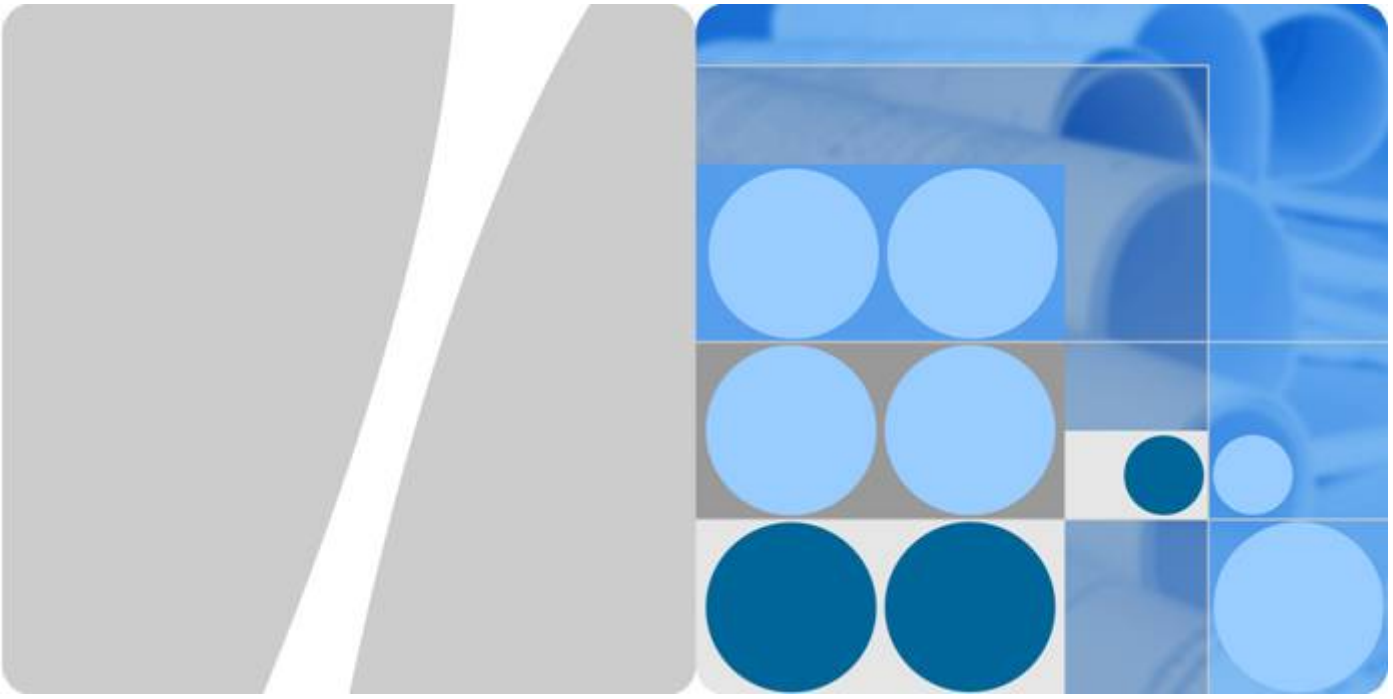


HUAWEI NetEngine80E/40E 路由器

V600R003C00

故障处理-系统

文档版本　02

发布日期　2011-09-10

华为技术有限公司

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

概述

说明

- 手册中所使用的链路接口编号和链路类型以 NE40E-X8 为例，实际使用时以现网设备为准。
- NE80E/40E 系列中的非 X1/X2 设备的线路处理板称为 LPU，交换网板称为 SFU；X1/X2 设备没有 LPU 和 SFU，由 NPU 集中实现报文交换和转发功能。

本文档针对的 HUAWEI NetEngine80E/40E 各类业务，从常见故障及其处理方法、故障处理案例、FAQ 等方面分析介绍了故障的处理过程。

本文档提供了 HUAWEI NetEngine80E/40E 故障的处理流程和方法。

产品版本

与本文档相对应的产品版本如下所示。

产品名称	产品版本
HUAWEI NetEngine80E/40E 路由器	V600R003C00

读者对象

本文档主要适用于以下工程师：

- 系统维护工程师
- 调测工程师
- 网络监控工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

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

命令行格式约定

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

修订记录

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

文档版本 02 (2011-09-10)

第二次正式发布，文档内容更新如下：

- 新增 **11 ACL 抓包故障处理**
- 新增 **9 时钟同步故障处理**

文档版本 01 (2011-05-30)

第一次正式发布

目 录

1 Telnet 故障处理

关于本章

1.1 Telnet 登录失败的定位思路

1.1.1 常见原因

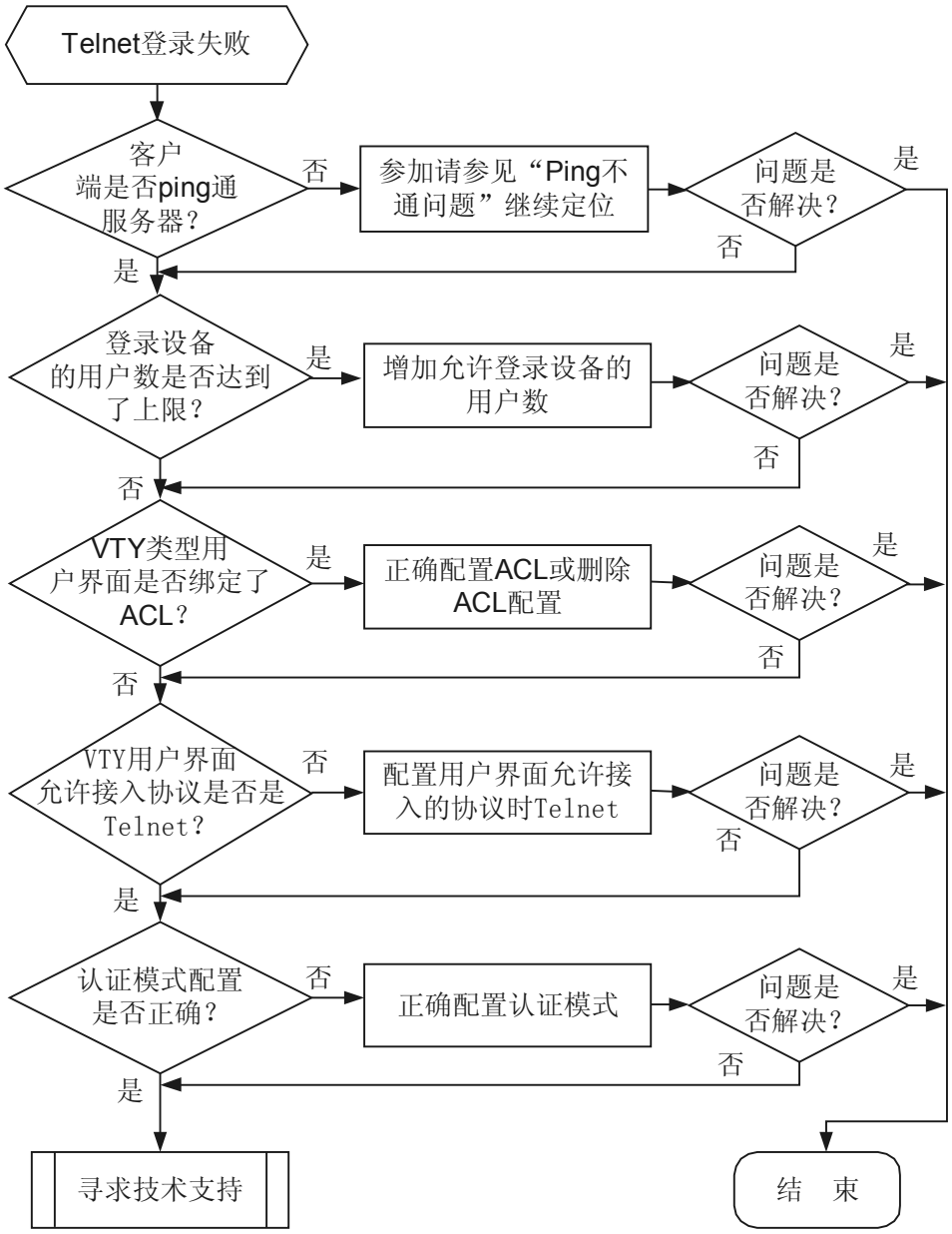
本类故障的常见原因主要包括：

- 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。

1.1.2 故障诊断流程

故障诊断流程如图 **1-1** 所示。

图 1-1 Telnet 故障流程诊断流程图



1.1.3 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 检查客户端能否 Ping 通服务器。

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

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

步骤 2 检查登录设备的用户数是否到达了上限。

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

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

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

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

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

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

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

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

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

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

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

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

步骤 5 检查扩展 VTY 通道 vty 16 20 是否可以登录。

user-interface vty 16 20 是预留给网管的通道。无论 user-interface 0 14 有没有登录满，普通用户都不会登录到 user-interface vty 16 20。只有网管类型（net-manager）的用户才能登录到 user-interface vty 16 20。

可以执行命令 **display users** 查看每个用户界面的用户登录信息。

步骤 6 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 password** 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 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

1.1.4 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])

