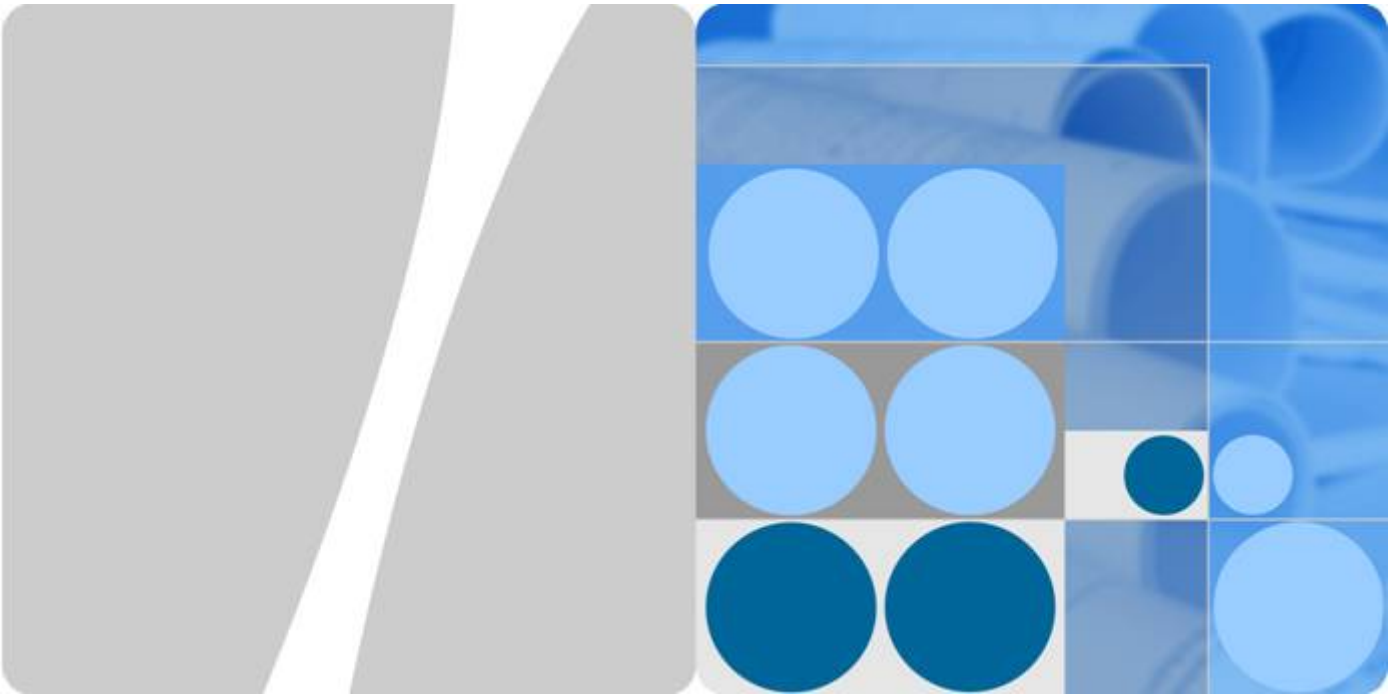


HUAWEI NetEngine80E/40E 路由器

V600R003C00

故障处理-VPN

文档版本　02

发布日期　2011-09-10

华为技术有限公司

商标声明


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

注意

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

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

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

前 言

概述

说明

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

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

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

产品版本

与本文档相对应的产品版本如下所示。

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

读者对象

本文档主要适用于以下工程师：

- 系统维护工程师
- 调测工程师
- 网络监控工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

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

命令行格式约定

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

修订记录

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

文档版本 02 (2011-09-10)

第二次正式发布，相对于上一版本无变更。

文档版本 01 (2011-05-30)

第一次正式发布

目 录

1 L3VPN 故障处理

关于本章

介绍了 L3VPN 故障常见的原因和定位思路。

1.1 私网流量中断的定位思路

1.1.1 常见原因

BGP 私网流量中断是指在 BGP 邻居正常的情况下依赖 BGP 私网路由的流量的中断。

本类故障的常见原因主要包括：

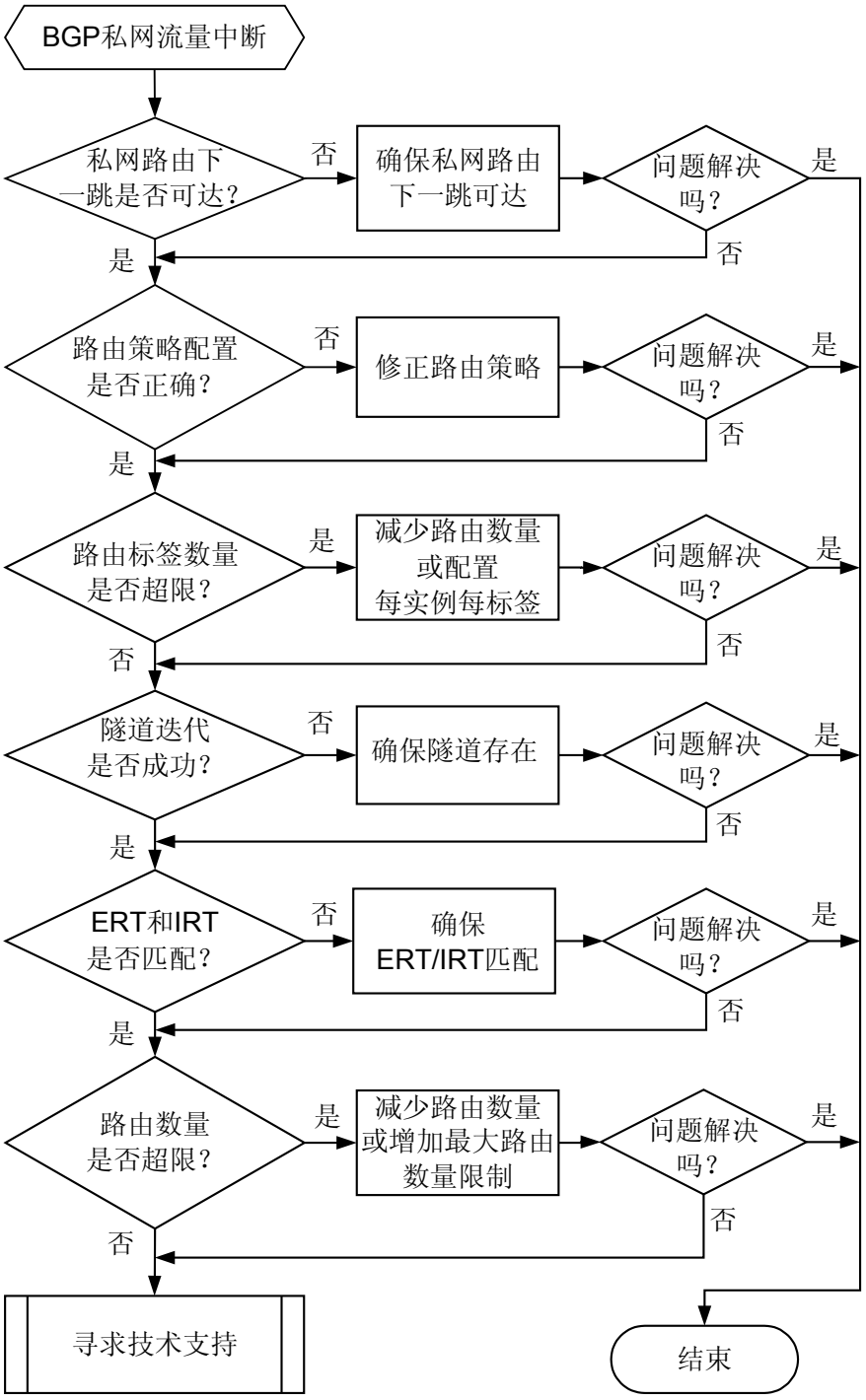
- 路由下一跳不可达导致路由不活跃。
- 路由策略配置不当导致路由无法发布/接收。
- 标签超限导致私网路由无法发布。
- 私网路由迭代不到隧道导致路由不活跃。
- ERT/IRT 不匹配导致路由无法交叉到私网路由表中。
- 路由超限导致收到的路由被丢弃。

1.1.2 故障诊断流程

在配置 BGP 协议后发现 BGP 私网流量中断。

可按照故障诊断流程图 1-1 排除故障。

图 1-1 BGP 私网流量中断故障诊断流程图



1.1.3 故障处理步骤

背景信息

说明

请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

操作步骤

步骤 1 检查路由下一跳是否可达

在路由的发送端(本端 PE)执行 **display bgp vpnv4 vpn-instance** *vpn-instance-name* **routing-table** *ipv4-address* [*mask* | *mask-length*]命令查看目标路由（*ipv4-address* 表示目标路由前缀），确认路由是否存在。

- 如果路由不存在，请确认 CE 路由是否发布到 PE。
- 如果路由存在，请按照下面示例确认路由是否活跃。

以 1.1.1.1/32 这条路由举例，下面命令显示此路由是活跃的（valid）优选的（best），此路由的 BGP 下一跳为 3.3.3.3（Original nexthop），经过迭代后的下一跳为 20.1.1.2（Relay IP Nexthop）。

```
<HUAWEI> display bgp vpnv4 vpn-instance vpna routing-table 1.1.1.1

 BGP local router ID : 20.1.1.2
 Local AS number : 100
 Paths:   1 available, 1 best, 1 select
 BGP routing table entry information of 1.1.1.1/32:
 From: 20.1.1.1 (1.1.1.1)
 Route Duration: 00h00m03s
 Relay IP Nexthop: 20.1.1.2
 Relay IP Out-Interface: Pos1/0/0
 Original nexthop: 3.3.3.3
 Qos information : 0x0
 AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, valid, internal, best, select,
active, pre 255
 Not advertised to any peer yet
```

- 如果目标路由不活跃，请确认 IP 路由表中是否存在到 BGP 下一跳（Original nexthop）的路由，如果不存在说明 BGP 路由不发布是由于路由下一跳不可达导致，请确认为何没有到 BGP 下一跳（Original nexthop）的路由（一般属于 IGP 或静态路由问题）。
- 如果目标路由活跃，却没有被优选（没有 best），请确认 IP 路由表中是否有其他协议优先级（preference）更高的路由存在。如果有请确认是否需要将此路由引入到 BGP 中或调整提协议优先级。 如果没有请联系华为技术工程师。

  说明

  在 BGP 路由表中同一前缀可能有多跳路由，其中最多只有 1 条路由会被优选（best），并且只有被优选的路由才会被添加到 IP 路由表中并发送给其他邻居。BGP 路由与其他协议路由进行比较时是靠协议优先级（preference）来决定哪个更优的。

- 如果目标路由活跃且被优选，但没有显示发送给路由接收端，请执行**步骤 2**（重点检查路由发送端的出口策略）。

在路由接收端执行 **display bgp vpnv4 all routing-table** *network* { *mask* | *mask-length* }查看是否收到目标路由。

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

步骤 2 检查路由策略是否正确

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

说明

由于是私网流量中断，只需要关注 BGP-VPNv4 地址族或 BGP-VPN 实例地址族下的邻居。

```
<HUAWEI> display current-configuration configuration bgp
#
bgp 100
 peer 1.1.1.1 as-number 200
 #
 ipv4-family unicast
  undo synchronization
  peer 1.1.1.1 enable
 #
 ipv4-family vpnv4
  policy vpn-target
  peer 1.1.1.1 enable
  peer 1.1.1.1 filter-policy acl-name acl-name import
  peer 1.1.1.1 filter-policy acl-name acl-name export
  peer 1.1.1.1 as-path-filter 1 import
  peer 1.1.1.1 as-path-filter 1 export
  peer 1.1.1.1 ip-prefix prefix-name import
  peer 1.1.1.1 ip-prefix prefix-name export
  peer 1.1.1.1 route-policy policy-name import
  peer 1.1.1.1 route-policy policy-name export
 #
 ipv4-family vpn-instance vpna
  peer 10.1.1.1 as-number 300
  peer 10.1.1.1 filter-policy acl-name acl-name import
  peer 10.1.1.1 filter-policy acl-name acl-name export
  peer 10.1.1.1 as-path-filter 1 import
  peer 10.1.1.1 as-path-filter 1 export
  peer 10.1.1.1 ip-prefix prefix-name import
  peer 10.1.1.1 ip-prefix prefix-name export
  peer 10.1.1.1 route-policy policy-name import
  peer 10.1.1.1 route-policy policy-name export
#
return
```

- 如果两端配置了出口/入口策略，则需要确认这些策略是否会把目标路由过滤掉，导致该路由无法正常收发。路由策略的具体配置请参见《HUAWEI NetEngine80E/40E 配置指南-IP 路由》。
- 如果两端没有配置相应的出口/入口策略，请直接执行**步骤 3**。

步骤 3 检查是否迭代不到隧道导致路由不活跃

在路由的接收端（远端 PE）执行 **display bgp vpnv4 all routing-table** *ipv4-address* [*mask* | *mask-length*]命令查看目标路由，确认 VPNv4 路由是否可以迭代到隧道。

以路由 50.1.1.2/32 为例，显示信息中 Relay Tunnel Out-Interface 和 Relay token 字段不为空表示该路由可以迭代到隧道。

```
<HUAWEI> dis bgp vpnv4 all routing-table 50.1.1.2
BGP local router ID : 2.2.2.2
 Local AS number : 100

 Total routes of Route Distinguisher(1:2): 1
 BGP routing table entry information of 50.1.1.2/32:
 Label information (Received/Applied): 13316/NULL
 From: 1.1.1.1 (1.1.1.1)
 Route Duration: 00h00m08s
 Relay IP Nexthop: 20.1.1.1
 Relay IP Out-Interface: Pos1/0/0

 Relay Tunnel Out-Interface: Pos1/0/0

 Relay token: 0x1002
 Original nexthop: 1.1.1.1
 Qos information : 0x0
 Ext-Community:RT <1 : 1>
 AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, valid, internal, best, select,
pre 255
 Not advertised to any peer yet
```

```
Total routes of vpn-instance vpna: 1
BGP routing table entry information of 50.1.1.2/32:
Label information (Received/Applied): 13316/NULL
From: 1.1.1.1 (1.1.1.1)
Route Duration: 00h00m07s
Relay Tunnel Out-Interface: Pos1/0/0

Relay token: 0x1002
Original nexthop: 1.1.1.1
Qos information : 0x0
Ext-Community:RT <1 : 1>
AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, valid, internal, best, select,
active, pre 255
Not advertised to any peer yet
```

- 如果迭代不到隧道，请执行 **display ip vpn-instance verbose [*vpn-instance-name*]**命令检查 Tunnel Policy 字段。如果没有显示该字段，表示没有为 VPN 实例配置隧道策略，VPN 实例使用的隧道为 LDP LSP。如果 VPN 实例使用 MPLS-TE 隧道需要配置隧道策略。Tunnel Policy 字段值表示 VPN 实例使用隧道策略，可以在隧道策略视图下执行 **display this** 检查隧道策略的配置。

  ```
  [HUAWEI-tunnel-policy-p1] display this
  #
  tunnel-policy p1
   tunnel select-seq cr-lsp load-balance-number 1
  #
  ```

  说明

  如果隧道策略下配置了 **tunnel binding destination** *dest-ip-address* **te** { **tunnel** *interface-number* }，还需要在 Tunnel 接口下使能 **mpls te reserved-for-binding** 命令。

  如果隧道没有 Up，请参考 **LDP LSP Down 的定位思路**或者 **TE Tunnel 状态为 Down 的定位思路**继续定位，使隧道状态 Up。
- 如果迭代到隧道，请直接执行**步骤 4**。

步骤 4 检查是否 ERT/IRT 不匹配导致路由无法交叉到私网路由表中

在路由的发送端（本端 PE）/接收端（远端 PE）执行 **display current-configuration configuration vpn-instance** 命令查看是否本端 VPN 实例的 ERT 与远端 VPN 实例的 IRT 不匹配，导致路由发送到远端 PE 后无法交叉到远端 VPN 实例中。

export-extcommunity 表示 ERT， import-extcommunity 表示 IRT。

```
<HUAWEI> display current-configuration configuration vpn-instance
#
ip vpn-instance vpna
 route-distinguisher 1:1
 apply-label per-instance
 vpn-target 1:1 export-extcommunity
 vpn-target 1:1 import-extcommunity
ip vpn-instance vpnb
 route-distinguisher 1:2
 vpn-target 1:1 export-extcommunity
 vpn-target 1:1 import-extcommunity
#
return
```

- 如果 ERT 和 IRT 不匹配，请在 VPN 实例下配置匹配的 vpn-target。
- 如果 ERT 和 IRT 匹配，请执行**步骤 5**。

步骤 5 检查是否标签超限

首先在路由发送端（本端 PE）确认是否使能了 mpls。然后，使用 **display bgp vpnv4 all routing-table** *ipv4-address* [*mask* | *mask-length*]查看目标路由，确定该目标路由是否分到私网标签。

如果显示信息中没有 Label information 字段，则可能是标签资源不足，导致无法为该路由申请到标签而不会给其它对等体。

```
<HUAWEI> display bgp vpnv4 all routing-table 100.1.1.1

 BGP local router ID : 10.1.1.2
 Local AS number : 100

 Total routes of Route Distinguisher(1:1): 1
 BGP routing table entry information of 100.1.1.0/24:
 Imported route.
 Label information (Received/Applied): NULL/13312


 From: 0.0.0.0 (0.0.0.0)
 Route Duration: 00h21m24s
 Direct Out-interface: NULL0
 Original nexthop: 0.0.0.0
 Qos information : 0x0
 Ext-Community:RT <1 : 1>
 AS-path Nil, origin incomplete, MED 0, pref-val 0, valid, local, best, select, pre 255
 Advertised to such 1 peers:
    1.1.1.1

 Total routes of vpn-instance vpna: 1
 BGP routing table entry information of 100.1.1.0/24:
 Imported route.
 From: 0.0.0.0 (0.0.0.0)
 Route Duration: 00h21m24s
 Direct Out-interface: NULL0
 Original nexthop: 0.0.0.0
 Qos information : 0x0
 AS-path Nil, origin incomplete, MED 0, pref-val 0, valid, local, best, select, pre 60
 Not advertised to any peer yet
```

- 如果是标签不足，可在 VPN 实例视图下通过命令 **apply-label per-instance** 配置每实例每标签，来减少标签的使用量。也可以通过路由聚合来减少路由数量。
- 如果标签没有超限，请执行**步骤 6**。

步骤 6 检查路由是否超限

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

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

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

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

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

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

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

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

说明

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

步骤 7 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

1.1.4 相关告警与日志

相关告警

BGP_1.3.6.1.4.1.2011.5.25.177.1.3.1 hwBgpPeerRouteNumThresholdExceed

相关日志

BGP/3/ROUTPRIX_EXCEED

1.2 相关案例

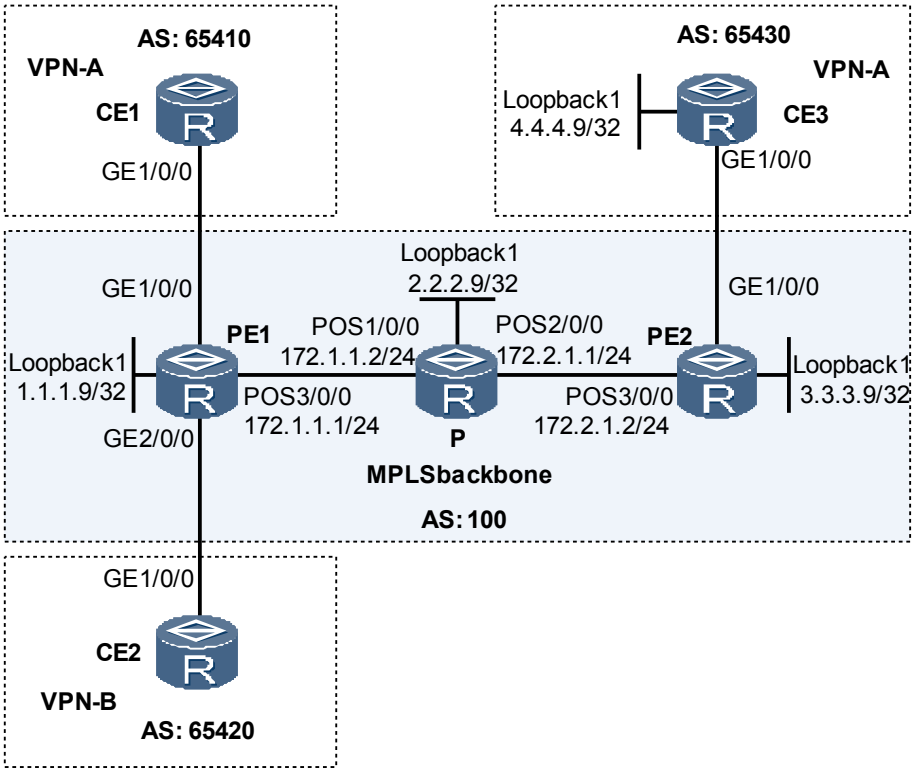
1.2.1 已配置相同 RT 的不同 VPN 之间不能互通

网络环境

在图 1-2 的网络中配置 BGP/MPLS VPN 业务，CE1 与 CE3 属于 VPN-A，CE2 属于 VPN-B。由于某特殊业务的需求，在 VPN-A 和 VPN-B 上配置相同的 VPN Target，实现不同 VPN 间互通。

配置完成后，CE1 可以 Ping 通 VPN-A 中的 4.4.4.9,但 CE2 无法 Ping 通 VPN-A 中的 4.4.4.9，即 VPN-B 与 VPN-A 未实现互通。

图 1-2 BGP/MPLS VPN 业务组网图



故障分析

1. 在 PE1 上执行 **display bgp peer** 或 **display bgp vpnv4 all peer** 命令，显示结果中的 Status 项为“Established”，表示 PE 之间的 BGP 对等体已成功建立。
2. 依次在 PE1、P、PE2 上执行 **display mpls ldp session** 命令，显示结果中的 Status 项为“Operational”，表示 PE1 与 P、P 与 PE2 之间的 LDP 会话已成功建立。
3. 在 PE1 和 PE2 上分别执行 **display ip vpn-instance verbose** 命令，查看到 VPN-A 和 VPN-B 的 VPN Target 是相同的。
4. 依次在 PE1、P、PE2 上执行 **display mpls ldp lsp** 命令，检查标签分配情况。发现 PE1 与 PE2 之间的公网标签、私网标签均已分配。
5. 在 PE 上执行 **display ip interface brief** 查看接口 IP 地址的配置，发现 VPN-B 和 VPN-A 绑定了相同的 IP 地址。

```
[PE1] display ip interface brief
......
Interface                         IP Address/Mask      Physical   Protocol
......
Gigabitethernet1/0/0              10.1.1.2/30          up         up
Gigabitethernet2/0/0              10.1.1.2/30          up         up
......
```

在 PE 上的路由交叉过程中，VPN-B 进程中只选择了本地直连接口路由，未选择通往 VPN-A 的 BGP 路由。并且由于不同 VPN 间绑定了相同的 IP 地址不会显示 IP 地址冲突告警，所以配置成功，但 VPN 未实现互通。

操作步骤

步骤 1 在 PE1 和 CE2 上执行以下操作，执行命令 **system-view**，进入系统视图。

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

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置接口的 IP 地址。

说明

将 VPN-A 和 VPN-B 绑定不同的 IP 地址。

步骤 4 执行命令 **quit**,退出接口视图

步骤 5 执行命令 **bgp** *as-number*，进入 BGP 视图。

步骤 6 执行命令 **ipv4-family vpn-instance** *vpn-instance-name*，进入 BGP VPN 实例视图。在 CE2 上不需要执行此步骤，直接进入 BGP 视图即可。

步骤 7 执行命令 **undo peer** *ipv4-address* ，删除原来的对等体。

步骤 8 执行命令 **peer** *ipv4-address* **as-number** *as-number*，配置新的 BGP 对等体。

完成上述操作后，在 CE2 上 ping 对端 CE3，可以 ping 通，故障排除。

----结束

案例总结

PE 上有种特殊的路由——来自本地 CE 的属于不同 VPN 的路由。对于这种路由，如果其下一跳直接可达或可迭代成功，PE 会将其与本地其他 VPN 实例的 Import Target 属性匹配，如果匹配成功，PE 就将这条路由加入本地其它 VPN 的路由表，该过程称为本地交叉。

本案例由于误将本地不同的 VPN 绑定了相同的 IP 地址，在本地路由交叉过程中，互访的路由不被优选。虽然不同 VPN 之间的 VPN Target 匹配成功，但是仍然无法互通。将 IP 地址修改为不同即可解决问题。

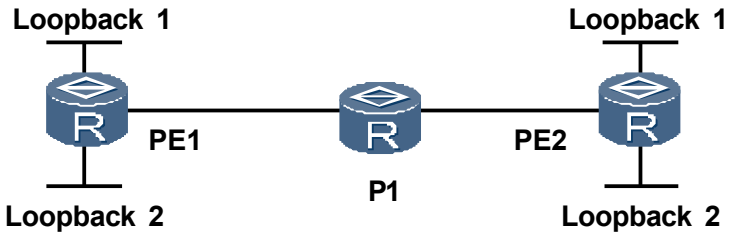
1.2.2 PE 私网之间无法 ping 通

网络环境

在图 1-3 的网络中配置 BGP/MPLS VPN 业务，两台 PE 之间无法交换 VPN 私网路由，相互之间 ping 不通。

在两台 PE 上分别建立两个 Loopback 接口。Loopback1 接口为公网接口，IP 地址分别为 1.1.1.1/32 和 1.1.1.2/32。Loopback2 接口绑定 VPN 实例 test，且 IP 地址分别为 10.1.1.1/24 和 10.1.1.2/24。

图 1-3 BGP/MPLS VPN 组网图



故障分析

1. 在 PE1 和 PE2 上执行 **display ip routing-table** 命令，检查是否有去往对端网段的路由。可以看到路由表中有去往对端 Loopback1 接口网段的路由。
2. 在 P1 上执行 **display mpls ldp peer** 命令，看到成功建立了 **PeerID** 为 1.1.1.1 和 1.1.1.2 的 LDP 会话。在 P1 上执行 **display mpls lsp** 命令，看到成功建立了 **FEC** 为 1.1.1.1 和 1.1.1.2 的 LSP。
3. 在 PE1 或 PE2 上执行 **display bgp peer** 命令，检查邻居是否正常建立。看到与 1.1.1.2 或 1.1.1.1 的对等体关系 **State** 显示为 **Established**，表示 IBGP 对等体关系建立成功。
4. 在 PE1 或 PE2 上执行 **display bgp vpnv4 all peer** 命令，检查 VPNv4 的对等体信息。看到与 1.1.1.2 或 1.1.1.1 的对等体关系 **State** 显示为 **Established**，表示邻居正常建立并且正常向外发送私网路由。
5. 排除以上故障原因后，在 PE1 和 PE2 上执行 **display ip routing-table vpn-instance** 命令查看私网路由表中的路由。发现只有一条路由：**10.1.1.0/24 Direct**，是路由设备自身 Loopback2 接口路由。同时发现掩码是 24 位，而不是 32 位。

   这样的话两台 PE 的 Loopback2 接口地址便在同一网段内了。其实设备已经收到了私网路由，但是与其自身 Loopback2 接口地址在同一网段，相当有两条相同的路由，一条为直连路由，一条为 BGP 路由。此时设备会优选直连路由创建到自身路由表，所以私网路由表中没有 BGP 私网路由。导致 PE 间无法 ping 通。

操作步骤

步骤 1 在 PE1 和 PE2 上分别执行下列步骤，执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface loopback** *loopback-number*，进入 Loopback2 接口视图。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置接口的 IP 地址。

说明

将 Loopback 接口 IP 地址的掩码改为 32 位。

完成上述操作后，两台 PE 之间可以 ping 通，故障排除。

----结束

案例总结

如果到同一个网段有两条相同的路由，设备只会选择其中之一更新到路由表。

1.2.3 设备公私网不能互访

网络环境

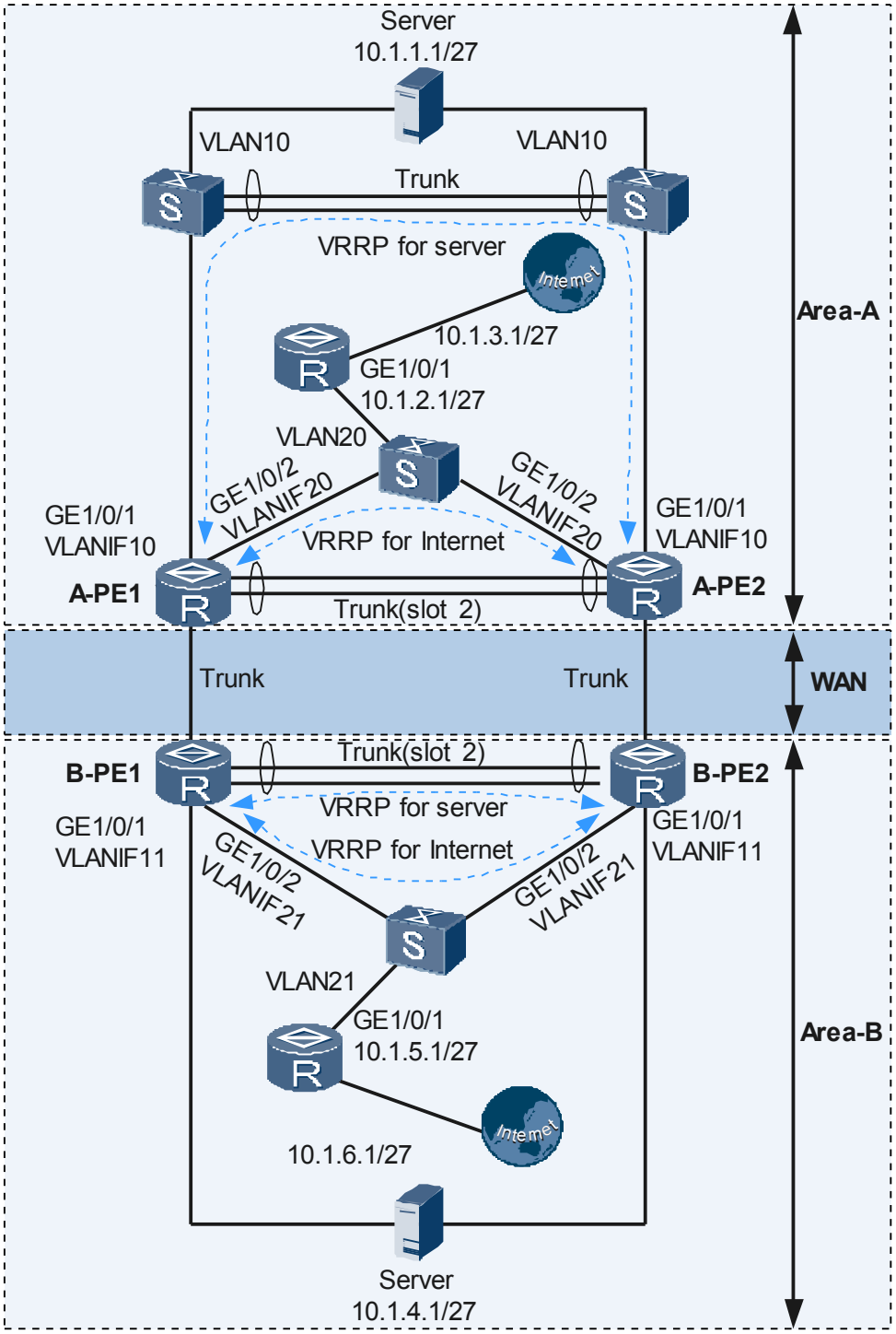
如图 1-4 所示，网络分为两个局点：Area-A 和 Area-B（以下分别简称 A 区域和 B 区域）。每个区域都有两台 PE，并且在每个 PE 上分别为应用系统和 Internet 业务配置 VRRP 保护，如图 1-4 中蓝色虚线所示。

在每个区域的 PE 上配置 VPN 与 Internet 互联功能后，发现 B 区域的公私网互访不成功，而同样的配置在 A 区域却是可以的。两个区域的业务模型一样，唯一的差别就是相对于 B 区域，A 区域的 PE 和业务系统间通过两台交换机进行二层透明传输。

说明

A 区域和 B 区域的应用系统（Server）有两个接口。两个接口是主备关系，备用接口处于 inactive 状态，不响应任何协议报文。

图 1-4 设备公私网不能互访组网图



说明

两个区域的 IP 地址都是 10.X.X.X，公私网的区分在于是否捆绑了 VPN。

故障分析

因 VPN 公私网互访是比较简单的功能，所以按照下面的思路进行分析：

1. 执行命令 **display current-configuration** 检查设备的配置，发现配置没有问题。如**表 1-1** 所示:

表 1-1 PE 的关键配置

	A-PE1	A-PE2	B-PE1	B-PE2
路由配置	# ip route-static 10.1.1.0 255.255.255.224 Vlanif10 10.1.1.10 ip route-static vpn-instance Media 10.1.3.0 255.255.255.224 10.1.2.1 public #	# ip route-static 10.1.1.0 255.255.255.224 Vlanif10 10.1.1.1 ip route-static vpn-instance Media 10.1.3.0 255.255.255.224 10.1.2.1 public #	# ip route-static 10.1.4.0 255.255.255.224 vpn-instance Media 10.11.4.10 ip route-static vpn-instance Media 10.1.6.0 255.255.255.224 10.1.5.1 public #	# ip route-static 10.1.4.0 255.255.255.224 vpn-instance Media 10.11.4.10 ip route-static vpn-instance Media 10.1.6.0 255.255.255.224 10.1.5.1 public #
VLANIF10	# interface Vlanif10 ip binding vpn-instance Media ip address 10.1.1.2 255.255.255.224 vrrp vrid 10 virtual-ip 10.1.1.10 vrrp vrid 10 priority 120 #	# interface Vlanif10 ip binding vpn-instance Media ip address 10.1.1.3 255.255.255.224 vrrp vrid 10 virtual-ip 10.1.1.10 #	-	-
VLANIF20	# interface Vlanif20 ip address 10.1.2.2 255.255.255.224 vrrp vrid 20 virtual-ip 10.1.2.10 vrrp vrid 20 priority 120 #	# interface Vlanif20 ip address 10.1.2.3 255.255.255.224 vrrp vrid 20 virtual-ip 10.1.2.10 #	-	-

	A-PE1	A-PE2	B-PE1	B-PE2
VLANIF11	-	-	# interface Vlanif11 ip binding vpn-instance Media ip address 10.1.4.2 255.255.255.224 vrrp vrid 11 virtual-ip 10.1.4.10 vrrp vrid 11 priority 120 #	# interface Vlanif11 ip binding vpn-instance Media ip address 10.1.4.3 255.255.255.224 vrrp vrid 11 virtual-ip 10.1.4.10 #
VLANIF21	-	-	# interface Vlanif21 ip address 10.1.5.2 255.255.255.224 vrrp vrid 21 virtual-ip 10.1.5.10 vrrp vrid 21 priority 120 #	# interface Vlanif21 ip address 10.1.5.3 255.255.255.224 vrrp vrid 21 virtual-ip 10.1.5.10 #

并且 A 区域与 B 区域的配置是类似的，但 A 区域的设备却能正常运行，也能说明配置思路是正确的。

2. 在 B-PE2 上，执行命令 **display ip routing-table** 查看公网中 10.1.4.1 的路由信息，发现去往 10.1.4.1 的路由是一个网段路由，出接口是 VLANIF11。B-PE2 选择的是 VLAN11 的一个成员接口 GE1/0/1 作为实际的出接口。
3. 执行命令 **display arp slot 1** 查看接口 GE1/0/1 的 ARP 表项，发现没有 10.1.4.1 的 ARP 表项。
4. 执行命令 **display arp slot 2** 查看 2 号接口板的 ARP 表项，发现 10.1.4.1 的 ARP 表项的出接口是 Eth-trunk（该 Trunk 是两台 PE 间的二层链路，使用的是 2 号槽位，承载 VRRP 的协议报文）。因此，可以确定该故障是由于没有 ARP 表项导致公网无法访问私网。
5. 1 号接口板没有 ARP 表项的原因是：

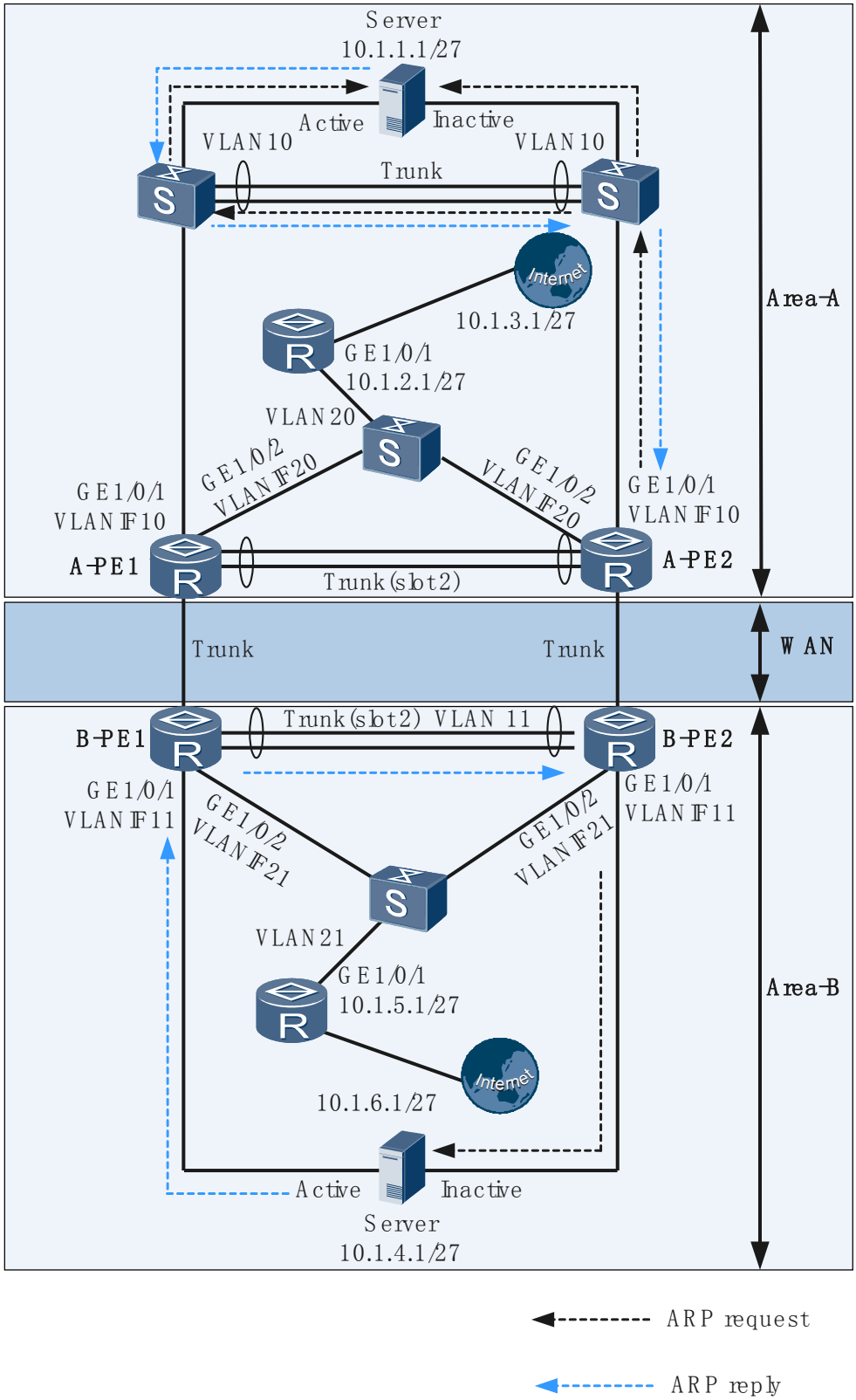
   (1) B 区域的 PE 发生故障时，由于 PE 上配置的静态路由是 10.1.4.0 这个网段路由，出接口是 VLANIF11，因此在公网中无法获得具体的主机路由。

