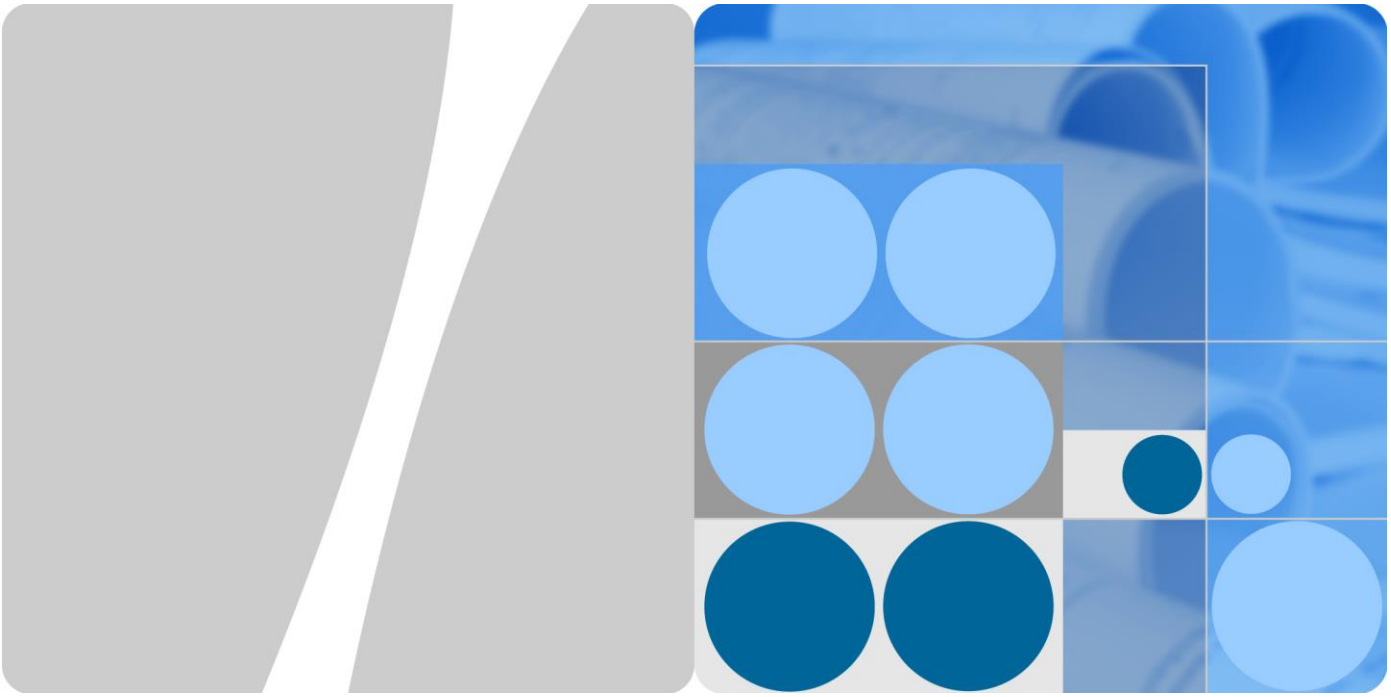


HUAWEI NE 系列路由器

配置规范与部署规范

文档版本 05

发布日期 2017-1-16

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

目 录

1 配置规范.....1
1.1 基础配置.....2
1.1.1 配置用户登录的配置规范.....2
1.1.1.1 设备作为 SSH 客户端保存 SSH 公钥数应少于 20 个.....2
1.1.1.2 VTY 通道配置 ACL 的配置规范.....3
1.2 系统管理.....4
1.2.1 NTP.....4
1.2.1.1 NTP 需要配置 preference 参数设置优先选择的服务器.....4
1.2.1.2 NTP MD5/SHA56 认证配置规范.....4
1.2.2 NQA.....5
1.2.2.1 NQA 探测周期配置规范.....5
1.3 可靠性.....7
1.3.1 BFD 的配置规范.....7
1.3.1.1 BFD for LSP 会话报文来回路径需要一致才能保证 LSP 路径正常切换.....7
1.3.1.2 静态 BFD 两端设备配置对称实现流量不中断.....9
1.3.1.3 BFD 描述符配置规范.....12
1.3.1.4 静态 BFD for CR-LSP 隧道往返路径需要保持一致才能实现业务正常切换.....14
1.3.1.5 内层链路的 BFD 检测间隔应小于外层链路的检测间隔.....17
1.3.1.6 双向 LSP 场景下两端设备的 BFD 配置需对称.....19
1.3.2 多机备份的配置规范.....21
1.3.2.1 双机热备场景下部署共享地址池时需要配置保护隧道.....21
1.3.2.2 双机热备场景下部署共享地址池时网络侧接口需要去使能 URPF.....23
1.3.3 VRRP 的配置规范.....26
1.3.3.1 VRRP 中间链路需要配置 Eth-Trunk 保护的配置规范.....26
1.3.4 TE Tunnel 没有配置误码倒换导致业务受损.....28
1.4 接口管理.....29
1.4.1 接口管理的配置规范.....29
1.4.1.1 物理接口需要配置接口延迟发出信号.....29
1.4.1.2 物理接口需要配置接口延迟 Down 或延迟告警功能.....30
1.5 局域网与城域网接入.....31
1.5.1 MAC 的配置规范.....31

1.5.1.1 二层设备上行流量少的场景下 MAC 老化时间需要配置大于或接近 ARP 老化时间 31
1.5.2 Eth-Trunk 的配置规范 33
1.5.2.1 部署 E-Trunk 的两台设备全局配置需完全一致 33
1.5.2.2 Eth-Trunk 需配置 LACP 模式或成员接口绑定 BFD 会话 35
1.5.2.3 一端未加入 Eth-Trunk 导致流量不通 37
1.5.3 IP-Trunk 的配置规范 39
1.5.3.1 IP-Trunk 需配置成员接口绑定 BFD 会话 39
1.6 IP 业务 42
1.6.1 IP 性能配置的配置规范 42
1.6.1.1 TCP window-size 配置规范 42
1.6.2 IPv6 基础配置的配置规范 43
1.6.2.1 TCP6 window-size 配置规范 43
1.7 IP 路由 44
1.7.1 IGP 公共的配置规范 44
1.7.1.1 IGP 邻居超时时间配置规范 44
1.7.1.2 IGP 引入路由优先级需要高于 IGP 的路由避免流量绕行 47
1.7.2 OSPF 的配置规范 51
1.7.2.1 OSPF 两端接口网络类型需要配置一致才能实现邻居建立后正常学习路由 51
1.7.3 ISIS 的配置规范 53
1.7.3.1 割接过程中需要删除发布的缺省路由 53
1.7.3.2 IS-IS 配置 IPv6 标准拓扑模式下使用 IPv6 拓扑 55
1.7.4 BGP 的配置规范 58
1.7.4.1 BGP 路由优先级配置规范 58
1.8 IP 组播 61
1.8.1 PIM 的配置规范 61
1.8.1.1 三层组播的备路径或等价链路接口要使能 PIM 功能 61
1.9 MPLS 62
1.9.1 MPLS LDP 的配置规范 62
1.9.1.1 多链路或本远共存场景的参数配置规范 62
1.9.1.2 接口下需要配置 LDP-IGP 联动 66
1.9.2 MPLS TE 的配置规范 68
1.9.2.1 跨 IGP 域建立 TE 隧道需要配置显示路径 68
1.9.2.2 RSVP-TE GR 功能需要在 RSVP-TE 接口下配置 RSVP-TE Hello 70
1.9.2.3 IGP 多进程或多区域场景 CSPF 算路与预期不符 72
1.9.2.4 TE 隧道建议部署在主控板 76
1.9.2.5 TE Tunnel 配置路由发布功能后，需要同时配置 LDP Remote 会话 77
1.9.2.6 TE FRR 场景需要在旁路隧道的 PLR(Point of Local Repair)节点和 MP(Merge Point)节点间建立 Hello 会话的配置规范 78
1.10 VPN 79
1.10.1 BGP/MPLS IP VPN 的配置规范 79

1.10.1.1 B 类型单板的 L3VPN 配置规范 79
1.10.1.2 CE 双归组网中相同的 VPN 实例 RD 不能相同 82
1.10.1.3 取消接口与 VPN 实例的绑定关系导致联动删除 BFD 的配置 84
1.11 安全 87
1.11.1 IPSec 的配置规范 87
1.11.1.1 多块 VSUI-20-A 部署 IPSec 双机热备场景下需要配置绑定保护组的 VSU 单板数门限值 87
1.11.1.2 IPSec 业务场景下需要配置 IKE DPD 保证 IPSec 隧道两端状态一致 89
1.11.1.3 IPSec 双机热备场景下主备 IPSec 设备之间链路的 MTU 值需要配置大于 2000 89
1.11.2 URPF 的配置规范 92
1.11.2.1 多路负载分担场景下需要配置 URPF 对匹配缺省路由的报文进行转发处理 92
1.12 用户接入 93
1.12.1 地址管理配置规范 93
1.12.1.1 限制 DHCP 用户连接请求防止业务繁忙影响正常用户上线 93
1.12.1.2 RUI 用户触发上线获取的地址不是域下地址池范围内的地址 94
1.12.2 WLAN 无线漫游场景的参数配置规范 94
1.12.3 一 MAC 多 Session 用户接入场景错误案例 96
1.12.4 WEB 用户上线 ACL 配置规范 97
1.13 增值业务 98
1.13.1 DAA 的配置规范 98
1.13.1.1 对配置了 DAA 业务的用户做 NAT 地址转换必须在业务模板下绑定正确的 VPN 实例 98
1.14 IPv6 过渡技术 99
1.14.1 CGN 的配置规范 99
1.14.1.1 CGN 需要配置冗余备份 99
1.14.1.2 CGN 场景 port-range 参数配置规范 105
2 部署规范 107
2.1 用户接入侧场景下需要配置冗余备份 108
2.2 网络侧链路需要配置冗余备份 113
2.3 路由器和周边服务器对接场景下需要配置冗余备份 114
2.4 双机热备场景下 RBS 需要配置 track 网络侧接口 114
2.5 CGN 需要配置冗余备份 117
2.6 GRE 需要配置冗余备份 122
2.7 L2TP 需要配置冗余备份 123
2.8 Hybrid Access 需要配置冗余备份 123

1 配置规范

关于本章

说明

本文档介绍了 NE 系列路由器在某些应用场景中的配置规范，此规范要求用户在 NE 系列路由器部分特性的配置与维护时，必须按照配置规范要求进行业务部署，避免因错误配置、错误使用或可靠性缺失造成业务中断。

1.1 基础配置
1.2 系统管理
1.3 可靠性
1.4 接口管理
1.5 局域网与城域网接入
1.6 IP 业务
1.7 IP 路由
1.8 IP 组播
1.9 MPLS
1.10 VPN
1.11 安全
1.12 用户接入
1.13 增值业务
1.14 IPv6 过渡技术

1.1 基础配置

1.1.1 配置用户登录的配置规范

1.1.1.1 设备作为 SSH 客户端保存 SSH 公钥数应少于 20 个

当设备保存的 SSH 公钥数达到 20 个，设备作为 SSH 客户端无法登录新的服务器。

应用场景

设备作为 SSH 客户端登录 SSH 服务器。

配置规范

设备作为 SSH 客户端，保存的 SSH 公钥数需要少于 20 个。

非规范配置的风险

风险描述

设备保存的 SSH 公钥数达到 20 个时，通过 **stelnet** 命令无法登录到新的 SSH 服务器。

风险的判断方法

在用户视图下，执行 **display current-configuration** | *include assign rsa-key* 命令，查看客户端公钥数是否达到 20 个。

从显示信息可以看出，如下客户端公钥数已达到 20 个。

```
<HUAWEI> display current-configuration | include assign rsa-key
#
ssh client 1.1.1.1 assign rsa-key 1.1.1.1
ssh client 2.2.2.2 assign rsa-key 2.2.2.2
ssh client 3.3.3.3 assign rsa-key 3.3.3.3
ssh client 4.4.4.4 assign rsa-key 4.4.4.4
ssh client 5.5.5.5 assign rsa-key 5.5.5.5
ssh client 6.6.6.6 assign rsa-key 6.6.6.6
ssh client 7.7.7.7 assign rsa-key 7.7.7.7
ssh client 8.8.8.8 assign rsa-key 8.8.8.8
ssh client 9.9.9.9 assign rsa-key 9.9.9.9
ssh client 1.1.2.1 assign rsa-key 1.1.2.1
ssh client 1.1.3.1 assign rsa-key 1.1.3.1
ssh client 1.1.4.1 assign rsa-key 1.1.4.1
ssh client 1.1.5.1 assign rsa-key 1.1.5.1
ssh client 1.1.6.1 assign rsa-key 1.1.6.1
ssh client 1.1.7.1 assign rsa-key 1.1.7.1
ssh client 1.1.8.1 assign rsa-key 1.1.8.1
ssh client 1.1.9.1 assign rsa-key 1.1.9.1
ssh client 1.1.10.1 assign rsa-key 1.1.10.1
ssh client 1.1.11.1 assign rsa-key 1.1.11.1
ssh client 1.1.12.1 assign rsa-key 1.1.12.1
#
```

风险的恢复方案

删除不使用的客户端公钥。

```
<HUAWEI> system-view
[HUAWEI] undo ssh client 1.1.1.2 assign rsa-key
```

1.1.1.2 VTY 通道配置 ACL 的配置规范

当 VTY 下不配置 ACL 时可能受到外部攻击，造成 CPU 使用率高。

应用场景

用户通过 Telnet 或者 SSH 方式登录设备。

配置规范

VTY 通道中通过配置 ACL 设置呼入呼出权限限制。

非规范配置的风险

风险描述

VTY 通道下未配置 ACL，设备受到外部报文攻击时，设备 CPU 使用率高，严重时会影响业务运行。

风险的判断方法

在用户视图下执行 **display current-configuration** 命令，查看 VTY 下面是否所有通道都配置了 **acl** *acl-number* **inbound** | **outbound**。

从显示信息可以看出，VTY 16-20 未配置 **acl** *acl-number* **inbound** | **outbound**。

```
<HUAWEI> display current-configuration configuration
#
user-interface vty 0 14
 acl 3100 inbound
 authentication-mode aaa
 protocol inbound ssh
user-interface vty 16 20
 authentication-mode aaa
 protocol inbound ssh
#
```

风险的恢复方案

请按照配置规范进行配置。

1.2 系统管理

1.2.1 NTP

1.2.1.1 NTP 需要配置 preference 参数设置优先选择的服务器

通过 **ntp-service unicast-server** *server-ip* 命令指定多个不同的 NTP 服务器时，要为其中一个 NTP 服务器增加 preference 参数，将其设置为优选服务器，可以避免本设备在不同的 NTP 服务器之间反复震荡切换。

应用场景

在系统视图下，执行 **ntp-service unicast-server** *server-ip* 命令指定多个不同的 NTP 远端服务器。

配置规范

在系统视图下执行 **ntp-service unicast-server** *server-ip* **preference** 命令，将其中一个服务器设置为优选服务器。

非规范配置的风险

风险描述

当在远端服务器上执行 **ntp-service unicast-server** *server-ip* 命令，未配置 **preference** 参数时，NTP 客户端会在多个远端服务器之间反复切换，导致 NTP 客户端时间频繁变化，并记录大量日志。

风险的判断方法

在用户视图下，执行 **display current-configuration configuration** *ntp* 命令查询 NTP 客户端的配置。

从显示信息可以看出，指定的远端服务器个数超过 1 个并且都没有配置 **preference** 参数。

```
<HUAWEI> display current-configuration configuration ntp
#
ntp-service unicast-server 10.1.1.1
ntp-service unicast-server 10.1.1.2
#
```

风险的恢复方案

请按照配置规范进行配置。

1.2.1.2 NTP MD5/SHA56 认证配置规范

NTP 设置 MD5/SHA56 认证方式并且配置 **ntp-service authentication enable** 命令后必须同时配置多条命令，否则无法和 NTP 服务器进行时钟同步。

应用场景

设备作为 NTP 客户端，在系统视图下配置了 **ntp-service authentication enable** 命令，使能 NTP 验证功能。

配置规范

在系统视图下，如下命令必须同时配置，才能保证 NTP 客户端和 NTP 服务器进行时钟同步。

```
<HUAWEI> system-view
[HUAWEI] ntp-service authentication enable
[HUAWEI] ntp-service reliable authentication-keyid 169
[HUAWEI] ntp-service unicast-server 172.0.0.1 authentication-keyid 169
[HUAWEI] ntp-service authentication-keyid 169 authentication-mode md5 cipher
Root@123
```

非规范配置的风险

风险描述

缺少以下一条或多条配置时，NTP 客户端无法和服务器进行时钟同步。

- **ntp-service authentication-keyid** *key-id* **authentication-mode** *mode* **cipher** *password*
- **ntp-service reliable authentication-keyid** *key-id key-id*
- **ntp-service unicast-server** *server-ip* **authentication-keyid** *key-id*（该命令仅客户端涉及，服务器端不涉及）

风险的判断方法

在用户视图下，执行 **display current-configuration configuration** *ntp* 命令查询 NTP 客户端的配置。

从显示信息可以看出，设备启用了 NTP 身份验证功能，缺少密钥的配置。

```
<HUAWEI> display current-configuration configuration ntp
#
ntp-service authentication enable
#
```

风险的恢复方案

请按照配置规范进行配置。

1.2.2 NQA

1.2.2.1 NQA 探测周期配置规范

NQA 测试例周期配置过短，在测试例一轮探测尚未执行结束，下一轮就开始了，导致测试结果为 no result，影响其他联动协议，存在其他协议联动 NQA 失效的风险。

应用场景

NQA 探测。

配置规范

1. 在 NQA 视图下，执行 **stop** 命令，停止测试例执行。
2. 在 NQA 视图下，执行 **frequency** *interval* 命令，配置 NQA 探测周期。需确保：探测周期>（探测次数-1）* 探测间隔 + 探测超时时间。
3. 在 NQA 视图下，执行 **start now** 命令，开始执行测试例。

非规范配置的风险

风险描述

在 NQA 视图下，执行 **frequency** *interval* 命令配置 NQA 测试例的探测周期，如果配置的探测周期<（探测次数-1）*探测间隔+探测超时时间，则发生问题时单板重启，NQA 联动的其他业务，如路由协议、VRRP 等，会出现联动功能失效，从而影响到业务转发。

业务现象如下：

NQA 测试结果为 no result。

风险的判断方法

用户视图下，执行 **display current-configuration configuration** *nqa* 命令查看 NQA 测试例配置。

从显示信息可以看出，NQA 测试例的探测周期为 20 秒，探测次数为 5，探测间隔为 6 秒，探测超时时间为 4 秒。探测周期< （探测次数-1）* 探测间隔 + 探测超时时间。因此该测试例探测结果为“no result”。

```
<HUAWEI> display current-configuration configuration nqa
#
nqa test-instance 1 1
 test-type icmp
 destination-address ipv4 127.0.0.1
 frequency 20
 interval seconds 6
 timeout 4
 probe-count 5
 start now
#
```

风险的恢复方案

请按照配置规范进行配置。

1.3 可靠性

1.3.1 BFD 的配置规范

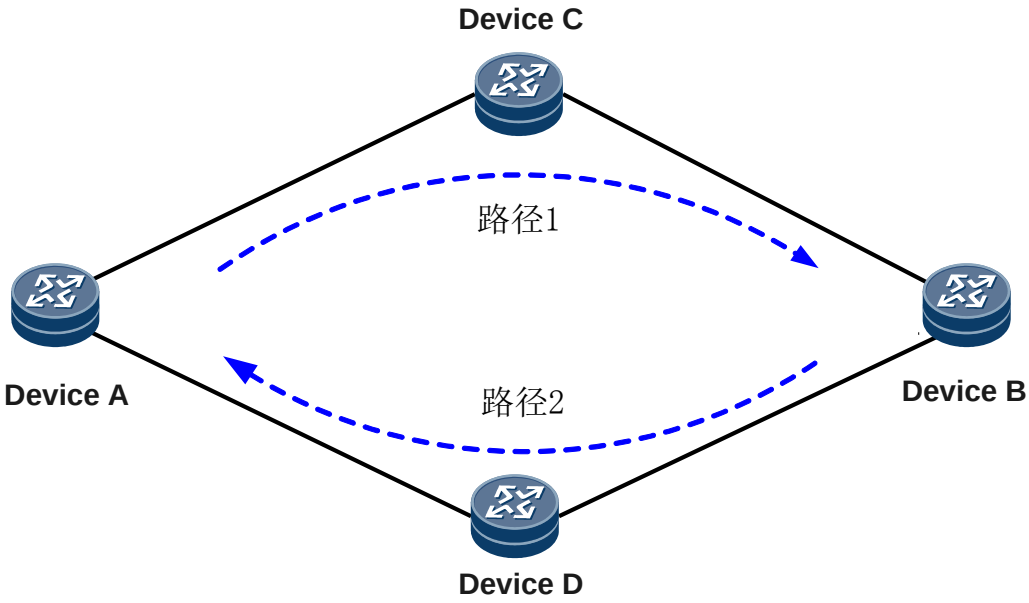
1.3.1.1 BFD for LSP 会话报文来回路径需要一致才能保证 LSP 路径正常切换

配置 BFD for LSP 会话检测时，从源端设备到宿端设备的 LSP 路径与回程的 LSP 或者 IP 路径不一致。回程 LSP 或者 IP 路径故障时，BFD 会话 Down，导致 LSP 路径误切换。

应用场景

如图 1-1 所示，RouterA 与 RouterB 之间存在两条路径，路径 1 和路径 2。

图1-1 BFD for LSP 会话报文来回路径不一致导致 LSP 路径误切换组网图



配置规范

在网络部署 BFD for LSP 会话检测时：

1. 动态 BFD for LSP 会话，可以考虑配置路由约束方式，保证来回路径一致，例如使用高优先级的静态路由。
2. 静态 BFD for LSP 会话（不包括 BFD for TE-LSP），可以考虑配置路由约束方式，保证来回路径一致，例如使用高优先级的静态路由。
3. 静态 BFD for TE-LSP 会话，通过严格显式路径约束 LSP 来回路径，且来回路径均配置 BFD for TE-LSP 类型会话，保证来回路径一致。

非规范配置的风险

风险描述

1. 配置动态 BFD for LSP 会话检测，去程路径 1 为 LSP 路径，回程路径 2 为 IP 路径。
2. 配置静态 BFD for LSP 会话（不包括 BFD for TE-LSP），回程路径 2 为 LSP 路径，且与 RouterA 到 RouterB 的 LSP 路径不共路。
3. 路径 1 和路径 2 都配置 BFD for TE-LSP 会话，RouterA 和 RouterB 的的 TE-LSP 没有配置严格的显式路径。

当满足上述任意一个条件时，BFD 会话去程和回程路径不一致，回程路径故障时，可能导致去程 LSP 路径误切换。

业务现象如下：

BFD 会话本意用来检测路径 1，但是当路径 2 故障时，由于 BFD 回程路径不通，会话 Down，触发路径 1 上的 LSP 误切换到故障路径 2 上，导致业务流量丢失。

风险的判断方法

1. 下面以动态 BFD 会话去程为 LSP 路径，回程为 IP 路由为例。其它情况的判断方法请根据实际组网情况而定，必须确保 BFD 会话报文的去程和回程路径一致。
2. 在 RouterA 查询 BFD 会话邻居信息。

   # 在用户视图下，执行 **display bfd session all verbose** 命令查看 RouterA 到 RouterB 的 BFD 邻居信息。加粗字体为 RouterA 到 RouterB 的 BFD 会话的邻居和下一跳。

```
<HUAWEI> display bfd session all verbose
-------------------------------------------------------------------------------
-
  State : Up                Name : dyn 16396
-------------------------------------------------------------------------------
-
  Local Discriminator    : 16396          Remote Discriminator   : 16392
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type         : TE_LSP
  Bind Session Type      : Dynamic
  Bind Peer IP Address   : 2.2.2.2
  NextHop Ip Address     : 10.1.1.2
  ......
```

3. 在 RouterB 查询 BFD 会话的邻居信息。

   # 在用户视图下，执行 **display bfd session all verbose** 命令查看 RouterB 到 RouterA 的 BFD 邻居信息。加粗字体为 RouterB 到 RouterA 的 BFD 会话的邻居。

```
<HUAWEI> display bfd session all verbose
-------------------------------------------------------------------------------
-
  (Multi Hop) State : Up                Name : dyn_16392
-------------------------------------------------------------------------------
-
  Local Discriminator    : 16392          Remote Discriminator   : 16396
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type         : Peer IP Address
```

```
 Bind Session Type     : Entire_Dynamic
 Bind Peer IP Address  : 1.1.1.1
 ......
```

4. 在 RouterB 查询到 RouterA 的路由信息。

   在用户视图下，执行 **display ip routing-table** *ip-address mask* **verbose** 命令查询 RouterB 到 RouterA 的路由信息。加粗字体为 RouterB 到 RouterA 的路由下一跳。BFD 会话从 RouterA 到 RouterB 的下一跳为 10.1.1.2，而从 RouterB 到 RouterA 的下一跳为 10.2.1.2，BFD 会话报文来回路径不一致。

```
<HUAWEI> display ip routing-table 1.1.1.1 32 verbose
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black
hole route
------------------------------------------------------------------------------
Routing Table :  public
Summary Count : 1
Destination: 1.1.1.1/32
    Protocol: ISIS-L2        Process ID: 1
  Preference: 15                 Cost: 10
     NextHop: 10.2.1.2        Neighbour: 0.0.0.0
       State: Inactive Adv         Age: 1d04h15m09s
         Tag: 0               Priority: high
       Label: NULL             QoSInfo: 0x0
  IndirectID: 0xE600087A
RelayNextHop: 0.0.0.0          Interface: GigabitEthernet0/5/5
    TunnelID: 0x0                Flags:
```

风险的恢复方案

请按照配置规范进行配置。

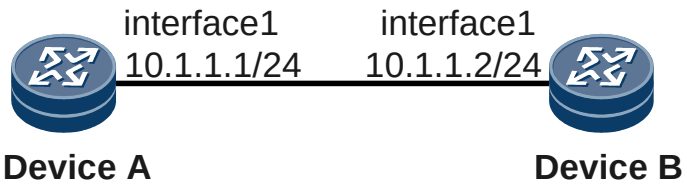
1.3.1.2 静态 BFD 两端设备配置对称实现流量不中断

配置静态 BFD 会话检测，两端设备配置不对称导致业务切换行为不一致，流量中断。

应用场景

如图 1-2 所示，配置静态 BFD 会话检测 RouterA 和 RouterB 之间的链路。

图1-2 静态 BFD 两端设备配置不对称导致流量中断组网图



配置规范

在对称的静态 BFD 会话上配置对称的本地行为参数：

- 两端设备分别在 BFD 会话视图下执行 **wtr** *wtr-value* 命令配置相同的等待恢复时间。
- 两端设备分别在 BFD 会话视图下执行 **process-interface-status** 命令配置当前 BFD 会话与其绑定的接口进行状态联动。
- 两端设备分别在 BFD 会话视图下执行 **process-pst** 命令配置允许 BFD 会话修改端口状态表 PST。

非规范配置的风险

风险描述

当不满足配置规范的任意一个条件时，两端业务切换行为不一致，流量中断。

风险的判断方法

1. 查询静态 BFD 会话的 **wtr** *wtr-value* 信息。

   # 在 RouterA 的 BFD 会话视图下，执行 **display this** 命令进行查询。**discriminator local** 必须要求与 RouterB 上远端描述符匹配。RouterA 配置了 wtr 且时间为 2 分钟。

   ```
   <HUAWEI> system-view
   [HUAWEI] bfd session a
   [HUAWEI-bfd-session-a] display this
   #
   bfd a bind peer-ip 10.1.1.2
    discriminator local 1
    discriminator remote 2
    wtr 2
    commit
   #
   return
   ```

   # 在 RouterB 的 BFD 会话视图下，执行 **display this** 命令进行查询。**discriminator local** 必须与 RouterA 上远端描述符匹配。RouterB 没有配置 wtr，与 RouterA 配置不一致。

   ```
   <HUAWEI> system-view
   [HUAWEI] bfd session a
   [HUAWEI-bfd-session-a] display this
   #
   bfd a bind peer-ip 10.1.1.1
    discriminator local 2
    discriminator remote 1
    commit
   #
   return
   ```

2. 查询静态组播 BFD 会话的两端设备 **process-interface-status** 信息。

   # 在 RouterA 的 BFD 会话视图下，执行 **display this** 命令进行查询。**discriminator local** 必须与 RouterB 上远端描述符相匹配。RouterA 配置了端口联动。

   ```
   <HUAWEI> system-view
   [HUAWEI] bfd session a
   [HUAWEI-bfd-session-a] display this
   #
   bfd a bind peer-ip default-ip interface GigabitEthernet1/0/0
   ```

```
 discriminator local 11
 discriminator remote 12
 process-interface-status
 commit
#
return
```

在 RouterB 的 BFD 会话视图下，执行 **display this** 命令进行查询。**discriminator local** 必须与 RouterA 上远端描述符相匹配。RouterB 没有配置端口联动，与 RouterA 配置不一致。

```
<HUAWEI> system-view
[HUAWEI] bfd session a
[HUAWEI-bfd-session-a] display this
#
bfd a bind peer-ip default-ip interface GigabitEthernet1/0/0
 discriminator local 12
 discriminator remote 11
 commit
#
return
```

3. 查询的静态 BFD 会话的两端 **process-pst** 信息。

   # 在 RouterA 的 BFD 会话视图下，执行 **display this** 命令进行查询。**discriminator local** 必须与 RouterB 上远端描述符相匹配。RouterA 配置了 pst 联动。

```
<HUAWEI> system-view
[HUAWEI] bfd session a
[HUAWEI-bfd-session-a] display this
#
bfd a bind peer-ip 10.1.1.2 interface GigabitEthernet1/0/0
 discriminator local 11
 discriminator remote 12
 process-pst
 commit
#
return
```

在 RouterB 的 BFD 会话视图下，执行 **display this** 命令进行查询。**discriminator local** 必须与 RouterA 上远端描述符相匹配。RouterB 没有配置 pst 联动，与 RouterA 配置不一致。

```
<HUAWEI> system-view
[HUAWEI] bfd session a
[HUAWEI-bfd-session-a] display this
#
bfd a bind peer-ip 10.1.1.1 interface GigabitEthernet1/0/0
 discriminator local 12
 discriminator remote 11
 commit
#
return
```

风险的恢复方案

请按照配置规范进行配置。

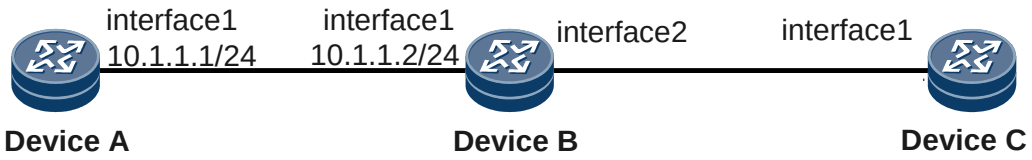
1.3.1.3 BFD 描述符配置规范

配置静态 BFD 会话的情况下，在路由相互可达的网络设备上很可能出现配置的 BFD 会话远端描述符冲突，导致 BFD 会话震荡。

应用场景

如图 1-3 所示，配置静态 BFD 会话检测网络上两个网络节点 RouterA 和 RouterB 间链路。

图1-3 BFD 描述符配置冲突导致 BFD 会话周期性震荡组网图



配置规范

在部署网络 BFD 会话检测时，描述符需要统一规划，避免冲突。

非规范配置的风险

风险描述

1. RouterB 配置静态 BFD 和 RouterA 建立会话，并在 BFD 视图下执行 **discriminator local** *discr-value* 命令配置本地描述符为 a；
2. RouterC 上配置一个静态 BFD 会话，并在 BFD 视图下执行 **discriminator remote** *discr-value* 命令配置其远端描述符也为 a。

当满足上述条件时，BFD 会话周期性震荡，引起绑定 BFD 会话的业务震荡。

业务现象如下：

BFD 会话会周期性震荡，且查看两端设备中 BFD 会话 Down 的原因都是因为邻居 Down。

风险的判断方法

1. 查询已经配置的静态 BFD 会话的两端配置信息。

   # 在 RouterB 的 BFD 会话视图下，执行 **display this** 命令。**discriminator local** 必须与 RouterA 上远端描述符相匹配。

```
<HUAWEI> system-view
[HUAWEI] bfd session a
[HUAWEI-bfd-session-a] display this
#
bfd a bind peer-ip 10.1.1.2
 discriminator local 1
 discriminator remote 2
 commit
```

```
#
return
```

在 RouterA 的 BFD 会话视图下，执行 **display this** 命令。**discriminator local** 必须与 RouterB 上远端描述符相匹配。

```
<HUAWEI> system-view
[HUAWEI] bfd session a
[HUAWEI-bfd-session-a] display this
#
bfd a bind peer-ip 10.1.1.1
 discriminator local 2
 discriminator remote 1
 commit
#
return
```

2. 查询 BFD 会话的详细信息。

   # 在用户视图下，执行 **display bfd session all verbose** 命令查询 RouterA 的会话详细信息。BFD 会话邻居状态为 Down。

```
<HUAWEI> display bfd session all verbose
-------------------------------------------------------------------------------
-
  (Multi Hop) State : Down               Name : a
-------------------------------------------------------------------------------
-
  Local Discriminator    : 1             Remote Discriminator   : 2
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type          : Peer IP Address

  Active Multi           : -
  Last Local Diagnostic  : Neighbor Signaled Session Down
  ……
```

   # 在用户视图下，执行 **display bfd session all verbose** 命令查询 RouterB 的会话详细信息。BFD 会话邻居状态为 Down。

```
<HUAWEI> display bfd session all verbose
-------------------------------------------------------------------------------
-
  (Multi Hop) State : Down               Name : a
-------------------------------------------------------------------------------
-
  Local Discriminator    : 2             Remote Discriminator   : 1
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type          : Peer IP Address

  Active Multi           : -
  Last Local Diagnostic  : Neighbor Signaled Session Down
……
```

3. 查询网络中其他设备上的 BFD 会话配置。

   # 网络中与 RouterA 和 RouterB 有路由连接的其他设备（RouterC）上，在用户视图下执行 **display current-configuration configuration bfd-session** 命令查询网络中的其他设备上是否存在本地描述符冲突的 BFD 会话。**discriminator remote** 与 B 设备上远端描述符冲突。

```
<HUAWEI> display current-configuration configuration bfd-session
```

```
#
bfd a bind peer-ip 20.1.1.1
 discriminator local 5
 discriminator remote 1
 commit
#
return
```

风险的恢复方案

修改 RouterC 上的 BFD 会话的远端描述符为其他值。

1.3.1.4 静态 BFD for CR-LSP 隧道往返路径需要保持一致才能实现业务正常切换

静态 BFD 检测 CR-LSP 时，如果往返路径不一致，可能导致 BFD 检测 Down，触发业务误切换，可能导致业务中断。

应用场景

配置静态 BFD for CR-LSP。

配置规范

配置静态 BFD for CR-LSP 时，配置往返 TE 隧道的显示路径一致。

非规范配置的风险

风险描述

当静态 BFD 检测的 CR-LSP 往返路径不一致时，BFD 检测可能 Down，检测结果不能反映实际的 CR-LSP 的连通性。

业务现象如下：

BFD 检测 Down，触发业务误切换，可能导致业务中断。

风险的判断方法

1. 在用户视图下，执行 **display current-configuration bfd-session** 命令，查看 BFD 配置。

   由显示信息可以看出，Tunnel0/0/27 的主 LSP 本地标识符为 local1，远端标识符为 remote2；Tunnel0/0/27 的备 LSP 本地标识符为 local3，远端标识符为 remote4。

```
<HUAWEI> display current-configuration configuration bfd-session
#
bfd tunnel1 bind mpls-te interface Tunnel0/0/27 te-lsp
 discriminator local 1
 discriminator remote 2
 process-pst
 commit
#
bfd tunnel1-back bind mpls-te interface Tunnel0/0/27 te-lsp backup
 discriminator local 3
 discriminator remote 4
```

```
 process-pst
 commit
#
return
```