1.2 故障案例

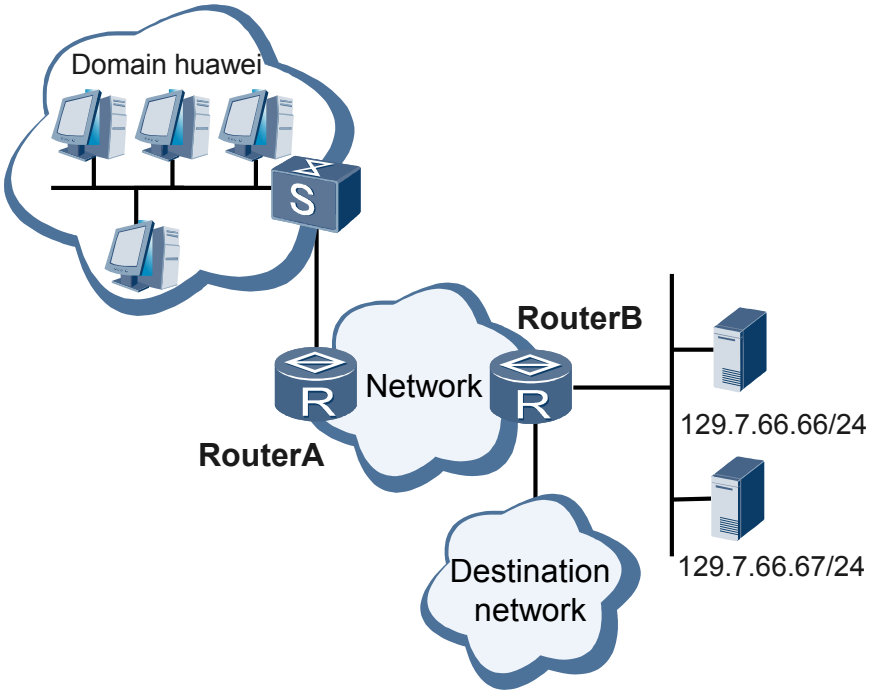
1.2.1 用户登录设备十几秒内被强制下线

网络环境

在图 1-2 所示的网络中，用户通过网络接入服务器 RouterB 访问网络，在 RouterB 上对用户登录进行认证、授权和计费。

RouterB 原来使用 RADIUS 协议对用户进行认证和计费，由于 RADIUS 服务器故障，管理员临时采用本地认证。

图 1-2 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 RouterB 上执行 **display trapbuffer** 和 **display logbuffer** 命令，查看是否有强制用户下线的告警和日志信息。发现有如下告警信息：

   ```
   AAA cut user!
   ```

2. 在 RouterB 上执行 **display current-configuration** 命令，查看 AAA 的配置信息。发现 AAA 采用了本地认证和远端计费，配置如下：

   ```
   radius-server template provera
    radius-server shared-key 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

    #
    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** { **local** | **none** }，将计费方式改为本地计费或者不计费。
  - 针对 PPPoE 等普通性用户时，由于涉及收费上网，可以改用本地计费，继续保持对用户上网的计费。
  - 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，计费方案必须是本地计费或者不计费，否则将导致用户下线。

2 FTP 故障处理

关于本章

2.1 FTP 登录失败的定位思路

2.1.1 常见原因

本类故障的常见原因主要包括：

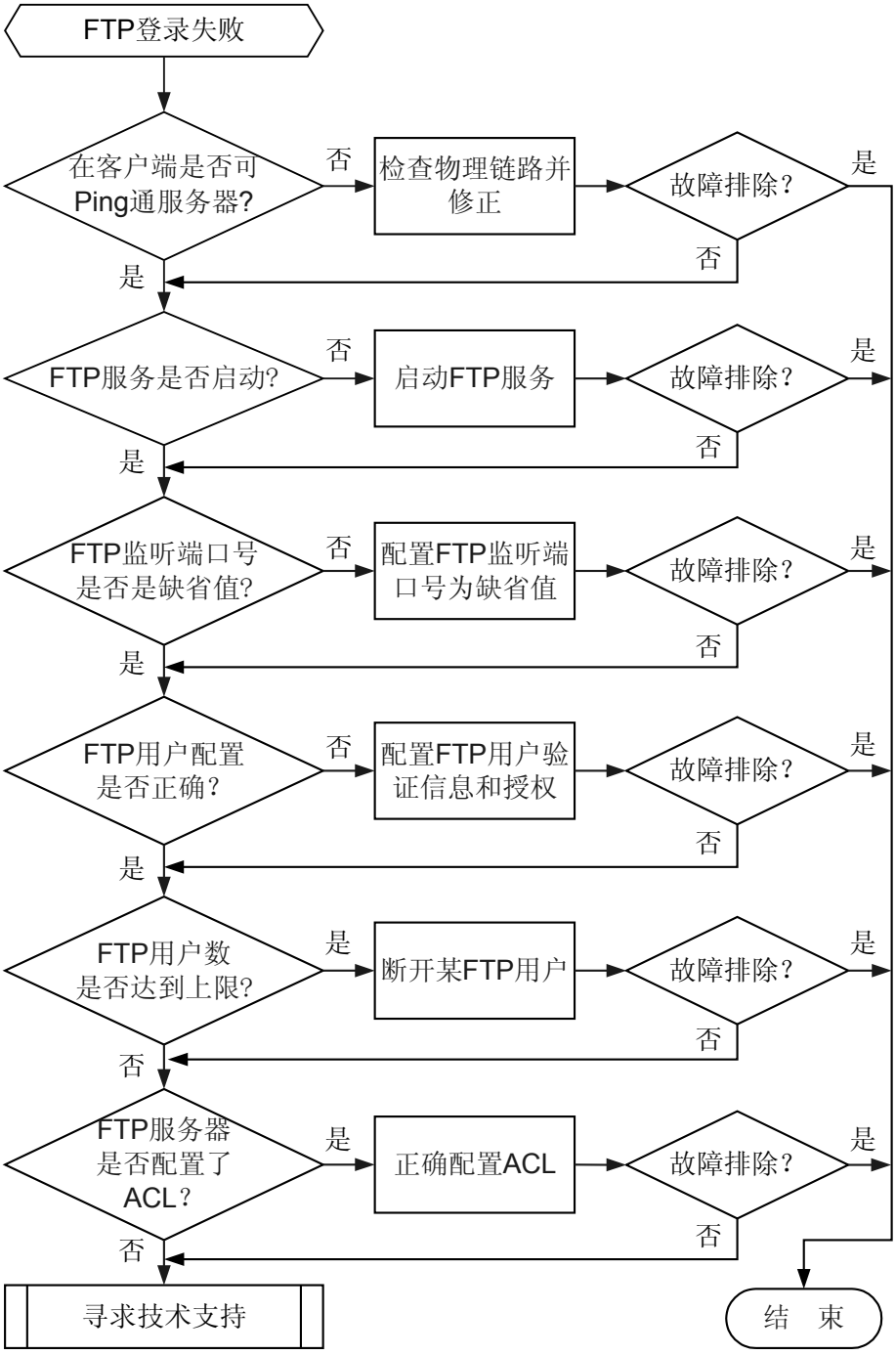
- 客户端与服务器之间的路由不可达。
- FTP 服务器功能没有启动。
- FTP 服务器指定监听端口号不是缺省端口号，且 FTP 客户端登录时没有指定端口号。
- 未配置 FTP 用户的验证信息和工作目录。
- 登录 FTP 服务器的用户数达到上限。
- FTP 服务器配置了 ACL 规则限制客户端登录。

2.1.2 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 2-1 所示。

图 2-1 FTP 登录失败故障诊断流程图



2.1.3 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。

```
<HUAWEI> 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 **Ping 不通问题**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。

```
<HUAWEI> 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。

```
<HUAWEI> system-view
[HUAWEI] 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**。

```
<HUAWEI> 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。

```
<HUAWEI> 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。

```
<HUAWEI> 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。

```
<HUAWEI> system-view
[HUAWEI] undo ftp server
[HUAWEI] 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

2.1.4 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])

2.2 FTP 传输失败的定位思路

2.2.1 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。

2.2.2 故障诊断流程

略。

2.2.3 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 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

2.2.4 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]")

2.3 FTP 传输速度慢的定位思路

2.3.1 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。

2.3.2 故障诊断流程

略。

2.3.3 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 检查存储设备是否有 Flash。

Flash 的特点是读取速度快，但是写速度慢。**表 2-1** 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 2-1 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

测试对象	get	put
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 2-2 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 2-2 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