   (2) 当公网需要访问 10.1.4.1 时，B-PE2 发现出接口是 VLANIF11，由于配置了静态路由（**ip route-static 10.1.4.0 255.255.255.224 vpn-instance Media 10.1.4.10**），因此 B-PE2 只能随机选择 VLANIF11 的一个成员接口（这里 B-PE2 选择的出接口是 GE1/0/1），然后再从接口 GE1/0/1 发送 ARP 请求和学习相应的 ARP 表项。

   (3) 业务系统（Server 10.1.4.1）有两个主备关系的接口。主用接口（Active）连接 B-PE1，备用接口（Inactive）连接 B-PE2。备用接口不处理任何协议报文。因此，业务系统（Server 10.1.4.1）从备用接口收到 B-PE2 的 ARP 请求报文后，不会从备用接口回应 ARP 请求。这样，B-PE2 的接口 GE1/0/1 虽然与 10.1.4.1 直连，但是却不能收到 10.1.4.1 的 ARP 应答报文，B-PE2 的 GE1/0/1 接口上就无法生成 10.1.4.1 对应的 ARP 表项。由于没有 ARP 表项，而导致公网无法访问私网。

(4) 业务系统（Server 10.1.4.1）的 ARP 应答报文只会从 Server 的主用接口发送给 B-PE1 的接口 GE1/0/1，该接口加入了 VLAN11，并且 B-PE1 的 Eth-trunk 也加入了 VLAN11。ARP 应答报文会通过 Eth-trunk 接口，发送到 B-PE2 的 Eth-trunk 接口上，因此，在 B-PE2 上查看 2 号接口板的 ARP 表项，会发现 10.1.4.1 的 ARP 表项的出接口是 Eth-trunk。如**图 1-5** 所示。

图 1-5 ARP 请求与应答组网图



而 A 区域的公网私网可以互通，原因就在于 PE 和 Server 之间有交换机，进行二层透明传输。如图 1-5 所示。

通常情况下，VLANIF 接口学习到 ARP 表项后会生成一条 32 位主机路由，用于 VLANIF 选择出接口。而当 PE 配置了静态路由后，VLANIF 只能随机选择出接口，无法正确生成的 32位主机路由信息。

综上所述，此例中的 PE 上配置静态网段路由后，由于出接口是 VLAINF 接口，PE 只会随机选中 VLANIF 的一个成员接口发送报文。此时如果 PE 选择的接口不正确，就会出现互访不通的情况(本例中，ARP 表项学习都是正常的，问题就出在配置了静态网段路由)。

操作步骤

步骤 1 执行命令 **system-view**，进入 B 区域 PE 的系统视图。

步骤 2 执行命令 **undo ip route-static 10.1.4.0 255.255.255.224 vpn-instance Media 10.1.4.10**，在 PE 上删除已配置的公网访问私网的静态路由。

步骤 3 执行命令 **ip route-static 10.1.4.1 255.255.255.255 vpn-instance Media 10.1.4.1**，在 B 区域 PE 上重新配置公网访问私网的静态路由。

完成上述配置后，发现设备的公私网可以互通，故障排除。

----结束

案例总结

由此可知，配置 VPN 的公网私网互通时，当 VLANIF 作为出接口时，不能配置网段路由，而需要配置 32 位主机路由，从而规避配置静态路由后，VLANIF 随机选择出接口带来的问题。

1.2.4 全连接组网 NSSA 区域 ABR 与 BAS 链路中断导致部分 VPN 业务中断

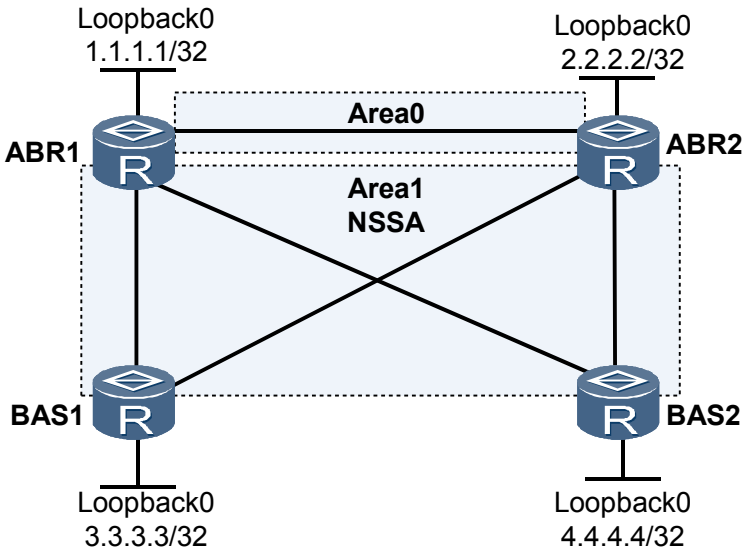
网络环境

如图 1-6 所示，ABR1、ABR2、BAS1 和 BAS2 建立全连接组网。所有的路由器都运行 OSPF，整个自治系统划分为 2 个区域，其中 ABR1 和 ABR2 互联为骨干区域 Area0，2 台 ABR 与 2 台 BAS 互联区域 Area1 配置为 NSSA 区域。

所有链路启用 MPLS LDP，承载 MPLS L3VPN 业务。但由于 BAS 性能有限，所以对其 LSP 分配进行限制，不承担 transit 节点的角色。

当 BAS1 与 ABR1 链路中断时，ABR1 与 BAS1 的 VPN 业务中断。

图 1-6 配置 OSPF NSSA 区域组网图



故障分析

1. 在 ABR1 上执行 **display ospf routing** 命令，查看的 OSPF 路由信息，可以看到 ABR1 的 Loopback0 接口在 Area0 区域发布。因为 OSPF 路由选路，优选同一区域内的 OSPF 路由，所以 ABR1 到 BAS1 的 IGP 路径为 ABR1-->BAS2-->ABR2-->BAS1。
2. 在 BAS2 上执行 **display mpls ldp lsp** 命令，检查标签分配情况，可以看到 LSP 的入/出标签值 **In/OutLabel** 为 NULL/**，即 BAS2 没有给上一跳 ABR1 分配标签。这是由于 BAS2 不作为 transit 节点，不会为 ABR1 的 Loopback0 口分配标签，因此 BAS2 无法收到 ABR1 的 MPLS 公网标签，导致 VPN 业务中断。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number.subinterface-number*，新建一个子接口。

步骤 3 执行命令 **ip address**，配置接口的 IP 地址。

步骤 4 执行命令 **quit**，退回到系统视图。

步骤 5 执行命令 **ospf** *process-id* ，进入 OSPF 视图。

步骤 6 执行命令 **area** 1，进入 OSPF 区域 1 视图。

步骤 7 执行命令 **network** *ip-address wildcard-mask*，将新建的子接口划分到 Area1 中。

步骤 8 执行命令 **nssa**，配置 Area1 区域为 NSSA 区域。

完成上述操作后，在 ABR1 上 ping BAS1，可以 ping 通，故障排除。

----结束

案例总结

设备 Loopback 接口应发布到正确的区域。

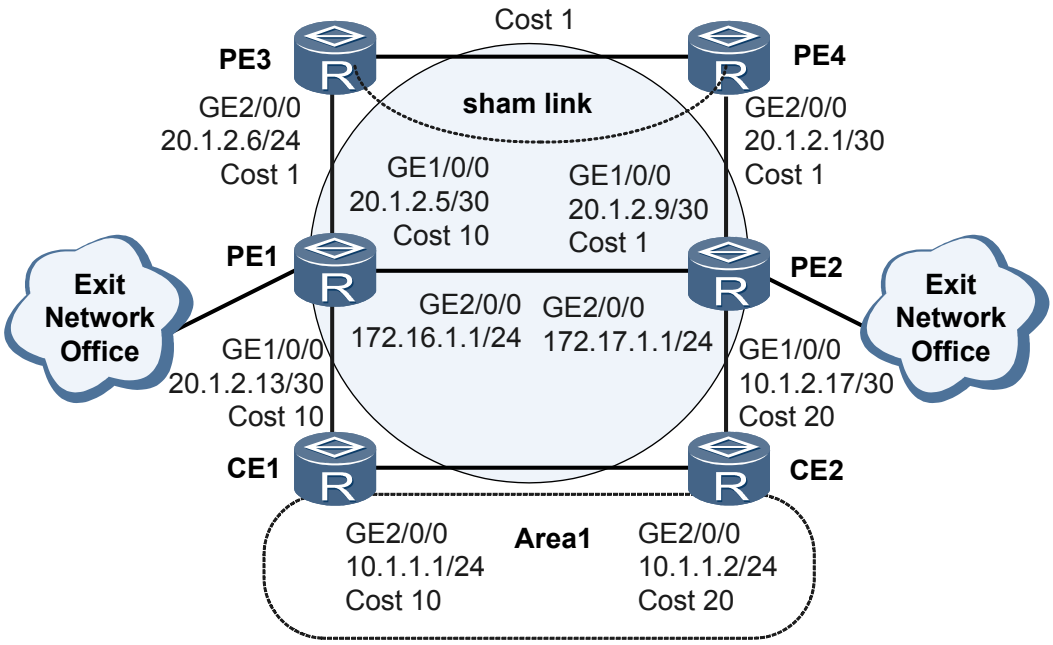
1.2.5 PE 使用 sham link 导致路由环路

网络环境

如图 1-7 所示，网络使用 OSPF，CE1 和 CE2 分别接到 PE1 和 PE2 上。PE3 和 PE4 之间建立 sham link，通过建立 sham link 传递 LSA 信息。PE1 与 PE2 之间没有三层互连接口。CE 把 interface GE1/0/0 放在 Area0，把 interface GE2/0/0 放在 Area1。CE2 与 PE2 之间的链路 Cost 设大来让流量优选 CE1 与 PE1 之间的链路。其它地方使用默认的 Cost 值。CE2 在 interface GE2/0/0 上运行 VRRP，CE1 做为 VRRP 网关。

发现在网络 10.1.1.0/24 的设备无法访问 PE4 和 PE2。在网络 10.1.1.0/24 的设备可以正常访问 PE3 和 PE1。在办公室网络的机器可以访问 PE4，PE2，PE3，PE1。

图 1-7 OSPF 伪连接配置组网图



故障分析

可能的原因：

- 网络中存在防火墙，报文被防火墙过滤。
- 网络中存在链路故障。
- 路由设计错误。
- 设备故障。

针对上述原因分析，逐步检查。

1. 组网中不存在防火墙，排除防火墙问题。
2. 查看网络中各直连链路都能 **ping** 通，说明没有链路异常。
3. 执行命令 **tracert** [**-a** *source-ip-address*] *host*，测试数据包从 10.1.1.0/24 下的设备到 CE2 所经过的网关，发现在 PE2 和 PE4 之间形成环路。理论上 OSPF 具有天然的防环功能，为什么网络中会有环路呢？
4. 执行命令 **display ip routing-table** 命令，查看 PE2 上的路由信息，发现到 10.1.1.0/24 网段的下一跳指向 PE4，Cost 值是 32。而 PE2 和 CE2 之间链路的 Cost 值是 20。为什么 PE2 不优选指向 CE2 的路由呢？
5. 执行命令 **ping** [**-a** *source-ip-address*] *host*，检查 PE2 与 CE2 互联的链路，发现可以 ping 通，链路正常。执行命令 **display ospf peer** 查看 OSPF 中各区域邻居的信息，发现邻居状态都是 full，PE2 与 CE2 的邻居状态正常。
6. 执行命令 **display ospf lsdb** 命令，查看 PE2 上的 OSPF 的链路状态数据库信息，发现包含 CE1 和 CE2 发布的到 10.1.1.0/24 的 LSA。其中 CE2 发布的 LSA 所带的 metric 值是 20。对比分析 OSPF 的 Cost 值，PE2 不优选下一跳是 CE2 的原因在于 OSPF LSDB 中显示的 LSA 的 metric 指的是发布这条 LSA 的路由器到这个网段的 Cost，而不是本路由器到这个网段的 cost 值。OSPF 计算的时候还要算上到发布路由器的 Cost 值。这样计算出来从 PE2 经过 CE2 到 10.1.1.0/24 的 Cost 值是 20 +20=40。而 PE2 经过 PE4－>PE3－>PE1－>CE1 到达 10.1.1.0/24 的 Cost 值是 10+1 +1+10+10=32。

   按照这种算法，PE4 经过 PE3－>PE1－>CE1 到达 10.1.1.0/24 的 Cost 值为 22；而 PE4 经过 PE2－>CE2 到达 10.1.1.0/24 的 Cost 值为 41。PE4 应优选下一跳是 PE3 的路由而不是下一跳指向 PE2 的路由。
7. 执行命令 **display ospf lsdb** 命令，查看 PE4 上的 OSPF 的链路状态数据库信息，发现里面包含 CE1 发布的到 10.1.1.0/24 的 LSA 信息，但执行命令 **display ip routing-table 10.1.1.0 24 verbose** 命令，发现路由表中指向 10.1.1.0/24 的 OSPF 路由下一跳是 PE2，且还有一条指向 10.1.1.0/24 网段的下一跳是 PE3 的状态为 inactive 的路由，协议类型是 BGP。

   分析问题原因在于 PE4 上对于从 sham link 学过来的路由会把它当作 BGP 路由，由于 BGP 路由的协议优先级是 255，而 OSPF 路由的优先级是 10，所以 PE4 会优选从 PE2 学过来的路由。

   综上分析：问题的根本原因在于 PE 上对于 sham link 的处理比较特殊，会把路由类型改为 BGP，导致网络上 PE2-PE4 之间出现路由环路。

操作步骤

- 针对这个问题有四种解决方案，方案一：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp**，进入 BGP 视图。
  3. 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。
  4. 执行命令 **preference** { *external internal local* | **route-policy** *route-policy-name* }，在 PE4 上修改 BGP 协议的优先级，使 PE4 优选 sham link 学过来的路由。

     说明

     这样可以消除现有环路，但难以从根本上避免后续网络改动时再出现环路。
- 方案二：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ospf** *process-id* [**router-id** *router-id*] **vpn-instance** *vpn-instance-name*，进入 OSPF 视图。

3. 执行命令 **area** *area-id*，进入 OSPF 区域视图。
4. 执行命令 **sham-link** *source-ip-address destination-ip-address* [**smart-discover**] [**simple** [[**plain**] *plain-text* | **cipher** *cipher-text*] | { **md5** | **hmac-md5** } [*key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }] | **authentication-null**] [**cost** *cost*]，在 PE4 上修改 sham link 的优先级，使 PE2 不再优选从 PE4 学来的路由，这样也能消除环路。

   说明

   同样，这种方法也难以从根本上避免后续网络改动时再出现环路。

- 方案三：
  1. 在 PE3 和 PE4 之间增加一条私网链路，这种方法可以从根本上避免环路。

     说明

     这种方法实际上把 PE 当成 MCE 来用，MPLS VPN 没有任何作用。而且这种方法不便于 MPLS 域扩容。

- 方案四：

  对已有 OAM 网络进行优化，在 PE1 和 PE2 之间增加一条三层链路并加到 Area0。这样能解决当前问题，而且能够避免现有网络互访的流量（比如 CE1 与 PE2 之间互访）经过 PE 之间的链路来互通。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ospf** *process-id* ，进入 OSPF 视图。
  3. 执行命令 **area 0**，进入 OSPF Area0 视图。
  4. 执行命令 **network** *ip-address wildcard-mask*，将新建的链路接口划分到 Area0 中。

-

  说明

  综上分析，本着尽量减少对网络的改动的原则，可以先采用第二种方法解决问题，后续再采用第四种方法从根本上解决问题。

  在 PE3 和 PE4 上将 sham link 的 Cost 改为 100，PE2 上指向 10.1.1.0 /24 网段下一跳改为 10.1.2.17/30。修改后，10.1.1.0/24 网段下的设备能访问到 CE2，PE2，PE4，其它网段的也都正常。

----结束

案例总结

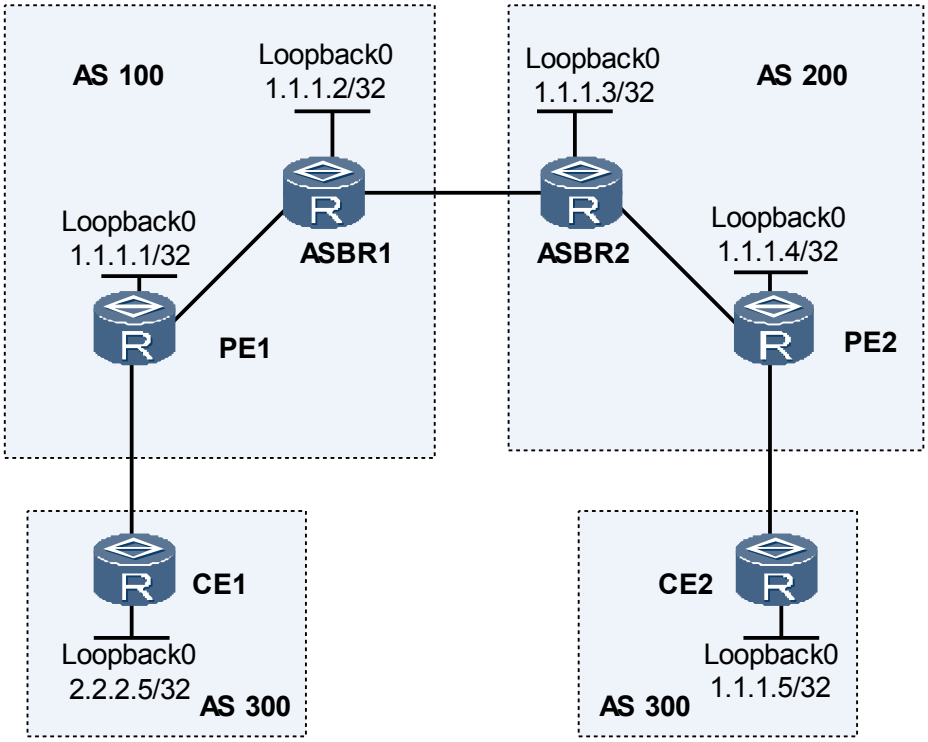
建议在网络规划时尽量避免使用 sham link，以免出现路由环路。

1.2.6 中间路由器 loopback 地址掩码错误导致跨域 Option-B 方式 VPN 路由学习不正常

网络环境

在图 1-8 所示跨域 Option-B 方式网络中，PE2 与 CE2 之间建立 EBGP 对等体关系，引入 VPN 路由。配置完成后，发现在 CE2 上可以学习到 CE1 上的 2.2.2.5 路由，但 CE1 学习不到 CE2 上的 1.1.1.5 路由。

图 1-8 跨域 Option-B 方式组网图



故障分析

说明

正常情况下，不应该出现单方向不能学习路由的情况。对于 Option-B 跨域方式，由于中间的 ASBR 也需要保留 VPN 路由，所以可以通过在设备上检查 BGP VPNV4 的路由来确认路由是在何处丢失。

1. 按照 PE2->ASBR2->ASBR1->PE1 的顺序，依次在设备上执行 **display bgp vpnv4 all routing-table** 命令查看是否含有目的地址为 1.1.1.5 的 VPNv4 路由。发现所有设备都包含该路由，但是在 PE1 上的 1.1.1.5 的路由并非最优路由。
2. 执行 **display current-configuration** 命令检查设备配置，发现 ASBR1 的 Loopback0 地址配置成了 1.1.1.2 255.255.255.252。路由器在通过 LDP 协议建立 LSP 的时候，默认只针对 32 位的主机路由分配标签，而由于 ASBR1 上的 Loopback0 配置成了 30 位掩码，不满足分配 LDP 标签的条件，于是无法正常分配到标签，对应的标签转发所需的 LSP 也就建立不起来。而当 PE1 学习到 vpnv4 的路由后，会检查该路由的 LSP 转发路径是否有效。如果该 LSP 并未建好（路径上标签未分配完整），便不会将 vpnv4 路由保存到 VPN 路由表中。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface loopback** *loopback-number*，进入 Loopback 接口视图。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置接口的 IP 地址。

说明

将 Loopback 接口 IP 地址的掩码改为 32 位。

步骤 4 执行命令 **reset mpls ldp vpn-instance** *vpn-instance-name*，重启指定的 LDP 私网实例，被重启的 LDP 实例上存在的接口、对等体、会话、LSP 和 CR-LSP 都将被删除重建。

完成上述操作后，执行 **display ip routing-table vpn-instance** *vpn-instance-name* 命令可以看到 IPv4 VPN vpna 实例路由表中包含 1.1.1.5 的路由。在 PE1 上执行命令 **ping -vpn-instance** *vpn-instance-name* **-a** *source-ip-address* ，可以 ping 通，故障排除。

----结束

案例总结

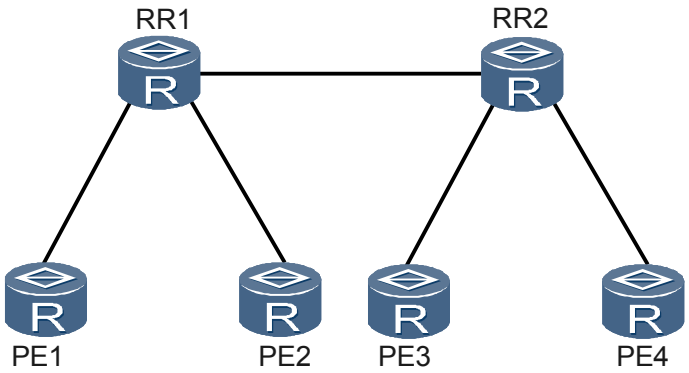
路由器在通过 LDP 协议建立 LSP 的时候，默认只针对 32 位的主机路由分配标签。当不满足分配 LDP 标签的条件时，对应的 LSP 就建立不起来。

1.2.7 RR 上配置 policy vpn-target 后导致 PE 无法学习路由

网络环境

如图 1-9 所示，网络中部署 VPN 时，为了提高可靠性，可配置带双反射器的 VPN，即在骨干网相同 AS 内的 P 设备中选择两个作为路由反射器，互为备份，反射公网及 VPNv4 的路由。PE1、PE2、PE3、PE4 上均配置 VPN 实例 vpna。配置完成后，发现 PE1 和 PE2 学不到 PE3 和 PE4 的路由，反之亦然。

图 1-9 带双反射器的 VPN 组网图



故障分析

1. 检查是否 RR 路由策略限制。在 RR1 和 RR2 上依次执行 **display route-policy** 命令，查看 RR 路由策略，发现 RR 没有限制反射与接收的路由。
2. 检查是否路由冲突。在 PE 设备上依次执行 **display ip routing-table vpn-instance** *vpn-instance-name* 命令，发现 vpna 实例路由没有冲突，排除路由冲突。
3. 检查是否 RR 配置问题。在 RR1 和 RR2 上执行 **display current-configuration** 命令，查看 RR 路由器 BGP 配置，发现其 **ipv4-family vpnv4** 下配置了 **policy vpn-target**。**policy vpn-target** 命令用来对接收到的 VPNv4 路由使能 VPN-Target 过滤功

能，只有 Export RT 属性与本地 Import RT 属性匹配的 VPNv4 路由才被加入到路由表。RR 没有配置 VPN 实例 vpna，导致 RR 不接受包含 vpna RT 值的路由。

操作步骤

- 解决方案一：取消对 VPNv4 路由的 VPN-Target 过滤，接收所有 VPNv4 路由。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
  3. 执行命令 **ipv4-family vpnv4**，进入该 BGP 的 VPNv4 地址族视图。
  4. 执行命令 **undo policy vpn-target**，取消对 VPNv4 路由的 VPN-Target 过滤，即接收所有 VPNv4 路由。

     完成上述操作后，在 PE1 和 PE2 上执行 **display ip routing-table** 命令，发现到达 PE3 和 PE4 的路由信息，反之亦然，故障排除。
- 解决方案二，在 RR 新增 VPN 实例 vpna。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ip vpn-instance** *vpn-instance-name*，创建 VPN 实例 vpna。
  3. 执行命令 **vpn-target** *vpn-target*，将当前 VPN 实例与 VPN Target 进行关联。

     说明

     vpn-target 应保持与 PE 中配置的 VPN 实例 vpna 的 *vpn-target* 保持一致。

     完成上述操作后，在 PE1 和 PE2 上执行 **display ip routing-table** 命令，发现到达 PE3 和 PE4 的路由信息，反之亦然，故障排除。

----结束

案例总结

配置 **policy vpn-target** 时应注意其过滤功能，避免影响属性匹配的 VPNv4 路由不被加入到路由表

1.2.8 PE 的私网路由表中没有远端 PE 发来的路由

网络环境

图 1-10 BGP/MPLS IPv6 VPN 组网图

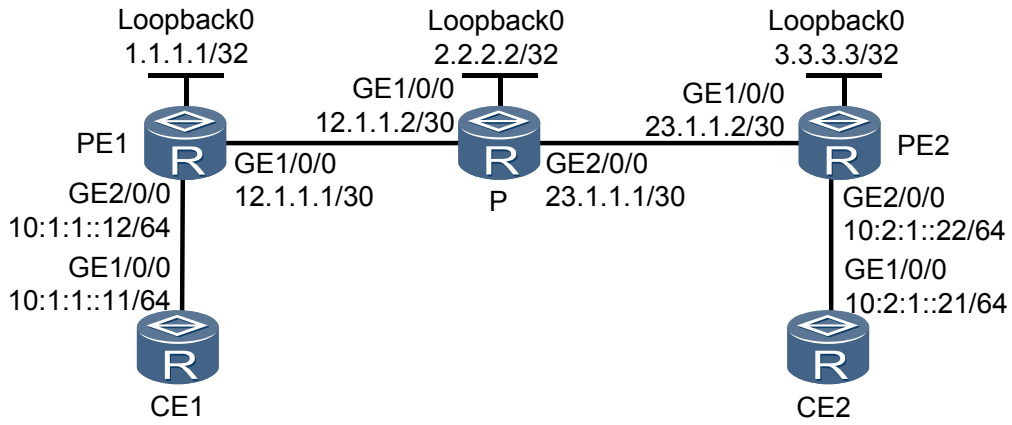


图 1-10 中，采用了如下的配置：

- PE 和 CE 之间采用 EBGP
- PE1 和 PE2 间建立 IBGP 邻居传递携带内层标签的 VPNv6 路由信息
- PE1、P、PE2 间使用任意 IGP 传递公网路由信息
- PE1、P、PE2 上运行了 MPLS 和 MPLS LDP。

配置完成后，发现 PE1 上有 CE1 发送来的私网路由，但 PE2 和 CE2 上没有。

故障分析

1. 在 PE 上执行 **display bgp vpnv6 all peer** 命令查看到 IBGP 对等体已达到“Established”状态，说明 IBGP 对等体已建立。
2. 在 PE2 上执行 **display bgp vpnv6 all routing-table peer** *ipv4-address* **received-routes** 命令，发现 PE2 已收到了 PE1 发来的 VPNv6 路由。
3. 在 PE2 上执行 **display bgp vpnv6 vpn6-instance** *vpn6-instance-name* **routing-table** *ipv6-address* [*mask-length*]命令查看指定路由所迭代到的隧道信息。

   如果显示的 Relay token 的值为 0x0，表示到 *ipv6-address* 的路由没有找到关联的隧道，是由于到该路由下一跳的 LSP 没有建立起来，如：

   ```
   <PE2> display bgp vpnv6 vpn-instance vpna routing-table 66::66 128
   BGP local router ID : 3.3.3.3
    Local AS number : 100
    Paths:   1 available, 0 best, 0 select
    BGP routing table entry information of 66::66/128
    Label information  (Received/Applied) : 105472/NULL
    From: 1.1.1.1  (1.1.1.1)
    Route Duration: 00h02m17s
    Relay Tunnel Out-Interface:
    Relay token: 0x0
    Original nexthop: ::FFFF:1.1.1.1
    Qos information : 0x0
    Ext-Community:RT <1 : 1>
    AS-path 65420, origin igp, MED 0, localpref 100, pref-val 0, internal, pre 255
    Not advertised to any peer yet
   ```

4. 查看是否有到下一跳（1.1.1.1）的 LSP：

   ```
   <PE2> display mpls lsp include 1.1.1.1 32
   ```

   显示结果为空，即没有到 1.1.1.1 的 LSP，说明 LSP 隧道没有建立成功。

5. 查看 PE1 与 P、P 与 PE2 之间的接口是否配置了 MPLS LDP：

   ```
   [PE1] interface gigabitethernet 1/0/0
   [PE1-GigabitEthernet1/0/0] display this
   #
   interface GigabitEthernet1/0/0
    ip address 12.1.1.1 255.255.255.252
    mpls
   #
   ```

   以上显示结果表明没有在接口模式下配置 MPLS LDP。

操作步骤

步骤 1 在 PE1 上执行命令 **interface gigabitethernet 1/0/0**，进入接口视图。

步骤 2 在该接口下执行命令 **mpls ldp**，使能接口的 LDP 能力即可。

----结束

案例总结

要将私网流量通过公网传递到另一端，需要有一条公网隧道承载这个私网流量。

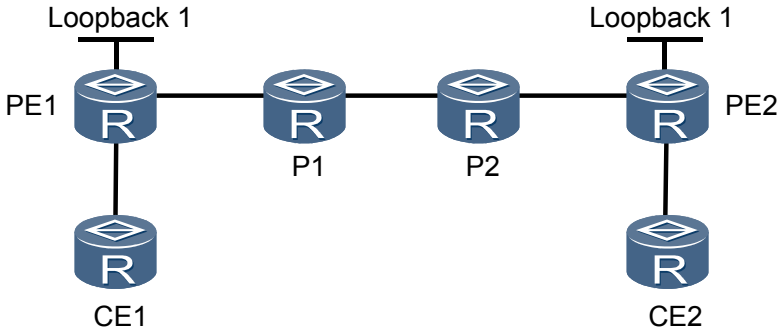
公网隧道没有的可能原因是接口没有配置 MPLS LDP，LDP Session 没有建立起来，导致 PE 上收到远端 PE 发来的私网路由不优选。

1.2.9 CE 间不能互通

网络环境

在图 1-11 的网络中配置 BGP/MPLS IPv6 VPN 业务，CE1 与 CE2 属于同一 IPv6 VPN。配置完成后，发现 CE1 ping 不通 CE2。

图 1-11 BGP/MPLS IPv6 VPN 组网图



故障分析

说明

这里以 PE2 的配置错误为例，PE1 与之类似，此不赘述。

1. 在 PE2 上执行 **display bgp vpnv6 all peer** 检查 PE2 与 PE1 之间的 IBGP 对等体关系，发现 IBGP 对等体关系建立不成功。
2. 检查 BGP 配置，发现两个 PE 建立 IBGP 连接时，没有通过 **peer** *peer-ip-address* **connect-interface loopback** *interface-number* 命令指定本端 IBGP 会话的出接口为 Loopback 接口。

   如果没有指定本端 IBGP 会话的出接口，默认以数据流的出接口为该会话的出接口。PE 之间一般使用 32 位掩码的 Loopback 接口来建立 IBGP 对等体，IBGP 会话的出接口也需要设置成该 Loopback 接口。

操作步骤

步骤 1 在系统视图下执行 **interface loopback** *interface-number*。

步骤 2 输入命令 **ip address** *ip-address* **32**，配置 Loopback 接口的 IP 地址。

步骤 3 输入命令 **quit** 返回到系统视图。

步骤 4 执行 **bgp** *as-number* 进入 BGP 视图。

步骤 5 执行命令 **peer** *peer-ip-address* **connect-interface loopback** *interface-number*，指定使用 Loopback 接口作为 IBGP Peer 会话的出接口。

步骤 6 保存配置。

在 CE 上 ping 对端 CE。如果可以 ping 通，则故障被排除。

----结束

案例总结

在配置 PE 对等体时，需要指定本端 IBGP 会话的出接口为本端的 Loopback 接口。

1.2.10 私网大包不通

网络环境

华为路由器与其他公司设备配合组网，使用以太网接口，部署三层 MPLS IPv6 VPN 业务时，发现私网用户之间不能通过 1492 字节以上的大包。用户不能打开部分网站，也不能通过 FTP 下载文件。

执行 **ping** 命令检验时发现，在指定 ICMP 的净荷为 1464 字节以上时就 ping 不通。

故障分析

1. 以太接口默认 MTU 值为 1500 字节。MPLS IPv6 VPN 在数据转发时，会在 IP 报文头与二层帧头之间加上 4 个或者 8 个字节的 MPLS 报文头。即倒数第二跳和倒数第一跳设备之间转发时加 4 个字节标签，其他的 P 设备之间转发时加 8 个字节标签。
2. 链路层并不清楚 MPLS 的处理，还是默认接收最大为 1500 字节的数据包，这样，IP 层大小为 1492 ～ 1500 字节的报文再加上 MPLS 报文头之后就会超过 1500，从而导致链路层不能接收，影响数据转发。

操作步骤

步骤 1 调整其他公司设备物理接口的 MTU 值，使链路层接收网络层的 MTU 值至少是 1508。

步骤 2 华为路由器以太口默认可以接收和发送超长帧，不需要调整。

----结束

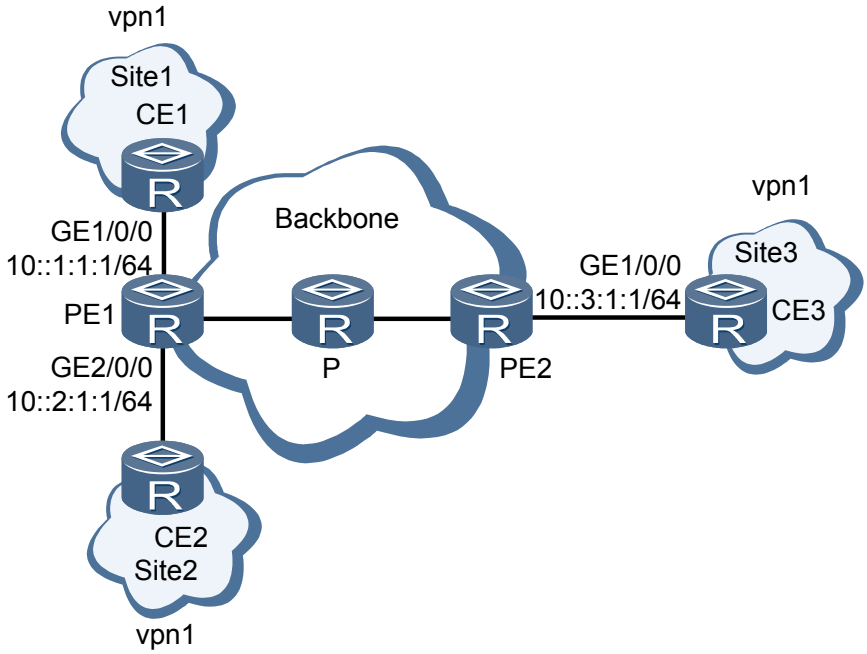
案例总结

当大包不能接收时，请查看入接口的 MTU 值是否过小。

1.2.11 PE Ping 不通远端 CE 网段

网络环境

图 1-12 BGP/MPLS IPv6 VPN 组网图



如图 1-12，PE1 上配置多个私网接口绑定同一个 VPN 实例后，在 CE1 和 CE2 上执行 **ping ipv6 10::3:1:1** 命令，均能 Ping 通 PE1 的远端 CE3 网段，但 PE1 上执行 **ping ipv6 vpn6-instance vpn1 10::3:1:1** 命令 Ping 不通 CE3 网段。

故障分析

当 Ingress 节点（PE）上有多个私网接口绑定同一个 IPv6 VPN 实例，在 PE 上 **ping** 或 **tracert** 远端 CE 网段时，ICMPv6 报文的源地址填的是本 PE 上处于 Up 状态的最小的私网地址；如果远端 CE 没有引入这个私网地址，就会引起该 ICMPv6 报文不能返回。

所以，要用 **ping ipv6 vpn6-instance** *vpn6-instance-name dest-ipv6-address* 命令 ping 通远端 CE 网段，需要确保远端 CE 上有本 PE 的所有处于 Up 状态的私网地址。如果在 **ping** 命令中指定源 IP 地址为本 PE 上的处于 Up 状态的私网地址，且该私网地址已被引入到远端 CE 上，那么 PE 也能 ping 通远端 CE 网段。

操作步骤

步骤 1 确保远端 CE 上有本 PE 的所有处于 Up 状态的私网地址。

步骤 2 为确保能把本 PE 上的私网路由通过 MP-BGP 全部发布出去，可在本 PE 的 BGP VPN 实例视图下执行 **import-route direct** 命令。或者把 **ping ipv6 vpn6-instance** *vpn6-instance-name dest-ip-address* 命令改为 **ping ipv6 -a** *source-ipv6-address* **vpn6-instance** *vpn6-instance-name dest-ipv6-address*。

----结束

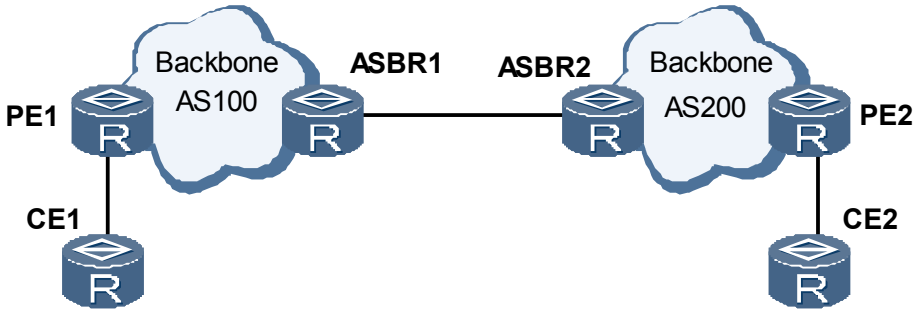
案例总结

在 PE 上 ping 远端 CE 网段时，建议指定 Ping 报文的源地址，否则可能 ping 不通。

1.2.12 跨域 IPv6 VPN-OptionC 中 CE 之间不能通信

网络环境

图 1-13 跨域 IPv6 VPN-OptionC 组网图



如图 1-13，在配置跨域 IPv6 VPN-OptionC 时，PE1 与 PE2 之间的 MP-EBGP 对等体关系已经建立，但 CE1 与 CE2 不能通信。

查看路由表或转发表，发现 PE2 与 ASBR2 之间 IGP 路由存在两条负载分担路径，并且其中一条路径 Link_A 上有 LDP LSP，而另一条 Link_B 上没有。

故障分析

ASBR 将同一 AS 的 PE 上的 Loopback 接口路由引入到 BGP 中时，如果存在多条等价的去往 PE 的 Loopback 的 IGP 路由，系统会随机选其中的一条。如果选中的该路由，没有迭代到相应的 LDP LSP，则后续数据转发到 ASBR 上时，会将数据报丢弃，从而造成 CE 之间不能互通。

ASBR2 上运行命令 **display bgp routing-table** 查看去往 PE2 上 Loopback 接口的 BGP 路由信息，发现这里优选了 Link_B 所在路径的路由，由于 Link_B 上没有建立 LDP LSP，从而造成 CE 之间不能互通。

```
<ASBR2> display bgp routing-table 4.4.4.9

 BGP local router ID : 3.3.3.9
 Local AS number : 200
 Paths:   1 available, 1 best, 1 select
 BGP routing table entry information of 4.4.4.9/32:
 Network route.
 Label information (Received/Applied): NULL/13312
 From: 0.0.0.0 (0.0.0.0)
 Route Duration: 03h58m55s
 Direct Out-interface: Pos3/0/0
 Original nexthop: 162.1.1.2
 Qos information : 0x0
 AS-path Nil, origin igp, MED 2, pref-val 0, valid, local, best, select, pre 10
 Advertised to such 1 peers:
    192.1.1.1
```