2. 在用户视图下，执行 **display current-configuration interface Tunnel** 命令，查看 TE 隧道配置。

   由显示信息可以看出，隧道目的地址为 **192.168.1.1**，主 LSP 的显示路径为 **main-to-devicea**，备 LSP 的显示路径为 **backup-to-devicea**。

```
<HUAWEI> display current-configuration interface Tunnel 0/0/27
#
interface Tunnel0/0/27
 description huawei
 mtu 1600
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 192.168.1.1
 mpls te tunnel-id 27
 mpls te record-route label
 mpls te path explicit-path main-to-devicea
 mpls te path explicit-path backup-to-devicea secondary
 mpls te backup hot-standby mode revertive wtr 60
 mpls te backup ordinary best-effort
 mpls te igp shortcut
 mpls te igp metric absolute 10
 mpls te commit
 isis enable 100
 statistic enable #
return
```

3. 在用户视图下，执行 **display mpls te tunnel-interface** *tunnel-name* 命令，查看隧道的三元组信息。

   由显示信息可以看出，Tunnel 0/0/27 的 Session ID 为 27，Ingress LSR ID 为 192.168.1.2，主 LSP ID 为 3，备 LSP ID 为 32772。

```
<HUAWEI> display mpls te tunnel-interface Tunnel 0/0/27
------------------------------------------------------------------
                Tunnel0/0/27
------------------------------------------------------------------
 Tunnel State Desc   :  UP
 Active LSP          :  Primary LSP
 Session ID          :  27
 Ingress LSR ID      :  192.168.1.2    Egress LSR ID:  192.168.1.1
 Admin State         :  UP             Oper State    :  UP
 Primary LSP State     : UP
 Main LSP State      : READY             LSP ID  : 3
 Hot-Standby LSP State  : UP
 Main LSP State      : READY             LSP ID  : 32772
```

4. 查询隧道实际经过的路径。查询到的路径用于后面和对端设备查询的路径进行比较。

   执行 **display current-configuration interface tunnel 0/0/27** 命令，查看是否配置了 **mpls te record-route**（或 **mpls te record-route label**），如果配置了，执行 **display mpls te tunnel path lsp-id** *ingress-lsr-id session-id local-lsp-id* 命令，查询隧道实际经过的路径。

否则，执行 **tracert lsp te tunnel***interface-number* 命令查询。

```
<HUAWEI> display mpls te tunnel path lsp-id 192.168.1.2 27 3
 Tunnel Interface Name : Tunnel0/0/27
 Lsp ID : 192.168.1.2 :27 :3
 Hop Information
  Hop 0   192.168.1.2
  Hop 1   100.0.2.7
  Hop 2   100.0.2.8
  Hop 3   192.168.1.1
<HUAWEI> tracert lsp te Tunnel 0/0/27
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel0/0/1, press CTRL_C
to break.
  TTL   Replier          Time    Type      Downstream
  0                           Ingress   192.168.1.2/[3 ]
  1    192.168.1.1      32 ms   Egress
```

5. 在用户视图下，使用命令行 **display explicit-path** *path-name*，查看隧道的显式路径配置。
   - 如果设备上没有配置显式路径或隧道配置中没有使用显式路径，建议配置严格显式路径并在隧道下配置使用。
   - 如果配置的显式路径与隧道实际经过的路径相比，缺少某些跳，建议修改显式路径的配置，将其补充完整。
   - 如果显式路径配置为松散模式，建议修改为严格模式，并将路径补充完整。

```
<HUAWEI> display explicit-path main-to-devicea
1     62.231.253.26      Strict     Include
2     62.231.253.166     Strict     Include
3     62.231.253.77      Strict     Include
4     62.231.253.133     Strict     Include
5     62.231.253.53      Strict     Include
<HUAWEI> display explicit-path backup-to-devicea
1     62.231.253.162     Strict     Include
2     62.231.253.73      Strict     Include
3     62.231.253.129     Strict     Include
```

6. 根据 TE 隧道目的地址（192.168.1.1），找到 TE 隧道尾节点的设备。在 TE 隧道尾节点设备上，根据头节点静态 BFD for CR-LSP 的标示符，找到静态 BFD for CR-LSP 信息。

   用户视图下执行 **display bfd configuration discriminator** *local-discr-value* **verbose** 命令，其中参数 *local-discr-value* 指定头节点静态 BFD for CR-LSP 会话中 Remote Discriminator 的值（2），找到对应 TE 隧道(Tunnel0/0/28)。

```
<HUAWEI> display bfd configuration discriminator 2 verbose
-------------------------------------------------------------------------------
-
  BFD Session Configuration Name : to 3
-------------------------------------------------------------------------------
-
  Local Discriminator    : 2            Remote Discriminator   : 1
  BFD Bind Type         : TE LSP
  Bind Session Type     : Static
  Bind Interface        : Tunnel0/0/28    TE LSP Type          : Primary
  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       : LSPM | L2VPN
 Session Description    : -
--------------------------------------------------------------------------------
-
```

7. 在 TE 隧道尾节点设备上，针对上一步获取到的隧道名称（如例子中的 Tunnel0/0/28），根据上述步骤，找出该隧道实际经过的路径，并与查到 Tunnel0/0/28 路径进行比较。

   如果一致（方向相反），则不存在问题。如果不一致，则说明往返路径不一致。

风险的恢复方案

修改显式路径，将隧道实际经过的路径调整为与 TE 隧道头节点上对应隧道的路径一致。

1.3.1.5 内层链路的 BFD 检测间隔应小于外层链路的检测间隔

多层保护场景下，如果内层链路的 BFD 检测间隔大于外层链路的检测间隔，当外层链路感知故障时，内层保护尚未切换。

应用场景

配置了多层保护的场景。例如，配置 BFD for RSVP、BFD for CR-LSP 或 BFD for TE 的场景。

配置规范

在网络部署 BFD 会话检测时，存在多层保护场景情况下，对 BFD 检测间隔的配置遵循内层小外层大的原则。

不同场景下，BFD 检测间隔的配置不同。例如：

- BFD for RSVP 场景：请参见（可选）调整 BFD 检测参数。
- 静态 BFD for CR-LSP 场景：请参见配置入节点 BFD 参数和配置出节点 BFD 参数。
- 动态 BFD for CR-LSP 场景：请参见（可选）调整入节点的 BFD 检测参数。
- BFD for TE 场景：请参见配置入节点 BFD 参数和配置出节点 BFD 参数。

非规范配置的风险

风险描述

多层保护场景下，内层链路的 BFD 检测间隔大于外层链路的检测间隔，当 Tunnel 出现故障时，检测外层 Tunnel 的 BFD 会话由于检测间隔小，则先感知到链路故障，通知 Tunnel 业务做保护切换，因此浪费了内层的检测 LSP 的保护切换。

内层保护机制浪费、整体切换方案退化为只剩外层冗余保护，切换性能也随之退化。

业务现象如下：

外层链路已经感知故障，而内层保护尚未切换，如果外层链路配置了保护路径，则可能出现保护切换退化为外层保护，因此浪费了内层的保护切换策略。

风险的判断方法

如下判断方法适用内层为动态 BFD for CR-LSP，外层为静态 BFD for TE，且 BFD for CR-LSP 和 BFD for TE 绑定同一个 Tunnel 接口的场景。其它场景下，请根据实际情况来进行判断。

在用户视图下，执行 **display bfd session all verbose** 命令查看 BFD 的检测间隔。

从显示信息可以看出，检测内层链路的 BFD Bind Type 为 TE_LSP 的会话的检测间隔 Detect Interval (ms)为 2664，而检测外层链路的 BFD Bind Type 为 TE_TUNNEL 的会话的检测间隔 Detect Interval (ms)为 300，即内层链路的 BFD 检测间隔大于外层链路的检测间隔。

```
<HUAWEI> display bfd session all verbose
--------------------------------------------------------------------------------
 State : Up                Name : dyn 16393
--------------------------------------------------------------------------------
 Local Discriminator    : 16393          Remote Discriminator   : 16402
 Session Detect Mode    : Asynchronous Mode Without Echo Function
 BFD Bind Type          : TE_LSP
 Bind Session Type      : Dynamic
 Bind Peer IP Address   : 2.2.2.2
 NextHop Ip Address     : 10.1.1.2
 Bind Interface         : Tunnel1        TE LSP Type          : Primary
 Tunnel ID              : 33
 FSM Board Id           : 9             TOS-EXP              : 6
 Min Tx Interval (ms)   : 999            Min Rx Interval (ms)   : 888
 Actual Tx Interval (ms): 999            Actual Rx Interval (ms): 888
 Local Detect Multi     : 48             Detect Interval (ms)   : 2664
 Echo Passive           : Disable        Acl Number           : -
 Destination Port       : 3784           TTL                  : 1
 Proc Interface Status  : Disable          Process PST          : Enable
 WTR Interval (ms)      : -              Config PST           : Enable
 Active Multi           : 3
 Last Local Diagnostic  : No Diagnostic
 Bind Application       : TE
 Session TX TmrID       : -              Session Detect TmrID   : -
 Session Init TmrID     : -              Session WTR TmrID      : -
 Session Echo Tx TmrID  : -
 Session Description    : -
--------------------------------------------------------------------------------


--------------------------------------------------------------------------------
 State : Up                Name : te
--------------------------------------------------------------------------------
 Local Discriminator    : 111            Remote Discriminator   : 111
 Session Detect Mode    : Asynchronous Mode Without Echo Function
 BFD Bind Type          : TE_TUNNEL
 Bind Session Type      : Static
 Bind Peer IP Address   : 2.2.2.2
 NextHop Ip Address     : -.-.-.-
 Bind Interface         : Tunnel1
 Tunnel ID              : 33
 FSM Board Id           : 9             TOS-EXP              : 1
 Min Tx Interval (ms)   : 100            Min Rx Interval (ms)   : 100
 Actual Tx Interval (ms): 100            Actual Rx Interval (ms): 100
```

```
 Local Detect Multi    : 3             Detect Interval (ms)   : 300
 Echo Passive         : Disable        Acl Number           : -
 Destination Port      : 3784          TTL                 : 1
 Proc Interface Status  : Disable        Process PST          : Disable
 WTR Interval (ms)     : -             Config PST           : Disable
 Active Multi         : 3
 Last Local Diagnostic  : No Diagnostic
 Bind Application      : No Application Bind
 Session TX TmrID      : -             Session Detect TmrID   : -
 Session Init TmrID    : -             Session WTR TmrID     : -
 Session Echo Tx TmrID  : -
 Session Description    : -
------------------------------------------------------------------------------

Total UP/DOWN Session Number : 2/0
```

风险的恢复方案

调整内层保护链路的 BFD 会话检测间隔小于外层链路的 BFD 会话的检测间隔。

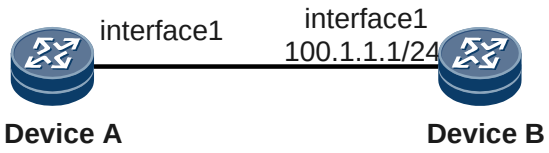
1.3.1.6 双向 LSP 场景下两端设备的 BFD 配置需对称

双向 LSP 场景下，BFD 两端配置不对称，导致 LDP LSP 状态 Down，LDP LSP 承载的业务中断。

应用场景

如图 1-4 所示，从 RouterA 到 RouterB 存在 LSP，且从 RouterB 到 RouterA 也存在 LSP。RouterA 配置 BFD For Peer IP，RouterB 配置 BFD For TE-LSP，同时 RouterA 存在与 Peer IP 地址相同的 LDP LSP，当 TE LSP 故障后，LDP LSP 承载的业务中断。

图1-4 BFD 两端配置不对称导致 LDP LSP 业务中断组网图



配置规范

两端设备 BFD 检测类型配置保持一致，均为 BFD For TE-LSP。

非规范配置的风险

风险描述

RouterB 的 TE LSP 故障后，LDP LSP 承载的业务中断。

业务现象如下：

TE LSP 故障后，LDP LSP 的 BFD 状态 Down 导致业务中断。

风险的判断方法

1. 查看两端的 BFD 配置是否对称。

   如下显示信息说明两端 BFD 配置不对称。RouterA 配置的是 BFD For Peer IP，RouterB 配置的是 BFD For TE-LSP。

   # 在 RouterA 任意视图下执行 **display current-configuration configuration bfd** 命令。

```
<HUAWEI> display current-configuration configuration bfd
#
bfd ieclsptowac bind peer-ip 100.1.1.1
 discriminator local 101
 discriminator remote 302
 min-tx-interval 50
 min-rx-interval 50
 commit
#
```

   # 在 RouterB 任意视图下执行 **display current-configuration configuration bfd** 命令。

```
<HUAWEI> display current-configuration configuration bfd
#
bfd ieclsptowac bind mpls-te interface Tunnel0/0/1 te-lsp
discriminator local 302
 discriminator remote 101
 min-tx-interval 50
 min-rx-interval 50
 commit
#
```

2. 查询 RouterA 检测 Peer IP 的 BFD 会话的状态。

   # 在 RouterA 的任意图下执行 **display bfd session all** 命令，发现 BFD 会话状态为 Down。

```
<HUAWEI> display bfd session all
--------------------------------------------------------------------------------
Local Remote    PeerIpAddr     State    Type       InterfaceName
--------------------------------------------------------------------------------
5     6         100.1.1.1      Down     S IP PEER        -
--------------------------------------------------------------------------------
Total UP/DOWN Session Number : 0/1
```

   # 在 RouterB 的任意视图下执行 **display mpls lsp include** *ip-address mask-len* **verbose** 命令，发现 LDP LSP 的 BFD 状态为 Down。

```
<HUAWEI> display mpls lsp include 100.1.1.1 32 verbose
------------------------------------------------------------------------------
              LSP Information: LDP LSP
------------------------------------------------------------------------------
  No               :  1
  VrfIndex         :
  Fec              :  100.1.1.1/32
  Nexthop          :  100.2.1.1
  In-Label         :  NULL
  Out-Label        :  153468
  In-Interface     :  ----------
  Out-Interface    :  GigabitEthernet1/0/0
```

```
 LspIndex          :  191839
 Token             :  0x2001476
 FrrToken          :  0x0
 LsrType           :  Ingress
 Outgoing token    :  0x0
 Label Operation   :  PUSH
 Mpls-Mtu          :  9000
 TimeStamp         :  144908sec
 Bfd-State         :  Down
BGPKey            :  ------
```

风险的恢复方案

由于 LDP LSP 已经被 BFD 置 Down，需要在配置 BFD For TE-LSP 的一端配置 BFD For Peer IP 先让 BFD 协商 UP，再删除 BFD 配置，LDP LSP 的转发状态即可恢复。

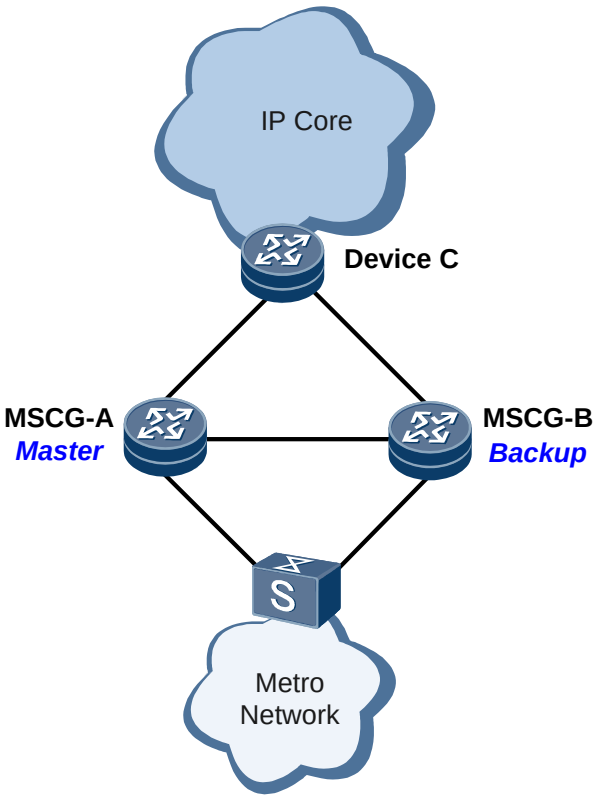
1.3.2 多机备份的配置规范

1.3.2.1 双机热备场景下部署共享地址池时需要配置保护隧道

双机热备场景下部署共享地址池时需要配置保护隧道，如果不配置，可能导致当主设备的用户侧链路故障时，下行流量无法入保护隧道到达用户，流量流失。

应用场景

双机热备场景下部署共享地址池，组网如下图所示。



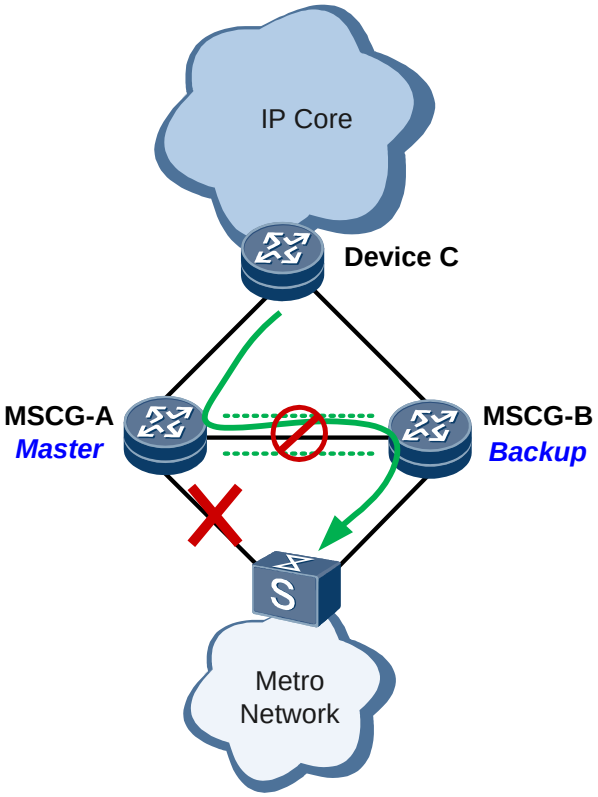
配置规范

详情请参考：配置共享地址池方式下的用户信息备份。

非规范配置的风险

风险描述

按照现在双机热备份的部署，对于共享地址池的部署方式，当主设备的用户侧链路发生故障时，到达主设备的下行流量通过入保护隧道形式到达备用设备最后到达用户，如果未设置保护隧道，则下行流量无法顺利到达用户，导致下行流量丢失故障。



风险的判断方法

- 通过 **display remote-backup-service** *service-name* 命令，查看所有的 RBS 信息。
  - 判断 RBS 是否绑定了共享地址池：

    查看回显中的“ip pool”字段下是否有地址池名称。

    如有，说明 RBS 下绑定了共享地址池，继续判断。

    如果没有，说明此双机热备场景不是共享地址池，不涉及本配置规范。
  - 判断 RBS 是否配置了保护隧道：

    查看回显中是否有保护隧道类型，查看是否有出接口，回显中的“Protect-type”和“Out-interface”字段。

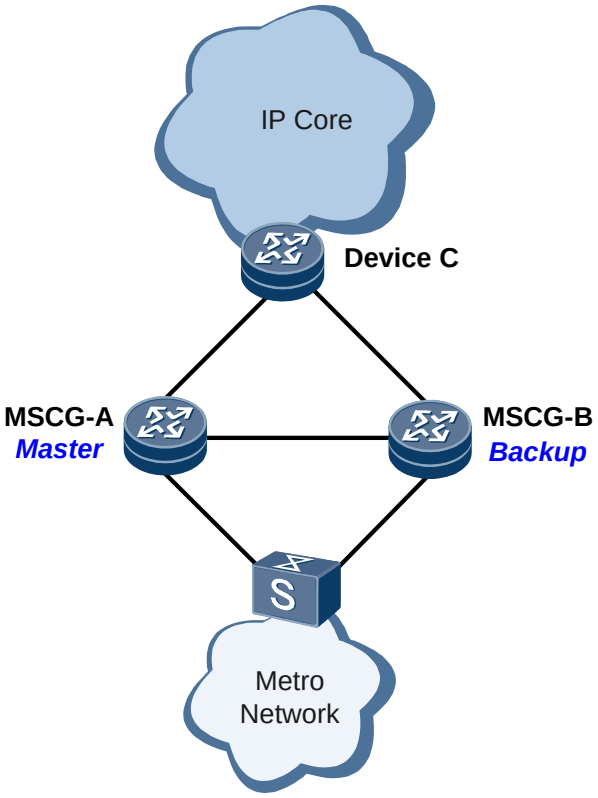
风险的恢复方案

同配置规范。

1.3.2.2 双机热备场景下部署共享地址池时网络侧接口需要去使能 URPF

应用场景

双机热备场景下部署共享地址池，组网如下图所示。



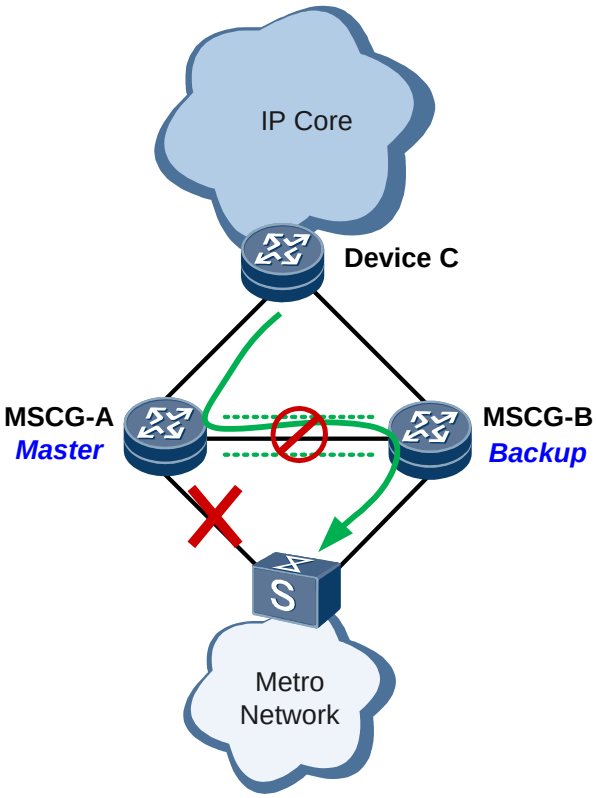
配置规范

网络侧接口需要去使能 URPF，即配置 **undo ip urpf**。

非规范配置的风险

风险描述

在双机热备设备上配置共享地址池时，当主设备的用户侧链路发生故障时，流量会经过保护隧道迂回到用户，如果网络侧接口下配置 URPF，会概率导致下行流量无法入保护隧道到达用户，流量流失。



风险的判断方法

- 通过 **display remote-backup-service** *service-name* 命令，查看所有的 RBS 信息。
  - 判断 RBS 是否绑定了共享地址池：
    查看回显中的“ip pool”字段下是否有地址池名称。
    如有，说明 RBS 下绑定了共享地址池，继续判断。
    如果没有，说明此双机热备场景不是共享地址池，不涉及本配置规范。
  - 判断 RBS 是否配置了保护隧道：
    查看回显中是否有保护隧道类型，查看是否有出接口，回显中的“Protect-type”和“Out-interface”字段。

```
[HUAWEI] display remote-backup-service rbs
------------------------------------------------------------
 Service-Index    : 2
 Service-Name     : rbs
 TCP-State        : Initial
 Peer-ip          : 28.1.1.1
 Source-ip        : 6.6.6.3
 TCP-Port         : 6002
 Track-BFD        : --
 Uplink state     : 2 (1:DOWN 2:UP)
 Domain-map-list  : --
------------------------------------------------------------

 ip pool:
       zw metric 20
 ipv6 pool:
 Failure ratio    : 100%
```

```
 Failure duration : 0 min
------------------------------------------------------------
 Rbs-ID        : 2
 Protect-type   : ip-redirect
 Next-hop      : 115.1.1.2
 Vlanid        : 0
 Peer-ip       : 115.1.1.2
 Vrfid         : 0
 Tunnel-state   : UP
 Tunnel-OperFlag: NORMAL
 Spec-interface : GigabitEthernet1/0/2
 Total users    : 0
 Path 1:
    Tunnel-index   : 0x0
    Tunnel-index-v6: 0x0
    Out-interface  : GigabitEthernet1/0/2
    Vc-lable      : 4294967295
    Vc-lable-v6    : 4294967295
    User-number    : 0
    Public-Lsp-Load: FALSE

------------------------------------------------------------
 Rbs-ID        : 2
 Protect-type   : public(LSP)
 Peer-ip       : 17.17.17.17
 Vrfid         : 4091
 Tunnel-state   : UP
 Tunnel-OperFlag: NORMAL
 Spec-interface : Null
 Total users    : 0
 Path 1:
    Tunnel-index   : 0x400000f
    Tunnel-index-v6: 0x0
    Out-interface  : GigabitEthernet2/0/1
    Vc-lable      : 4294967295
    Vc-lable-v6    : 4294967295
    User-number    : 0
    Public-Lsp-Load: TRUE
```

- 在网络侧接口视图下，执行 **display this**，查看是否配置了 URPF。

```
[HUAWEI -GigabitEthernet2/0/1] display this
#
interface GigabitEthernet2/0/1
 description ith
 undo shutdown
 ipv6 enable
 ip address 186.0.0.17 255.255.255.0
 ipv6 address 13:16::2/64
 mpls
 mpls ldp
 undo dcn
 ip urpf strict
ipv6 urpf strict
#
```

风险的恢复方案

同配置规范。

1.3.3 VRRP 的配置规范

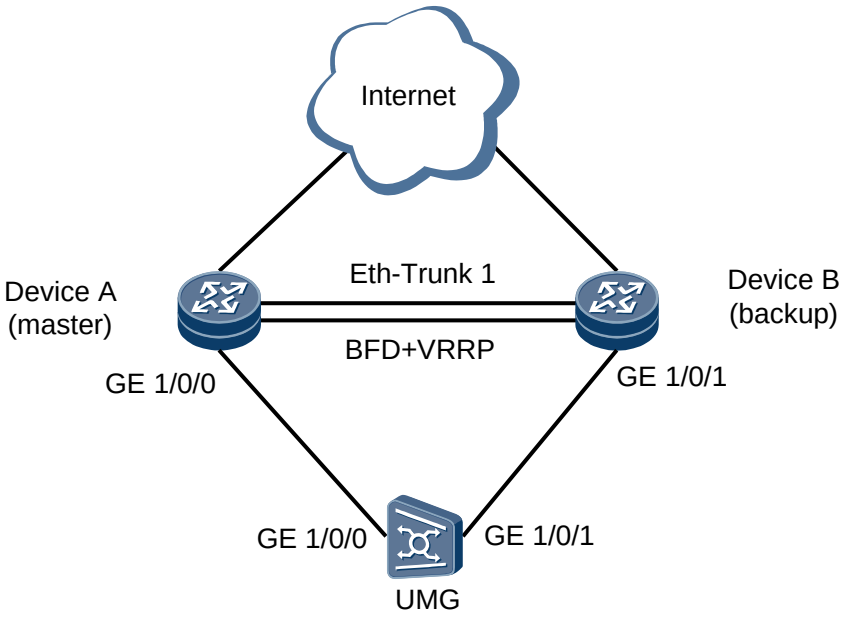
1.3.3.1 VRRP 中间链路需要配置 Eth-Trunk 保护的配置规范

部署 VRRP 时，如果接入设备的上行网关的端口采用了端口间的备份，即无故障的情况下只有一个端口转发流量，在转发流量的端口发生故障之后备份端口开始转发流量。此时，如果 VRRP 的中间心跳丢失则会导致 VRRP 出现双主的情况，此时很有可能导致接入设备上的流量中断。

应用场景

如图 1-5 所示，UMG 上行网关的端口 GE1/0/0 和 GE1/0/1 采用的端口间的备份，只有一个端口转发功能被开启。在 DeviceA 和 DeviceB 上部署 VRRP 功能，同时在 VRRP 中间心跳链路配置 Eth-Trunk 保护。

图1-5 VRRP 中间链路配置 Eth-Trunk 保护组网图



配置规范

在 DeviceA 和 DeviceB 上配置 VRRP 备份组。在 DeviceA 上配置较高优先级，作为 Master 设备承担流量；在 DeviceB 上配置较低优先级，作为备用路由器，实现冗余备份。

在 DeviceA 和 DeviceB 上均需配置 Eth-Trunk 接口，并将以太网物理接口加入 Eth-Trunk 接口，同时添加跨板成员口，确保一个单板故障之后 Eth-Trunk 中仍有状态是 Up 的链路。

非规范配置的风险

风险描述

当 Eth-Trunk 的成员口所在的心跳链路故障之后，同时满足下列条件时，UMG 的业务大概率中断：

- UMG 的上行网关的端口只支持端口间的备份，即一般只能有一个端口 Up；
- DeviceA 和 DeviceB 的 VRRP 备份组间，心跳链路所在的端口未使用跨板 Trunk 方式。

风险的判断方法

说明
需要在 DeviceA 和 DeviceB 两台设备上都要执行此命令检查是否存在跨板成员口。

1. 查看对应 Eth-Trunk 的成员口是否是跨板成员口。

```
<HUAWEI> display interface eth-trunk 1
Eth-Trunk1 current state : UP
Line protocol current state : UP
Link quality grade : GOOD
Description:HUAWEI, Eth-Trunk1 Interface
Switch Port, TPID : 8100(Hex), Hash arithmetic : According to flow,Maximal BW:
2G, Current BW: 1G, The Maximum Transmit Unit is 1500
IP Sending Frames' Format is PKTFMT ETHNT 2, Hardware address is 0018-82d9-e71b
Physical is ETH TRUNK
Current system time: 2017-04-11 12:15:41
   Last 300 seconds input rate 0 bits/sec, 0 packets/sec
   Last 300 seconds output rate 0 bits/sec, 0 packets/sec
   Realtime 2 seconds input rate 0 bits/sec, 0 packets/sec
   Realtime 2 seconds output rate 0 bits/sec, 0 packets/sec
   Input: 3 packets,939 bytes
         0 unicast,0 broadcast,3 multicast
         0 errors,0 drops
   Output:3 packets,917 bytes
         0 unicast,0 broadcast,3 multicast
         0 errors,0 drops
   Input bandwidth utilization  :    0%
   Output bandwidth utilization :    0%
-------------------------------------------------------
PortName                  Status     Weight
-------------------------------------------------------
GigabitEthernet1/1/8        DOWN       1
GigabitEthernet3/1/0        UP         1
-------------------------------------------------------
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 1
```

2. 如果确定 Eth-Trunk 存在多个成员口并且成员口来自不同单板，比如 GigabitEthernet1/1/8 和 GigabitEthernet3/1/0，前者是 1 号单板端口，后者是 3 号单板端口，则此时不存在该风险；否则如果成员口都来自同一个单板，则存在风险。

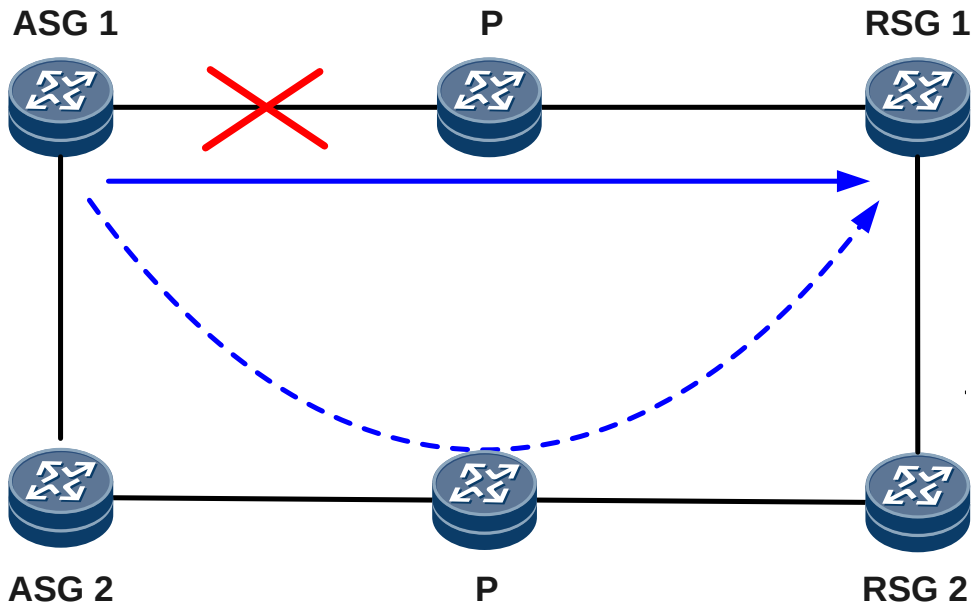
风险的恢复方案

在 DeviceA 和 DeviceB 上均需配置 Eth-Trunk 接口，并将以太网物理接口加入 Eth-Trunk 接口，同时添加跨板成员口，确保一个单板故障之后 Eth-Trunk 中仍有状态是 Up 的链路。

1.3.4 TE Tunnel 没有配置误码倒换导致业务受损

应用场景

如下图所示，在 IPRAN 场景中，ASG 和 RSG 之间部署 TE hot-standby。



配置规范

在 ASG 的 Tunnel 口上，通过命令行 **mpls te bit-error-detection** 配置 RSVP-TE 隧道的误码倒换功能。

非规范配置的风险

风险描述

当未配置误码倒换功能时，由于 ASG 和 RSG 之间的传输设备存在误码，会导致 ASG 下挂的基站产生中断。

风险的判断方法

查看 ASG 上的 Tunnel 配置，看是否已经配置了误码倒换。

风险的恢复方案

同配置规范。

1.4 接口管理

1.4.1 接口管理的配置规范

1.4.1.1 物理接口需要配置接口延迟发出信号

应用场景

1. 当设备双归接入其他厂商的设备时，设备无法控制其他厂商设备的接口流量切换。
2. 当设备与其他厂商设备直连时，设备被下电重启但配置恢复没有完成。

配置规范

需要执行命令 **port-tx-enabling-delay** *port-tx-delay-time*，配置接口延迟发出信号功能，接口初始化后不立即发送信号，而是到达用户配置的延迟时间后才开始发出信号，可有效避免因链路不能同步切换或设备未完成配置恢复导致的数据丢失。配置方法详见：配置接口延迟发出信号。

说明
配置接口延迟发出信号的延迟时间时需要综合考虑该设备上配置的其他业务。

非规范配置的影响

风险描述

当设备双归接入其他厂商的设备时，设备无法控制其他厂商设备的接口流量切换。这种情况下，设备与其他厂商设备不能保证同步完成链路切换，若接口初始化后立即发送信号，可能会导致部分数据丢失。

当设备与其他厂商设备直连时，设备被下电重启但配置恢复没有完成，若接口初始化后立即发送信号，可能会导致部分数据丢失。

风险的判断方法

在用户视图下，执行命令 **display port-tx-enabling-delay**，查看接口延迟发光的配置参数以及当前延时状态信息。以 GE 接口为例，查看 **port-tx-enabling delay time** 后的参数是否为“0”：

```
<HUAWEI> display port-tx-enabling-delay interface gigabitethernet 1/0/0
GigabitEthernet 1/0/0 setted port-tx-enabling delay time is: 100 ms
GigabitEthernet 1/0/0 remanent time of enabling port-tx is: 20 ms
```

风险的恢复方案

同配置规范。

1.4.1.2 物理接口需要配置接口延迟 Down 或延迟告警功能

应用场景

设备和波分、传输设备物理接口对接场景。

配置规范

- **Ethernet/GE/10G LAN/40GE/100GE**

  执行命令 **carrier down-hold-time** *interval*，设置接口状态转为 Down 后，系统的响应抑制时间。详见：配置接口 Up/Down 响应抑制时间。

- **其他接口**

  执行命令 **transmission-alarm holdoff-timer** *holdoff-time*，使能设备管理模块过滤接口状态变为 Down 的告警信息的功能，并设置过滤时间间隔。详见：设置传输告警的过滤时间间隔。

非规范配置的影响

风险描述

波分、传输设备倒换导致设备接口状态频繁变化引起震荡，从而导致接口上承载的业务中断。

风险的判断方法

在用户视图下，执行命令 **display current-configuration** [**interface** [*interface-type* [*interface-number*]]]，查看接口的 Up/Down 响应抑制时间。以 GE 接口为例，查看 **carrier down-hold-time** 后的参数是否为“0”：

```
<HUAWEI> display current-configuration interface GigabitEthernet 1/0/0
interface GigabitEthernet1/0/0
carrier down-hold-time 100
carrier up-hold-time 10
```

