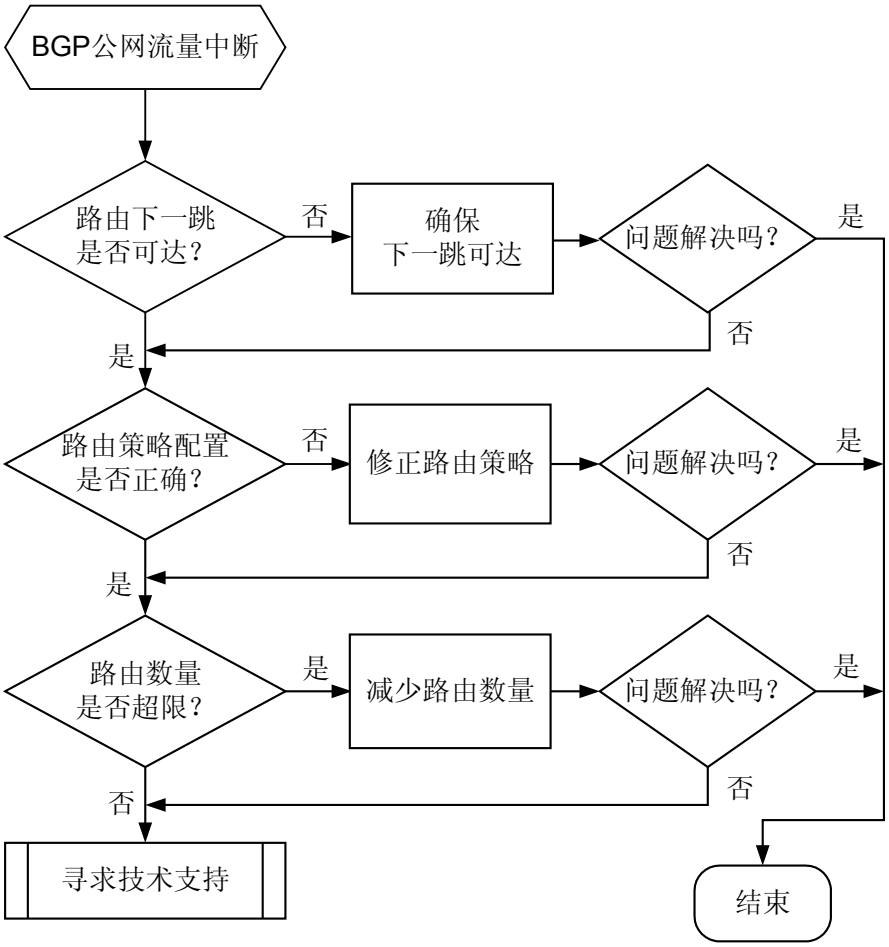
- 路由下一跳不可达导致路由不活跃。
- 路由策略配置不当导致路由无法发布/接收。
- 路由数量超限导致收到的路由被丢弃。

故障诊断流程

在配置 BGP 协议后发现 BGP 公网流量中断。

可按照故障诊断流程图 7-20 排除故障。

图 7-20 BGP 公网流量中断故障诊断流程图



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 检查路由下一跳是否可达

在路由的发送端执行 **display bgp routing-table** *network* { *mask* | *mask-length* }命令查看目标路由（*network* 表示目标路由前缀），确认路由是否活跃，并且查看此路由是否已经被发送给路由接收端。命令示例如下：

以 13.0.0.0/8 这条路由举例，显示此路由是活跃的（valid）和优选的（best），并且发送给了邻居 3.3.3.3，此路由的 BGP 下一跳为 1.1.1.1（Original nexthop），经过迭代后的下一跳为 172.1.1.1（Relay IP Nexthop）。

```
<Quidway> display bgp routing-table 13.0.0.0 8

 BGP local router ID : 23.1.1.2
 Local AS number : 100
 Paths:   1 available, 1 best, 1 select
 BGP routing table entry information of 13.0.0.0/8:
 From: 1.1.1.1 (121.1.1.1)
 Route Duration: 4d21h29m39s
 Relay IP Nexthop: 172.1.1.1
 Relay IP Out-Interface: GigabitEthernet1/0/2
 Original nexthop: 1.1.1.1
 Qos information : 0x0
 AS-path Nil, origin incomplete, localpref 100, pref-val 0, valid, internal, best, select, active,
pre 255
 Aggregator: AS 100, Aggregator ID 121.1.1.1
 Advertised to such 1 peers:
    3.3.3.3
```

- 如果目标路由不活跃，请确认 IP 路由表中是否存在到 BGP 下一跳（Original nexthop）的路由，如果不存在说明 BGP 路由不发布是由于路由下一跳不可达导致，请确认为何没有到 BGP 下一跳（Original nexthop）的路由（一般属于 IGP 或静态路由问题）。
- 如果目标路由活跃，却没有优选，请联系华为技术工程师。

  说明

  只要有 BGP 路由活跃，则必然有一条路由会被优选。
- 如果目标路由活跃且被优选，但没有显示发送给路由接收端，请执行**步骤 2**（重点检查路由发送端的出口策略）。

在路由接收端执行 **display bgp routing-table** *network* { *mask* | *mask-length* }查看是否收到目标路由。

- 如果收到目标路由，请重复执行**步骤 1** 判断路由下一跳是否可达并且是否被优选。
- 如果没有收到目标路由，请执行**步骤 2**（重点检查路由接收端的入口策略）。

步骤 2 检查路由策略是否正确

在路由的发送端/接收端执行 **display current-configuration configuration bgp** 命令查看 BGP 配置，确认是否配置邻居的出口/入口策略。

```
<Quidway> display current-configuration configuration bgp
#
bgp 100
 peer 1.1.1.1 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  filter-policy ip-prefix aaa import
  filter-policy ip-prefix aaa export
  peer 1.1.1.1 enable
  peer 1.1.1.1 filter-policy acl-name acl-name import
```

```
  peer 1.1.1.1 filter-policy acl-name acl-name export
  peer 1.1.1.1 as-path-filter 1 import
  peer 1.1.1.1 as-path-filter 1 export
  peer 1.1.1.1 ip-prefix prefix-name import
  peer 1.1.1.1 ip-prefix prefix-name export
  peer 1.1.1.1 route-policy policy-name import
  peer 1.1.1.1 route-policy policy-name export
#
return
```

- 如果两端配置了出口/入口策略，则需要确认这些策略是否会把目标路由过滤掉，导致该路由无法正常收发。路由策略的具体配置请参见《AC6605 无线接入控制器配置指南-IP 路由》。
- 如果两端没有配置相应的出口/入口策略，请直接执行**步骤 3**。

步骤 3 检查路由是否超限

在路由接收端执行 **display current-configuration configuration bgp | include peer** *destination-address* 和 **display current-configuration configuration bgp | include peer** *group-name*（如果 Peer 被加入到对等体组中）命令查看 BGP 配置，确认是否配置邻居路由限制。

例如，限制只能从邻居 1.1.1.1 收 5 条路由，超限之后将丢弃路由并记录日志。

```
<Quidway> display current-configuration configuration bgp | include peer 1.1.1.1
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 route-limit 5 alert-only
  peer 1.1.1.1 enable
```

如果 BGP 邻居被加入到组中，显示信息中有可能没有 route-limit 的配置。

```
<Quidway> display current-configuration configuration bgp | include peer 1.1.1.1
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 group IBGP
  peer 1.1.1.1 enable
  peer 1.1.1.1 group IBGP
```

这种情况下，需要使用 **display current-configuration configuration bgp | include peer** *group-name* 来查看该对等体组的配置。

```
<Quidway> display current-configuration configuration bgp | include peer IBGP
 peer IBGP route-limit 5 alert-only
  peer IBGP enable
```

如果流量中断时，产生了路由超限日志 BGP/3/ROUTPRIX_EXCEED，表示路由超限导致目标路由被丢弃，则需要扩大本端的路由限制数值。

说明

修改 BGP 邻居限制的最大路由数量时会中断邻居，建议在路由发送端通过路由聚合以减少路由数量来解决。

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

BGP_1.3.6.1.4.1.2011.5.25.177.1.3.1 hwBgpPeerRouteNumThresholdExceed

相关日志

BGP/3/ROUTPRIX_EXCEED

相关告警与日志

相关告警

BGP_1.3.6.1.4.1.2011.5.25.177.1.3.1 hwBgpPeerRouteNumThresholdExceed

相关日志

BGP/3/ROUTPRIX_EXCEED

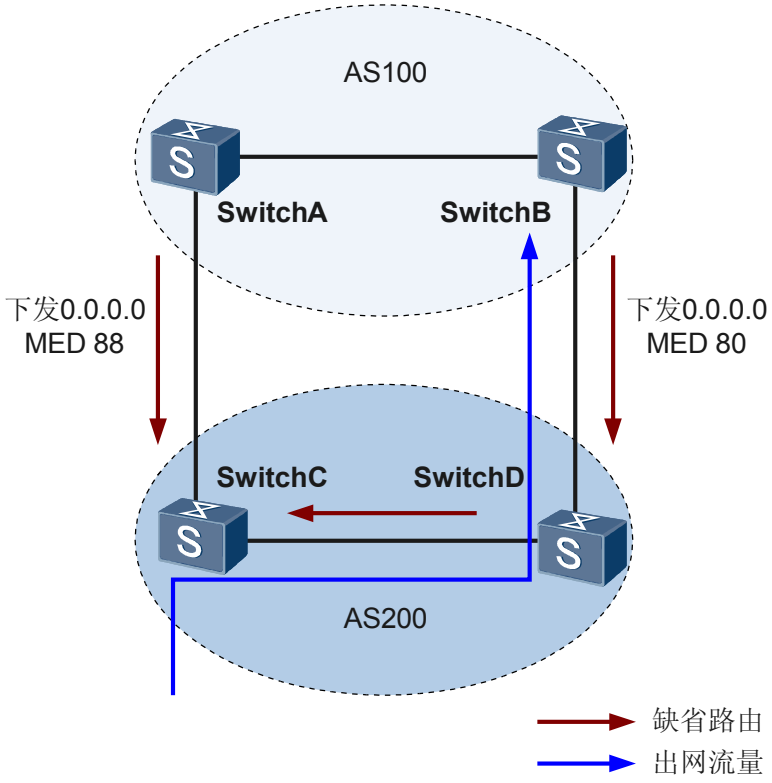
7.6.3 故障案例

BGP 下发缺省路由的 MED 值不同，导致对端 AS 出口设备间流量穿越

网络环境

在图 7-21 的网络中，AS100 和 AS200 间配置了 EBGP 对等体。AS 内的设备间配置了 IBGP 对等体。SwitchA 和 SwitchB 下发缺省路由后，在 SwitchC 上查看 BGP 缺省路由的详细信息，发现 AS200 的出网流量全部指向了 SwitchD，即 BGP 缺省路由的下一跳是 SwitchD。流量穿越了 SwitchC。

图 7-21 AS 出口设备间流量穿越组网图



故障分析

在 SwitchC 上执行 **display bgp routing-table 0.0.0.0** 命令查看 BGP 缺省路由的详细信息，发现 SwitchA 和 SwitchB 设置的 MED 值不同，导致 AS200 的出网流量穿越了 SwitchC。

操作步骤

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

步骤 2 执行命令 **bgp** *as-number*，进入 BGP 视图。

步骤 3 执行命令 **ipv4-family unicast**，进入 BGP-IPv4 单播地址族视图。

步骤 4 执行命令 **default med** *med*，修改 BGP 路由的缺省 MED 值，使 SwitchA 和 SwitchB 一致。

完成上述操作后，在 SwitchC 上执行 **display bgp routing-table 0.0.0.0** 命令查看 BGP 缺省路由的详细信息，AS200 的出网流量通过 SwitchC，故障排除。

----结束

案例总结

两个 AS 间存在多个出口设备时，需要将其下发缺省路由的 MED 值配置一致。由于 local-preference、MED 等值都一致，BGP 对等体会优选从 EBGP 学来的路由，避免流量穿越。

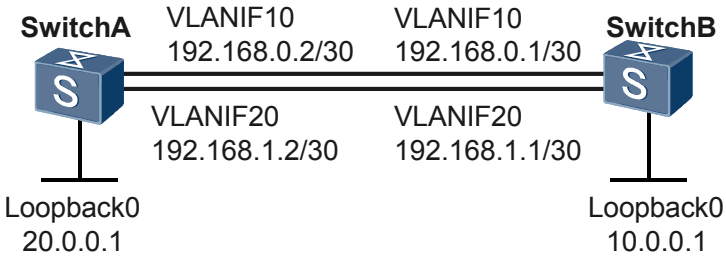
路由迭代导致 BGP 邻居 Down

缺省情况下，路由迭代是使能的，在实际网络中可能会引起不期望的结果，如 BGP 邻居 Down。

网络环境

如图 7-22 所示 SwitchA 和 SwitchB 通过 Loopback 接口建立 BGP 邻居关系。SwitchA 的 VLANIF10 接口 Down 掉后，SwitchA 和 SwitchB 的 BGP 邻居 Down，一直处于 OpenSent 状态。但是从 SwitchA 上可以 ping 通对端 SwitchB 的 Loopback 地址。

图 7-22 路由迭代导致 BGP 邻居 Down 组网图



故障分析

1. 发现 SwitchA 的 VLANIF10 接口 Down 掉后，在 SwitchA 上执行命令 **display ip routing-table** *ip-address* 查看 NextHop 为 10.0.0.1 的路由有两条，出接口分别为 Vlanif20 和 NULL0。而 SwitchA 的 VLANIF10 原来没有 Down 时，查看 NextHop 为 10.0.0.1 的路由出接口分别为 Vlanif20 和 Vlanif10。

   在 SwitchA 上执行命令 **display bgp peer**，地址为 10.0.0.1 的 BGP 邻居状态为 OpenSent。

2. 等值路由的出接口发生改变，应该是因为发生了路由迭代。如果没有发生路由迭代，SwitchA 的 VLANIF10 接口 Down 掉后，应该只有一条出接口为 Vlanif20 的路由。

3. 检查 SwitchA 的配置，分析出接口迭代到 NULL0 的原因。SwitchA 上配置了指向 SwitchB 的 Loopback 接口地址 10.0.0.1 的 32 位掩码的静态路由。

   ```
   ip route-static 10.0.0.1 255.255.255.255 192.168.1.1
   ip route-static 10.0.0.1 255.255.255.255 192.168.0.1
   ```

   SwitchA 的 VLANIF10 接口 Down 掉后，如上的静态路由配置导致 SwitchA 进行路由迭代，查找路由表中是否存在到达 192.168.0.1 的路由。通过查看配置文件，发现有如下的静态路由配置：

   ```
   ip route-static 192.168.0.0 255.255.255.0 NULL0 preference 255
   ```

   因此双上行的两条等值路由其中一条下一跳变为 NULL 口。

4. 再分析出接口为 NULL0 和 BGP 邻居 Down 的关系。VLANIF10 接口 Down 后，SwitchA 的双上行路由变为：

   ```
   Destination/Mask    Proto   Pre  Cost      NextHop         Interface
         10.0.0.1/32   BGP     100  0         10.0.0.1        Vlanif20
                       BGP     100  0         10.0.0.1        NULL0
   ```

   此时从 SwitchA 上可以 ping 通 SwitchB 的 Loopback 接口地址 10.0.0.1。一般情况下 BGP 邻居不应该 Down。但由于 SwitchA 是双路由上行，发包存在 Hash 问题。执

行不带源地址的 **ping** 命令，Hash 的结果是出接口为 Vlanif20，因此可以 ping 通。如果在 SwitchA 上执行以 Loopback 地址 20.0.0.1 作为源地址的 **ping** 命令，Hash 结果就是出接口为 Vlanif10，导致 ping 不通。而 Loopback 地址正是 SwitchA 和 SwitchB建立 BGP 邻居的源地址和目的地址，Vlanif10 现在迭代到的路由下一跳是 NULL0，因此 SwitchA 上的 BGP 邻居 Down。

故障排除思路：中止 SwitchA 上的路由迭代。

操作步骤

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

在 SwitchA 的 VLANIF10 接口 Down 掉后，迭代到如上静态路由就迭代中止了，宣布出接口为 Vlanif10 的静态路由不可达，从路由表中删除该路由，到达 SwitchB 的所有报文只能有唯一的出口 VLANIF20。

步骤 2 执行命令 **undo ip route-static 10.0.0.1 255.255.255.255 192.168.1.1** 和 **undo ip route-static 10.0.0.1 255.255.255.255 192.168.0.1**，删除原有的静态路由配置。

步骤 3 执行命令 **ip route-static 10.0.0.1 255.255.255.255 VLANIF20 192.168.1.1** 和 **ip route-static 10.0.0.1 255.255.255.255 VLANIF10 192.168.0.1**，配置静态路由并指定下一跳和对应的出接口。

步骤 4 执行命令 **display bgp peer**，查看到地址为 10.0.0.1 的 BGP 邻居状态为 Established。BGP 邻居正常，故障排除。

----结束

案例总结

缺省情况下，路由迭代是使能的。在实际网络中，需要分析路由迭代是否会引起不期望的结果。

由于迭代深度问题导致静态路由不生效

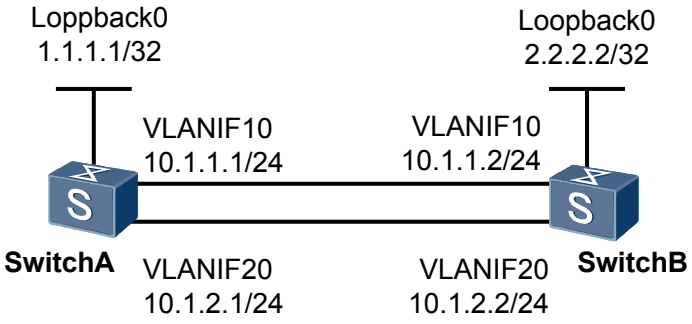
网络环境

在图 7-23 所示的网络中，SwitchA 与 SwitchB 采用两条链路相连，并且建立 EBGP 邻居。SwitchA 上配置两条静态路由：

```
ip route-static 2.2.2.2 255.255.255.255 Vlanif10 10.1.1.2
ip route-static 2.2.2.2 255.255.255.255 10.1.2.2
```

查看路由表，去往 SwitchB 的路由只有一个下一跳出接口 Vlanif10。

图 7-23 由于迭代深度问题导致静态路由不生效组网图



故障分析

由于 SwitchA 上配置的路由 **ip route-static** “2.2.2.2 255.255.255.255” **vlanif10 10.1.1.2** 指定了出接口，不需要迭代，迭代深度为 0；而另一条路由 **ip route-static 2.2.2.2 255.255.255.255 10.1.2.2** 没有指定出接口，需要进行 1 次迭代，迭代深度为 1。

BGP 选择迭代深度最小的静态路由，因此，选中上述第一条迭代深度为 0 的，所以 BGP 路由出接口都为 Vlanif10。

操作步骤

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

步骤 2 执行命令 **undo ip route-static 2.2.2.2 255.255.255.255 10.1.2.2**，删除静态路由。

步骤 3 执行命令 **ip route-static 2.2.2.2 255.255.255.255 vlanif20 10.1.2.2**，配置静态路由，并指定出接口。

完成上述操作后，BGP 选择迭代深度最小的静态路由，两条静态路由同时命中，所以在 SwitchA 上查看路由表，可以看到两个出接口 Vlanif10 和 Vlanif20。

----结束

案例总结

配置静态路由时指定出接口，可以避免由于迭代深度不同造成某些静态路由不生效。

7.7 RIP 故障处理

7.7.1 RIP 没有学到部分或全部路由的定位思路

常见原因

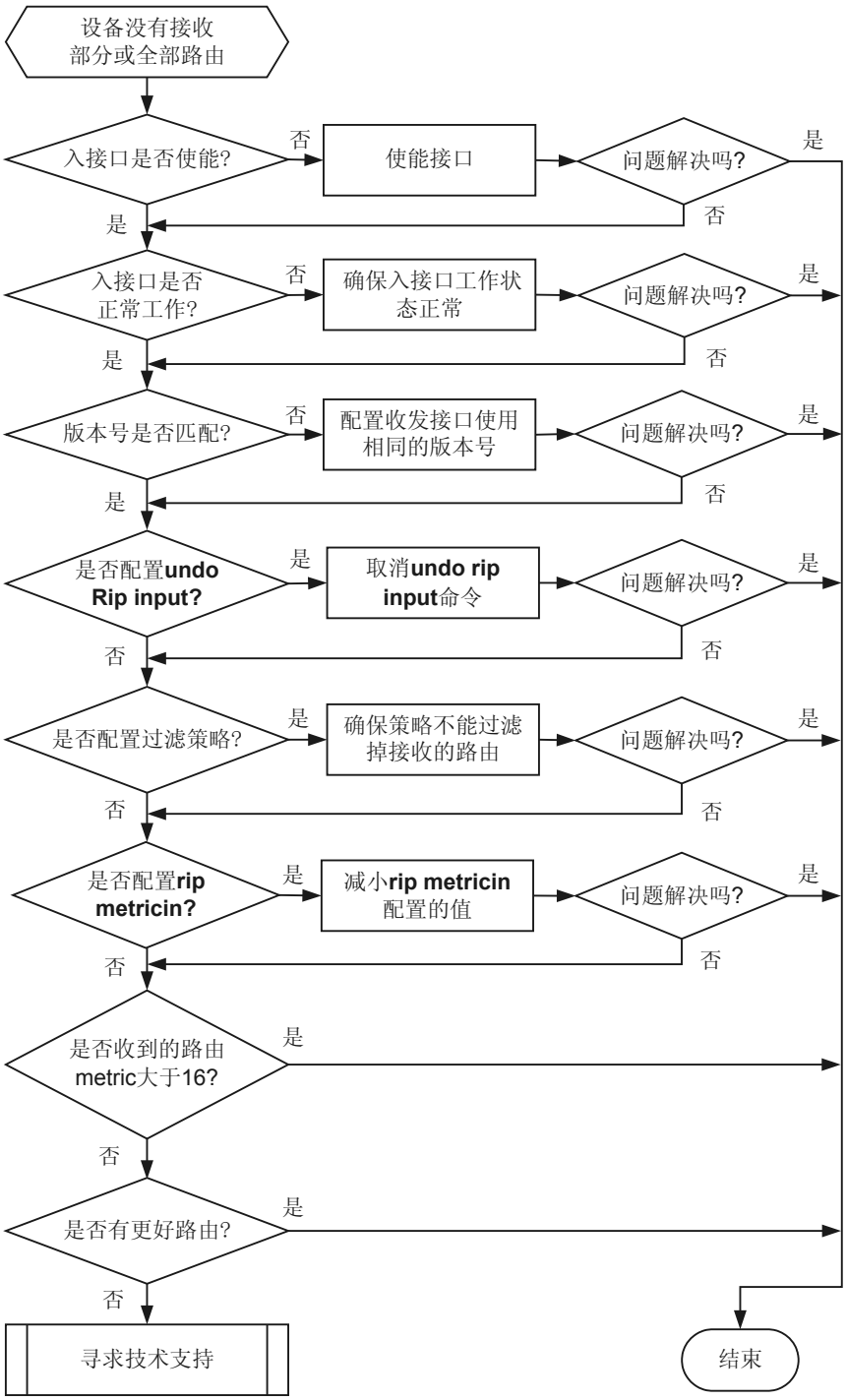
本类故障的常见原因主要包括：

- 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

在配置各交换机后，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 7-24 所示。

图 7-24 RIP 路由接收故障诊断流程图



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。

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

7.7.2 设备没有发送部分或全部 RIP 路由的定位思路

常见原因

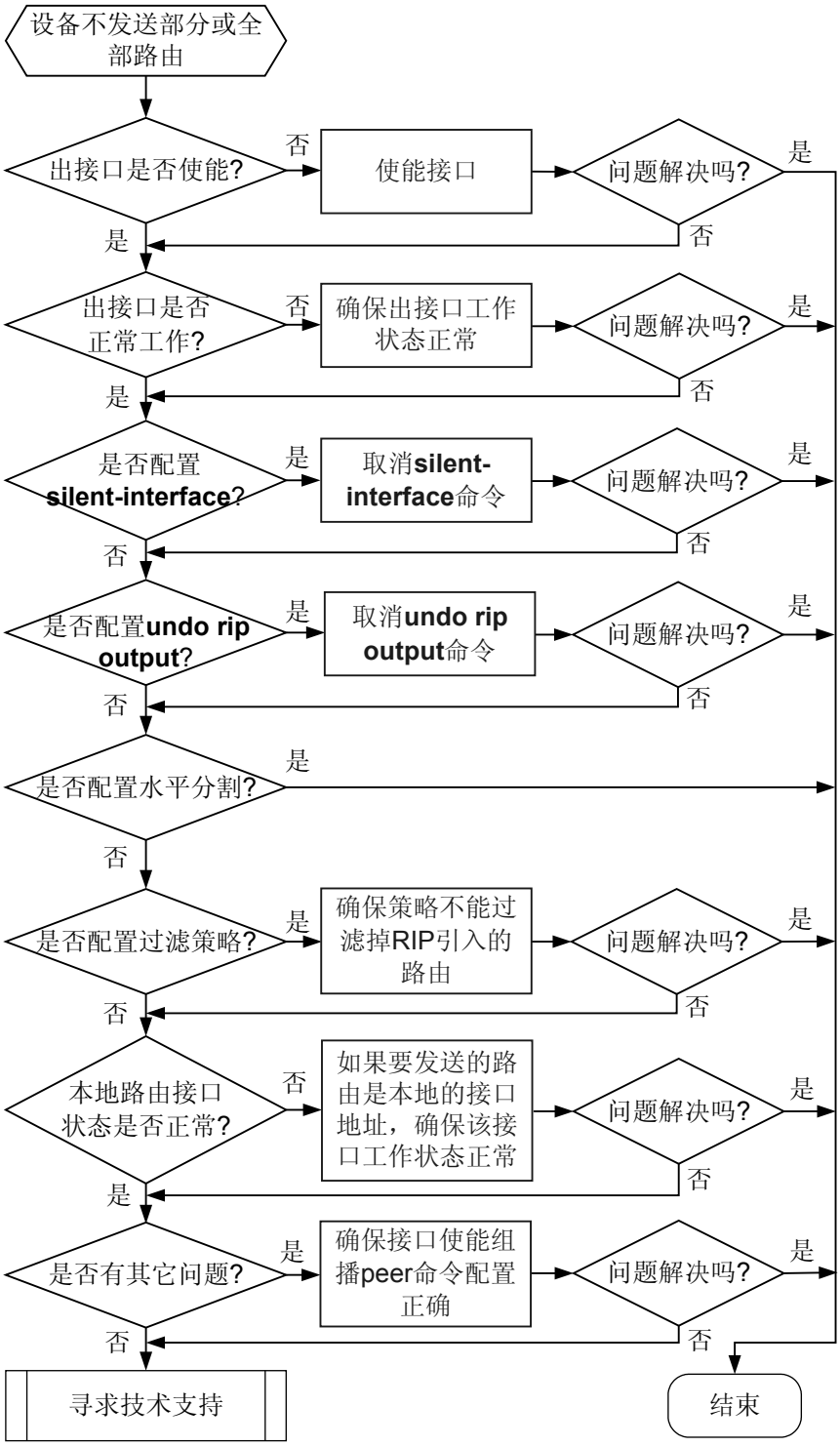
本类故障的常见原因主要包括：

- 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.

故障诊断流程

在配置各交换机后发现交换机不发送部分或全部路由。请使用下面的故障诊断流程，如图 7-25 所示。

图 7-25 RIP 路由发送故障诊断流程图



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。

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

7.8 MCE 故障处理

介绍 MCE 常见故障的定位思路。

7.8.1 VPN 内部用户无法互相访问的定位思路

介绍 VPN 内部用户无法互相访问的故障原因、处理流程和详细的故障处理步骤。

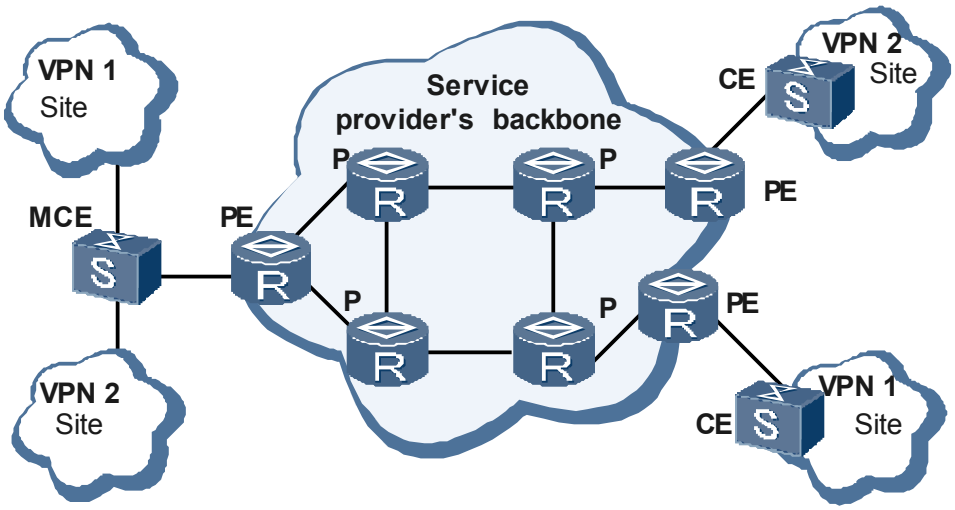
常见原因

MCE 典型组网如图 7-26 所示，整个网络由 CE/MCE、PE、P、Site 组成，其中：

- PE（Provider Edge）：服务提供商边缘设备，是服务提供商网络的边缘设备，与 CE 直接相连。在 MPLS 网络中，对 VPN 的所有处理都发生在 PE 上。
- P（Provider）：服务提供商网络中的骨干设备，不与 CE 直接相连。P 设备只需要具备基本 MPLS 转发能力，不维护 VPN 信息。
- CE（Customer Edge）：为用户网络边缘设备，有接口直接与服务提供商 SP（Service Provider）网络相连。CE 可以是交换机或路由器，也可以是一台主机。通常情况下，CE“感知”不到 VPN 的存在，也不需要支持 MPLS。
- MCE（Multi-VPN-Instance CE）：也为用户边缘设备，MCE 通过将 VLANIF 接口与 VPN 绑定，在一台设备上为每个 VPN 创建和维护独立的路由转发表，实现不同地域相同部门之间的访问，同时实现了不同 VPN 用户之间的业务完全隔离。

使用 MCE（Multi-VPN-Instance CE）技术，可以有效解决多 VPN 网络带来的用户数据安全与网络成本之间的矛盾。其中 AC6605 作为 MCE 设备。

图 7-26 MCE 典型组网图



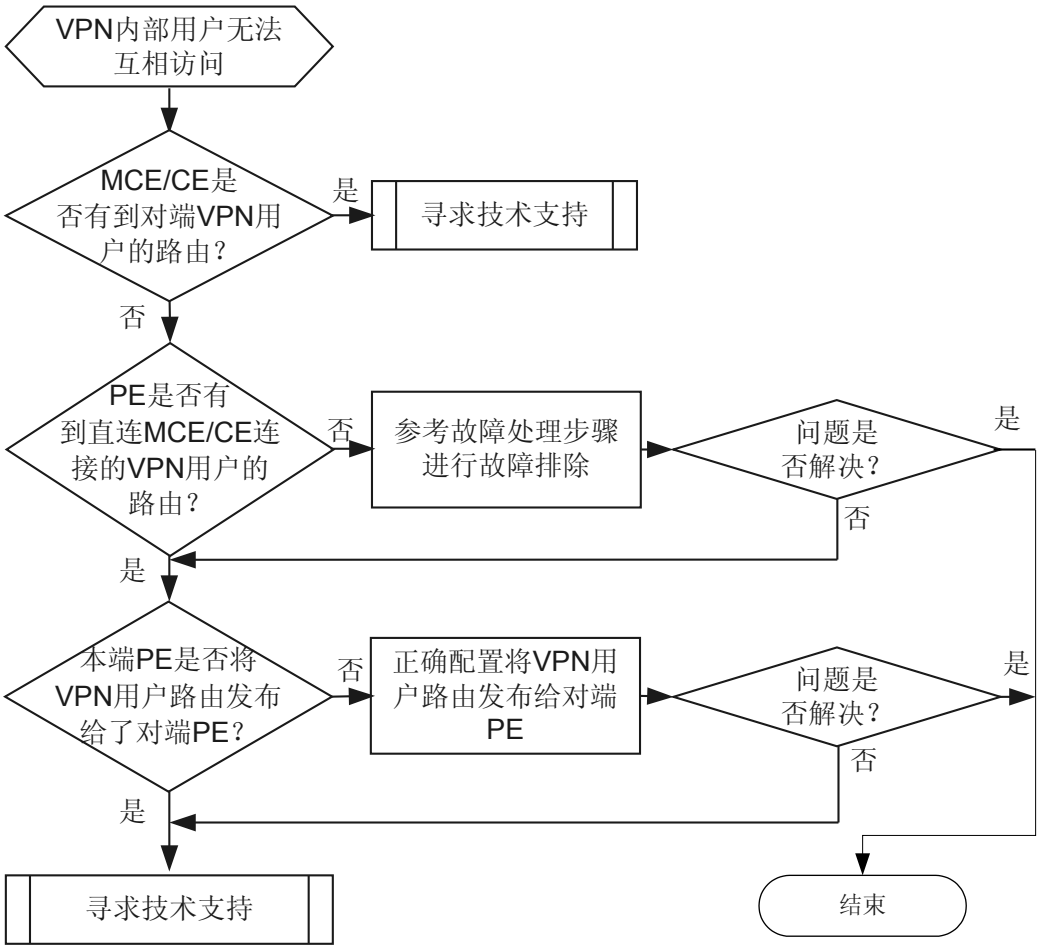
如图所示，VPN 1 用户之间不能正常互访，可能有如下原因：

- CE 和 MCE 之间的路由问题
- CE 或 MCE 和主机之间的路由问题

故障诊断流程

详细处理流程如图 7-27 所示。

图 7-27 VPN 内部用户无法互相访问的故障诊断流程图



故障处理步骤

说明

在执行下面操作前，请注意如下事项：

- 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。
- 请确保 PE 和 CE、MCE 之间网络层互通，如果 PE 和 CE、MCE 之间网络层互通存在故障请参见 **PING 故障处理**进行故障排除。
- 请确保 VPN 用户和对应的 MCE/CE 之间网络层互通，如果 VPN 用户和对应的 MCE/CE 之间网络层互通存在故障请参见 **PING 故障处理**进行故障排除。
- 请确保 PE 和 PE 之间网络层互通，如果 PE 和 PE 之间互通存在故障请参考对应产品的故障处理手册排除 PE 和 PE 之间故障。

操作步骤

步骤 1 检查 MCE/CE 是否有到对端 VPN 用户的路由。

在本端 MCE/CE 上执行命令 **display ip routing-table** *ip-address*，查看本端路由表中是否有到对端 VPN 用户的路由，其中 *ip-address* 为对端 VPN 用户的网段地址。

- 如果显示信息为空，证明没有到对端的 VPN 用户的路由，请执行步骤 2。

- 如果显示信息不为空，但下一跳指向不是和 MCE/CE 直连的 PE，请检查两端的 VPN 用户是否使用相同的地址段，如果是请重新规划地址，保证两端的 VPN 用户使用不同的地址段。
- 如果显示信息不为空，且下一跳指向和 MCE/CE 相连的 PE，证明有到对端的 VPN 用户的路由，请执行步骤 4。

步骤 2 检查 PE 是否有到直连 MCE/CE 连接的 VPN 用户的路由。

请参考对应产品的操作手册查看 PE 上是否有到直连 MCE/CE 连接的 VPN 用户的路由

- 如果 PE 上没有到直连 MCE/CE 连接的 VPN 用户的路由，请执行如下操作：
  - 如果 MCE/CE 和 PE 之间使用的静态路由，证明 PE 上未配置到直连 MCE/CE 连接的 VPN 用户的静态路由，此时请参考 PE 对应产品的操作手册配置到 MCE/CE 连接的 VPN 用户的静态路由。
  - 如果 MCE/CE 和 PE 之间采用的是动态路由协议（RIP、OSPF、BGP、ISIS），证明 MCE/CE 配置发布给 PE 的路由中未引入 VPN 用户路由，此时请参考“配置指南-IP 路由”中“在 MCE 与 PE 间配置路由多实例”进行路由配置。
- 如果 PE 上有到直连 MCE/CE 连接的 VPN 用户的路由请执行步骤 3。

步骤 3 检查本端 PE 是否将 VPN 用户路由发布给了对端 PE。

请检查 PE 配置，确保本端 PE 将 VPN 用户路由发布给了对端 PE，如果未作相关配置，请参见对应产品手册完成相关配置。执行完上述操作后如果故障依然存在请执行步骤 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

8 组播类

关于本章

8.1 二层组播故障处理
介绍了二层组播常见故障的定位思路和案例。

8.2 三层组播故障处理
介绍了三层组播常见故障的定位思路和案例。

8.1 二层组播故障处理

介绍了二层组播常见故障的定位思路和案例。

8.1.1 用户 VLAN 下用户无法收到组播报文故障（IGMP Snooping）处理思路

常见原因

本类故障的常见原因主要包括：

- 硬件（单板、光纤、网线等）引起的 AC6605 上、下行链路故障，导致二层组播流量不通；
- 全局或用户 VLAN 的二层组播配置错误（如未使能 IGMP Snooping），导致二层组播流量不通；
- 组播 VLAN 与用户 VLAN 对应关系配置错误，导致二层组播流量不通；
- AC6605 存在其他二层组播配置冲突（如配置了禁用接口动态学习功能、组播组策略、接口快速离开功能、igmp-snooping require-router-alert 和接口下二层组播数据过滤等），导致二层组播流量不通；
- 当前 AC6605 的二层组播转发表项已达到设备支持的规格上限。

故障诊断流程

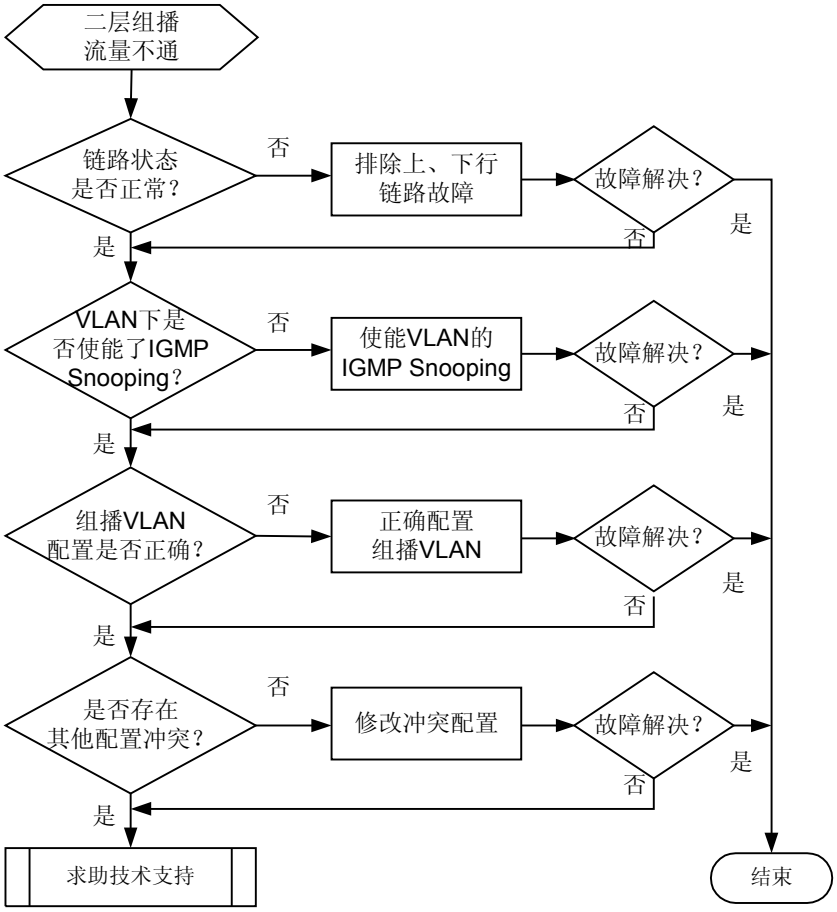
在配置二层组播后发现用户 VLAN 下主机无法收到组播报文。

故障的定位思路如下：

- 检查是否存在链路故障
- 检查是否存在配置错误或冲突
- 检查是否超出支持规格

详细处理流程如图 8-1 所示。

图 8-1 用户 VLAN 下用户无法收到组播报文（IGMP Snooping）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 检查上、下行链路状态是否 Up。

在系统视图下执行 **display interface brief** 命令，检查配置二层组播业务的端口状态是否正常。

- 如果端口物理状态为*down，表示 Administratively Down，则在接口下执行 **undo shutdown** 操作，打开物理端口。
- 如果端口物理状态为 down，则需要检查上、下行物理链路。
- 如果端口物理和协议状态均为 Up，请执行步骤 2。

步骤 2 检查全局和 VLAN 下是否使能了 IGMP Snooping。

系统视图下显示 igmp-snooping enable 字段，则表示全局 IGMP Snooping 已使能。

在 VLAN 视图下执行 **display igmp-snooping configuration** 命令，检查 VLAN 的 IGMP Snooping 配置。

- 如果全局和对应 VLAN 下未显示 igmp-snooping enable 字段，请分别在系统视图和 VLAN 视图下执行 **igmp-snooping enable** 命令，使能 IGMP Snooping。
- 如果全局和对应 VLAN 的 IGMP Snooping 已经使能，请执行步骤 3。

步骤 3 检查组播 VLAN 配置是否正确。

执行 **display multicast-vlan vlan** *vlan-id* 命令，查看 User-vlan 是否绑定了正确的组播 VLAN。

- 如果组播 VLAN 与用户 VLAN 的绑定关系不正确，请执行 **multicast-vlan user-vlan** 命令正确配置。
- 如果组播 VLAN 与用户 VLAN 的绑定关系正确，请执行步骤 4。

  如下所示组播 VLAN10 和用户 VLAN100、VLAN200 的绑定关系正确。

```
[Quidway]display multicast-vlan vlan 10
 Multicast-vlan         : 10
 User-vlan Number       : 2
 IGMP snooping state    : Enable
 MLD  snooping state    : Disable
 User-vlan              Snooping-state
 ------------------------------------------------
 100                     IGMP Enable /MLD Disable
 200                     IGMP Enable /MLD Disable
```

步骤 4 查看是否存在配置冲突，导致二层组播流量不通。

在设备上检查是否存在以下相关配置冲突：

- 配置了禁止接口或 VLAN 动态学习功能

  如果配置了禁止 VLAN 的路由器接口动态学习功能，VLAN 不再监听 IGMP Query 报文，无法生成路由器端口。在 VLAN 视图下执行 **igmp-snooping router-learning** 命令，使能 VLAN 的路由器接口动态学习功能。

- 配置了成员接口快速离开功能

  当某 VLAN 内的接口下仅有一个成员主机时，才能配置接口快速离开功能。如果某 VLAN 内的接口下不止一个接收主机，该 VLAN 配置了成员接口快速离开功能，则当 AC6605 从成员接口收到 IGMP Leave 报文时，不发送特定组查询报文，立即将该接口的转发表项从设备的组播转发表中删除，导致流量不通。

  在 VLAN 视图下，执行 **undo igmp-snooping prompt-leave** 命令，取消成员接口快速离开功能。

- 配置了 igmp-snooping require-router-alert

  如果配置了 igmp-snooping require-router-alert，则 AC6605 会检查 IGMP 报文中的 Option 字段，对于不携带 Option 字段的报文会丢弃。

  在 VLAN 视图下，执行 **undo igmp-snooping require-router-alert** 命令，取消相关配置，则 AC6605 不再检查 IGMP 报文的 Option 字段。

- 配置了组播组策略

  组播组策略可能限制 VLAN 下的主机加入某些组播组，可以在 VLAN 下执行 **display igmp-snooping configuration** 命令，查看组播组策略限制是否正确。如果配置了 ACL 规则，再查看对应的 ACL 规则是否正确。

- 配置了接口下的二层组播数据过滤功能

  如果设备接口下配置了二层组播数据过滤功能，设备端口下会对来自某 VLAN 的 UDP 报文进行过滤，导致二层组播流量不通。

进入物理接口视图，执行 **undo multicast-source-deny vlan** 命令，取消接口下的二层组播数据过滤功能。

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

8.1.2 故障案例

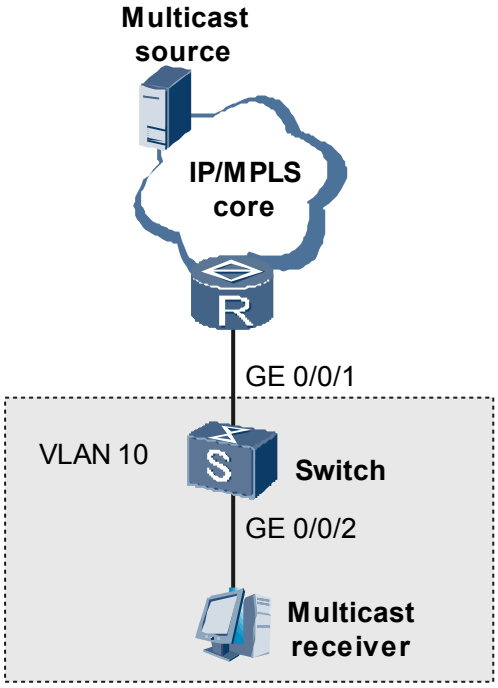
介绍了二层组播的实际处理案例。

未使能 IGMP Snooping 查询器功能导致组播转发异常

网络环境

在如图 8-2 所示的网络中，Switch 利用二层技术实现组播。在 Switch 上配置 IGMP Snooping 后客户端可以正常接收到组播流量，但是只能持续 2 分钟左右。在 Switch 上查看二层组播转发表项发现，当客户端发起组播点播操作时，Switch 上的组播表项可以正常建立，但是只能维持约 2 分钟，组播转发表项消失后则组播转发中断。

图 8-2 未使能 IGMP Snooping 查询器功能导致组播转发异常组网图



故障分析

1. 由于只是组播流量会中断，所以排除链路故障。
2. 通过分析组网发现 IGMP 查询报文不能发送到客户端，因为路由器是静态配置组播组因而不发送 IGMP 查询报文，Switch 上又没有配置主动查询的功能。

   客户端开始点播时发出了 IGMP Report 报文，所以二层组播转发表项能够正常建立。但是由于 IGMP Snooping 默认没有使能表项更新的机制，所以表项老化后除非客户端重新点播，否则二层组播转发表项一直为空。表项建立后默认老化时间是 130 秒（查询间隔 * 健壮系数 + 最大老化时间=60*2+10），所以出现了客户端收到的组播流量只能维持 2 分钟左右的现象。

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 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **igmp-snooping querier enable**，使能 IGMP Snooping 查询器功能。

该命令是强制 Switch 在运行 IGMP Snooping 的情况下也发送 IGMP Query 报文以刷新 Switch 组播转发表项的老化时间，从而保证组播转发的持续。

完成上述步骤后，客户端正常接收到组播流量，不会中断。

----结束

案例总结

当上层路由器的 IGMP 报文因为某些原因不能到达 AC6605，或上层路由器的组播转发表项不需要动态学习而是静态配置时，可在 AC6605 上配置查询器，代替上层路由器发送 IGMP Query 消息。

8.2 三层组播故障处理

介绍了三层组播常见故障的定位思路和案例。

8.2.1 组播业务不通的定位思路

介绍三层组播网络中组播业务不通的故障原因、处理流程和详细故障流程。

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 VLAN 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