操作步骤

- 方案一：可考虑删除没有建立 LDP LSP 的链路，从而只有关联了 LDP LSP 的路由引入到 BGP 中。
- 方案二：可根据相应的 IGP 路由协议调整链路的 cost，以保证 IBGP 没有等价的 IGP 路由，使得关联了 LDP LSP 的路由能够优选。以 ospf 为例说明：
  1. 执行命令 **interface** *interface-type interface-number*，进入到要调整 cost 的接口视图下。
  2. 执行命令 **ospf cost** *cost*，调整当前接口的 cost 值。
- 方案三：没有建立 LDP LSP 的链路上全局及接口下使能 MPLS、MPLS LDP，建立 LDP LSP。
  1. 执行命令 **mpls**，使能本节点的 MPLS，并进入 MPLS 视图。
  2. 执行命令 **mpls ldp**，使能全局的 LDP 功能，并进入 MPLS-LDP 视图。
  3. 执行命令 **quit**，退回到系统视图。
  4. 执行命令 **interface** *interface-type interface-number*，进入到接口视图下。
  5. 执行命令 **mpls**，使能接口的 MPLS 能力。
  6. 执行命令 **mpls ldp**，使能接口的 LDP 功能。

----结束

案例总结

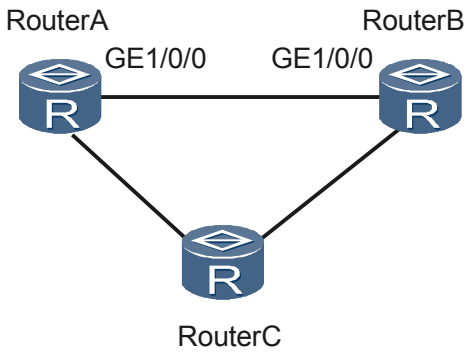
将 PE 的 Looopback 接口路由引入到 BGP 中时，需要确保该路由能关联到 LDP LSP。

1.2.13 因物理接口振荡导致了 L3VPN 的私网路由频繁振荡

网络环境

在图 1-14 的网络中。RouterA、RouterB 和 RouterC 使用 ISIS 路由协议，配置了 L3VPN 业务。配置完成后，发现 RouterA 到 RouterC 的业务出现闪断的现象。

图 1-14 因物理接口振荡导致了 L3VPN 的私网路由频繁振荡组网图



故障分析

1. 在 RouterA 上执行命令 **display ip routing-table 1.1.1.1** 和 **display fib 1.1.1.1**，查看路由类型，发现是 ISIS 协议生成的路由，并且配置的是 LDP Over TE。

```
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
```

```
Routing Table : Public
Summary Count : 1

Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

 1.1.1.1/32         ISIS   15   10           D  1.1.1.2  Tunnel0/0/1
  Route Entry Count: 1
Destination/Mask   Nexthop         Flag TimeStamp     Interface       TunnelID
1.1.1.1/32         1.1.1.2         DGHU t[17635149]   Tun0/0/1        0x1008e
```

2. 在 RouterA 上执行命令 **display isis lsdb verbose** 查看设备的 ISIS 邻居，发现建立时间很长，没有震荡的情况，说明 ISIS 邻居状态是正常的。

```
Database information for ISIS(100)
                    ----------------------------------
                       Level-2 Link State Database
LSPID                 Seq Num      Checksum      Holdtime      Length  ATT/P/OL
0000.0255.0239.00-00  0x00003038   0xd401        867           367     0/0/0
 INTF ADDR    1.1.1.1
 Router ID    1.1.1.1
```

3. 在 RouterA 上执行命令 **display isis lsdb 0000.0255.0239.00-00**，根据 LSPID 查看 LSP 是否发生变化。

```
                    Database information for ISIS(100)
                    ----------------------------------
                       Level-2 Link State Database
LSPID                 Seq Num      Checksum      Holdtime      Length  ATT/P/OL
--------------------------------------------------------------------------------
0000.0255.0239.00-00  0x00003038   0xd401        831           367     0/0/0
    *(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
          ATT-Attached, P-Partition, OL-Overload
                    Database information for ISIS(100)
                    ----------------------------------
                       Level-2 Link State Database
LSPID                 Seq Num      Checksum      Holdtime      Length  ATT/P/OL
--------------------------------------------------------------------------------
0000.0255.0239.00-00  0x00003038   0xd401        829           367     0/0/0
    *(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
          ATT-Attached, P-Partition, OL-Overload
```

通过上面的显示信息可以看出该 LSP 正常，长度没有变化，老化时间也没有突变，排除 ISIS 导致路由震荡的可能。

4. 在 RouterA 上执行命令 **display mpls lsp include 1.1.1.1 32**，查看 TE 隧道是否存在震荡，发现去向该路由的 LSP 并没有发生震荡。但是 LDP 的 LSP 存在时间很短，说明是 LDP 的 LSP 在震荡，导致该条路由震荡。

```
--------------------------------------------------------------------------------
                LSP Information: RSVP LSP
--------------------------------------------------------------------------------

  No                  :  1
  SessionID           :  12
  IngressLsrID        :  1.1.1.3
  LocalLspID          :  32778
  Tunnel-Interface    :  Tunnel0/0/12
  Fec                 :  1.1.1.1/32
  Nexthop             :  1.1.2.1
  In-Label            :  65542
  Out-Label           :  65686
  In-Interface        :  GigabitEthernet8/0/0
  Out-Interface       :  GigabitEthernet7/0/0
  LspIndex            :  2123
  Token               :  0x700bef8
  LsrType             :  Transit
  Bypass In Use       :  Not Exists
  Bypass Tunnel Id    :  0x0
  BypassTunnel        :  Tunnel Index[---]
  Mpls-Mtu            :  1600
```

```
TimeStamp          :  309526sec
Bfd-State          :  ---

No                 :  2
SessionID          :  12
IngressLsrID       :  1.1.1.2
LocalLspID         :  1
Tunnel-Interface   :  Tunnel0/0/12
Fec                :  1.1.1.1/32
Nexthop            :  1.1.2.1
In-Label           :  NULL
Out-Label          :  65817
In-Interface       :  ----------
Out-Interface      :  GigabitEthernet7/0/0
LspIndex           :  2181
Token              :  0x700bf18
LsrType            :  Ingress
Bypass In Use      :  Not Exists
Bypass Tunnel Id   :  0x0
BypassTunnel       :  Tunnel Index[---]
Mpls-Mtu           :  1600
TimeStamp          :  309524sec
Bfd-State          :  ---

No                 :  3
SessionID          :  12
IngressLsrID       :  1.1.1.2
LocalLspID         :  32773
Tunnel-Interface   :  Tunnel0/0/12
Fec                :  1.1.1.1/32
Nexthop            :  1.1.2.2
In-Label           :  NULL
Out-Label          :  65581
In-Interface       :  ----------
Out-Interface      :  GigabitEthernet8/0/0
LspIndex           :  2827
Token              :  0x80094a9
LsrType            :  Ingress
Bypass In Use      :  Not Exists
Bypass Tunnel Id   :  0x0
BypassTunnel       :  Tunnel Index[---]
Mpls-Mtu           :  1600
TimeStamp          :  1825411sec
Bfd-State          :  ---
------------------------------------------------------------------------------
              LSP Information: LDP LSP
------------------------------------------------------------------------------
No                 :  4
VrfIndex           :
Fec                :  1.1.1.1/32
Nexthop            :  1.1.1.2
In-Label           :  1102
Out-Label          :  3
In-Interface       :  ----------
Out-Interface      :  Tunnel0/0/12
LspIndex           :  72894
Token              :  0x1008f
FrrToken           :  0x0
LsrType            :  Transit
Outgoing token     :  0x0
Label Operation    :  SWAP
Mpls-Mtu           :  ------
TimeStamp          :  10sec
Bfd-State          :  ---

No                 :  5
VrfIndex           :
Fec                :  1.1.1.1/32
Nexthop            :  1.1.1.2
```

```
  In-Label            :  NULL
  Out-Label           :  3
  In-Interface        :  ----------
  Out-Interface       :  Tunnel0/0/12
  LspIndex            :  72897
  Token               :  0x1008e
  FrrToken            :  0x0
  LsrType             :  Ingress
  Outgoing token      :  0x0
  Label Operation     :  PUSH
  Mpls-Mtu            :  ------
  TimeStamp           :  10sec
  Bfd-State           :  ---
```

5. 在 RouterA 上执行命令 **display mpls ldp session**，查看 LDP 邻居，发现 LDP 邻居也在震荡。

```
 LDP Session(s) in Public Network
 ------------------------------------------------------------------------------
 Peer-ID            Status      LAM  SsnRole  SsnAge      KA-Sent/Rcv
 ------------------------------------------------------------------------------
 ......
 1.1.1.1:0          Operational DU   Passive  000:00:00   20492/20493
 ......
 ------------------------------------------------------------------------------
 TOTAL: 36 session(s) Found.
 LAM : Label Advertisement Mode      SsnAge Unit : DDD:HH:MM
```

6. 在 RouterA 上执行命令 **display mpls ldp peer**，查看 LDP 对等体信息，发现存在两个对等体，一个是远端 LDP 对等体，一个是本地 LDP 对等体。

```
LDP Peer Information in Public network
 ------------------------------------------------------------------------------
 Peer-ID                Transport-Address  Discovery-Source
 ------------------------------------------------------------------------------
 1.1.1.1:0              1.1.1.1            Remote Peer : otb-to-trg
 ------------------------------------------------------------------------------
 TOTAL: 36 Peer(s) Found.
LDP Peer Information in Public network
 ------------------------------------------------------------------------------
 Peer-ID                Transport-Address  Discovery-Source
 ------------------------------------------------------------------------------
 1.1.1.1:0              1.1.1.1            GigabitEthernet1/0/0
 ------------------------------------------------------------------------------
 TOTAL: 36 Peer(s) Found.
```

7. 在 RouterA 上执行命令 **display interface gigabitEthernet1/0/0**，发现接口状态频繁的在 UP 和 DOWN 之间切换，这也是路由震荡的原因所在。

```
GigabitEthernet1/0/0 current state : UP
Line protocol current state : DOWN
Description:10G_Link_to-TRG_Through_ODF 23/24
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-82d7-b2e5
The Vendor PN is SXP3101SV-H12
BW: 10G, Transceiver Mode: SingleMode
WaveLength: 1550nm, Transmission Distance: 40km
Rx Power: -4.50dBm, Tx Power: 1.14dBm
Loopback:none, LAN full-duplex mode, Pause Flowcontrol:Receive Enable and Send Enable
Last physical up time   : 2010-05-20 21:33:42
Last physical down time : 2010-05-20 21:31:58
Statistics last cleared:2010-04-25 02:10:55
    Last 300 seconds input rate: 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate: 0 bits/sec, 0 packets/sec
    Input: 486833280327643 bytes, 720675974914 packets
    Output: 66656626810850 bytes, 400094354049 packets
    Input:
      Unicast: 720675171257 packets, Multicast: 797735 packets
      Broadcast: 5922 packets, JumboOctets: 38836146308 packets
      CRC: 688 packets, Symbol: 200 packets
```

```
      Overrun: 0 packets
      InRangeLength: 0 packets
      LongPacket: 0 packets, Jabber: 0 packets,
      Fragment: 3 packets, Undersized Frame: 0 packets
      RxPause: 0 packets
    Output:
      Unicast: 400093379625 packets, Multicast: 973669 packets
      Broadcast: 755 packets, JumboOctets: 1138327781 packets
      System: 0 packets, Overruns: 0 packets
      TxPause: 0 packets
      Unknown Vlan: 0 packets
GigabitEthernet1/0/0 current state : UP
Line protocol current state : DOWN
Description:10G_Link_to-TRG_Through_ODF 23/24
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-82d7-b2e5
The Vendor PN is SXP3101SV-H12
BW: 10G, Transceiver Mode: SingleMode
WaveLength: 1550nm, Transmission Distance: 40km
Rx Power: -4.50dBm, Tx Power: 1.14dBm
Loopback:none, LAN full-duplex mode, Pause Flowcontrol:Receive Enable and Send Enable
Last physical up time   : 2010-05-20 21:33:45
Last physical down time : 2010-05-20 21:31:43
Statistics last cleared:2010-04-25 02:10:55
    Last 300 seconds input rate: 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate: 0 bits/sec, 0 packets/sec
    Input: 486833280327643 bytes, 720675974914 packets
    Output: 66656626810850 bytes, 400094354049 packets
    Input:
      Unicast: 720675171257 packets, Multicast: 797735 packets
      Broadcast: 5922 packets, JumboOctets: 38836146308 packets
      CRC: 688 packets, Symbol: 200 packets
      Overrun: 0 packets
      InRangeLength: 0 packets
      LongPacket: 0 packets, Jabber: 0 packets,
      Fragment: 3 packets, Undersized Frame: 0 packets
      RxPause: 0 packets
    Output:
      Unicast: 400093379625 packets, Multicast: 973669 packets
      Broadcast: 755 packets, JumboOctets: 1138327781 packets
      System: 0 packets, Overruns: 0 packets
      TxPause: 0 packets
      Unknown Vlan: 0 packets
```

操作步骤

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

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

步骤 3 在 RouterA 上执行命令 **shutdown**，将接口关闭。

完成上述操作后，报文不是从 RouterA 直接到达 RouterB，而是 RouterA 的报文经过 RouterC 到 RouterB，业务恢复正常，故障排除。

----结束

案例总结

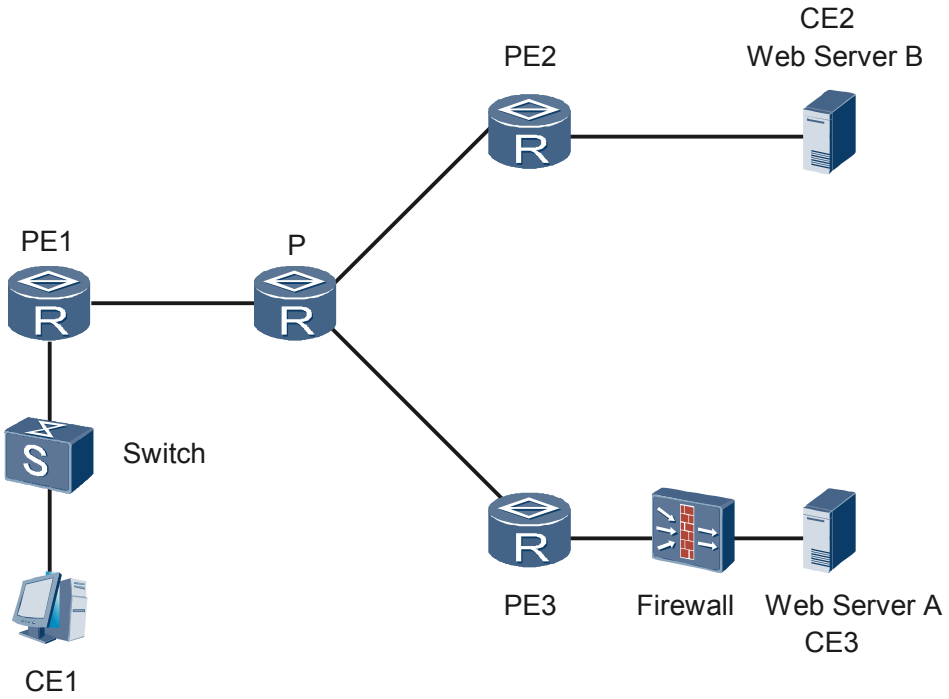
在出现某条路由震荡时，首先需要查看该路由的类型，先分析清楚该路由的具体类型，然后采取由下至上的方法，查看相关的协议是否在震荡，如果不是协议震荡，则需要排查是否存在 IP 地址冲突等情况。

1.2.14 链路 MTU 导致 CE 无法访问部分 Web 服务器

网络环境

在图 1-15 的网络中，PE 上配置 BGP/MPLS VPN 业务，CE1、Web Server A 和 Web Server B 属于同一个 VPN。PE3 与 Web Server A 之间通过防火墙相连。配置完成后，发现 CE 无法访问部分 Web 服务器。

图 1-15 链路 MTU 导致 CE 无法访问部分 Web 服务器组网图



故障分析

1. 在 PE1 和 PE2 上执行命令 **display bgp vpnv4 all peer**，可以看到 PE 之间、PE 和 CE 之间的 BGP 对等体关系已经建立，并达到 Established 状态。
2. 在 PE1、PE2 和 PE3 上执行命令 **ping -vpn-instance** *vpn-instance-name*，各个 PE 能 ping 通接入的 CE 设备。
3. 在 PE1、PE2 和 PE3 上执行命令 **display current-configuration configuration vpn-instance** *vpn-instance-name*，查看 VPN 实例的配置信息，可以发现 PE 上的 VPN 实例配置正确，Import 属性和 Export 属性也相互匹配。
4. 通过在 PE 上抓包发现 Web 服务器发布的 IP 层包长为 1496 字节，且为不可分片报文。此数据包在进入 MPLS 网络后长度为 1496+8(MPLS 每个标签长度为 4 个字节，共两个标签)=1504 字节。
5. 在 PE1、PE2 和 P 设备上执行命令 **display mpls interface**，查看接口的 MPLS 报文的 MTU，发现 P 设备的 MPLS 报文的 MTU 值为 1500，这样就导致长度为 1504 的 MPLS 报文在 PE 或者 P 设备上被丢弃。

操作步骤

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

步骤 2 执行命令 **interface** *interface-type interface-number*，进入 P 与 PE 相连的接口视图。

步骤 3 执行命令 **mtu** *mtu*，重新配置接口的 MTU 值。

步骤 4 执行命令 **mpls mtu 1600**，重新配置接口的 MPLS 报文的 MTU。

说明

接口的 MPLS MTU 与接口本身的 MTU 之间存在下述关系：

- 如果没有配置接口的 MPLS MTU 值，则采用接口的 MTU 值。
- 如果配置了接口的 MPLS MTU 值，则与接口的 MTU 值比较，采用两者中的较小值。

步骤 5 执行命令 **restart**，重新启动当前接口。

完成上述操作后，发现 CE1 可以正常访问 Web Server A 和 Web Server B，故障排除。

----结束

案例总结

本案例产生的原因是：

- Web 服务器发出的报文为不可分片报文，且 Web 服务器发送的报文大小加上两层 MPLS 标签后，超过中间 P 设备的 MPLS MTU 值，导致报文在 P 设备上被丢弃。
- 防火墙禁止了 ICMP 报文，导致路径 MTU 发现机制失灵。

路径 MTU 发现的基本原理是：

1. 源主机最初假设到目的主机的路径 MTU 为源主机发送这个报文的第一跳接口的 MTU，并把发送到主机的所有 IP 报文 IP 头中的 DF（Don't Fragment）Bit 位设置为 1。
2. 在转发路径中的某个设备收到报文后，要从某个出接口转发该报文的时候，如果设备发现该报文大于出接口的 MTU，并且其 DF 位为 1，该设备则丢弃本报文，并且返回一个 ICMP 目的地址不可达报文（type=3,code=4，fragment needed but don't-fragment bit set）通知被丢弃报文的源主机。
3. 源主机收到这个 ICMP 报文后就减小假定的这条路径上的 MTU 值，重新发送。

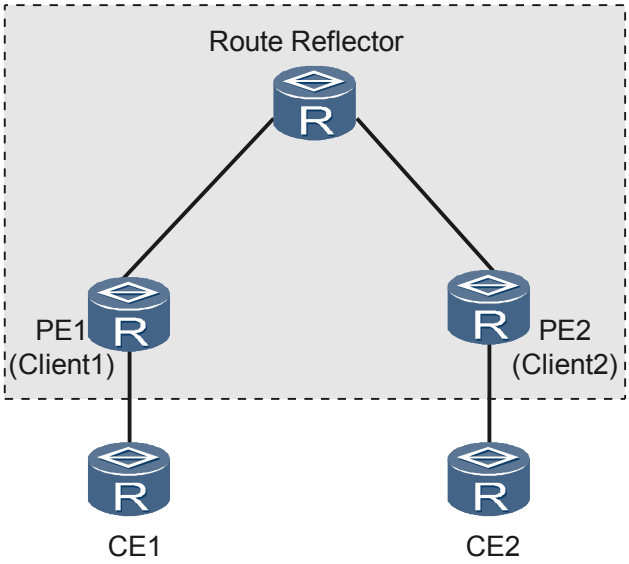
此案例属于 MTU 值配置错误问题，可以通过重新配置 MTU 来解决问题。

1.2.15 路由反射器反射 VPN 路由失败

网络环境

在图 1-16 的网络中。配置路由反射器优化 BGP/MPLS VPN 业务，CE1 和 CE2 属于同一 VPN。配置完成后，发现 PE1 发布的一条 VPNv4 路由，RR 能成功学到这条 VPNv4 路由，但是 PE2 上没有学到这条 VPNv4 路由。

图 1-16 路由反射器反射 VPN 路由失败组网图



故障分析

1. 依次在 RR 和 PE 上执行命令 **display current-configuration configuration bgp**，可以看到 RR 与两台 PE 的路由反射关系配置正确。
2. 在 RR 上执行命令 **display bgp vpnv4 all peer**，可以看到 RR 与 PE 之间的 IBGP 对等体关系已经建立，并达到 Established 状态（BGP current state: Established, Up for 00:21:15）。
3. 在 RR 上执行命令 **display ip extcommunity-filter**，查看扩展团体属性过滤器的信息。

```
Extended Community filter Number 1
        deny rt : 100:1
        permit rt : 200:1
```

通过上面的显示信息发现 RT 值 100：1 的路由被过滤掉了。

4. 在 PE1 上执行命令 **display ip vpn-instance verbose**，查看所有 VPN 实例的详细信息。

```
 Total VPN-Instances configured : 1

 VPN-Instance Name and ID : a, 1
 Create date : 2010/06/23 20:18:40 UTC+08:00 DST
 Up time : 0 days, 00 hours, 02 minutes and 27 seconds
 Route Distinguisher : 1:1
 Export VPN Targets :  100:1
 Import VPN Targets :  111:1
 Label Policy : label per route
 Import Route Policy : p1
 Export Route Policy : p2
 The diffserv-mode Information is : uniform
 The ttl-mode Information is : pipe
 The VPN QoS configuration information : based on VPN
 CIR: 10000000 PIR: 10000000  QoS-profile name: profile1
 Tunnel Policy : tnlpolicy1
 Description : This is a VPN for company1.
 Maximum Routes Limit : 100
 Log Interval : 5
 Interfaces : GigabitEthernet1/0/0
```

通过上面的显示信息可以看出 PE1 上的 **Export VPN Targets** 字段的值在 RR 上被过滤了，因此 RR 不会再向它的客户机 PE2 反射路由。

操作步骤

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

步骤 2 在 RR 上执行命令 **ip extcommunity-filter 1 permit rt 100:1**，将 PE1 的 Export RT 属性与 RR 扩展团体属性过滤器中的 RT 值匹配。

步骤 3 在 RR 上执行命令 **bgp** *as-number*，进入 BGP 视图。

步骤 4 在 RR 上执行命令 **ipv4-family vpnv4**，进入 BGP-VPNv4 地址族视图。

步骤 5 在 RR 上执行命令 **undo rr-filter**，删除原路由反射器的反射策略。

步骤 6 在 RR 上执行命令 **rr-filter 1**，重新指定路由反射器的反射策略。

完成上述操作后，PE2 上能够学到 PE1 发布的 VPNv4 路由，故障排除。

----结束

案例总结

在配置路由反射器时，需要注意路由反射器的 Import 值和 Export 值均能和 Client 的 RT 值一一对应。

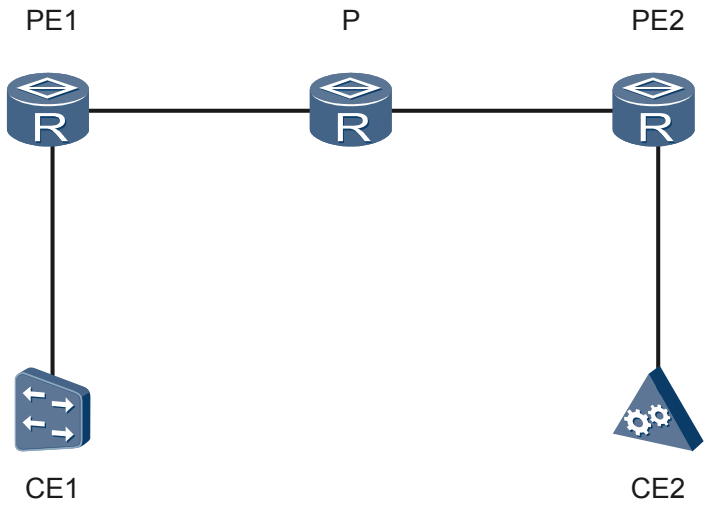
为了防止配置错误，也可以使用命令 **undo policy vpn-target**，接收所有 VPNv4 路由。

1.2.16 VPN 实例路由数量超过限制导致 CE1（Access Gateway 设备）无法注册到 CE2（Soft3000 软交换设备）

网络环境

在图 1-17 的网络中，PE 上配置 BGP/MPLS VPN 业务，并划分为信令 VPN 和媒体 VPN。CE1 为 AG（Access Gateway）设备，CE2 为软交换设备（Soft3000），CE1 与 CE2 属于同一 VPN。配置完成后，发现 CE1 无法注册到 CE2。

图 1-17 VPN 实例路由数量超过限制导致 CE1 无法注册到 CE2 组网图



故障分析

1. 在两台 PE 上分别执行命令 **display bgp vpnv4 all peer**，可以看到 PE 之间、PE 与 CE 之间的 BGP 对等体已经建立，并达到 Established 状态。
2. 在两台 PE 上分别执行命令 **ping -vpn-instance** *vpn-instance-name*，各个 PE 能 ping 通自己接入的 CE。
3. 在两台 PE 上执行命令 **display ip routing-table vpn-instance** *vpn-instance-name*，可以看到两台 PE 上分别存在到对端 PE 的 VPN 实例路由。
4. 在 PE1 上执行命令 **display bgp vpnv4 all routing-table 10.1.1.1**，查看 10.1.1.1/24 网段 BGP 路由信息，可以发现信令 VPN 内只存在两条路由，在 VPN 实例下没有路由信息。

```
 Total routes of Route Distinguisher(65029:2995): 2

 BGP routing table entry information of 10.1.1.1/24:
 Label information (Received/Applied): 589826/NULL
 From: 11.1.1.1 (11.1.1.1)
 Original nexthop: 12.1.1.1
 Ext-Community: <65029 : 2995>
 AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, valid, internal, best, pre
255
 Originator:  12.1.1.1
 Cluster list: 11.1.1.1
 Not advertised to any peer yet


 BGP routing table entry information of 172.16.7.20/30:
 Label information (Received/Applied): 589826/NULL
 From: 11.1.1.2 (11.1.1.2)
 Original nexthop: 12.1.1.1
 Ext-Community: <65029 : 2995>
 AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, valid, internal, pre 255
 Originator:  12.1.1.1
 Cluster list: 11.1.1.2
 Not advertised to any peer yet
```

5. 在 PE1 上执行命令 **display current-configuration configuration vpn-instance** *vpn-instance-name*，查看 VPN 实例的配置信息，发现 PE1 的信令 VPN 内配置了路由限制。

```
ip vpn-instance ngn-signal
 route-distinguisher 65029:2995
 apply-label per-instance
 routing-table limit 100 80
 vpn-target 65029:2995 export-extcommunity
 vpn-target 65029:2995 import-extcommunity
```

6. 在 PE1 上执行命令 **display ip routing-table vpn-instance** *vpn-instance-name* **statistics**，查看 VPN 路由的统计信息，发现实际的 VPN 实例路由数量已经达到路由上限。

```
Proto   total    original active  original added      deleted    freed
        routes   routes   routes  active   routes     routes     routes
DIRECT  10       10       10      10       10         0          0
STATIC  1        1        1       1        2          1          1
RIP     0        0        0       0        0          0          0
OSPF    8        8        6       6        13         5          5
IS-IS   0        0        0       0        0          0          0
BGP     81       81       34      34       0          0          0
Total   100      100      51      51       25         6          6
```

由于 VPN 实例路由数量已经达到路由限制的上限，来自 PE2 的新的 VPN 实例路由无法添加到 PE1 的 VPN 路由表中，这样就使得 AG 设备无法注册到软交换设备。

操作步骤

步骤 1 在 PE1 上执行命令 **system-view**，进入系统视图。

步骤 2 在 PE1 上执行命令 **ip vpn-instance** *vpn-instance-name*，进入 VPN 实例视图。

步骤 3 在 PE1 上执行命令 **routing-table limit 200 80**，重新限制当前 VPN 实例支持的最多路由。

完成上述操作后，CE1 上 pingCE2 可以 ping 通，CE1 可以注册到 CE2，故障排除。

----结束

案例总结

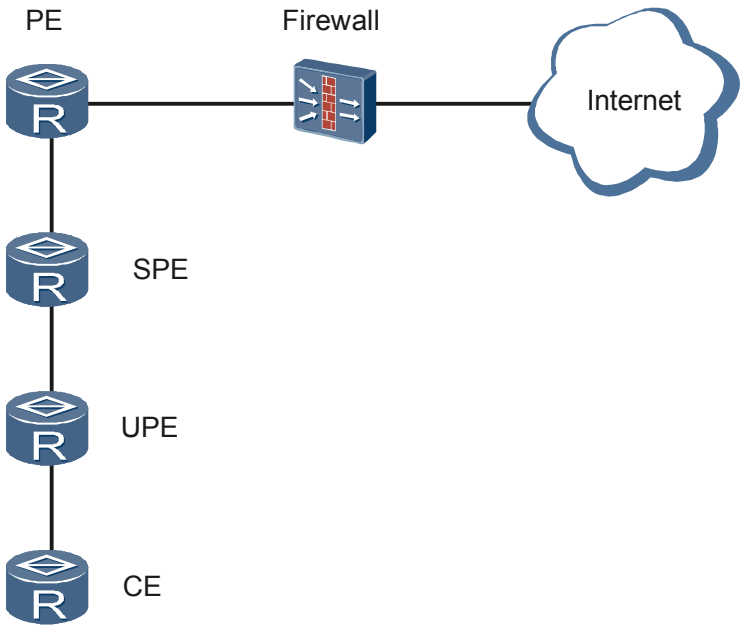
如果 VPN 实例配置了 VPN 实例的最大路由数量限制，需要确认实际的 VPN 实例路由数量是否已达路由限制的上限。

1.2.17 BGP/MPLS IP VPN 业务中 CE 侧用户无法正常访问外网

网络环境

在图 1-18 的网络中，中心 PE 与 SPE 连接，SPE 下连接 UPE，构成分层的结构。各 PE 上部署多个 VPN 实例，在一个 VPN 实例内有多个 Export RT 和 Import RT。中心 PE 上通过多个逻辑接口分别绑定各 VPN 实例并与防火墙连接。在 SPE 上对 UPE 下发各 VPN 缺省路由，用来引导上行流量。配置完成后，发现 CE 用户无法访问 Internet。

图 1-18 CE 侧用户无法正常访问外网组网图



故障分析

1. 在 UPE 上执行命令 **display ip routing-table vpn-instance**，可以看到各 VPN 实例可以学习到缺省路由，且在一个 VPN 实例中可学到 2 条缺省路由。
2. 在 UPE 上执行命令 **display current-configuration configuration vpn-instance**，查看 VPN 实例的配置，可以看到 UPE 的 VPN 实例配置了多个 Export RT 和 Import RT。
3. 在 SPE 上执行命令 **display current-configuration configuration vpn-instance**，查看 VPN 实例的配置，发现 SPE 上由于存在多个 VPN 实例的 RT 互相引入，将从两个 VPN 分别学到的缺省路由通过 Export RT 发布给了 UPE，并与 UPE 的 VPN 实例中的多个 Import RT 相匹配。这样导致 UPE 在一个 VPN 中学到多条缺省路由。这样 CE 流量上行到 SPE 后存在多个不同的 BGP 下一跳，在防火墙上无法正常建立状态表项，用户无法访问 Internet。

操作步骤

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

步骤 2 在 UPE 上执行命令 **ip vpn-instance** *vpn-instance-name*，进入 VPN 实例视图。

步骤 3 在 UPE 上执行命令 **vpn-target** *vpn-target* &<1-8> **import-extcommunity**，为 VPN 实例配置 VPN target 扩展团体属性。

UPE 上的每个 VPN 实例中只能配置一个 Import RT，这样只学到一条缺省路由。完成上述操作后，CE 侧用户可以正常访问 Internet，故障排除。

----结束

案例总结

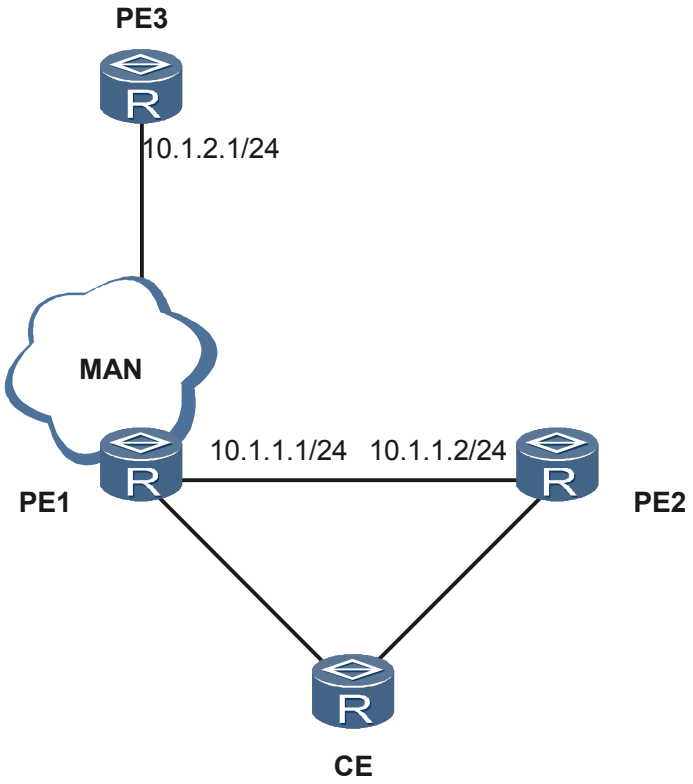
与普通 PE 或 SPE 不同，分层 PE 中的 UPE 仅需要缺省路由引导上行流量，因此在配置 RT 时根据情况可配置多个 Export RT，但只需要配置一个 Import RT 即可，否则可能会导致故障产生。

1.2.18 PE 的 VPNv4 路由无法生效

网络环境

在图 1-19 的网络中，三台 PE 设备上配置 BGP/MPLS VPN 业务。CE 设备的报文等值负载分担到 PE1 和 PE2 两台设备，PE1 通过城域网连接到 PE3，PE2 通过 PE1 连接 PE3。配置完成后，发现 PE1 可以正常学习到 10.1.2.0 网段的路由，PE2 的 BGP VPNv4 路由表中也可以看到 10.1.2.0 网段信息，但是在 PE2 的 VPN 实例路由表中没有 10.1.2.0 这个表项。

图 1-19 PE 的 VPNv4 路由无法生效组网图



故障分析

1. 在 PE2 上执行命令 **display bgp vpnv4 all routing-table**，查看 PE2 的 BGP VPNv4 的路由表时，发现虽然 PE2 学习到 10.1.2.0 网段路由，但不是最优路由。

```
     Network            NextHop        MED        LocPrf    PrefVal Community
*>   1.1.1.0/24         1.1.1.1          0                        0      no-export
*    1.1.1.2/32         1.1.1.1          0                        0      no-export
*i   10.1.2.0/24        10.1.1.1       100                        0      no-export
```

2. 在 PE2 上执行命令 **display ip routing-table vpn-instance vpn1 10.1.2.0 verbose**，查看 VPN 实例的路由表信息。

```
Routing Table : vpn1
Summary Count : 1

Destination: 10.1.2.0/24
    Protocol: BGP             Process ID: 0
  Preference: 255                   Cost: 0
     NextHop: 10.1.1.1        Interface: NULL0
RelayNextHop: 0.0.0.0         Neighbour: 10.1.1.1
       Label: 109568          Tunnel ID: 0x0
                            SecTunnel ID: 0x0
   BkNextHop: 0.0.0.0         BkInterface:
     BkLabel: NULL            Tunnel ID: 0x0
                            SecTunnel ID: 0x0
       State: Inactive Adv WaitQ     Age: 22h35m37s
```

通过路由信息可以看出，下一跳可达的出接口显示为 NULL0，报文被丢弃。

VPNv4 私网路由转发时，会去迭代公网的 LSP 表项完成转发。VPNv4 的路由在写入路由表的时候也会检查是否存在可以迭代的公网 LSP 表项，如果不存在，便不会写入 VPN 实例的路由表。

3. 在 PE2 上执行命令 **display mpls lsp**，发现不存在 10.1.1.1 的转发表项，说明 PE1 与 PE2 的邻居关系没有建立。

操作步骤

步骤 1 在 PE1 上分别执行命令 **system-view**，进入系统视图。

步骤 2 在 PE1 上分别执行命令 **mpls**，使能本节点的 MPLS，并进入 MPLS 视图。

步骤 3 在 PE1 上分别执行命令 **quit**，退回到系统视图。

步骤 4 在 PE1 上分别执行命令 **mpls ldp**，使能全局的 LDP 功能，并进入 MPLS-LDP 视图。

步骤 5（可选）在 PE1 上分别执行命令 **lsr-id** *lsr-id*，配置 LDP 实例的 LSR ID。

步骤 6 在 PE1 上分别执行命令 **quit**，返回系统视图。

步骤 7 在 PE1 上分别执行命令 **interface** *interface-type interface-number*，进入与对端 PE 相连接的接口视图。

步骤 8 在 PE1 上分别执行命令 **mpls**，使能接口的 MPLS 功能。

步骤 9 在 PE1 上分别执行命令 **mpls ldp**，使能接口的 LDP 功能。

说明

请在 PE2 上执行与 PE1 上相同的操作。

完成上述操作后，发现 PE1 上可以正常学习到 10.1.2.0 网段路由，PE2 的 BGP VPNv4 路由表中和 VPN 实例路由表中也存在到 10.1.2.0 网段信息，故障排除。

----结束

案例总结

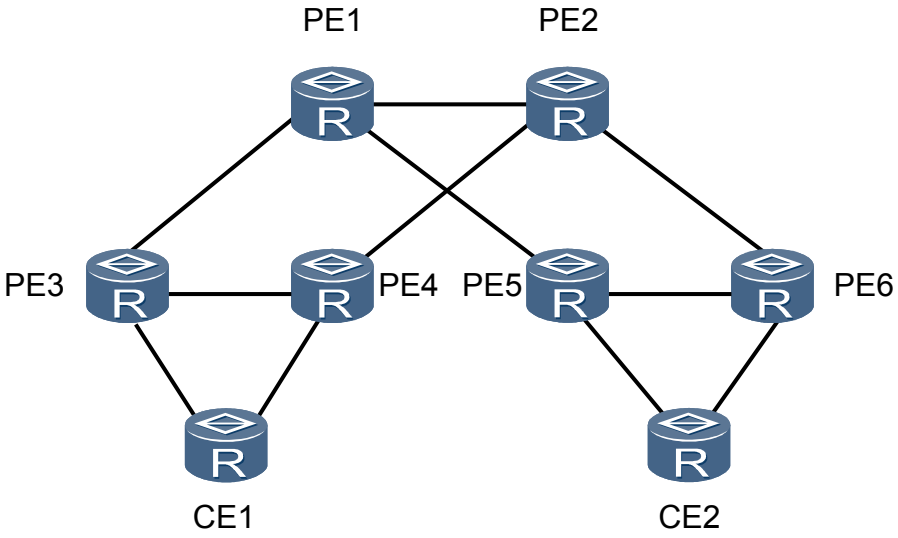
VPNv4 的私网路由在转发时，会去迭代公网的 LSP 表项来完成转发。此外 VPNv4 的路由在写入活跃路由的时候也会检查是否存在可以迭代的公网 LSP 表项。如果不存在，该 VPNV4 路由就不会被写入 VPNv4 的路由表中。