在用户视图下，执行命令 **display transmission-alarm configuration** [*interface-type interface-number*]，查看指定接口的告警定制与抑制配置。以 GE 接口为例，查看 **Holdtime** 后的参数是否为“0”：

```
<HUAWEI> display transmission-alarm configuration gigabitethernet 1/2/0
 Interface: GigabitEthernet1/2/0
  Filter function: enabled (Holdtime is 55)
  Damping function: enabled
  Suppress value: 999
  Ceiling value: 6000
  Reuse value: 500
  OK half decay value: 500
  NG half decay value: 1000
```

风险的恢复方案

同配置规范。

1.5 局域网与城域网接入

1.5.1 MAC 的配置规范

1.5.1.1 二层设备上行流量少的场景下 MAC 老化时间需要配置大于或接近 ARP 老化时间

二层设备上行流量少的场景下 MAC 老化时间需要配置大于或接近 ARP 老化时间

应用场景

说明

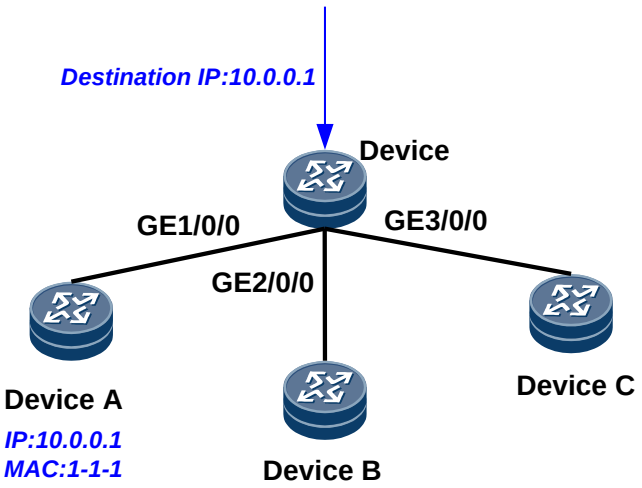
此场景仅 LPUF-50/LPUI-21-L/LPUF-50-L/LPUF-51/LPUI-51/LPUS-51/LPUF-101/LPUI-101/LPUS-101/LPUI-51-E/LPUF-51-E/LPUF-102/LPUF-102-E/LPUI-102-E/LPUF-120/LPUF-120-E/LPUI-120/LPUS-120/LPUF-240/LPUF-240-E/LPUI-240/LPUI-52-E/LPUI-120-E/LPUF-200-E 单板涉及。

如下图所示，Device 下有 3 个二层设备 Device A、Device B、Device C，由 GE1/0/0、GE2/0/0、GE3/0/0 分别连接，GE1/0/0、GE2/0/0、GE3/0/0 加入 VLANIF10。GE1/0/0 学到 Device A 的 ARP 和 MAC 地址。如果目的 IP 为 10.0.0.1 的下行流量到 Device，Device 将首先根据目的 IP 查路由表，然后根据得到的下一跳 IP 地址查 ARP 表项，得到 VLAN 和 MAC 地址，最后根据 VLAN+MAC 表查 MAC 表，根据 MAC 表的出接口，将流量转发到 GE1/0/0 给 Device A。

在这种场景下，Device 上的 ARP 表项、MAC 地址的更新方式有 2 种：

- 第一种是根据系统设置的老化时间，每隔一段时间自动检测
- 第二种是根据二层设备的上行流量读取更新

如果 Device A 往 Device 的上行流量很少，那 Device 上的 ARP 表项、MAC 地址的更新就只能通过 ARP 每隔一段时间自动检测。



配置规范

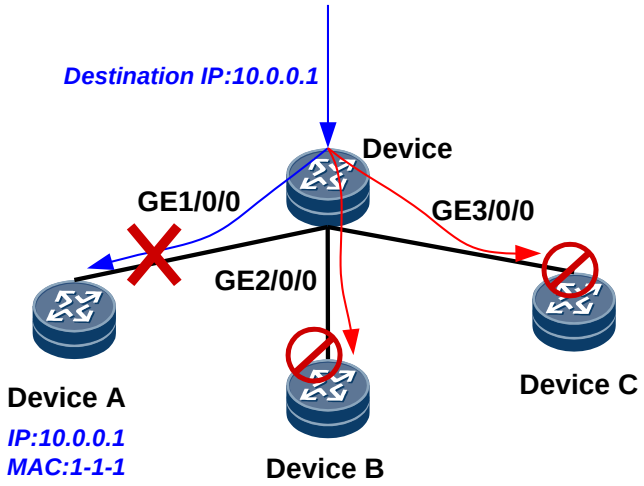
1. 查询当前的 ARP 老化时间。进入对应的接口视图，执行命令 **display this**，查看是否有“arp expire-time”的配置，如果没有，ARP 老化时间是默认值 1200 秒（20 分钟），如果有配置，以配置的值为准。

2. 设置 MAC 老化时间。进入系统视图，执行命令 **mac-address aging-time** *seconds*，设置 *seconds* 大于等于上面查询到的 ARP 老化时间。*seconds* 的默认值为 300 秒（5 分钟）。

非规范配置的风险

风险描述

由于 Device A 往 Device 的上行流量很少，那 Device 上的 ARP 表项、MAC 地址的更新就只能通过 ARP 每隔一段时间自动检测。这时，如果 Device 的 MAC 老化时间比 ARP 老化时间短，Device A 的 MAC 地址会被老化掉，但是 ARP 地址还在。此时 Device 收到发往 Device A 的流量时，转发时会查不到 MAC 表，从而在 VLAN 10 内广播，Device B 和 Device C 设备都会收到 发往 Device A 的流量，导致 Device B、Device C 设备的正常业务受到影响。



风险的判断方法

1. 查询当前的 ARP 老化时间。进入对应的接口视图，执行命令 **display this**，查看是否有“arp expire-time”的配置，如果没有，ARP 老化时间是默认值 1200 秒（20 分钟），如果有配置，以配置的值为准。

   例如，下述举例中，没有“arp expire-time”的配置，所以 ARP 老化时间是默认值 1200 秒（20 分钟）。

```
[HUAWEI-GigabitEthernet1/0/0] display this
#
interface GigabitEthernet1/0/0
 portswitch
 undo shutdown
 port link-type access
 port default vlan 10
#
return
```

2. 查询 MAC 老化时间，如果 MAC 老化时间低于上述查询到的 ARP 老化时间，则存在风险。进入系统视图，执行命令 **display mac-address aging-time**，查看字段“Aging time”的显示数值。例如，下述回显显示，系统的 MAC 老化时间为 300 秒。

```
<HUAWEI> display mac-address aging-time
  Aging time: 300 second(s)
```

风险的恢复方案

同配置规范。

1.5.2 Eth-Trunk 的配置规范

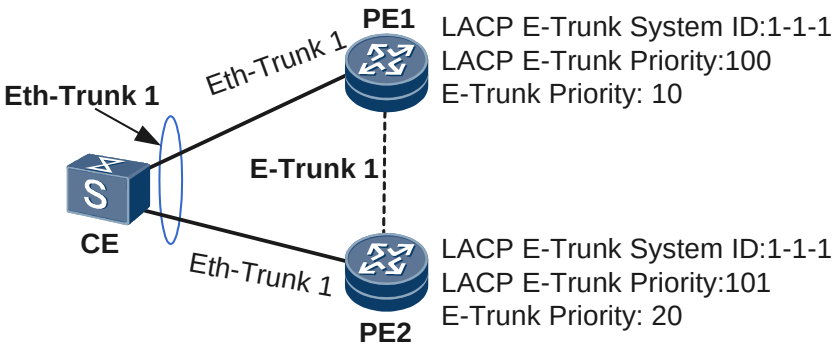
1.5.2.1 部署 E-Trunk 的两台设备全局配置需完全一致

对于 Eth-Trunk 配置静态 LACP、Eth-Trunk 加入 E-Trunk 场景，要求部署 E-Trunk 的两台设备全局配置 **lacp e-trunk system-id** *system-id* 和 **lacp e-trunk priority** *priority* 命令并且配置完全一致，否则存在 E-Trunk 成员口 Eth-Trunk 状态和预期不一致的风险。

应用场景

如图 1-6 所示，Eth-Trunk 配置静态 LACP 模式，并且加入 E-Trunk。

图1-6 LACP E-Trunk 全局配置不对称导致 Eth-Trunk 状态错误组网图



静态 LACP 模式的 Eth-Trunk 接口场景请参见 NE40E&NE80E 支持的 Eth-Trunk 接口特性。

配置规范

配置静态 LACP 模式的 Eth-Trunk 接口，并且将 Eth-Trunk 接口加入 E-Trunk 后，部署 E-Trunk 的 PE1 和 PE2 设备系统视图下均配置 **lacp e-trunk system-id** *system-id* 和 **lacp e-trunk priority** *priority* 命令，且两台设备的 *system-id* 和 *priority* 参数取值一致。

非规范配置的风险

风险描述

部署 E-Trunk 的 PE1 和 PE2 设备的 **System ID** 和 **System Priority** 信息不一致，会导致 E-Trunk 成员口 Eth-Trunk 状态和预期主备不一致的风险。

风险的判断方法

Eth-Trunk 的两端设备上，任意视图下执行 **display eth-trunk** *eth-trunk-id* 命令查看 **System ID** 和 **System Priority** 回显信息。

如下回显信息说明 PE1 和 PE2 设备上，系统 ID **System ID** 一致，但是系统优先级 **System Priority** 不一致。

查看 PE1 设备，发现 Eth-Trunk1 加入了 E-Trunk1。

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] display this
#
interface Eth-Trunk1
 mode lacp-static
 e-trunk 1
#
[HUAWEI] display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                WorkingMode: STATIC
Preempt Delay: Disabled    Hash arithmetic: According to flow
System Priority: 100       System ID: 0001-0001-0001
Least Active-linknumber: 1  Max Active-linknumber: 16
Operate status: down       Number Of Up Port In Trunk: 0
--------------------------------------------------------------------------------
ActorPortName        Status   PortType PortPri PortNo PortKey PortState Weight
Partner:
--------------------------------------------------------------------------------
ActorPortName        SysPri   SystemID      PortPri PortNo PortKey PortState
```

查看 PE2 设备，发现 Eth-Trunk1 加入了 E-Trunk1。

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] display this
#
interface Eth-Trunk1
 mode lacp-static
 e-trunk 1
#
[HUAWEI] display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                WorkingMode: STATIC
Preempt Delay: Disabled    Hash arithmetic: According to flow
System Priority: 101       System ID: 0001-0001-0001
Least Active-linknumber: 1  Max Active-linknumber: 16
Operate status: up       Number Of Up Port In Trunk: 0
--------------------------------------------------------------------------------
ActorPortName        Status   PortType PortPri PortNo PortKey PortState Weight
Partner:
--------------------------------------------------------------------------------
ActorPortName        SysPri   SystemID      PortPri PortNo PortKey PortState
```

风险的恢复方案

问题发生后，PE1 和 PE2 设备分别执行 **lacp e-trunk system-id** *system-id* 和 **lacp e-trunk priority** *priority* 命令，修改两台设备的 *system-id* 和 *priority* 参数取值修改为一致。

1.5.2.2 Eth-Trunk 需配置 LACP 模式或成员接口绑定 BFD 会话

在 Eth-Trunk 接口下存在成员接口没有绑定 BFD 会话，且该 Eth-Trunk 接口的工作模式不是静态 LACP 模式，链路出现故障无法及时发现。

应用场景

设备配置 Eth-Trunk 接口。

配置规范

配置 Eth-Trunk 接口为静态 LACP 模式，或者配置 Eth-Trunk 成员口绑定 BFD 会话。

- 当采用配置 Eth-Trunk 接口为静态 LACP 模式时，建议 LACP 超时时间设为默认值(3s)。
- 当采用配置 Eth-Trunk 成员口绑定 BFD 会话解决方案时，需要将所有的 Eth-Trunk 成员口都绑定 BFD 会话，同时建议配置 BFD 回切延时(WTR)。

非规范配置的风险

风险描述

Eth-Trunk 未配置为 LACP 模式且成员接口没有绑定 BFD 会话，Eth-Trunk 成员口发生链路故障时不能及时发现，业务不能及时切换。如果 Eth-Trunk 成员接口绑定 BFD 会话时，建议使能 BFD 回切延时（WTR）功能，避免因 BFD 会话频繁震荡，导致 Eth-Trunk 成员接口频繁震荡，影响业务收敛。

风险的判断方法

1. 查看 Eth-Trunk 接口是否配置了静态 LACP 模式。

   如下回显表示 Eth-Trunk1 配置了静态 LACP 模式，而 Eth-Trunk2、Eth-Trunk3 未配置静态 LACP 模式，Eth-Trunk2、Eth-Trunk3 可能存在本案例描述的问题，需要查看 Eth-Trunk2、Eth-Trunk3 的成员口是否绑定了 BFD 会话。

   ```
   <HUAWEI> display current-configuration interface Eth-Trunk
   ……
   #
   interface Eth-Trunk1
   mode lacp-static
   #
   interface Eth-Trunk2
   #
   interface Eth-Trunk3
   #
   ```

2. 查看 Eth-Trunk 成员口是否绑定 BFD 会话。

   如下回显表示 Eth-Trunk2 的成员口 GigabitEthernet1/0/0 绑定了 BFD 会话，而其成员口 GigabitEthernet3/0/0 未绑定了 BFD 会话；Eth-Trunk3 的两个成员口虽然绑定了 BFD 会话，但未配置 BFD 回切延时。

因此，Eth-Trunk2、Eth-Trunk3 都存在本案例描述的问题。

查看 Eth-Trunk 的成员口。

```
<HUAWEI> display eth-trunk 2
Eth-Trunk2's state information is:
WorkingMode: NORMAL       Hash arithmetic: According to flow
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 16
Operate status: up        Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
-
PortName                  Status     Weight
GigabitEthernet1/0/0           Up         1
GigabitEthernet3/0/0           Up         1
<HUAWEI> display eth-trunk 3
Eth-Trunk3's state information is:
WorkingMode: NORMAL       Hash arithmetic: According to flow
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 16
Operate status: up        Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
-
PortName                  Status     Weight
GigabitEthernet2/0/0           Up         1
GigabitEthernet4/0/0           Up         1
```

查看 Eth-Trunk 所有成员口是否绑定 BFD 会话

```
<HUAWEI> display current-configuration configuration bfd-session
#
bfd eth-trunk2-1 bind peer-ip default-ip interface GigabitEthernet1/0/0
 discriminator local 6013
 discriminator remote 6213
 wtr 10
 process-interface-status
 commit
//成员口 GigabitEthernet3/0/0 未绑定 BFD
#
bfd eth-trunk3-1 bind peer-ip default-ip interface GigabitEthernet2/0/0
 discriminator local 6013
 discriminator remote 6213
 process-interface-status
 commit
//BFD 未配置回切延时
#
bfd eth-trunk3-2 bind peer-ip default-ip interface GigabitEthernet4/0/0
 discriminator local 6013
 discriminator remote 6213
 process-interface-status
 commit
//BFD 未配置回切延时
#
```

风险的恢复方案

配置 Eth-Trunk 1、Eth-Trunk 2、Eth-Trunk 3 接口为静态 LACP 模式，或者配置 Eth-Trunk 2、Eth-Trunk 3 成员口绑定 BFD 会话。

- 配置 Eth-Trunk 接口为 LACP 模式。

  # 配置 Eth-Trunk 1 接口。

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] mode lacp-static
[HUAWEI-Eth-Trunk1] quit
```

  # 配置 Eth-Trunk 2 接口。

```
[HUAWEI] interface eth-trunk 2
[HUAWEI-Eth-Trunk2] mode lacp-static
[HUAWEI-Eth-Trunk2] quit
```

  # 配置 Eth-Trunk 3 接口。

```
[HUAWEI] interface eth-trunk 3
[HUAWEI-Eth-Trunk3] mode lacp-static
```

- 配置 Eth-Trunk 成员口绑定 BFD 会话。

  # 配置 Eth-Trunk 2 接口。

```
<HUAWEI> system-view
[HUAWEI] bfd eth-trunk2-1 bind peer-ip default-ip interface
GigabitEthernet1/0/0
[HUAWEI-bfd-session-eth-trunk2-1] wtr 10
[HUAWEI-bfd-session-eth-trunk2-1] process-interface-status
[HUAWEI-bfd-session-eth-trunk2-1] quit
[HUAWEI] bfd eth-trunk2-2 bind peer-ip default-ip interface
GigabitEthernet3/0/0
[HUAWEI-bfd-session-eth-trunk2-2] wtr 10
[HUAWEI-bfd-session-eth-trunk2-2] process-interface-status
```

  # 配置 Eth-Trunk 3 接口。

```
<HUAWEI> system-view
[HUAWEI] bfd reth-trunk3-1 bind peer-ip default-ip interface
GigabitEthernet2/0/0
[HUAWEI-bfd-session-eth-trunk3-1] wtr 10
[HUAWEI-bfd-session-eth-trunk3-1] process-interface-status
[HUAWEI-bfd-session-eth-trunk3-1] quit
[HUAWEI] bfd eth-trunk3-2 bind peer-ip default-ip interface
GigabitEthernet4/0/0
[HUAWEI-bfd-session-eth-trunk3-2] wtr 10
[HUAWEI-bfd-session-eth-trunk3-2] process-interface-status
```

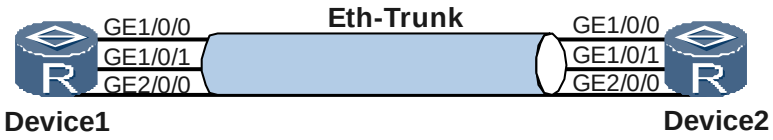
1.5.2.3 一端未加入 Eth-Trunk 导致流量不通

当链路一端设备的接口加入到 Eth-Trunk 中，另一端设备的接口未加入 Eth-Trunk 时，会导致流量不通。

应用场景

两台路由器通过 3 个 GE 接口直连，将这 3 个 GE 接口捆绑，形成一个 Eth-Trunk 接口，从而实现了增加带宽和提高可靠性的目的。

图1-7 Eth-Trunk 使用场景图



配置规范

对接 Eth-Trunk 的两台设备，两台设备上的对接接口需要全部加入到 Eth-Trunk 中。

非规范配置的风险

风险描述

如果出现链路一端接口加入到 Eth-Trunk 中，但是另一端没有加入，数据流量走到该链路上的话，可能会导致流量不通。

业务现象如下：

接口均加入到 Eth-Trunk 的设备在转发流量时会将报文分担到全部接口上，但是对端存在接口没有加入到 Eth-Trunk，那么对端未加入到 Eth-Trunk 的接口无法接收、转发流量。

风险的判断方法

在两侧设备上查看是否对接的接口都加入到了 Eth-Trunk 中。

```
<Device1> display eth-trunk 10
Eth-Trunk10's state information is:
WorkingMode: NORMAL       Hash arithmetic: According to flow
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 16
Operate status: up        Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------
PortName                  Status     Weight
GigabitEthernet1/0/0        Up         1
GigabitEthernet1/0/1        Up         1
GigabitEthernet2/0/0        Up         1
<Device2> display eth-trunk 10
Eth-Trunk10's state information is:
WorkingMode: NORMAL       Hash arithmetic: According to flow
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 16
Operate status: up        Number Of Up Port In Trunk: 1
--------------------------------------------------------------------------------
PortName                  Status     Weight
GigabitEthernet1/0/0        Up         1
```

风险的恢复方案

将对接接口加入到 Eth-Trunk 中。

```
<Device2> system-view
[Device2] interface GigabitEthernet1/0/1
[Device2-GigabitEthernet1/0/1] eth-trunk 10
```

```
[Device2-GigabitEthernet1/0/1] quit
[Device2] interface GigabitEthernet2/0/0
[Device2-GigabitEthernet2/0/0] eth-trunk 10
[Device2-GigabitEthernet2/0/0] quit
```

1.5.3 IP-Trunk 的配置规范

1.5.3.1 IP-Trunk 需配置成员接口绑定 BFD 会话

在 IP-Trunk 接口下存在成员接口没有绑定 BFD 会话，链路出现故障无法及时发现。

应用场景

设备配置 IP-Trunk 接口。

配置规范

配置 IP-Trunk 成员口绑定 BFD 会话。

- 当采用配置 IP-Trunk 成员口绑定 BFD 会话解决方案时，需要将此 IP-Trunk 的所有成员口都绑定 BFD 会话。

说明
建议配置 BFD 会话的等待恢复时间(WTR)。

非规范配置的风险

风险描述

IP-Trunk 成员接口没有绑定 BFD 会话，IP-Trunk 成员口发生链路故障时不能及时发现，业务不能及时切换。

如果 IP-Trunk 成员接口绑定 BFD 会话时，建议使能 BFD 会话的等待恢复时间（WTR）功能，避免因 BFD 会话频繁震荡，影响业务收敛。

风险的判断方法

1. 查看 IP-Trunk 成员口是否绑定 BFD 会话。

   如下回显表示：

   - IP-Trunk1 的成员口 POS1/0/0 绑定了 BFD 会话且配置了 WTR 功能
   - IP-Trunk1 的成员口 POS1/0/1 绑定了 BFD 会话，但未配置 WTR 功能。
   - IP-Trunk2 的两个成员口均未绑定 BFD 会话。

   因此，IP-Trunk1、IP-Trunk2 都存在本案例描述的问题。

   # 查看 IP-Trunk 的成员口。

```
<HUAWEI> display interface ip-trunk 1
Ip-Trunk1 current state : DOWN
Line protocol current state : DOWN
Link quality grade : --
Description:HUAWEI, Ip-Trunk1 Interface
Route Port,Hash arithmetic : According to flow,Maximal BW: 311M, Current BW: 0M,
 The Maximum Transmit Unit is 4470
Internet protocol processing : disabled Link layer protocol is nonstandard HDLC
```

```
Physical is IP_TRUNK
Current system time: 2017-03-28 17:10:01-08:00
   Last 300 seconds input rate 0 bits/sec, 0 packets/sec
   Last 300 seconds output rate 0 bits/sec, 0 packets/sec
   Realtime 0 seconds input rate 0 bits/sec, 0 packets/sec
   Realtime 0 seconds output rate 0 bits/sec, 0 packets/sec
   Input: 0 packets,0 bytes
         0 unicast,0 broadcast,0 multicast
         0 errors,0 unknownprotocol
   Output:0 packets,0 bytes
         0 unicast,0 broadcast,0 multicast
         0 errors
   Input bandwidth utilization  :   0%
   Output bandwidth utilization :   0%
-------------------------------------------------------
PortName                  Status     Weight
-------------------------------------------------------
Pos1/0/0                  DOWN       1
Pos1/0/1                  DOWN       1
-------------------------------------------------------

<HUAWEI> display interface ip-trunk 2
Ip-Trunk2 current state : DOWN
Line protocol current state : DOWN
Link quality grade : --
Description:HUAWEI, Ip-Trunk2 Interface
Route Port,Hash arithmetic : According to flow,Maximal BW: 311M, Current BW: 0M,
 The Maximum Transmit Unit is 4470
Internet protocol processing : disabled Link layer protocol is nonstandard HDLC
Physical is IP TRUNK
Current system time: 2017-03-28 17:15:51-08:00
   Last 300 seconds input rate 0 bits/sec, 0 packets/sec
   Last 300 seconds output rate 0 bits/sec, 0 packets/sec
   Realtime 99 seconds input rate 0 bits/sec, 0 packets/sec
   Realtime 99 seconds output rate 0 bits/sec, 0 packets/sec
   Input: 0 packets,0 bytes
         0 unicast,0 broadcast,0 multicast
         0 errors,0 unknownprotocol
   Output:0 packets,0 bytes
         0 unicast,0 broadcast,0 multicast
         0 errors
   Input bandwidth utilization  :   0%
   Output bandwidth utilization :   0%
-------------------------------------------------------
PortName                  Status     Weight
-------------------------------------------------------
Pos1/0/2                  DOWN       1
Pos1/0/3                  DOWN       1
-------------------------------------------------------
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 0
```

查看 IP-Trunk 所有成员口是否绑定 BFD 会话

```
<HUAWEI> display current-configuration configuration bfd-session
```

```
#
bfd BFD-IPtrunk1-1 bind peer-ip default-ip interface Pos1/0/0
 discriminator local 6013
 discriminator remote 6213
 wtr 10
 process-interface-status
 commit
#
//IP-Trunk 成员口 Pos1/0/0 绑定了 BFD 会话且配置了 BFD 会话的等待恢复时间
bfd BFD-IPtrunk1-2 bind peer-ip default-ip interface Pos1/0/1
 discriminator local 6010
 discriminator remote 6213
 process-interface-status
 commit
#
//IP-Trunk 成员口 Pos1/0/1 未配置 BFD 会话的等待恢复时间
//IP-trunk2 的成员 Pos1/0/2、Pos1/0/3 未绑定 BFD
return
```

风险的恢复方案

配置 IP-Trunk 成员口绑定 BFD 会话，并配置 BFD 会话的等待恢复时间。

- IP-Trunk1 的成员口 POS1/0/1 配置 BFD 会话的等待恢复时间。

```
<HUAWEI> system-view
[HUAWEI] bfd BFD-IPtrunk1-2
[HUAWEI-bfd-session-BFD-IPtrunk1-2] wtr 10
```

- IP-Trunk2 的成员口 POS1/0/2 及 POS1/0/3 绑定 BFD 会话且配置 BFD 会话的等待恢复时间。

```
<HUAWEI> system-view
[HUAWEI] bfd BFD-Iptrunk2-1 bind peer-ip default-ip interface Pos1/0/2
[HUAWEI-bfd-session-BFD-Iptrunk2-1] discriminator local 6000
[HUAWEI-bfd-session-BFD-Iptrunk2-1] discriminator remote 6001
[HUAWEI-bfd-session-BFD-Iptrunk2-1] wtr 10
[HUAWEI-bfd-session-BFD-Iptrunk2-1] process-interface-status
[HUAWEI-bfd-session-BFD-Iptrunk2-1] commit
[HUAWEI-bfd-session-BFD-Iptrunk2-1] quit
[HUAWEI] bfd BFD-Iptrunk2-2 bind peer-ip default-ip interface Pos1/0/3
[HUAWEI-bfd-session-BFD-Iptrunk2-2] discriminator local 6002
[HUAWEI-bfd-session-BFD-Iptrunk2-2] discriminator remote 6003
[HUAWEI-bfd-session-BFD-Iptrunk2-2] wtr 10
[HUAWEI-bfd-session-BFD-Iptrunk2-2] process-interface-status
[HUAWEI-bfd-session-BFD-Iptrunk2-2] commit
```

1.6 IP 业务

1.6.1 IP 性能配置的配置规范

1.6.1.1 TCP window-size 配置规范

由于 TCP 提供收发缓冲区进行报文缓存，如果配置的收发缓冲区过小，导致设备无法收发超过该大小的报文，可能导致 TCP 连接中断。

应用场景

部署使用 TCP 进行建连的业务，例如 BGP、LDP 等。

配置规范

在系统视图下，执行 **tcp window** *window-size* 命令，将 TCP 收发缓冲区大小调整为一个合理的值。

非规范配置的风险

风险描述

- 在系统视图下，执行 **tcp window** *window-size* 命令，设置 TCP 收发缓冲区大小。例如，设置 **tcp window 1** 将 TCP 的收发缓冲区设置为 1K 字节。
- 使用 TCP 的业务收发的报文超过 TCP 收发缓冲区大小。例如，上述配置条件下，使用 TCP 的业务收发的报文超过 1K 字节。

满足上述所有条件时，TCP 连接中断，从而影响到使用该 TCP 的业务转发。

业务现象：

TCP 连接中断。

风险的判断方法

在用户视图下，执行 **display tcp status** 命令，查看 TCP 连接状态。

连接正常时，可以看到对应的 TCP 连接存在。

```
<HUAWEI> display tcp status
TCPCB    Tid/Soid Local Add:port      Foreign Add:port     VPNID  State
7800b1ec 6  /1    0.0.0.0:21          0.0.0.0:0           23553  Listening
72094f08 144/4    0.0.0.0:22          0.0.0.0:0           23553  Listening
78000714 144/1    0.0.0.0:23          0.0.0.0:0           23553  Listening
7800a90c 175/3    0.0.0.0:179         1.1.1.1:0    0      Listening
7208f1d8 175/6    0.0.0.0:179         1.1.1.2:0      0     Listening
7374df44 175/327  2.2.2.2:54269       3.3.3.3:179    0     Syn_Sent
12d26d68 144/6    192.168.131.166:23    192.168.224.3:57582    0     Established
15691498 144/29   192.168.131.166:23    192.168.224.3:61044    0     Established
7375240c 144/23   192.168.131.166:23    192.168.242.37:50132   0     Established
12d23a60 144/5    192.168.131.166:23    192.168.242.37:54566   0     Established
7374bbc4 144/30   192.168.131.166:23    192.168.250.23:8426    0     Established
7067cff4 175/10   192.168.131.166:179   192.168.242.37:54512   0     Established
```

连接中断后，查看不到对应的 TCP 连接存在。

```
<HUAWEI> display tcp status
TCPCB    Tid/Soid Local Add:port       Foreign Add:port     VPNID  State
7800b1ec 6  /1    0.0.0.0:21          0.0.0.0:0           23553  Listening
72094f08 144/4    0.0.0.0:22          0.0.0.0:0           23553  Listening
78000714 144/1    0.0.0.0:23          0.0.0.0:0           23553  Listening
7800a90c 175/3    0.0.0.0:179         1.1.1.1:0    0     Listening
7208f1d8 175/6    0.0.0.0:179         1.1.1.2:0      0     Listening
7374df44 175/327  2.2.2.2:54269       3.3.3.3:179    0     Syn Sent
```

风险的恢复方案

请按照配置规范进行配置。

1.6.2 IPv6 基础配置的配置规范

1.6.2.1 TCP6 window-size 配置规范

由于 TCP6 提供收发缓冲区进行报文缓存，如果配置的收发缓冲区过小，导致设备无法收发超过该大小的报文，可能导致 TCP6 连接中断。

应用场景

部署使用 TCP6 进行建连的业务，例如 BGP、LDP 等。

配置规范

在系统视图下，执行 **tcp ipv6 window** *window-size* 命令，将 TCP6 收发缓冲区大小调整为一个合理的值。

非规范配置的风险

风险描述

- 在系统视图下，执行 **tcp ipv6 window** *window-size* 命令，设置 TCP6 收发缓冲区大小。例如，设置 **tcp ipv6 window 1** 将 TCP6 的收发缓冲区设置为 1K 字节。
- 使用 TCP6 的业务收发的报文超过 TCP6 收发缓冲区大小。例如，上述配置条件下，使用 TCP6 的业务收发的报文超过 1K 字节。

满足上述所有条件时，TCP6 连接中断，从而影响到使用该 TCP6 的业务转发。

业务现象如下：

TCP6 连接中断。

风险的判断方法

在用户视图下，执行 **display tcp ipv6 status** 命令，查看 TCP6 连接状态。

连接正常时，可以看到对应的 TCP6 连接存在。

```
<HUAWEI> display tcp ipv6 status
```

```
* - MD5 Authentication is enabled.
# - Keychain Authentication is enabled.
TCP6CB TID/SoID  Local Address       Foreign Address     State       VPNID
78004bdc 144/3    ::->22             ::->0             Listening   23553
78000dbc 144/2    ::->23             ::->0             Listening   23553
12d26d68 144/6   2000::1->23         2000::2->57582      Established  0
```

连接中断后，查看不到对应的 TCP6 连接存在。

```
<HUAWEI> display tcp ipv6 status
* - MD5 Authentication is enabled.
# - Keychain Authentication is enabled.
TCP6CB TID/SoID  Local Address       Foreign Address     State       VPNID
78004bdc 144/3    ::->22             ::->0             Listening   23553
78000dbc 144/2    ::->23             ::->0             Listening   23553
```

风险的恢复方案

请按照配置规范进行配置。

1.7 IP 路由

1.7.1 IGP 公共的配置规范

1.7.1.1 IGP 邻居超时时间配置规范

IGP 协议（OSPF、ISIS）配置的邻居超时时间过短，可能会导致邻居容易超时 Down 而影响业务。

应用场景

设备使能了相关 IGP 协议（比如 OSPF、ISIS）。

配置规范

建议采用 **ospf timer dead** *interval* 命令缺省的邻居的超时时间。

非规范配置的风险

风险描述

- 对于使能了 IS-IS 的接口，若其接口视图下配置了 **isis timer hello 3** 命令且未配置 **isis timer holding-multiplier** *number* 命令，则认为其配置了过短的邻居超时时间。
- 对于使能了 OSPF 的接口，满足以下任一条件则认为其配置了过短的邻居超时时间：
  - 接口视图下配置了 **ospf timer hello 1** 命令且没有配置 **ospf timer dead** *interval* 命令。
  - 接口视图下配置了 **ospf timer dead** *interval* 命令，且 *interval* 取值不大于 4。

当满足上述任意一个条件时，可能会导致邻居超时 Down，进而影响业务。

风险的判断方法

1. 查询是否使能了 IGP 协议（OSPF、ISIS）。

   # 在任意视图下执行 **display current-configuration configuration isis** 命令和 **display current-configuration configuration ospf** 命令，查看是否存在相关协议的的配置信息。

```
<HUAWEI> display current-configuration configuration isis
#
isis 100
 is-level level-2
 cost-style wide
 network-entity 10.0000.0100.0005.00
#
<HUAWEI> display current-configuration configuration ospf
#
ospf 100
 area 0.0.0.0
  network 31.1.1.0 0.0.0.255
  network 12.3.3.0 0.0.0.255
#
```

2. 查询使能了 IGP 协议（OSPF、ISIS）的接口。

   # 在任意视图下执行 **display isis interface verbose** 命令，查询使能了 ISIS 协议的接口。下面显示信息中，**GigabitEthernet3/0/6.1001** 接口使能了 ISIS 协议。

```
<HUAWEI> display isis interface verbose
                  Interface information for ISIS(100)
                  ------------------------------------
 Interface      Id     IPV4.State         IPV6.State     MTU  Type  DIS
 GE3/0/6.1001   001        Up               Down        1497 L1/L2 --
  Circuit MT State          : Standard
  Circuit Parameters        : p2p
  Description              : HUAWEI, GigabitEthernet3/0/6.1001 Interface
  SNPA Address             : 0018-8266-56be
  IP Address               : 26.1.1.5
  IPV6 Link Local Address    :
  IPV6 Global Address(es)    :
  Csnp Timer Value          :  L12   10
  Hello Timer Value         :       10
  DIS Hello Timer Value      :
  Hello Multiplier Value     :     1000
  LSP-Throttle Timer        :  L12   50
  Cost                     :  L1    10  L2    10
  Ipv6 Cost                :  L1    10  L2    10
  Retransmit Timer Value     :  L12    5
  Bandwidth-Value           :  Low 1000000000  High        0
  Static Bfd               :  NO
  Dynamic Bfd              :  NO
  Dynamic IPv6 Bfd          :  NO
  Fast-Sense Rpr           :  NO
  Extended-Circuit-Id Value   :  0000000001
  Suppress Base             :  NO
  IPv6 Suppress Base         :  NO
  Link quality adjust cost    :  NO
Link quality             :  0x0(Best)
```

在任意视图下执行 **display ospf interface all** 命令，查询使能了 OSPF 协议的接口。下面显示信息中，**GigabitEthernet3/0/4** 和 **GigabitEthernet3/0/9** 接口使能了 OSPF 协议。

```
<HUAWEI> display ospf interface all
       OSPF Process 100 with Router ID 20.1.1.2
             Interfaces
 Area: 0.0.0.0         (MPLS TE not enabled)
```

Interface: 12.3.3.1 (**GigabitEthernet3/0/4**)

```
 Cost: 1      State: BDR      Type: Broadcast    MTU: 1500
 Priority: 1
 Designated Router: 12.3.3.2
 Backup Designated Router: 12.3.3.1
 Timers: Hello 10 , Dead 40 , Poll  120 , Retransmit 5 , Transmit Delay 1
 Interface: 31.1.1.1 (GigabitEthernet3/0/9)
 Cost: 1      State: DR       Type: Broadcast    MTU: 1500
 Priority: 1
 Designated Router: 31.1.1.1
 Backup Designated Router: 31.1.1.2
 Timers: Hello 10 , Dead 40 , Poll  120 , Retransmit 5 , Transmit Delay 1
```

3. 查询是否配置了过短的邻居超时时间。

   对于使能了 ISIS 的接口，若其接口视图下配置了 **isis timer hello 3** 命令且未配置 **isis timer holding-multiplier** *number* 命令，则认为其配置了过短的邻居超时时间。

   对于使能了 OSPF 的接口，满足以下任一条件则认为其配置了过短的邻居超时时间：

   （1）接口视图下配置了 **ospf timer hello 1** 命令且没有配置 **ospf timer dead** *interval* 命令。

   （2）接口视图下配置了 **ospf timer dead** *interval* 命令，且 *interval* 取值不大于 4。

   # 查看 GigabitEthernet3/0/6.1001 接口，该接口配置了过短的邻居超时时间。