2.3.4 相关告警与日志

相关告警

无

相关日志

无

3 SNMP 故障处理

关于本章

3.1 SNMP 无法连接的定位思路

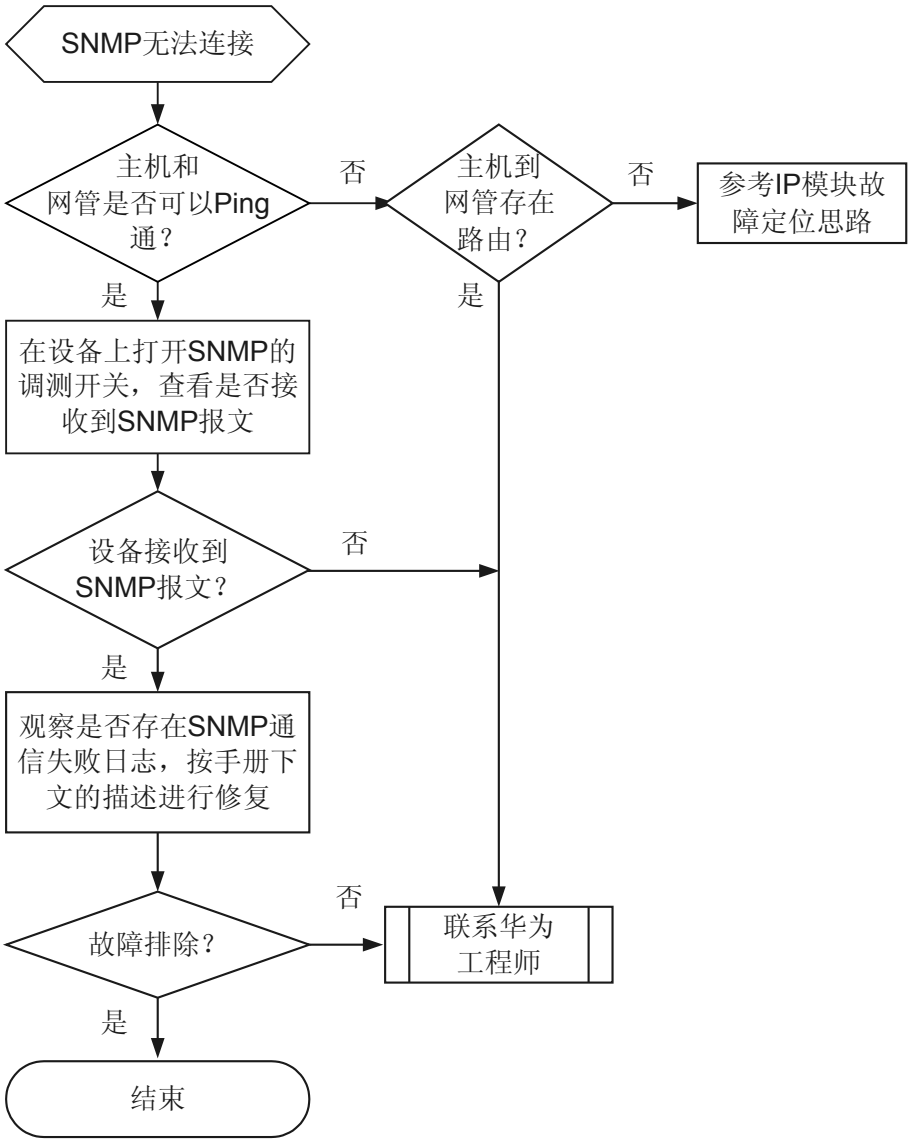
3.1.1 常见原因

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。

3.1.2 故障诊断流程

图 3-1 SNMP 无法连接诊断流程图



3.1.3 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 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 **Ping 不通问题**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 3-1 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阀值。	1. 执行 **snmp-agent packet max-size** 命令增大报文阀值。 ● 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。

日志	日志解释	处理建议
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。
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。

日志	日志解释	处理建议
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

3.1.4 相关告警与日志

相关告警

无

相关日志

SNMP/6/CNFM_VERSION_DISABLE
SNMP/4/SNMP_SET

3.2 网管无法收到主机发送的告警的定位思路

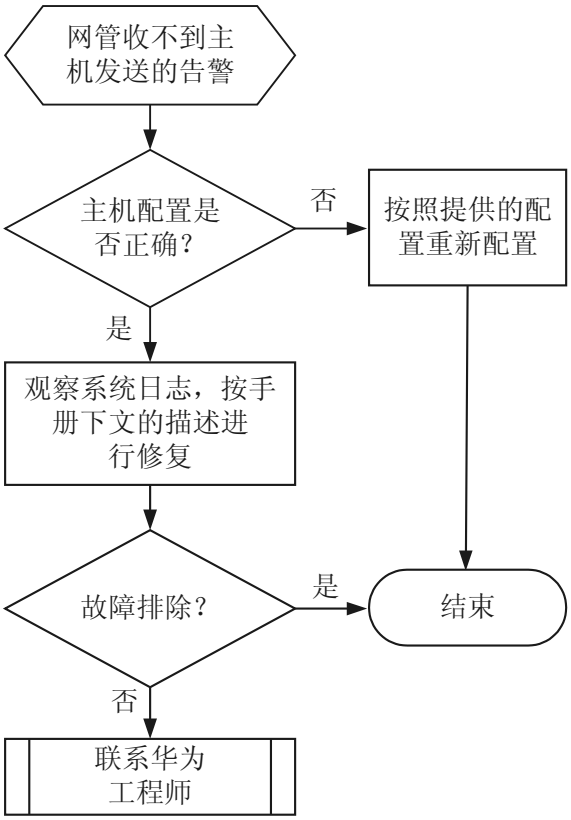
3.2.1 常见原因

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。

3.2.2 故障诊断流程

图 3-2 网管收不到主机告警的诊断流程图



3.2.3 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 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 3-2 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）	<HUAWEI> system-view [HUAWEI] snmp-agent target-host trap address udp-domain 192.168.1.1 params securityname huawei v2c
配置一个版本为 SNMPv2c 的告警主机，端口号为 163，用户名为 huawei，IP 地址为 192.168.1.1，且 192.168.1.1 这个地址属于 VPN VPN－TEST（huawei 必须是一个确实存在的用户）	<HUAWEI> system-view [HUAWEI] snmp-agent target-host trap address udp-domain 192.168.1.1 udp-port 163 vpn-instance VPN-TEST 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。 <HUAWEI> system-view [HUAWEI] snmp-agent mib-view included Huawei_view iso # 配置用户组。 [HUAWEI] snmp-agent group v3 huawei_group read-view Huawei_view write-view Huawei_view notify-view Huawei_view # 配置用户。 [HUAWEI] snmp-agent usm-user v3 huawei huawei_group
配置一个版本为 V3 的告警主机，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）	<HUAWEI> system-view [HUAWEI] snmp-agent target-host trap address udp-domain 192.168.1.1 params securityname huawei v3
配置一个版本为 V3 的告警主机，端口号为 163，用户名为 huawei，IP 地址为 192.168.1.1，且 192.168.1.1 这个地址属于 VPN VPN－TEST（huawei 必须是一个确实存在的用户）	<HUAWEI> system-view [HUAWEI] snmp-agent target-host trap address udp-domain 192.168.1.1 udp-port 163 vpn-instance VPN-TEST 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《HUAWEI NetEngine80E/40E 配置指南-系统管理》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

3.2.4 相关告警与日志

相关告警

无

相关日志

无

4 SSH 故障处理

关于本章

4.1 通过 SSH 登录 SSH Server 失败的定位思路

4.1.1 常见原因

本类故障的常见原因主要包括：

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

4.1.2 故障诊断流程

无

4.1.3 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 SSH 客户端和服务器之间网络是否畅通。

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

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

步骤 2 查看 SSH 服务器端的 SSH 服务是否启动。

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

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

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

```
<HUAWEI> system-view
```

```
[HUAWEI] sftp server enable
[HUAWEI] stelnet server enable
```

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

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

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

步骤 4 检查在 SSH 服务器端是否配置了 RSA 公钥。

设备作为 SSH 服务器时，必须配置本地密钥对。

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

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

步骤 5 （可选）检查 SSH 服务器端上是否配置了用户服务类型、认证类型和认证服务类型（只针对密码认证方式）。

SSH 服务器端上应该正确配置了用户服务类型、认证类型和认证服务类型。执行命令 **display ssh user-information**，查看 SSH 用户的配置信息。如果不存在配置信息，请在系统视图下分别执行命令 **ssh user**、**ssh user authentication-type** 和 **ssh user service-type**，新建 SSH 用户并配置 SSH 用户的认证方式和 SSH 用户的服务方式。

执行命令 **display local-user username** *user-name* 来查看与 SSH 同名用户的详细信息。如果不存在配置信息，请在 AAA 视图下执行命令 **local-user password** 与 **local-user service-type**，增加一个与 SSH 用户同名的本地用户并设置本地用户的接入类型。

说明

对于 SFTP 服务，还需在系统视图下执行命令 **ssh user sftp-directory**，配置 SSH 用户的 SFTP 服务授权目录。

- 创建 SSH 用户。

```
[HUAWEI] ssh user abc
[HUAWEI] ssh user abc authentication-type all
[HUAWEI] ssh user abc service-type all
[HUAWEI] ssh user abc sftp-directory cfcard:/ssh
```

同时在 AAA 视图下配置同名用户，并配置认证服务类型。

```
[HUAWEI] aaa
[HUAWEI] local-user abc password simple abc-pass
[HUAWEI] local-user abc service-type ssh
```

- 对 SSH 用户配置缺省密码验证。

```
[HUAWEI] ssh authentication-type default password
```

同时在 AAA 视图下配置同名用户，并配置认证服务类型。

```
[HUAWEI] aaa
[HUAWEI] local-user abc password simple abc-pass
[HUAWEI] local-user abc service-type ssh
```

步骤 6 检查登录 SSH 服务器端的用户数是否到达了上限。

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

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

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

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

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

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

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

在 SSH 服务器端上执行命令 **display acl**，查看该访问控制列表中是否 **deny** 了 SSH Client 的地址。如果 VTY 下绑定了 ACL，但 ACL 规则中未指定 deny 客户端的 IP 地址，则使用 Telnet 或 FTP 登录设备时将被默认拒绝而导致失败。即，如果需要使用某 IP 地址通过 Telnet 或 FTP 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 8 查看 SSH 客户端和服务器上 SSH 版本信息。

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

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

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

```
<HUAWEI> system-view
[HUAWEI] ssh server compatible-sshlx enable
```

- 如果使用 SSHv2 版本的客户端登录服务器，则服务器端版本兼容配置需要设置为不使能。

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

步骤 9 查看 SSH 客户端是否使能了首次认证功能。

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

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

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

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

步骤 10 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

4.1.4 相关告警与日志

相关告警

无

相关日志

SSH/4/SSH_FAIL:Failed to log in through SSH. (Ip=[STRING], UserName=[STRING], Times=[ULONG]).

SSH/4/STELNET_SERVER:The STELNET server is not started. Use the command' stelnet server enable' to start it.

SSH/4/USER_NOTEXIST:The user [STRING] does not exist.