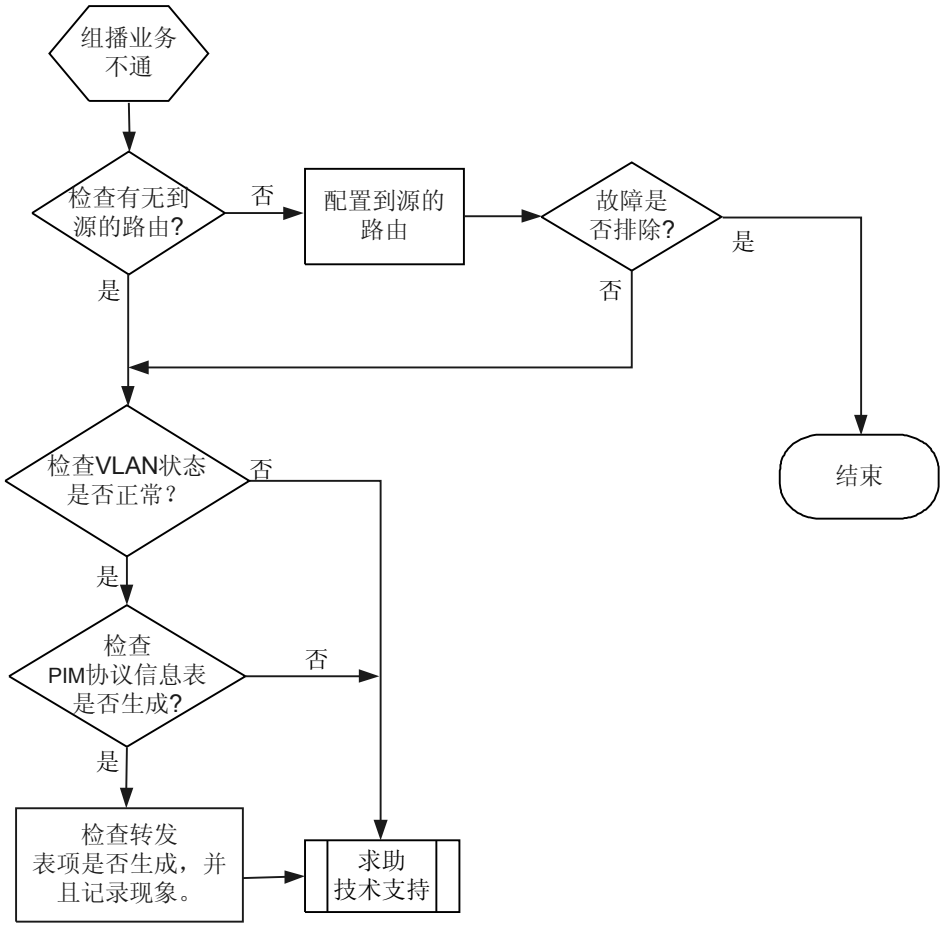
在配置三层组播使能后发现组播业务不通。

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、入接口对应的 VLAN 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 8-3 所示。

图 8-3 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、入接口对应的 VLAN 状态是否正常。

在设备上执行 **display interface vlanif** *vlan-id* 命令，检查 VLAN 状态是否正常。

- 如果组播转发表项出、入接口对应的 VLAN 状态不正常，则组播转发表项无法生成，请参考 **5.1 VLAN 故障处理**排除 VLAN 故障。

  如下显示 VLANIF 90 的状态为 DOWN：

```
[Quidway] display interface Vlanif 90
Vlanif90 current state : DOWN
Line protocol current state : DOWN
Description:HUAWEI, Quidway Series, Vlanif90 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 1.1.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-2000-0140
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input:  0 packets, 0 bytes
Output:  0 packets, 0 bytes
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

- 如果 VLAN 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

相关告警与日志

相关告警

无

相关日志

无

8.2.2 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：

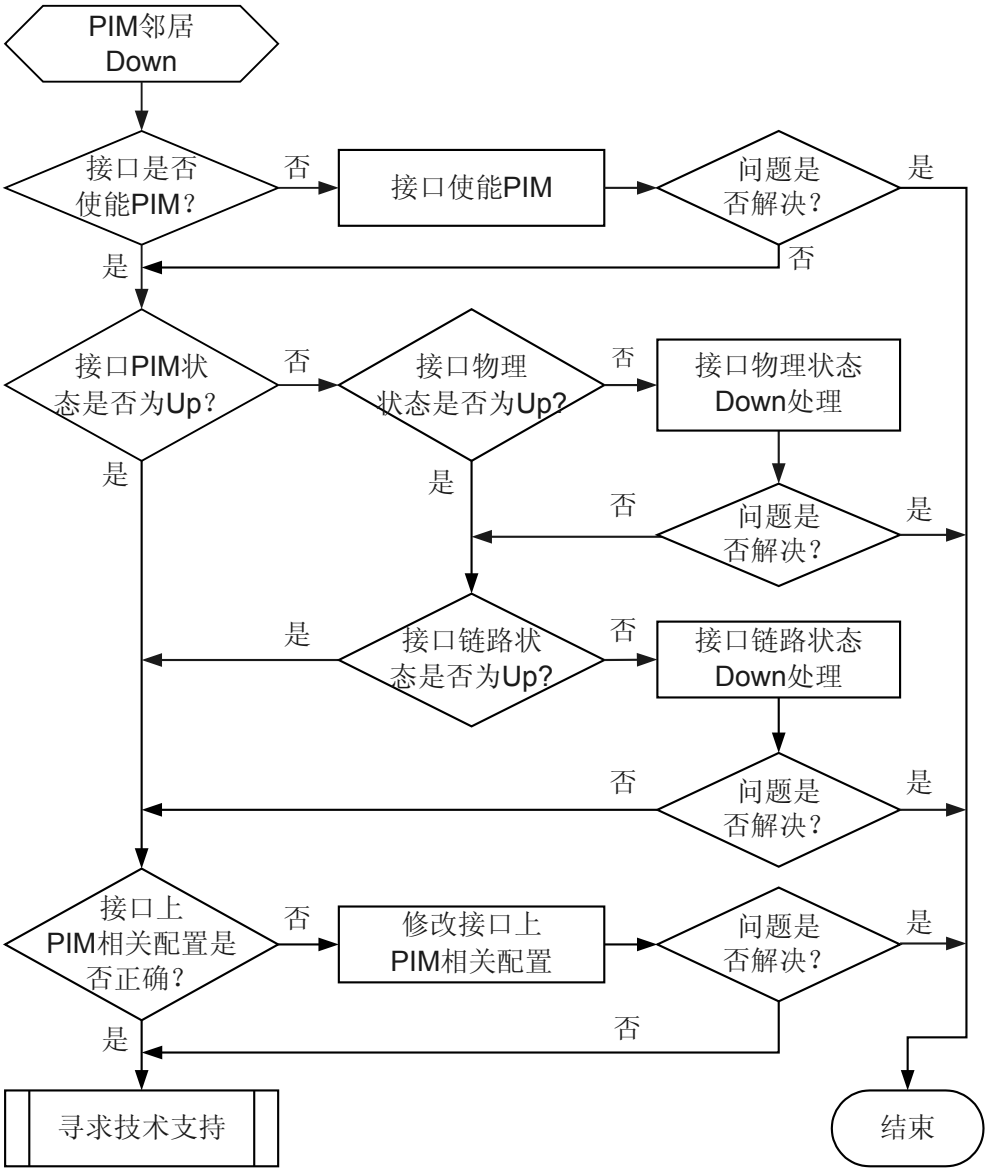
- 接口物理状态或协议状态为 Down
- 接口没有使能 PIM
- 接口的 PIM 相关配置不正确

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 8-4 排除故障。

图 8-4 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。

- 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

8.2.3 PIM-SM 网络中 RPT 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：

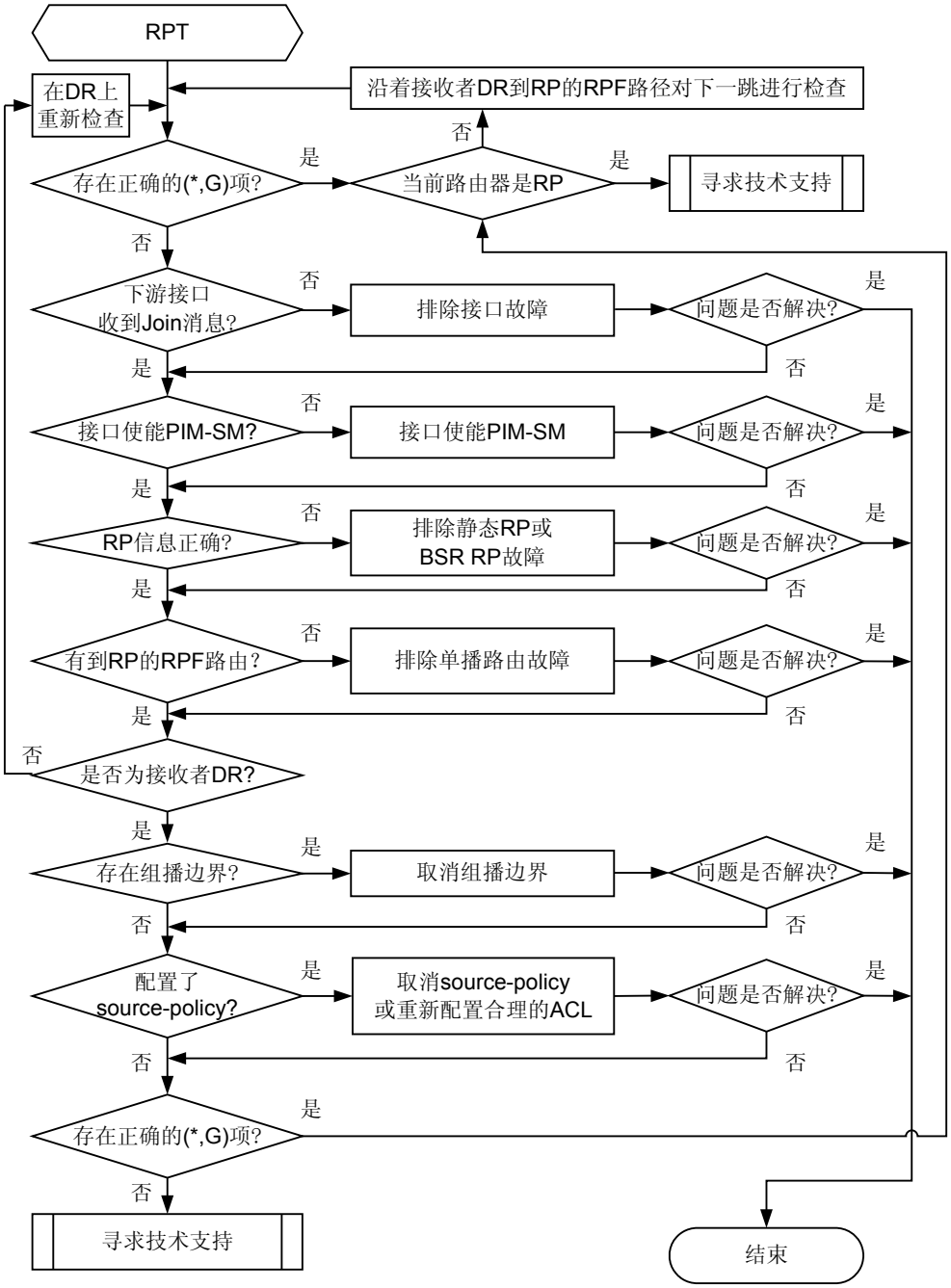
- 组播设备到 RP 的单播路由不通
- 各组播设备的 RP 地址不一致
- 组播设备的下游接口没有收到（*，G）加入
- 接口没有使能 PIM-SM
- 到 RP 的 RPF 路由不正确（举例：单播路由环路）
- 配置问题（举例：TTL、MTU 或组播边界配置不当等）

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 8-5 排除故障。

图 8-5 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

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 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。

- 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。

- 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

8.2.4 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：

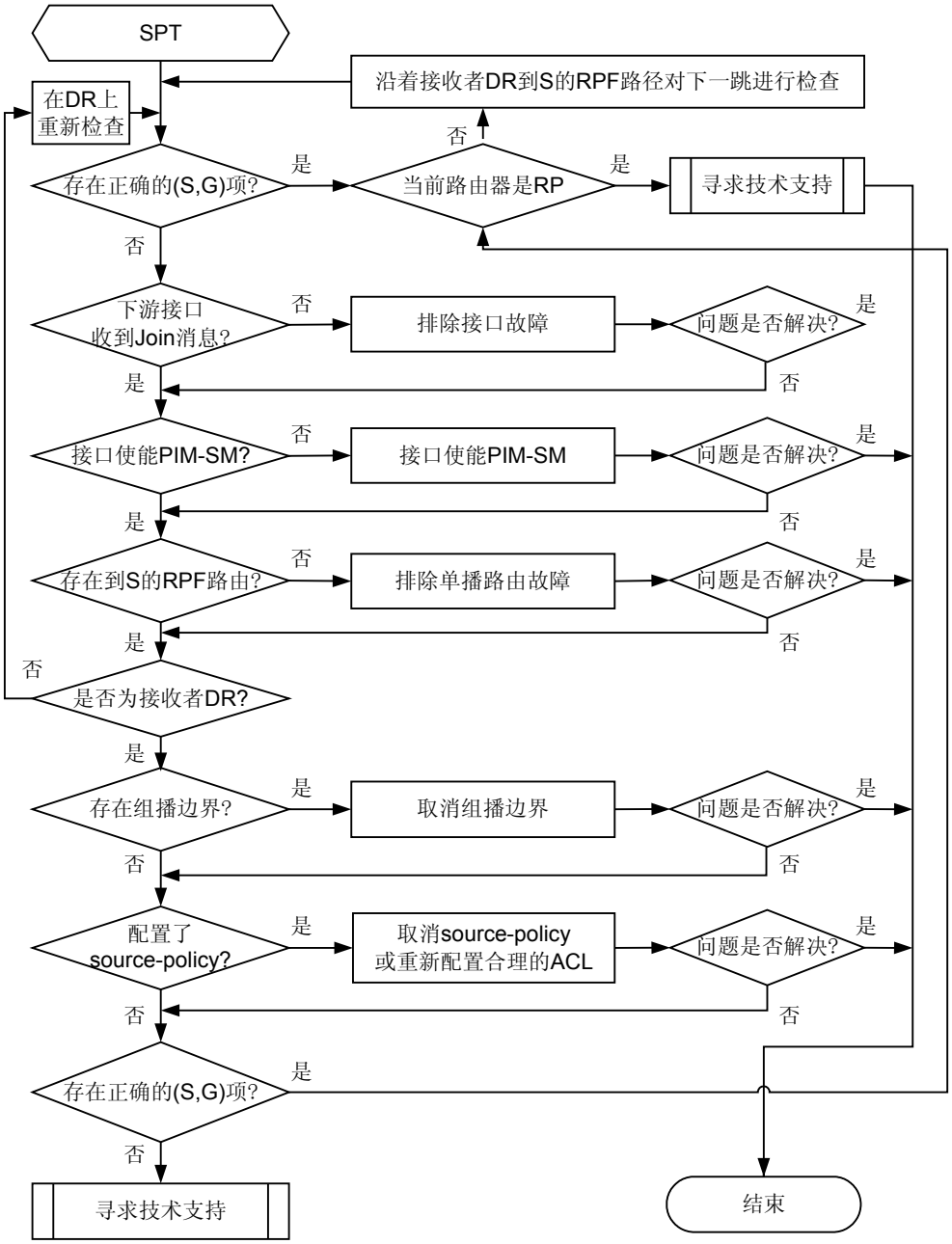
- 组播设备的下游接口没有收到（S，G）加入
- 接口没有使能 PIM-SM
- 到组播源的 RPF 路由不正确（举例：单播路由环路）
- 配置问题（举例：TTL、MTU、切换阈值或组播边界配置不当等）

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 **8-6** 排除故障。

图 8-6 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

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 PIM 路由表中是否存在正确的（S,G）表项

在设备上执行 **display pim routing-table** 命令，查看 PIM 路由表中是否存在正确的（S,G）表项。

- 如果 PIM 路由表中存在正确的（S,G）表项：
  - 查看 Flag 中是否有 SPT 标志。
    - 如果组播组属于 ASM 范围，且 SPT 切换由 RP 触发，RP 的上游接口是注册接口，则说明 RP 收到了源 DR 发送的注册报文，但是 SPT 没有成功建立，请联系华为技术支持工程师。
    - 如果组播组属于 ASM 范围，且 SPT 切换由接收者 DR 触发，上游接口是朝向 RP 的 RPF 接口，而不是到达组播源的 SPT 接口，则表明 SPT 没有成功建立。

      在接收者 DR 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“spt-switch-threshold traffic-rate”或“spt-switch-threshold infinity”，请执行 **undo spt-switch-threshold** 命令删除配置信息或执行 **spt-switch-threshold** *traffic-rate* 命令重新配置合理的 traffic-rate。
  - 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

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。

- 如果配置信息中出现“source-policy acl-number”或“source-policy acl-name”，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

8.2.5 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

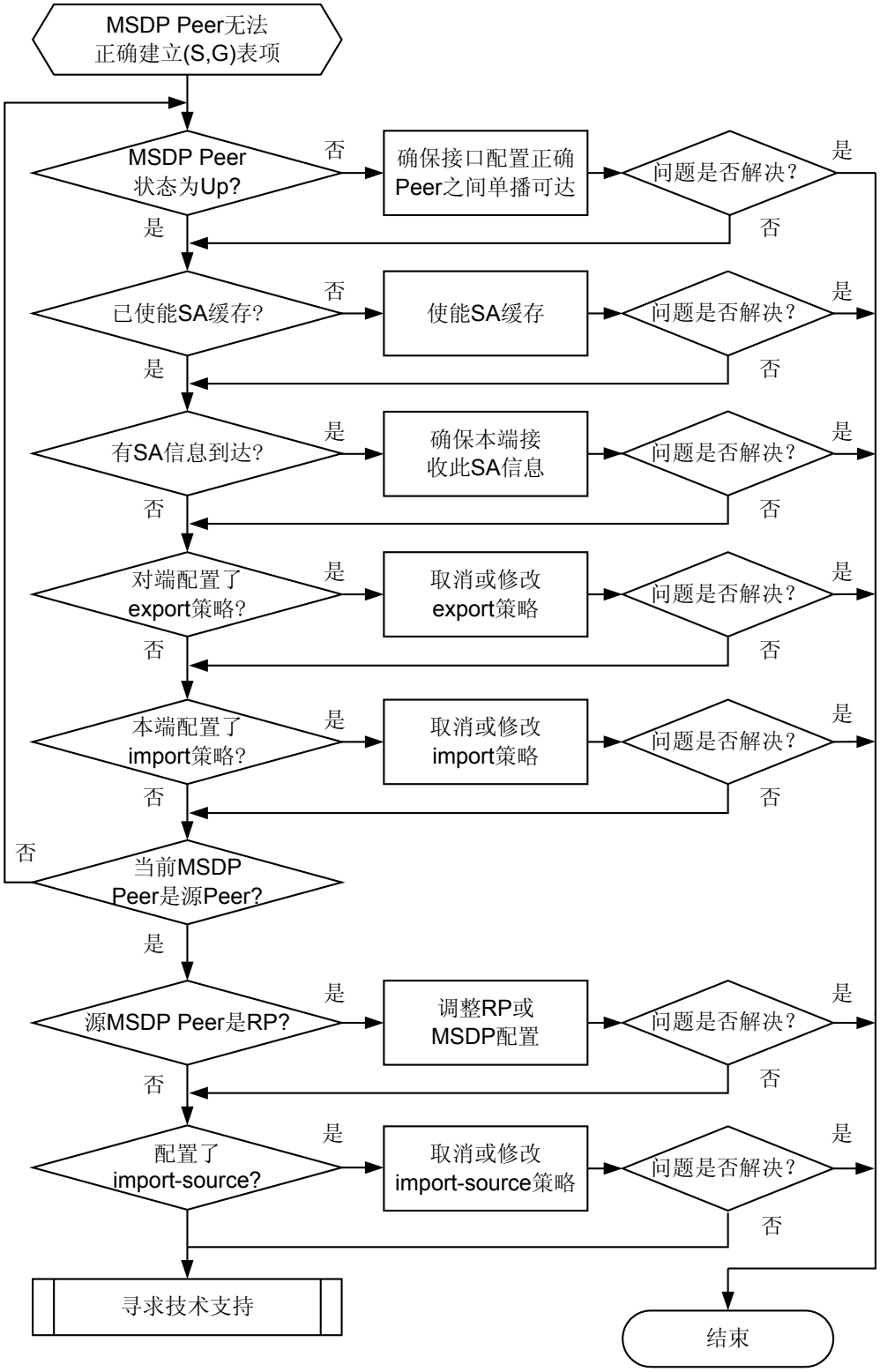
- 域内组播协议采用的不是 PIM-SM
- 到组播源的 RPF 路由不正确（举例：单播路由环路）
- 配置问题（举例：SA-Policy、import-policy、TTL、切换阈值或组播边界配置不当等）
- SA 消息没有通过 RPF 检查

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 8-7 排除故障。

图 8-7 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。

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”或“peer peer-address sa-policy export acl acl-name”，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”或“peer peer-address sa-policy import acl acl-name”，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* | *acl-name* }]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”“import-source acl ac-name”，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

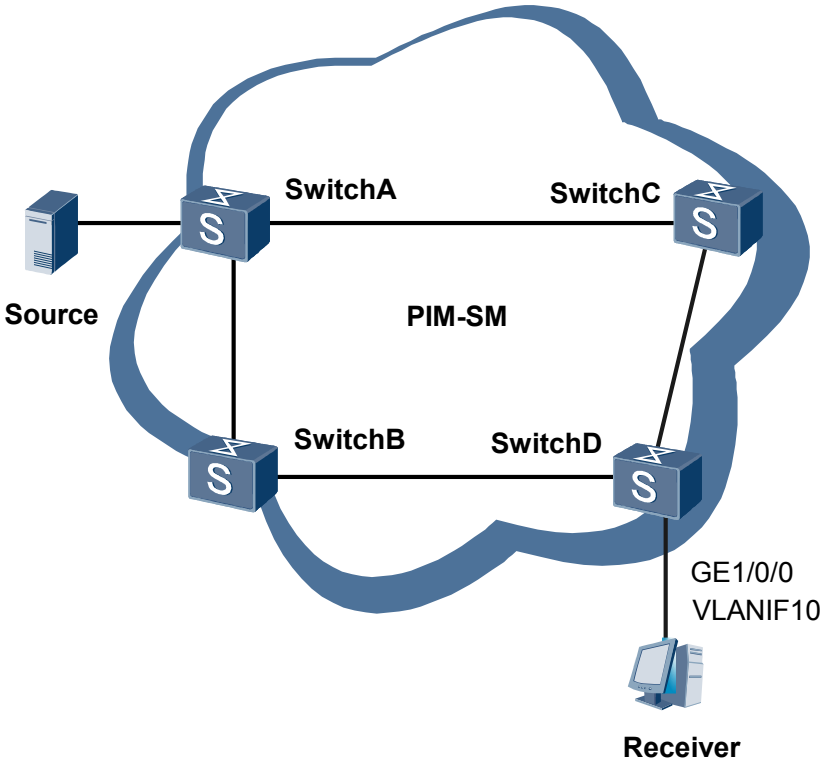
8.2.6 故障案例

RPF 检查失败导致设备无法正确处理 BSR 报文

网络环境

在图 8-8 的网络中部署组播业务，SwitchA 作为 BSR 和 RP，各交换机间采用 PIM-SM 协议。SwitchD 上连接组播接收者。配置完成后，接收者无法接收组播流量。

图 8-8 组播网络基本组网图



故障分析

1. 在各交换机上执行 **display pim neighbor** 命令查看 PIM 邻居是否正常建立。
2. 在 SwitchD 上执行 **display igmp routing-table** 命令查看 SwitchD 是否存在 IGMP 加入请求，针对 SwitchD 的 VLANIF10 接口存在如下显示信息：

```
Total 1 entry

00001.  (*, 225.1.1.1)
        List of 1 downstream interface
         Vlanif10 (10.100.0.1),
                   Protocol: IGMP
```

则 SwitchD 上有加入请求，排除该问题。

3. 在各设备上执行 **display pim rp-info** 命令，查看各设备上 RP 是否正确建立。发现 SwitchD 没有学习到 RP。使用测试仪抓包发现，SwitchC 已经向 SwitchD 发送了 BSR 报文。
4. 在 SwitchD 上执行 **debugging pim event** 命令，发现是由于 RPF 检查失败导致 SwitchD 忽略从 SwitchC 发送的 BSR 报文。
5. 在 SwitchD 上执行 **display ip routing-table** 命令，发现 SwitchD 到达 BSR 及 RP 的路由下一跳是 SwitchB，而不是 SwitchC。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

在 SwitchD 上进行如下配置。

步骤 2 执行命令 **ip route-static** *ip-address*，配置 SwitchD 的下一跳为 SwitchC。

完成上述操作后，SwitchD 可以正常学习到 RP，接收者能够接收到组播数据，故障排除。

----结束

案例总结

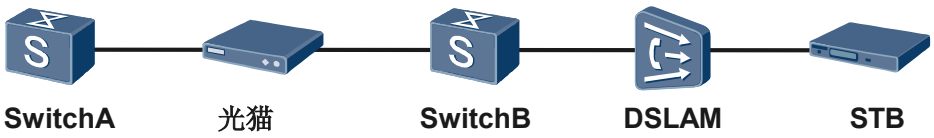
RPF 检查失败会导致协议报文无法被正确处理。RPF 检查不仅影响组播报文的转发，同时也会对 BSR 等协议报文进行检查。在部署组播业务时，要确保单播路由表的状态，以保证 RPF 检查能够正确完成。

部署 QinQ 后用户不能观看 IPTV

网络环境

如图 8-9 所示，网络中部署了 IPTV 业务，在 SwitchB 上部署了 QinQ 后，用户无法正常观看 IPTV，但是 SwitchB 在未部署 QinQ 之前，IPTV 可以正常观看。

图 8-9 在 Switch 上部署 QinQ 后用户不能观看 IPTV 的组网图



故障分析

QinQ 报文与普通 VLAN 报文相比，QinQ 报文长度的最大值增加了 4 字节，即 1522 字节。由于在部署了 QinQ 后，用户无法观看 IPTV，怀疑链路上有设备无法处理 1522 字节的报文：

1. 在 SwitchA 的下行接口和 SwitchB 的上行接口分别抓取报文，观察后发现在 SwitchB 的上行接口获取的 1522 字节的报文在 SwitchA 的下行接口处丢失，说明 1522 字节的报文在中间网络丢失。
2. 将 SwitchA 和 SwitchB 间的光猫传输更换为尾纤直连后，发现可以正常观看 IPTV，可判定为中间光猫无法处理大于等于 1522 字节的报文而引起故障。

操作步骤

步骤 1 将 SwitchA 和 SwitchB 间的光猫传输更换为尾纤直连。

完成上述操作后，无法观看的 IPTV 恢复正常，故障排除。

----结束

案例总结

对应类似故障，如果现场无法抓包，也可以在 SwitchA 配置 QinQ 终结子接口，并在 DSLAM 处 Ping 目的地址为 SwitchA 大小为 1522 字节的报文，然后在 SwitchA 端确认该报文在传输过程中丢失，同样可以定位出问题。

说明

配置 QinQ 后可能因 QinQ 配置错误导致业务不通。

9 安全类

关于本章

9.1 AAA 故障处理
介绍了 AAA（Authentication，Authorization，Accounting）常见故障的定位思路和案例。

9.2 ARP 安全故障处理
介绍了 ARP 安全常见故障的定位思路。

9.3 NAC 故障处理
介绍了 NAC（Network Access Control）常见故障的定位思路。

9.4 DHCP Snooping 故障处理
介绍了 DHCP Snooping 常见故障的定位思路和案例。

9.5 流量抑制故障处理
介绍流量抑制常见故障的定位思路。

9.6 CPU Defend 故障处理
介绍 CPU 防攻击常见故障的定位思路。

9.7 MFF 故障处理
介绍 MFF 常见故障的定位思路。

9.8 ACL 故障处理
介绍 ACL 常见故障的定位思路和故障处理案例。

9.9 PPPoE+故障处理
介绍 PPPoE+常见故障的定位思路。

9.10 URPF 故障处理
介绍了 URPF（Unicast Reverse Path Forward）常见故障案例。

9.1 AAA 故障处理

介绍了 AAA（Authentication，Authorization，Accounting）常见故障的定位思路和案例。

9.1.1 RADIUS 用户认证失败的定位思路

介绍 RADIUS 用户认证失败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：

- 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
- AC6605 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 AC6605 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

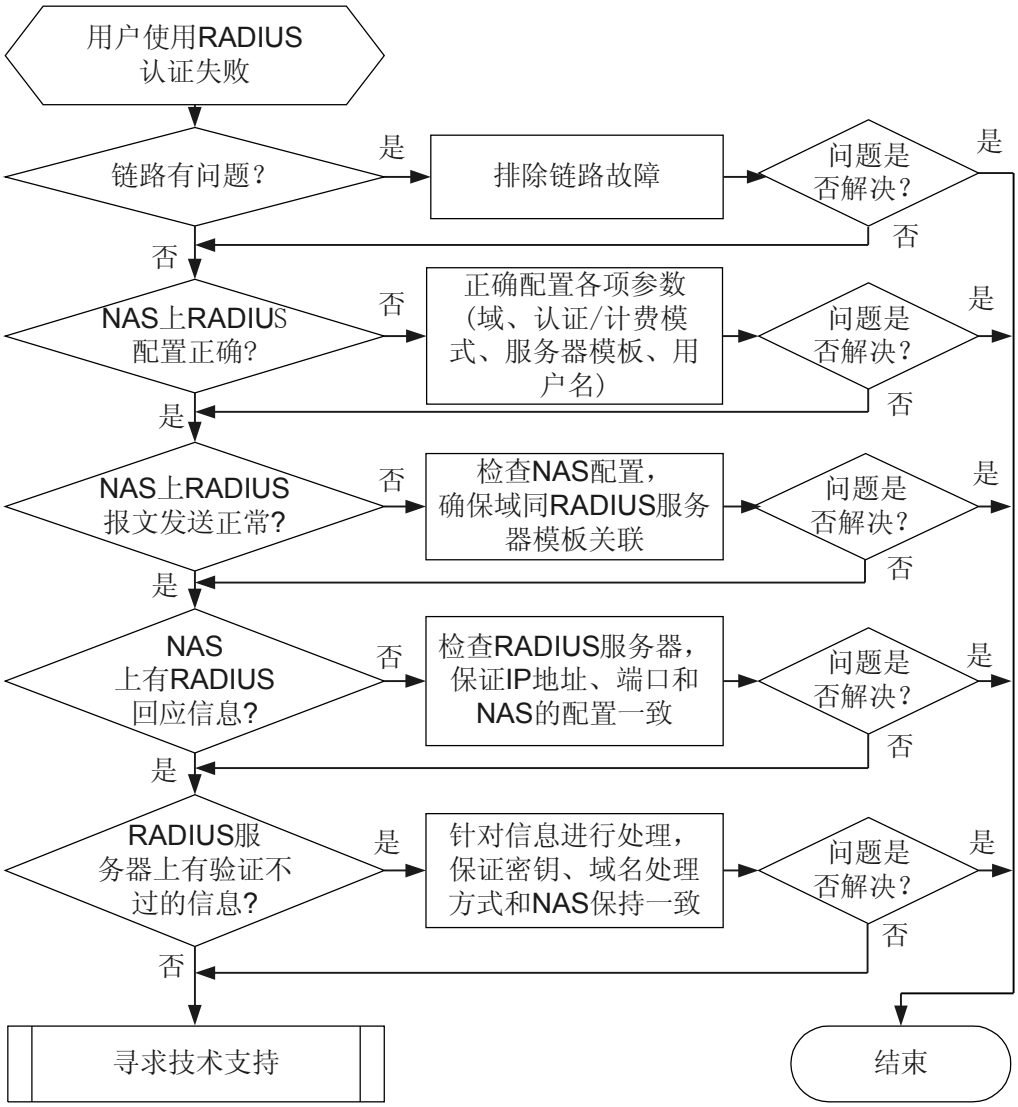
在配置 RADIUS 后，发现用户不能通过 RADIUS 认证。

故障的定位思路如下：

- 检查 AC6605 和 RADIUS 服务器的链路连接是否正常
- 检查 AC6605 上的 RADIUS 配置是否正确，包括域名、服务器模板、认证模式、计费模式
- 检查 RADIUS 服务器是否正常，包括配置的 NAS 的 IP 地址、端口、共享密钥是否一致

详细处理流程如图 9-1 所示。

图 9-1 RADIUS 用户认证失败的故障诊断流程图



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 通过 **ping** 检查 NAS（Network Access Server）设备与 RADIUS 服务器之间的路由是否有故障。

AC6605 就是 NAS 设备，即充当网络接入服务器的角色。

- 如果 ping 不通，请先根据 **7.2.1 PING 不通故障处理思路**排除路由的故障。
- 如果能 ping 通，请执行步骤 2。

步骤 2 检查 AC6605 的 RADIUS 配置。

- 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。
- 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 3。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 3 检查 RADIUS 报文收发是否正常。

在 AC6605 的用户视图下执行命令 **debugging radius packet** 打开 RADIUS 调试信息开关，观察是否有 RADIUS 报文的发送和接收。

```
<Quidway> debugging radius packet
<Quidway> terminal debugging
<Quidway> 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 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 Quidway 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 AC6605 上的 RADIUS 认证报文能正常向外发送。
Nov 10 2010 15:23:34.260.6 Quidway %%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 NAS 设备地址、端口和对端一致，并且服务器上相关端口的服务已经启动。
Nov 10 2010 15:23:34.260.6 Quidway RDS/7/ debug2: [RDS (Evt):] Send a msg (Auth reject) Nov 10 2010 15:23:34.260.7 Quidway 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 NAS 设备的地址和共享密钥。 ● RADIUS 服务器给 NAS 设备配置的共享密钥和对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 NAS 设备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 4。

步骤 4 检查在线用户数是否达到了定义的最大值。

NAS 设备和 RADIUS 服务器对接入的用户数都有规格限制。在 AC6605 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，需要从用户端去排查问题，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 **3.3.1 Telnet 登录失败的定位思路**、**3.4.1 FTP 登录失败的定位思路**。
- 如果是接入用户，请参考 **9.3 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

9.1.2 HWTACACS 用户认证失败的定位思路

介绍 HWTACACS 用户认证失败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：

- 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
- AC6605 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 AC6605 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

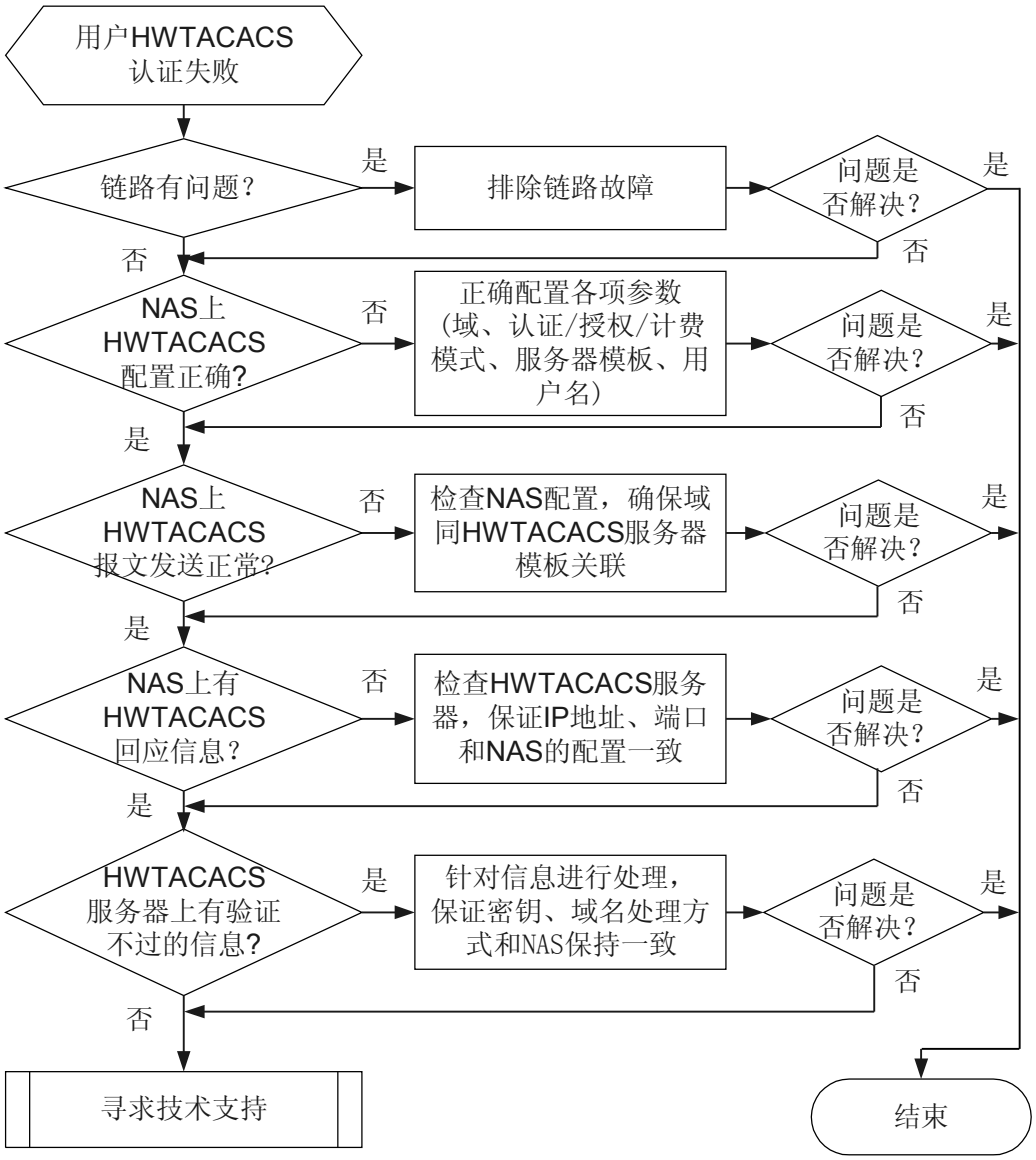
在配置 HWTACACS 后，发现用户不能通过 HWTACACS 认证。

故障的定位思路如下：

- 检查 AC6605 和 HWTACACS 服务器的链路连接是否正常
- 检查 AC6605 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、服务器模板
- 检查 HWTACACS 服务器是否正常，包括 NAS 设备的 IP 地址、端口、共享密钥是否一致

详细处理流程如图 9-2 所示。

图 9-2 HWTACACS 用户认证失败的故障诊断流程图



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 通过 **ping** 检查 NAS（Network Access Server）设备与 HWTACACS 服务器之间的路由是否有故障。

AC6605 就是 NAS 设备，即充当网络接入服务器的角色。

- 如果 ping 不通，请先根据 **7.2.1 PING 不通故障处理思路**排除路由的故障。

- 如果能 ping 通，请执行步骤 2。

步骤 2 检查 AC6605 设备的 HWTACACS 配置。

- 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。
- 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 3。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 3 检查 HWTACACS 报文收发是否正常。

在 AC6605 的用户视图下执行命令 **debugging hwtacacs all** 打开 HWTACACS 调试信息开关，观察是否有 HWTACACS 报文的发送和接收。

```
<Quidway> debugging hwtacacs all
<Quidway> terminal debugging
<Quidway> 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 Quidway TAC/7/ Event:HandleReqMsg: Session status is not connect now. Nov 10 2010 15:43:35.500.7 Quidway TAC/7/ Event:statistics: transmit flag: 1-SENDPACKET, server flag: 0-authentication, packet flag: 0xff Nov 10 2010 15:43:35.550.1 Quidway TAC/7/ Event:HandleResp: Session status is connect now. Nov 10 2010 15:43:35.550.2 Quidway 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 AC6605 发送 HWTACACS 认证报文成功。
Nov 10 2010 15:49:18.430.6 Quidway TAC/7/ Event:HandleReqMsg: Session status is not connect now. Nov 10 2010 15:49:18.430.7 Quidway TAC/7/ Event:statistics: transmit flag: 1-SENDPACKET, server flag: 0-authentication, packet flag: 0xff Nov 10 2010 15:49:18.480.2 Quidway TAC/7/ Event:HandleResp: Session status is connect now. Nov 10 2010 15:49:18.480.3 Quidway 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 NAS 设备地址、端口和对端一致，并且服务器上相关端口的服务已经启动。
Nov 10 2010 16:02:35.760.1 Quidway 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 NAS 设备的地址和共享密钥。 ● HWTACACS 服务器给 NAS 设备配置的共享密钥和对端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 NAS 设备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 4。

步骤 4 检查在线用户数是否达到了定义的最大值。

NAS 设备和 HWTACACS 服务器对接入的用户数都有规格限制。在 AC6605 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，需要从用户端去排查问题，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 **3.3.1 Telnet 登录失败的定位思路**、**3.4.1 FTP 登录失败的定位思路**。
- 如果是接入用户，请参考 **9.3 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

9.1.3 故障案例

介绍了 AAA 的实际处理案例。

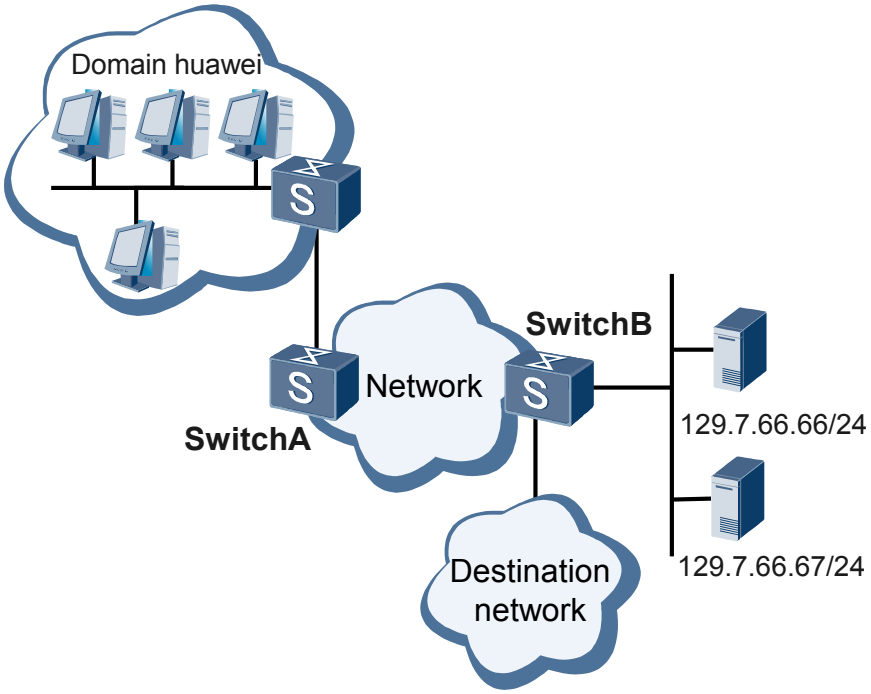
用户登录设备十几秒内被强制下线

网络环境

在图 9-3 所示的网络中，用户通过网络接入服务器 SwitchB 访问网络，在 SwitchB 上对用户登录进行认证、授权和计费。

SwitchB 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，管理员临时采用本地认证。

图 9-3 用户接入组网图



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 SwitchB 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 SwitchB 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 xxxxxx
    radius-server authentication 129.7.66.66 1645
    radius-server accounting 129.7.66.66 1646
    undo radius-server user-name domain-included
   #
   aaa
    local-user telenor password cipher xxxxxxx
    authentication-scheme default
    #
    authentication-scheme provera
     authentication-mode  radius  local
    #
    authorization-scheme default
    #
    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 xxxxxxx
 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，这两个参数有命令 **radius-server timeout** 和 **radius-server retransmit** 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

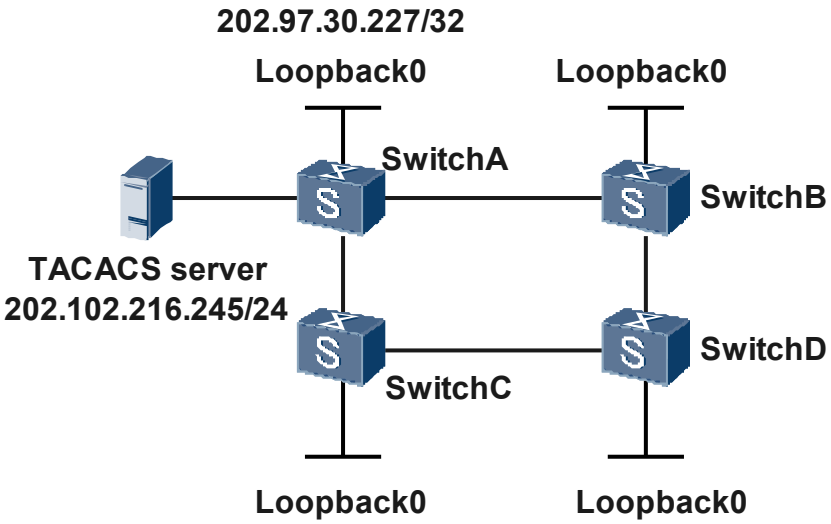
在接入网络中，通过 AAA 验证用户登录设备时，如果远端服务器不可用需要暂时使用本地认证时，计费方案必须是不计费，否则将导致用户下线。

合法的用户名和密码不能通过 HWTACACS 认证

网络环境

在图 9-4 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，其中四台交换机属于同一个 AS 域，路由协议采用 IBGP、ISIS。现按照客户规划新的私有 AS 号重新配置交换机，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 9-4 核心网 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 SwitchA 上执行 **ping** 命令，检查交换机和 HWTACACS Server 是否互通，发现能够 ping 通。
3. 在 SwitchA 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 SwitchA 的 Loopback 接口地址。

   由于删除的 ISIS 协议中包括 Loopback 接口的 IP 地址，并且 HWTACACS 使用 SwitchA 的 Loopback 接口地址作为源 IP，因此考虑可能是交换机无法收到 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 SwitchA 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 SwitchA 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。

   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，交换机无法接收 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

AC6605 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 用户使用本地帐号时无法登录设备。

故障分析

1. 802.1x 用户认证正常，说明 AC6605 和 RADIUS 服务器的连接没有问题。
2. AC6605 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 123456
 radius-server authentication 192.168.1.27 1645
 radius-server accounting 192.168.1.27 1646
#
......
interface GigabitEthernet0/0/1
 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
 #
 accounting-scheme default
 accounting-scheme account
 #
 domain default
  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 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 AC6605 上配置 Telnet 用户使用本地认证。

  创建新的域供 Telnet 用户使用。

```
<Quidway> system-view
[Quidway] aaa
[Quidway-aaa] domain telnet
[Quidway-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）。

```
<Quidway> 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       : -

<Quidway> display authentication-scheme default

  Authentication-scheme-name    : default
  Authentication-method         : Local
  Authentication-super method   : Super authentication-super
<Quidway> display authorization-scheme default
------------------------------------------------------------------------------
 Authorization-scheme-name   : default
 Authorization-method        : Local
......
<Quidway> 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。

```
<Quidway> system-view
[Quidway] aaa
```

```
[Quidway-aaa] local-user telnetuser@telnet password simple 123456
[Quidway-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。

