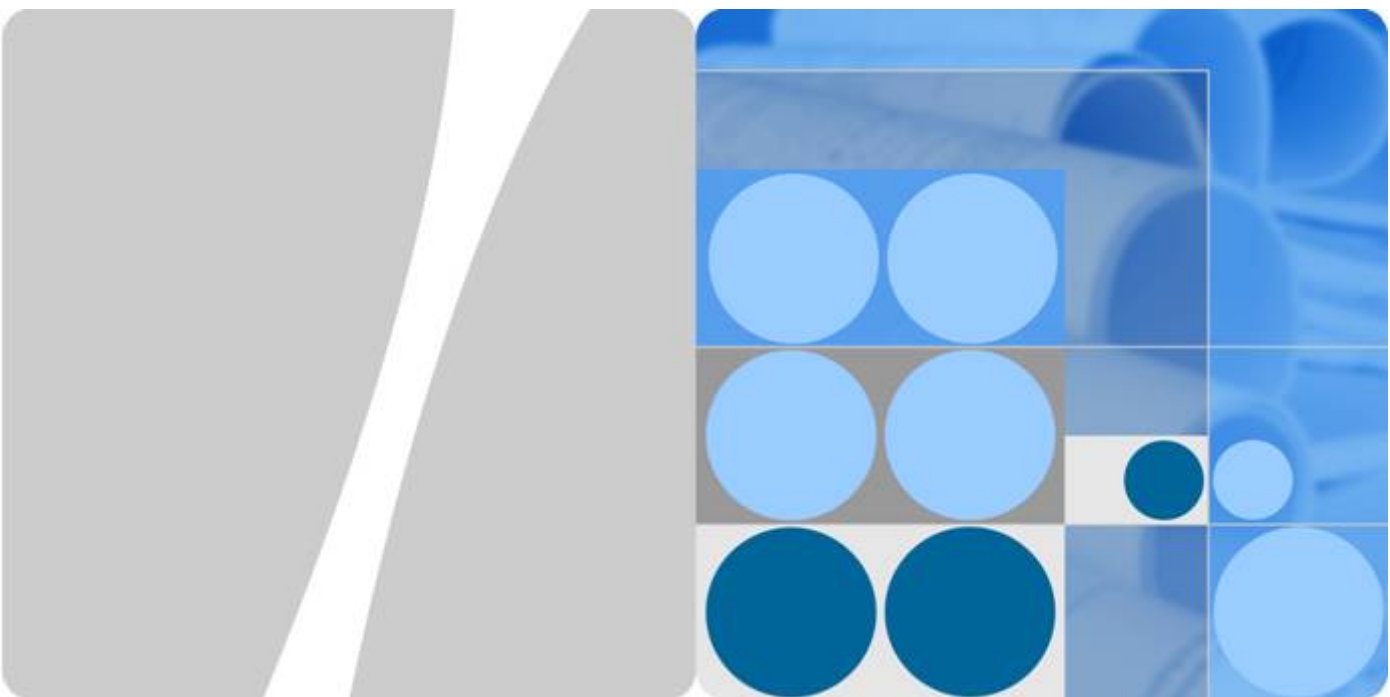




HUAWEI NetEngine80E/40E 路由器

V600R003C00

配置指南-可靠性

文档版本 02

发布日期 2011-09-10

版权所有 © 华为技术有限公司 2011。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

华为技术有限公司

地址：深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址：<http://www.huawei.com>

客户服务邮箱：support@huawei.com

客户服务电话：4008302118

前言

概述

本文档针对 NE80E/40E 中的可靠性配置，从功能介绍、配置方法、维护和配置举例方面进行介绍，包含可靠性概述、接口备份配置、APS 配置、VRRP 配置、BFD 配置、GR 配置、NSR 配置、以太网 OAM 配置、Y.1731 配置、MPLS-TP OAM 配置、多机备份配置。

本文档指导产品的配置过程，供用户参考。

 说明

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

产品版本

与本文档相对应的产品版本如下所示。

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

读者对象

本文档（本指南）主要适用于以下工程师：

- 调测工程师
- 数据配置工程师
- 网络监控工程师
- 系统维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

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

修订记录

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

文档版本 02 (2011-09-10)

第二次正式发布，文档内容更新如下：

- **APS 配置**
 - 由于新增 APS 1+1 双向倒换保护模式特性，在 [3.2.4（可选）配置 APS Group 的工作模式](#)、[3.3.4 配置 APS Group 的工作模式](#) 中新增 APS 1+1 双向倒换保护模式命令关键字和描述。
 - 在 [3.2.3 配置 APS Group 的保护接口](#)、[3.3.3 配置 APS Group 的保护接口](#) 中，新增配置 APS 保护接口 K 字节中端口信号故障请求码的优先级为低优先级的命令关键字和描述。
- **Y.1731 配置**
 - 本章新增 [9.10.12 配置基于 QoS 简单流分类的 Y.1731 统计功能示例](#)。

文档版本 01 (2011-05-30)

第一次正式发布。

目录

前言.....	ii
1 可靠性概述.....	1
1.1 可靠性简介.....	2
1.1.1 可靠性技术概述.....	2
1.1.2 可靠性度量指标.....	2
1.1.3 可靠性需求级别.....	3
1.1.4 高可靠 IP 网络组网原则.....	3
1.2 IP 网络可靠性技术.....	3
1.2.1 IP 网络故障检测技术.....	3
1.2.2 IP 网络保护倒换技术.....	4
1.3 NE80E/40E 支持的可靠性技术.....	4
1.3.1 FRR（Fast ReRoute）.....	4
1.3.2 OAM（Operation Administration & Maintenance）.....	6
1.3.3 VRRP（Virtual Router Redundancy Protocol）.....	6
1.3.4 BFD（Bidirectional Forwarding Detection）.....	7
1.4 IP 网络可靠性组网方案.....	7
1.4.1 中间节点故障或中间节点相邻链路故障-LDP/TE FRR.....	7
1.4.2 传输中间链路故障.....	8
1.4.3 远端接入端点路由器故障-VPN FRR.....	9
1.4.4 接入端点路由器下行接口故障——IP FRR.....	10
2 接口备份配置.....	11
2.1 接口备份简介.....	12
2.1.1 接口备份概述.....	12
2.1.2 NE80E/40E 支持的接口备份特性.....	13
2.2 配置主备接口备份.....	14
2.2.1 建立配置任务.....	14
2.2.2 指定主接口使用的备份接口.....	15
2.2.3 配置主/备接口切换的延时.....	15
2.2.4 检查配置结果.....	15
2.3 配置负载分担接口备份.....	16
2.3.1 建立配置任务.....	16
2.3.2 指定主接口使用的备份接口.....	17

2.3.3 配置负载分担的百分比门限.....	17
2.3.4 （可选）配置主接口的带宽、流量检测时间间隔.....	18
2.3.5 检查配置结果.....	18
2.4 维护接口备份.....	19
2.4.1 监控接口备份运行状况.....	19
2.5 配置举例.....	19
2.5.1 配置主备接口备份示例.....	20
2.5.2 配置负载分担接口备份示例.....	23
3 APS 配置.....	27
3.1 简介.....	28
3.1.1 APS 概述.....	28
3.1.2 NE80E/40E 支持的 APS 特性.....	30
3.2 配置单机 APS.....	30
3.2.1 建立配置任务.....	31
3.2.2 配置 APS Group 的工作接口.....	31
3.2.3 配置 APS Group 的保护接口.....	32
3.2.4 （可选）配置 APS Group 的工作模式.....	32
3.2.5 （可选）配置 APS Group 的倒换模式.....	33
3.2.6 （可选）配置 APS Group 的倒回等待时间.....	33
3.2.7 将 APS Group 成员加入 Trunk.....	34
3.2.8 检查配置结果.....	34
3.3 配置 E-APS.....	35
3.3.1 建立配置任务.....	35
3.3.2 配置 APS Group 的工作接口.....	36
3.3.3 配置 APS Group 的保护接口.....	37
3.3.4 配置 APS Group 的工作模式.....	37
3.3.5 （可选）配置 APS Group 的倒换模式.....	38
3.3.6 （可选）配置发送 APS 协商报文的时间间隔和保持连接状态的时间.....	39
3.3.7 （可选）配置 PGP 协议认证字符串.....	39
3.3.8 （可选）配置 APS Group 的倒回等待时间.....	40
3.3.9 将 APS Group 成员加入 Trunk.....	40
3.3.10 检查配置结果.....	41
3.4 配置举例.....	42
3.4.1 配置 CPOS 接口下基于 APS 的 TDM 功能.....	42
3.4.2 配置 CPOS-Trunk 的 APS 保护倒换示例.....	49
3.4.3 配置 PW Redundancy 与 E-APS 1:1 保护联动示例.....	52
4 VRRP 配置.....	66
4.1 VRRP 简介.....	68
4.1.1 VRRP 概述.....	68
4.1.2 NE80E/40E 支持的 VRRP 特性.....	68
4.2 配置 VRRP 备份组.....	71

4.2.1 建立配置任务.....	71
4.2.2 创建备份组并配置虚拟 IP 地址.....	72
4.2.3 配置接口在备份组中的优先级.....	74
4.2.4 检查配置结果.....	75
4.3 配置 VRRP 监视接口状态.....	76
4.3.1 建立配置任务.....	76
4.3.2 配置 VRRP 监视接口状态.....	77
4.3.3 检查配置结果.....	78
4.4 配置 VRRP 快速切换（普通方式）	79
4.4.1 建立配置任务.....	80
4.4.2 监视 BFD 会话状态.....	80
4.4.3 监视 BFD 会话状态.....	82
4.4.4 监视 SPU-Group 状态.....	84
4.4.5 检查配置结果.....	85
4.5 配置 VRRP 快速切换（使用 BFD Sampling）	86
4.5.1 建立配置任务.....	86
4.5.2 配置业务 VRRP 监视管理 VRRP 状态.....	88
4.5.3 配置管理 VRRP 监视 BFD 会话状态.....	88
4.5.4 配置管理 VRRP 切换的阈值.....	90
4.5.5 配置管理 VRRP 状态变化和路由的联动功能.....	90
4.5.6 检查配置结果.....	91
4.6 配置管理 VRRP 忽略接口 Down 事件功能.....	92
4.6.1 建立配置任务.....	92
4.6.2 配置管理 VRRP 备份组.....	94
4.6.3 配置业务 VRRP 监视管理 VRRP 状态.....	94
4.6.4 配置管理 VRRP 监视 BFD 会话状态.....	95
4.6.5 配置管理 VRRP 切换的阈值.....	96
4.6.6 配置管理 VRRP 状态变化和路由的联动功能.....	96
4.6.7 检查配置结果.....	97
4.7 配置 VRRP 在 VLANIF 的应用.....	98
4.7.1 建立配置任务.....	98
4.7.2 配置 VLANIF 上的 VRRP.....	98
4.7.3 （可选）super-VLAN 中 VRRP 报文发送方式.....	99
4.7.4 检查配置结果.....	99
4.8 配置 VRRP 安全功能.....	100
4.8.1 建立配置任务.....	100
4.8.2 配置 VRRP 报文认证方式.....	101
4.8.3 检查配置结果.....	101
4.9 配置 VRRP 平滑倒换功能.....	102
4.9.1 建立配置任务.....	102
4.9.2 配置 VRRP 平滑倒换功能.....	103
4.9.3 检查配置结果.....	103