4.2 相关案例

4.2.1 因密钥长度不一致导致网络管理员无法通过 SSH 登录路由器

网络环境

在图 4-1 的网络中，网络管理员希望通过 SSH 协议登录路由器（SSH Server），但是配置完成后，管理员总是登录失败。

图 4-1 网络管理员无法通过 SSH 登录路由器的组网图

故障分析

1. 查看管理员登录时的相关提示信息，发现有如下信息。

```
$ ssh -l client001 10.1.1.1
ssh_rsa_verify: RSA modulus too small: 512 < minimum 768 bits
key_verify failed for server_host_key
```

可以分析出，由于服务器端生成的密钥长度小于 768，无法建立 SSH 连接。

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 **rsa local-key-pair create**，修改设备的密钥长度为 1024。

输入该命令后，会提示用户输入主机密钥的位数。如果 RSA 密钥已经存在，则系统将提示用户确认是否替换原有密钥。具体配置方法如下：

```
[HUAWEI]rsa local-key-pair create
The key name will be: HUAWEI_Host
% RSA keys defined for HUAWEI_Host already exist.
Confirm to replace them? [Y/N]:y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]:1024
Generating keys...
.................++++++++++++
...++++++++++++
.................................++++++++
.............++++++++
```

完成上述操作后，用户成功登录到 SSH Server，故障排除。

----结束

案例总结

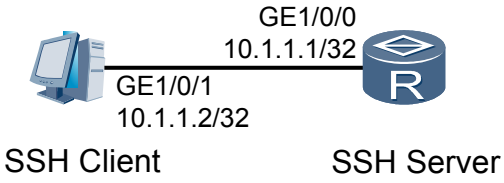
SSH 客户端有些工具对密钥的长度有要求，服务器端密钥的长度需要满足此要求。

4.2.2 RSA 密钥没有配置导致登录 SSH 服务器失败

网络环境

Router 作为 SSH Server。通过在 Router 和客户端配置 SSH，使 SSH Client 可以通过 SSH 方式登录到 SSH Server。

图 4-2 RSA 密钥没有配置导致登录 SSH 服务器失败组网图



配置完成后，发现用户登录 SSH Server 失败。

故障分析

1. 在 Router 上，使用命令 **display current-configuration configuration**，查看设备上相关的配置信息：

```
#
user-interface vty 0 4
 protocol inbound ssh authentication-mode aaa
#
aaa  local-user abc password simple huawei ssh user huawei
  authentication-type password
```

通过以上信息可以看出，Router 上配置了 SSH 采用密码验证，但没有配置生成本地 RSA 密钥对。

当用户界面的协议为 SSH 时，SSH 功能开启后必须执行命令 **rsa local-key-pair create**，生成本地 RSA 密钥对。

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 **rsa local-key-pair create**，产生本地 RSA 密钥对。

配置完成后，SSH 用户登录 SSH Server 成功，故障排除。

----结束

案例总结

成功完成 SSH 登录的首要操作是配置并生成本地 RSA 密钥对。在进行其它 SSH 配置之前，必须完成 **rsa local-key-pair create** 配置，生成本地密钥对。

5 RMON 故障处理

关于本章

5.1 网管无法接收 RMON 告警信息的定位思路

5.1.1 常见原因

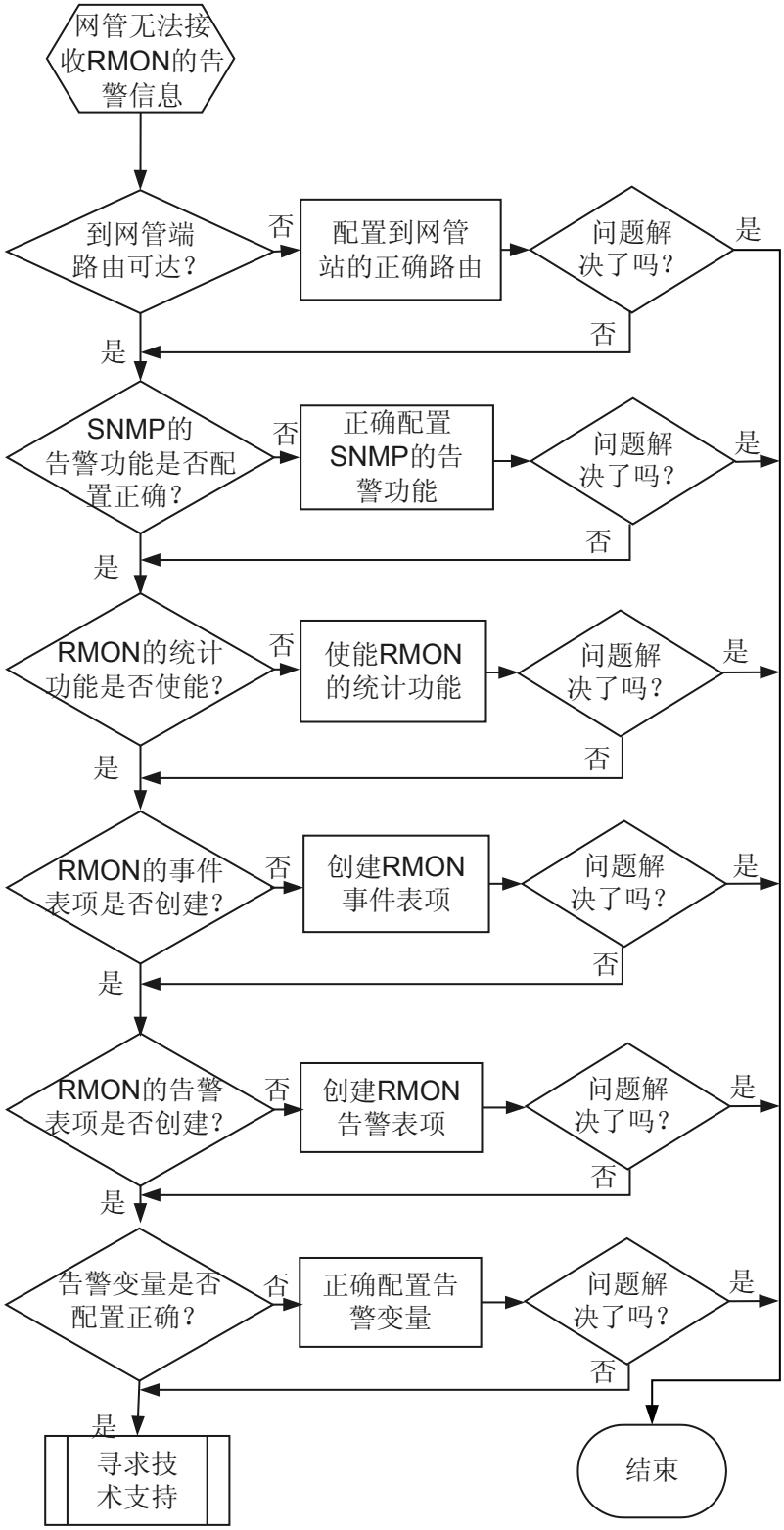
本类故障的常见原因主要包括：

- 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。

5.1.2 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 5-1 所示。

图 5-1 网管无法接收 RMON 告警信息故障诊断流程图



5.1.3 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 检查路由器到网管端是否路由可达

在路由器端 Ping 网管端是否可以 Ping 通。

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

步骤 2 检查 SNMP 告警功能是否配置正确

在网管端检查是否可以接收到其他的告警信息，如无法接收到其他的告警信息。

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

步骤 3 检查是否配置了 RMON 统计表

在路由器端执行命令 **display rmon statistics** [**ethernet** *interface-number* | **gigabitethernet** *interface-number* | **xgigabitethernet** *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 4 检查是否使能了 RMON 统计功能

在路由器端执行命令 **display rmon statistics** [**ethernet** *interface-number* | **gigabitethernet** *interface-number* | **xgigabitethernet** *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，请在 RMON 监控的接口上使能 RMON 的统计功能。