9.2 ARP 安全故障处理

介绍了 ARP 安全常见故障的定位思路。

9.2.1 合法用户的 ARP 表项被修改的定位思路

介绍合法用户的 ARP 表项被修改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：

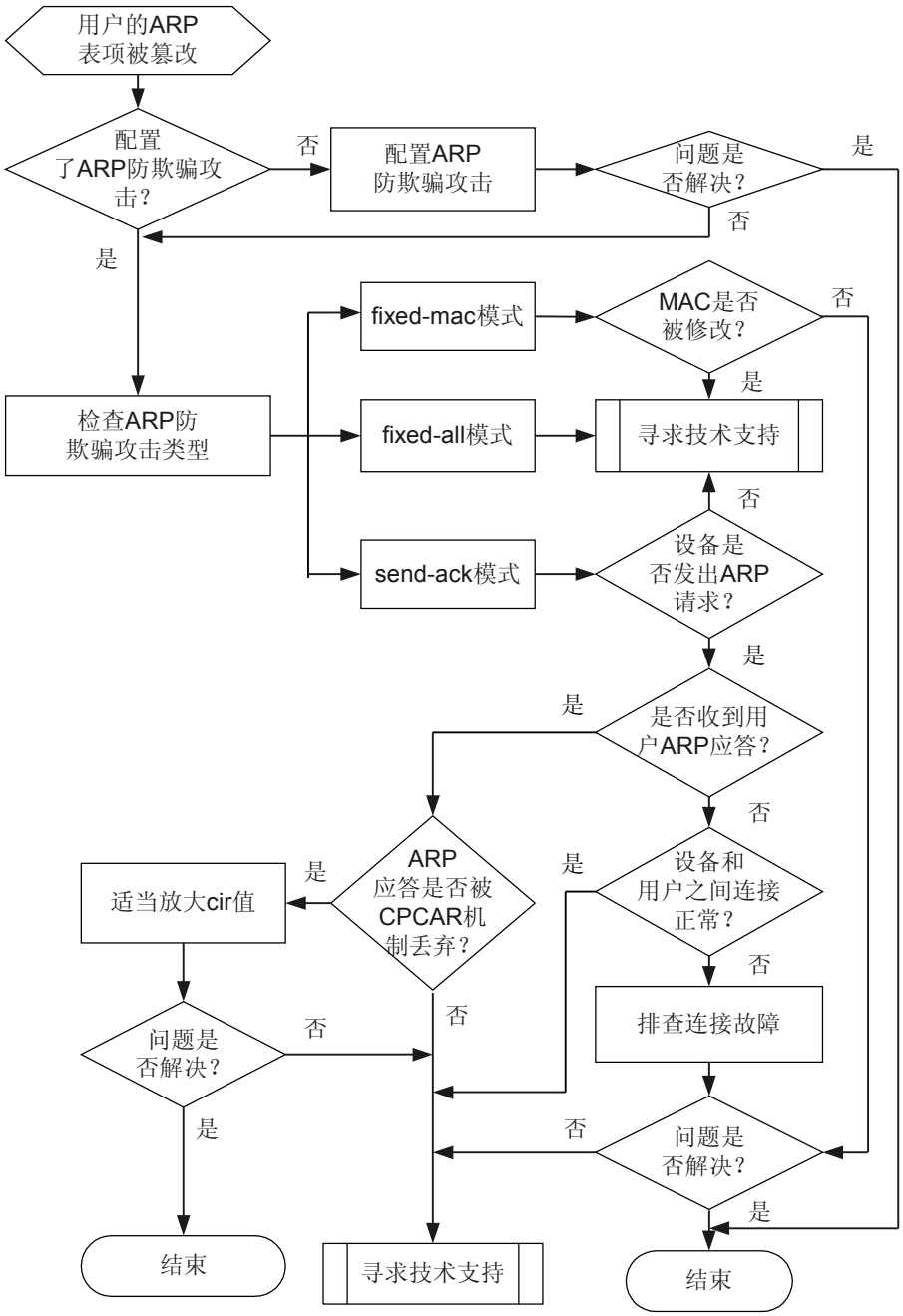
- 攻击者伪造合法用户的 ARP 报文修改合法用户的 ARP 表项

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 9-5 所示。

图 9-5 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 AC6605 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。

- 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 vlanif** *vlan-id* 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 AC6605 没有发出 ARP 请求，请直接执行步骤 4。
2. 如果 AC6605 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 **car** 命令适当放大 **cir** 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

9.2.2 网关地址被仿冒的定位思路

介绍网关地址被仿冒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：

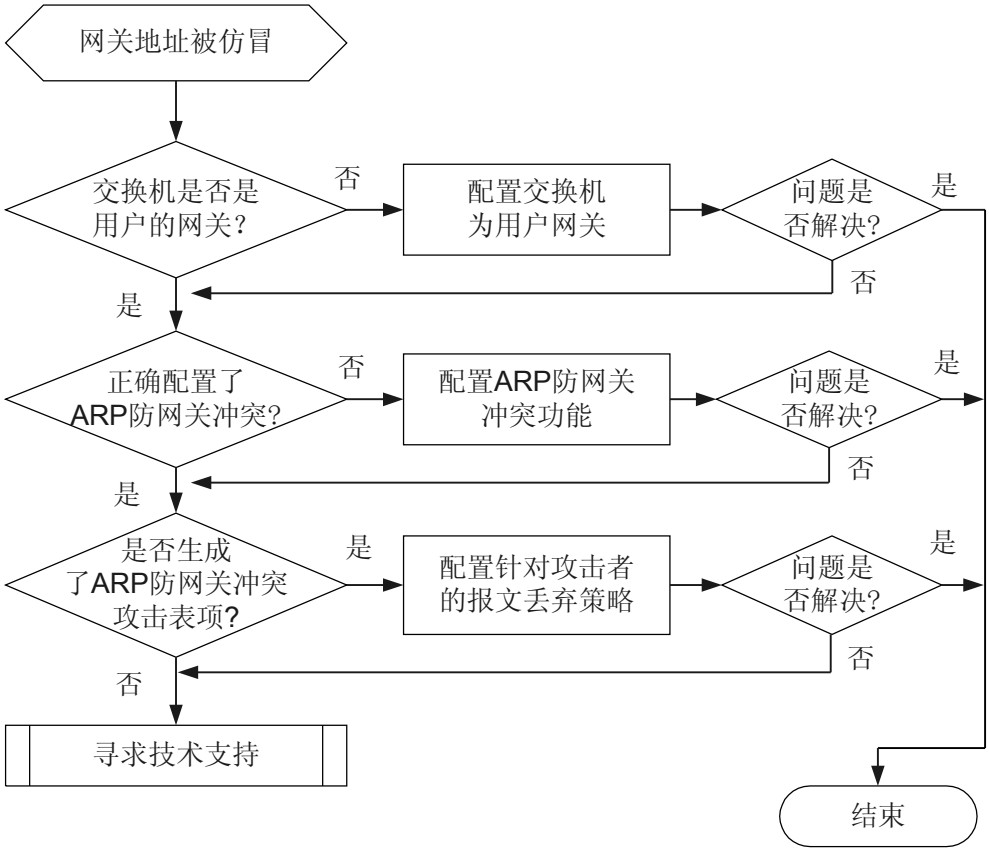
- 攻击者冒充网关发送免费 ARP 报文给用户，用户修改网关地址
- 攻击者冒充网关发送 ICMP 不可达攻击报文或者 ICMP 重定向报文给用户

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 9-6 所示。

图 9-6 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 AC6605 设备是否为用户网关。如果网关不在 AC6605 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 AC6605 上。

- 执行命令 **display arp all**，查看网关地址对应的表项类型。

  如果 **TYPE** 为 **I-**，表示接口本身的表项地址。

```
<Quidway> display arp all
IP ADDRESS    MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE    VPN-INSTANCE
                                        VLAN
------------------------------------------------------------------------------
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 AC6605 上。

```
<Quidway> display ip routing-table 1.1.1.1
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       InLoopback0
```

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 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

- 1.3.6.1.4.1.2011.5.25.165.2.2.2.1

相关日志

无

9.2.3 ARP 报文攻击导致用户流量中断的定位思路

介绍 ARP 报文攻击导致用户流量中断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：

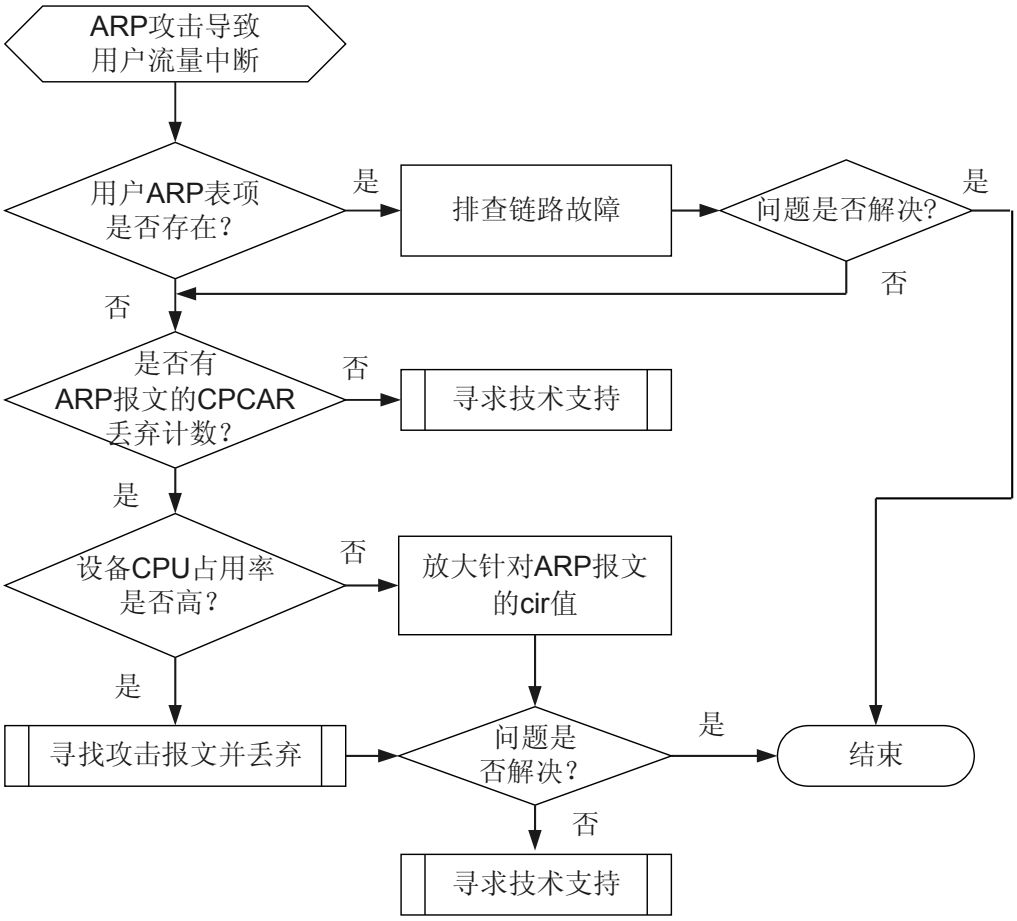
- 攻击者发送大量 ARP 请求，导致目的网段的负担加重。如果 AC6605 配置了三层接口，这些 ARP 报文还会送到 CPU 增加了 CPU 的负担，同时有可能导致合法用户流量中断，形成拒绝服务攻击。

故障诊断流程

AC6605 的 ARP 请求报文在上送 CPU 时有 CPCAR 机制进行限速，如果攻击者发送大量伪 ARP 请求，与合法用户的 ARP 请求报文共享 CPCAR 限制的带宽，就会导致合法的 ARP 请求报文被丢弃，从而导致用户流量中断。

详细处理流程如图 9-7 所示。

图 9-7 ARP 报文攻击导致用户流量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 执行命令 **display arp all** 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（超过 70%），可能是 ARP 攻击报文被丢弃。请执行步骤 5。

步骤 4 执行命令 **car** 适当放大针对 ARP Request 报文的 CPCAR 的限制值。

car 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 AC6605 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 AC6605 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 AC6605 系统视图下执行命令 **arp speed-limit source-ip** [*ip-address*] **maximum** *maximum* 或者 **arp speed-limit source-mac** [*mac-address*] **maximum** *maximum*，配置 ARP 报文源抑制速率。

ARP 报文按源 IP 地址抑制功能和 ARP 报文按源 MAC 地址抑制功能不使能，即不进行 ARP 报文源抑制。

步骤 7 执行命令 **display arp anti-attack configuration log-trap-timer** 查看是否配置了写 ARP 日志和告警功能。

缺省情况下，ARP 的日志记录是关闭的。可以在系统视图下使用命令 **arp anti-attack log-trap-timer** *timer* 打开 ARP 日志告警功能。这样再有针对 ARP 的攻击时，系统可以写日志并发送告警信息。

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

- 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
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.7
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.11

相关日志

无

9.2.4 IP 地址扫描攻击的定位思路

介绍 IP 地址扫描攻击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：

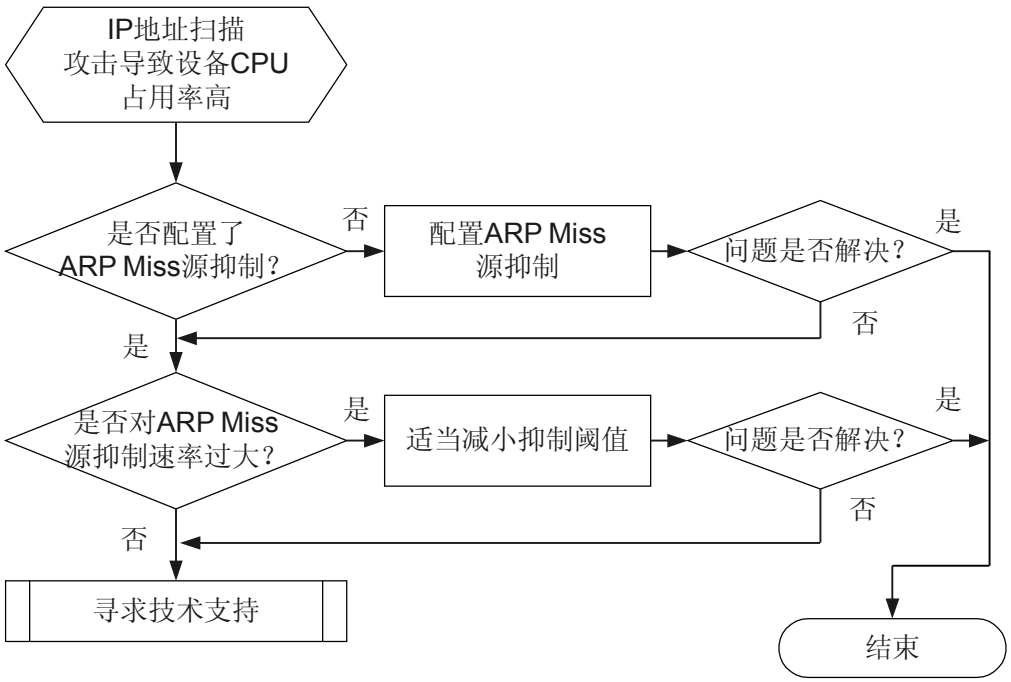
- 攻击者发送大量目的不可达报文，报文上送到 AC6605 的 CPU，触发 ARP Miss 消息，同时向网络上发送 ARP 请求进行 ARP 学习，消耗 CPU 资源。

故障诊断流程

AC6605 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 9-8 所示。

图 9-8 IP 地址扫描攻击故障诊断流程图



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 AC6605 上执行命令 **display cpu-usage**，查看主用主控板的 CPU 占用率信息。

名为 **ARQ** 的任务指的是 ARP 报文处理任务。

步骤 2 执行命令 **display arp all** 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。

```
<Quidway> display arp all
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE    VPN-INSTANCE
                                          VLAN
------------------------------------------------------------------------------
10.10.10.12     0018-82d2-0e08            I -         Vlanif200
10.10.10.13     Incomplete      0         D-0         Vlanif200
                                          3004/-
10.10.10.14     Incomplete      0         D-0         Vlanif200
                                          3004/-
20.20.20.33     000c-76bd-43d6            I -         Vlanif300
20.20.20.55     0013-7227-842f  17        D-0         Vlanif300
...                                       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 **ARQ** 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 AC6605 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 AC6605 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 500pps，即每秒 500 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** [*ip-address*] **maximum** *maximum* 命令修改速率限制值。

步骤 5 在 AC6605 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。

- 如果全局、VLAN 或接口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、VLAN 视图或接口视图下执行命令 **arp-miss anti-attack rate-limit** *packet-number* [**interval-value**]命令修改 ARP Miss 消息的限速时间和限速值。

步骤 6 执行命令 **display arp anti-attack configuration log-trap-timer** 查看是否配置了写 ARP 日志和告警功能。

缺省情况下，ARP 的日志记录是关闭的。可以在系统视图下使用命令 **arp anti-attack log-trap-timer** *timer* 打开 ARP 日志告警功能。这样再有针对 ARP 的攻击时，系统可以写日志并发送告警信息。

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

相关告警

- 1.3.6.1.4.1.2011.5.25.165.2.2.2.8
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.9
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.10
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.12

相关日志

无

9.2.5 ARP 学习失败的定位思路

介绍交换机 ARP 学习失败的故障处理流程和详细的故障处理步骤。

常见原因

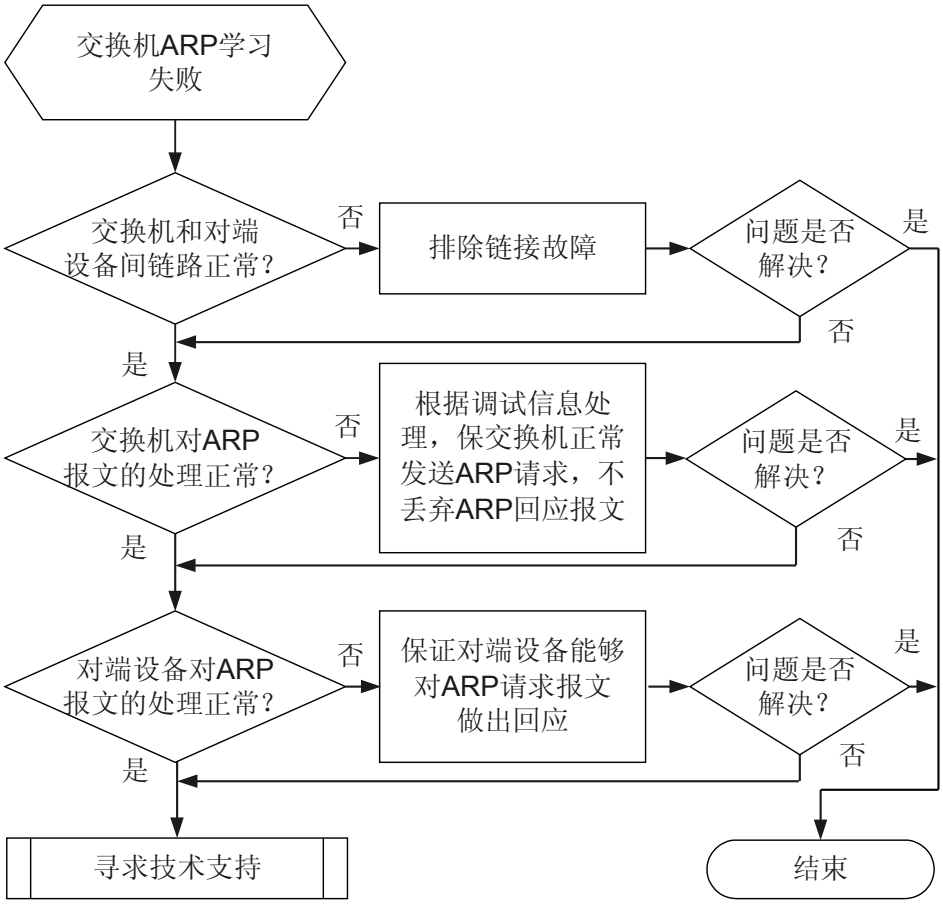
ARP 学习失败，有以下几种可能（假设 AC6605 发送 ARP 请求）：

可能情况	可能原因
ARP 请求报文没有发出去	AC6605 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 CAR 机制丢掉
对方的响应报文没有达到 AC6605	传输链路问题
对方的响应报文到达 AC6605 但是没有送到 CPU	被 AC6605 的 CPCAR 机制或 ARP 限速丢弃
对方响应报文到达 AC6605 的 CPU，但是被丢弃了	AC6605 的 ARP 处理模块出错

故障诊断流程

详细处理流程如图 9-9 所示。

图 9-9 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 AC6605 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 AC6605 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 **9.2.4 IP 地址扫描攻击的定位思路**进行处理。
- 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

- 系统视图、VLAN 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

9.3 NAC 故障处理

介绍了 NAC（Network Access Control）常见故障的定位思路。

9.3.1 802.1x 认证失败的定位思路

介绍 802.1x 认证失败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：

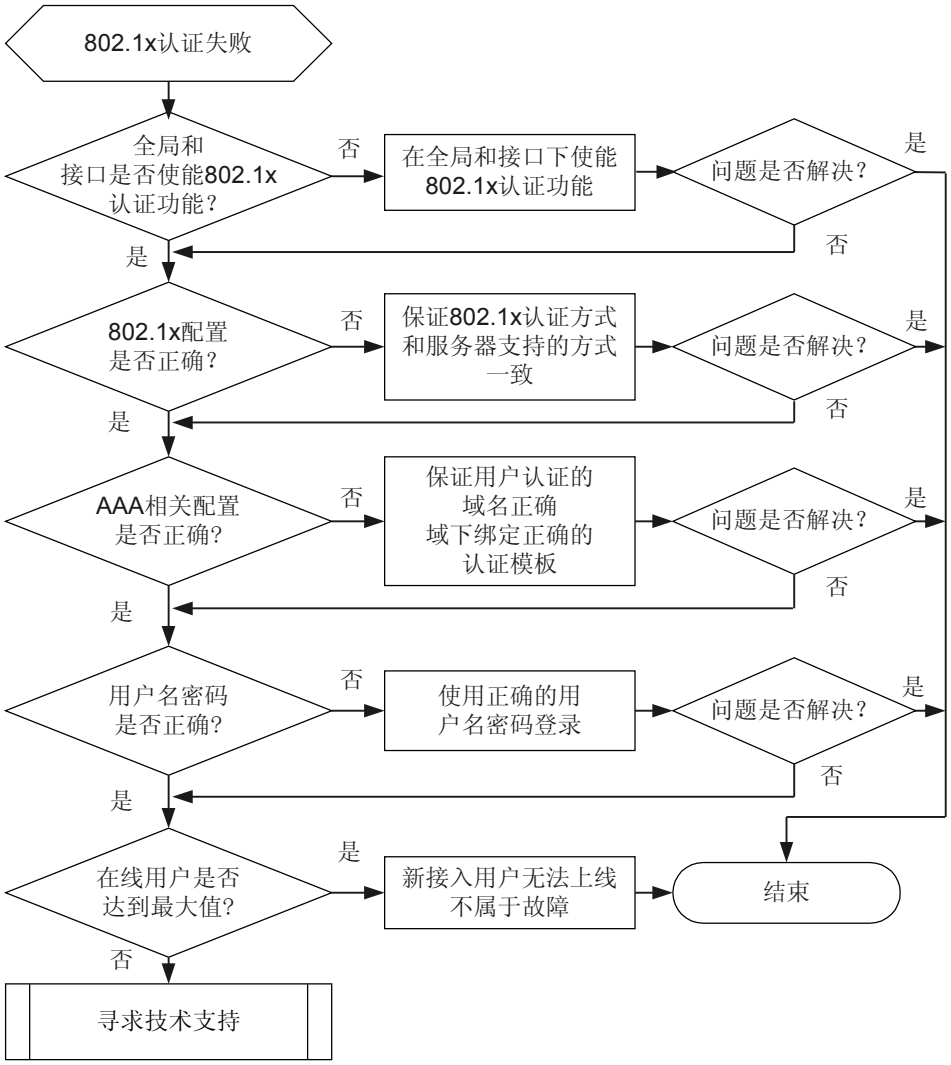
- 配置遗漏或配置错误（包括 802.1x 的配置，以及 AAA 方面的域、认证服务器、认证模板等配置）
- 用户登录的用户名和密码不正确
- 上线的用户数已达到最大数量

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 9-10 所示。

图 9-10 802.1x 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。

操作步骤

步骤 1 检查 AC6605 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。

AC6605 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。

- AC6605 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 AC6605 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 AC6605 上 RADIUS 故障或 HWTACACS 故障的处理方法，请参见 **9.1.1 RADIUS 用户认证失败的定位思路**和 **9.1.2 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。

- 如果认证服务器的用户属性包括 VLAN 授权信息，而 VLAN 在 AC6605 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 AC6605 上未创建，或 ACL 格式与 AC6605 的要求不一致，会导致 ACL 授权失败，用户授权不成功。需要在 AC6605 上创建相应的 ACL。或者保证服务器下发的 ACL 格式符合 AC6605 对 ACL 授权格式的要求。

  说明

  AC6605 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**

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

  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。

如果 AC6605 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 AC6605 上的 RADIUS 配置，保证配置正确。检查内容可以参考 **RADIUS 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 AC6605 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，AC6605 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。
- 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

9.3.2 MAC 地址认证失败的定位思路

介绍 MAC 地址认证失败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：

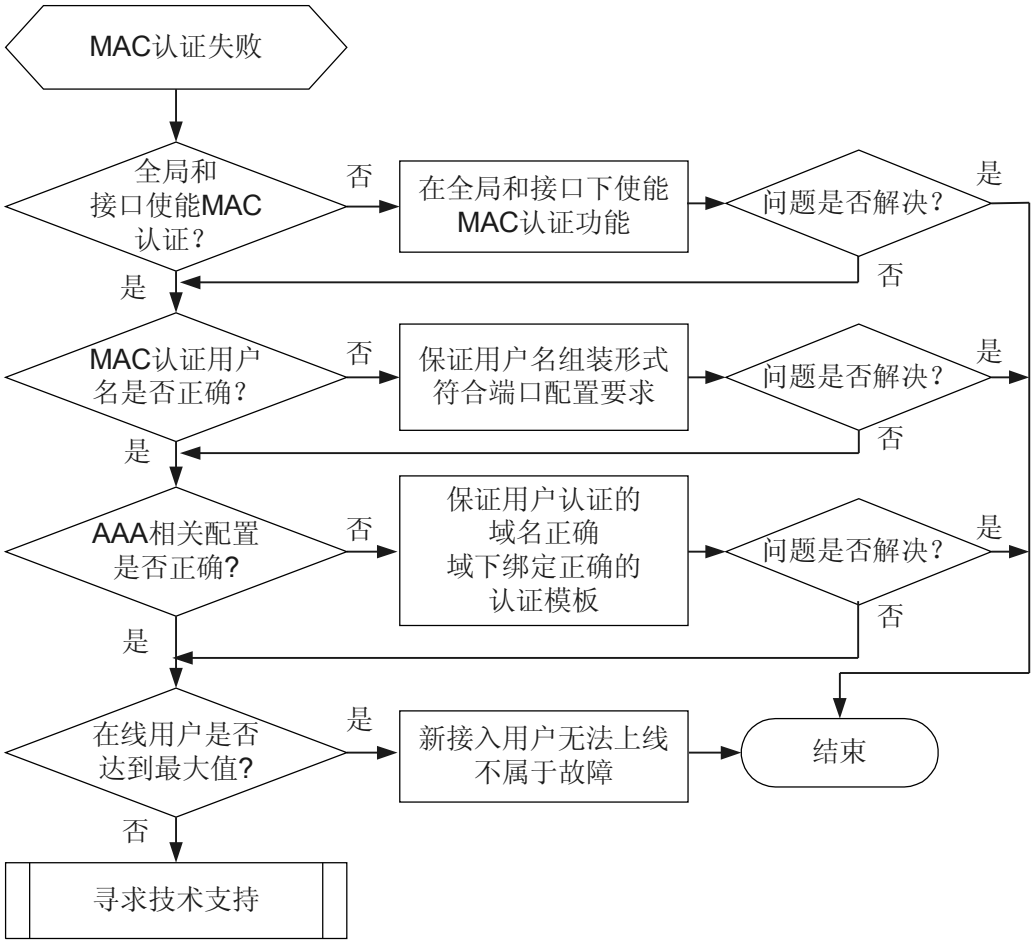
- 配置遗漏或配置错误（包括 MAC 认证的配置，以及 AAA 方面的域、认证服务器、认证模板等配置）
- 上线的用户数已达到最大数量

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 9-11 所示。

图 9-11 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 AC6605 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 AC6605 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。

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，AC6605 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。

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 AC6605 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 AC6605 上 RADIUS 故障或 HWTACACS 故障的处理方法，请参见 **9.1.1 RADIUS 用户认证失败的定位思路**和 **9.1.2 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 AC6605 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 AC6605 上未创建，或 ACL 格式与 AC6605 的要求不一致，会导致 ACL 授权失败，用户授权不成功。需要在 AC6605 上创建相应的 ACL。或者保证服务器下发的 ACL 格式符合 AC6605 对 ACL 授权格式的要求。

说明

AC6605 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**

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

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。

如果 AC6605 和认证服务器上的配置都正确，请执行步骤 5。

步骤 5 在 AC6605 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，AC6605 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

9.3.3 MAC 旁路认证失败的定位思路

介绍 MAC 旁路认证失败的故障处理流程和详细的故障处理步骤。

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 AC6605 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。

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 **9.3.2 MAC 地址认证失败的定位思路**。

9.3.4 Web 认证失败的定位思路

介绍 Web 认证失败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：

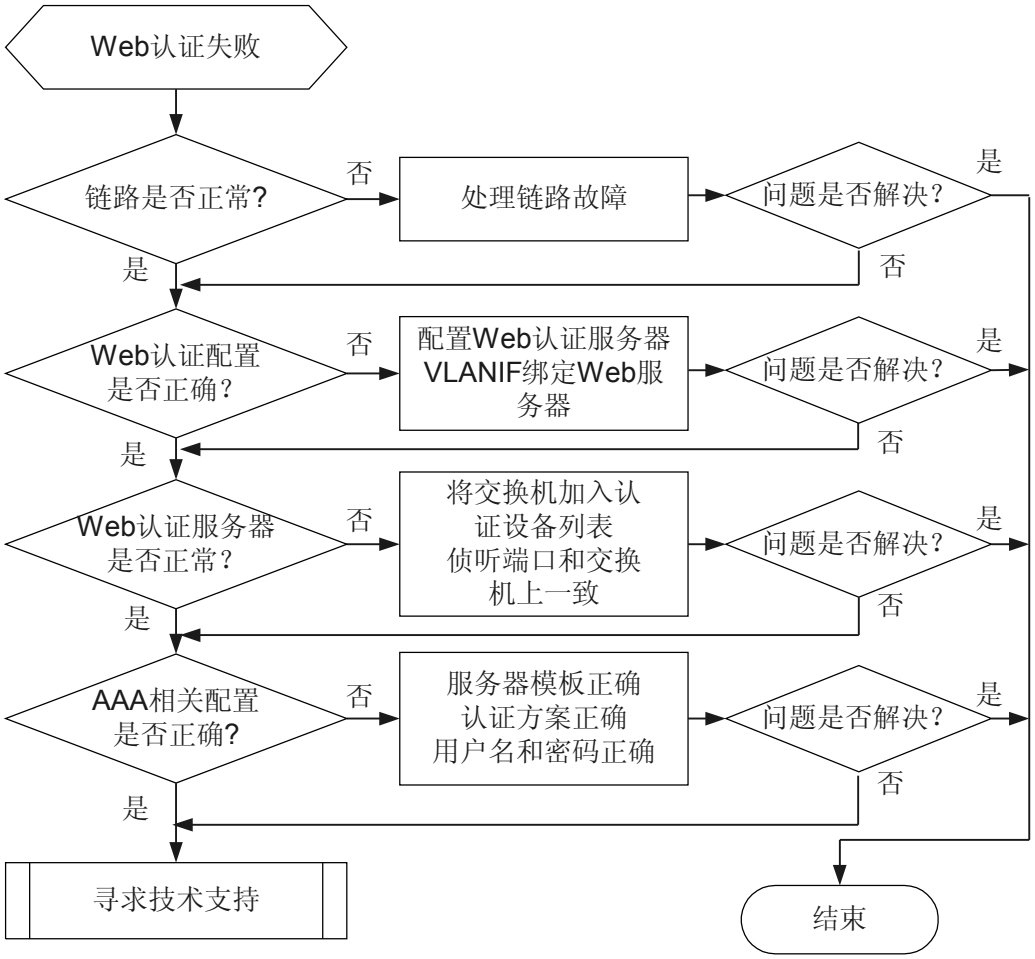
- 配置遗漏或配置错误（包括 Web 认证的配置，以及 AAA 方面的域、认证服务器、认证模板等配置）
- Web 认证服务器不可达或不可用
- 用户登录的用户名和密码不正确

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 9-12** 所示。

图 9-12 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 AC6605 和 Web 认证服务器之间、AC6605 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 **7.2.1 PING 不通故障处理思路**排除链路的故障。
- 如果能 ping 通，请执行步骤 2。

步骤 2 检查 AC6605 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。

  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 AC6605 加入了认证设备列表。
- 查看 Web 认证服务器和 AC6605 交互 Portal 报文的端口号，是否与 AC6605 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 AC6605 的 IP 地址组中。

保证 Web 认证服务器将 AC6605 加入了认证设备列表，侦听端口和 AC6605 的配置一致，且用户的 IP 地址在 AC6605 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 AC6605 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 AC6605 上 RADIUS 故障或 HWTACACS 故障的处理方法，请参见 **9.1.1 RADIUS 用户认证失败的定位思路**和 **9.1.2 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

相关日志

无

9.4 DHCP Snooping 故障处理

介绍了 DHCP Snooping 常见故障的定位思路和案例。

9.4.1 DHCP Snooping 导致用户无法上线的定位思路

介绍 DHCP Snooping 导致用户无法上线的故障处理流程和详细的故障处理步骤。

常见原因

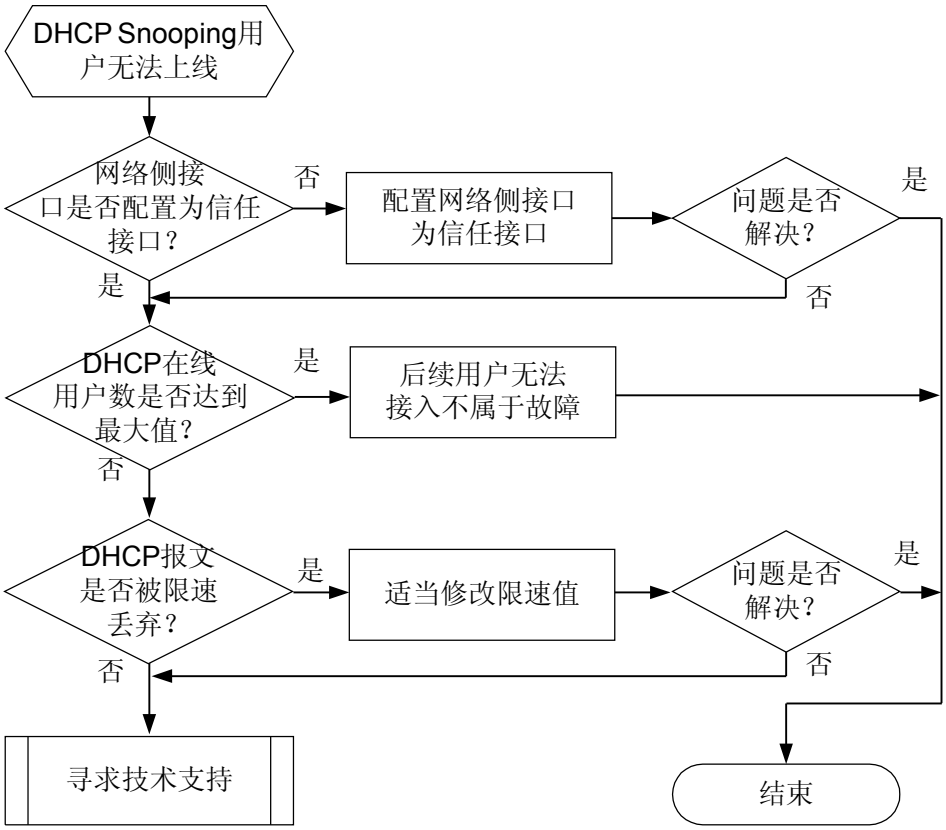
本类故障的常见原因主要包括：

- 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 9-13 所示。

图 9-13 配置 DHCP Snooping 后用户无法上线故障诊断流程图



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。

说明

“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：AC6605 只处理信任接口收到的 DHCP Reply 报文，不信任接口收到 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”。如果网络侧接口不是信任接口，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。
- 在系统视图下执行命令 **display this** 查看是否有“dhcp snooping global 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；如果三个视图下都配置了该参数，系统会取三者中的最小值来限制。

执行命令 **display dhcp snooping user-bind all** 查看当前 AC6605 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 snooping check dhcp-rate xx”信息，表示使用缺省的限速值 100。

DHCP Snooping 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 snooping 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。

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

9.4.2 故障案例

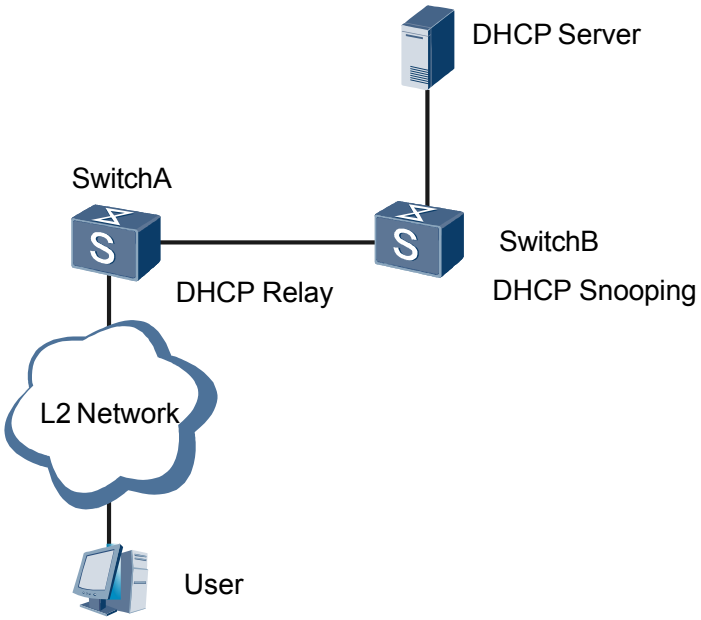
介绍 DHCP Snooping 的实际故障处理案例。

开启 DHCP Snooping 导致用户无法申请 IP 地址

网络环境

如图 9-14 所示，SwitchA 启用了 DHCP Relay 功能，SwitchB 为其他厂商设备，在 SwitchB 上配置了 DHCP Snooping 功能。用户无法正常申请到 IP 地址。

图 9-14 开启 DHCP Snooping 导致用户无法申请 IP 地址组网图



故障分析

1. 检查 SwitchA 和 SwitchB 的 DHCP 配置是否正确。发现配置正常。怀疑是 DHCP 报文被丢弃。
2. 查看 SwitchB 对 DHCP Discover 报文的处理是否正常。

   通过抓取 SwitchB 的报文并分析，发现 DHCP Discover 报文还没有入 DHCP Snooping 队列就被丢弃了。丢弃的报文特征是：源端口号和目的端口号都是 67。
3. 分析组网，发现 DHCP Snooping 的设备（SwitchB）部署在 DHCP Relay 和 DHCP Server 之间，DHCP Relay 发送的 DHCP Discover 报文的源和目的端口号正好都是 67。
4. 经确认，SwitchB 对该类型报文判断为非法，直接丢弃了。

操作步骤

步骤 1 联系 SwitchB 厂商，在 SwitchB 上增加源和目的端口号都为 67 的 DHCP 报文的合法性。此问题得以解决。

----结束

案例总结

常见 DHCP 组网是 PC---Relay---Server，DHCP Snooping 一般应用在 Relay 设备上或是 Relay 和 Client 之间。如果应用在不同的场景，要注意 Snooping 机制对 DHCP 报文的处理方式是否会对报文转发造成影响。

9.5 流量抑制故障处理

介绍流量抑制常见故障的定位思路。

9.5.1 广播流量抑制无效的定位思路

介绍广播流量抑制无效的常见原因、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：

- 接口下没有配置广播流量抑制或者配置的广播流量抑制值过大。
- 广播风暴报文在入接口没有丢弃。

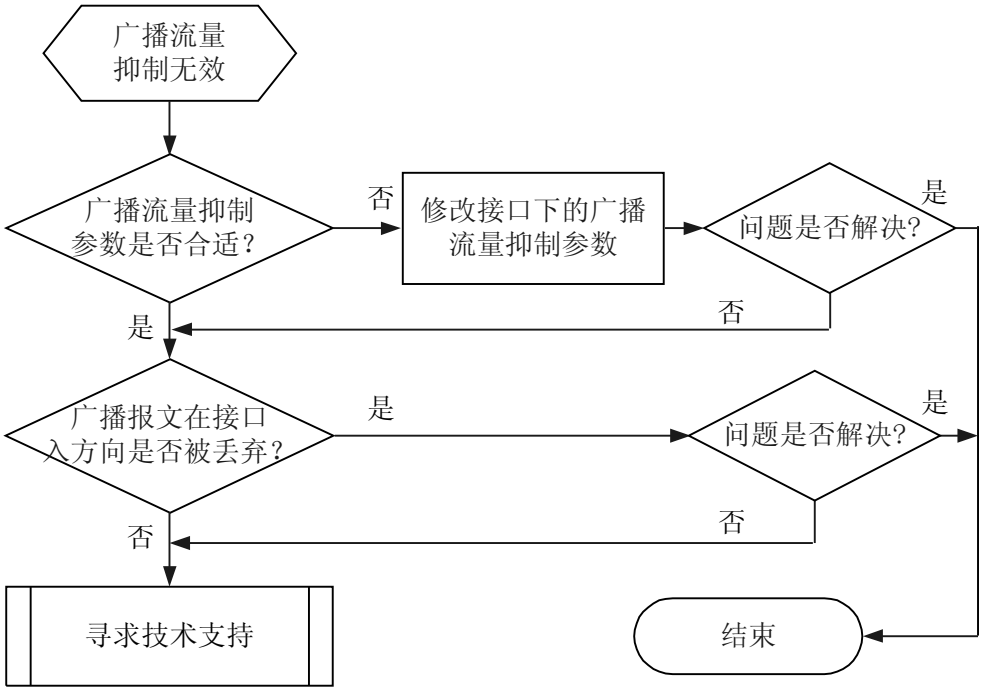
故障诊断流程

当端口出现广播风暴，正常流量中断，而端口配置的广播流量抑制功能无效时，可使用如图 9-15 所示流程进行处理。

说明

- 可使用命令 **display interface** *interface-type interface-number* 检查端口收发报文情况，如果入、出任何一方向的速率达到几百兆且几乎都是广播报文，则判断端口出现广播风暴。
- 网络中正常的广播报文并不多，一般只有 ARP 和 DHCP 报文。广播风暴一般是由网络成环所致，当网络存在物理环路时，我们必须使能环路保护协议比如 STP、RRPP 等来防止网络环路。当由于某些原因环路保护失效，网络出现环路时，如果没有广播风暴抑制网络很难恢复正常。对于广播风暴的问题，广播流量抑制只是事后补救措施，最根本的是要消除网络环路，对于环路保护的处理请参见 **MSTP 故障处理**和 **RRPP 故障处理**。

图 9-15 因广播风暴导致端口流量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。
- 本文以广播流量抑制故障处理为例，组播和未知单播流量抑制的故障处理步骤与此类似。

操作步骤

步骤 1 检查接口下的流量抑制配置

说明

流量抑制的功能是在接口的入方向对进入 AC6605 的流量进行控制。AC6605 连接用户侧和网络侧的接口都需要配置流量抑制。如果只在一侧接口（如网络侧接口）配置广播流量抑制，仅能控制从上游过来的广播流量。当下游的设备向所连接的 AC6605 发送大量广播报文时，假如这些连接接口上没有配置广播流量抑制，仍会发生广播风暴。

正常网络上广播流量不是很多，几百 Kbit/s 流量就可以满足正常广播报文所需，所以一般将广播流量抑制在几百 Kbit/s 内。包速率和比特速率的转换公式为：PPS = CIR*1000/(84*8)，其中 84 为平均报文长度，（包括 60 字节的报文和 20 字节的帧间隙以及 4 字节的 CRC），8 是每字节 bit 数。

用户视图下执行命令 **display flow-suppression interface** *interface-type interface-number*，查看输出信息中 **broadcast** 字段对应的 **rate mode** 和 **set rate value** 值，看其是否合适：

- 如果不合适，请在接口视图下执行命令 **broadcast-suppression** { *percent-value* | **packets** *packets-per-second* }修改广播流量抑制参数。
- 如果合适，执行步骤 2。

步骤 2 检查广播报文在接口入方向是否被丢弃

有两种方法：

- 用户视图下执行命令 **display interface** *interface-type interface-number*，查看输出信息中 **Input bandwidth utilization** 是否在抑制前后有较大变化。正常情况下，在配置流量抑制之后，接口丢弃超过阈值限制的报文，接口带宽利用率会降低。如果没有变化或变化很小，请执行步骤 3。
- 准备另外一个接口 B，将要检查的接口 A（即配置流量抑制的接口）和接口 B 加入相同 VLAN，查看接口 B 的出方向流量是否为接口 A 上配置的抑制后的流量。如果不是，说明报文没有在接口 A 的入方向被丢弃。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

相关告警和日志

相关告警

无

相关日志

无

9.6 CPU Defend 故障处理

介绍 CPU 防攻击常见故障的定位思路。

9.6.1 协议报文没有上送 CPU 的定位思路

介绍协议报文没有上送 CPU 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：

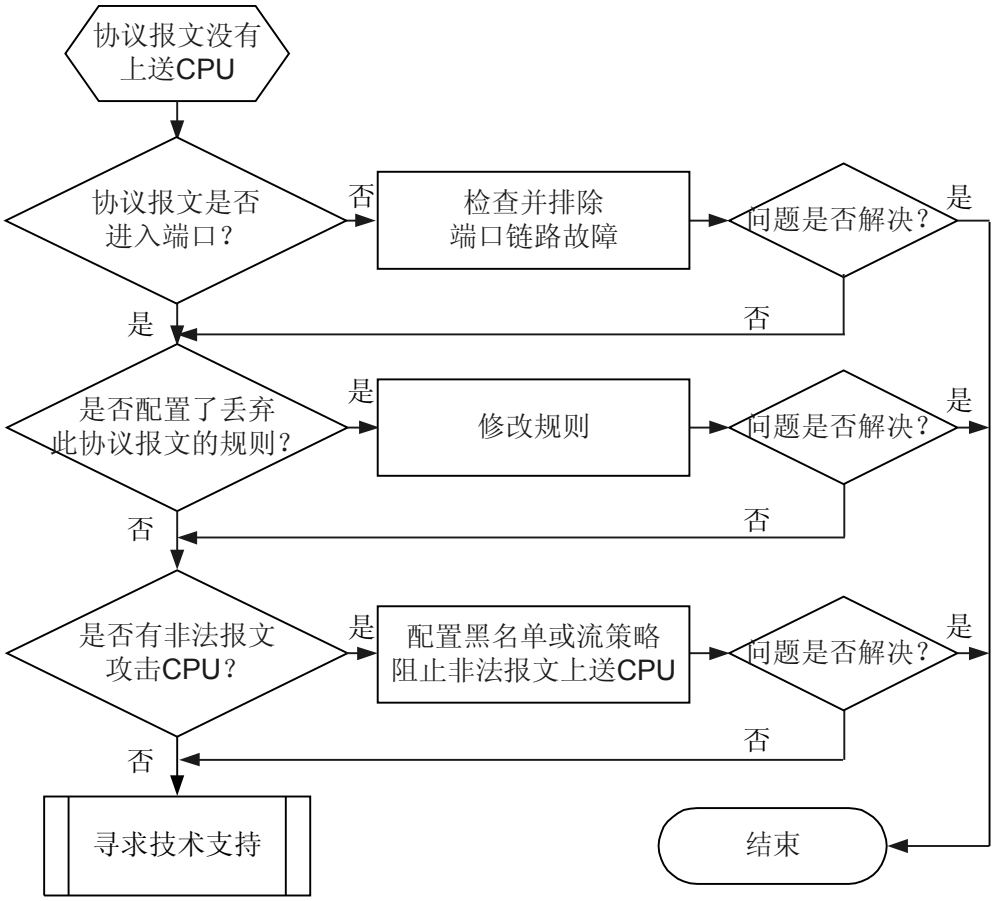
- 协议报文没有进入端口
- AC6605 上配置了匹配协议报文且动作为丢弃的规则（如黑名单、针对该类协议报文的上送规则为 deny）
- 非法报文攻击 CPU 导致协议报文无法上送

