H3C CR16000-F 故障处理手册

目 录

1 简介……1-1

1.1 故障处理注意事项……1-1

1.2 收集设备运行信息……1-1

1.2.1 logfile 日志……1-2

1.2.2 diagfile 日志……1-3

1.2.3 诊断信息……1-3

1.2.4 单板启动信息……1-5

1.3 故障处理求助方式……1-5

2 密码遗忘问题处理……2-6

2.1 遗忘 Console 口密码……2-6

2.1.1 通过 Telnet 登录设备修改 Console 口密码……2-6

2.1.2 通过 BootWare 菜单修改 Console 口密码……2-7

2.2 遗忘 Telnet 登录密码……2-12

3 使用配置文件恢复配置……3-13

4 硬件类故障处理……4-14

4.1 配置系统故障……4-14

4.1.1 终端无显示故障处理……4-14

4.1.2 终端显示乱码故障处理……4-14

4.2 单板故障……4-14

4.2.1 故障描述……4-14

4.2.2 故障处理步骤……4-15

4.3 电源故障……4-17

4.3.1 故障描述……4-17

4.3.2 故障处理步骤……4-17

4.4 风扇故障……4-17

4.4.1 故障描述……4-17

4.4.2 故障处理步骤……4-18

4.5 温度告警……4-18

4.5.1 故障描述……4-18

4.5.2 故障处理步骤……4-18

4.6 故障诊断命令……4-19

5 IRF 类故障处理 ····· 5-19
5.1 IRF 无法形成 ····· 5-19
5.1.1 故障描述 ····· 5-19
5.1.2 故障处理步骤 ····· 5-20
5.2 IRF 出现分裂 ····· 5-22
5.2.1 故障描述 ····· 5-22
5.2.2 故障处理步骤 ····· 5-22
5.3 故障诊断命令 ····· 5-25
6 系统管理维护类故障处理 ····· 6-26
6.1 CPU 占用率高 ····· 6-26
6.1.1 故障描述 ····· 6-26
6.1.2 故障处理步骤 ····· 6-28
6.2 内存占用率高 ····· 6-30
6.2.1 故障描述 ····· 6-30
6.2.2 故障处理步骤 ····· 6-30
6.3 资源不足 ····· 6-32
6.3.1 故障描述 ····· 6-32
6.3.2 故障处理步骤 ····· 6-33
6.4 主控板启动慢 ····· 6-38
6.4.1 故障描述 ····· 6-38
6.4.2 故障处理步骤 ····· 6-39
7 LDP 故障处理 ····· 7-41
7.1 LDP 会话振荡 ····· 7-41
7.1.1 故障描述 ····· 7-41
7.1.2 故障诊断流程 ····· 7-41
7.1.3 故障处理步骤 ····· 7-42
7.2 LDP 会话 down ····· 7-43
7.2.1 故障描述 ····· 7-43
7.2.2 故障诊断流程 ····· 7-43
7.2.3 故障处理步骤 ····· 7-46
7.3 LDP LSP 振荡 ····· 7-46
7.3.1 故障描述 ····· 7-46
7.3.2 故障诊断流程 ····· 7-47
7.3.3 故障处理步骤 ····· 7-47
7.4 LDP LSP down ····· 7-48
7.4.1 故障描述 ····· 7-48

7.4.2 故障诊断流程 ····· 7-48
7.4.3 故障处理步骤 ····· 7-50
8 MPLS TE 故障处理 ····· 8-51
8.1 TE 隧道状态为 down ····· 8-51
8.1.1 故障描述 ····· 8-51
8.1.2 故障诊断流程 ····· 8-51
8.1.3 故障处理步骤 ····· 8-53
8.2 TE 隧道接口由 up 突然变 down ····· 8-53
8.2.1 故障描述 ····· 8-53
8.2.2 故障诊断流程 ····· 8-53
8.2.3 故障处理步骤 ····· 8-53
8.3 TE 隧道存在环路 ····· 8-54
8.3.1 故障描述 ····· 8-54
8.3.2 故障处理步骤 ····· 8-54
8.4 SR TE 故障处理 ····· 8-54
8.4.1 故障描述 ····· 8-54
8.4.2 故障处理步骤 ····· 8-54
9 MPLS L3VPN 故障处理 ····· 9-55
9.1 缺少去往对端 VPN 实例的路由 ····· 9-55
9.1.1 故障描述 ····· 9-55
9.1.2 故障诊断流程 ····· 9-55
9.1.3 故障处理步骤 ····· 9-57
9.2 VPN 实例下的 FIB 表项异常 ····· 9-58
9.2.1 故障描述 ····· 9-58
9.2.2 故障诊断流程 ····· 9-59
9.2.3 故障处理步骤 ····· 9-59
10 MPLS L2VPN/VPLS 故障处理 ····· 10-60
10.1 VPLS 的 VSI 不能 up ····· 10-60
10.1.1 故障描述 ····· 10-60
10.1.2 故障诊断流程 ····· 10-62
10.1.3 故障处理步骤 ····· 10-64
11 MPLS 业务丢包故障处理 ····· 11-65
11.1 故障描述 ····· 11-65
11.1 L3VPN 丢包故障处理步骤 ····· 11-65
11.1.1 Ingress 节点丢包定位 ····· 11-65
11.1.2 P 节点丢包定位 ····· 11-66

11.1.3 egress 节点丢包定位 ····· 11-66
11.1.4 联系技术支持工程师 ····· 11-66
11.2 L2VPN 丢包故障处理步骤 ····· 11-67
11.2.1 Ingress 节点丢包定位 ····· 11-67
11.2.2 P 节点丢包定位 ····· 11-67
11.2.3 egress 节点丢包定位 ····· 11-68
11.2.4 联系技术支持工程师 ····· 11-68
11.3 VPLS 丢包故障处理步骤 ····· 11-68
11.3.1 Ingress 节点丢包定位 ····· 11-68
11.3.2 P 节点丢包定位 ····· 11-69
11.3.3 egress 节点丢包定位 ····· 11-69
11.3.4 联系技术支持工程师 ····· 11-69
11.4 MPLS 丢包问题定位实例 ····· 11-70
11.4.1 组网环境 ····· 11-70
11.4.2 使用 QoS 策略定位丢包设备 ····· 11-70
11.4.3 使用 diffserver 定位丢包设备 ····· 11-72
12 报文转发故障处理 ····· 12-73
12.1 ping 不通或丢包 ····· 12-73
12.1.1 故障描述 ····· 12-73
12.1.2 故障处理步骤 ····· 12-73
12.2 VLAN 转发故障 ····· 12-75
12.2.1 故障描述 ····· 12-75
12.2.2 故障处理步骤 ····· 12-75
12.3 聚合口故障 ····· 12-75
12.3.1 故障描述 ····· 12-75
12.3.2 故障处理步骤 ····· 12-76
12.4 MAC 地址学习故障 ····· 12-76
12.4.1 故障描述 ····· 12-76
12.4.2 故障处理步骤 ····· 12-77
12.5 L3 转发故障 ····· 12-77
12.5.1 故障描述 ····· 12-77
12.5.2 故障处理步骤 ····· 12-78
12.6 MPLS 转发故障 ····· 12-79
12.6.1 故障描述 ····· 12-79
12.6.2 故障处理步骤 ····· 12-79
12.7 VXLAN 转发故障 ····· 12-81

12.7.1 故障描述 ····· 12-81
12.7.2 故障处理步骤 ····· 12-82
12.8 BFD 转发故障 ····· 12-83
12.8.1 故障描述 ····· 12-83
12.8.2 故障诊断流程 ····· 12-84
12.8.3 故障处理步骤 ····· 12-84
12.9 RADIUS 故障 ····· 12-86
12.9.1 故障描述 ····· 12-86
12.9.2 故障处理步骤 ····· 12-86
12.10 NAT 故障 ····· 12-88
12.10.1 故障描述 ····· 12-88
12.10.2 故障处理步骤 ····· 12-88
12.11 PTP 故障 ····· 12-90
12.11.1 故障描述 ····· 12-90
12.11.2 故障处理步骤 ····· 12-90
12.12 NetStream 故障处理 ····· 12-92
12.12.1 常见原因 ····· 12-92
12.12.2 故障诊断流程 ····· 12-93
12.12.3 故障处理步骤 ····· 12-93
12.13 L2MC 转发故障 ····· 12-95
12.13.1 故障描述 ····· 12-95
12.13.2 故障处理步骤 ····· 12-95
12.14 L3MC 转发故障 ····· 12-96
12.14.1 故障描述 ····· 12-96
12.14.2 故障处理步骤 ····· 12-96
12.15 QACL 业务故障 ····· 12-106
12.15.1 故障描述 ····· 12-106
12.15.2 故障处理步骤 ····· 12-106
12.16 QoS 业务故障 ····· 12-109
12.16.1 故障描述 ····· 12-109
12.16.2 故障处理步骤 ····· 12-109
12.17 NQA TWAMP-light 测试故障 ····· 12-109
12.17.1 故障描述 ····· 12-109
12.17.2 故障处理步骤 ····· 12-110
12.18 路径服务质量测试故障 ····· 12-110
12.18.1 故障描述 ····· 12-110

12.18.2 故障处理步骤 ····· 12-111
12.19 UDP-jitter 测试故障 ····· 12-111
12.19.1 故障描述 ····· 12-111
12.19.2 故障处理步骤 ····· 12-111
12.20 Y.1564 测试故障 ····· 12-112
12.20.1 故障描述 ····· 12-112
12.20.2 故障处理步骤 ····· 12-112
13 链路端口故障处理 ····· 13-114
13.1 端口错包 ····· 13-114
13.1.1 故障描述 ····· 13-114
13.1.2 故障处理步骤 ····· 13-115
13.2 端口无法 up ····· 13-116
13.2.1 故障描述 ····· 13-116
13.2.2 故障处理步骤 ····· 13-116
13.3 端口由 up 变成 down ····· 13-117
13.3.1 故障描述 ····· 13-117
13.3.2 故障处理步骤 ····· 13-117
13.4 端口频繁 up/down ····· 13-118
13.4.1 故障描述 ····· 13-118
13.4.2 故障处理步骤 ····· 13-118
13.5 光模块故障 ····· 13-118
13.5.1 故障描述 ····· 13-118
13.5.2 故障处理步骤 ····· 13-118
13.6 端口不可见 ····· 13-121
13.6.1 故障描述 ····· 13-121
13.6.2 故障处理步骤 ····· 13-122
13.7 WAN 口协议不 up ····· 13-123
13.7.1 故障描述 ····· 13-123
13.7.2 故障处理步骤 ····· 13-123
13.8 WAN 口物理不 up ····· 13-123
13.8.1 故障描述 ····· 13-123
13.8.2 故障处理步骤 ····· 13-124
13.9 WAN 口打印告警信息 ····· 13-125
13.9.1 故障描述 ····· 13-125
13.9.2 故障处理步骤 ····· 13-125
13.10 故障诊断命令 ····· 13-126

14 IP 业务故障处理 14-126
14.1 ARP 故障 14-126
14.1.1 故障描述 14-126
14.1.2 故障处理步骤 14-126
14.2 DHCP 中继故障处理 14-129
14.2.1 故障描述 14-129
14.2.2 故障处理步骤 14-129
14.3 ND 故障处理 14-130
14.3.1 故障描述 14-130
14.3.2 故障处理步骤 14-130
14.4 IPv6 Ping 不通或丢包 14-130
14.4.1 故障描述 14-130
14.4.2 故障处理步骤 14-131
14.5 MTU 故障处理 14-132
14.5.1 故障描述 14-132
14.5.2 故障处理步骤 14-132
15 硬件转发故障 15-134
15.1 HG 故障 15-134
15.1.1 故障描述 15-134
15.1.2 故障处理步骤 15-136
15.2 FMEA 故障 15-137
15.2.1 故障描述 15-137
15.2.2 故障处理步骤 15-137

1 简介

本文档介绍 CR16000-F 产品软、硬件常见故障的诊断及处理措施。

本文档适用于 Release CR16000-CMW710-R8151PXX。

1.1 故障处理注意事项

注意

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

在进行故障诊断和处理时，请注意以下事项：

- 设备出现故障时，请尽可能全面、详细地记录现场信息（包括但不限于以下内容），收集信息越全面、越详细，越有利于故障的快速定位。
  - 记录具体的故障现象、故障时间、配置信息。
  - 记录完整的网络拓扑，包括组网图、端口连接关系、故障位置。
  - 收集设备的日志信息和诊断信息（收集方法见 1.2 收集设备运行信息）。
  - 记录设备故障时单板、电源、风扇指示灯的状态，或给现场设备拍照记录。
  - 记录现场采取的故障处理措施（比如配置操作、插拔线缆、手工重启设备）及实施后的现象效果。
  - 记录故障处理过程中配置的所有命令行显示信息。
- 更换和维护设备部件时，请佩戴防静电手腕，以确保您和设备的安全。
- 故障处理过程中如需更换硬件部件，请参考与软件版本对应的版本说明书，确保新硬件部件和软件版本的兼容性。比如说：带有微动开关的网板，只要出现过弹开又合上的情况，一定要重新拔插一下网板。

1.2 收集设备运行信息

说明

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

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

表1 设备运行信息介绍

分类	文件名	内容
logfile日志	logfileX.log	命令行记录、设备运行中产生的记录信息
diagfile日志	diagfileX.log	设备运行中产生的诊断日志信息，如系统运行到错误流程时的参数值、单板无法启动时的信息、主控板与接口板通信异常时的握手信息。
诊断信息	XXX.gz	系统当前多个功能模块运行的统计信息，包括设备状态、CPU状态、内存状态、配置情况、软件表项、硬件表项等


说明

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

1.2.1 logfile 日志

(1) 执行 **logfile save** 命令将日志文件缓冲区中的内容全部保存到日志文件中。日志文件缺省存储在存储设备根目录下的 logfile 文件夹中。

```
<Sysname> logfile save
The contents in the log file buffer have been saved to the file
cfa0:/logfile/logfile1.log
```

(2) 查看设备上主用主控板、备用主控板、IRF 中主设备/从设备上各主用/备用主控板的日志文件数目和名称。

- 主用主控板 logfile 日志：

```
<Sysname> dir cfa0:/logfile/
Directory of cfa0:/logfile
   0 -rw-       21863 Jul 11 2013 16:00:37   logfile1.log

1021104 KB total (421552 KB free)
```

- 备用主控板 logfile 日志：

```
<Sysname> dir slot1#cfa0:/logfile/
Directory of slot1#cfa0:/logfile
   0 -rw-       21863 Jul 11 2013 16:00:37   logfile1.log

1021104 KB total (421552 KB free)
```

- IRF 备框主控板 logfile 日志，如备框有两块主控板，则两块都需要检查：

```
<Sysname> dir chassis2#slot0#cfa0:/logfile/
Directory of chassis2#slot0#cfa0:/logfile
   0 -rw-       21863 Jul 11 2013 16:00:37   logfile1.log

1021104 KB total (421552 KB free)
```

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

1.2.2 diagfile 日志

(1) 执行 **diagnostic-logfile save** 命令将诊断日志文件缓冲区中的内容全部保存到诊断日志文件中。诊断日志文件缺省存储在存储设备根目录下的 diagfile 文件夹中。

- 在设备上收集对应的诊断日志文件。

```
<Sysname> diagnostic-logfile save
The contents in the diagnostic log file buffer have been saved to the file
cfa0:/diagfile/diagfile1.log
```

(2) 查看设备上主用主控板、备用主控板、IRF 中主设备/从设备上各主用/备用主控板的诊断日志文件数目和名称。

- 主用主控板 diagfile 日志：

```
<Sysname> dir cfa0:/diagfile/
Directory of cfa0:/diagfile
   0 -rw-      161321 Jul 11 2013 16:16:00   diagfile1.log

1021104 KB total (421416 KB free)
```

- 备用主控板 diagfile 日志：

```
<Sysname> dir slot1#cfa0:/diagfile/
Directory of slot1#cfa0:/diagfile
   0 -rw-      161321 Jul 11 2013 16:16:00   diagfile1.log

1021104 KB total (421416 KB free)
```

- IRF 各成员设备主控板 diagfile 日志，如果成员设备有两块主控板，则两块都需要检查：

```
<Sysname> dir chassis2#slot0#cfa0:/diagfile/
Directory of chassis2#slot0#cfa0:/diagfile
   0 -rw-      161321 Jul 11 2013 16:16:00   diagfile1.log

1021104 KB total (421416 KB free)
```

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

1.2.3 诊断信息

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

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

说明

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

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

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

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

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

(3) 选择将诊断信息保存至文件中，还是将直接在屏幕上显示。

- 输入“Y”，以及保存诊断信息的路径和名称，将诊断信息保存至文件中。

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

1021808 KB total (259072 KB free)
```

- 输入“N”，将诊断信息直接显示在屏幕上。

```
Save or display diagnostic information (Y=save, N=display)? [Y/N] :N
============================================================
  ===============display alarm===============
No alarm information.
============================================================
  ===============display boot-loader===============
Software images on slot 0:
Current software images:
  cfa0:/BOOT-R8151PXX.bin
  cfa0:/SYSTEM-R8151PXX.bin
Main startup software images:
  cfa0:/BOOT-R8151PXX.bin
  cfa0:/SYSTEM-R8151PXX.bin
Backup startup software images:
  None
============================================================
  ===============display counters inbound interface===============
Interface         Total (pkts)   Broadcast (pkts)   Multicast (pkts)  Err (pkts)
BAGG1                        0                  0                  0           0
GE4/0/1                      0                  0                  0           0
GE4/0/2                      2                  2                  0           0
GE4/0/3                      0                  0                  0           0
GE4/0/4                      0                  0                  0           0
GE4/0/5                      0                  0                  0           0
GE4/0/6                      0                  0                  0           0
GE4/0/7                      0                  0                  0           0
GE4/0/8                      0                  0                  0           0
GE4/0/9                      0                  0                  0           0
```

```
GE4/0/10                    0                   0                   0           0
```

1.2.4 单板启动信息

单板启动阶段的最后 32 条信息会记录到保留内存，不管单板能否启动，只要不下电就能查看。单板正常启动状态为 normal 后，在 probe 视图下，通过 **display hardware internal boot information current** 命令行查看。当接口板启动时发生重启且一直重启无法正常启动，就无法通过此命令行查看，此时，单板会在 boot 阶段将上一次启动前的信息上传到主控板并保存到 CF 卡的 info 目录下以供查看。

当接口板无限重启只会保存最开始的 2 个文件，之后的不再保存以节约空间。可以通过以下步骤进行查看单板启动信息：

(1) 进入 CF 卡下的 info 目录可以查看上传的文件。

```
<Sysname>cd cfa0:/info/
<Sysname>dir
Directory of cfa0:/info
   0 -rw-        6952 Jul 07 2016 10:19:24   info_3_0.bin
```

以上显示信息中 3 为上传的接口板槽位号，0 为序号，如果有多个文件就会依次排序。

(2) 在 probe 视图下通过命令行 **display drvplat boot-info-record file** 就可以查看该单板的启动信息。

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] probe
[Sysname-probe] display drvplat boot-info-record file cfa0:/info/info_3_0.bin

 Slot 0, CPU 0
 Total number of boot info in reserved memory: 32
 ------------------------------------------------------------
2016/07/07, 09:19:07. NAT GMAC init end [OK]
2016/07/07, 09:18:48. IBC phase2 init end [OK]
2016/07/07, 09:18:48. Contorl channel count record init [OK]
2016/07/07, 09:18:45. BFD global data init [OK]
2016/07/07, 09:18:45. FWD phase2 init end [OK]
2016/07/07, 09:18:45. FWD init phase2 pe traffic enable pass, init phase2 end.
2016/07/07, 09:18:44. Get clock global config succeed. [OK]
2016/07/07, 09:18:44. BRAS task init [OK]
2016/07/07, 09:18:44. Mpls phase2 init [OK]
```

1.3 故障处理求助方式

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

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

2 密码遗忘问题处理

2.1 遗忘Console口密码

您可以通过如下方法恢复 Console 口密码。

- 方法一：通过 Telnet 登录设备修改 Console 口密码。请优先使用该方法。
- 方法二：通过 BootWare 菜单修改 Console 口密码。

2.1.1 通过 Telnet 登录设备修改 Console 口密码

使用本方法需满足以下条件：

- 用户可以通过 Telnet 登录设备（比如忘记了 Telnet 登录密码，就不符合本条件；此时建议联系技术支持进行协助）。
- 用户角色名为 network-admin 或 level-15。

(1) 通过 Telnet 方式登录设备，并确认当前 VTY 用户的用户角色名。

查看当前正在使用的用户线及用户的相关信息。

```
<Sysname> display users
  Idx  Line    Idle       Time               Pid     Type
  0    CON 0   00:01:13   Feb 19 17:34:43    543
+ 28   VTY 0   00:00:00   Nov 11 11:38:55    1865    TEL

Following are more details.
VTY 0   :
        Location: 192.168.33.13
 +    : Current operation user.
 F    : Current operation user works in async mode.
```

以上显示信息表明，当前有两个用户已经登录设备，用户自己使用的是 VTY 0 用户线，用户的 IP 地址为 192.168.33.13；另一个用户使用的是 CON 0 用户线。

在 VTY 0 用户视图下查看配置、确认该用户的权限：可看到 VTY 0 的用户角色权限为 level-15，有权限修改 Console 口密码。

```
[Sysname] line vty 0
[Sysname-line-vty0] display this
#
line aux 0
 user-role network-operator
#
line con 0
 user-role network-admin
#
line vty 0
 authentication-mode none
 user-role level-15
 user-role network-admin
 user-role network-operator
```

```
#
return
```

(2) 修改 Console 用户的密码（假设认证方式为 password 方式）。

```
<Sysname> system-view
[Sysname] line console 0
[Sysname-line-console0] user-role level-15
[Sysname-line-console0] user-role network-admin
[Sysname-line-console0] authentication-mode password
[Sysname-line-console0] set authentication password simple 12345678
[Sysname-line-console0] return
```

(3) 为了防止重启后配置丢失，请保存配置。

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N] :y
Please input the file name(*.cfg)[flash:/default.cfg]
(To leave the existing filename unchanged, press the enter key):default.cfg
Validating file. Please wait....
Saved the current configuration to mainboard device successfully.
```

2.1.2 通过 BootWare 菜单修改 Console 口密码

通过 BootWare 菜单解决 Console 口密码遗忘问题的方式与设备上是否使能了密码恢复功能相关，可通过以下方法判断设备是否使能了密码恢复功能：

- 通过进入 BootWare 主菜单后的显示信息来判断。
- telnet 登录当前设备后，通过查看当前设备上的配置信息来判断。

查看当前设备上的配置信息。

```
<Sysname> display current-configuration
#
 version 7.1.075, Release 8151P12
#
mdc Admin id 1
#
 sysname Sysname
#
 command-alias enable
 command-alias mapping undo no
 command-alias mapping quit exit
 command-alias mapping return end
#
system-working-mode bridgee
 password-recovery enable
#
```

以上显示信息表明，当前设备使能了密码恢复功能。

1. 密码恢复功能处于使能状态

使能密码恢复功能后，设备的 BootWare 菜单支持配置“Skip Authentication for Console Login”选项，选择该选项并重启设备后，设备以下次启动配置文件启动，登录 Console 口时会跳过认证密码，进入到命令行操作界面。

注意

- 进入 BootWare 菜单需要重启设备，会导致业务中断，请视具体情况做好业务备份，并尽量选择业务量较少的时间操作。
- 跳过 Console 口密码登录后请马上配置新的密码，否则登录超时或重启后，仍需要跳过密码来登录。
- 在此操作过程中不要对设备下电。

(1) 用串口线连接配置终端和设备，然后重启设备，当终端屏幕上出现“Press Ctrl+B to access EXTENDED-BOOTWARE MENU...”的 3 秒钟之内，键入<Ctrl+B>，系统将进入 BootWare 主菜单。

```
System is starting...
Press Ctrl+D to access BASIC-BOOTWARE MENU...
Press Ctrl+T to start memory test
Booting Normal Extended BootWare
The Extended BootWare is self-decompressing.........Done.

********************************************************************************
*                                                                              *
*                       H3C BootWare, Version 1.48                             *
*                                                                              *
********************************************************************************
Compiled Date         : Mar 4 2020
CPU Type              : XLP316
CPU Clock Speed       : 1200MHz
Memory Type           : DDR3 SDRAM
Memory Size           : 8192MB
Memory Speed          : 667MHz
BootWare Size         : 1536KB
Flash Size            : 500MB
BASIC CPLD Version    : 1.0
EXTENDED CPLD Version : 1.0
PCB Version           : Ver.A


BootWare Validating...
Press Ctrl+B to access EXTENDED-BOOTWARE MENU...
```

(2) 键入“8”并回车，跳过 Console 口密码登录。

```
Password recovery capability is enabled.
Note: The current operating device is flash
Enter < Storage Device Operation > to select device.

==========================<EXTENDED-BOOTWARE MENU>==========================
|<1> Boot System                                                           |
|<2> Enter Serial SubMenu                                                  |
|<3> Enter Ethernet SubMenu                                                |
```

```
|<4> File Control                                                          |
|<5> Restore to Factory Default Configuration                              |
|<6> Skip Current System Configuration                                     |
|<7> BootWare Operation Menu                                               |
|<8> Skip Authentication for Console Login                                 |
|<9> Storage Device Operation                                              |
|<0> Reboot                                                                |
==========================================================================
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format File System
Enter your choice(0-9): 8
Clear Image Password Success!
```

(3) 重启设备。

```
==========================<EXTENDED-BOOTWARE MENU>==========================
|<1> Boot System                                                           |
|<2> Enter Serial SubMenu                                                  |
|<3> Enter Ethernet SubMenu                                                |
|<4> File Control                                                          |
|<5> Restore to Factory Default Configuration                              |
|<6> Skip Current System Configuration                                     |
|<7> BootWare Operation Menu                                               |
|<8> Skip Authentication for Console Login                                 |
|<9> Storage Device Operation                                              |
|<0> Reboot                                                                |
==========================================================================
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format File System
Enter your choice(0-9):  0
System is starting...
Booting Normal Extend BootWare
The Extend BootWare is self-decompressing.............................
Done.
```

(4) 完成设备启动后，通过 Console 口登录时不需要认证。登录后请及时修改 Console 口密码（假设认证方式为 password 方式）。

```
<Sysname> system-view
[Sysname] line console 0
[Sysname-line-console0] authentication-mode password
[Sysname-line-console0] set authentication password simple 12345678
[Sysname-line-console0] return
```

(5) 为防止重启后配置丢失，请保存配置。

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N] :y
Please input the file name(*.cfg)[flash:/default.cfg]
(To leave the existing filename unchanged, press the enter key):default.cfg
Validating file. Please wait....
Saved the current configuration to mainboard device successfully.
```

2. 密码恢复功能处于关闭状态

密码恢复功能处于关闭状态时，设备的 BootWare 菜单支持配置“Restore to Factory Default Configuration”选项，选择该选项并重启设备后，设备会先自动删除下次启动配置文件，再以出厂配置启动。

 注意

- 恢复出厂配置后原有配置会丢失，造成业务中断，请谨慎。
- 在此操作过程中不要对设备进行下电。

---

(1) 用串口线连接配置终端和设备，然后重启设备，当终端屏幕上出现“Press Ctrl+B to access EXTENDED-BOOTWARE MENU...”的 3 秒钟之内，键入<Ctrl+B>，系统将进入 BootWare 主菜单。

```
System is starting...
Press Ctrl+D to access BASIC-BOOTWARE MENU...
Press Ctrl+T to start memory test
Booting Normal Extended BootWare
The Extended BootWare is self-decompressing.........Done.

********************************************************************************
*                                                                              *
*                       H3C BootWare, Version 1.48                             *
*                                                                              *
********************************************************************************
Compiled Date         : Mar  4 2020
CPU Type              : XLP316
CPU Clock Speed       : 1200MHz
Memory Type           : DDR3 SDRAM
Memory Size           : 8192MB
Memory Speed          : 667MHz
BootWare Size         : 1536KB
Flash Size            : 500MB
BASIC CPLD Version    : 1.0
EXTENDED CPLD Version : 1.0
PCB Version           : Ver.A


BootWare Validating...
Press Ctrl+B to access EXTENDED-BOOTWARE MENU...
```

(2) 键入“5”并回车，恢复出厂默认配置。

```
Password recovery capability is disabled.
Note: The current operating device is flash
Enter < Storage Device Operation > to select device.

==========================<EXTENDED-BOOTWARE MENU>==========================
```

```
|<1> Boot System                                                        |
|<2> Enter Serial SubMenu                                               |
|<3> Enter Ethernet SubMenu                                             |
|<4> File Control                                                       |
|<5> Restore to Factory Default Configuration                           |
|<6> Skip Current System Configuration                                  |
|<7> BootWare Operation Menu                                            |
|<8> Skip Authentication for Console Login                              |
|<9> Storage Device Operation                                           |
|<0> Reboot                                                             |
==========================================================================
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format File System
Enter your choice(0-9): 5
Because the password recovery capability is disabled, this operation can
cause the configuration files to be deleted, and the system will start up
with factory defaults. Are you sure to continue?[Y/N]Y
Setting...Done.
```

(3) 重启设备，以出厂默认配置启动。

```
============================<EXTENDED-BOOTWARE MENU>============================
|<1> Boot System                                                        |
|<2> Enter Serial SubMenu                                               |
|<3> Enter Ethernet SubMenu                                             |
|<4> File Control                                                       |
|<5> Restore to Factory Default Configuration                           |
|<6> Skip Current System Configuration                                  |
|<7> BootWare Operation Menu                                            |
|<8> Skip Authentication for Console Login                              |
|<9> Storage Device Operation                                           |
|<0> Reboot                                                             |
==========================================================================
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format File System
Enter your choice(0-9):  0
System is starting...
Booting Normal Extend BootWare
The Extend BootWare is self-decompressing.............................
Done.
```

(4) 设备以出厂默认配置启动后，通过 Console 口登录时不需要认证。登录后请及时修改 Console 口密码（假设认证方式为 password 方式）。

```
<Sysname> system-view
[Sysname] line console 0
[Sysname-line-console0] authentication-mode password
[Sysname-line-console0] set authentication password simple 12345678
[Sysname-line-console0] return
```

(5) 为防止重启后配置丢失，请保存配置。

```
<Sysname> save
```

```
The current configuration will be written to the device. Are you sure? [Y/N] :y
Please input the file name(*.cfg)[flash:/default.cfg]
(To leave the existing filename unchanged, press the enter key):default.cfg
Validating file. Please wait....
Saved the current configuration to mainboard device successfully.
```

2.2 遗忘Telnet登录密码

如果 Telnet 登录密码丢失，可以通过 Console 口登录设备后重新配置 Telnet 登录密码。

(1) 通过 Console 口登录设备。

(2) 对 VTY 用户（下面以 VTY0～63 为例）配置密码 123456，并保存配置。

```
<Sysname> system-view
[Sysname] line vty 0 63
[Sysname-line-vty0-63] authentication-mode password
[Sysname-line-vty0-63] set authentication password simple 123456
[Sysname-line-vty0-63] return
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N] :y
Please input the file name(*.cfg)[flash:/default.cfg]
(To leave the existing filename unchanged, press the enter key):default.cfg
Validating file. Please wait....
Saved the current configuration to mainboard device successfully
```

3 使用配置文件恢复配置

缺省情况下，设备的启动配置文件为flash:/config.cfg。设备上电时，从缺省存储路径中读取config.cfg文件进行设备的初始化操作。如果缺省存储路径中没有配置文件，则设备采用缺省参数进行初始化配置。

如果想要将设备当前配置恢复成以前保存过的某个配置，可以通过下面的步骤完成。

(1) 通过FTP或TFTP方式将用于恢复的配置文件上传到设备的所有主控板上（以FTP方式举例，上传的配置文件名为 config.cfg）。

将用于恢复的配置文件上传到主用主控板。

```
<Sysname> ftp 192.168.33.13
Press CTRL+C to abort.
Connected to 192.168.33.13 (192.168.33.13).
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User (192.168.33.13:(none)): 1
331 Give me your password, please
Password:
230 Logged in successfully
Remote system type is MSDOS.
ftp> binary
200 Type is Image (Binary)
ftp> get config.cfg
227 Entering Passive Mode (192,168,33,13,209,24)
150 "F:\config.cfg" file ready to send (18494 bytes) in IMAGE / Binary mode
226 Transfer finished successfully.
18494 bytes received in 0.0383 seconds (471.1 kbyte/s)
ftp> quit
221 Windows FTP Server (WFTPD, by Texas Imperial Software) says goodbye
```

将主用主控板的 config.cfg 配置文件拷贝到备用主控板。

```
<Sysname> copy config.cfg slot1#cfa0:/config.cfg
Copy cfa0:/config.cfg to slot1#cfa0:/config.cfg?[Y/N] :y
.
%Copy file cfa0:/config.cfg to slot1#cfa0:/config.cfg...Done.
```

(2) 设置下次启动时使用的配置文件，以便下次启动后设备恢复到此配置。

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

需要注意的是，如果用于恢复的配置文件名为 config.cfg（和设备缺省启动的配置文件名相同），则本步骤可选；如果不是 config.cfg，则本步骤必选。

(3) 重启设备，重启完成后设备会以上面设置的配置文件恢复配置。

说明

上述步骤的操作过程中，不能进行 **save** 命令的操作，否则设备将以当前保存的配置启动。

---

4 硬件类故障处理

说明

关于设备各部件指示灯的详细情况，请参见《H3C CR16000-F 路由器安装指导》。

4.1 配置系统故障

路由器上电后，如果系统正常，将在配置终端上显示启动信息；如果配置系统出现故障，配置终端可能无显示或者显示乱码。

4.1.1 终端无显示故障处理

如果上电后配置终端无显示信息，首先要做以下检查：

- 电源系统是否正常工作。
- 主控板是否正常工作。
- 是否已将配置电缆接到主控板的配置口（Console 口或 USB Console 口）。

如果以上检查未发现问题，很可能有如下原因：

- 配置电缆连接的串口错误（实际选择的串口与终端设置的串口不符）。
- 配置终端参数设置错误（参数要求：设置波特率为 9600，数据位为 8，奇偶校验为无，停止位为 1，流量控制为无）。
- 配置电缆本身有问题，可以尝试更换配置电缆。

4.1.2 终端显示乱码故障处理

如果配置终端上显示乱码，很可能是配置终端参数设置错误（设置波特率为 9600，数据位为 8，奇偶校验为无，停止位为 1，流量控制为无，选择终端仿真为 VT100），请进行相应检查。

4.2 单板故障

4.2.1 故障描述

说明

假如设备上出现 Forwarding fault、Board fault: chassis X slot Y, please check it 等日志信息，请参考“15 硬件转发故障”。

1. 单板状态异常

- 单板状态指示灯出现如下情况，则有可能是单板异常：

- 对于 CSR05SRP1L1、CSR05SRP1L3、CSR05SRP1P3A、CSR05SRP1P3 主控板，单板状态指示灯 RUN 和 ALM 灯同时闪烁或者常亮。
- 对于 CR16000-F 路由器，CSFC-08E1、CSFC-16E、CSFC-08E1A、CSFC-16EA、T 类交换网板启动完成后 RUN 指示灯灯灭；其他交换网板上的 RUN 指示灯灭或闪烁，且 ALM 灯常亮。

- 通过 **display device** 命令查看设备，如果发现单板状态出现 Fault、Off、Offline、Illegal，或该槽位存在单板但状态却是 Absent 的，说明单板可能出现故障，请参考 4.2.2 故障处理步骤 处理。

```
<Sysname> display device
Slot No. Brd Type         Brd Status   Software Version
 0       CSR05SRP1L3      Master       CR16000-CMW710-R8151PXX
 1       CSR05SRP1L3      Standby      NONE
 2       CSPC-XP8LB       Normal       CR16000-CMW710-R8151PXX
 3       CMPE-1104        Normal       CR16000-CMW710-R8151PXX
   Sub1  MIC-SP4L         Normal
   Sub2  MIC-SP4L         Normal
   Sub3  MIC-CLP2L        Normal
   Sub4  MIC-GP4L         Normal
 4       CSPC-XP8LB       Normal       CR16000-CMW710-R8151PXX
 5       NONE             Absent       NONE
 6       CSFC-04D         Normal       CR16000-CMW710-R8151PXX
 7       NONE             Absent       NONE
 8       NONE             Absent       NONE
 9       NONE             Absent       NONE
```

2. 单板重启异常

单板出现异常重启或不断重启等故障时，可以通过 logfile 日志、**display version**、**display kernel reboot** 查看设备启动后运行时间来确认单板有没有出现过重启，出现过重启的单板运行时间会明显短于设备上其他单板。如果有单板出现过重启，请参考 4.2.2 故障处理步骤。