步骤 5 检查是否使能 RMON 的事件表

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

步骤 6 检查是否使能 RMON 的告警表

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

步骤 7 检查告警变量的配置是否正确

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

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

- 上述步骤的执行结果。

- 设备的配置文件、日志信息、告警信息。

----结束

5.1.4 相关告警与日志

相关告警

无

相关日志

无

6 RMON2 故障处理

关于本章

6.1 网管无法查询到主机流经过设备的流量的定位思路

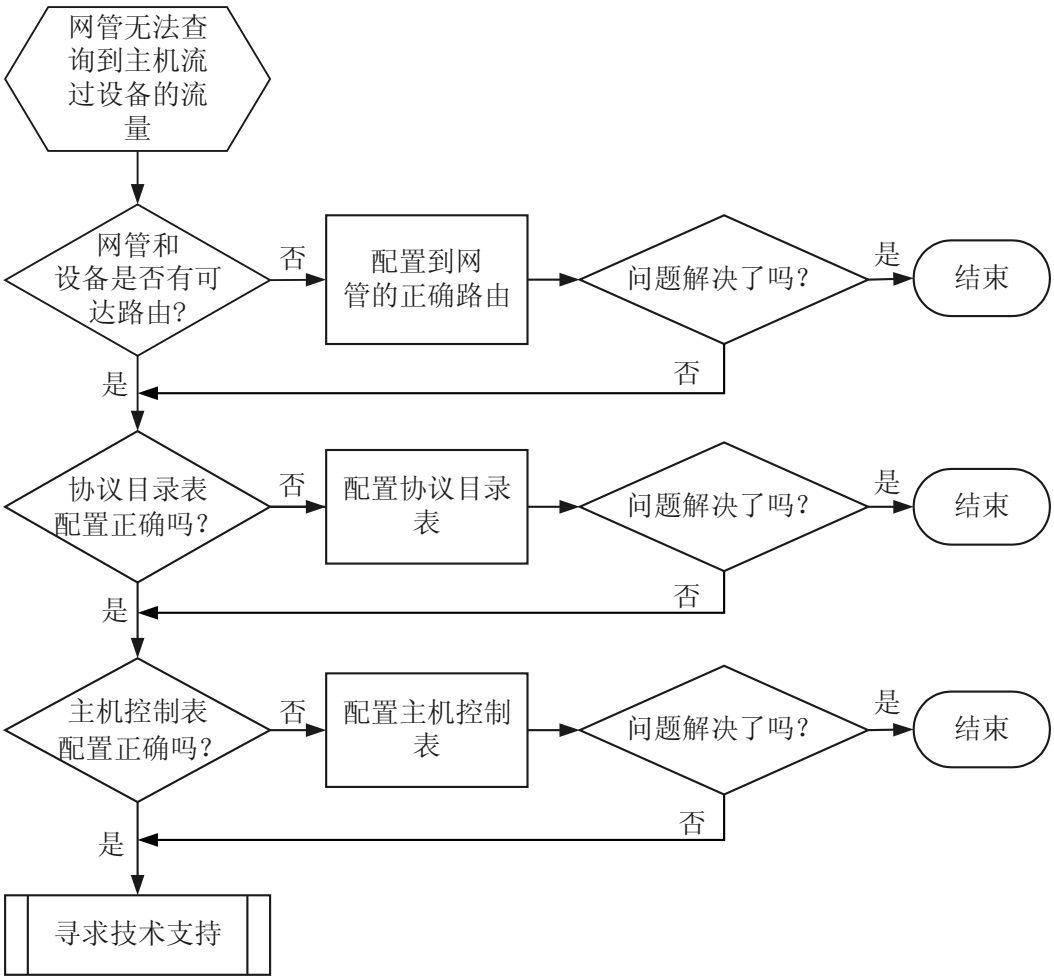
6.1.1 常见原因

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。
- RMON2 协议目录表配置不正确。
- RMON2 主机控制表配置不正确。

6.1.2 故障诊断流程

图 6-1 网管无法查询到主机流经过设备的流量故障诊断流程图



6.1.3 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 检查路由器到网管端是否路由可达

在路由器端 Ping 网管端是否可以 Ping 通。

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

步骤 2 检查 RMON2 协议目录表配置是否正确

执行命令 **display rmon2 protocoldirtable** 查看协议目录表的 protocolDirHostConfig 的值是否为 supportedOn，如果不是则主机表为空，请执行命令 **rmon2 protocoldirtable protocoldirid** 配置为 supportOn。查看协议目录表的 protocolDirStatus 的值是否为 active，如果不是则主机表为空，请配置 protocolDirStatus 为 active。

步骤 3 检查 RMON2 主机控制表配置是否正确

执行命令 **display rmon2 hlhostcontroltable** [**index** *ctrl-index*]查看主机控制表中的信息。

检查主机控制表的 hlHostControlStatus 值是否为 active，如果不是则主机表为空，请执行命令 **rmon2 hlhostcontroltable** 配置 hlHostControlStatus 值为 active。

步骤 4 如果经过上述的检查步骤，仍然无法查询到主机表的信息，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

6.1.4 相关告警与日志

相关告警

无

相关日志

无

7 NQA 故障处理

关于本章

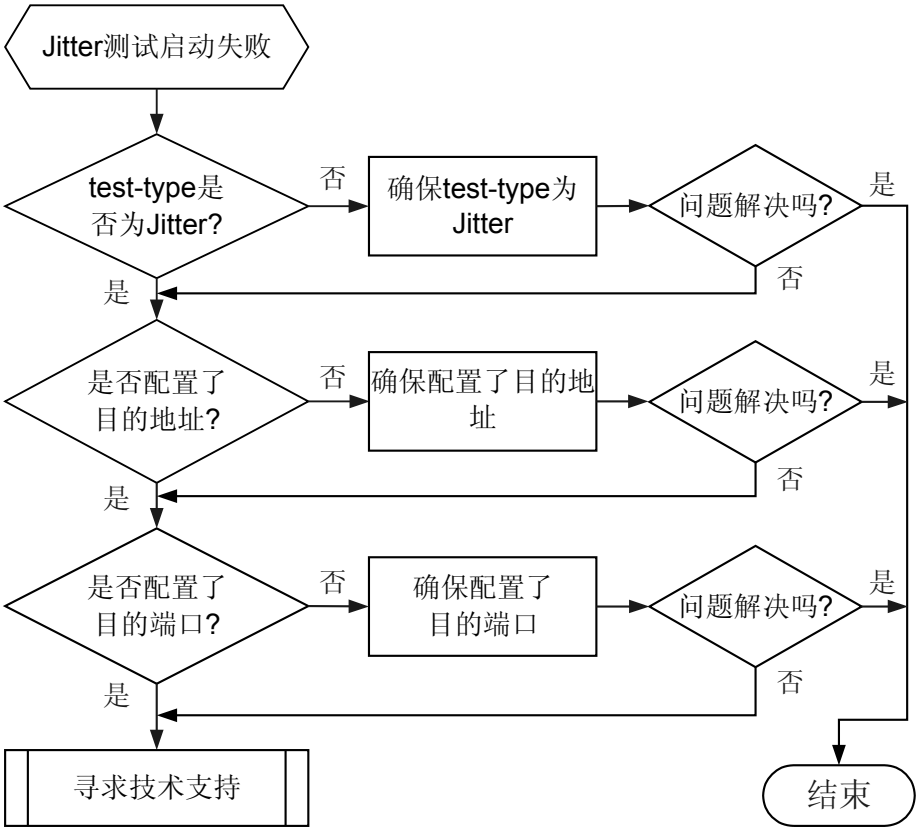
7.1 无法启动 UDP Jitter 测试的定位思路

7.1.1 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。

7.1.2 故障诊断流程

图 7-1 UDP Jitter 测试无法启动故障诊断流程图



7.1.3 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。

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

7.1.4 相关告警与日志

相关告警

无

相关日志

无

7.2 UDP Jitter 测试结果有 drop 记录的定位思路

7.2.1 常见原因

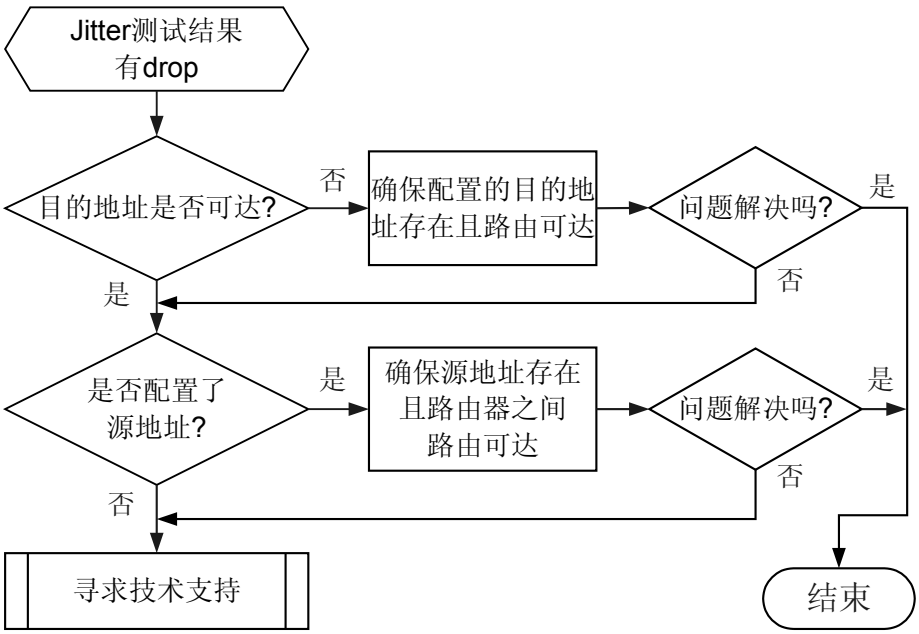
UDP Jitter 测试结果有 drop 记录是指使用 **display nqa results** 命令查看 NQA 测试的结果统计时，显示信息中“Drop operation number”字段的值不是 0。

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。

7.2.2 故障诊断流程

图 7-2 UDP Jitter 测试结果有 drop 记录的故障诊断流程图



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

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

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

- 如果是，在 NQA 客户端执行 **display ip interface brief** 命令查看是否存在配置了该源地址的接口。
  - 如果是，在 NQA 服务器端执行命令 **display ip routing-table** 查看到客户端的单播路由是否存在。
    - 如果存在，执行命令 **ping** 检查路由是否可达。
      - 如果路由可达，请执行步骤 3。
      - 如果路由不可达，请参见 **Ping 不通问题**。