故障诊断流程

如果由于协议报文没有上送 CPU 导致某功能失效，请使用如**图 9-16** 所示流程进行处理。

通过执行命令 **display cpu-defend statistics** 查看该协议报文的 Pass 字段对应的统计计数来判断协议报文是否上送 CPU。

图 9-16 协议报文没有上送 CPU 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 检查协议报文是否进入端口

在对应端口抓包，查看协议报文是否进入端口：

- 如果报文没有进入端口，请执行命令 **display interface** *interface-type interface-number* 检查端口的物理状态是否 Up。
  - 如果端口物理状态 Down，请参见**以太网接口物理 DOWN 的定位思路**排除端口故障。
  - 如果端口物理状态 Up，请执行步骤 3。
- 如果报文已进入端口，请执行步骤 2。

步骤 2 检查 AC6605 上是否配置了匹配协议报文且动作为丢弃的规则

说明

AC6605 中，如下两种情况会导致协议报文被丢弃而无法上送 CPU:

- 配置了黑名单，且协议报文命中了黑名单中的 ACL。
- 配置的针对该协议报文的上送 CPU 的规则为 deny。

在系统视图执行命令 **display this**，查看配置的防攻击策略，然后执行命令 **display cpu-defend policy** 检查防攻击策略下是否配置了黑名单，或检查配置的针对此协议报文的上送 CPU 规则是否为 **deny**。

- 如果配置了黑名单，请执行命令 **display acl** 检查黑名单的规则是否匹配协议报文：
  - 如果匹配，请根据业务规划调整规则。
  - 如果不匹配，请执行步骤 3。
- 如果针对此协议报文的上送 CPU 规则为 deny，请执行命令 **car**，将上送规则修改为 CAR。
- 如果没有配置黑名单，针对此协议报文的上送 CPU 规则也不是 **deny**，请执行步骤 3。

步骤 3 检查上送 CPU 的统计信息

说明

如果某类协议报文过多（如存在非法报文攻击 CPU），会导致其他协议报文无法上送 CPU。

执行命令 **display cpu-defend statistics**，检查上送 CPU 的统计信息，看是否有大量协议报文被丢弃：

- 如果有大量协议报文被丢弃，则该协议报文可能为非法攻击报文，请分析报文是否为非法攻击报文（如通过攻击溯源功能），如果确定是非法攻击报文，请使用黑名单或者流策略阻止此协议报文上送 CPU。

  说明

  - 有关攻击溯源功能的配置请参考《AC6605 无线接入控制器 配置指南-安全》中的“配置攻击溯源”。
  - 有关黑名单的配置请参考《AC6605 无线接入控制器 配置指南-安全》中的“配置防攻击策略”。
  - 有关流策略的配置请参考《AC6605 无线接入控制器 配置指南-QoS》中的“配置基于复杂流分类的流策略”。
- 如果没有协议报文被丢弃，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

相关告警和日志

相关告警

无

相关日志

无

9.6.2 黑名单功能无效的定位思路

介绍黑名单功能无效的常见原因、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：

- 黑名单应用失败。
- 黑名单的规则与报文不匹配。

故障诊断流程

略

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 检查黑名单是否应用成功

执行命令 **display cpu-defend policy** *policy-name*，查看防攻击策略相关信息中黑名单是否应用成功。如：

```
<Quidway> display cpu-defend policy 1
 Related slot : <0>
 Configuration :
   Blacklist 1 ACL number : 2001
```

- “Related slot : <0>”表示防攻击策略已下发成功。
- “Blacklist 1 ACL number : 2001 ”表示策略中配置了黑名单。

步骤 2 检查黑名单的规则是否与报文匹配

从防攻击策略显示信息中查看到黑名单对应的 ACL，然后执行命令 **display acl** *acl-number*，检查 ACL 中的规则是否与业务需求一致：

- 如果不一致，请在对应 ACL 视图下执行命令 **rule**，修改规则，使之与业务需求一致。
- 如果一致，可能是设备 ACL 资源不足造成黑名单应用失败。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

相关告警和日志

相关告警

无

相关日志

无

9.6.3 攻击溯源功能无效的定位思路

介绍攻击溯源功能无效的常见原因、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：

- 配置攻击溯源的防攻击策略没有被应用。
- 攻击溯源的检测阈值过大，导致攻击溯源不认为该报文为攻击报文。

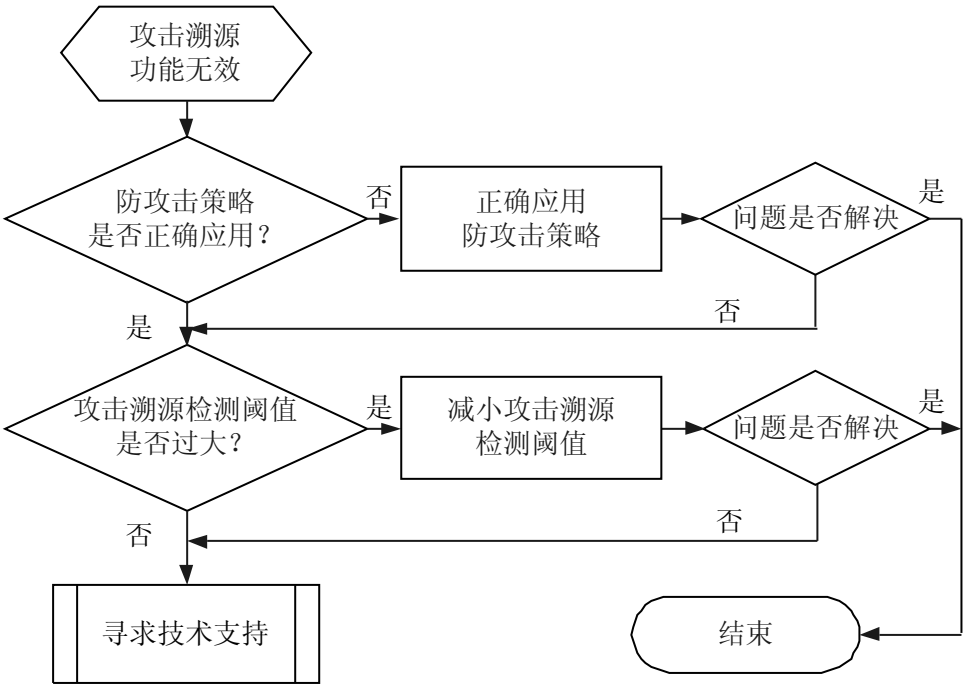
故障诊断流程

CPU 受到攻击时，如果配置了攻击溯源功能，但攻击溯源没有统计到攻击源，即使用命令 **display auto-defend attack-source** 没有看到相应的攻击源列表，请使用如图 9-17 所示流程进行处理。

说明

攻击溯源只能统计出下面的几种常见报文：ARP 报文、DHCP 报文、ICMP 报文、IGMP 报文、Telnet 报文、TCP 报文和 TTL-Expired 报文。

图 9-17 攻击溯源功能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 检查配置了攻击溯源的防攻击策略是否被正确应用

在系统视图下执行命令 **display this**，检查是否配置了 **cpu-defend-policy global** 命令。

或者执行命令 **display auto-defend configuration** 查看“Name”字段取值（防攻击策略名）和“Related Slot”取值（下发到哪个槽位）。

- 如果没有配置，在系统视图下执行命令 **cpu-defend-policy global** 进行配置。
- 如果已配置，请执行步骤 2。

步骤 2 检查攻击溯源检测阈值是否过大

说明

如果攻击溯源检测阈值设置过大，会导致攻击溯源不认为该报文为攻击报文，从而不进行攻击溯源统计。

在防攻击策略视图下执行命令 **auto-defend threshold** 减小攻击溯源的阈值，并执行命令 **auto-defend action** 配置对攻击源的报文做丢弃处理。

过段时间再执行命令 **display auto-defend attack-source** 查看是否有攻击源列表。如果仍然没有，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

相关告警和日志

相关告警

- 1.3.6.1.4.1.2011.5.25.165.2.2.1.1
- 1.3.6.1.4.1.2011.5.25.165.2.2.1.2

相关日志

无

9.7 MFF 故障处理

介绍 MFF 常见故障的定位思路。

9.7.1 配置 MFF 功能后用户不能上网的定位思路

介绍配置 MFF 功能后用户不能上网的故障诊断流程、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：

- 用户绑定表未生成
- 用户相关配置不正确（如用户接口未使能 DHCP Snooping、网络接口未配置为“信任”状态、网关 IP 与用户 IP 不在同一网段等）
- MFF 相关配置不正确（如用户接口未加入 MFF 的 VLAN、未配置网络接口等）
- AC6605 未收到网关的 ARP 应答报文（如 AC6605 到网关路由故障、链路繁忙）

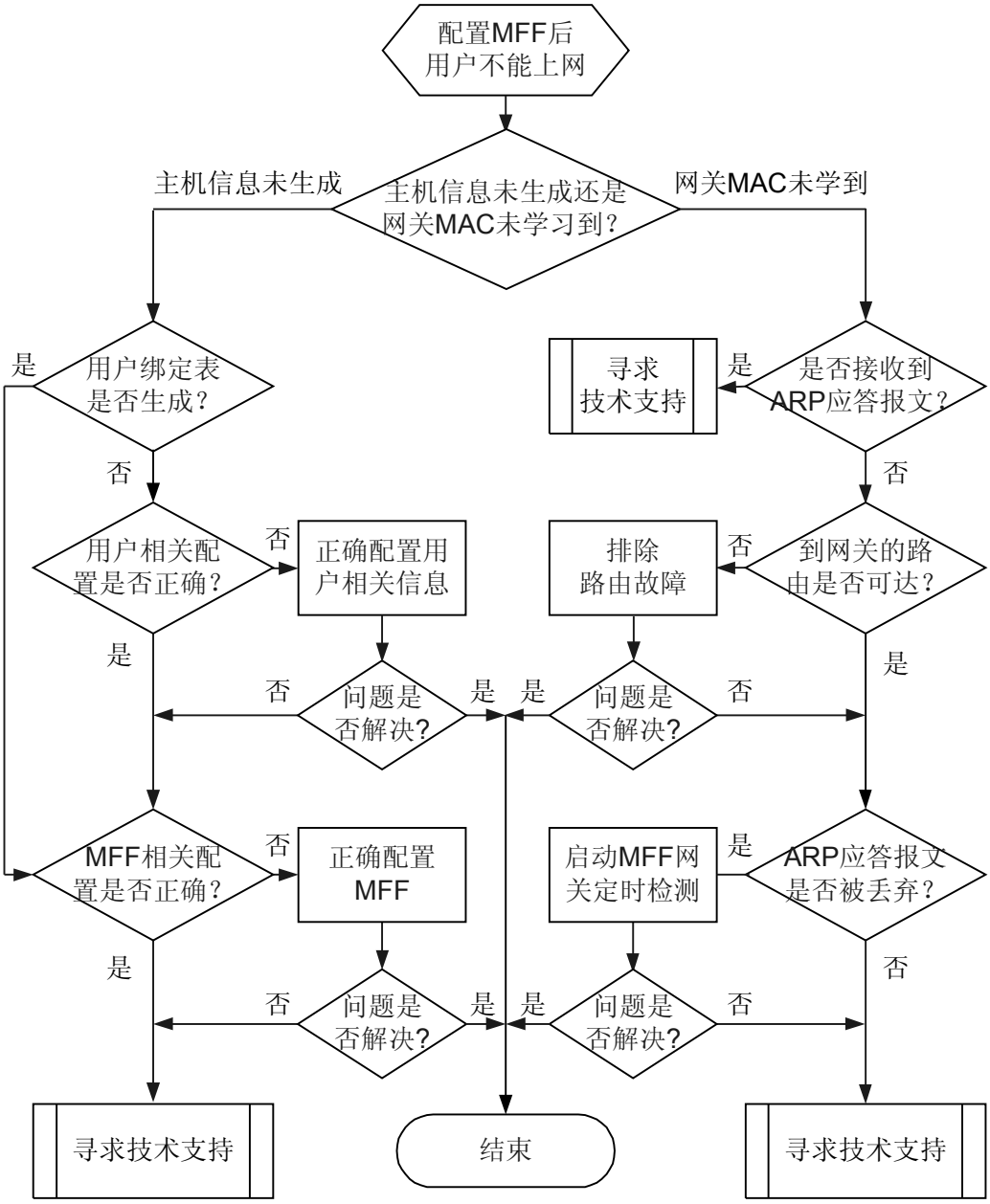
故障诊断流程

配置 MFF 功能后，如果发现用户不能访问网络，请采用如下定位思路：

- 检查 MFF 表项中主机信息是否生成、网关 MAC 是否学习到。
- 排查 MFF 主机信息未生成故障。
- 排查 MFF 未学习到网关 MAC 故障。

详细处理流程如图 9-18 所示。

图 9-18 配置 MFF 功能后用户不能上网故障诊断流程图



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 执行命令 **display mac-forced-forwarding vlan** *vlan-id*，检查 MFF 生成信息。

- 如果输出信息中 User IP 和 User MAC 字段的显示内容为空，表示主机信息未生成，请执行步骤 2。

- 如果输出信息中 Gateway MAC 字段的显示内容为空，表示没有学习到网关 MAC，请执行步骤 3。

步骤 2 MFF 主机信息未生成排查过程

1. 检查用户相关配置是否正确

用户类型	检查项	检查方法	输出处理
动态用户	用户接口是否使能 DHCP Snooping 功能	进入用户接口视图，执行命令 **display this**，检查是否有 **dhcp snooping enable** 命令。	如果没有，请在接口视图下执行命令 **dhcp snooping enable** 配置。此命令也可以在 VLAN 视图下执行，需保证用户接口加入到该 VLAN 中。
	网络接口是否为“信任”状态	进入网络接口视图，执行命令 **display this**，检查是否有 **dhcp snooping trusted** 命令。	如果没有，请在接口视图下执行命令 **dhcp snooping trusted** 配置。也可以在 VLAN 视图下执行命令 **dhcp snooping trusted interface** 配置。需保证接口已加入该 VLAN。
	用户是否成功上线	在确保用户接口使能 DHCP Snooping 功能、网络接口为“信任”状态后，执行命令 **display dhcp snooping user-bind vlan** *vlan-id*，查看 DHCP Snooping 表项。	如果不存在用户 IP 对应的 DHCP Snooping 表项，说明用户没有成功上线，请参考 **DHCP Snooping 导致用户无法上线的定位思路**解决用户不能成功上线问题。
静态用户	静态网关地址是否正确配置	进入配置 MFF 的 VLAN 视图，执行命令 **display this**，检查是否有 **mac-forced-forwarding static-gateway** *ip-address* 命令，并观察静态网关 IP 地址是否与静态用户 IP 地址属于同一网段。	如果没有或者静态用户 IP 地址与静态网关 IP 地址不在同一网段，请执行命令 **mac-forced-forwarding static-gateway** *ip-address* 配置与静态用户在同一网段的静态网关。

如果表中检查项均正确或者修改配置后问题仍然存在，请执行下一步。

2. 检查 MFF 相关配置是否正确
   - 进入用户接口视图，执行命令 **display this**，查看接口是否加入配置 MFF 的 VLAN。如果没有加入，请执行相应命令加入。
   - 进入网络接口视图，执行命令 **display this**，查看该接口上是否配置有 **mac-forced-forwarding network-port** 命令，如果没有，请执行该命令配置。

   如果用户接口和网络接口的 MFF 配置均正确，请执行步骤 4。

步骤 3 MFF 未学习到网关 MAC 排查过程

1. 检查 AC6605 是否接收到网关的 ARP 应答报文

   用户视图下执行命令 **debugging ethernet packet arp interface** *interface-type interface-number*，查看 AC6605 是否接收到来自网关的 ARP 应答报文：
   - 如果没有接收到 ARP 应答报文，静态用户请执行步骤 b，动态用户请执行步骤 c。
   - 如果接收到 ARP 应答报文，MFF 仍然没有学习到网关 MAC，请执行步骤 4。
2. 检查 AC6605 到网关设备的链路是否有问题

   从 AC6605 Ping 网关设备以检查路由是否可达：
   - 如果 Ping 不通，请先根据 **7.2.1 PING 不通故障处理思路**排除路由故障。
   - 如果能 Ping 通，请执行步骤 c。
3. 检查 ARP 应答报文是否被丢弃
   - 系统视图、VLAN 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“arp anti-attack rate-limit xxx”，配置的阈值过小，则有可能 ARP 应答报文被丢弃。使用命令 **arp anti-attack rate-limit** 可以修改速率抑制大小。
   - 进入配置 MFF 的 VLAN 视图，执行命令 **mac-forced-forwarding gateway-detect** 启动 MFF 网关定时探测功能，以重新发送 ARP 请求获取网关的 MAC 地址。

   如果仍然获取不到网关的 MAC 地址，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

相关告警和日志

相关告警

无

相关日志

无

9.8 ACL 故障处理

介绍 ACL 常见故障的定位思路和故障处理案例。

9.8.1 用户自定义 ACL 不生效的定位思路

介绍用户自定义 ACL 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

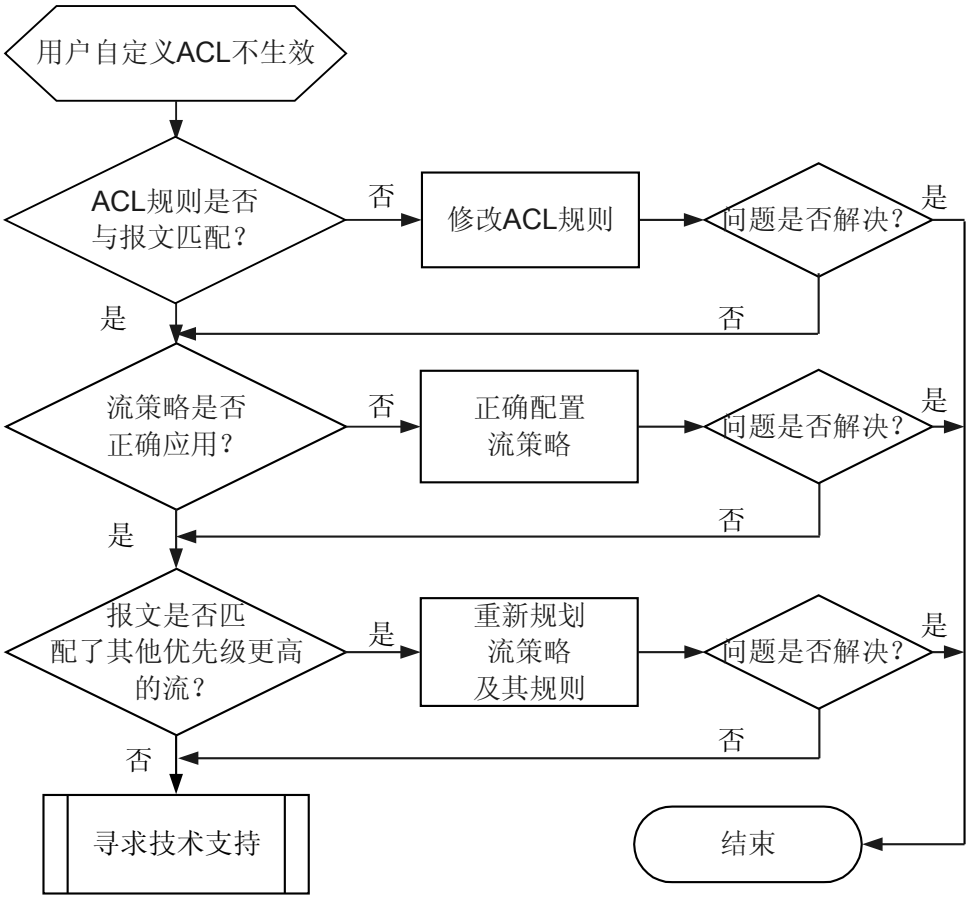
本类故障的常见原因主要包括：

- 报文与用户自定义 ACL 中的规则不匹配
- 用户自定义 ACL 所属流策略应用不正确（如应用对象与业务需求不符合、应用方向不正确）
- 报文匹配了其他优先级更高的流策略

故障诊断流程

如果发现用户自定义 ACL 不生效，请采用如图 9-19 所示流程进行处理。

图 9-19 用户自定义 ACL 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 检查报文是否与用户自定义 ACL 中的规则匹配

注意

系统是按 4 字节作为一个单元来匹配用户自定义 ACL 的，因此配置用户自定义 ACL 时，建议配置满 4 字节。如果配置时只指定两个字节，系统缺省将这两字节作为四字节的低两字节。

执行命令 **display acl**，查看用户自定义 ACL 中的规则，然后抓包查看报文，分析报文中的信息（如 IP 地址、MAC 地址、DSCP 值、VLAN ID、802.1p 值等）是否与用户自定义 ACL 中的规则匹配：

- 如果不匹配，执行命令 **rule** 修改用户自定义 ACL 中的规则，使之与报文中的信息匹配。
- 如果匹配，执行步骤 2。

步骤 2 检查用户自定义 ACL 所属流策略是否正确应用

1. 确定用户自定义 ACL 所属流策略

   执行命令 **display current-configuration**，查看设备当前配置文件，从中找取包含 **if-match acl** *acl-number* 命令的流分类，然后再找取绑定该流分类的流策略。

2. 检查流策略用户自定义 ACL 所属流策略是否正确应用

   执行命令 **display traffic-policy applied-record** 查看当前流策略的应用记录信息，关注流策略的应用对象（如 VLAN、接口）是否与业务需求一致，以及应用方向是否正确（应用用户自定义 ACL 时，AC6605 只支持对进入的报文实施策略，流策略应用方向为 **inbound**。）：

   - 如果流策略应用对象与业务需求不一致，请在正确位置上执行命令 **traffic-policy** 应用流策略。
   - 如果流策略应用方向不正确，则先执行命令 **undo traffic-policy** 取消应用，再执行命令 **traffic-policy** 重新将流策略应用在正确方向上。
   - 如果流策略应用对象与业务需求一致，且流策略应用方向正确，则执行步骤 3。

步骤 3 检查报文是否匹配了其他优先级更高的流策略

请参见“流策略不生效的定位思路”中“故障处理步骤”的步骤 2 进行处理。

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

相关告警和日志

相关告警

无

相关日志

无

9.8.2 故障处理案例

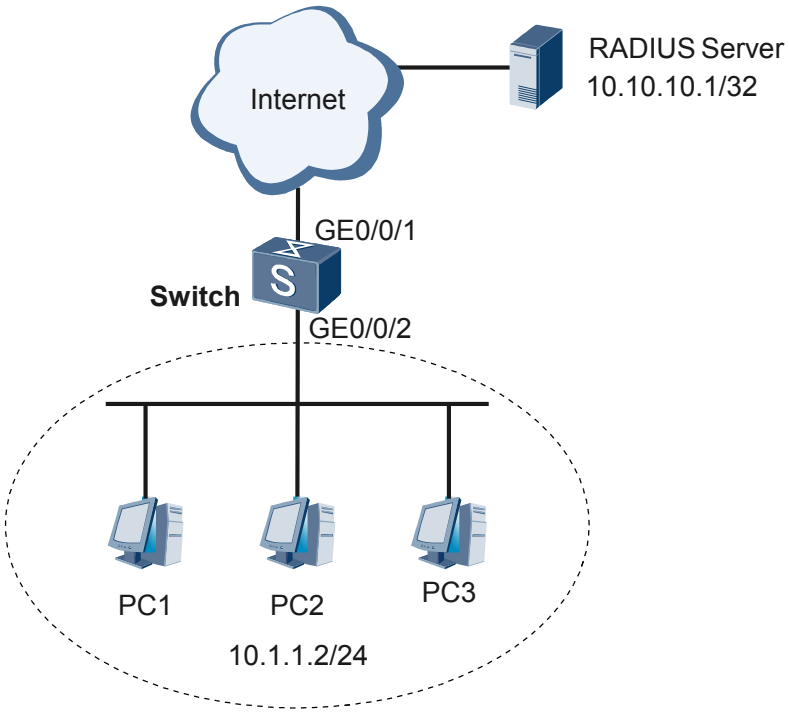
介绍用户自定义 ACL 相关的典型故障案例。

通过用户自定义 ACL 实现报文限速无效

网络环境

如图 9-20 所示组网中，PC 通过 PPPoE 拨号器从 GE0/0/1 上线，并到 RADIUS 服务器上进行认证，为避免用户报文过多而使 RADIUS 认证服务器瘫痪，在 Switch 上通过用户自定义 ACL 对用户发送的 UDP 报文进行限速，配置用户自定义 ACL 5000，配的是 rule 5 permit l2-head 0x0011 0x00ff 30，做的动作是限速 20M 和统计，策略名为 udf，发现没有进行限速，也没有统计到流量。

图 9-20 通过用户自定义 ACL 实现报文限速无效故障组网图



在 Switch 上进行如下配置：

```
<Quidway> system-view
[Quidway] acl 5000
```

```
[Quidway-acl-user-5000] rule permit l2-head 0x0011 0x00ff 30
[Quidway] traffic classifier udp
[Quidway-classifier-udp] if-match acl 5000
[Quidway-classifier-udp] quit
[Quidway] traffic behavior udp
[Quidway-behavior-udp] statistic  enable
[Quidway-behavior-udp] car cir 20000
[Quidway-behavior-udp] quit
[Quidway] traffic policy udp
[Quidway-trafficpolicy-udp] classifier udp behavior udp
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] traffic-policy udp inbound
```

配置完成后，通过测试仪模拟大量用户上线，并观察进入接口 GE0/0/2 的报文流量，发现速率仍然高于 20M，限速无效，执行命令 **display traffic policy statistics interface** *interface-type interface-number* **inbound**，显示如下信息：

```
[Quidway-GigabitEthernet0/0/2] display traffic policy statistics interface gigabitethernet0/0/2
inbound

 Interface: GigabitEthernet0/0/2
 Traffic policy inbound: udp
 Rule number: 1
 Current status: OK!
 Board : 3
Item                              Packets                    Bytes
-----------------------------------------------------------------------
Matched                                 0                        0
  +--Passed                             0                        0
  +--Dropped                            0                        0
    +--Filter                           0                        0
    +--URPF                             -                        -
    +--CAR                              0                        0
```

显示信息表明，流量统计也无效，说明报文没有匹配到配置有 ACL 5000 规则的流策略 udp。

故障分析

1. 检查报文是否与 ACL 规则匹配

   在 Switch 上执行命令 **display acl 5000**，显示信息如下：

   ```
   [Quidway] display acl 5000
   User ACL 5000, 1 rule
   Acl's step is 5
    rule 5 permit 0x00000011 0x000000ff 30
   ```

   在接口 GE0/0/2 上抓包，并分析 Switch 发往 RADIUS 服务器的报文格式，发现 UDP 协议为 0x11，距二层头目的 MAC 地址的偏移量为 30，0x11 应该对应规则高 16 位，而规则是低 16 位，导致报文不能匹配规则。

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 **acl 5000**，进入用户自定义 ACL 视图。

步骤 3 执行命令 **undo rule 5**，删除规则。

步骤 4 执行命令 **rule permit l2-head 0x00110000 0x00ff0000 30**，重新定义规则。

修改完成后，通过测试仪模拟大量用户上线，并观察进入接口 GE0/0/2 的报文流量，发现速率不再高于 20M，故障排除。

----结束

案例总结

AC6605 中，系统是将 4 字节作为一个单元来匹配用户自定义 ACL 的，因此配置用户自定义 ACL 时，建议配置满 4 字节。如果配置时只指定两个字节，系统缺省将这两字节作为四字节的低两字节。

9.9 PPPoE+故障处理

介绍 PPPoE+常见故障的定位思路。

9.9.1 PPPoE 用户无法上线的定位思路

介绍 PPPoE 用户无法上线的常见原因、故障诊断流程、故障处理步骤和相关告警与日志。

常见原因

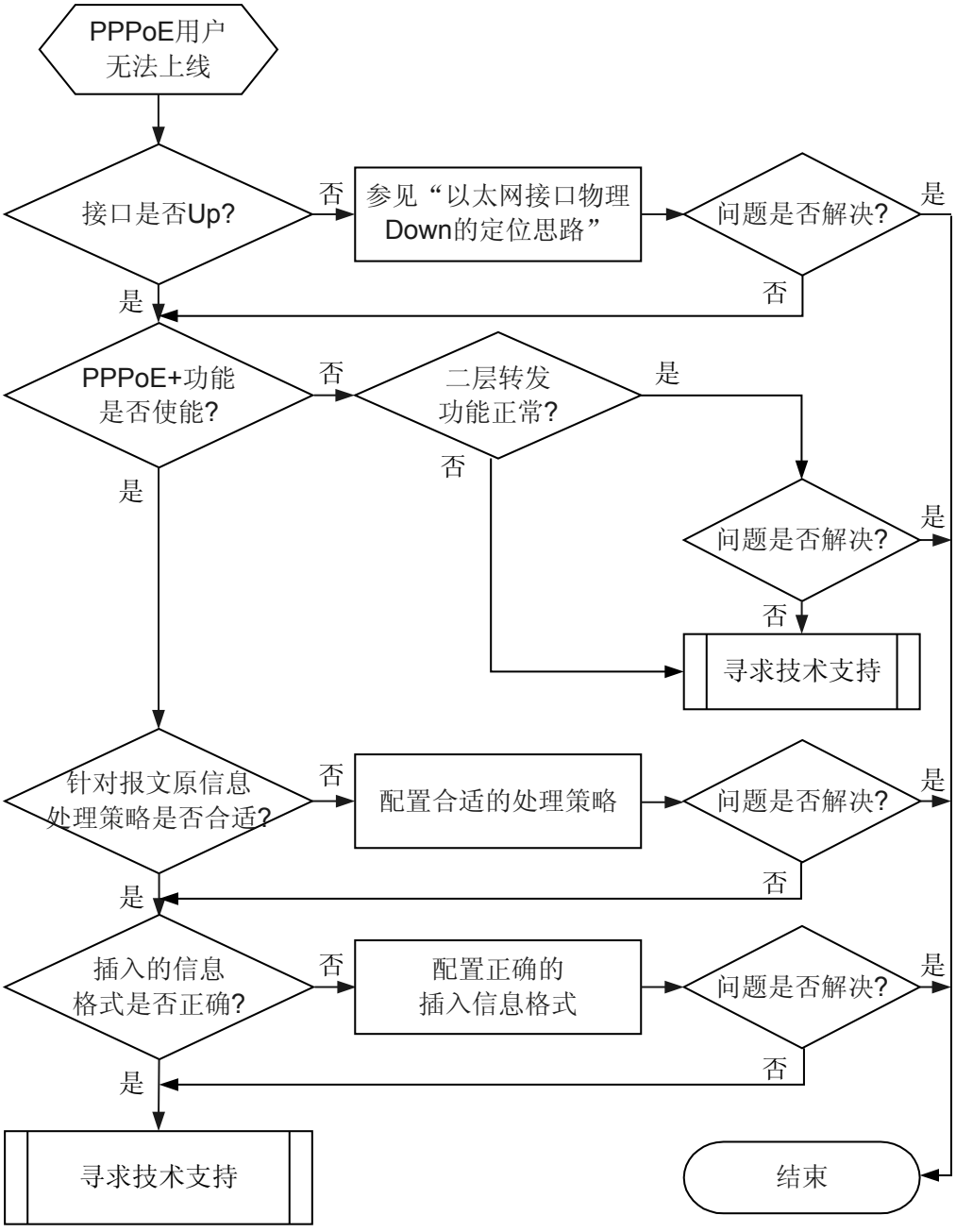
本类故障的常见原因主要包括：

- PPPoE 客户端与服务器之间的链路故障。
- PPPoE+配置不正确，如网络侧接口为非信任接口、针对 PPPoE 报文原信息的处理策略错误或插入的信息格式错误。

故障诊断流程

如果 PPPoE 用户无法上线，请采用如**图 9-21** 所示流程进行处理。

图 9-21 PPPoE 用户无法上线故障诊断流程图



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 检查用户与设备、设备与 PPPoE 服务器之间的接口是否 Up

- 如果接口物理 Down，请先根据**以太网接口物理 Down 的定位思路**排除故障。

- 如果接口物理 Up，请执行步骤 2。

步骤 2 检查是否使能了 PPPoE+功能

在系统视图执行命令 **display this**，检查是否配置了 **pppoe intermediate-agent information enable** 命令。如果没有配置此命令，则表示未使能 PPPoE+功能。

- 如果未使能 PPPoE+功能，AC6605 不处理 PPPoE 报文，对 PPPoE 报文直接进行二层转发。如果 PPPoE 报文没有从 AC6605 转发出去，或者二层转发正常，但 PPPoE 用户仍然无法上线，请执行步骤 4。
- 如果使能了 PPPoE+功能，请执行步骤 3。

步骤 3 检查 PPPoE+配置是否正确

1. 检查与 PPPoE 服务器连接的网络侧接口是否为信任接口

   如果网络侧接口不为信任接口，则系统丢弃 PPPoE 报文，从而使合法 PPPoE 用户无法上线。

   进入网络侧接口视图，执行命令 **display this**，检查接口上是否配置了 **pppoe uplink-port trusted** 命令：

   - 如果没有配置，网络侧接口为非信任接口，请执行命令 **pppoe uplink-port trusted** 配置。
   - 如果已经配置，网络侧接口为信任接口，请执行步骤 b。

2. 检查针对 PPPoE 报文中原有信息字段的处理动作是否合适

   在系统视图以及 PPPoE 用户侧接口视图下分别执行命令 **display this**，查看全局和接口上配置的 **pppoe intermediate-agent information policy** 命令。如果接口和全局均配置了针对 PPPoE 报文中原有信息字段的处理动作，以接口配置的动作为准。如果均没有配置，缺省采用 **replace** 动作。

   检查处理动作是否合适，即是否与业务需求符合：

   - 如果不合适，请执行命令 **pppoe intermediate-agent information policy** 配置合适的处理动作。
   - 如果合适，请执行步骤 c。

3. 检查插入的信息格式是否正确

   执行命令 **display pppoe intermediate-agent information format** 查看在 PPPoE 报文插入的信息格式是否正确，即是否与 PPPoE 服务器要求的格式一致：

   - 如果不正确，请执行命令 **pppoe intermediate-agent information format** 修改，使之与 PPPoE 服务器要求的格式一致。
   - 如果正确，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

相关告警和日志

相关告警

无

相关日志

无

9.10 URPF 故障处理

介绍了 URPF（Unicast Reverse Path Forward）常见故障案例。

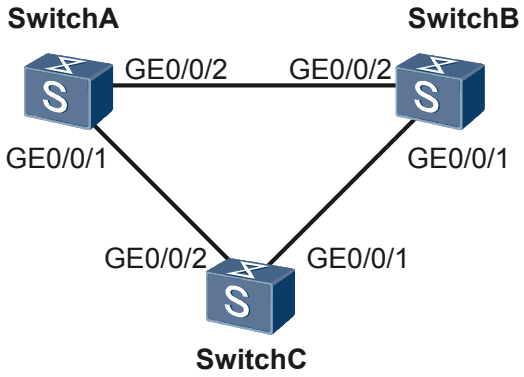
9.10.1 故障案例

互联接口时断时通

网络环境

在如图 9-22 所示的网络中部署 URPF，通过 OSPF 实现设备间互通。其中 SwitchA 和 SwitchB 之间 Cost 值是 800，SwitchC 与 SwitchA、SwitchB 之间 cost 值是 1000。

图 9-22 互联接口时断时通故障案例组网图



配置完成后，SwitchA Ping SwitchC 接口 GE0/0/1 的 IP 地址，发现时断时通。

故障分析

1. 在 SwitchC 上执行 **display ip routing-table** 命令，检查 OSPF 路由表项，发现 OSPF 路由表正常。
2. 结合 URPF 原理，分析 Ping 报文来回路径，SwitchA Ping SwitchC 接口 GE0/0/1 地址时，去方向报文路径中 A->B->C Cost 为 1800，A->C Cost 为 2000，优选前者。回包路径为 C->A 或 C->B->A COST 都为 1800，所以 2 条路径等值。
   - 当回包与发包路径一致时，URPF 检测通过，可以 ping 通。
   - 当回包与发包路径不一致时，URPF 检测不通过，丢弃报文，导致无法 ping 通。

说明

设备接收到报文，获取报文的目的地址，针对目的地址查找转发表，如果找到了就转发报文，否则丢弃该报文。而 URPF 通过获取报文的源地址和入接口，在转发表中查找以源地址为目的地址的表项，该表项对应的出接口是否与入接口匹配，如果不匹配，则认为源地址是非法的，直接丢弃该报文。通过这种方式，URPF 能够有效地防范网络中通过修改报文源 IP 地址而进行恶意攻击。

因此，该问题是由于互联接口配置 URPF，并且两条路径的 Cost 相同，检查接收的报文时，从一条路径接收的报文通过，而从另外一条路径接收的报文不通过，出现 Ping 测试时断时通。

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 **undo urpf**，删除接口上 URPF 的配置。

完成上述操作后，SwitchA Ping SwitchC 接口 GE0/0/1 的 IP 地址，可以正常 ping 通，故障排除。

----结束

案例总结

建议将 URPF 部署在网络接入侧或网络侧，互联端口不需部署 URPF。

10 QoS 类

关于本章

10.1 流策略故障处理
介绍流策略故障的定位思路和典型案例。

10.2 优先级映射故障处理
介绍优先级映射故障的定位思路和典型案例。

10.3 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。

10.4 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。

10.5 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。

10.6 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。

10.1 流策略故障处理

介绍流策略故障的定位思路和典型案例。

10.1.1 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

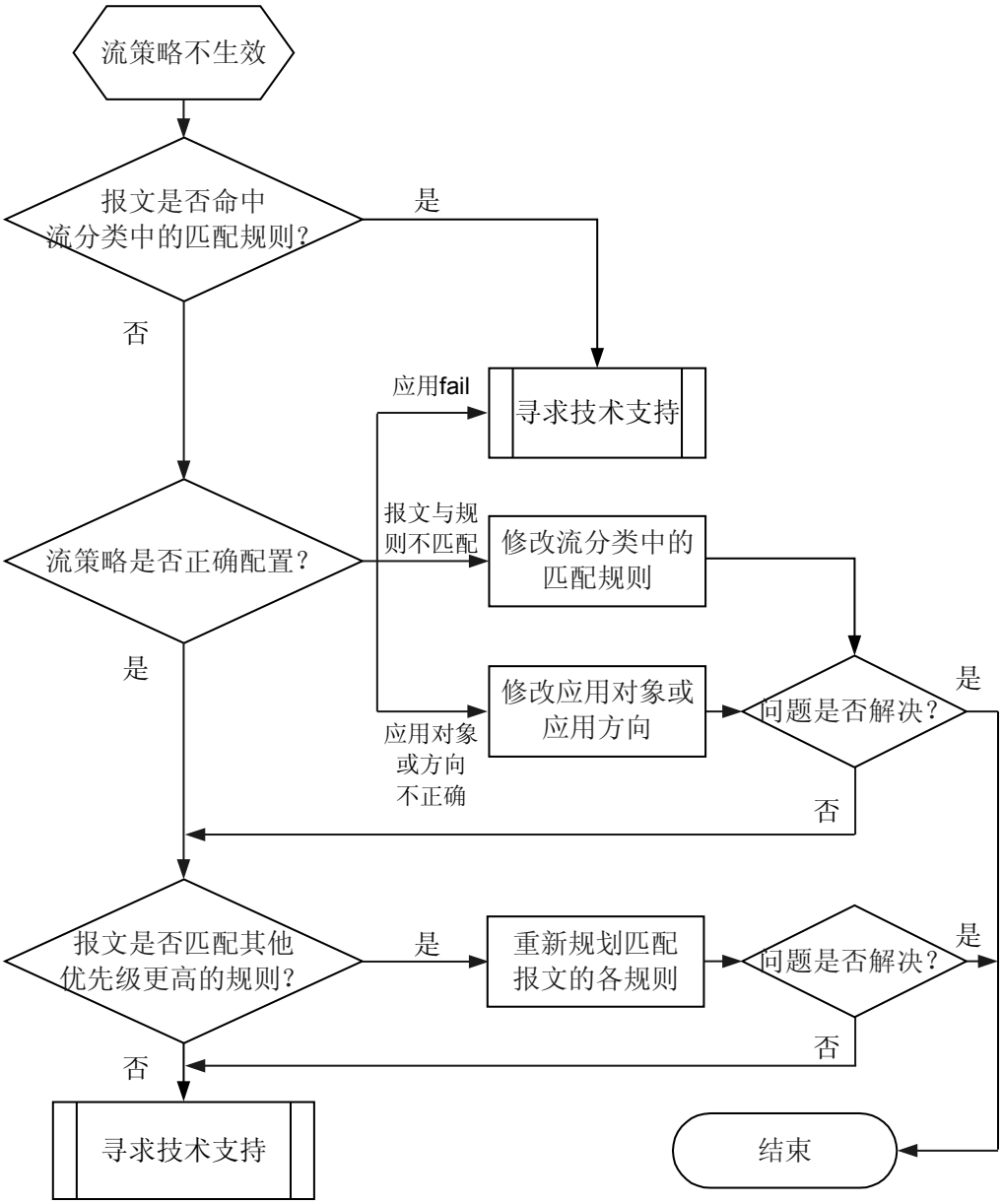
流策略不生效的常见原因包括：

- 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。
- 流策略应用不正确。
- 流策略同时应用在其他优先级更高的对象。流策略的应用对象中，端口、VLAN、全局的优先级逐次降低。
- 与已经应用的其他流策略冲突，且报文匹配了该流策略中的规则。

故障诊断流程

可按照图 10-1 排除流策略不生效故障。

图 10-1 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**，查看全局、接口或 VLAN 下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 2。

步骤 2 检查流策略是否正确配置

1. 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 b。

2. 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 c。

3. 检查流策略是否正确应用

   执行命令 **display traffic-policy applied-record** 查看当前流策略的应用记录信息，关注流策略应用是否 **success**、流策略的应用对象（如全局/槽位、接口、VLAN）是否与组网符合，以及应用方向是否正确（对进入 AC6605 的报文实施策略时，流策略应用方向应为 inbound；对从 AC6605 发出的报文实施策略时，应用方向应为 outbound）：

   - 如果流策略的应用对象或应用方向不正确，则执行命令 **traffic-policy** 重新将流策略正确应用。
   - 如果流策略应用 **fail**，请执行步骤 4。
   - 如果流策略应用正确，则执行步骤 3。

步骤 3 检查报文是否匹配了其他优先级更高的规则。

执行命令 **display current-configuration**，查看 AC6605 上配置的匹配规则，检查是否有其他规则匹配报文：

说明

对于 AC6605，还需关注流策略的匹配顺序。

- 如果没有匹配报文的其他规则，执行步骤 4。
- 如果存在匹配报文的其他规则，对于流策略中流分类的匹配顺序为 **auto** 的 AC6605，请根据如下步骤判断生效的规则。

  1. 首先分析规则所在流分类的类型。

     AC6605 支持 Layer 2、Layer 3、Layer 2 and Layer 3、UDF（User Defined Flow）四种流分类类型。不同类型流分类中的规则优先级由高到低依次为 UDF、Layer 2 and Layer 3、Layer 3、Layer 2。

     流分类类型的定义如下：

- Layer 2：流分类中仅有二层规则。
- Layer 3：流分类中仅有三层规则。
- Layer 2 and Layer 3：流分类中既有二层规则又有三层规则，且流分类间规则是逻辑“与”的关系。
- UDF：流分类中仅有用户自定义规则。

规则分类标准见**表 10-1** 所述。

表 10-1 规则分类表

规则类型	规则
二层	● **if-match acl 4000 ～ 4999** ● **if-match any** ● **if-match cvlan-8021p** ● **if-match cvlan-id** ● **if-match 8021p** ● **if-match vlan-id** ● **if-match destination-mac** ● **if-match source-mac** ● **if-match inbound-interface** ● **if-match outbound-interface** ● **if-match discard** ● **if-match double-tag** ● **if-match l2-protocol**
三层	● **if-match acl 2000 ～ 2999** ● **if-match acl 3000 ～ 3999** ● **if-match dscp** ● **if-match ip-precedence** ● **if-match protocol** ● **if-match tcp**
用户自定义	● **if-match acl 5000 ～ 5999**

2. 其次分析规则所属流策略的应用对象。

   AC6605 中，流策略可以应用在全局/槽位、接口和 VLAN。规则所在流分类类型相同时，流策略应用在不同对象时，规则优先级由高到低依次为接口、VLAN、全局/槽位。优先级高的生效。

如果匹配报文的其他规则的优先级高于当前规则，则其他规则对应的流动作生效，请重新规划匹配报文的规则，确保当前规则生效，又不影响其他业务。否则，执行步骤 4。

- 如果存在匹配报文的其他规则，对于流策略中流分类的匹配顺序为 **config** 的 AC6605，请根据如下步骤判断生效的规则：

1. 若此规则与当前规则不在同一个流策略，则比较流策略的应用对象，AC6605中，流策略应用在全局、接口和 VLAN 时，规则优先级由高到低依次为接口、VLAN、全局，优先级高的生效。
2. 若此规则与当前规则在同一个流策略，但不在同一个流分类，则比较流分类在流策略中显示的先后顺序，位置在前的生效。
3. 若此规则与当前规则在同一个流策略和流分类，且属于同一个 ACL，则比较规则在 ACL 中显示的先后顺序，位置在前的生效。

如果生效的是匹配报文的其他规则，则请重新规划匹配报文的规则，确保当前规则生效，又不影响其他业务。否则，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

相关告警和日志

相关告警

无

相关日志

无

10.1.2 故障处理案例

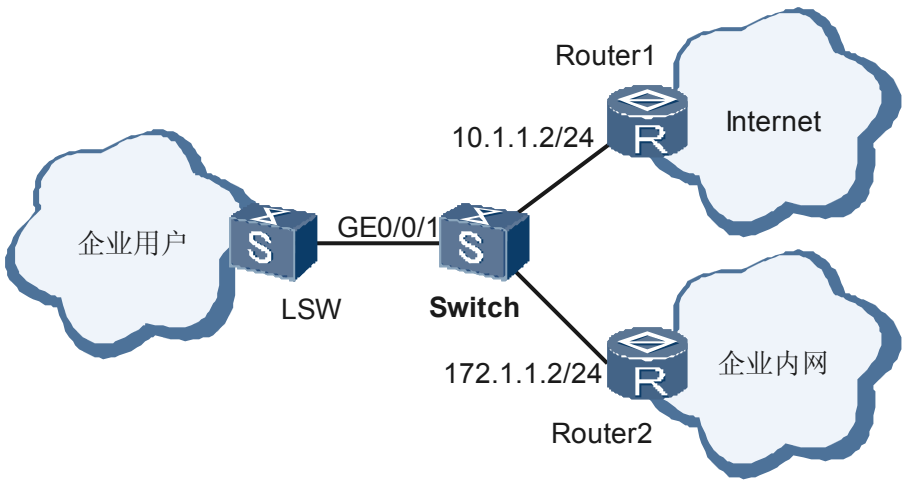
介绍流策略相关的典型故障案例。

基于流策略的策略路由不生效

网络环境

如图 10-2 所示组网中，在 Switch 上配置基于流策略的策略路由，使企业网内部用户访问 Web 业务时采用不同的下一跳 10.1.1.2/24，以便控制。

图 10-2 基于流策略的策略路由不生效组网图



配置完成后，企业网内部用户访问 Web 业务时，数据流没有被重定向到 10.1.1.2。

故障分析

1. 企业网内部用户访问 Web 业务时，在 Switch 的入接口 GE0/0/1 处抓包，发现能抓取到用户访问 Web 业务的报文。
2. 执行命令 **display ip routing-table** 查看路由表，发现有去往 10.1.1.2/24 的路由。
3. 检查数据流是否匹配了其它优先级更高的规则。
   a. 进入入接口 GE0/0/1 的视图，执行命令 **display this**

```
[Switch-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
 traffic-policy tp1 inbound
#
return
```

   b. 执行命令 **display traffic policy user-defined**，查看流策略配置信息。

```
[Switch] display traffic policy user-defined tp1
  User Defined Traffic Policy Information:
  Policy: tp1
   Classifier: tc1
     Operator: AND
     Behavior: tb1
      Deny
   Classifier: tc2
     Operator: AND
     Behavior: tb2
      Redirect:
        Redirect ip-nexthop 10.1.1.2
```

   c. 执行命令 **display current-configuration**，查看流策略中流分类的匹配顺序。

   流策略 tp1 中绑定两个流分类，因此需要检查流策略中流分类的匹配顺序。

```
<Quidway> display current-configuration
#
traffic policy tp1
 classifier tc1 behavior tb1
 classifier tc2 behavior tb2
```