4.10 调整优化 VRRP.....	104
4.10.1 建立配置任务.....	104
4.10.2 配置发送 VRRP 通告报文的时间间隔.....	105
4.10.3 设置备份组中路由器的抢占延迟时间.....	106
4.10.4 使能虚拟地址可达性测试开关.....	107
4.10.5 禁止检测 VRRP 报文的跳数.....	108
4.10.6 配置 Master 发送免费 ARP 报文的超时时间.....	108
4.10.7 检查配置结果.....	109
4.11 配置管理 VRRP 备份组.....	110
4.11.1 建立配置任务.....	110
4.11.2 配置管理 VRRP 备份组.....	111
4.11.3 （可选）配置成员 VRRP 备份组并将其与管理 VRRP 备份组绑定.....	112
4.11.4 （可选）配置业务接口与管理 VRRP 备份组绑定.....	113
4.11.5 （可选）配置 VPLS 方式 PW 与管理 VRRP 备份组绑定.....	113
4.11.6 检查配置结果.....	114
4.12 配置 VRRP 协议版本升级.....	115
4.12.1 建立配置任务.....	115
4.12.2 配置 VRRPv3 版本.....	115
4.12.3 检查配置结果.....	116
4.13 维护 VRRP.....	116
4.13.1 监控 VRRP 运行状况.....	116
4.14 配置举例.....	117
4.14.1 配置主备备份 VRRP 示例.....	117
4.14.2 配置负载分担 VRRP 示例.....	121
4.14.3 配置多实例 VRRP 示例.....	125
4.14.4 配置 VRRP 快速切换功能示例.....	130
4.14.5 配置 VRRP 快速切换示例（使用单臂 ECHO 功能）.....	135
4.14.6 配置 VRRP 快速切换（使用 BFD Sampling）.....	141
4.14.7 配置管理 VRRP 忽略接口 Down 事件功能.....	159
4.14.8 配置 VRRP 在 VLANIF 中的应用示例.....	178
4.14.9 配置 QinQ 终结子接口支持 VRRP 示例（控制免费 ARP 报文方式）.....	185
4.14.10 配置 QinQ 终结子接口支持 VRRP6 示例（控制 ND 报文方式）.....	193
4.14.11 配置主备备份 VRRP6 示例.....	201
4.14.12 配置负载分担 VRRP6 示例.....	205
5 BFD 配置.....	210
5.1 BFD 简介.....	212
5.1.1 BFD 概述.....	212
5.1.2 NE80E/40E 支持的 BFD 特性.....	212
5.2 配置 BFD 单跳检测.....	219
5.2.1 建立配置任务.....	219
5.2.2 使能全局 BFD 功能.....	219
5.2.3 建立 BFD 会话.....	220

5.2.4 检查配置结果.....	221
5.3 配置 BFD 被动回声功能.....	222
5.3.1 建立配置任务.....	223
5.3.2 配置 BFD 被动回声功能.....	223
5.3.3 检查配置结果.....	224
5.4 配置 BFD 状态与接口状态联动.....	225
5.4.1 建立配置任务.....	225
5.4.2 配置 BFD 状态与接口状态联动.....	226
5.4.3 检查配置结果.....	226
5.5 配置 BFD 状态与子接口状态联动.....	227
5.5.1 建立配置任务.....	227
5.5.2 配置 BFD 会话状态与子接口状态联动.....	228
5.5.3 检查配置结果.....	229
5.6 配置 BFD 修改端口状态表.....	230
5.6.1 建立配置任务.....	230
5.6.2 使能 BFD 修改端口状态表.....	231
5.6.3 检查配置结果.....	231
5.7 配置 BFD 多跳检测.....	232
5.7.1 建立配置任务.....	232
5.7.2 使能全局 BFD 功能.....	233
5.7.3 建立 BFD 会话.....	233
5.7.4 检查配置结果.....	234
5.8 配置静态标识符自协商 BFD.....	235
5.8.1 建立配置任务.....	235
5.8.2 使能全局 BFD 功能.....	236
5.8.3 建立 BFD 会话.....	236
5.8.4 检查配置结果.....	237
5.9 配置 BFD 会话延迟 UP 功能.....	238
5.9.1 建立配置任务.....	238
5.9.2 配置 BFD 会话延迟 UP 功能.....	238
5.9.3 检查配置结果.....	239
5.10 配置单臂 ECHO 功能.....	240
5.10.1 建立配置任务.....	240
5.10.2 使能全局 BFD 功能.....	241
5.10.3 建立 BFD 会话.....	241
5.10.4 检查配置结果.....	242
5.11 调整 BFD 检测参数.....	243
5.11.1 建立配置任务.....	243
5.11.2 调整 BFD 检测时间.....	243
5.11.3 配置 BFD 等待恢复时间.....	244
5.11.4 配置 BFD 会话的描述信息.....	245
5.11.5 检查配置结果.....	245

5.12 配置全局多跳端口号功能.....	247
5.12.1 建立配置任务.....	247
5.12.2 配置全局多跳端口号.....	247
5.12.3 检查配置结果.....	248
5.13 配置全局 TTL 功能.....	249
5.13.1 建立配置任务.....	249
5.13.2 配置全局 TTL.....	249
5.13.3 检查配置结果.....	250
5.14 配置 Trap 消息定时器的时间间隔.....	250
5.14.1 建立配置任务.....	250
5.14.2 配置发送告警消息定时器的时间间隔.....	251
5.14.3 检查配置结果.....	251
5.15 维护 BFD.....	252
5.15.1 清除 BFD 的统计数据.....	252
5.15.2 监控 BFD 运行状况.....	252
5.16 配置举例.....	253
5.16.1 配置三层物理链路单跳检测示例.....	253
5.16.2 配置 IP-Trunk 成员链路单跳检测示例.....	256
5.16.3 配置 IP-Trunk 单跳检测示例.....	260
5.16.4 配置三层 Eth-Trunk 成员链路单跳检测示例.....	266
5.16.5 配置三层 Eth-Trunk 单跳检测示例.....	271
5.16.6 配置 VLANIF 接口单跳检测示例.....	277
5.16.7 配置 BFD 状态与接口状态联动示例.....	281
5.16.8 配置 BFD 状态与子接口状态联动示例.....	285
5.16.9 配置 BFD 多跳检测示例.....	290
5.16.10 配置 BFD 查询模式示例.....	292
5.16.11 配置单臂 ECHO 功能示例.....	295
5.16.12 配置 BFD 检测 VPN 路由示例.....	298
5.16.13 配置 Dot1q 终结子接口支持 BFD 示例.....	303
5.16.14 配置 QinQ 终结子接口支持 BFD 示例.....	309
5.16.15 配置三层物理链路单跳检测示例（BFD6）.....	317
5.16.16 配置 BFD 多跳检测示例（BFD6）.....	319
6 GR 配置.....	324
6.1 GR 简介.....	325
6.1.1 HA 概述.....	325
6.1.2 NE80E/40E 中的 GR 特性.....	331
6.2 配置系统级 GR.....	332
6.2.1 建立配置任务.....	332
6.2.2 （可选）设置缺省的备板槽位号.....	332
6.2.3 使能主备板配置数据自动同步功能.....	333
6.2.4 使能强制主备倒换功能.....	333
6.2.5 （可选）重启备板.....	334

6.2.6 检查配置结果.....	334
6.3 维护 HA.....	334
6.3.1 监控 HA 运行状况.....	334
6.4 配置举例.....	335
6.4.1 配置系统级 GR 示例.....	335
7 NSR 配置.....	340
7.1 NSR 简介.....	341
7.1.1 NSR 概述.....	341
7.1.2 NE80E/40E 支持的 NSR 特性.....	342
7.2 配置 NSR.....	342
7.2.1 建立配置任务.....	343
7.2.2 使能 NSR 功能.....	343
7.2.3 检查配置结果.....	344
8 以太网 OAM 配置.....	345
8.1 以太网 OAM 简介.....	347
8.1.1 以太网 OAM 概述.....	347
8.1.2 NE80E/40E 支持的以太网 OAM.....	347
8.2 配置 EFM OAM 基本功能.....	355
8.2.1 建立配置任务.....	355
8.2.2 全局使能 EFM OAM 功能.....	356
8.2.3 配置接口的 EFM OAM 工作模式.....	356
8.2.4 （可选）配置 EFM OAM 协议报文的最大尺寸.....	357
8.2.5 （可选）配置 EFM OAM 协议报文接收超时时间.....	357
8.2.6 使能接口的 EFM OAM 功能.....	357
8.2.7 检查配置结果.....	358
8.3 配置 EFM OAM 链路监控.....	359
8.3.1 建立配置任务.....	359
8.3.2 （可选）配置 EFM OAM 误帧检测.....	359
8.3.3 （可选）配置 EFM OAM 误码检测.....	360
8.3.4 （可选）配置 EFM OAM 误帧秒检测.....	360
8.3.5 检查配置结果.....	361
8.4 配置物理链路丢包率检测.....	362
8.4.1 建立配置任务.....	362
8.4.2 配置 EFM OAM 远端环回.....	363
8.4.3 发送测试报文.....	363
8.4.4 查看测试报文的返回统计.....	364
8.4.5 （可选）手动取消 EFM OAM 远端环回.....	364
8.4.6 检查配置结果.....	365
8.5 配置 EFM OAM 和接口联动.....	366
8.5.1 建立配置任务.....	366
8.5.2 配置 EFM OAM 和接口联动.....	367

8.5.3 检查配置结果.....	367
8.6 配置以太网 CFM 基本功能.....	368
8.6.1 建立配置任务.....	368
8.6.2 切换版本.....	370
8.6.3 全局使能以太网 CFM 功能.....	370
8.6.4 创建 MD.....	370
8.6.5 （可选）创建默认 MD.....	371
8.6.6 创建 MA.....	371
8.6.7 创建 MEP.....	372
8.6.8 配置 RMEP.....	373
8.6.9 （可选）配置 MIP 生成规则.....	374
8.6.10 配置 CC 检测.....	375
8.6.11 （可选）创建指定 VLAN.....	376
8.6.12 检查配置结果.....	376
8.7 配置以太网 CFM 的相关参数.....	380
8.7.1 建立配置任务.....	380
8.7.2 （可选）配置 RMEP 激活时间.....	381
8.7.3 （可选）配置告警恢复防抖时间.....	381
8.7.4 （可选）配置告警产生防抖时间.....	382
8.8 配置以太网的故障确认.....	382
8.8.1 建立配置任务.....	382
8.8.2 （可选）执行 802.1ag MAC Ping.....	383
8.8.3 （可选）执行通用 Gmac ping.....	384
8.9 配置以太网的故障定位.....	384
8.9.1 建立配置任务.....	384
8.9.2 （可选）执行 802.1ag MAC Trace.....	385
8.9.3 （可选）执行通用 Gmac trace.....	386
8.10 配置以太网 CFM 和接口联动.....	387
8.10.1 建立配置任务.....	387
8.10.2 配置以太网 CFM 和接口联动.....	389
8.10.3 检查配置结果.....	390
8.11 配置 EFM OAM 和以太网 CFM 之间的联动.....	390
8.11.1 建立配置任务.....	390
8.11.2 配置 ETH OAM 联动.....	391
8.11.3 检查配置结果.....	392
8.12 配置以太网 CFM 和 VPLS 的组合应用.....	392
8.12.1 建立配置任务.....	392
8.12.2 在 PE 和 PE 之间配置基于 VPLS 的以太网 CFM 功能.....	393
8.12.3 在 CE 和本端 PE 之间配置以太网 CFM 功能.....	394
8.12.4 在 CE 和对端 PE 之间配置以太网 CFM 功能.....	395
8.12.5 检查配置结果.....	395
8.13 配置以太网 CFM 和 VLL 的组合应用（使用 QinQ 终结子接口）.....	395