4.2.2 故障处理步骤

1. 单板状态异常

- 单板状态 Absent

(1) 确认单板是否插稳，如检查单板与机框之间是否有空隙，也可以将单板拔出后重插入。

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

(3) 检查单板面板的指示灯是否发光。

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

(5) 确认主机软件版本是否支持该单板

a. 通过 **display version** 命令查看主机软件版本；

b. 联系技术支持，确认当前主机软件版本是否支持该单板；

c. 如果当前软件版本不支持该单板，请升级到正确版本。

(6) 如果单板是主控板，连上 Console 口配置电缆后，使用尖细工具（如笔尖）按单板上的系统复位键（RESET）或通过 **reboot slot** *slotid* **force** 命令重启单板，查看配置终端上的显示信息是否恢复正常，同时查看单板状态指示灯是否恢复正常。

(7) 如果单板是带有 CONSOLE 口的交换网板，连上 Console 口配置电缆后，通过执行 **reboot slot** *slotid* **force** 命令或拔出该单板重新插入设备来重启单板，查看配置终端上的显示信息是否恢复正常，同时查看单板状态指示灯是否恢复正常。

(8) 如果单板是业务板，请先确保主控板处于正常工作状态。

(9) 如确认为单板故障，请更换单板并将故障信息发送技术支持人员分析。

- 单板状态 Power-off。

(1) 确认用户有无通过 **debug sysm power-down** 命令对单板执行下电操作。如果是用户操作导致，请通过 **debug sysm power-up** 命令对单板重新上电。

(2) 确认设备环境是否存在过温下电，通过 Probe 视图下命令 **display power-info** 查看是否存在环境温度过高，单板被下电的记录。

(3) 如果确认是过温下电，请排查环境单板槽位是否插满，如果单板槽位已插满单板或者挡风板，请通过命令 **display fan-speed** 确认风扇工作是否正常，如不正常，请将故障信息发送技术支持人员分析。

(4) 否则，单板存在电源故障，请更换单板并将故障信息发送技术支持人员分析。

- 单板状态 Fault。

(5) 等待一段时间（大约 10 分钟左右）确认下单板是一直 Fault 还是 Normal 后又再次重启。如单板是 Normal 后又自动重启，请将故障信息发送技术支持人员分析。

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

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

(7) 将单板放到别的槽位，进一步确认是不是单板故障。

(8) 如确认为单板故障，请更换单板并将故障信息发送技术支持人员分析。

2. 单板重启异常

这里的单板重启是指单板出现过重启，而当前单板状态是 Normal。

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

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

```
<Sysname> display version
H3C Comware Software, Version 7.1.075, Release 8151P12
Copyright (c) 2004-2017 New H3C Technologies Co. Ltd. All rights reserved.
H3C CR16006-F uptime is 0 weeks, 0 days, 4 hours, 24 minutes
Last reboot reason : Cold reboot……
```

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

(4) 确认日志中重启时有无出现类似“Warning: Standby board on slot 1 is not compatible with master board.”或“Warning: The LPU board on slot 1 is not compatible with MPU board.”提示信息，这种情况是业务板、备用主控板或网板与主用主控板的设备标识不一致，请联系技术支持人员更换。

(5) 如无法确认，请搜集故障信息并发送技术支持人员分析。

4.3 电源故障

4.3.1 故障描述

设备出现如下情况，表示电源可能出现故障：

- CR16000-F 和 CR16000-FA 设备的电源模块指示灯出现如下情况：
  - 交流电源模块的指示灯，AC 灯灭或者 DC 灯为红色常亮。
  - 直流电源模块的指示灯，INP OK 灯灭或者 DC/FLT 灯为红色常亮。
- 通过 **`display power`** 命令显示的电源模块状态为 Error。
- logfile 日志中出现电源故障相关诊断信息。

4.3.2 故障处理步骤

(1) Power 是电源模块。请检查模块是否在位并插稳，电源模块状态指示灯是否正常。如某个模块不正常，请对怀疑的故障模块拔插、与正常的模块更换做交叉验证。

(2) 检查电源线的连接：拔下再重新连接电源线，确认电源线是否松动；更换电源线，然后查看电源模块指示灯是否恢复正常。

(3) 检查路由器连接的供电系统：确认供电系统正常供电，电压正常。

(4) 检查电源模块是否存在输出短路、输出过流、输出过压、输入欠压、温度过热等问题。

(5) 通过 **display power** 命令检查 Power State 状态是否是 Normal，如果物理上电源模块实际是在位的，但是却显示为空或者 Absent，则说明存在问题。

```
<Sysname> display power
 Power         0 State: Normal
 Power         1 State: Absent
 Power         2 State: Absent
 Power         3 State: Absent
```

(6) 如电源模块故障，请更换对应的模块；如故障无法确认，请将信息发送给技术支持人员协助分析。

4.4 风扇故障

4.4.1 故障描述

设备出现如下情况，表示风扇可能出现故障：

- 风扇框 OK 指示灯灭且 FAIL 指示灯常亮。

- 通过 **display fan** 命令显示的风扇状态为 Absent 或 Fault 状态。
- logfile 日志中出现风扇故障相关诊断信息。

4.4.2 故障处理步骤

(1) 如果所有指示灯都为灭，请确认电源模块是否正常工作，具体请参见“4.3 电源故障”。

(2) 风扇框在位时，用手放在设备出风口，判断是否有出风，如果出风口无风，则风扇异常。

(3) 检查风扇的入风口、出风口是否被挡住或积累太多灰尘。

(4) 检查风扇框是否正常在位，各个风扇的状态是否正常、转速是否相差达到 50%以上。如存在异常，建议通过风扇框拔插、更换交叉进一步确的认。

```
<Sysname> display fan
Fan Frame 0  State: Normal
<Sysname> system-view
[Sysname] probe
[Sysname-probe] debug sysm fan 0 get-speed


Frame 0 fan 1 speed is 2854 (R.P.M)
Frame 0 fan 2 speed is 2841 (R.P.M)
Frame 0 fan 3 speed is 3348 (R.P.M)
Frame 0 fan 4 speed is 3412 (R.P.M)
Frame 0 fan 5 speed is 3343 (R.P.M)
Frame 0 fan 6 speed is 3345 (R.P.M)
Frame 0 fan 7 speed is 3379 (R.P.M)
Frame 0 fan 8 speed is 3376 (R.P.M)
```

(5) 如果故障不能恢复，需要更换该风扇框，但当前没有风扇框，请关闭设备以免发生温度高导致单板烧坏；如果有降温措施保证系统工作在 50 度以下，可以暂时继续使用设备。

(6) 如果通过上述步骤仍然无法排除故障，请联系代理商或当地用服工程师进行处理。

4.5 温度告警

4.5.1 故障描述

设备打印温度过低、过高等告警信息，如：

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

4.5.2 故障处理步骤

(1) 检查环境温度是否正常。如果环境温度较高，请确认原因，比如机房通风不畅、空调制冷故障等。

(2) 检查设备当前的 temperature 温度是否超出上下的 Warning、Alarm 门限。也可以用手触摸单板，确认单板是不是很烫，如单板温度很高，请立即检查原因。持续处于较高的温度下，可能会导致单板损坏。

- 如果温度过高，请参照 4.4 风扇故障确认是否风扇故障导致，并同时检查设备的入风口和出风口是否被灰尘或棉絮等异物堵住。
- 如果温度值为 error 或出现明显不合实际的值，可能是通过 I2C 总线访问单板温度传感器异常。设备光模块信息访问也是通过相同的 I2C 总线，请继续检查单板读取光模块信息是否正常。
- 如光模块访问异常，请更换光模块重新查看，如光模块访问正常，请进行下一步检查；如光模块访问还是异常，请联系技术支持。
- 如光模块访问正常，请使用下面命令重新设置单板温度，并通过 **display environment** 查看是否设置成功。

```
[Sysname] temperature-limit slot 1 hotspot 1 -5 85 100
[Sysname] display environment
System temperature information (degree centigrade):
 ---------------------------------------------------------------------
 Slot  Sensor    Temperature  Lower  Warning  Alarm  Shutdown
 3     hotspot 1 39           0      80       97     NA
 3     hotspot 2 50           0      80       97     NA
 7     inflow  1 31           0      71       90     NA
 7     outflow 1 45           0      80       99     NA
 7     hotspot 1 53           0      88       107    NA
```

(3) 如果仍然无法确认故障原因，请搜集信息并发送给技术支持人员协助分析。

4.6 故障诊断命令

命令	说明
display device	显示设备信息，检查各单板的状态是否正常
display environment	显示路由器的温度信息，检查环境温度是否正常（是否超出温度告警阈值）
display fan	显示设备内置风扇的工作状态
display fan-speed	显示设备当前风扇转速
display power	显示设备内置电源的工作状态
display version	显示系统版本信息、单板的运行时间以及最后一次重启的原因
save	将当前配置保存到指定文件
temperature-limit	设置设备的温度告警门限

5 IRF 类故障处理

5.1 IRF无法形成

5.1.1 故障描述

IRF 无法正常建立。

5.1.2 故障处理步骤

通常为配置错误引起，请检查以下配置是否正确：

(1) 仅 CR16006-F、CR16010F 或 CR16014-F 路由器之间，CR16010H-F 和 CR16010H-F 路由器之间，CR16018-F 和 CR16018-F 路由器之间，CR16010H-FA 和 CR16010H-FA 路由器之间，CR16018-FA 和 CR16018-FA 路由器之间可以建立 IRF，其他路由器暂不支持建立 IRF。

(2) 确认成员设备的软件版本、主控板类型、OEM Flag 是否一致，确认组成 IRF 的两台设备上均配置为 A 类交换网板或丝印完全相同的其他类型交换网板。

```
<Sysname-1> display device
Chassis   Slot No. Brd Type         Brd Status   Software Version
1         0        NONE             Absent       NONE
1         1        CSR05SRP1L3      Master       CR16000-CMW710-R8151PXX
1         2        NONE             Absent       NONE
1         3        NONE             Absent       NONE
1         4        CSPC-XP8LB       Normal       CR16000-CMW710-R8151PXX
1         5        CSPC-XP8LB       Normal       CR16000-CMW710-R8151PXX
1         6        CSFC-04D         Normal       CR16000-CMW710-R8151PXX
1         7        NONE             Absent       NONE
1         8        NONE             Absent       NONE
1         9        NONE             Absent       NONE
<Sysname-2> display device
Chassis   Slot No. Brd Type         Brd Status   Software Version
2         0        NONE             Absent       NONE
2         1        CSPC-CP1LCX      Normal       CR16000-CMW710-R8151PXX
2         2        NONE             Absent       NONE
2         3        NONE             Absent       NONE
2         4        CSR05SRP1L3      Standby      CR16000-CMW710-R8151PXX
2         5        CSR05SRP1L3      Standby      CR16000-CMW710-R8151PXX
2         6        NONE             Absent       NONE
2         7        CSPC-XP8LB       Normal       CR16000-CMW710-R8151PXX
2         8        NONE             Absent       NONE
2         9        NONE             Absent       NONE
2         10       CSFC-08B         Normal       CR16000-CMW710-R8151PXX
2         11       NONE             Absent       NONE
2         12       NONE             Absent       NONE
2         13       NONE             Absent       NONE
[Sysname-probe] display hardware internal sysm eeprom 380 4 6
0x380:  0xa5 0x8 0x58 0x2
```

(3) 确认 IRF 物理端口是否 UP。

通过 **display interface** 查询 IRF 物理端口状态是否 UP：

```
<Sysname> display interface Ten-GigabitEthernet 2/7/0/1
Ten-GigabitEthernet2/7/0/1
Current state: UP
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 80f6-5665-4302
Description: Ten-GigabitEthernet2/7/0/1 Interface
Bandwidth: 10000000kbps
Loopback is not set
```

```
Media type is optical fiber,Port hardware type is 10G_BASE_SR_SFP
……
```

(4) 确认 IRF 端口连接是否异常，一台设备的 IRF-Port1 口只能与另一台设备的 IRF-Port2 口连接。

```
<Sysname> display irf configuration
 MemberID NewID    IRF-Port1                       IRF-Port2
 1        1        Ten-GigabitEthernet1/5/0/1      disable
                   Ten-GigabitEthernet1/5/0/2
                   Ten-GigabitEthernet1/5/0/5
 2        2        disable                         Ten-GigabitEthernet2/7/0/1
```

(5) CR16000-F 设备在只有 1 块交换网板的条件下，确认该交换网板未插在交换网板的第二槽位。

(6) CR16000-F 设备确认已 UP 的 IRF 物理口和 IRF 物理口对接，不存在一侧已配置成 IRF 物理口且 UP，但对接的另一侧为非 IRF 物理口的情况。

(7) 确认使用 **irf-port-configuration active** 命令激活 IRF 物理端口。但在激活前应该先 save 保存配置，然后再激活。

(8) 确认两台设备的成员编号是否相同，可以使用 **display device** 命令行查看，如果成员编号相同，可以使用 **irf member remember** 重新设置，重启后生效。

```
[Syname] irf member x remember y
```

(9) 在需要安装补丁包的情况下，可使用 **display install active** 命令行查看各成员设备上安装包的情况。需要确认各成员设备均安装了该补丁包，且使用 **install commit** 命令提交补丁。

```
<Sysname> display install active
Active packages on slot 0:
  cfa0:/BOOT-R8151PXX.bin
  cfa0:/SYSTEM-R8151PXX.bin
  cfa0:/DEVKIT-R8151PXX.bin
  cfa0:/SYSTEM-R8151PXX.bin
Active packages on slot 4:
  cfa0:/BOOT-R8151PXX.bin
  cfa0:/SYSTEM-R8151PXX.bin
  cfa0:/DEVKIT-R8151PXX.bin
  cfa0:/SYSTEM-R8151PXX.bin
```

(10) 确认两台设备的 vlan 模式是否一致，可以使用 **display system-vlan-mode** 命令行查看。如果不一致可以使用 **system-vlan-mode** 命令行来设置，重启设备后生效。

```
<Sysname> display system-vlan-mode
The current system vlan mode: standard.
The system vlan mode for next startup: standard.
```

(11) 确认两台设备的 MAC 数目是否一致，如果不一致将不能正常组建 IRF，可以使用 **display hardware internal lif interface-mac slot** 命令行查看。

```
[Sysname-probe] display hardware internal lif interface-mac slot 1
 System Total MAC Number: 512
---------------------- MAC Information ------------------------
 Total MAC Number      :  512
  MDCID                :  1
  Bridge MAC           :  1234-5678-9000
```

```
M-Ethernet MAC       :  1234-5678-9001
Global Interface MAC :  1234-5678-9002 (VLAN RAGG RPR VE-VPN)
Router Intf Base MAC :  1234-5678-9036 (NP Router interface)
```

5.2 IRF出现分裂

5.2.1 故障描述

IRF 运行过程中出现分裂。

5.2.2 故障处理步骤

(1) IRF 分裂时会打印 IRF 端口 down，可以确定 IRF 分裂的时间。

```
%Jun 26 10:13:46:233 2014 H3C STM/2/STM_LINK_STATUS_TIMEOUT: IRF port 1 is down because heartbeat timed out.
%Jun 26 10:13:46:436 2014 H3C STM/3/STM_LINK_STATUS_DOWN: -MDC=1; IRF port 2 is down.
```

(2) IRF 物理端口所在接口板的状态是否正常，若不正常，请参照 4.2 单板故障排查是否单板故障。

(3) 检查各个 IRF 物理端口的状态是否正常。若端口状态不正常，请确认故障原因。

```
<Sysname> display interface Ten-GigabitEthernet 2/7/0/1
Ten-GigabitEthernet2/7/0/1
Current state: UP
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 80f6-5665-4302
Description: Ten-GigabitEthernet2/7/0/1 Interface
Bandwidth: 10000000kbps
Loopback is not set
Media type is optical fiber,Port hardware type is 10G_BASE_SR_SFP
……
```

(4) 通过设备运行时间或日志检查 IRF 中各个成员设备及 IRF 物理端口所在的接口板在 IRF 分裂时是否重启过，并参照 4.3 电源故障确认是否为电源故障导致。

```
<Sysname> display version
H3C Comware Software, Version 7.1.075, Release 8151PXX
Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.
H3C CR16006-F uptime is 0 weeks, 0 days, 4 hours, 49 minutes
Last reboot reason : USER reboot

Boot image: cfa0:/BOOT-R8151PXX.bin
Boot image version: 7.1.075, Release 8151PXX
  Compiled Nov 11 2014 08:49:26
System image: cfa0:/SYSTEM-R8151PXX.bin
System image version: 7.1.075, Release 8151PXX
  Compiled Nov 11 2014 08:49:26
Feature image(s) list:

MPU(M) Chassis 1 Slot 1:
Uptime is 0 weeks,0 days,5 hours,2 minutes
BOARD TYPE:          CSR05SRP1L3
```

```
DRAM:               8192M bytes
CFCARD:             4002M bytes
FLASH:              500M bytes
NVRAM:              1M bytes
PCB 1 Version:      VER.A
Bootrom Version:    116
CPLD 1 Version:     001
CPLD 2 Version:     001
CPLD 3 Version:     001
Release Version:    H3C CR16006-F-R8151PXX
Patch Version  :    None
Reboot Cause   :    UserReboot
Clock card:
  Type        : SR07CK3C
  PCB         : Ver.A
  FPGA version: 100

LPU Chassis 1 Slot 4:
Uptime is 0 weeks,0 days,2 hours,32 minutes
BOARD TYPE:         CSPC-GP44XP4LCX
DRAM:               4096M bytes
PCB 1 Version:      VER.A
Bootrom Version:    116
CPLD 1 Version:     002
Release Version:    H3C CR16006-F-R8151PXX
Patch Version  :    None
Reboot Cause   :    ColdReboot
 Number of Exist Subcards: 0


LPU Chassis 1 Slot 5:
Uptime is 0 weeks,0 days,4 hours,56 minutes
BOARD TYPE:         CSPC-XP12LAX
DRAM:               4096M bytes
PCB 1 Version:      VER.A
Bootrom Version:    116
CPLD 1 Version:     001
Release Version:    H3C CR16006-F-R8151PXX
Patch Version  :    None
Reboot Cause   :    UserReboot
 Number of Exist Subcards: 0


NPU Chassis 1 Slot 6:
Uptime is 0 weeks,0 days,4 hours,56 minutes
BOARD TYPE:         CSFC-04D
DRAM:               1024M bytes
PCB 1 Version:      VER.B
```

```
Bootrom Version:    512
CPLD 1 Version:     002
Release Version:    H3C CR16006-F-R8151PXX
Patch Version  :    None
Reboot Cause   :    UserReboot

LPU Chassis 2 Slot 1:
Uptime is 0 weeks,0 days,4 hours,38 minutes
BOARD TYPE:         CSPC-CP1LCX
DRAM:               4096M bytes
PCB 1 Version:      VER.A
Bootrom Version:    116
CPLD 1 Version:     001
Release Version:    H3C CR16006-F-R8151PXX
Patch Version  :    None
Reboot Cause   :    UserReboot
 Number of Exist Subcards: 0


MPU(S) Chassis 2 Slot 4:
Uptime is 0 weeks,0 days,3 hours,56 minutes
BOARD TYPE:         CSR05SRP1L3
DRAM:               8192M bytes
CFCARD:             4002M bytes
FLASH:              500M bytes
NVRAM:              1M bytes
PCB 1 Version:      VER.A
Bootrom Version:    116
CPLD 1 Version:     001
CPLD 2 Version:     001
CPLD 3 Version:     001
Release Version:    H3C CR16010-F-R8151PXX
Patch Version  :    None
Reboot Cause   :    UserReboot
Clock card:
  Type        : SR07CK3C
  PCB         : Ver.A
  FPGA version: 100

MPU(S) Chassis 2 Slot 5:
Uptime is 0 weeks,0 days,5 hours,2 minutes
BOARD TYPE:         CSR05SRP1L3
DRAM:               8192M bytes
CFCARD:             4002M bytes
FLASH:              500M bytes
NVRAM:              1M bytes
PCB 1 Version:      VER.A
Bootrom Version:    116
```

```
CPLD 1 Version:     001
CPLD 2 Version:     001
CPLD 3 Version:     001
Release Version:    H3C CR16010-F-R8151PXX
Patch Version  :    None
Reboot Cause   :    UserReboot
Clock card:
  Type        : SR07CK3C
  PCB         : Ver.A
  FPGA version: 100

LPU Chassis 2 Slot 7:
Uptime is 0 weeks,0 days,4 hours,55 minutes
BOARD TYPE:         CSPC-XP24LCX
DRAM:               4096M bytes
PCB 1 Version:      VER.A
Bootrom Version:    116
CPLD 1 Version:     001
Release Version:    H3C CR16006-F-R8151PXX
Patch Version  :    None
Reboot Cause   :    UserReboot
 Number of Exist Subcards: 0


NPU Chassis 2 Slot 10:
Uptime is 0 weeks,0 days,4 hours,56 minutes
BOARD TYPE:         CSFC-08B
DRAM:               1024M bytes
PCB 1 Version:      VER.B
Bootrom Version:    514
CPLD 1 Version:     005
Release Version:    H3C CR16006-F-R8151PXX
Patch Version  :    None
Reboot Cause   :    UserReboot
```

(5) 如故障确认，可以通过如更换光模块、更换单板的方式使设备重新形成 IRF；如故障无法确认，请搜集各个成员设备的信息，并将信息发送给技术支持人员协助分析。

5.3 故障诊断命令

命令	说明
debug ipv4-drv show config	显示当前IPv4配置信息
display device	显示设备信息。用于检查各成员设备的软件版本、主控板类型是否一致
display install active	显示当前系统中处于激活状态的软件包的相关信息
display interface	显示指定接口的相关信息。用于检查IRF物理端口状态是否UP
display irf configuration	显示所有成员设备的IRF配置信息。用于检查IRF端口连接是否异常，一台

命令	说明
	设备的IRF-Port1口只能与另一台设备的IRF-Port2口连接
display system-vlan-mode	显示系统当前运行的VLAN模式和下次启动后运行的VLAN模式
display version	显示系统版本信息、单板的运行时间。通过设备运行时间确认IRF中各个成员设备是否重启过，主控板及IRF端口所在接口板是否发生重启
display irf topology	查看当前拓扑信息。显示IRF拓扑状态

6 系统管理维护类故障处理

6.1 CPU占用率高

6.1.1 故障描述

设备单板 CPU 占用率持续在 60%以上，配置命令时设备反应很慢。

```
<Sysname> display cpu-usage
Slot 1 CPU 0 CPU usage:
      60% in last 5 seconds
      60% in last 1 minute
      60% in last 5 minutes

Slot 4 CPU 0 CPU usage:
       3% in last 5 seconds
       3% in last 1 minute
       3% in last 5 minutes

Slot 5 CPU 0 CPU usage:
       2% in last 5 seconds
       2% in last 1 minute
       2% in last 5 minutes

Slot 6 CPU 0 CPU usage:
       3% in last 5 seconds
       3% in last 1 minute
       3% in last 5 minutes
<Sysname> monitor thread dumbtty slot 1
375 processes; 414 threads
Thread states: 3 running, 411 sleeping, 0 stopped, 0 zombie
CPU0: 72.62% idle, 0.00% user, 26.11% kernel, 1.27% interrupt, 0.00% steal
CPU1: 47.78% idle, 7.00% user, 43.31% kernel, 1.91% interrupt, 0.00% steal
CPU2: 100.00% idle, 0.00% user, 0.00% kernel, 0.00% interrupt, 0.00% steal
CPU3: 88.47% idle, 0.00% user, 11.53% kernel, 0.00% interrupt, 0.00% steal
CPU4: 98.08% idle, 0.00% user, 1.28% kernel, 0.64% interrupt, 0.00% steal
CPU5: 0.00% idle, 0.00% user, 100.00% kernel, 0.00% interrupt, 0.00% steal
CPU6: 100.00% idle, 0.00% user, 0.00% kernel, 0.00% interrupt, 0.00% steal
CPU7: 0.00% idle, 0.00% user, 100.00% kernel, 0.00% interrupt, 0.00% steal
```

```
CPU8: 100.00% idle, 0.00% user, 0.00% kernel, 0.00% interrupt, 0.00% steal
CPU9: 100.00% idle, 0.00% user, 0.00% kernel, 0.00% interrupt, 0.00% steal
CPU10: 100.00% idle, 0.00% user, 0.00% kernel, 0.00% interrupt, 0.00% steal
CPU11: 100.00% idle, 0.00% user, 0.00% kernel, 0.00% interrupt, 0.00% steal
CPU12: 100.00% idle, 0.00% user, 0.00% kernel, 0.00% interrupt, 0.00% steal
CPU13: 98.73% idle, 0.00% user, 0.00% kernel, 1.27% interrupt, 0.00% steal
CPU14: 98.72% idle, 0.00% user, 1.28% kernel, 0.00% interrupt, 0.00% steal
CPU15: 89.81% idle, 0.00% user, 10.19% kernel, 0.00% interrupt, 0.00% steal
Memory: 7933M total, 5447M available, page size 4K
        JID        TID  LAST_CPU  PRI  State  HH:MM:SS   MAX    CPU    Name
        262        262       5    105    R    15:53:12    29   5.28%   [RXCP]
        261        261       7    105    R    15:44:03     1   5.25%   [RXCS]
        404        404       1    120    S    01:35:13     1   1.23%   diagd
        404      98278       1    120    R    00:00:00     1   1.09%   diagd
        382        382       3    120    D    00:56:52     1   0.54%   [BFD_SesScan]
        205        205       0    116    D    01:38:19     1   0.51%   [bcmLINK.4]
        385        385       8    100    D    01:23:59     0   0.48%   [NAT0]
        389        389      12    100    D    01:15:59     0   0.45%   [NAT4]
        386        386       9    100    D    01:14:16     0   0.40%   [NAT1]
        387        387      10    100    D    00:59:01     0   0.31%   [NAT2]
        391        391      14    100    D    00:52:09     0   0.31%   [NAT6]
        388        388      11    100    D    00:49:52     0   0.28%   [NAT3]
……
```

通过 **display cpu-usage history** 命令可以查看单板最近 60 分钟的 CPU 占用情况。如横坐标时间为 20，则表示 20 分钟前的 CPU 使用率。

```
<Sysname> display cpu-usage history slot 1
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|                                  # #
 20%|############################################################
 15%|############################################################
 10%|############################################################
  5%|############################################################
    ------------------------------------------------------------
              10        20        30        40        50        60  (minutes)
```

```
cpu-usage (CPU 0) last 60 minutes (SYSTEM)
```

6.1.2 故障处理步骤

CPU 占用率高的原因通常有：

- 路由振荡
- 配置过多的路由策略
- 报文攻击
- 链路环路

1. 路由策略排查

通过 **display route-policy** 命令可以查看设备配置的路由策略，请检查配置的路由策略是否过多，导致 CPU 处理的负担增加。

```
<Sysname> display route-policy
Route-policy: policy1
  permit : 1
          if-match cost 10
          continue: next node 11
          apply comm-list a delete
```

2. 报文攻击排查

在设备端口抓包，使用报文捕获工具（如 Sniffer、Wireshark、WinNetCap 等）分析报文特征，确认攻击源。然后针对攻击源配置报文防攻击。

3. 链路环路

以太网接口工作在二层模式并且链路存在环路时，可能出现广播风暴和网络振荡，大量的协议报文上送 CPU 处理可能导致 CPU 占用率升高，设备很多端口的流量会变得很大，端口使用率达到 90% 以上：

```
<Sysname> display interface gigabitethernet2/0/1
GigabitEthernet2/0/1
Current state: UP
Line protocol current state: UP
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0000-e80d-c000
Description: GigabitEthernet2/0/1 Interface
Bandwidth: 1000000kbps
Loopback is not set
Media type is twisted pair
Port hardware type is 1000_BASE_T
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
……
Last clearing of counters: Never
 Peak value of input: 123241940 bytes/sec, at 2014-02-27 14:33:15
 Peak value of output: 80 bytes/sec, at 2014-02-27 14:13:00
 Last 300 seconds input:  26560 packets/sec 123241940 bytes/sec 99%
 Last 300 seconds output:  0 packets/sec 80 bytes/sec 0%
```

……

如链路出现环路：

- 排查链路连接、端口配置是否正确。
- 是否使能 STP 协议，配置是否正确。
- 邻接设备 STP 状态是否正常。
- 如以上配置均正确，可能为 STP 协议计算错误或协议计算正确但端口驱动层没有正常 Block 阻塞，可以 **shutdown** 环路上端口、拔插端口让 STP 重新计算来快速恢复业务，并将故障信息反馈给技术支持人员分析。

4. 进程调用栈搜集

如果通过上述处理还是无法确认具体原因，请再搜集 CPU 占用率高的进程的调用栈信息，一起发送给技术支持人员分析，搜集方法如下：

(1) 通过 **display process cpu** 命令确认 CPU 占用率高的进程 JID，如此处 2 号槽位单板的 DFRS 进程 CPU 占用率较高，其对应的 JID 为 28：

```
<Sysname> display process cpu slot 2
CPU utilization in 5 secs: 6.2%; 1 min: 6.1%; 5 mins: 6.1%
    JID      5Sec      1Min      5Min    Name
      1      0.0%      0.0%      0.0%    scmd
      2      0.0%      0.0%      0.0%    [kthreadd]
      3      0.0%      0.0%      0.0%    [migration/0]
      4      0.0%      0.0%      0.0%    [ksoftirqd/0]
      5      0.0%      0.0%      0.0%    [watchdog/0]
```

……

(2) 查询 JID 为 28 的 DFRS 进程的调用栈信息，请查询 5 次以上，发送给技术支持人员分析，以便于分析该进程具体在做什么处理导致 CPU 占用率持续升高。

```
<Sysname> system-view
[Sysname] probe
[Sysname-probe] follow process 28 slot 2
Attaching to process 28 ([ksoftirqd/8])
Iteration 1 of 5
------------------------------
Kernel stack:
[<ffffffff8045aaa8>] schedule+0x6b8/0xff0
[<ffffffff8024a9f0>] ksoftirqd+0x120/0x170
[<ffffffff8025e4d0>] kthread+0x130/0x140
[<ffffffff80218b50>] kernel_thread_helper+0x10/0x20

Iteration 2 of 5
------------------------------
Kernel stack:
[<ffffffff8045aaa8>] schedule+0x6b8/0xff0
[<ffffffff8024a9f0>] ksoftirqd+0x120/0x170
[<ffffffff8025e4d0>] kthread+0x130/0x140
[<ffffffff80218b50>] kernel_thread_helper+0x10/0x20

Iteration 3 of 5
```

```
------------------------------
Kernel stack:
[<ffffffff8045aaa8>] schedule+0x6b8/0xff0
[<ffffffff8024a9f0>] ksoftirqd+0x120/0x170
[<ffffffff8025e4d0>] kthread+0x130/0x140
[<ffffffff80218b50>] kernel_thread_helper+0x10/0x20

Iteration 4 of 5
------------------------------
Kernel stack:
[<ffffffff8045aaa8>] schedule+0x6b8/0xff0
[<ffffffff8024a9f0>] ksoftirqd+0x120/0x170
[<ffffffff8025e4d0>] kthread+0x130/0x140
[<ffffffff80218b50>] kernel_thread_helper+0x10/0x20

Iteration 5 of 5
------------------------------
Kernel stack:
[<ffffffff8045aaa8>] schedule+0x6b8/0xff0
[<ffffffff8024a9f0>] ksoftirqd+0x120/0x170
[<ffffffff8025e4d0>] kthread+0x130/0x140
[<ffffffff80218b50>] kernel_thread_helper+0x10/0x20
```

6.2 内存占用率高

6.2.1 故障描述

多次查看单板内存占用率，发现内存占用率持续偏高，始终处于 70%以上（未使用的内存占用率低于 30%）。Total 表示总的内存，Used 表示当前使用的内存，FreeRatio 表示未使用的内存占用率。

```
<Sysname> display memory slot 2
The statistics about memory is measured in KB:
Slot 2:
             Total      Used      Free    Shared   Buffers    Cached   FreeRatio
Mem:        774280    591932    182348         0         0      6548       23.6%
-/+ Buffers/Cache:    175800    598480
Swap:            0         0         0
```

6.2.2 故障处理步骤

这类问题通常为软件问题引起，如内存泄露，也可能是路由数目过多导致。请按照下面步骤进一步搜集信息发送给技术支持人员分析。

1. 若达到内存门限，会记录到 diagfile.log 文件中

查看 diagfile.log 中内核态和用户态的内存占用情况，查看内存占用率高的模块。同时可以通过 Probe 视图下的 **display system internal kernel memory pool name** 命令来查看具体的 tag 模块。

2. 查询单板各进程的内存使用信息

通过 **display process memory** 命令多次查询单板各进程的内存使用信息。Dynamic 类型的内存为设备动态申请的，在内存出现泄露时会变得很大，通过前后比较观察可以确认哪个进程的内存占用持续增加。如果持续增加，说明该进程可能发生了泄露，请记录下进程的 JID。下面以查询 JID 为 78 的 diagd 进程为例说明。

```
<Sysname> display process memory slot 2
   JID       Text      Data      Stack    Dynamic    Name
     1        116      8808         32         92    scmd
     2          0         0          0          0    [kthreadd]
     3          0         0          0          0    [migration/0]
     4          0         0          0          0    [ksoftirqd/0]
     5          0         0          0          0    [watchdog/0]
     6          0         0          0          0    [migration/1]
     7          0         0          0          0    [ksoftirqd/1]
     8          0         0          0          0    [watchdog/1]
……
```

通过 **display system internal kernel memory pool** 命令查询缓存池内存使用情况，如果 Number*Size 结果持续增加，说明可能发生了泄漏，请记录下 Name。

```
[Sysname-probe] display system internal kernel memory pool slot 0
Active    Number  Size     Align Slab Pg/Slab ASlabs  NSlabs Name
0         0       168      0     33   2       0       0      IPSEC_Flow_cache
0         0       64       0     28   1       0       0      IPSEC_DPD_cache
0         0       216      0     27   2       0       0      IPSEC_TNL_cache
0         0       520      0     27   4       0       0      IPSEC_SA_cache
0         0       80       0     25   1       0       0      memSESS_hotbackup_hash
0         0       112      0     42   2       0       0      memSESS_hotbackup_hash
0         0       200      0     29   2       0       0      memSESSION_TCPSEQ_CHECK
0         0       168      0     33   2       0       0      Connlmt_Stat_Nodes_IPv4
0         0       192      0     30   2       0       0      Connlmt_Stat_Nodes_IPv6
……
```

也可通过 **display system internal kernel memory pool tag** 命令查询，如果 Bytes 数持续增加，说明可能发生了泄漏，请记录下 Tag 模块 ID。

```
[Sysname-probe] display system internal kernel memory pool tag slot 0
Tag         MemoryPool    Actives  Bytes
0xcc1d0ba6  1             1        2048
0xcc1d05e4  1             1        64
0x6170022   1             1        32
0x6110022   1             3        192
0xcc1d019b  1             1        64
0x611007b   1             1        96
0xcc1d036d  1             1        2048
0xcc1d2fa3  1             457      1871872
0x6170044   1             1        2048
……
```

3. 确认哪种字节大小的内存块发生泄露

再进一步确认 JID 为 78 的 diagd 进程的哪种字节大小的内存块发生泄露。如下命令所示，Size 表示内存块的字节大小，Total 表示总的申请个数，Used 表示使用数目，Free 表示未使用的数目，Free Ratio 表示未使用的内存块百分比。通过多次查询并比较查询值可以看出哪个 Size 的内存块 Used 个数持续增加。查询完毕后，请将搜集到的信息发送给技术支持人员分析。

```
<Sysname> display process memory heap job 1 verbose
Heap usage:
Size       Free       Used       Total      Free Ratio
32         1          340        341        0.3%
48         1          97         98         1.0%
64         0          108        108        0.0%
80         1          15         16         6.3%
96         0          53         53         0.0%
112        0          4          4          0.0%
144        0          3          3          0.0%
160        0          1          1          0.0%
176        0          50         50         0.0%
208        1          53         54         1.9%
224        0          5          5          0.0%
256        23         1          24         95.8%
288        2          1          3          66.7%
304        0          2          2          0.0%
320        1          0          1          100.0%
336        0          2          2          0.0%
512        7          0          7          100.0%
528        0          3          3          0.0%
704        0          152        152        0.0%
768        5          0          5          100.0%
896        0          9          9          0.0%
1056       0          2          2          0.0%
1248       1          0          1          100.0%
2080       0          1          1          0.0%
4112       0          1          1          0.0%
4208       1          0          1          100.0%
7264       1          0          1          100.0%
Summary:
Total virtual memory heap space(in bytes)  :  204800
Total physical memory heap space(in bytes) :  204800
Total allocated memory(in bytes)           :  177504
```

6.3 资源不足

6.3.1 故障描述

资源使用超规格时会打印包含以下内容的日志信息和告警信息：

```
The resources are insufficient.
```

```
No enough resource!
```

```
Not enough resources are available to complete the operation.
```