```
<HUAWEI> display current-configuration interface GigabitEthernet3/0/6.1001
#
interface GigabitEthernet3/0/6.1001
 vlan-type dot1q 1001
 ip address 26.1.1.5 255.255.255.0
 isis enable 100
 isis circuit-type p2p
 isis timer hello 3
#
return
```

   # 查看 GigabitEthernet3/0/4 接口，该接口配置了过短的邻居超时时间。

```
<HUAWEI> display current-configuration interface GigabitEthernet3/0/4
#
interface GigabitEthernet3/0/4
 undo shutdown
 ip address 12.3.3.1 255.255.255.0
 ospf timer hello 1
#
return
```

   # 查看 GigabitEthernet3/0/9 接口，该接口配置了过短的邻居超时时间。

```
<HUAWEI> display current-configuration interface GigabitEthernet3/0/9
```

```
#
interface GigabitEthernet3/0/9
 undo shutdown
 ip address 31.1.1.1 255.255.255.0
 ospf timer hello 3
 ospf timer dead 4
#
return
```

风险的恢复方案

请按照配置规范进行配置。

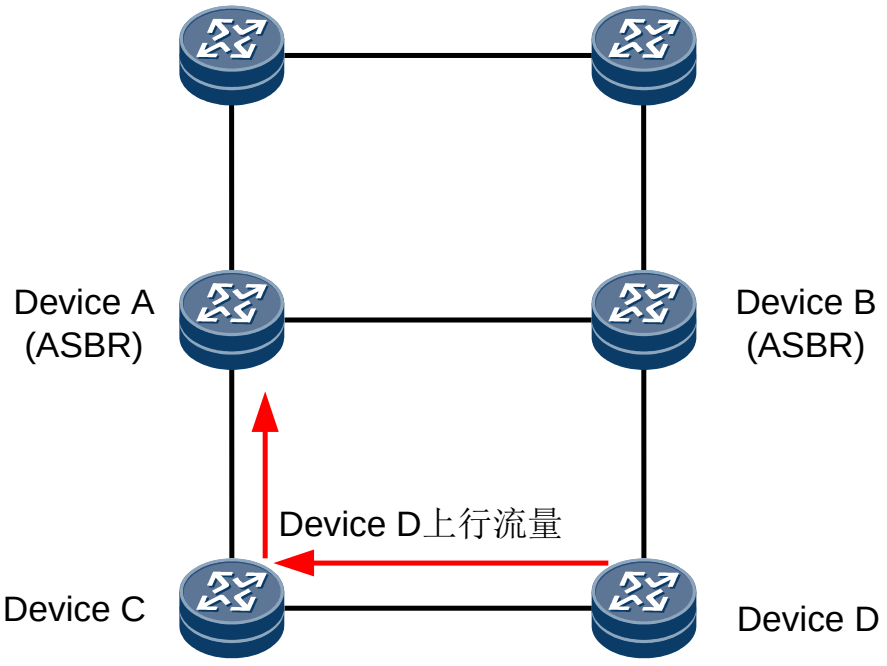
1.7.1.2 IGP 引入路由优先级需要高于 IGP 的路由避免流量绕行

网络中同时存在多台 ASBR 设备的 IGP 引入外部路由时，如果外部路由的优先级低于 IGP，则会只有一台设备 IGP 能够成功引入外部路由，其他 ASBR 上通过 IGP 学习到路由，导致流量绕行。

应用场景

如图 1-8 所示，RouterA 和 RouterB 为出口设备，在 RouterA 和 RouterB 上 OSPF 都引入 BGP 路由重发布给 RouterC 和 RouterD 引导上行流量。由于 BGP 路由优先级低于 OSPF，可能会出现 RouterB 学习到 RouterA 重发布的 OSPF 路由后，RouterB 上的 BGP 路由变为不活跃状态，RouterB 就不会重发布路由给 RouterD。这样 RouterD 上行流量就会绕行 RouterC，到达 RouterA 出口。

图1-8 IGP 引入路由优先级低于 IGP 的路由导致流量绕行组网图



配置规范

执行 **preference** 命令调整 IGP 协议的路由优选先级低于被引入的路由协议优先级（数值越小，优先级越高）。

说明
修改优先级时需要注意避免影响正常业务。

非规范配置的风险

风险描述

1. 网络中多台 ASBR 设备的 IGP 引入外部路由。
2. 被引入的外部路由优先级低于 IGP 的路由协议优先级。

当同时满足上述条件时，业务流量绕行。

业务现象如下：

业务流量没有按照原始路由协议的路径转发，而是通过 IGP 路由绕行到一台 ASBR 上，然后按照原始路由协议转发。

风险的判断方法

1. 执行如下命令，查看配置中 IGP 协议是否引入了外部路由。

   # 在任意视图下执行 **display current-configuration configuration ospf** 命令，查看配置中 OSPF 协议是否引入了外部路由。显示信息说明 OSPF 协引入了 BGP 路由。

```
<HUAWEI> display current-configuration configuration ospf
#
ospf 1 router-id 1.1.1.6
 import-route bgp
 area 0.0.0.0
  network 1.1.19.6 0.0.0.0
#
return
```

   # 在任意视图下执行 **display current-configuration configuration ospfv3** 命令，查看配置中 OSPFv3 协议是否引入了外部路由。显示信息说明 OSPFv3 协引入了静态路由。

```
<HUAWEI> display current-configuration configuration ospfv3
#
ospfv3 1
 router-id 1.1.1.1
 import-route static
#
return
```

   # 在任意视图下执行 **display current-configuration configuration isis** 命令，查看配置中 ISIS 协议是否引入了外部路由。显示信息说明 ISIS 协引入了静态路由。

```
<HUAWEI> display current-configuration configuration isis
#
isis 1
 cost-style wide
```

```
 network-entity 10.000a.0011.0006.00
 import-route static
#
return
```

2. 通过配置查看被引入到 IGP 协议的路由优先级。

   # 查看 OSPF 协议配置。OSPF 区域内和区域间路由的优先级为 200，OSPF ASE 和 NSSA 路由优先级为 200。

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] display this
#
ospf 1
 preference 200
 preference ase 200
#
return
```

   # 查看 OSPFv3 协议配置。OSPFv3 区域内和区域间路由的优先级为 100，OSPFv3 ASE 和 NSSA 路由优先级为 100。

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] display this
#
ospfv3 1
 router-id 1.1.19.6
 preference 100
 preference ase 100
#
return
```

   # 查看 ISIS 协议配置。ISIS 区域内和区域间路由的优先级为 200。

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1]  display this
#
isis 1
 cost-style wide
 network-entity 00.0005.0000.0019.0006.00
 preference 200
#
return
```

   # 查看 BGP 协议配置。EBGP 路由的优先级为 200，IBGP 协议的优先级为 180，BGP Local 的优先级为 150。

```
<HUAWEI> system-view
[HUAWEI] bgp
[HUAWEI-bgp] display this
#
bgp 100
 #
 ipv4-family unicast
  undo synchronization
  preference 200 180 150
#
```

查看 RIP 协议配置。RIP 路由的优先级为 200。

```
<HUAWEI> display current-configuration configuration rip
#
rip 1
 preference 200
#
return
```

查看 RIPng 协议配置。RIPng 路由的优先级为 200。

```
<HUAWEI> display current-configuration configuration ripng
#
ripng 1
 preference 200
#
return
```

查看静态路由配置。静态路由的优先级为 200。

```
<HUAWEI> display current-configuration configuration
#
 ……
ip route-static 1.1.1.1 32 NULL 0 preference 200
#
```

3. 如果没有配置路由优先级，华为设备各协议缺省优先级如下：

Route soure	Huawei Prefrence
DIRECT	0
OSPF	10
IS-IS	15
STATIC	60
RIP	100
OSPF ASE	150
OSPF NSSA	150
IBGP	255
EBGP	255
BGP Local	255

如果 IGP 的路由协议优先级高于引入的外部路由优先级，则存在流量绕行的风险。

风险的恢复方案

请按照配置规范进行配置。

1.7.2 OSPF 的配置规范

1.7.2.1 OSPF 两端接口网络类型需要配置一致才能实现邻居建立后正常学习路由

OSPF 两端接口网络类型不一致，一端为点对点，一端为广播网，导致邻居建立后无法学习路由。

应用场景

设备使能了 OSPF 协议。

配置规范

在接口视图下，执行命令 **ospf network-type** 命令，将两端设备接口下的 OSPF 网络类型修改为一致。

非规范配置的风险

风险描述

当 OSPF 两端接口网络类型不一致，一端为点对点，一端为广播网时，虽然 OSPF 邻居可以正常建立，但是无法正确计算路由，进而导致依赖这些路由的业务不通。

业务现象如下：

OSPF 邻居可以正常建立，但是无法学习路由。

风险的判断方法

1. 在用户视图下执行 **display ospf interface all** 命令，查看所有接口的 OSPF 详细信息。

   从显示信息可以看出，OSPF 在 GigabitEthernet1/0/1 和 GigabitEthernet1/1/0 接口建立广播网邻居。

```
<HUAWEI> display ospf interface all
       OSPF Process 101 with Router ID 1.1.1.1
              Interfaces

 Area: 0.0.0.0        (MPLS TE not enabled)

 Interface: 192.168.1.1 (GigabitEthernet1/0/1)
 Cost: 1      State: DROther    Type: Broadcast    MTU: 1500  Priority: 123
 Designated Router: 192.168.1.3
 Backup Designated Router: 0.0.0.0
 Timers: Hello 10 , Dead 40 , Poll  120 , Retransmit 5 , Transmit Delay 1

 Interface: 192.168.2.1 (GigabitEthernet1/1/0)
 Cost: 1      State: DROther    Type: Broadcast    MTU: 1500
 Priority: 0
 Designated Router: 192.168.2.3
 Backup Designated Router: 0.0.0.0
 Timers: Hello 10 , Dead 40 , Poll  120 , Retransmit 5 , Transmit Delay 1
```

2. 在用户视图下，执行 **display ospf peer** *interface-name* 命令，查看接口所建立的 OSPF 邻居。

   如果没有邻居或者邻居状态不为 Full，则检查下一个接口；否则需要根据接口类型判断两端接口类型是否一致。

说明

- 广播网接口的邻居的 DR 字段必须有 IP 地址，若该字段显示为 DR: None，则认为两端接口类型不一致。
- 点对点接口的邻居的 DR 字段必须显示为 DR: None，如果显示为其它，则认为两端接口类型不一致。

从显示信息可以看出，广播网接口 GigabitEthernet1/0/1 的 Full 邻居的 DR 字段没有 IP 地址，可以判断为两端接口类型不一致。

```
<HUAWEI> display ospf peer GigabitEthernet1/0/1
       OSPF Process 101 with Router ID 1.1.1.1
              Neighbors

 Area 0.0.0.0 interface 192.168.1.1(GigabitEthernet1/0/1)'s neighbors
 Router ID: 1.1.1.3   Address: 192.168.1.3
   State: Full  Mode:Nbr is  Master  Priority: 123
   DR: None   BDR: None   MTU: 0
   Dead timer due in 33  sec
   Retrans timer interval: 5
   Neighbor is up for 00:45:35
   Authentication Sequence: [ 0 ]
<HUAWEI> display ospf peer GigabitEthernet1/1/0

       OSPF Process 101 with Router ID 1.1.1.1
              Neighbors

 Area 0.0.0.0 interface 192.168.2.1(GigabitEthernet1/1/0)'s neighbors
 Router ID: 1.1.1.3   Address: 192.168.2.3
   State: Full  Mode:Nbr is  Master  Priority: 1
DR: 192.168.2.3  BDR: None   MTU: 0       Dead timer due in 32  sec
   Retrans timer interval: 5
   Neighbor is up for 00:23:12
   Authentication Sequence: [ 0 ]
```

风险的恢复方案

将两端设备接口下的 OSPF 网络类型修改为一致。

在接口视图下，执行命令 **ospf network-type** 命令，将两端设备接口下的 OSPF 网络类型修改为一致。

1. 由显示信息可以看出，GigabitEthernet1/0/1 接口网络类型已经被修改为点对点。

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet1/0/1
[HUAWEI-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 192.168.1.1 255.255.255.0
 ospf network-type p2p
 ospf dr-priority 123
```

```
#
return
```

2. 在两端设备的用户视图下执行 **display ospf peer** *interface-name* 命令，查看 OSPF 邻居的 DR 字段。

   由显示信息可以看出，GigabitEthernet1/0/1 的 DR 字段已经显示为 IP 地址，配置正确。

```
<HUAWEI> display ospf peer GigabitEthernet1/0/1
       OSPF Process 101 with Router ID 1.1.1.1
             Neighbors

 Area 0.0.0.0 interface 192.168.1.1(GigabitEthernet1/0/1)'s neighbors
 Router ID: 1.1.1.3   Address: 192.168.1.3
   State: Full  Mode:Nbr is  Master  Priority: 123
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 38  sec
   Retrans timer interval: 5
   Neighbor is up for 00:00:07
   Authentication Sequence: [ 0 ]
```

1.7.3 ISIS 的配置规范

1.7.3.1 割接过程中需要删除发布的缺省路由

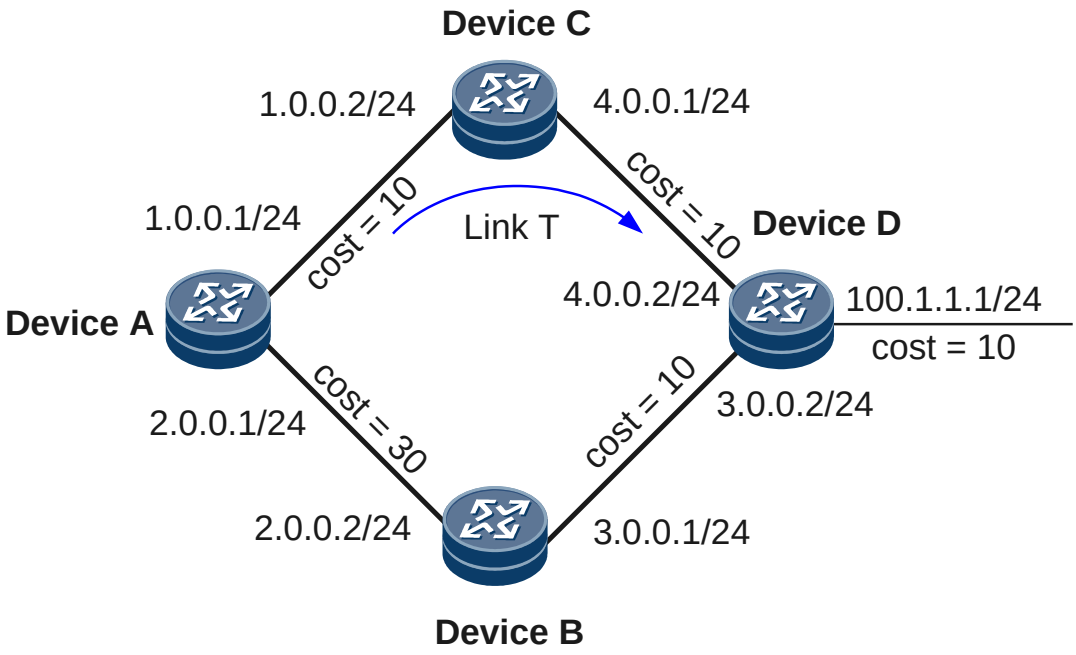
IS-IS 可以通过 LSP 中设置过载标志位，使得经过该设备的路由切换到备份路径。但是设置过载标志位并不会影响发布缺省路由，缺省路由不会切换路径。

应用场景

如图 1-9 所示，RouterA、RouterB、RouterC、RouterD 之间建立 IS-IS 邻居。链路 T 为业务主路径，RouterA->RouterB->RouterD 为备份路径。

- 割接过程中，RouterC 的 IS-IS 视图下配置 **set-overload** 命令，将业务切换到备份路径场景。
- RouterC 的 IS-IS 视图下配置 **set-overload on-startup** 命令，设备主备倒换或者重启后，路由延时回切场景。

图1-9 IS-IS 协议设置过载标志位不会取消发布缺省路由组网图



配置规范

割接过程中，IS-IS 视图下，删除发布缺省路由命令，割接完成后需要再重新配置。

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] undo default-route-advertise
```

非规范配置的风险

风险描述

当 RouterC 的 IS-IS 视图下配置了 **set-overload** [**on-startup**]命令设置非伪节点 LSP 的过载标志位，并且配置了 **default-route-advertise** 命令，发布缺省路由时，缺省路由不会切换到备份路径。此时如果设备上没有明细路由，则会导致业务中断。

业务现象如下：

设备重启后 600 秒内，缺省路由没有切换到备份路径。

风险的判断方法

在任意视图下执行 **display isis** *process-id* **lsdb local verbose** 命令查看 LSP 信息，如果 **OL** 位为 **1**，说明已经设置了过载标志位。同时如果发布了缺省路由，说明问题发生。加粗字体表示设置了 **overload** 同时发布了缺省路由。

```
<HUAWEI> display isis 1 lsdb local verbose
       ATTENTION: System is overloaded
       Manual overload set     YES     OverLoad on Startup     NO
       System Memory Low       NO      Memory Allocate Failure NO
```

```
                    Level-2 Link State Database
LSPID            Seq Num    Checksum    Holdtime     Length  ATT/P/OL
--------------------------------------------------------------------------------
abcd.0001.0031.00-00* 0x0000008e   0x6726       1183         76     0/0/1
 SOURCE      abcd.0001.0031.00
 NLPID       IPV4
 AREA ADDR    10
 INTF ADDR    10.10.1.1
 INTF ADDR    30.1.1.2
+NBR  ID     aaaa.0001.0030.00  COST: 10
+IP-Extended  10.10.1.1     255.255.255.255  COST: 0
+IP-Extended  30.1.1.0      255.255.255.0    COST: 10
abcd.0001.0031.00-01* 0x00000001   0x289a       1179         34     0/0/0
 SOURCE      abcd.0001.0031.00
+IP-Extended  0.0.0.0       0.0.0.0         COST: 0
   *(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
         ATT-Attached, P-Partition, OL-Overload
```

风险的恢复方案

请按照配置规范进行配置。

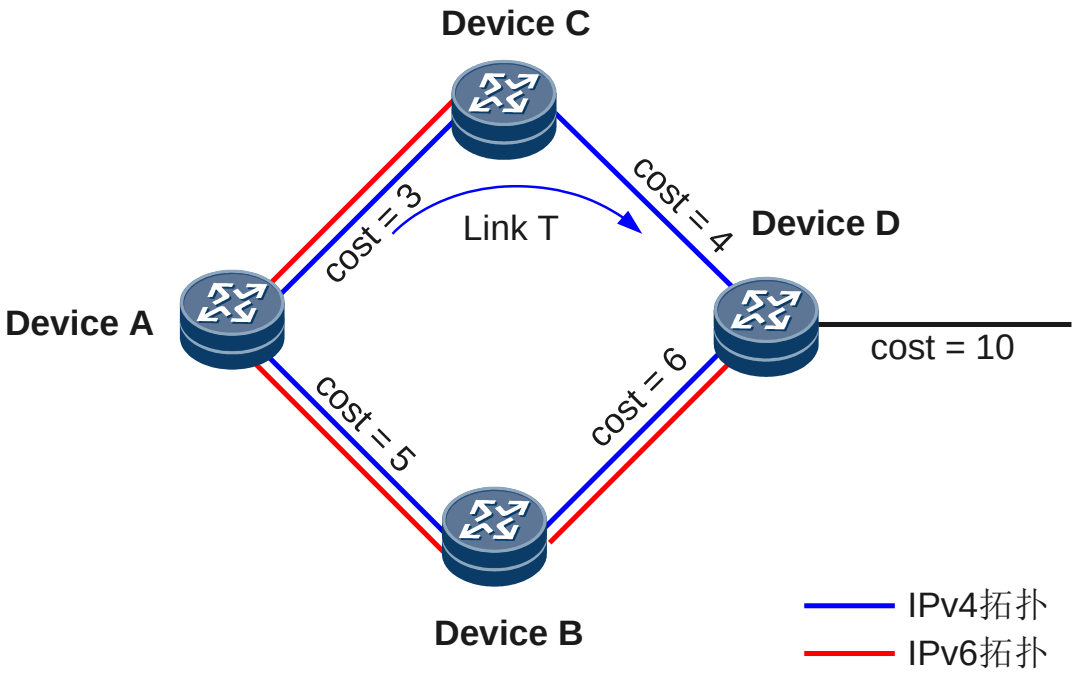
1.7.3.2 IS-IS 配置 IPv6 标准拓扑模式下使用 IPv6 拓扑

IS-IS IPv6 标准拓扑模式，IPv6 与 IPv4 共享最短路径树，如果最短路径树上存在出接口只支持 IPv4 协议的设备，则会在该设备上形成 IPv6 黑洞路由或者路由环路，导致 IPv6 业务受损。

应用场景

如图 1-10 所示，RouterA、RouterB、RouterC、RouterD 之间建立 IS-IS 邻居。IS-IS 部署 IPv4 和 IPv6 业务，使用 IPv6 标准拓扑。

图1-10 IPv6 标准拓扑模式下 IPv6 路由到 IPv4 单栈接口转发不通组网图



配置规范

网络中部署 IPv6 时，建议使用 IS-IS IPv6 拓扑，与 IS-IS IPv4 分开进行最短路径树计算。

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] display this
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0001.00
 #
 ipv6 enable topology ipv6
 #
#
return
```

非规范配置的风险

风险描述

当在 IS-IS 进程视图下，执行 **ipv6 enable topology standard** 命令使能 IS-IS 进程的 IPv6 能力，并指定拓扑类型为标准模式，如果 IS-IS 最短路径上存在只支持 IPv4 协议的接口，IPv6 业务流量到达只支持 IPv4 协议的设备后形成黑洞路由，导致业务不通。

业务现象如下：

IPv6 业务流量不通。

风险的判断方法

1. 在任意视图下，执行 **display current-configuration configuration isis** 命令，查看 IS-IS 进程视图下是否配置了 IPv6 标准拓扑模式。

```
<HUAWEI> display current-configuration configuration isis
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0001.00
 #
 ipv6 enable topology standard
 #
#
return
```

2. 在任意视图下，执行 **display isis** *process-id* **interface verbose** 命令，查看 IS-IS 接口状态以及拓扑模式，找到 **IPV4.State** 为 **UP**、**IPV6.State** 为 **Down**，并且 **Circuit MT State** 为 **Standard** 的接口。如下显示信息中为 GE1/0/0.1 接口。

```
<HUAWEI> display isis 1001 interface verbose
                  Interface information for ISIS(1001)
                  ------------------------------------
 Interface      Id     IPV4.State         IPV6.State     MTU  Type  DIS
 GE1/0/0.1   001        Up               Down        1497 L1/L2 --
  Circuit MT State           : Standard
  Circuit Parameters         : p2p
  Description               : HUAWEI, GigabitEthernet1/0/0.1 Interface
  SNPA Address              : 781d-ba56-fa3a
  IP Address                : 20.1.1.6
  IPV6 Link Local Address    :
  IPV6 Global Address(es)    :
  Csnp Timer Value          :  L12   10
  Hello Timer Value         :       10
  DIS Hello Timer Value      :
  ……
```

3. 在任意视图下，执行 **display current-configuration configuration interface** *interface-name* 命令，查看业务路径的出接口是否配置 IPv6 协议。下面显示中，GE1/0/0.1 接口下没有配置 **isis ipv6 enable**，说明存在问题。

```
<HUAWEI> display current-configuration interface GigabitEthernet1/0/0.1
#
interface GigabitEthernet1/0/0.1
 ip address 1.2.0.1 255.255.255.0
 isis enable 1
 isis circuit-type p2p
#
```

风险的恢复方案

在该接口下配置 IPv6。

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet1/0/0.1
[HUAWEI-interface-GigabitEthernet1/0/0.1] display this
#
interface GigabitEthernet1/0/0.1
 ipv6 enable
```

```
ip address 1.2.0.1 255.255.255.0
ipv6 address auto link-local
isis enable 1
isis ipv6 enable 1
isis circuit-type p2p
#
```

1.7.4 BGP 的配置规范

1.7.4.1 BGP 路由优先级配置规范

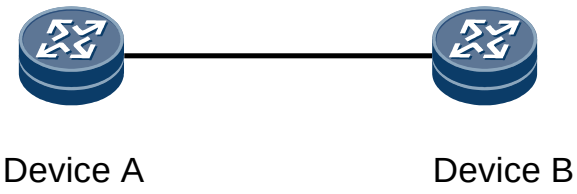
在设备上的静态路由通过 OSPF 协议发给对端设备后，对端又经过 BGP 协议发回给自己，如果在 BGP 视图配置了 **preference** 命令导致 BGP 路由协议优先级高于静态路由，就会引起 BGP 路由震荡。

应用场景

如图 1-11 所示组网中：

1. RouterA 将某一条静态路由引入到 OSPF 路由表后，通过 OSPF 协议发送给 RouterB。
2. RouterB 再将 OSPF 协议引入到 BGP 路由表中，然后通过 BGP 协议将该路由发回给 RouterA。
3. 此时如果 RouterA 的 BGP 视图下配置 **preference** 命令修改了路由协议的优先级，使得 BGP 路由协议的优先级比静态路由更高，就会导致静态路由不活跃。那么 OSPF 就会撤销这条路由，同时向 RouterB 发布撤销。
4. RouterB 的 BGP 路由也会撤销，同时向 RouterA 发布撤销。RouterA 的 BGP 路由一旦撤销，那么静态路由重新活跃，OSPF 重新引入该静态路由，回到步骤 1。这个过程会一直重复，导致路由震荡。

图1-11 修改 BGP 路由优先级导致 BGP 路由震荡组网图



配置规范

BGP 路由协议优先级低于静态路由优先级。

非规范配置的风险

风险描述

RouterA 和 RouterB 之间配置了 OSPF 和 BGP 邻居，RouterA 配置一条静态路由，并引入到 OSPF 路由表，RouterB 通过 **import-route** 或 **network** 命令将路由引入到 BGP 路

由表中，如果 RouterA 上 BGP 视图配置了 **preference** 命令修改了 BGP 路由协议的优先级，使得 BGP 路由协议的优先级比静态路由更高，则会出现路由震荡，使业务受到影响。

风险的判断方法

1. RouterA 上连续多次查看 IP 路由表路由，发现 IP 路由表静态和 IBGP 路由震荡交替。下面以 IP 地址为 20.0.0.0 为例。

```
<HUAWEI> display ip routing-table 20.0.0.0 verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
Destination: 20.0.0.0/8
    Protocol: Static          Process ID: 0
  Preference: 60                  Cost: 0
     NextHop: 0.0.0.0         Neighbour: 0.0.0.0
       State: Active Adv            Age: 04h36m27s
         Tag: 0               Priority: medium
       Label: NULL              QoSInfo: 0x0
  IndirectID: 0x0
 RelayNextHop: 0.0.0.0          Interface: NULL0
    TunnelID: 0x0                 Flags:  D
<HUAWEI> display ip routing-table 20.0.0.0 verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 2
Destination: 20.0.0.0/8
    Protocol: IBGP            Process ID: 0
  Preference: 20                  Cost: 1
     NextHop: 30.1.0.4       Neighbour: 30.1.0.4
       State: Active Adv Relied      Age: 00h00m00s
         Tag: 0               Priority: low
       Label: NULL              QoSInfo: 0x0
  IndirectID: 0x1ee
 RelayNextHop: 0.0.0.0          Interface: Vlanif503
    TunnelID: 0x0                 Flags: RD
Destination: 20.0.0.0/8
    Protocol: Static          Process ID: 0
  Preference: 60                  Cost: 0
     NextHop: 0.0.0.0         Neighbour: 0.0.0.0
       State: Inactive Adv           Age: 04h36m28s
         Tag: 0               Priority: medium
       Label: NULL              QoSInfo: 0x0
  IndirectID: 0x0
 RelayNextHop: 0.0.0.0          Interface: NULL0
    TunnelID: 0x0                 Flags:
```

2. RouterB 也进行连续多次查看 IP 路由表的路由，发现路由也在震荡。

```
<HUAWEI> display ip routing-table 20.0.0.0 verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
```

```
Destination: 20.0.0.0/8
    Protocol: O_ASE          Process ID: 20
  Preference: 150                 Cost: 1
     NextHop: 30.1.0.3       Neighbour: 0.0.0.0
       State: Active Adv           Age: 00h00m14s
         Tag: 1               Priority: medium
       Label: NULL              QoSInfo: 0x0
  IndirectID: 0x0
 RelayNextHop: 0.0.0.0         Interface: Vlanif503
    TunnelID: 0x0                Flags:  D
<HUAWEI> display ip routing-table 20.0.0.0 verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
Destination: 20.0.0.0/8
    Protocol: O_ASE          Process ID: 20
  Preference: 150                 Cost: 1
     NextHop: 30.1.0.3       Neighbour: 0.0.0.0
       State: Active Adv           Age: 00h00m00s
         Tag: 1               Priority: medium
       Label: NULL              QoSInfo: 0x0
  IndirectID: 0x0
 RelayNextHop: 0.0.0.0         Interface: Vlanif503
    TunnelID: 0x0                Flags:  D
<HUAWEI> display ip routing-table 20.0.0.0 verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
Destination: 20.0.0.0/8
    Protocol: O ASE          Process ID: 20
  Preference: 150                 Cost: 1
     NextHop: 30.1.0.3       Neighbour: 0.0.0.0
       State: Active Adv           Age: 00h00m01s
         Tag: 1               Priority: medium
       Label: NULL              QoSInfo: 0x0
  IndirectID: 0x0
 RelayNextHop: 0.0.0.0         Interface: Vlanif503
    TunnelID: 0x0                Flags:  D
```

风险的恢复方案

方案一：删除 RouterA 上 BGP 公网 IPv4 地址族的 **preference** 命令。

方案二：增大静态路由的优先级，使其高于 BGP 的优先级。

1.8 IP 组播

1.8.1 PIM 的配置规范

1.8.1.1 三层组播的备路径或等价链路接口要使能 PIM 功能

在三层组播的备路径或等价链路接口中，需要配置 PIM 使能，否则切换时可能导致业务中断。

应用场景

组播业务存在主备链路或等价路由。

配置规范

在三层组播的备路径或等价链路接口中，需要使能 PIM 功能。

非规范配置的风险

风险描述

主备链路或等价链路中，当前在用的链路配置了 PIM 使能而其他链路没有配置 PIM 使能。当由配置、路由、链路等变化导致组播路径切换时，切换后的路径没有配置 PIM，业务切换到缺少配置的路径时会出现组播业务中断的现象。

业务现象如下：

切换后 PIM 路由无法建立，组播业务不通。

风险的判断方法

在用户视图下，执行 **display pim interface** 命令，查看组播业务主备链路或等价链路的接口是否配置了 PIM 使能。

如果指定的接口可以查到，则说明配置正常，否则，缺少配置。如下显示说明 Ethernet1/0/0 接口使能了 PIM 功能。

```
<HUAWEI> display pim interface Ethernet1/0/0
 VPN-Instance: public net
 Interface     State   NbrCnt   HelloInt   DR-Pri    DR-Address
 Ethernet1/0/0  up     1       30         1         1.1.1.1
```

风险的恢复方案

在缺少配置的接口视图下，使能 PIM 使能。

1.9 MPLS

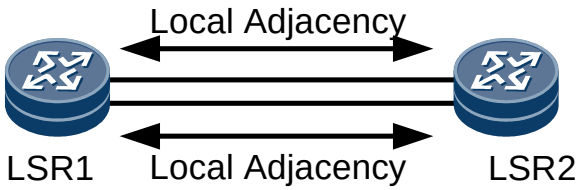
1.9.1 MPLS LDP 的配置规范

1.9.1.1 多链路或本远共存场景的参数配置规范

两个 LSR 之间存在多条链路或本远共存时，LDP 会话最终只能建立在一条链路上或者无法建立成功。

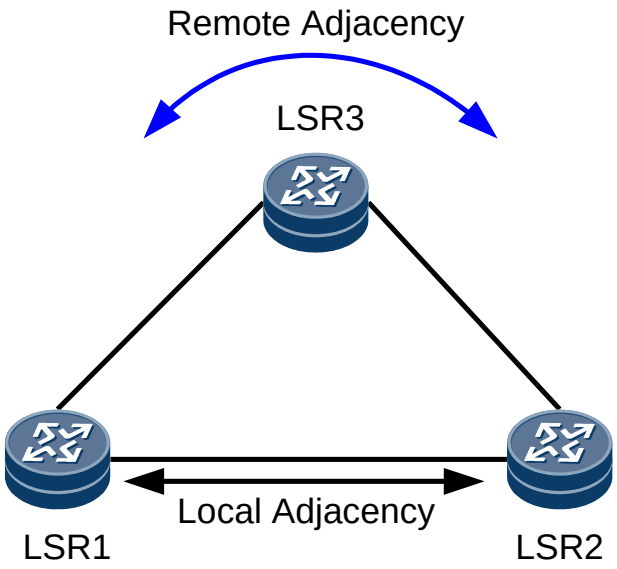
应用场景 1 – 两个 LSR 之间存在多链路的场景

图1-12 多链路组网图



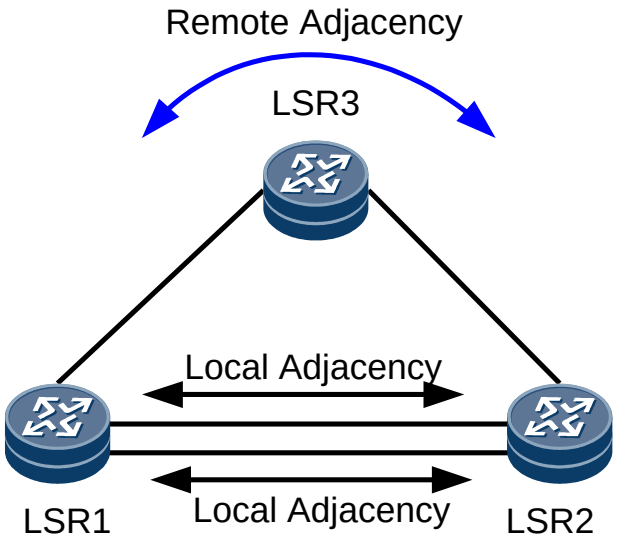
应用场景 2 – 两个 LSR 之间存在本远共存的场景

图1-13 本远共存组网图



应用场景 3 - 两个 LSR 之间既存在多链路场景又存在本远共存的场景

图1-14 多链路与本远共存组网图



配置规范

上述场景中，LDP 接口视图和 LDP 远端对等体视图中参数需配置一致。

1. 如果同一个 LDP 对等体的所有本地接口视图中，部分配置了 **mpls ldp transport-address** 命令，或全部都配置了 **mpls ldp transport-address** 命令但没有指定相同的接口地址，则需要将所有本地接口的传输地址指定成同一个地址或者全都不配置以使用默认值。
2. 如果同一个私网 LDP 对等体的所有本地接口视图中，没有全部指定相同的传输地址 **mpls ldp transport-address** 命令，则需要将所有本地接口的传输地址指定成同一个地址。
3. 如果同一个 LDP 对等体的所有本地接口视图和 LDP 远端对等体视图中，部分配置了 **mpls ldp timer keepalive-hold** 命令，或者全部都配置了 **mpls ldp timer keepalive-hold** 命令但没有指定相同的参数，则需要将所有本地接口视图和 LDP 远端对等体视图的 keepalive-hold 参数配置相同值或者全都不配置以使用默认值。
4. 如果同一个 LDP Peer 的所有本地接口视图和 LDP 远端对等体视图中，部分配置了 **mpls ldp timer keepalive-send** 命令，或者全部都配置了 **mpls ldp timer keepalive-send** 命令但没有指定相同的参数，则需要将所有本地接口视图和 LDP 远端对等体视图的 keepalive-send 参数配置相同值或者全都不配置以使用默认值。
5. 如果同一个 LDP 对等体的所有本地接口视图和 LDP 远端对等体视图中，部分配置了 **mpls ldp advertisement** 命令，或者全部都配置了 **mpls ldp advertisement** 命令但没有指定相同的参数，则需要将所有本地接口视图和 LDP 远端对等体视图的标签发布模式指定成同一种或者全都不配置以使用默认值。
6. 如果同一个 LDP 对等体的所有本地接口视图和 LDP 远端对等体视图中，部分配置了 **mpls ldp local-lsr-id** 命令，或者全部都配置了 **mpls ldp local-lsr-id** 命令但没