- 如果不存在，请执行相应的路由配置命令，重新配置路由。
- 如果否，请重新分配接口的 IP 地址并检查 NQA 配置。

- 如果否，请执行步骤 3。

步骤 3 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

7.2.4 相关告警与日志

相关告警

无

相关日志

无

7.3 UDP Jitter 测试结果有 busy 记录的定位思路

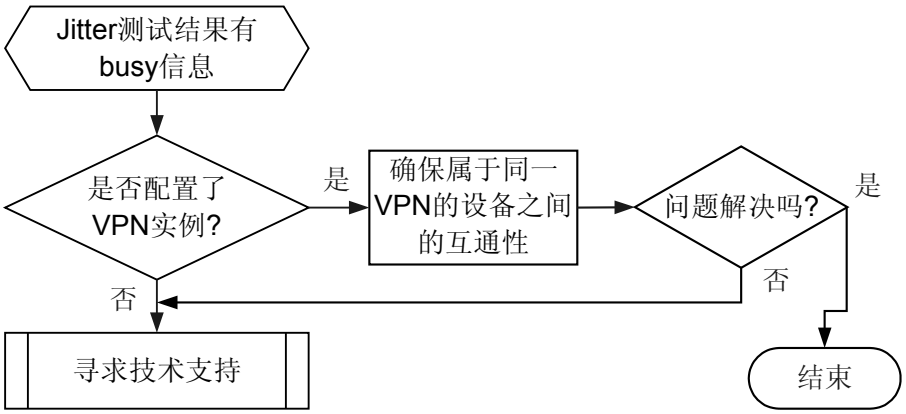
7.3.1 常见原因

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。

7.3.2 故障诊断流程

图 7-3 UDP Jitter 测试结果有 busy 记录的故障诊断流程图



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

- 如果是，请执行步骤 2。
- 如果否，请执行步骤 3。

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

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

步骤 3 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

7.3.4 相关告警与日志

相关告警

无

相关日志

无

7.4 UDP Jitter 测试结果有 timeout 记录的定位思路

7.4.1 常见原因

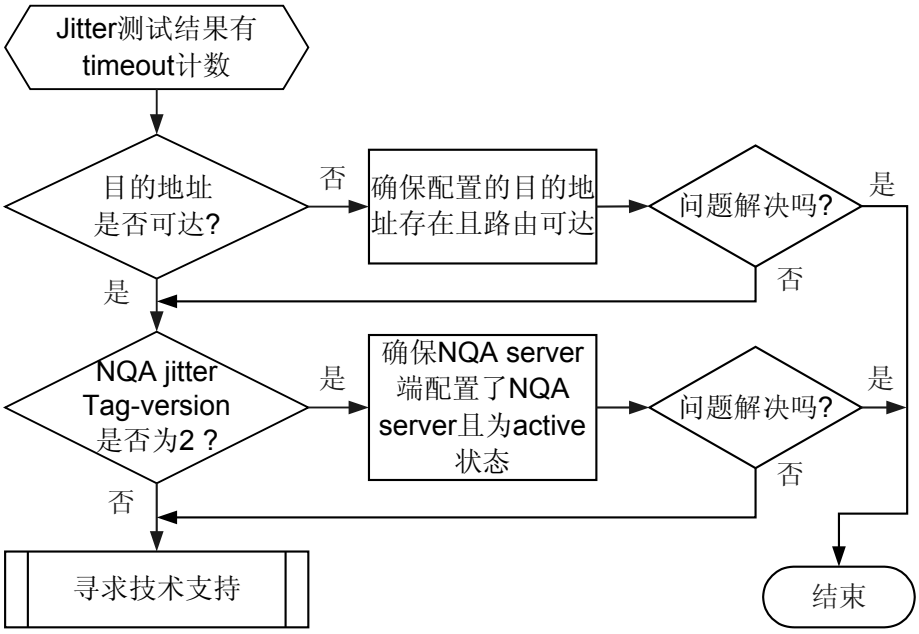
UDP Jitter 测试结果有 timeout 记录是指使用 **display nqa results** 命令查看 NQA 测试的结果统计时，显示信息中“Operation timeout number”字段的值不是 0。

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

7.4.2 故障诊断流程

图 7-4 UDP Jitter 测试结果有 timeout 记录的故障诊断流程图



7.4.3 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。

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

操作步骤

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

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

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

- 如果是，请执行步骤 3。
- 如果否，请执行步骤 4。

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

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

- 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

7.4.4 相关告警与日志

相关告警

无

相关日志

无

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

7.5.1 常见原因

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

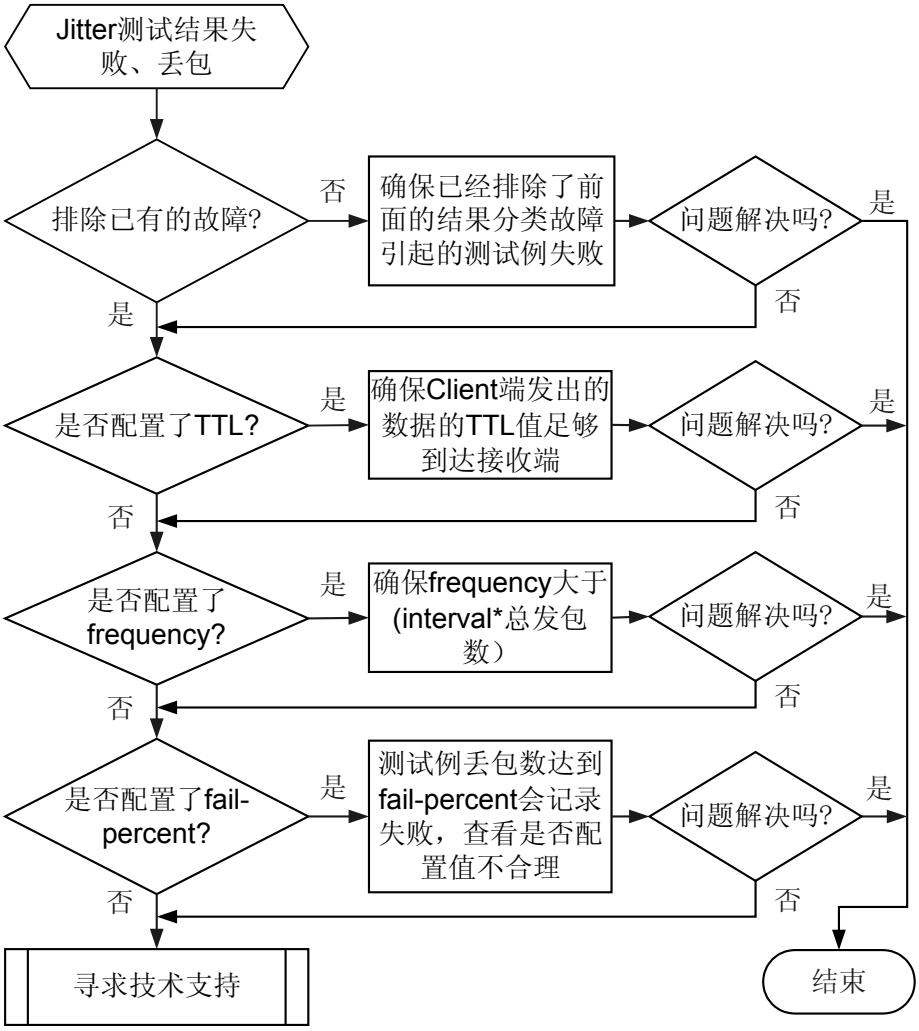
- 如果显示信息中“Completion”字段的值为“failed”，说明测试结果失败。
- 显示信息中“Completion”字段的值为“no result”，说明测试没有得到结果。
- 显示信息中“Lost packet ratio”字段的值不是 0%，说明有丢包。

本类故障的常见原因是：

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

7.5.2 故障诊断流程

图 7-5 UDP Jitter 测试结果 failed、no result 或者有丢包的故障诊断流程图



7.5.3 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。

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

7.5.4 相关告警与日志

相关告警

无

相关日志

无

8 NTP 故障诊断思路

关于本章

8.1 时钟未同步的定位思路

8.1.1 常见原因

- 链路震荡
- 链路不通

8.1.2 故障处理步骤

说明

请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

操作步骤

步骤 1 查看 NTP 状态。

```
<HUAWEI> display ntp-service status
 clock status: unsynchronized
 clock stratum: 16
 reference clock ID: none
 nominal frequency: 100.0000 Hz
 actual frequency: 99.9995 Hz
 clock precision: 2^18
 clock offset: 0.0000 ms
 root delay: 0.00 ms
 root dispersion: 0.00 ms
 peer dispersion: 0.00 ms
 reference time: 14:25:55.477 UTC Jun 9 2010(CFBA22F3.7A4B76F6)
```