8.13.1 建立配置任务.....	395
8.13.2 在 PE 和 PE 之间配置基于 VLL 的以太网 CFM 功能.....	397
8.13.3 在 Switch 和本端 PE 之间配置以太网 CFM 功能.....	398
8.13.4 在 Switch 和对端 PE 之间配置以太网 CFM 功能.....	399
8.13.5 检查配置结果.....	400
8.14 配置以太网 CFM 和 VPLS 的组合应用（使用 QinQ 终结子接口）	401
8.14.1 建立配置任务.....	401
8.14.2 在 PE 和 PE 之间配置基于 VPLS 的以太网 CFM 功能.....	403
8.14.3 在 Switch 和本端 PE 之间配置以太网 CFM 功能.....	404
8.14.4 在 Switch 和对端 PE 之间配置以太网 CFM 功能.....	404
8.14.5 检查配置结果.....	404
8.15 配置 ETH OAM 和 MPLS OAM/BFD 组合应用.....	406
8.15.1 建立配置任务.....	406
8.15.2 配置 ETH OAM 功能.....	407
8.15.3 配置 ETH OAM 和 MPLS OAM/BFD 的联动.....	408
8.15.4 检查配置结果.....	408
8.16 配置以太网 CFM 和组播 VLAN 1+1 保护功能.....	409
8.17 维护以太网 OAM.....	409
8.17.1 清除错误 CCM 消息统计信息.....	409
8.17.2 监控以太网 OAM 运行状况.....	409
8.18 配置举例.....	410
8.18.1 配置 EFM OAM 示例.....	410
8.18.2 配置链路丢包率检测示例.....	413
8.18.3 配置以太网 CFM 基本功能示例.....	416
8.18.4 配置以太网 CFM 默认 MD 功能示例.....	424
8.18.5 配置以太网 CFM 和接口联动示例.....	432
8.18.6 配置 EFM OAM 和以太网 CFM 联动示例.....	437
8.18.7 配置基于 VPLS 的以太网 CFM 示例.....	441
8.18.8 配置基于 VPLS 的以太网 CFM 示例（使用 QinQ 终结子接口）	452
8.18.9 配置基于 VLL 的以太网 CFM 示例（使用 QinQ 终结子接口）	465
8.18.10 配置 EFM OAM 与 MPLS OAM 联动功能示例.....	474
8.18.11 配置 EFM OAM 扩展 FOR VRRP 示例.....	484
8.18.12 配置 EFM OAM 扩展 FOR 静态路由示例.....	493
9 Y.1731 配置.....	504
9.1 Y.1731 简介.....	506
9.1.1 Y.1731 概述.....	506
9.1.2 NE80E/40E 支持的 Y.1731 特性.....	509
9.2 配置 VLL 的单端丢包统计功能.....	509
9.2.1 建立配置任务.....	509
9.2.2 配置 MA 与 VLL 绑定.....	511
9.2.3 配置对端设备接收 LMM 报文功能.....	512
9.2.4 使能 VLL 的单端丢包统计功能.....	512

9.2.5 检查配置结果.....	514
9.3 配置 VLL 的双端丢包统计功能.....	516
9.3.1 建立配置任务.....	516
9.3.2 配置 MA 与 VLL 绑定.....	517
9.3.3 使能 VLL 的双端丢包统计功能.....	518
9.3.4 检查配置结果.....	519
9.4 配置 VLL 的单向时延统计功能.....	519
9.4.1 建立配置任务.....	519
9.4.2 配置 MA 与 VLL 绑定.....	521
9.4.3 配置对端设备接收 DM 报文功能.....	522
9.4.4 使能 VLL 的单向时延统计功能.....	522
9.4.5 检查配置结果.....	524
9.5 配置 VLL 的双向时延统计功能.....	525
9.5.1 建立配置任务.....	525
9.5.2 配置 MA 与 VLL 绑定.....	526
9.5.3 配置对端设备接收 DMM 报文功能.....	528
9.5.4 使能 VLL 的双向时延统计功能.....	528
9.5.5 检查配置结果.....	530
9.6 配置 VPLS 的单端丢包统计功能.....	531
9.6.1 建立配置任务.....	531
9.6.2 配置 MA 与 VPLS 绑定.....	532
9.6.3 配置对端设备接收 LMM 报文功能.....	532
9.6.4 使能 VPLS 的单端丢包统计功能.....	533
9.6.5 检查配置结果.....	534
9.7 配置 VPLS 的双端丢包统计功能.....	534
9.7.1 建立配置任务.....	534
9.7.2 配置 MA 与 VPLS 绑定.....	536
9.7.3 使能 VPLS 的双端丢包统计功能.....	536
9.7.4 检查配置结果.....	536
9.8 配置 VPLS 的单向时延统计功能.....	537
9.8.1 建立配置任务.....	537
9.8.2 配置 MA 与 VPLS 绑定.....	538
9.8.3 配置对端设备接收 DM 报文功能.....	539
9.8.4 使能 VPLS 的单向时延统计功能.....	539
9.8.5 检查配置结果.....	540
9.9 配置 VPLS 的双向时延统计功能.....	540
9.9.1 建立配置任务.....	541
9.9.2 配置 MA 与 VPLS 绑定.....	542
9.9.3 配置对端设备接收 DMM 报文功能.....	542
9.9.4 使能 VPLS 的双向时延统计功能.....	543
9.9.5 检查配置结果.....	543
9.10 配置举例.....	544

9.10.1 配置 VLL 的单端丢包统计功能示例（按需统计）	544
9.10.2 配置 VLL 的单端丢包统计功能示例（连续统计）	548
9.10.3 配置 VLL 的双端丢包统计功能示例（连续统计）	552
9.10.4 配置 VLL 的单向时延统计功能示例（按需统计）	556
9.10.5 配置 VLL 的单向时延统计功能示例（连续统计）	559
9.10.6 配置 VLL 的双向时延统计功能示例（按需统计）	564
9.10.7 配置 VLL 的双向时延统计功能示例（连续统计）	567
9.10.8 配置 VPLS 的单端丢包统计功能示例（按需统计）	571
9.10.9 配置 VPLS 的双端丢包统计功能示例（连续统计）	576
9.10.10 配置 VPLS 的单向时延统计功能示例（按需统计）	580
9.10.11 配置 VPLS 的双向时延统计功能示例（按需统计）	585
9.10.12 配置基于 QoS 简单流分类的 Y.1731 统计功能示例	590
10 MPLS-TP OAM 配置	598
10.1 MPLS-TP OAM 简介	599
10.1.1 MPLS-TP OAM 概述	599
10.1.2 NE80E/40E 支持的 MPLS-TP OAM 特性	600
10.2 配置 LSP 的 MPLS-TP OAM 功能	601
10.2.1 建立配置任务	601
10.2.2 配置 ME 实例和接口绑定	603
10.2.3 （可选）配置 LSP 持续连通性和转发故障检测（CC/CV）功能	604
10.2.4 （可选）配置 LSP 按需连通性检测（LB）功能	605
10.2.5 （可选）配置 LSP 丢包率统计（LM）功能	606
10.2.6 （可选）配置 LSP 时延和抖动统计（DM）功能	607
10.2.7 （可选）配置 LSP 告警抑制（AIS）功能	609
10.2.8 检查配置结果	609
10.3 配置 PW 的 MPLS-TP OAM 功能	611
10.3.1 建立配置任务	611
10.3.2 配置 ME 实例和 PW 绑定	613
10.3.3 （可选）配置 PW 持续连通性和转发故障检测（CC/CV）功能	614
10.3.4 （可选）配置 PW 按需连通性检测（LB）功能	615
10.3.5 （可选）配置 PW 丢包率统计（LM）功能	615
10.3.6 （可选）配置 PW 时延和抖动统计（DM）功能	617
10.3.7 检查配置结果	618
10.4 配置举例	621
10.4.1 配置 LSP 持续连通性和转发故障检测（CC/CV）功能示例	621
10.4.2 配置 LSP 按需连通性检测（LB）功能示例	625
10.4.3 配置 LSP 丢包率统计（LM）功能示例	628
10.4.4 配置 LSP 时延和抖动统计（DM）功能示例	632
10.4.5 配置 LSP 告警指示信号（AIS）功能示例	636
10.4.6 配置 PW 持续连通性和转发故障检测（CC/CV）功能示例	639
10.4.7 配置 PW 按需连通性检测（LB）功能示例	644
10.4.8 配置 PW 丢包率统计（LM）功能示例	647

10.4.9 配置 PW 时延和抖动统计（DM）功能示例.....	652
11 多机备份配置.....	657
11.1 简介.....	658
11.1.1 多机备份概述.....	658
11.1.2 NE80E/40E 支持的多机备份特性.....	658
11.2 建立多机备份平台.....	659
11.2.1 建立配置任务.....	659
11.2.2 配置 VRRP.....	660
11.2.3 配置远端备份服务.....	661
11.2.4 配置远端备份策略.....	662
11.2.5 检查配置结果.....	662
11.3 配置 ARP 双机热备.....	663
11.3.1 建立配置任务.....	663
11.3.2 配置远端备份策略支持备份 ARP 业务.....	664
11.3.3 将远端备份策略绑定到接口下.....	664
11.3.4 检查配置结果.....	664
11.4 维护.....	665
11.4.1 显示备份信息.....	665
11.4.2 清除备份信息.....	666
11.5 配置举例.....	666
11.5.1 配置 ARP 双机热备示例.....	666
A 术语.....	671
B 缩略语.....	675

1 可靠性概述

关于本章

主要从两个方面提高网络的可靠性，一种是使用有效的检测机制实现 FRR，另一种是可靠性的组网方案。

1.1 可靠性简介

可靠性是降低网络中断时间、提高网络性能的一项技术。

1.2 IP 网络可靠性技术

从故障检测技术和网络倒换技术两方面介绍可靠性技术。

1.3 NE80E/40E 支持的可靠性技术

可靠性技术主要包括两个方面：IP 网络故障检测技术和 IP 网络保护倒换技术。

1.4 IP 网络可靠性组网方案

IP 网络可靠性组网方案主要介绍 FRR 的各种应用场景及解决方案。

1.1 可靠性简介

可靠性是降低网络中断时间、提高网络性能的一项技术。

1.1.1 可靠性技术概述

可靠性技术是实现高可靠性的一系列技术。它主要涉及到系统及硬件可靠性设计方法、软件可靠性设计方法、可靠性测试验证方法和 IP 网络可靠性设计。

对于路由器而言，可靠性问题涉及以下几个方面：

- 系统及硬件可靠性设计方法
- 软件可靠性设计方法
- 可靠性测试验证方法
- IP 网络可靠性设计

随着网络的快速普及和应用的日益深入，各种增值业务在网络上得到了广泛部署，网络带宽也以指数级增长，网络短时间的中断就可能影响大量业务，造成重大损失。

作为业务承载主体的基础网络，其可靠性也因此成为日益关注的焦点。

本文关注的是 NE80E/40E 上实现的 IP 网络可靠性技术。

1.1.2 可靠性度量指标

可靠性度量指标包括：MTTR、MTBF 和可用度。

通常使用平均修复时间 MTTR（Mean Time to Repair）和平均故障间隔时间 MTBF（Mean Time Between Failure）这两个指标来评价产品或系统的可靠性。