典型的系统资源包括：

- ACL
- FIB
- MAC
- MPLS LSP
- 组播
- ARP

6.3.2 故障处理步骤

1. ACL 资源

下列这些特性会占用 ACL 资源：

- QoS 策略
- Packet filter
- 策略路由
- URPF
- DHCP Snooping
- LLDP

(1) 通过 **display qos-acl resource** 命令查看单板 ACL 资源使用情况，其中 Total 表示总的资源数，Configured 表示使用资源数，Remaining 表示剩余的资源数，Usage 表示使用的百分比。

```
<Sysname> display qos-acl resource slot 3
Interfaces: GE3/3/1 to GE3/3/8, Pos3/4/1 to Pos3/4/4
------------------------------------------------------------------------
 Type             Total      Reserved   Configured Remaining  Usage
------------------------------------------------------------------------
 IPv4Acl          65536      0          2          65534      0%
 IPv6Acl          16384      0          0          16384      0%
 Car&Cnt          32768      0          1          32767      0%
 InBRASCar        65536      0          0          65536      0%
 OutBRASCar       65536      0          0          65536      0%
 TCPCar           16384      0          0          16384      0%
 CarProf          220        0          2          218        0%
 Sampler          32768      0          0          32768      0%
```

(2) 如果 ACL 资源使用率超过 95%，请根据具体情况进行优化，比如删除或合并 ACL 规则。如果无法优化，请将信息发送给技术支持人员协助分析。

2. FIB 资源

(1) 使用命令行查看 FIB 表项资源使用情况。

- CMPE-1104 或 CSPC 单板：

```
[Sysname-probe] debug ipv4-drv show statistics slot 2
```

```
**********************************************************
- IPv4 Statistics        Slot 2
**********************************************************
- ROUTE TOTAL COUNT:             40
- ECMP COUNT:                    0
- ARP NH COUNT:                  8
- IPV4 NH CHANGE NUM:            16
- ARP Prefix ADD NUM:            12
- ARP Prefix MODIFY NUM:         2
- ARP Prefix DEL NUM:            0
- ARP Prefix AddSuccessed NUM:   0
- ARP Prefix ModSuccessed NUM:   0
- ARP Prefix DelSuccessed NUM:   0
- IPV6 NH CHANGE NUM:            0
- IPV4 Plat ARP Demand NUM:      16
- IPV4 ARP Successed NUM:        16
- IPV4 Plat Route Demand NUM:    47
- IPV4 Route Successed NUM:      47
-----------------------------------------------
- IPv4Uc_Sm Owner:               -1
- IPv4Uc_Sm Count:               0
- L3UcPbr_Sm Owner:              -1
- L3UcPbr_Sm Count:              0
……略
[Sysname-probe] debug ipv4-drv show config slot 2


**********************************************************
- IPv4 Config    Slot 2
**********************************************************
- ARP SIZE:              16384
- ArpCanNotSetToHW:      NO
- IPV4 ROUTE SIZE:       65536
- ECMP SIZE:             8
- ND SIZE:               8192
- IPV6 ROUTE SIZE:       8192
- IPV6 LongPrefRT:       128
- VLAN INTF MODE:        2
- NH SIZE:               16384
- ECMPGP SIZE:           256
- L3INTF SIZE:           4096
- VLAN INTF SIZE:        4096
- SUBVLAN SIZE:          3072
- MC INTF SIZE:          4005
- MPLS INTF SIZE:        4000
- TUNNEL INTF SIZE:      511
- VMAC SIZE:             256
```

```
- VMAC PER INTF SIZE:    16
- VLAN MAPPING SIZE:     4094
- ARP SET TO DEFIP:      1
- HG PROXY FLAG:         0
- BOARD TYPE:            0
- Is Set CPUPktPri:      1
- L3uc Opt:              NO
- NetMFw FLAG:           Fw_Hw

- RESERVED EGRESS:
- CPU EGRESS:            100001
- BLACKHOLE EGRESS:      100002
- HG PROXY EGRESS:
- UINT:0
          0: Egress:100003  Mod:63  port:27
          1: Egress:100004  Mod:63  port:27

- L3VPN SPECS:
- GLOBAL VRF NUM:        2048

- UPRF SPECS:
- URPF GLOBAL SUPPORT:   YES
- URPF INTF SUPPORT:     NO
- DEFAULT ROUTE DENY:    NO
- IPv4 MaxRoute:         65536
- IPv6 MaxRoute:         4096
- CHIP SUPPORT TYPE:     TRIUMPHV4EXT
```
……略

ROUTE TOTAL COUNT 表示实际占用的 IPv4 表项资源，IPv4 MaxRoute 表示 IPv4 表项总的资源。

- CSPC-GE16XP4L-E、CSPC-GE24L-E、CSPC-GP24GE8XP2L-E、CSPEX-1104-E 和 CSPEX-1204 单板：

```
[Sysname-probe] display hardware internal pe table all slot 3

============================Table Instruction ================================
============
 PID:        PES Table ID
 PTY:        PES Table type
 KAL:        PES Key Align len
 RAL:        PES Result Align Len
 SID:        SDK TABLE ID
 TableName:  SDK Table name
 STY:        SDK Table type
 LOCA:       SDK Location
 MaxEntry:   SDK Max Entries
 ES:         SDK Entry_size
 MID:        SDK Moudle ID
 CID:        SDK DDR CTRL ID
 CNAME:      SDK DDR CTRL NAME
```

```
 KSZ:        SDK Key Size
 RSZ:        SDK Result Size
================================================================================
============
 PID PTY KAL RAL SID TABLENAME                       STY LOCA MAXENTRY ES MID CID
 CNAME  KSZ RSZ
 0   TAB 4   16  1   ipct                          TBL REG  256      16 0   255
 NULL   0   16
 1   TAB 4   16  2   remote-ipct                   TBL DDR  131072   16 72  18
 DDR7   0   16
 2   TAB 4   4   3   v4_vrrp                       BMP BRAM 32768    1  0   255
 NULL   0   1
 3   TAB 4   4   4   v6_vrrp                       BMP BRAM 32768    1  0   255
 NULL   0   1
 4   TAB 4   4   5   ipv4-vrrp-e                   BMP BRAM 524288   1  0   255
 NULL   0   1
 5   TAB 4   4   6   ipv6-vrrp-e                   BMP BRAM 524288   1  0   255
 NULL   0   1
 6   HAS 8   32  144 rpr-mac-hash                 DLH DDR  147456   32 99  30
 DDR2   6   32
                 8   rpr-mac(Dhash Res)          TBL DDR  131072   32 100 30
 DDR2   0   32
 7   HAS 8   8   145 rpr-node-mac-hash            DSH DDR  131072   16 80  24
 DDR6_0 8   16
                 9   rpr-node-mac(Dhash Res)      TBL DDR  65536    16 81  24
 DDR6_0 0   16
 8   TAB 4   32  10  inlif                       TBL DDR  1048576  32 88  27
 NULL   0   32
 9   HAS 4   32  132 remote-inlif-hash            SHA DDR  163840   32 66  16
 DDR0_0 4   3
 10  CSD 8   32  129 Ve-QinQ-inlif-hash           SHA DDR  294912   32 72  18
 DDR7   6   3
 11  TAB 4   32  12  Ve-QinQ-inlif(CSD Res)      TBL DDR  262144   32 88  27
 NULL   0   32
 12  LPM 8   8   118 ipv4-lpm                    LP4 CPU  0        8  0   255
 NULL   0   8
 13  TAB 4   16  119 ftn                         TBL DDR  4194304  16 64  16
 DDR0_0 0   16
```

IPv4 表项总的资源为 3000000 条。使用 **display hardware internal pe table** 命令查找 ftn 对应的表项的 PID，再使用 **display hardware internal pe table entrycount** 命令可以查看该表项实际占用的 IPv4 表项资源。

```
[Sysname-probe] display hardware internal pe table 13 entrycount slot 3

 There are 16 entries!
```

- CSPEX 类单板（CSPEX-1204 和 CSPEX-1104-E 除外）和 CEPC 类单板：
  - TCAM 模式：

    ```
    [Sysname-probe] display hardware internal exttcam nfs  db-info ipv4 slot 5 chip 0
    ```

```
Database name:           IPV4
Database capacity:       4194304
Current entry count:     148052
Start index:             0x0
End index:               0x5fffff
Key width Type:          0
Key real size in bytes:  6
Key size defined by NPS: 8
Res size defined by NPS: 32
```

Current entry count 表示 TCAM 芯片中实际占用的 IPv4 表项资源，Database capacity 表示 TCAM 芯片中 IPv4 表项总的资源。

- Fast_IP 模式：

```
[System-probe] display hardware internal np table all slot 5 chip 0
```

TblID	Name	StruNum	StruID	Type	KeyLen	ResLen	MaxEntry
0	IPCT	255	0	PORT	1	16	192
1	REMOTE_IPCT	66	48	TABLE	2	16	65536
2	VRRP_MAC	86	62	HASH	7	8	32768
7	RPR_MAC	89	64	HASH	6	20	131072
8	RPR_NODE_MAC	69	51	HASH	8	8	1024
9	INLIF	28	16	TABLE	3	32	1048576
10	REMOTE_INLIF	67	49	HASH	4	32	65536
12	QINQ_INLIF	65	47	HASH	6	32	65536
14	VE_INLIF	42	28	HASH	5	32	16384
19	ILM	27	15	TABLE	3	32	1048576
20	ILM_ALIAS	88	15	TABLE	3	32	1048576
21	TUNNEL_ILM	71	53	HASH	6	24	65536
22	MAC	4	0	HASH	8	16	1048576
23	MAC_SMAC	45	0	HASH	8	16	1048576
24	MAC_SMAC_INNER	46	0	HASH	8	16	1048576
26	MINM_TUNNEL_END	48	31	HASH	13	8	65536
27	PROTOCOL_MAC	62	44	HASH	12	8	65536
28	RRPP_FILTER	93	67	TREE	12	4	65536
29	RRPP_FILTER_RESULT	95	68	TABLE	3	8	65536
30	PPPOE_USER	61	43	HASH	15	32	65536
31	V4IPOE_USER	34	22	HASH	11	32	65536
32	V4IPOE_SEGMENT_USER	36	24	TREE	7	4	4096
33	V4IPOE_SEGMENT_USER_RES	40	26	TABLE	2	32	8192
34	V6IPOE_USER	35	23	HASH	23	32	65536
35	V6IPOE_SEGMENT_USER	38	25	TREE	18	4	4096
36	V6IPOE_SEGMENT_USER_RES	40	26	TABLE	2	32	8192
37	L2TP_USER	41	27	HASH	16	32	131072
38	PPPOE_FILTER	60	42	HASH	5	8	262144
39	TCP_STREAM	70	52	HASH	39	32	917504
40	MLL	49	32	TABLE	3	16	8388608
41	OUTLIF	6	2	TABLE	3	32	2097152
42	OUTLIF_NOACL	44	2	TABLE	3	32	2097152

```
43    OUTLIF_TUNNEL          96    2     TABLE    3    32    2097152
44    OUTLIF_MLOG            98    2     TABLE    3    32    2097152
45    UDP_TUNNEL_START       13    7     TABLE    3    32    131072
46    IPV6_TUNNEL_START      80    59    TABLE    3    32    131072
47    USER                   73    55    TABLE    2    16    65536
48    ARP                    7     3     TABLE    3    32    1048576
49    RPR_ARP                90    65    TABLE    2    32    8192
50    NS_ARP                 51    34    TABLE    3    32    1048576
51    FTN                    21    13    FASTIP   6    4     4194304
```

……略

DDR 内存中 IPv4 表项总的资源为 3000000 条。使用 **display np table all** 命令查找 FTN 对应的表项的 *TblID*，再使用 **display np table** *TblID* **entrycount slot** 命令可以查看该表项在 DDR 内存中实际占用的 IPv4 表项资源。

(2) 如果 FIB 资源使用率超过 95%，请搜集信息并发送给技术支持人员协助分析。

3. MAC 资源

MAC 资源不足在大型二层网络中容易出现，MAC 地址过多，老的 MAC 还没有老化，导致新的 MAC 地址学习不到。

```
<Sysname> display mac-address count
 49 mac address(es) found
```

建议：

- 减小学习到的 MAC 的老化时间，便于 MAC 地址快速老化。
- 优化组网，根据不同的业务或部门等划分 VLAN，不同 VLAN 间采用三层互联。

4. MPLS LSP 资源

(1) 查看 MPLS LSP 资源使用情况。

```
<Sysname> display mpls lsp statistics
LSP Type       Ingress/Transit/Egress  Active
Static LSP     0/0/0                   0/0/0
Static CRLSP   0/0/0                   0/0/0
LDP LSP        0/0/1                   0/0/1
RSVP CRLSP     0/0/0                   0/0/0
BGP LSP        0/0/0                   0/0/0
Local LSP      0/0/0                   0/0/0
------------------------------------------------------
Total          0/0/1                   0/0/1
```

(2) 如 MPLS LSP 资源使用过多导致资源不足，请搜集信息并发送给技术支持人员协助分析。

5. 其他系统资源

其他系统资源的使用情况需要专业技术支持人员进行分析，请联系技术支持处理。

6.4 主控板启动慢

6.4.1 故障描述

主控板启动时加载较慢，Loading 时间较长。

6.4.2 故障处理步骤

(1) 查看存储介质剩余空间

通过 **dir** 命令查看设备的存储介质剩余空间大小。如果剩余空间较小，则会影响主控板的加载启动时间。

(2) 查看 BootWare 版本

需要确认主控板 Bootware 版本是否已经升级，如果重启前后 Bootware 版本不一致，将导致启动过程耗时较长。

```
System is starting...
Press Ctrl+D to access BASIC-BOOTWARE MENU...
Press Ctrl+T to start memory test
Booting Normal Extended BootWare
The Extended BootWare is self-decompressing...........Done.
********************************************************************************
*                                                                              *
*                          BootWare, Version 1.45                              *
*                                                                              *
********************************************************************************
Compiled Date         : Jun 20 2018
CPU Type              : XLP316
CPU Clock Speed       : 1200MHz
Memory Type           : DDR3 SDRAM
Memory Size           : 8192MB
Memory Speed          : 667MHz
BootWare Size         : 1536KB
Flash Size            : 500MB
cfa0 Size             : 4002MB
BASIC CPLD Version    : 1.0
EXTENDED CPLD Version : 1.0
PCB Version           : Ver.A
BootWare Validating...
Press Ctrl+B to access EXTENDED-BOOTWARE MENU...
Loading the main image files...
Loading file cfa0:/SYSTEM-R7951P07.bin.....................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
...........Done.---- 耗时累计 7 分 14 秒
Loading file cfa0:/DEVKIT-TEST.bin.....................
.Done.
Loading file cfa0:/BOOT-TEST.bin.......................
.............................Done.
Extended BootWare Version is not equal,updating? [Y/N]
```

```
Updating Extended BootWare.........Done.
Basic BootWare Version is not equal,updating? [Y/N] -------- 这里升级 bootware 1.45 到 1.46
版本，然后 bootware 重启，重新开始加载；
Updating Basic BootWare.........Done.
BootWare updated,System is rebooting now.
System is starting..----- 耗时累计 8 分 50 秒
Press Ctrl+D to access BASIC-BOOTWARE MENU...
Press Ctrl+T to start memory test
Booting Normal Extended BootWare
The Extended BootWare is self-decompressing........Done.
******************************************************************************
*                                                                            *
*                          BootWare, Version 1.46                            *
*                                                                            *
******************************************************************************
Compiled Date         : Oct 19 2018
CPU Type              : XLP316
CPU Clock Speed       : 1200MHz
Memory Type           : DDR3 SDRAM
Memory Size           : 8192MB
Memory Speed          : 667MHz
BootWare Size         : 1536KB
Flash Size            : 500MB
cfa0 Size             : 4002MB
BASIC CPLD Version    : 1.0
EXTENDED CPLD Version : 1.0
PCB Version           : Ver.A
BootWare Validating...
Press Ctrl+B to access EXTENDED-BOOTWARE MENU...
Loading the main image files...
Loading file cfa0:/SYSTEM-TEST.bin.....................
.......................................................................
.......................................................................
.......................................................................
.......................................................................
.......................................................................
.......................................................................
.......................................................................
..........Done.
Loading file cfa0:/DEVKIT-TEST.bin.....................Done.
Loading file
cfa0:/BOOT-TEST.bin.....................................................Done.
Image file cfa0:/BOOT-TEST.bin is
self-decompressing.....................................Done.
System image is starting...
Line con1 is available.
```

7 LDP 故障处理

7.1 LDP会话振荡

7.1.1 故障描述

指定的 LDP 会话信息未正确生成，不断的出现和消失。

```
<Sysname> display mpls ldp peer
Total number of peers: 1
Peer LDP ID             State         Role     GR   MD5  KA Sent/Rcvd
2.2.2.9:0               Operational   Passive  Off  Off  39/39
```

7.1.2 故障诊断流程

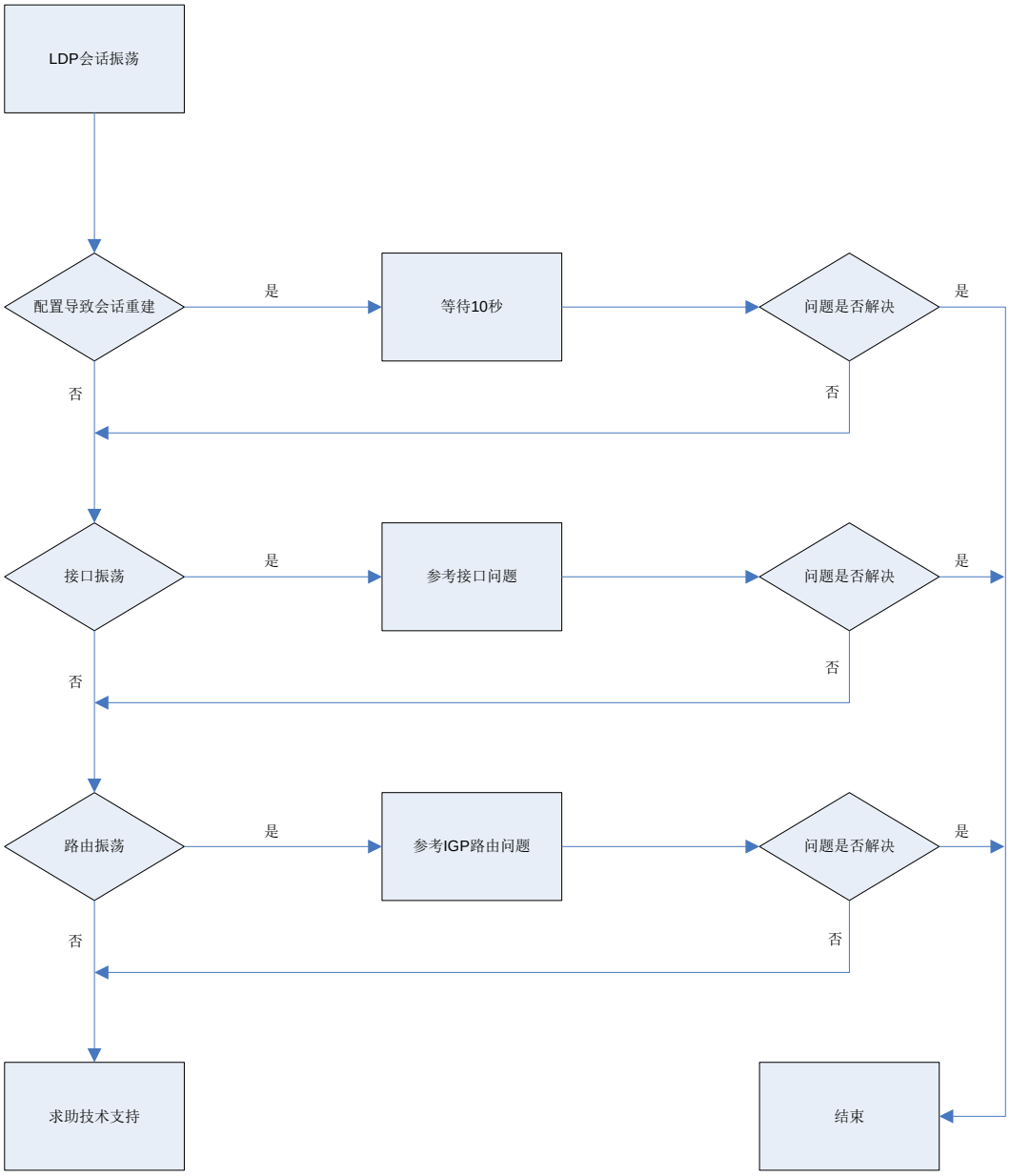
LDP 会话频繁振荡的故障定位思路如下：

(1) 检查是否进行了 LDP GR 等配置。

(2) 检查接口是否振荡。

(3) 检查路由是否振荡。

图1 LDP 会话振荡故障诊断流程图



7.1.3 故障处理步骤

1. 检查是否进行了 LDP GR、LDP Keepalive 定时器、LDP 认证、LDP MTU 或传输地址等配置

在 LDP 视图下执行 **display this** 命令，查看是否进行了 LDP GR 配置。

```
[Sysname-ldp]display this
#
mpls ldp
 graceful-restart
#
```

如果显示信息中包含 **graceful-restart** 配置，则表示进行了 LDP GR 配置。请等待 10 秒，再查看 LDP 会话是否振荡。

2. 检查接口是否振荡

执行 **display ip interface brief** 命令，查看 Physical 和 Protocol 字段。

当 Physical 和 Protocol 字段均显示 up 时，表示接口状态是 up，否则表示接口状态是 down。若相关接口一直在 up 和 down 两种状态间切换则表示接口振荡，请参考接口振荡问题。

3. 检查路由是否振荡

执行 **display fib** 命令，查看路由信息。建议迅速查看。路由存在时，会显示相关路由信息。路由不存在时，则不会显示相关路由信息。如果相关路由信息一直在显示和不显示两种情况切换，则表示路由振荡，请参见 Ping 不通问题，排除 IGP 路由问题。

4. 请收集如下信息，并联系技术支持工程师

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

7.2 LDP会话down

7.2.1 故障描述

执行 **display mpls ldp peer** 命令，发现指定的 LDP 不是 Operational 状态。

```
<Sysname> display mpls ldp peer
Total number of peers: 1
Peer LDP ID             State         Role     GR   MD5  KA Sent/Rcvd
2.2.2.9:0               Operational   Passive  Off  Off  39/39
```

7.2.2 故障诊断流程

LDP 会话 down 的故障定位思路如下：。

(1) 检查是否建立会话的接口被关闭。

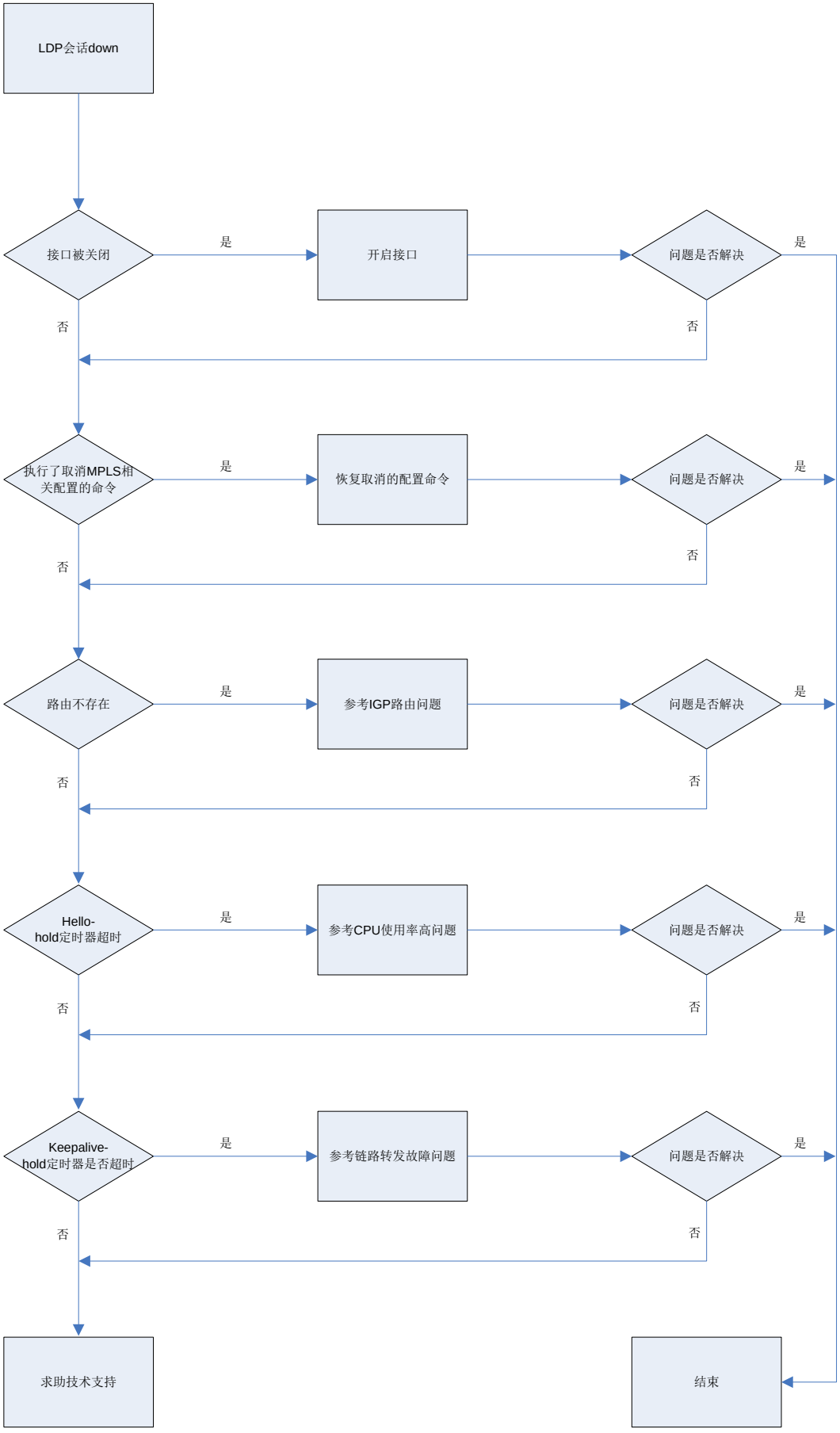
(2) 检查是否执行了取消 MPLS 相关配置的命令。

(3) 检查路由是否存在。

(4) 检查 LDP Hello-hold 定时器是否超时。

(5) 检查 LDP Keepalive-hold 定时器是否超时。

图2 LDP 会话 Down 故障诊断流程图


LDP会话down
接口被关闭
是
开启接口
问题是否解决
是
否
否
执行了取消MPLS相关配置的命令
是
恢复取消的配置命令
问题是否解决
是
否
否
路由不存在
是
参考IGP路由问题
问题是否解决
是
否
否
Hello-hold定时器超时
是
参考CPU使用率高问题
问题是否解决
是
否
否
Keepalive-hold定时器是否超时
是
参考链路转发故障问题
问题是否解决
是
否
否
求助技术支持
结束

7.2.3 故障处理步骤

1. 检查建立 LDP 会话的接口是否被关闭

在接口视图下执行 **display this** 命令，如果显示信息中有 **shutdown** 命令，表示接口被关闭。请在接口下执行 **undo shutdown** 命令启动接口。

2. 检查是否执行了取消 MPLS 相关配置的命令。

执行 **display current-configuration** 命令，查看是否执行了取消 MPLS 相关配置的命令。如果显示信息中没有包含 **mpls ldp** 命令，表示取消了 MPLS LDP 的配置，请执行相应的配置命令恢复被取消的配置。

3. 检查路由是否可达

执行 **display ip routing-table** 命令，查看 Destination/Mask 字段，是否存在到达会话对端的路由。

若路由不存在会直接导致不能建立 TCP 连接，请参见 OSPF 路由协议问题或者 IS-IS 路由协议问题，排除路由问题。

如果存在到达对端的路由，请执行 **ping** 命令，查看对端是否有应答。如果有应答则表示路由可达。如果无应答，则表示路由不可达，请参见 Ping 不通问题。

4. 检查 LDP Hello-hold 定时器是否超时

执行 **display mpls ldp peer verbose** 命令，检查会话两端的 Hello 消息是否都正常发送。建议每 3 秒执行一次 **display mpls ldp peer verbose** 命令，查看收发 Hello 消息的计数。若连续几次执行命令后发现发送或接受的计数没有变化，则表示 Hello 消息收发异常，Hello-hold 定时器超时，请参考 CPU 使用率高问题。

5. 检查 LDP Keepalive-hold 定时器是否超时

执行 **display mpls ldp peer verbose** 命令，检查会话两端的 Keepalive 消息是否都正常发送。建议每 5 秒执行一次 **display mpls ldp peer verbose** 命令，查看收发的 Keepalive 消息的计数。若连续几次执行命令后发现发送或接收的计数没有变化，则表示 Keepalive 消息收发异常，Keepalive-hold 定时器超时，请参见 Ping 不通问题，排除报文转发问题。

6. 请收集如下信息，并联系技术支持工程师

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

7.3 LDP LSP振荡

7.3.1 故障描述

指定的 LDP LSP 信息未正确生成，不断的出现和消失。

```
<Sysname> display mpls ldp lsp 112.1.1.1 32
Status Flags: * - stale, L - liberal, B - backup
FECs: 1           Ingress: 1           Transit: 1           Egress: 0
```

```
FEC                 In/Out Label        Nexthop          OutInterface
112.1.1.1/32        -/1150              200.100.12.2     RAGG1
```

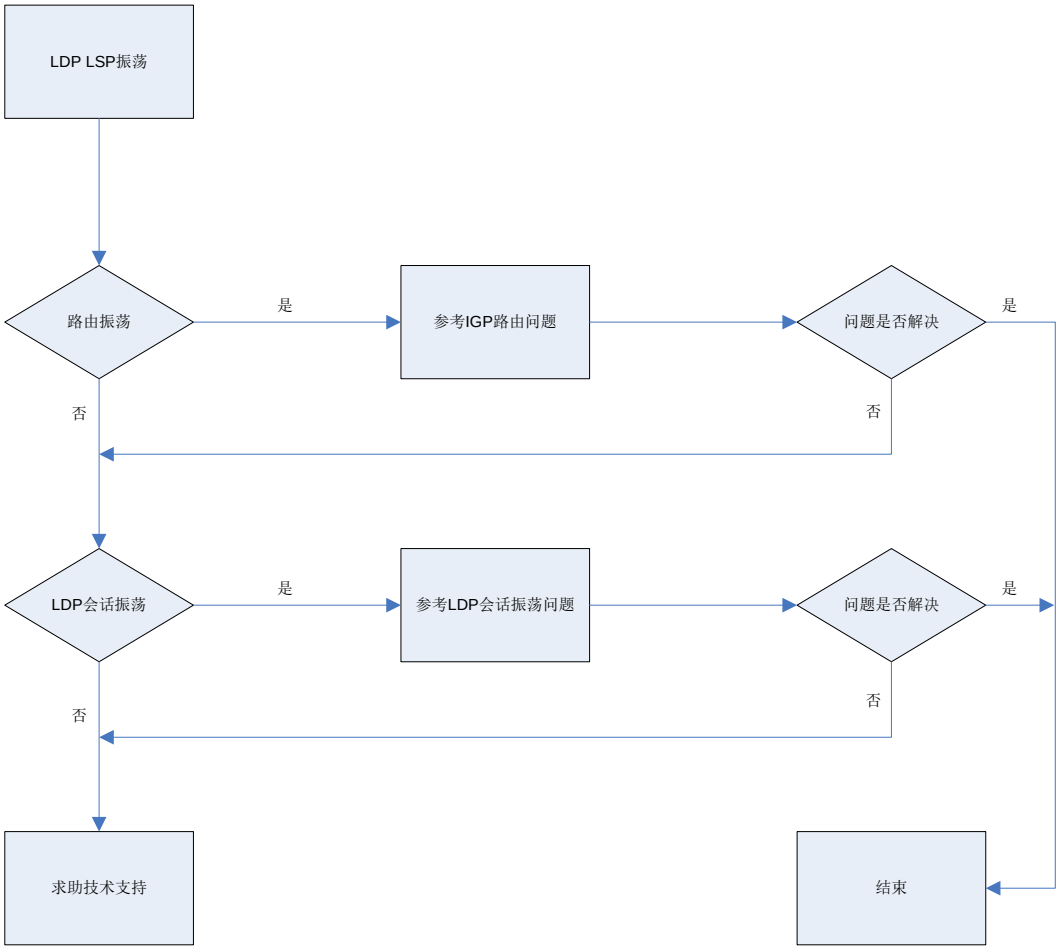
7.3.2 故障诊断流程

LDP LSP 频繁振荡的故障定位思路如下：

(1) 检查路由是否振荡。

(2) 检查 LDP 会话是否振荡。

图3 LDP LSP 振荡故障诊断流程图



7.3.3 故障处理步骤

1. 检查路由是否振荡

执行 **display ip routing-table** 命令，查看到 LSP 目的地址的路由信息。

建议每 1 秒执行一次 **display ip routing-table** 命令。路由存在时，会显示相关路由信息。路由不存在时，则不会显示相关路由信息。如果相关路由信息一直在显示和不显示两种情况切换，则表示路由振荡，请参见 Ping 不通问题，排除 IGP 路由问题。

2. 检查 LDP 会话是否振荡

执行 **display mpls ldp peer** 命令，查看显示信息的 Status 字段。

建议每 1 秒执行一次。如果该字段的显示信息在 Operational 和 Initialized 之间切换，则表示 LDP 会话振荡，请参见 LDP 会话振荡。

3. 请收集如下信息，并联系技术支持工程师

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

7.4 LDP LSP down

7.4.1 故障描述

执行 **display mpls ldp lsp** 命令，发现指定的 LSP 未正确生成。

```
<Sysname> display mpls ldp lsp 112.1.1.1 32
Status Flags: * - stale, L - liberal, B - backup
FECs: 1           Ingress: 1           Transit: 1           Egress: 0

FEC                In/Out Label        Nexthop         OutInterface
112.1.1.1/32       -/1150              200.100.12.2    RAGG1
```

7.4.2 故障诊断流程

LDP LSP down 的故障定位思路如下：

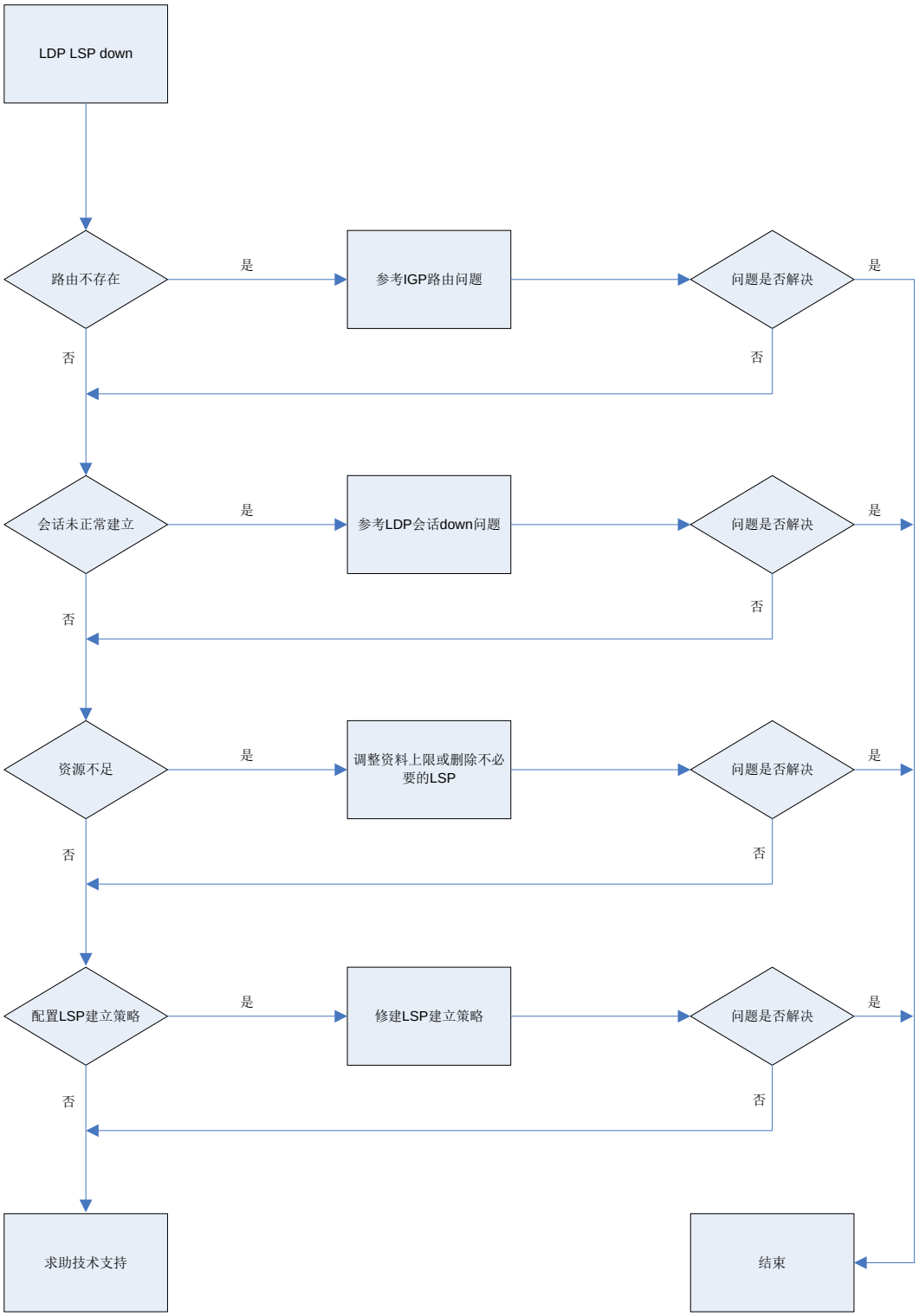
(1) 检查路由是否存在。

(2) 检查 LDP 会话是否正常建立。

(3) 检查是否存在资源不足问题。

(4) 检查是否配置了 LSP 建立策略。

图4 LDP LSP down 故障诊断流程图



7.4.3 故障处理步骤

1. 检查路由是否存在

执行 **display ip routing-table verbose** 命令，查看到 LSP 目的地址的路由信息。

如果存在路由信息，并且显示信息中的 State 字段为 Active Adv，则表示存在 LSP 对应的路由，且该路由处于活跃状态。

对于公网 BGP 路由需要检查是否带标签，如果 Label 字段非 NULL，则表示带标签。

如果路由不存在、路由没有处于活跃状态或 BGP 路由没有带标签，请参见 Ping 不通问题。

2. 检查 LDP 会话是否正常建立

执行 **display mpls ldp peer** 命令，查看显示信息的 Status 字段。如果该字段的显示为 Operational，则表示 LDP 会话已建立并处于 up 状态。如果该字段显示为 Initialized，则表示 LDP 会话没有正常建立，请参见 LDP 会话 down 问题继续定位。