1.2.19 MPLS VPN 路由收敛速度慢

网络环境

6 台 PE 设备之间运行 ISIS 和 BGP 协议并配置了 MPLS VPN 业务协议。6 台 PE 设备都采用相同的 RD 值，PE1 和 PE2 作为 RR。PE1 的 Router ID 值小于 PE2 的 Router ID 值；PE3 的 Router ID 值小于 PE4 的 Router ID 值；PE5 的 Router ID 值小于 PE6 的 Router ID 值。两台 CE 属于同一个 VPN。

图 1-20 MPLS VPN 典型组网图



配置完成后，发现当 PE3 重启后，在 PE5 和 PE6 上需要等 2 分钟左右才能学习到 PE4 下 CE1 的业务网段。

故障分析

PE5 和 PE6 会通过 PE3 和 PE4 学习到 CE1 的两条 MPLS VPN 等价路由，因为 PE3 的 Router ID 值小于 PE4 的 Router ID 值，因此 IGP 路由表中只会选择 PE3 作为到 CE1 的路由。

当 PE3 重启时，两台 RR（PE1 和 PE2）需要等到确定与 PE3 已经无法建立 BGP 邻居关系后，才会向 PE5 和 PE6 转发 CE1 的业务网段路由。只有 IGP 协议状态正常之后，MPLS VPN 才开始建立邻居关系。而且 MPLS VPN 邻居建立的时间与路由器的路由表的数量有关，因此 MPLS VPN 路由表收敛速度较慢，一般在 2 分钟左右。

操作步骤

步骤 1 在 PE3 上执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip vpn-instance vpn-access** ，进入 PE3 上对应的 VPN 实例视图。

步骤 3 执行命令 **route-distinguisher 22:1**，将 PE3 上 VPN 实例的 RD 修改为与其他 PE 不同。

配置完成后，PE5 和 PE6 上会通过 PE3 和 PE4 分别学习到两条到 CE1 的 MPLS VPN 路由（其中一条为 active，另一条为 inactive），并且 PE5 和 PE6 的下一跳地址不同。

再次重启 PE3，MPLS VPN 的 active 路由消失，inactive 路由可以很快切换为 active 路由，不需要等待 IGP 路由正常后再收敛，因此 PE5 和 PE6 上的路由表收敛速度很快，故障排除。

----结束

案例总结

当因为 IGP 协议收敛慢导致 MPLS VPN 路由收敛慢时，可以通过配置不同的 RD 值，使 MPLS VPN 路由备份来解决此问题。采用 VPN FRR 也可以解决此问题。

1.2.20 未配置 vpn-target import-extcommunity 导致 CE 之间单通

网络环境

在图 1-21 的网络中，CE 设备（UMG）双归属接入 PE。PE 分别属于两个平面：

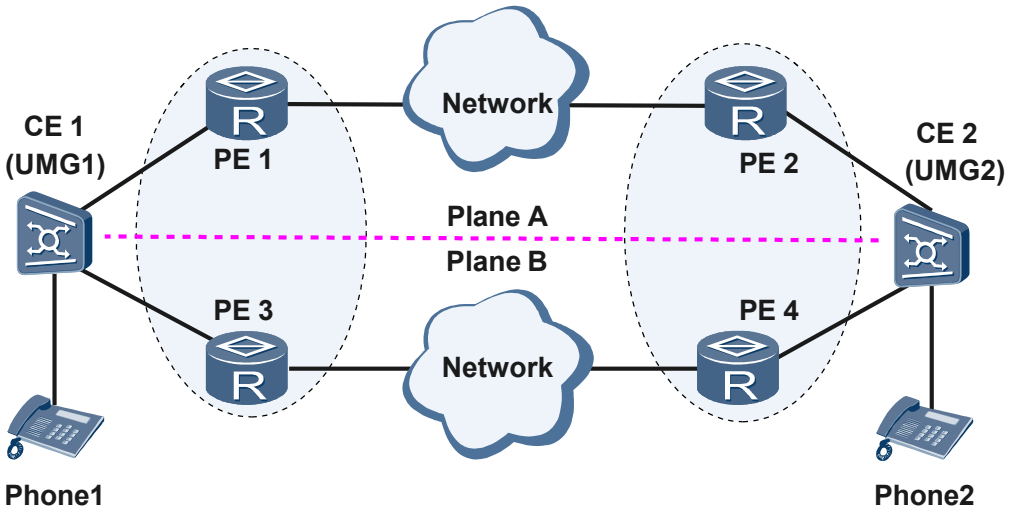
- PE1 与 PE2 属于平面 A。
- PE3 与 PE4 属于平面 B。

正常情况下 CE 之间流量主走平面 B。CE1 与 CE2 属于同一 VPN。

PE 上配置不同的 VPN 实例，分别用来承载 CE 设备的信令流量和媒体流量。

配置完成后，Phone1 与 Phone2 进行拨号测试通话，发现第一次拨通后 Phone2 可以听到 Phone1 的话音，而 Phone1 听不到 Phone2 的话音，CE 之间出现单通现象。第二次拨通后双方都可以正常听到对方话音。

图 1-21 CE 之间单通组网图



故障分析

1. CE 之间的呼叫可以建立，说明承载 CE 之间信令流量的 VPN 没有问题，故障只可能出现在承载 CE 之间媒体流量的 VPN 之中。
2. 在 PE3 上执行 **display current-configuration configuration vpn-instance** 命令，查看承载媒体流量的 VPN 配置。发现没有配置 **vpn-target import-extcommunity** 命令。

   这样，PE3 就无法接收从 PE4 发送来的承载媒体流量的 VPN 路由，从而导致 CE2 的媒体流量无法发送到 CE1（即 Phone2 的话音无法传送到 Phone1），因此出现了第一次拨通电话的单通故障现象。

   在 CE 侧，媒体流量通过主备方式发送到 PE。首次通话时，媒体流量通过平面 B 传输，一旦平面 B 上出现流量不通（即一端 CE 没收到另一端 CE 发送的流量），则下次拨号媒体流量就通过平面 A 传输，这样当第二次拨号时，双方通话正常。

操作步骤

步骤 1 在 PE3 上执行命令 **system-view**，进入系统视图。

步骤 2 在 PE3 上执行命令 **ip vpn-instance** *vpn-instance-name*，进入承载 CE 之间媒体流量的 VPN 实例视图。

步骤 3 在 PE3 上执行命令 **vpn-target** *vpn-target* &<1-8> **import-extcommunity**，为 VPN 实例配置 VPN-target 扩展团体属性，定义可以接收带有指定扩展团体属性值的路由信息。

完成上述操作后，Phone1 和 Phone2 重新拨号测试通话，通话正常。

----结束

案例总结

BGP/MPLS VPN 在 NGN（Next Generation Network）的应用组网中，不同的 VPN 实例分别用来承载 CE 设备的信令流量和媒体流量。发生故障时，需要根据故障现象来判断主要是信令流的 VPN 问题还是媒体流的 VPN 问题。

此外，配置 VPN 实例的属性时，VPN Target 没有缺省值，必须在创建 VPN 实例时配置。用户可以通过指定关键字“both/export/import”，来将当前 VPN 实例与一个或多个 VPN Target 进行关联，缺省值为“both”。

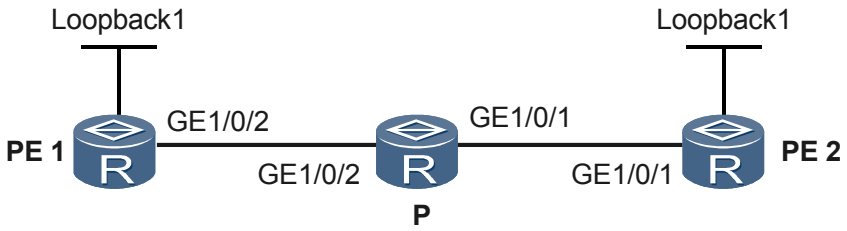
1.2.21 Loopback 接口的掩码未配置为 32 位导致 PE 间无法交换私网路由

网络环境

在图 1-22 的网络中配置 BGP/MPLS IP VPN 业务，两台 PE 与 P 之间启用了 OSPF 协议。在两台 PE 上分别创建一个 Loopback 接口，并绑定 VPN 实例 vpn1, PE1 与 PE2 的 loopback 地址分别为 1.1.1.1 和 1.1.1.2。

配置完成后，发现 PE 之间无法交换 VPN 私网路由，相互之间 ping 不通。

图 1-22 PE 之间无法交换 VPN 私网路由的组网图



故障分析

1. 在 PE 上执行 **display ospf peer** 命令，可以看到邻居状态 State 为 Full。在 PE 上执行 **display ip routing-table** 命令，可以看到 PE 之间学习到对方的 Loopback1 接口路由。

2. 在 P 上执行 **display mpls ldp session** 命令，可以看到 P 与 PE 之间的 LDP 对等体关系的 Status 为“Operational”，即 LDP 对等体关系已建立。
3. 在 PE 上执行 **display mpls lsp** 命令，检查标签分配情况，可以看到 PE 之间存在到对方的 LSP。
4. 在 PE 上在 BGP-VPNv4 地址族视图下执行 **display this** 命令，发现配置了 **peer** *ipv4-address* **enable** 命令。执行 **display bgp vpnv4 all peer** 命令，可以看到 State 字段为 Established，说明 PE 之间、PE 与 CE 之间的 BGP 对等体关系已建立，并达到 Established 状态。
5. 在 PE 上执行 **display ip routing-table vpn-instance vpn1** 命令，查看 VPN 路由表。发现存在一条路由：1.1.1.0/24 direct，出接口为设备的 Loopback1 接口，这条路由的掩码是 24 位，而不是 32 位。

   以 PE1 的显示为例。

   ```
   Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface
   1.1.1.0/24          Direct 0    0           D  1.1.1.1         LoopBack1
   ```

6. 在 PE 上执行 **display ip interface brief** 命令，发现 Loopback1 的接口 IP 地址掩码确实配置的是 24 位，而不是 32 位。

   以 PE1 的显示为例。

   ```
   Interface                  IP Address/Mask      Physical   Protocol
   LoopBack1                  1.1.1.1/24           up         up(s)
   ```

   这样，两台 PE 的 Loopback 地址便在同一网段内（1.1.1.0/24）。事实上，PE 设备已经收到了彼此的 VPN 路由，但是该 VPN 路由与自己的 Loopback1 地址在同一网段，相当于去往对端 PE 的 Loopback1 接口地址，同时有两条相同的路由，一条为直连路由，一条为 BGP 路由。此时设备会优选直连路由放入路由表中，所以 VPN 路由表中无私网路由，也就无法 ping 通对端 PE 的 Loopback1 接口地址。

操作步骤

步骤 1 在 PE1 和 PE2 上执行命令 **system-view**，进入系统视图。

步骤 2 在 PE1 和 PE2 上执行命令 **interface loopback1**，进入与 VPN 实例绑定的 Loopback1 接口视图。

步骤 3 在 PE1 和 PE2 上执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置接口 IP 地址，其中掩码为 32 位。

完成上述操作后，PE 可以互相 ping 通对端 PE 的 Loopback1 接口地址，故障排除。

----结束

案例总结

配置 BGP/MPLS IP VPN 时，需要注意不同 PE 上与同一个 VPN 实例绑定的接口，其 IP 地址应该配置为不同的网段。

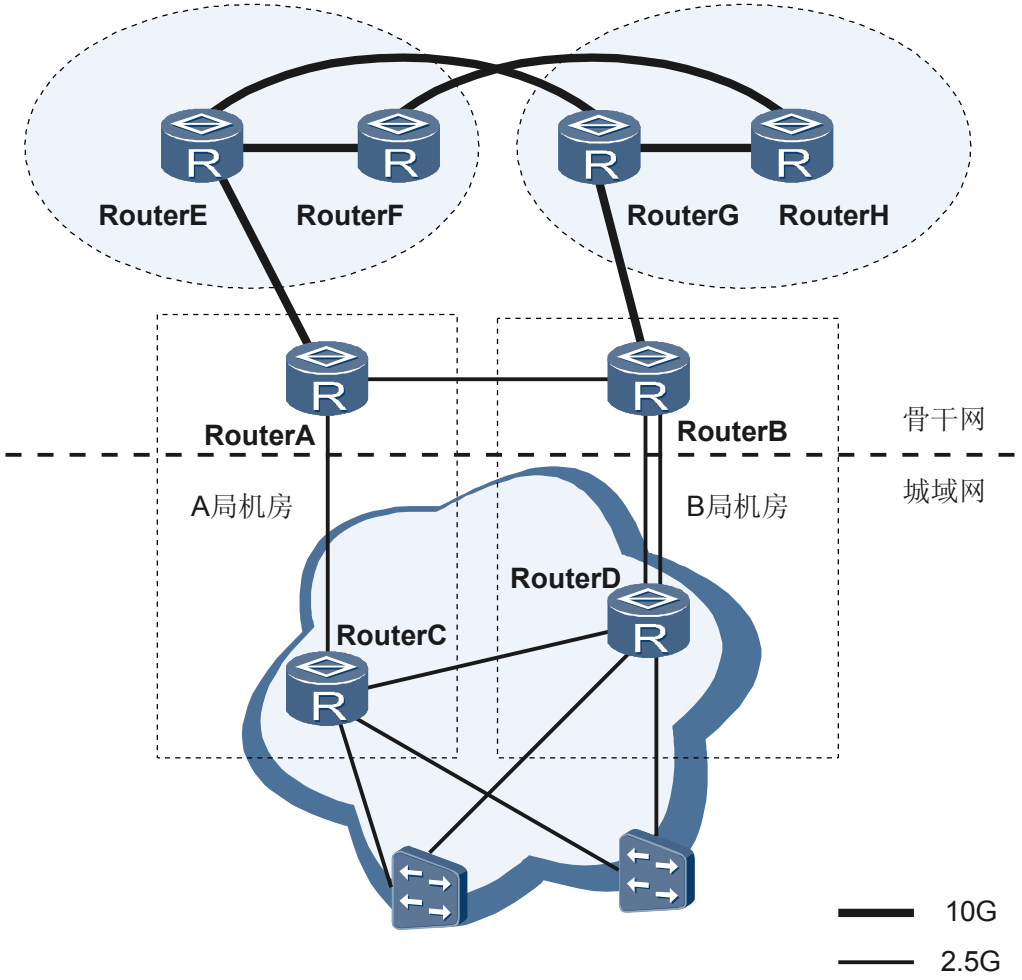
1.2.22 设备割接上线后部分 MPLS VPN 业务异常

网络环境

如图 1-23 所示，除 RouterA 外，其他设备均为其他厂商设备。某运营商的城域网核心现状是：A 局和 B 局分别使用其他厂商设备 RouterC 和 RouterD 作为城域网出口核心路由器。城域网出口总带宽为 3×2.5G，其中 A 局的 RouterC 到骨干节点 RouterA 的带宽为

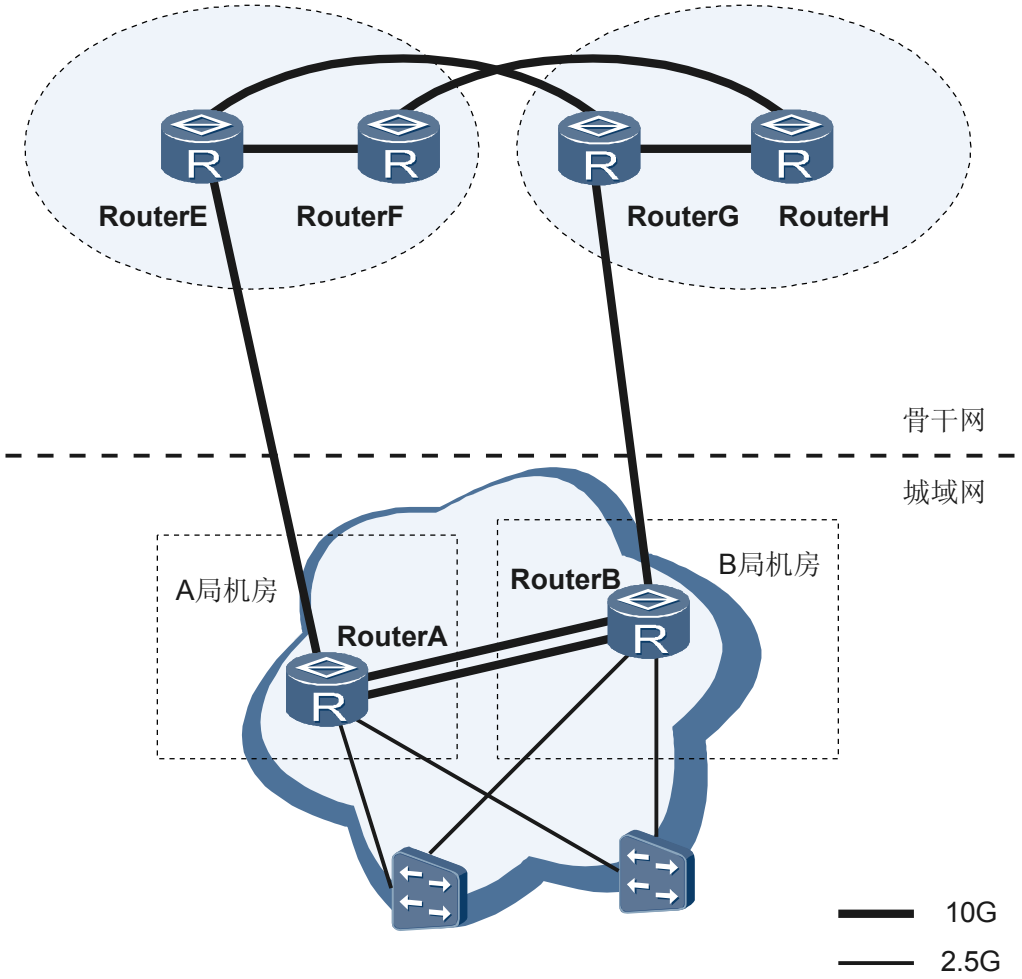
1×2.5G，B 局的 RouterD 到骨干节点 RouterB 的带宽为 2×2.5G。两骨干网节点的出口带宽为 2×10G。

图 1-23 运营商城域网割接前组网图



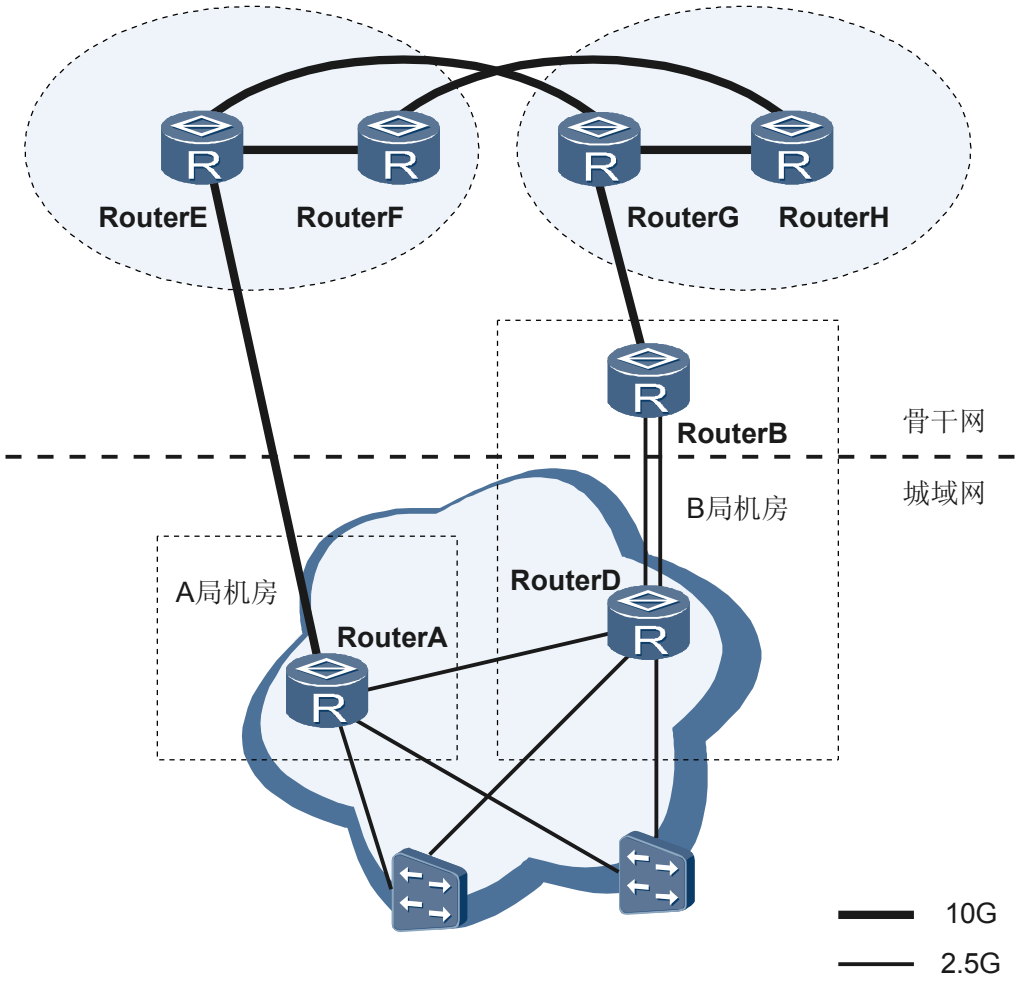
为适应业务的发展，该运营商对城域网和骨干网进行优化。如图 1-24 所示，将骨干节点 RouterA 和 RouterB 下沉至城域网出口核心路由器，直接与骨干网的 RouterE 和 RouterG 建立 EBGP 邻居关系；原城域网核心路由器留做他用。城域网保留私有 AS 号，两城域网核心路由器 RouterA 和 RouterB 之间建立 IBGP 邻居关系。原下挂在 RouterC 和 RouterD 上的 SR 和 BRAS 改接至 RouterA 和 RouterB。

图 1-24 运营商城域网割接后目标组网图



如图 1-25 所示，RouterA 完成割接后做业务测试时，发现 BRAS 下的部分 MPLS VPN 业务不正常，而同一 VPN 实例中部分用户的 MPLS VPN 业务正常。

图 1-25 运营商城域网割接后目标组网图



故障分析

1. 在 RouterA 上，执行 **display current-configuration configuration** 命令查看配置文件，没有问题。
2. 查看 RouterA 接口的 MTU 配置和 BRAS 配置，没有问题。
3. 在 RouterA 上使用命令 **ping lsp -a** *source-ip*（*source-ip* 为 RouterA 的 Loopback 地址）来 Ping BRAS 的 Loopback 地址，可以 ping 通，说明 RouterA 与 BRAS 之间转发没有问题。
4. 在 BRAS 上使用命令 **ping lsp -a** *source-ip*（*source-ip* 为 BRAS 的 Loopback 地址）来 Ping VPN 内无法通信的 PE 设备的 Loopback 地址，没有 Ping 通。
5. 在 BRAS 上，执行 **display mpls ldp peer** 命令来查看 LDP 对等体的信息时，发现 RouterD 与 BRAS 建立 LDP 对等体的地址不是 Loopback0 地址，而是 Loopback1 地址。因客户有特殊业务需求，将 RouterC 的 Loopback1 地址与 RouterA 的 Loopback1 地址设为相同。
6. 在 RouterA 上，执行 **display mpls ldp peer** 命令来查看 LDP 对等体时，发现 RouterD 与 RouterA 建立 LDP 对等体的地址也是 Loopback1 地址，而非 Loopback0 地址。

7. 在 RouterD 上，执行 **display current-configuration configuration** 命令查看配置文件，发现 RouterD 上建立 LDP 对等体的地址设置错误，本应设为 Loopback0 地址，却设成了 Loopback1 地址，导致部分 MPLS VPN 业务由 RouterD 转发而无法正常访问。RouterA 割接前是经过原城域网核心路由器访问，割接时将这部分流量转向 RouterD，但 RouterA 割接成功后没有及时将流量导回至 RouterA 而导致故障。

操作步骤

步骤 1 将 RouterD 上的 LDP 对等体地址设置为 Loopback0 地址。

----结束

案例总结

产生该问题的主要原因是 MPLS LSP 转发不正常。使用带有源地址的 **ping lsp** 命令在 PE 之间进行互 ping，有助于尽快定位此类故障原因。

2 VPLS 故障处理

关于本章

介绍了 VPLS 故障常见的原因和定位思路。

2.1 Martini 方式 VPLS 的 VSI 不能 Up 的定位思路
介绍 Martini 方式 VPLS 网络中 VSI 不能 Up 的故障处理流程和详细的故障处理步骤。

2.2 Kompella 方式 VPLS 的 VSI 不能 UP 的定位思路
介绍 Kompella 方式 VPLS 网络中 VSI 不能 UP 的故障处理流程和详细的故障处理步骤。

2.3 只有一端 VSI 状态 Up 的定位思路
介绍 VPLS 网络中只有一端 VSI 状态 Up 的故障处理流程和详细的故障处理步骤。

2.4 Kompella 方式 VPLS 和其他厂商设备互通，PW 无法建立的定位思路
介绍 Kompella 方式 VPLS 网络中华为设备和其他厂商设备互通，PW 无法建立的故障处理流程和详细的故障处理步骤。

2.5 相关案例

2.1 Martini 方式 VPLS 的 VSI 不能 Up 的定位思路

介绍 Martini 方式 VPLS 网络中 VSI 不能 Up 的故障处理流程和详细的故障处理步骤。

2.1.1 常见原因

本类故障的常见原因主要包括：

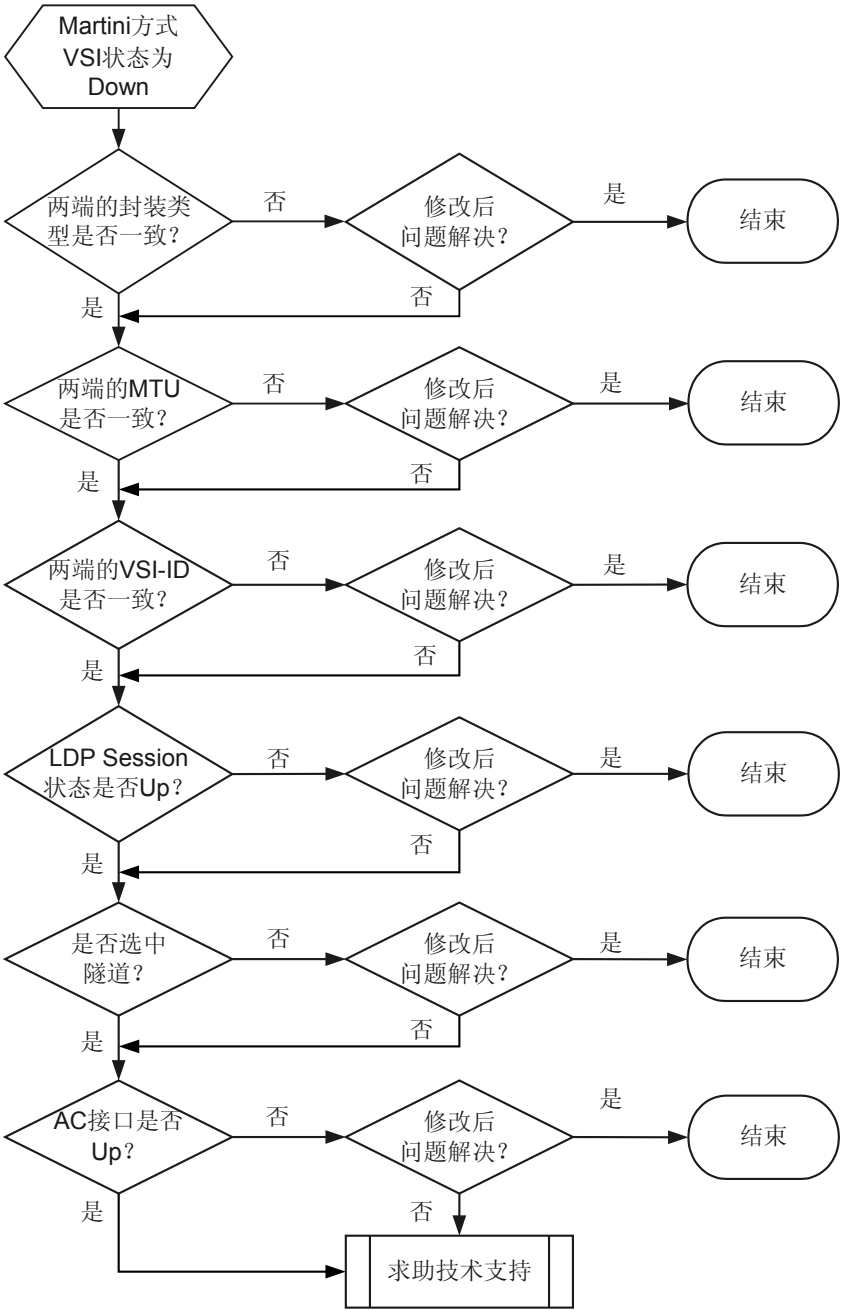
- 两端封装类型不一致。
- 两端 MTU 值不一致。
- 两端的 VSI-ID 不一致。
- LDP session 状态没有 Up。
- 公网隧道想选择 TE 隧道，但是隧道策略配置不正确。
- 本端或者远端的隧道没 Up。
- 本端或者远端的 AC 接口没有 Up。

2.1.2 故障诊断流程

在配置 Martini 方式 VPLS 后发现 VSI 不能 Up。

详细处理流程如图 2-1 所示。

图 2-1 Martini 方式 VPLS 的 VSI 不能 Up 的故障诊断流程图



2.1.3 故障处理步骤

说明

请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

操作步骤

步骤 1 检查两端的封装类型否一致

```
<HUAWEI> display vsi name tt
Vsi                         Mem    PW   Mac       Encap     Mtu   Vsi
Name                        Disc   Type Learn     Type      Value State
------------------------------------------------------------------------------
tt                          static ldp  unqualify vlan      1500  up
```

- 如果两端的封装类型不一致，在 VSI 视图下配置命令 **encapsulation** { **ethernet** | **vlan** } 修改其中一端的封装类型，使两端的封装类型一致。
- 如果两端的封装类型已经一致，请执行步骤 2。

说明

两端封装类型一致是 VSI 的状态 Up 的必要条件之一。

步骤 2 检查两端的 MTU 值是否一致

```
<HUAWEI> display vsi name tt
Vsi                         Mem    PW   Mac       Encap     Mtu   Vsi
Name                        Disc   Type Learn     Type      Value State
------------------------------------------------------------------------------
tt                          static ldp  unqualify vlan      1500  up
```

- 如果两端的 MTU 不一致，在 VSI 视图下配置命令 **mtu** *mtu-value* 修改其中一端的 MTU，使两端的 MTU 一致。
- 如果两端的 MTU 已经一致，请执行步骤 3。

说明

两端 MTU 一致是 VSI 的状态 Up 的必要条件之一。

步骤 3 检查两端的 VSI ID 值或者协商 ID 值是否一致

```
<HUAWEI> display vsi name tt verbose

 ***VSI Name               : tt
    Administrator VSI      : no
    Isolate Spoken         : disable
    VSI Index              : 3
    PW Signaling           : ldp
    Member Discovery Style : static
    PW MAC Learn Style     : unqualify
    Encapsulation Type     : vlan
    MTU                    : 1500
    Diffserv Mode          : uniform
    Service Class          : --
    Color                  : --
    DomainId               : 255
    Domain Name            :
    Tunnel Policy Name     : p1
    Ignore AcState         : disable
    Create Time            : 2 days, 2 hours, 47 minutes, 40 seconds
    VSI State              : up

    VSI ID                 : 101
   *Peer Router ID         : 2.2.2.2
    VC Label               : 187393
    Peer Type              : dynamic
    Session                : up
    Tunnel ID              : 0xc0060401

    Broadcast Tunnel ID    : 0xc0060401
    CKey                   : 6
    NKey                   : 5
    StpEnable              : 0
    PwIndex                : 0

    Interface Name         : GigabitEthernet8/0/0.12
    State                  : up
    Last Up Time           : 2010/02/05 06:36:57
    Total Up Time          : 2 days, 2 hours, 40 minutes, 19 seconds
```

- 如果两端的 VSI ID 值或者协商 ID 值不一致，在 VSI-LDP 视图下配置命令 **pwsignal ldp** 修改其中一端的 VSI ID 值，或者在 VSI-LDP 视图下配置命令 **peer** *peer-address* **negotiation-vc-id** *vc-id* 修改协商 ID 值，使两端一致。
- 如果两端的 VSI ID 值或者协商 ID 值已经一致，请执行步骤 4。

说明

两端的 VSI ID 值或者协商 ID 值一致是 VSI 的状态 Up 的必要条件之一。

步骤 4 检查两端的 LDP 会话是否 UP

执行 **display vsi name** *vsi-name* **verbose** 命令，检查 Session 字段值是否为 Up。

```
<HUAWEI> display vsi name tt verbose

 ***VSI Name               : tt
    Administrator VSI      : no
    Isolate Spoken         : disable
    VSI Index              : 3
    PW Signaling           : ldp
    Member Discovery Style : static
    PW MAC Learn Style     : unqualify
    Encapsulation Type     : vlan
    MTU                    : 1500
    Diffserv Mode          : uniform
    Service Class          : --
    Color                  : --
    DomainId               : 255
    Domain Name            :
    Tunnel Policy Name     : p1
    Ignore AcState         : disable
    Create Time            : 2 days, 2 hours, 47 minutes, 40 seconds
    VSI State              : up

    VSI ID                 : 101
   *Peer Router ID         : 2.2.2.2
    VC Label               : 187393
    Peer Type              : dynamic
    Session                : up
    Tunnel ID              : 0xc0060401
    Broadcast Tunnel ID    : 0xc0060401
    CKey                   : 6
    NKey                   : 5
    StpEnable              : 0
    PwIndex                : 0

    Interface Name         : GigabitEthernet8/0/0.12
    State                  : up
    Last Up Time           : 2010/02/05 06:36:57
    Total Up Time          : 2 days, 2 hours, 40 minutes, 19 seconds
```

- 如果两端的 LDP 会话没有 UP，请参见“LDP 会话 DOWN”一节继续定位，使 LDP 会话状态为 Up。
- 如果 LDP 会话状态已经是 Up，请执行步骤 5。

说明

只有 LDP 会话 Up，两端的 L2VPN 才能开始协商。

步骤 5 检查 VSI 是否选中隧道

执行 **display vsi name** *vsi-name* **verbose** 命令：

- 检查 Tunnel ID 字段值是否为 0x0。如果 Tunnel ID 字段为 0x0，表明 VSI 没有选中隧道。
- 检查 Tunnel Policy Name 字段的值，如果没有显示该字段，表示 VSI 使用的隧道为 LDP LSP，或者没有为 VSI 配置隧道策略。如果 VSI 使用 MPLS-TE 隧道需要配置隧

道策略。Tunnel Policy Name 字段值表示 VSI 使用隧道策略，可以在隧道策略视图下执行 **display this** 检查隧道策略的配置。

```
[HUAWEI-tunnel-policy-p1] display this
#
tunnel-policy p1
 tunnel select-seq cr-lsp load-balance-number 1
#
```

说明

如果隧道策略下配置了 **tunnel binding destination** *dest-ip-address* **te** { **tunnel** *interface-number* }，还需要在 Tunnel 接口下使能 **mpls te reserved-for-binding** 命令。

如果两端的隧道没有 Up，请参考“LSP 隧道 down”一节或者“Te Tunnel 状态为 down”一节继续定位，使隧道状态 Up。如果两端的隧道状态已经 UP 并且 TE 接口配置正确，请执行步骤 6。

说明

隧道 Up 是 VSI 的状态 Up 的必要条件之一。

步骤 6 检查两端的 AC 接口状态是否 Up

在两端 PE 上分别执行 **display vsi name** *vsi-name* **verbose** 命令，检查 Interface Name 字段对应的接口的 State 是否为 Up。

- 如果两端的 AC 接口状态没有 Up，请参考“物理对接&接口类”一节继续定位，使 AC 接口状态 Up。
- 如果两端 AC 接口状态已经 Up，请执行步骤 7。

说明

两端 AC 接口状态 Up 是 VSI 的状态 Up 的必要条件之一。

步骤 7 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

2.1.4 相关告警与日志

相关告警

无

相关日志

无

2.2 Kompella 方式 VPLS 的 VSI 不能 UP 的定位思路

介绍 Kompella 方式 VPLS 网络中 VSI 不能 UP 的故障处理流程和详细的故障处理步骤。

2.2.1 常见原因

本类故障的常见原因主要包括：

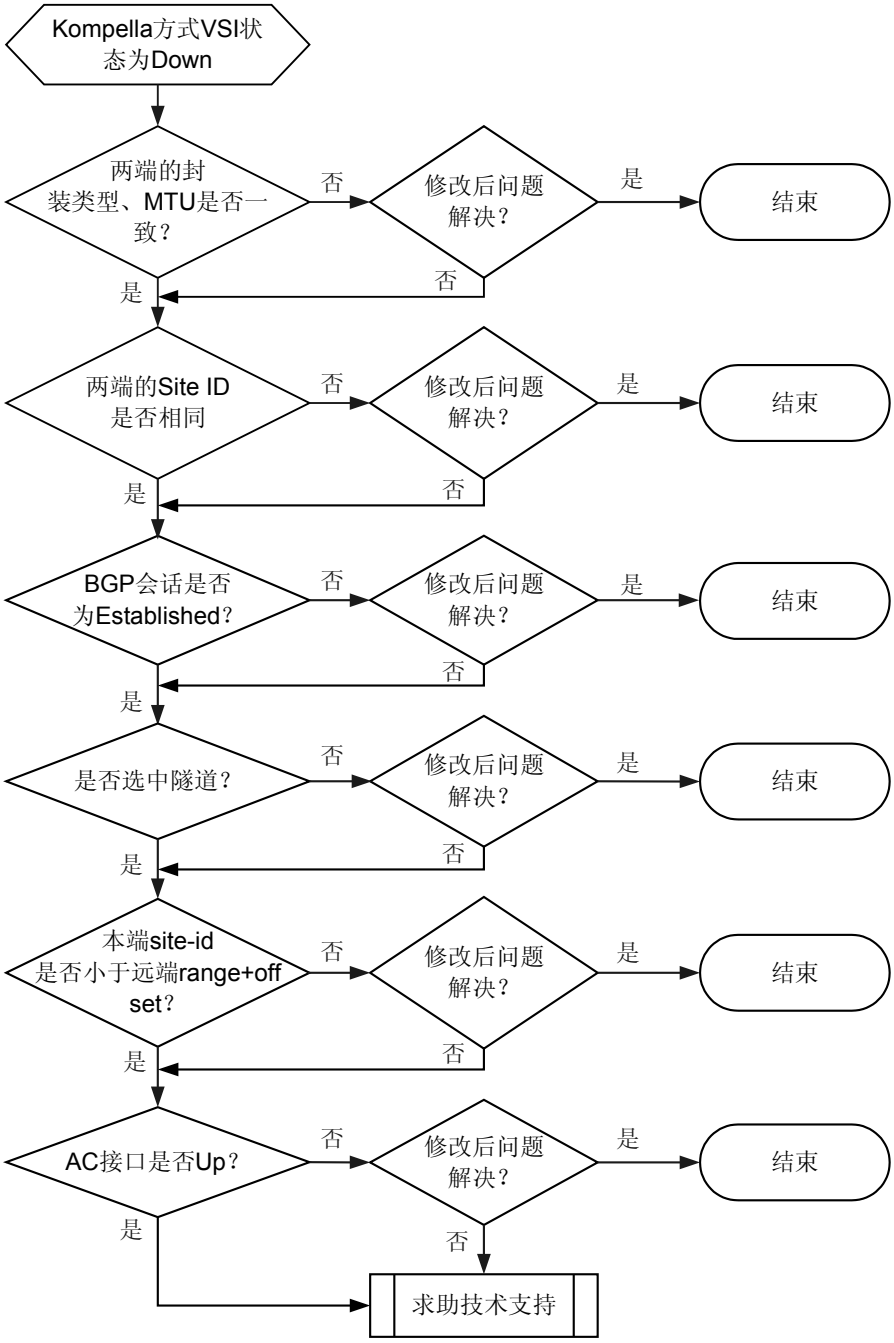
- 两端封装类型不一致。
- 两端 MTU 值不一致。
- BGP 状态不是“Established”。
- 公网隧道想选择 TE 隧道，但是隧道策略配置不正确。
- 本端的 site-id 大于远端 range+offset。
- 本端或者远端的 AC 接口没有 Up。