   显式信息表明，流策略 tp1 中流分类的匹配顺序为 **auto**。

   说明

   auto 为缺省设置，配置文件中不显示。

   d. 执行命令 **display traffic classifier user-defined**，查看流分类 tc1 和 tc2 的配置，显示信息如下:

```
[Switch] display traffic classifier user-defined tc1
  User Defined Classifier Information:
   Classifier: tc1
    Operator: AND
    Rule(s) : if-match any
              if-match dscp 6
[Switch] display traffic classifier user-defined tc2
  User Defined Classifier Information:
   Classifier: tc2
    Operator: AND
    Rule(s) : if-match acl 3000
```

   e. 执行命令 **display acl 3000** 查看 ACL 3000 规则的内容。

```
[Switch] display acl 3000
Advanced ACL 3000, 1 rule
```

```
Acl's step is 5
 rule 5 permit tcp destination-port eq www
```

从以上显示信息可以看出，流策略中流分类的匹配顺序为 **auto**，流策略中绑定有两个流分类 tc1 和 tc2，tc1 的匹配规则为 **if-match any** 和 **if-match dscp 6**；tc2 的匹配规则是 **if-match acl 3000**，因此，流分类 tc1 属于 Layer 2 and Layer 3 类型，流分类 tc2 属于 Layer 3 型。AC6605 中，如果流策略中流分类的匹配顺序为 **auto**，Layer 2 and Layer 3 类型的流分类优先级高于 Layer 3 类型的流分类，因此，报文匹配 tc1，其对应动作为 **deny**，使企业内部用户访问 Web 的业务报文被丢弃，致使不能重定向到 10.1.1.2/24。

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 **traffic policy tp1**，进入流策略 tp1 视图。

步骤 3 执行命令 **undo traffic classifier tc1**，取消流分类 tc1 在流策略中的绑定。

完成上述操作后，企业网内部用户访问 Web 时，业务报文被重定向到 10.1.1.2，故障排除。

说明

此处的修复操作前提是流分类 tc1 在组网中没有应用。实际修复时应根据现网重新规划各规则优先级。

----结束

案例总结

基于流策略的策略路由不生效的可能原因包括：

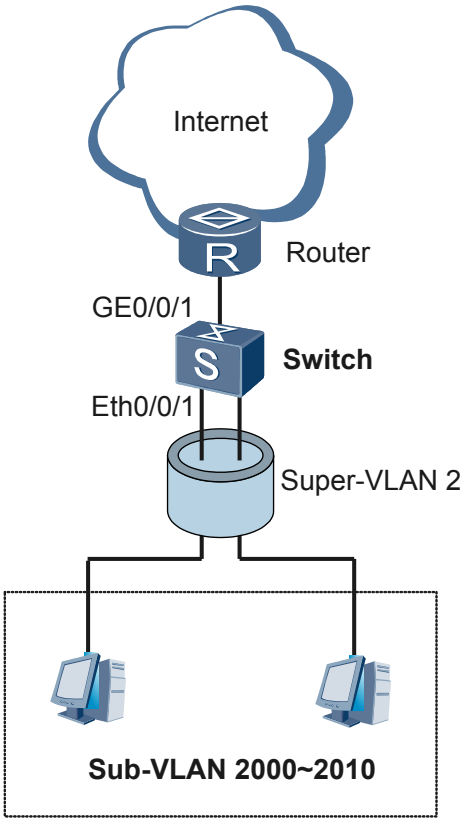
- 数据流与配置的规则不匹配。
- 路由表中没有下一跳路由。
- 数据流匹配了其它优先级更高的规则，规则优先级高低判断准则请参见 **10.1.1 流策略不生效的定位思路**中的**故障处理步骤**。

Super-VLAN 下应用流策略导致重标记报文功能不生效

网络环境

如**图 10-3** 所示的网络中，在 Switch 上配置重标记功能，将用户报文中的 DSCP 重标记为统一的优先级，以便上游 Router 对用户报文进行统一的 QoS 控制。

图 10-3 Super-VLAN 下应用流策略导致重标记报文功能不生效组网图



配置完成后，分别在 Switch 上报文的入接口 GE0/0/1 和出接口 GE0/0/1 接口抓包，发现出入接口上报文的 DSCP 值没有改变，重标记功能没有生效。

故障分析

1. 执行命令 **display current-configuration** 检查 Switch 的当前配置。

   命令显示结果如下：

```
<Switch> display current-configuration
traffic classifier temp operator and
 if-match any
traffic behavior temp
 statistic enable
 remark dscp af23
traffic policy temp
 classifier temp behavior temp
vlan 2
 traffic-policy temp inbound
 aggregate-vlan
 access-vlan 2000 to 2010

#
interface GigabitEthernet0/0/1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 2000 to 2010
#
interface GigabitEthernet0/0/1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 2000 to 2010
```

流策略为对任何流量的报文重标记 DSCP 为 AF23，流策略应用在 Super-VLAN 2 的入方向，且该设备上没有配置其他流策略，配置上没有问题。

2. 在 Switch 上使用 **display traffic policy statistics vlan 2** 命令，查看流策略是否匹配到。

   命令显示结果如下：

```
<Switch> display traffic policy statistics vlan 2 inbound verbose classifier-base
 Vlan: 2
 Traffic policy inbound: temp
 Rule number: 1
 Current status: OK!
-------------------------------------------------------------------------
 Classifier: temp operator and
 Behavior: temp
 Board : 0
Item                                Packets                         Bytes
-------------------------------------------------------------------------
Matched                                   0                             0
  +--Passed                               0                             0
  +--Dropped                              0                             0
    +--Filter                             0                             0
    +--URPF                               -                             -
    +--CAR                                0                             0
```

   结果显示，该 VLAN 下的流策略没有被匹配。

3. 分析入接口 GE0/0/1 上抓取的报文，发现用户报文中的 VLAN 为 2000，而流策略是应用在 Super-VLAN 2 上。

   当流策略应用在 Super-VLAN 下时，策略仅匹配带有 Super-VLAN 的 VLAN ID 的报文，因此对 Sub-VLAN 下的用户报文不生效。

操作步骤

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

步骤 2 执行命令 **vlan 2**，进入 VLAN 视图。

步骤 3 执行命令 **undo traffic-policy inbound**，取消流策略在 VLAN 2 上的应用。

步骤 4 执行命令 **quit**，退出 VLAN 视图。

步骤 5 执行命令 **traffic classifier temp**，进入流分类 temp 视图。

步骤 6 执行命令 **if-match vlan-id 2000 to 2010**，修改流分类的匹配规则为匹配所有 Sub-VLAN。

步骤 7 执行命令 **interface gigabitethernet0/0/1**，进入用户报文入接口视图。

步骤 8 执行命令 **traffic-policy temp inbound**，将流策略应用在入接口的入方向。

修改后，用户重新发送报文，在入接口 GE0/0/1 和出接口 GE0/0/1 上分别抓取报文，发现 DSCP 值已被重新标记为 AF23，问题解决。

说明

AC6605 支持动态修改流策略，因此，只需进行步骤 1、5、6 的操作即可。

----结束

案例总结

流策略应用在 Super-VLAN 下时，策略匹配的是 Super-VLAN 的 *vlan-id*，而不是该 Super-VLAN 中的 Sub-VLAN 的 VLAN ID。如果需要对 Super-VLAN 中的报文应用流策

略，则需要配置匹配所有 Sub-VLAN 的流策略，并将该流策略应用在 Sub-VLAN 对应的接口上。

10.2 优先级映射故障处理

介绍优先级映射故障的定位思路和典型案例。

10.2.1 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

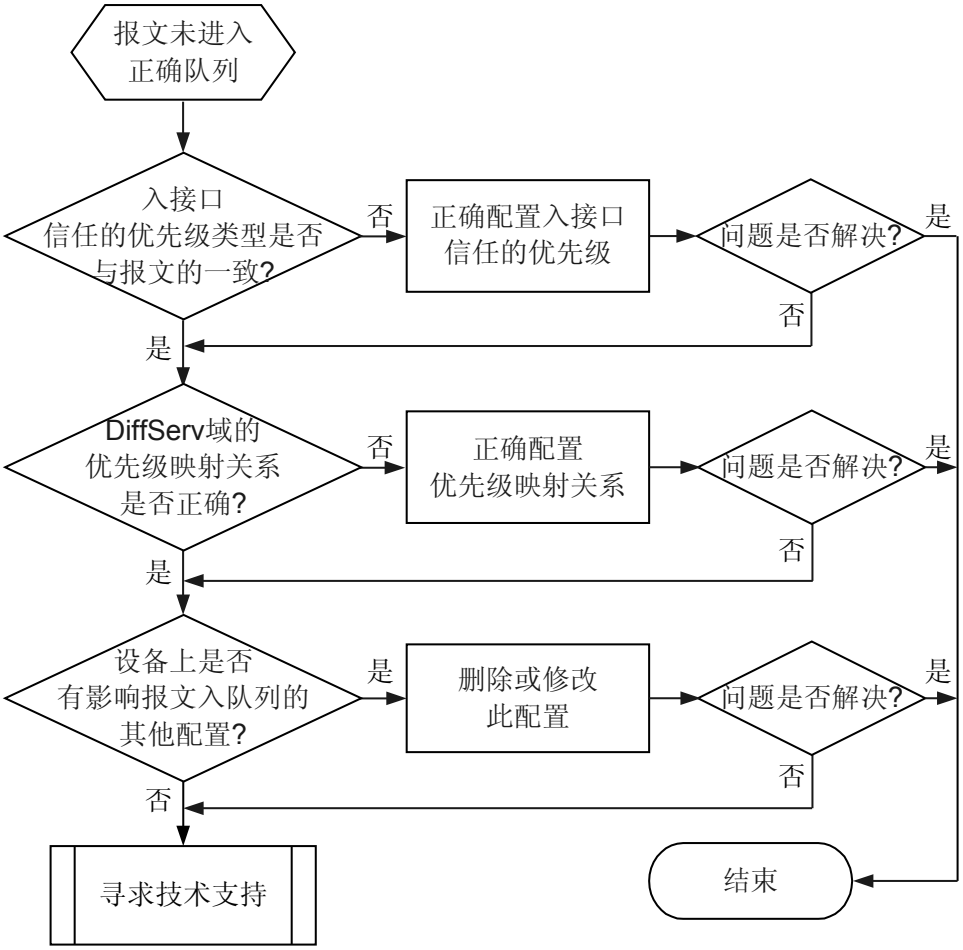
报文未进入正确队列的常见原因主要包括：

- 报文携带的优先级类型与入接口信任的优先级类型不一致。
- 入接口信任的 DiffServ 域下的优先级映射关系与要求不一致。
- 入接口有影响报文入队列的配置，如：
  - **port vlan-stacking**
  - **port vlan-mapping vlan inner-vlan** 或 **port vlan-mapping vlan map-vlan**
  - **trust upstream none**
  - **port link-type dot1q-tunnel**
  - 入方向且与报文匹配的 **traffic-policy**，流策略下有 **remark 8021p**、**remark dscp**、**remark local-precedence** 或 **remark ip-precedence** 动作。
- 报文所属 VLAN 下配置有入方向的 **traffic-policy**，流策略下有 **remark 8021p**、**remark dscp**、**remark local-precedence** 或 **remark ip-precedence** 动作。
- 全局有影响报文入队列的配置，如：
  - **qos local-precedence-queue-map**
  - 入方向且与报文匹配的 **traffic-policy**，流策略下有 **remark 8021p**、**remark dscp**、**remark local-precedence** 或 **remark ip-precedence** 动作。

故障诊断流程

如果报文未按优先级入队列，可按照图 10-4 所述流程排除故障。

图 10-4 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类型是否与报文携带的一致

进入入接口视图，执行命令 **display this**，查看入接口配置的 **trust** 命令（如果没有配置，则系统缺省信任外层 802.1p 优先级），然后抓取入接口的报文，分析其携带的优先级类型并与接口信任的优先级类型进行比较：

- 如果入接口信任的优先级类型与报文携带的不一致，执行命令 **trust** 修改入接口信任的优先级类型，使之一致。
- 如果入接口信任的优先级类型与报文携带的一致，执行步骤 2。

步骤 2 检查优先级映射关系是否正确

进入入接口视图，执行命令 **display this**，查看入接口配置的 **trust upstream** 命令（如果没有配置，系统缺省信任 default 域），然后执行命令 **display diffserv domain name** *domain-name* 检查 DiffServ 域中配置的优先级映射关系是否与业务规划符合：

- 如果配置符合业务规划，请使用命令 **ip-dscp-inbound**、**ip-dscp-outbound**、**8021p-inbound** 或 **8021p-outbound** 正确配置优先级映射关系。
- 如果配置符合业务规划，请执行步骤 3。

步骤 3 检查设备上是否有影响报文入队列的其他配置

1. 检查入接口是否有影响报文入队列的其他配置

   如果入接口配置了：

   - **port vlan-stacking**，且命令中带有 **remark-8021p** 参数，则报文的 802.1p 优先级为 **remark** 后的，影响 802.1p 优先级到本地优先级的映射，进而会影响报文入队列。
   - **port vlan-mapping vlan inner-vlan** 或 **port vlan-mapping vlan map-vlan**，且命令中带有 **remark-8021p** 参数，则报文的 802.1p 优先级为 **remark** 后的，影响 802.1p 优先级到本地优先级的映射，进而会影响报文入队列。
   - 入方向且与报文匹配的 **traffic-policy**，则若流策略下配置了 **remark local-precedence** 动作，系统按照 **remark** 后的本地优先级入队列。
   - 入方向且与报文匹配的 **traffic-policy**，则若流策略下有 **remark 8021p**、**remark ip-precedence** 或 **remark dscp** 动作，则系统根据 **remark** 后的报文优先级进行报文优先级到本地优先级的映射，并根据映射后的本地优先级入队列。
   - **trust upstream none**，则进入该接口的所有报文不进行优先级映射，报文按照接口的缺省优先级入队列。
   - **port link-type dot1q-tunnel**，且该接口下没有配置 **trust 8021p inner**，则进入该接口的所有报文将根据端口缺省优先级入对应的队列。

   进入入接口视图，执行命令 **display this**，检查入接口是否有上述影响报文入队列的配置：

   - 如果有，请根据实际情况删除或修改该配置。
   - 如果没有，执行步骤 b。

2. 检查报文所属 VLAN 下是否有影响报文入队列的配置

   如果报文所属 VLAN 下配置了：

   - 入方向的 **traffic-policy**，则若流策略下配置了 **remark local-precedence** 动作，系统按照 **remark** 后的本地优先级入队列。
   - 入方向且与报文匹配的 **traffic-policy**，则若流策略下有 **remark 8021p**、**remark ip-precedence** 或 **remark dscp** 动作，则系统根据 **remark** 后的报文优先级进行报文优先级到本地优先级的映射，并根据映射后的本地优先级入队列。

   进入报文所属 VLAN，执行命令 **display this**，检查报文所属 VLAN 下是否有上述影响报文入队列的配置：

   - 如果有，请根据实际情况删除或修改该配置。
   - 如果没有，执行步骤 c。

3. 检查全局是否有影响报文入队列的配置

   如果全局配置了：

   - **qos local-precedence-queue-map**，则系统按照此命令指定的本地优先级与队列之间的映射关系入队列
   - 入方向且与报文匹配的 **traffic-policy global**，则若流策略下配置了 **remark local-precedence** 动作，系统按照 **remark** 后的本地优先级入队列。

- 入方向且与报文匹配的 **traffic-policy global**，则若流策略下有 **remark 8021p**、**remark ip-precedence** 或 **remark dscp** 动作，则系统根据 **remark** 后的报文优先级进行报文优先级到本地优先级的映射，并根据映射后的本地优先级入队列。

执行命令 **display current-configuration**，检查全局是否有上述影响报文入队列的配置：

- 如果有，请根据实际情况删除或修改该配置。
- 如果没有，执行步骤 4。

说明
流策略应用在不同应用对象时，按照接口、VLAN、全局的优先顺序选择生效。

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

相关告警和日志

相关告警

无

相关日志

无

10.2.2 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。

常见原因

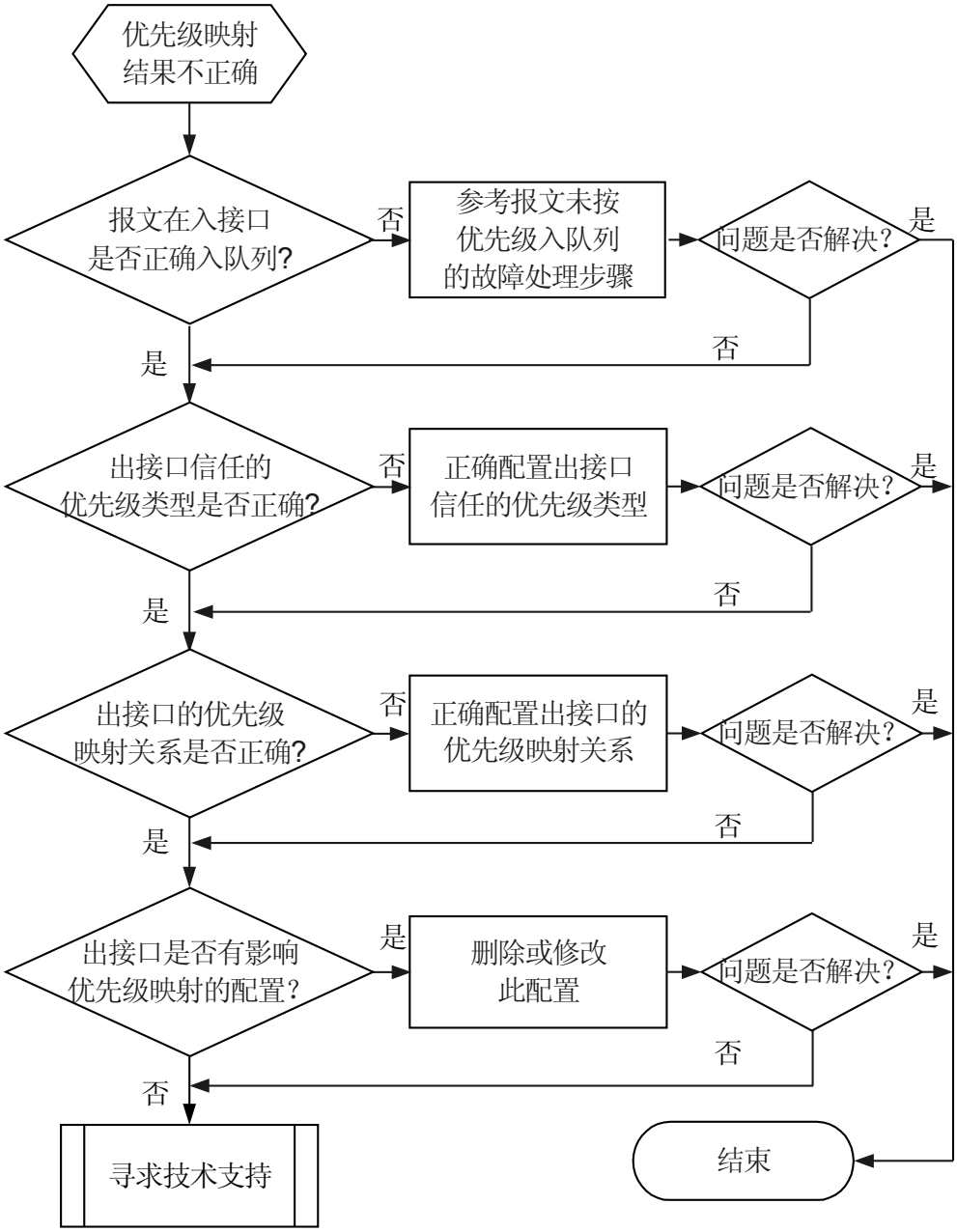
优先级映射结果不正确的常见原因主要包括：

- 报文在入接口未按报文优先级入队列。
- 出接口信任的优先级类型与要求不一致。
- 出接口信任的 DiffServ 域下配置的优先级映射关系与要求不一致。
- 出接口有影响优先级映射的配置，如：
  - **undo qos phb marking enable**
  - **trust upstream none**
  - 出方向且与报文匹配的 **traffic-policy**，且流策略下有 **remark 8021p**、**remark ip-precedence** 或 **remark dscp** 动作。

故障诊断流程

如果从 AC6605 出去的报文优先级不正确，可按照图 10-5 排除故障。

图 10-5 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 检查报文在出接口是否进入正确的队列

执行命令 **display qos queue statistics interface** *interface-type interface-number*，检查报文在出接口是否按照要求进入了相应的队列。

- 如果报文在出接口没有按照要求入队列，请参见 **10.2.1 报文未进入正确队列的定位思路**定位故障。
- 如果报文在出接口进入了正确的队列，执行步骤 2。

步骤 2 检查出接口信任的优先级类型是否正确

进入出接口视图，执行命令 **display this**，查看出接口配置的 **trust** 命令（如果没有配置，则系统缺省信任外层 802.1p 优先级），看信任的优先级类型是否与业务规划符合：

- 如果不符合，执行命令 **trust** 正确配置出接口信任的优先级类型。
- 如果符合，执行步骤 3。

步骤 3 检查出接口信任的 DiffServ 域中的优先级映射关系是否正确

进入出接口视图，执行命令 **display this**，查看出接口配置的 **trust upstream** 命令（如果没有配置，系统缺省信任 default 域）。

然后执行命令 **display diffserv domain name** *domain-name*，检查本地优先级到报文优先级的映射是否与业务规划符合：

说明

本地优先级即入接口优先级映射后的本地优先级。

- 如果不符合，执行命令 **ip-dscp-outbound** 或 **8021p-outbound** 正确配置本地优先级到报文优先级的映射。
- 如果符合，执行步骤 3。

步骤 4 检查出接口是否有影响优先级映射的其他配置

如果出接口配置了：

- **undo qos phb marking enable**，则系统对接口出方向的报文不进行 PHB 映射。
- **trust upstream none**，则系统对从此接口出去的报文不进行优先级映射。
- 出方向且与报文匹配的 **traffic-policy**，则若流策略下有 **remark 8021p**、**remark ip-precedence** 或 **remark dscp** 动作，报文优先级为 **remark** 后的报文优先级。

进入出接口视图，执行命令 **display this**，检查出接口是否有上述影响优先级映射的配置：

- 如果有，请根据实际情况删除或修改该配置。
- 如果没有，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

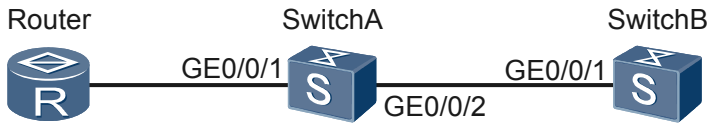
10.2.3 故障处理案例

介绍优先级映射相关的典型故障案例。

报文未进入正确队列

网络环境

图 10-6 组网图



在如图 10-6 所示组网中，Router 过来的报文带 VLAN 100，优先级为 0 ～ 7，在 SwitchA 上执行命令 **display qos queue statistics** 查看报文在出接口 GE0/0/2 处的流量统计，发现报文未按照其优先级入队列，显示如下信息：

```
<SwitchA> display qos queue statistics interface gigabitethernet 0/0/2
 Queue  CIR/PIR(kbps)          Passed(Packet/Byte)          Dropped(Packet/Byte)
-------------------------------------------------------------------------------
   0              0                 58,489,690                        0
                  1000000           5,848,935,830                     0
-------------------------------------------------------------------------------
   1              0                 0                                 0
                  1000000           0                                 0
-------------------------------------------------------------------------------
   2              0                 58,487,970                        0
                  1000000           5,848,797,000                     0
-------------------------------------------------------------------------------
   3              0                 58,487,969                        0
                  1000000           5,848,796,900                     0
-------------------------------------------------------------------------------
   4              0                 58,487,968                        0
                  1000000           5,848,796,800                     0
-------------------------------------------------------------------------------
   5              0                 58,487,967                        0
                  1000000           5,848,796,700                     0
-------------------------------------------------------------------------------
   6              0                 58,487,967                        0
                  1000000           5,848,796,600                     0
-------------------------------------------------------------------------------
   7              0                 116,975,932                       0
                  1000000           11,697,593,000                    0
-------------------------------------------------------------------------------
```

优先级为 1 的报文没有按照报文优先级进入 af1 队列。

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 SwitchA 的入接口应用的 DiffServ 域，看是否改变了优先级映射关系。
   a. 在 SwitchA 的入接口 GE0/0/1 处执行命令 **display this**。

```
[SwitchA-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
```

```
 port link-type trunk
 port trunk allow-pass vlan 100
#
return
```

显示信息表明，入接口 GE0/0/1 上应用的是缺省的 DiffServ 域，即 default 域；信任缺省的外层 802.1p 优先级。

b. 执行命令 **display diffserv domain name default**，查看 default 域的优先级映射关系。

```
<SwitchA> display diffserv domain name default
diffserv domain name:default
 8021p-inbound 0 phb be green
 8021p-inbound 1 phb af1 green
 8021p-inbound 2 phb af2 green
 8021p-inbound 3 phb af3 green
 8021p-inbound 4 phb af4 green
 8021p-inbound 5 phb ef green
 8021p-inbound 6 phb cs6 green
 8021p-inbound 7 phb cs7 green
 8021p-outbound be green map 0
 8021p-outbound be yellow map 0
 8021p-outbound be red map 0
 8021p-outbound af1 green map 1
 8021p-outbound af1 yellow map 1
 8021p-outbound af1 red map 1
 8021p-outbound af2 green map 2
 8021p-outbound af2 yellow map 2
 8021p-outbound af2 red map 2
 ......
```

显示信息表明，入接口的优先级映射关系是正确的。

2. 检查 SwitchA 的出接口应用的 DiffServ 域，看是否改变了优先级映射关系。

在 SwitchA 的出接口 GE0/0/2 处执行命令 **display this**。

```
[SwitchA-GigabitEthernet0/0/2] display this
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 100
#
return
```

显示信息表明，出接口 GE0/0/2 上应用的也是缺省的 DiffServ 域，信任的也是缺省的外层 802.1p 优先级。从前面显示的 default 域的配置信息来看，出接口处的优先级映射关系也是正确的。

3. 执行命令 **display current-configuration configuration system**，检查 SwitchA 上是否有影响报文入队列的其他配置。

```
<SwitchA> display current-configuration configuration system
#
 sysname SwitchA
#
 vlan batch 1 100
#
 qos car car1 cir 10000 cbs 1880000
#
 qos local-precedence-queue-map  af1  7
return
```

显示信息表明，SwitchA 上配置了本地优先级与入队列的映射关系，此配置导致 802.1p 优先级为 1 的报文均进入了优先级 7 的队列中了。

操作步骤

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

步骤 2 执行命令 **undo qos local-precedence-queue-map af1 7**，取消本地优先级 AF1 到队列 7 的映射关系。

完成上述操作后，执行命令 **display qos queue statistics interface gigabitethernet0/0/2**，看到 802.1p 优先级为 0 ～ 7 的报文均能够按其优先级入队列。

----结束

案例总结

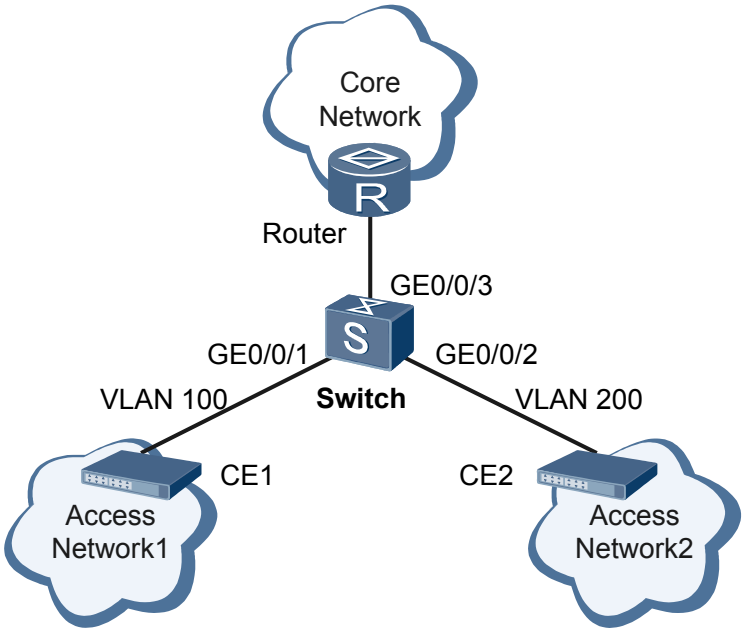
报文未按优先级入队列的一般原因是由于系统有影响报文入队列的配置，如 **port vlan-stacking**、**port vlan-mapping**、**qos local-precedence-queue-map**、**trust upstream none** 或 **port link-type dot1q-tunnel**，或 **traffic-policy** 且流策略下有 **remark** 动作，这些都会改变优先级映射关系，使报文未按照其优先级入相应队列。

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 10-7 所示组网中，Access Netwaork1 和 Access Netwaork2 通过 Switch 接入核心网企业网网络，来自 Access Netwaork1 和 Access Netwaork2 的报文携带 802.1p 优先级，而核心网企业网网络设备根据报文的 DSCP 优先级进行 QoS 处理，因此在 Switch 上配置优先级映射，使来自 Access Network1 的报文携带 DSCP 值为 10，来自 Access Network2 的报文携带 DSCP 值为 63，从而使核心网企业网网络设备能根据 DSCP 值进行不同的 QoS 处理。

图 10-7 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 Router 上接收到的来自 Access Netwaork1 与 Access Netwaork2 的报文的 DSCP 值均与实际不符。

故障分析

1. 检查 Switch 入接口配置的优先级映射关系及信任的报文优先级是否正确。

   a. 分别在 Access Netwaork1 和 Access Netwaork2 的接入接口上抓取报文，分析报文优先级。发现报文的 802.1p 优先级为 0。

   b. 然后分别进入入接口 GE0/0/1 和 GE0/0/2 视图，执行命令 **display this**，查看接口配置。

```
[Switch-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
 trust upstream ds1
#
return
[Switch-GigabitEthernet0/0/2] display this
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
 trust upstream ds2
#
return
```

   显示信息表明，入接口 GE0/0/1 和 GE0/0/2 分别配置了 DiffServ 域 ds1 和 ds2，信任优先级为缺省的外层 802.1p 优先级。执行命令 **display diffserv domain name** 分别查看 ds1 和 ds2 的配置。

```
<Switch> display diffserv domain name ds1
diffserv domain name:ds1
 8021p-inbound 0 phb af2 green
 8021p-inbound 1 phb af2 green
 8021p-inbound 2 phb af2 green
 8021p-inbound 3 phb af2 green
 8021p-inbound 4 phb af2 green
 8021p-inbound 5 phb af2 green
 8021p-inbound 6 phb af2 green
 8021p-inbound 7 phb af2 green
......
<Switch> display diffserv domain name ds2
diffserv domain name:ds2
 8021p-inbound 0 phb cs7 green
 8021p-inbound 1 phb cs7 green
 8021p-inbound 2 phb cs7 green
 8021p-inbound 3 phb cs7 green
 8021p-inbound 4 phb cs7 green
 8021p-inbound 5 phb cs7 green
 8021p-inbound 6 phb cs7 green
 8021p-inbound 7 phb cs7 green
......
```

   显示信息表明，来自 Access Netwaork1 的报文进入 Switch 的 AF2 队列，来自 Access Netwaork2 的报文进入 CS7 队列。

2. 检查出接口配置的优先级映射关系及信任的优先级类型是否正确。

   进入接口 GE0/0/3 视图，执行命令 **display this**，查看接口配置。

```
[Switch-GigabitEthernet0/0/3] display this
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 200
 trust upstream out-ds
#
return
<Quidway> display diffserv domain name out-ds
ip-dscp-outbound be green map 0
```

```
ip-dscp-outbound be yellow map 0
ip-dscp-outbound be red map 0
ip-dscp-outbound af1 green map 10
ip-dscp-outbound af1 yellow map 12
ip-dscp-outbound af1 red map 14
ip-dscp-outbound af2 green map 10
ip-dscp-outbound af2 yellow map 10
ip-dscp-outbound af2 red map 10
ip-dscp-outbound af3 green map 26
ip-dscp-outbound af3 yellow map 28
ip-dscp-outbound af3 red map 30
ip-dscp-outbound af4 green map 34
ip-dscp-outbound af4 yellow map 36
ip-dscp-outbound af4 red map 38
ip-dscp-outbound ef green map 46
ip-dscp-outbound ef yellow map 46
ip-dscp-outbound ef red map 46
ip-dscp-outbound cs6 green map 48
ip-dscp-outbound cs6 yellow map 48
ip-dscp-outbound cs6 red map 48
ip-dscp-outbound cs7 green map 63
ip-dscp-outbound cs7 yellow map 63
ip-dscp-outbound cs7 red map 63
```

显示信息表明，出接口 GE0/0/3 配置了信任 DiffServ 域 out-ds，out-ds 域将 AF2 映射为 DSCP 10，将 CS7 映射为 DSCP 63，映射关系正确。

但出接口上没有配置信任报文优先级，因此采用缺省设置，即信任外层 802.1p 优先级。因此，从 Switch 的出接口 GE0/0/3 发出去的报文并没有按照 out-ds 域的映射关系标记用户报文，即将来自 Access Netwaork1 的报文的 DSCP 标记为 10，来自 Access Netwaork2 的报文的 DSCP 标记为 63。

操作步骤

步骤 1 执行命令 **interface** gigabitethernet0/0/3，进入接口视图。

步骤 2 执行命令 **trust dscp**，配置信任 DSCP 优先级。

执行完上述操作后，模拟 Access Netwaork1 和 Access Netwaork2 中的用户，分别向 Switch 发送报文，在出接口 GE0/0/3 处抓包，发现报文的 DSCP 均与要求一致，故障排除。

----结束

案例总结

优先级映射不正确时，需要关注出入接口配置的映射关系，以及信任的报文优先级，任何一处不正确，都有可能导致映射错误。

10.3 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。

10.3.1 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 或聚合 CAR 的流策略，因此其故障定位思路与流策略的相同，请参见 **10.1.1 流策略不生效的定位思路**。

10.3.2 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

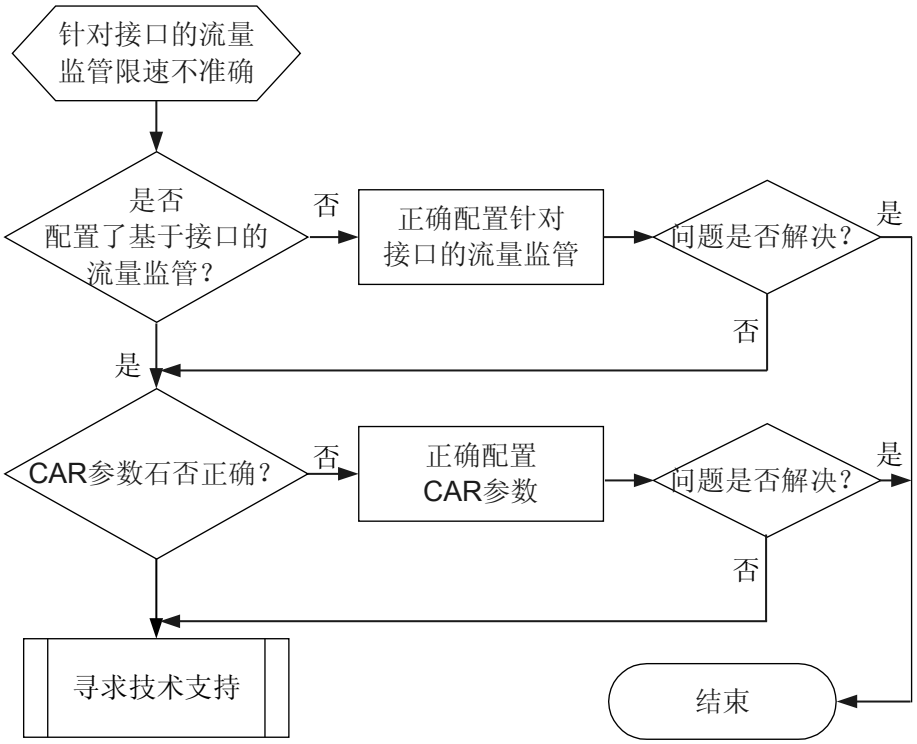
本类故障的常见原因主要包括：

- 接口上没有配置 **qos lr inbound**。
- CAR 参数配置不正确（与业务规划不符）。

故障诊断流程

如果针对接口的流量监管限速不准确，请使用如图 10-8 所示的故障诊断流程处理。

图 10-8 针对接口的流量监管限速不准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。

操作步骤

步骤 1 检查接口上是否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 lr inbound**。

- 如果没有配置，请执行命令 **qos lr inbound** 正确配置。
- 如果已配置，执行步骤 2。

步骤 2 检查 CAR 参数是否正确配置。

执行命令 **display qos lr**，检查 CAR 参数是否正确（即是否与业务规划一致）。

说明

AC6605 上，基于接口的流量监管粒度是 8K，即：如果 1<= CAR 值/8 < 2，按照(64+8)K 处理；如果 2 <= CAR 值/8 < 3，按照(64+8*2)K 处理，依次类推。

- 如果配置不正确，请执行命令 **qos lr inbound** 正确配置。
- 如果配置正确，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

相关告警和日志

相关告警

无

相关日志

无

10.3.3 故障处理案例

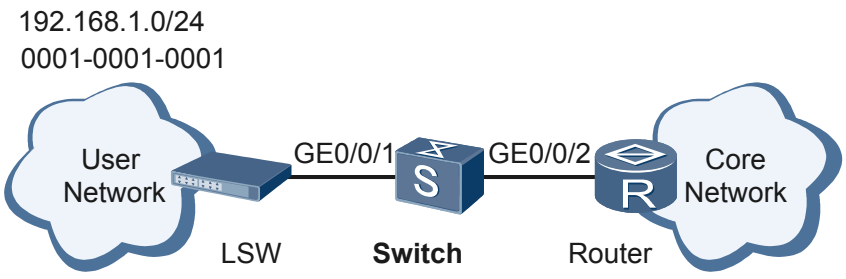
介绍 QoS CAR 相关的典型故障案例。

基于类的流量监管不生效

网络环境

如图 10-9 所示，用户通过 LSW 接入 Switch，用户所在网段为 192.168.1.0/24，MAC 地址为 0001-0001-0001。在 Switch 接口 GE0/0/1 上配置流量监管，限制 Switch 上行流量速率为 50Mbit/s，但是从 LSW 往 Switch 发送速率为 100Mbit/s 的流量时，发现从 Switch 发出去的流量速率仍然为 100Mbit/s，流量监管功能没有生效。

图 10-9 基于类的流量监管失效组网图



故障分析

1. 检查接口上是否配置了入方向的流策略。

   进入接口 GE0/0/1 视图，然后执行命令 **display this**，查看接口配置的流策略。

```
[Quidway-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
 traffic-policy tp1 inbound
#
return
```

   显示信息表明，接口 GE0/0/1 上配置有入方向的流策略 tp1。

2. 查看流策略中的流分类及流行为是否正确。

   执行命令 **display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看流策略中是否绑定流分类及流动作，流动作中是否配置 CAR 以及 CAR 配置是否正确。

```
[Quidway] display traffic policy user-defined tp1
  User Defined Traffic Policy Information:
  Policy: tp1
   Classifier: tc1
    Operator: AND
     Behavior: tb1
        Committed Access Rate:
        CIR 5000 (Kbps), CBS 625000 (Byte)
        PIR 5000 (Kbps), PBS 625000 (Byte)
        Green Action   : pass
        Yellow Action  : pass
        Red Action     : discard
```

   执行命令 **display traffic classifier**，查看流分类中配置的匹配规则是否正确。

```
[Quidway] display traffic classifier user-defined tc1
  User Defined Classifier Information:
   Classifier: tc1
    Operator: AND
    Rule(s) : if-match acl 4000
[Quidway] display acl 4000
Advanced ACL 4000, 1 rule
Acl's step is 5
 rule 5 permit source-mac 0001-0001-0001 ffff-ffff-0fff
```

   检查发现流策略 tp1 中流分类与流行为配置均正确。

3. 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 GE0/0/1 上基于流策略的流量统计信息。显示信息如下：

```
[Quidway] display traffic policy statistics interface gigabitethernet 0/0/1 inbound
 Interface: GigabitEthernet0/0/1
 Traffic policy inbound: tp1
 Rule number: 1
 Current status: OK!
-------------------------------------------------------------------------
 Board : 0
Item                              Packets                       Bytes
-------------------------------------------------------------------------
Matched                                 0                           -
  +--Passed                             0                           -
  +--Dropped                            0                           -
    +--Filter                           0                           -
    +--URPF                             -                           -
    +--CAR                              0                           -
```

显示信息表明，报文没有命中流分类中的规则。

4. 检查报文流是否匹配了更高优先级的规则。

执行命令 **display current-configuration**，查看系统配置的流策略。

```
[Quidway] display current-configuration
#
 sysname Quidway
#
acl number 3000
 rule 5 permit ip source 192.168.1.0 0.0.0.255
#
acl number 4000
 rule 5 permit rule 10 permit source-mac 0001-0001-0001 ffff-ffff-0fff
#
traffic classifier test operator or
 if-match acl 3000
traffic classifier tcl operator or
 if-match acl 4000
#
traffic behavior test
 permit
traffic behavior tbl
 car cir 50000 pir 50000 cbs 6250000 pbs 6250000 green pass yellow pass red discard
#
traffic policy test
 classifier test behavior test
traffic policy tpl
 classifier tcl behavior tbl
#
 traffic-policy test global inbound
#
interface GigabitEthernet0/0/1 port link-type trunk
 port trunk allow-pass vlan 100
 traffic-policy tpl inbound
#
return
```

显示信息表明，Switch 上全局存在一个流策略 test，该流策略下绑定的流分类为 test，流行为为 test；流分类中配置的规则是 ACL 3000，该规则是匹配源 IP 地址 192.168.1.0，属于 Layer 3 类型规则；流行为 test 采用动作为 permit。

AC6605 中，包含 Layer 3 类型规则的流策略优先级高于包含 Layer 2 类型规则的流策略。因此，来自 192.168.1.0/24 网段，源 MAC 地址 0001-0001-0001 的报文同时有两个规则匹配，但是只有包含 ACL 3000 规则的流策略 test 生效，报文被直接转发了，导致流量监管功能失效。

操作步骤

步骤 1 进入系统视图，执行命令 **undo traffic-policy global inbound**，取消流策略 test 在全局的应用。

取消全局应用的流策略 test 后，向接口 GE0/0/1 发送速率为 100Mbit/s 的流量，从接口 GE0/0/2 发送出去的流量速率为 50Mbit/s，故障排除。

----结束

案例总结

如果基于类的流量监管不生效，则采用 **10.1.1 流策略不生效的定位思路**，重点关注报文有没有命中流量监管策略。

10.4 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。

10.4.1 队列流量整形结果不正确的定位思路

介绍针对队列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准确包括如下现象：

- 队列流量整形不生效。
- 队列流量整形 CIR 没有得到保证。

队列流量整形结果不准确的常见原因包括：

- 没有配置正确的队列整形参数。
- 端口整形 CIR 小于端口队列整形 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。

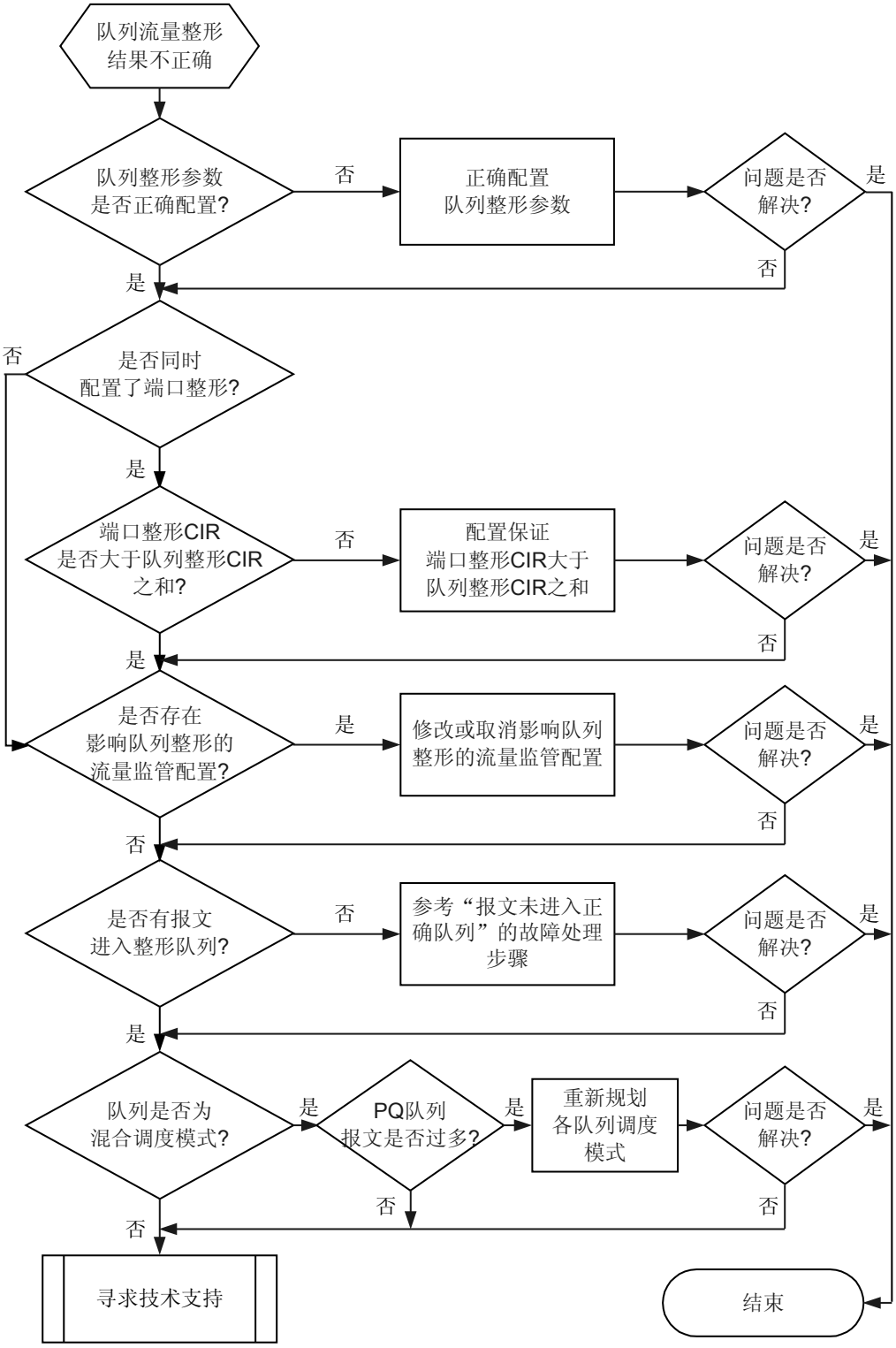
  说明

  混合调度模式下，队列的流量整形 PIR 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

如果流量整形结果不正确，请使用如图 10-10 所示的故障诊断流程处理。

图 10-10 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。

操作步骤

步骤 1 检查端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**，检查端口上是否配置有 **qos queue shaping** 命令：

- 如果没有配置或配置的队列整形参数不符合业务规划，请使用命令 **qos queue shaping** 进行正确配置。
- 如果已配置，且同时配置了端口整形 CIR（使用命令 **qos lr outbound**），请执行步骤 2。
- 如果已配置，但没有配置端口整形 CIR，请执行步骤 3。