有指定相同的接口地址，则需要将所有本地接口视图和 LDP 远端对等体视图的 local-lsr-id 指定成同一个地址或者全都不配置以使用默认值。

非规范配置的风险

风险描述

用户视图下，执行命令 **display mpls ldp adjacency all**，如果查看到设备上存在 Peer ID 相同的 LDP 邻接体，则 LDP 会话的部分发现源无法绑定，导致不能形成负载分担的 LDP LSP 或者本远共存会话保护，而且由于 LDP 会话建立不成功会导致承载业务受损。

风险的判断方法

1. 在任意视图下，执行命令 **display mpls ldp adjacency all** 查询 LDP 邻接体信息。如果没有回显信息，则说明不涉及本问题。否则需要继续检查。

   如下显示中，加粗字体表示相同 Peer ID 存在多链路或本远共存的情况，需要排查 1.1.1.2、1.1.1.3 和 6.6.6.6 的 Peer ID。

```
<HUAWEI> display mpls ldp adjacency all
LDP Adjacency Information in Public Network
 Codes: R: Remote Adjacency, L: Local Adjacency
 A '*' before an adjacency means the adjacency is being deleted.
 ------------------------------------------------------------------------------
 SN   SourceAddr     PeerID      VrfID AdjAge(DDDD:HH:MM) RcvdHello Type
 ------------------------------------------------------------------------------
  1   2.2.2.1       1.1.1.2      0    0000:00:37        449       L
  2   2.2.1.1       1.1.1.4      0    0000:00:04        57        L
  3   1.1.1.2      1.1.1.2      0    0000:00:09        148       R
  4   3.3.3.3       1.1.1.2      0    0000:00:00        11        L
  5   2.2.3.1       1.1.1.3      0    0000:00:20        258       L
  6   1.1.1.2      1.1.1.3      0    0000:00:20        76        R
 ------------------------------------------------------------------------------
LDP Adjacency Information in VPN-Instance: vpn1
 Codes: R: Remote Adjacency, L: Local Adjacency
 A '*' before an adjacency means the adjacency is being deleted.
 ------------------------------------------------------------------------------
 SN   SourceAddr    PeerID       VrfID AdjAge(DDDD:HH:MM) RcvdHello Type
 ------------------------------------------------------------------------------
  1   2.3.2.1       6.6.6.6        1    0000:00:08        103       L
  2   2.4.2.1       6.6.6.6        1    0000:00:02        33        L
 ------------------------------------------------------------------------------
TOTAL: 8 Record(s) found.
```

2. 对相同 Peer ID 的多个邻接体进行排查。

   # 如果是本地邻接体，在任意视图下执行命令 **display ip routing-table** *ip-address* 查看对应的出接口。以 Peer ID 为 1.1.1.2 为例，有两个本地邻接体 2.2.2.1 和 3.3.3.3，有一个远端邻接体 1.1.1.2。

```
<HUAWEI> display ip routing-table 2.2.2.1
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
```

```
2.2.2.1/32  Direct  0    0          D   127.0.0.1      GigabitEthernet1/0/0
```

在任意视图下执行命令 **display current-configuration interface** *interface-type interface-number* 查看接口的配置信息。如下显示信息说明接口下使能了 LDP。

```
<HUAWEI> display current-configuration interface GigabitEthernet 1/0/0
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 2.2.2.1 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
 dcn
#
```

如果是私网路由，在任意视图下执行命令 **display ip routing-table vpn-instance** *vpn-instance-name ip-address*，查看对应的出接口。

```
<HUAWEI> display ip routing-table vpn-instance vpn1 2.3.2.1
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : vpn1
Summary Count : 1
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
2.4.2.0/24        Direct  0    0           D   10.5.6.5        Ethernet0/0/1
```

如果是远端邻接体，在任意视图下执行命令 **display mpls ldp remote-peer peer-id** *lsr-id*，查看对应的 LDP 远端对等体视图名称。

```
<HUAWEI> display mpls ldp remote-peer peer-id 1.1.1.2

                    LDP Remote Entity Information
 ------------------------------------------------------------------------------
 Remote Peer Name  : 5to3
 Remote Peer IP    : 1.1.1.2         LDP ID       : 1.1.1.1:0
 Transport Address : 1.1.1.1          Entity Status : Active

 Configured Keepalive Hold Timer : 45 Sec
 Configured Keepalive Send Timer : ---
 Configured Hello Hold Timer     : 45 Sec
 Negotiated Hello Hold Timer     : 45 Sec
 Configured Hello Send Timer     : ---
 Configured Delay Timer         : 10 Sec
 Hello Packet sent/received      : 272/271
 Label Advertisement Mode        : Downstream Unsolicited
 Remote Peer Deletion Status     : No
 Auto-config                  : ---
 ------------------------------------------------------------------------------
```

在任意视图下执行命令 **display current-configuration configuration mpls-ldp-remote** *name* 查看 LDP 远端对等体视图的配置信息。如下显示信息表示配置了远端邻接体。

```
<HUAWEI> display current-configuration configuration mpls-ldp-remote 5to3
#
mpls ldp remote-peer 5to3
 remote-ip 1.1.1.2
#
return
```

3. 根据上面方法找到的接口视图或 LDP 远端对等体视图下存在如下列举的任意情况，即表明可能存在本问题。
   a. 同一个 LDP 对等体的所有本地接口视图中，部分配置了 **mpls ldp transport-address** 命令，或者全部都配置了 **mpls ldp transport-address** 命令但没有指定相同的接口地址。
   b. 同一个私网 LDP 对等体的所有本地接口视图中，没有通过 **mpls ldp transport-address** 命令全部指定相同的传输地址。
   c. 同一个 LDP 对等体的所有本地接口视图和 LDP 远端对等体视图中，部分配置了 **mpls ldp timer keepalive-hold** 命令，或者全部都配置了 **mpls ldp timer keepalive-hold** 命令但没有指定相同的参数。
   d. 同一个 LDP 对等体的所有本地接口视图和 LDP 远端对等体视图中，部分配置了 **mpls ldp timer keepalive-send** 命令，或者全部都配置了 **mpls ldp timer keepalive-send** 命令但没有指定相同的参数。
   e. 同一个 LDP 对等体的所有本地接口视图和 LDP 远端对等体视图中，部分配置了 **mpls ldp advertisement** 命令，或者全部都配置了 **mpls ldp advertisement** 命令但没有指定相同的参数。
   f. 同一个 LDP 对等体的所有本地接口视图和 LDP 远端对等体视图中，部分配置了 **mpls ldp local-lsr-id** 命令，或者全部都配置了 **mpls ldp local-lsr-id** 命令但没有指定相同的接口地址。

风险的恢复方案

请按照配置规范进行配置。

1.9.1.2 接口下需要配置 LDP-IGP 联动

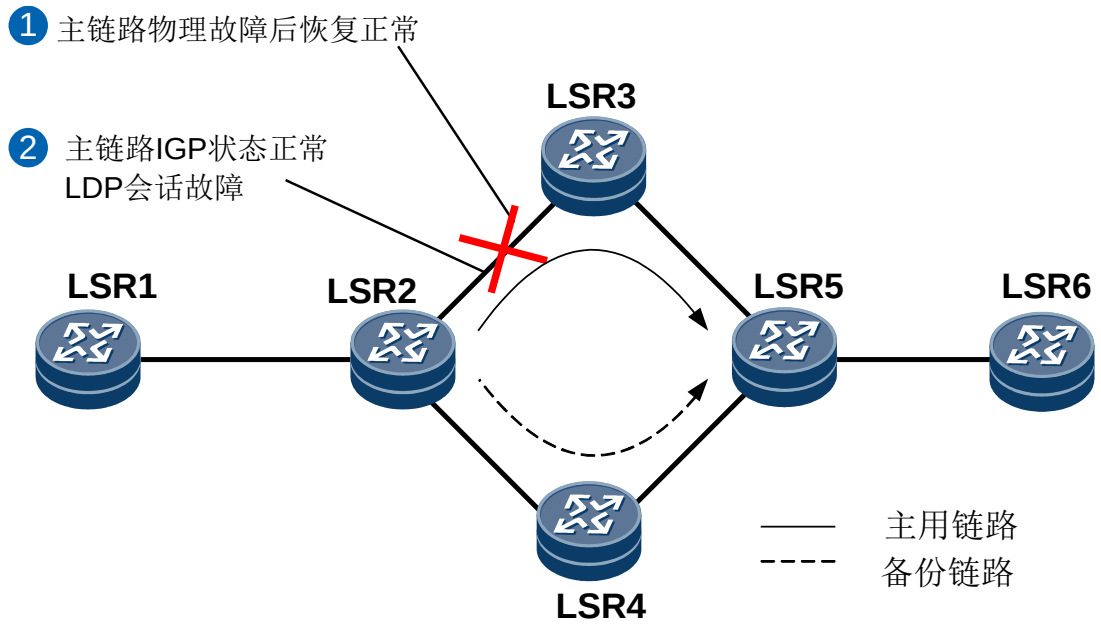
设备的接口上使能了 LDP 能力但未使能 LDP-IGP 联动，在 LDP 会话震荡或链路故障恢复业务回切等场景中，导致 LDP 隧道承载的业务受损或中断。

应用场景

由于 LDP 的收敛速度依赖于 IGP 路由的收敛，即 LDP 的收敛速度比 IGP 的收敛速度慢，因此如图 1-15 所示，存在主备链路的组网中有如下问题：

- 当主链路发生故障时，IGP 路由和 LSP 均切换到备份链路上（常通过 LDP FRR 实现）。但当主链路从故障中恢复时，IGP 会先于 LDP 切换回主链路，因此造成 LSP 流量丢失。
- 当主链路 IGP 运行正常，但主链路节点间的 LDP 会话发生故障时，IGP 路由仍然使用主链路，而主链路的 LSP 被删除。同时，由于备份链路不存在 IGP 优选路由，故 LSP 无法在备份链路建立，导致 LSP 流量丢失。

图1-15 LDP 接口下没有配置 LDP-IGP 联动导致业务受损组网图



配置规范

配置了 MPLS LDP 能力的接口视图下补充配置 LDP 和 IGP 同步功能，并将 hold-max-cost 定时器的值配置为 infinite。常见的 IGP 协议包含 IS-IS 和 OSPF，可根据现网业务需要决定配置哪种协议对应的联动能力。

非规范配置的风险

风险描述

在任意视图下，执行命令 **display current-configuration interface**，查看配置了 LDP 能力的接口，发现接口下没有配置 LDP 和 IGP 同步功能。此时，如果在用户视图下，执行命令 **display mpls lsp protocol ldp include** *ip-address* **32** 查询不到信息，表明承载业务的 LDP LSP 未建立成功。在 LDP 会话震荡或链路故障恢复业务回切等场景中，会出现 LDP LSP 承载的业务恢复较慢或长时间不能恢复，导致 LDP LSP 承载的业务受损或中断。

风险的判断方法

在任意视图下，执行命令 **display current-configuration interface** 查看接口配置。如果接口视图下仅配置了 MPLS LDP，但没有配置 LDP 和 IGP 同步功能，则可能存在问题。

如下显示信息说明接口视图下配置了 MPLS LDP，同时配置了 LDP 和 IS-IS 同步功能命令、LDP 和 OSPF 同步功能命令。

<HUAWEI> **display current-configuration interface**

```
#
interface GigabitEthernet1/0/0
```

```
 undo shutdown
 mtu 9192
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
isis ldp-sync
 isis timer ldp-sync hold-max-cost infinite
 ospf ldp-sync
 ospf timer ldp-sync hold-max-cost infinite
 mpls
 mpls ldp
 dcn
 negotiation auto
#
……
```

风险的恢复方案

配置了 MPLS LDP 能力的接口视图下补充配置 LDP 和 IGP 同步功能，并将 hold-max-cost 定时器的值配置为 infinite。

```
<HUAWEI> display current-configuration interface
#
interface GigabitEthernet1/0/0
 undo shutdown
 mtu 9192
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
isis ldp-sync
 isis timer ldp-sync hold-max-cost infinite
 ospf ldp-sync
 ospf timer ldp-sync hold-max-cost infinite
 mpls
 mpls ldp
……
```

1.9.2 MPLS TE 的配置规范

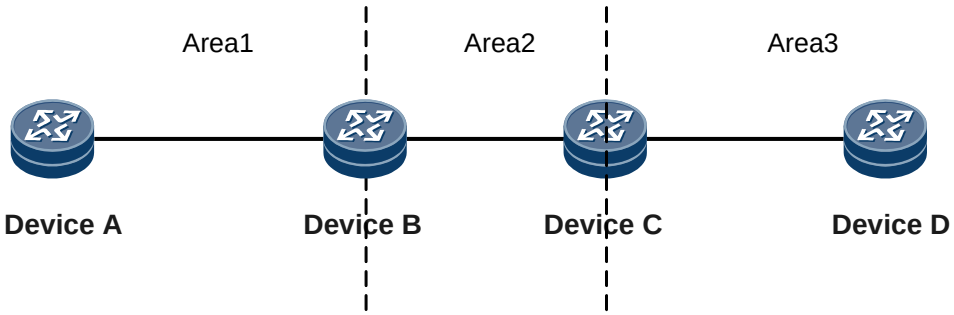
1.9.2.1 跨 IGP 域建立 TE 隧道需要配置显示路径

建立 TE 隧道经过多个 IGP 域时，需要隧道配置包含跨域节点 IP 地址的显示路径，同时隧道 Ingress 节点和跨域节点都使能 CSPF，否则，隧道可能建立失败。

应用场景

跨 IGP 域建立 TE 隧道。

图1-16 跨 IGP 域建立 TE 隧道组网图



如图 1-16 所示，TE 隧道从 RouterA 建到 RouterD，其中 RouterA 出接口、RouterB 入接口属于 IGP Area1，RouterB 出接口和 RouterC 入接口属于 IGP Area2，RouterC 出接口和 RouterD 入接口属于 IGP Area3，RouterB 和 RouterC 为跨域节点。

配置规范

建立 TE 隧道经过多个 IGP 域时，需要隧道配置包含跨域节点 IP 地址的显示路径，同时隧道 Ingress 节点和跨域节点设备都使能 CSPF。

非规范配置的风险

风险描述

建立 TE 隧道经过多个 IGP 域时，如果隧道没有配置包含跨域节点 IP 地址的显示路径且隧道经过的各设备都配置了 CSPF，则会导致隧道建立失败。

风险的判断方法

1. 在用户视图下，执行 **display current-configuration configuration mpls** 命令，查看全局 MPLS 配置。

   由以下显示信息可以看出，配置了 MPLS TE 和 MPLS TE CSPF。

```
<HUAWEI> display current-configuration configuration mpls
#
mpls lsr-id 1.1.1.1
#
mpls
 mpls te
 mpls rsvp-te
 mpls te cspf
#
return
```

2. 用户视图下，执行 **display current-configuration interface** *interface-type interface-number* 命令，查看隧道的配置信息，获取隧道的目的地址和显式路径。

   由以下显示信息可以看出，隧道的目的地址为 4.4.4.4,显示路径为 huawei。

```
<HUAWEI> display current-configuration interface Tunnel 0/0/1
#
interface Tunnel0/0/1
```

```
 tunnel-protocol mpls te
 destination 4.4.4.4
 mpls te record-route
 mpls te backup hot-standby
 mpls te tunnel-id 1
 mpls te path explicit-path huawei
#
return
```

3. 在用户视图下，执行 **display mpls te cspf tedb all** 命令，查看 CSPF TEDB 信息，如果没有隧道的目的地址，就可以确定是 IGP 跨域场景。

   由以下显示信息可以看出，TEDB 没有 4.4.4.4 的信息，是 IGP 跨域场景。

```
<HUAWEI> display mpls te cspf tedb all
Maximum Nodes Supported: 2000   Current Total Node Number: 4
Maximum Links Supported: 8000   Current Total Link Number: 6
Maximum SRLGs supported: 10000  Current Total SRLG Number: 0
Id    Router-Id       IGP     Process-Id    Area          Link-Count
1     1.1.1.1         ISIS    1             Level-1       2
2     2.2.2.2         ISIS    1             Level-1       1
3     1.1.1.1         ISIS    1             Level-2       2
4     2.2.2.2         ISIS    1             Level-2       1
```

4. 检查隧道的显示路径是否正确。
   - 如果没有配置显示路径，需要配置包含跨 IGP 域节点 IP 地址的显示路径。
   - 如果配置了显示路径，用户视图下，执行 **display current-configuration configuration explicit-path** *explicit-name* 命令，查看显示路径信息，确认显示路径是否包含跨 IGP 域节点的 IP 地址。

```
<HUAWEI> display current-configuration configuration explicit-path test
#
explicit-path test
 next hop 192.168.1.2 include loose
#
```

风险的恢复方案

请按照配置规范进行配置。

1.9.2.2 RSVP-TE GR 功能需要在 RSVP-TE 接口下配置 RSVP-TE Hello

部署 RSVP-TE GR 时，全局 MPLS 视图下配置 **mpls rsvp-te hello support-peer-gr** 或 **mpls rsvp-te hello full-gr** 后，还需要在使能了 RSVP-TE 的接口下配置 **mpls rsvp-te hello**。

应用场景

部署 RSVP-TE GR 场景，详细场景描述请参见配置 RSVP GR。

配置规范

部署 RSVP-TE GR 时，RSVP-TE 接口下需要配置 RSVP-TE Hello。

非规范配置的风险

风险描述

RSVP-TE 接口下没有配置 RSVP-TE Hello，会导致 RSVP-TE GR 功能失效，当 RSVP 节点进行主备倒换时，该节点与邻居之间的 RSVP 邻接关系会因信令协议超时而被拆除，从而删除 CR-LSP，导致 CR-LSP 承载的业务出现中断。

风险的判断方法

1. 在用户视图下，执行 **display current-configuration configuration mpls** 命令，查看全局 MPLS 配置中是否配置了 **mpls rsvp-te hello support-peer-gr** 或者 **mpls rsvp-te hello full-gr**，以判断是否部署了 GR。以下显示说明部署了 GR。

```
<HUAWEI> display current-configuration configuration mpls

#
mpls lsr-id 1.1.1.1
#
mpls
 mpls te
 mpls rsvp-te
 mpls rsvp-te hello
 mpls rsvp-te hello support-peer-gr
 mpls te cspf
#
return
```

2. 在用户视图下，执行 **display current-configuration interface** 命令，查看接口是否配置了 **mpls rsvp-te hello**。如果接口下没有配置 **mpls rsvp-te hello**，则说明存在该案例描述的问题。

```
<HUAWEI> display current-configuration interface
#
interface Ethernet3/0/0
 undo shutdown
 ip address 192.168.21.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
 mpls rsvp-te hello
#
```

风险的恢复方案

恢复措施

在 Ethernet3/0/0 接口视图下执行 **mpls rsvp-te hello** 命令，启动接口的 Hello 机制。

1.9.2.3 IGP 多进程或多区域场景 CSPF 算路与预期不符

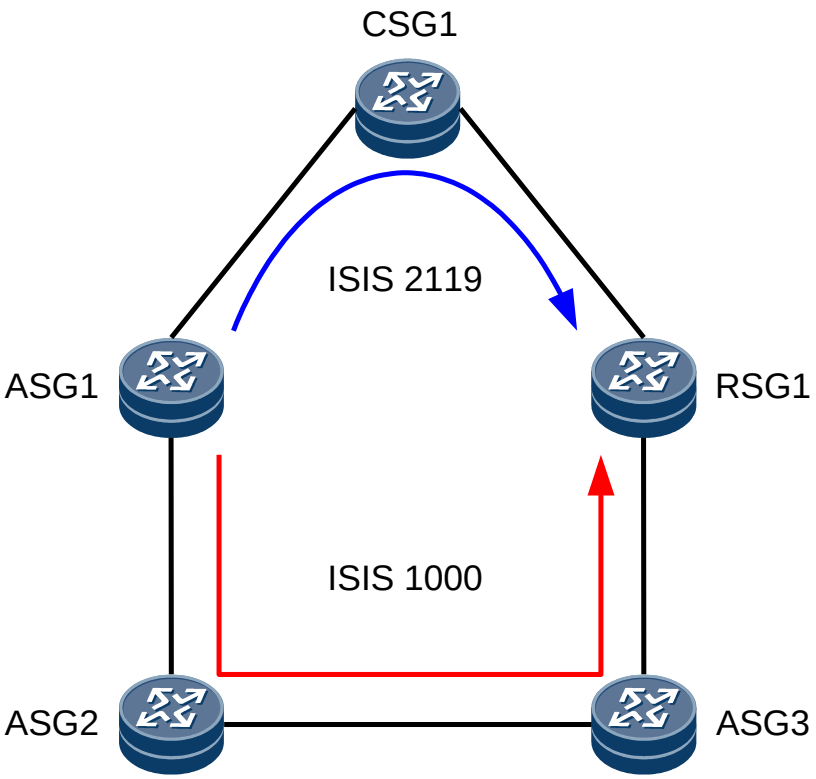
设备上部署多个使能了 MPLS TE 的 IGP 进程时，CSPF 在计算 TE 隧道路径时，不能在多个 IGP 进程之间计算出最优路径，在单个进程内计算出的最优路径不能保证与客户的预期路径一致，可能导致 TE 隧道承载的业务拥塞或中断。

应用场景

如图 1-17 所示，设备上部署 TE 隧道，隧道可能经过的多条路径分属不同的 IGP 进程。

以 IS-IS 协议为例，TE 隧道从 ASG1 建到 RSG1，头尾节点之间的路径中存在多个 IS-IS 进程（IS-IS 1000、IS-IS 2119）。正常情况下隧道路径如图 1-17 红色线所示，当接入环 IS-IS 2119 发生路由震荡，等到 TE 重优化时间后，隧道路径绕行 CSG，如图 1-17 蓝色线所示。

图1-17 IGP 多进程或多区域场景 CSPF 算路与预期不符问题组网图



配置规范

IGP 多进程使能了 MPLS TE 时，会先后通知 CSPF 更新 TEDB 信息。CSPF 在计算 TE 隧道路径时，以最后更新到 TEDB 中的 IGP 进程为准。不能在多个 IGP 进程之间通过比较不同进程的 IGP Cost 来计算出最优路径，而在单个进程内计算出的最优路径不能保证与客户的预期路径一致。

在配置时，主要有以下两种方案。

1. 主用方案：系统视图下配置显式路径，并在 TE 隧道下使用该显式路径。显式路径名称 pri1 为例。

   # 在系统视图下，执行命令 **explicit-path pri1** 配置显式路径。

   ```
   <HUAWEI> system-view
   [HUAWEI] explicit-path pri1
   ```

   # TE 隧道接口视图下，执行命令 **mpls te path explicit-path pri1** 配置显式路径。

   ```
   [HUAWEI] interface Tunnel 0/0/1
   [HUAWEI-Tunnel0/0/1] tunnel-protocol mpls te
   [HUAWEI-Tunnel1/0/0] mpls te path explicit-path pri1
   [HUAWEI-Tunnel1/0/0] mpls te commit
   ```

   说明

   如果现网存在 IGP 跨域的场景，在配置显式路径时需要包含跨域边界的设备，且在该设备上需要使能 CSPF。

   Hot-Standby LSP 也需要配置显式路径约束，否则在同样场景下也可能存在本问题。

2. 备选方案：在 MPLS 视图下配置 **mpls te cspf preferred-igp** 命令，使 CSPF 在算路时可以优先选择指定的 IGP 进程。

   # 如果 IGP 路由使用 ISIS 分进程方案，则在 MPLS 视图下，使用命令行 **mpls te cspf preferred-igp isis 1** 配置优选 ISIS 进程。

   ```
   <HUAWEI> system-view
   [HUAWEI] mpls
   [HUAWEI-mpls] mpls te cspf preferred-igp isis 1
   ```

   # 如果 IGP 路由使用 OSPF 分进程方案，则在 MPLS 视图下，使用命令行 **mpls te cspf preferred-igp ospf 1 area 0.0.0.0** 配置优选 OSPF 进程和域（参数 area 不是必配）。

   ```
   <HUAWEI> system-view
   [HUAWEI] mpls
   [HUAWEI-mpls] mpls te cspf preferred-igp ospf 1 area 0.0.0.0
   ```

   说明

   本方案只建议用作备选方案。因为即使配置了优选的 IGP 进程，若 CSPF 使用优选的 IGP 进程算路失败（链路临时有震荡等问题），会继续选择其他进程进行算路。若此时用其他进程算路成功，则会创建 LSP，而想要切回到优选的 IGP 进程中，则需要等待 TE 重优化，触发 CSPF 重新算路。因此本方案并不一定能彻底解决本问题。

   另外，配置的优选进程只能配置一个。如果不同 TE 隧道需要优选的 IGP 进程不同（比如 RSG 属于多个汇聚环，每个汇聚环的 IGP 进程都不同）的情况下，不适用本方案。

非规范配置的风险

风险描述

如果源宿设备上部署了 TE 隧道和 IGP 多进程，且源宿设备上的 TE 隧道路径为根据 IGP 路径自动计算，未部署显式路径或者其它约束，则会导致 TE 隧道经过的路径与预期不一致，业务拥塞或中断。

风险的判断方法

1. 查询是否使能 MPLS TE/RSVP-TE/CSPF。

在用户视图下，执行命令 **display current-configuration configuration mpls**。在使能了 MPLS TE、RSVP-TE 以及 CSPF 的情况下，可能会出现本案例描述的问题，需要进一步进行检查；如果没有使能其中任意一项，则问题不存在。

```
<HUAWEI> display current-configuration configuration mpls
#
mpls lsr-id 2.2.2.2
mpls
 mpls te
 mpls rsvp-te
 mpls te cspf
#
return
```

2. 查询是否存在多个 IS-IS/OSPF 进程。

   # 在用户视图下，使用命令行 **display current-configuration configuration isis** 或 **display current-configuration configuration ospf**。如果存在多个 IS-IS/OSPF 进程，可能会存在问题，还需要进一步进行检查。

```
<HUAWEI> display current-configuration configuration isis
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 10.0000.0002.0001.00
 traffic-eng level-2
#
isis 2
 is-level level-2
 cost-style wide
 network-entity 10.0000.0002.0002.00
 traffic-eng level-2
…
#
<HUAWEI> display current-configuration configuration ospf
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 1.1.1.2 0.0.0.0
  network 2.2.2.1 0.0.0.0
  network 11.2.1.0 0.0.0.255
  network 20.20.20.20 0.0.0.0
  mpls-te enable
#
ospf 2
 area 0.0.0.0
  network 101.1.10.0 0.0.0.255
  network 101.1.11.0 0.0.0.255
…
```

3. 查询 IS-IS/OSPF 下是否使能了 TE。

   # 使用的命令和视图与步骤 2 相同。如果超过 1 个 IS-IS/OSPF 进程使能了 TE，可能会存在问题，还需要继续步骤 5 的检查；如果只有 1 个 OSPF 进程使能 TE，还需要继续步骤 4 的检查；如果仅配置 1 个 IS-IS 进程使能 TE，则不存在问题。

```
<HUAWEI> display current-configuration configuration isis
```

```
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 10.0000.0002.0001.00
 traffic-eng level-2
#
<HUAWEI> display current-configuration configuration ospf
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 1.1.1.2 0.0.0.0
  network 2.2.2.1 0.0.0.0
  network 11.2.1.0 0.0.0.255
  network 20.20.20.20 0.0.0.0
  mpls-te enable
```

4. 查询 OSPF 是否配置了多个域。

   # 在用户视图下，执行命令 **display current-configuration configuration ospf**。如果存在多个 OSPF 区域，且每个域都使能了 MPLS TE，可能会存在问题，则需要进一步进行检查。

```
<HUAWEI> display current-configuration configuration ospf
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 1.1.1.2 0.0.0.0
  mpls-te enable
area 0.0.0.9
 network 1.1.1.9 0.0.0.0
 mpls-te enable
```

5. 查询隧道实际经过的路径。

   查询出隧道实际经过的路径后，对比规划的路径，查看是否一致，若不一致，则表明出现了本案例描述的问题。

   - 在用户视图下，执行命令 **display current-configuration interface Tunnel 0/0/1** 查询是否配置了记录路由。隧道接口以 Tunnel0/0/1 为例。

```
<HUAWEI> display current-configuration interface Tunnel 0/0/1
#
interface Tunnel0/0/1
 tunnel-protocol mpls te
 destination 4.4.4.4
 mpls te record-route label
 mpls te backup hot-standby
 mpls te tunnel-id 111
#
Return
```

   - 如果配置了 **mpls te record-route label** 命令，则在用户视图下，执行命令 **display mpls te tunnel path Tunnel0/0/1** 查询隧道实际经过的路径。

```
<HUAWEI> display mpls te tunnel path Tunnel0/0/1
 Tunnel Interface Name : Tunnel0/0/1
 Lsp ID : 3.3.3.3 :100 :3
```

```
Hop Information
 Hop 0   3.3.3.3
 Hop 1   10.1.1.1
 Hop 2   10.1.1.2
 Hop 3   2.2.2.2
```

- 如果没有配置 **mpls te record-route label** 命令，则用户视图下，执行命令 **tracert lsp te Tunnel 0/0/1** 查询隧道实际经过的路径。

```
<HUAWEI> tracert lsp te Tunnel 0/0/1
 LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel0/0/1, press
CTRL C to break.
 TTL   Replier          Time    Type     Downstream
 0                           Ingress   10.1.2.1/[3 ]
 1     3.3.3.3          32 ms   Egress
```

风险的恢复方案

请按照配置规范进行配置。

1.9.2.4 TE 隧道建议部署在主控板

在网络部署 TE 隧道时，需要把 TE 隧道部署在主控板。如果部署在接口板，Tunnel 所在接口板故障，会导致 TE 保护不生效，业务中断。

应用场景

部署 TE 隧道。

配置规范

在网络部署 TE 隧道时，把 TE 隧道部署在主控板。

非规范配置的风险

如果 TE Tunnel 部署在接口板，且接口板故障或拔出，会导致 TE 保护不生效，业务中断。

风险的判断方法

1. 在用户视图下，执行命令 **display ip interface brief Tunnel** 查看所有隧道接口，找到没有部署在主控板上的隧道接口。

   下面显示信息中，根据 Tunnel 接口编号发现 Tunnel1/0/0 部署在 1 号接口板，没有部署在主控板。

```
<HUAWEI> display ip interface brief Tunnel
*down: administratively down
!down: FIB overload down
^down: standby
(l): loopback
(s): spoofing
(d): Dampening Suppressed
(E): E-Trunk down
The number of interface that is UP in Physical is 181
```

```
The number of interface that is DOWN in Physical is 0
The number of interface that is UP in Protocol is 3
The number of interface that is DOWN in Protocol is 178

Interface                   IP Address/Mask     Physical   Protocol
Tunnel0/0/1                 1.1.2.7/32          up         down
Tunnel0/0/2                 1.1.2.7/32          up         down
Tunnel0/0/3                 1.1.2.7/32          up         down
Tunnel0/0/4                 1.1.2.7/32          up         down
Tunnel0/0/5                 1.1.2.7/32          up         down
Tunnel0/0/6                 1.1.2.7/32          up         down
Tunnel0/0/7                 1.1.2.7/32          up         down
Tunnel1/0/0                 1.1.2.7/32          up         up
```

2. 在用户视图下，执行>**display current-configuration interface** *interface-name* 命令，查看没有部署在主控板上隧道接口的配置。

   以下显示信息说明该隧道是 TE 隧道，存在本案例描述的问题。

```
<HUAWEI> display current-configuration interface Tunnel1/0/0
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack0
 tunnel-protocol mpls te
 destination 1.1.2.9
 mpls te tunnel-id 2000
 mpls te commit
```

风险的恢复方案

在网络部署 TE 隧道时，把 TE 隧道部署在主控板。

1.9.2.5 TE Tunnel 配置路由发布功能后，需要同时配置 LDP Remote 会话

LDP over TE 场景下，TE Tunnel 接口视图下配置 **mpls te igp advertise** 或 **mpls te igp advertise shortcut** 命令，使能路由发布功能后，针对该 Tunnel 的 **destination** 需要配置 LDP Remote 会话。

应用场景

LDP over TE 场景下，存在 TE Tunnel 接口，且该接口下配置了 **mpls te igp advertise** 或 **mpls te igp advertise shortcut** 命令。

配置规范

LDP over TE 场景下，TE Tunnel 接口视图下配置 **mpls te igp advertise** 或 **mpls te igp advertise shortcut** 命令后，针对该 Tunnel 的 **destination** 需要配置 LDP Remote 会话。

非规范配置的风险

风险描述

如果不配置 LDP Remote 会话，LDP LSP 无法建立，导致业务中断。

风险的判断方法

1. 在用户视图，执行 **display current-configuration interface** *interface-name* 命令，查看 Tunnel 中存在 **mpls te igp advertise** 或 **mpls te igp advertise shortcut** 配置，并记录 **destination** 地址。

```
<HUAWEI> display current-configuration interface Tunnel0/0/1
#
interface Tunnel0/0/1
 ip address unnumbered interface LoopBack0
 tunnel-protocol mpls te
 destination 10.1.1.1
 mpls te tunnel-id 2000
 mpls te igp advertise
 mpls te commit
```

2. 在用户视图，执行 **display current-configuration configuration mpls-ldp-remote** 命令，如果没有跟上述 **destination** 地址相同的 **remote-ip**，则存在本案例中描述的风险。

```
<HUAWEI> display current-configuration configuration mpls-ldp-remote
#
mpls ldp remote-peer test
remote-ip 10.10.10.1
#
return
```

风险的恢复方案

TE Tunnel 接口视图下配置 **mpls te igp advertise** 或 **mpls te igp advertise shortcut** 命令后，针对该 Tunnel 的 destination 需要配置 LDP Remote 会话。

1.9.2.6 TE FRR 场景需要在旁路隧道的 PLR(Point of Local Repair)节点和 MP(Merge Point)节点间建立 Hello 会话的配置规范

对于部署 TE FRR 的网络，为了使节点在 FRR 和 RSVP-TE GR 同时发生故障的情况下保护主隧道，需要在旁路隧道的 PLR(Point of Local Repair)节点和 MP(Merge Point)节点间建立 Hello 会话。

应用场景

部署 TE FRR 的网络。

配置规范

对于部署 TE FRR 的网络，需要在旁路隧道的 PLR(Point of Local Repair)节点和 MP(Merge Point)节点间建立 Hello 会话，在 MPLS 视图下配置 **mpls rsvp-te Hello nodeid-session** *ip-address* 命令。

非规范配置的风险

风险描述

如果不配置建立 Hello 会话，则不支持增强的 RSVP GR 功能，造成业务中断。

风险的判断方法

1. 在用户视图，执行 **display current-configuration interface** *interface-name* 命令，查看 Tunnel 中存在 **mpls te fast-reroute** 配置。

```
<HUAWEI> display current-configuration interface Tunnel0/0/1
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack0
 tunnel-protocol mpls te
 destination 1.1.2.9
 mpls te tunnel-id 2000
 mpls te fast-reroute
 mpls te commit
```

2. 在用户视图，执行 **display current-configuration configuration mpls** 命令，如果存在 GR 配置，但不存在 mpls rsvp-te Hello nodeid-session ip-address 配置，则存在案例描述的问题。

```
<HUAWEI> display current-configuration configuration mpls
#
 mpls lsr-id 2.2.2.2
 mpls
  mpls te
  mpls rsvp-te
  mpls rsvp-te Hello
  mpls rsvp-te Hello full-gr
  mpls rsvp-te Hello nodeid-session ip-address
  mpls te cspf
```

风险的恢复方案

在 PLR(Point of Local Repair)节点和 MP(Merge Point)节点上，mpls 视图下配置 **mpls rsvp-te Hello nodeid-session** *ip-address* 命令（对于 PLR 节点，*ip-address* 为 MP 节点的 lsr-id；对于 MP 节点，*ip-address* 为 PLR 节点的 lsr-id）。