2.2.2 故障诊断流程

在配置 Kompella 方式 VPLS 后发现 VSI 不能 Up。

详细处理流程如图 2-2 所示。

图 2-2 Kompella 方式 VPLS 的 VSI 不能 UP 的故障诊断流程图



2.2.3 故障处理步骤

说明

请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

操作步骤

步骤 1 检查两端的封装类型及 MTU 是否一致

```
<HUAWEI> display vsi name tt2
Vsi                          Mem    PW   Mac       Encap      Mtu   Vsi
Name                         Disc   Type Learn     Type       Value State
------------------------------------------------------------------------------
tt2                          auto   bgp  unqualify vlan       1500  up
```

- 如果两端的封装类型或者 MTU 不一致，在 VSI 视图下配置命令 **encapsulation** { **ethernet** | **vlan** }修改其中一端的封装类型，或者配置命令 **mtu** *mtu* 修改其中一端的 MTU，使两端的封装类型、MTU 一致。
- 如果两端的封装类型及 MTU 已经一致，请执行步骤 2。

说明

两端封装类型、MTU 一致是 VSI 状态 Up 的必要条件之一。

步骤 2 检查两端的 site ID 是否重复

```
[HUAWEI-vsi-tt2] display this
#
vsi tt2 auto
 pwsignal bgp
  route-distinguisher 200:1
  vpn-target 201:1 import-extcommunity
  vpn-target 201:1 export-extcommunity
  site 1 range 10 default-offset 0
#
return
```

- 如果两端的 site ID 重复，请执行 **site** *site-id* [**range** *site-range*] [**default-offset** { **0** | **1** }] 命令修改其中一端的 site ID 值，使两端的 site ID 不同。
- 如果两端的 site ID 值已经不同，请执行步骤 4。

说明

同一 VSI 的 site ID 不能够相同。

步骤 3 检查两端的 BGP 会话状态是否为 Established

执行 **display bgp vpls peer** [*ipv4-address* **verbose** | **verbose**] [| **count**] [| { **begin** | **exclude** | **include** } *regular-expression*]命令，检查两端的 BGP 会话状态。

```
<HUAWEI> display bgp vpls peer
 BGP local router ID : 200.1.1.1
 Local AS number : 100
 Total number of peers : 1                 Peers in established state : 1

Peer            V    AS  MsgRcvd  MsgSent    OutQ  Up/Down       State PrefRcv
1.1.1.1         4   100       14       16       0 00:10:06    Established    0
```

- 如果两端的 BGP 会话状态不是 Established，请参考 **BGP 邻居无法建立的定位思路**，使 BGP 会话状态成为 Established。
- 如果 BGP 会话状态已经为 Established，请执行步骤 4。

说明

只有 BGP 会话状态为 Established，两端的 L2VPN 才能开始协商。

步骤 4 检查 VSI 是否选中隧道。

执行 display vsi name vsi-name verbose 命令：

- 检查 Tunnel ID 字段值是否为 0x0。如果 Tunnel ID 字段为 0x0，表明 VSI 没有选中隧道。

- 检查 Tunnel Policy Name 字段的值。如果没有显示该字段，表示 VSI 使用的隧道为 LDP LSP，或者没有为 VSI 配置隧道策略。

  说明

  如果 VSI 使用 MPLS-TE 隧道需要配置隧道策略。

  Tunnel Policy Name 字段值表示 VSI 使用隧道策略，可以在隧道策略视图下执行 **display this** 检查隧道策略的配置。

```
[HUAWEI-tunnel-policy-p1] display this
#
tunnel-policy p1
 tunnel select-seq cr-lsp load-balance-number 1
#
```

说明

如果隧道策略下配置了 **tunnel binding destination** *dest-ip-address* **te** { **tunnel** *interface-number* }，还需要在 Tunnel 接口下使能 **mpls te reserved-for-binding** 命令。

如果两端的隧道没有 Up，请参考 **LDP LSP Down 的定位思路**或者 **TE Tunnel 状态为 Down 的定位思路**继续定位，使隧道状态 Up。如果两端的隧道状态已经 Up 并且 TE 接口配置正确，请执行步骤 6。

说明

隧道 Up 是 VSI 状态 Up 的必要条件之一。

步骤 5 检查本端的 site ID 是否小于远端的 range 与 default offset 之和。

```
[HUAWEI-vsi-tt2] display this
#
vsi tt2 auto
 pwsignal bgp
  route-distinguisher 168.1.1.1:1
  vpn-target 100:1 import-extcommunity
  vpn-target 100:1 export-extcommunity
  site 1 range 5 default-offset 0
#
returen
```

- 如果本端的 site ID 没有小于远端的 rang+default-offset 之和，则修改本端 site ID 或者远端 range 使之满足条件。
- 如果本地 site ID 已经小于远端 range+default-offset 之和，并且远端 site ID 小于本端的 range+default-offset 之和，请执行步骤 6。

步骤 6 检查两端的 AC 接口状态是否 Up

在两端 PE 上分别执行 **display vsi name** *vsi-name* **verbose** 命令，检查 Interface Name 字段对应的接口的 State 是否为 Up。

- 如果两端的 AC 接口状态没有 Up，请参考“物理对接&接口类”一节继续定位，使 AC 接口状态 Up。
- 如果两端 AC 接口状态已经 Up，请执行步骤 8。

步骤 7 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

2.2.4 相关告警与日志

相关告警

无

相关日志

无

2.3 只有一端 VSI 状态 Up 的定位思路

介绍 VPLS 网络中只有一端 VSI 状态 Up 的故障处理流程和详细的故障处理步骤。

2.3.1 常见原因

本类故障的常见原因主要包括：

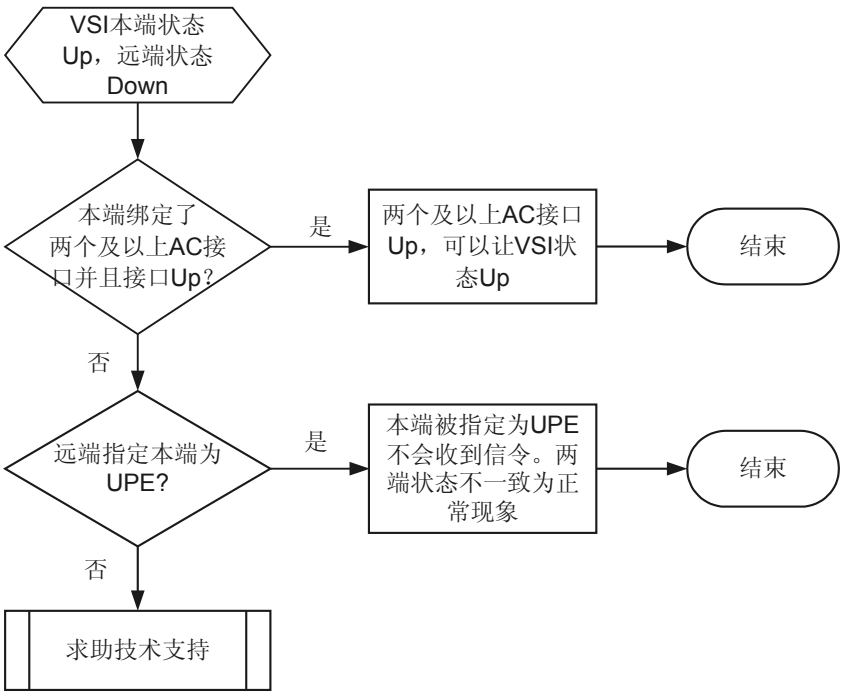
- 对端指定本端为 UPE。
- 本端有多个状态为 Up 的 AC 接口绑定到这个 VSI 但 PW 没有选到隧道。

2.3.2 故障诊断流程

在配置 VPLS 后发现只有一端 VSI 状态为 Up。

详细处理流程如图 2-3 所示。

图 2-3 只有一端 VSI 状态为 Up 的故障诊断流程图



2.3.3 故障处理步骤

说明

请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

操作步骤

步骤 1 确认本端是否有多个 AC 接口绑定到这个 VSI。

```
<HUAWEI> display vsi name tt verbose
 ***VSI Name               : tt
    Administrator VSI      : no
    Isolate Spoken         : disable
    VSI Index              : 3
    PW Signaling           : ldp
    Member Discovery Style : static
    PW MAC Learn Style     : unqualify
    Encapsulation Type     : vlan
    MTU                    : 1500
    Diffserv Mode          : uniform
    Service Class          : --
    Color                  : --
    DomainId               : 255
    Domain Name            :
    Tunnel Policy Name     : p1
    Ignore AcState         : disable
    Create Time            : 2 days, 6 hours, 3 minutes, 55 seconds
    VSI State              : up

    VSI ID                 : 101
   *Peer Router ID         : 2.2.2.2
    VC Label               : 187393
    Peer Type              : dynamic
    Session                : up
    Tunnel ID              : 0xc0060401
    Broadcast Tunnel ID    : 0xc0060401
    CKey                   : 6
    NKey                   : 5
    StpEnable              : 0
    PwIndex                : 0

    Interface Name         : GigabitEthernet8/0/0.12
    State                  : up
    Last Up Time           : 2010/02/05 06:36:57
    Total Up Time          : 2 days, 5 hours, 56 minutes, 34 seconds
    Interface Name         : GigabitEthernet8/0/0.3
    State                  : up
    Last Up Time           : 2010/02/07 12:33:13
    Total Up Time          : 0 days, 0 hours, 0 minutes, 18 seconds
```

说明

如果有两个及以上的接口绑定到此 VSI，此 VSI 状态是可以 Up 的。

步骤 2 远端是否指定本端为 UPE，远端 AC 接口故障。

```
[HUAWEI-vsi-tt-ldp] display this
#
  vsi-id 101
  peer 1.1.1.1 upe
#
```

- 如果远端指定本端为 upe，远端 AC 接口故障后不会通知本端撤销标签，可能出现只有一端 VSI 状态 Up。
- 如果远端没有指定本端为 upe，请执行步骤 3。

步骤 3 果上述步骤执行后故障还未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

2.3.4 相关告警与日志

相关告警

无

相关日志

无

2.4 Kompella 方式 VPLS 和其他厂商设备互通，PW 无法建立的定位思路

介绍 Kompella 方式 VPLS 网络中华为设备和其他厂商设备互通，PW 无法建立的故障处理流程和详细的故障处理步骤。

2.4.1 常见原因

本类故障的常见原因主要包括：

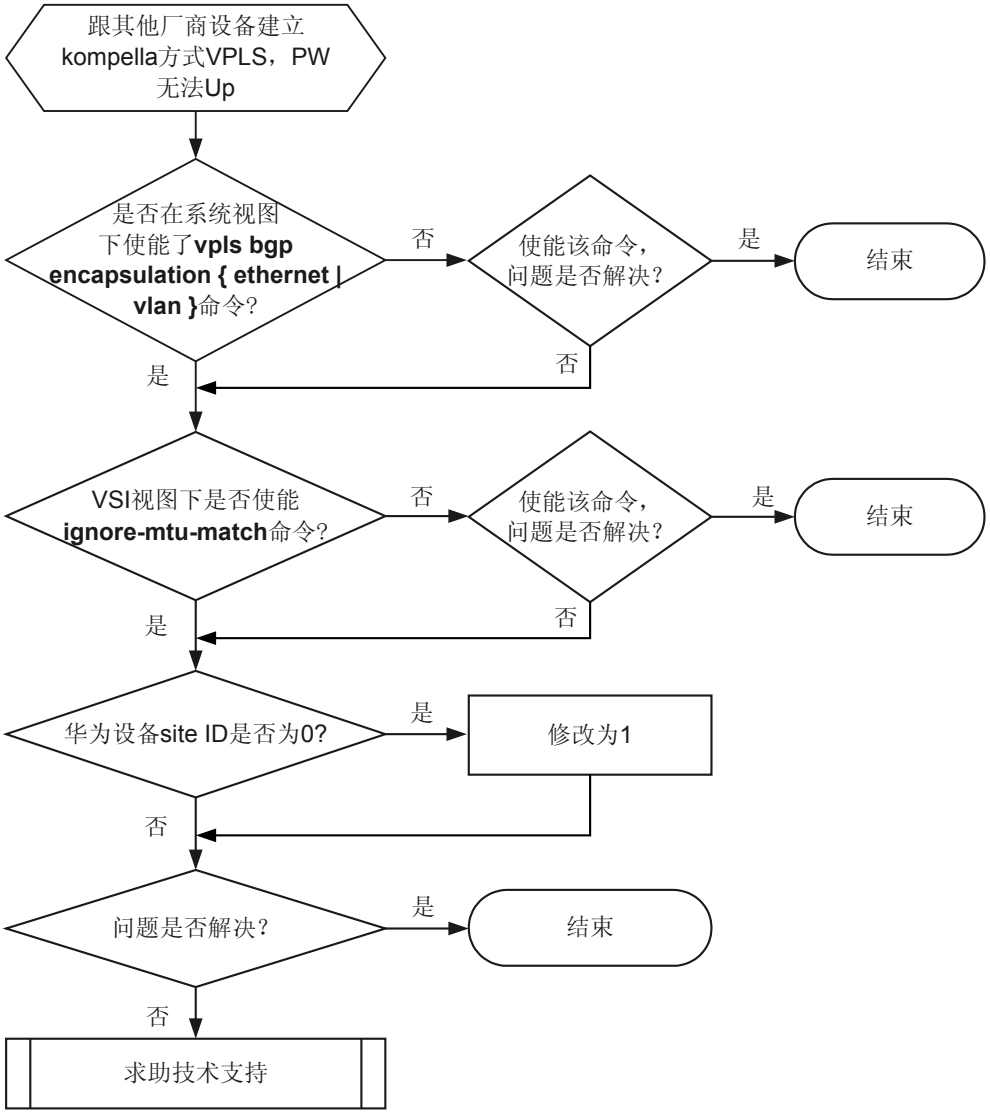
- 系统视图下未使能 **vpls bgp encapsulation** { **ethernet** | **vlan** }命令。
- VSI 视图下未使能 **ignore-mtu-match** 命令。
- 其他设备厂商的 default-offset 是 1，且无法配置，华为设备在与其他设备厂商互通时，需要将 default-offset 配置为 1，且 site ID 不要为 0。

2.4.2 故障诊断流程

在配置 Kompella 方式 VPLS 后发现华为设备和其他厂商设备互通，PW 无法建立。

详细处理流程如图 2-4 所示。

图 2-4 Kompella 方式 VPLS 和其他厂商设备互通，PW 无法建立的故障诊断流程图



2.4.3 故障处理步骤

说明

请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

操作步骤

步骤 1 系统视图下是否使能 **vpls bgp encapsulation** { **ethernet** | **vlan** }命令。

- 如果没有使能以上命令，请先配置这条命令。
- 如果已经配置了这条命令行，请执行步骤 2。

说明

其他厂商设备在 BGP 的 L2VPN 地址族下默认配置了“signaling”命令，其发送的 BGP Update 协议报文中使用的地址族是 VPLS 的地址族（AFI=25，SAFI=65），但其协议报文中多了一个非标准的 CSV 字段。该字段虽然在 Kompella VLL 中存在，但在 VPLS 的 RFC（RFC 4761）里并未规定。华为设备对于 VPLS 和 Kompella VLL 使用不同的地址族，因此在收到 Update 报文后通过解析发现是 VPLS地址族，在后续按 VPLS 报文进行处理时发现多了一个非标准的 CSV 字段（对于 VPLS 的报文来说没有此字段），造成协议报文长度不对，从而导致 BGP 邻居无法建立。

步骤 2 VSI 视图下是否使能了 **ignore-mtu-match** 命令。

- 如果没有使能以上命令，请先配置这条命令。
- 如果已经配置了这条命令行，请执行步骤 3。

说明

使能这条命令用来忽略跟其他厂商设备进行 MTU 的协商。

步骤 3 华为设备的 default-offset 是否配置为 1。

```
[HUAWEI-vsi-tt2] display this
#
vsi tt2 auto
 pwsignal bgp
  route-distinguisher 168.1.1.1:1
  vpn-target 100:1 import-extcommunity
  vpn-target 100:1 export-extcommunity
  site 1 range 5 default-offset 0
#
return
```

- 如果 default-offset 不为 1，请修改 default-offset 为 1。
- 如果已经是 1，请执行步骤 4。

步骤 4 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

2.4.4 相关告警与日志

相关告警

无

相关日志

无

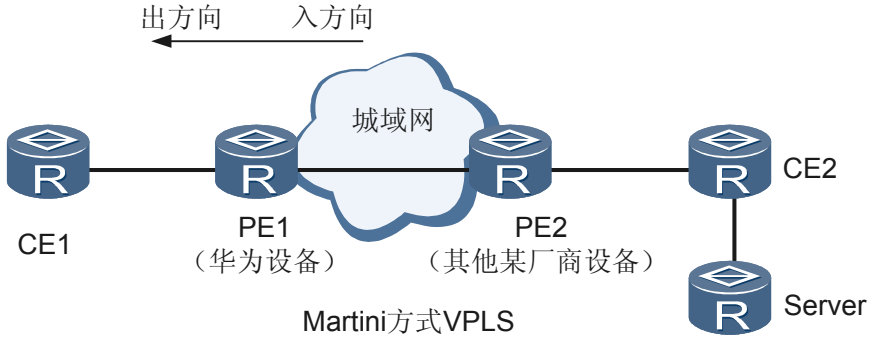
2.5 相关案例

2.5.1 VPLS 业务不通

网络环境

如图 2-5 所示，华为公司设备替换其他厂商的设备，成为新的 PE1 后，除 VPLS 业务不通外，其他业务正常。

图 2-5 Martini 方式 VPLS 组网图



故障分析

说明

华为设备替换其他厂商设备后只有 VPLS 业务不通，可排除网络链路故障及现网其他设备异常。

1. 在 PE1 上执行命令 **display current-configuration**，查看 PE1 的配置是否错误，以及和对端 PE2 的配置是否一致。可确认数据配置正确。
2. 在 PE1 上执行命令 **display vpls connection**，查看字段“VCState”的值。“VCState”为 Up，表明二层隧道已正常建立。
3. 在 CE1 ping Server 时，在 PE1 上执行命令 **display traffic-statistics vsi** *vsi-name* [**peer** *peer-address* [**negotiation-vc-id** *vc-id*]]，查看报文收发是否正常。可确认报文收发正常。
4. 在 CE1 ping Server 时，在城域网其他设备上抓取 PE1 入方向的 VPLS 报文和出方向的 VPLS 报文。

   抓取 PE1 入方向报文如下：

   ```
   0018 821D 2010 0014 1CD2 FC06 8847 22C0
   01FE 0019 E019 0D9E 0019 21D5 5FD6 0806
   0001 0800 0604 0002 0019 21D5 5FD6 0303
   0301 0019 E019 0D9E 0303 0302 0000 0000
   ```

   从上述报文中的 0806 字段可以看出，对端 PE2 发送过来的 VPLS 报文并没有带 VLAN tag，仅仅是普通的 ARP 报文。而两端 VSI 的封装方式都配置为 VLAN，导致 PE1 将 VSI 报文做添加 tag 处理。即在 PE1 上对报文添加 tag 之后，从 PE1 出方向转发出去。

   PE1 转发的出方向报文为：

   ```
   0019 E019 0D9E 0019 21D5 5FD6 8100 019b
   0800 0604 0002 0019 21D5 5FD6 0303 0301
   0019 E019 0D9E 0303 0302 0000 0000 0000
   ```

   PE1 将 ARP 报文中的 0806 字段（ARP 报文标识）覆盖成 8100（VLAN 报文标识）从而导致该报文不是 ARP 报文，所以业务不通。让其他厂商的 VLAN 封装方

式上送 VLAN 标签或将两端设备的 VSI 均改成 Ethernet 封装方式，则故障可以解决。

操作步骤

- 方法一：修改其他厂商设备的 VLAN 封装方式上送 VLAN 标签。
- 方法二：修改华为公司设备和其他厂商设备的 VSI 封装方式为 Ethernet。华为公司设备的配置如下：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **vsi** *vsi-name*，进入 VSI 视图。
  3. 执行命令 **encapsulation ethernet**，配置 VSI 的封装形式为 Ethernet。

     最终 CE 之间可以互通，VPLS 业务正常。

----结束

案例总结

什么原因导致 PE1 报文解析错误而 VPLS 二层隧道能够 Up?

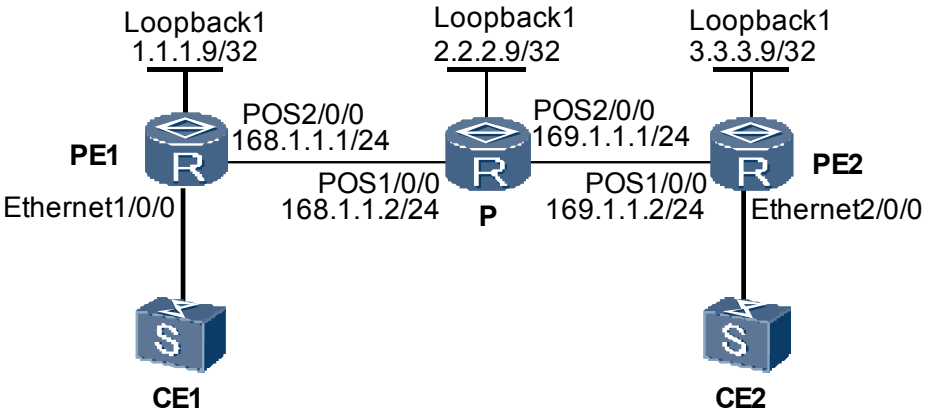
检查其他厂商设备，发现该设备的 VPLS 的收报文模式为混合模式，即任意报文均可以处理，但收到 VLAN 封装的 VPLS 报文则不带 VLAN 标签向外转发。从而导致 PE1 出现报文解析错误而二层隧道 Up 的故障。

根据 RFC4448 中规定：如果报文封装为 tagged 模式，在 PW 上传递的报文必须带 VLAN。

2.5.2 信令协议使用 LDP，VSI 不能进入 Up 状态

组网环境

图 2-6 VPLS 组网图



PE1、PE2 上配置以 LDP 为信令协议的 VPLS，在 PE1 上发起 CE-Ping，探测 CE2 上的 IP 地址，无法正常获得探测结果。通过查看原因得知 VSI 不能进入 Up 状态。

故障分析

1. 查看 PE1、PE2 上 VSI 的状态

   执行命令 **display vsi verbose**。

   PE1 上的显示结果如下：

```
VSI Name            : v1
    VSI Index               : 0
    PW Signaling            : ldp
    Member Discovery Style  : static
    PW MAC Learn Style      : unqualify
    Encapsulation Type      : vlan
    MTU                     : 1500
    VSI State               : down
    VSI ID                  : 1
   *Peer Router ID          : 3.3.3.9
    VC Label                : 17409
    Session                 : up
    Tunnel ID               : 0x6002002,
    Interface Name          : Ethernet1/0/0
    State                   : up
```

   PE2 上的显示结果如下：

```
VSI Name                    : v1
      VSI Index               : 0
      PW Signaling            : ldp
      Member Discovery Style  : static
      PW MAC Learn Style      : unqualify
    Encapsulation Type      : vlan
      MTU                     : 1500
      VSI State               : down
      VSI ID                  : 1
     *peer Router ID          : 2.2.2. 9
      VC Label                : 17408
     Session                 : up
     Tunnel ID               : 0x6002001,
     Interface Name          : Ethernet2/0/0
     State                   : up
```

   两端 AC 均为 UP。查看 PW 发现两端隧道存在（显示结果中存在“Tunnel ID”），且 Tunnel ID 的值不为 0x0。

2. 查看上述 PE1 和 PE2 上的 **display vsi verbose** 信息中有关 PW 的信息，发现 PE2 的远端 LDP Peer 指定错误，应该指定为 1.1.1.9，而不是 2.2.2.9。更改指定的 Peer。

操作步骤

步骤 1 PE 上执行 **display vsi verbose** 命令。

步骤 2 查看 VSI 状态和 AC 状态，发现 VSI 状态为 Down，AC 状态为 Up。

步骤 3 查看 PW 状态，发现 PW 不能建立。

步骤 4 查看隧道是否存在，发现隧道存在。

步骤 5 查看上述 PE1 和 PE2 上的 **display vsi verbose** 信息中有关 PW 的信息，发现 PE2 的远端 LDP Peer 指定错误，导致 PW 无法建立。远端 LDP Peer 应该指定为 1.1.1.9，而不是 2.2.2.9。更改指定的 Peer。

步骤 6 重新配置 PE2 的远端 LDP Peer，指定为 1.1.1.9。PW 成功建立。

----结束

案例总结

信令协议使用 LDP，VSI 不能进入 Up 状态，与 Peer 相关的配置错误有三种情况：

- Peer 指定错误；
- Peer 的地址不是对端的 LSR-ID，使得 LDP Remote Session 没有建立；
- 对端的 LSR-ID 被重新定义，使得 LDP Session 没有建立。

VSI 状态 Up 的条件是：至少两个 AC 状态为 Up；或者至少一个 AC 状态为 Up 并且一个 PW 状态为 Up。

定位这类问题时，可以从 AC、PW 状态入手。

AC Up 的条件比较简单：绑定了物理接口，且物理接口的协议状态为 Up。

问题通常出在 PW 上。PW 状态 Up 的条件较多，如 MTU、封装类型、VSI ID、对端的 Peer 的配置等。其中，关键是本端是否收到对端的标签、以及对端是否收到本端的标签。

可以使用 **display vsi remote** { **ldp** | **bgp** }命令。通过是否收到标签判断哪台路由器的配置出了问题。

2.5.3 VSI Up，但两个 PE 间转发不成功

组网环境

配置 VPLS 后，在 PE 上查看 VSI 状态，发现 VSI 为 Up，但两个 PE 间转发不成功。

故障分析

1. 查看 PW 是否存在。

   使用 **display vsi verbose** 查看 PW 是否存在。如果 PW 不存在，则表明 PW 信息没有下发到接口板。所以检查一下 PW 的下发状态是否为“up”。如果不是“up”，则转发信息还未下发到接口板，导致转发不成功。如果 PW 的下发状态是“up”转发仍然不成功，则应检查具体产品的接口板工作状态。

2. 查看配置的 MAC-limit 数值。

   如果 PW 已经存在，但两个 PE 间转发不成功，则使用 **display current-configuration | begin vsi** *vsi-name* 命令查看配置的 MAC-limit 数值。如果 MAC 地址表项的数目超过了配置的 MAC-limit 数值，请重新配置 MAC-limit 数值。

3. 查看 BGP 的对等体是否已重新建立。

   如果 MAC 地址的数目没有超过配置的 MAC-limit 数值，则使用 **display bgp peer** *peer-address* 命令查看 BGP 的对等体是否已成功建立。如果 BGP 的对等体正在重新建立，在很短的时间内，VSI 状态始终为 UP。

4. 查看两端 PE 的封装模式。

   如果 BGP 的对等体已经建立，则使用 **display current-configuration | begin vsi** *vsi-name* 查看两端 PE 的封装模式，如果两端 PE 的封装模式不一样，请重新配置两端 PE 的封装模式为一致。

   如果上述方法仍未能排除故障，请联系华为的技术支持工程师。

操作步骤

步骤 1 用 **display vsi** 命令检查对应 PW 的状态是否为 Up。

步骤 2 用 **display vpls connection** 命令检查 PW 是否存在。

步骤 3 如果已经 up 转发仍然不成功则应检查具体产品的接口板工作状态。

----结束

案例总结

VSI Up，但两个 PE 间转发不成功的故障原因可能是：

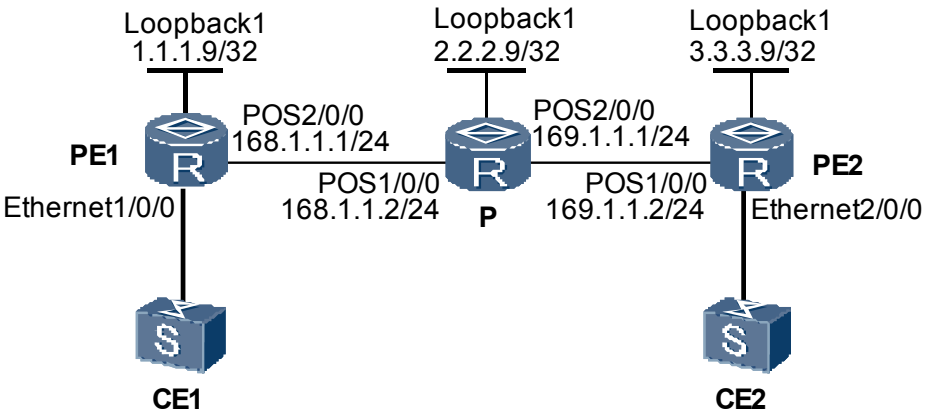
- PW 信息没有下发到接口板；
- MAC 地址表项的数目超过了配置的 MAC-limit 数值；
- BGP 的对端体正在重新建立，由于时间短，所以 VSI 状态始终为 UP；
- 两端 PE 封装模式不一样。

2.5.4 信令协议使用 BGP，VSI 不能进入 Up 状态

组网环境

PE1 与 PE2 之间建立 IBGP 关系并配置 VSI。配置完成后，PE1 和 PE2 上的 VSI 均不能进入 Up 状态。

图 2-7 VPLS 组网图



故障分析

1. 查看 PE1、PE2 上 VSI 的状态

   执行命令 **display vsi verbose**。

   PE1 的显示结果如下：

```
***VSI Name                 : bgp1
   VSI Index                : 0
   PW Signaling             : bgp
```

```
    Member Discovery Style : auto
    PW MAC Learn Style     : unqualify
    Encapsulation Type     : vlan
    MTU                    : 1500
    VSI State              : down
    BGP RD                 : 1:1
    SiteID/Range/Offset    : 1/10/0
    Import vpn target      : 2:2,
    Export vpn target      : 2:2,
    Local Label Block      : 19456/10/0,
    Interface Name         : Ethernet1/0/0
    State                  : up
```

PE2 的显示结果如下：

```
***VSI Name               : bgp1
    VSI Index              : 0
    PW Signaling           : bgp
    Member Discovery Style : auto
    PW MAC Learn Style     : unqualify
    Encapsulation Type     : vlan
    MTU                    : 1500
    VSI State              : down
    BGP RD                 : 1:2
    SiteID/Range/Offset    : 2/10/0
    Import vpn target      : 2:2,
    Export vpn target      : 2:2,
    Local Label Block      : 19456/10/0,
    Interface Name         : Ethernet2/0/0
    State                  : up
```

2. 查看是否收到对端标签

   在 PE1 和 PE2 上执行 **display vsi remote bgp** 命令，没有显示任何信息，这表示没有收到对端发来的标签。

   推断问题出在 BGP 的配置上。

操作步骤

步骤 1 查看 AC，发现两端 AC 均为 UP。

步骤 2 执行命令 **display vsi remote bgp**，没有任何信息显示，表示没有收到标签。

步骤 3 查看 VPN-Target 是否匹配。

步骤 4 如果 VPN-Target 匹配，查看隧道是否存在。

步骤 5 如果隧道存在，执行命令 **display bgp peer** 查看 BGP 邻居是否建立。

步骤 6 如果 BGP 邻居已经建立，执行 **display bgp vpls all** 查看是否收到对端标签块。发现没有收到远端标签块。

步骤 7 查看 BGP 配置，发现没有配置 VPLS 地址族。配置 VPLS 地址族后问题解决。

----结束

案例总结

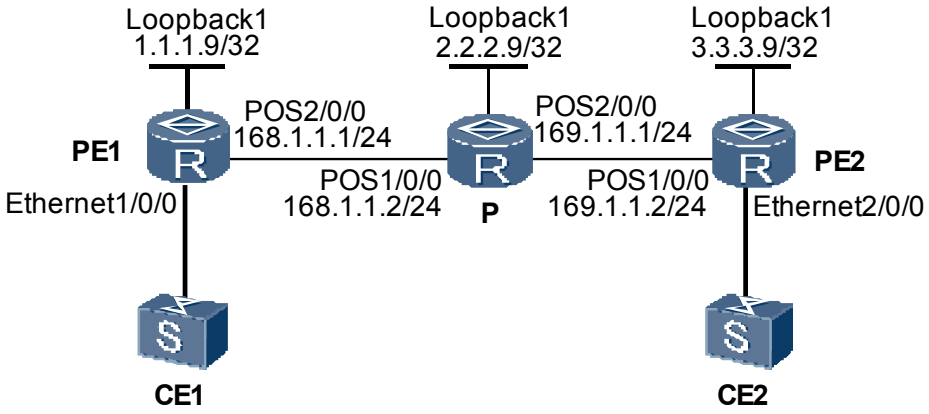
在 VPLS 配置中，采用 BGP 的信令方式与采用 LDP 信令方式的区别在于：BGP 中需要配置 VPLS 地址族，并在地址族下使能对端 peer。

使用 BGP 作为信令协议时，需要检查 BGP VPLS 的 peer 是否能够建立、是否能够接收到远端的标签块。VSI 能否进入 Up 状态仍然受 AC 和 PW 影响。另外，也要注意封装类型和 MTU 的设置。

2.5.5 VSI Up，但是设备之间仍无法互通

组网环境

图 2-8 VPLS 组网图



PE1、PE2 上配置以 BGP 为信令协议的 VPLS，VSI 能进入 Up 状态，但是 PE 之间无法实现互通

故障分析

1. 查看 PE1、PE2 上 VSI 的状态

   执行命令 **display vsi verbose**。

   PE1 上的显示结果如下：

```
***VSI Name               : v1
    VSI Index             : 0
    PW Signaling          : bgp
    Member Discovery Style : auto
    PW MAC Learn Style    : unqualify
    Encapsulation Type    : vlan
    MTU                   : 1500
    VSI State             : up
    BGP RD                : 168.1.1.1:1
    SiteID/Range/Offset   : 3/10000/0
    Import vpn target     : 100:1,
    Export vpn target     : 100:1,
    Remote Label Block    : 141293/10000/0,
    Local Label Block     : 140288/10000/0,
    Interface Name        : Vlan100
    State                 : up
   *Peer Ip Address       : 3.3.3.9
    PW State              : up
    Local VC Label        : 140289
    Remote VC Label       : 141296
    PW Type               : label
    Tunnel ID             : 0x1009,
```

   PE2 上的显示结果如下：

```
***VSI Name               : v1
    VSI Index             : 0
    PW Signaling          : bgp
    Member Discovery Style : auto
```

```
  PW MAC Learn Style      : unqualify
  Encapsulation Type      : ethernet
  MTU                     : 1500
  VSI State               : up
  BGP RD                  : 169.1.1.2:1
  SiteID/Range/Offset     : 3/10000/0
  Import vpn target       : 100:1,
  Export vpn target       : 100:1,
  Remote Label Block      :, 140288/10000/0
  Local Label Block       : 141293/10000/0,
  Interface Name          : Vlan100
  State                   : up
 *Peer Ip Address         : 1.1.1.9
  PW State                : up
  Local VC Label          : 141296
  Remote VC Label         : 140289
  PW Type                 : label
  Tunnel ID               : 0x1009,
```

两端 AC 均为 UP。查看 PW 发现两端隧道存在（显示结果中存在“Tunnel ID”），且 Tunnel ID 的值不为 0x0。

2. 在 PE2 执行 **display vsi remote bgp** 命令

   显示结果如下：

```
  Total Number     : 1
  **BGP RD             : 169.1.1.2:1                    Number     : 1
    NextHop            : 200.200.200.12
    EncapType          : ethernet
    MTU                : 1500
    Export vpn target  : 100:1,
    SiteID             : 3
    Remote Label Block : 140288/10000/0,
```

从显示结果可看出：PE2 认为从对端 PE1 接收到的 VPLS 报文的封装类型是 **ethernet**,但是从步骤 1 的内容可以看的到，PE1 发出的 VPLS 的报文封装类型是 **vlan**，发送和接收端认为 VPLS 报文的封装结构不同而导致设备无法互通。

操作步骤

步骤 1 PE 上执行 **display vsi verbose** 命令。

步骤 2 查看 VSI 状态和 AC 状态，发现 VSI 状态为 Up，AC 状态为 Up。

步骤 3 查看隧道是否存在，发现隧道存在。

步骤 4 在 PE 上使用 **display vsi remote bgp** 命令查看本端 PE 设备指定的接收到的 VPLS 报文的封装类型。发现本端指定接收到的 VPLS 报文的封装类型和对方实际封装的 VPLS 报文的类型不一致。

步骤 5 在 PE 上使用 **vpls bgp encapsulation** 命令重新指定本端 PE 设备接收到的 VPLS 报文的封装方式，使其和对端 PE 发出的 VPLS 报文的封装类型一致。

----结束

案例总结

在和友商设备互通时，本端 PE 设备指定接收到的 VPLS 报文的封装方式要和对端 PE 发出的 VPLS 报文的封装类型一致，否则设备之间无法互通。

2.5.6 由于报文封装方式不同导致 PE 设备之间的 VPLS 业务不通

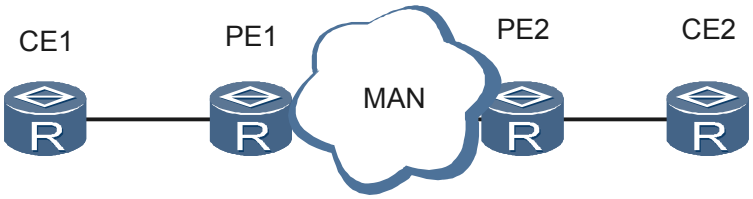
网络环境

在图 2-9 的网络中。PE 之间配置 VPLS 业务，其中 PE1 为 NE80E/40E，PE2 为其他厂商的设备。配置完成后，发现 CE 之间无法互通，VC 状态为 Down。

执行命令 **display mpls l2vc**，显示信息如下：

```
Total ldp vc : 1     0 up       1 down
 *Client Interface     : GigabitEthernet1/0/2.0
  Session State        : up
  AC Status           : up
  VC State            : down
  VC ID               : 6
  VC Type             : vlan
  Destination          : 1.1.1.1
  Local VC Label       : 117760
  Remote VC Label      : 0
  Control Word         : Disable
  Local VC MTU        : 1518
  Remote VC MTU       : 0
  Tunnel Policy Name   : --
  Traffic Behavior Name: --
  PW Template Name     : --
  Create time          : 0 days, 0 hours, 24 minutes, 56 seconds
  UP time              : 0 days, 0 hours, 0 minutes, 0 seconds
  Last change time     : 0 days, 0 hours, 24 minutes, 56 seconds
```

图 2-9 PE 设备之间的 VPLS 业务不通组网图



故障分析

1. 在 PE1 上执行命令 **display current-configuration**，查看 VSI 的相关配置确认没有配置错误。
2. 在 PE1 上执行命令 **display vpls connection**，检查 VPLS 的连接信息，VSI 的标签分配正确，VSI 的状态也为 Up。

```
1 total connections,
connections: 1 up, 0 down, 1 ldp
VSI Name: v1                                  Signaling: ldp
VsiID   EncapType              PeerAddr          InLabel   OutLabel  VCState
1       vlan                   1.1.1.1           17408     17409     up
```