MTTR

MTTR（Mean Time to Repair），平均修复时间，从可维护性方面标识故障的恢复能力。指一个组件或设备从故障到恢复正常所需的平均时间，实质上指的是设备的容错能力。广义的 MTTR 涉及备件管理、客户服务等，是设备维护的一项重要指标。

以下为 MTTR 的计算公式：

$$\text{MTTR} = \text{故障检测时间} + \text{单板更换时间} + \text{系统初始化时间} + \text{链路恢复时间} + \text{路由覆盖时间} + \text{转发恢复时间}$$

上述各项的值越小，平均修复时间 MTTR 也就越小，设备的可用性也就越高。

MTBF

MTBF（Mean Time Between Failure），平均故障间隔时间，从可靠性方面标识故障发生的概率。指一个组件或设备的无故障运行平均时间，通常以小时为单位。

可用度

可用度标识系统的出勤率，增大 MTBF 和减少 MTTR，都可以提高设备的可用性。

在电信行业，99.999%的可用度意味着设备因故障导致的业务中断时间平均每年不得超过 5 分钟。

在实际网络中，总是避免不了各种因素造成网络故障和服务中断。基于这个事实，能够让设备从故障中快速恢复的技术非常重要，即缩小 MTTR 一样可以达到要可用性的目的。

1.1.3 可靠性需求级别

可靠性需求的级别不同，其目标和实现方法就不同。

可靠性需求的 3 个级别、目标和实现方法如表 1-1 所示：

表 1-1 可靠性需求

级别	目标	实现方法
1	系统软件、硬件少出故障	● 硬件：简化设计、电路规范、器件可靠应用、外购件可靠性控制、生产工艺可靠性、环境适应性、可靠性试验（HALT/HASS）等 ● 软件：软件可靠性设计 CHECKLIST
2	即使发生故障，系统功能不受影响	冗余设计、倒换策略、提高倒换成功率
3	系统故障导致功能受损，但能够快速恢复	故障检测、诊断、隔离和恢复

1.1.4 高可靠 IP 网络组网原则

组网原则包括：分层组网、冗余技术和负载分担技术。

可靠性组网原则如下：

- 分层组网：将网络分为核心层，汇聚层，边缘层。根据业务现状或业务预测，接入边缘层接入节点时采用冗余备份设置，分别与汇聚节点相连。汇聚层设备双归到上层单点多设备或多点。汇聚层与核心层设备可以视情况合理设置。核心层设备采用全互连或半互连，大流量两点一条可达，避免使用多极互连。
- 同层内尽量多互连，单点考虑多设备。
- 下层双归或是多归到上层多个设备的单点上或是多点上。
- 局部根据业务流量情况适当调整。

1.2 IP 网络可靠性技术

从故障检测技术和网络倒换技术两方面介绍可靠性技术。

1.2.1 IP 网络故障检测技术

故障检测技术按使用限制分专用检测技术和通用检测技术：

- 专用的故障检测技术有：
 - Automatic Protection Switching（传输层）
 - Eth-OAM（链路层）
 - MPLS OAM（MPLS）
- 通用故障检测技术包括：BFD，可检测链路层，网络层等各个层面的故障。

以 TCP/IP 网络参考模型作为层次性划分，每个层面都有故障检测机制：

- 传输层/物理层：APS（Automatic Protection Switching）
- 链路层：MPLS OAM、Eth-OAM、STP/RSTP/MSTP/RRPP
- 网络层：各协议的 HELLO 机制、VRRP、GR
- 应用层：各种应用层协议本身的心跳、重传机制

网络故障检测的模式：

- 异步模式：周期性发送探测报文
- 查询模式：发一系列报文请求确认
- 回声模式：将对端发送过来的报文不作任何改动反射回去

1.2.2 IP 网络保护倒换技术

数据通信网络保护倒换标准是 50ms。链路冗余是保护倒换的基础。

链路保护方式包括：

- 端到端保护：1:1、1+1、1:N、M:N
- 本地保护：FRR

由故障检测触发的保护倒换方式包括：BFD 触发、FRR 技术、OAM 技术。

多种保护倒换功能包括：

- 本地请求保护
- 本地实效保护
- 倒换信号延迟处理
- 单端倒换防止
- 倒换请求共存与抢占
- 倒换恢复模式

1.3 NE80E/40E 支持的可靠性技术

可靠性技术主要包括两个方面：IP 网络故障检测技术和 IP 网络保护倒换技术。

以下将具体阐述上述 IP 网络故障检测技术和 IP 网络保护倒换技术在 NE80E/40E 中的应用。

1.3.1 FRR（Fast ReRoute）

FRR 是解决故障快速倒换最常用的技术，主要包括 IP FRR、LDP FRR、MPLS TE FRR 和 VPN FRR。

IP FRR

在转发模块中建立一张端口状态表，保存设备中每个端口的工作状态。当检测到端口不能正常工作时（如物理链路失效或人工操作将端口关闭），立即更新端口状态表。

同时，在报文转发过程中，如果查转发表得到的表项含有负载分担项（既有多个下一跳），在按照某种规则选定一个下一跳后，在端口状态表中检查这个下一跳出端口的状态，如果状态为失效，则使用另一个下一跳进行尝试，直至遍历全部负载分担项为止。

在检测到最后一个负载分担项时可以不再检查出端口的状态，而直接使用这个下一跳发送报文。

由于检测并更新端口状态的动作比路由收敛的动作快的多，所以本技术可以使重路由功能快速生效，并充分利用转发表中的多个负载分担项实现高可靠性的数据转发。

增强的 IP FRR 技术支持非等价负载分担的下一跳，IP 路由有一个主用下一跳，由 IGP 计算决定，并手工配置一个备用端口（下一跳），在故障时快速切换。

LDP FRR

传统的 IP FRR 无法有效保护 MPLS 网络中的流量，NE80E/40E 提供 LDP FRR 功能，为 MPLS 网络提供端口级的保护方案。

与 IGP 快速收敛相比，LDP FRR 会事先计算备份端口，在故障发生后无需另外花费时间进行路由计算以及 LSP 的重新建立，从而加快了保护倒换的速度。

LDP 工作在下游自主标签分发（DU）、有序标签控制（Ordered）以及自由标签保持方式（Liberal）时，LSR 会保存所有收到的标签映射，但只有从 FEC 对应路由的下一跳发送来的标签映射会生成标签转发表。

利用这一特点，如果为 Liberal 标签映射也生成标签转发表，就相当于建立了备份 LSP。

网络运行正常时，使用正常的 LSP 转发，如果正常 LSP 的出接口 Down，使用备份 LSP 转发，这样可以在网络收敛之前的短时间内保证流量不中断。

MPLS TE FRR

MPLS TE FRR 是现有的解决故障快速倒换最常用的技术之一。它的基本思路是在两个 PE 设备之间建立端到端的 TE 隧道，并且为需要保护的主用 LSP（标签交换路径）事先建立好备用 LSP，当设备检测到主用 LSP 不可用时（节点故障或者链路故障），将流量倒换到备用 LSP 上，从而实现业务的快速倒换。

从 MPLS TE FRR 技术的原理看，对于作为 TE 隧道起始点和终结点的两个 PE 设备之间的链路故障和节点故障，MPLS TE FRR 能够实现快速的业务倒换。

但是这种技术不能解决作为隧道起始点和终结点的 PE 设备的故障。一旦 PE 节点发生故障，只能通过端到端的路由收敛、LSP 收敛来恢复业务，其业务收敛时间与 MPLS VPN 内部路由的数量、承载网的跳数密切相关。在典型组网中一般在 5s 左右，无法达到节点故障端到端业务收敛小于 1s 的要求。

VPN FRR

VPN FRR 利用基于 VPN 的私网路由快速切换技术，通过预先在远端 PE 中设置指向主用 PE 和备用 PE 的主备用转发项，并结合 PE 故障快速探测，旨在解决 CE 双归属接入 PE 的 MPLS VPN 网络中，PE 节点故障导致的端到端业务收敛时间长（大于 1s）的问题，同时解决 PE 节点故障恢复时间与其承载的私网路由的数量相关的问题。在 PE 节点故障时，端到端业务收敛时间小于 1s。

在配置了 VPN FRR 的 PE 设备上，支持根据匹配策略选择符合条件的 VPNv4 路由。对于这些路由，除了优选下一跳发布的路由信息（包括转发前缀、内层标签、选中的外层 LSP 隧道），次优下一跳发布的路由信息（包括转发前缀、内层标签、选中的外层 LSP 隧道）也同样填写在转发项中。

当优选下一跳节点故障时，该 PE 设备通过 BFD、MPLS OAM 等技术感知到其与优选下一跳之间的外层隧道不可用，便将 LSP 隧道状态表中的对应标志设置为不可用并下刷到转发引擎中。转发引擎选中一个转发项之后，检查该转发项对应的 LSP 隧道状态，如果为不可用，则使用本转发项中携带的次优路由的转发信息进行转发。

1.3.2 OAM（Operation Administration & Maintenance）

使用 OAM 技术可以简化网络操作、随时检验网络性能、降低网络运行成本。此处仅介绍 MPLS OAM 技术。

MPLS 作为可扩展的下一代网络的关键承载技术，提供具有 QoS 保障的多业务能力。MPLS 引入了一个独特网络层次，这个新的网络层可能会引发故障。因此，MPLS 网络需要具备 OAM 能力。

MPLS 支持多种三层和二层协议，如 IP、FR、ATM、Ethernet 等。MPLS 提供一个完全不依赖于任何上层或下层的 OAM 机制，在 MPLS 的用户平面实现以下特性：

- 检测 TE LSP 的连通性。
- 在链路出现缺陷或故障时迅速进行保护倒换，以便能根据与客户签订的 SLA（Service Level Agreements）提供业务。

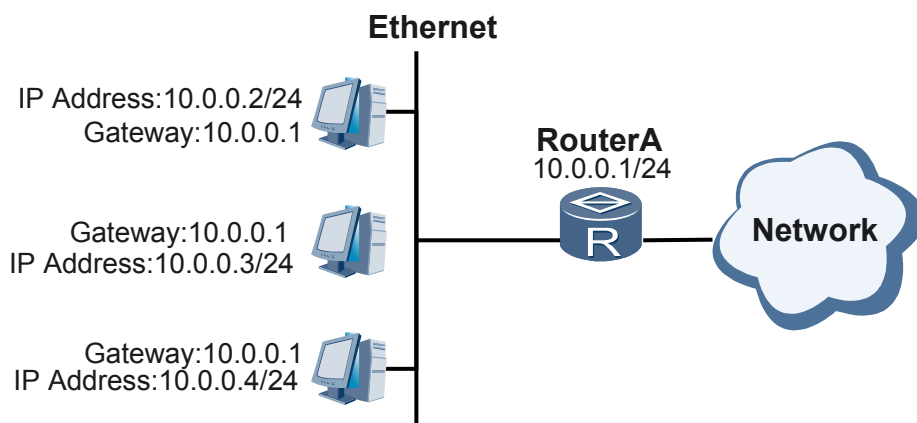
使用 MPLS OAM 机制，可以有效地检测、确认并定位出 MPLS 层网络内部的缺陷，然后报告缺陷并做出相应的处理。另外，在出现故障的时候，能够提供保护倒换的触发机制。