步骤 2 检查端口整形 CIR 是否大于端口队列整形 CIR 之和

比较端口整形 CIR 与该端口上各队列整形 CIR 之和：

- 如果端口整形 CIR 小于等于端口队列整形 CIR 之和，则队列要求的带宽将得不到保证，会出现流量整形不准现象，请使用命令 **qos lr outbound** 和 **qos queue shaping** 修改相应参数，保证端口整形 CIR 大于该端口上所有队列整形的 CIR 之和。
- 如果端口整形 CIR 大于端口队列整形 CIR 之和，则执行步骤 3。

步骤 3 检查设备上是否存在影响队列整形的流量监管配置

1. 检查入接口是否配置了基于接口的流量监管

   如果报文入接口上配置了基于接口的流量监管，且其 CIR 小于队列整形 CIR，则队列整形结果以基于接口的流量监管 CIR 为准。

   进入报文入接口视图，执行命令 **display this**，查看接口是否配置 **qos lr inbound** 命令，且其 CIR 值是否小于队列整形 CIR：

   - 如果配置了且其 CIR 小于队列整形 CIR，请根据实际情况，取消基于接口的流量监管配置，或者修改配置，使基于接口的流量监管 CIR 大于队列整形 CIR。
   - 如果没有配置，或者虽配置但其 CIR 大于队列整形 CIR，请执行步骤 b。

2. 检查设备上是否配置了基于类的流量监管

   如果设备上配置了基于类的流量监管，其 CIR 小于队列整形 CIR，且其流分类与队列流量匹配，则队列整形结果以基于类的流量监管 CIR 为准。

   分别进入全局、报文入接口以及报文所属 VLAN 的视图，执行命令 **display this**，查看是否配置了 **traffic-policy** 命令：

   - 如果配置了流策略，执行命令 **display traffic policy user-defined** 查看流策略中是否配置了 **car**，且其 CIR 值是否小于队列整形 CIR。
     - 如果是，请执行命令 **display traffic classifier user-defined**，查看流策略中的流分类，判断其是否与队列流量匹配。如果与队列流量匹配，请根据实际情况，取消流策略中的 **car** 配置，或者修改配置，使流策略中的 CIR 大于队列整形 CIR；如果与队列流量不匹配，请执行步骤 4。
     - 如果否，请执行步骤 4。

- 如果没有配置流策略，请执行步骤 4。

说明

- 流策略的优先级最高，如果同时配置了基于接口的流量监管和基于类的流量监管，基于类的流量监管生效。
- 如果全局、接口、VLAN 同时配置流策略，优先级由高到低依次为接口、VLAN、全局，优先级高的生效。

步骤 4 检查是否有报文进入整形队列

- 执行命令 **display qos queue statistics interface** *interface-type interface-number*
- 如果报文没有进入整形队列，请参见 **10.2.1 报文未进入正确队列的定位思路(AC6605)**进行故障定位。
- 如果有报文进入整形队列，但有大量报文（如 GigabitEthernet 接口上报文速率超过 100Mbit/s）进入 PQ 队列，则执行步骤 4。
- 如果报文进入整形队列，且没有大量报文进入 PQ 队列，则执行步骤 5。

步骤 5 检查端口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：

- 如果端口上既配置了 **qos wrr** 或 **qos drr**，又有队列配置了 **qos queue** *queue-index* **drr weight 0** 或 **qos queue** *queue-index* **wrr weight 0**，则端口各队列是混合调度模式。

  混合调度模式下，如果 PQ 队列没有限制带宽，当 PQ 队列有大量报文时，会影响 WRR/DRR 队列的流量整形效果，而队列整形是配置在调度模式为 WRR/DRR 的队列上的。此时，请使用命令 **qos** { **pq** | **drr** | **wrr** }、**qos queue** *queue-index* { **drr** | **wrr** }**weight** 重新规划各队列的调度模式及参数，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 PIR 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 **qos pq** 或 **qos wrr/drr**，则执行步骤 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。
- 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

10.4.2 故障处理案例

介绍流量整形相关的典型故障案例。

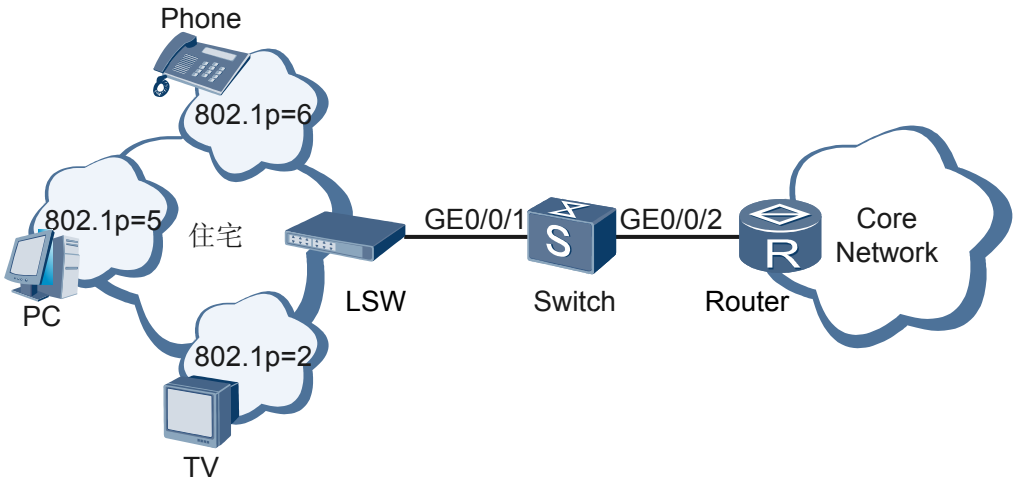
队列流量整形结果不正确

网络环境

在如图 10-11 所示组网中。由于来自网络侧的流量速率大于 LSW 接口的速率，Switch 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 Switch 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 128kbit/s
- 视频限速为 2000kbit/s
- 数据限速为 512kbit/s

图 10-11 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. 检查下行接口上配置的流量整形参数。

   进入下行接口 GE0/0/1 的视图，执行命令 **display this**，查看该接口上配置的流量整形参数。

```
[Switch-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 200
 qos lr outbound cir 2000 cbs 250000
 qos drr
 qos queue 0 drr weight 0
 qos queue 1 drr weight 0
 qos queue 2 drr weight 20
 qos queue 3 drr weight 0
 qos queue 4 drr weight 0
 qos queue 5 drr weight 50
 qos queue 6 drr weight 80
 qos queue 7 drr weight 0
 qos queue 2 shaping cir 2000 pir 2000
 qos queue 5 shaping cir 512 pir 512
```

```
 qos queue 6 shaping cir 128 pir 128

#
return
```

显示结果表明，出接口上配置了端口整形和队列整形，队列 2、5、6 采用 DRR 调度模式，各队列流量整形参数均正确。但是，端口整形的 CIR 小于队列 2、5、6 的整形 CIR 之和。

AC6605 上，当端口整形 CIR 小于队列整形 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 执行命令 **interface gigabitethernet0/0/1**，进入下行接口视图。

步骤 2 执行命令 **qos lr outbound cir 3000**，修改端口整形的 CIR 为 3000kbit/s，使之大于各队列的流量整形的 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

当端口整形 CIR 值小于队列整形 CIR 值之和时，队列要求的 CIR 将得不到保证。

10.5 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。

10.5.1 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

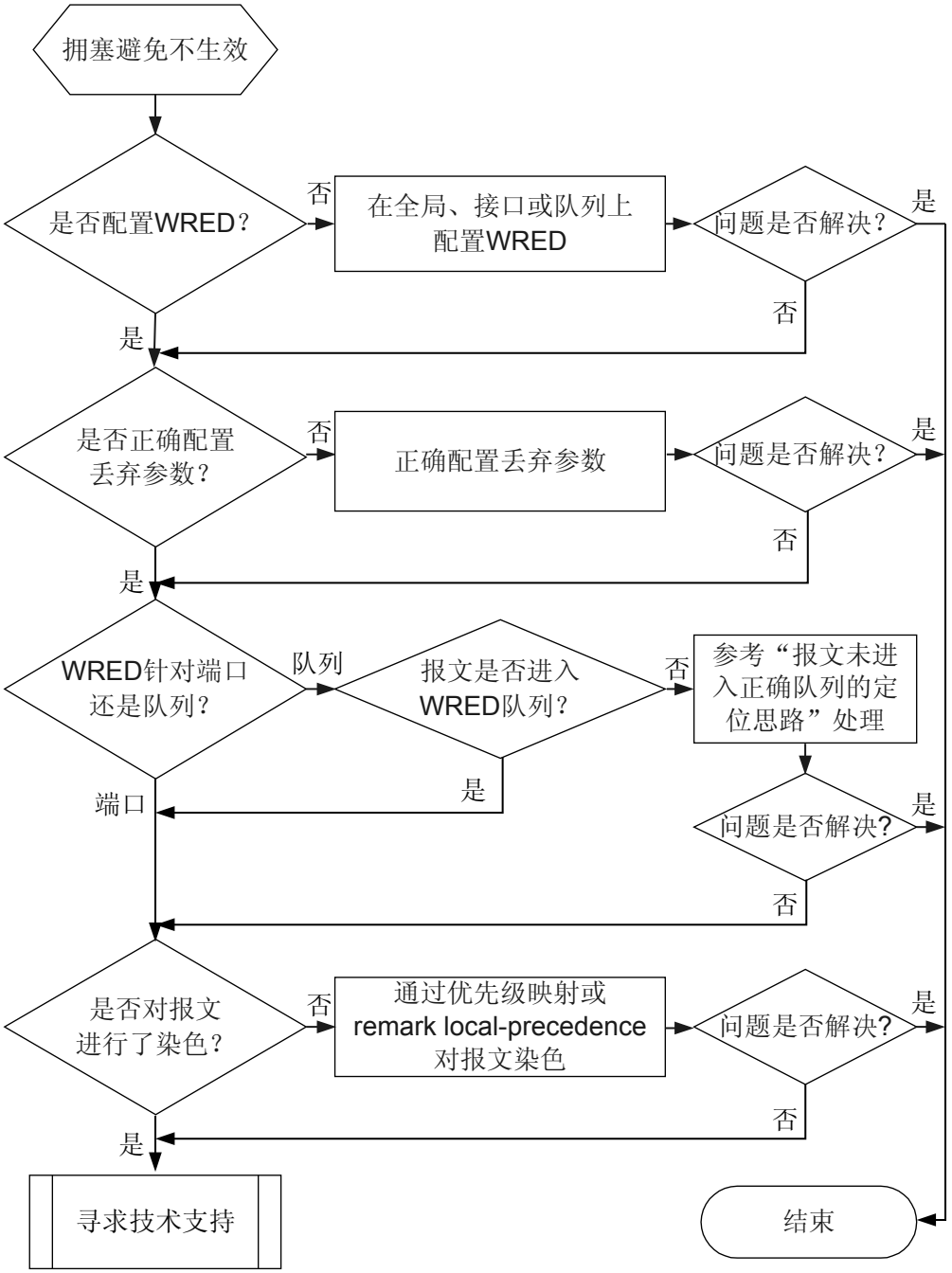
拥塞避免不生效的常见原因包括：

- 接口或队列没有成功配置 WRED。
- 没有通过优先级映射或 **remark local-precedence** 动作对报文染色。
- WRED 模板没有配置与报文颜色对应的丢弃参数。
- （针对队列级拥塞避免）报文没有进入配置了 WRED 模板的队列。

故障诊断流程

如果拥塞避免不生效，请使用如图 **10-12** 所示的故障诊断流程处理。

图 10-12 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。

操作步骤

步骤 1 检查全局、接口或接口队列上是否配置了 WRED 模板

1. 进入接口视图，执行命令 **display this**，检查接口上是否配置有 **qos wred** 或 **qos queue wred** 命令
   - 如果配置了，请执行步骤 2。
   - 如果均没有配置，请执行步骤 b。
2. 进入系统视图，执行命令 **display this**，检查全局是否配置了 **qos queue wred** 命令
   - 如果没有配置，请根据业务需求，执行命令 **qos queue wred** 或 **qos wred**，在全局或接口配置 WRED。
   - 如果配置了，请执行步骤 2。

说明

全局配置的 WRED 在所有接口生效。如果全局和接口同时配置了某队列的 WRED，接口配置的生效。

如果同时配置了接口和接口队列的 WRED，系统会执行两次 WRED，先队列后接口。

步骤 2 检查 WRED 模板中是否正确设置了丢弃参数

执行命令 **display drop-profile**，检查 WRED 模板中是否设置了与业务规划符合的丢弃参数：

- 如果没有配置，请执行命令 **color** 设置合适的丢弃参数。
- 如果已经配置，且接口配置了 **qos queue wred** 命令，执行步骤 3。
- 如果已经配置，且接口配置了 **qos wred** 命令，执行步骤 4。

步骤 3 检查报文是否进入配置了 WRED 的队列

执行命令 **display qos queue statistics**，检查 WRED 对应队列下是否有报文统计信息：

- 如果有，执行步骤 4。
- 如果没有，说明报文没有进入 WRED 对应的队列，请参见 **10.2.1 报文未进入正确队列的定位思路**进行故障定位。

步骤 4 检查是否通过优先级映射或流动作对报文染色

进入接口视图，执行命令 **display this**，依次检查接口上是否有如下配置。

1. 检查接口上是否配置了 **traffic-policy** 命令
   - 如果配置了，执行命令 **display traffic policy** 命令查看流策略中的动作，看是否配置了 **remark local-precedence** 动作：
     - 如果配置了 **remark local-precedence** 动作但没有指定 *color*，请重新执行该命令指定 *color*。
     - 如果配置了 **remark local-precedence** 动作，且配置了相应的颜色参数，系统按照配置染色报文，执行步骤 5。
     - 如果两者均没有配置，执行步骤 b。
2. 检查接口上是否配置了 **dei enable** 命令
   - 如果配置了，系统按照报文中的 CFI 标志位染色报文，如果 CFI=1，报文颜色标记为 yellow；如果 CFI=0，报文颜色标记为 green，执行步骤 5。
   - 如果没有配置，执行步骤 c。
3. 检查接口上是否配置了 **trust upstream** 命令

   如果配置了，系统按照配置的 Diffserv 域中的报文优先级到颜色的映射关系染色报文；如果没有配置，系统缺省信任 default 域，并采用此 default 域中的报文优先级到颜色的映射关系染色报文。此时，请执行命令 **display diffserv domain name** *diffserv-domain-name*，检查报文优先级到颜色的映射关系是否符合业务规划。

- 如果不符合，请根据业务规划，执行命令 **8021p-inbound**，修改报文优先级与颜色之间的映射关系。
- 如果符合，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

10.6 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。

10.6.1 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

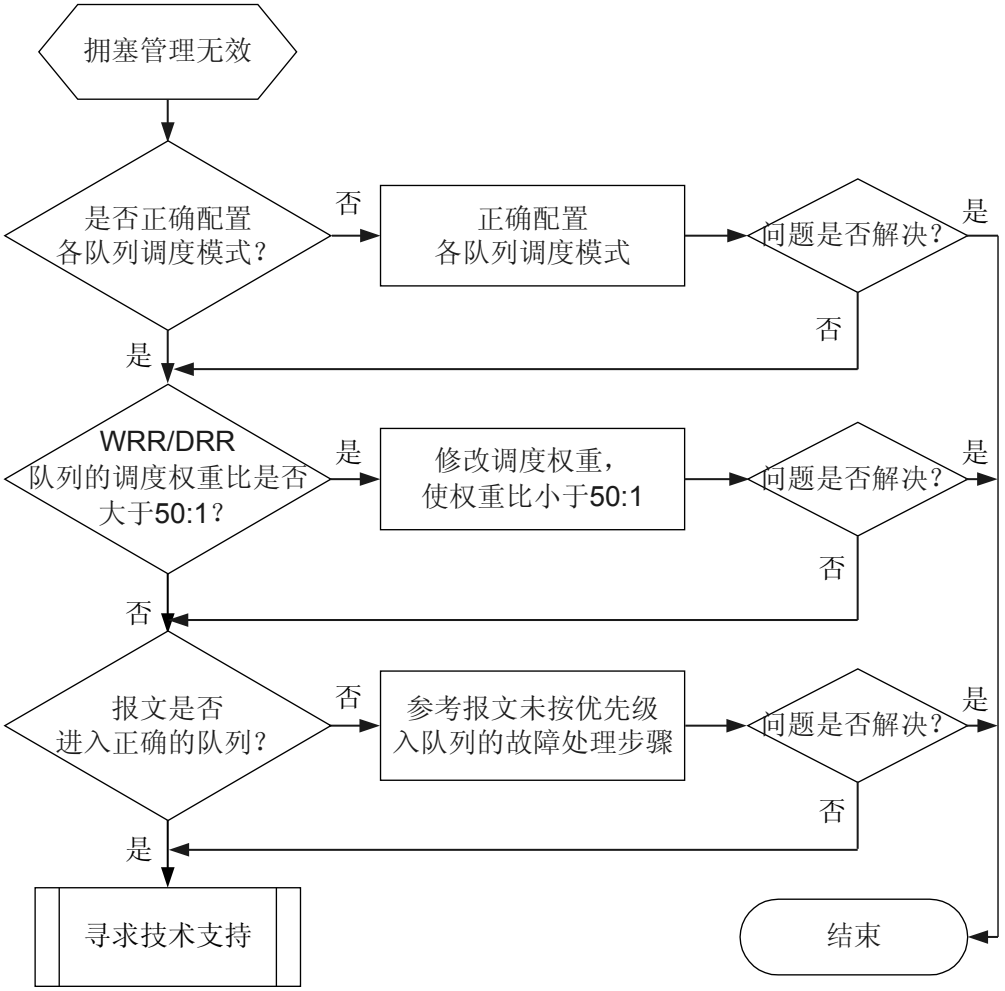
本类故障的常见原因主要包括：

- 队列调度模式设置不合适。
- WRR 或 DRR 队列的调度权重比超过 50:1。
- 报文未按业务规划入队列。

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 10-13** 所示的故障诊断流程处理。

图 10-13 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 检查各队列调度模式是否合适

进入接口视图，使用命令 **display this**，检查接口配置的各队列的调度模式是否能满足业务需求：

说明

设置队列调度模式时：

- 推荐采用 PQ+WRR/PQ+DRR 混合调度模式，将延迟敏感的关键业务设置为 PQ 调度模式，其他业务设置为 WRR/DRR 调度。
- 如果设置各队列采用 PQ 调度模式，则将延迟敏感的关键业务放入高优先级队列，将非关键业务放入低优先级队列。
- 如果设置各队列采用 WRR/DRR 调度模式，则给关键业务分配较高权重，给非关键业务分配较低权重。
- 报文平均长度变化不大时采用 WRR 调度，变化大时采用 DRR 调度。

- 如果不能满足业务需求，请执行命令 **qos** { **pq** | **wrr** | **drr** }重新设置各队列的调度模式。
- 如果能满足业务需求，请执行步骤 2。

步骤 2 检查 WRR/DRR 队列的调度权重比是否过大

说明

WRR 或 DRR 调度时，如果权重比例过大（大于 50:1），则会造成 WRR 或 DRR 调度不准，从而影响拥塞管理效果。

进入接口视图，使用命令 **display this**，检查并比较 WRR/DRR 调度队列的权重数值，看其比值是否大于 50:1：

- 如果是，使用命令 **qos queue** *queue-index* **drr weight** *weight* 或 **qos queue** *queue-index* **wrr weight** *weight* 修改 WRR/DRR 队列的调度权重，使其比例小于 50:1。
- 如果否，请执行步骤 3。

步骤 3 检查报文是否进入正确的队列

使用测试仪发送业务报文到 AC6605，然后执行命令 **display qos queue statistics** 查看队列统计信息，看业务报文是否进入对应的队列（与步骤 1 设置一致）：

- 如果报文没有进入正确的队列，请参见报文未进入正确队列的定位思路 **10.2.1 报文未进入正确队列的定位思路**(AC6605)进行故障定位。
- 如果报文进入正确的队列，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

相关告警和日志

相关告警

无

相关日志

无

10.6.2 故障处理案例

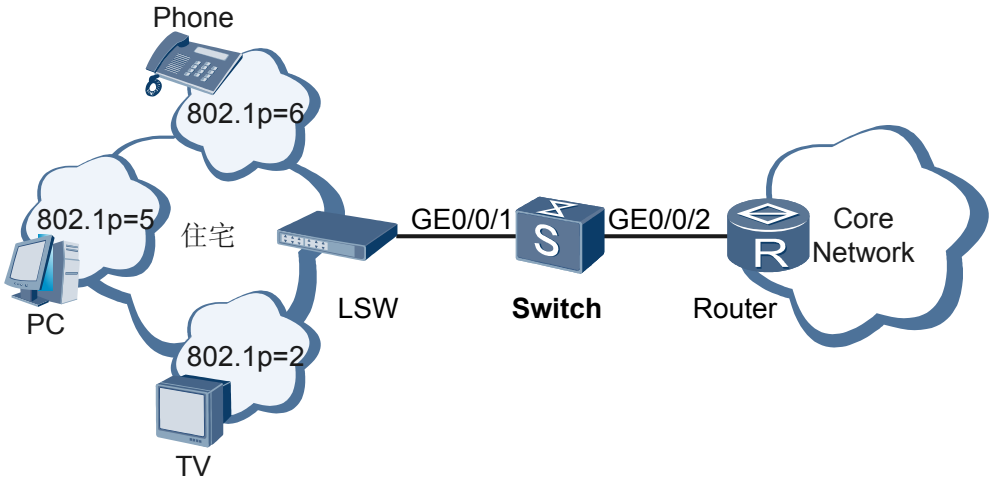
介绍拥塞管理相关的典型故障案例。

高优先级业务得不到优质服务

网络环境

在图 10-14 所示的网络中，Switch 通过接口 GE0/0/2 与路由器互连。来自网上的业务有语音、视频、数据。各类报文携带的 802.1p 优先级分别为 6、2、5。这些业务可经由路由器和 Switch 到达用户。为保证各类业务的服务质量，网络中配置拥塞管理功能。

图 10-14 高优先级业务得不到优质服务组网图



配置完成后，发现语音、视频信号有时会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

拥塞管理功能无效的可能原因是：

- 报文无法进入正确队列，导致低优先级的报文顺利通过，而高优先级对应的语音信号报文被丢弃。
- 优先级队列的队列调度模式及权重参数配置不恰当。

可通过如下步骤排查：

1. 查看接口各队列的流量统计和调度参数。

   执行命令 **display qos queue statistics** 查看指定接口上基于队列的流量统计信息和各队列的调度参数。

```
<Quidway> display qos queue statistics interface gigabitethernet 0/0/2
 Queue  CIR/PIR (kbps)          Passed (Packet/Byte)        Dropped (Packet/Byte)
------------------------------------------------------------------------------
   0         1000000                      0                           0
             1000000                      0                           0
------------------------------------------------------------------------------
   1         1000000                      0                           0
             1000000                      0                           0
------------------------------------------------------------------------------
   2            2000                   2457863                        0
                2000                 245786300                        0
------------------------------------------------------------------------------
   3         1000000                   2012324                        0
```

	1000000	201232400	0
4	1000000 1000000	2047189 204718900	0 0
5	512 512	0 0	0 0
6	1000000 1000000	0 0	0 0
7	128 128	0 0	0 0

显示信息表明，报文被映射到队列 AF2、AF3、AF4 队列。

2. 检查接口上配置的优先级映射和队列调度参数。

   在接口视图下执行命令 **display this**，查看该接口上是否指定对入报文按照 DiffServ 域中相应类别的优先级进行映射。

   - 如果流经该接口的是携带 DSCP 优先级的 IP 报文，接口上需要配置 **trust upstream** 和 **trust dscp**。
   - 如果流经该接口的是 VLAN 报文，接口上需要配置 **trust upstream** 和 **trust 8021p**。

```
[Quidway-GigabitEthernet0/0/2] display this
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 100 110 120
 qos queue 0 wrr weight 0
 qos queue 1 wrr weight 10
 qos queue 2 wrr weight 20
 qos queue 3 wrr weight 30
 qos queue 4 wrr weight 40
 qos queue 5 wrr weight 0
 qos queue 6 wrr weight 0
 qos queue 7 wrr weight 0
 trust upstream ds1
#
return
```

   显示信息表明，接口 GE0/0/2 上已绑定 DiffServ 域 ds1，且已信任外层 8021p 优先级，AF1 ～ AF4 队列调度模式均为 WRR 调度，调度权重分别为 10、20、30、40；BE、EF、CS6、CS7 队列均为 PQ 调度。

3. 查看 DiffServ 域的配置。

   执行命令 **display diffserv domain name ds1**，查看 DiffServ 域 ds1 下的 8021p 优先级映射关系。

```
<Quidway> display diffserv domain name ds1
diffserv domain name:ds1
 8021p-inbound 0 phb be green
 8021p-inbound 1 phb af1 green
 8021p-inbound 2 phb AF2 green
 8021p-inbound 3 phb af3 green
 8021p-inbound 4 phb af4 green
 8021p-inbound 5 phb AF3 green
 8021p-inbound 6 phb AF4 green
 8021p-inbound 7 phb cs7 green
 8021p-outbound be green map 0
 8021p-outbound be yellow map 0
```

   显示信息表明，802.1p 优先级分别为 6、5、2 的报文分别被映射到 AF4、AF3、AF2 队列，与业务规划符合。而 AF4、AF3、AF2 队列的调度模式均为 WRR 调度，调度权重分别为 40、30、20，这样的调度模式及权重设置在业务流量不高时，低时延

业务服务较好，但在业务流量较高时，并不能保证低时延业务的服务质量。因此，语音信号有时会出现断断续续的现象。

操作步骤

步骤 1 执行命令 **diffserv domain ds1**，进入 ds1 域视图。

步骤 2 执行命令 **8021p-inbound 2 phb af2 green**，配置 802.1p 优先级为 2 的报文映射到 AF2 队列。

步骤 3 执行命令 **8021p-inbound 5 phb ef green**，配置 802.1p 优先级为 5 的报文映射到 EF 队列。

步骤 4 执行命令 **8021p-inbound 6 phb cs7 green**，配置 802.1p 优先级为 6 的报文映射到 CS7 队列。

完成上述操作后，语音未再出现断断续续现象。

----结束

案例总结

在配置 DiffServ 域时，应格外注意报文优先级与队列的对应关系。

PQ 调度和 WRR/DRR 调度各有优缺点。单纯采用 PQ 调度时，低优先级队列中的报文长期得不到带宽，而单纯采用 WRR/DRR 调度时低延时需求业务得不到优先调度。因此，对于业务多样的场合，最好采用 PQ+WRR 或 PQ+DRR 混合调度模式。

11 可靠性类

关于本章

11.1 Smart Link 和 Monitor Link 故障处理
介绍了 Smart Link 和 Monitor Link 常见故障的定位思路。

11.2 VRRP 故障处理
介绍了 VRRP 常见故障原因、诊断流程、处理步骤、相关告警与日志。

11.3 Eth_OAM 故障处理
介绍了 Eth_OAM 常见故障的定位思路。

11.4 Y1731 问题
介绍了 Y1731 常见故障原因、诊断流程、处理步骤、相关告警与日志。

11.5 BFD 故障处理
介绍了 BFD 常见故障案例。

11.6 DLDP 故障处理
介绍了 DLDP 常见故障原因、诊断流程、处理步骤、相关告警与日志。

11.7 RRPP 故障处理

11.8 SEP 问题
介绍了 SEP 常见故障原因、诊断流程、处理步骤、相关告警与日志。

11.1 Smart Link 和 Monitor Link 故障处理

介绍了 Smart Link 和 Monitor Link 常见故障的定位思路。

11.1.1 Smart Link 主备链路切换失败故障的定位思路

介绍 Smart Link 主备链路切换失败的故障原因、处理流程和详细的故障处理步骤。

常见原因

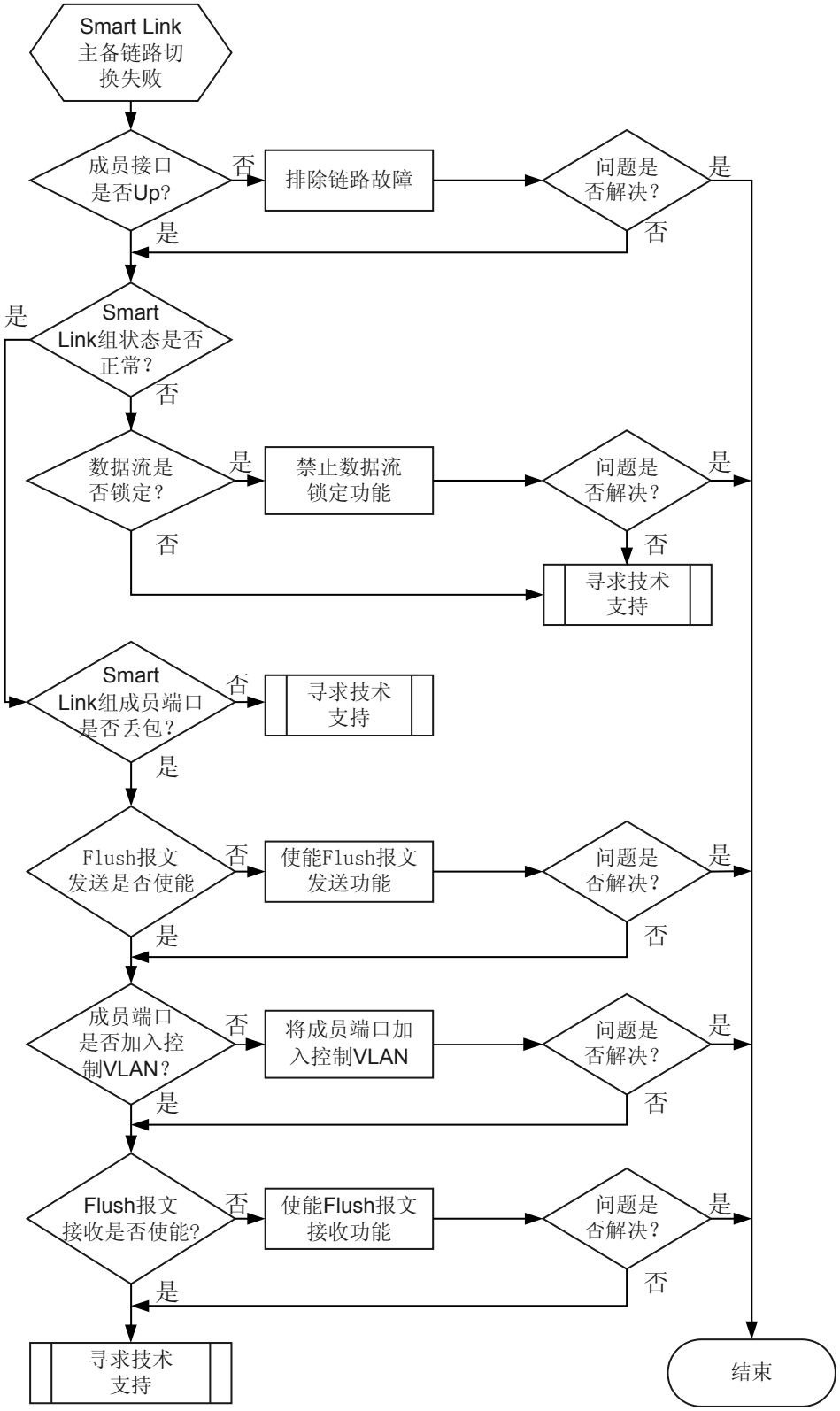
本类故障的常见原因主要包括：

- Smart Link 组的配置不正确，如：未使能 Smart Link 组、成员端口未加入业务 VLAN 等。
- 链路故障。
- 使能了 Smart Link 组数据流锁定功能。
- Flush 报文收发异常。

故障诊断流程

详细处理流程如图 **11-1** 所示。

图 11-1 Smart Link 主备链路切换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 查看 Smart Link 组成员端口的状态。

执行 **display interface** *interface-type interface-number* 命令，通过字段 current state，查看端口的状态。

- 如果显示信息中接口的 current state 为 Down，请先根据**以太网接口 DOWN 的定位思路**排除接口 Down 的故障。
- 如果显示信息中接口的 current state 为 Up,说明接口状态正常，请执行步骤 2。

步骤 2 检查 Smart Link 组状态。

执行 **display smart-link group** { **all** | *group-id* }命令，通过显示信息中的 State 字段查看 Smart Link 组的状态信息。

- 如果显示信息中一个端口的为 Active，另一个端口为 Inactive，说明 Smart Link 组的状态正常，请执行步骤 4。
- 如果 Smart link 组状态不正常，请执行步骤 3。

步骤 3 查看是否使能了 Smart Link 组数据流锁定功能。

执行 **display smart-link group** *group-id* 命令，通过 Link status 字段，查看是否使能了 Smart Link 组数据流锁定功能。

- 如果显示信息中 Link status 为 lock 或者 force，说明使能了 Smart Link 组数据流锁定功能，则执行 **undo smart-link** {**force** | **lock** }命令，禁止 Smart Link 组数据流锁定功能。
- 如果显示信息中没有对应信息，说明禁止 Smart Link 组数据流锁定功能，请执行步骤 8。

步骤 4 查看 Smart Link 组成员端口的丢包情况。

常用检查端口丢包的方法如下：

执行 **ping-c** *count* **-t** *timeout* 命令，通过查看显示信息中的丢包率可知端口是否存在丢包。

说明

对于可靠性较差的网络，建议发包次数（-c）和超时时间（-t）取较大值，这样可以更加准确的得到检测信息。

- 如果端口存在丢包，请执行步骤 5。
- 如果端口没有丢包，请执行步骤 8。

步骤 5 查看是否配置发送 Flush 报文使能。

在 Smart Link 组视图下上执行 **display this** 命令，查看是否使能了发送 Flush 报文。

- 如果显示信息中没有 flush send control-vlan vlan-id，执行 **flush send** 命令使能 Smart Link 组发送 Flush 报文功能。
- 如果显示信息中有 flush send control-vlan vlan-id，请执行步骤 6。

步骤 6 查看控制 VLAN 是否已经创建，确保 Smart Link 组成员端口都加入了该控制 VLAN。

执行 **display vlan** *vlan-id* 命令。

- 如果显示信息如下，说明成员端口均加入了该控制 VLAN，请执行步骤 7。

```
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------
10   common  TG:GE0/0/3(U)     GE0/0/2(U)
```

- 如果显示信息中没有对应信息，请创建控制 VLAN，并将 Smart Link 组成员端口都加入了该控制 VLAN。

步骤 7 在 Smart Link 组的对端设备上查看是否配置了 Flush 报文接收使能。

在接口视图下执行 **display this** 命令。

- 如果显示信息中有 smart-link flush receive control-vlan vlan-id，说明已使能 Flush 报文接收，请执行步骤 8。
- 如果显示信息中没有对应信息,说明未使能 Flush 报文接收，请执行 **smart-link flush receive** 命令使能接收 Flush 报文功能。

步骤 8 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。
- Smart Link 组设备上的 MAC 表项。

----结束

相关告警与日志

相关告警

无

相关日志

无

11.1.2 Monitor Link 组状态异常的定位思路

介绍 Monitor Link 组状态异常的原因、处理流程和详细的故障处理步骤。

常见原因

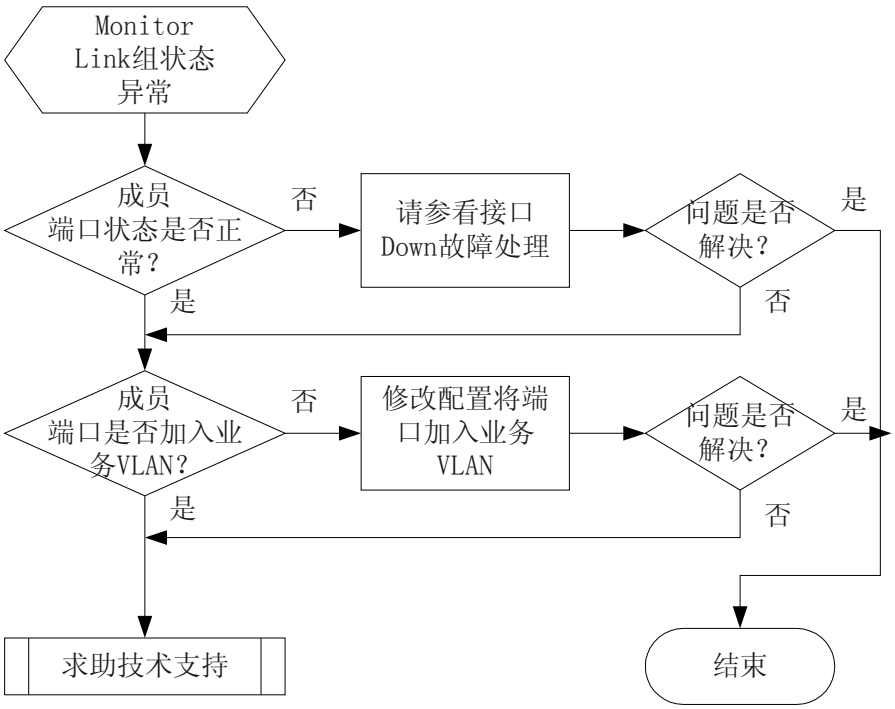
本类故障的常见原因主要包括：

- 链路故障。
- 成员端口未加入业务 VLAN。
- 下行端口被人为 shutdown。

故障诊断流程

详细处理流程如图 11-2 所示。

图 11-2 Monitor Link 组状态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 查看 Monitor Link 组成员接口的状态是否正常。

执行 **display monitor-link group** *group-id* 命令，查看 **State** 字段。

- 如果接口的 **state** 字段为 DOWN，请先根据以太网接口 DOWN 的定位思路排除接口 Down 的故障。

  说明

  上行端口出现故障包括链路故障、OAM 的单通故障、OAM 的连接无法建立等。如果上行端口是 Smart Link 组时，Smart Link 组使能情况下两个端口没有一个是 active 状态或者 Smart Link 组没有使能情况下两个端口都为 Down，才能认为该上行端口故障。

- 如果接口的 **state** 字段为 UP，请执行步骤 2。

步骤 2 查看成员接口是否加入了业务 VLAN。

在成员接口视图下执行 **display current-configuration interface** *interface-type interface-number* 命令，查看成员接口是否加入了业务 VLAN。

- 如果接口没有加入业务 VLAN，请将接口加入业务 VLAN。
- 如果接口已经加入了业务 VLAN，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

11.2 VRRP 故障处理

介绍了 VRRP 常见故障原因、诊断流程、处理步骤、相关告警与日志。

11.2.1 VRRP 备份组震荡的故障定位思路

介绍 VRRP 备份组震荡故障的原因、处理流程和详细的故障处理步骤。

常见原因

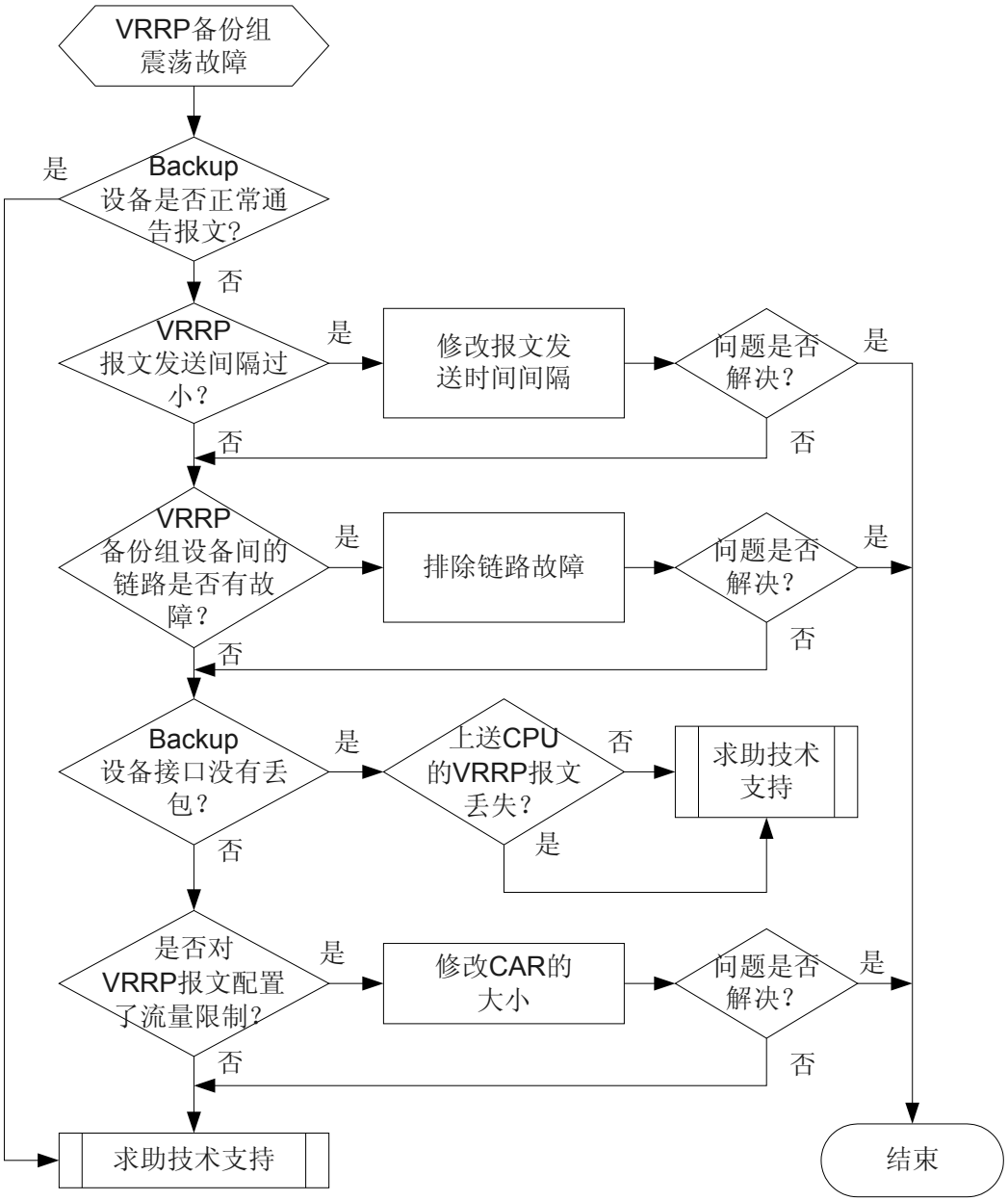
本类故障的常见原因主要包括：

- 传输 VRRP 通告报文的链路震荡。
- 通告报文的发送时间间隔过小。
- Backup 设备接口丢包。
- 报文拥塞导致 VRRP 报文被随机过滤掉。

故障诊断流程

详细处理流程如**图 11-3** 所示。

图 11-3 VRRP 备份组震荡的故障诊断流程图



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 查看 Backup 设备是否接收到了 VRRP 通告报文。

在 Backup 设备上执行 **debugging vrrp packet** 命令，查看是否有如下显示信息。

```
*Aug 27 19:45:04 2009 Quidway VRRP/7/DebugPacket:
Vlanif45 | Virtual Router 45:receiving from 45.1.1.4, priority = 100,timer = 1,
auth type is no, SysUptime: (0,121496722)
```

默认情况下，Master 设备都是 1 秒发送 1 个通告报文。

- 如果 Backup 设备不能收到通告报文，请执行步骤 2。
- 如果 Backup 设备能够收到通告报文，请执行步骤 6。

步骤 2 查看是否由于 VRRP 通告报文发送间隔时间设置过小。

执行 **vrrp vrid timer advertise** 命令，将 VRRP 报文发送间隔时间调大后在 Backup 设备上重复执行 **display vrrp** 命令查看 **State** 字段，显示信息一直保持不变说明 Backup 设备的状态稳定。

- 如果 Backup 的状态稳定，说明可能由于时间间隔过小导致 Backup 设备的状态的震荡。
- 如果 Backup 的状态不稳定，请将时间间隔恢复后执行步骤 3。

步骤 3 查看 VRRP 备份组设备间的链路是否有故障。

反复执行 **ping** 命令查看同一 VRRP 备份组实地址是否能 ping 通。

- 如果 ping 不通，请先根据 **ping 不通问题的定位思路**排除链路的故障。
- 如果时断时通，说明可能存在环路，需要进行相关环路检查。
- 如果一直都能 ping 通，请执行步骤 4。

步骤 4 查看 Backup 设备接口是否有丢包。

常用检查端口丢包的方法如下：

说明

在执行 **display interface** 命令前，需要先使用 **reset counters interface** 命令清除当前端口的统计信息。

执行 **display interface** *interface-type interface-number* 命令，通过查看端口显示信息 Input 和 Output 中的 Discard 字段可知端口是否存在丢包。

- 如果端口存在丢包现象，请执行步骤 5。
- 如果端口没有丢包，请执行步骤 7。

步骤 5 查看接口板是否对 VRRP 报文配置了流量限制。

执行 **display cpu-defend** [*packet-type*]**configuration** { **all** | **slot** *slot-id* }命令，查看是否存在如下显示信息：

```
-------------------------------------------------------------------
Packet Name                 Status       Cir(Kbps)    Cbs(Byte)    Queue
-------------------------------------------------------------------
vrrp                        Enabled            64        10000        2
```

默认情况下，Cir 为 64kbit/s，所以默认支持 100 个左右的 VRRP 备份组。

- 如果超过了这个规格，请执行 **car** 命令来修改 CAR 的大小。
- 如果没有超过这个规格，请执行步骤 7。

步骤 6 查看上送 CPU 的 VRRP 报文是否丢失。

执行 **display cpu-defend statistics slot** *slot-id* 命令，查看上送 CPU 的 VRRP 报文是否丢失。

- 如果显示信息中的 Drop(Packets)字段不为 0，说明上送 CPU 的 VRRP 报文丢失，请将结果记录并执行步骤 7。

- 如果显示信息中的 Drop(Packets)字段为 0，说明上送 CPU 的 VRRP 报文没有丢失，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

11.2.2 VRRP 备份组出现双主现象的定位思路

介绍 VRRP 备份组出现双主现象的故障原因、处理流程和详细的故障处理步骤。

常见原因

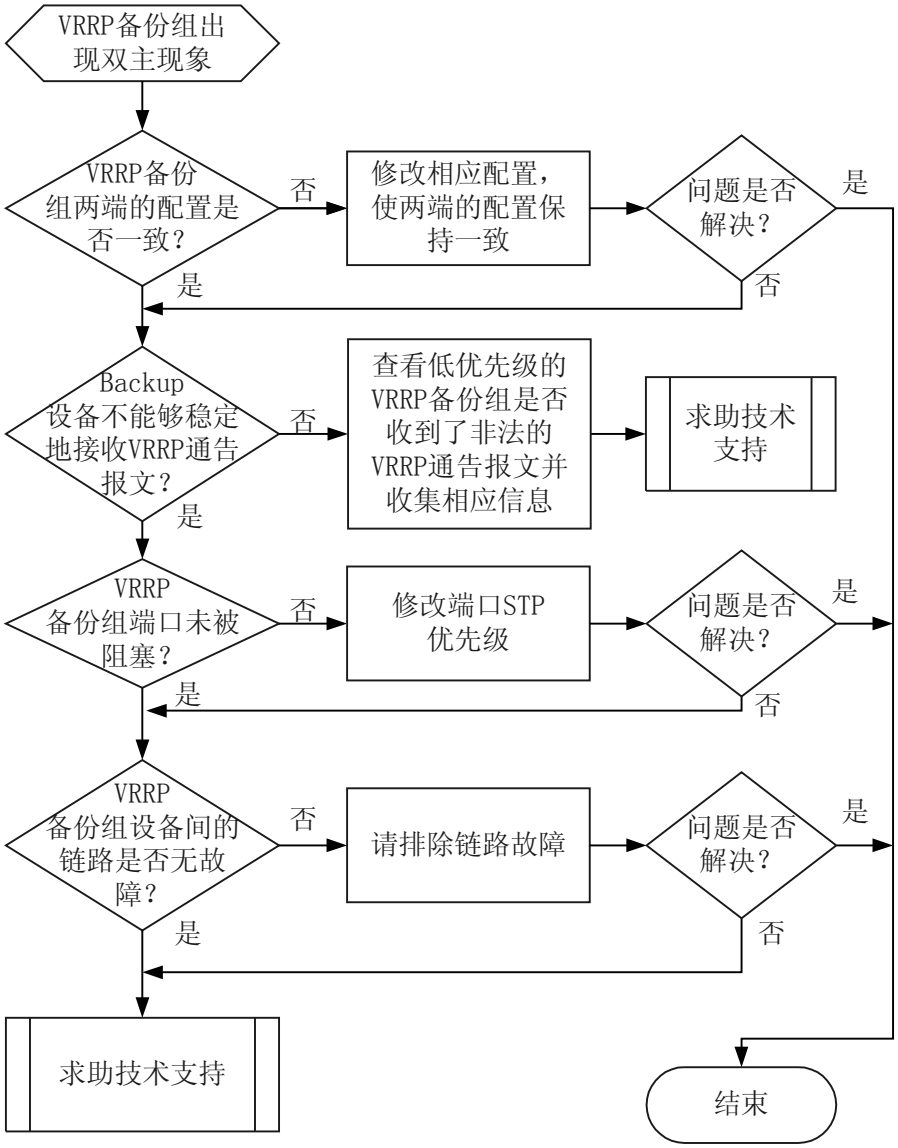
本类故障的常见原因主要包括：

- 两端的 VRRP 备份组配置不一致。
- 传输 VRRP 通告报文的链路故障。
- 链路形成环路。
- 低优先级的 VRRP 备份组将收到的 VRRP 通告报文作为非法报文被丢弃。