1.10 VPN

1.10.1 BGP/MPLS IP VPN 的配置规范

1.10.1.1 B 类型单板的 L3VPN 配置规范

B 类型单板承载 L3VPN 业务必须激活对应的 License，否则会导致 L3VPN 业务中断。

应用场景

说明

B 类型单板指的是：

- 单板名称中有-B 或者 Unit B 字样的单板。

单板名称可以使用 display elabel 中的 Description 字段显示出来。

1. **设备已经使用非 B 类型单板承载 L3VPN 业务，更换为 B 类型单板**
2. **设备已经使用 B 类型单板承载 L3VPN 业务，但 License 超期**

3. **设备使用 B 类型单板首次部署承载 L3VPN 业务**

配置规范

应用场景 1-现网设备已经使用非 B 类型单板承载 L3VPN 业务，更换为 B 类型单板

1. 根据待替换的 B 类型单板的具体型号，申请 GTL License。具体申请方法，请咨询华为工程师。
2. 获取到 License 文件后，请传输到设备主用主控板 CF 卡的根目录。具体请参考：文件操作举例。如果存在备用主控板，还需要执行命令：**copy** *source-filename* **slave#cfcard:/** *destination-filename*，复制文件到备用主控板 CF 卡的根目录。
3. 激活 License：**license active** *file-name*。
4. 设置下一次启动的 License 文件：**startup license**{ **default** | *file-name* } [**slave-board**]。
5. 更换单板，具体请参考：*部件更换->更换单板->更换业务处理板*。
6. 新单板上电后，执行命令：**service-enhance slot** *slot-id*。

应用场景 2-现网设备已经使用 B 类型单板承载 L3VPN 业务，但 License 超期

1. 根据 B 类型单板的具体型号，申请 GTL License。具体申请方法，请咨询华为工程师。
2. 获取到 License 文件后，请传输到设备主用主控板 CF 卡的根目录。具体请参考：文件操作举例。如果存在备用主控板，还需要执行命令：**copy** *source-filename* **slave#cfcard:/** *destination-filename*，复制文件到备用主控板 CF 卡的根目录。
3. 激活 License：**license active** *file-name*。

应用场景 3-设备使用 B 类型单板首次部署承载 L3VPN 业务

1. 安装单板并上电设备，具体请参考：*安装->安装单板与子卡*。
2. 根据待替换的 B 类型单板的具体型号，申请 GTL License。具体申请方法，请咨询华为工程师。
3. 获取到 License 文件后，请传输到设备主用主控板 CF 卡的根目录。具体请参考：文件操作举例。如果存在备用主控板，还需要执行命令：**copy** *source-filename* **slave#cfcard:/** *destination-filename*，复制文件到备用主控板 CF 卡的根目录。
4. 激活 License：**license active** *file-name*。
5. 执行命令：**service-enhance slot** *slot-id*。

非规范配置的风险

风险描述

B 类型单板默认不支持 L3VPN，需要申请 License 并激活，并使能 L3VPN 功能后才能承载 L3VPN 业务。如果 License 缺失、未激活、超期，将会导致 B 类型单板承载的 L3VPN 业务中断。

风险的判断方法

- **应用场景 1-现网设备已经使用非 B 类型单板承载 L3VPN 业务，更换为 B 类型单板**

确定需要更换的单板上，是否承载 L3VPN 业务。执行 **display fib** *slot-id* **statistics all**，查看对应槽位上的单板上是否有私网转发计数。例如：下面回显中，加粗的“IPv4 FIB VPN-instance 1 Route Prefix Count”、“IPv4 FIB VPN-instance 2 Route Prefix Count”、“IPv4 FIB VPN-instance dsc Route Prefix Count”后就有相应的计数，说明这台设备 4 号槽位上的单板上承载了 L3VPN 业务。需要更换前申请好 License。

```
<HUAWEI> display fib 4 statistics all
IPv4 FIB Route Prefix Capacity : 3379199
IPv4 FIB Total Route Prefix Count : 40; Entry Count : 41

IPv4 FIB Public Route Prefix Count : 34; Entry Count : 35
IPv4 FIB VPN-instance 1 Route Prefix Count : 1; Entry Count : 1
IPv4 FIB VPN-instance 2 Route Prefix Count : 1; Entry Count : 1
IPv4 FIB VPN-instance dsc Route Prefix Count : 4; Entry Count : 4
```

- **应用场景 2-设备已经使用 B 类型单板承载 L3VPN 业务，但 License 超期**

  通过命令 **display license** 查看 License 有效期。例如：下面回显中字段“Expired date”显示的日期是否超过当前日期。如超期，需要申请 License。

```
<HUAWEI> display license
Active license : cfcard:/licortf201476-f2cffd7e56 me60.dat
License state : Normal
Revoke ticket : No ticket

RD of Huawei Technologies Co., Ltd.

Product name : ME60
Product version : V600R008
License Serial No : LIC2014081100D550
Creator : Huawei Technologies Co., Ltd.
Created Time : 2012-08-11 14:02:06
Feature name : MEFEA
Authorize type : COMM
Expired date : 2017-08-11
Trial days : --
Feature name : MEFEB
Authorize type : COMM
Expired date : 2017-08-11
Trial days : --

Item name Item type Value Description
-------------------------------------------------------------
LME0NGMVPN Function YES Multicast NG MVPN
LME0HAGF01 Function YES Cross-chassis HAG
LME0FWF01 Function YES Firewall for SSU
LME0P8200G00 Function YES SWCAP
LME0BRAS01 Function YES BRAS Function(4k subscribers)
LME0MDI00 Function YES DIST MQE License
LME0VPDN01 Function YES LNS&LTS Function
LME0RDPXY00 Function YES Radius-proxy Function
LME0LIF01 Function YES Lawful Interception
LME0EPT00 Function YES RFC2544 Function
LME0FPM00 Function YES IP FPM Function
LME0SSGF01 Function YES DSG Function
LME0WIFI00 Function YES ME60 Wifi Gateway Enhance Function License
```

```
LME0REMMIR00 Function YES Remote Mirroring License
LME0CONN01 Resource 256 Concurrent Users(1k)
LME0SMVP00 Resource 32 EnhanceLicense_MVPN
LME0STUN00 Resource 32 TUNNEL
LME0SNAT00 Resource 32 NAT for SPU C
LME0SNET00 Resource 32 ENHANCE_NS
LME0VIDE00 Resource 32 MQE License
LME0IPSEC00 Resource 32 IPSEC License
LME0NATDS00 Resource 256 2M NAT Session
LME0L2NATDS00 Resource 32 L2NAT license
LME0DSLITEDS00 Resource 32 DS-lite license
LME04020G00 Resource 32 20G NAT BandWidth
LME0L2NAT01 Resource 32 L2NAT License for VSUF
LME0DSLITE01 Resource 32 DS-Lite License for VSUF
LME0PCP00 Resource 32 PCP License for VSUF
LME0NAT6401 Resource 32 NAT64 License for VSUF
LME0TUNL00 Resource 224 GTL license for Hybrid Access Tunnel
LME0SGTN00 Resource 16 ME60 SoftGRE 1k Tunnel License

Item name (View)Resource License Command-line
------------------------------------------------------------
LME0IPSEC00 (License)active ipsec slot slot-id
LME0NATDS00 (License)active nat session-table size
LME0L2NATDS00 (License)active l2nat slot slot-id
LME0DSLITEDS00 (License)active ds-lite slot slot-id
LME04020G00 (License)active nat bandwidth-enhance slot slot-id
LME0L2NAT01 (License)active l2nat vsuf slot slot-id
LME0DSLITE01 (License)active ds-lite vsuf slot slot-id
LME0PCP00 (License)active pcp vsuf slot slot-id
LME0NAT6401 (License)active nat64 vsuf slot slot-id

Master board license state: Normal.
```

- **应用场景 3-设备使用 B 类型单板首次部署承载 L3VPN 业务**

  无

风险的恢复方案

同配置规范。

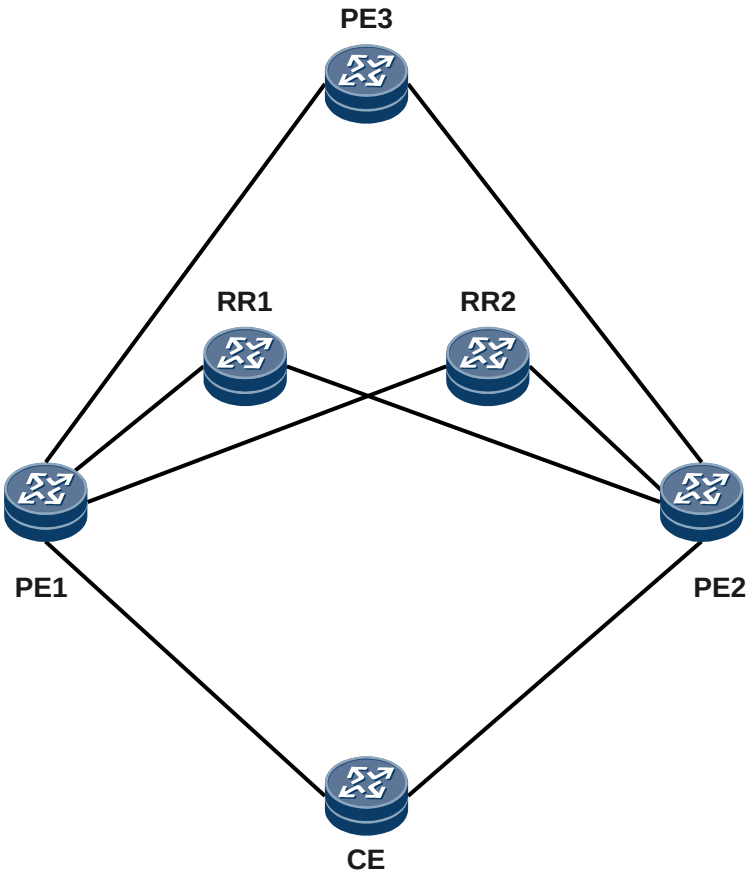
1.10.1.2 CE 双归组网中相同的 VPN 实例 RD 不能相同

CE 双归到两个 PE，BGP 路由经过 RR 反射时两个 PE 上相同的 VPN 实例的 RD 建议配置为不同，否则会造成远端 PE 上只能看到一条路由，造成 VPN FRR 不生效。

应用场景

如图 1-18 所示，CE 双归到 PE1 和 PE2，相同 VPN 实例配置的 RD 相同，导致 PE3 上无法形成 VPN FRR。

图1-18 CE 双归 PE 组网中 RD 相同导致 VPN FRR 不生效组网图



配置规范

两个 PE 上相同 VPN 实例配置不同的 RD。

非规范配置的风险

风险描述

如果主 PE 故障或者主 PE 与远端 PE3 之间的隧道故障，则 PE3 无法形成 VPN FRR 表项，无法触发 VPN FRR 切换，导致丢包超过秒级。

风险的判断方法

1. 查看 PE1 和 PE2 的配置，发现存在相同 RD 的 VPN 实例。
2. 在 PE3 上任意视图下执行 **display ip routing-table vpn-instance** *vpn-instance-name ip-address* **verbose** 命令，发现没有生成路由的备份下一跳，备份隧道和标签。说明在 PE3 上没有形成 VPN FRR 表项。

```
<HUAWEI> display ip routing-table vpn-instance vpn1 10.1.1.0 verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : vpn1
Summary Count : 1
```

```
Destination: 10.3.1.0/24
   Protocol: BGP          Process ID: 0
  Preference: 255              Cost: 0
    NextHop: 2.2.2.2       Neighbour: 2.2.2.2
      State: Active Adv GotQ      Age: 00h15m06s
        Tag: 0             Priority: low
      Label: 15361           QoSInfo: 0x0
  IndirectID: 0x13
RelayNextHop: 0.0.0.0        Interface: Pos2/0/0
   TunnelID: 0x6002002          Flags: RD
```

风险的恢复方案

两个 PE 上相同 VPN 实例配置不同的 RD。

1.10.1.3 取消接口与 VPN 实例的绑定关系导致联动删除 BFD 的配置

当取消接口与 VPN 实例的绑定关系时，之前与该接口存在联动关系的 BFD 会话会同时被联动删除，可能导致绑定到该 BFD 会话的静态路由的状态发生变化，造成业务受损。

应用场景

如图 1-19 所示：

1. 接口下配置 **ip binding vpn-instance** *vpn-instance-name* 命令绑定 VPN 实例。
2. 存在静态 BFD 会话绑定步骤 1 中的接口。
3. 存在静态路由绑定步骤 2 中的 BFD 会话，和 BFD 形成联动关系。

以上配置，当删除步骤 1 中接口下的 **ip binding vpn-instance** *vpn-instance-name* 命令时，会联动删除对应的 BFD 会话，BFD 会话被删除时又会解除绑定到本会话的静态路由的联动关系，这样在某些场景下可能导致业务受损。

图1-19 取消接口与 VPN 实例的绑定关系导致联动删除 BFD 组网图

Device1 和 Device2 之间建立静态 BFD 会话，分别绑定 GE1/0/0 接口。

1. 在 Device1 上查询 GE1/0/0 的和 BFD 会话的配置。

```
[Huawei] display current-configuration interface GigabitEthernet1/0/0
#
interface GigabitEthernet1/0/0
 ip binding vpn-instance vpn1   //绑定了 VPN 实例
 ip address 12.0.0.1 255.255.255.0
#
return
```

```
[Huawei] display current-configuration configuration bfd-session
#
bfd bfd1 bind peer-ip 12.0.0.2 vpn-instance vpn1 interface GigabitEthernet1/0/0
 discriminator local 1
 discriminator remote 2
 commit   //绑定了接口
```

2. Device1 上查询 BFD1 会话状态。

```
<HUAWEI> display bfd session all
--------------------------------------------------------------------------------
-
Local Remote    PeerIpAddr     State    Type       InterfaceName
--------------------------------------------------------------------------------
-
1    2        12.0.0.2       Up       S IP IF    GigabitEthernet1/0/0
--------------------------------------------------------------------------------
-
    Total UP/DOWN Session Number : 1/0
```

3. Device1 上查询静态路由的配置和状态。

```
[Huawei] display current-configuration  | include ip route
ip route-static 10.0.0.0 255.255.255.0 13.0.0.3 track bfd-session bfd1  //绑定了
BFD 会话
```

静态路由活跃。

```
[Huawei] display ip routing-table 10.0.0.1
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.0.0.0/24  Static  60   0           RD   13.0.0.3       GigabitEthernet1/0/0
```

4. 当 BFD1 会话 Down 后，Device1 上对应的静态路由撤销。

```
[Huawei] display bfd session all
--------------------------------------------------------------------------------
-
Local Remote    PeerIpAddr     State    Type       InterfaceName
--------------------------------------------------------------------------------
-
1    2        12.0.0.2       Down     S IP IF    GigabitEthernet1/0/0    //bfd
会话 down
--------------------------------------------------------------------------------
[Huawei] display ip routing-table 10.0.0.1  //路由撤销
```

5. Device1 上删除 GigabitEthernet1/0/0 接口下的 **ip binding vpn-instance** *vpn-instance-name* 命令。

```
[Huawei-GigabitEthernet1/0/0] undo ip binding vpn-instance vpn1  //删除配置
[Huawei] display current-configuration | include ip route
ip route-static 10.0.0.0 255.255.255.0 13.0.0.3  //track bfd 的配置被联动删除
[Huawei] display ip routing-table 10.0.0.1     //路由重新活跃
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
```

```
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.0.0.0/24  Static  60   0         RD   13.0.0.3       GigabitEthernet1/0/0
```

配置规范

当取消接口与 VPN 实例的绑定关系时：

1. 如果之前存在 BFD 会话和该接口联动，则重新创建静态绑定接口的 BFD 会话。

```
[Huawei]bfd bfd1 bind peer-ip 12.0.0.2 interface GigabitEthernet1/0/0
 discriminator local 1
 discriminator remote 2
 commit
```

2. 如果之前存在静态路由绑定该 BFD 会话，则需要再次将静态路由绑定到新创建的 BFD 会话。

```
ip route-static 10.0.0.0 255.255.255.0 13.0.0.3 track bfd-session bfd1
```

非规范配置的风险

风险描述

去使能接口下 VPN 实例绑定命令，联动删除了 BFD 会话，而 BFD 会话删除又会解除静态路由和本 BFD 会话的联动关系，导致静态路由可能重新活跃，并迭代到错误的下一跳，导致业务受损。

风险的判断方法

1. 取消接口与 VPN 实例的绑定前，在任意视图下执行 **display ip routing-table protocol static** 命令，记录活跃的静态路由的详细情况。

```
<HUAWEI> display ip routing-table  protocol static
_public_ Routing Table : Static
```

2. 取消接口与 VPN 实例的绑定后，在任意视图下执行 **display ip routing-table protocol static** 命令，记录活跃的静态路由的详细情况。

```
<HUAWEI> display ip routing-table protocol static
 public  Routing Table : Static
        Destinations : 1       Routes : 1       Configured Routes : 1

Static routing table status : <Active>
        Destinations : 1       Routes : 1

Destination/Mask    Proto   Pre  Cost       Flags NextHop         Interface

     100.0.0.0/24  Static  60   0           D   12.0.0.2       Ethernet0/1/0

Static routing table status : <Inactive>
        Destinations : 0       Routes : 0
```

3. 对比取消接口与 VPN 实例的绑定前后静态路由，如果有新的静态路由活跃，并且是由于静态路由 Track 的 BFD 被联动删除导致其活跃，则存在风险。

风险的恢复方案

请按照配置规范进行配置。

1.11 安全

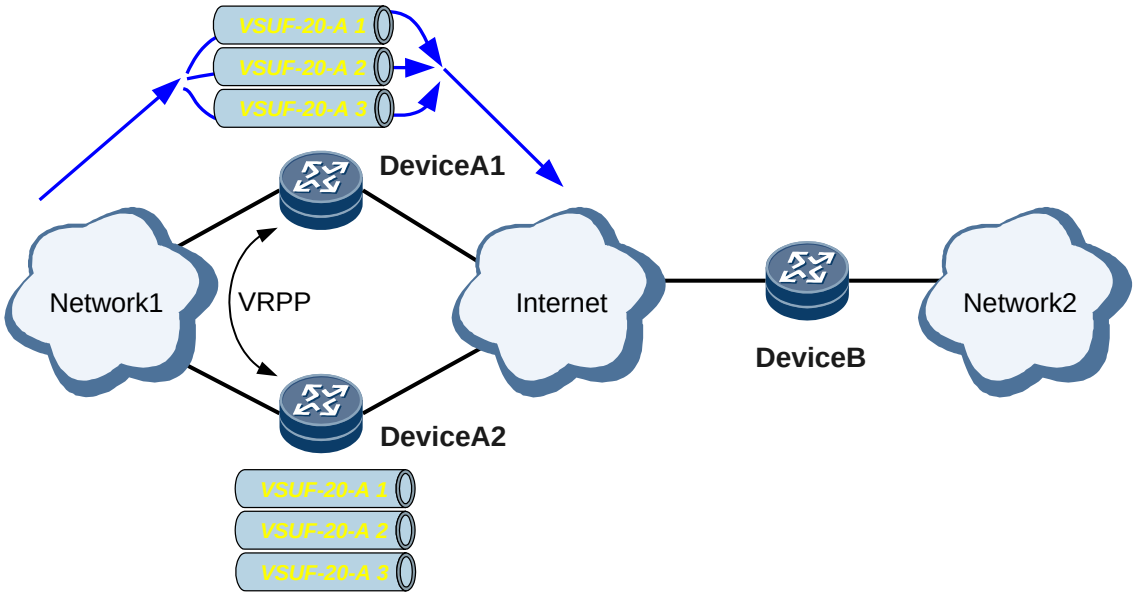
1.11.1 IPSec 的配置规范

1.11.1.1 多块 VSUI-20-A 部署 IPSec 双机热备场景下需要配置绑定保护组的 VSU 单板数门限值

默认情况，当设备上某一块 VSUI-20-A 单板故障时，此故障单板上的 IPSec 隧道需要到其他剩余的单板上重建，IPSec 流量也将会负载分担到其他剩余的单板。如果 IPSec 业务量过大，可能会导致其他剩余的单板承载过多流量，影响其他剩余的单板上的 IPSec 业务。故障单板恢复正常后，业务也不回切，造成 IPSec 业务板间负载分担不均。

应用场景

如下图所示，Network1 和 Network2 通过插有 VSUI-20-A 单板的 DeviceA1、DeviceA2、DeviceB 设备建立 IPSec 隧道穿越网络进行互访，IPSec 业务量十分大。DeviceA1、DeviceA2 部署 IPSec 框间备份，DeviceA1、DeviceA2 与 Network1 互联口部署 VRRP。DeviceA1、DeviceA2 上分别有 3 块 VSUI-20-A 单板绑定在保护组内以负载分担方式承载 IPSec 业务。



配置规范

配置 IPsec 双机热备主备倒换时绑定保护组的 VSUI-20-A 单板数量的门限值，并且门限值必须配置成绑定保护组的 VSUI-20-A 单板数量减 1，即当 1 块 VSUI-20-A 单板故障后，设备立即实现框间主备倒换。

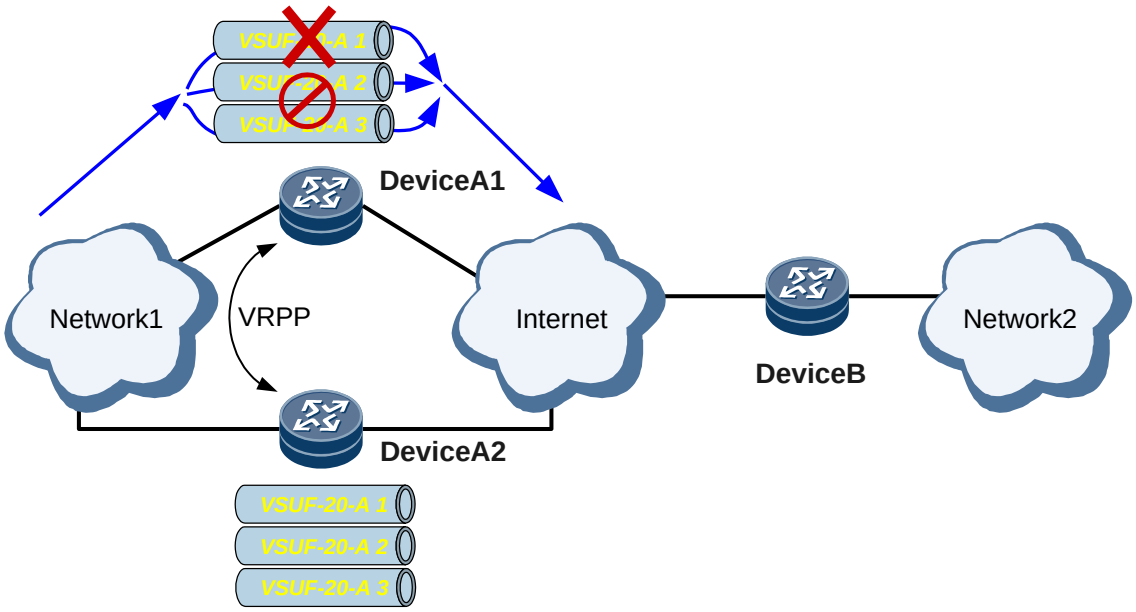
- IPsec 实例视图下，执行命令 **hrp least active-slot-number** *slot-number*，*slot-number* 值为绑定的 VSUI-20-A 单板数减 1。*slot-number* 的默认值为 0，因此当绑定的单板数为 1 时，无需配置。

详情参考：（可选）配置 IPsec 双机热备。

非规范配置的风险

风险描述

默认情况，当设备上某一块 VSUI-20-A 单板故障时，此故障单板上的 IPSec 隧道需要到其他剩余的单板上重建，IPSec 流量也将会负载分担到其他剩余的单板。如果 IPSec 业务量过大，可能会导致其他剩余的单板承载过多流量，影响其他剩余的单板上的 IPSec 业务。故障单板恢复正常后，业务也不回切，造成 IPSec 业务板间负载分担不均。



风险的判断方法

在用户视图下，通过 **display current-configuration configuration** *configuration-type* 查看 IPSec 实例的配置。“hrp least active-slot-number”字段的显示值需要为“bind slot”字段数量减 1，例如下述回显中，绑定 VSU 单板数是 2，配置的门限值是 1，不存在风险。

```
[HUAWEI] display current-configuration configuration ipsec-instance
#
ipsec instance 6
 hrp peer 10.0.1.2
 hrp track interface GigabitEthernet3/0/7
 hrp vrrp vrid 1 interface GigabitEthernet3/0/11
bind slot 2 backup-id 1
bind slot 3 backup-id 2
 hrp least active-slot-number 1
#
Return
```

风险的恢复方案

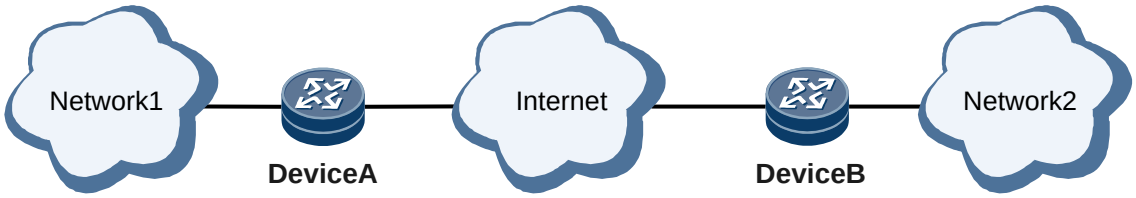
同配置规范。

1.11.1.2 IPSec 业务场景下需要配置 IKE DPD 保证 IPSec 隧道两端状态一致

DPD 使用 IPsec 流量来最小化 peer 状态检测所需消息报文的数量，此机制不使用周期发送消息的机制。此机制是 IKE 存活机制的一种替代机制。部署 IPSec 业务时，必须配置 IKE DPD，从而 IPSec 隧道两端发送报文感知对端状态，保证两端 IPSec 隧道状态一致和 IPSec 业务转发的正常运行。

应用场景

如下图所示，DeviceA 设备和 DeviceB 设备之间部署 IPSec 隧道穿越 Internet，Network1 与 Network2 通过此隧道互访。



配置规范

通过命令行 **ike dpd** 配置 DPD 功能。详见：（可选）配置 IKE 对等体检测功能。

非规范配置的风险

风险描述

当 IPSec 隧道两端状态不一致时，IPSec 流量无法即时删除重建，将会出现黑洞，IPSec 业务转发报文不通。

风险的判断方法

在用户视图下，通过 **display current-configuration | include ike dpd** 查看是否配置了 **ike dpd**，如果没有回显，则未配置 ike dpd。

```
[HUAWEI] display current-configuration | include ike dpd
 ike dpd 30
```

风险的恢复方案

同配置规范。

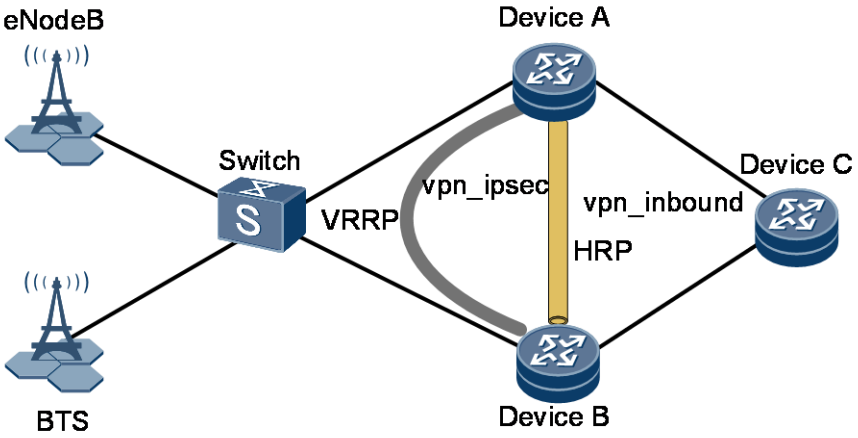
1.11.1.3 IPSec 双机热备场景下主备 IPSec 设备之间链路的 MTU 值需要配置大于 2000

应用场景

如下图所示，IPSec 双机热备场景下，IPSec 双机设备之间有直连的接口相连接，部署 HRP 业务。

IPSec 隧道下应用了安全策略组并绑定了 IPSec 实例（在 IPSec 隧道视图下，执行了命令 **ipsec policy** *policy-name* **instance** *instance-id*），并且 IPsec 安全提议配置传送数据时

采用的安全协议是 **ah-esp**（在安全提议视图下，执行了命令 **transform ah-esp**，配置传送数据时采用的安全协议，先使用 ESP 协议对报文进行保护，再使用 AH 协议对报文进行保护）。



配置规范

需要将用来备份数据的本端接口（即通过命令 **hrp track interface** *interface-type interface-number* 配置的接口）的 MTU 值设置为大于或等于 2000，请根据本端接口的类型选择以下配置方式：

- 本端接口类型为 GE 接口时，在 GE 接口视图下执行 **mtu** *mtu* 命令，设置 GE 接口的 MTU 值。
- 本端接口类型为 Eth-Trunk 接口时，在 Eth-Trunk 接口视图下执行 **mtu** *mtu* 命令，设置 Eth-Trunk 接口的 MTU 值。

非规范配置的风险

风险描述

IPSec 双机热备场景下主备 IPSec 设备之间链路的 MTU 值如果小于 2000，会导致 IPSec SA 信息备份失败，主备倒换后业务中断。

风险的判断方法

1. 在用户视图下，通过 **display ipsec proposal** 查看配置传送数据时采用的安全协议是否为 **ah-esp-new**。如果有，说明配置传送数据时采用的安全协议是先使用 ESP 协议对报文进行保护，再使用 AH 协议对报文进行保护。

```
<HUAWEI> display ipsec proposal

  IPsec proposal name: 1
    encapsulation mode: tunnel
    transform: ah-esp-new
    AH protocol: authentication md5-hmac-96
    ESP protocol: not use authentication, encryption des
```

2. 确认备份链路的接口。在用户视图下，通过 **display current-configuration configuration ipsec-instance**，确定备份数据的本端接口。

```
#
ipsec instance 1
 hrp peer 20.30.40.2
 hrp track interface GigabitEthernet1/0/1
 hrp vrrp vrid 1 interface GigabitEthernet1/0/1.1
 bind slot 2 backup-id 1
```

3. 以 GE 接口为例：在用户视图下，通过 **display interface gigabitethernet** *interface-number*，查看接口的 MTU 值。

```
<HUAWEI> display interface GigabitEthernet 1/0/1
GigabitEthernet1/0/1 current state : DOWN
Line protocol current state : DOWN
Link quality grade : --
Description:HUAWEI, GigabitEthernet1/0/1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Sending Frames' Format is PKTFMT ETHNT 2, Hardware address is 00e0-fc7b-9c00
The Vendor PN is TXN132241013AS3
BW: 10G, Transceiver Mode: SingleMode
WaveLength: 1310nm, Transmission Distance: 10km
RX Power: -19.75dBm, TX Power: -3.51dBm
Media type: fiber ,loopback: none , Scramble enabled, clock master , WAN full-
du
plex mode ,Pause Flowcontrol:Receive Enable and Send Enable
Flag J0 ""
Flag J1 ""
Flag C2 26(0x1a)
Last physical up time  : -
Last physical down time : 2000-03-17 20:09:54 UTC+08:00
Current system time: 2000-04-03 15:28:35+08:00
Statistics last cleared:never
   Last 300 seconds input rate: 0 bits/sec, 0 packets/sec
   Last 300 seconds output rate: 0 bits/sec, 0 packets/sec
   Input: 0 bytes, 0 packets
   Output: 0 bytes, 0 packets
   Input:
     Unicast: 0 packets, Multicast: 0 packets
     Broadcast: 0 packets, JumboOctets: 0 packets
     CRC: 0 packets, Symbol: 0 packets
     Overrun: 0 packets, InRangeLength: 0 packets
     LongPacket: 0 packets, Jabber: 0 packets
     Fragment: 0 packets, Undersized Frame: 0 packets
     RxPause: 0 packets
   Output:
     Unicast: 0 packets, Multicast: 0 packets
     Broadcast: 0 packets, JumboOctets: 0 packets
     System: 0 packets, Overrun: 0 packets
     TxPause: 0 packets
     Unknown Vlan: 0 packets
   Input bandwidth utilization  :    0%
   Output bandwidth utilization :    0%
```

风险的恢复方案

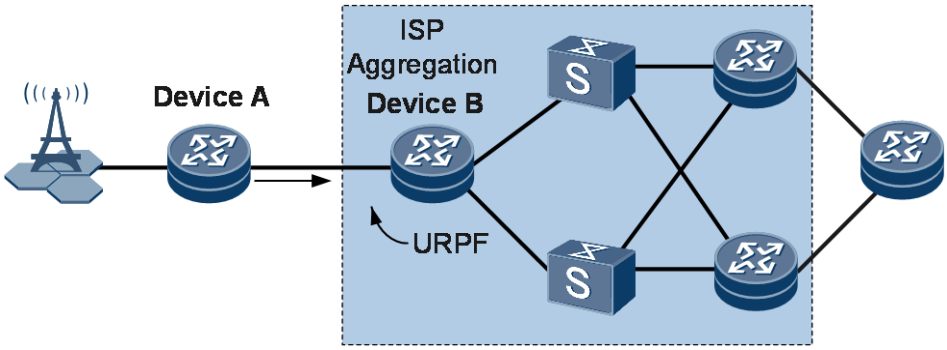
同配置规范。

1.11.2 URPF 的配置规范

1.11.2.1 多路负载分担场景下需要配置 URPF 对匹配缺省路由的报文进行转发处理

应用场景

如下图所示，用户通过 Device A 与 ISP 聚合设备（Device B）连接，在 Device A 的上行接口配置 URPF，可以保护 ISP 设备和 Internet 其他部分免受来自客户网络的源地址欺骗攻击。



配置规范

在 ISP 聚合设备（Device B）上配置流量策略，允许指定网段的流量通过 URPF 检查。详见：配置基于复杂流分类的流量策略。

在 Device A 的上行接口上，执行命令 **ip urpf strict allow-default**，配置 URPF 对匹配缺省路由的报文进行转发处理功能。

非规范配置的风险

风险描述

多路负载分担场景下，如果未配置 URPF 对匹配缺省路由的报文进行转发处理，将会导致业务中断。

风险的判断方法

在用户视图下，通过 **display current-configuration interface**，查看 URPF 配置，如配置不为 **ip urpf strict allow-default** 则存在风险。

```
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address  192.168.1.1
 ip urpf loose
#
……
```

风险的恢复方案

同配置规范。

1.12 用户接入

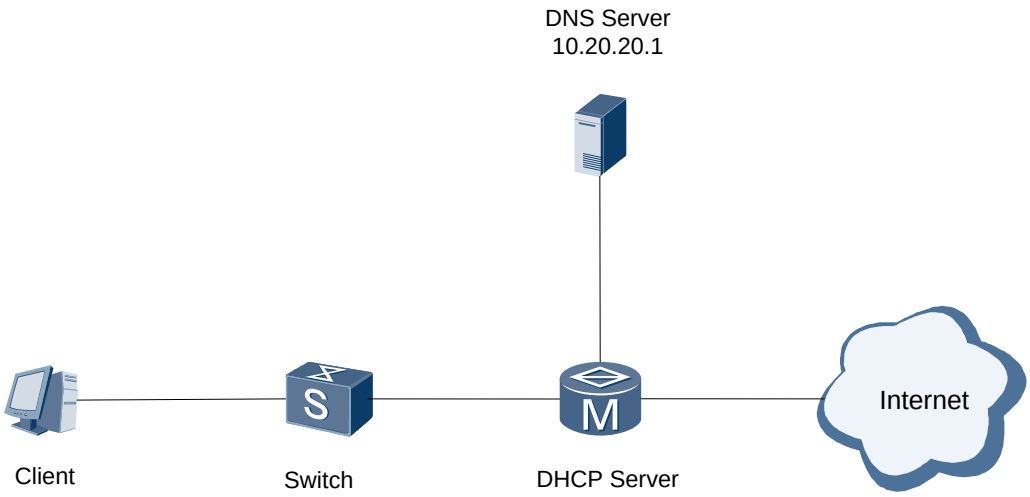
1.12.1 地址管理配置规范

1.12.1.1 限制 DHCP 用户连接请求防止业务繁忙影响正常用户上线

应用场景

如果网络上存在大量无效的连接请求报文或者 Discover 攻击报文，可能造成业务繁忙，严重时可能影响正常用户上线。

DHCP 用户上线场景，组网如下图所示。



配置规范

为防止因业务繁忙严重时可能影响正常用户上线的情况出现，可以在系统视图下配置 **dhcp connection chasten** { **authen-packets** *authen-packets* | **request-packets** *request-packets* } * **check-period** *check-period* **restrain-period** *restrain-period* [**slot** *slotid*]，设置合理的参数可以限制攻击报文缓解业务压力。