3. 在 PE1 上执行命令 **display mpls l2vc**，查看报文的封装类型。

```
  Total ldp vc : 1     0 up       1 down
 *Client Interface     : GigabitEthernet1/0/2.0
  Session State        : up
  AC Status           : up
  VC State            : down
  VC ID               : 6
  VC Type             : vlan
```

发现发送过来的 ARP 报文被 PE1 转发出去的时候加上了 VLAN 报文标识，而 PE2 设备对报文的封装方式为 Ethernet，两端设备的封装方式不同，因此 VPLS 业务不通。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vsi** *vsi-name*，进入 VSI 视图。

步骤 3 执行命令 **encapsulation ethernet**，配置 VSI 的封装方式为 Ethernet 封装。

完成上述操作后，VPLS 业务恢复正常，CE 之间可以互通，故障排除。

----结束

案例总结

PE2 设备的 VPLS 业务的接收报文模式为混合模式，该模式下带 VLAN Tag 或者不带 VLAN Tag 的报文都可以处理。但如果收到 VLAN 封装的报文，则转发时不带 VLAN 标签，从而就导致 PE1 出现报文解析错误的故障现象。

根据 RFC4448 中规定：如果报文封装为 Tagged 模式，则在 PW 上传递的报文必须带 VLAN Tag。

3 VLL 故障处理

关于本章

介绍了 VLL 故障常见的原因和定位思路。

3.1 Martini 方式 VLL 的 VC 不能 UP 的定位思路

3.2 Kompella 方式 VLL 的 VC 不能 UP 的定位思路
介绍 Kompella 方式 VLL 网络中 VC 不能 UP 的故障处理流程和详细的故障处理步骤。

3.3 Kompella 方式 VLL 两端 AC 接口为以太子接口，封装类型为 tagged，PW 无法 Up 的定位思路
介绍 Kompella 方式 VLL 网络中两端 AC 接口为以太子接口，封装类型为 tagged，PW 无法 Up 的详细的故障处理步骤。

3.4 Kompella 方式的 VLL 和其他厂商设备互通 VC 不能 Up 的定位思路
介绍 Kompella 方式网络中 VLL 和其他厂商设备互通 VC 不能 Up 的详细的故障处理步骤。

3.5 相关案例

3.1 Martini 方式 VLL 的 VC 不能 UP 的定位思路

3.1.1 常见原因

本类故障的常见原因主要包括：

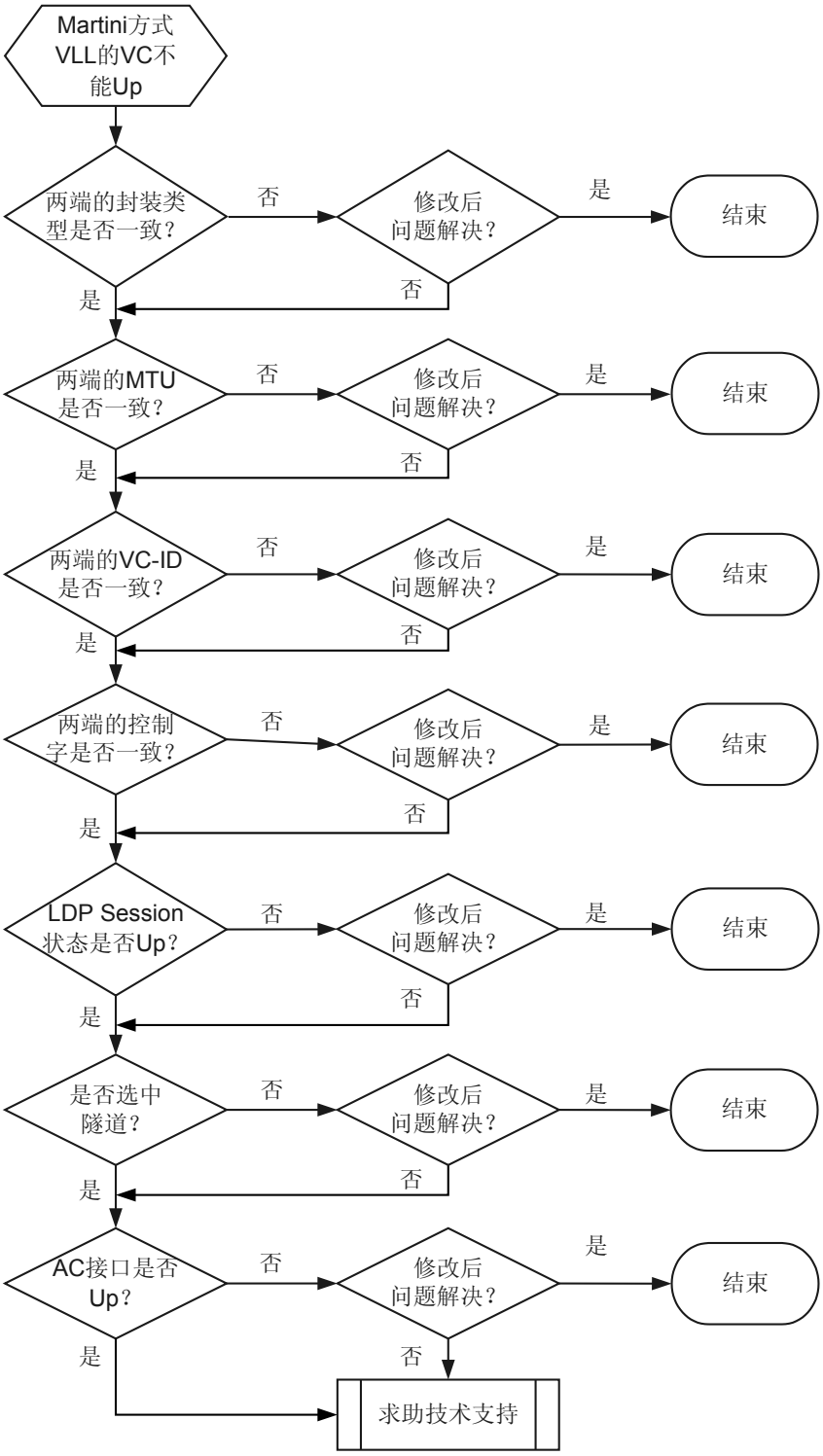
- 两端封装类型不一致。
- 两端 MTU 值不一致。
- 两端的 VC-ID 不一致。
- 两端的控制字配置不一致。
- LDP session 状态没有 Up。
- 公网隧道想选择 TE 隧道，但是隧道策略配置不正确。
- 本端或者远端的隧道没有 Up。
- 本端或者远端的 AC 接口没有 Up。

3.1.2 故障诊断流程

在配置 Martini 方式 VLL 后发现 VC 不能 Up。

详细处理流程如图 3-1 所示。

图 3-1 Martini 方式 VLL 的 VC 不能 UP 的故障诊断流程图



3.1.3 故障处理步骤

说明

请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

操作步骤

步骤 1 检查两端的封装类型及 MTU 是否一致

执行 **display mpls l2vc** *vc-id* 命令，检查 VC 信息。

```
<HUAWEI> display mpls l2vc 102
 total LDP VC : 1     1 up       0 down

 *client interface     : GigabitEthernet8/0/0.5
  session state        : up
  AC status            : up
  VC state             : up
  VC ID                : 102
  VC type              : VLAN
  destination          : 2.2.2.2
  local VC label       : 146433       remote VC label      : 146432
  control word         : disable
  forwarding entry     : exist
  local group ID       : 0
  manual fault         : not set
  active state         : active
  link state           : up
  local VC MTU         : 1500         remote VC MTU        : 1500
  tunnel policy name   : --
  traffic behavior name: --
  PW template name     : --
  primary or secondary : primary
  create time          : 1 days, 1 hours, 14 minutes, 17 seconds
  up time              : 0 days, 0 hours, 3 minutes, 16 seconds
  last change time     : 0 days, 0 hours, 3 minutes, 16 seconds
  VC last up time      : 2010/02/17 08:23:07
  VC total up time     : 0 days, 21 hours, 43 minutes, 43 seconds
```

如果两端的封装类型或者 MTU 不一致，那么修改其中一端的封装类型及 MTU 使两端的封装类型及 MTU 一致。

如果两端的封装类型及 MTU 已经一致，请执行步骤 2。

说明

两端封装类型、MTU 一致是 VC 状态 Up 的必要条件之一。

步骤 2 检查两端的 VC ID 是否一致

```
<HUAWEI> display mpls l2vc 102
 total LDP VC : 1     1 up       0 down

 *client interface     : GigabitEthernet8/0/0.5
  session state        : up
  AC status            : up
  VC state             : up
  VC ID                : 102
  VC type              : VLAN
  destination          : 2.2.2.2
  local VC label       : 146433       remote VC label      : 146432
  control word         : disable
  forwarding entry     : exist
  local group ID       : 0
  manual fault         : not set
  active state         : active
  link state           : up
  local VC MTU         : 1500         remote VC MTU        : 1500
  tunnel policy name   : --
```

```
 traffic behavior name: --
 PW template name     : --
 primary or secondary : primary
 create time          : 1 days, 1 hours, 14 minutes, 17 seconds
 up time              : 0 days, 0 hours, 3 minutes, 16 seconds
 last change time     : 0 days, 0 hours, 3 minutes, 16 seconds
 VC last up time      : 2010/02/17 08:23:07
 VC total up time     : 0 days, 21 hours, 43 minutes, 43 seconds
```

如果两端的 VC ID 不一致，那么修改其中一端的 VC ID 使两端的 VC ID 一致。

如果两端的 VC ID 已经一致，请执行步骤 3。

说明

两端 VC ID 一致是 VC 状态 Up 的必要条件之一。

步骤 3 检查两端的 CW 配置是否一致

```
<HUAWEI> display mpls l2vc 102
 total LDP VC : 1     1 up       0 down

 *client interface     : GigabitEthernet8/0/0.5
  session state        : up
  AC status            : up
  VC state             : up
  VC ID                : 102
  VC type              : VLAN
  destination          : 2.2.2.2
  local VC label       : 146433       remote VC label      : 146432
  control word         : disable
  forwarding entry     : exist
  local group ID       : 0
  manual fault         : not set
  active state         : active
  link state           : up
  local VC MTU         : 1500         remote VC MTU        : 1500
  tunnel policy name   : --
  traffic behavior name: --
  PW template name     : --
  primary or secondary : primary
  create time          : 1 days, 1 hours, 14 minutes, 17 seconds
  up time              : 0 days, 0 hours, 3 minutes, 16 seconds
  last change time     : 0 days, 0 hours, 3 minutes, 16 seconds
  VC last up time      : 2010/02/17 08:23:07
  VC total up time     : 0 days, 21 hours, 43 minutes, 43 seconds
```

如果两端的 CW 配置不一致，那么修改其中一端的 CW 配置使两端的 VC ID 一致。

如果两端的 CW 配置已经一致，请执行步骤 4。

说明

两端 CW 配置一致是 VC 状态 Up 的必要条件之一。

步骤 4 检查两端的 LDP 会话状态是否 UP

```
<HUAWEI> display mpls l2vc 102
 total LDP VC : 1     1 up       0 down

 *client interface     : GigabitEthernet8/0/0.5
  session state        : up
  AC status            : up
  VC state             : up
  VC ID                : 102
  VC type              : VLAN
  destination          : 2.2.2.2
  local VC label       : 146433       remote VC label      : 146432
  control word         : disable
  forwarding entry     : exist
```

```
local group ID       : 0
manual fault         : not set
active state         : active
link state           : up
local VC MTU         : 1500         remote VC MTU        : 1500
tunnel policy name   : --
traffic behavior name: --
PW template name     : --
primary or secondary : primary
create time          : 1 days, 1 hours, 14 minutes, 17 seconds
up time              : 0 days, 0 hours, 3 minutes, 16 seconds
last change time     : 0 days, 0 hours, 3 minutes, 16 seconds
VC last up time      : 2010/02/17 08:23:07
VC total up time     : 0 days, 21 hours, 43 minutes, 43 seconds
```

如果两端的 LDP 会话没有 UP，请参见“LDP 会话 DOWN”一节继续定位，使 LDP 会话状态为 Up。

如果 LDP 会话已经 UP，请执行步骤 5。

说明

只有 LDP 会话 UP，两端的 VC 才能开始协商。

步骤 5 检查 PW 是否选中隧道

执行 **display mpls l2vc** *vc-id* 命令：

- 检查 VC tunnel/token info 字段值。如果 VC tunnel/token info 字段值为 0 tunnels/tokens，表明 PW 没有选中隧道。
- 检查 tunnel policy name 字段的值：
  - 如果该字段值为“-”，表示 PW 使用的隧道为 LDP LSP，或者没有配置隧道策略。如果 PW 使用 MPLS-TE 隧道需要配置隧道策略。
  - 如果该字段值不是“-”，表示 VLL 使用隧道策略，可以在隧道策略视图下执行 **display this** 检查隧道策略的配置。

```
[HUAWEI-tunnel-policy-p1] display this
#
tunnel-policy p1
 tunnel select-seq cr-lsp load-balance-number 1
#
```

说明

如果隧道策略下配置了 **tunnel binding destination** *dest-ip-address* **te** { **tunnel** *interface-number* }，还需要在 Tunnel 接口下使能 **mpls te reserved-for-binding** 命令。

如果两端的隧道没有 Up，请参考“LSP 隧道 down”一节或者“Te Tunnel 状态为 down”一节继续定位，使隧道状态 Up。如果两端的隧道状态已经 UP 并且 TE 接口配置正确，请执行步骤 6。

说明

隧道 Up 是 VC 状态 up 的必要条件之一。

步骤 6 检查两端的 AC 接口状态是否 Up

在两端 PE 上分别执行 **display mpls l2vc** *vc-id* 命令，检查 AC status 字段值是否为 Up。

- 如果两端的 AC 接口状态没有 Up，请参考“物理对接&接口类”一节继续定位，使 AC 接口状态 Up。
- 如果两端 AC 接口状态已经 Up，请执行步骤 7。

说明

两端 AC 接口状态 Up 是 VC 状态 Up 的必要条件之一。

步骤 7 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

3.1.4 相关告警与日志

相关告警

无

相关日志

无

3.2 Kompella 方式 VLL 的 VC 不能 UP 的定位思路

介绍 Kompella 方式 VLL 网络中 VC 不能 UP 的故障处理流程和详细的故障处理步骤。

3.2.1 常见原因

本类故障的常见原因主要包括：

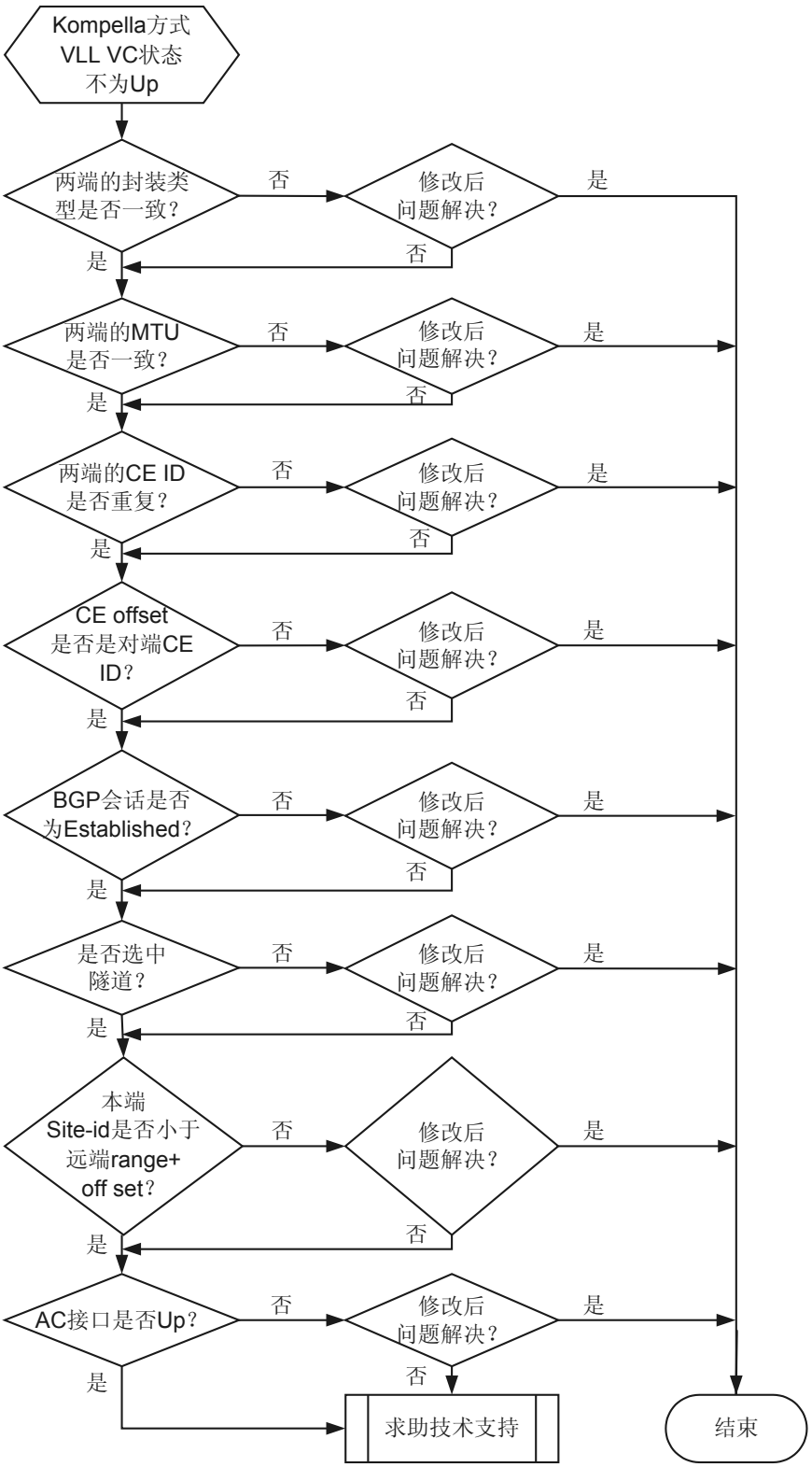
- 两端封装类型不一致。
- 两端 MTU 值不一致。
- 两端的 CE ID 重复
- 本端的 ce offset 不等于远端的 ce-id。
- BGP 状态不是“Established”。
- 公网隧道想选择 TE 隧道，但是隧道策略配置不正确。
- 本端的 ce-id 大于远端 range+default offset。
- 本端或者远端的 AC 接口没有 Up。

3.2.2 故障诊断流程

在配置 Kompella 方式 VLL 后发现 VC 不能 Up。

详细处理流程如图 3-2 所示。

图 3-2 Kompella 方式 VLL 的 VC 不能 UP 的故障诊断流程图



3.2.3 故障处理步骤

说明

请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

操作步骤

步骤 1 检查两端的封装类型及 MTU 是否一致

```
<HUAWEI> display mpls l2vpn vpn1
VPN name: vpn1, encap type: ethernet, local ce number(s): 1, remote ce number(s): 1
route distinguisher: 100:1, MTU: 1500
import vpn target: 100:1,
export vpn target: 100:1,

remote vpn site(s) :
no.  remote-pe-id    route-distinguisher
1    1.1.1.1         100:1
```

如果两端的封装类型或者 MTU 不一致，请在系统视图下执行命令 **mpls l2vpn** *l2vpn-name* **encapsulation** *vc-type*，修改其中一端的封装类型或者在 MPLS-L2VPN 实例视图下执行命令 **mtu** *mtu-value* 修改 MTU，使两端的封装类型、MTU 一致。

如果两端的封装类型及 MTU 已经一致，请执行步骤 2。

说明

两端封装类型、MTU 一致是 VC 状态 Up 的必要条件之一。

步骤 2 检查两端的 CE ID 是否重复

```
<HUAWEI> display mpls l2vpn connection interface GigabitEthernet 2/0/2.10
conn-type: remote
     local vc state:             up
     remote vc state:            up
     local ce-id:                2
     local ce name:              ce2
     remote ce-id:               1
     intf(state,encap):          GigabitEthernet2/0/2.10(up,ethernet)
     peer id:                    1.1.1.1
     route-distinguisher:        100:1
     local vc label:             179221
     remote vc label:            179222
     tunnel policy:              default
     primary or secondary:       primary
     forward entry exist or not: true
     forward entry active or not:true
     manual fault set or not:    not set
     AC OAM state:               up
     BFD for PW session index:   --
     BFD for PW state:           invalid
     BFD for LSP state:          true
     Local C bit is not set
     Remote C bit is not set
     tunnel type:                lsp
     tunnel id:                  0x2008004
```

如果两端的 CE ID 值重复，执行命令 **ce** *ce-name* **id** *ce-id*，修改其中一端的 CE ID 值，使两端不同。

如果两端的 CE ID 值已经不同，请执行步骤 4。

说明

Kompella VLL PW 的两端 CE ID 不能相同。

步骤 3 检查本端的 ce-offset 是否为对端的 CE ID

检查 MPLS-L2VPN-CE 视图下的配置：

```
[HUAWEI] mpls l2vpn vpn1
[HUAWEI-mpls-l2vpn-vpn1] display this
#
 mpls l2vpn vpn1 encapsulation ppp
  route-distinguisher 100:1
  vpn-target 100:1 import-extcommunity
  vpn-target 100:1 export-extcommunity
  ce ce1 id 2 range 10 default-offset 0
   connection ce-offset 1 interface Pos1/0/0
 #
return
```

如果本端的 ce-offset 不等于对端的 CE ID，请先在 MPLS-L2VPN-CE 视图下执行命令 **undo connection ce-offset** *id* 删掉该 CE 的 Kompella 方式连接，然后在 MPLS-L2VPN-CE 视图下执行命令 **connection** [**ce-offset** *id*] **interface** *interface-type interface-number*，修改本端的 ce-offset，使其等于对端的 CE ID。

如果本端的 ce-offset 已经等于对端的 CE ID，请执行步骤 4。

说明

只有本端 ce-offset 等于对端的 CE ID 才能协商成功。

步骤 4 检查两端的 BGP 会话状态是否为 Established

执行 **display bgp l2vpn peer** [*ipv4-address* **verbose** | **verbose**]命令，检查两端的 BGP 会话状态。

```
<HUAWEI> display bgp l2vpn peer

 BGP local router ID : 1.1.1.1
 local AS number : 100
 Total number of peers : 1                 Peers in established state : 1

  Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv

  1.25.1.3        4         100  13433    836      0     00:00:39      Established
```

如果两端的 BGP 会话状态不是 Established，请参考“BGP 邻居无法建立”一节，使 BGP 会话状态成为 Established。

如果 BGP 会话状态已经为 Established，请执行步骤 4。

说明

只有 BGP 会话状态为 Established，两端的 L2VPN 才能开始协商。

步骤 5 检查 VC 是否选中隧道

执行 **display mpls l2vpn connection interface** *interface-type interface-number* 命令：

- 检查 tunnel id 字段值是否为 0x0。如果 tunnel id 字段为 0x0，表明 VC 没有选中隧道。
- 检查 tunnel policy 字段的值。如果该字段值为 default，表示 VC 使用的隧道为 LDP LSP，或者没有为 VC 配置隧道策略。

  说明

  如果 VC 使用 MPLS-TE 隧道需要配置隧道策略。

  tunnel policy 字段值表示 VC 使用的隧道策略，可以在隧道策略视图下执行 **display this** 检查隧道策略的配置。

```
[HUAWEI-tunnel-policy-p1] display this
#
tunnel-policy p1
 tunnel select-seq cr-lsp load-balance-number 1
#
```

说明

如果隧道策略下配置了 **tunnel binding destination** *dest-ip-address* **te** { **tunnel** *interface-number* }，还需要在 Tunnel 接口下使能 **mpls te reserved-for-binding** 命令。

如果两端的隧道没有 Up，请参考“LSP 隧道 down”一节或者“Te Tunnel 状态为 down”一节继续定位，使隧道状态 Up。如果两端的隧道状态已经 Up 并且 TE 接口配置正确，请执行步骤 6。

说明

隧道 Up 是 VC 状态 Up 的必要条件之一。

步骤 6 检查本端的 CE ID 是否小于远端的 range 与 default offset 之和。

检查 MPLS-L2VPN-CE 视图下的配置：

```
[HUAWEI] mpls l2vpn vpn1
[HUAWEI-mpls-l2vpn-vpn1] display this
#
 mpls l2vpn vpn1 encapsulation ppp
  route-distinguisher 100:1
  vpn-target 100:1 import-extcommunity
  vpn-target 100:1 export-extcommunity
  ce ce1 id 2 range 10 default-offset 0
   connection ce-offset 1 interface Pos1/0/0
 #
return
```

如果本端的 CE ID 没有小于远端的 rang 与 default offset 之和，则执行 **ce** *ce-name* [**id** *ce-id* [**range** *ce-range*] [**default-offset** *ce-offset*]]命令，修改本端 CE ID 或者远端 range 使之满足条件。

如果本地 CE ID 已经小于远端 range 与 default offset 之和，并且远端 CE ID 小于本端的 range 与 offset 之和，请执行步骤 7。

步骤 7 检查两端的 AC 接口状态是否 Up

在两端 PE 上分别执行 **display mpls l2vpn connection interface** *interface-type interface-number* 命令，检查 intf(state,encap)字段对应的 AC 接口的 state 是否为 Up。

- 如果两端的 AC 接口状态没有 Up，请参考“物理对接&接口类”一节继续定位，使 AC 接口状态 Up。
- 如果两端 AC 接口状态已经 Up，请执行步骤 8。

步骤 8 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

3.2.4 相关告警与日志

相关告警

无

相关日志

无

3.3 Kompella 方式 VLL 两端 AC 接口为以太子接口，封装类型为 tagged，PW 无法 Up 的定位思路

介绍 Kompella 方式 VLL 网络中两端 AC 接口为以太子接口，封装类型为 tagged，PW 无法 Up 的详细的故障处理步骤。

3.3.1 常见原因

本类故障的常见原因主要包括：

- VPN 实例的封装类型跟 PW 的封装类型不一致。

3.3.2 故障处理步骤

说明

请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

操作步骤

步骤 1 检查 PW 的封装类型是否跟 VPN 实例的封装类型一致

查看 VPN 实例的封装类型：

```
<HUAWEI> display mpls l2vpn vpn1
VPN name: vpn1, encap type: ethernet, local ce number(s): 1, remote ce number(s)
: 1
route distinguisher: 100:1, MTU: 1500
import vpn target: 200:1,
export vpn target: 200:1,
remote vpn site(s) :
no.   remote-pe-id    route-distinguisher
1     2.2.2.2         100:1
```

查看 PW 的封装类型：

```
<HUAWEI> display mpls l2vpn connection interface GigabitEthernet 8/0/0.13
conn-type: remote
     local vc state:             up
     remote vc state:            up
     local ce-id:                1
     local ce name:              ce1
     remote ce-id:               2
     intf(state,encap):          GigabitEthernet8/0/0.13(up,ethernet)
     peer id:                    2.2.2.2
     route-distinguisher:        100:1
     local vc label:             179222
     remote vc label:            228373
     tunnel policy:              default
     primary or secondary:       primary
     forward entry exist or not: true
     forward entry active or not:true
     manual fault set or not:    not set
     AC OAM state:               up
     BFD for PW session index:   --
     BFD for PW state:           invalid
     BFD for LSP state:          true
     Local C bit is not set
```

```
Remote C bit is not set
tunnel type:                lsp
tunnel id:                  0x4008018
```

只有 PW 的封装类型跟 VPN 实例的封装类型一致才能进行正常的协商。如果 PW 的封装类型已经跟 VPN 实例的封装类型一致，并且已经按照前面的步骤执行排查，请联系华为技术支持。

----结束

3.3.3 相关告警与日志

相关告警

无

相关日志

无

3.4 Kompella 方式的 VLL 和其他厂商设备互通 VC 不能 Up 的定位思路

介绍 Kompella 方式网络中 VLL 和其他厂商设备互通 VC 不能 Up 的详细的故障处理步骤。

3.4.1 常见原因

本类故障的常见原因主要包括：

- 其他厂商设备的 default-offset 是 1，且无法配置；华为设备在与其他厂商设备互通时，需要将 default-offset 配置为 1，且 CE ID 不能为 0。
- MPLS-L2VPN 实例视图下未使能 **ignore-mtu-match** 命令。

3.4.2 故障处理步骤

说明

请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

操作步骤

步骤 1 MPLS-L2VPN 实例视图下是否使能了 **ignore-mtu-match** 命令。

如果没有使能以上命令，请先配置这条命令。

如果已经配置了这条命令行，请执行步骤 2。

说明

使能这条命令用来忽略跟其他厂商设备进行 MTU 的协商。

步骤 2 华为设备的 default-offset 是否配置为 1。

```
[HUAWEI] mpls l2vpn vpn1
[HUAWEI-mpls-l2vpn-vpn1] display this
#
 mpls l2vpn vpn1 encapsulation ppp
  route-distinguisher 100:1
  vpn-target 100:1 import-extcommunity
  vpn-target 100:1 export-extcommunity
  ce ce1 id 2 range 10 default-offset 1
   connection ce-offset 1 interface Pos1/0/0
 #
return
```

如果 default-offset 不为 1，请修改 default-offset 为 1。如果已经是 1，请联系华为技术支持。

----结束

3.4.3 相关告警与日志

相关告警

无

相关日志

无

3.5 相关案例

3.5.1 改变链路层协议后，接口下的 VC 消失了

网络环境

配置过程如下：

在 PE 连接 AC 的接口上配置 MPLS L2VC（VC ID 为 100）：

```
[PE-Pos4/0/0] mpls l2vc 1.1.1.8 100
```

该接口的配置如下：

```
[PE-Pos4/0/0] display this
#
interface Pos4/0/0
 link-protocol fr
 mpls l2vc 1.1.1.8 100
#
return
```

该接口存在 VC，VC ID 为 100。

```
[PE-Pos4/0/0] display mpls l2vc interface pos 4/0/0
*client interface       : Pos4/0/0 is down
  session state          : down
  AC state               : down
  VC state               : down
  VC ID                  : 100
```

```
  VC type               : fr
  destination           : 1.1.1.8
  local group ID        : 0           remote group ID      : 0
  local VC label        : 146433      remote VC label      : 0
  local AC OAM State    : up
  local PSN State       : up
  local forwarding state : not forwarding
  BFD for PW            : unavailable
  manual fault          : not set
  active state          : active
  forwarding entry      : not exist
  link state            : down
  local VC MTU          : 4470        remote VC MTU        : 0
  local VCCV            : Disable
  remote VCCV           : none
  local control word    : disable     remote control word  : none
  tunnel policy name    : --
  traffic behavior name : --
  PW template name      : --
  primary or secondary  : primary
  VC tunnel/token info  : 0 tunnels/tokens
  create time           : 0 days, 0 hours, 3 minutes, 24 seconds
  up time               : 0 days, 0 hours, 0 minutes, 0 seconds
  last change time      : 0 days, 0 hours, 3 minutes, 24 seconds
  VC last up time      : 2009/04/07 16:19:26
  VC total up time     : 0 days, 0 hours, 12 minutes, 37 seconds
```

PE 的另一个接口也存在 VC，且 VC-ID 也是 100（链路协议为 HDLC）：

```
[PE-Pos4/1/0] display mpls l2vc interface pos 4/1/0
*client interface       : Pos4/1/0 is down
  session state         : down
  AC state              : down
  VC state              : down
  VC ID                 : 100
  VC type               : hdlc
  destination           : 2.2.2.8
  local group ID        : 0           remote group ID      : 0
  local VC label        : 146433      remote VC label      : 0
  local AC OAM State    : up
  local PSN State       : up
  local forwarding state : not forwarding
  BFD for PW            : unavailable
  manual fault          : not set
  active state          : active
  forwarding entry      : not exist
  link state            : down
  local VC MTU          : 4470        remote VC MTU        : 0
  local VCCV            : Disable
  remote VCCV           : none
  local control word    : disable     remote control word  : none
  tunnel policy name    : --
  traffic behavior name : --
  PW template name      : --
  primary or secondary  : primary
  VC tunnel/token info  : 0 tunnels/tokens
  create time           : 0 days, 0 hours, 3 minutes, 24 seconds
  up time               : 0 days, 0 hours, 0 minutes, 0 seconds
  last change time      : 0 days, 0 hours, 3 minutes, 24 seconds
  VC last up time      : 2009/04/07 16:19:26
  VC total up time     : 0 days, 0 hours, 12 minutes, 37 seconds
```

把接口 POS4/0/0 的链路协议改为 HDLC。

```
[PE-Pos4/0/0] link-protocol hdlc
```

再次查看接口 POS4/0/0 的 VC，发现不存在 VC（显示为空）。

```
[PE-Pos4/0/0] display mpls l2vc interface pos 4/0/0
```

查看 PE 上所有的 VC，只剩一条，是接口 POS4/1/0 上的，其链路协议为 HDLC：

```
[PE] display mpls l2vc
 Total ldp vc : 1     0 up       1 down

*client interface     : Pos4/1/0
  session state        : down
  AC status            : down
  VC state             : down
  VC ID                : 100
  VC type              : hdlc
  destination          : 2.2.2.8
  local VC label       : 146433       remote VC label      : 0
  control word         : disable
  forwarding entry     : not exist
  local group ID       : 0
  manual fault         : not set
  active state         : active
  link state           : down
  local VC MTU         : 4470         remote VC MTU        : 0
  tunnel policy name   : --
  traffic behavior name: --
  PW template name     : --
  primary or secondary : primary
  create time          : 0 days, 0 hours, 5 minutes, 45 seconds
  up time              : 0 days, 0 hours, 0 minutes, 0 seconds
  last change time     : 0 days, 0 hours, 5 minutes, 45 seconds
  VC last up time      : 2009/04/07 16:19:26
  VC total up time     : 0 days, 0 hours, 12 minutes, 37 seconds
```

故障分析

当 PE 上的某接口（如 POS4/1/0）下已经存在 PW ID 为 100、PW Type 为 HDLC 的 PW 时，改变另一接口（如 POS4/0/0）的链路层协议，使之与 POS4/1/0 下 PW 的封装类型一致（改变为 HDLC）。由于两条 PW 的 VC ID 和 VC Type 均相同，系统自动将 POS4/0/0 下的 PW 删除。

操作步骤

步骤 1 如果要改动 VC 的链路协议，请先查看同一设备上的其他接口上的 VC 是否具有与更改后相同的 PW ID 和 VC Type 的组合。

----结束

案例总结

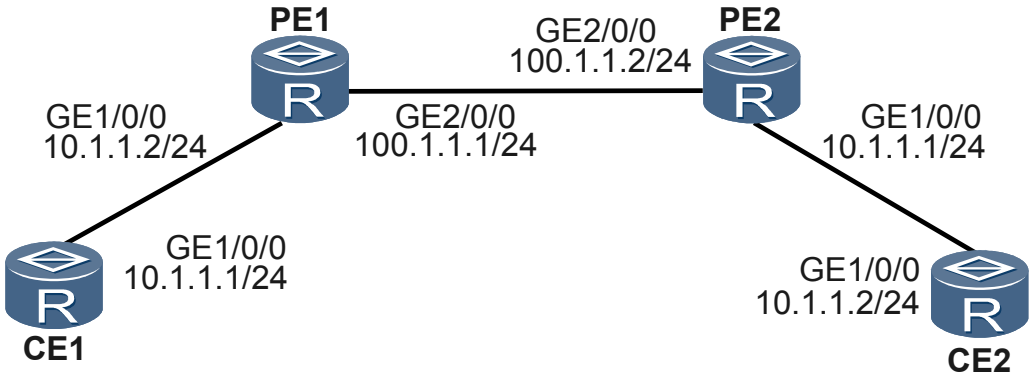
VC ID 和 VC Type 的组合在同一设备上必须唯一。

如果改变链路层协议后，VC-ID 和 VC-Type 的组合与其他 VC 冲突，则改动链路层协议的 VC 将被自动删除。

3.5.2 Session 和 AC 的状态为 Up，但 VC 不能 Up

网络环境

图 3-3 组网图



如图 3-3 所示，配置了 Martini 方式的 VLL 后，发现 VC 状态不能 Up，有关 Remote 的值均为 0，即无效值。查看 Session 和 AC 的状态，两者的状态均为 Up。

故障处理

在 PE 端执行 **display mpls l2vc** *vc-id* 命令查看两端的 MTU 值是否一致。例如：

查看 PE1 上的 MTU 值。

```
[PE1-GigabitEthernet1/0/0] display mpls l2vc 100
 total LDP VC : 1     0 up       1 down

 *client interface     : GigabitEthernet1/0/0
  session state        : up
  AC status            : up
  VC state             : down
  VC ID                : 100
  VC type              : ethernet
  destination          : 2.2.2.2
  local VC label       : 146433       remote VC label      : 0
  control word         : disable
  forwarding entry     : not exist
  local group ID       : 0
  manual fault         : not set
  active state         : active
  link state           : down
  local VC MTU         : 80           remote VC MTU        : 120
  tunnel policy name   : --
  traffic behavior name: --
  PW template name     : pwt1
  primary or secondary : primary
  create time          : 0 days, 0 hours, 18 minutes, 44 seconds
  up time              : 0 days, 0 hours, 12 minutes, 37 seconds
  last change time     : 0 days, 0 hours, 12 minutes, 37 seconds
  VC last up time      : 2009/04/07 16:19:26
  VC total up time     : 0 days, 0 hours, 12 minutes, 37 seconds
```

查看 PE2 上的 MTU 值。

```
[PE2-GigabitEthernet1/0/0] display mpls l2vc 100
 total LDP VC : 1     0 up       1 down

 *client interface     : GigabitEthernet1/0/0
  session state        : up
  AC status            : up
  VC state             : down
  VC ID                : 100
  VC type              : ethernet
  destination          : 1.1.1.1
  local VC label       : 146433       remote VC label      : 0
  control word         : disable
  forwarding entry     : not exist
  local group ID       : 0
  manual fault         : not set
  active state         : active
  link state           : down
  local VC MTU         : 120          remote VC MTU        : 80
  tunnel policy name   : --
  traffic behavior name: --
  PW template name     : pwt1
  primary or secondary : primary
  create time          : 0 days, 0 hours, 18 minutes, 44 seconds
  up time              : 0 days, 0 hours, 12 minutes, 37 seconds
  last change time     : 0 days, 0 hours, 12 minutes, 37 seconds
  VC last up time      : 2009/04/07 16:19:26
  VC total up time     : 0 days, 0 hours, 12 minutes, 37 seconds
```

从显示信息看，远端和本端的 MTU 值不一致，导致参数协商不能通过。

在其中一端 PE 上连接 AC 的接口上修改 MTU 值，使之与另一端的 MTU 值一致。

例如，把 PE2 上的接口 MTU 值修改成与 PE1 的相同。

```
[PE2-GigabitEthernet1/0/0] mtu 80
[PE2-GigabitEthernet1/0/0] shutdown
[PE2-GigabitEthernet1/0/0] undo shutdown
```

修改后，VC 状态变为 Up。

```
[PE2-GigabitEthernet1/0/0] display mpls l2vc 100
total LDP VC : 1     1 up       0 down

 *client interface     : GigabitEthernet1/0/0
  session state        : up
  AC status            : up
  VC state             : up
  VC ID                : 100
  VC type              : ethernet
  destination          : 1.1.1.1
  local VC label       : 146433       remote VC label      : 146433
  control word         : disable
  forwarding entry     : exist
  local group ID       : 0
  manual fault         : not set
  active state         : active
  link state           : up
  local VC MTU         : 80         remote VC MTU        : 80
  tunnel policy name   : --
  traffic behavior name: --
  PW template name     : --
  primary or secondary : primary
  create time          : 0 days, 0 hours, 43 minutes, 12 seconds
  up time              : 0 days, 0 hours, 37 minutes, 5 seconds
  last change time     : 0 days, 0 hours, 37 minutes, 5 seconds
  VC last up time      : 2009/04/07 16:19:26
  VC total up time     : 0 days, 0 hours, 37 minutes, 5 seconds
```