3. 检查是否存在资源不足，如 Paf/License、Token、Label 达到上限以及内存不足的问题

执行下列步骤检查是否存在资源不足：

(1) 检查 LSP 数量是否已经达到 Paf/License 最大值。

执行 **display mpls lsp statistics** 命令，查看 LDP LSP 对应的 Total 字段。将 Total 字段显示的数值和 Paf 文件规定的 LSP 数量比较，如果大于 Paf 文件规定的 LSP 数量，则资源不足。

(2) 对于 Ingress LSP 或 Transit LSP，检查 Token 是否已经用光。

执行 **display mpls nid** 命令，查看统计信息。检查所有的 nid 都处于已用状态。

(3) 检查 Label 使用数量是否已经达到最大值。

执行 **display mpls lable all** 命令，查看统计信息。检查所有的 Label 是否都处于已用状态。

如果存在资源不足，请调整资源上限或删除不必要的 LSP。

4. 检查是否配置了 LSP 建立策略

(1) 在 MPLS LDP 视图下执行 **display this** 命令，如果显示信息中有 **lsp-trigger** 命令，则需要检查 IP 前缀策略中是否屏蔽了相关 LSP。

(2) 在系统视图下执行 **display ip prefix-list** 命令，如果显示信息中无相关路由的 LSP，请在策略中增加 LSP 对应的路由信息。

5. 请收集如下信息，并联系技术支持工程师

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

8 MPLS TE 故障处理

8.1 TE隧道状态为down

8.1.1 故障描述

指定的 TE 隧道的状态为 down。

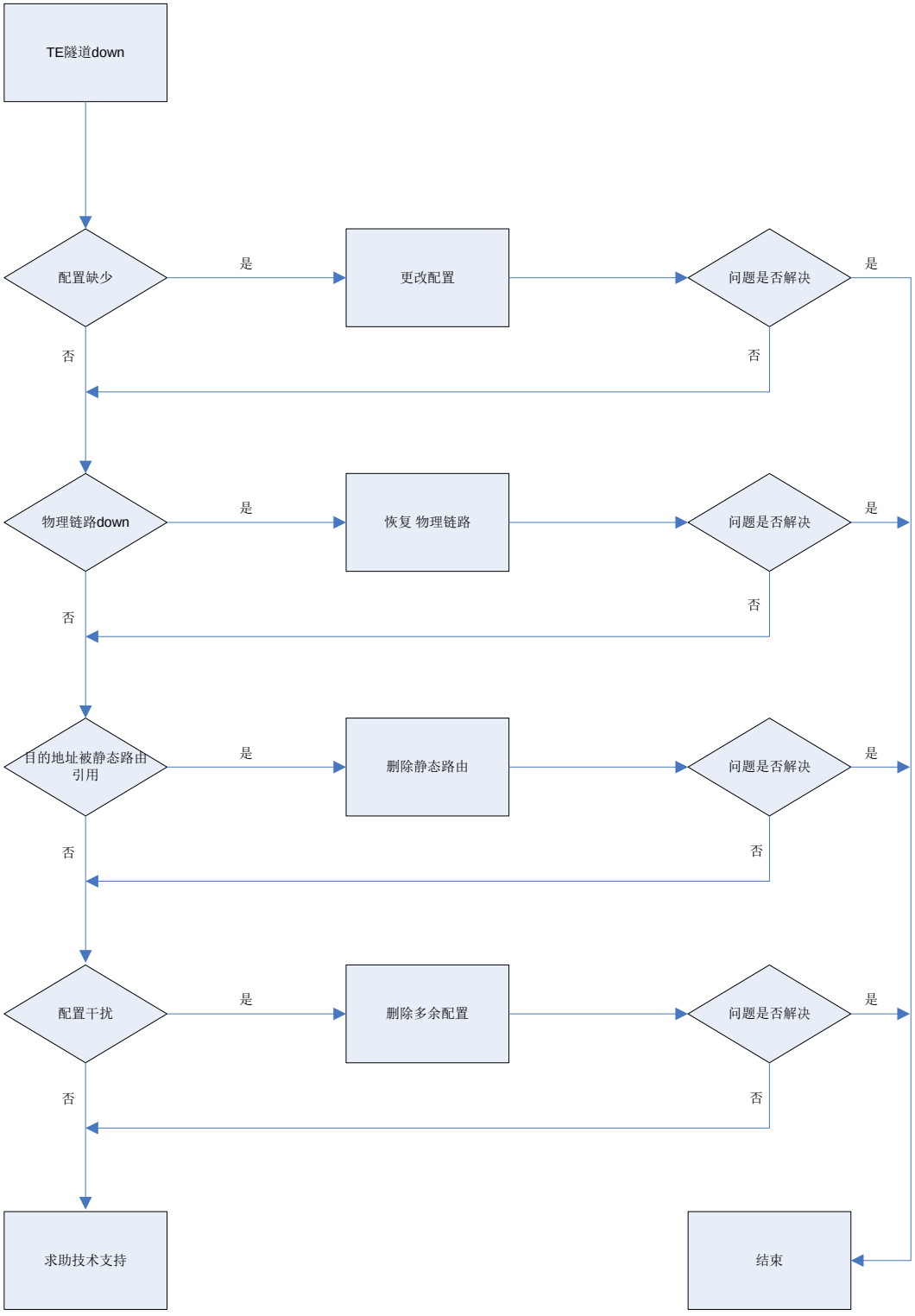
```
<Sysname> display interface tunnel 1
Tunnel1
Current state: DOWN
Line protocol state: DOWN
Description: Tunnel1 Interface
Bandwidth: 64kbps
Maximum transmission unit: 1476
Internet address: 10.1.2.1/24 (primary)
Tunnel source 2002::1:1 (Vlan-interface10), destination 2001::2:1
Tunnel TOS 0xC8, Tunnel TTL 255
Tunnel protocol/transport GRE/IPv6
    GRE key value is 1
    Checksumming of GRE packets disabled
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

8.1.2 故障诊断流程

TE 隧道状态为 down 的故障定位思路如下：

- 配置缺少。
- 物理链路 down。
- 隧道的目的地址被静态路由引用。
- 多余配置的干扰。

图5 TE 隧道状态为 down 故障诊断流程图



8.1.3 故障处理步骤

1. 检查配置

一般比较容易忽略的配置如下：

(1) 检查 OSPF 区域下是否配置 **mpls te enable** 命令。

(2) LSR ID、Router ID 和 LoopBack 接口地址最好保持一致。

(3) 检查是否配置 **rsvp**、**mpls te signaling rsvp-te** 和 **rsvp enable** 命令。

2. 查看 TE 隧道的物理链路是否为 up 状态

执行 **display interface** 命令，查看 TE 隧道的物理链路是否为 up 状态。

3. 查看 TE 隧道的目的地址是否被静态引用

执行 **display current-configuration | include** *destination* 命令，查看 TE 隧道的目的地址是否被静态引用。如果被静态路由引用，需取消这个静态路由。

4. 配置干扰

查看 TE 隧道下的配置，删除不必要的配置，防止干扰。

8.2 TE 隧道接口由up突然变down

8.2.1 故障描述

指定的 TE 隧道的状态由 up 突然变 down。

8.2.2 故障诊断流程

TE 隧道接口由 up 突然变 down 接口的定位思路如下：

- 隧道的配置被删除。
- 物理链路为 down。
- RSVP 消息超时。

同 TE 隧道状态为 down 的故障处理流程。

8.2.3 故障处理步骤

1. 隧道的配置被删除

参见 TE 隧道状态为 down 的故障处理步骤。

2. 物理链路为 down

参见 TE 隧道状态为 down 的故障处理步骤。

3. RSVP 消息超时

参见报文收发模块协议上送故障处理过程。

8.3 TE隧道存在环路

8.3.1 故障描述

流量走隧道不通，流量在设备间成环路。

8.3.2 故障处理步骤

1. 接口 IP 地址重复

RSVP-TE 不允许环路。当出现环路时，大部分情况下是接口 IP 重复导致的，请检查 TE 隧道经过的不同设备上接口 IP 地址是否重复。

2. 静态/动态 SR TE 特殊处理

静态和动态 SR TE 可以手动实现环路，请查看配置是否正确。

8.4 SR TE故障处理

8.4.1 故障描述

指定的 TE 隧道的状态为 down。

8.4.2 故障处理步骤

1. 检查配置

- 如果配置的是静态 SR TE，使用 **display mpls static-sr-mpls** 命令查看 LSP 是否为 up 状态。
- 如果配置的是动态 SR TE，使用 **display mpls lsp** 命令，查看到达隧道目的地址的 LSP 是否形成标签和出接口，如果没有形成，建议检查各设备的 SR TE 配置。

2. 查看 TE 隧道的物理链路是否是 UP 状态

执行 **display interface** 命令，查看 TE 隧道的物理链路是否为 up 状态。

3. 查看 TE 隧道的目的地址是否被静态路由引用

执行 **display current-configuration | include** *destination* 命令，查看 TE 隧道的目的地址是否被静态路由引用。如果被静态路由引用，需取消这个静态路由。

4. 配置干扰

查看 TE 隧道下的配置，删除不必要的配置，防止干扰。

9 MPLS L3VPN 故障处理

9.1 缺少去往对端VPN实例的路由

9.1.1 故障描述

执行 **display bgp peer vpnv4** 命令，查看 BGP VPNv4 对等体信息，不是 Established 状态或者不存在对等体信息。

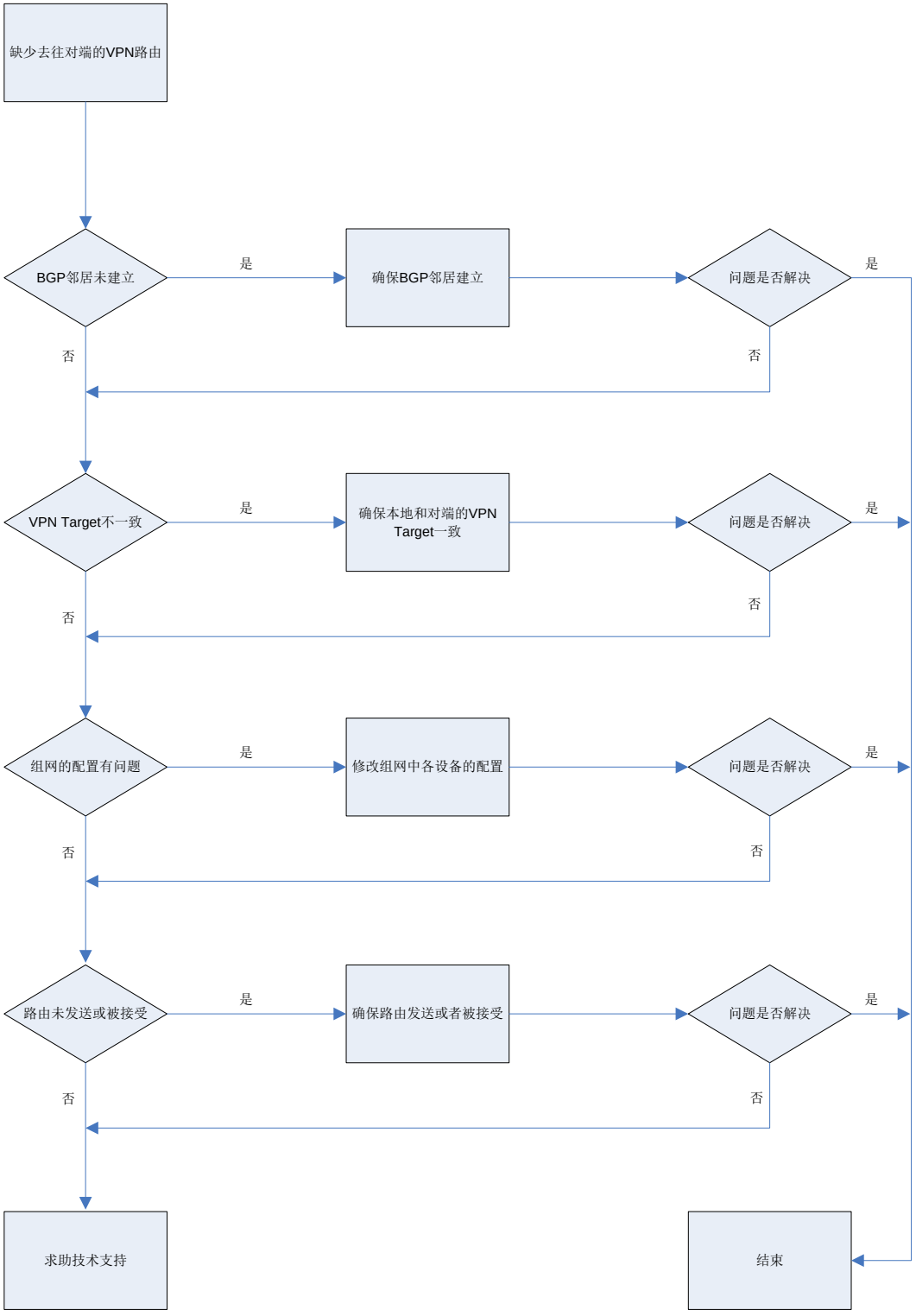
```
<Sysname> display bgp peer vpnv4

 BGP local router ID: 111.1.1.1
 Local AS number: 100
 Total number of peers: 1                 Peers in established state: 1

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

  113.1.1.1              100        3        4    0       0 00:00:52 Established
```

9.1.2 故障诊断流程

导致缺少去往对端 VPN 实例的路由常见的原因有以下几种：

- BGP 邻居没有建立。
- VPN Target 是否一致。
- 组网的配置是否有问题。
- 确认路由是否发送或被接受。

图6 故障诊断流程图


缺少去往对端的VPN路由
BGP邻居未建立
是
确保BGP邻居建立
问题是否解决
是
否
否
VPN Target不一致
是
确保本地和对端的VPN Target一致
问题是否解决
是
否
否
组网的配置有问题
是
修改组网中各设备的配置
问题是否解决
是
否
否
路由未发送或被接受
是
确保路由发送或者被接受
问题是否解决
是
否
否
求助技术支持
结束

9.1.3 故障处理步骤

1. BGP 邻居没有建立

执行 **display bgp peer vpnv4** 命令，查看 BGP VPNv4 对等体信息，确保 BGP 配置正确。

```
<Sysname> display bgp peer vpnv4

 BGP local router ID: 111.1.1.1
 Local AS number: 100
 Total number of peers: 1                 Peers in established state: 1

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

  113.1.1.1               100        3        4    0       0 00:00:52 Established
```

2. VPN Target 配置不一致

执行 **display current-configuration vpn-instance** 命令分别查看本地和对端的 VPN Target，确保一端的 import Target 与另一端的 export Target 一致。

```
<Sysname> display current-configuration vpn-instance
#
ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 111:1 import-extcommunity
 vpn-target 111:1 export-extcommunity
#
```

3. 组网中的配置有问题

若在 B 类跨域组网下，反射器设备没有关闭 VPN-Target 过滤功能，请关闭 VPN-Target 过滤功能。检查在跨域的部分设备是否配置了 **mpls enable** 命令，注意不需要配置 **mpls ldp enable** 命令。

4. 确认路由是否发送或被接受

发送方执行 **display bgp routing-table vpnv4 advertise-info** 命令，接收方执行 **display bgp routing-table vpnv4** 命令，确认路由是否发送或被接受。

- 查看发送方

```
<Sysname> display bgp routing-table vpnv4 3.3.3.3 32 advertise-info
……
 BGP routing table information of 3.3.3.3/32(TxPathID:0):
 Advertised to VPN peers (1 in total):
    113.1.1.1
 Inlabel              : 1151
```

- 查看接收方

```
<Sysname> display bgp routing-table vpnv4 3.3.3.3 32
……
 BGP routing table information of 3.3.3.3/32:
 From            : 111.1.1.1 (111.1.1.1)
……
```

5. 联系技术支持工程师

请收集如下信息，并联系技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

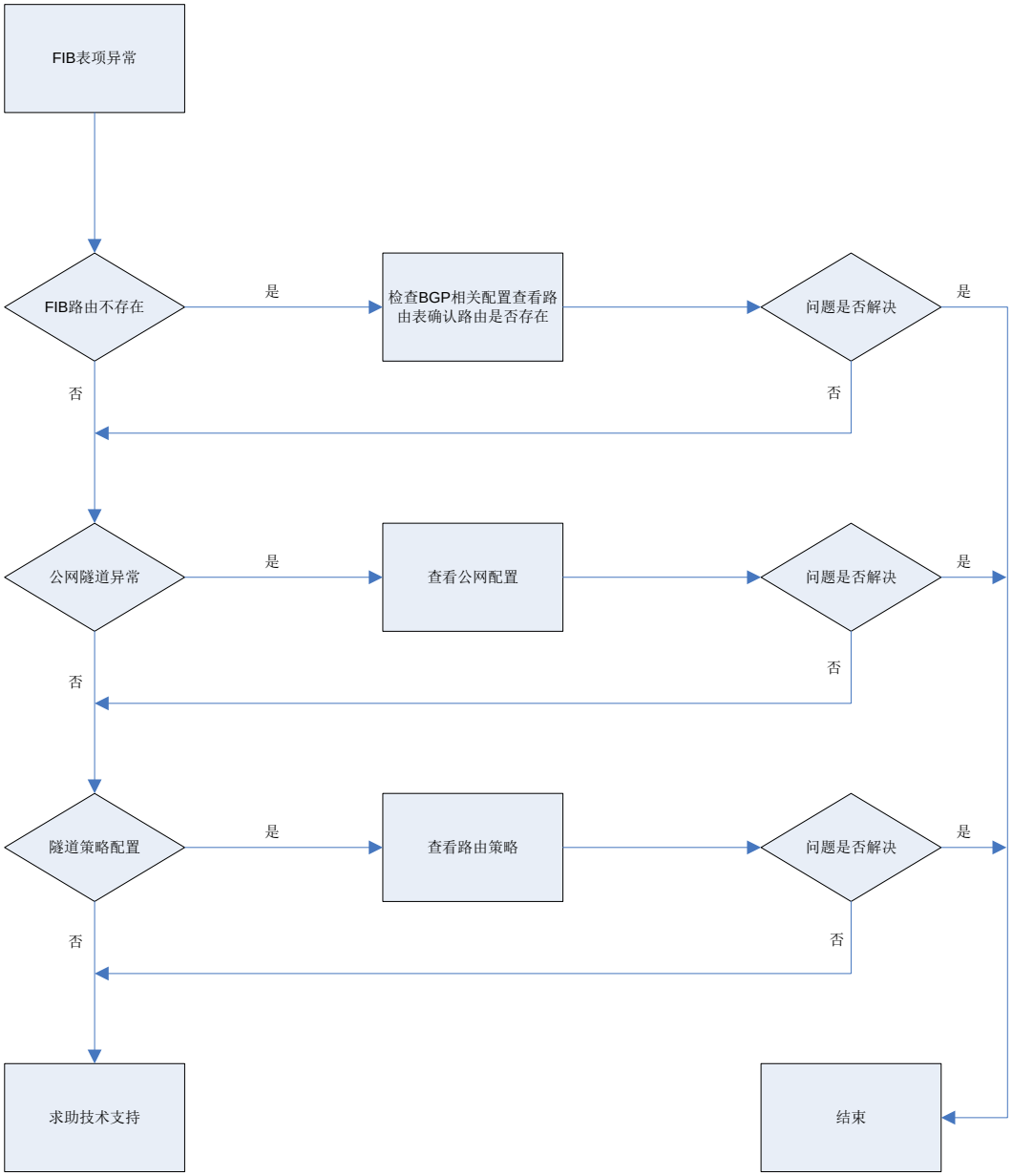
9.2 VPN实例下的FIB表项异常

9.2.1 故障描述

VPN 实例下的 FIB 表项中的路由不存在或 Token 值不存在。

9.2.2 故障诊断流程

图7 故障诊断流程图



9.2.3 故障处理步骤

1. FIB 表项中的路由不存在

执行 **display ip routing-table vpn-instance** 命令，查看 VPN 实例下的路由表，查看路由是否存在，若不存在，请检查 BGP 配置 是否正确。

2. Token 值不存在

(1) 执行 **display mpls ldp lsp** 命令，查看到 LSP，若 LSP 未正确生成，请确保公网隧道配置正确，且 BGP 配置了 **peer connect-interface** 命令。

(2) 查看配置的隧道策略是否正确。

3. 请收集如下信息，并联系技术支持工程师

上述步骤的执行结果。

10 MPLS L2VPN/VPLS 故障处理

说明

MPLS L2VPN 和 VPLS 协议的协商过程一致，以下步骤均以 VPLS 为例。

10.1 VPLS的VSI不能up

10.1.1 故障描述

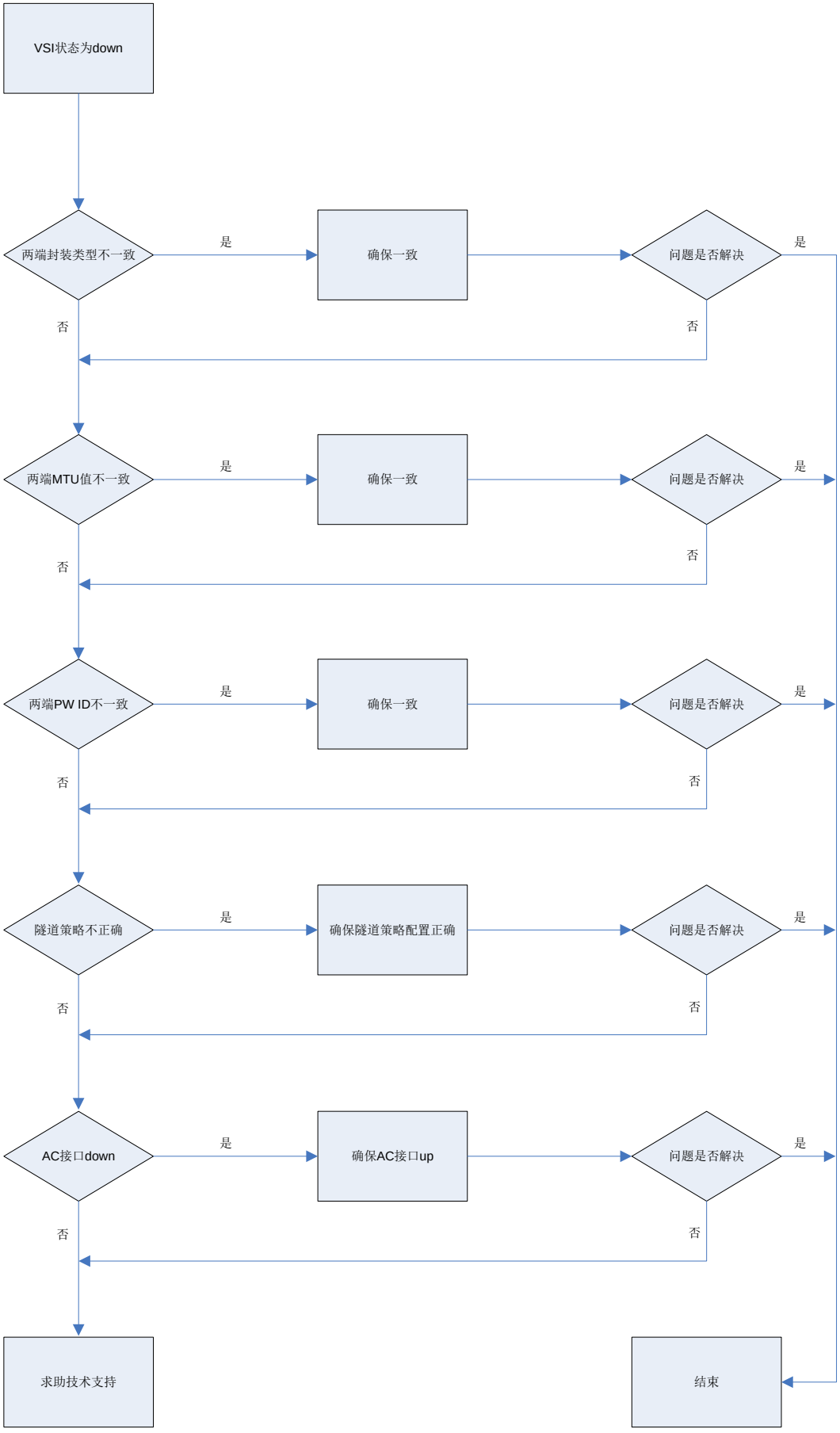
执行 **display l2vpn vsi verbose** 命令，查看对应 VSI 的状态不是 up 的状态。

```
<Sysname> display l2vpn vsi verbose
VSI Name: vpls1
  VSI Index               : 0
  VSI Description         : vsi for vpls1
  VSI State               : Up
  MTU                     : 1500
  Diffserv Mode           : -
  Bandwidth               : Unlimited
  Broadcast Restrain      : 5120 kbps
  Multicast Restrain      : 5120 kbps
  Unknown Unicast Restrain: 5120 kbps
  MAC Learning            : Enabled
  MAC Table Limit         : Unlimited
  MAC Learning rate       : Unlimited
  Drop Unknown            : Disabled
  PW Redundancy Mode      : Independent
  Flooding                : Enabled
  Statistics              : Disabled
  VXLAN ID                : -
  LDP PWs:
    Peer            PW ID           Link ID    State
    192.3.3.3       1               8          Up
    192.3.3.3       1001            8          Blocked
  BGP PWs:
    Peer            Remote Site     Link ID    State
    192.4.4.4       1               9          Up
```

```
ACs:
  AC                              Link ID    State
  GE3/1/1                         1          Up
```

10.1.2 故障诊断流程

图8 故障诊断流程图


VSI状态为down
两端封装类型不一致
是
确保一致
问题是否解决
是
否
否
两端MTU值不一致
是
确保一致
问题是否解决
是
否
否
两端PW ID不一致
是
确保一致
问题是否解决
是
否
否
隧道策略不正确
是
确保隧道策略配置正确
问题是否解决
是
否
否
AC接口down
是
确保AC接口up
问题是否解决
是
否
否
求助技术支持
结束

10.1.3 故障处理步骤

1. 检查两端的封装类型/MTU 是否一致

执行 **display l2vpn ldp verbose** 命令，查看两端的封装类型/MTU 是否一致。

- 如果两端的封装类型不一致，在 PW 模板视图下，配置 **pw-type** 命令修改其中一端的封装类型，使两端的封装类型一致。
- 如果两端的 MTU 不一致，在 VSI 视图下，配置 **mtu** 命令修改其中一端的 MTU，使两端的 MTU 一致。

```
<Sysname> display l2vpn ldp verbose
Peer: 2.2.2.9          PW ID: 500
  VSI Name: ccc
  PW State: Up
  PW Status Communication: Notification method
  PW Preferential Forwarding Status Bit: Process
  PW ID FEC (Local/Remote):
    PW Type     : VLAN/VLAN
    Group ID    : 0/0
    Label       : 1552/1552
    Control Word: Disabled/Disabled
    VCCV CV Type: -/-
    VCCV CC Type: -/-
    Flow Label  : Send/Recv
    MTU         : 1500/1500
    PW Status   : PW forwarding/PW forwarding
```

2. 检查两端的 PW-ID 是否一致

如果两端的 PW-ID 不一致，在 VSI LDP 信令视图下，配置 **peer** 命令修改 **pw-id** 参数，使两端一致。

3. 隧道策略选取是否正确

查看隧道策略配置，确认隧道策略选取的隧道类型，并通过 **display mpls forwarding nhlfe** 命令查看该类型的隧道是否存在且 up，若不存在，请建立该类型的隧道。

4. 检查两端的 AC 接口状态是否 Up

执行 **display interface brief** 命令，查看接口信息，确保接口状态为 up。

5. 请收集如下信息，并联系技术支持工程师

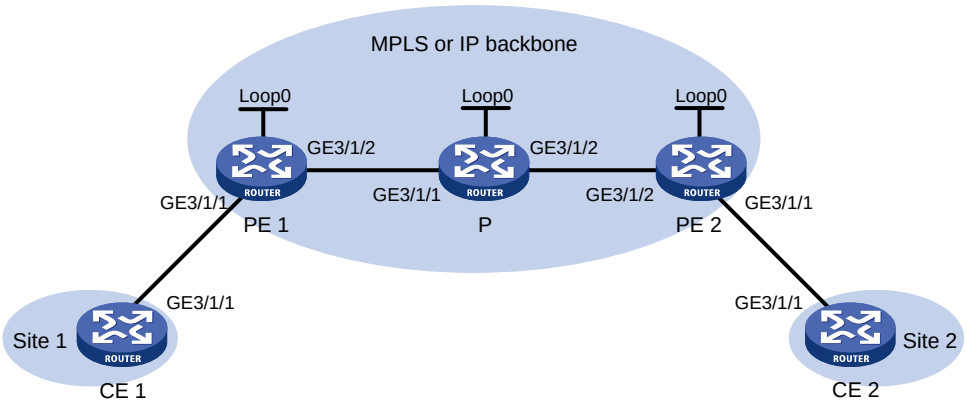
上述步骤的执行结果

11 MPLS 业务丢包故障处理

11.1 故障描述

MPLS 常见的组网如图 11-1 所示。MPLS 相关业务正常，CE1 与 CE2 之间发现存在丢包情况。

图9 MPLS 组网图



11.1 L3VPN丢包故障处理步骤

11.1.1 Ingress 节点丢包定位

1. 查看 FIB 表，确定 NID 值

执行 **display fib** 命令。查看 CE2 为目的地址的 FIB 表项，找到其 Token 值，Token 值即 NID 值。若 Token 值不存在，请参考 9.2 VPN 实例下的 FIB 表项异常。

```
[PE1]display fib vpn-instance vpn1 88.1.2.2 24

FIB entry count: 1

Flag:
  U:Usable    G:Gateway    H:Host    B:Blackhole    D:Dynamic    S:Static
  R:Relay      F:FRR

Destination/Mask    Nexthop         Flag      OutInterface/Token       Label
88.1.2.0/24         116.1.1.1       UGR       3081                     3029
```

2. 根据 NID 值查找出接口和公网标签

根据 NID 值，执行 **display mpls forwarding nhlfe** 命令，确认出接口和公网标签。

```
[PE1]display mpls forwarding nhlfe 3081
Flags: T - Forwarded through a tunnel
       N - Forwarded through the outgoing interface to the nexthop IP address
       B - Backup forwarding information
       A - Active forwarding information
       M - P2MP forwarding information
```

```
NID        Tnl-Type    Flag OutLabel Forwarding Info
------------------------------------------------------------------------------
3081       LSP         NA   3082     XGE3/1/2                 10.0.0.2
```

3. 根据接口报文出入的统计，确定是否丢包

执行 **display counters inbound** 命令，查看输入报文的流量统计，执行 **display counters outbound** 命令，查看输出报文的流量统计，若出入报文的统计计数不相等，则可以判断为在 ingress 节点丢包。

11.1.2 P 节点丢包定位

1. 确认入标签

通过 **display mpls ldp lsp** 命令查找 P 节点的入标签是否与 ingerss 节点的出标签一致。

2. 查找出接口和公网标签

根据 ingress 节点查到的出标签，执行 **display mpls forwarding ilm** 命令，查找 P 节点的出标签值。

```
[P]display mpls forwarding ilm 3082
Flags: T - Forwarded through a tunnel
       N - Forwarded through the outgoing interface to the nexthop IP address
       B - Backup forwarding information
       A - Active forwarding information
       M - P2MP forwarding information

InLabel Oper    VRF    Flag SwapLabel Forwarding Info
------------------------------------------------------------------------------
3082    SWAP    0      NA   3083      XGE3/1/2                  12.11.2.1
```

3. 根据接口报文出入的统计，确定是否丢包

执行 **display counters inbound** 命令，查看输入报文的流量统计，执行 **display counters outbound** 命令，查看输出报文的流量统计，若出入报文的统计计数不相等，则可以判断为在 P 节点丢包。

11.1.3 egress 节点丢包定位

1. 根据接口报文出入的统计，确定是否丢包

执行 **display counters inbound** 命令，查看输入报文的流量统计，执行 **display counters outbound** 命令，查看输出报文的流量统计，若出入报文的统计计数不相等，则可以判断为在 egress 节点丢包。

11.1.4 联系技术支持工程师

收集上述信息，并联系技术支持工程师。

11.2 L2VPN丢包故障处理步骤

11.2.1 Ingress 节点丢包定位

1. 确定 PW 对应的 NID 值

执行 **display l2vpn forwarding pw** 命令。查看指定 PW 的 NID 值。

```
<PE1> display l2vpn forwarding pw xconnect-group aaa
Total number of cross-connections: 1
Total number of PWs: 1, 1 up, 0 blocked, 0 down

Xconnect-group Name             In/Out Label    NID         Link ID    State
aaa                             1279/1046       3081        64         Up
```

2. 根据 NID 值查找出接口和公网标签

根据 NID 值，执行 **display mpls forwarding nhlfe** 命令，确认出接口和公网标签。

```
[PE1]display mpls forwarding nhlfe 3081
Flags: T - Forwarded through a tunnel
       N - Forwarded through the outgoing interface to the nexthop IP address
       B - Backup forwarding information
       A - Active forwarding information
       M - P2MP forwarding information

NID         Tnl-Type    Flag OutLabel Forwarding Info
------------------------------------------------------------------------------
3081        LSP         NA   3082     XGE3/1/2                 10.0.0.2
```

3. 根据接口报文出入的统计，确定是否丢包

执行 **display counters inbound** 命令，查看输入报文的流量统计，执行 **display counters outbound** 命令，查看输出报文的流量统计，若出入报文的统计计数不相等，则可以判断为在 ingress 节点丢包。

11.2.2 P 节点丢包定位

1. 确认入标签

通过 **display mpls ldp lsp** 命令查找 P 节点的入标签是否与 ingerss 节点的出标签一致。

2. 查找出接口和公网标签

根据 ingress 节点查到的出标签，执行 **display mpls forwarding ilm** 命令，查找 P 节点的出标签值。

```
[P]display mpls forwarding ilm 3082
Flags: T - Forwarded through a tunnel
       N - Forwarded through the outgoing interface to the nexthop IP address
       B - Backup forwarding information
       A - Active forwarding information
       M - P2MP forwarding information

InLabel Oper    VRF   Flag SwapLabel Forwarding Info
```

```
--------------------------------------------------------------------------------
3082    SWAP    0     NA   3083      XGE3/1/2                  12.11.2.1
```

3. 根据接口报文出入的统计，确定是否丢包

执行 **display counters inbound** 命令，查看输入报文的流量统计，执行 **display counters outbound** 命令，查看输出报文的流量统计，若出入报文的统计计数不相等，则可以判断为在 P 节点丢包。

11.2.3 egress 节点丢包定位

1. 根据接口报文出入的统计，确定是否丢包

执行 **display counters inbound** 命令，查看输入报文的流量统计，执行 **display counters outbound** 命令，查看输出报文的流量统计，若出入报文的统计计数不相等，则可以判断为在 egress 节点丢包。

若实际组网环境不能通过接口流量定位可参见 11.4 MPLS 丢包问题定位实例。

11.2.4 联系技术支持工程师

收集上述信息，并联系技术支持工程师。

11.3 VPLS丢包故障处理步骤

11.3.1 Ingress 节点丢包定位

1. 确定 PW 对应的 NID 值

执行 **display l2vpn forwarding pw** 命令。查看指定 VSI 内 PW 的 NID 值。