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

步骤 2 查看 NTP 连接状态。

```
<HUAWEI> display ntp-service sessions
        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：

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

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

步骤 4 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

8.1.3 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

9 时钟同步故障处理

关于本章

9.1 接口无法参与选源的定位思路

9.1.1 常见原因

本类故障的常见原因主要包括：

- 同步时钟功能没有使能。
- 没有配置 SSM 参与控制。
- 接口没有配置时钟优先级。
- 接口时钟同步功能没有使能。

9.1.2 故障处理步骤

操作步骤

步骤 1 检查接口状态及链路是否正常。

请检查接口状态及链路是否正常。详细的故障处理方法请参见物理对接类的定位。如果接口及链路正常，请执行下一步。

步骤 2 如果是以太网接口，检查时钟同步功能是否使能。

执行命令 **display clock config**，查看 Ethernet synchronization 的状态是否为 enable。

- 如果状态为 disable，请在系统视图下执行命令 **clock ethernet-synchronization enable**，使能时钟同步功能。
- 如果状态为 enable 但故障仍未排除，请执行下一步。
- 如果不是以太网接口，请执行下一步。

步骤 3 检查是否配置 SSM 参与控制。

当需要保证设备在时钟选源时根据各时钟的质量等级进行选源时，才需要配置 SSM 参与控制选源。如果确认不需要配置 SSM 参与控制选源，请直接执行下一步。

执行命令 **display clock config**，查看 SSM control 状态是否为 on。

- 如果状态为 off，同时需要保证设备在时钟选源时根据各时钟的质量等级进行选源时，请执行命令 **clock ssm-control on** ，配置 SSM 参与控制。
- 如果状态为 on，但故障仍未排除，请执行下一步。

步骤 4 检查接口的配置是否正确。

在无法参与选源的接口视图下执行命令 **display clock config**，查看显示信息中该接口下是否出现“Sync enable”，Pri 项是否配置相应优先级。

- 如果没有出现“Sync enable”（没有使能接口的时钟同步功能），请在接口视图下执行命令 **clock synchronization enable** 进行配置，使能接口的时钟同步功能。
- 如果没有出现 Pri 项（没有配置接口的时钟参考源优先级），请在接口视图下执行命令 **clock** [**2msync-1** | **2msync-2**] **priority** *priority-value*，配置接口的时钟参考源优先级。

说明

配置完成后可以执行命令 **display this**，以检查配置情况。

完成上述步骤后，如果故障仍未排除，请执行下一步。

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

9.1.3 相关告警与日志

相关告警

无

相关日志

无

9.2 接口输入与对端输出的 SSM 等级不一致的定位思路

9.2.1 常见原因

执行命令 **display clock source**，发现接口输入的 SSM 等级与对端输出的 SSM 等级不一致。

本类故障的常见原因主要包括：

- 强制设置了接口的 SSM 等级。
- CE1 接口的帧格式未配置为 CRC4。

9.2.2 故障处理步骤

操作步骤

步骤 1 检查接口上是否配置了时钟源的 SSM 级别。

在发生故障的接口视图下执行命令 **display clock config**，查看该接口下是否出现 SSM 及相应级别的显示信息。

如果接口上配置了时钟源的 SSM 级别，则对端输出的时钟级别不会生效，仅以接口上的 SSM 级别为准。

只有在接口不支持 SSM 但又需要参与时钟选源时，才需要配置接口时钟源的 SSM 级别，用此级别参与时钟选源。

- 如果接口不支持 SSM 但又需要参与时钟选源，则接口输入与对端输出的 SSM 等级不一致为正常现象。无需处理。
- 如果接口支持 SSM 且接口上配置了时钟源的 SSM 级别，请在接口视图下执行命令 **undo clock ssm** 取消指定。
- 如果接口支持 SSM 且没有指定 SSM 等级，但故障仍无法排除，请执行下一步。

步骤 2 检查接口是否正常接收到了对端发送的时钟报文。

请检查并排除以下可能原因：

- 对端不能正常发送时钟报文。
- 链路故障，报文不能正常到达本端。

如果排除以上可能原因后，故障仍无法排除，请执行下一步。

步骤 3 如果是 CE1 接口，检查如下内容：

1. 在 CE1 接口视图下执行命令 **display this**，查看接口是否配置了 CRC4 的帧格式。对应配置文件如下：

   ```
   frame-format crc4
   ```

   缺省情况下，CE1 接口的帧格式为 no-CRC4。

   - 如果接口未配置帧格式为 CRC4，则对端输出的时钟级别不会生效，仅以接口上的 SSM 级别为准，请在接口视图下执行 **frame-format crc4** 进行配置。
   - 如果接口已经配置帧格式为 CRC4，故障仍无法排除，请检查两端 CE1 接口上承载 SSM 的 sa 时隙是否一致。

2. 执行命令 **display clock**，查看两端 CE1 接口上承载 SSM 的 sa 时隙是否一致。

   CE1 通过时隙携带 SSM 信息，对端要正确的收到 SSM 值需要配置两端时隙相同。

   - 如果两端 CE1 接口上承载 SSM 的 sa 时隙不一致，请在系统视图下执行 **clock sa-bit** 进行配置。
   - 如果两端 CE1 接口上承载 SSM 的 sa 时隙一致，故障仍无法排除，请执行下一步。

   如果不是 CE1 接口，请直接执行下一步。

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

9.2.3 相关告警与日志

相关告警

无

相关日志

无

9.3 无法选择高 SSM 等级时钟源的定位思路

9.3.1 常见原因

执行命令 **display clock source**，发现 SSM 等级高的接口时钟未被选为系统时钟。

本类故障的常见原因主要包括：

- 在需要 SSM 参与选源的情况下：
  - 没有配置 SSM 参与控制选源。
  - 强制或手动选择了某一时钟源。
- 在根据接口时钟源优先级选源的情况下为：
  时钟源的优先级数值越小，SSM 等级越高。

9.3.2 故障处理步骤

操作步骤

步骤 1 请根据选源模式选择以下处理步骤：

- 如果需要 SSM 参与控制选源的情况下，请执行命令 **display clock config**，查看 SSM control 的状态。
  - 如果状态为 off，请在系统视图下执行命令 **clock ssm-control on**，配置 SSM 参与控制选源。
  - 如果状态为 on 但故障仍无法排除，请执行步骤 2。
- 如果需要根据时钟源优先级选源的情况下，请执行命令 **display clock config**，检查该 Pri(sys/2m-1/2m-2)项的优先级数值是否较大。
  时钟源的优先级值越大，优先级越低。
  - 如果时钟源优先级较低，请根据时钟源类型选择配置：
    - 如果是线路时钟源，在接口视图下执行命令 **clock** [**2msync-1** | **2msync-2**] **priority** *priority-value*，调高时钟源的优先级。
    - 如果是 BITS 和 PTP 时钟源，在系统视图下执行命令 **clock priority**，调高时钟源的优先级。
  - 如果时钟源优先级数值合理但故障仍无法排除，请执行步骤 3。

步骤 2 检查是否强制选择了某一时钟源。

执行命令 **display clock config**，查看 switch config 的 sys pll 项是否出现 clock force。

- 如果是，请在系统视图下执行命令 **clock clear**，清除强制选源方式。
- 如果没有配置强制选源且故障仍无法排除，请执行步骤 3。

说明

如果进行了强制选源，系统不会根据时钟源的 SSM 级别进行选源。

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

9.3.3 相关告警与日志

相关告警

无

相关日志

无

10 NetStream

关于本章

说明

NetStream 特性在 NE80E/40E 系列中的 X1 和 X2 设备上不支持。

10.1 相关案例

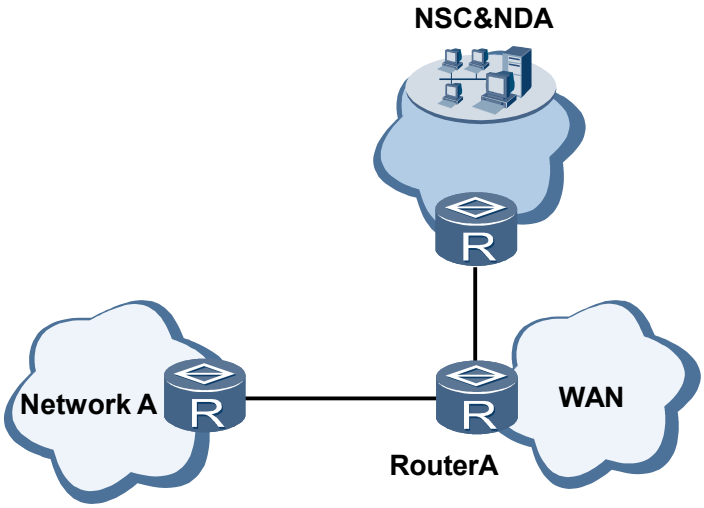
10.1.1 Netstream 无法正常采样

网络环境

在图 10-1 的网络中，网络 A 通过 RouterA 接入到 WAN（Wide Area Network）中，在 RouterA 启用 NetStream 功能，通过 NetStream 业务板集中进行流聚合和流输出的处理，将采集聚合后的流量发送到 NSC（NetStream Collector）中。NSC 设备收集和存储接收到的流量统计数据信息。NDA（NetStream Data Analyzer）对统计信息进行分析。

配置完成后，发现 NSC 无法正常接收采样数据。

图 10-1 Netstream 无法正常采样的组网图



故障分析

1. 在 RouterA 上执行命令 **display device**，检查 NetStream 业务板是否正常。发现状态 Status 为 normal，说明 NetStream 业务板正常。

```
Slot #    Type       Online    Register      Status      Primary
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
2         LPU        Present   Registered    Normal      NA
3         SPU        Present   Registered    Normal      NA
6         LPU        Present   Registered    Normal      NA
9         MPU        Present   NA            Normal      Master
10        MPU        Present   Registered    Normal      Slave
11        SFU        Present   Registered    Normal      NA
12        SFU        Present   Registered    Normal      NA
13        SFU        Present   Registered    Normal      NA
14        SFU        Present   Registered    Normal      NA
15        CLK        Present   Registered    Normal      Master
18        PWR        Present   Registered    Normal      NA
19        FAN        Present   Registered    Normal      NA
```

```
20        FAN         Present   Registered    Normal      NA
21        LCD         Present   Registered    Normal      NA
```

2. 在 RouterA 上执行命令 **display netstream all** 查看 NetStream 的配置信息，发现未指定 NetStream 业务板。所以设备无法正常输出采样报文。

```
ip netstream sampler fix-packets 1000 inbound
 ip netstream sampler fix-packets 1000 outbound
 ip netstream export source 192.168.2.1
 ip netstream export host 192.168.2.2 9001
```

操作步骤

步骤 1 在 RouterA 上执行命令 **set board-type slot** *slot-id* **netstream**，配置 SPUC 单板业务模式为 NetStream 模式。

配置完成之后，执行 **display device** *slot-id* 命令查看 Description 字段，应该显示为“Service Processing Unit - Netstream”。

步骤 2 在 RouterA 上执行命令 **system-view** 命令，进入系统视图。

步骤 3 在 RouterA 上执行命令 **slot** *slot-id*，进入需要进行 NetStream 采样的接口板的槽位视图。

步骤 4 在 RouterA 上执行命令 **ip netstream sampler to slot** *slot-id*，配置 NetStream 业务处理方式为集中式，并指定处理采样流量的 NetStream 业务板。

产品支持多块 NetStream 板，所以需要通过命令指定采样报文送到哪块 NetStream 板处理。

完成上述操作后，NSC 可以正常接受采样数据，故障排除。

----结束

案例总结

集中式的 NetStream 业务处理方式为：接口板对报文进行采样后，将采样报文送到 NetStream 业务板集中进行流聚合和流输出的处理。但是，NetStream 板需要通过命令行指定，否则会无法输出采样报文。

10.1.2 VLANIF 接口下 Netstream 原始流采样失败

网络环境

在路由器的 VLANIF 2051 上配置 NetStream 上行采样，以原始流输出。在报文分析设备上，发现没有收到采样报文，原始流采样失败。

故障分析

1. 在路由器上使用 **display ip netstream cache** 命令，查看指定 NetStream 统计输出报文的各种信息。