操作步骤

步骤 1 检查两端 PE 是否正确设置了对端的地址

步骤 2 检查两端的 VC ID 是否一致。

步骤 3 检查两端封装类型是否一致

步骤 4 检查两端控制字使能状态。两端必须都使能控制字或者都不使能控制字。

步骤 5 查看两端的 MTU 值是否一致。

步骤 6 两端的 MTU 值不一致则在任意一端 PE 上连接 AC 的接口上修改 MTU 值，使之与另一端的 MTU 值一致。

步骤 7 修改了 MTU 值的接口上执行 **shutdown** 命令，然后执行 **undo shutdown** 命令。

----结束

案例总结

PWE3 扩展了 Martini 的接口参数。对于这些接口参数，有些是必须支持，有些是可选支持；参数协商时，有些不需要匹配，有些则必须匹配。

以下是 Martini 的接口参数：

代码	所占字段	说明
0x01	4	Interface MTU in octets
0x02	4	Maximum Number of concatenated ATM cells
0x03	up to 82	Optional Interface Description string
0x04	4	CEM [8] Payload Bytes
0x05	4	CEM options

以下是 PWE3 的接口参数：

代码	所占字段	说明
0x01	4	Interface MTU in octets
0x02	4	Maximum Number of concatenated ATM cells
0x03	up to 82	Optional Interface Description string
0x04	4	CEP/TDM Payload Bytes
0x05	4	CEP options
0x06	4	Requested VLAN ID
0x07	6	CEP/TDM bit-rate
0x08	4	Frame-Relay DLCI Length

代码	所占字段	说明
0x09	4	Fragmentation indicator
0x0A	4	FCS retension indicator
0x0B	4/8/12	TDM options
0x0C	4	VCCV parameter

代码为 0x06 ～ 0x0C 的项是 PWE3 扩展的接口参数。

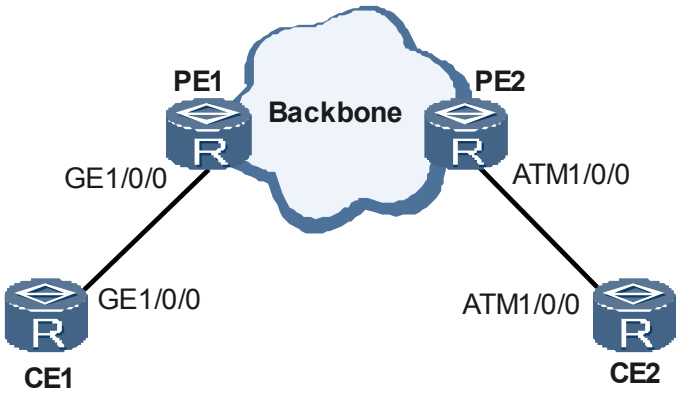
配置接口参数时请注意：

- Ethernet 类型的接口必须携带 MTU，如果 MTU 不一致，PW 状态不能 Up。
- ATM 信元（0x0003 ATM transparent cell transport、0x0009 ATM n-to-one VCC cell transport、0x000A ATM n-to-one VPC cell transport）方式，需要向对方传递 max ATM Cell number 值，通告对方自己一次能处理信元的个数。对方封装报文时不能超过该值。两端是否大小相等不影响 PW 的状态。
- 分片能力和 ATM 信元处理方式一致。可选，不需要双方一致。仅通告对方自己是否可以进行报文重组；对方是否分片根据报文大小以及远端分片能力决定。分片能力不影响 PW 状态，不需要两端一致。
- VCCV 处理与 ATM 信元和分片能力基本相同。可选，通告对方自己的 VCCV 能力。对方在进行 VCCV 处理时，根据自己和远端的能力选择通道（CC）和方法（CV）。不影响 PW 的状态，不需要两端一致。
- Requested VLAN ID，通告对方自己的能力。转发时要求远端在二层头中填入该 VLAN ID，还可以采用其它方式。可选，如果携带，不要求两端的 VLAN ID 相等。

3.5.3 Ethernet 与 ATM 互连，VC 状态 Up，但 CE-CE 间 ping 不通

网络环境

图 3-4 Ethernet 与 ATM 互连的 L2VPN 组网



如图 3-4，Ethernet 与 ATM 互连。配置 L2VPN 异种介质互连后，两端的 VC 状态都是 Up，但是 CE 之间不能互相 ping 通。

故障分析

检查两端 CE 的 IP 地址是否在一个网段内。CE 两端的 IP 地址必须在同一网段。

在 PE 上执行 **display local-ce mac** 命令，在 CE 上执行 **display arp** 命令检查以太网链路 ARP 表项是否建立成功。

如果没有建立成功，在 PE 上配置 CE 以太网接口的 IP 地址、MAC 地址、并使能 MAC 广播，即配置 **local-ce ip** 命令、**local-ce mac** 和 **local-ce mac broadcast** 命令。

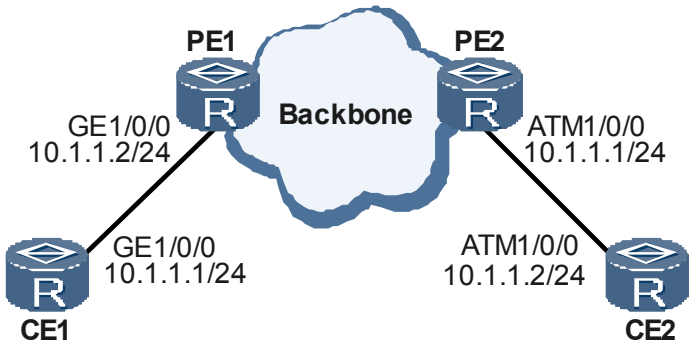
具体配置请参见《HUAWEI NetEngine80E/40E 路由器 配置指南 VPN》“VLL 配置”中的关于配置 L2VPN 异种介质互通的介绍。

对于 ATM 链路的 ARP，可以使用下面两种方式之一配置：

- 指定使用 INARP 动态生成 MAP，正确配置 IP 地址的例子如图 3-5。其中配置方法如下：

```
[PE2] interface atm 1/0/0
[PE2-Atm1/0/0] pvc 100/200
[PE2-atm-pvc-Atm1/0/0-100/200] map ip inarp broadcast
[PE2-atm-pvc-Atm1/0/0-100/200] ip address 10.1.1.1 255.255.255.0
[CE2] interface atm 1/0/0
[CE2-Atm1/0/0] pvc 100/200
[CE2-atm-pvc-Atm1/0/0-100/200] map ip inarp broadcast
[CE2-atm-pvc-Atm1/0/0-100/200] ip address 10.1.1.2 255.255.255.0
```

图 3-5 IP 地址正确的配置方法



- 使用静态 MAP。在 AC 两端的 ATM 接口的 PVC 视图下配置 **map ip** *peer-ce-address* **broadcast** 命令或 **map ip default broadcast**。例如：

```
[PE2] interface atm 1/0/0
[PE2-Atm1/0/0] pvc 100/200
[PE2-atm-pvc-Atm1/0/0-100/200] map ip 10.1.1.2 broadcast
[PE2-atm-pvc-Atm1/0/0-100/200] ip address 10.1.1.1 255.255.255.0
[CE2] interface atm 1/0/0
[CE2-Atm1/0/0] pvc 100/200
[CE2-atm-pvc-Atm1/0/0-100/200] map ip 10.1.1.1 broadcast
[CE2-atm-pvc-Atm1/0/0-100/200] ip address 10.1.1.2 255.255.255.0
```

操作步骤

步骤 1 检查两端 CE 的 IP 地址是否在一个网段内。CE 两端的 IP 地址必须在同一网段。

步骤 2 在 PE 上执行 **display local-ce mac** 命令，在 CE 上执行 **display arp** 命令检查以太网链路 ARP 表项是否建立成功。

步骤 3 如果 ARP 建立不成功，对于以太网，在 PE 的 AC 以太网接口上配置 IP 地址，MAC 地址并使能 MAC 广播；对于 ATM 链路，使用 INARP 动态生成 MAP 或使用静态 MAP。

----结束

案例总结

在异种介质互应用中，如果出现 VC 状态 Up 但 CE 之间不能互相 ping 通的问题，多数原因是配置不正确。

应根据链路特性进行配置，保证正确生成 ARP 表项。

3.5.4 CE 使用 VLAN 接入不能互通

网络环境

CE 使用 VLAN 接入，更改 VLAN ID 后两端 CE 无法互通。

故障分析

如果修改 VLAN ID，需要沿报文发送方向，对沿途的 AC 接口依次修改。为了使修改生效，还需要对各 VLAN 接口先执行 **shutdown** 命令，再执行 **undo shutdown** 命令。

操作步骤

步骤 1 沿 CE－PE、PE－CE 方向依次在相关 AC 接口上执行 **vlan-type dot1q** 命令，修改 VLAN ID。

步骤 2 在修改了 VLAN ID 的接口上执行 **shutdown** 命令，使接口失效。

步骤 3 在修改了 VLAN ID 的接口上执行 **undo shutdown** 命令，使接口重新生效。

----结束

案例总结

CE 与 PE 间使用 VLAN 接入时，报文途经的同一 AC 两端接口的最小 VLAN ID 必须设置成一致，否则报文转发不通。隧道两端 CE 的接口最小 VLAN ID 不需要设置成一致。

3.5.5 Static-VC Up，但 CE 不能互访

网络环境

配置 Static-VC 后，Static-VC 状态为 Up，但 CE 之间无法互访。

例如：

```
[PE1] display mpls static-l2vc
 Total svc connections:  1,  1 up,  0 down
 *Client Interface     : GigabitEthernet2/0/1 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : ethernet
  Destination          : 2.2.2.2
  Transmit VC Label    : 200
```

```
  Receive VC Label     : 100
  Control Word         : Disable
  VCCV Capability      : alert lsp-ping bfd
  Tunnel Policy Name   : --
  Traffic Behavior     : --
  PW Template Name     : --
  Main or Secondary    : Main
  Create time          : 0 days, 0 hours, 0 minutes, 17 seconds
  UP time              : 0 days, 0 hours, 0 minutes, 17 seconds
  Last change time     : 0 days, 0 hours, 0 minutes, 17 seconds
  VC last up time : 2008/07/24 12:31:31
  VC total up time: 0 days, 2 hours, 12 minutes, 51 seconds
  CKey                 : 6
  NKey                 : 3
```

故障分析

在另一端 PE 上查看该 Static-VC 的标签值：

```
[PE2] display mpls static-l2vc
 Total svc connections:  1,  1 up,  0 down
 *Client Interface     : GigabitEthernet1/0/1 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : ethernet
  Destination          : 1.1.1.1
  Transmit VC Label    : 200
  Receive VC Label     : 100
  Control Word         : Disable
  VCCV Capability      : alert lsp-ping bfd
  Tunnel Policy Name   : --
  Traffic Behavior     : --
  PW Template Name     : --
  Main or Secondary    : Main
  Create time          : 0 days, 0 hours, 0 minutes, 17 seconds
  UP time              : 0 days, 0 hours, 0 minutes, 17 seconds
  Last change time     : 0 days, 0 hours, 0 minutes, 17 seconds
  VC last up time : 2008/07/24 12:31:31
  VC total up time: 0 days, 2 hours, 12 minutes, 51 seconds
```

本端的标签设置与对端不对应。

进行如下配置后，CE 之间可以互通。

```
[PE1-GigabitEthernet2/0/1] mpls static-l2vc destination 2.2.2.2 transmit-vpn-label 100 receive-vpn-label 200
```

操作步骤

步骤 1 在其中一端删除该 Static-VC，重新配置，注意标签值的设置。

----结束

案例总结

Static-VC 的标签值设置错误时，虽然可以使 VC Up，但数据不能正确转发。因此配置静态 VC 时，需注意 VC 两端标签值的对应关系。

- 本端的 transmit-vpn-label 与远端的 receive-vpn-label 一致。
- 本端的 receive-vpn-label 与远端的 transmit-vpn-label 一致。

3.5.6 L2VPN 两端 CE 间大报文丢失

网络环境

CE 之间建立 L2VPN 连接，发送大报文时有丢失现象。

故障分析

能收发报文，但有丢失现象，可能是沿途出接口 MTU 值小于源接口的 MTU 值，使发送的报文被分片。

操作步骤

步骤 1 在发送报文的源接口上执行 **display interface** 命令，确认源接口的 MTU。

步骤 2 在报文发送的沿途 PE 上执行 **display interface** 命令，检查是否有出接口的 MTU 小于源接口的 MTU。

步骤 3 在 CE 或 PE 的出接口视图下执行 **mtu** 命令，修改 MTU 值，使 CE 发送的报文不被分片。

----结束

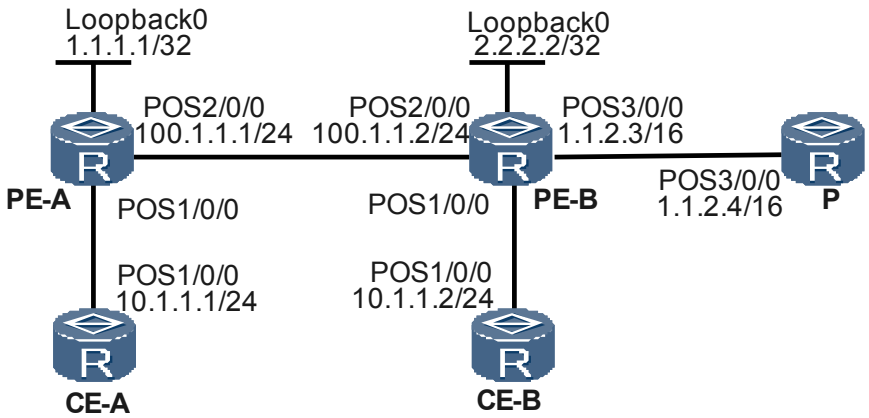
案例总结

CE 之间通过 L2VPN 连接时，发送的报文在沿途 PE 上不能被分片，否则将不能正确接收。

3.5.7 RIP-1 作为 L2VPN 骨干网 IGP，PE 之间的 MPLS LDP 会话建立不成功

网络环境

图 3-6 RIP 作为 L2VPN 骨干网 IGP 的简单组网



L2VPN 骨干网运行 RIP-1 发布本端的 Loopback0 和接口 IP 地址，发现 PE 之间 MPLS LDP 会话建立不成功。

PE-A 上出现提示信息：

```
Del Session : EncdecEncode ldp notify msg failure.
```

查看 PE-A 上的 MPLS LDP 会话，显示结果如下。

```
[PE-A] display mpls ldp session
 LDP Session(s) in Public Network
 Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
 A '*' before a session means the session is being deleted.
 ------------------------------------------------------------------------------
 PeerID            Status      LAM  SsnRole  SsnAge      KASent/Rcv
 ------------------------------------------------------------------------------
 2.2.2.2:0         NonExistent      Passive             0/0
 ------------------------------------------------------------------------------
 TOTAL: 0 session(s) Found.
```

PE-B 上出现提示信息：

```
Del Session : Tcp connection down
```

查看 PE-B 上的 MPLS LDP 会话，显示结果如下。

```
[PE-A] display mpls ldp session
 LDP Session(s) in Public Network
 Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
 A '*' before a session means the session is being deleted.
 ------------------------------------------------------------------------------
 PeerID            Status      LAM  SsnRole  SsnAge      KASent/Rcv
 ------------------------------------------------------------------------------
 1.1.1.1:0         Initialized      Active              0/0
 ------------------------------------------------------------------------------
 TOTAL: 0 session(s) Found.
```

故障分析

查看 PE-B 上的路由表，显示结果如下。

```
[PE-B] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 10       Routes : 10
Destination/Mask    Proto  Pre  Cost       NextHop         Interface
        1.0.0.0/8   RIP    100  1          100.1.1.1       Pos2/0/0
        1.1.0.0/16  Direct 0    0          1.1.2.3         Pos3/0/0
        1.1.2.3/32  Direct 0    0          127.0.0.1       InLoopBack0
        1.1.2.4/32  Direct 0    0          1.1.2.4         Pos3/0/0
        2.2.2.2/32  Direct 0    0          127.0.0.1       InLoopBack0
      100.1.1.0/24  Direct 0    0          100.1.1.2       Pos2/0/0
      100.1.1.2/32  Direct 0    0          127.0.0.1       InLoopBack0
      127.0.0.0/8   Direct 0    0          127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0          127.0.0.1       InLoopBack0
```

RIP-1 只能识别 A、B、C 类这样的自然网段的路由，而 PE-B 上的路由表中，去往 Peer 1.1.1.1 的匹配路由共有两条

- RIP-1 学到的 8 位掩码地址 1.0.0.0/8
- 与 PE-B 直连的 16 位掩码地址 1.1.0.0/16

根据最长匹配原则，报文将被发往 16 位掩码地址 1.1.0.0/16 的接口 POS3/0/0。而与 POS3/0/0 接口相连的网段里没有 1.1.1.1/32 的 Loopback 地址。因此 MPLS LDP 会话就会建立不成功。

操作步骤

步骤 1 使用 RIP-2 替代 RIP-1 来发布 PE 上作为 MPLS LDP 会话地址的 32 位 Loopback 接口地址。

----结束

案例总结

RIP-1 只能识别 A、B、C 类这样的自然网段的路由，因此应该使用 RIP-2 来发布 PE 的 32 位 Loopback 接口地址。

4 PWE3 故障处理

关于本章

介绍了 PWE3 故障常见的原因和定位思路。

4.1 PW 不能 UP 的定位思路
介绍 PW 不能 UP 的故障处理流程和详细的故障处理步骤。

4.2 相关案例

4.1 PW 不能 UP 的定位思路

介绍 PW 不能 UP 的故障处理流程和详细的故障处理步骤。

4.1.1 常见原因

本类故障的常见原因主要包括：

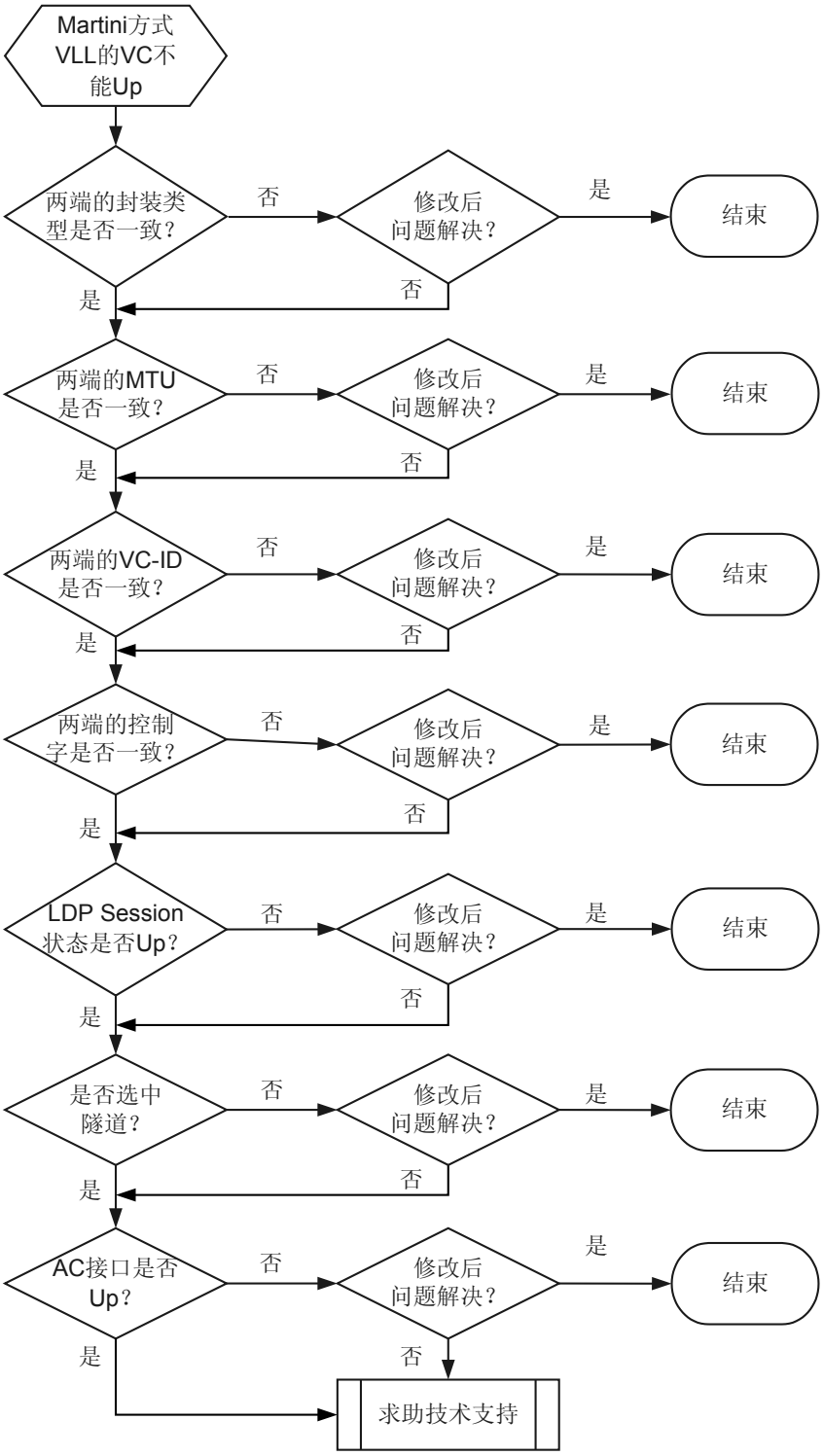
- 两端封装类型不一致。
- 两端 MTU 值不一致。
- 两端的 VC-ID 不一致。
- 两端的控制字配置不一致。
- LDP session 状态没有 Up。
- 公网隧道想选择 TE 隧道，但是隧道策略配置不正确。
- 本端或者远端的隧道没有 Up。
- 本端或者远端的 AC 接口没有 Up。

4.1.2 故障诊断流程

在配置 Martini 方式 VLL 后发现 VC 不能 Up。

详细处理流程如图 4-1 所示。

图 4-1 Martini 方式 VLL 的 VC 不能 UP 的故障诊断流程图



4.1.3 故障处理步骤

说明

请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

操作步骤

步骤 1 检查两端的封装类型及 MTU 是否一致

执行 **display mpls l2vc** *vc-id* 命令，检查 VC 信息。

```
<HUAWEI> display mpls l2vc 102
 total LDP VC : 1     1 up       0 down

 *client interface     : GigabitEthernet8/0/0.5
  session state        : up
  AC status            : up
  VC state             : up
  VC ID                : 102
  VC type              : VLAN
  destination          : 2.2.2.2
  local VC label       : 146433       remote VC label      : 146432
  control word         : disable
  forwarding entry     : exist
  local group ID       : 0
  manual fault         : not set
  active state         : active
  link state           : up
  local VC MTU         : 1500         remote VC MTU        : 1500
  tunnel policy name   : --
  traffic behavior name: --
  PW template name     : --
  primary or secondary : primary
  create time          : 1 days, 1 hours, 14 minutes, 17 seconds
  up time              : 0 days, 0 hours, 3 minutes, 16 seconds
  last change time     : 0 days, 0 hours, 3 minutes, 16 seconds
  VC last up time      : 2010/02/17 08:23:07
  VC total up time     : 0 days, 21 hours, 43 minutes, 43 seconds
```

如果两端的封装类型或者 MTU 不一致，那么修改其中一端的封装类型及 MTU 使两端的封装类型及 MTU 一致。

如果两端的封装类型及 MTU 已经一致，请执行步骤 2。

说明

两端封装类型、MTU 一致是 VC 状态 Up 的必要条件之一。

步骤 2 检查两端的 VC ID 是否一致

```
<HUAWEI> display mpls l2vc 102
 total LDP VC : 1     1 up       0 down

 *client interface     : GigabitEthernet8/0/0.5
  session state        : up
  AC status            : up
  VC state             : up
  VC ID                : 102
  VC type              : VLAN
  destination          : 2.2.2.2
  local VC label       : 146433       remote VC label      : 146432
  control word         : disable
  forwarding entry     : exist
  local group ID       : 0
  manual fault         : not set
  active state         : active
  link state           : up
  local VC MTU         : 1500         remote VC MTU        : 1500
  tunnel policy name   : --
```

```
 traffic behavior name: --
 PW template name     : --
 primary or secondary : primary
 create time          : 1 days, 1 hours, 14 minutes, 17 seconds
 up time              : 0 days, 0 hours, 3 minutes, 16 seconds
 last change time     : 0 days, 0 hours, 3 minutes, 16 seconds
 VC last up time      : 2010/02/17 08:23:07
 VC total up time     : 0 days, 21 hours, 43 minutes, 43 seconds
```

如果两端的 VC ID 不一致，那么修改其中一端的 VC ID 使两端的 VC ID 一致。

如果两端的 VC ID 已经一致，请执行步骤 3。

说明

两端 VC ID 一致是 VC 状态 Up 的必要条件之一。

步骤 3 检查两端的 CW 配置是否一致

```
<HUAWEI> display mpls l2vc 102
 total LDP VC : 1     1 up       0 down

 *client interface     : GigabitEthernet8/0/0.5
  session state        : up
  AC status            : up
  VC state             : up
  VC ID                : 102
  VC type              : VLAN
  destination          : 2.2.2.2
  local VC label       : 146433       remote VC label      : 146432
  control word         : disable
  forwarding entry     : exist
  local group ID       : 0
  manual fault         : not set
  active state         : active
  link state           : up
  local VC MTU         : 1500         remote VC MTU        : 1500
  tunnel policy name   : --
  traffic behavior name: --
  PW template name     : --
  primary or secondary : primary
  create time          : 1 days, 1 hours, 14 minutes, 17 seconds
  up time              : 0 days, 0 hours, 3 minutes, 16 seconds
  last change time     : 0 days, 0 hours, 3 minutes, 16 seconds
  VC last up time      : 2010/02/17 08:23:07
  VC total up time     : 0 days, 21 hours, 43 minutes, 43 seconds
```

如果两端的 CW 配置不一致，那么修改其中一端的 CW 配置使两端的 VC ID 一致。

如果两端的 CW 配置已经一致，请执行步骤 4。

说明

两端 CW 配置一致是 VC 状态 Up 的必要条件之一。

步骤 4 检查两端的 LDP 会话状态是否 UP

```
<HUAWEI> display mpls l2vc 102
 total LDP VC : 1     1 up       0 down

 *client interface     : GigabitEthernet8/0/0.5
  session state        : up
  AC status            : up
  VC state             : up
  VC ID                : 102
  VC type              : VLAN
  destination          : 2.2.2.2
  local VC label       : 146433       remote VC label      : 146432
  control word         : disable
  forwarding entry     : exist
```

```
local group ID       : 0
manual fault         : not set
active state         : active
link state           : up
local VC MTU         : 1500         remote VC MTU        : 1500
tunnel policy name   : --
traffic behavior name: --
PW template name     : --
primary or secondary : primary
create time          : 1 days, 1 hours, 14 minutes, 17 seconds
up time              : 0 days, 0 hours, 3 minutes, 16 seconds
last change time     : 0 days, 0 hours, 3 minutes, 16 seconds
VC last up time      : 2010/02/17 08:23:07
VC total up time     : 0 days, 21 hours, 43 minutes, 43 seconds
```

如果两端的 LDP 会话没有 UP，请参见“LDP 会话 DOWN”一节继续定位，使 LDP 会话状态为 Up。

如果 LDP 会话已经 UP，请执行步骤 5。

说明

只有 LDP 会话 UP，两端的 VC 才能开始协商。

步骤 5 检查 PW 是否选中隧道

执行 **display mpls l2vc** *vc-id* 命令：

- 检查 VC tunnel/token info 字段值。如果 VC tunnel/token info 字段值为 0 tunnels/tokens，表明 PW 没有选中隧道。
- 检查 tunnel policy name 字段的值：
  - 如果该字段值为“-”，表示 PW 使用的隧道为 LDP LSP，或者没有配置隧道策略。如果 PW 使用 MPLS-TE 隧道需要配置隧道策略。
  - 如果该字段值不是“-”，表示 VLL 使用隧道策略，可以在隧道策略视图下执行 **display this** 检查隧道策略的配置。

```
[HUAWEI-tunnel-policy-p1] display this
#
tunnel-policy p1
 tunnel select-seq cr-lsp load-balance-number 1
#
```

说明

如果隧道策略下配置了 **tunnel binding destination** *dest-ip-address* **te** { **tunnel** *interface-number* }，还需要在 Tunnel 接口下使能 **mpls te reserved-for-binding** 命令。

如果两端的隧道没有 Up，请参考“LSP 隧道 down”一节或者“Te Tunnel 状态为 down”一节继续定位，使隧道状态 Up。如果两端的隧道状态已经 UP 并且 TE 接口配置正确，请执行步骤 6。

说明

隧道 Up 是 VC 状态 up 的必要条件之一。

步骤 6 检查两端的 AC 接口状态是否 Up

在两端 PE 上分别执行 **display mpls l2vc** *vc-id* 命令，检查 AC status 字段值是否为 Up。

- 如果两端的 AC 接口状态没有 Up，请参考“物理对接&接口类”一节继续定位，使 AC 接口状态 Up。
- 如果两端 AC 接口状态已经 Up，请执行步骤 7。

说明

两端 AC 接口状态 Up 是 VC 状态 Up 的必要条件之一。

步骤 7 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

4.1.4 相关告警与日志

相关告警

无

相关日志

无

4.2 相关案例

4.2.1 执行 reset pw 命令不能改变 PW 属性

网络环境

在 PE 配置 PW 后，更改 PW 属性。

执行 **reset pw pw-template** *pw-template-name* 或 **reset pw** *pw-id pw-type* 命令后，PW 属性不变。

在 PE 上查看 PW 模板的配置情况。

```
[PE] display pw-template pwt1
  PW Template Name : pwt1
  PeerIP           : 1.1.1.1
  Tnl Policy Name  : --
  CtrlWord         : Disable
  MTU              : 1500
  Max Atm Cells    : 28
  ATM Pack Overtime: 1000
  Seq-Number       : Disable
  TDM Encapsulation Number: 32
  Jitter-Buffer           : 20
  Idle-Code               : ff
  Rtp-Header              : Disable
  VCCV Capability  : alert lsp-ping bfd
  Behavior Name    : --
  Total PW         : 1, Static PW : 0, LDP PW : 1
```

应用该 PW 模板配置 PW。

```
[PE-Atm2/1/0.100] mpls l2vc pw-t pwt1 2.2.2.2 100
```

PW 的配置结果。

```
[PE-Atm2/1/0.100] display mpls l2vc 100
```

```
 total LDP VC : 1     0 up       1 down

 *client interface     : Atm2/1/0.100
  session state        : down
  AC status            : up
  VC state             : down
  VC ID                : 100
  VC type              : atm aal5 sdu
  destination          : 2.2.2.2
  local VC label       : 146433       remote VC label      : 0
  control word         : disable
  forwarding entry     : not exist
  local group ID       : 0
  manual fault         : not set
  active state         : active
  link state           : down
  local VC MTU         : 1500         remote VC MTU        : 0
  tunnel policy name   : --
  traffic behavior name: --
  PW template name     : pwt1
  primary or secondary : primary
  create time          : 0 days, 0 hours, 17 minutes, 26 seconds
  up time              : 0 days, 0 hours, 0 minutes, 0 seconds
  last change time     : 0 days, 0 hours, 17 minutes, 26 seconds
  VC last up time      : 2009/04/07 16:19:26
  VC total up time     : 0 days, 0 hours, 32 minutes, 36 seconds
```

在 PW 模板上重新指定该 PW 的对端地址。

```
[PE] pw-template pwt1
[PE-pw-template-pwt1] peer-address 3.3.3.3
 Info: The attribute of this PW template has been modified, please use PW restar
t command to update PW's attribute
```

根据上述提示信息进行如下配置。

```
[PE-pw-template-pwt1] return
```

对 PW 进行 reset 操作。

```
<PE> reset pw 100 atm-aal5-sdu
```

查看结果，发现 PW 的对端 Peer 的 IP 地址并没有改变。

```
<PE> display mpls l2vc 100
 total LDP VC : 1     0 up       1 down

 *client interface     : Atm2/1/0.100
  session state        : down
  AC status            : up
  VC state             : down
  VC ID                : 100
  VC type              : atm aal5 sdu
  destination          : 2.2.2.2
  local VC label       : 146433       remote VC label      : 0
  control word         : disable
  forwarding entry     : not exist
  local group ID       : 0
  manual fault         : not set
  active state         : active
  link state           : down
  local VC MTU         : 1500         remote VC MTU        : 0
  tunnel policy name   : --
  traffic behavior name: --
  PW template name     : pwt1
  primary or secondary : primary
  create time          : 0 days, 0 hours, 17 minutes, 26 seconds
  up time              : 0 days, 0 hours, 0 minutes, 0 seconds
  last change time     : 0 days, 0 hours, 17 minutes, 26 seconds
```

```
  VC last up time      : 2009/04/07 16:19:26
  VC total up time     : 0 days, 0 hours, 32 minutes, 36 seconds
```

重新启动该 PW 模板。

```
<PE> reset pw pw-template pwt1
```

查看结果，发现 PW 的对端 Peer 的 IP 地址仍没有改变。

```
<PE> display mpls l2vc 100
 total LDP VC : 1     0 up       1 down

 *client interface     : Atm2/1/0.100
  session state        : down
  AC status            : up
  VC state             : down
  VC ID                : 100
  VC type              : atm aal5 sdu
  destination          : 2.2.2.2
  local VC label       : 146433       remote VC label      : 0
  control word         : disable
  forwarding entry     : not exist
  local group ID       : 0
  manual fault         : not set
  active state         : active
  link state           : down
  local VC MTU         : 1500         remote VC MTU        : 0
  tunnel policy name   : --
  traffic behavior name: --
  PW template name     : pwt1
  primary or secondary : primary
  create time          : 0 days, 0 hours, 17 minutes, 26 seconds
  up time              : 0 days, 0 hours, 0 minutes, 0 seconds
  last change time     : 0 days, 0 hours, 17 minutes, 26 seconds
  VC last up time      : 2009/04/07 16:19:26
  VC total up time     : 0 days, 0 hours, 32 minutes, 36 seconds
```

故障分析

PW 的一些属性可以通过 PW 模板来配置，也可以通过命令行配置，通过命令行配置的优先级较高。

如果在命令行中指定了 PW 属性，则 PW 模板中的相应 PW 属性不起作用，因此执行 **reset pw pw-template** *pw-template-name* 或 **reset pw** *pw-id pw-type* 命令，PW 属性不会改变。

可以将需要更改的 PW 属性设置在 PW 模板上，而不是通过命令指定。操作如下：

在 PW 模板上指定对端 Peer 的 IP 地址。

```
[PE] pw-template pwt1
[PE-pw-template-pwt1] peer-address 3.3.3.3
[PE-pw-template-pwt1] quit
```

把该模板应用到 PW 上。

```
[PE] interface atm 2/1/0.100
[PE-Atm2/1/0.100] mpls l2vc pw-t pwt1 100
```

查看结果，此时 PW 对端 Peer 的 IP 地址没有改变。

```
[PE-Atm2/1/0.100] display mpls l2vc 100
 total LDP VC : 1     0 up       1 down

 *client interface     : Atm2/1/0.100
  session state        : down
  AC status            : up
```

```
  VC state             : down
  VC ID                : 100
  VC type              : atm aal5 sdu
  destination          : 2.2.2.2
  local VC label       : 146433       remote VC label      : 0
  control word         : disable
  forwarding entry     : not exist
  local group ID       : 0
  manual fault         : not set
  active state         : active
  link state           : down
  local VC MTU         : 1500         remote VC MTU        : 0
  tunnel policy name   : --
  traffic behavior name: --
  PW template name     : pwt1
  primary or secondary : primary
  create time          : 0 days, 0 hours, 18 minutes, 44 seconds
  up time              : 0 days, 0 hours, 12 minutes, 37 seconds
  last change time     : 0 days, 0 hours, 12 minutes, 37 seconds
  VC last up time      : 2009/04/07 16:19:26
  VC total up time     : 0 days, 0 hours, 12 minutes, 37 seconds
[PE-Atm2/1/0.100] return
<PE> reset pw 100 atm-aal5-sdu
```

查看结果，发现对端 Peer 的 IP 地址已改变了。

```
<PE> display mpls l2vc 100
 total LDP VC : 1     0 up       1 down

 *client interface     : Atm2/1/0.100
  session state        : down
  AC status            : up
  VC state             : down
  VC ID                : 100
  VC type              : atm aal5 sdu
  destination          : 3.3.3.3
  local VC label       : 146433       remote VC label      : 0
  control word         : disable
  forwarding entry     : not exist
  local group ID       : 0
  manual fault         : not set
  active state         : active
  link state           : down
  local VC MTU         : 1500         remote VC MTU        : 0
  tunnel policy name   : --
  traffic behavior name: --
  PW template name     : pwt1
  primary or secondary : primary
  create time          : 0 days, 0 hours, 18 minutes, 44 seconds
  up time              : 0 days, 0 hours, 12 minutes, 37 seconds
  last change time     : 0 days, 0 hours, 12 minutes, 37 seconds
  VC last up time      : 2009/04/07 16:19:26
  VC total up time     : 0 days, 0 hours, 12 minutes, 37 seconds
```

操作步骤

步骤 1 创建 PW 模板，在 PW 模板上设置 PW 的属性（特别是需要更改的属性）。

步骤 2 将该模板 PW 模板应用到该 PW 上。

步骤 3 用户视图下执行 **reset pw pw-template** *pw-template-name* 或 **reset pw** *pw-id pw-type* 命令对 PW 属性进行更改。

----结束

案例总结

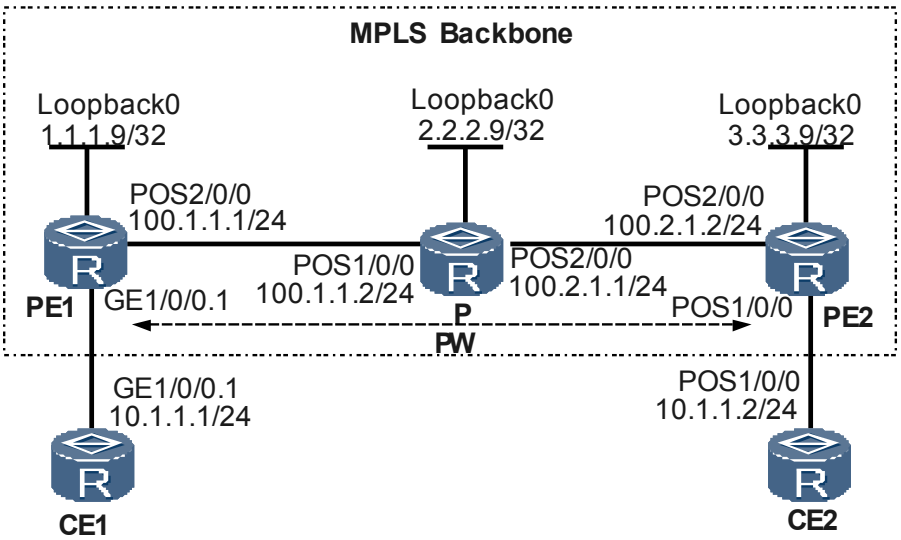
reset pw pw-template *pw-template-name* 或 **reset pw** *pw-id pw-type* 命令只能更改创建时由 PW 模板指定的属性。