非规范配置的风险

风险描述

案例：设备上配置 **dhcp connection chasten request-packets *3* check-period *60* restrain-period *180***，1 分钟内收到请求报文（Discover 报文或 Request 报文）超过 3 个，则抑制该用户的报文 3 分钟。抑制报文时间为 180 秒配置的不合理，导致正常的 DHCP 用户上线慢。

风险的判断方法

执行命令 **display current-configuration** 查询所有的配置信息，查看是否有 **dhcp connection chasten** 配置。

```
<HUAWEI> display current-configuration
#
dhcp connection chasten request-packets 3 check-period 60 restrain-period 180
#
…
```

风险的恢复方案

有两种恢复方案：

1. 在系统视图下执行命令 **undo dhcp connection chasten** 删除 DHCP 用户上线请求连接限制。
2. 根据现网情况合理调整配置限制 DHCP 用户请求连接的参数值。

1.12.1.2 RUI 用户触发上线获取的地址不是域下地址池范围内的地址

应用场景

RUI 主机用户上线后，设备 ARP 探测失败导致用户下线。用户下线后，设备删除了原有的地址池，重新配置新地址池。

配置规范

无。

非规范配置的风险

风险描述

RUI 用户再次触发上线，获取到的地址不是新配置的地址池范围内的地址。

风险的判断方法

无。

风险的恢复方案

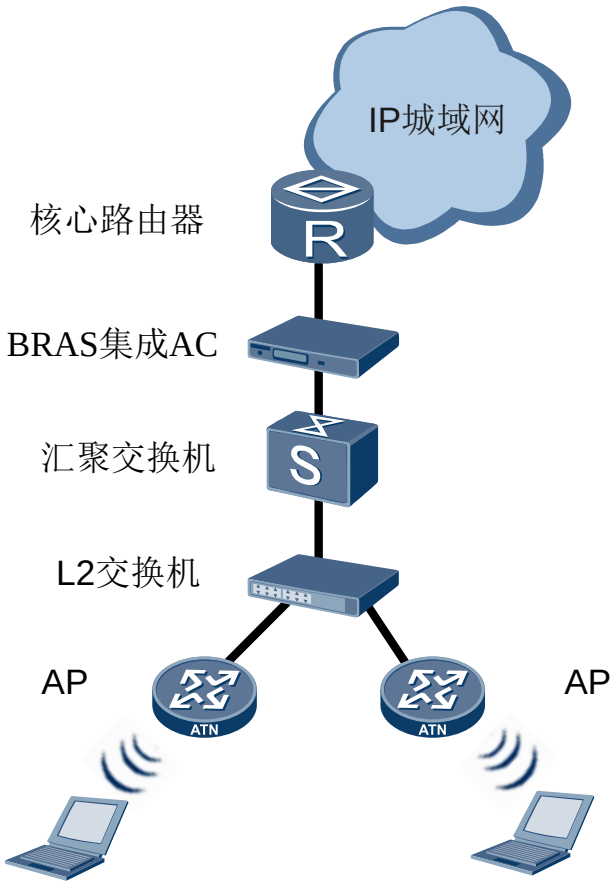
RUI 用户触发上线获取的地址不是域下地址池范围内的地址，需要重启客户端重新获取地址，或者等地址租期到期且续租不成功。客户下线后重新上线就能获取到新配置的地址池范围内的地址。

1.12.2 WLAN 无线漫游场景的参数配置规范

应用场景

AC 和 AP 中间为二层网络的组网方式场景。数据直接转发组网如图 1-20 所示：

图1-20 数据直接转发组网



配置规范

WLAN 无线漫游场景，如果终端的物理位置信息发生变化（MAC 地址不变），终端重新发起 DHCP 上线请求或 ND 上线请求。可根据现网需要决定是否配置 **dhcp session-mismatch action offline**、**dhcp session-mismatch action roam ipv4** 命令。

如果现网需要立即感知终端用户状态变化,则可以通过配置 **dhcp session-mismatch action offline** 命令，触发已在线用户下线，再重新上线。

如果现网需要在用户业务不中断的情况下，处理物理位置信息变化的 DHCP 请求报文，则可以配置 **dhcp session-mismatch action roam ipv4** 命令。

非规范配置的风险

风险描述

终端用户在两个非邻接热点漫游或者手动切换 SSID 时，会引起终端的物理位置信息发生变化（MAC 地址不变），终端重新发起 DHCP 上线请求。 由于物理位置信息变化，MAC 地址不变，设备会认为终端重新发起的 DHCP 上线请求报文或 ND 上线请求报文为攻击报文，将 DHCP 上线请求报文或 ND 上线请求报文丢弃，这时设备认为终端用户还在线，但终端用户可能已经下线，设备不能立即感知到终端用户已下线，导致终端用户不能快速上线。

风险的判断方法

在任意视图，执行命令 **display current-configuration interface**，查看 BAS 接口配置。如果 BAS 接口视图下仅配置了用户接入方式，但未配置 **dhcp session-mismatch action offline**、**dhcp session-mismatch action roam ipv4** 命令，则可能存在问题。

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet2/0/0.77
[HUAWEI-GigabitEthernet2/0/0.77] bas
[HUAWEI-GigabitEthernet2/0/0.77-bas] access-type layer2-subscriber
[HUAWEI-GigabitEthernet2/0/0.77-bas] dhcp session-mismatch action offline
```

配置影响

缺省情况下，物理位置信息发生变化、MAC 地址不变的已在线用户重新发起 DHCP 上线请求或 ND 上线请求时，不会触发已在线用户下线。

配置了 **dhcp session-mismatch action offline** 命令后，当终端再发起 DHCP 上线请求或 ND 上线请求时，会触发终端用户下线，当终端继续发起 DHCP 上线请求或 ND 上线请求时，使用户重新上线，这样用户就能较快速地上线。

说明

执行该命令后，如果攻击源伪造 MAC 地址信息发起 DHCP 上线请求或 ND 上线请求时，会导致正常在线用户掉线，可能导致安全隐患，请谨慎使用。

1. 执行命令 **dhcp session-mismatch action roam ipv4** 用来指定 WLAN 用户从别的接口漫游到此接口时，可以由此接口收到的用户 DHCP discover 或 request 报文触发用户的漫游处理，用户能够不认证，直接再次联接网络。

```
[HUAWEI] interface GigabitEthernet2/0/0.77
[HUAWEI-GigabitEthernet2/0/0.77] bas
[HUAWEI-GigabitEthernet2/0/0.77-bas] access-type layer2-subscriber
[HUAWEI-GigabitEthernet2/0/0.77-bas] dhcp session-mismatch action roam ipv4
```

配置影响

缺省情况下，在设备存在用户的情况下，收到用户物理位置信息变化的 DHCP 请求报文时，会将请求报文直接丢弃，不处理。 配置了 dhcp session-mismatch action roam ipv4 命令后，会处理物理位置信息变化了的 DHCP 请求报文，将用户原来的 IP 地址回应给用户，然后切换用户在设备上的物理位置，保证用户业务不中断。

说明

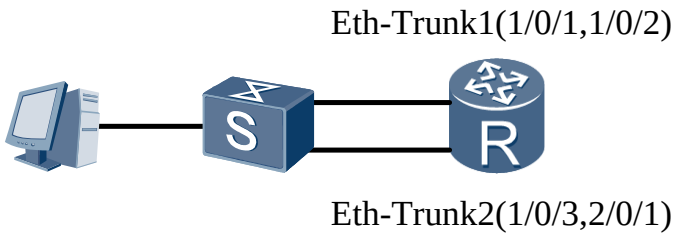
执行该命令后，如果攻击源伪造 MAC 地址信息发起 DHCP 上线请求，会导致正常在线用户流量被切换到攻击源，而正常用户无法联接网络，可能导致安全隐患，请谨慎使用。

1.12.3 一 MAC 多 Session 用户接入场景错误案例

应用场景

同一 MAC 的用户分别从两个 Eth-Trunk 接口上线（Eth-Trunk1 同板 Trunk，Eth-Trunk2 跨板 Trunk，两个 Trunk 口有相同的板）。

图1-21 一 MAC 多 Session 用户上线接入示意图



问题描述

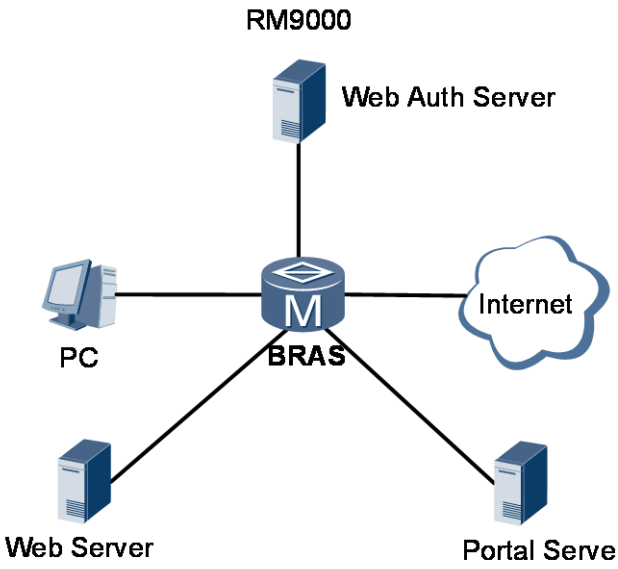
用户现在 Eth-Trunk 1(同板 Trunk，1 号板)上上线，之后又从 Eth-Trunk2 的 2 号板上线，一 MAC 多 Session 在接口板有限制，所以从 Eth-Trunk2 上线的在 1 号板无法生成 PPP 表，之后 Eth-Trunk2 的用户从 1 号板收到 echo reply 报文，转给 2 号单板，连续 3 次后，设备认为主处理板应该切换为 1 号单板。进行单板切换，但是 1 号板没有 ppp 表，用户下线，LPUF-20/21(灵活插卡)、LPUS-20(固定单板）下线原因为 UCM failed to update work-slot of trunk-interface user，LPUF-120/LPUF-120-B/LPUF-120-E/LPUF-102/LPUF-102-E(灵活插卡)、LPUI-120/LPUI-120-B/LPUI-102-E/LPUS-120(固定单板）下线原因为 PPP echo fail。

1.12.4 WEB 用户上线 ACL 配置规范

应用场景

用户通过 Web 认证方式上线。

图1-22 WEB 用户上线组网图



配置规范

1. ACL 视图下执行命令 **rule** *rule-id* **permit ip source user-group web-before destination ip-address** *ip-address* 配置用户前域访问权限允许用户访问部分 IP 地址，并在 traffic classifier 视图下绑定该 ACL 规则。
2. ACL 视图下执行命令 **rule** *rule-id* **permit tcp source user-group web-before destination-port eq www** 配置 ACL 规则匹配 TCP 报文，并在 traffic behavior 视图下配置 **http-redirect** 命令，对前域不允许访问的 IP 地址一律强推 HTTP。

非规范配置的风险

风险描述

流行为视图下配置 **http-reply enable** 使能 Web 增强快回，同时执行命令 **rule** *rule-id* **permit tcp source user-group web-before** 配置简化的 ACL 规则。

则当用户的报文匹配该简化规则时，就会进行快回操作。用户报文会在单板上环回转发，耗尽单板资源会导致整板业务受损，用户频繁掉线。

风险的恢复方案

删除简化规则的配置，按照配置规范配置 ACL 规则。

1.13 增值业务

1.13.1 DAA 的配置规范

1.13.1.1 对配置了 DAA 业务的用户做 NAT 地址转换必须在业务模板下绑定正确的 VPN 实例

应用场景

用户上线后需要做 NAT 地址转换，同时配置了 DAA 增值业务，却没有在 DAA 业务模板下绑定正确的 VPN 实例。

配置规范

1. 如果用户确认需要配置 DAA，DAA 业务模板下配置的 user-group 必须绑定正确的 VPN 实例。
2. 如果用户不需要增值业务，则在 AAA 域下执行命令行 **undo value-added-service policy（AAA 域视图）** 删除 DAA 模板配置。

非规范配置的风险

风险描述

用户流量匹配了 DAA 业务模板定义的规则，由于 DAA 业务模板中未绑定正确的 VPN，导致无法引流到 CGN 单板，用户报文被丢弃。

风险的判断方法

在用户视图下，通过 **display value-added-service user user-id** *used-id* 查看用户是否携带增值业务。如果有”The used VAS service id table are”回显，则说明用户配置了DAA 业务。

```
<HUAWEI> display value-added-service user user-id 0
------------------------------------------------------------------------------
 User access index         : 0
 State                    : Used
 User name                : 0000000000ad@zw
 User service number       : 1
 COPS server name          : --
 DAA rate limit mode outbound: --
 ------------------------------------------------------------------------------
 The used VAS service id table are:
 (    0,    1)
 ------------------------------------------------------------------------------
 ------------------------------------------------------------------------------
```

风险的恢复方案

1. 针对配置规范场景 1：按照配置规范操作。
2. 针对配置规范场景 2：如果用户已经上线激活了 DAA 业务，而实际用户不需要DAA 业务，则在 AAA 域下执行命令行 **undo value-added-service policy（AAA 域视图）** 删除 DAA 模板配置，用户重新上线即可。

1.14 IPv6 过渡技术

1.14.1 CGN 的配置规范

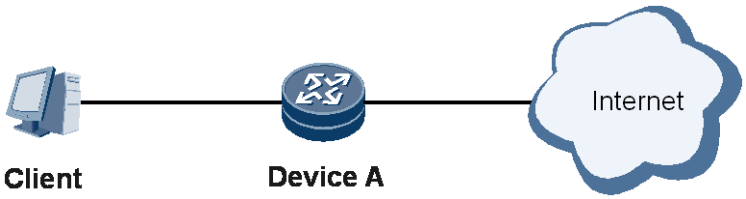
1.14.1.1 CGN 需要配置冗余备份

使用 VSUF 单板或者 VSUI 单板配置 CGN 业务时，如果未配置冗余备份，当单板发生故障时，该单板上承载的用户无法访问网络。为了避免此类现象发生，需要部署多块VSUF/VSUI 单板，并配置 CGN 业务冗余备份。

应用场景

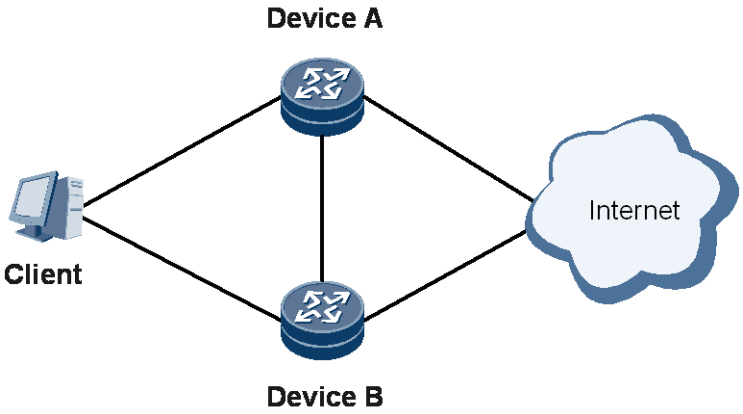
如图 1-23 所示，用户通过插有 VSUF 单板或者 VSUI 单板的 Device A 进行 CGN 转换后访问网络。

图1-23 用户通过 Device A 进行 CGN 转换后访问网络组网图



或者，如图 1-24 所示，用户通过插有 VSUF 单板或者 VSUI 单板的 Device A 和 Device B 进行 CGN 转换后访问网络。

图1-24 用户通过 Device A 和 Device B 进行 CGN 转换后访问网络组网图



配置规范

使用 VSUF 单板或者 VSUI 单板配置 CGN 业务时，需要部署多块 VSUF 单板或者 VSUI 单板，对 CGN 业务进行冗余备份。具体配置方法请参考：

- 配置 NAT 单机板间热备功能（VSUF-40/80/160、VSUI-160-E 业务板）
- 配置 NAT 双机框间热备功能（VSUF-40/80/160、VSUI-160-E 业务板）
- 配置 NAT 单机板间热备功能（VSUI-20-A 业务板）

非规范配置的影响

风险描述

当配置 CGN 业务的单板发生故障无法使用时，该单板承载的 CGN 用户无法访问网络。

风险的判断方法

对于 VSUF 单板，当前 CGN 业务的冗余备份方式分为板间备份和框间备份两种，判断风险的方法具体如下：

- 板间备份的风险判断方法如下：

a. 在用户视图下，通过 **display device** 或 **display version slot** *slot-id* 命令查看至少有两块 VSUF 单板。

```
<HUAWEI> display device
Devicename-X8's Device status:
Slot #    Type      Online    Register     Status     Primary
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
-
1         LPU       Present   Registered   Normal     NA
2         LPU       Present   Registered   Normal     NA
5         VSU       Present   Registered   Normal     NA
8         VSU       Present   Registered   Normal     NA
9         MPU       Present   NA           Normal     Master
10        MPU       Present   Registered   Normal     Slave
11        SFU       Present   Registered   Normal     NA
12        SFU       Present   Registered   Normal     NA
13        SFU       Present   Registered   Normal     NA
14        CLK       Present   Registered   Normal     Master
15        CLK       Present   Registered   Normal     Slave
16        PWR       Present   Registered   Abnormal   NA
17        PWR       Present   Registered   Normal     NA
18        FAN       Present   Registered   Normal     NA
19        FAN       Present   Registered   Normal     NA

<HUAWEI> display version slot 5
VSU 5  : uptime is 2 days, 16 hours, 49 minutes
         StartupTime   2002/07/12   21:46:09
  Host    processor :
  SDRAM Memory Size: 4096M  bytes
  Flash Memory Size:  128M  bytes
  VSU version information
  PCB         Version : CR57VSUF80 REV B
  EPLD        Version : 109
  EPLD2       Version : 106
  EPLD3       Version : 102
  BootROM     Version : 2.30
  BootLoad    Version : 2.19
  FSURTP      Version : Version 2.1 RELEASE 0372
  FSUKERNEL   Version : Version 2.1 RELEASE 0372
  ASE         Version : 009
  MonitorBUS version information:
  Software    Version : 10.51
  Configure license items:
  2M NAT Session License

<HUAWEI> display version slot 8
VSU 8  : uptime is 0 day, 18 hours, 27 minutes
         StartupTime   2006/07/14   17:13:48
  Host    processor :
  SDRAM Memory Size: 4096M  bytes
  Flash Memory Size:  128M  bytes
  VSU version information
  PCB         Version : CR57VSUF160 REV B
  EPLD        Version : 109
  EPLD2       Version : 106
  EPLD3       Version : 102
```

```
 BootROM    Version : 2.30
 BootLoad   Version : 2.19
 FSURTP     Version : Version 2.1 RELEASE 0372
 FSUKERNEL  Version : Version 2.1 RELEASE 0372
 ASE       Version : 009
 MonitorBUS version information:
 Software   Version : 10.51
 Configure license items:
 2M NAT Session License
 20G NAT BandWidth License
```

b. 在用户视图下，通过 **display nat instance** 命令查看其绑定的 **service-location**，再使用 **display service-location** [*service-location-id*]命令查看是否有 **Backup slot ID** 字段，如果有，则有板间备份保护；如果没有，则没有板间备份保护。

```
<HUAWEI> display nat instance
nat instance dtest id 22
 port-range 4096
 service-instance-group dtest
 nat address-group dtest group-id 22
   section 0 100.100.100.0 mask 255.255.255.0
 nat outbound 2222 address-group dtest

<HUAWEI> display service-location
service-location 58
 Location slot ID: 5 engine ID: 0
 Current location slot ID: 5 engine ID: 0
 Backup slot ID: 8 engine ID: 0
 Current backup slot ID: 8 engine ID: 0
 Bound service-instance-group number: 1
 Batch-backup state: finished
```

- 框间备份的风险判断方法如下：

  在用户视图下，通过 **display nat instance** 命令查看其绑定的 **service-location**，再使用 **display service-location** [*service-location-id*]命令查看是否有 **Remote-backup interface** 字段，如果有，则有框间备份保护；如果没有，则没有框间备份保护。

```
<HUAWEI> display service-location 22
service-location 22
 Backup scene type: inter-box
 Location slot ID: 5 engine ID: 0
 Remote-backup interface: GigabitEthernet2/2/1.1
 Peer: 22.255.255.2
 Vrrp ID: 22
 Vrrp bind interface: GigabitEthernet2/2/1.1
 Vrrp state: master
 Bound service-instance-group number: 1
 Batch-backup state: finished
```

对于 VSUI 单板，风险判断方法如下：

1. 在用户视图下，通过 **display device** 命令查看至少两块 VSUI 单板。

```
<HUAWEI> display device
Devicename-X8's Device status:
Slot #    Type      Online    Register     Status     Primary
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1         LPU       Present   Registered   Normal     NA
2         VSU       Present   Registered   Normal     NA
3         VSU       Present   Registered   Normal     NA
4         LPU       Present   Registered   Normal     NA
5         TSU       Present   Registered   Normal     NA
6         TSU       Present   Registered   Normal     NA
8         LPU       Present   Registered   Normal     NA
10        MPU       Present   NA           Normal     Master
11        SFU       Present   Registered   Normal     NA
13        SFU       Present   Registered   Normal     NA
15        CLK       Present   Registered   Normal     Master
16        PWR       Present   Registered   Normal     NA
17        PWR       Present   Registered   Normal     NA
18        FAN       Present   Registered   Normal     NA
19        FAN       Present   Registered   Normal     NA
<HUAWEI> display device 2
 slot2's detail information:
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
  Description: Integrated Versatile Service Unit 20 A(VSUI-20-A)
  Board status:      Normal
  Register:          Registered
  Uptime:            2012/07/13   11:49:55
Clock information:
  State item         State
  Current syn-clock:  10
  Syn-clock state:    Locked    VCXO OK    REF OK
  Syn-clock 9 state:  Inactived
  Syn-clock 10 state: Actived
Statistic information:
  Statistic item     Statistic number
  SERDES interface link lost:           0
  MPU switches:      0
  Syn-clock switches: 1
CPU0 information:
  CPU Online:        Present
  CPU Register:      Registered
  CPU SDRAM Memory Size:               4G
  CPU Utilization(%): 33%
  CPU Mem Usage(%):   28%
  VCPU Utilization
  VCPU0  :33%  VCPU1  :3 %  VCPU2  :3 %  VCPU3  :0 %
  VCPU4  :0 %  VCPU5  :0 %  VCPU6  :0 %  VCPU7  :0 %
  VCPU8  :0 %  VCPU9  :0 %  VCPU10 :0 %  VCPU11 :0 %
  VCPU12 :0 %  VCPU13 :0 %  VCPU14 :0 %  VCPU15 :0 %
  VCPU16 :0 %  VCPU17 :0 %  VCPU18 :0 %  VCPU19 :0 %
  VCPU20 :0 %  VCPU21 :0 %  VCPU22 :0 %  VCPU23 :0 %
  VCPU24 :0 %  VCPU25 :0 %  VCPU26 :0 %  VCPU27 :0 %
  VCPU28 :0 %  VCPU29 :0 %  VCPU30 :0 %  VCPU31 :0 %
CPU1 information:
  CPU Online:        Present
  CPU Register:      Registered
```

```
 CPU SDRAM Memory Size:               4G
 CPU Utilization(%): 28%
 CPU Mem Usage(%):   27%
 VCPU Utilization
 VCPU0  :28%  VCPU1  :3 %  VCPU2  :3 %  VCPU3  :0 %
 VCPU4  :0 %  VCPU5  :0 %  VCPU6  :0 %  VCPU7  :0 %
 VCPU8  :0 %  VCPU9  :0 %  VCPU10 :0 %  VCPU11 :0 %
 VCPU12 :0 %  VCPU13 :0 %  VCPU14 :0 %  VCPU15 :0 %
 VCPU16 :0 %  VCPU17 :0 %  VCPU18 :0 %  VCPU19 :0 %
 VCPU20 :0 %  VCPU21 :0 %  VCPU22 :0 %  VCPU23 :0 %
 VCPU24 :0 %  VCPU25 :0 %  VCPU26 :0 %  VCPU27 :0 %
 VCPU28 :0 %  VCPU29 :0 %  VCPU30 :0 %  VCPU31 :0 %
CPU2 information:
 CPU Online:        Present
 CPU Register:      Registered
 CPU SDRAM Memory Size:               4G
 CPU Utilization(%): 29%
 CPU Mem Usage(%):   27%
 VCPU Utilization
 VCPU0  :29%  VCPU1  :3 %  VCPU2  :3 %  VCPU3  :0 %
 VCPU4  :0 %  VCPU5  :0 %  VCPU6  :0 %  VCPU7  :0 %
 VCPU8  :0 %  VCPU9  :0 %  VCPU10 :0 %  VCPU11 :0 %
 VCPU12 :0 %  VCPU13 :0 %  VCPU14 :0 %  VCPU15 :0 %
 VCPU16 :0 %  VCPU17 :0 %  VCPU18 :0 %  VCPU19 :0 %
 VCPU20 :0 %  VCPU21 :0 %  VCPU22 :0 %  VCPU23 :0 %
 VCPU24 :0 %  VCPU25 :0 %  VCPU26 :0 %  VCPU27 :0 %
 VCPU28 :0 %  VCPU29 :0 %  VCPU30 :0 %  VCPU31 :0 %
CPU3 information:
 CPU Online:        Present
 CPU Register:      Registered
 CPU SDRAM Memory Size:               4G
 CPU Utilization(%): 29%
 CPU Mem Usage(%):   27%
 VCPU Utilization
 VCPU0  :29%  VCPU1  :3 %  VCPU2  :3 %  VCPU3  :0 %
 VCPU4  :0 %  VCPU5  :0 %  VCPU6  :0 %  VCPU7  :0 %
 VCPU8  :0 %  VCPU9  :0 %  VCPU10 :0 %  VCPU11 :0 %
 VCPU12 :0 %  VCPU13 :0 %  VCPU14 :0 %  VCPU15 :0 %
 VCPU16 :0 %  VCPU17 :0 %  VCPU18 :0 %  VCPU19 :0 %
 VCPU20 :0 %  VCPU21 :0 %  VCPU22 :0 %  VCPU23 :0 %
 VCPU24 :0 %  VCPU25 :0 %  VCPU26 :0 %  VCPU27 :0 %
 VCPU28 :0 %  VCPU29 :0 %  VCPU30 :0 %  VCPU31 :0 %
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

2. 在用户视图下，通过 **display nat instance** 命令查看配置，是否有“add slot x slave”或者“nat address-group xxx rui-slave metric xx”字段，如果有其一，则说明 CGN 业务配置了冗余备份；如果都没有，则无冗余备份。

```
<HUAWEI> display nat instance
nat instance nat444-1
 nat filter mode full-cone
 port-range 4096
 add slot 2 master
 add slot 3 slave
 nat address-group addressgroup1
```

```
 section 0 182.148.135.0 mask 24
nat outbound 2080 address-group addressgroup1
```

风险的恢复方案

同配置规范。

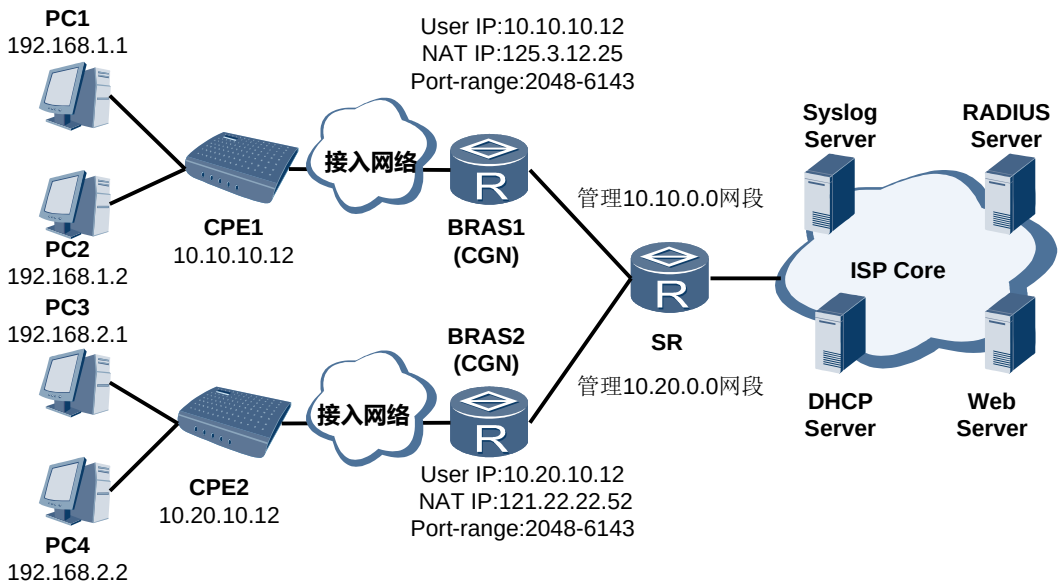
1.14.1.2 CGN 场景 port-range 参数配置规范

NAT 实例下，端口预分配的范围 port-range 配置为 1024，NAT 地址池的转换模式采用五元组，部分用户打开网站时由于端口不够用，NAT session 无法建立。

应用场景

如图 1-25 所示，在分布式 CGN 场景中，CPE 拨号到 BRAS（BRAS 集成 CGN 功能）上线，BRAS 为 CPE 分配上线地址以及对应 NAT 地址和端口段。当终端用户对外发起访问时，CPE 对用户 PC 发出报文进行一次 NAT 转换，BRAS 对 CPE 发出报文做第二次转换。因为网络中存在两次地址转换，同时由于 CGN 功能分布在各个 BRAS 接入点。

图1-25 基于端口预分配的分布式 NAT444 解决方案示意图



配置规范

在 NAT/DS-Lite/NAT64 实例下，为了防攻击，需要通过命令 **port-range** 配置端口预分配功能。配了端口预分配后，对于某个用户使用的端口数是固定的。为了节省端口及 P2P 等应用的需要，同时需要将 NAT 地址池的转换模式配置为三元组。

在 NAT/DS-Lite/NAT64 实例下配置端口预分配的范围，现网部署 NAT 时端口预分配的范围至少是 2048，如果低于该值，就需要配置端口半动态分配模式。以 NAT 实例为例，端口预分配配置规范如下：

1. 配置端口分配方式。采用两种模式，如下所示：

- 以端口预分配方式配置，配置如下:

```
nat instance nat444-rui id 1
 port-range 4096
```

- 以端口半动态分配方式配置，并且需要在实例下使能三元组模式，配置如下：

```
nat instance nat444-rui id 1
 port-range 1024 extended-port-range 1024 extended-times 1
```

2. 实例下配置三元组。

```
nat instance nat444-rui id 1
 nat filter mode full-cone
```

非规范配置的影响

风险描述

执行命令 **port-range** 配置端口预分配范围 *initial-port-range* 低于 2048，并且实例下采用五元组时，部分用户打开网站时由于端口不够用，NAT session 无法建立。

风险的判断方法

1. 在任意视图下，执行命令 **display nat instance** 或者 **display ds-lite instance** 或者 **display nat64 instance** 查看实例配置。通过 **port-range** 判断端口预分配的范围是否低于 2048。
2. 在实例视图下，执行命令 **display this** 查看实例下是否配置了三元组模式。

   端口预分配的范围低于 2048，且实例下没有配置三元组模式会导致部分用户打开网站时由于端口不够用，NAT session 无法建立。

风险的恢复方案

在实例下执行命令 **port-range** *initial-port-range* 将端口预分配的范围调整到 2048 及以上，并且实例下执行命令 **nat filter mode full-cone** 配置 NAT 地址池的转换模式为三元组。

2 部署规范

关于本章

说明

本文档介绍了 NE 系列路由器在某些应用场景中的部署规范，此规范要求用户在 NE 系列路由器部分特性的配置与维护时，必须按照部署规范要求进行业务部署，避免因错误配置、错误使用或可靠性缺失造成业务中断。

2.1 用户接入侧场景下需要配置冗余备份

用户接入侧场景下，必须配置可靠性部署方案。如果不配置，当接入侧的链路（包含光模块、光纤等）、接口、单板、设备等发生故障，会导致业务由于没有备份而中断。

2.2 网络侧链路需要配置冗余备份

网络侧链路必须配置为 GE 接口的跨板多上行链路或 Eth-Trunk 跨板上行链路等可靠性部署方案，如果不配置，可能会出现由于接口、链路或单板故障导致业务中断的情况。

2.3 路由器和周边服务器对接场景下需要配置冗余备份

2.4 双机热备场景下 RBS 需要配置 track 网络侧接口

双机热备场景下 RBS 需要配置 track 网络侧接口，如果不配置，可能导致网络侧链路带宽不足。

2.5 CGN 需要配置冗余备份

使用 VSUF 单板或者 VSUI 单板配置 CGN 业务时，如果未配置冗余备份，当单板发生故障时，该单板上承载的用户无法访问网络。为了避免此类现象发生，需要部署多块 VSUF/VSUI 单板，并配置 CGN 业务冗余备份。

2.6 GRE 需要配置冗余备份

2.7 L2TP 需要配置冗余备份

2.8 Hybrid Access 需要配置冗余备份

2.1 用户接入侧场景下需要配置冗余备份

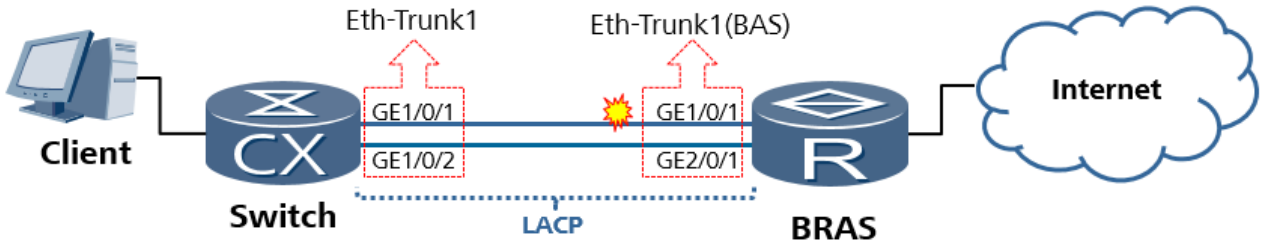
用户接入侧场景下，必须配置可靠性部署方案。如果不配置，当接入侧的链路（包含光模块、光纤等）、接口、单板、设备等发生故障，会导致业务由于没有备份而中断。

应用场景

在用户接入侧的冗余备份场景中，大致可以分为三种场景：跨板 Eth-trunk 热备份、延时响应冷备份、RUI 多机热备份等。单台设备必须部署跨板 Eth-trunk 或者延时响应冷备份，设备之间备份时可使用 RUI 多机热备或延时响应冷备份，重要节点设备必须使用设备间备份。