1.3.3 VRRP（Virtual Router Redundancy Protocol）

VRRP 将一组路由器联合组成一台虚拟路由器，将网络内主机的缺省网关设置为该虚拟路由器的 IP 地址。

通常情况下，内部网络中的所有主机都设置一条相同的缺省路由，指向出口网关（即图 1-1 中的路由器 RouterA），实现主机与外部网络的通信。当出口网关发生故障时，主机与外部网络的通信就会中断。

图 1-1 局域网缺省网关



VRRP 是 RFC3768 定义的一种容错协议，通过物理设备和逻辑设备的分离，实现在多个出口网关之间选路，很好地解决了上述问题。

在具有组播或广播能力的以太网中，VRRP 提供逻辑网关确保高利用度的传输链路，不仅能够解决因某网关设备故障带来的业务中断，而且无需修改路由协议的配置。

1.3.4 BFD (Bidirectional Forwarding Detection)

BFD 是一套全网统一的检测机制，它可以快速检测网络中的故障，减小设备故障对业务的影响，提高网络的可用性。

BFD（双向转发检测）是一套全网统一的检测机制，用于快速检测、监控网络中链路或者 IP 路由的转发连通状况。为改善网络性能，相邻系统之间应能快速检测到通信故障，更快地建立起备用通道恢复通信。

BFD 提供如下功能：

- 对相邻转发引擎之间的通道故障提供轻负荷、短持续时间的检测。
- 用单一的机制对任何介质、任何协议层进行实时检测，并支持不同的检测时间与开销。

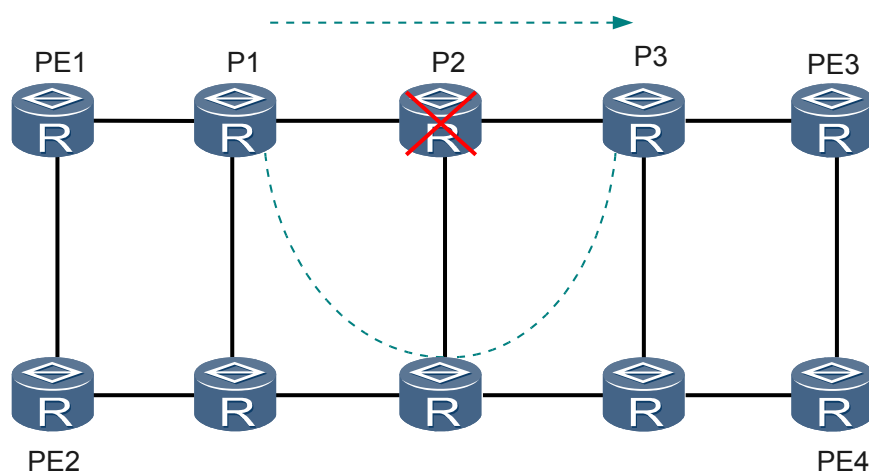
1.4 IP 网络可靠性组网方案

IP 网络可靠性组网方案主要介绍 FRR 的各种应用场景及解决方案。

1.4.1 中间节点故障或中间节点相邻链路故障-LDP/TE FRR

在 LDP/TE 中，在 P 设备之间有传输设备时，可以使用 BFD 或者是 OAM 机制来检测传输链路。

图 1-2 LDP/TE FRR 应用组网图



如图 1-2 所示，使用 LDP 作为公网隧道，在 P 设备之间启用 TE 保障 QoS。这种部署增强了全网的 QoS 能力，同时也降低了更换 PE 设备带来的 TE 部署的困难。在没有传输

设备的情况下，如果故障发生在 P1 到 P2 的链路（非广播网络）或者 P2 故障（P1 到 P2 非广播网），LDP FRR 在 PE1 上切换，保证切换时间在 50ms 之内。

上述情况的前提是没有传输设备，因为 TE/LDP FRR 的切换，依赖于对接口状态即电信号或者光信号的感知。如果中间有传输设备，并且传输中间链路产生问题，那么路由器并不会感知到光电信号的中断，因此无法产生切换。此时，必须要使用另外的机制来检测传输链路，那就是 BFD 和 OAM。

1.4.2 传输中间链路故障

可以使用 BFD 或者是 OAM 机制来检测中间链路，使用 VRRP 来实现链路的快速切换。

OAM

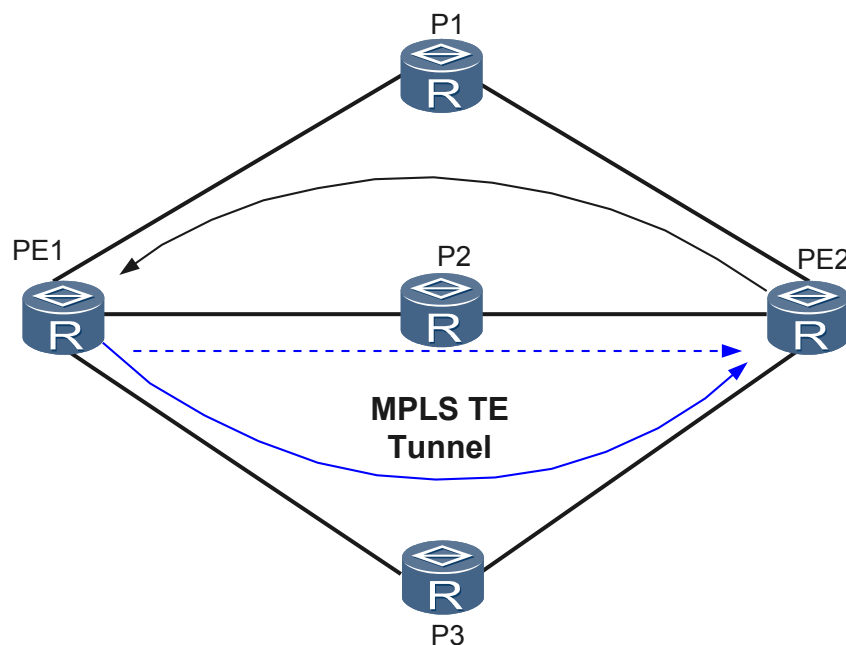
OAM 是单向的检测机制，当然完全可以双向都配置 OAM 以做到双向保护。OAM 的探测端发送探测报文，检查链路，接收端在正常情况下能按时收到探测端的探测报文。

如果在定义的时间内收不到探测报文，则通过一条与正向不同的反向路径发出链路中断报文，报告探测端被探测链路出了问题。然后探测端将进行其它一系列操作，这其中最常见的就是 OAM 保护组的切换。

OAM 保护组的含义是创建主备两条隧道，形成一个保护组。只要保护组中的一条隧道状态可用，那么这个主隧道在逻辑上也是可用的。在主隧道正常的情况下，转发使用主隧道，也称作 **work-tunnel**；在主隧道 Down 而备隧道可用时，逻辑上迭代到的路径仍然是主隧道，而实际使用的路径是备用隧道，也称作 **protect-tunnel**。

在 OAM 的快速检测下，保护组在转发表项中存在两个表项：一主一备，做到检测后的快速切换，实现网络路径的高可靠性。

图 1-3 MPLS OAM 保护倒换功能组网图



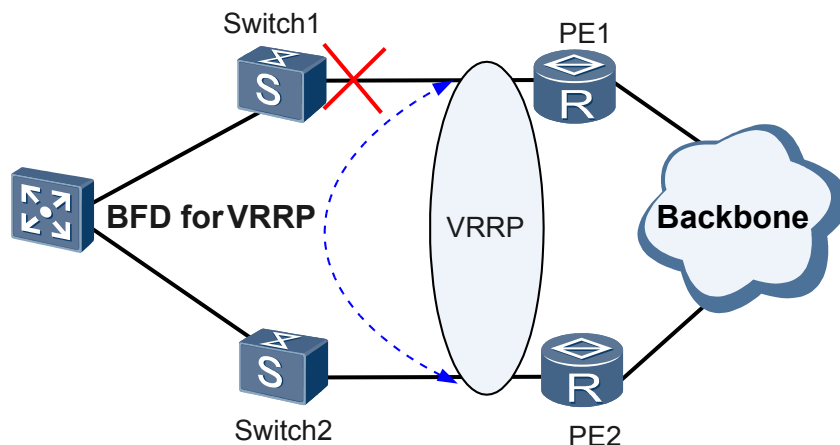
如图 1-3 所示，入节点 PE1 和出节点 PE2 之间建立两条 TE 隧道，构成保护组。PE2 和 PE1 之间（通过 P1）建立一条 TE 隧道，作为反向通道，向入节点 PE1 通告故障。

BFD

BFD 和 OAM 有很多类似的地方，都是定义了一套机制，包括探测、故障报告、故障切换等。探测主要是用快速的探测报文，这些报文按照预期的路径发送，探测链路状态，如果链路不通，那么探测报文就会丢失。为了防止抖动，可以定义发送多少探测报文失效表示链路中断。

BFD 是双向的检测机制，探测报文也是双向发送，任何一端在规定时间内没有收到对端的探测报文就会认为链路中断，同时报送其它模块进行切换等一系列操作。

图 1-4 BFD for VRRP 功能组网图

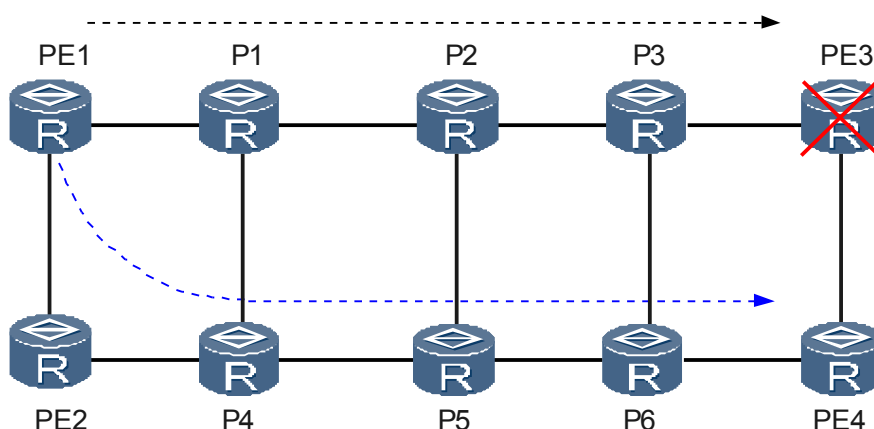


如图 1-4 所示，PE1 和 PE2 组成 VRRP 主备备份组，互为备份。VRRP 监视 BFD 会话。以 PE1 作为主用 PE 为例，当 Switch1 与 PE1 之间的传输链路出现故障时，BFD 快速检测出故障并通知 VRRP，VRRP 备份组快速切换，此时 PE2 切换为主用 PE。