故障诊断流程

详细处理流程如图 11-4 所示。

图 11-4 VRRP 备份组出现双主现象故障诊断流程图



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 VRRP 备份组两端的配置是否一致。

在配置 VRRP 备份组两端的 VLANIF 接口上，执行 **display this** 命令，查看备份组两端的如下配置。

显示信息	判断及处理方法
ip address	接口 IP 地址是否在同一网段，如果 IP 地址不在同一网段，请执行 **ip address** 来修改配置。
vrid	接口上的备份组 ID 是否相同，如果不同请执行 **vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address* 命令修改配置。
Virtual IP	VRRP 组的虚拟 IP 地址是否相同，如果不同请执行 **vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address* 命令修改配置。
TimerRun	VRRP 中通告报文时间间隔是否相同，如果不同请执行 **vrrp vrid** *virtual-router-id* **timer advertise** *adver-interval* 命令修改配置。
Auth Type	VRRP 报文认证方式是否相同，如果不同请执行 **vrrp vrid** *virtual-router-id* **authentication-mode** { **simple** *key* | **md5** *md5-key* }命令修改配置。

- 如果两端配置一致，请执行步骤 2。

步骤 2 查看 Backup 设备是否能够收到 VRRP 通告报文。

打开 Backup 设备的 debug 开关，查看是否有如下显示信息。

```
*Aug 27 19:45:04 2010 Quidway VRRP/7/DebugPacket:
Vlanif45 | Virtual Router 45:receiving from 45.1.1.4, priority = 100,timer = 1,
auth type is no, SysUptime: (0,121496722)
```

默认情况下 Master 设备都是 1 秒发送 1 个通告报文。

- 如果 Backup 设备不能收到通告报文，请执行步骤 3。
- 如果 Backup 设备能够收到通告报文，请执行步骤 5。

步骤 3 在配置 VRRP 备份组两端设备及传输 VRRP 通告报文的所经过的设备上，检查是否有端口被阻塞。

执行 **display stp brief** 命令，查看 **STP State** 字段。

- 如果 **STP State** 字段的值为 **FORWARDING**，说明端口没有被阻塞，请执行步骤 4。
- 如果 **STP State** 字段的值为 **DISCARDING**，说明端口被阻塞，请修改端口 STP 优先级以保证互连端口能够正常进行 VRRP 协议报文转发。

步骤 4 执行 **ping** 命令查看 VRRP 备份组设备间的链路是否有故障。

- 如果 ping 不通，请先根据 **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 6。

步骤 5 查看低优先级的 VRRP 备份组是否收到了非法的 VRRP 通告报文。

执行 **display vrrp statistics** 命令，查看 **Received invalid type packets** 字段，将收集到的信息记录并执行步骤 6。

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

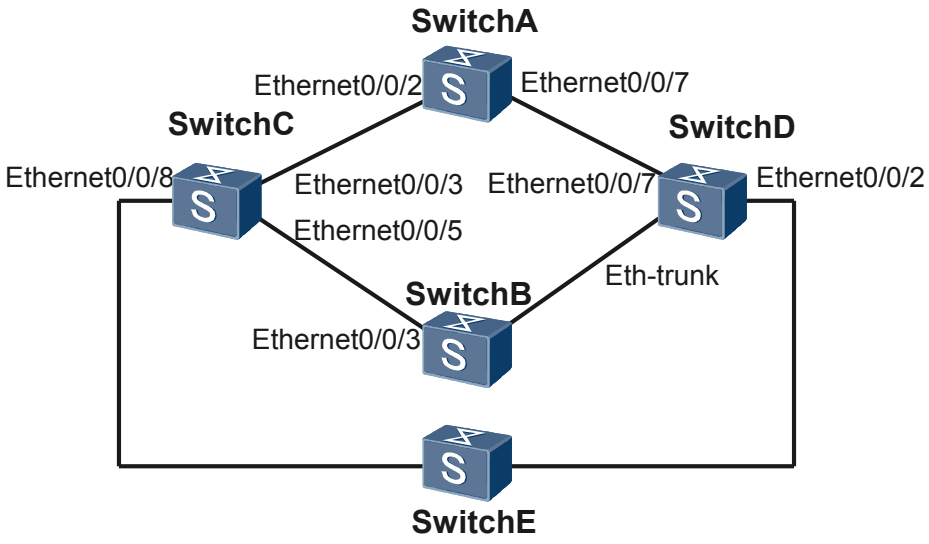
11.2.3 故障案例

VRRP 环境中数据包丢失

网络环境

在如图 11-5 所示的网络中，部署了 VRRP 业务，SwitchA 和 SwitchB 分别作为 VRRP 备份组的 Master 和 Backup 设备，SwitchC 作为交换机连接 SwitchA 和 SwitchB。

图 11-5 VRRP 组网图



配置完成后，发现从 SwitchE 发往 SwitchD 的设备出现了严重丢包。

故障分析

1. 依次在 SwitchA 和 SwitchB 上执行 **display vrrp** [**interface** *interface-type interface-number*] [*virtual-router-id*] **statistics** 命令，检查 VRRP 备份组主备设备的接口 GE0/0/2 和接口 GE0/0/3 的流量状态。发现 Master 设备 SwitchA 的 GE0/0/2 接口有少量流量，Backup 设备 SwitchB 的 GE0/0/3 接口没有流量。

   在 SwitchC 上执行 **display interface-statistics** *interface-type interface-number* 命令，检查 SwitchC 接口 GE0/0/4、GE0/0/3、GE0/0/5 的流量状态，发现 GE0/0/3 和

GE0/0/5 的流量状态和 SwitchA 的 GE0/0/2、SwitchB 的 GE0/0/3 流量状态一致，但 GE0/0/4 有大量流量。说明流量在 SwitchC 发生丢失。

2. 在 SwitchC 上执行 **display mac-address dynamic** 命令，检查 MAC 表项，发现学到的 SwitchA 的 MAC 地址是从 GE0/0/4 发出去的，而连接主、备设备的出接口分别是 GE0/0/3 和 GE0/0/5，MAC 地址表项错误。如下：

```
MAC address table of slot 0:
-------------------------------------------------------------------------------
MAC Address    VLAN/       PEVLAN CEVLAN Port            Type      LSP/
               VSI/SI                                              MAC-Tunnel
-------------------------------------------------------------------------------
0000-0a0a-0102 1           -      -      GigabitEthernet0/0/4        dynamic
-
0000-5e00-0101 1           -      -      GigabitEthernet0/0/4        dynamic
-
0098-0113-0005 1           -      -      GigabitEthernet0/0/4        dynamic
-
0018-824f-f5d1 1           -      -      GigabitEthernet0/0/3        dynamic
-
-------------------------------------------------------------------------------
```

3. 在 SwitchC 上执行 **display current-configuration interface** *interface-type interface-number* 命令，查看 GE0/0/4 的配置。如下：

```
#
 interface GigabitEthernet0/0/4
  undo shutdown
  loopback internal
  portswitch
  port default vlan 1
```

看出 GE0/0/4 接口配置了环回，即发往 GE0/0/4 接口的流量会原样返回。

4. 在 SwitchC 上执行 **display interface-statistics** *interface-type interface-number* 命令，查看 GE0/0/3、GE0/0/4、GE0/0/5 接口的流量，发现 GE0/0/4 有大量流量。判断是由于该端口的配置导致流量丢失。但是 GE0/0/3 也有少量流量通过。

5. 在 SwitchC 上多次执行 **display mac-address dynamic** 命令，检查 MAC 表项，交换机不同时间学到的 MAC 地址不同。如下：

```
[SwitchC] display mac-address dynamic
MAC address table of slot 0:
-------------------------------------------------------------------------------
MAC Address    VLAN/       PEVLAN CEVLAN Port            Type      LSP/
               VSI/SI                                              MAC-Tunnel
-------------------------------------------------------------------------------
0000-0a0a-0102 1           -      -      GigabitEthernet0/0/4        dynamic
-
0000-5e00-0101 1           -      -      GigabitEthernet0/0/4        dynamic
-
0098-0113-0005 1           -      -      GigabitEthernet0/0/5        dynamic
-
0018-824f-f5d1 1           -      -      GigabitEthernet0/0/4        dynamic
-
-------------------------------------------------------------------------------
Total matching items on slot 0 displayed = 4
[SwitchC] display mac-address dynamic
MAC address table of slot 0:
-------------------------------------------------------------------------------
MAC Address    VLAN/       PEVLAN CEVLAN Port            Type      LSP/
               VSI/SI                                              MAC-Tunnel
-------------------------------------------------------------------------------
0000-0a0a-0102 1           -      -      GigabitEthernet0/0/4        dynamic
-
0000-5e00-0101 1           -      -      GigabitEthernet0/0/3        dynamic
-
0098-0113-0005 1           -      -      GigabitEthernet0/0/5        dynamic
-
0018-824f-f5d1 1           -      -      GigabitEthernet0/0/4        dynamic
```

```
-
--------------------------------------------------------------------------------
Total matching items on slot 0 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 Backup 设备不发送 VRRP 通告报文。

说明

配置的时候如果有一台设备的 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。GE0/0/4 属于 VLAN 1，也会收到交换机发送的 VRRP 通告报文。由于 GE0/0/4 配置了端口环回功能，报文会从 GE0/0/4 原封不动的返回，这样就会在 MAC 表中记录 GE0/0/4 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。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入 GE0/0/4 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。

11.3 Eth_OAM 故障处理

介绍了 Eth_OAM 常见故障的定位思路。

11.3.1 以太 OAM 802.1ag MAC Trace 不通定位思路

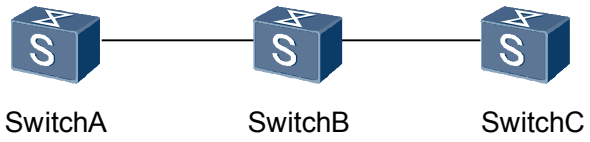
介绍以太 OAM 802.1ag MAC Trace 不通的故障原因、处理流程和详细的故障处理步骤。

常见原因

如图 11-6 所示，SwitchA 基于 802.1ag 的 MAC Trace SwitchC 不通：

```
[SwitchA-md-1-ma-1] trace mac-8021ag mac 0018-823c-c449
Tracing the route to 0018-823c-c449 over a maximum of 64 hops:
Request timed out.
```

图 11-6 以太 OAM 802.1ag MAC Trace 不通故障组网图

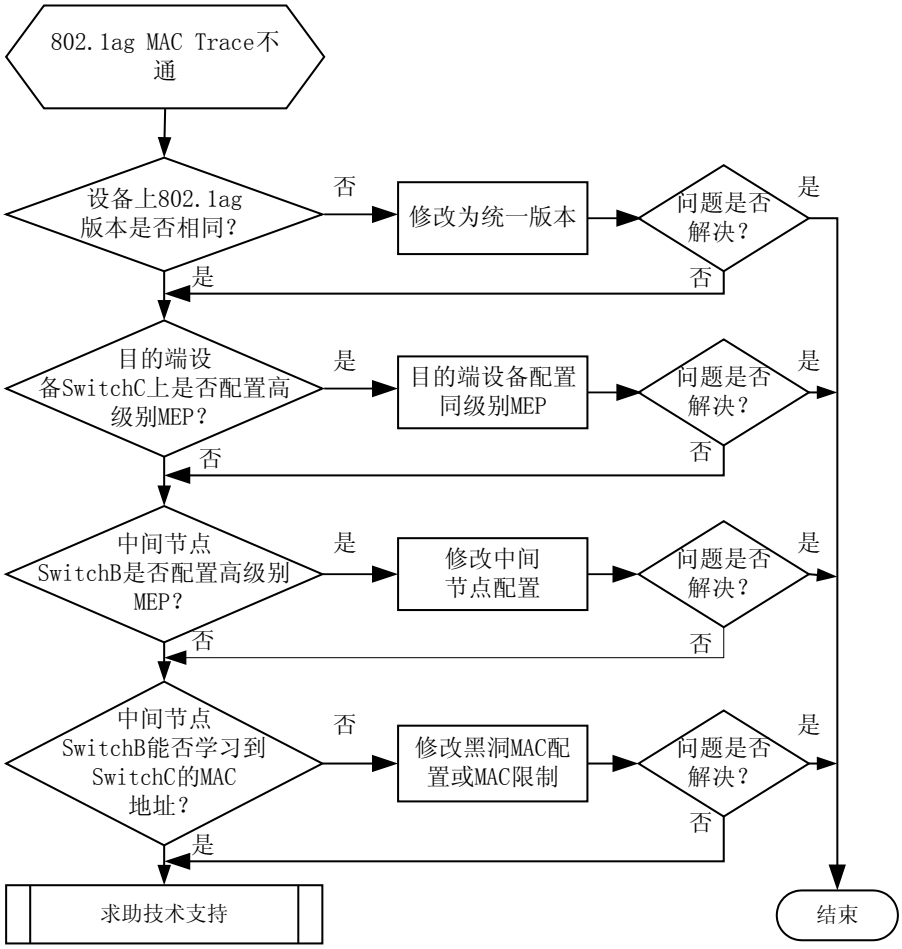


本类故障的常见原因主要包括：

- 目的节点 SwitchC 上没有配置和 SwitchA 同级别的 MEP。
- 中间节点上存在和 SwitchA 同级别或比 SwitchA 高级别的 MEP。
- 中间节点没有到目的节点 SwitchC 的 MAC 表项。

故障诊断流程

图 11-7 以太网 OAM 802.1ag MAC Trace 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。

以下操作步骤请在故障产生节点和故障点下游的 MEP 或 MIP 上执行。

操作步骤

步骤 1 执行 **display oam global configuration** 命令查看 Trace 路径上各设备的 802.1ag 版本是否相同。

- 如果 Trace 路径上各设备 1ag 版本相同，则执行步骤**步骤 2**。
- 如果 Trace 路径上各设备 1ag 版本不相同，执行 **cfm version** 命令配置设备的 1ag 版本，实现以太网 CFM 802.1ag 协议的 draft7 草案版本和 standard2007 标准版本之间进行切换。

注意

切换版本后，原来的 CFM 的所有配置将被删除，请谨慎使用。

  - 如果 SwitchA 基于 802.1ag 的 MAC Trace Switch 成功，故障排除。
  - 否则执行步骤**步骤 2**。

步骤 2 在目的节点和源节点的 MD 视图下，执行 **display this** 命令查看目的节点是否与源节点配置同级别 MEP。

- 如果目的节点与源节点配置 MEP 级别相同，则执行步骤**步骤 3**。
- 如果目的节点与源节点配置 MEP 级别不相同，请删除原来的 MD，执行 **cfm md** 命令创建新的 MD 并配置目的节点的 MEP 级别，保持与源节点 MEP 级别一致。
  - 如果 SwitchA 基于 802.1ag 的 MAC Trace SwitchC 成功，则故障排除。
  - 否则执行步骤**步骤 3**。

步骤 3 执行 **display cfm mep** 命令查看中间节点上是否配置同级别或高级别 MEP。

说明

低级别 MD 的 802.1ag 协议报文进入高级别的 MD 后被丢弃，高级别 MD 的 802.1ag 协议报文可以穿越低级别的 MD。相同级别的 MD 的 802.1ag 协议报文不能彼此穿越。

- 如果中间节点上不存在同级别或高级别 MEP，则执行步骤**步骤 4**。
- 如果中间节点上存在同级别或高级别 MEP，请删除原来的 MD，执行 **cfm md** 命令创建新的 MD，并配置中间节点的 MEP 级别。
  - 如果 SwitchA 基于 802.1ag 的 MAC Trace SwitchC 成功，则故障排除。
  - 否则执行步骤**步骤 4**。

步骤 4 执行 **display mac-address dynamic** [*slot-id*] [*interface-type interface-number* | **vlan** *vlan-id*]命令查看中间节点是否有到目的节点的 MAC 表项。

- 如果中间节点存在到目的节点的 MAC 表项，则执行步骤**步骤 5**。

- 如果中间节点不存在到目的节点的 MAC 表项，则执行 **ping mac-8021ag** 命令让中间节点学习到目的节点 SwitchC 的 MAC 表项。
  - 如果 SwitchA 基于 802.1ag 的 MAC Trace SwitchC 成功，则故障排除。
  - 否则执行步骤**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

EOAM1AG_1.3.6.1.4.1.2011.5.25.136.1.6.1 hwCfmFaultAlarm

相关日志

EOAM1AG/0/ALARM_CONFIG_ERR

EOAM1AG/3/DEL_MD_ERR

11.4 Y1731 问题

介绍了 Y1731 常见故障原因、诊断流程、处理步骤、相关告警与日志。

11.4.1 VLAN 组网下单向时延统计没有统计数据的定位思路

介绍 VLAN 组网下单向时延统计时没有统计数据的故障原因、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：

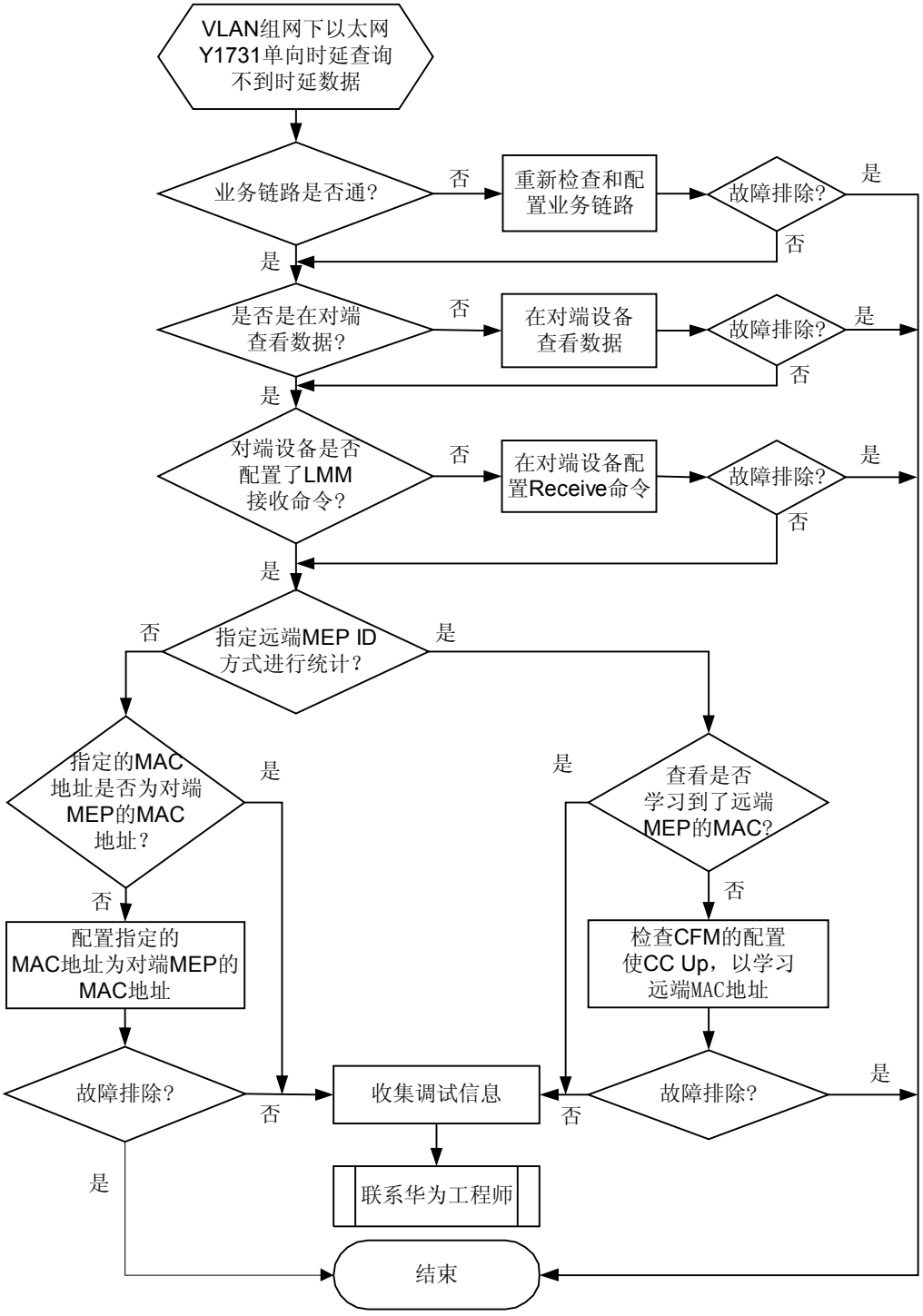
- 业务链路不通。
- 不是在对端设备查看数据。
- 对端设备没有配置 Receive 命令。
- 通过指定远端 MEP ID 方式进行单向时延统计时，没有学习到远端 MEP 的 MAC 地址。
- 通过指定对端 MAC 地址方式进行单向时延统计时，指定的 MAC 地址不是对端 MEP 的 MAC 地址。

故障诊断流程

VLAN 组网下，在配置单向时延统计功能后，发现无时延统计数据。

详细的处理流程如**图 11-8** 所示。

图 11-8 VLAN 组网单向时延无统计数据故障诊断流程图



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 检查业务链路是否正常。

执行 **display vlan** *vlan-id* **verbose** 命令，查看“VLAN state”的值。

- 如果“VLAN state”的值为 Up，请执行步骤 2。
- 如果“VLAN state”的值不为 Up，请检查 VLAN 相关配置。VLAN 配置请参见《AC6605 无线接入控制器 配置指南-以太网配置》中的 VLAN 配置章节。

步骤 2 检查是否在对端设备查看数据。

单向时延统计需要在报文接收设备上查看数据，而不是在单向时延的发起端。如果在对端设备上没有查看到数据，请执行步骤 3。

步骤 3 检查远端设备是否配置了 **delay-measure one-way receive** 命令。

在对端设备上，MD 视图下执行 **display this** 命令，查看配置信息。

- 如果没有配置 **delay-measure one-way receive** 命令，请配置。
- 如果配置 **delay-measure one-way receive** 命令，请执行步骤 4。

步骤 4 检查 MEP 方向是否正确。

在对等 MEP 两端设备上执行 **display cfm mep** 命令查看“Direction”的值。

- 如果对等 MEP 两端设备上“Direction”的值为 Outward，则表示 MEP 方向配置正确，请执行步骤 5。
- 如果对等 MEP 两端设备上“Direction”的值不为 Outward，则表示 MEP 方向配置错误，请执行命令 **mep** *mep-id* **inteface** *interface-type interface-num* **outward** 重新配置 MEP 的方向。

步骤 5 检查进行单向时延统计时指定的参数。

如果指定的参数是 **remote-mep mep-id** *mep-id*，执行 **display cfm remote-mep md** *md-name* **ma** *ma-name* **mep-id** *mep-id* 命令查看“MAC”的值。是否学到了对端 MEP 的 MAC 地址。

- 如果“MAC”的值为“-”，则检查 CFM 的配置，使 CC Up，以学习对端 MEP 的 MAC 地址。
- 如果“MAC”的值不为“-”，请执行步骤 6。

如果指定的参数是 **mac** *mac-address*，查看参数 *mac-address* 是否为对端 MEP 的 MAC 地址。

- 如果 MAC 地址一致，请执行步骤 6。
- 如果 MAC 不一致，请指定对端 MEP 的 MAC 地址进行单向时延统计。

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

无

11.4.2 VLAN 组网下双向时延统计没有统计数据的定位思路

介绍 VLAN 组网下双向时延统计时没有统计数据的故障原因、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：

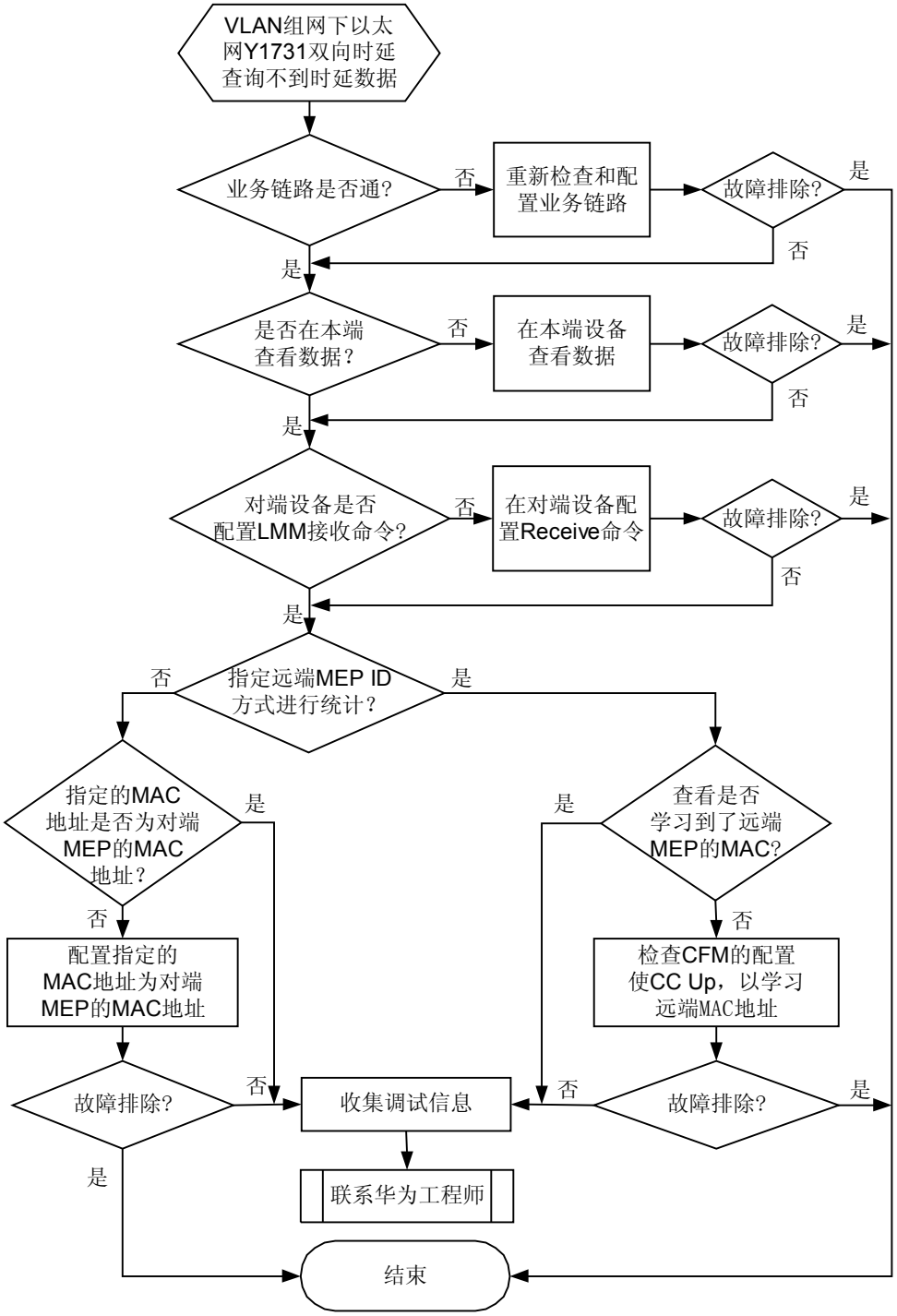
- 业务链路不通。
- 不是在本端设备查看数据。
- 对端设备没有配置 Receive 命令。
- 通过指定远端 MEP ID 方式进行双向时延统计时，没有学习到远端 MEP 的 MAC 地址。
- 通过指定对端 MAC 地址方式进行双向时延统计时，指定的 MAC 地址不是对端 MEP 的 MAC 地址。

故障诊断流程

VLAN 组网下，在配置双向时延统计功能后，发现无时延统计数据。

详细的处理流程如图 **11-9** 所示。

图 11-9 VLAN 组网双向时延无统计数据故障诊断流程图



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 检查业务链路是否正常。

执行 **display vlan** *vlan-id* **verbose** 命令，查看“VLAN state”的值。

- 如果“VLAN state”的值为 Up，请执行步骤 2。
- 如果“VLAN state”的值不为 Up，则请检查 VLAN 相关配置。VLAN 配置请参见《AC6605 无线接入控制器 配置指南-以太网》中的 VLAN 配置章节。

步骤 2 检查是否在本端设备查看数据。

双向时延统计需要在时延发起设备上查看数据。如果在本端设备上没有查看到数据，请执行步骤 3。

步骤 3 检查远端设备是否配置了 **delay-measure two-way receive** 命令。

在对端设备上，MD 视图下执行 **display this** 命令，查看配置信息。

- 如果没有配置 **delay-measure two-way receive** 命令，请配置。
- 如果配置 **delay-measure two-way receive** 命令，请执行步骤 4。

步骤 4 检查 MEP 方向是否正确。

在对等 MEP 两端设备上执行 **display cfm mep** 命令查看“Direction”的值。

- 如果对等 MEP 两端设备上“Direction”的值为 outward，则表示 MEP 方向配置正确，请执行步骤 5。
- 如果对等 MEP 两端设备上“Direction”的值不为 Outward，则表示 MEP 方向配置错误，请执行命令 **mep** *mep-id* **interface** *interface-type interface-num* **outward** 重新配置 MEP 的方向。

步骤 5 检查进行双向时延统计时指定的参数。

如果指定的参数是 **remote-mep mep-id** *mep-id*，执行 **display cfm remote-mep md** *md-name* **ma** *ma-name* **mep-id** *mep-id* 命令查看“MAC”的值。是否学到了对端 MEP 的 MAC 地址。

- 如果“MAC”的值为“-”，则检查 CFM 的配置，使 CC Up，以学习对端 MEP 的 MAC 地址。
- 如果“MAC”的值不为“-”，请执行步骤 6。

如果指定的参数是 **mac** *mac-address*，查看参数 *mac-address* 是否为对端 MEP 的 MAC 地址。

- 如果 MAC 地址一致，请执行步骤 6。
- 如果 MAC 不一致，请指定对端 MEP 的 MAC 地址进行双向时延统计。

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

无

11.5 BFD 故障处理

介绍了 BFD 常见故障案例。

11.5.1 BFD 会话无法 Up 的定位思路

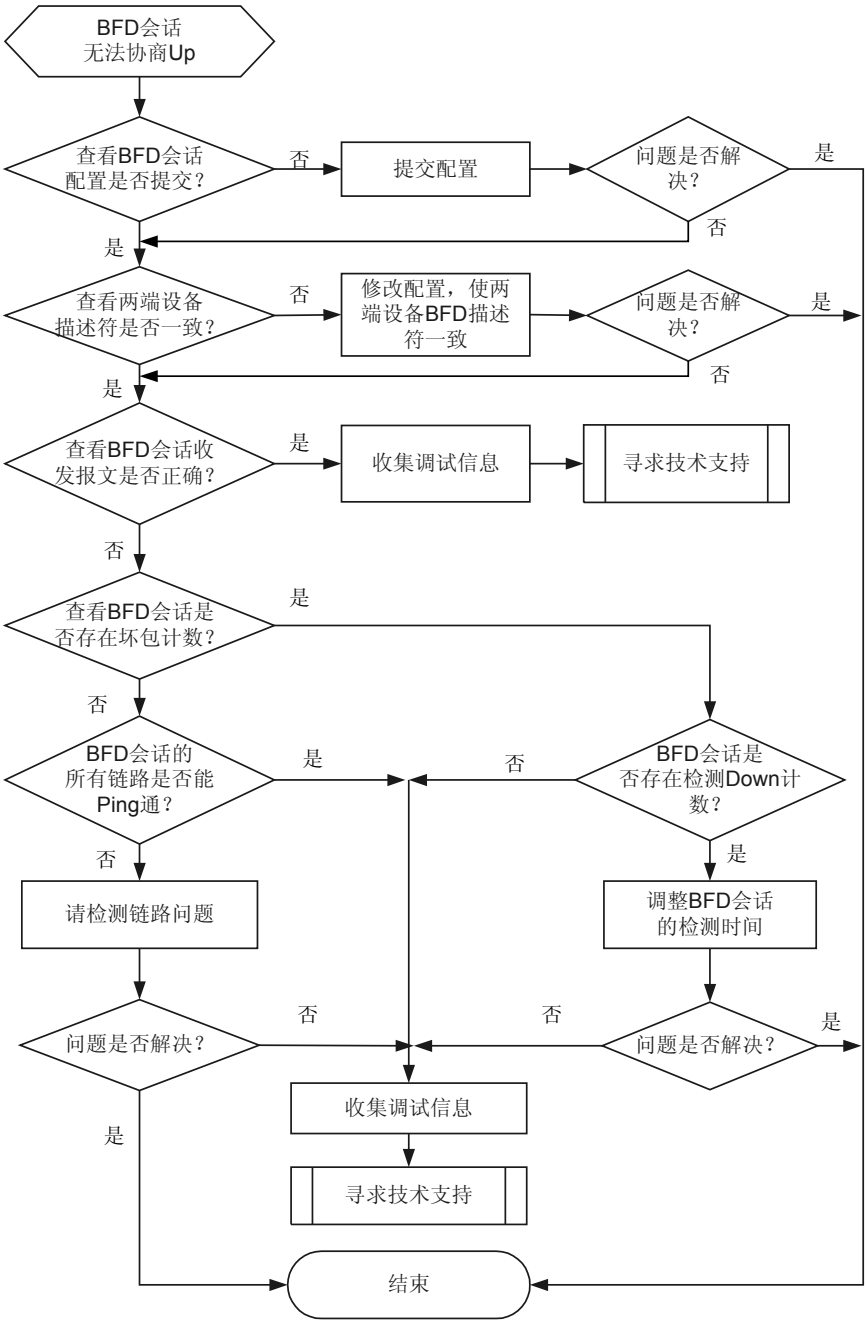
常见原因

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。

故障诊断流程

图 11-10 BFD 会话无法 Up 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** 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**。

- 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 不通问题的定位思路**排除转发故障。
- 如果能 ping 通，请检查接口下的相应配置。

  说明

  由于 BFD 报文是通过缺省 VLAN 传送的，因此在配置 BFD Session 时，需要将承载 BFD 报文的缺省 VLAN 在接口配置时允许其通过。

  - 如果接口的参数设置不正确，请修改相应配置。
  - 如果接口的参数设置正确，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

- BFD_1.3.6.1.4.1.2011.5.25.38.3.1 hwBfdSessDown
- BFD_1.3.6.1.4.1.2011.5.25.38.3.2 hwBfdSessUp

相关日志

- BFD/4/STACHG_TODWN
- BFD/4/STACHG_TOUP

11.5.2 BFD 会话检测 Down 影响接口转发的定位思路

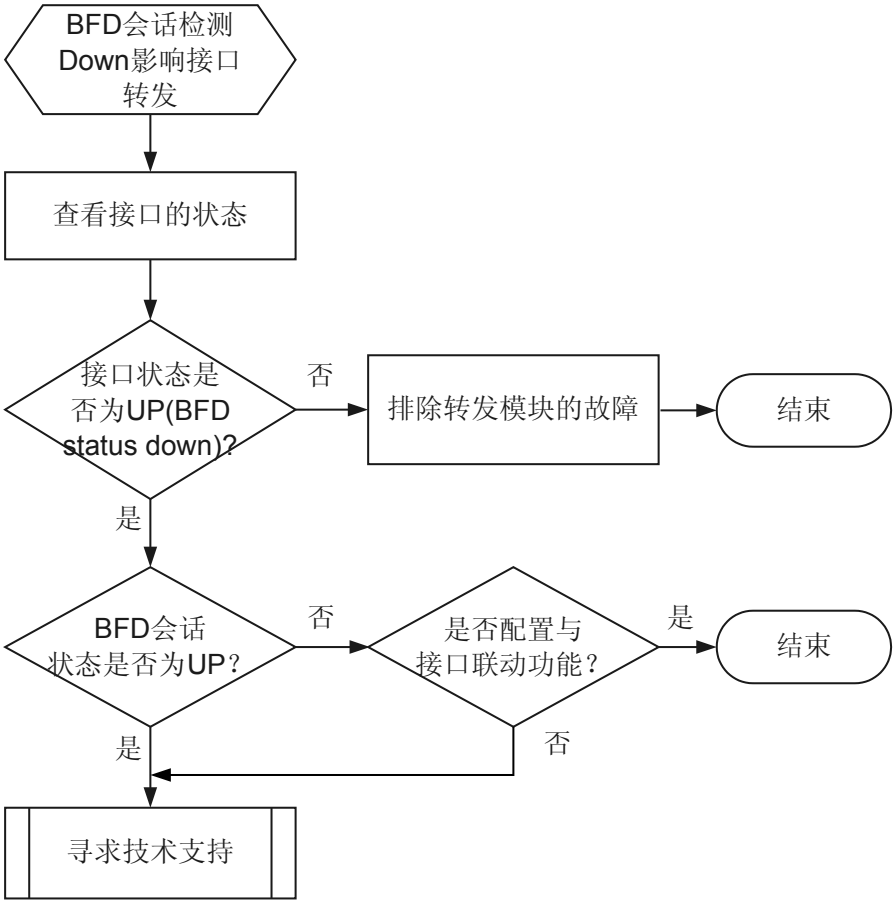
常见原因

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。

故障诊断流程

图 11-11 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 不通问题的定位思路**，排除转发模块的故障。

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

11.5.3 修改 BFD 会话检测参数不生效的定位思路

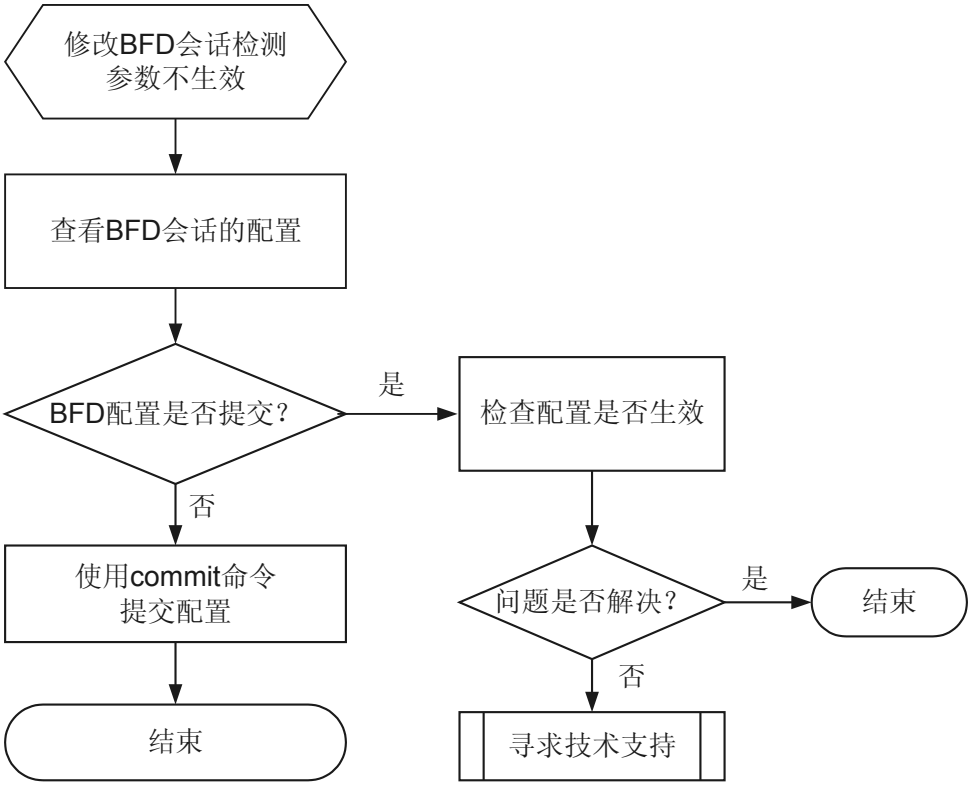
常见原因

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。

故障诊断流程

图 11-12 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**。

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

11.5.4 动态 BFD 会话没有创建成功的定位思路

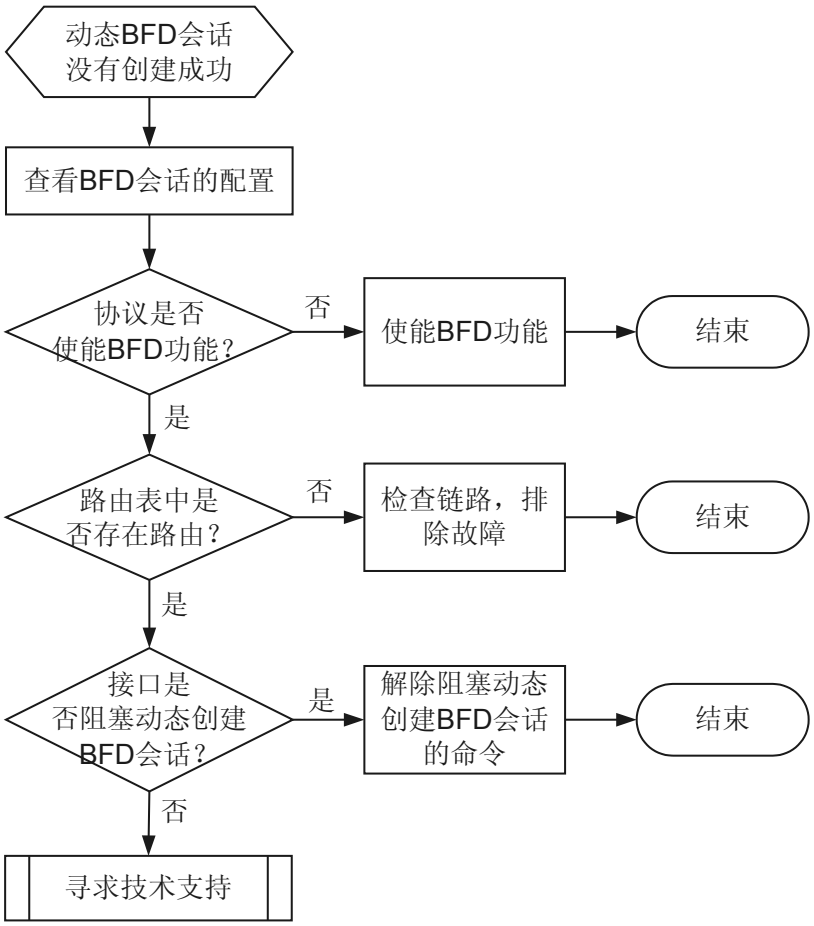
常见原因

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。

故障诊断流程

图 11-13 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。

- 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 不通问题的定位思路**，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

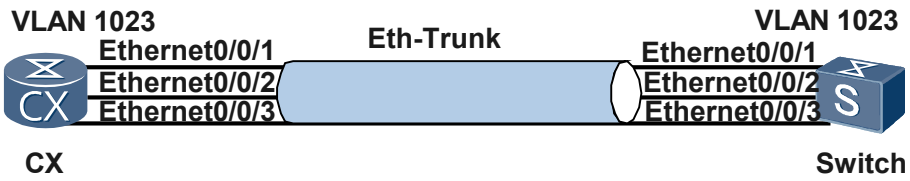
11.5.5 故障案例

接口不允许缺省 VLAN 的报文通过导致 BFD Session 一直为 Down

网络环境

在图 11-14 的网络中 CX600 和 Switch 通过以太网口 Eth-Trunk 捆绑对接静态 BFD。配置完成后，发现 BFD Session 一直为 Down。

图 11-14 接口不允许缺省 VLAN 的报文通过导致 BFD Session 无法建立的组网图



故障分析

1. 在 Switch 上执行 **display current-configuration configuration bfd-session** 命令查看 BFD 会话是否提交。检查后发现有 **commit** 字段，说明 BFD Session 已提交。
2. 在 Switch 上执行 **ping** 命令，检查网络层是否连通，发现网络层可达,说明链路本身没有故障。
3. 在 Switch 上执行 **display current-configuration interface** *interface-type interface-number* 命令，发现接口下有如下配置。