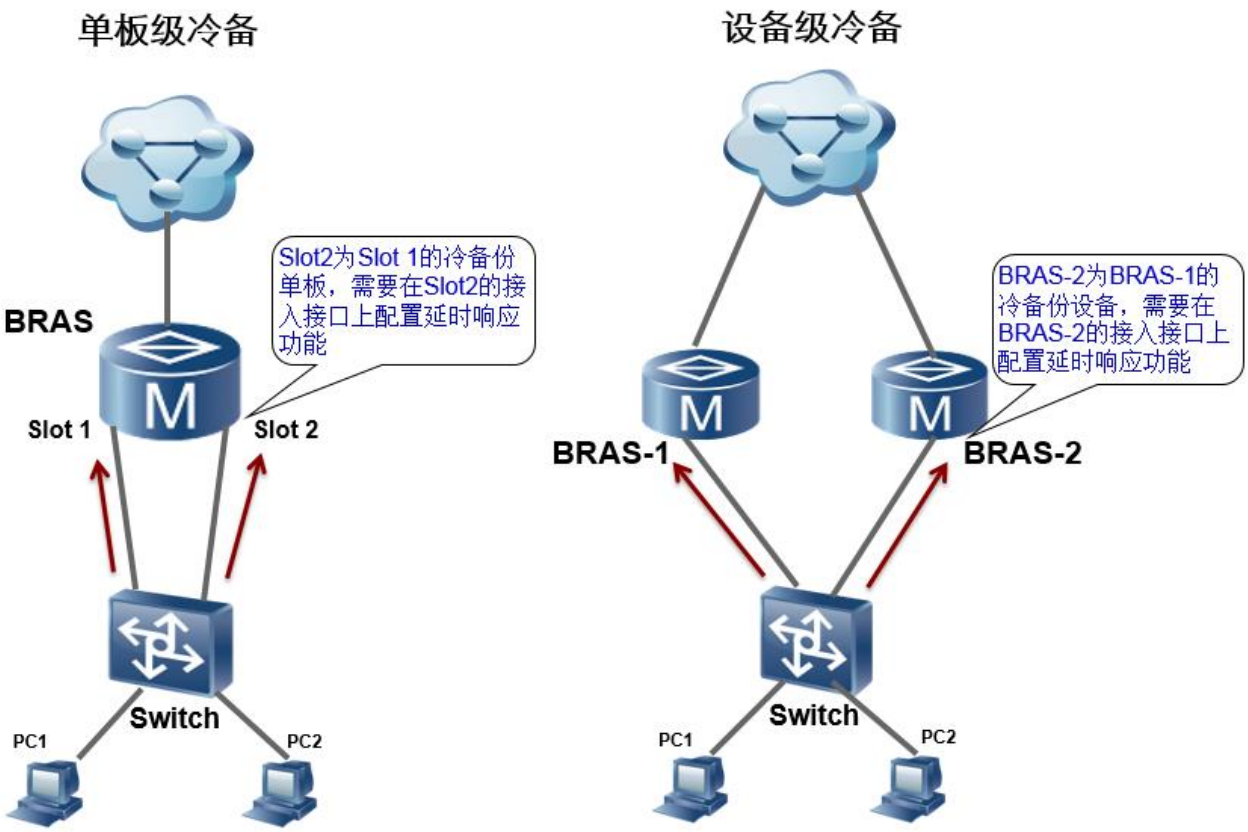
- 跨板 Eth-Trunk 热备份是利用 Eth-Trunk 下成员口分属不同的成员板的特点，能够避免由于 Eth-Trunk 成员接口或链路以及成员口所在单板等故障造成的流量中断等网络事故，提升用户接入业务的可靠性。

  图2-1 跨板 Eth-Trunk 热备份场景组网图



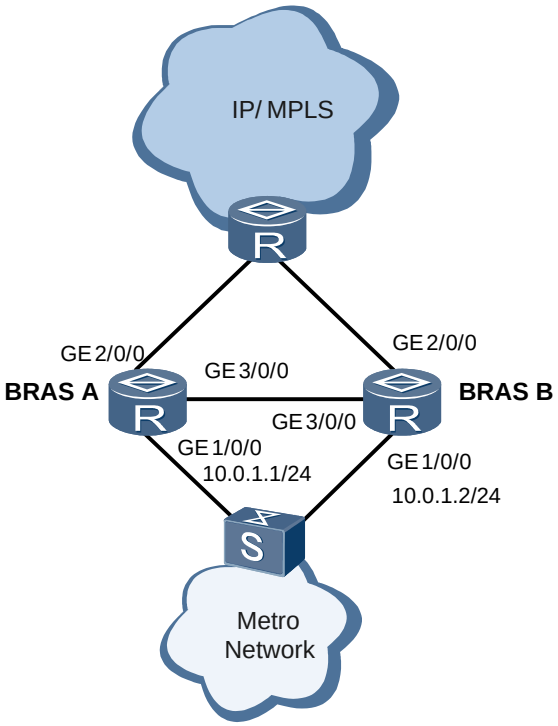
- 延时响应冷备份是指通过在 BAS 接口配置不同的用户接入响应时延策略，设备按照配置策略延长从此接口上线用户的首包报文响应时间，同时需要下游接入设备的多个接口对用户接入报文进行广播。延时响应冷备份按部署场景可分为单板级和设备级冷备份。

图2-2 延时响应冷备份场景组网图



- RUI 多机热备份是通过设备间的用户信息实时备份达到设备级热备份，避免链路、单板或设备故障时造成的用户下线或业务中断的情况。具体请参考产品文档中“配置 BRAS 用户信息多机备份”章节。

图2-3 RUI 多机热备份场景组网图



配置规范

- **跨板 Eth-Trunk 热备份**

  在配置用户接入侧接口时，必须要使用跨板的 Eth-Trunk 接口，应至少包含两个不同成员板的成员接口，能够避免由于 Eth-Trunk 成员接口或链路以及成员口所在单板等故障造成的流量中断等网络事故，提升用户接入业务的可靠性。同时也可以支持用户流量在 Eth-Trunk 的成员板之间的负载分担。具体请参考产品文档中“配置跨板端口备份模式 Eth-Trunk 接口”章节。

- **延时响应冷备份**

  跨板延时响应冷备份从组网上划分为单板级和设备级的冷备份。主要是在两个互为备份的单板或设备的 BAS 接口上配置用户接入响应延时策略命令 **access-delay** *delay-time* [**circuit-id-include** *access-node-id* | **even-mac** | **odd-mac**]。

  延时响应冷备份配置示例：

```
[HUAWEI] interface GigabitEthernet 1/0/9.1
[HUAWEI-GigabitEthernet 1/0/9] user-vlan 55
[HUAWEI-GigabitEthernet 1/0/9-vlan-55-55] bas
[HUAWEI-GigabitEthernet 1/0/9-bas] access-type layer2-subscriber
[HUAWEI-GigabitEthernet 1/0/9-bas] authentication-method ppp
[HUAWEI-GigabitEthernet 1/0/9-bas] access-delay 500 odd-mac
[HUAWEI-GigabitEthernet 1/0/9-bas] quit
[HUAWEI] interface GigabitEthernet 2/1/4.1
[HUAWEI-GigabitEthernet 2/1/4] user-vlan 55
[HUAWEI-GigabitEthernet 2/1/4-vlan-55-55] bas
[HUAWEI-GigabitEthernet 2/1/4-bas] access-type layer2-subscriber
[HUAWEI-GigabitEthernet 2/1/4-bas] authentication-method ppp
```

```
[HUAWEI-GigabitEthernet 1/0/9-bas] access-delay 500 even-mac
[HUAWEI-GigabitEthernet 2/1/4-bas] quit
```

- **RUI 多机热备份**

  在设备上配置远端备份服务和远端备份模板等 RUI 多机备份部署的相关配置，并在用户接入接口下绑定远端备份模板，具体配置方法请参考产品文档中“配置 BRAS 用户信息多机备份”和多机备份配置举例等章节。

非规范配置的影响

- **跨板 Eth-Trunk 热备份**

  风险描述

  当用户接入侧接口不是跨板的 Eth-Trunk 接口时，如果发生成员接口或链路以及成员口所在单板等故障，因没有可靠性冗余备份，会导致用户掉线，流量中断等情况。

  风险的判断方法

  - 如果接入侧接口为普通 GE 接口或子接口，则需要根据配置规范进行整改。
  - 如果接入侧接口为 Eth-Trunk 接口，但不是跨单板的情况，也需要根据配置规范进行整改。

    可执行如下命令查看：

    ```
    [HUAWEI] display eth-trunk
    Eth-Trunk10's state information is:
    WorkingMode: NORMAL       Hash arithmetic: According to flow
    Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 16
    Operate status: up        Number Of Up Port In Trunk: 1
    --------------------------------------------------------------------------------
    ------
      PortName               Status     Weight
      GigabitEthernet1/1/1         Up         1
    ```

- **延时响应冷备份**

  风险描述

  当组网中没有备份的单板或设备时，如果当前用户接入的接口、单板或整机发生故障，则没有备份链路让用户上线，导致用户掉线后业务不能及时恢复，流量中断的情况。

  风险的判断方法

  - 首先需要确定网络中接入侧是否满足“延时响应冷备份场景组网图”中的组网条件，具体方法请参考网络拓扑。
  - 然后查看备份的单板或设备的 BAS 接口上是否配置了延时接入响应策略命令 **access-delay** *delay-time* [**circuit-id-include** *access-node-id* | **even-mac** | **odd-mac**]。

- **RUI 多机热备份**

  风险描述

  当 BRAS A 的接入侧链路、网络侧链路、单板及设备整机发生故障时，用户信息没有备份到 BRAS B 设备，导致用户掉线，访问网络不通等情况。

  风险的判断方法

- 首先需要确认设备上是否配置了远端备份服务和远端备份模板等多机备份相关的配置。
- 通过 **display remote-backup-profile** 和 **display remote-backup-service** 命令查看设备的备份策略和服务配置是否正确，用户上线后有无备份用户信息。

当远端信息备份策略配置成功时，可以看到配置的备份业务类型为 **bras**，此备份策略 profile1 绑定在用户上线接口 **GigabitEthernet1/0/0.1** 下，并且设备 A 状态为 **Master**。

```
<HUAWEI-A> display remote-backup-profile profile1
-----------------------------------------------
 Profile-Index       : 0x802
 Profile-Name        : profile1
 Service             : bras
 Remote-backup-service: service1
 Backup-ID           : 10
 track protocol      : VRRP
 VRRP-ID             : 1
 VRRP-Interface      : GigabitEthernet1/0/0.2
 Access-Control      : Even-Mac
 State               : Master
 Peer-state          : Slave
 VRRP-ID             : 2
 VRRP-Interface      : GigabitEthernet1/0/0.3
 Access-Control      : Odd-Mac
 State               : Slave
 Peer-state          : Master
 Interface           :
                     GigabitEthernet1/0/0.1
 Backup mode         : hot
 Slot-Number         : 1
 Card-Number         : 0
 Port-Number         : 0
 Nas logic-port      : Gigabitethernet 1/0/0
 Nas logic-ip        : 10.2.3.4
 Nas logic-sysname   : huawei
 Traffic interval    : 10(minutes)
```

当远端备份服务配置成功时，可以看到 TCP 连接的状态为 **Connected**。

```
<HUAWEI-A> display remote-backup-service service1
-------------------------------------------------------------
 Service-Index   : 0
 Service-Name    : service1
 TCP-State       : Connected
 Peer-ip         : 10.88.88.88
 Source-ip       : 10.22.22.22
 TCP-Port        : 2046
 Track-BFD       : --
 Track-interface0 : GigabitEthernet2/0/0
 Track-interface1 : --
-------------------------------------------------------------
......
```

待用户上线后，可以查看备份用户的信息。

```
<HUAWEI> display backup-user
```

```
 Remote-backup-service: service1
 Total Users Numer: 10
------------------------------------------------------------------------------
 100    101    102    103    104    105    106    107    108    109
------------------------------------------------------------------------------
```

风险的恢复方案

同配置规范。

2.2 网络侧链路需要配置冗余备份

网络侧链路必须配置为 GE 接口的跨板多上行链路或 Eth-Trunk 跨板上行链路等可靠性部署方案，如果不配置，可能会出现由于接口、链路或单板故障导致业务中断的情况。

应用场景

对网络侧链路进行可靠性部署，从接口部署方式上可以分为 GE 接口和 Eth-Trunk 接口；从设备互连方式上可以分为单上行和多上行场景。主要目的是建立路由转发的备份场景，确保用户侧到网络侧的业务不中断。

配置规范

网络侧链路备份配置为 GE 接口的跨板多上行链路或 Eth-Trunk 跨板上行链路。

非规范配置的影响

风险描述

网络侧无备份链路时，当接口、链路或单板发生故障后，会造成用户的业务流量中断等情况。

风险的判断方法

1. 执行命令 **display ip routing-table**，查看缺省路由或网络侧的明细路由的路由表信息需要至少存在 2 个出接口。
2. 查看是否存在多个路由出接口且分布在不同单板上。

风险的恢复方案

同配置规范。

2.3 路由器和周边服务器对接场景下需要配置冗余备份

应用场景

路由器和周边服务器（如 DHCP、Radius、Web、Diameter、DNS 等）对接时，需要有服务器的冗余备份方案，以确保当服务器发生故障或服务器不可达时，路由器的对接业务可以正常运行。

配置规范

- 服务器自身需要有冗余备份部署，应部署多台服务器或服务器内部为负载均衡等备份方式。
- 路由器上针对对接的各类服务器，应配置多个服务器 IP 地址，通过主备或负载分担的方式来实现冗余备份。

非规范配置的影响

风险描述

当服务器自身冗余备份未部署且路由器和服务器不能正常通信时，会造成业务受损。

当路由器未配置主备或负载分担模式的服务器且路由器和服务器通信故障时，路由器不能自动进行业务切换，会造成业务受损。

风险的判断方法

查看路由器上的服务器相关配置是否配置了多个 IP 地址，具体方法请参考产品文档“配置 RADIUS 认证/计费服务器”和“配置 DHCPv4 服务器组”等章节。

风险的恢复方案

同配置规范。

2.4 双机热备场景下 RBS 需要配置 track 网络侧接口

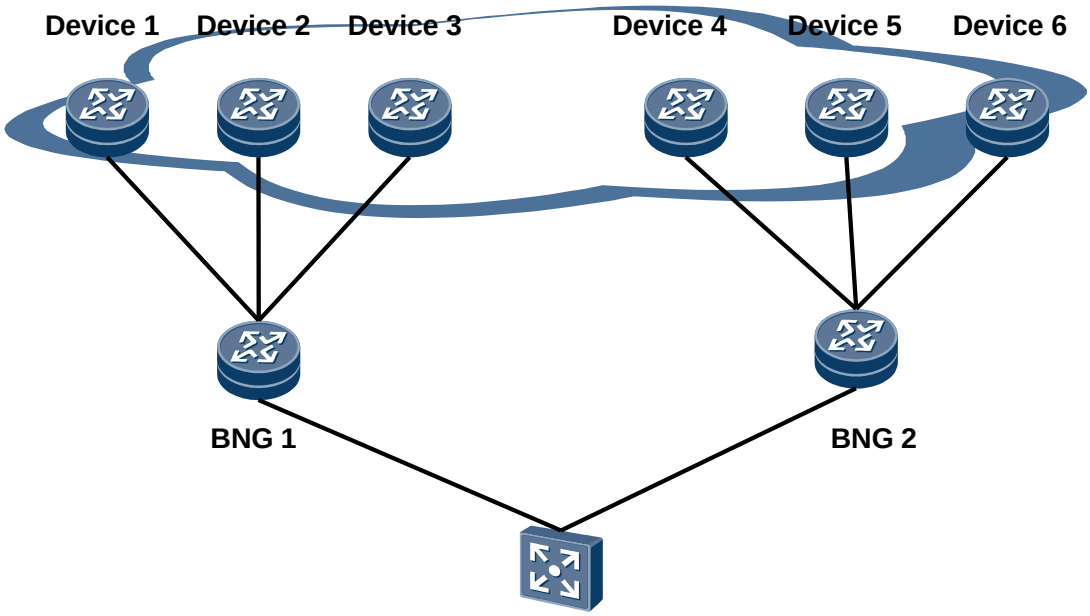
双机热备场景下 RBS 需要配置 track 网络侧接口，如果不配置，可能导致网络侧链路带宽不足。

应用场景

在备份过程中，RBS 作为一个通用备份模块，并使用 TCP 作为传输协议。RBS 向其他业务模块提供备份处理的注册接口，提供批量备份、实时备份两种服务。TCP 连接建立成功后，将通过备份协议进行批量备份和实时备份的数据传送。同时，RBP 为用户提供风格一致的多机备份配置的用户界面，各种多机备份配置的应用都基于 RBP 进行。

在进行配置远端备份服务时，用户需要检测 RBS 所建立的 TCP 连接是否发生故障以及故障恢复状态。

图2-4 双机热备场景组网图



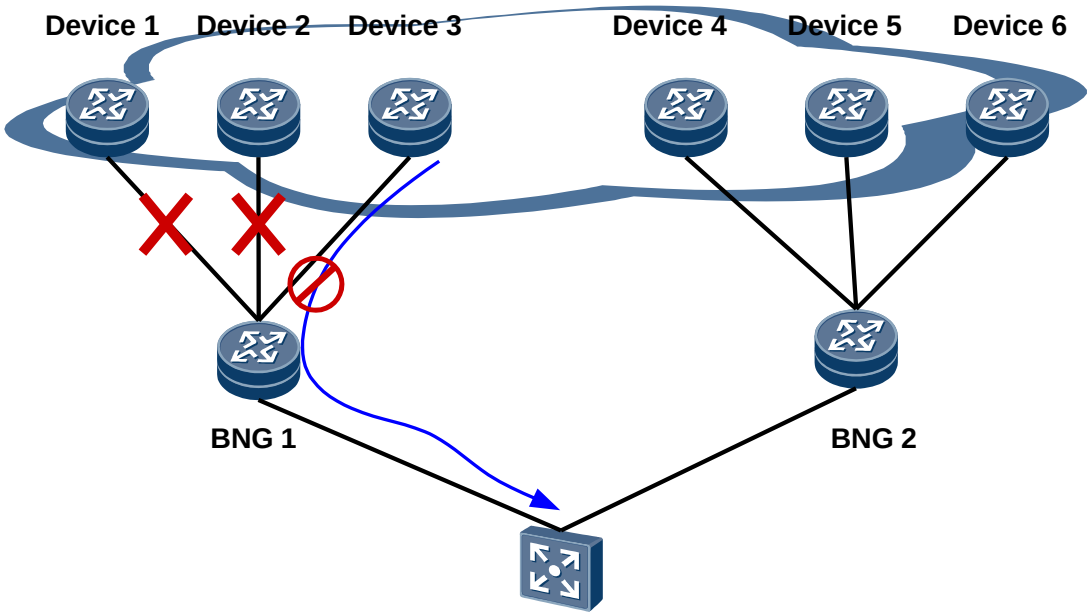
配置规范

1. 在进行配置远端备份服务时，必须配置命令 **track interface** *interface-name* [**weight** *weight*]，配置远端备份服务跟踪网络侧接口的状态，检测远端备份服务所建立的TCP 连接是否发生故障以及故障恢复状态。
2. 必须配置 **switchover uplink** { **failure-ratio** *failure-ratio* | **duration** *duration* } *，配置上行链路故障的切换阈值和持续时间，控制 RBS 下绑定的地址池路由撤销。

非规范配置的风险

风险描述

图2-5 双机热备场景组网图



当 BNG1 多条网络侧接口故障的情况下，由于 RBS 未能检测到 BNG1 的网络侧接口状态，导致双机备份不能切换到 BNG2，BNG1 只有一条链路工作，网络侧链路带宽不足可能会导致网络不通。

风险的判断方法

- 首先需要确定网络侧接口的编号，具体方法请参考网络拓扑。
- 通过 **display remote-backup-service** *rbs-name* 命令，查看回显中的“Track-interface0”字段是否有该网络侧接口。以下回显表明：
  - RBS**hw** 已经 track 网络侧接口 **GigabitEthernet2/0/5**

```
[HUAWEI] display remote-backup-service hw
------------------------------------------------------------
Service-Index    : 1
Service-Name     : hw
TCP-State        : Connected
Peer-ip          : 28.1.1.2
Source-ip        : 28.1.1.1
TCP-Port         : 6001
Track-BFD        : --
Track-interface0 : GigabitEthernet2/0/5
Weight : 10
Uplink state     : 2 (1:DOWN 2:UP)
Last up time     : 2006-07-28 10:36:16
Last down time   : 2006-07-28 10:33:50
Last down reason : TCP closed for echo time out.
Domain-map-list  : --
```

风险的恢复方案

同配置规范。

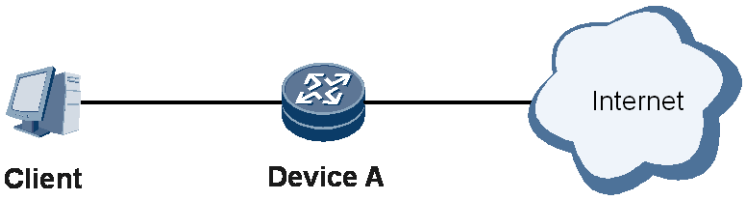
2.5 CGN 需要配置冗余备份

使用 VSUF 单板或者 VSUI 单板配置 CGN 业务时，如果未配置冗余备份，当单板发生故障时，该单板上承载的用户无法访问网络。为了避免此类现象发生，需要部署多块 VSUF/VSUI 单板，并配置 CGN 业务冗余备份。

应用场景

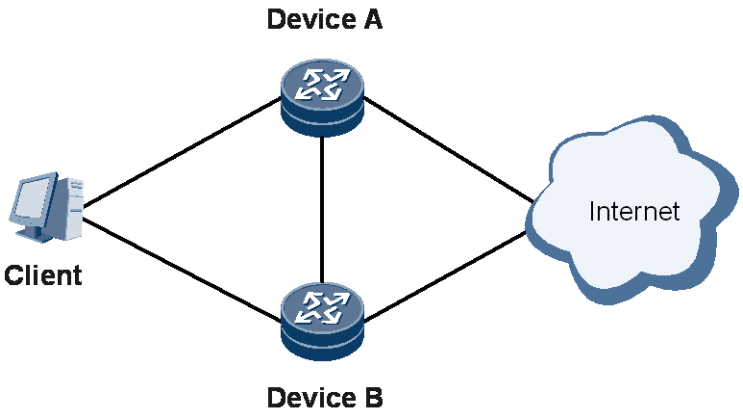
如图 2-6 所示，用户通过插有 VSUF 单板或者 VSUI 单板的 Device A 进行 CGN 转换后访问网络。

图2-6 用户通过 Device A 进行 CGN 转换后访问网络组网图



或者，如图 2-7 所示，用户通过插有 VSUF 单板或者 VSUI 单板的 Device A 和 Device B 进行 CGN 转换后访问网络。

图2-7 用户通过 Device A 和 Device B 进行 CGN 转换后访问网络组网图



配置规范

使用 VSUF 单板或者 VSUI 单板配置 CGN 业务时，需要部署多块 VSUF 单板或者 VSUI 单板，对 CGN 业务进行冗余备份。具体配置方法请参考：

- 配置 NAT 单机板间热备功能（VSUF-40/80/160、VSUI-160-E 业务板）
- 配置 NAT 双机框间热备功能（VSUF-40/80/160、VSUI-160-E 业务板）
- 配置 NAT 单机板间热备功能（VSUI-20-A 业务板）

非规范配置的影响

风险描述

当配置 CGN 业务的单板发生故障无法使用时，该单板承载的 CGN 用户无法访问网络。

风险的判断方法

对于 VSUF 单板，当前 CGN 业务的冗余备份方式分为板间备份和框间备份两种，判断风险的方法具体如下：

- 板间备份的风险判断方法如下：
  a. 在用户视图下，通过 **display device** 或 **display version slot** *slot-id* 命令查看至少有两块 VSUF 单板。

```
<HUAWEI> display device
Devicename-X8's Device status:
Slot #    Type      Online    Register     Status     Primary
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
-
1         LPU       Present   Registered   Normal     NA
2         LPU       Present   Registered   Normal     NA
5         VSU       Present   Registered   Normal     NA
8         VSU       Present   Registered   Normal     NA
9         MPU       Present   NA           Normal     Master
10        MPU       Present   Registered   Normal     Slave
11        SFU       Present   Registered   Normal     NA
12        SFU       Present   Registered   Normal     NA
13        SFU       Present   Registered   Normal     NA
14        CLK       Present   Registered   Normal     Master
15        CLK       Present   Registered   Normal     Slave
16        PWR       Present   Registered   Abnormal   NA
17        PWR       Present   Registered   Normal     NA
18        FAN       Present   Registered   Normal     NA
19        FAN       Present   Registered   Normal     NA

<HUAWEI> display version slot 5
VSU 5  : uptime is 2 days, 16 hours, 49 minutes
       StartupTime  2002/07/12  21:46:09
  Host   processor :
  SDRAM Memory Size: 4096M  bytes
  Flash Memory Size:  128M  bytes
  VSU version information
  PCB        Version : CR57VSUF80 REV B
  EPLD       Version : 109
  EPLD2      Version : 106
  EPLD3      Version : 102
  BootROM    Version : 2.30
  BootLoad   Version : 2.19
  FSURTP     Version : Version 2.1 RELEASE 0372
  FSUKERNEL  Version : Version 2.1 RELEASE 0372
  ASE        Version : 009
  MonitorBUS version information:
  Software   Version : 10.51
  Configure license items:
```

```
  2M NAT Session License

<HUAWEI> display version slot 8
VSU 8  : uptime is 0 day, 18 hours, 27 minutes
        StartupTime   2006/07/14   17:13:48
  Host    processor :
  SDRAM Memory Size: 4096M  bytes
  Flash Memory Size:  128M  bytes
  VSU version information
  PCB        Version : CR57VSUF160 REV B
  EPLD       Version : 109
  EPLD2      Version : 106
  EPLD3      Version : 102
  BootROM    Version : 2.30
  BootLoad   Version : 2.19
  FSURTP     Version : Version 2.1 RELEASE 0372
  FSUKERNEL  Version : Version 2.1 RELEASE 0372
  ASE        Version : 009
  MonitorBUS version information:
  Software   Version : 10.51
  Configure license items:
  2M NAT Session License
  20G NAT BandWidth License
```

b. 在用户视图下，通过 **display nat instance** 命令查看其绑定的 **service-location**，再使用 **display service-location** [*service-location-id*]命令查看是否有 **Backup slot ID** 字段，如果有，则有板间备份保护；如果没有，则没有板间备份保护。

```
<HUAWEI> display nat instance
nat instance dtest id 22
 port-range 4096
 service-instance-group dtest
 nat address-group dtest group-id 22
   section 0 100.100.100.0 mask 255.255.255.0
 nat outbound 2222 address-group dtest

<HUAWEI> display service-location
service-location 58
 Location slot ID: 5 engine ID: 0
 Current location slot ID: 5 engine ID: 0
 Backup slot ID: 8 engine ID: 0
 Current backup slot ID: 8 engine ID: 0
 Bound service-instance-group number: 1
 Batch-backup state: finished
```

- 框间备份的风险判断方法如下：

  在用户视图下，通过 **display nat instance** 命令查看其绑定的 **service-location**，再使用 **display service-location** [*service-location-id*]命令查看是否有 **Remote-backup interface** 字段，如果有，则有框间备份保护；如果没有，则没有框间备份保护。

```
<HUAWEI> display service-location 22
service-location 22
 Backup scene type: inter-box
 Location slot ID: 5 engine ID: 0
```

```
Remote-backup interface: GigabitEthernet2/2/1.1
Peer: 22.255.255.2
Vrrp ID: 22
Vrrp bind interface: GigabitEthernet2/2/1.1
Vrrp state: master
Bound service-instance-group number: 1
Batch-backup state: finished
```

对于 VSUI 单板，风险判断方法如下：

1. 在用户视图下，通过 **display device** 命令查看至少两块 VSUI 单板。

```
<HUAWEI> display device
Devicename-X8's Device status:
Slot #    Type      Online    Register     Status     Primary
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1         LPU       Present   Registered   Normal     NA
2         VSU       Present   Registered   Normal     NA
3         VSU       Present   Registered   Normal     NA
4         LPU       Present   Registered   Normal     NA
5         TSU       Present   Registered   Normal     NA
6         TSU       Present   Registered   Normal     NA
8         LPU       Present   Registered   Normal     NA
10        MPU       Present   NA           Normal     Master
11        SFU       Present   Registered   Normal     NA
13        SFU       Present   Registered   Normal     NA
15        CLK       Present   Registered   Normal     Master
16        PWR       Present   Registered   Normal     NA
17        PWR       Present   Registered   Normal     NA
18        FAN       Present   Registered   Normal     NA
19        FAN       Present   Registered   Normal     NA
<HUAWEI> display device 2
 slot2's detail information:
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
  Description: Integrated Versatile Service Unit 20 A(VSUI-20-A)
  Board status:      Normal
  Register:          Registered
  Uptime:            2012/07/13   11:49:55
Clock information:
  State item         State
  Current syn-clock:  10
  Syn-clock state:    Locked    VCXO_OK    REF_OK
  Syn-clock 9 state:  Inactived
  Syn-clock 10 state: Actived
Statistic information:
  Statistic item     Statistic number
  SERDES interface link lost:           0
  MPU switches:      0
  Syn-clock switches: 1
CPU0 information:
  CPU Online:        Present
  CPU Register:      Registered
  CPU SDRAM Memory Size:               4G
  CPU Utilization(%): 33%
  CPU Mem Usage(%):   28%
  VCPU Utilization
```

```
  VCPU0  :33%  VCPU1  :3 %  VCPU2  :3 %  VCPU3  :0 %
  VCPU4  :0 %  VCPU5  :0 %  VCPU6  :0 %  VCPU7  :0 %
  VCPU8  :0 %  VCPU9  :0 %  VCPU10 :0 %  VCPU11 :0 %
  VCPU12 :0 %  VCPU13 :0 %  VCPU14 :0 %  VCPU15 :0 %
  VCPU16 :0 %  VCPU17 :0 %  VCPU18 :0 %  VCPU19 :0 %
  VCPU20 :0 %  VCPU21 :0 %  VCPU22 :0 %  VCPU23 :0 %
  VCPU24 :0 %  VCPU25 :0 %  VCPU26 :0 %  VCPU27 :0 %
  VCPU28 :0 %  VCPU29 :0 %  VCPU30 :0 %  VCPU31 :0 %
CPU1 information:
  CPU Online:        Present
  CPU Register:      Registered
  CPU SDRAM Memory Size:               4G
  CPU Utilization(%): 28%
  CPU Mem Usage(%):  27%
  VCPU Utilization
  VCPU0  :28%  VCPU1  :3 %  VCPU2  :3 %  VCPU3  :0 %
  VCPU4  :0 %  VCPU5  :0 %  VCPU6  :0 %  VCPU7  :0 %
  VCPU8  :0 %  VCPU9  :0 %  VCPU10 :0 %  VCPU11 :0 %
  VCPU12 :0 %  VCPU13 :0 %  VCPU14 :0 %  VCPU15 :0 %
  VCPU16 :0 %  VCPU17 :0 %  VCPU18 :0 %  VCPU19 :0 %
  VCPU20 :0 %  VCPU21 :0 %  VCPU22 :0 %  VCPU23 :0 %
  VCPU24 :0 %  VCPU25 :0 %  VCPU26 :0 %  VCPU27 :0 %
  VCPU28 :0 %  VCPU29 :0 %  VCPU30 :0 %  VCPU31 :0 %
CPU2 information:
  CPU Online:        Present
  CPU Register:      Registered
  CPU SDRAM Memory Size:               4G
  CPU Utilization(%): 29%
  CPU Mem Usage(%):  27%
  VCPU Utilization
  VCPU0  :29%  VCPU1  :3 %  VCPU2  :3 %  VCPU3  :0 %
  VCPU4  :0 %  VCPU5  :0 %  VCPU6  :0 %  VCPU7  :0 %
  VCPU8  :0 %  VCPU9  :0 %  VCPU10 :0 %  VCPU11 :0 %
  VCPU12 :0 %  VCPU13 :0 %  VCPU14 :0 %  VCPU15 :0 %
  VCPU16 :0 %  VCPU17 :0 %  VCPU18 :0 %  VCPU19 :0 %
  VCPU20 :0 %  VCPU21 :0 %  VCPU22 :0 %  VCPU23 :0 %
  VCPU24 :0 %  VCPU25 :0 %  VCPU26 :0 %  VCPU27 :0 %
  VCPU28 :0 %  VCPU29 :0 %  VCPU30 :0 %  VCPU31 :0 %
CPU3 information:
  CPU Online:        Present
  CPU Register:      Registered
  CPU SDRAM Memory Size:               4G
  CPU Utilization(%): 29%
  CPU Mem Usage(%):  27%
  VCPU Utilization
  VCPU0  :29%  VCPU1  :3 %  VCPU2  :3 %  VCPU3  :0 %
  VCPU4  :0 %  VCPU5  :0 %  VCPU6  :0 %  VCPU7  :0 %
  VCPU8  :0 %  VCPU9  :0 %  VCPU10 :0 %  VCPU11 :0 %
  VCPU12 :0 %  VCPU13 :0 %  VCPU14 :0 %  VCPU15 :0 %
  VCPU16 :0 %  VCPU17 :0 %  VCPU18 :0 %  VCPU19 :0 %
  VCPU20 :0 %  VCPU21 :0 %  VCPU22 :0 %  VCPU23 :0 %
  VCPU24 :0 %  VCPU25 :0 %  VCPU26 :0 %  VCPU27 :0 %
  VCPU28 :0 %  VCPU29 :0 %  VCPU30 :0 %  VCPU31 :0 %
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

2. 在用户视图下，通过 **display nat instance** 命令查看配置，是否有“add slot x slave”或者“nat address-group xxx rui-slave metric xx”字段，如果有其一，则说明 CGN 业务配置了冗余备份；如果都没有，则无冗余备份。

```
<HUAWEI> display nat instance
nat instance nat444-1
 nat filter mode full-cone
 port-range 4096
 add slot 2 master
 add slot 3 slave
 nat address-group addressgroup1
  section 0 182.148.135.0 mask 24
 nat outbound 2080 address-group addressgroup1
```

风险的恢复方案

同配置规范。

2.6 GRE 需要配置冗余备份

应用场景

使用 GRE 隧道的场景。

配置规范

当设备上配置多块隧道业务板时，可以通过命令 **target-board** *slot-number* **backup** *slot-numer2* 参数指定备份隧道业务板配置 GRE 隧道的 1：1 保护功能，增强 GRE 业务的可靠性。配置 GRE 隧道的 1：1 保护功能后，必须在主用和备用隧道业务板上配置两条同源同宿的 GRE 隧道。当主板上的隧道工作时，备板上的隧道不工作，当主用隧道业务板故障时，业务切换到备用隧道业务板上的 GRE 隧道。具体配置方法请参考：GRE 协议配置。

非规范配置的影响

风险描述

当配置 GRE 业务的单板发生故障无法使用时，该单板承载的 GRE 业务无法访问网络。

风险的判断方法

通过 **display tunnel gre backup** 命令查看 GRE 的备份绑定信息。如果没有“Tunnel binding slave slot”信息，则说明没有配置 GRE 备份板。

```
<HUAWEI> display tunnel gre backup
GRE tunnel backup binding information:
Tunnel binding master slot:  1
Tunnel binding slave slot:   2
Tunnel processing slot:      1
```

风险的恢复方案

同配置规范。

2.7 L2TP 需要配置冗余备份

应用场景

使用 L2TP 隧道的场景。

配置规范

一个 LNS 组可指定多块隧道板，多块隧道板之间基于隧道进行轮换式的负载分担。当设备上配置多块隧道业务板时，可以在 LNS 组视图下通过命令 **bind slot** *slot-id* 在 LNS 备份组下绑定 2 块及以上隧道板，实现备份。具体配置方法请参考：配置 LNS 侧的隧道参数。

非规范配置的影响

风险描述

当配置 L2TP 业务的单板发生故障无法使用时，该单板承载的 L2TP 业务无法访问网络。

风险的判断方法

通过 **display lns-group all** 命令查看 LNS 组绑定的接口和隧道板。如果一个 LNS 组绑定的槽位号只有一个，则说明没有配置 L2TP 备份板。

```
<HUAWEI> display lns-group all
------------------------------------------------------
 GroupNum GroupName    Interface           AllSlot
 0         lns1        Loopback0            ----
 1         test        Loopback1           2
 ------------------------------------------------------
```

风险的恢复方案

同配置规范。

2.8 Hybrid Access 需要配置冗余备份

应用场景

使用 Hybrid Access 的场景。

配置规范

当设备上配置多块业务板时，可以在用户视图下通过命令 **set board-type slot** *slot-id* **hybrid-access** 配置 2 块及以上业务板的工作模式为 **hybrid-access**，实现备份。具体配置方法请参考：配置 VSUF 保序功能。

非规范配置的影响

风险描述

当配置 Hybrid Access 业务的单板发生故障无法使用时，该单板承载的 Hybrid Access 业务无法访问网络。

风险的判断方法

通过 **display board-type** 命令查看设备上已注册业务处理板当前的业务模式。如果 Hybrid Access 类型的槽位号只有一个，则说明没有配置 Hybrid Access 备份板。

```
<HUAWEI> display board-type
Devicename's board-type:
Slot     board-type

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1        Hybrid-access
2        Netstream
3        LPU
```

风险的恢复方案

同配置规范。