1.4.3 远端接入端点路由器故障-VPN FRR

VPN FRR 中，可以使用 BFD 检测 PE 之间的连通性故障。

图 1-5 VPN FRR 应用组网图



如图 1-5 所示，PE3 和 PE4 接入 VPN。如果 PE1 左侧的用户网路需要和 PE3 右侧的用户网路进行通信，则在 PE1 上到达右侧的用户网路会有两个出口 PE(PE3 和 PE4)。这种情况下，可以让 PE3 和 PE4 互为备份，PE1 上针对 PE3 和 PE4 的互相备份，称作 VPN FRR。

VPN FRR 和所有的 FRR 相同，事先总会存在一个可用的备份路径，在主路径失效的情况下，能够做到快速切换。VPN FRR 就是事先对于远端 PE 收到的私网路由保存两个下一跳（远端 PE），这样可以确立一个为主，一个为备，选择主备 PE 的规则是由用户自己控制的。

对于上图而言，在 PE1 上，对于远端 VPN 的路由，存在两个下一跳，分别为 PE3、PE4，此时在 PE1 上面就可以选择 PE3、PE4 其中一个为主用的下一跳，另外一个为备用的下一跳。

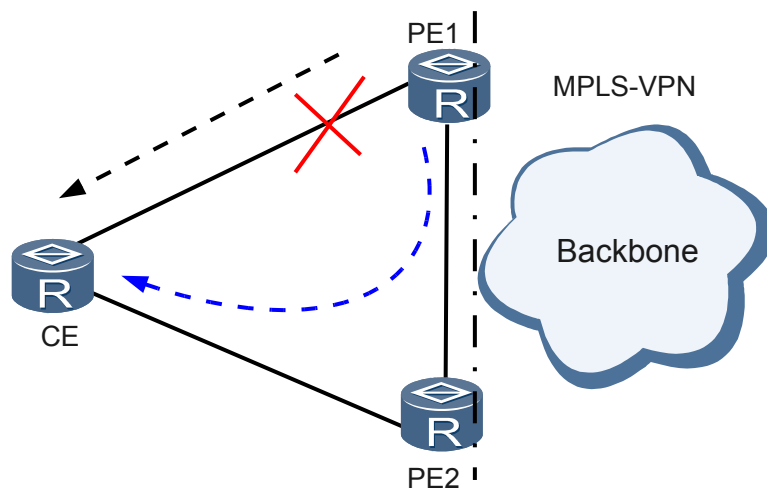
- 在没有配置 VPN FRR 的情况下，控制层面只会对转发层面下发一个主用的下一跳，当主用下一跳失效以后，备用下一跳再下刷到转发层面，这样速度较慢。
- 配置了 VPN FRR 后，控制层面会把两个下一跳都下刷到转发层面。当主用下一跳失效后，转发层面能够快速使用备用下一跳，提高了切换速度。

使用 BFD 机制探测主用下一跳 PE 失效后，可以在非常短的时间内进行切换，实现了相当高的可靠性。

1.4.4 接入端点路由器下行接口故障——IP FRR

IP FRR 中，当 CE 和 PE 之间的的主用路径故障时，可以将流量切换到备份路径上。

图 1-6 IP FRR 应用组网图



如图 1-6 所示，去往 CE 的流量经过 PE1（主用 PE）转发，如果 PE1 到 CE 的链路出现故障，则 IP FRR 将流量从 CE 到 PE1 的链路切换到 CE 到 PE2 的链路上。

FRR 的原理归根到底都是转发层面保持备份的路径，以做到快速切换。同样此处使用 IP FRR 时，PE1 到达 CE 的路径有两条，一是通过直连路径，另外一条就是通过 PE1 到达 PE2 再转发到 CE。

通常情况下都会使用 PE 接入 L3VPN，因此此处的 IP FRR 也在私网中使用。此时 PE1 和 PE2 之间需要建立私网邻居，在 PE1 上实现到达 CE 有主备路径。

2 接口备份配置

关于本章

通过为主接口配置备份接口，实现主接口故障时备份接口承担网络流量。

2.1 接口备份简介

接口备份机制中，接口分为主接口和备份接口。接口备份的两种工作方式是主备备份和负载分担。

2.2 配置主备接口备份

主备接口备份是指主接口承担所有业务，备份接口不承担。

2.3 配置负载分担接口备份

负载分担接口备份是指主接口和备份接口均承担业务。

2.4 维护接口备份

通过维护接口备份，可以监控接口备份的运行状况。

2.5 配置举例

接口备份的两种方式是主备接口备份和负载分担接口备份。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

2.1 接口备份简介

接口备份机制中，接口分为主接口和备份接口。接口备份的两种工作方式是主备备份和负载分担。

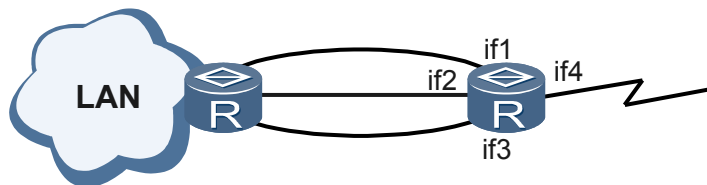
2.1.1 接口备份概述

接口备份是指同一设备上的接口之间形成备份关系，当某个接口出现故障时，可以将流量快速的切换到备份接口。

路由器在网络中承担重要任务，当路由器上某个接口出现故障时，如何快速平滑地将该接口上的业务切换到其他正常接口，是保障业务安全通畅的重要手段。

接口备份（Interface Backup）是指同一台设备上的各接口之间形成备份关系，通常一个接口承担业务，其余接口处于备份状态。如图 2-1 所示。

图 2-1 接口备份简介



路由器 if1、if2 和 if3 三个接口形成备份关系，if2 接口承担业务传输，if1 和 if3 接口处于备份状态，并有不同的备份优先级。

路由器跟踪各接口状态，当发现 if2 接口出现故障时，启动优先级最高的备份接口来承担传输业务，从而确保平滑、通畅的可靠传输。

在接口备份机制中，接口按照是否承担业务传输分为两类：主接口、备份接口。

说明

POS 和 ATM 接口特性在 NE80E/40E 系列中的 X1 和 X2 设备上不支持。

主接口

主接口承担业务传输，是得到备份服务的接口（如图 2-1 中的 if2 接口）。

主接口可以是路由器上任意一个物理接口或子接口，如 POS、Ethernet、ATM 接口。大带宽的主接口将提供更高的传输效率。

备份接口

备份接口不承担该业务传输，通常处于空闲状态，是为主接口提供备份功能的接口（如图 2-1 中的 if1 和 if3 接口）。

备份接口可以是路由器上任意一个物理接口（如 POS、Ethernet、ATM、AUX 接口）。

说明

- 一个主接口可以有多个备份接口。当主接口出现故障时，多个备份接口根据优先级来决定接替工作的顺序。
- 一个备份接口只能为一个主接口提供备份。
- 对于 ISDN BRI/PRI 这类具有多个物理通道的接口，可以通过 DCC（Dial Control Center）配置中的 Dialer route 来为多个主接口提供备份。

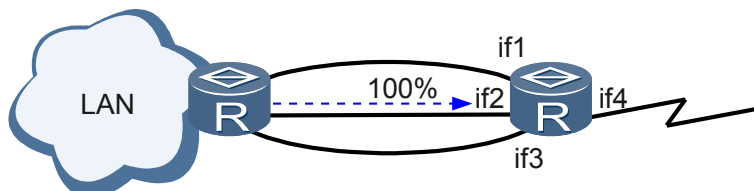
2.1.2 NE80E/40E 支持的接口备份特性

接口备份包括主备备份方式和负载分担方式。

主备备份方式

如图 2-2，if2 接口作为主接口。

图 2-2 主备备份方式



在主备备份方式下，任何时间都只有一个接口传输业务。

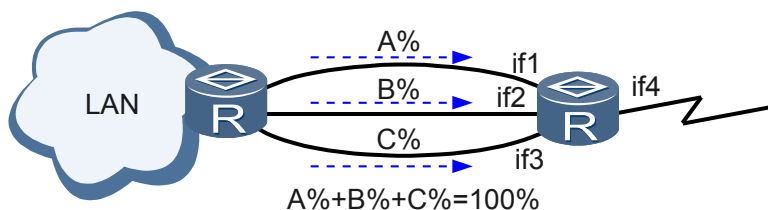
- 如果主接口正常工作，即使流量超负荷，备份接口（如 if1 和 if3 接口）也不转发流量，所有流量都通过主接口传输。
- 只有当主接口故障时，优先级最高的备份接口才接替工作，并承担所有流量的传输。
- 当原先故障的主接口恢复正常时，业务会重新切换到主接口。

负载分担方式

在负载分担方式下，流量在多个接口间实现负载均衡：

- 当主接口流量达到预先设定的上限阈值时，路由器会自动启动一个优先级最高、状态可用的备份接口，该备份接口同主接口一起传输业务，进行负载分担。
- 当这两个接口的流量再次达到上限阈值时，路由器会启动另一个可用的高优先级接口，在这三个接口间进行负载分担。以此类推。
- 当主接口流量小于设定的下限阈值时，路由器关闭一个优先级最低的备份接口。以此类推，直到仅剩主接口承担业务流量。

图 2-3 负载分担方式





说明

采用主备备份还是负载分担方式，根据用户是否配置负载分担的百分比门限决定。一旦配置了百分比门限，则采用负载分担方式，否则采用主备备份方式。

2.2 配置主备接口备份

主备接口备份是指主接口承担所有业务，备份接口不承担。

2.2.1 建立配置任务

在配置主备接口备份功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

配置接口备份功能，可以在多个设备间通过备份接口的方式提高可靠性。

在主备备份方式中，主接口承担所有业务，而备份接口处于闲置状态，不承担业务。

主备备份方式的重要参数是切换延时，选择合适的延时不仅能确保及时切换，而且还可以避免频繁倒换。

前置任务

在配置主备接口备份之前，需完成以下任务：

- 配置接口的物理参数
- 配置接口的链路属性
- 配置接口的 IP 地址
- 配置通过主/备接口到目的网段的静态路由



说明

主接口和备份接口都需要配置上述参数。为了节省 IP 地址，备份接口可以借用主接口地址。

数据准备

在配置主备接口备份的功能之前，需准备以下数据：

序号	数据
1	为主接口提供备份服务的备份接口
2	备份接口优先级
3	主/备接口切换延时

2.2.2 指定主接口使用的备份接口

通过指定主接口使用的备份接口，实现当主接口故障时，备份接口接替主接口工作，并承担网络流程的传输。

背景信息

在路由器上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

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

步骤 3 执行命令 **standby interface interface-type interface-number [priority]**，配置为主接口提供备份服务的备份接口及优先级。

 说明

- 如果要为 1 个主接口配置多个备份接口，则需要多次使用 **standby interface** 命令配置备份接口。
- 1 个主接口最多允许有 3 个备份接口。1 个备份接口只能为 1 个主接口提供备份。
- NE80E/40E 允许最多同时存在 10 个主接口。