```
[HUAWEI] display ip netstream cache origin slot 1
Info: No required stream can be found in the cache.
```

发现原始流 cache 为空，NetStream 没有输出报文。

2. 执行命令 **display interface vlanif 2051**，检查接口是否收到了报文。

```
[HUAWEI] display interface vlanif 2051
...
    Last 300 seconds input rate: 1392 bits/sec, 0 packets/sec
    Last 300 seconds output rate: 6032 bits/sec, 0 packets/sec
```

```
    Input: 11501041 bytes, 7726 packets
    Output: 50618185 bytes, 40620 packets
    Input:
      Unicast: 15 packets, Multicast: 7664 packets
      Broadcast: 47 packets, JumboOctets: 0 packets
      CRC: 0 packets, Symbol: 0 packets
      Overrun: 0 packets, InRangeLength: 0 packets
      LongPacket: 0 packets, Jabber: 0 packets, Alignment: 0 packets
      Fragment: 0 packets, Undersized Frame: 0 packets
      RxPause: 0 packets
....
```

发现 Last 300 seconds input rate 和 input 报文情况正常，没有问题。

3. 执行命令 **display netstream all**，检查 NetStream 配置是否正确。

```
[HUAWEI]display netstream all
 system
 ip netstream sampler random-packets 1000 inbound
 ip netstream export source 10.1.1.2
 ip netstream export host 60.1.1.1 20

slot 0
Vlanif2051
 ip netstream inbound

slot 2
 ip netstream sampler to slot self
```

发现 NetStream 报文的源或目的地址配置正确，VLANIF 2051 正确使能了上行 NetStream。

但是采样方式为随机报文间隔采样，VLANIF 接口不支持随机采样，只支持固定包采样，因此原始流 Cache 为空。

操作步骤

步骤 1 在 VLANIF2051 接口视图下，执行命令 **ip netstream sampler fix-packets 1000 inbound**，配置采样方式为固定包采样。

步骤 2 执行命令 **display ip netstream cache origin slot 1**，检查原始流 Cache。

```
[HUAWEI] display ip netstream cache origin slot 1
 Show information of IP and MPLS cache of slot 1 is starting.
 get show cache user data success.


 DstIf                    DstP  Msk       Pro Tos Flags Packets
 SrcIf                    SrcP  Msk       NextHop
 DstIP                                         DstAs
 SrcIP                                         SrcAs
 BGP: BGP NextHop                 TopLabelType    Direction
 Label1           Exp1            Bottom1
 Label2           Exp2            Bottom2
 Label3           Exp3            Bottom3
 TopLabelIpAddress                VlanId
 ------------------------------------------------------------------------------
 Null                     179   0         6   192 24    72
 VL2501                   51971 0         0.0.0.0
 50.1.1.2                                      0
 50.1.1.1                                      0
 0.0.0.0                          0              in
 0                0               0
 0                0               0
 0                0               0
 0.0.0.0                                       2501
```

原始流 Cache 正常出现流，故障解决。

----结束

案例总结

VLANIF 等逻辑接口只支持 NetStream 固定包采样，不支持随机采样。

11 ACL 抓包故障处理

关于本章

11.1 配置 ACL 抓包后无法捕获报文的定位思路

11.1.1 常见原因

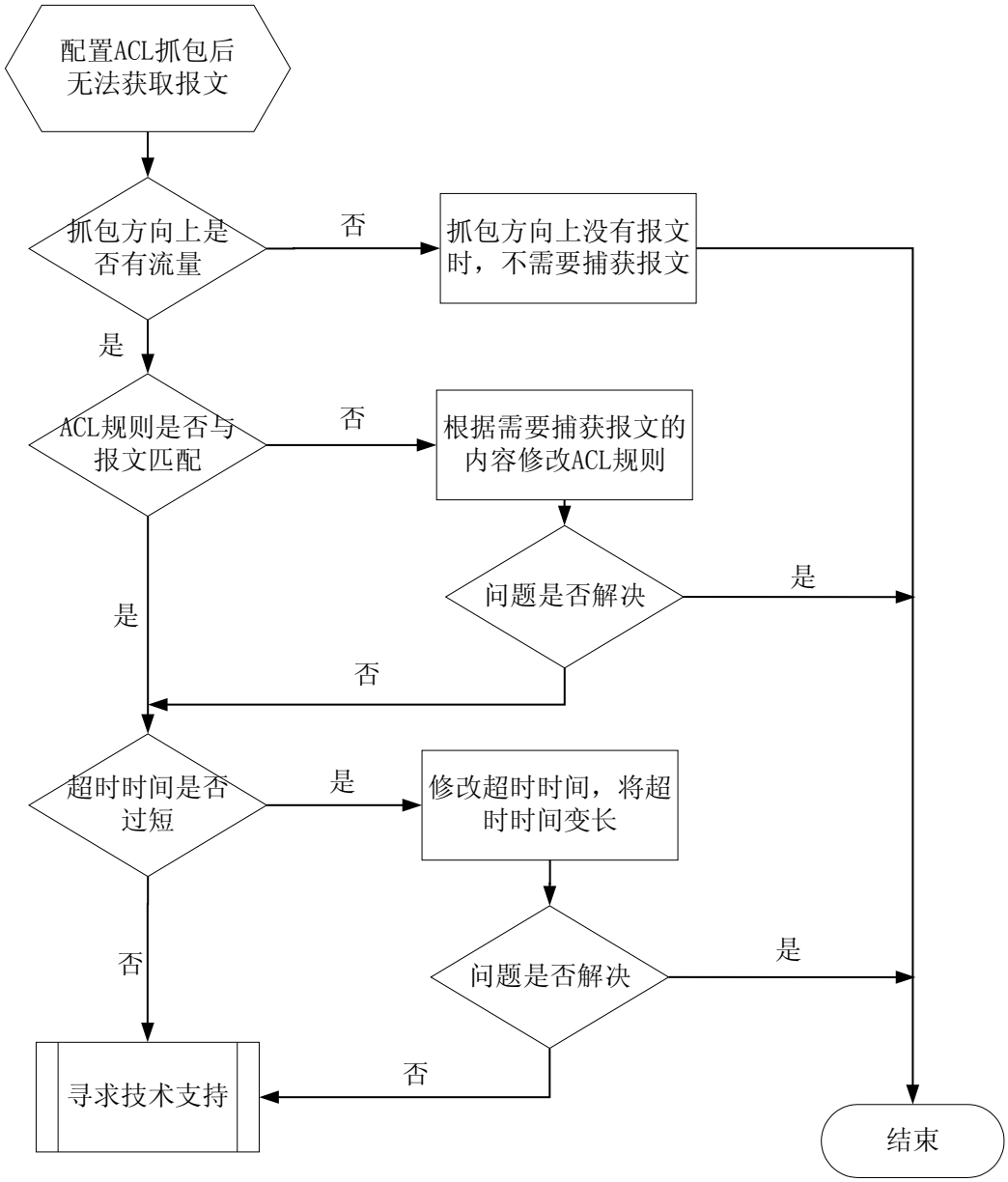
本类故障的常见原因主要包括：

- 进行 ACL 抓包的接口上无流量。
- ACL 规则匹配不正确。
- 配置超时时间过短。

11.1.2 故障诊断流程

详细处理流程如图 11-1 所示。

图 11-1 配置 ACL 抓包后无法捕获报文故障诊断流程图



11.1.3 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 检查待抓包接口是否有流量。

在设备上执行命令 **display interface** *interface-type interface-number*，查看接口是否有流量。

- 如果接口无流量，就无法捕获报文，请检查链路状况是否正常。如果链路不正常，请修复链路。
- 如果接口有流量，请执行步骤 2。

步骤 2 ACL 匹配不正确，会出现无法捕获报文或捕获到错误报文的情况。

在设备上执行命令 **display acl***acl-number*，查看配置的 ACL 规则，确认所配置的 ACL 规则是否是预期的内容。

```
<HUAWEI> display acl 3000
Advanced ACL 3000, 1 rule
Acl's step is 5
 rule 5 permit ip
```

- 如果 ACL 规则不正确，在对应的 ACL 视图下使用命令 **rule** 配置正确的规则。
- 如果配置的 ACL 规则正确，请执行步骤 3。

步骤 3 查看抓包配置的超时时间，如果超时时间过短，可能会造成捕获不到报文。

在设备上执行命令 **display capture-packet config-state** 查看抓包配置的超时时间。在捕获特定报文时，如单包攻击报文，可能超过一个小时才会有一个报文，而默认超时时间是 3600s，可以根据场景需求适当放大超时时间。

说明

攻击报文分多种，比较常见的是泛洪攻击，即大流量的攻击报文；也有利用协议 bug 单个报文就会造成重大影响的攻击方式，即单包攻击报文。

```
<HUAWEI> display capture-packet config-state
......
 ----------------------------------------
 TemplateID  : 4
 Status      : running
 CaptureType : forwarding
 Interface   : GigabitEthernet1/1/9
 Direction   : inbound
 AclNum      : --
 EnableTime  : 2011-6-24 15-41-11
 Timeout     : 3600 seconds
 PacketNum   : 10 packets
 PacketLen   : 60 Bytes
 FileSize    : 1 MB
 FileName    : cap_fwd_g1.1.9_in_2011-6-24-15-41-11.cap
 SystemID    : --
 LinkType    : --
 ----------------------------------------
......
```

- 如果超时时间过短，请执行命令 **capture-packet local-host** 配置较长的超时时间。
- 如果超时时间足够长，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。

----结束

11.1.4 相关告警与日志

相关告警

无

相关日志

无