```
#
interface Eth-Trunk1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 1023
#
```

显示信息说明接口仅能通过 VLAN 1023，而 Switch 的 BFD 报文是通过缺省 VLAN 传送的，默认情况下为 VLAN 1，因此 BFD 会话无法建立。

操作步骤

- 由于接口不允许承载 BFD 的报文的缺省 VLAN 通过，可以选择修改接口上的配置使得 VLAN 1 的报文通过，或者修改接口上的 PVID 值并使得接口允许该 VLAN 的报文通过两种方法来消除故障现象。
  1. 修改接口上的配置使得 VLAN 1 的报文通过。
     a. 在 Switch 上执行命令 **system-view**，进入系统视图。
     b. 执行命令 **interface** *interface-type interface-number*，进入 Eth-trunk 视图。
     c. 执行命令 **port trunk allow-pass vlan 1**，使得接口允许 VLAN 1 的报文通过。
  2. 修改接口上的 PVID 值并使得接口允许该 VLAN 的报文通过。
     a. 在 Switch 上执行命令 **system-view**，进入系统视图。
     b. 执行命令 **interface** *interface-type interface-number*，进入 Eth-trunk 视图。
     c. 执行命令 **port trunk pvid vlan** *vlan-id*，设置接口的缺省 VLAN。
     d. 执行命令 **port trunk allow-pass vlan** *vlan-id*，使得接口允许缺省 VLAN 的报文通过。

  完成上述操作后，在 Switch 上检查 BFD 的状态，BFD Session 建立成功，故障排除。

----结束

案例总结

由于 BFD 报文是通过缺省 VLAN 传送的，因此在配置 BFD Session 时，需要将承载 BFD 报文的缺省 VLAN 在接口配置时允许其通过。

BFD Session 一直为 Down 的原因还可能是由于在配置 BFD Session 后没有提交或者是两端配置不一致，建议用户在定位故障时首先检查配置。

11.6 DLDP 故障处理

介绍了 DLDP 常见故障原因、诊断流程、处理步骤、相关告警与日志。

11.6.1 DLDP 无法发现直连邻居的故障定位思路

介绍 DLDP 无法发现直连邻居的原因、处理流程和详细的故障处理步骤。

常见原因

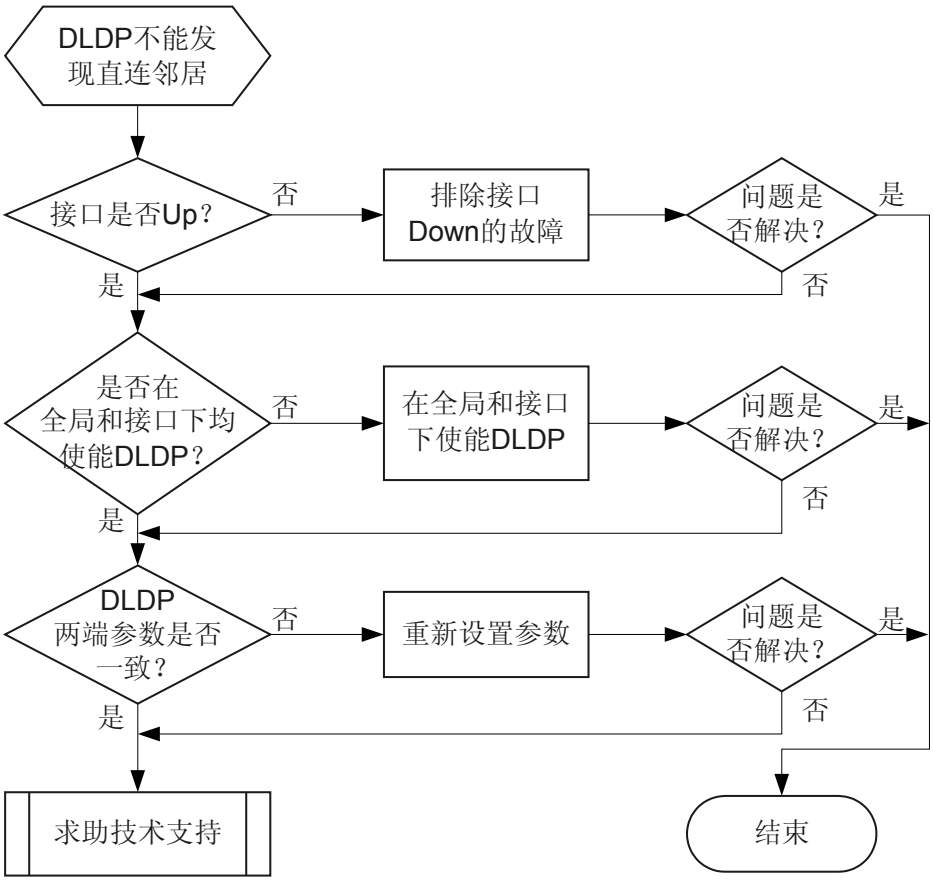
本类故障的常见原因主要包括：

- 链路故障。
- 使能了 DLDP 功能的对端设备的 DLDP 功能被去使能。
- DLDP 参数配置不一致。

故障诊断流程

详细处理流程如图 11-15 所示。

图 11-15 DLDP 无法发现直连邻居故障诊断流程图



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 检查不能发现邻居的接口状态是否正常。

执行 **display interface** *interface-type interface-name* 命令，查看 **current state** 字段。

- 如果接口的状态为 Down，请先根据**以太网接口 DOWN 的定位思路**排除接口 Down 的故障。
- 如果接口的状态为 Up，请执行步骤 2。

步骤 2 检查是否使能了 DLDP 功能。

执行 **display dldp** 命令，通过 **DLDP global status** 字段查看是否全局使能了 DLDP 功能；在接口视图下执行 **display this**，如果显示信息中有 **dldp enable** 字段，说明在接口下已经使能，如果没有对应显示信息则说明接口没有使能 DLDP 功能。

- 如果没有在全局或者接口下使能 DLDP 功能，请执行 **dldp enable** 命令在对应视图下使能 DLDP 功能。
- 如果设备已经使能了 DLDP 功能，请执行步骤 3。

步骤 3 检查 DLDP 的参数配置是否一致。

执行 **display dldp** 命令，查看下表的显示信息。

查看字段	检查方法及处理建议
DLDP interval	检查两端设备配置发送报文的时间间隔是否一致。如果两端配置不一致，请在两端设备系统视图下执行 **dldp interval** *interval-value* 命令修改配置。
DLDP authentication-mode	检查两端设备配置认证方式和认证密码是否正确。如果两端设备配置认证方式或认证密码不同，请在两端设备系统视图下执行 **dldp authentication-mode** { **md5** *cipher-value* | **none** | **simple** *cipher-value* }配置两端设备认证方式相同。

- 如果两端配置均一致，请执行步骤 3。

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

11.7 RRPP 故障处理

11.7.1 RRPP 临时环路的定位思路

常见原因

配置 RRPP 后，出现临时环路。

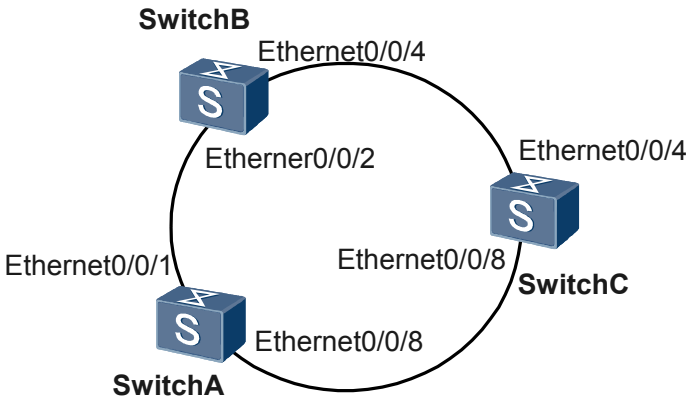
本类故障的常见原因有：

- 配置错误。
- 环上配置的 Failtime 不一致。

故障诊断流程

如图 11-16 所示，RRPP 临时环路的故障处理将基于该网络。

图 11-16 RRPP 组网图

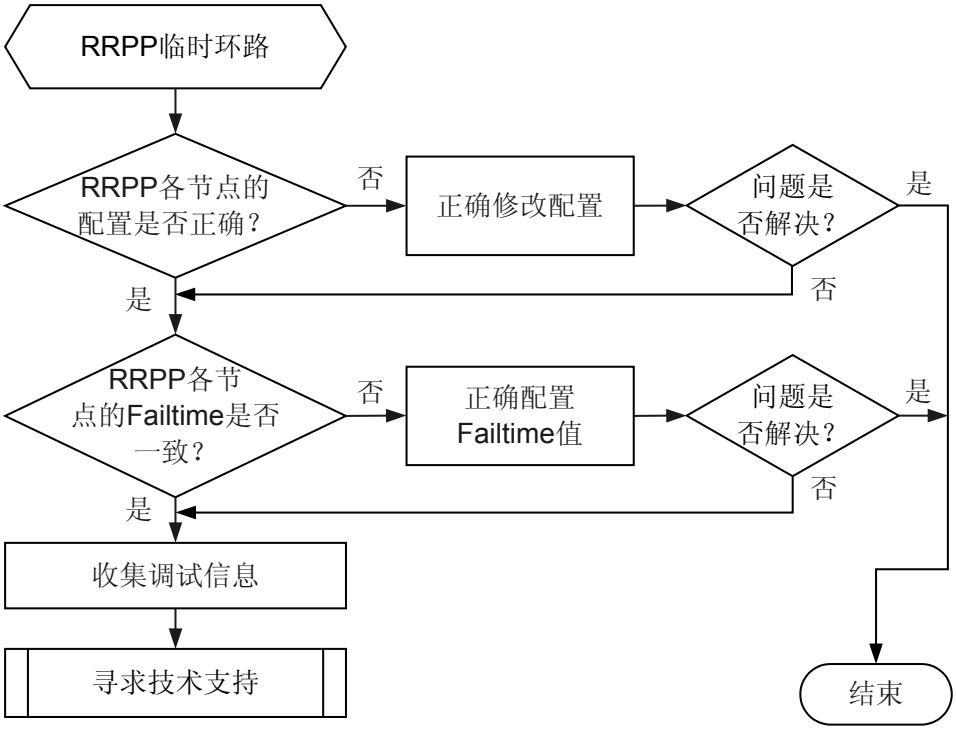


故障诊断思路：

- 检查 RRPP 各节点的配置是否正确。
- 检查 RRPP 各节点的 Failtime 定时器值设置是否一致。

可按照图 11-17 排除此类故障。

图 11-17 RRPP 临时环路故障诊断流程图



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 RRPP 环上各节点配置是否正确。

分别在 RRPP 环上各节点的 RRPP 域视图下执行命令 **display this** 查看 RRPP 相关配置。

```
[SwitchA-rrpp-domain-region1] display this
#
rrpp domain 1
 control-vlan 100
 protected-vlan reference-instance 0
 timer hello-timer 1 fail-timer 3
 ring 1 node-mode master primary-port GigabitEthernet0/0/2 secondary-port GigabitEthernet0/0/4 level
0
 ring 1 enable
#
return
```

查看 RRPP 环上各节点是否在同一个域中，创建的控制 VLAN、实例是否一致，及 RRPP 环上是否只有一个主节点。

- 如果以上配置是正确的，请执行**步骤 2**。
- 如果以上其中一项配置错误，均会导致 RRPP 配置错误，请参见《AC6605 配置指南-可靠性配置》中的 RRPP 配置章节正确配置。

步骤 2 检查 RRPP 环上各节点的 Failtime 定时器设置是否一致。

在任意视图下执行命令 **display rrpp verbose domain** *domain-id* 查看 RRPP 配置的详细信息。

```
[RouterA-rrpp-domain-region1] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 20    sub 21
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 3 sec(default is 3 sec)
RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Complete
Is Enabled    : Enable                       Is Active : Yes
Primary port  : GigabitEthernet0/0/1         Port status: UP
Secondary port: GigabitEthernet0/0/2         Port status: BLOCKED
```

- 如果 RRPP 环上各节点的 Failtime 定时器设置不一致，请参见《AC6605 配置指南-可靠性配置》中的 RRPP 配置章节正确配置。
- 如果 RRPP 环上各节点的 Failtime 定时器设置一致，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

RRPP_1.3.6.1.4.1.2011.5.25.113.4.2 hwRrppRingFail

相关日志

RRPP/3/FAIL

RRPP/5/PBLK

RRPP/5/RESTORE

11.8 SEP 问题

介绍了 SEP 常见故障原因、诊断流程、处理步骤、相关告警与日志。

11.8.1 SEP 链路流量转发不通

介绍 SEP 链路流量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

环网上配置 SEP 协议后，流量无法正常转发。

本类故障的常见原因有：

- SEP 配置错误
- 端口没有允许数据 VLAN 通过
- 物理端口故障

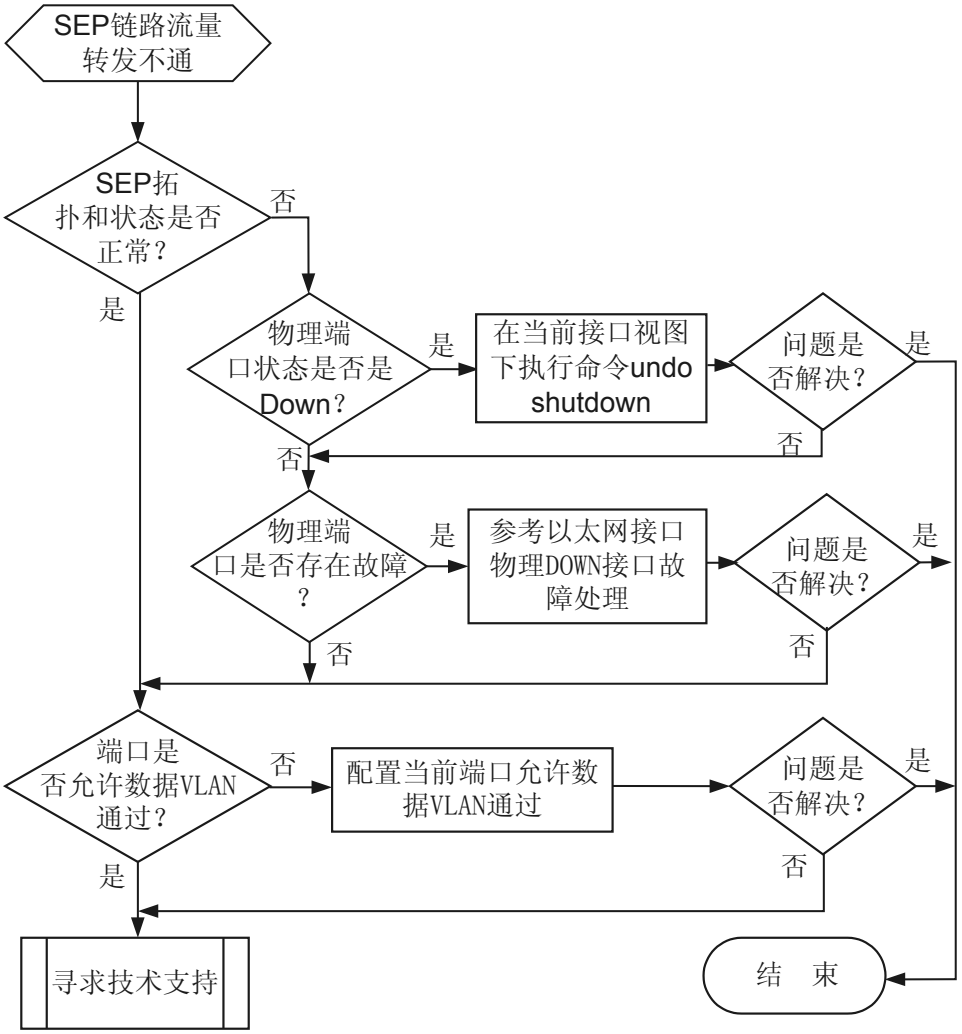
故障诊断流程

故障诊断思路：

- 检查 SEP 拓扑和状态是否正常。
- 检查环网上的端口是否已经允许数据 VLAN 通过。
- 检查环网上的物理端口状态是否是 Down。
- 检查环网上的物理端口是否存在故障。

可按照图 11-18 排除此类故障。

图 11-18 SEP 链路流量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 SEP 拓扑和状态是否正常。

正常情况下，SEP 段上的端口角色应该只有一个主边缘端口、一个副边缘端口、其他端口角色均是普通端口。

在任意视图下执行命令 **display sep topology** [**segment** *segment-id*] [**verbose**]查看 SEP 段的拓扑状态信息。

```
<Quidway> display sep topology
SEP segment 1
------------------------------------------------------------------
System Name      Port Name           Port Role       Port Status
------------------------------------------------------------------
LSW1             GigabitEthernet0/0/1       primary         forwarding
LSW2             GigabitEthernet0/0/1       common          forwarding
LSW2             GigabitEthernet0/0/2       common          forwarding
LSW3             GigabitEthernet0/0/0       common          forwarding
LSW3             GigabitEthernet0/0/2       common          discarding
LSW4             GigabitEthernet0/0/1       common          forwarding
LSW4             GigabitEthernet0/0/2       common          forwarding
LSW5             GigabitEthernet0/0/1       common          forwarding
LSW5             GigabitEthernet0/0/3       common          forwarding
LSW1             GigabitEthernet0/0/3       secondary       forwarding
```

- 如果 SEP 段的拓扑和状态不正常:
  - 请检查 SEP 配置是否正确。SEP 配置请参见《AC6605 无线接入控制器 配置指南-以太网》中的 SEP 配置章节。
  - 请检查加入 SEP 段的端口状态，请执行**步骤 2**。
- 如果 SEP 段的拓扑和状态正常，请执行**步骤 4**。

步骤 2 查看当前端口状态是否是 Down。

在任意视图下执行命令 **display interface** 查看接口当前运行状态。

```
<Quidway> display interface GigabitEthernet 0/0/1
GigabitEthernet0/0/1 current state : DOWN
Line protocol current state : DOWN
Description:HUAWEI, Quidway Series, GigabitEthernet0/0/1 Interface
Switch Port, PVID :    1, TPID : 8100(Hex), The Maximum Frame Length is 1600
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 000b-0918-8bc1
Port Mode: COMMON COPPER
Speed :   10,  Loopback: NONE
Duplex: HALF,  Negotiation: ENABLE
Mdi    : AUTO
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec, Record time: -
Output peak rate 0 bits/sec, Record time: -
Input:  0 packets, 0 bytes
Unicast        :                0, Multicast         :                0
Broadcast      :                0, Jumbo             :                0
CRC            :                0, Giants            :                0
Jabbers        :                0, Fragments         :                0
Runts          :                0, DropEvents        :                0
Alignments     :                0, Symbols           :                0
Ignoreds       :                0, Frames            :                0
Discard        :                0, Total Error       :                0
```

```
Output:  0 packets, 0 bytes
Unicast         :                0, Multicast          :                0
Broadcast       :                0, Jumbo              :                0
Collisions      :                0, Deferreds          :                0
Late Collisions:                 0, ExcessiveCollisions:                0
Buffers Purged :                 0
Discard         :                0, Total Error        :                0
    Input bandwidth utilization threshold : 100.00%
    Output bandwidth utilization threshold: 100.00%
    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
```

- 如果当前接口状态是 Down，请在当前接口视图下执行命令 **display this** 查看接口下是否被 shutdown。
  - 如果是 shutdown，请在当前接口视图下执行命令 **undo shutdown**。
  - 如果没有显示 shutdown，请执行**步骤 3**。
- 如果当前接口状态是 Up，请执行**步骤 4**。

步骤 3 查看物理端口是否存在故障。

- 如果物理接口存在故障，请参考 **4.1.1 以太网接口物理 Down 的定位思路**。
- 如果物理接口不存在故障，请执行**步骤 4**。

步骤 4 检查 SEP 段上的端口是否允许数据 VLAN 通过。

在当前接口视图下执行命令 **display this** 查看当前接口是否允许指定数据 VLAN 通过。

```
[Quidway] interface GigabitEthernet 0/0/1
[Quidway-GigabitEthernet0/0/1] display this
 port link-type trunk
 port trunk allow-pass vlan 10 100
 stp disable
 sep segment 1 edge primary
#
return
```

- 如果当前端口没有配置允许指定数据 VLAN 通过，请正确配置当前端口允许指定数据 VLAN 通过。
- 如果当前端口已经允许指定数据 VLAN 通过，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。

12 WLAN 故障处理

关于本章

本文档介绍 AC6605 中出现的一些故障原因及处理步骤。

12.1 STA 无法搜索到无线信号的定位思路

12.1.1 常见原因

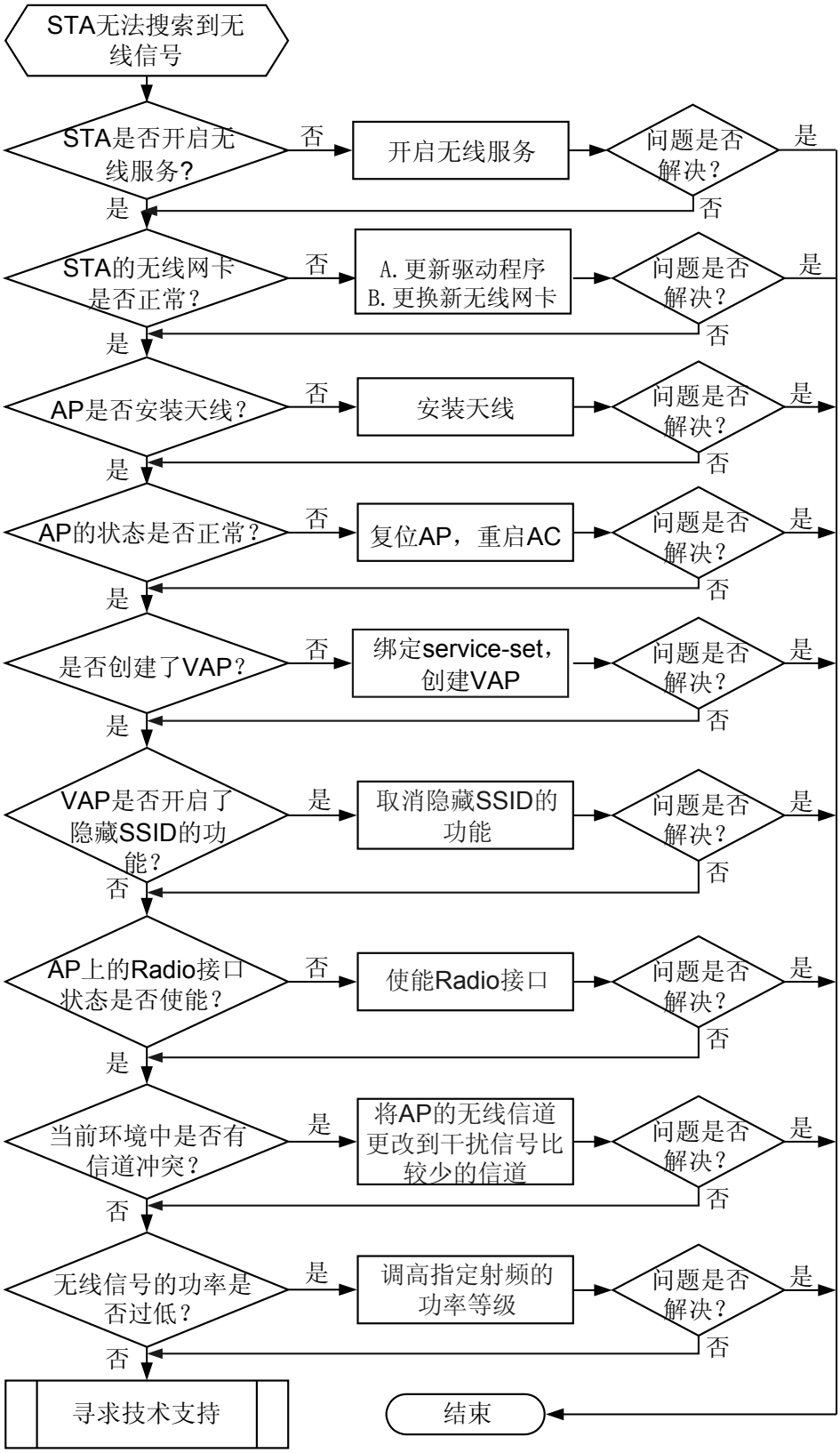
本类故障的常见原因主要包括：

- STA 的操作系统未打开无线服务。
- STA 的无线网卡故障。
- AP 未安装天线。
- AP 的状态 Fault。
- AC6605 上未创建 VAP。
- VAP 开启了隐藏 SSID 的功能。
- AP 上的 Radio 接口状态未使能。
- AC6605 上对 AP 的无线信号功率设置过低。

12.1.2 故障诊断流程

详细处理流程如图 12-1 所示。

图 12-1 STA 无法搜索到无线信号的故障诊断流程图



12.1.3 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 STA 的操作系统是否开启了无线服务。

- 如果没有开启无线服务，请开启。
- 如果已经开启了无线服务，请执行步骤 2。

步骤 2 检查 STA 的无线网卡是否正常。

1. 更新无线网卡的驱动程序，检查是否能够搜索到无线信号。
   - 如果可以搜索到无线信号，说明原 STA 的驱动程序故障，更新驱动程序即可。
   - 如果仍然搜索不到无线信号，请执行步骤 b。
2. 使用其他无线网卡，检查是否能够搜索到无线信号。
   - 如果可以搜索到无线信号，说明原 STA 的无线网卡故障，请更换新的无线网卡。
   - 如果同样也搜索不到无线信号，请执行步骤 3。

步骤 3 检查 AP 是否安装天线。

肉眼目测检查 AP 设备是否安装了天线。

- 如果没有安装天线，请安装天线。
- 如果已经安装天线，请执行步骤 4。

步骤 4 检查 AP 的状态是否正常。

在 AC6605 上，执行 **display ap id** *ap-id* 命令查看关键字 **State**。

- 如果 **State** 值显示为 **fault**，说明 AP 故障，请手动重启 AP。
  - 如果重启 AP 后，AP 的状态也不能变为 **normal**，请重启 AC6605，如果 AP 的状态还是不能变为 **normal**，请执行步骤 9。
  - 如果重启 AP 后，AP 的状态变为 **normal**，请执行步骤 5。
- 如果 **State** 值显示为 **normal**，说明 AP 状态正常，请执行步骤 5。

步骤 5 检查 AC6605 上是否创建 VAP。

在 AC6605 上，执行 **display vap** 命令查看是否创建 VAP。

- 如果返回 **Error:VAP does not exist**，说明没有创建 VAP，请执行 **radio-profile** 命令在指定射频上先绑定 radio-profile，然后再执行 **service-set** 命令在指定射频上绑定 service-set，创建 VAP。
- 如果显示 VAP 的相关信息，说明已经创建了 VAP，请执行步骤 6。

步骤 6 检查 VAP 是否开启了隐藏 SSID 的功能。

在 AC6605 上，执行 **display service-set** 命令查看 VAP 是否开启了隐藏 SSID 的功能。

- 如果 **Hide SSID** 值显示为 **enable**，说明 VAP 开启了隐藏 SSID 的功能，请执行 **undo ssid-hide** 命令取消隐藏 SSID 的功能。

- 如果 **Hide SSID** 值显示为 **disable**，说明 VAP 没有开启隐藏 SSID 的功能，请执行步骤 7。

步骤 7 检查 AP 上的 Radio 接口状态是否使能。

在 AC6605 上，执行 **display radio config** 命令查看 Radio 接口的状态。

- 如果 **Administrate status** 值显示为 **disable**，说明 Radio 接口未使能，请执行 **radio enable** 命令使能 Radio 接口。
- 如果 **Administrate status** 值显示为 **enable**，说明 Radio 接口已使能，请执行步骤 8。

步骤 8 检查 AC6605 上对 AP 的无线信号功率设置。

在 AC6605 上，执行 **display actual channel-power** 命令查询指定射频上当前实际的信道和功率值。

说明

POWER-LEVEL 表示射频当前的实际发送功率等级，取值范围是 0~15，0 表示满功率，1 表示满功率减少 1dbm，2 表示满功率减少 2dbm，以此类推，显示的最大值为 12，即当配置射频功率等级为 12~15，显示的都为 12。

- 如果 **POWER-LEVEL** 值显示为 **12** 或者比较低的值，说明射频当前的实际发送功率过低，导致 STA 无法搜索到无线信号，请执行 **power-level** 命令调高指定射频的功率等级。
- 如果 **POWER-LEVEL** 值显示为 **0** 或者比较高的值，说明射频当前的实际发送功率正常，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

12.1.4 相关告警与日志

相关告警

无

相关日志

无

12.2 无线用户经常掉线的定位思路

12.2.1 常见原因

本类故障的常见原因主要包括：

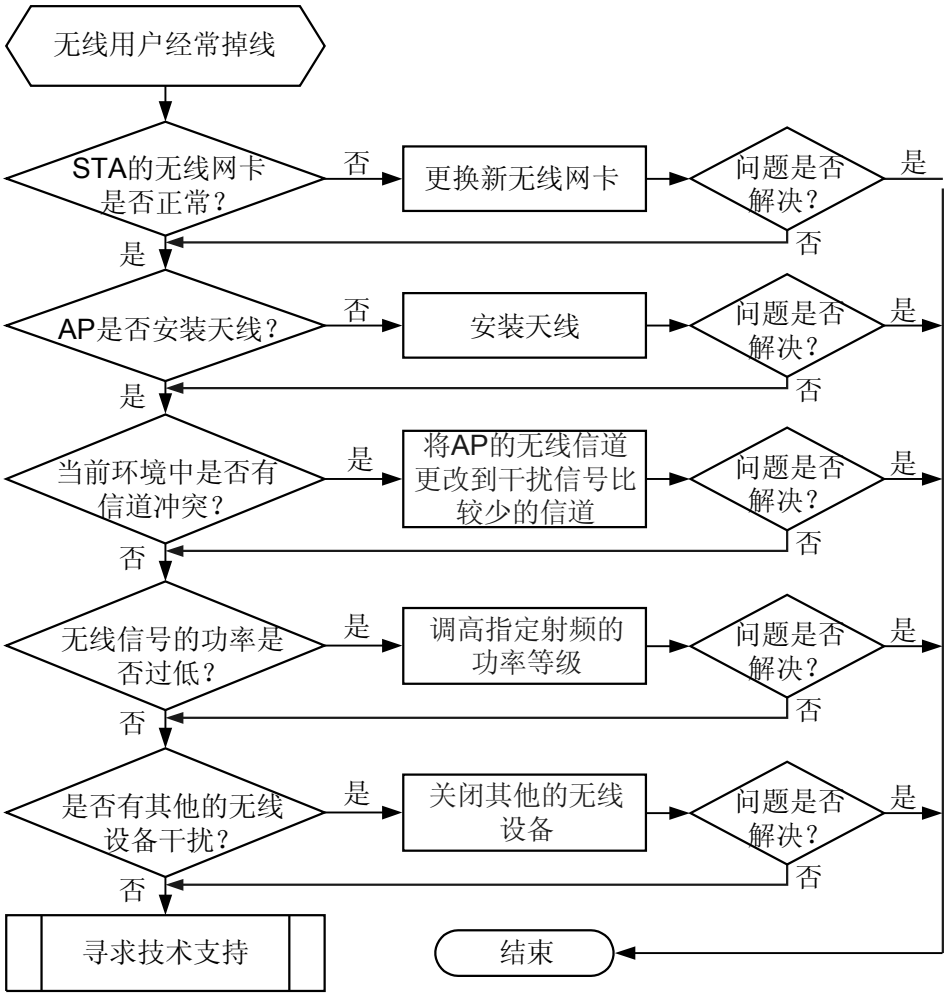
- STA 的无线网卡故障。

- AP 未安装天线。
- 信道冲突。
- AC6605 上对 AP 的无线信号功率设置过低。
- 其他的无线设备干扰 AP 的无线信号。

12.2.2 故障诊断流程

详细处理流程如图 12-2 所示。

图 12-2 无线用户经常掉线的故障诊断流程图



12.2.3 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 STA 的无线网卡是否正常。

使用其他无线网卡，检查无线用户是否也经常掉线。

- 如果无线用户正常接入并稳定在线，说明原 STA 的无线网卡故障，请更换新的无线网卡。
- 如果同样也出现经常掉线的情况，请执行步骤 2。

步骤 2 检查 AP 是否安装天线。

肉眼目测检查 AP 设备是否安装了天线。

- 如果没有安装天线，请安装天线。
- 如果已经安装天线，请执行步骤 3。

步骤 3 检查当前环境中是否有信道冲突。

使用 NetStumbler 软件扫描，发现当前信道 11 上无线信号较多，信道 1 上没有无线信号，此时可以执行 **channel** 命令将 AP 的无线信道从信道 11 更改为信道 1。如果故障仍然没有排除，请执行步骤 4。

步骤 4 检查 AC6605 上对 AP 的无线信号功率设置。

在 AC6605 上，执行 **display actual channel-power** 命令查询指定射频上当前实际的信道和功率值。

说明

POWER-LEVEL 表示射频当前的实际发送功率等级，取值范围是 0~15，0 表示满功率，1 表示满功率减少 1dbm，2 表示满功率减少 2dbm，以此类推，显示的最大值为 12，即当配置射频功率等级为 12~15，显示的都为 12。

- 如果 **POWER-LEVEL** 值显示为 **12** 或者比较低的值，说明射频当前的实际发送功率过低，导致无线用户经常掉线，请执行 **power-level** 命令调高指定射频的功率等级。
- 如果 **POWER-LEVEL** 值显示为 **0** 或者比较高的值，说明射频当前的实际发送功率正常，请执行步骤 5。

步骤 5 检查当前环境中是否存在其他的无线设备。

肉眼目测检查当前环境中是否存在其他的无线设备，比如正在工作的微波炉等，这些无线设备会干扰 AP 的无线信号，导致无线用户经常掉线。

- 如果存在其他的无线设备，请关闭这些设备后再尝试连接无线网络。
- 如果不存在其他的无线设备，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

12.2.4 相关告警与日志

相关告警

无

相关日志

无

12.3 AP 无法上线的定位思路

12.3.1 常见原因

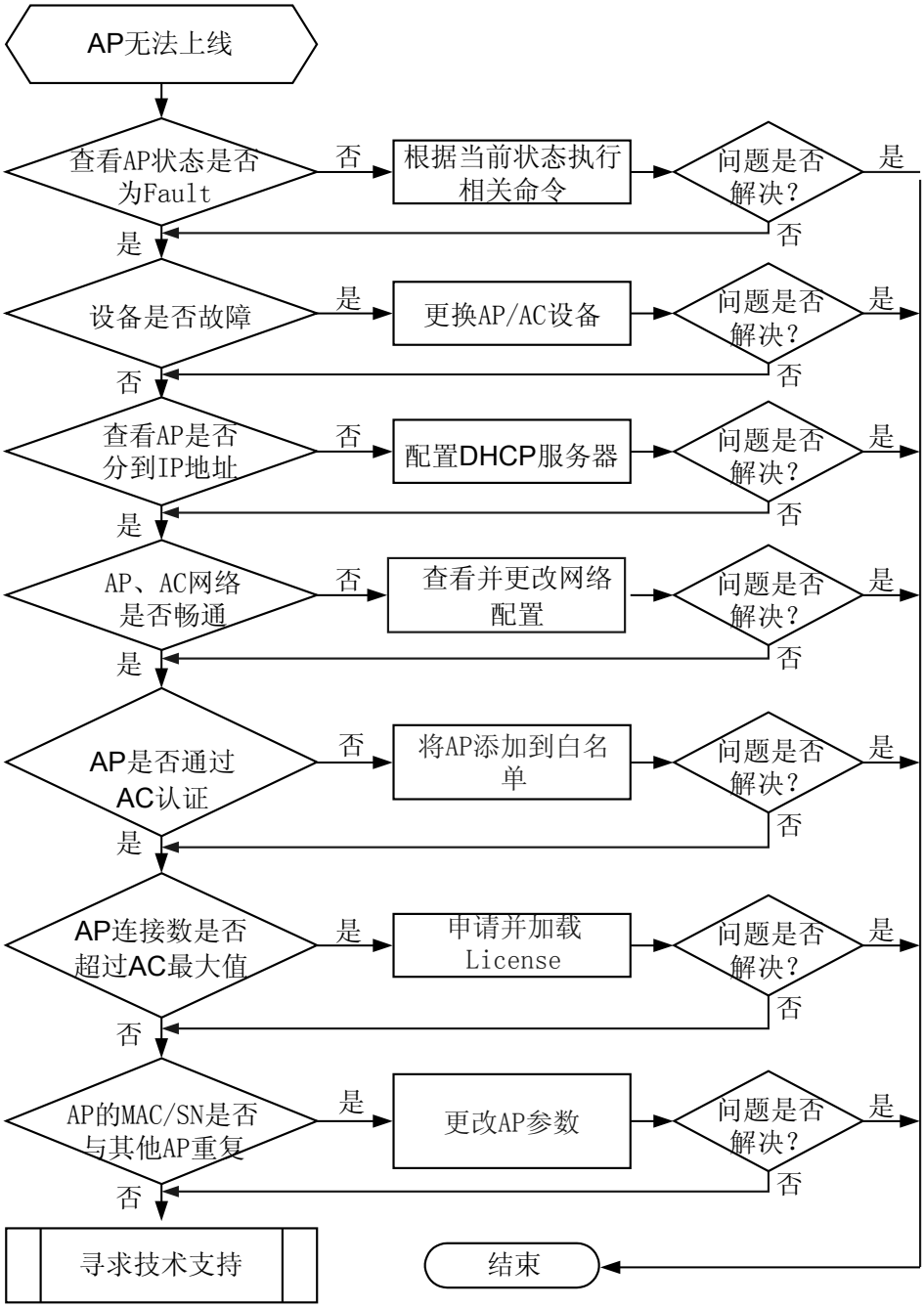
本类故障的常见原因主要包括：

- AP 故障。
- AP 未分配到 IP 地址。
- AP、AC 之间网络不通。
- AP 认证不通过。
- AC 最大连接数限制。
- AP 配置参数(MAC、SN)重复。
- AP 与 AC 的版本不匹配。
- AC 不支持关联该类型 AP。
- 离线增加的 AP 类型与 AP 实际类型不符。

12.3.2 故障诊断流程

详细处理流程如图 12-3 所示。

图 12-3 AP 无法上线故障诊断流程图



12.3.3 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 查看 AP 当前状态。

登录 AC6605 执行命令 **display ap id** *ap-id* 查看关键字 **State**，查看 AP 状态。

- 如果 AP 状态为 fault。请手动重启 AP。如果重启后，AP 的状态仍然不能变为 normal，请重启 AC6605，如果 AP 的状态还是不能变为 normal，请执行步骤 2。
- 如果 AP 状态为 type-not-match，则修改配置的 AP 类型为实际 AP 类型，后复位 AP。查看结果。如果 AP 状态为 fault，则执行步骤 2。

步骤 2 查看 AP 设备是否故障。

肉眼目测 AP，查看电源指示灯、网线指示灯是否正常闪烁。

- 如果不正常，请检查电源线、网线连接是否正常。如果电源线和网线连接正常，则执行步骤 8。
- 正常闪烁，则执行步骤 3。

步骤 3 查看 AP 是否分配到 IP 地址。

在 DHCP 服务器上通过执行命令 **display ip pool** { **interface** *interface-name* | **name** *ip-pool-name* } **used** 查看该 AP 是否分配到 IP 地址。

- 如果 AP 未分到 IP 地址，如果 AP 与 AC 间是二层组网，则配置 DHCP 服务器；如果 AP 与 AC 间是三层组网，则需要配置 DHCP option43 和 DHCP 服务器。
- 如果 AP 已分配到 IP 地址。则执行步骤 4。

步骤 4 查看 AP、AC 间网络是否畅通。

在 AC6605 上和 AP 上分别执行 ping 命令，查看能否相互 ping 通。

- 如果无法或单方 ping 通，则查看并修改 VLAN 方面的配置。
- 如果 AP、AC 互通，则执行步骤 5。

步骤 5 检查 AP 是否通过 AC 认证。

在 AC6605 上，执行 **display ap-auth-mode** 命令查看当前认证模式。

- 如果认证模式为 mac 认证或 sn 认证。则执行 **display unauthorized-ap record** 查看是否存在未认证 AP，存在则 wlan 视图下执行 **ap-confirm** 命令添加 AP 到白名单中。
- 如果认证模式为不认证或已将 AP 添加到白名单中，则执行步骤 6。

步骤 6 查看 AP 连接数是否超过 AC 最大连接数。

1. 未加载 license 文件时，AC6605 默认支持 AP 数为 8。通过 **display ap all** 查看当前状态为 normal 的 AP 数量。
   - 如果超过当前的最大连接数，则申请并加载 AP license。
   - 如果未超过当前的最大连接数，则执行步骤 7。
2. 如果已加载 license 文件，但是当前 AP 数量已超过 license 规格的话，可以执行命令 **display license resource usage** 查看 License 文件中定义的资源项的使用情况。
   - 如果超过当前的最大连接数，则申请并加载 AP license。
   - 如果未超过当前的最大连接数，则执行步骤 7。

步骤 7 查看 AP 的 mac 或 sn 是否与其他 AP 冲突。

通过 **display ap id** *ap-id* 命令查看 AP 的 mac 与 sn 信息。

- 如果与其他 AP 信息冲突，则根据 AP 信息更改配置。
- 如果与其他 AP 信息不冲突，则执行步骤 8。

步骤 8 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

12.3.4 相关告警与日志

相关告警

- WLAN_1.3.6.1.4.1.2011.6.139.2.1.1.1 hwApFaultNotify
- WLAN_1.3.6.1.4.1.2011.6.139.2.1.1.2 hwApNormalNotify
- WLAN_1.3.6.1.4.1.2011.6.139.2.1.1.3 hwApTypeNotMatchNotify
- WLAN_1.3.6.1.4.1.2011.6.139.2.1.1.9 hwApAddOffLineNotify
- WLAN_1.3.6.1.4.1.2011.6.139.2.1.1.19 hwAcDevicesSwitchNotify
- WLAN_1.3.6.1.4.1.2011.6.139.2.1.1.20 hwApTimeSynFailNotify
- WLAN_1.3.6.1.4.1.2011.6.139.2.1.1.21 hwDyingGaspTrapNotify
- WLAN_1.3.6.1.4.1.2011.6.139.2.1.1.42 hwApColdBootNotify
- WLAN_1.3.6.1.4.1.2011.6.139.2.1.1.43 hwApColdBootRestoreNotify
- WLAN_1.3.6.1.4.1.2011.6.139.2.1.1.44 hwApHotBootNotify
- WLAN_1.3.6.1.4.1.2011.6.139.2.1.1.45 hwApHotBootRestoreNotify

相关日志

无

12.4 WDS（AP 无法通过无线上线）的定位思路

12.4.1 常见原因

本类故障的常见原因主要包括：

AP 自身原因分析:

- AP 信号不佳。
- AP 类型不支持网桥。
- AP 版本过低或该类型 AP 不支持网桥功能。
- AP 未打开网桥开关以及未配置模式 middle 和 leaf。

AP 配置原因分析：

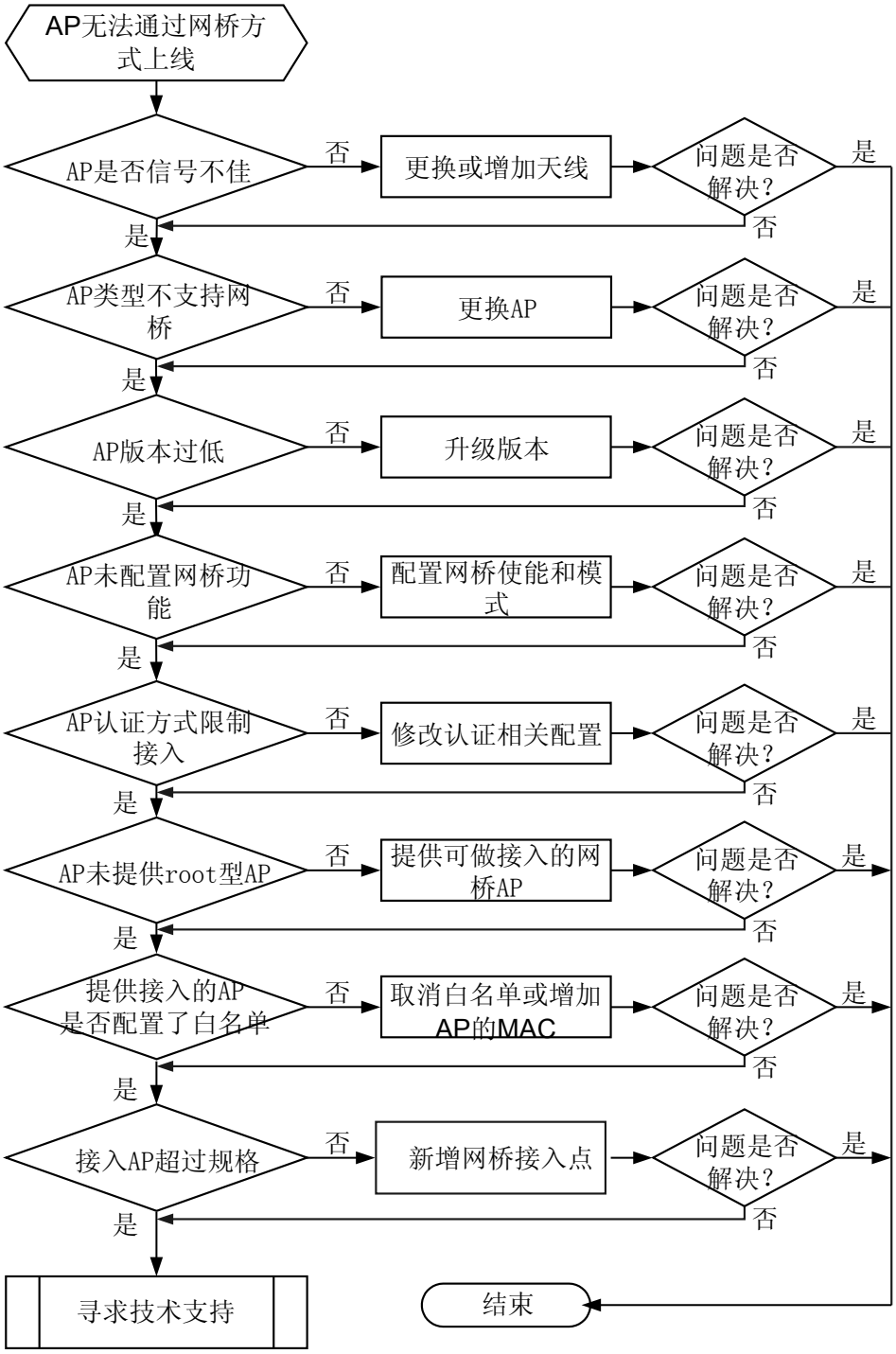
- AC 认证方式，限制了 AP 接入。
- 没有可以提供网桥接入的 root 或者 middle 类型 AP。

- 在提供网桥接入的 AP 上配置了网桥白名单使能，但是未将新 AP 加入到白名单列表，或者加入到白名单列表中的 AP MAC 错误。
- AC 上提供接入 root 或 middle 模式的 AP，已经连接了满规格的 AP（不超过 6 个），不再提供接入服务。

12.4.2 故障诊断流程

详细处理流程如图 12-4 所示。

图 12-4 AP 无法通过网桥上线故障诊断流程图



12.4.3 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 AP 是否信号不佳

- 检查 AP 是否安装了天线，可以更换高增益的天线或尝试将该 AP 靠近 root 型 AP。
- 如果 AP 信号强度良好，请执行步骤 2。

步骤 2 检查 AP 类型是否支持网桥功能

- 执行命令 **display ap id** *ap-id* 查看 AP 的类型，如果 AP 不支持网桥功能，请更换 AP。

  说明

  不支持网桥功能的 AP 类型有：WA601、WA631、WA651、WA602、WA632、WA652、WA653DE、WA603DE。

- 如果 AP 类型支持网桥功能，请执行步骤 3。

步骤 3 检查 AP 版本是否过低。

通过串口连接到 AP，根据 AP 提供的初始密码，登陆到 AP 上查看版本信息。

- 如果 AP 版本过旧(属于 V200R001C00 之前的版本)，请升级 AP 版本。
- 如果 AP 版本正常，请执行步骤 4。

步骤 4 查看 AP 是否配置了网桥功能

- 通过串口或远程方式连接到 AP，根据 AP 提供的初始密码，登陆到 AP 上，进入 config 模式。
  1. 执行命令 **interface wireless**，进入 AP 射频。
  2. 执行命令 **show wds-config**，查看射频 WDS 功能是否使能。
  3. 如果 WDS 功能没有使能，则执行命令 **wds enable** 使能网桥功能，并执行命令 **wds mode** 配置网桥模式。
- 如果使能了网桥功能，请执行步骤 5。

步骤 5 检查 AP 的认证方式。

登录 AC6605 执行命令 **display ap-auth-mode** 命令查看当前认证模式。

- 如果认证模式为 mac 认证或 sn 认证。可以
  - 执行命令 **ap-auth-mode**，配置 AP 认证模式为不认证；
  - 执行命令 **ap-whitelist**，增加 AP 设备的 MAC 地址或 SN 到白名单中。
- 如果认证模式为不认证或已将 AP 添加到白名单中，则执行步骤 6。

步骤 6 检查 AC 是否配置了提供接入的 root 或者 middle 型 AP。

在 wlan 视图下执行 **display this** 命令，查看是否有配置了提供接入的 AP。并且确保该 AP 可以被新增 AP 搜索到，在其射频范围内。

- 如果没有配置提供接入的 AP，则配置 AP 接入类型为 root。
- 如果存在提供接入的 AP，则执行步骤 7。

说明

新增 AP 必须可以搜索到配置了网桥功能的 AP 无线信号，如果搜索不到，则需要重新配置一个提供网桥接入的 AP。

配置完成后，commit 完，并重启设备。

步骤 7 检查提供接入的 AP 是否使能了网桥白名单。

执行命令 **display bridge-whitelist**,查看网桥白名单的配置信息。

- 如果配置了网桥白名单，则需要查看新增 AP 设备上的 MAC 标签，执行命令 **peer** 在网桥白名单中添加该 AP 的 MAC 地址。
- 如果没有配置网桥白名单。则执行步骤 8。

步骤 8 检查提供接入服务的 AP 是否超过了允许接入的最大规格数（默认最大支持数为 6 个）。

- 执行命令 **display bridge-link all**，查看该 AP 链接了多少个 AP。如果链接数已达到最大值，请新增接入 AP。
- 如果链接数没有达到最大值，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

12.4.4 相关告警与日志

相关告警

无

相关日志

无