```
<PE1> display l2vpn forwarding pw vsi aaa
Total number of VSIs: 1
Total number of PWs: 2, 2 up, 0 blocked, 0 down

VSI Name                        In/Out Label    NID        Link ID    State
aaa                             1279/1046       3081       64         Up
```

2. 根据 NID 值查找出接口和公网标签

根据 NID 值，执行 **display mpls forwarding nhlfe** 命令，确认出接口和公网标签。

```
[PE1]dis mpls forwarding nhlfe 3081
Flags: T - Forwarded through a tunnel
       N - Forwarded through the outgoing interface to the nexthop IP address
       B - Backup forwarding information
       A - Active forwarding information
       M - P2MP forwarding information

NID        Tnl-Type   Flag OutLabel Forwarding Info
--------------------------------------------------------------------------------
3081       LSP        NA   3082     XGE3/1/2                10.0.0.2
```

3. 根据接口报文出入的统计，确定是否丢包

执行 **display counters inbound** 命令，查看输入报文的流量统计，执行 **display counters outbound** 命令，查看输出报文的流量统计，若出入报文的统计计数不相等，则可以判断为在 ingress 节点丢包。

若实际组网环境不能通过接口流量定位可参见 11.4 MPLS 丢包问题定位实例。

11.3.2 P 节点丢包定位

1. 确认入标签

通过 **display mpls ldp lsp** 命令查找 P 节点的入标签是否与 ingerss 节点的出标签一致。

2. 查找出接口和公网标签

根据 ingress 节点查到的出标签，执行 **display mpls forwarding ilm** 命令，查找 P 节点的出标签值。

```
[P]display mpls forwarding ilm 3082
Flags: T - Forwarded through a tunnel
       N - Forwarded through the outgoing interface to the nexthop IP address
       B - Backup forwarding information
       A - Active forwarding information
       M - P2MP forwarding information

InLabel Oper    VRF   Flag SwapLabel Forwarding Info
------------------------------------------------------------------------------
3082    SWAP    0     NA   3083      XGE3/1/2                  12.11.2.1
```

3. 根据接口报文出入的统计，确定是否丢包

执行 **display counters inbound** 命令，查看输入报文的流量统计，执行 **display counters outbound** 命令，查看输出报文的流量统计，若出入报文的统计计数不相等，则可以判断为在 P 节点丢包。

若实际组网环境不能通过接口流量定位可参见 11.4 MPLS 丢包问题定位实例。

11.3.3 egress 节点丢包定位

1. 根据接口报文出入的统计，确定是否丢包

执行 **display counters inbound** 命令，查看输入报文的流量统计，执行 **display counters outbound** 命令，查看输出报文的流量统计，若出入报文的统计计数不相等，则可以判断为在 egress 节点丢包。

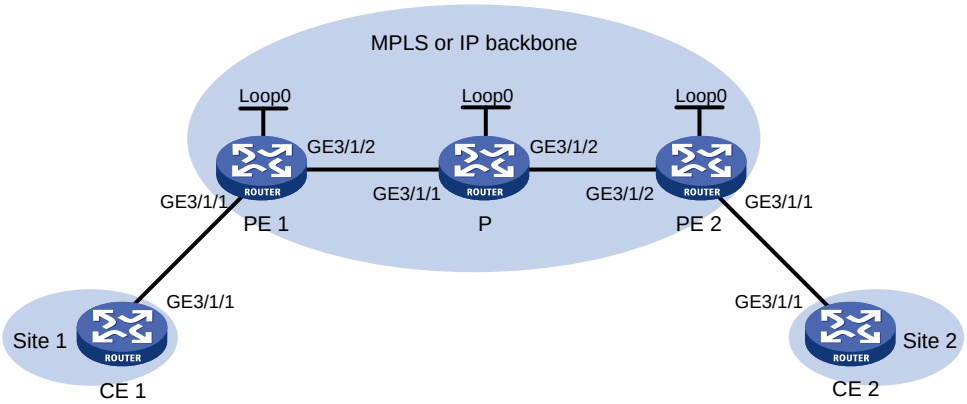
11.3.4 联系技术支持工程师

收集上述信息，并联系技术支持工程师。

11.4 MPLS丢包问题定位实例

11.4.1 组网环境

图10 组网环境图



11.4.2 使用 QoS 策略定位丢包设备

1. 配置步骤

(1) 配置 PE1 设备

配置 QoS 策略。

```
[PE1] traffic classifier 1 operator and
[PE1-classifier-1] if-match dscp cs4
[PE1-classifier-1] quit
[PE1] traffic behavior 1
[PE1-behavior-1] remark mpls-exp 1
[PE1-behavior-1] quit
[PE1] qos policy 1
[PE1-qospolicy-1] classifier 1 behavior
```

接口应用 QoS 策略。

```
[PE1] interface gigabitethernet 3/1/1
[PE1-GigabitEthernet3/1/1] qos apply policy 1
```

在接口上配置端口优先级信任模式为 auto。

```
[PE1-GigabitEthernet3/1/1] qos trust auto
[PE1-GigabitEthernet3/1/1] quit
[PE1] interface gigabitethernet 3/1/2
[PE1-GigabitEthernet3/1/2] qos trust auto
[PE1-GigabitEthernet3/1/2] quit
```

(2) 配置 P 设备

配置 QoS 策略。

```
[P] traffic classifier 1 operator and
[P-classifier-1] if-match dscp cs4
[P-classifier-1] quit
```

```
[P] traffic behavior 1
[P-behavior-1] remark mpls-exp 1
[P-behavior-1] quit
[P] qos policy 1
[P-qospolicy-1] classifier 1 behavior
```

接口应用 QoS 策略。

```
[P] interface gigabitethernet 3/1/1
[P-GigabitEthernet3/1/1] qos apply policy 1
[P-GigabitEthernet3/1/1] quit
[P] interface gigabitethernet 3/1/2
[P-GigabitEthernet3/1/2] qos apply policy 1
[P-GigabitEthernet3/1/2] quit
```

在接口上配置端口优先级信任模式为 auto。

```
[P-GigabitEthernet3/1/1] qos trust auto
[P-GigabitEthernet3/1/1] quit
[P] interface gigabitethernet 3/1/2
[P-GigabitEthernet3/1/2] qos trust auto
[P-GigabitEthernet3/1/2] quit
```

(3) 配置 PE2 设备

配置 QoS 策略。

```
[PE2] traffic classifier 1 operator and
[PE2-classifier-1] if-match dscp cs4
[PE2-classifier-1] quit
[PE2] traffic behavior 1
[PE2-behavior-1] remark mpls-exp 1
[PE2-behavior-1] quit
[PE2] qos policy 1
[PE2-qospolicy-1] classifier 1 behavior
```

接口应用 QoS 策略。

```
[PE2] interface gigabitethernet 3/1/1
[PE2-GigabitEthernet3/1/1] qos apply policy 1
```

在接口上配置端口优先级信任模式为 auto。

```
[PE2-GigabitEthernet3/1/1] qos trust auto
[PE2-GigabitEthernet3/1/1] quit
[PE2] interface gigabitethernet 3/1/2
[PE2-GigabitEthernet3/1/2] qos trust auto
[PE2-GigabitEthernet3/1/2] quit
```

2. 操作流程

完成以上配置后，进行以下操作：

(1) 清除设备的端口计数。

(2) 在设备上配置 **debugging ip icmp** 命令打开 ICMP 调试信息开关。

(3) 在 CE1 带 tos 字段去 ping，如 ping -a 1.1.1.1 -tos 96 -s 1000 –m 1 –t 0 -c 10 2.2.2.2。通过 **display qos queue-statistics interface outbound** 命令查看沿途设备的接口的哪个队列没有报文，ping 的时候的 tos 字段就用哪个队列。

(4) 查看 ping 操作后的 ICMP 报文的打印情况。通过 **display qos queue-statistics interface outbound** 查看经过各设备端口的报文数量是否一致，若不一致，则发生丢包。

(5) 进行 CE2 带 tos 字段去 ping，操作方法与上述操作类似。

11.4.3 使用 diffserver 定位丢包设备

1. 配置步骤

(1) 配置 PE1 设备的 diffserver

通过 **display qos queue-statistics interface outbound** 命令查看沿途设备的接口的哪个队列没有报文，diffserver 设置为相关值。

- 在 MPLS L3VPN 组网中。

```
[PE1] ip vpn-instance vpn
[PE1-vpn-instance-vpn] diffserv-mode pipe cs6
```

- 在 MPLS L2VPN 组网中。

```
[PE1] xconnect-group vpn
[PE1-xcg-vpn] connection 1
[PE1-xcg-vpn-1] diffserv-mode pipe cs6
```

- 在 VPLS 组网中。

```
[PE1] vsi vpn
[PE1-vsi-vpn] diffserv-mode pipe cs6
```

(2) 配置 PE2 设备的 diffserver

与 PE1 配置类似，请参考 PE1 的配置。

(3) 配置 P 设备

配置 QoS 策略。

```
[P] traffic classifier 1 operator and
[P-classifier-1] if-match dscp cs4
[P-classifier-1] quit
[P] traffic behavior 1
[P-behavior-1] remark mpls-exp 1
[P-behavior-1] quit
[P] qos policy 1
[P-qospolicy-1] classifier 1 behavior
```

接口应用 QoS 策略。

```
[P] interface gigabitethernet 3/1/1
[P-GigabitEthernet3/1/1] qos apply policy 1
[P-GigabitEthernet3/1/1] quit
[P] interface gigabitethernet 3/1/2
[P-GigabitEthernet3/1/2] qos apply policy 1
[P-GigabitEthernet3/1/2] quit
```

在接口上配置端口优先级信任模式为 auto。

```
[P-GigabitEthernet3/1/1] qos trust auto
[P-GigabitEthernet3/1/1] quit
[P] interface gigabitethernet 3/1/2
```

```
[P-GigabitEthernet3/1/2] qos trust auto
[P-GigabitEthernet3/1/2] quit
```

2. 操作流程

完成以上配置后，进行以下操作：

(1) 清除设备的端口计数。

(2) 在 CE1 带 tos 字段去 ping，如 ping -a 1.1.1.1 -tos 96 -s 1000 –m 1 –t 0 -c 10 2.2.2.2。通过 **display qos queue-statistics interface outbound** 命令查看沿途设备的接口的哪个队列没有报文，ping 的时候的 tos 字段就用哪个队列。

(3) 通过 **display qos queue-statistics interface outbound** 查看经过各设备端口的报文数量是否一致，若不一致，则发生丢包。

(4) 进行 CE2 带 tos 字段去 ping，操作方法与上述操作类似。

12 报文转发故障处理

12.1 ping不通或丢包

12.1.1 故障描述

报文转发丢包，ping 不通或 ping 丢包，tracert 异常。

```
<Sysname> ping 10.0.0.5
PING 10.0.0.5 (10.0.0.5): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- 10.0.0.5 ping statistics ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

12.1.2 故障处理步骤

1. 查看 ICMP 调试信息

在 ping 的源和目的设备上，使用 **debugging ip icmp** 命令打开 ICMP 调试信息开关；中间硬转发设备可做流统。当对端 ping 本设备时，可以看到下列调试信息。如果未显示 ICMP 请求报文信息，则说明未接收到请求报文；如果未显示 ICMP 应答报文，则说明本设备未应答 ICMP 请求。

打开 ICMP 的调试信息开关。对端 ping 本设备时，本设备会输出下列调试信息。

```
<Sysname> debugging ip icmp
*Feb  8 18:28:47:417 2011 Sysname SOCKET/7/ICMP:
ICMP Input:
 ICMP Packet: src = 192.168.20.14, dst = 192.168.20.13
              type = 8, code = 0 (echo)
```

// 接收 ICMP 请求报文，报文源 IP 地址为 192.168.20.14，报文目的 IP 地址为 192.168.20.13

```
*Feb  8 18:28:47:451 2011 Sysname SOCKET/7/ICMP:
```

```
ICMP Output:
 ICMP Packet: src = 192.168.20.13, dst = 192.168.20.14
              type = 0, code = 0 (echo-reply)
```

// 发送 ICMP 应答报文，报文源 IP 地址为 192.168.20.13，报文目的 IP 地址为 192.168.20.14

2. 设备入出报文统计

报文转发异常通常会涉及多台设备，需要逐一排查。为方便排查，排查前建议先明确报文的转发走向，如经过哪些中间设备，在设备的哪些接口进入设备，又会从哪些接口出去。通过镜像抓包或配置 ACL 规则统计设备有没有收到或发出相应的业务报文，以配置 ACL 规则统计端口入方向 Ping 报文为例：

(1) 定义相关的 ACL

```
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 1 permit ip destination 1.1.1.1 0
```

(2) 定义流分类和流行为

```
[Sysname] traffic classifier  statistic_1
[Sysname-classifier-static] if-match acl 3000
[Sysname] traffic behavior statistic_1
[Sysname-classifier-static] accounting packet
```

(3) 定义策略

```
[Sysname] qos policy statistic_1
[Sysname-classifier-static] classifier statistic_1 behavior statistic_1
```

(4) 将策略应用到端口入方向

```
[Sysname] interface gigabitehternet 8/0/1
[Sysname-GigabitEthernet8/0/1] qos apply policy statistic_1 inbound
```

(5) 检查入方向报文统计计数，可以通过 reset counter interface 命令清除计数

```
<Sysname> display qos policy interface gigabitethernet8/0/1
Interface: GigabitEthernet8/0/1

  Direction: Inbound

  Policy: statistic_1
   Classifier: statistic_1
     Operator: AND
     Rule(s) : If-match acl 3000
     Behavior: statistic_1
      Accounting Enable:
         1000 (Packets)
```

3. 报文计数分析

如果设备未收到 Ping 报文，请排查上游的相邻设备；如果设备发送的 Ping 报文计数正确，建议排查下游的相邻设备；如果 Ping 报文入出计数不正确，请参照 L3 转发故障、MPLS 转发故障继续排查。

12.2 VLAN转发故障

12.2.1 故障描述

故障现象通常有二层 VLAN 单播、广播业务异常。

12.2.2 故障处理步骤

1. 检查生成树协议的状态

使用 **display stp brief** 命令查看设备上是否开启了生成树协议。

```
[Sysname] display stp brief
 MST ID   Port                                Role  STP State   Protection
 0        Bridge-Aggregation1                 DESI  FORWARDING  NONE
 0        Ten-GigabitEthernet3/2/4            DESI  LEARNING    NONE
```

如果因为开启了生成树协议导致二层 VLAN 流量不通，可以使用 **undo stp global enable** 命令全局关闭生成树协议。

2. 检查 VLAN 配置的正确性

(1) 通过 **display interface** 命令检查端口是否允许打入流量的 VLAN 通过。如果端口未允许打入流量的 VLAN 通过，则需要在端口下配置允许该 VLAN 通过。

(2) 使用命令 **display vlan 4094** 命令查看 VLAN 4094 是否被创建。

```
[Sysname] display vlan 4094
 VLAN ID: 4094
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 4094
 Name: VLAN 4094
 Tagged ports:   None
 Untagged ports: None
```

- 以下单板的端口不支持 VLAN 4094。请不要将这些端口加入 VLAN 4094。
  - CSPC 类单板（CSPC-GE16XP4L-E、CSPC-GE24L-E 和 CSPC-GP24GE8XP2L-E 除外）
  - CMPE-1104 单板

3. 检查 QinQ 配置的正确性

使用 **display qinq** 命令检查端口是否使能了 QinQ。

当端口上配置了 QinQ 功能后，不论从该端口收到的报文是否带有 VLAN Tag，设备都会为该报文添加本端口 PVID 的 Tag。注意此时该端口打入流量的实际生效 VLAN 是 QinQ 功能封装的 VLAN。

12.3 聚合口故障

12.3.1 故障描述

故障现象通常为二层聚合口、三层聚合口业务异常，例如聚合成员口无法选中、聚合负载分担业务异常。

12.3.2 故障处理步骤

1. 聚合成员端口无法选中

(1) 通过 **display link-aggregation verbose** 命令查看聚合接口对应聚合组的详细信息。

```
[Sysname] display link-aggregation verbose Route-Aggregation 12
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation12
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status  Priority Oper-Key
  XGE7/2/1         U       32768    2
  XGE7/2/2         U       32768    2
```

(2) 检查聚合口下的成员口物理状态是否 UP，如果是 DOWN 状态，请检查连线。

```
[Sysname]display interface Ten-GigabitEthernet 3/2/4
Ten-GigabitEthernet3/2/4
Current state: DOWN
Line protocol state: DOWN(LAGG)
Description: Ten-GigabitEthernet3/2/4 Interface
Bandwidth: 10000000 kbps Flow-control is not enabled
```

(3) 检查聚合口下的配置和成员口的配置是否一致，如果不一致，会出现成员端口无法选中的现象。

(4) 检查聚合口下各成员口的速率配置是否一致，如果不一致，可以通过 `link-aggregation ignore speed` 命令用来配置聚合组选择选中端口时忽略端口速率。如果聚合组两端本命令配置不一致，动态聚合组可以通过 LACP 协议协商状态，使链路两端端口状态一致；静态聚合组无法协商状态，为了防止报文丢失，所以要求静态聚合组两端本命令配置一致。配置本命令后，如果聚合组中选中端口速率不同，聚合组中流量负载分担时，速率较小的选中端口可能存在丢包现象，请按需配置本功能。开启和关闭本功能后，操作 Key 会发生变化，导致聚合接口震荡，请按需配置本功能。

(5) 如果聚合口下的配置和成员口的配置相同，聚合成员口还是无法选中，则联系技术支持。

2. 聚合负载分担业务异常。

请联系技术支持。

12.4 MAC地址学习故障

12.4.1 故障描述

故障现象通常为端口没有学习到报文的源 MAC 地址。

12.4.2 故障处理步骤

1. 检查源 MAC 地址的正确性

通过 **display mac-address** 或 **display l2vpn mac-address** 命令检查源 MAC 地址。

源 MAC 地址学习仅支持单播 MAC 地址，不支持组播 MAC 地址、不支持全 0 的 MAC 地址。MAC 地址的第一个字节最低为 0 是单播 MAC 地址，如 00-00-00-00-00-01，组播 MAC 地址为 01-00-00-00-00-01。

2. 检查源 MAC 老化时间的正确性

使用 **display mac-address aging-time** 命令查看 MAC 地址的老化时间，如果配置的老化时间过低，MAC 地址的数量很大，会出现 MAC 地址被快速老化删除的情况。

```
[Sysname] display mac-address aging-time
MAC address aging time: 10s.
[Sysname] display l2vpn mac-address count
875613 mac address(es) found.
```

3. 检查端口状态

端口状态为 down 时，不会学习 MAC 地址。使用 **display interface** 命令查看端口的状态。

```
[Sysname] display interface Ten-GigabitEthernet 7/2/3
Ten-GigabitEthernet7/2/3
Current state: DOWN
Line protocol state: DOWN
...
```

4. 检查端口是否有流量进入

端口没有流量进入时，不会学习 MAC 地址。使用 **display counters inbound** 命令查看端口是否有流量进入。

```
<Sysname> display counters inbound interface Ten-GigabitEthernet 7/2/3
Interface                   Total(pkt) Broadcast(pkt) Multicast(pkt) Err(pkt)
XGE7/2/3                             0              0              0        0

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

5. 检查设备是否出现迁移流量

迁移流量指两条源 MAC 地址相同的流量进入不同的端口时，MAC 地址会在两个端口之前来回迁移。如果配置了聚合接口并且按报文的目的 IP 地址进行聚合负载分担（**destination-ip**），当源 MAC 地址相同但目的 IP 地址不同的报文进入该聚合接口时，可能会出现迁移流量，导致其中一个成员端口学习到的 MAC 地址迁移到另一个成员端口。

使用 **display link-aggregation load-sharing mode** 命令查看全局采用的聚合负载分担类型，如果为 **destination-ip** 类型，请联系技术支持。

12.5 L3转发故障

12.5.1 故障描述

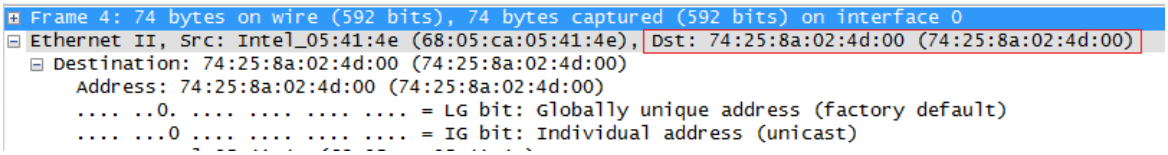
故障现象通常有三层业务异常、ping/tracert 丢包/不通。

12.5.2 故障处理步骤

1. 报文目的 MAC 检查

报文在路由器上进行三层转发的条件是报文的目的 MAC 为路由器本身的 MAC。通过镜像或抓包确认这个条件是否满足，“镜像”的详细介绍，请参见“网络管理和监控配置指导”中的“镜像”。如下图，报文的目的 MAC 为路由器接口的 MAC，说明报文目的 MAC 正确。

图11 报文目的 MAC




```
<Sysname> display interface GigabitEthernet 3/2/2
GigabitEthernet3/2/2
Current state: UP
Line protocol state: UP
Description: GigabitEthernet3/2/2 Interface
Bandwidth: 1000000kbps
Maximum Transmit Unit: 1500
Internet Address is 10.0.0.1/24 Primary
IP Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 7425-8a02-4d00
IPv6 Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 7425-8a02-4d00
Media type is not sure, Port hardware type is 10G_BASE_SR_SFP
Port priority: 0
Last clearing of counters: Never
 Last 300 seconds input:  20 packets/sec 2565 bytes/sec  0%
 Last 300 seconds output: 0 packets/sec 30 bytes/sec  0%
 Input  (total): 219479 packets, 28092544 bytes
          219476 broadcasts, 0 multicasts, - pauses
 Input  (normal): 219479 packets, 28092544 bytes
          - broadcasts, - multicasts, 0 pauses
 Input: 0 input errors, 0 runts, 0 giants, 0 throttles
          0 CRC, 0 frame, 0 overruns, - aborts
          0 ignored, - parity errors
 Output  (total): 4608 packets, 316764 bytes
          3378 broadcasts, 1154 multicasts, - pauses
```

2. 路由表检查

检查设备到某一目的 IP 网段的路由是否存在，如路由不存在，请检查路由协议配置、状态是否正确。

```
<Sysname> display ip routing-table 1.1.1.0
Summary Count : 1
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
1.1.1.0/24          Static 60   0            10.0.0.2        GE3/2/2
```

需要注意的是，当 32 位掩码的主机路由与 ARP 表项的出接口不一致时，以主机路由的出接口为准。

3. FIB 表检查

检查设备到某一目的 IP 网段的 FIB 表项是否存在，如路由存在、FIB 表项异常，请将故障信息发送技术支持人员分析。

```
<Sysname> display fib 1.1.1.0
Destination count: 1 FIB entry count: 1
Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay     F:FRR
Destination/Mask    Nexthop         Flag     OutInterface/Token       Label
1.1.1.0/24          10.0.0.2        USG      GE3/2/2                   Null
```

4. ARP 检查

检查设备 ARP 学习的接口是否正确，如学习接口不正确，请通过 reset arp 命令重新学习 ARP，必要时可以使用 arp static 命令配置静态 ARP。如 ARP 学习的接口一直不正确，请将故障信息发送技术支持人员分析。

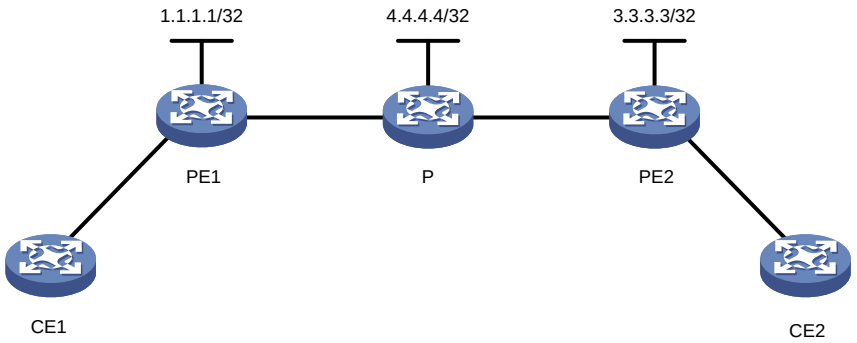
```
<Sysname> display arp 10.0.0.2
Type: S-Static    D-Dynamic    M-Multiport    I-Invalid
IP address      MAC address    VLAN     Interface                Aging Type
10.0.0.2        0000-0000-0001 N/A       GE3/2/2                  N/A   S
```

12.6 MPLS转发故障

12.6.1 故障描述

MPLS 常见的组网如图 12-2 所示。MPLS 转发故障时，CE1 与 CE2 之间报文发送接收错误。

图12 MPLS 组网图



12.6.2 故障处理步骤

L2VPN、VPLS、L3VPN 是基于 LSP 建立的。在 LSP 入节点（图 12-2 中的 PE1）上通过下列方式来检查、确认 MPLS 网络中哪台设备存在配置错误。

1. MPLS LSP

(1) 检查配置的 LSP 是否存在，如不存在，请检查 MPLS LSP 配置是否正确。

```
[PE1] display mpls lsp
```

```
FEC                         Proto    In/Out Label    Interface/Out NHLFE
100.100.100.100/32          LDP      3/-             -
4.4.4.4/32                  LDP      NULL/3          GE3/0/1
90.0.0.0/24                 LDP      NULL/3          GE3/0/1
1.1.1.1/32                  LDP      3/NULL          InLoop0
50.0.0.0/24                 LDP      NULL/3          GE3/0/1
70.0.0.0/24                 LDP      NULL/3          GE3/0/1
3.3.3.3/32                  LDP      NULL/1025       GE3/0/1
```

(2) 检查 MPLS LDP 会话，如果状态不是 Operational，说明会话存在错误，请转步骤（3）、（4）；如果 MPLS LDP 会话正常，请转步骤（5）。

```
[PE1] display mpls ldp peer
Total number of peers: 1
Peer LDP ID             State         Role     GR   MD5  KA Sent/Rcvd
4.4.4.4:0               Operational   Passive  Off  Off  39/39
```

(3) 通过 **display mpls ldp interface** 命令查看 LDP 接口的相关信息。如配置信息不正确，请检查 MPLS LDP 配置。

```
[PE1] display mpls ldp interface
Interface                MPLS         LDP             Auto-config
Vlan103                  Enabled      Configured      -
GE3/0/2                  Enabled      Configured      -
XGE2/0/6                 Enabled      Configured      -
```

(4) 检查接口下是否使能 MPLS、MPLS LDP。如未使能，请使能 MPLS 和 MPLS LDP。建立 LSP 的所有接口上均需要使能 MPLS 和 MPLS LDP。

```
[PE1] interface gigabitethernet 3/0/1
[PE1-GigabitEthernet3/0/1] display this
#
interface GigabitEthernet3/0/1
 ip address 1.1.1.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
return
```

(5) 检查配置的 **mpls lsr-id** 是不是等于 Loopback 接口 IP 地址。推荐使用设备上某个 Loopback 接口的地址作为 LSR ID。

```
<PE1> display current-configuration | include lsr-id
 mpls lsr-id 2.2.2.2
<PE1> display ip interface brief
*down: administratively down
(s): spoofing
Interface                   Physical Protocol IP Address      Description
Loop0                       up       up(s)    100.100.100.100 LoopBack0..
Loop2                       up       up(s)    100.100.100.102 LoopBack2..
M-E0/0/0                    up       up       192.168.147.7   M-Etherne..
<PE1> system-view
[PE1] mpls lsr-id 100.100.100.100
```

2. 路由排查

(1) 检查路由表中 PE1、P、PE2 的环回口 IP 及远端 VLAN 接口的 IP 表项是否存在，如不存在，请检查路由协议配置。

```
[PE1] display ip routing-table
         Destinations : 10       Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

1.1.1.1/32          Direct  0    0            127.0.0.1       InLoop0
3.3.3.3/32          O_INTER 10   2            103.0.0.4       GE3/0/1
4.4.4.4/32          O_INTER 10   1            103.0.0.4       GE3/0/1
50.0.0.0/24         O_INTER 10   2            103.0.0.4       GE3/0/1
70.0.0.0/24         O_INTER 10   2            103.0.0.4       GE3/0/1
90.0.0.0/24         O_INTER 10   2            103.0.0.4       GE3/0/1
103.0.0.0/24        Direct  0    0            103.0.0.1       GE3/0/1
103.0.0.1/32        Direct  0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct  0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0            127.0.0.1       InLoop0
```

(2) 检查路由协议状态是否正常（下面以查看 OSPF 协议状态为例），如不正常，请检查路由协议配置。

```
[PE1] display ospf peer

                 OSPF Process 1 with Router ID 1.1.1.1
                      Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time Interface       State
 4.4.4.4         103.0.0.4       1   37        Vlan103         Full/BDR
```

(3) 检查协议中环回口、VLAN 接口的路由是否被通告，如不正确，请添加配置。

```
[PE1-ospf-1] display this
#
ospf 1
 area 0.0.0.0
  network 103.0.0.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
#
return
```

(4) 如仍不正常，请检查本端、对端设备的路由协议配置。

(5) 如仍无法确认，请将故障信息发送技术支持人员分析。

12.7 VXLAN转发故障

12.7.1 故障描述

VXLAN 转发不通。

12.7.2 故障处理步骤

1. VXLAN 隧道检查

检查配置的用于转发的 IPv4/IPv6 VXLAN 隧道是否 UP，如果不 UP 则查看两台设备间是否路由可达。

使用接口 IPv4/IPv6 地址时，需要保证物理链路 UP 且两端 IPv4/IPv6 地址配置正常。使用环回口 IPv4/IPv6 地址时，需要保证两台设备间环回口路由可达。

```
<Sysname> display interface Tunnel 1
Tunnel1
Current state: UP
Line protocol state: UP
Description: Tunnel1 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1500
Internet protocol processing: Disabled
Last clearing of counters: Never
Tunnel source 10.10.1.2, destination 10.10.1.1
Tunnel protocol/transport UDP_VXLAN/IP
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops

<Sysname> display l2vpn vsi name 1 verbose
VSI Name: 1
  VSI Index               : 2
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : Unlimited
  Broadcast Restrain      : 5120 kbps
  Multicast Restrain      : 5120 kbps
  Unknown Unicast Restrain: 5120 kbps
  MAC Learning            : Enabled
  MAC Table Limit         : Unlimited
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
  VXLAN ID                : 1
  Tunnels:
    Tunnel Name          Link ID    State    Type        Flood proxy
    Tunnel1              0x5000001  UP       Manual      Disabled
  ACs:
    AC                              Link ID    State
    GE3/1/3                         0          Up
```

2. UDP 端口号检查

检查两台设备上配置的 UDP 端口号是否相同。可以用 **display current-configuration** 命令查看当前配置文件中是否配置了 **vxlan udp-port** 命令；未配置的情况下，VXLAN 报文的目的 UDP 端口号为缺省值 4789。

3. VXLAN ID 检查

检查两台设备上 VSI 配置的 VXLAN ID 是否相同，如果不相同请修改为相同的 VXLAN ID。

```
<Sysname> system-view
[Sysname] vsi 1
[Sysname-vsi-1] display this
#
vsi 1
 vxlan 1
  tunnel 1
#
return
```

4. 检查是否配置了泛洪抑制

检查当前 VSI 下是否配置了泛洪抑制命令 **flooding disable all**，如果配置了该命令，则只有单播流量可以转发到远端，其它流量均不会泛洪到远端。

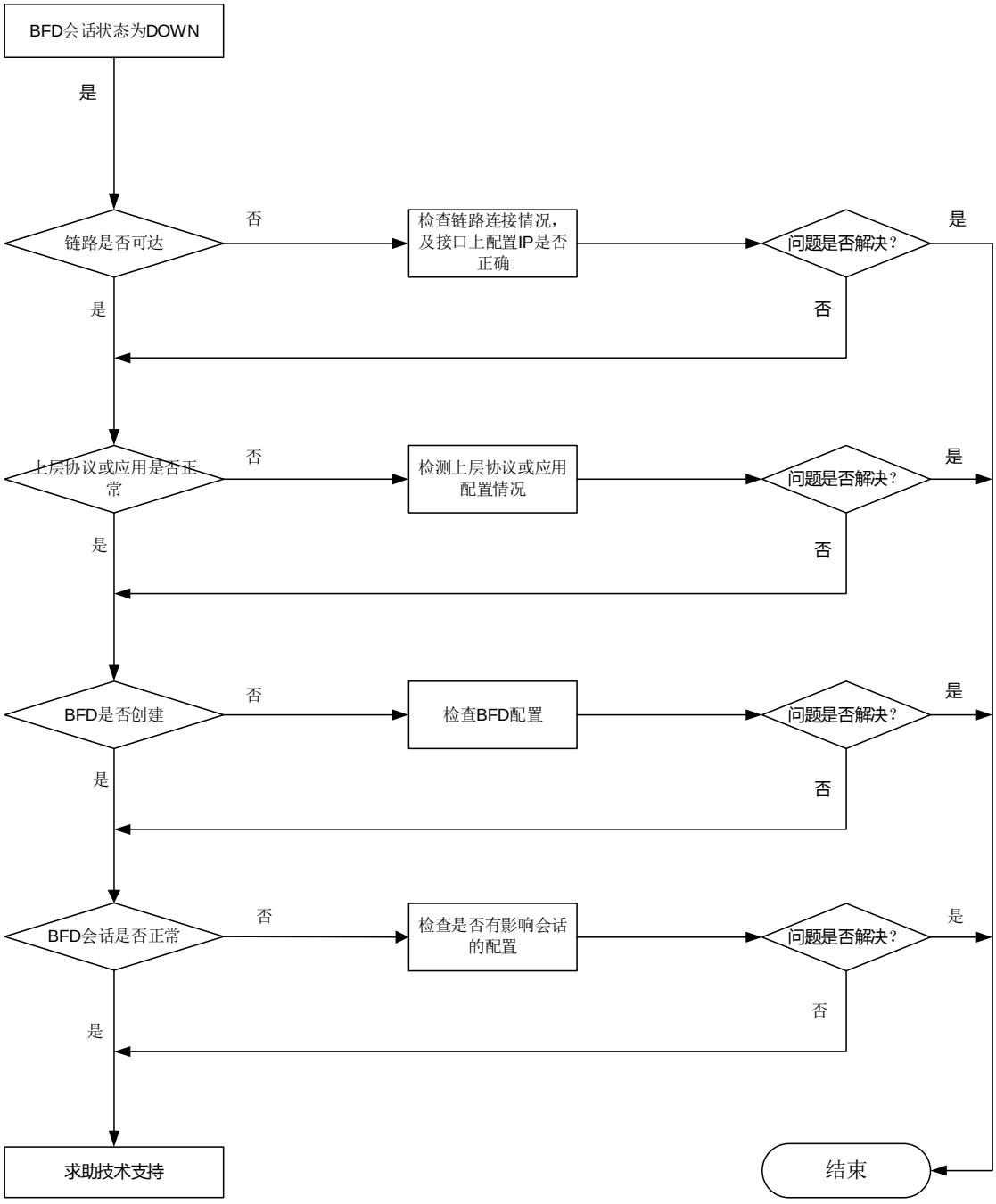
```
[Sysname-vsi-1] display this
#
vsi 1
 flooding disable all
 vxlan 1
  tunnel 1
#
return
```

12.8 BFD转发故障

12.8.1 故障描述

- BFD 会话没有创建。
- BFD 会话一直显示状态为 DOWN。
- BFD 会话震荡。

12.8.2 故障诊断流程



12.8.3 故障处理步骤

BFD 配置配在两台设备或两个节点上，首先要保证两个节点在物理链路上可达，检查两节点之间的连接是否正确，检查 BFD 配置是否正确。

1. BFD 会话没有创建或者状态显示一直为 down

会话没有创建，现象表现为：display bfd session 没有会话显示。

(1) 首先检查各个节点之间的可达性，如不可达，请检查物理连接或接口上的配置。

(2) BFD 关联的协议是否 UP,若没有检查相关协议配置。

(3) 查看 BFD 服务的上层协议是否 UP，如果没有 UP，请检查相关协议的配置。

如果配置和路由协议联动的 BFD，请检查路由协议的状态，如下（此处以 OSPF 为例）：

```
<Sysname> display ospf peer

          OSPF Process 1 with Router ID 43.43.43.43
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 15.15.15.22     50.1.1.2        1   36         Full/BDR          GE3/1/4
```

如果是和隧道进行联动，请查看隧道的状态，如下（此处以 TE 隧道为例）：

```
<Sysname> display interface Tunnel brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP         Description
Tun22                UP   UP       --
```

(4) 协议使能 BFD 配置是否正确：不同协议使能 BFD 配置不同。例如：OSPF 联动 BFD,则在接口视图配置 ospf bfd enable。Mpls TE 联动 BFD,TE 接口视图使能 mpls bfd。

对于 BFD 会话，和不同的上层协议联动，BFD 使能的配置不一样，配置的视图也不一样，如 TE BFD 会话的使能配置是在系统视图下和 tunnel 接口视图下，如下：