4.2.2 PE 之间的 VPN 业务不通

组网环境

在某次测试过程中，配置 PWE3 异种介质互通业务，组网图如图 4-2 所示。

图 4-2 PWE3 异种介质互通案例组网图



配置完成后，发现从 CE1 可以将数据报文发送到 CE2，但 CE2 无法将数据报文发送到 CE1。

故障分析

1. 通过诊断命令 **ping vc** 检查 PE 之间的 VC 是否可以正常转发。操作后发现 PE 之间的 VC 可以正常转发业务报文。说明问题不在 PE 之间。

```
<PE1> ping vc ip-interworking 100 control-word remote 100
    Reply: bytes=100 Sequence=1 time = 11 ms
    Reply: bytes=100 Sequence=2 time = 4 ms
    Reply: bytes=100 Sequence=3 time = 4 ms
    Reply: bytes=100 Sequence=4 time = 4 ms
    Reply: bytes=100 Sequence=5 time = 4 ms
--- FEC: FEC 128 PSEUDOWIRE (NEW). Type = ethernet, ID = 100 ping statistics---
     5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 4/5/11 ms
```

2. 通过 **tracert** 命令，发现 CE2 可以正常接收来自 CE1 报文，并且 CE2 所发送的报文可以到达 PE1，则可以确定问题出在 PE1 向 CE1 发送的方向。

3. 在 PE1 的接口 GE1/0/0.1 下执行 **display this** 命令，查看 AC 接口的配置，发现没有配置 **local-ce ip** 和 **local-ce mac** 命令。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入 PE1 的 AC 接口视图。

步骤 3 执行命令 **local-ce ip** *ip-address*，配置本地 CE 接口的 IP 地址。或者执行命令 **local-ce mac** *mac-address*，配置本地 CE 接口的 MAC 地址。

完成上述操作后，本端 CE 可以 Ping 通对端 CE，故障排除。

----结束

案例总结

配置 PWE3 异种介质互通业务时，如果 PE 的 AC 接口是以太网接口，则必须使用 **local-ce ip** 命令或者 **local-ce mac** 命令配置 CE 的接口 MAC 地址或者 CE 的接口 IP 地址。

对于 PE3 的异种介质互通业务，CE 与 PE 直接进行协商。当 AC 接口是以太网类型时，协商就是 MAC 地址学习的过程。PE1 向 CE1 发送报文时，PE1 必须要知道 CE1 接口的 MAC 地址，可以通过 **local-ce mac** 命令将 CE1 接口 MAC 地址配置到 PE1 的直连端口上，这样在发送报文时，PE1 会直接封装配置的 MAC 地址。也可以通过 **local-ce mac** 命令将 CE1 接口的 IP 地址配置在 PE 的 AC 接口上，PE 通过该 IP 地址来学习到 CE1 接口 MAC 地址。

4.2.3 CE 的 MTU 设置不当，导致 CE 之间 OSPF 邻居无法建立

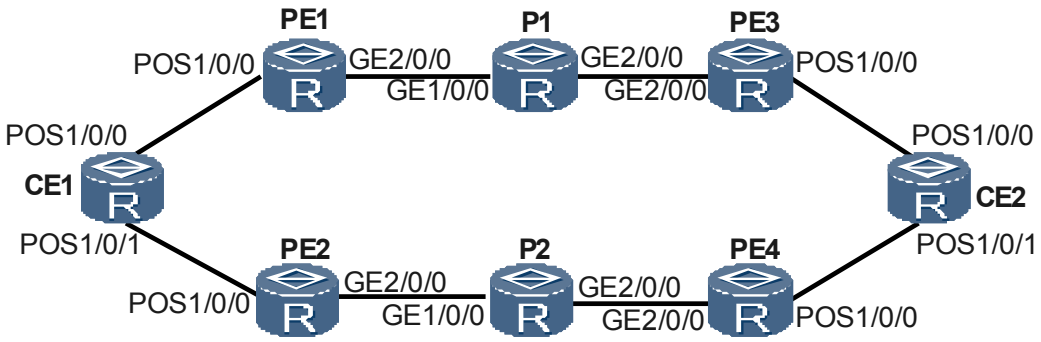
组网环境

如图 4-3，CE1 以双归属方式接入 PE1 和 PE2，CE2 以双归属方式接入 PE3 和 PE4。其中：

- CE1 和 CE2 使用 FR 接入 PE。
- 在 PE1 和 PE3 之间及 PE2 和 PE4 之间建立 PW，使用 MPLS LSP 作为隧道。
- 当路径 CE2-PE3-P-PE1-CE1 发生故障时，L2VPN 的流量能快速切换到备份路径 CE2-PE4-PE2-CE1 上。
- 当路径 CE2-PE3-P-PE1-CE1 故障恢复时，L2VPN 的流量能回切到主路径上。

在 PE 上配置了 VLL FRR（对称组网），在 CE 上创建了 128 个子接口并配置了不同的 IP 地址，然后在 CE1 和 CE2 上运行 OSPF，将各自的子接口地址发布给对端 CE。此时发现 CE 上发现大量的邻居状态不能为 FULL 状态，CE 之间无法互通。

图 4-3 CE 的 MTU 设置不当，导致 CE 之间 OSPF 邻居无法建立案例组网图



故障分析

CE 上 Ethernet 接口的 MTU 值为 4470，PE 与 P 之间为以太类型链路，其 MTU 值最大为 1500。当 CE 上配置了大量 OSPF 邻居的时候，OSPF 报文信息是一个大于 1500 的报文。由于 VLL 不支持分片，这些来自 CE 的较大的报文，通过 VLL 穿越 PE 与 P 之间的以太链路时，报文会被丢弃，因此 CE 之间的 OSPF 邻居也就无法建立。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number.subinterface-number*，进入 AC 子接口视图。

步骤 3 执行 **mtu** *mtu* 命令，配置接口的 MTU 值。

步骤 4 执行 **shutdown** 和 **undo shutdown** 命令，使 MTU 更改生效。

----结束

案例总结

由于 L2VPN 不支持对报文分片，所以从 CE 侧发送到 PE 的较大报文就无法向 PSN 侧进行转发。因此配置 VLL 时，建议在 CE 连接 PE 的接口上使用 **mtu** 命令配置接口的 mtu 值为 1500，这样 CE 对发往 PE 的较大报文会先进行分片，分片之后的报文可以在公网上被正确转发。

5 L2VPN IPRAN 故障处理

关于本章

介绍了 L2VPN IPRAN 故障常见的原因和定位思路。

5.1 集成场景的 IPRAN 组网-HVPLS+L3VPN/IP 存在丢包或多包问题的故障处理的定位思路
介绍 HVPLS+L3VPN/IP 组网的 IPRAN 中，CSG 设备上存在丢包或多包问题的故障处理流程和详细的故障处理步骤。

5.2 背靠背场景的 IPRAN-PWE3+(VSI+L3VPN)组网主备 PW 切换后丢包、多包或流量中断故障处理的定位思路
介绍背靠背场景的 IPRAN-PWE3+(VSI+L3VPN)组网中，主备 PW 切换后 CSG 设备上存在丢包、多包或流量中断问题的故障处理流程和详细的故障处理步骤。

5.3 背靠背场景的 IPRAN-HVPLS+L3VPN 组网丢包或流量中断故障处理的定位思路
介绍背靠背场景的 IPRAN-HVPLS+L3VPN 组网中，主备 PW 切换或回切后 CSG 设备上存在丢包或流量中断问题的故障处理流程和详细的故障处理步骤。

5.4 TDM/ATM 基站 PW Redundancy+APS 1:1 方式 IPRAN 组网 AC 侧链路切换后 L2VPN 业务流量中断故障处理的定位思路
TDM/ATM 基站 PW Redundancy+APS 1:1 方式 IPRAN 组网 AC 侧链路切换后 L2VPN 业务流量中断故障处理流程和详细的故障处理步骤。

5.5 故障案例

5.1 集成场景的 IPRAN 组网-HVPLS+L3VPN/IP 存在丢包或多包问题的故障处理的定位思路

介绍 HVPLS+L3VPN/IP 组网的 IPRAN 中，CSG 设备上存在丢包或多包问题的故障处理流程和详细的故障处理步骤。

5.1.1 常见原因

本类故障的常见原因主要包括：

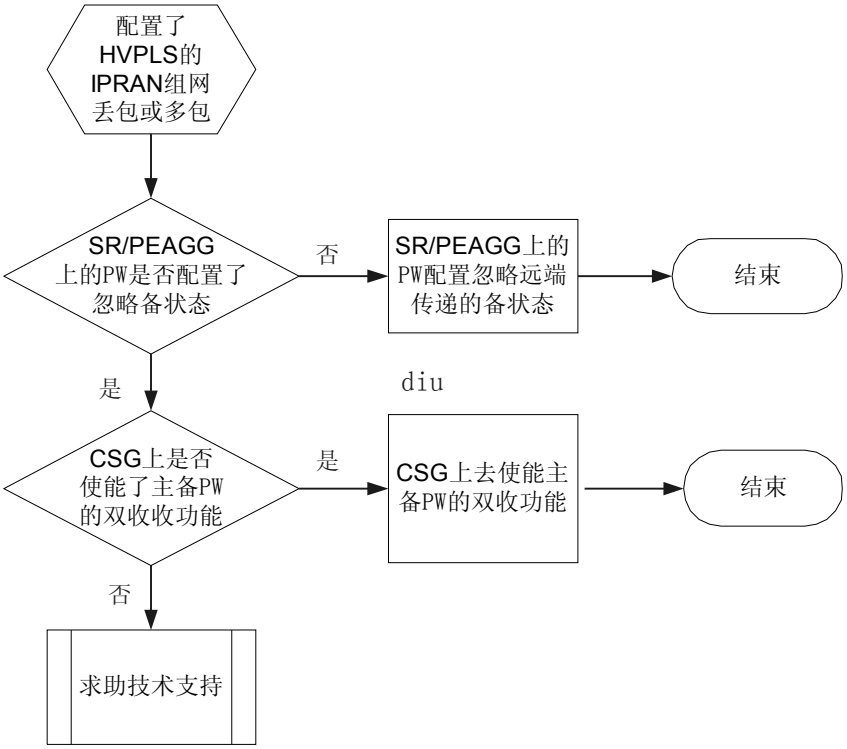
- SR 或 PEAGG 设备上配置 VPLS PW 时，没有配置 **ignore-standby-state** 参数。
- CSG 设备上配置了主备 PW 的双收功能，即主备 PW 同时具有接收报文的能力。

5.1.2 故障诊断流程

在配置 HVPLS+L3VPN/IP 组网的 IPRAN 后发现存在丢包或多包问题。

详细处理流程如图 5-1 所示。

图 5-1 HVPLS+L3VPN/IP 组网的 IPRAN 存在丢包或多包问题的故障诊断流程图



5.1.3 故障处理步骤

说明

请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

操作步骤

步骤 1 检查故障现象

- 如果出现丢包问题，请执行步骤 2。
- 如果出现多包问题，请执行步骤 3。

步骤 2 检查 SR 或 PEAGG 设备上配置 VPLS PW 时是否配置了 **ignore-standby-state** 参数

在 VSI-LDP 视图下执行 **display this**，检查配置的 PW 是否有 **ignore-standby-state** 参数。

- 如果没有配置 **ignore-standby-state** 参数，在 VSI-LDP 视图下执行 **undo peer** *peer-address* [**negotiation-vc-id** *vc-id*]命令删除原 PW，并执行 **peer** *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] **ignore-standby-state** 命令，重新创建 VPLS PW，使其忽略远端传递的备状态。

  说明

  - 在删除 VPLS PW 后，重新创建 VPLS PW 前的这段时间内，业务会临时中断。
  - 在采用了 M/S 模式的 PW Redundancy 组网中，当主用 PW 故障，切换到备份 PW 时，如果 SR 或 PEAGG 设备上的 PW 没有配置忽略远端传递的备状态，则该备状态会使本端 PW 不转发业务流量，直到远端 CSG 将备状态更新为主状态并将主状态传递本端后，本端 PW 才可以转发业务流量，这个过程可能导致数据包丢失。因此需要在 SR 或 PEAGG 设备上配置 PW 时选择 **ignore-standby-state** 参数，使 PW 忽略远端传递的备状态而始终处于转发状态，防止主备切换过程中丢包。
- 如果已经配置 **ignore-standby-state** 参数，请执行步骤 2。

步骤 3 检查 CSG 设备上是否配置了主备 PW 的双收功能

在 CSG 的 AC 接口视图下执行 **display this** 命令，查看是否配置了 **mpls l2vpn stream-dual-receiving** 命令。

- 如果配置了主备 PW 的双收功能，在 AC 接口视图下配置命令 **undo mpls l2vpn stream-dual-receiving** 命令取消该功能。

  说明

  配置主备 PW 双收功能的命令只能应用在 L2VPN 采用 PWE3 的组网中，用来在信令同步主备状态过程中减少丢包。而 L2VPN 采用 HVPLS 的组网不允许配置双收功能，这是因为 VPLS 广播会导致基站收到两份数据报文。
- 如果没有配置主备 PW 的双收功能，请执行步骤 3。

步骤 4 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

5.1.4 相关告警与日志

相关告警

无

相关日志

无

5.2 背靠背场景的 IPRAN-PWE3+(VSI+L3VPN)组网主备 PW 切换后丢包、多包或流量中断故障处理的定位思路

介绍背靠背场景的 IPRAN-PWE3+(VSI+L3VPN)组网中，主备 PW 切换后 CSG 设备上存在丢包、多包或流量中断问题的故障处理流程和详细的故障处理步骤。

5.2.1 常见原因

本类故障的常见原因主要包括：

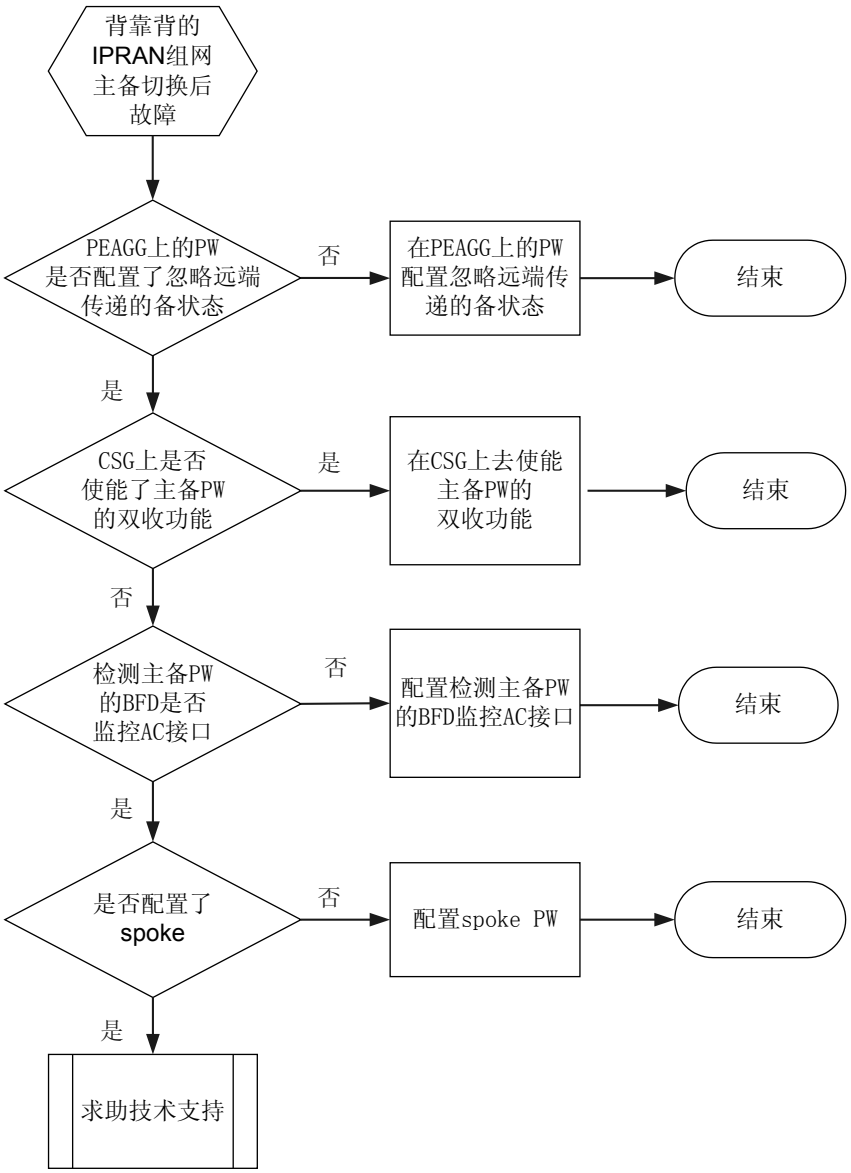
- PEAGG 上配置 PW 时没有配置忽略远端传递的备状态。
- CSG 节点使能了双收功能。
- UPE1 和 UPE2 之间没有配置 spoke PW。
- VRRP 监控的下行链路的接口没有转换为二层接口。
- 检测主备 PW 的 BFD 没有监控 AC 接口状态。

5.2.2 故障诊断流程

在配置背靠背场景的 IPRAN 组网后发现当主备 PW 切换后出现丢包、多包或流量中断问题。

详细处理流程如图 5-2 所示。

图 5-2 背靠背场景的 IPRAN 组网主备 PW 切换后丢包、多包或流量中断的故障诊断流程图



5.2.3 故障处理步骤

说明

请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

操作步骤

步骤 1 检查故障现象

- 如果出现丢包问题，请执行步骤 2。
- 如果出现多包问题，请执行步骤 4。

- 如果数据流量中断，请执行步骤 5。

步骤 2 检查 PEAGG 设备上配置 VPLS PW 时是否配置了 **ignore-standby-state** 参数

在 VSI-LDP 视图下执行 **display this**，检查配置的 PW 是否有 **ignore-standby-state** 参数。

- 如果没有配置 **ignore-standby-state** 参数，在 VSI-LDP 视图下执行 **undo peer** *peer-address* [**negotiation-vc-id** *vc-id*]命令删除原 PW，并执行 **peer** *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] **ignore-standby-state** 命令，重新创建 VPLS PW，使其忽略远端传递的备状态。

  说明

  - 在删除 VPLS PW 后，重新创建 VPLS PW 前的这段时间内，业务会临时中断。
  - 在采用了 M/S 模式的 PW Redundancy 组网中，当主用 PW 故障，切换到备份 PW 时，如果 PEAGG 设备上的 PW 没有配置忽略远端传递的备状态，则该备状态会使本端 PW 不转发业务流量，直到远端将备状态更新为主状态并将主状态传递本端后，本端 PW 才可以转发业务流量，这个过程可能导致数据包丢失。因此需要在 PEAGG 设备上配置 PW 时选择 **ignore-standby-state** 参数，使 PW 忽略远端传递的备状态而始终处于转发状态，防止主备切换过程中丢包。

- 如果已经配置 **ignore-standby-state** 参数，请执行步骤 3。

步骤 3 检查检测主备 PW 状态的 BFD 是否配置了监控 AC 接口状态

在 PEAGG1 和 PEAGG2 上执行 **display bfd configurationpwinterface*interface-typeinterface-number*verbose** 命令，其中 **interface** *interface-type interface-number* 为配置 PW 的 AC 接口。查看“Bind Interface”选项，BFD 会话监视的接口是否为 AC 接口。

```
<HUAWEI> display bfd configuration pw interface gigabitethernet 1/0/2.1 verbose
------------------------------------------------------------------------------
  BFD Session Configuration Name : test
------------------------------------------------------------------------------
  Local Discriminator    : 1               Remote Discriminator   : 1
  BFD Bind Type          : PW(Master)
  Bind Session Type      : Static
  Bind Interface         : GigabitEthernet1/0/2.1
  PW TTL Mode            : Auto            PW TTL                 : -
  Node                   : UPE
  Remote Peer            : 8.8.8.8
  Encapsulation Type     : -               Vc Id                  : -
  Select Board           : -
  Track Interface        : GigabitEthernet1/0/2.1
  TOS-EXP                : 7               Local Detect Multi     : 3
  Min Tx Interval (ms)   : 10              Min Rx Interval (ms)   : 10
  WTR Interval (ms)      : -               Process PST            : Enable
  Proc Interface Status  : Disable
  Bind Application       : L2VPN | OAM_MANAGER | MPLSFW
  Session Description    : -
------------------------------------------------------------------------------
```

- 如果不是，在系统视图下配置命令 **bfd** *cfg-name* **bind pw interface** *interface-type interface-number* [**remote-peer** *remote-peer-address* **pw-ttl** { **auto-calculate** | *ttl-number* }] **track-interface**，配置 BFD 会话检测主 PW 并监视 AC 接口状态。

  说明

  配置 BFD 检测 PW 的同时，要监视 AC 接口状态，保证 PEAGG 和 UPE 之间链路故障时 PW 能够同步切换，否则会导致主备 PW 切换过程中丢包。

- 如果是，请执行步骤 6。

步骤 4 检查 CSG 设备上是否配置了主备 PW 的双收功能

在 CSG 的 AC 接口视图下执行 **display this** 命令，查看是否配置了 **mpls l2vpn stream-dual-receiving** 命令。

- 如果配置了主备 PW 的双收功能，在 AC 接口视图下配置命令 **undo mpls l2vpn stream-dual-receiving** 命令取消该功能。

  说明

  配置主备 PW 双收功能的命令只能应用在 L2VPN 采用 PWE3 的组网中，用来在信令同步主备状态过程中减少丢包。而 L2VPN 采用 HVPLS 的组网不允许配置双收命令，这是因为 VPLS 广播会导致基站收到两份数据报文。

- 如果没有配置主备 PW 的双收功能，请执行步骤 6。

步骤 5 检查 PEAGG 或 UPE 之间是否配置了 spoke PW

下面以 UPE1 和 UPE2 之间需要配置 spoke PW 为例。

在 UPE1 和 UPE2 上执行 **display vsi** [**name** *vsi-name*] [**verbose**]命令，查看是否存在“PW Type”项为“MEHVPLS”的 PW。

- 如果不存在，在 VSI-LDP 视图下执行命令 **peer** *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] **upe ignore-standby-state** 配置 spoke PW。UPE1 和 UPE2 设备上都需要配置，且配置相同。

  说明

  主备 PW 切换后，数据流量要从 spoke PW 绕行，如果没有配置 spoke PW，会导致流量中断。

- 如果存在，请执行步骤 6。

步骤 6 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

5.2.4 相关告警与日志

相关告警

无

相关日志

无

5.3 背靠背场景的 IPRAN-HVPLS+L3VPN 组网丢包或流量中断故障处理的定位思路

介绍背靠背场景的 IPRAN-HVPLS+L3VPN 组网中，主备 PW 切换或回切后 CSG 设备上存在丢包或流量中断问题的故障处理流程和详细的故障处理步骤。

5.3.1 常见原因

本类故障的常见原因主要包括：

- VRRP 监控的下行链路的接口没有转换为二层接口。

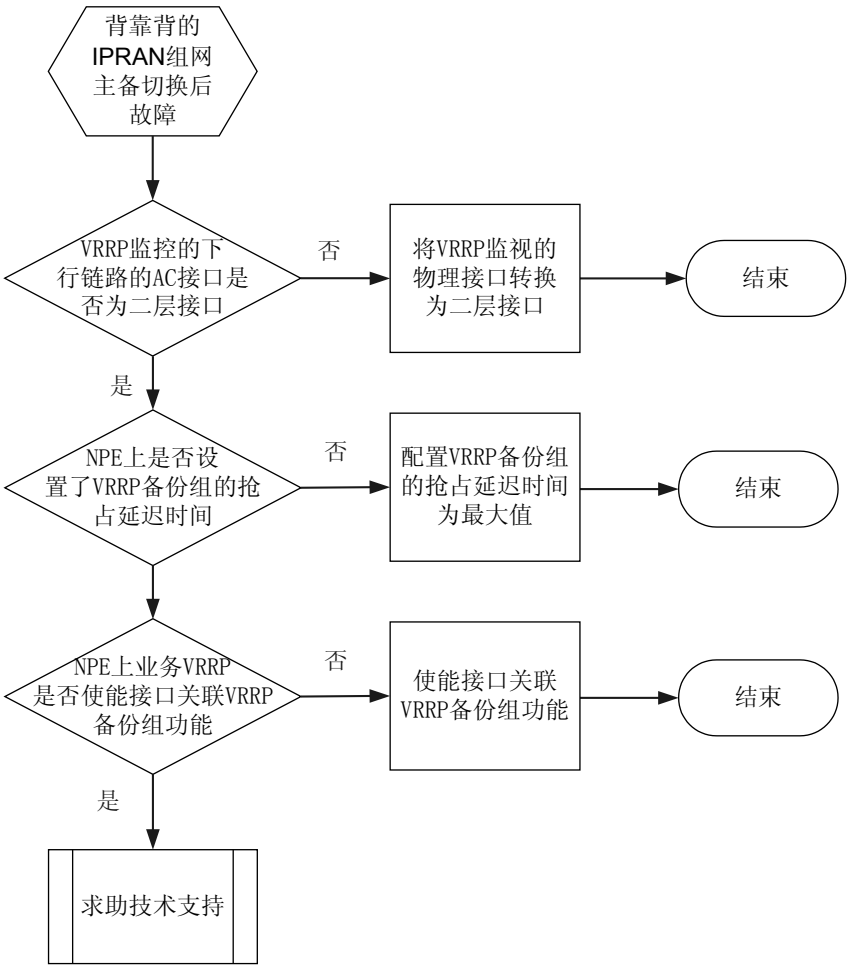
- NPE 设备上的管理 VRRP 备份组没有设置了抢占延迟时间或设置的延迟时间过短。
- NPE 设备上的业务 VRRP 没有使能接口关联 VRRP 备份组功能。

5.3.2 故障诊断流程

在配置背靠背场景的 IPRAN－HVPLS+L3VPN 组网后发现当主备 PW 切换或回切后出现丢包或流量中断问题。

详细处理流程如图 5-3 所示。

图 5-3 背靠背场景的 IPRAN－HVPLS+L3VPN 组网主备 PW 切换或回切后丢包或流量中断的故障诊断流程图



5.3.3 故障处理步骤

说明

请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

操作步骤

步骤 1 检查故障现象

- 如果数据流量中断，请执行步骤 2。
- 如果出现丢包问题，请执行步骤 3。

步骤 2 检查 VRRP 监控的下行链路的 AC 接口是否为二层接口。

在 UPE1 或 UPE2 上 AC 接口下执行 **display this** 命令，查看该接口下是否配置了 **portswitch** 命令。

- 如果没有配置，则在该接口视图下配置命令 **portswitch** 将该接口转换为二层接口。

  说明

  此处配置 VRRP 通过监视接口的状态来实现主备快速切换的功能，是为了当 PEAGG 和 UPE 之间的物理链路故障时，VRRP 可以实现快速切换，与 PW 主备切换保持一致。VRRP 监视的是该接口的协议状态，如果接口为三层接口，由于配置了 L2VPN 导致协议状态始终为 down，VRRP 无法成功协商。因此要将 VRRP 监控的物理接口转换为二层接口，协议状态为 up，VRRP 才能正确协商主备。

- 如果已经配置，请执行步骤 5。

步骤 3 检查 NPE1 上是否设置了管理 VRRP 备份组中路由器的抢占延迟时间。

在 NPE1 设备上配置管理 VRRP 的接口视图下执行 **display this** 命令，检查是否配置了 **vrrp vrid preempt-mode timer delay**，即是否设置了 VRRP 备份组中路由器的抢占延迟时间。

- 如果没有该配置或配置数值较小，请在该接口视图下执行 **vrrp vrid***virtual-router-id***preempt-modetimerdelay** *delay-value* 命令，将设备抢占延迟时间 **delay** *delay-value* 设置为最大值。

  说明

  当 PE-AGG1 节点故障恢复时，对于 RNC 到基站的数据流量，如果 VRRP 回切快而 CSG 到 PE-AGG1 的 PW 或 spoke PW 恢复慢，RSG1 通过 VPN 回切将流量转发到 NPE1，而 NPE1 将流量转发到 PE-AGG1 后流量就找不到 PW 转发而中断。因此需要在 NPE1 的管理 VRRP 上配置回切延时，延长 VRRP 的回切时间，等到 PW 建立并回切后再回切。

- 如果已经配置且设备抢占延迟时间 **delay** *delay-value* 设置为最大值，请执行步骤 4。

步骤 4 检查 NPE1 设备上业务 VRRP 是否使能接口关联 VRRP 备份组功能。

在 NPE1 设备上配置业务 VRRP 的接口视图下执行 **display this** 命令，检查是否配置了 **direct-route track vrrp**，即是否使能接口关联 VRRP 备份组功能，设备根据 VRRP 备份组状态来调整接口的链路开销值。

- 如果没有该配置，请执行 **direct-route track vrrp vrid** *virtual-router-id* **degrade-cost** *cost* 命令使能接口关联 VRRP 备份组功能。

  说明

  VRRP 备份组中，不论设备处于 Master 还是 Backup 状态下，其接口网段的 IP 地址都会发布给 L3VPN，上一步骤的延时功能并不能保证 RSG1 的 VPN FRR 在 VRRP 之后回切，因此需要在 NPE1 上的业务 VRRP 上配置直连路由联动优先级，通过降低 Backup 状态下的路由优先保证 RSG1 上的延时回切。

- 如果已经配置，请执行步骤 5。

步骤 5 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。

- 设备的配置文件、日志信息、告警信息。

----结束

5.3.4 相关告警与日志

相关告警

无

相关日志

无

5.4 TDM/ATM 基站 PW Redundancy+APS 1:1 方式 IPRAN 组网 AC 侧链路切换后 L2VPN 业务流量中断故障处理的定位思路

TDM/ATM 基站 PW Redundancy+APS 1:1 方式 IPRAN 组网 AC 侧链路切换后 L2VPN 业务流量中断故障处理流程和详细的故障处理步骤。

5.4.1 常见原因

本类故障的常见原因主要包括：

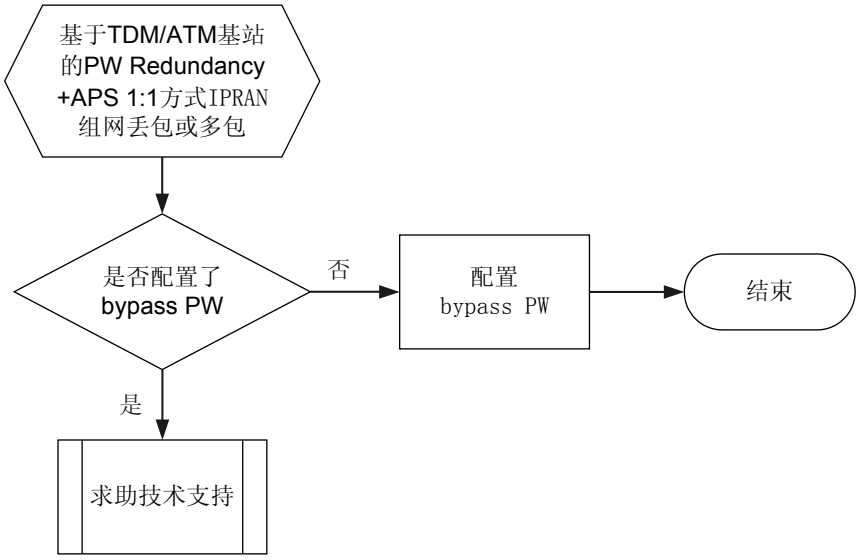
- 没有配置 Bypass PW。

5.4.2 故障诊断流程

在配置 TDM/ATM 基站 PW Redundancy+APS 1:1 方式 IPRAN 组网 AC 侧链路切换后发现 L2VPN 业务流量中断。

详细处理流程如图 5-4 所示。

图 5-4 TDM/ATM 基站 PW Redundancy+APS 1:1 方式 IPRAN 组网 AC 侧链路的故障诊断流程图



5.4.3 故障处理步骤

说明

请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

操作步骤

步骤 1 检查 RSG1 和 RSG2 之间是否配置了 bypass PW

在 RSG1 和 RSG2 的 AC 接口下执行 **display mpls l2vc interface** *interface-type interface-number* 命令，查看 AC 接口下配置的 PW 中，是否存在“primary or secondary or bypass”项为“bypass”的 PW。

- 如果不存在，在 AC 接口视图下执行命令 **mpls l2vc** { *ip-address* | **pw-template** *pw-template-name* }* *vc-id* [**group-id** *group-id* | **tunnel-policy** *policy-name* | [**control-word** | **no-control-word**] | [**ip-interworking** | **ip-layer2** | **raw** | **tagged**]]* **bypass**，创建 Bypass PW。RSG1 和 RSG2 设备上都需要配置，且配置相同。

  说明

  主备 PW 切换后，数据流量要从 bypass PW 绕行，如果没有配置 bypass PW，会导致流量中断。
- 如果存在，请执行步骤 2。

步骤 2 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

5.4.4 相关告警与日志

相关告警

无

相关日志

无

5.5 故障案例

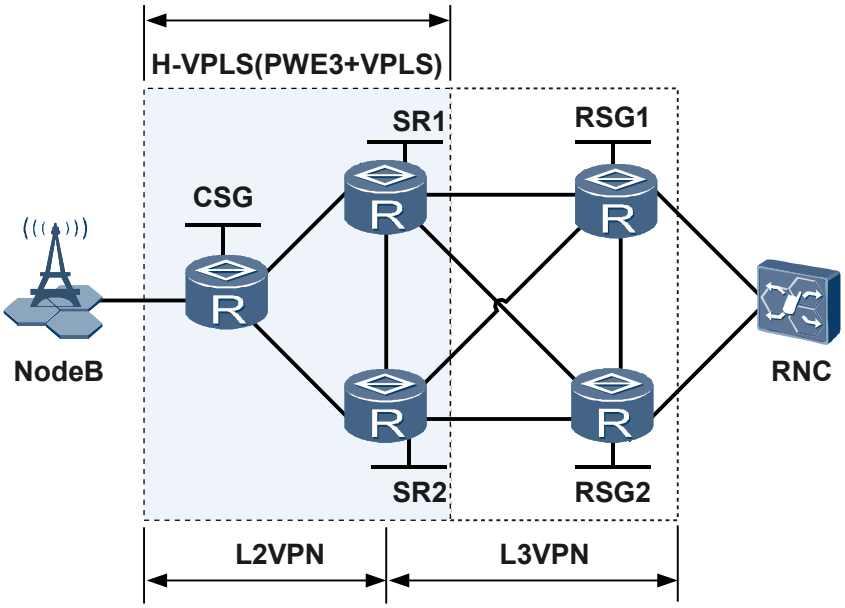
5.5.1 配置 VPLS 的 PEER 时没有配置忽略远端主备状态参数导致切换过程中丢包过多

在 HVPLS+L3VPN/IP 组网的 IPRAN 中，配置 VPLS 的 PEER 时没有配置忽略远端主备状态参数，会导致导切换过程中丢包过多。

网络环境

如图 5-5 所示，在 HVPLS+L3VPN/IP 组网的 IPRAN 中，L2VPN 配置了 HVPLS（PWE3 接入 VPLS），并采用 M/S 方式 PW 冗余确定主备。配置完成后发现主备 PW 切换过程中丢包过多。

图 5-5 HVPLS+L3VPN 的 IPRAN 组网图



故障分析

1. 在 CSG 上执行命令 **display mpls l2vc interface** *interface-type interface-number*，查看字段“PW redundancy mode”的值为 master，配置的 PW 冗余确定主备的方式为 M/S，表明主备 PW 切换的过程中 CSG 会向 SR1 和 SR2 发送主备切换的消息。

2. 在 SR1 和 SR2 上执行命令 **display vpls connection**，查看字段“VCState”的值。“VCState”为 Up，表明二层隧道已正常建立。
3. 在 SR1 和 SR2 上的 VSI-LDP 视图下执行 **display this**，查看配置的 PW 是否有 **ignore-standby-state** 参数，发现没有配置忽略远端主备状态参数。

   在采用了 M/S 模式的 PW Redundancy 组网中，当主用 PW 故障，切换到备份 PW 时，如果备份 PW 处于备状态，则无法转发业务流量，可能导致数据包丢失。此时需要在 SR 设备上配置 PW 时选择 **ignore-standby-state** 参数，使 PW 忽略远端传递的备状态而始终处于转发状态，可以防止主备切换时丢包。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vsi** *vsi-name*，进入 VSI 视图。

步骤 3 执行命令 **undo peer** *peer-address* [**negotiation-vc-id** *vc-id*]命令删除原 PW。

步骤 4 执行命令 **peer** *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] **ignore-standby-state**，重新创建 VPLS PW，使其忽略远端传递的备状态。

完成上述操作后，可以检测到丢包数量大幅度减少，故障排除。

----结束

案例总结

在 HVPLS+L3VPN/IP 组网的 IPRAN 中，配置 VPLS 的 peer 时，应该配置 **ignore-standby-state** 参数，使 PW 忽略远端传递的备状态而始终处于转发状态，减少在主备切换时信令同步主备状态的过程中丢包。

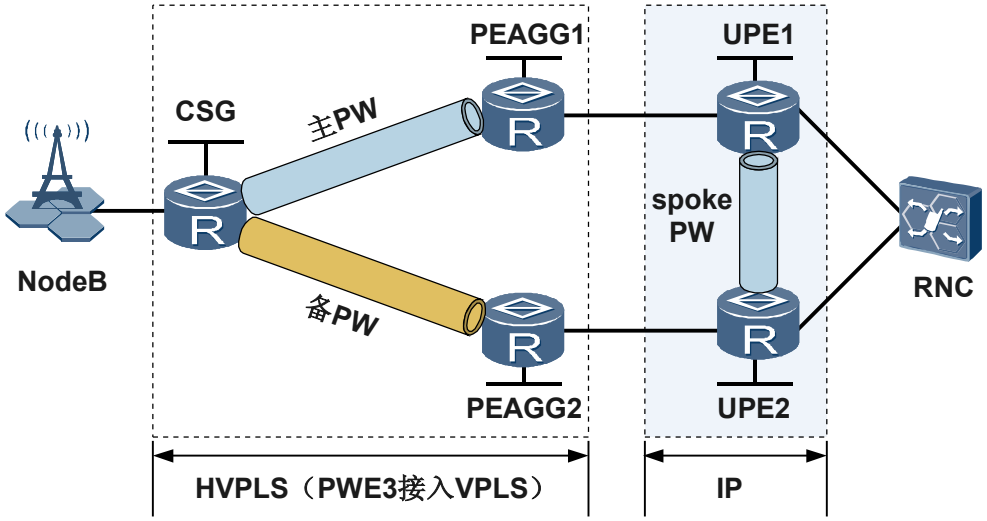
5.5.2 背靠背场景的 IP RAN－PWE3+(VSI+IP)组网主备 PW 切换后流量中断

背靠背场景的 IP RAN－PWE3+(VSI+IP)组网中，VRRP 监控的下行链路的 AC 接口没有转换为二层接口，会导致下挂 VPLS 业务不通。

网络环境

如图 5-6 所示，二三层网络之间为背靠背关系，L2VPN 配置了 HVPLS，并采用 M/S 方式 PW 冗余确定主备。UPE1 和 UPE2 之间配置 spoke PW 实现故障隔离。配置完成后发现主备 PW 切换后流量中断。

图 5-6 背靠背场景 IP RAN－PWE3+(VSI+IP)组网图



故障分析

1. 在 UPE1 和 UPE2 上执行 **display vsi** [**name** *vsi-name*] [**verbose**]命令，查看“PW Type”选项为“MEHVPLS”，表明配置了 spoke PW。
2. 在 UPE1 和 UPE2 上 AC 接口下执行 **display this** 命令，发现该接口下没有配置 **portswitch**，VRRP 监视该接口的协议状态，由于该接口绑定了 VSI，因此协议一直 down，VRRP 无法协商成功。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入 UPE1 和 UPE2 的接口视图。

步骤 3 执行命令 **portswitch**，将该接口转换为二层接口。

步骤 4 执行命令 **quit**，返回系统视图。

完成上述操作后，数据流量恢复，故障排除。

----结束

案例总结

由于 VRRP 检测接口的状态为该接口的协议状态，为了保证在检测的接口在没有配置 IP 地址的情况下协议状态为 UP，需要在该接口下执行 **portswitch** 命令，将该接口转换为二层接口。