----结束

2.2.3 配置主/备接口切换的延时

通过配置切换时延，防止由于接口状态不稳定而导致的主备接口之间的频繁切换。

背景信息

为避免接口状态不稳定导致频繁切换，当主接口状态由 UP 转为 DOWN 后，系统并不立即切换到备份接口，而是等待一个预先设置好的延时。

- 如果超过这个延时后，主接口的状态仍为 DOWN，切换到备份接口。
- 若在延时时间段中，主接口状态恢复正常，则不进行切换。

在路由器上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

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

步骤 3 执行命令 **standby timer delay enable-delay disable-delay**，配置主/备接口的切换延时。

参数 *enable-delay* 和 *disable-delay* 取值为 0 时，表示立即切换。

----结束

2.2.4 检查配置结果

通过查看主接口的状态信息等内容，来检查配置是否成功。

前提条件

已经完成主备接口备份功能的所有配置。

操作步骤

步骤 1 使用 **display standby state** 命令查看主/备接口的状态信息。

----结束

任务示例

执行 **display standby state** 命令可以看到各主备接口的状态信息如下：

```
<HUAWEI> display standby state
Interface          Interfacestate Backupstate Backupflag Pri Loadstate
GigabitEthernet3/0/0      UP      MUP      MU
GigabitEthernet3/0/4      STANDBY STANDBY  BU      20
Backup-flag meaning:
M---MAIN  B---BACKUP  V---MOVED  U---USED
D---LOAD  P---PULLED  G---LOGICCHANNEL
```

从以上信息可以看出，GE3/0/0 作为主接口，其状态为 UP，GE3/0/4 作为其备份接口，其状态为 STANDBY，而且优先级为 20。

2.3 配置负载分担接口备份

负载分担接口备份是指主接口和备份接口均承担业务。

2.3.1 建立配置任务

在配置负载分担接口备份功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

配置接口备份功能，可以在多个设备间通过备份接口的方式提高可靠性。

在负载分担方式中，如果主接口承担业务量超过门限阈值，则系统自动启动备份接口承担业务传输。

负载分担方式的重要参数有两个：

- 负载分担的百分比门限
- 主接口带宽

这两个指标影响各接口承接的业务量，同时，接口备份优先采用主接口备份带宽。

前置任务

在配置负载分担中心之前，需完成以下任务：

- 配置接口的物理参数
- 配置接口的链路属性
- 配置接口的 IP 地址

- 配置通过主接口和备份接口到目的网段的静态路由



说明

主接口和备份接口都需要配置上述参数。为了节省 IP 地址，备份接口上可以借用主接口地址。

数据准备

在配置负载分担中心的功能之前，需准备以下数据：

序号	数据
1	为主接口提供备份服务的备份接口，及备份接口优先级
2	使能/禁止负载分担的百分比门限
3	主接口的带宽大小
4	主接口流量的检测时间间隔

2.3.2 指定主接口使用的备份接口

通过指定主接口使用的备份接口，实现当主接口故障时，备份接口接替主接口工作，并承担网络流程的传输。

背景信息

在路由器上进行如下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **interface interface-type interface-number**，进入主接口视图。
- 步骤 3** 执行命令 **standby interface interface-type interface-number [priority]**，配置为主接口提供备份服务的备份接口及优先级。



说明

- 如果要为 1 个主接口配置多个备份接口，则需要重复使用 **standby interface** 命令配置备份接口。
- 1 个主接口最多允许有 3 个备份接口。1 个备份接口只能为 1 个主接口提供备份。
- NE80E/40E 允许最多同时存在 10 个主接口。

----结束

2.3.3 配置负载分担的百分比门限

通过配置负载分担的百分比门限，实现备份接口可以承担网络流量。

背景信息

在路由器上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

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

步骤 3 执行命令 **standby threshold enable-threshold disable-threshold**，配置负载分担的百分比门限。

缺省情况下，系统不支持负载分担功能，即没有配置百分比门限。必须在指定主接口的备份接口后才能为主接口配置负载分担百分比门限。

当所有活动接口的流量达到预先设定的上限阈值 *enable-threshold* 时，路由器自动启动一个优先级最高、状态可用的备份接口，同主接口一起传输业务。

当所有活动接口流量小于设定的下限阈值 *disable-threshold* 时，路由器关闭一个正在执行负载分担的、优先级最低的备份接口。

----结束

2.3.4 （可选）配置主接口的带宽、流量检测时间间隔

根据不同的网络需求，设置主接口的带宽和流量检测时间间隔。

背景信息

在路由器上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

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

步骤 3 执行命令 **standby bandwidth size**，配置主接口的最大可传输带宽。

缺省情况下，采用系统提供的主接口实际物理带宽作为主接口的最大可用带宽。

步骤 4 执行命令 **standby timer flow-check time**，配置检测主接口流量的时间间隔。

缺省情况下，流量检测间隔为 30 秒。

----结束

2.3.5 检查配置结果

通过查看主接口的状态信息或者是流量统计信息等内容，来检查配置是否成功。

前提条件

已经完成负载分担接口备份功能的所有配置。

操作步骤

- 使用 **display standby flow** 命令查看参与负载分担的主接口的流量统计数据。
- 使用 **display standby state** 查看主/备接口的状态信息。

----结束

任务示例

配置完成后，执行 **display standby flow** 命令，可以看到主接口的流量信息。

```
<HUAWEI> display standby flow
InterfaceName      : GigabitEthernet 2/0/0
Flow-interval(s)   : 30
LastInOctets       : 5298
LastOutOctets      : 398807420
InFlow(Octets)     : 1038
OutFlow(Octets)    : 78717892
BandWidth(b/s)     : 40000000
UsedBandWidth(b/s) : 20991432
```

配置完成后，执行 **display standby state** 命令，可以看到接口的主备状态。

```
<HUAWEI> display standby state
Interface      Interfacestate Backupstate Backupflag Pri Loadstate
GigabitEthernet 2/0/0      UP      MUP      MUD
GigabitEthernet 1/0/0      UP      UP      BU      40
GigabitEthernet 3/0/0      STANDBY STANDBY BU      20
Backup-flag meaning:
M---MAIN  B---BACKUP  V---MOVED  U---USED
D---LOAD  P---PULLED  G---LOGICCHANNEL
```

2.4 维护接口备份

通过维护接口备份，可以监控接口备份的运行状况。

2.4.1 监控接口备份运行状况

通过监控接口备份运行状况，可以了解运行过程中接口的相关信息。

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解接口备份的运行状况。

操作步骤

- 在任意视图下执行 **display standby state** 命令，查看接口备份的配置和状态信息。
- 在任意视图下执行 **display standby flow** 命令，显示参与备份负载分担的主接口的流量统计数据。

----结束

2.5 配置举例

接口备份的两种方式是主备接口备份和负载分担接口备份。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

背景信息

 说明

手册中所使用的链路接口编号和链路类型以 NE40E-X8 为例，实际使用时以现网设备为准。

2.5.1 配置主备接口备份示例

本示例中，通过配置主备接口备份，实现主接口故障时，备份接口接替主接口工作，并承担网络流程的传输。

组网需求

 说明

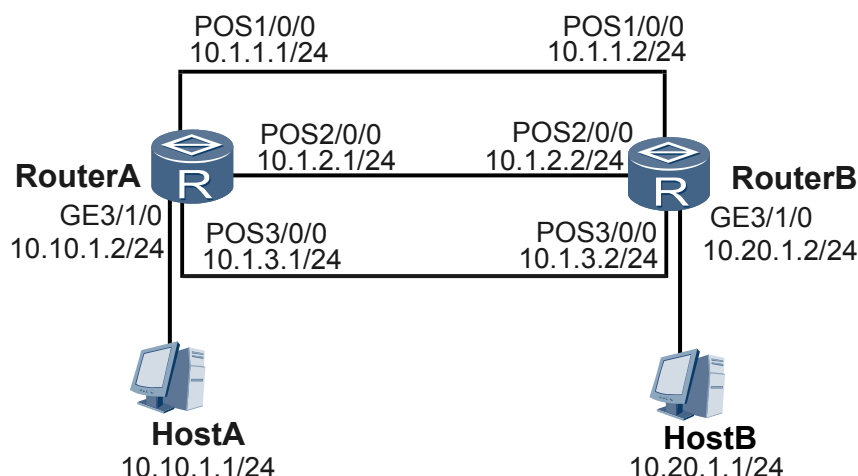
POS 接口特性在 NE80E/40E 系列中的 X1 和 X2 设备上不支持。

如图 2-4 所示，RouterA 和 RouterB 连接。

RouterB 上的多个接口形成主备备份关系：

- POS2/0/0 作为主接口。
- 接口 POS1/0/0 和 POS3/0/0 作为 POS2/0/0 接口的备份接口。
- 接口 POS1/0/0 优先提供备份服务。

图 2-4 配置主备接口备份组网图



配置思路

采用如下的思路在路由器接口上配置主备接口备份：

1. 在 RouterB 上配置 POS2/0/0 作为主接口，承担所有业务。
2. 在 POS2/0/0 的接口视图下配置 POS1/0/0 和 POS3/0/0 作为备份接口，不承担任何业务，POS1/0/0 优先级较高。

数据准备

为完成本配置例，需要预先规划各备份接口的优先级。

操作步骤

步骤 1 配置网络层互通

按**组网需求**配置各接口的 IP 地址，具体配置过程略。

在 RouterA 上配置去往 HostB 所在网段的静态路由。

```
<RouterA> system-view
[RouterA] ip route-static 10.20.1.0 255.255.255.0 pos1/0/0
[RouterA] ip route-static 10.20.1.0 255.255.255.0 pos2/0/0
[RouterA] ip route-static 10.20.1.0 255.255.255.0 pos3/0/0
```

在 RouterB 上配置去往 HostA 所在网段的静态路由。

```
<RouterB> system-view
[RouterB] ip route-static 10.10.1.0 255.255.255.0 pos1/0/0
[RouterB] ip route-static 10.10.1.0 255.255.255.0 pos2/0/0
[RouterB] ip route-static 10.10.1.0 255.255.255.0 pos3/0/0
```

配置 HostA 和 HostB 分别以 RouterA 和 RouterB 做为各自的网关，具体配置过程略。
配置完成后，HostA 和 HostB 可以互相 Ping 通。

步骤 2 在 RouterB 上配置接口备份

配置 POS2/0/0 为主接口，POS1/0/0 和 POS3/0/0 为备份接口，POS1/0/0 具有较高的优先级。采用立即切换。

```
[RouterB] interface pos 2/0/0
[RouterB-Pos2/0/0] standby interface pos 1/0/0 40
[RouterB-Pos2/0/0] standby interface pos 3/0/0 20
[RouterB-Pos2/0/0] quit
```

配置完成后，在 RouterB 上查看主/备接口的状态信息，可以看到 POS2/0/0 的状态是 UP，POS1/0/0 和 POS3/0/0 的状态是 STANDBY。

```
[RouterB] display standby state
```

Interface	Interfacestate	Backupstate	Backupflag	Pri	Loadstate
Pos 2/0/0	UP	MUP	MU		
Pos 1/0/0	STANDBY	STANDBY	BU	40	
Pos 3/0/0	STANDBY	STANDBY	BU	20	

Backup-flag meaning:
M---MAIN B---BACKUP V---MOVED U---USED
D---LOAD P---PULLED G---LOGICCHANNEL