```
[Sysname] mpls bfd enable
[Sysname] interface tunnel 22 mode mpls-te
[Sysname-Tunnel22] mpls bfd
```

2. BFD 反复在状态变化

现象表现为 BFD 反复打印 log：UP->DOWN, INIT->DOWN。同时会打印出 BFD 震荡的 DIAG:

会话能协商 UP 说明链路可达，UP 不能维持说明链路、设备可能存在丢包或者延时的情况。

常见 BFD 震荡的 diag：

```
1 -- Control Detection Time Expired  /* 会话超时 down */
2 -- Echo Function Failed            /* echo BFD 超时 down */
3 -- Neighbor Signaled Session Down  /* BFD 邻居超时 down */
7 -- Administratively Down           /* 协议主动 down */
```

(1) 首先检查各个节点之间的可达性以及传输延时情况，通过 ping 可以初步判断链路基本状态。

(2) 根据具体现象具体分析

1. Echo 会话: 单独检测，会话震荡只可能是 UP->DOWN, 震荡的 Diag 为 2：表示 echo 会话超时。
2. Crtl 会话：ctrl 会话震荡情况比较多，常见的有：

   1）本端 BFD 打印 UP->DOWN:Diag 1, 对端 BFD 打印 UP->DOWN:Diag 3.

   说明：本端收不到包超时，关注对端过来的 BFD 报文情况。

   2）一端 BFD 打印 UP->DOWN:Diag 1, 对端 BFD 打印 UP->DOWN:Diag 1.

   说明：两边都是收不到包超时，其实这种情况往往肯定其中一端先 DOWN，但是通知邻居 down 的报文没有及时发出，所以对端也表现为超时 DOWN。这种情况最好是配

置时间同步（NTP 等），先判断出哪端先超时。在有条件的情况下结合抓包来锁定报文丢失的位置。

3）一端 BFD 反复打印 UP->DOWN， 对端 INIT->DOWN 状态变化

此种情况基本可以断定是本端发送问题，可以排除本端发送路径丢包情况。

4）一端 BFD 打印 UP->DOWN:Diag 3，对端未有 BFD UP->DOWN 打印。

这种情况，基本可以确认是对端协议邻居主动删除 BFD.

5）一端 BFD 打印 UP->DOWN:Diag 1，对端未有 BFD UP->DOWN 打印。

有两种可能：

A. 本端因为收不到包超时 down，通知邻居 down，协议邻居 down 的信息先与 BFDdown 信息发送给对端。对端就表现出协议先 down，在删除 BFD.

B. 本端超时 down 是因为对端邻居先 down 导致 BFD 删除而发不出包.。此时需要关注对端邻居 down 的原因：是因为 BFDdown、协议邻居 down 等情况导致。

(3) 其它的配置对 BFD 会话的影响。

URPF 配置：当 echo 报文源 IP 地址不是本设备上的 IP 地址时，不能配置 uRPF 功能。

Easy IP：配置 BFD 功能的接口不能开启 Easy IP 功能，否则可能导致 BFD 功能不能正常使用。

QinQ 终结：配置 BFD 功能的三层以太网子接口、三层聚合子接口不能配置 QinQ 终结功能。

QoS 配置：BFD 会话建立后，需要在 CSPC 类单板、CSPEX-1812X 单板、CSPEX-1104-E 单板、CEPC 类单板、CSPEX-1602X 单板、CSPEX1204 单板、CSPEX-1404X 单板或 CSPEX-1504X 单板上查询转发表项，此时在该单板上的接口配置 QoS 策略如使用 **qos lr** 命令配置限速，会导致对端收到 BFD 报文有延时而出现 BFD 出现震荡的现象。

VLAN 配置：对于 VLAN 接口上的 BFD 会话，某些 STP 配置（如配置 STP 的接口不允许配置 BFD 会话的接口所在 VLAN 的报文通过）也会导致 BFD 报文在设备内部进行转发时出现丢弃。

如果链路一端配置了 ECHO BFD 会话，建议在对端接口上使用 **qos trust** 命令配置优先级信任模式。否则，当对端接口上出现拥塞时，ECHO BFD 报文在对端可能会因为优先级较低而出现丢包的现象。

与华为设备对接建立多跳 BFD 会话，华为设备上，在 BFD 视图下配置 peer-ip 的 TTL 参数为 255 即可。命令如下：peer-ip ip-address mask-length ttl multi-hop 255 。

12.9 RADIUS故障

12.9.1 故障描述

设备与 RADIUS 服务器交互故障。

12.9.2 故障处理步骤

通过以下命令查看设备和所有 RADIUS 服务器交互的报文统计信息。

```
<Sysname> display radius statistics
Authentication packets:
  Requests                  : 8          Retransmissions        : 0
  Pending requests          : 0          Packet timeouts        : 0
  Request failures          : 0          Challenge packets      : 0
  Packets without responses : 0          Packets with responses : 0
  Accept responses          : 8          Reject responses       : 0
```

```
  Unknown-type responses     : 0          Malformed responses    : 0
  Bad authenticators         : 0          Dropped responses      : 0

Accounting packets:
  Requests                   : 16         Retransmissions        : 0
  Start requests             : 8          Realtime requests      : 0
  Stop requests              : 8          Pending requests       : 0
  Packet timeouts            : 0          Request failures       : 0
  Packets without responses  : 0          Packets with responses : 0
  Unknown-type responses     : 0          Malformed responses    : 0
  Bad authenticators         : 0          Dropped responses      : 0

DAE packets:
  DM:
    Requests                 : 0          Request retransmissions: 0
    ACKs                     : 0          NAKs                   : 0
    Timeouts                 : 0          Malformed requests     : 0
    Bad authenticators       : 0          Dropped requests       : 0
  CoA:
    Requests                 : 0          Request retransmissions: 0
    ACKs                     : 0          NAKs                   : 0
    Timeouts                 : 0          Malformed requests     : 0
    Bad authenticators       : 0          Dropped requests       : 0
  Unknown-type requests      : 0

Session-control packets:
  Terminate:
    Requests                 : 0          Successes              : 0
    Failures                 : 0          Timeouts               : 0
  Set-policy:
    Requests                 : 0          Successes              : 0
    Failures                 : 0          Timeouts               : 0
  Unknown-type requests      : 0          Malformed requests     : 0
  Bad authenticators         : 0          Dropped requests       : 0

Authentication servers: 1
  IP:  1.1.1.1                            Port: 1812
  VPN:
  Authentication packets:
    Requests                  : 8          Retransmissions        : 0
    Pending requests          : 0          Packet timeouts        : 0
    Request failures          : 0          Challenge packets      : 0
    Accept responses          : 8          Reject responses       : 0
    Unknown-type responses    : 0          Malformed responses    : 0
    Bad authenticators        : 0          Dropped responses      : 0

Accounting servers: 1
  IP:  1.1.1.1                            Port: 1813
```

```
VPN:
Accounting packets:
  Requests                  : 16        Retransmissions        : 0
  Start requests            : 8         Realtime requests      : 0
  Stop requests             : 8         Pending requests       : 0
  Packet timeouts           : 0         Request failures       : 0
  Unknown-type responses    : 0         Malformed responses    : 0
  Bad authenticators        : 0         Dropped responses      : 0
```

12.10 NAT故障

12.10.1 故障描述

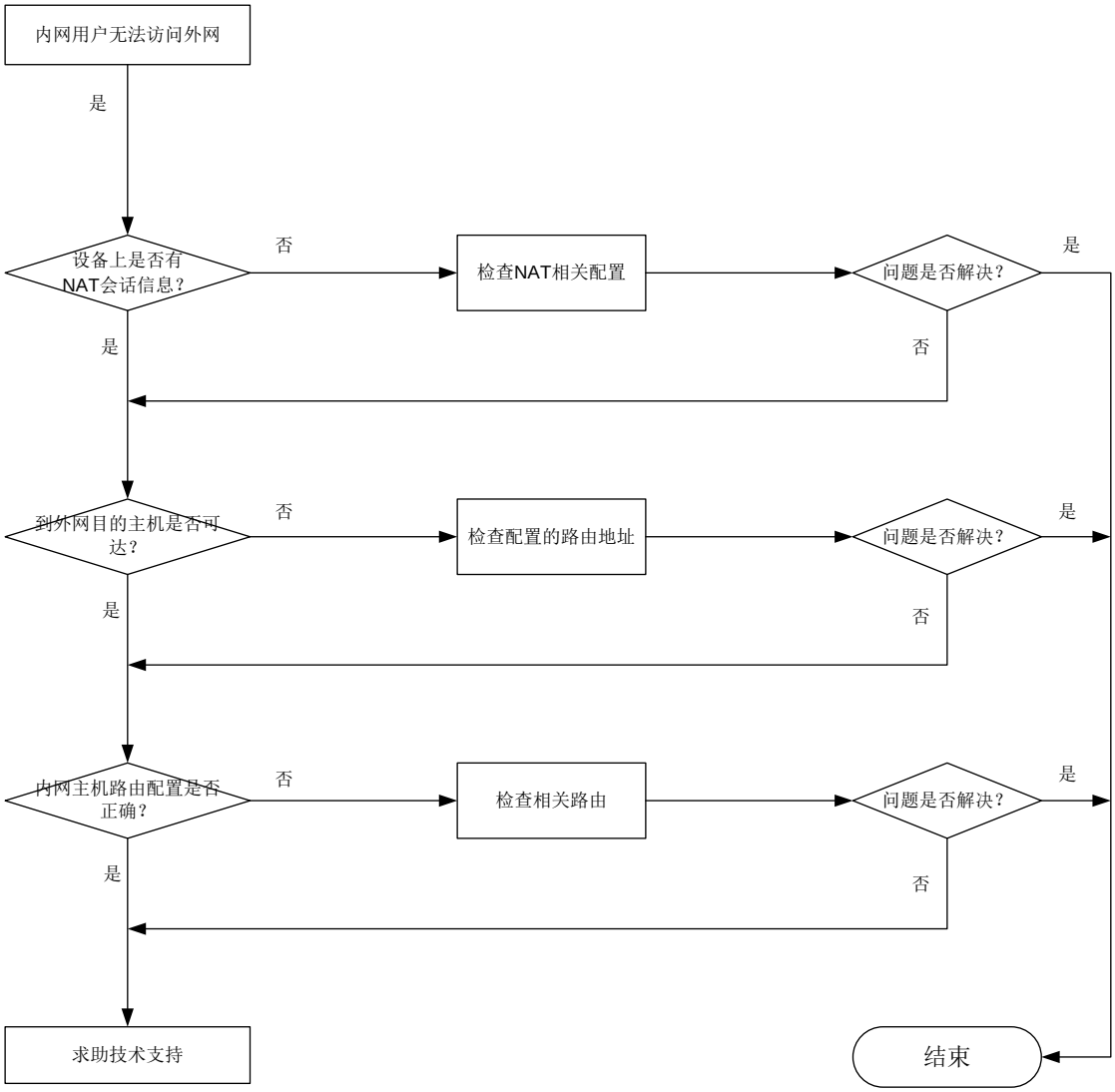
NAT 地址转换失败。

12.10.2 故障处理步骤

NAT 地址转换失败的常见原因如下：

- NAT 规则配置错误。
- NAT 网关与外部网络路由不可达。
- ACL 规则配置错误导致报文匹配失败。
- 内网用户主机到 NAT 网关路由不可达。

请按照下面步骤进行故障排查。(本章只涉及接口板做多核 NAT 业务)



(1) 检查 NAT 业务是否有正确的会话信息

检查 NAT 业务是否建立正确的会话信息。如果没有会话信息，请检查 NAT 相关配置是否正确。

```
<Sysname> display nat session slot 3 verbose
Slot 3:
Initiator:
  Source      IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet3/1/1
Responder:
  Source      IP/port: 192.168.1.55/22
  Destination IP/port: 192.168.1.10/1877
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet3/1/2
```

```
State: TCP_SYN_SENT
Application: SSH
Role: Standby
Failover group ID: 1
Start time: 2017-10-18 11:22:45
Initiator->Responder:         1 packets         48 bytes
Responder->Initiator:         0 packets          0 bytes

Total sessions found: 1
```

(2) 检查 NAT 设备到外网目的主机是否可达。

执行 ping 命令确认 NAT 设备和外网主机是否可达，如果 ping 外网目的主机不通，执行 **display ip routing-table** 命令查看路由表信息，检查设备是否配置了到达外网的正确路由，同时检查 IP 地址是否和外网地址有冲突。

(3) 检查内网主机的路由配置

执行 **display ip routing-table** 命令检查内网主机上配置的路由是否正确，是否能够将内网向外网发送的报文到达 NAT 转换设备。

如果上送排查检查通过，仍然无法恢复，请将故障信息发送技术支持人员分析。

12.11 PTP故障

12.11.1 故障描述

PTP 常见故障现象有：

- PTP 无法选举出 Slave 接口。
- PTP 时间同步精度异常和同步以太网功能异常。

12.11.2 故障处理步骤

1. 检查 PTP 配置正确性

(1) 使用 **display ptp clock** 命令查看设备的 PTP 时钟信息。

```
<Sysname> display ptp clock
PTP profile         : ITU-T G.8275.1
PTP mode            : T-BC
Slave only          : No
Holdover state      : No
Clock ID            : 1CAB34-FFFE-3B1000
Clock type          : Local
Clock domain        : 24
Number of PTP ports : 2
Priority1      : 128
Priority2      : 128
Local priority : 128
Clock quality :
 Class                 : 248
 Accuracy              : 254
 Offset (log variance) : 65535
```

```
Offset from master  : 21 (ns)
Mean path delay     : 572 (ns)
Steps removed       : 1
Local clock time    : Wed Sept 11 01:59:40 2019
Clock source info:
 Clock   LP   Pri2 Accuracy Class TimeSrc Direction In-Status Offset(log variance)
 ------------------------------------------------------------------
 Local   128  128  254      248   160     N/A       N/A       65535
 ToD0    128  128  32       6     32      N/A       Inactive  65535
 ToD1    128  128  32       6     32      N/A       Inactive  65535
```

- 检查各设备上配置的 PTP profile 和 Clock domain 一致，PTP mode 是否正常。
- 检查配置的两个优先级 Priority1 和 Priority2 是否正常，该值越小优先级越高。

(2) 使用 **display ptp statistics** 命令查看 PTP 端口收发包信息。

```
<Sysname> display ptp statistics interface ten-gigabitethernet 3/1/1
                    Received packets
------------------------------------------------------------------------
Announce :81         Sync      :160        Signaling          :0
DelayReq :0          DelayResp :160        FollowUp           :160
PdelayReq:0          PdelayResp:0          PdelayRespFollowUp :0

                    Sent packets
------------------------------------------------------------------------
Announce :0          Sync      :0          Signaling          :0
DelayReq :160        DelayResp :0          FollowUp           :0
PdelayReq:0          PdelayResp:0          PdelayRespFollowUp :0

                    Discarded packets
------------------------------------------------------------------------
Announce :0          Sync      :0          Signaling          :0
DelayReq :0          DelayResp :0          FollowUp           :0
PdelayReq:0          PdelayResp:0          PdelayRespFollowUp :0
```

- 查看端口 Received 和 Sent 报文是否正常，是否有 Discarded 的异常丢弃的报文计数。
- 检查 Sync 和 DelayReq 的计数是否匹配。

(3) 使用 **display ptp interface brief** 命令查看 PTP 接口角色。

```
<Sysname> display ptp interface brief
Name             State         Delay mechanism  Clock step  Asymmetry correction
XGE3/1/1         Slave         E2E              Two         0
```

- 检查接口的 State 状态是 Slave 还是 Master。
- 检查接口配置，二层以太和三层 UDP 模式、端口强制状态是否匹配。

(4) 使用 **display ptp corrections** 命令查看 PTP 时间调节精度。

```
<Sysname> display ptp corrections
Slave port              Correction time        Corrections(s,ns)     Rate ratio
XGE3/1/1                Sep 11 02:07:50 2019  -0,4                   N/A
XGE3/1/1                Sep 11 02:07:50 2019   0,6                   N/A
XGE3/1/1                Sep 11 02:07:51 2019  -0,1                   N/A
```

Corrections 项表示当前设备与 Master 的时间偏差。

2. 检查同步以太配置正确性

(1) 使用 **display network-clock source** 命令查看时钟监控的参考源状态。

```
<Sysname> display network-clock source
Traced reference: XGE3/1/1
Reference   State   Priority  SSM level Force SSM Sa-Bit  LPU port  Frequency
BITS0       Lost    255       Unknown   ON        4       N/A       2 Mbps
BITS1       Lost    255       Unknown   ON        4       N/A       2 Mbps
PTP         N/A     255       Unknown   ON        N/A     N/A       N/A
XGE6/1/1    Lost    18        Unknown   ON        N/A     Yes       N/A
XGE3/1/1    Normal  18        Unknown   ON        N/A     Yes       N/A
```

- 检查同步以太使能端口和优先级配置是否正确。LPU port 项为 Yes 是表示端口下使能了同步以太，Priority 项表示该端口的优先级，值越小优先级越高。
- 如果开启了 SSM 等级控制选源，需要检查 SSM 等级相关信息。检查端口是否使能了 ESMC，全局配置下是否关闭了 SSM 等级强制 Force 状态为 OFF。

(2) 使用 **display network-clock status** 命令查看同步以太当前状态。

```
<Sysname> display network-clock status
Mode              : Auto
Reference         : N/A
Traced reference  : XGE3/1/1
Lock mode         : Locked
SSM output level  : SSUB
SSM control enable: Off
```

SSM control enable 表示当前选源是否由 SSM 等级控制选源。Lock mode 表示当前是否有端口同步了上游时钟，即 LOCKED 状态。

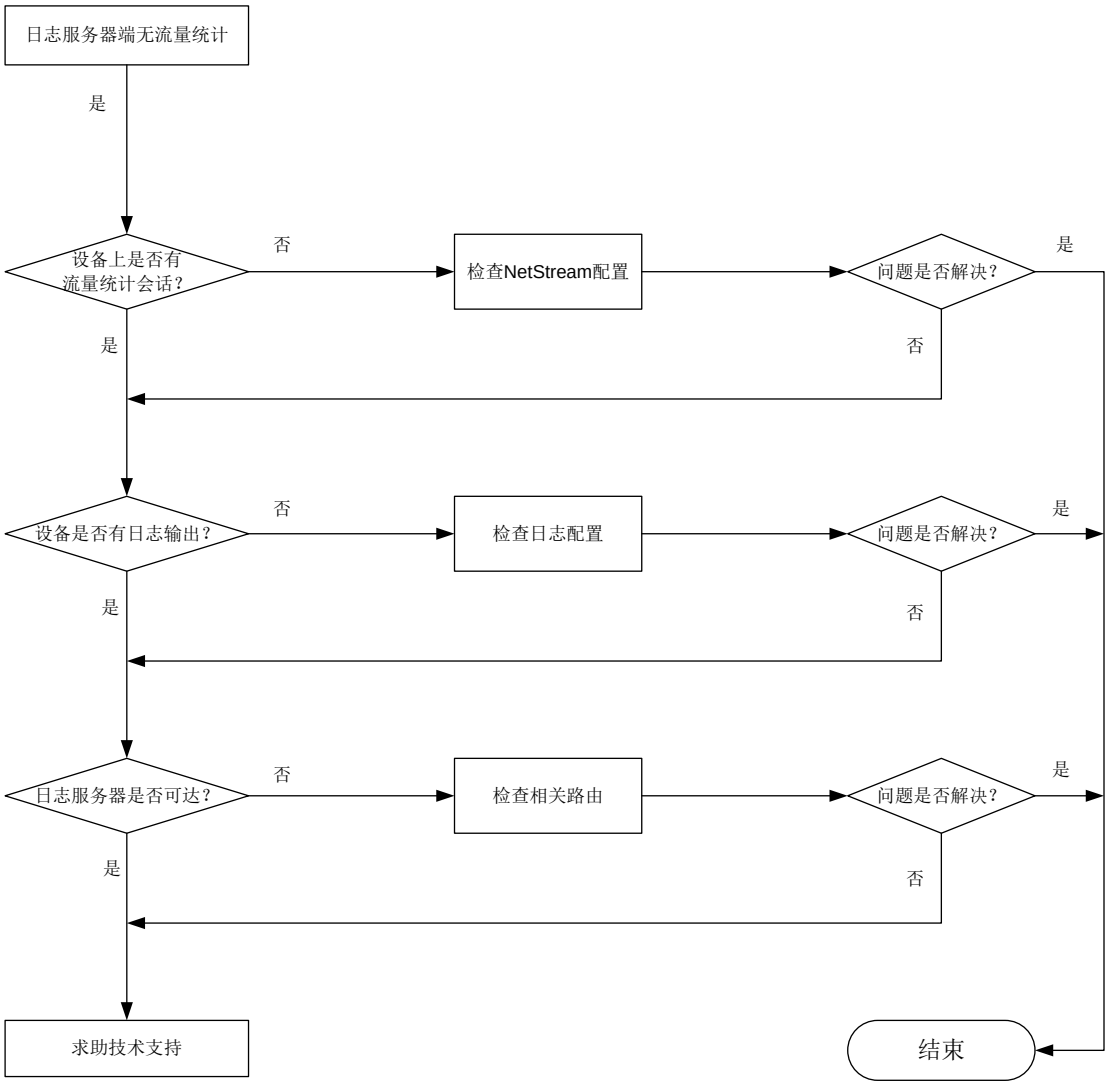
12.12 NetStream故障处理

介绍 NetStream 故障处理的流程和详细的故障处理步骤。

12.12.1 常见原因

- NetStream 配置错误，导致 NetStream 无法统计。
- NetStream 日志输出端不可达，导致无法解析统计输出的报文。
- ACL 配置错误导致部分流量无法匹配上做 NetStream 统计。

12.12.2 故障诊断流程



12.12.3 故障处理步骤

1. 检查设备上是否有流量统计信息

执行命令**display ip netstream cache verbose slot** *slot-id* 或**display ipv6 netstream cache verbose slot** *slot-id* 检查 NetStream 业务是否建立正确的会话信息。如果没有会话信息需要检查 NetStream 相关配置，详细参加 NetStream 配置手册。

```
<Sysname> display ip netstream cache verbose slot 3
IP NetStream cache information:
  Active flow timeout                : 1 min
  Inactive flow timeout              : 30 sec
  Max number of entries              : 409600
  IP active flow entries             : 1
  MPLS active flow entries           : 0
  L2 active flow entries             : 0
```

```
  IPL2 active flow entries          : 0
  IP flow entries counted           : 0
  MPLS flow entries counted         : 0
  L2 flow entries counted           : 0
  IPL2 flow entries counted         : 0
  Last statistics resetting time    : Never

IP packet size distribution (525266 packets in total):
 1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
 .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

  512  544  576 1024 1536 2048 2560 3072 3584 4096 4608 >4608
 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

 Protocol          Total   Packets     Flows   Packets  Active(sec)  Idle(sec)
                   Flows   /sec        /sec    /flow    /flow        /flow
------------------------------------------------------------------------------

Type DstIP(Port)         SrcIP(Port)         Pro ToS VNI   If(Direct)  Pkts
     DstMAC(VLAN)        SrcMAC(VLAN)
     TopLblType(IP/MASK) Lbl-Exp-S-List
------------------------------------------------------------------------------
IP   200.0.0.2(1024)     3.3.3.255(1024)     17  0   N/A   GE3/2/4(O)  526126
     TCPFlag:       0
     DstMask:      32       SrcMask:      26       NextHop:         200.0.0.2
     DstAS:         0       SrcAS:         0       BGPNextHop:        0.0.0.0
     OutVRF:      N/A
     Bgp-community1:0
     Bgp-community2:0
     Bgp-community3:0
     Bgp-community4:0
     SamplerMode: Fixed       SamplerInt:    1
     Active:       10       Bytes/Pkt:   128
     First packet arrived: 06/26/2019, 10:47:11
     Last packet arrived:  06/26/2019, 10:47:21
```

2. 检查设备是否有 NetStream 日志输出。

执行命令 **display ip netstream export** 或 **display ipv6 netstream export** 检查 NetStream 业务是否有日志输出信息。如果没有会话信息需要检查 NetStream 相关配置，详细参加 NetStream 配置手册。

```
<Sysname> display ip netstream export
IP export information:
  Flow source interface                          : Not specified
  Flow destination VPN instance                  : Not specified
  Flow destination IP address (UDP)              : 100.0.0.2 (9020)
  Version  5 exported flow number                : 0
  Version  5 exported UDP datagram number (failed): 0 (0)
  Version  9 exported flow number                : 1
```

```
  Version  9 exported UDP datagram number (failed): 1 (0)
  Version 10 exported flow number                 : 0
  Version 10 exported UDP datagram number (failed): 0 (0)

MPLS export information:
  Flow source interface                           : Not specified
  Flow destination VPN instance                   : Not specified
  Flow destination IP address (UDP)               : 100.0.0.2 (9020)
  Version  9 exported flow number                 : 0
  Version  9 exported UDP datagram number (failed): 0 (0)
  Version 10 exported flow number                 : 0
  Version 10 exported UDP datagram number (failed): 0 (0)

IPL2 export information:
  Flow source interface                           : Not specified
  Flow destination VPN instance                   : Not specified
  Flow destination IP address (UDP)               : 100.0.0.2 (9020)
  Version  9 exported flow number                 : 0
  Version  9 exported UDP datagram number (failed): 0 (0)
  Version 10 exported flow number                 : 0
  Version 10 exported UDP datagram number (failed): 0 (0)
```

3. 检查日志服务器端是否可达。

执行命令 **ping** 确认设备和服务器端是否可达，如果 **ping** 不通目的主机，需要执行命令 **display ip routing-table** 查看当前的路由表信息，检查设备是否配置了到达的正确路由，同时检查 IP 地址是否和外网地址有冲突。

12.13 L2MC转发故障

12.13.1 故障描述

L2MC 常见故障现象有：

- 组播转发表项未建立。
- 组播转发表项未添加下游出接口。

12.13.2 故障处理步骤

(1) 查看二层组播转发表项是否下发。

```
<Sysname> display igmp-snooping group
Total 1 entries.

VLAN 10: Total 1 entries.
  (0.0.0.0, 226.1.1.1)
    Host ports (1 in total):
      GE3/0/1                                 (00:04:00)
```

(2) 查看 VLAN 上是否正确配置二层组播。

```
[Sysname-vlan10] display this
```

```
#
vlan 10
 igmp-snooping enable
 igmp-snooping drop-unknown
#
```

(3) 查看二层组播表项是否添加下游出接口。

```
<Sysname> display igmp-snooping group
Total 1 entries.

VLAN 10: Total 1 entries.
  (0.0.0.0, 226.1.1.1)
    Host ports (1 in total):
      GE3/0/1                                  (00:04:00)
```

(4) 查看出接口上是否接收到 IGMP REPORT 报文。

```
<Sysname> terminal monitor
<Sysname> terminal debugging
<Sysname> debugging igmp report
<Sysname>*Feb 19 14:01:59:422 2013 Sysname MCS/7/PACKET: -MDC=1-Slot=3; Receive IGMPv2
report packet from port GE3/0/1 on VLAN 10.
*Feb 19 14:01:59:436 2013 Sysname MCS/7/PACKET: -MDC=1; Receive IGMPv2 report packet from
another slot, the packet receive from port
 GE3/0/1 on VLAN 10.
*Feb 19 14:01:59:437 2013 Sysname MCS/7/PACKET: -MDC=1; Forward the IGMP packet locally.
*Feb 19 14:01:59:437 2013 Sysname MCS/7/PACKET: -MDC=1; Forward the IGMP membership packet
which destination IP address is 226.1.1.1
 and source IP address is 192.85.1.3 on VLAN 10.
*Feb 19 14:01:59:449 2013 Sysname MCS/7/PACKET: -MDC=1; Send the IGMP packet up to IP.
*Feb 19 14:01:59:453 2013 Sysname MCS/7/PACKET: -MDC=1-Slot=5; Forward the IGMP membership
packet which destination IP address is 22
6.1.1.1 and source IP address is 192.85.1.3 on VLAN 10.
*Feb 19 14:01:59:457 2013 Sysname MCS/7/PACKET: -MDC=1-Slot=3; Forward the IGMP membership
packet which destination IP address is 22
6.1.1.1 and source IP address is 192.85.1.3 on VLAN 10.
```

12.14 L3MC转发故障

12.14.1 故障描述

L3MC 常见故障现象有：

- 组播转发表项未建立。
- 组播转发表项未添加下游出接口。

12.14.2 故障处理步骤

1. 组播转发表项未建立处理步骤

(1) 查看三层组播转发表项是否下发。

```
<Sysname> display multicast forwarding-table
```

```
Total 1 entries, 1 matched

00001. (11.1.1.2, 226.1.1.1)
     Flags: 0x0
     Uptime: 00:35:00, Timeout in: 00:03:21
     Incoming interface: GigabitEthernet3/0/2
     Matched 193 packets(5970 bytes), Wrong If 0 packets
     Forwarded 140 packets(140 bytes)
```

(2) 检查接口是否配置 PIM 协议。

```
[Sysname-GigabitEthernet3/0/2] display this
#
interface GigabitEthernet3/0/2
 port link-mode route
 ip address 11.1.1.1 255.255.255.0
 pim sm
#
```

(3) 检查设备是否学习到 BSR。

```
<Sysname> display pim bsr-info
 Scope: non-scoped
     State: Elected
     Bootstrap timer: 00:00:18
     Elected BSR address: 11.1.1.1
       Priority: 64
       Hash mask length: 30
       Uptime: 00:23:52
     Candidate BSR address: 11.1.1.1
       Priority: 64
       Hash mask length: 30
```

(4) 检查设备是否学习到 RP。

```
<Sysname> display pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4
       RP address               Priority  HoldTime  Uptime    Expires
       11.1.1.1 (local)         192       180       00:24:22  00:02:38
```

(5) 如果组播表项建立但入接口不正确，则利用组播源 IP 检查其 RPF 口是否正确。

```
<Sysname> display multicast rpf-info 11.1.1.2
 RPF information about source 11.1.1.2:
     RPF interface: GigabitEthernet3/0/2
     Referenced route/mask: 11.1.1.0/24
     Referenced route type: unicast (direct)
     Route selection rule: preference-preferred
     Load splitting rule: disable
     Source AS: 0
     C-multicast route target: 0x0000000000000000
```

2. 组播转发表项未添加下游出接口处理步骤

(1) 查看三层组播转发表项是否生成下游出接口。

```
<Sysname> display multicast forwarding-table
Total 1 entries, 1 matched

00001. (11.1.1.2, 226.1.1.1)
     Flags: 0x0
     Uptime: 00:36:10, Timeout in: 00:03:26
     Incoming interface: GigabitEthernet3/0/2
     List of 1 outgoing interfaces:
       1: GigabitEthernet3/0/1
     Matched 198 packets(5975 bytes), Wrong If 0 packets
     Forwarded 145 packets(145 bytes)
```

(2) 检查下游出接口是否配置 IGMP 或者 PIM SM。

- 下游直连主机

```
interface GigabitEthernet3/0/1
 port link-mode route
 ip address 12.1.1.1 255.255.255.0
 igmp enable
```

- 下游链接其它路由设备

```
interface GigabitEthernet3/0/1
 port link-mode route
 ip address 12.1.1.1 255.255.255.0
 pim sm
```

(3) 查看下游出接口上是否收到 IGMP 加入协议报文或者 PIM JOIN 协议报文。

- 下游直连主机

```
<Sysname> terminal monitor
<Sysname> terminal debugging
<Sysname> debugging igmp report
<Sysname>*Feb 19 13:26:11:796 2013 Sysname IGMP/7/REPORT: -MDC=1; Received IGMPv2 report for group 226.1.1.1 on interface GigabitEthernet3/0/1(12.1.1.1) (G161021)
*Feb 19 13:26:11:797 2013 Sysname IGMP/7/REPORT: -MDC=1; Process IS_EX packet for INCLUDE group(226.1.1.1) on interface GigabitEthernet3/0/1(12.1.1.1) (G116517)
```

- 下游链接其它路由设备

```
<Sysname> terminal monitor
<Sysname> terminal debugging
<Sysname> debugging pim join-prune
<Sysname>*Feb 19 13:35:55:780 2013 Sysname PIM/7/JP: -MDC=1; PIM ver 2 JP received 12.1.1.2 -> 224.0.0.13 on interface GigabitEthernet3/0/1 (SM141304)
*Feb 19 13:35:55:781 2013 Sysname PIM/7/JP: -MDC=1;  Upstream: 12.1.1.1, Number of groups: 2, Holdtime: 210 (SM141306)
*Feb 19 13:35:55:781 2013 Sysname PIM/7/JP: -MDC=1;  Group: 226.1.1.1 --- 1 joins 0 prunes (SM141312)
*Feb 19 13:35:55:782 2013 Sysname PIM/7/JP: -MDC=1;  Join: 11.1.1.1 --- Flags: SWR (SM141316)
*Feb 19 13:35:55:783 2013 Sysname PIM/7/JP: -MDC=1;  Group: 239.1.1.1 --- 1 joins 0 prunes (SM141312)
*Feb 19 13:35:55:784 2013 Sysname PIM/7/JP: -MDC=1;  Join: 11.1.1.1 --- Flags: SWR (SM141316)
```

3. PIM 邻居 Down

(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。
- 如果接口已经使能 PIM，请执行步骤 2。

(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。

- 如果显示信息为“Current state: DOWN”，说明接口物理状态为 Down。请校正组网及接口接线。
- 如果显示信息为“Line protocol state: DOWN”，说明接口的协议状态为 Down，则执行如下检查：
  - 检查该接口是否处于 Shutdown 状态。

    执行 **display current-configuration interface** *interface-type interface-number* 命令，查看接口上的当前配置。若显示信息中出现“shutdown”，请在接口视图下使用 **undo shutdown** 命令，取消此配置。
  - 检查该接口是否配置 IP 地址。

    执行 **display current-configuration interface** *interface-type interface-number* 命令查看接口地址。如果发现接口未配置 IP 地址或地址与主机不在同一网段，请使用 **ip address** *ip-address* { *mask* | *mask-length* }命令为接口配置 IP 地址。
- 如果接口 PIM 状态为 Up，请执行步骤 3。

(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 邻居过滤策略，而 PIM 邻居的地址被过滤策略过滤掉了。

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

4. PIM-SM 网络中 RPT 无法正常转发数据

(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 秒查看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 11。

- 如果 PIM 路由表中不存在正确的（*,G）表项，请执行步骤 2。

(2) 检查下游接口是否收到 Join 消息。

在设备上执行 **display pim statistics** 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 JP 报文计数没有增加，在下游设备上执行 **display pim statistics**，查看下游是否向上游发出了 JP 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 11。
  - 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。

(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：

- 朝向 RP 的 RPF 邻居接口。
- 朝向 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，建议在该接口上配置 **pim sm**。
- 如果设备的所有接口均已使能 PIM-SM，请执行步骤 4。

(4) 检查 RP 信息是否正确。

在设备上执行 **display pim rp-info** 命令，查看设备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 11。
- 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。

(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或 MBGP 路由，执行 **display current-configuration** 命令查看组播静态路由或 MBGP 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。

(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。

(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。

(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。

(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。

(10) 如果故障仍未排除，请联系技术支持工程师。

5. PIM-SM 网络中 SPT 无法正常转发数据

(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。

  a. 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，而不是朝向组播源的 RPF 接口，则表明 SPT 没有成功建立。

b. 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。

c. 查看显示信息中的“Matched”计数是否保持增长。

- 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 10。
- 如果“Matched”计数停止且当前设备不是源 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，请执行步骤 10。
- 如果“Matched”计数停止且当前设备已是源 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 10。

- 如果 PIM 路由表中不存在正确的（S,G）表项，请执行步骤 2。

(2) 检查下游接口是否收到 Join 消息（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 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。

(3) 检查接口是否使能 PIM-SM。

以下接口没有使能 PIM-SM 是常见的故障原因：

- 朝向组播源的 RPF 邻居接口。
- 朝向组播源的 RPF 接口。

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，请在该接口上配置 **pim sm**。
- 如果设备的所有接口均已使能 PIM-SM，请执行步骤 4。

(4) 检查是否存在到达组播源的 RPF 路由。

在设备上执行 **display multicast rpf-info** *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组播源的 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组播源的 RPF 路由：
  - 如果显示信息表明 RPF 路由为组播静态路由或 MBGP 路由，执行 **display current-configuration** 命令，查看组播静态路由或 MBGP 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组播源的 RPF 路由，且路由配置合理，请执行步骤 5。

(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。

(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。

(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。

(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。

(9) 如果故障仍未排除，请联系技术支持工程师。

6. 组播设备无法正常建立 IGMP 或 MLD 表项

(1) 检查设备是否使能组播。

在直连用户主机网段的设备上执行 **display current-configuration** 命令，查看当前配置信息。

- 如果显示信息中没有“multicast routing”，请首先在系统视图下执行 **multicast routing** 命令使能组播功能，然后补充其他的 IGMP/MLD 相关配置。
- 如果设备已经使能组播，请执行步骤 2。

(2) 检查接口是否为 Up 状态。

在设备上执行 **display interface** *interface-type interface-number* 命令，指定该设备上与用户主机网段直连的接口，查看接口的显示信息。

- 如果显示信息为“Current state: DOWN”，说明接口物理状态为 Down。请校正组网及接口接线。
- 如果显示信息为“Line protocol state: DOWN”，说明接口的协议状态为 Down，则执行如下检查：
  - 检查该接口是否处于 Shutdown 状态。

    执行 **display current-configuration interface** *interface-type interface-number* 命令，查看接口上的当前配置。若显示信息中出现“shutdown”，请在接口视图下使用 **undo shutdown** 命令，取消此配置。
  - 检查该接口是否配置 IP 地址。

    执行 **display current-configuration interface** *interface-type interface-number* 命令查看接口地址。如果发现接口未配置 IP 地址或地址与主机不在同一网段，请使用 **ip address** *ip-address* { *mask* | *mask-length* }命令为接口配置 IP 地址。
- 如果接口为 Up 状态，请执行步骤 3。

(3) 检查接口是否使能 IGMP/MLD。

在设备上执行 **display current-configuration interface** *interface-type interface-number* 命令，查看直连客户端的接口的当前配置。

- 如果显示信息中没有“igmp enable”或“mld enable”，说明未使能 IGMP/MLD。请在接口视图下执行 **igmp enable** 命令或 **mld enable** 命令，使能 IGMP 或 MLD。
- 如果接口已经使能 IGMP 或 MLD，请执行步骤 4。

(4) 检查组播组 G 是否属于 SSM 组地址范围。

在直连用户主机网段的设备上执行 **display current-configuration configuration pim** 命令，查看 PIM 视图下的当前配置信息。如果显示信息中出现“ssm-policy acl-number”，则表明在该设备上指定了 SSM 组地址范围。执行 **display acl** *acl-number* 命令，查看该 ACL 的配置信息。

- 如果显示信息表明 ACL 允许的组范围包括该组播组 G，则说明组播组 G 属于 SSM 组范围。
  - 则确保用户主机和设备接口之间运行 IGMPv3 或 MLDv2 版本。
  - 如果主机上运行的 IGMP 或 MLD 版本无法升级，则需要在设备的接口上使能 SSM Mapping 功能，并设置与组播组 G 相关的 SSM 静态映射规则。
- 如果显示信息表明 ACL 允许的组范围不包括组播组 G，则说明组播组 G 属于 ASM 组范围，需要调整相应的 ACL 指定的组地址范围，使组播组 G 在该 ACL 的允许范围内。
- 如果组播组 G 是否属于 SSM 组地址范围且 IGMP 或 MLD 版本配置正确，请执行步骤 5。

(5) 检查接口上是否配置了限制用户加入的组范围。

执行 **display current-configuration interface** *interface-type interface-number* 命令查看是否查看直连客户端的接口上的当前配置。

- 如果显示信息配置了“igmp group-policy”，IGMP 或 MLD 将按照指定的 ACL 过滤组成员加入信息。检查该 ACL 的所允许的组范围，如果组播组 G 在 ACL 允许范围外，请修改 ACL，或删除该配置，确保 IGMP 或 MLD 为组播组 G 的组成员服务。
- 如果接口没有配置限制用户加入的组范围，请执行步骤 6。

(6) 检查表项及接口数量是否超过产品许可证允许的最大值。

- 如果表项及接口数量超过产品许可证允许的最大值，请重新规划网络部署。
- 如果检查结束，故障仍然无法排除，请执行步骤 7。

(7) 如果故障仍未排除，请收集如下信息，并联系技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

7. 用户侧组播流量不通

(1) 检查上下行的接口状态是否 Up。

在接口下执行命令 **display this interface**，检查组播业务所使用的接口是否 Down。

- 如果管理 Down，则对接口执行 **undo shutdown** 操作。
- 如果管理 Up 但接口状态为 Down，则进行物理链路的检查。
- 如果管理和接口状态都为 Up，请执行下一步骤。

(2) 检查是否存在配置不当。

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 IGMP 和 PIM。

- 如果接口上没有使能 IGMP 和 PIM，请在接口视图下执行 **igmp enable** 命令和 **pim sm** 命令分别使能 IGMP 和 PIM。
- 如果接口上已经使能 IGMP 和 PIM，请执行下一步骤。

(3) 检查用户是否上线。

在设备上执行 **display access-user** 命令，检查用户是否上线。

- 如果没有用户上线，请进行用户上线操作。
- 如果用户已经上线，请执行下一步骤。

(4) 检查 IGMP 协议表项是否生成。

在设备上执行 **display igmp group** 命令，检查 IGMP 协议表项是否生成。

- 如果没有表项显示，请参见 12.14.2 6. 组播设备无法正常建立 IGMP 或 MLD 表项的定位思路。
- 如果有表项显示，请执行下一步骤。

(5) 检查 PIM 协议表项是否生成。

在设备上执行 **display pim routing-table** 命令，检查 PIM 协议表项是否生成。

- 如果没有表项显示，请参见 12.14.2 4. PIM-SM 网络中 RPT 无法正常转发数据的定位思路或 12.14.2 5. PIM-SM 网络中 SPT 无法正常转发数据的定位思路。

- 如果有表项显示，请执行下一步骤。

(6) 检查转发表项是否生成。

在设备上执行 **display multicast forwarding-table** 命令，检查转发协议表项是否生成。

- 如果没有表项显示，请执行下一步骤。
- 如果有表项显示，请执行下一步骤。

(7) 请收集如下信息，并联系技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

12.15 QACL业务故障

本节中描述的“QACL 业务”是指通过预先配置的规则、对匹配规则的报文进行过滤的各种业务的统称，包括：报文过滤、策略路由、QoS 策略、DHCP Snooping。

12.15.1 故障描述

用户配置的 QACL 业务功能没有达到预期的配置效果。

12.15.2 故障处理步骤

当 QACL 业务出现故障时，请按如下步骤处理。

1. 检查报文是否被高优先级的 QACL 业务误匹配

路由器支持将多种 QACL 业务，不同 QACL 业务的优先级不同，优先级顺序依次为：uRPF > 全局应用的报文过滤 > 接口应用的报文过滤 > VLAN 应用的报文过滤 > 全局上送 cpu 的规则 > 端口上送 cpu 的规则 > vlan 上送 cpu 的规则 > dhcp snooping > 接口应用的策略路由 > VLAN 应用的策略路由 > 全局应用的 QoS 策略 > 接口应用的 QoS 策略 > VLAN 应用的 QoS 策略。

如果某类报文同时匹配了多个不同优先级的 QACL 业务规则，只有优先级最高的 QACL 业务规则匹配成功。因此，如果 QACL 业务下发后，实际功能没有生效，需要排查其他更高优先级的 QACL 业务规则中是否已匹配了该类报文。对于此类问题，请结合实际需求，修改相关 QACL 业务的规则，达到预期的匹配效果。

2. 检查 QoS 策略的配置是否已正确应用

在 QoS 策略的配置中，有很多配置不支持或配置之间存在冲突。如果在配置过程中，路由器上未开启 **terminal debugging** 和 **terminal monitor** 功能，即使有冲突的配置下发了，路由器也不会有提示。此时，您可以通过以下两种方法进行排查：

- 在设备上开启 **terminal debugging** 和 **terminal monitor** 功能，并重新应用 QoS 策略（重新应用之前请先执行 **undo** 命令取消之前的 QoS 策略应用），查看路由器是否打印配置冲突或配置不支持的提示信息。
- 通过 **display** 命令查看 QoS 策略应用是否成功。

常见的 QoS 策略的配置未正确下发的提示信息分为以下几类：

(1) and 类型的类中，定义的规则存在冲突。

```
<Sysname> terminal debugging
```

```
<Sysname> terminal monitor
[Sysname] system-view
[Sysname] undo qos apply policy p1 global inbound
[Sysname] qos apply policy p1 global inbound
[Sysname] %Mar 19 15:44:53:648 2014 Sysname
QOS/4/QOS_POLICY_APPLYGLOBAL_CBFAIL:-MDC=1-Slot=6; Failed to apply
classifier-behavior c1 in policy p1 to the inbound direction globally. In a classifier
with AND operator, you cannot configure multiple ACL match rules.
```

上例中的提示信息说明 and 类型的类 c1 不支持定义多条 ACL 规则。此时也可以通过 display 命令也可以查看到当前 QoS 策略应用失败：

```
[Sysname] display qos policy global slot 3 inbound

  Direction: Inbound

  Policy: p1
   Classifier: c1 (Failed)
     Operator: AND
     Rule(s) :
      If-match acl 3000
      If-match acl 3001
     Behavior: b1
      Filter enable: Deny
```

对于此类问题，应该重新定义该类，并指定该类下的规则之间的逻辑为 or。

(2) 类中定义的某条规则不支持。

```
<Sysname> terminal debugging
<Sysname> terminal monitor
[Sysname] system-view
[Sysname] undo qos apply policy p1 global inbound
[Sysname] qos apply policy p1 global inbound
[Sysname] %Aug  3 18:53:41:817 2024 Sysname QOS/4/QOS_POLICY_APPLYGLOBAL_CBFAIL:
-MDC=1-Slot=3; Failed to apply classifier-behavior c1 in policy p1 to the inbound
direction globally. Customer-VLAN match rule is not supported.
```

上例中的提示信息说明不支持在全局 QoS 策略的入方向匹配 customer-vlan-id。此时也可以通过 **display** 命令也可以查看到当前 QoS 策略应用失败：

```
[Sysname] display qos policy global slot 3

  Direction: Inbound

  Policy: p1
   Classifier: c1 (Failed)
     Operator: AND
     Rule(s) :
      If-match customer-vlan-id 100
      If-match acl 3000
     Behavior: b1
      Marking:
        Remark service-vlan-id 201
```

对于此类问题，应该删除类中不支持的规则。

(3) 流行为中的动作冲突。

```
<Sysname> terminal debugging
<Sysname> terminal monitor
[Sysname] system-view
[Sysname] interface gigabitethernet6/0/12
[Sysname-GigabitEthernet6/0/12] undo qos apply policy p1 inbound
[Sysname-GigabitEthernet6/0/12] qos apply policy p1 inbound
[Sysname-GigabitEthernet6/0/12] %Mar 19 16:58:41:624 2014 Sysname
QOS/4/QOS_POLICY_APPLYIF_CBFAIL: -MDC=1-Slot=6; Failed to apply classifier-behavior c1
in policy p1 to the inbound direction of interface GigabitEthernet6/0/12.Filter deny
conflicts with redirect to CPU.
```

上例中的提示信息说明流行为中的 filter deny 动作和 redirect to cpu 动作冲突。此时也可以通过 **display** 命令也可以查看到当前 QoS 策略应用失败：

```
[Sysname] display qos policy interface inbound

Interface: GigabitEthernet6/0/12

  Direction: Inbound

  Policy: p1
   Classifier: c1 (Failed)
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: b1
      Filter enable: Deny
      Redirecting:
        Redirect to the CPU
```

对于此类问题，应该删除流行为中冲突的动作。

3. 检查规则中的时间段

用户可以通过设置 time-range 字段来设定规则生效的时间范围。如果发现表项功能不生效，并且表项中带 time-range 字段，需要检查 time-range 配置的时间范围是否正确，检查方法介绍如下：

```
[Sysname] display time-range t1
Current time is 09:59:37 8/14/2013 Wednesday
Time-range: t1 (Inactive)
 09:25 to 09:30 working-day
```

此时发现时间段 t1 的状态是 Inactive，说明系统当前时间在所设置的时间内未生效，需要修改时间段的时间范围。

4. 检查 QoS 和 ACL 资源的使用情况

通过检查 QoS 和 ACL 资源的使用情况可以用来判断当前功能失效的原因是否是由于资源不足，下面介绍下资源检查的方法：

```
[Sysname] display qos-acl resource slot 3
Interfaces: GE3/3/1 to GE3/3/8, Pos3/4/1 to Pos3/4/4
------------------------------------------------------------------------
 Type             Total      Reserved   Configured Remaining  Usage
------------------------------------------------------------------------
```

```
IPv4Acl          65536      0          2          65534      0%
IPv6Acl          16384      0          0          16384      0%
Car&Cnt          32768      0          1          32767      0%
InBRASCar        65536      0          0          65536      0%
OutBRASCar       65536      0          0          65536      0%
TCPCar           16384      0          0          16384      0%
CarProf          220        0          2          218        0%
Sampler          32768      0          0          32768      0%
```

显示信息中 Type 表示资源类型，Total 表示总的资源数，Configured 表示使用资源数，Remaining 表示剩余的资源数，Usage 表示使用的百分比。

当剩余的资源数为 0 或者使用的百分比达到 100%时，表示该类表项的资源不足。对于此类故障，请直接联系技术支持。

5. 如仍还无法排查，请把故障信息发送给技术支持人员分析

12.16 QoS业务故障

12.16.1 故障描述

QoS 常见故障现象为队列拥塞/丢包。

12.16.2 故障处理步骤

1. 检查缓存是否达到队列缓存门限

通过 **display qos queue-statistics interface outbound** 命令查询队列的统计计数信息，确认队列深度是否达到队列缓存门限。

2. 检查队列或者端口是否有限速相关配置。

```
<Sysname> display qos lr interface
Interface: GigabitEthernet3/1/1
 Direction: Outbound
  CIR 10000 (kbps), CBS 625000 (Bytes)
<Sysname> display qos gts interface
Interface: GigabitEthernet3/1/1
 Rule: If-match queue 1
  CIR 10000 (kbps), CBS 625000 (Bytes)
```

3. 如仍还无法排查，请把故障信息发送给技术支持人员分析

12.17 NQA TWAMP-light测试故障

12.17.1 故障描述

TWAMP-light 探测结果为丢包 100%。

12.17.2 故障处理步骤

1. 检查 TWAMP-light 探测对应的真实数据流是否在链路上转发正常

通过 ping 等手段检查 TWAMP-light 探测的源地址和目的地址之间链路是否正常。

- 如果链路不正常，则基本可以排除 TWAMP-light 故障，TWAMP-light 的探测结果只是反应了当前网络的真实情况；
- 如果链路是正常的，则怀疑 TWAMP-light 功能故障。

2. 检查会话是否是激活状态，如果不是激活状态则检查配置是否正确

```
<Sysname>display nqa twamp-light client test-session 1
Session ID                            : 1
  Status                                : Active
  Session type                        : Permanent
  Source interface                  : -
  Service instance                  : -
  Source IP                             : 1.1.1.1
  Source IPv6                         : -
  Destination IP                      : 1.1.1.2
  Destination IPv6                   : -
  Source port                          : 10001
  Destination port                    : 10002
  Source MAC                         : -
```

3. 检查 client 端和 server 端查看相关表项是否下发到硬件

```
[Sysname-probe] display hardware internal nqa software client all slot 5
=======================ProbeID(0x2       )======================
SessionType: TWAMP, RTCID:3       , VEInlifID:8195    , SamplePeriodID:7
SamplerPeriod = 2000    , TxPktCnt:0       , TcamHandle:4294967295, AclIndex1:40
      ,AclIndex2:42      , StatisIndex:1       , CounterID:10241   , VsiIndex:42
94967295
[Sysname-probe] display hardware internal nqa software server twamp all slot 5
=======================ReflectorId(0x1       )======================
SessionType: Reflector, Ifindex:0       , SceneType:8
VEInlifID:8196    , VsiIndex:4294967295
AclIndexNum:1       , TcamHdlNum:0
================================================================
AclIndex 0-0:44
AclIndex 0-1:46
```

4. 如果仍然无法排查，请把故障信息发送给技术支持人员分析

12.18 路径服务质量测试故障

12.18.1 故障描述

RFC2544 探测（路径服务质量测试）失败，丢包率为 100%。

12.18.2 故障处理步骤

1. 检查探测是否成功

```
<Sysname> display nqa result 2544 2544
NQA entry (admin 2544, tag 2544) test results:
  Basic results     :
    Initial speed(Kbps) : 100000
    Probe duration(s)   : 60
    Probe interval(s)   : 4

  Frame-loss results:
    Frame size(Byte): 1518
      Current speed(Kbps): 100000
      Frame-loss         : 0.0000000%
      Status             : Succeeded
      Time               : 2020-03-17 13:39:03.4
```

2. 检查探测对应的真实数据流是否在链路上转发正常

通过 ping 等手段检查路径服务质量探测的源地址和目的地址之间链路是否正常。

- 如果链路不正常，则基本可以排除路径服务质量故障，路径服务质量的探测结果只是反应了当前网络的真实情况；
- 如果链路是正常的，路径服务质量检测丢包 100%，则怀疑路径服务质量功能故障。

3. 检查客户端和服务端配置相关配置

检查客户端和服务端配置是否正确。如果配置正确，请联系技术支持工程师。

12.19 UDP-jitter测试故障

12.19.1 故障描述

UDP-jitter 探测失败。

12.19.2 故障处理步骤

1. 检查探测是否成功

```
<Sysname> display nqa result
NQA entry (admin 13, tag 13) test results:
    Send operation times: 10              Receive response times: 10
    Min/Max/Average round trip time: 1/1/1
    Square-Sum of round trip time: 10
    Last packet received time: 2020-04-16 19:12:18.4
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
```

```
    Packets arrived late: 0
  UDP-jitter results:
   RTT number: 10
    Min positive SD: 1                    Min positive DS: 0
    Max positive SD: 1                    Max positive DS: 0
    Positive SD number: 1                 Positive DS number: 0
    Positive SD sum: 1                    Positive DS sum: 0
    Positive SD average: 1                Positive DS average: 0
    Positive SD square-sum: 1             Positive DS square-sum: 0
    Min negative SD: 1                    Min negative DS: 0
    Max negative SD: 1                    Max negative DS: 0
    Negative SD number: 2                 Negative DS number: 0
    Negative SD sum: 2                    Negative DS sum: 0
    Negative SD average: 1                Negative DS average: 0
    Negative SD square-sum: 2             Negative DS square-sum: 0
    SD average: 1                         DS average: 0
  One way results:
    Max SD delay: 0                       Max DS delay: 0
    Min SD delay: 0                       Min DS delay: 0
    Number of SD delay: 0                 Number of DS delay: 0
    Sum of SD delay: 0                    Sum of DS delay: 0
    Square-Sum of SD delay: 0             Square-Sum of DS delay: 0
    SD lost packets: 0                    DS lost packets: 0
    Lost packets for unknown reason: 0
```

2. 检测客户端和服务端之间是否路由可达

执行命令**ping**确认客户端和服务器端是否可达，如果**ping**不通目的主机，需要执行命令**display ip routing-table**查看当前的路由表信息，检查设备是否配置了正确路由。

3. 检查客户端和服务端配置

探测丢包率为100%时，需要检查客户端和服务端配置是否正确。如果配置正确，请联系技术支持工程师。

12.20 Y.1564测试故障

12.20.1 故障描述

Y.1564探测失败，丢包率为100%。

12.20.2 故障处理步骤

1. 检查探测是否成功

```
<Sysname> display nqa result 1564 1564
NQA entry (admin 1564, tag 1564) test results:
  Status                    : Unknown error
  Last test                 : Service performance test
  Estimated total time (s)  : 919
  Actual test time used (s) : 16
```

```
Detailed test results:
  CIR test (with the step of 1):
    Start time                : 2020-03-17 12:28:49.1
    End time                  : 2020-03-17 12:28:57.1
    Status                    : Succeeded
    Min/Max/Average IR (kbps) : 68703/70000/69739
    Min/Max/Average FTD (us)  : 23/64/48
    Min/Max/Average FDV (us)  : 0/43/1
    FL count/FLR              : 0/0.000%
    Packets out of order      : 0
    Severely Err Secs/AVAIL   : 0/100.000%
  PIR test (color-blind):
    Start time                : 2020-03-17 12:28:57.1
    End time                  : 2020-03-17 12:29:05.1
    Status                    : Succeeded
    Min/Max/Average IR (kbps) : 138855/140000/139770
    Min/Max/Average FTD (us)  : 19/64/48
    Min/Max/Average FDV (us)  : 0/41/1
    FL count/FLR              : 0/0.000%
    Packets out of order      : 0
    Severely Err Secs/AVAIL   : 0/100.000%
  Service performance test:
    Start time                : 2020-03-17 12:29:05.1
    End time                  : 2020-03-17 12:29:05.2
    Status                    : Unknown error
    Min/Max/Average IR (kbps) : 0/0/0
    Min/Max/Average FTD (us)  : 0/0/0
    Min/Max/Average FDV (us)  : 0/0/0
    FL count/FLR              : 0/0.000%
    Packets out of order      : 0
    Severely Err Secs/AVAIL   : 0/0.000%
```

2. 检查探测对应的真实数据流是否在链路上转发正常

通过 ping 等手段检查 Y.1564 探测的源地址和目的地址之间链路是否正常。

- 如果链路不正常，则基本可以排除 Y.1564 故障，Y.1564 的探测结果只是反应了当前网络的真实情况；
- 如果链路是正常的，Y.1564 检测丢包 100%，则怀疑 Y.1564 功能故障。

3. 检查客户端和服务端配置相关配置

检查客户端和服务端配置是否正确。如果配置正确，请联系技术支持工程师。

13 链路端口故障处理

13.1 端口错包

13.1.1 故障描述

使用 **display interface** 命令查询端口的入、出方向流量统计信息，发现错包统计计数不为 0。

```
<Sysname> display interface gigabitethernet3/1/1
GigabitEthernet3/1/1
Current state: UP
Line protocol state: UP
Description: GigabitEthernet3/1/1 Interface
Bandwidth: 1000000kbps
Flow-control is not enabled
Maximum transmission unit: 1500
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
Internet protocol processing: Disabled
IP packet frame type: Ethernet II, hardware address: 9c06-1b04-31fe
IPv6 packet frame type: Ethernet II, hardware address: 9c06-1b04-31fe
Media type is not sure, port hardware type is No connector
Port priority: 0
Loopback is not set
unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
The maximum frame length is 10240
Last link flapping: Never
Last clearing of counters: Never
Current system time:2020-04-28 11:42:09
Last time when physical state changed to up:-
Last time when physical state changed to down:2020-04-28 11:40:45
 Peak input rate: 0 bytes/sec, at 2020-04-28 11:42:08
 Peak output rate: 0 bytes/sec, at 2020-04-28 11:42:08
 Last 5 seconds input: 0 packets/sec 0 bytes/sec 0 bits/sec -%
 Last 5 seconds output: 0 packets/sec 0 bytes/sec 0 bits/sec -%
 Input (total):  0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, - pauses
 Input (normal):  0 packets, - bytes
          - unicasts, - broadcasts, - multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
          0 CRC, 0 frame, 0 overruns, - aborts
          0 ignored, - parity errors
 Output (total): 0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, - pauses
 Output (normal): 0 packets, 0 bytes
```

```
          - unicasts, - broadcasts, - multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
          0 aborts, 0 deferred, - collisions, 0 late collisions
          - lost carrier, - no carrier
```

1. 端口入方向报文计数错误字段解释

- input errors：端口接收的错误报文的统计值。
- runts：表示接收到的超小帧个数。超小帧即超小帧是指长度小于 64 字节、格式正确且包含有效的 CRC 字段的帧。
- giants：接收到的超大帧的数量。超大帧即有效长度大于端口允许通过最大报文长度的帧。
- CRC：接收到的 CRC 校验错误、长度正常的帧的数量。
- frame：接收到的 CRC 校验错误、且长度不是整字节数的帧的数量。
- throttles：超小而且 CRC 错误的帧的数量。

2. 端口出方向报文计数错误字段解释

- output errors：各种发送错误的报文总数。
- aborts：表示发送失败的报文总数。
- deferred：表示延迟报文的总数。报文延迟是指因延迟过长的周期而导致发送失败的报文，而这些报文由于发送媒质繁忙而等待了超过 2 倍的最大报文发送时间。
- collisions：表示冲突帧总数，即在发送过程中检测到冲突而停止发送的报文。
- late collisions：表示延迟冲突帧，即发送过程中发生延迟冲突超过 512bit 时间的帧。

13.1.2 故障处理步骤

1. 端口入方向出现 CRC、frame、throttles 错包且计数持续增加

(1) 使用仪器测试链路，链路质量差或者线路光信号衰减过大会导致报文在传输过程中出错。如链路故障请更换网线或光纤。

(2) 如端口使用光模块，参照 13.5 光模块故障确认是否光模块故障导致。

(3) 与别的正常的端口更换网线或光纤光模块，如端口更换后错包消失，端口更换回来错包又再次出现端口相关，应为单板端口故障，请更换端口并将故障信息发送技术支持人员分析；如更换到其他正常端口仍会出现错包，则对端设备、中间传输链路故障的可能性较大，请排查。

(4) 排查对端设备或者中间的传输设备。

(5) 如故障无法确认，请将故障信息发送技术支持人员分析。

2. 端口入方向出现 Overrun 错包且计数持续增加

Overrun 计数是由于端口输入速率超出本端口处理能力，导致丢包。

(1) 如果只有某一个端口收发包异常，或者某一个端口下挂设备的业务不通，同时这个单板上的其他端口都是正常的，可以多次查询 **display interface** 命令，如果 input errors 有增加，且等于 overruns 的增加，那么可以怀疑是单板内部拥塞或堵死，请将故障信息发送技术支持人员分析。

(2) 如果仍然无法确认，请将故障信息发送技术支持人员分析。

3. 端口入方向出现 giants 错包且计数持续增加

(1) 检查两端的 jumbo 配置是否一致，如 jumbo 是否使能，端口默认的最大报文长度是否一致，允许最大报文长度是否一致，可以通过 **display interface** 命令查到，即 The maximum frame length 所显示的数值。

(2) 如果仍然无法确认，请将故障信息发送技术支持人员分析。

4. 端口出方向出现错包且计数持续增加

(1) 检查端口是否配置为半双工模式，如为半双工，请更改为全双工模式。

(2) 如果仍然无法确认，请将故障信息发送技术支持人员分析。

13.2 端口无法up

13.2.1 故障描述

端口无法正常 up。

13.2.2 故障处理步骤

1. 端口无法 up

(1) 测试端口之间网线、光纤链路是否正常，光纤两端的发送/接收端是否错连；更换端口之间的网线、光纤或将网线、光纤放到别的正常端口，以确认是否中间传输链路故障。

(2) 通过 **display interface** 命令查看端口状态是否为 UP，如果不是，请使用 **undo shutdown** 命令激活相应的以太网端口。

(3) 检查本端、对端端口配置是否正确，如端口是否 shutdown，速率、双工的协商模式、MDI 是否正确。

```
[Sysname] display current-configuration interface Ten-gigabitethernet 6/0/1
#
interface Ten-GigabitEthernet6/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 3102
 port link-aggregation group 1
#
return
```

说明

- 光类型接口和位于 CSPEX 类单板、CEPC 类单板上的接口子卡的电口不支持 **duplex half** 命令。
- 位于 CSPEX-1204 单板上的 MIC 接口子卡的接口仅支持配置接口速率为 1000Mbps 和 **auto**。
- 当 PIC-GP10L 子卡的光口与 MIC 接口子卡或千兆以太网 CSPC 单板（如 CSPC-GP48LB）的光口直连时，如果使用本命令配置一端接口速率为 1000，另一端的速率请配置为 **auto**。

(4) 如端口使用光模块，请检查两端光模块类型是否一致，如速率、波长、单模多模状态等；由于部分子卡一个端口支持两种速率，请使用和端口实际速率一致的光模块；与正常的光模块交叉更换，并参照 13.5 光模块故障排除是否为光模块故障导致。

```
[Sysname] display transceiver interface Ten-gigabitethernet 2/9/0/1
Ten-GigabitEthernet2/9/0/1 transceiver information:
  Transceiver Type              : 10G_BASE_SR_SFP
  Connector Type                : LC
  Wavelength(nm)                : 850
  Transfer Distance(km)         : 80(50um),20(62.5um),300(om3)
  Digital Diagnostic Monitoring : YES
  Vendor Name                   : H3C
  Ordering Name                 : SFP-XG-SX-MM850-A
```

(5) 如端口为 WAN 口。请检查 WAN 口的速率是否与光模块匹配，如果不匹配，请更换。

(6) 如确认为光模块故障，请更换光模块，并将故障信息发送技术支持人员分析。

13.3 端口由up变成down

13.3.1 故障描述

端口状态由 up 变成 down。

13.3.2 故障处理步骤

(1) 查看本设备及对端设备日志，确认有无端口 **shutdown** 操作。

(2) 查看两端端口状态，确认是否为协议异常或在线诊断模块检测到异常将端口 shutdown。如这里的 GE2/6/0/1 端口出现“Protect DOWN”，是由于 hardware-failure-detection 配置为 isolate 级别，当设备在线诊断模块检测到端口故障时，将端口 shutdown 隔离，以便流量切换到备份链路。请将故障信息发送技术支持人员分析。

```
[Sysname] display interface gigabitethernet2/6/0/1
GigabitEthernet2/6/0/1
current state: Protect DOWN
Line protocol current state: DOWN
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0000-e80d-c000
Description: GigabitEthernet2/6/0/1 Interface
Loopback is not set
Media type is optical fiber, Port hardware type is 1000_BASE_SX_SFP
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
The Maximum Frame Length is 9216
  ……
```

(3) 参照 13.2 端口无法 up，排查两端端口配置，网线、光模块、光纤等链路是否正常。

(4) 如仍无法确认，请搜集本端、对端设备信息，并将信息发送技术支持人员分析。

13.4 端口频繁up/down

13.4.1 故障描述

端口频繁 up/down。

13.4.2 故障处理步骤

(1) 对于光口，请参照 13.5 光模块故障确认光模块是否异常。查看光模块 alarm 信息来排查两端光模块以及中间光纤问题；对于支持诊断功能的光模块可以通过查看 diagnosis 信息确认光模块的光功率是否处于上下门限临界值。如发送光功率处于临界值，请更换光模块做交叉验证；如接收光功率处于临界值，请排查对端光模块及中间光纤链路。

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

(3) 对于 WAN 口，请检查两端时钟是否配置，需在主控板有时钟扣板的一端配置为 Master，另一端配置为 slave。

(4) 如果故障依然存在，请排查链路、对端设备、中间设备。

(5) 如仍无法确认，请将故障信息发送技术支持人员分析。

13.5 光模块故障

13.5.1 故障描述

安装光模块的接口不能正常工作。

13.5.2 故障处理步骤

(1) 检查光模块 Alarm 告警信息。告警信息中如果存在接收有问题那一般是对端端口、光纤或中转传输设备导致；如果是发送有问题或者电流、电压异常那就需要排查本端端口。

```
<Sysname> display transceiver alarm interface GigabitEthernet 2/0/1
GigabitEthernet2/0/1 transceiver current alarm information:
  TX fault
  RX power high
```

表1 光模块告警信息说明

字段	描述
SFP/SFP+/CFP/QSFP+	
RX loss of signal	接收信号丢失
RX power high	接收光功率高告警
RX power low	接收光功率低告警
TX fault	发送错误
TX bias high	偏置电流高告警
TX bias low	偏置电流低告警

字段	描述
TX power high	发送光功率高告警
TX power low	发送光功率低告警
Temp high	温度高告警
Temp low	温度低告警
Voltage high	电压高告警
Voltage low	电压低告警
Transceiver info I/O error	模块信息读写错误
Transceiver info checksum error	模块信息校验和错误
Transceiver type and port configuration mismatch	模块类型和端口配置不匹配
Transceiver type not supported by port hardware	端口不支持该模块类型
XFP	
RX loss of signal	接收信号丢失
RX not ready	接收状态未就绪
RX CDR loss of lock	RX CDR时钟失锁
RX power high	接收光功率高告警
RX power low	接收光功率低告警
TX not ready	发送状态未就绪
TX fault	发送错误
TX CDR loss of lock	TX CDR时钟失锁
TX bias high	偏置电流高告警
TX bias low	偏置电流低告警
TX power high	发送光功率高告警
TX power low	发送光功率低告警
Module not ready	模块状态未就绪
APD supply fault	APD（Avalanche Photo Diode，雪崩光电二极管）错误
TEC fault	TEC（Thermoelectric Cooler，热电冷却器）错误
Wavelength unlocked	光信号波长失锁
Temp high	温度高告警
Temp low	温度低告警
Voltage high	电压高告警
Voltage low	电压低告警
Transceiver info I/O error	模块信息读写错误

字段	描述
Transceiver info checksum error	模块信息校验错误
Transceiver type and port configuration mismatch	模块类型和端口配置不匹配
Transceiver type not supported by port hardware	端口不支持该模块类型

(2) 检查光模块的接收、发送光功率是否正常（即在该光模块的光功率上下门限值之内）。

对于 H3C 定制且支持诊断功能的光模块，可以通过命令行查询光模块的接收、发送光功率是否超出其上下门限值；其他光模块可以使用同样命令尝试查询，但有可能查询不到。

a. 查看光模块的电子标签信息，Verdor Name 显示为 H3C 表示是 H3C 定制光模块。

```
<Sysname> display transceiver manuinfo interface Ten-gigabitethernet 1/2/0/15
Ten-GigabitEthernet1/2/0/15 transceiver manufacture information:
  Manu. Serial Number : 213410A0000054000251
  Manufacturing Date  : 2012-10-26
  Vendor Name         : H3C
```

b. 通过下述命令确认光模块是否支持诊断功能，Digital Diagnostic Monitoring 为 YES 表示支持诊断功能。

```
<Sysname> display transceiver interface
Ten-GigabitEthernet1/2/0/15 transceiver information:
  Transceiver Type              : 10G_BASE_LR_XFP
  Connector Type                : LC
  Wavelength(nm)                : 1310
  Transfer Distance(km)         : 10(SMF)
  Digital Diagnostic Monitoring : YES
  Vendor Name                   : H3C.
```

c. 通过命令 **display transceiver diagnosis interface** 查询光模块的实时接收、发送光功率。

```
<Sysname> display transceiver diagnosis interface
Ten-GigabitEthernet1/2/0/15 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp.(°C) Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM)
    41         3.26        42.43     -40.00         -2.20
```

d. 通过 **display transceiver interface** 或 **display transceiver diagnosis interface** 命令查询光模块的接收发送光功率的上下门限值。

有可能出现通过这两个命令行都可以查询、且查询出来的接收发送光功率上下门限值存在差异的情况，此时请以范围最小的上下门限值为准。

display transceiver diagnosis interface 命令还可以查询实时的接收发送光功率、温度及其上下门限值、电压及其上下门限值、偏置电流及其上下门限值，命令行中 Current diagnostic parameters 下数据表示光模块当前的温度、电压、偏置电流、接收光功率、发送光功率，Alarm thresholds 下 High、Low 数据表示温度、电压、偏置电流、接收光功率、发送光功率的上下门限值。

```
<Sysname> display transceiver interface Ten-GigabitEthernet 1/2/0/15
Ten-GigabitEthernet1/2/0/15 transceiver information:
  Transceiver Type              : 10G_BASE_SR_SFP
  Connector Type                : LC
```

```
  Wavelength(nm)                : 850
  Transfer Distance(km)         : 80(50um),20(62.5um),300(om3)
  Digital Diagnostic Monitoring : YES
  Vendor Name                   : H3C
  Ordering Name                 : SFP-XG-SX-MM850-A
<Sysname> display transceiver diagnosis interface Ten-GigabitEthernet 1/2/0/15
Ten-GigabitEthernet1/2/0/15 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp.(°C) Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM
    43         3.35        46.33     -3.60          -2.38
  Alarm thresholds:
           Temp.(°C) Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM
    High  73         3.80        92.40     2.50           3.50
    Low   -3         2.81        1.00      -16.40         -11.20
  Parameters when first used on N/A:
    Temp.(°C) Voltage(V)  Bias(mA)  RX power(dBm)  TX power(dBm)
    N/A        N/A         N/A       N/A            N/A
  Total account of alarms: 0
  Latest occurrence of different alarms:
    Type       Date           Description
    Temp.      N/A            N/A
    Voltage    N/A            N/A
    Bias       N/A            N/A
    RX power   N/A            N/A
    TX power   N/A            N/A
    TX         N/A            N/A
    RX         N/A            N/A
    Others     N/A            N/A
  Latest three alarms:
    Date           Description
    N/A            N/A
    N/A            N/A
    N/A            N/A
```

(3) 对怀疑故障的光模块进行交叉验证，如更换端口、与正常的光模块互换，确认是光模块本身故障还是相邻设备或中间链路故障。

(4) 如仍无法确认，请将故障信息发送技术支持人员分析。

建议尽量使用 H3C 定制光模块。可通过 **display transceiver manuinfo** 命令来查询光模块的定制厂商信息，如果 Vendor Name 为 H3C，说明是 H3C 定制光模块。

13.6 端口不可见

13.6.1 故障描述

端口不可见。

13.6.2 故障处理步骤

(1) 通过 **display device** 查看所在单板或子卡的状态，有可能是单板或子卡还处于启动状态，需保证单板和子卡状态为 NORMAL。

```
<Sysname> display device
Slot No. Brd Type         Brd Status   Software Version
 0       CSR05SRP1L3      Master       CR16000-CMW710-R8151PXX
 1       CSR05SRP1L3      Standby      NONE
 2       CSPC-XP8LB       Normal       CR16000-CMW710-R8151PXX
 3       CMPE-1104        Normal       CR16000-CMW710-R8151PXX
   Sub1  MIC-SP4L         Normal
   Sub2  MIC-SP4L         Normal
   Sub3  MIC-CLP2L        Normal
   Sub4  MIC-GP4L         Normal
 4       CSPC-XP8LB       Normal       CR16000-CMW710-R8151PXX
 5       NONE             Absent       NONE
 6       CSFC-04D         Normal       CR16000-CMW710-R8151PXX
 7       NONE             Absent       NONE
 8       NONE             Absent       NONE
 9       NONE             Absent       NONE
```

(2) 如果单板或子卡已经恢复配置，再查看当前的接口信息中是否有目标端口。

```
<Sysname> display interface brief
Brief information on interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Main IP         Description
GE5/1/1              DOWN DOWN     --
GE5/1/1.1            DOWN DOWN     110.0.1.1
GE5/1/1.2            DOWN DOWN     110.0.2.1
GE5/1/1.3            DOWN DOWN     110.0.3.1
GE5/1/1.4            DOWN DOWN     110.0.4.1
GE5/1/1.5            DOWN DOWN     110.0.5.1
GE5/1/1.6            DOWN DOWN     110.0.6.1
GE5/1/1.7            DOWN DOWN     110.0.7.1
GE5/1/1.8            DOWN DOWN     110.0.8.1
GE5/1/1.9            DOWN DOWN     110.0.9.1
GE5/1/1.10           DOWN DOWN     110.0.10.1
GE5/1/1.11           DOWN DOWN     110.0.11.1
GE5/1/1.12           DOWN DOWN     110.0.12.1
GE5/1/1.13           DOWN DOWN     110.0.13.1
```

(3) 有的子卡支持类型切换，接口类型不匹配时，需要手工切换。如：1602 单板插的是 GP20L 子卡，子卡更换为 XP20L 后，端口类型是 GE 的，非 10GE，想用 10GE 接口需要命令行切换。

(4) 如查不到端口，有可能是还在配置恢复过程中，需耐心等待一段时间，如过了较长时间后问题仍没有消除，请将故障信息发送技术支持人员分析。

13.7 WAN口协议不up

13.7.1 故障描述

WAN 口物理链路能 up，但协议不 up。

13.7.2 故障处理步骤

(1) 检查 WAN 口两端配置协议是否一致。如果不一致，需配置成相同的协议。

(2) 通过 **display interface** 查看两端端口上是否有错包，两端端口配置是否一致。如果有错包计数，请检查下光模块是否和该端口匹配，检查光纤和光模块是否良好。如果两端端口的配置不一致，请配置成一致。

(3) 如仍无法解决，请将故障信息发送技术支持人员分析。

13.8 WAN口物理不up

13.8.1 故障描述

WAN 口物理链路不 up。

通过 **display interface pos** 命令查看接口的信息，Alarm 字段出现告警。

```
<Sysname> display interface pos 2/2/1
Pos2/2/1
Current state: DOWN
Line protocol state: DOWN
Description: pos-interface
Bandwidth: 155520 kbps
Maximum transmission unit: 1500
Hold timer: 10 seconds, retry times: 5
Dampening enabled:
 Penalty: 0 (not suppressed)
 Ceiling: 6000
 Reuse: 750
 Suppress: 2000
 Half-life: 54 seconds
 Max-suppress-time: 162 seconds
 Flap count: 0
Internet protocol processing: Disabled
Link layer protocol: PPP
LCP: initial
Port priority: 0
Last link flapping: Never
Last clearing of counters: Never
Current system time:2017-12-15 17:18:19
Last time when physical state changed to up:-
Last time when physical state changed to down:2017-12-11 09:57:36
Port connector type is No connector
Physical layer is packet over SDH
```

```
Port speed type: STM-1
Loopback is not set
FCS: 32-bit CRC
Clock source: Slave
Clock grade: Quality unknown(existing synchronization network)
SPE scrambling: Enable
BER thresholds:
    SD: 10e-6    SF: 10e-4
Regenerator section layer:
    J0(TX): "CR16000"
            43 52 31 36 30 30 30 00 00 00 00 00 00 00 00 00
    J0(RX): ""
            00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    Alarm: LOS
    Error: 0 BIP(B1)
Multiplex section layer:
    Alarm: None
    Error: 0 BIP(B2), 0 REI(M1)
Higher order path layer:
    C2(TX): 0x16    C2(RX): 0xef
    J1(TX): "CR16000"
            43 52 31 36 30 30 30 00 00 00 00 00 00 00 00 00
    J1(RX): ""
            00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    Alarm: None
    Error: 0 BIP(B3), 0 REI(G1)
           0 PJE, 0 NJE
Port statistic:start time: 2017-12-11 09:57:46
UP time: 0 H 0 M 0 S
Section: ES        0   SES        0   SEFS        0
Line   : ES        0   SES        0   UAS         0   FE-ES        0
Input speed in last 300 seconds: 0 packets/s, 0 bytes/s
Output speed in last 300 seconds: 0 packets/s, 0 bytes/s
Input: 0 packets,  0 bytes(good), 0 bytes(all)
        0 FCS errors,  0 Aborts,  0 FIFO overflow
        0 Runs,  0 Giants
Output: 0 packets,  0 bytes(good), 0 bytes(all)
        0 FIFO underflow,  0 Aborts,  0 Runts
Peak value of input: 0 bytes/sec, at 2017-12-15 00:01:34
Peak value of output: 0 bytes/sec, at 2017-12-15 00:01:34
```

13.8.2 故障处理步骤

1. Alarm 字段出现 LOF（loss of framer）告警

出现 LOF 告警表示出现了帧丢失问题，表明传输的信号质量较差。

(1) 查看两端 POS 接口速率是否一致。若两端 POS 接口速率不一致，请重新配置两端 POS 接口速率，保持一致。

(2) 查看光模块类型与 POS 接口速率是否匹配，低速率光模块不能用于高速率 POS 接口，若光模块类型与 POS 接口速率不匹配，请更换及时光模块。

(3) 查看光纤是否损坏，若光纤出现损坏，请及时更换光纤。

(4) 如仍无法解决，请将故障信息发送技术支持人员分析。

2. Alarm 字段出现 LOS（loss of single）告警

如果 POS 接口收不到光信号或者连续收到 LOF 告警，就会产生 LOS 告警。

(1) 查看 POS 接口光模块是否安插正常。若未安插光模块或者光模块接触不良，请保证光模块安插正常。

(2) 查看 POS 接口光纤是否安装插正常。若未插光纤或者收发光纤插反，请保证光纤安插正常。

(3) 查看光纤是否损坏。若光纤出现损坏，请及时更换光纤。

(4) 查看两端 POS 接口速率是否一致。若两端 POS 接口速率不一致，请重新配置两端 POS 接口速率，保持一致。

(5) 查看光模块类型与 POS 接口速率是否匹配。低速率光模块不能用于高速率 POS 接口，若光模块类型与 POS 接口速率不匹配，请更换及时光模块。

(6) 查看对端 POS 接口是否关闭。若对端 POS 接口已关闭，请开启的对端 POS 接口。

(7) 查看对端 POS 接口是否使能了内部环回功能。若使能了内部环回功能，则需要去使能内部环回功能。

(8) 查看光纤与光模块是否匹配，若不匹配，请更换光纤或者光模块。

(9) 如仍无法解决，请将故障信息发送技术支持人员分析。

13.9 WAN口打印告警信息

13.9.1 故障描述

WAN 口打印告警信息，如：

```
H3C WAN/4/ALARM: -MDC=1-Slot=5;
 Cpos5/1/1 : Path 1 Alarm AIS report! Start Time : 2014-04-04 11:40:53:533!
H3C WAN/4/ALARM: -MDC=1-Slot=5;
 Cpos5/1/1 : Path 1 Alarm AIS recover! Start Time : 2014-04-04 11:41:09:769!
```

13.9.2 故障处理步骤

通过 **display interface pos** 命令查看接口的 Alarm 字段的告警信息。各告警标志的处理方法请参见表 13-2。

表2 告警标志处理方法

告警标志	说明	处理方法
LOF	表示出现了帧丢失问题，表明传输的信号质量较差	参见13.8.2
LOS	POS接口收不到光信号或者连续收到LOF告警	参见13.8.2
PSLM	本端和对端的信号标记字节C2配置不一致	重新配置本端和对端的信号标记字节C2，使其保持一致
PTIM	本端和对端的SONET/SDH帧的通道踪迹字节J1配置不	重新配置本端和对端的SONET/SDH

告警标志	说明	处理方法
	一致	帧的通道踪迹字节J1，使其保持一致
PRDI	本端和对端的信号标记字节C2配置不一致或者SONET/SDH帧的通道踪迹字节J1配置不一致	重新配置本端和对端的信号标记字节C2或者SONET/SDH帧的通道踪迹字节J1，使其保持一致

如果上述检查完成后故障仍无法排除，可通过 **display diagnostic-information** 命令收集设备的diagnostic-information，联系 H3C 的技术支持工程师。

```
<H3C> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:Y
```

13.10 故障诊断命令

命令	说明
display current-configuration	显示设备当前生效的配置，指定interface可以显示指定接口当前生效的配置
display interface	查询端口的入、出方向流量统计信息、端口状态。可查看是否存在错包及错包统计信息。
display transceiver alarm interface	显示可插拔接口模块的当前故障告警信息
display transceiver diagnosis	显示可插拔光模块的数字诊断参数的当前测量值，包括温度、电压、偏置电流、接收光功率、发送光功率
display transceiver interface	显示指定接口可插拔接口模块的主要特征参数。检查两端光模块类型是否一致，如速率、波长、单模多模状态等
display transceiver manuinfo	显示可插拔接口模块的电子标签信息。可用来查询光模块的定制厂商。

14 IP 业务故障处理

14.1 ARP故障

14.1.1 故障描述

无法学习到对端设备的 ARP 表项。

14.1.2 故障处理步骤

1. 查看 ARP 调试信息

使用 **debugging arp packet** 命令打开 ARP 调试信息开关，当对端 ping 本设备时，可以看到下列调试信息。如果未显示 ARP 请求报文信息，则说明未接收到请求报文；如果未显示 ARP 应答报文，则说明本设备未应答 ARP 请求。

```
<Sysname>*Sep 24 19:15:52:655 2019 H3C ARP/7/ARP_RCV: -MDC=1-Slot=5; Received an ARP message,
operation: 1, sender MAC: 1cab-343a-6145,sender IP: 222.3.1.2, target MAC: 0000-0000-0000,
target IP: 222.3.1.1
```

// 接收 ARP 请求报文

```
*Sep 24 19:15:52:656 2019 H3C ARP/7/ARP_SEND: -MDC=1-Slot=5; Sent an ARP message, operation:
2, sender MAC: 70f9-6da7-5074, sender IP: 222.3.1.1, target MAC: 1cab-343a-6145, target IP:
222.3.1.2
```

// 发送 ARP 应答报文

2. 报文计数分析

如果设备未收到 Ping 报文，请排查上游的相邻设备；如果设备收到 Ping 报文，分析 ARP 报文在本端是否上送给平台。

对端 ping 本设备，本端设备使用 **display hardware internal rxpkt-in slot** *slotid* **cpu** *cpuid* 命令查看报文收发模块收到的上送报文：

```
[Sysname-probe]display hardware internal rxtx rxpkt-in slot 2 cpu 0
[H3C-probe]%Aug 11 08:34:36:459 2022 H3C IFNET/3/PHY_UPDOWN: -MDC=1; GigabitEthernet2/2/1
link status is up.
%Aug 11 08:34:36:459 2022 H3C IFNET/5/LINK_UPDOWN: -MDC=1; Line protocol on the interface
GigabitEthernet2/2/1 is up.
*Aug 11 08:34:41:006 2022 H3C RXTX/7/DBG: -MDC=1-Slot=2;
 Time on LPU: 2022-08-11  08:34:41  5ms
Receive packet from chip :
 DevNum = 9, PhyPortNo = 33, PacketLen = 60, CpuCode = 17, Left = 14
0000: ff ff ff ff ff ff 00 00 2e 3b f4 03 08 06 00 01
0010: 08 00 06 04 00 01 00 00 2e 3b f4 03 16 01 00 02
0020: 00 00 00 00 00 00 16 01 00 02 00 00 00 00 00 00
0030: 00 00 00 00 00 00 00 00 00 00 00 00 33 d4 92 9c

*Aug 11 08:34:41:007 2022 H3C RXTX/7/DBG: -MDC=1-Slot=2;
 Time on LPU: 2022-08-11  08:34:41  7ms
Receive packet from chip :
 DevNum = 9, PhyPortNo = 33, PacketLen = 60, CpuCode = 17, Left = 13
0000: ff ff ff ff ff ff 00 00 2e 3b f4 03 08 06 00 01
0010: 08 00 06 04 00 01 00 00 2e 3b f4 03 16 01 00 02
0020: 00 00 00 00 00 00 16 01 00 02 00 00 00 00 00 00
0030: 00 00 00 00 00 00 00 00 00 00 00 00 33 d4 92 9c
```

本端设备使用 **display hardware internal rxtx packet statistic slot** *slotid* **cpu** *cpuid* **clear** 命令查看报文收发模块上送 CPU 计数，

```
[Sysname-probe]display hardware internal rxtx packet statistic slot 2 cpu 0 clear
Net port packet loss count:
 code       counter
Rx packets statistic:
                     counter     success        rate
 NET  ->RXTX   :           6           6           0 pps

Cpu code input list:
 code       counter       success
   17             2             2
   30             4             4
```

```
Callback function packets statistic:
            total(r)   success(r)     total(c)   success(c)
  MACL:            0            0            0            0
  NATL:            0            0            0            0
   BFD:            0            0            0            0

Task input pkt statistics:
 Task name           total       success
 Main Task :             6             6
 Icmp Task :             0             0
```

3. 查看本机路由和 Inlif 表项

若报文收发模块没有收到报文，请查看本机路由和 InLif 表是否下发正确。

(1) 检查本机路由下发是否正确，如果上送标记 Th 没有置位，请联系技术支持人员分析。

```
[H3C-probe]display hardware internal l3 np fib 22.1.0.1 32 slot 2 chip 0

 The FTN/FIB table Handle<0x10> ECMPNum<0/1>!
 ChipID is 0
 LPM:
 LPM KEY: VPNID = 0  IP_Prefix = 22.1.0.1/4294967295
 LPM RESULT:
   00001017 0fffff00
 Ipv4-route tag:
 Valid = 1     Parity = 1    Local = 1
 Drop = 0      ToHost = 1    Ecmp = 0
 Dft_Sys = 0   Dft_User = 0  NextHopIdxOrEcmpPtr = 16
 LifId = 1048575     EcmpNum = 0
 FWD-FTN:
 FWD-FTN KEY: NextHopIdx = 0x10
 FWD-FTN RESULT:
 ECMP = 0  Th = 1  Normal = 0 Drop = 0
 OutlifId/ToHostId = 76
 Dft_User = 0  Dft_Sys = 0
 Es = 0  Ts = 0  DhcpH = 0
 Local = 1  Parity = 1  V = 1 TTL = 255
 StackEnd = 0  Label_v = 0  Label = 0  Label_bak = 0
 Rd = 0  Rq = 0  Dscp = 0  QosLocalId = 0
```

(2) 查看 Inlif 表项，L3，IPv4，ArpProxy 是否置位，如果没置位，请联系技术支持人员分析。

```
[Sysname-probe]display hardware internal lif np inlif slot 2 GigabitEthernet 2/2/1

 Inlif Table : KEY(vlan=4095,port=32)
               RESULT(08060001, 0030d001, 00008000, 00000000, 00000000, 00000000, 00000000,
00000000)
 RES:
 un0.gen.uiSa:1 = 0
 un0.gen.uiV4m:1 = 0
 un0.gen.uiBlock:1 = 0
```

```
 un0.gen.uiDs:1 = 0
 un0.gen.uiV4Acl:1 = 1
 un0.gen.uiV4Rpf:1 = 0
 un0.gen.uiV4Qppb:1 = 0
 un0.gen.uiV4Sq:1 = 0
 un0.gen.uiMldv2:1 = 0
 un0.gen.ui8021ag:1 = 0
 un0.gen.uiRsvp:1 = 0
 un0.gen.uiMpls:1 = 0
 un0.gen.uiIf:1 = 0
 un0.gen.uiIpv4:1 = 1
 un0.gen.uiL3:1 = 1
 un0.gen.uiL3Vpn:1 = 0
 un0.gen.uiPppoe:1 = 0
…..
 un2.gen.uiV6RpfL:1 = 0
 un2.gen.uiV6RpfAcl:1 = 0
 un2.gen.uiArpProxy:1 = 1
 un2.gen.uiFrIsis:1 = 0
 un2.gen.uiFrTh:1 = 0
 un2.gen.uiV42Acl:1 = 0
```

14.2 DHCP中继故障处理

14.2.1 故障描述

客户端无法通过 DHCP 中继获取 IP 地址。

14.2.2 故障处理步骤

客户端无法通过 DHCP 中继获取 IP 地址一般是由以下的原因造成的：

- 中继和服务器间的路由错误
- 中继没有指定服务器的地址
- DHCP 中继功能未使能

1. 查看中继代理与 DHCP 服务器间的路由是否存在

在 DHCP 中继代理和 DHCP 服务器上执行 http://127.0.0.1:7890/pages/31189898/01/31189898/01/resources/software/nev8r10_vrpv8r16/user/vrp/display_ip_routing-table.html 命令来查看到对方的路由表项是否存在，如不存在请配置静态路由后查看故障是否排除，如依然存在请执行步骤 2。

2. 查看 DHCP 中继是否指定了 DHCP 服务器地址

在 DHCP 中继上指定 DHCP 服务器的地址 **dhcp relay server-address** *ip-address*，查看故障是否排除，如依然存在请执行步骤 3。

3. 查看 DHCP 中继功能是否使能

配置接口工作在 DHCP 中继模式 **dhcp select relay**，查看故障是否排除，如依然存在请联系技术支持人员分析。

14.3 ND故障处理

14.3.1 故障描述

无法学习到对端设备的 ND 表项。

14.3.2 故障处理步骤

1. 查看 ND 调试信息

使用 **debugging ipv6 nd packet** 命令打开 ND 调试信息开关，当对端 ping 本设备时，可以看到下列调试信息。如果未显示 NS 请求报文信息，则说明未接收到请求报文；如果未显示 NA 应答报文，则说明本设备未应答邻居请求。

```
<Sysname>*Sep 24 19:44:59:161 2019 H3C ND/7/ND_PACKET: -MDC=1-Slot=5;
 Sent NS packet:
 Interface: XGE5/4/3          First VLAN ID: 0   Second VLAN ID: 0
 SrcEthMAC: 70f9-6da7-5074    SrcIP: 2004::1
 DstEthMAC: 0000-0000-0000    DstIP: ff02::1:ff00:2
 LinkId: 0xffff    VsiIndex: 0xffffffff
// 接收 NS 请求报文
*Sep 24 19:44:59:163 2019 H3C ND/7/ND_PACKET: -MDC=1-Slot=5;
 Received NA packet:
 Interface: XGE5/4/3          First VLAN ID: 0   Second VLAN ID: 0
 SrcEthMAC: 1cab-343a-6145    SrcIP: 2004::2
 DstEthMAC: 70f9-6da7-5074    DstIP: 2004::1
 LinkId: 0xffff    VsiIndex: 0xffffffff
// 发送 NA 应答报文
```

2. 报文计数分析

如果设备未收到 Ping 报文，请排查上游的相邻设备；如果设备收到 Ping 报文，分析 NS 报文在本端是否上送给平台。具体步骤请参照 ARP 故障

14.4 IPv6 Ping不通或丢包

14.4.1 故障描述

报文转发丢包，ping 不通或 ping 丢包，tracert 异常。

```
[Sysname]ping ipv6 1001::1
Ping6(56 data bytes) 1::1 --> 1001::1, press CTRL+C to break
Request time out
Request time out
Request time out
Request time out
Request time out
```

```
--- Ping6 statistics for 1001::1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

14.4.2 故障处理步骤

1. 查看 ICMPv6 调试信息

使用 **debugging ipv6 icmp** 命令打开 ICMPv6 调试信息开关，当对端 ping 本设备时，可以看到下列调试信息。如果未显示 ICMPv6 请求报文信息，则说明未接收到请求报文；如果未显示 ICMPv6 应答报文，则说明本设备未应答 ICMPv6 请求。

打开 ICMPv6 的调试信息开关。对端 ping 本设备时，本设备会输出下列调试信息。

```
<Sysname> debugging ipv6 icmp
*Sep 24 17:49:18:717 2019 H3C SOCKET/7/ICMPv6: -MDC=1-Slot=5;
ICMP6 Input:
 ICMPv6 Packet: vpn = PUBLIC(0), src = 2004::2, dst = 2004::1
                type = 128, code = 0 (echo-request)
```

// 接收 ICMP 请求报文，报文源 IPv6 地址为 2004::2，报文目的 IPv6 地址为 2004::1

```
*Sep 24 17:49:18:717 2019 H3C SOCKET/7/ICMPv6: -MDC=1-Slot=5;
ICMP6 Output:
 ICMPv6 Packet: vpn = PUBLIC(0), src = 2004::1, dst = 2004::2
                type = 129, code = 0 (echo-reply)
```

// 发送 ICMP 应答报文，报文源 IPv6 地址为 2004::1，报文目的 IPv6 地址为 2004::2

2. 设备入出报文统计

报文转发异常通常会涉及多台设备，需要逐一排查。为方便排查，排查前建议先明确报文的转发走向，如经过哪些中间设备，在设备的哪些接口进入设备，又会从哪些接口出去。通过镜像抓包或配置 ACL 规则统计设备有没有收到或发出相应的业务报文，以配置 ACL 规则统计端口入方向 Ping 报文为例：

(1) 定义相关的 ACL

```
[Sysname] acl ipv6 advanced 3000
[Sysname-acl-ipv6-adv-3000] rule 1 permit ipv6 destination 2004::1
```

(2) 定义流分类和流行为

```
[Sysname] traffic classifier  statistic_1
[Sysname-classifier-static] if-match acl 3000
[Sysname] traffic behavior statistic_1
[Sysname-classifier-static] accounting packet
```

(3) 定义策略

```
[Sysname] qos policy statistic_1
[Sysname-classifier-static] classifier statistic_1 behavior statistic_1
```

(4) 将策略应用到端口入方向

```
[Sysname] interface gigabitehternet 8/0/1
[Sysname-GigabitEthernet8/0/1] qos apply policy statistic_1 inbound
```

(5) 检查入方向报文统计计数，可以通过 reset counter interface 命令清除计数

```
<Sysname> display qos policy interface gigabitethernet8/0/1
Interface: GigabitEthernet8/0/1
```

```
 Direction: Inbound

 Policy: statistic_1
  Classifier: statistic_1
    Operator: AND
    Rule(s) : If-match acl 3000
    Behavior: statistic_1
     Accounting Enable:
         1000 (Packets)
```

3. 报文计数分析

如果设备未收到 Ping 报文，请排查上游的相邻设备；如果设备发送的 Ping 报文计数正确，建议排查下游的相邻设备；如果 Ping 报文入出计数不正确，请参照继续排查。

14.5 MTU故障处理

14.5.1 故障描述

在网络中，由于不同厂商，甚至同一厂商不同型号的设备，对 MTU 的定义和 MTU 分片机制不尽相同，常出现 MTU 引起的网络问题，常表现为游戏卡、部分网站或链接打不开，Email 无法发送附件，部分网页或对话框无法打开等。遇到此类问题时，建议先检查是否接口 MTU 不匹配导致。

此外，OSPF、IS-IS、L2VPN、VPLS 等协议邻居关系无法建立，也可能是链路两端 MTU 值不一致导致。

14.5.2 故障处理步骤

对于 MTU 值问题处理，需要分析数据包传递的全路径上的 MTU 值设置。通用处理步骤如下：

(1) 分析数据转发路径。

(2) 检查数据包传递的全路径上各设备的出接口 MTU 值、站点间传输设备的 MTU 值。

(3) 逐段 ping 大包测试。大包长度分别为大于、小于、等于接口 MTU 值。

(4) 如果 ping 长度大于接口 MTU 时不通，小于等于接口 MTU 时能通，可初步认为是 MTU 问题。

(5) 分析报文头格式。

(6) 根据出问题的报文的最大长度修改 MTU。在修改 MTU 值时，需要注意不同厂商设备 MTU 值的定义。

设备 MTU 下发情况可以通过查询 Outlif 表项查看：

```
[Sysname-probe]display hardware internal l3 np fib 22.1.0.2 32 slot 2 chip 0

 The FTN/FIB table Handle<0x14> ECMPNum<0/1>!
 ChipID is 0
 LPM:
 LPM KEY: VPNID = 0  IP_Prefix = 22.1.0.2/4294967295
 LPM RESULT:
   00001403 0030d000
 Ipv4-route tag:
 Valid = 1     Parity = 1    Local = 0
```

```
 Drop = 0      ToHost = 0    Ecmp = 0
 Dft_Sys = 0   Dft_User = 0  NextHopIdxOrEcmpPtr = 20
 LifId = 12496     EcmpNum = 0
 FWD-FTN:
 FWD-FTN KEY: NextHopIdx = 0x14
 FWD-FTN RESULT:
 ECMP = 0  Th = 0  Normal = 1 Drop = 0
 OutlifId/ToHostId = 67607
 Dft_User = 0  Dft_Sys = 0
 Es = 0  Ts = 0  DhcpH = 0
 Local = 0  Parity = 1  V = 1 TTL = 255
 StackEnd = 0  Label_v = 0  Label = 0  Label_bak = 0
 Rd = 0  Rq = 0  Dscp = 0  QosLocalId = 0
 Outlif Table : KEY(outlifid = 67607) RESULT(00008201, 10030901, 00000000, 00000000, 00000000,
00000000, 05dc0000, fff10817)
 RES:
 un0.tunnel.uiReserve1:1 = 0
 un0.tunnel.uiBak:1 = 0
 un0.tunnel.uiBcm:1 = 0
 un0.tunnel.uiReserve2:1 = 0
 un0.tunnel.uiFwd:1 = 0
 un0.tunnel.uiEs:1 = 0
 un0.tunnel.uiTs:1 = 0
 un0.tunnel.uiReserve3:1 = 0
 un0.tunnel.uiMct:1 = 0
 un0.tunnel.uiGre:1 = 0
 un0.tunnel.uiIpt:1 = 0
 un0.tunnel.uiUdp:1 = 0
 un0.tunnel.uiReserve4:1 = 0
 un0.tunnel.ui6to4:1 = 0
 un0.tunnel.uiAuto:1 = 0
 un0.tunnel.uiMacInMac:1 = 0
 un0.tunnel.uiL3Port:1 = 1
……
 un5.v4ipt.uiIdentIndex:16 = 0
 un5.v4ipt.uiTos:8 = 0
 un5.v4ipt.uiTtl:8 = 0
 un5.v6ipt.uiV6Dip:32 = 0
 un5.minm.uiIsid:32 = 0
 un6.gen.uiMtu:16 = 1500
```

(7) 再次 ping 大包测试。

15 硬件转发故障

15.1 HG故障

15.1.1 故障描述

在现网业务中，设备如果正常运行，转发通道是不会丢包的。但是如果某个时间，转发路径出现大量丢包或者直接不通的情况，需要排查内部转发通道是否出现故障。缺省情况下，路由器上已使能互连单板之间的转发通道检查功能，互连的单板之间会定时检测互连的转发通道是否正常。

- 对于 CEPC 类单板、CMPE-1104 单板和 CSPC 单板可以通过 **display hardware internal hgmonitor info** 命令用来显示指定槽位单板的指定芯片的转发通道检测记录。

如设备转发链路异常，则显示信息中会有 Link 状态为 down 的记录，例如：

```
[Sysname-probe] display hardware internal hgmonitor info 4 0
  Link status change notice event:
  Unit    Port    Link    Clock                        Number
   0       hg0    up      08:08:03:755732 11/12/2014    1
   0       hg0    down    09:22:23:977918 11/12/2014    2
   0       hg1    up      08:12:19:398227 11/12/2014    1
   0       hg2    up      08:08:05:465720 11/12/2014    1
   0       hg3    up      08:12:21:391922 11/12/2014    1
```

可以通过查看 Link 状态为 down 的时间是否为发生故障的时间，如果时间一样则表示互连链路出现了故障。

- 对于 CSPEX-1204 单板可以通过 **display hardware internal forward fpga counter** 命令用来显示 CSPEX-1204 单板的转发通道检测记录。

如设备转发链路异常，则显示信息中 HG 部分会有 HG 端口状态为 down 的状态，例如：

```
[Sysname-probe] display hardware internal forward fpga counter slot 3
……
5 HG
------------------------------------------------------------------------------
-------------------------
      Value(HEX)           Value(DEC)     |  Address   |             Description
------------------------------------------------------------------------------
-------------------------
 0x0                 0                    | 0x005D0003 | SEND: HG_0 (DOWN)
 OUT
 0x0                 0                    | 0x00610003 | SEND: HG_1 (UP)
 OUT
 0x0                 0                    | 0x00650003 | SEND: HG_2 (DOWN)
 OUT
 0x0                 0                    | 0x00690003 | SEND: HG_3 (UP)
 OUT
------------------------------------------------------------------------------
-------------------------
 0x0                 0                    | 0x005D0005 | RECV: HG_0 (DOWN)
 IN
```

```
 0x0                0                    | 0x00610005 | RECV: HG_1 (UP)
 IN
 0x0                0                    | 0x00650005 | RECV: HG_2 (DOWN)
 IN
 0xA27              2599                 | 0x00690005 | RECV: HG_3 (UP)
 IN
--------------------------------------------------------------------------------
-------------------------
......
```

- 对于 CSPEX 类单板（除 CSPEX-1204 之外）、CEPC 类单板可以通过 **display hardware internal np serdes fabric status** 命令用来显示单板的转发通道检测记录。如设备转发链路异常，则显示信息中 HG 部分会有 HG 端口状态为 down 的状态，例如：

```
[Sysname-probe] display hardware internal np serdes fabric status slot 18 chip 0
SERDES  STATUS  NP_PORT  IF_NUM  PEER_SLOT  IF_TYPE
20      UP      106      10      23         40GE(UP)
21      UP      106      10      23         40GE(UP)
22      UP      106      10      23         40GE(UP)
23      UP      106      10      23         40GE(UP)
8       DOWN    104      8       23         40GE(DOWN)
9       DOWN    104      8       23         40GE(DOWN)
10      DOWN    104      8       23         40GE(DOWN)
11      DOWN    104      8       23         40GE(DOWN)

 Hg port tuning Record:
 Port     Event         Clock
  10 Tuning_start    09:41:03:039327
  10 Tuning_end(S)   09:41:04:118066
  10 Switch_Route    09:41:24:705325
   8 Tuning_start    09:41:04:118068
   8 Tuning_end(S)   09:41:05:195958
   8 Switch_Route    09:41:24:705327
```

- 转发链路检测失败，上报综合诊断模块，打印如下信息：

```
%@169696^Dec 21 16:04:06:987 2017 H3C SWFA/2/SWFA: -Chassis=1-Slot=15; 0x0F1E0000 [3060]:
 HG Monitor check fail: (SrcSlot[15].SrcChip[0])->(DstSlot[10].DstChip[0]))
```

上述信息表示转发链路可能存在故障，上报综合诊断模块进行分析。

```
%@169696^Dec 21 16:04:06:987 2017 H3C SWFA/2/SWFA: -Chassis=1-Slot=15; 0x0F1E0000 [3060]:
 HG Monitor check Recover: (SrcSlot[15].SrcChip[0])->(DstSlot[10].DstChip[0]))
```

上述信息表示转发链路可能存在故障，上报综合诊断模块进行修复。（仅适用于 CSPEX 类单板（CSPEX-1204、CSPEX-1104-E 和 CSPEX-1802X 除外）、SPE 类单板和 CEPC 类单板）

```
%@169696^Dec 21 16:04:06:987 2017 H3C SWFA/2/SWFA: -Chassis=1-Slot=15; 0x0F1E0000 [3060]:
 HG Monitor check clear: (SrcSlot[15].SrcChip[0])->(DstSlot[10].DstChip[0]))
```

上述信息表示转发链路故障已恢复，清除上报综合诊断模块的信息。

```
%@169694^Dec 21 16:04:06:927 2017 H3C SWFA/2/SWFA: -Chassis=1-Slot=15; 0x0F1E0000 [401]:
 16:04:06:927390 12/21/2017: unit 0 port 23 is isolated by local.
%@169695^Dec 21 16:04:06:859 2017 H3C SWFA/2/FWD: -Chassis=1-Slot=10; 0x0FD93001 [377]:
 16:04:06:859252 12/21/2017: unit 0 port 67 isolated by rpc.
```

上述信息表示转发链路可能存在故障，上报综合诊断模块对此条链路进行隔离。

```
%@169694^Dec 21 16:04:06:927 2017 H3C SWFA/2/SWFA: -Chassis=1-Slot=15; 0x0F1E0000 [401]:
 16:04:06:927390 12/21/2017: unit 0 port 23 is fault, not isolated by local.
%@169695^Dec 21 16:04:06:859 2017 H3C SWFA/2/FWD: -Chassis=1-Slot=10; 0x0FD93001 [377]:
 16:04:06:859252 12/21/2017: unit 0 port 67 is fault, not isolated by rpc.
```

上述信息表示转发链路可能存在故障，且无备份链路，上报综合诊断模块对此条链路进行隔离。

```
%Aug 13 15:58:18:186 2019 H3C DIAG/4/DIAG_AI: -MDC=1; Board fault: chassis 0 slot 8 or chassis
0 slot 12, please check them
```

上述输出信息表示多个槽位可能存在故障。

```
%Aug 13 15:58:18:186 2019 H3C DIAG/4/DIAG_AI: -MDC=1; Board fault: chassis 0 slot 8, please
check it
```

上述输出信息表示单个槽位可能存在故障。

15.1.2 故障处理步骤

由于主控板和交换网板分离，交换网板负责业务流量转发，流量在多块交换网板之间负载分担，而主控板仅负责控制管理，不参与业务流量转发。

(1) CR16006-F 路由器上使用的是交换网板型号为 CSFC-04-1、CSFC-04-2、CSFC-04-3 和 CSFC-04-4，请直接联系技术支持人员；

(2) 如果流量的入端口和出端口在同一 CSPC 单板或 CMPE-1104 单板上，请直接联系技术支持人员；

(3) 如果流量的入端口和出端口在同一 CSPEX 类单板、CEPC 类单板上或者流量的入端口和出端口不在同一单板上，请在系统视图下执行 **switch-fabric isolate** 命令逐块隔离交换网板（确保交换网板数量大于等于 1，且不能只剩余第二块交换网板），观察交换网板隔离后故障是否消失。以 CR16010-F 为例说明网板隔离步骤，其中 10～13 槽位为交换网板：

a. 隔离 10 号槽位交换网板，隔离后等待一段时间（大约等待 1 分钟），观察故障是否消失。

b. 执行 **undo switch-fabric isolate** 命令取消 10 号槽位交换网板隔离，待网板重启 Normal 后，再等待一段时间（大约等待 3 分钟以上），隔离 11 槽位网板并观察故障是否消失。

c. 按照上面的方法，依次隔离 12～13 槽位网板，直到所有网板隔离确认一遍。

(4) 如果隔离某块交换网板后故障消失，说明该交换网板故障；如果所有交换网板隔离一遍后故障仍存在，那么应该为接口板故障导致，建议将该接口板上的业务转移到其他接口板之后再通过单板隔离或更换接口板的方式进一步确认。

(5) 如仍还无法排查，请直接联系技术支持人员。

对于上报综合诊断模块，打印的信息的故障处理步骤如下：

(1) 通过 **display hardware-failure-detection** 命令查看设备的硬件故障检测和修复信息。

(2) 排查互连两端 HG 状态是否为正常 Up，如果是有互连 HG 状态是 Down，表明存在硬件故障。

(3) 如仍还无法排查，请直接联系技术支持人员。

15.2 FMEA故障

15.2.1 故障描述

FMEA 是硬件器件失效检测，出现异常时 logfile 打印带有 FMEA 或 Hardware error 标记的诊断信息，如

```
%@3458327%Jan  2 23:16:42:223 2020 H3C DIAG/2/FMEA: -Chassis=2-Slot=3; Hardware error detected on chassis 2 slot 3.
```

15.2.2 故障处理步骤

FMEA 检测覆盖主控板、接口板和网板，检测到故障输出到诊断日志，默认配置下不会执行动作，仅做信息输出。如果诊断信息持续打印，请注意观察是否有其他业务异常，同时将故障信息发送给技术支持人员帮助分析。