在 HostA 上对 HostB 的地址进行 Tracert 测试，可以看到报文通过 RouterB 的 POS2/0/0 所在链路到达目的地。

```
C:\> tracert 10.20.1.1
tracert to 10.20.1.1 (10.20.1.1), max hops: 30, packet length: 40, press CTRL_C to break
 1  60 ms  60 ms  50 ms  10.10.1.2
 2  50 ms  40 ms  70 ms  10.1.2.2
 3  70 ms  70 ms  60 ms  10.20.1.1
Trace complete.
```

步骤 3 验证配置结果

对 RouterB 的主接口 POS2/0/0 执行 **shutdown** 命令，模拟主接口故障。

```
[RouterB] interface pos 2/0/0
[RouterB-Pos2/0/0] shutdown
[RouterB-Pos2/0/0] quit
```

再次查看主/备接口的状态信息，可以看到 POS1/0/0 的状态变为 UP，POS3/0/0 的状态仍然是 STANDBY。

```
<RouterB> display standby state
```

Interface	Interfacestate	Backupstate	Backupflag	Pri	Loadstate
Pos 2/0/0	DOWN	MDOWN	MU		
Pos 1/0/0	UP	UP	BU	40	
Pos 3/0/0	STANDBY	STANDBY	BU	20	

Backup-flag meaning:

M---MAIN B---BACKUP V---MOVED U---USED
D---LOAD P---PULLED G---LOGICCHANNEL

在 HostA 上对 HostB 的地址进行 Tracert 测试，可以看到报文通过 RouterB 的 POS1/0/0 所在链路到达目的地。

```
C:\> tracert 10.20.1.1
tracert to 10.20.1.1 (10.20.1.1), max hops: 30, packet length: 40, press CTRL_C to break
 1  60 ms  60 ms  50 ms  10.10.1.2
 2  50 ms  40 ms  70 ms  10.1.1.2
 3  70 ms  70 ms  60 ms  10.20.1.1
Trace complete.
```

----结束

配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.2.1 255.255.255.0
#
interface Pos3/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.3.1 255.255.255.0
#
interface GigabitEthernet4/0/0
 undo shutdown
 ip address 10.10.1.2 255.255.255.0
#
ip route-static 10.20.1.0 255.255.255.0 Pos1/0/0
ip route-static 10.20.1.0 255.255.255.0 Pos2/0/0
ip route-static 10.20.1.0 255.255.255.0 Pos3/0/0
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.2.2 255.255.255.0
 standby interface Pos1/0/0 40
 standby interface Pos3/0/0 20
#
interface Pos3/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.3.2 255.255.255.0
#
interface GigabitEthernet4/0/0
```

```
undo shutdown
ip address 10.20.1.2 255.255.255.0
#
ip route-static 10.10.1.0 255.255.255.0 Pos1/0/0
ip route-static 10.10.1.0 255.255.255.0 Pos2/0/0
ip route-static 10.10.1.0 255.255.255.0 Pos3/0/0
#
return
```

2.5.2 配置负载分担接口备份示例

本示例中，通过配置负载分担接口备份，实现主接口和备份接口均承担业务。

组网需求

说明

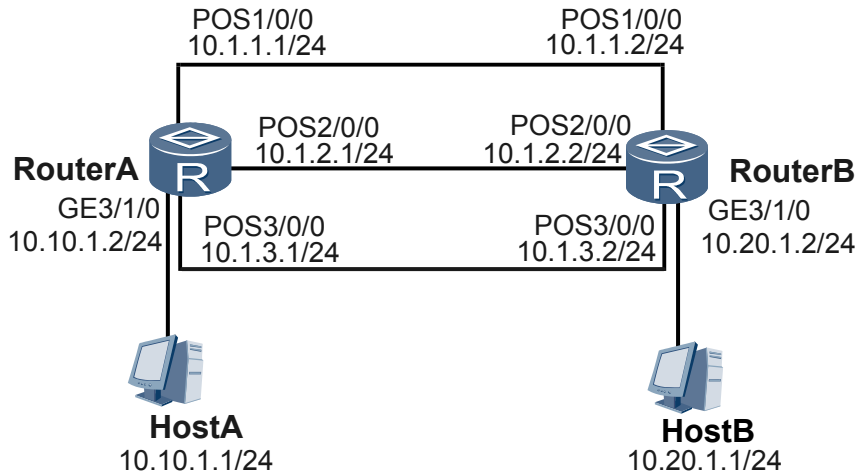
POS 接口特性在 NE80E/40E 系列中的 X1 和 X2 设备上不支持。

如图 2-5 所示。路由器 RouterA 和 RouterB 连接。

在 RouterB 上多个接口形成负载分担关系，其中 POS2/0/0 作为主接口，POS1/0/0 和 POS3/0/0 作为 POS2/0/0 的负载分担接口。

设置主接口的最大可传输带宽为 40Mbit/s，当主接口流量达到此带宽的 50%时，优先启动 POS1/0/0 接口进行负载分担，当主接口流量低于此带宽的 30%时，关闭低优先级的备份接口。

图 2-5 配置负载分担接口备份组网图



配置思路

采用如下的思路在 RouterB 上配置负载分担接口备份：

1. 在 RouterB 上配置 POS2/0/0 作为主接口。
2. 在 POS2/0/0 的接口视图下配置 POS1/0/0 和 POS3/0/0 作为备份接口，POS1/0/0 优先级较高。
3. 配置主接口带宽、负载分担的百分比门限。

数据准备

数据规划如下：

- 备份接口的优先级
- 负载分担的百分比门限、主接口带宽

操作步骤

步骤 1 配置网络层互通

按图 2-5 配置各接口的 IP 地址，具体配置过程略。

在 RouterA 上配置去往 HostB 所在网段的静态路由。

```
<RouterA> system-view
[RouterA] ip route-static 10.20.1.0 255.255.255.0 pos1/0/0
[RouterA] ip route-static 10.20.1.0 255.255.255.0 pos2/0/0
[RouterA] ip route-static 10.20.1.0 255.255.255.0 pos3/0/0
```

在 RouterB 上配置去往 HostA 所在网段的静态路由。

```
<RouterB> system-view
[RouterB] ip route-static 10.10.1.0 255.255.255.0 pos1/0/0
[RouterB] ip route-static 10.10.1.0 255.255.255.0 pos2/0/0
[RouterB] ip route-static 10.10.1.0 255.255.255.0 pos3/0/0
```

配置 HostA 和 HostB 分别以 RouterA 和 RouterB 做为各自的网关，具体配置过程略。

配置完成后，HostA 和 HostB 可以互相 Ping 通。

步骤 2 在 RouterB 上配置接口备份

配置 POS2/0/0 为主接口，接口 POS1/0/0 和 POS3/0/0 为备份接口，优先级分别为 40 和 20。

```
[RouterB] interface pos 2/0/0
[RouterB-Pos2/0/0] standby interface pos1/0/0 40
[RouterB-Pos2/0/0] standby interface pos3/0/0 20
```

配置主接口带宽、负载分担的百分比门限

```
[RouterB-Pos2/0/0] standby bandwidth 40000
[RouterB-Pos2/0/0] standby threshold 50 30
```

步骤 3 验证配置结果

在 RouterB 上使用 **display standby state** 命令查看主/备接口的状态信息，可以看到 POS2/0/0 的状态是 UP，POS1/0/0 和 POS3/0/0 的状态是 STANDBY。同时可以使用 **display standby flow** 命令查看主接口 POS2/0/0 的流量变化情况。

```
<RouterB> display standby state
Interface      Interfacestate Backupstate Backupflag Pri Loadstate
Pos 2/0/0      UP           MUP           MU
Pos 1/0/0      STANDBY     STANDBY       BU        40
Pos 3/0/0      STANDBY     STANDBY       BU        20
Backup-flag meaning:
M---MAIN  B---BACKUP  V---MOVED  U---USED
D---LOAD  P---PULLED   G---LOGICCHANNEL
<RouterB> display standby flow
Interfacename      : Pos2/0/0
Flow-interval(s)   : 30
LastInOctets       : 2494
LastOutOctets      : 86086500
InFlow(Octets)     : 258
```



```
OutFlow(Octets)      : 258
BandWidth(b/s)       : 40000000
UsedBandWidth(b/s)   : 64
```

在 RouterA 上向 HostB 所在网段发送大流量，使 POS2/0/0 上的流量超过 20Mbit/s。30 秒后再次查看 RouterB 上主/备接口的状态信息，可以看到 POS2/0/0 和 POS1/0/0 的状态都是 UP。

```
<RouterB> display standby state
Interface          Interfacestate Backupstate Backupflag Pri Loadstate
Pos 2/0/0           UP             MUP          MUD
Pos 1/0/0           UP             UP           BU      40
Pos 3/0/0           STANDBY       STANDBY      BU      20
Backup-flag meaning:
M---MAIN  B---BACKUP  V---MOVED  U---USED
D---LOAD  P---PULLED  G---LOGICCHANNEL
<RouterB> display standby flow
Interfacename : Pos2/0/0
Flow-interval(s) : 30
LastInOctets : 5298
LastOutOctets : 398807420
InFlow(Octets) : 1038
OutFlow(Octets) : 78717892
BandWidth(b/s) : 40000000
UsedBandWidth(b/s) : 20991432
```

----结束

配置文件

● RouterA 的配置文件

```
#
sysname RouterA
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.2.1 255.255.255.0
#
interface Pos3/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.3.1 255.255.255.0
#
interface GigabitEthernet4/0/0
 undo shutdown
 ip address 10.10.1.2 255.255.255.0
#
ip route-static 10.20.1.0 255.255.255.0 Pos1/0/0
ip route-static 10.20.1.0 255.255.255.0 Pos2/0/0
ip route-static 10.20.1.0 255.255.255.0 Pos3/0/0
#
return
```

● RouterB 的配置文件

```
#
sysname RouterB
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
```

```
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.2.2 255.255.255.0
 standby interface Pos1/0/0 40
 standby interface Pos3/0/0 20
 standby threshold 50 30
 standby bandwidth 40000
#
interface Pos3/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.3.2 255.255.255.0
#
interface GigabitEthernet4/0/0
 undo shutdown
 ip address 10.20.1.2 255.255.255.0
#
 ip route-static 10.10.1.0 255.255.255.0 Pos1/0/0
 ip route-static 10.10.1.0 255.255.255.0 Pos2/0/0
 ip route-static 10.10.1.0 255.255.255.0 Pos3/0/0
#
return
```

3 APS 配置

关于本章

对于 SDH 体系中的 STM-N 链路，利用 APS 协议可以在通信链路出现故障时将业务快速迁移到正常的链路上，保证通信正常进行。

3.1 简介

APS 协议通过控制线性复用段保护方式下的倒换和恢复动作实现故障时将业务快速迁移。

3.2 配置单机 APS

一台设备通过两条链路与另一条设备相连，这两台设备均支持 APS，配置单机 APS 可以提高链路的可靠性。

3.3 配置 E-APS

配置 E-APS 可以实现跨设备的 APS 倒换。

3.4 配置举例

介绍 APS 的各种示例。配置示例中包括组网需求、配置注意事项和配置思路等。

3.1 简介

APS 协议通过控制线性复用段保护方式下的倒换和恢复动作实现故障时将业务快速迁移。

3.1.1 APS 概述

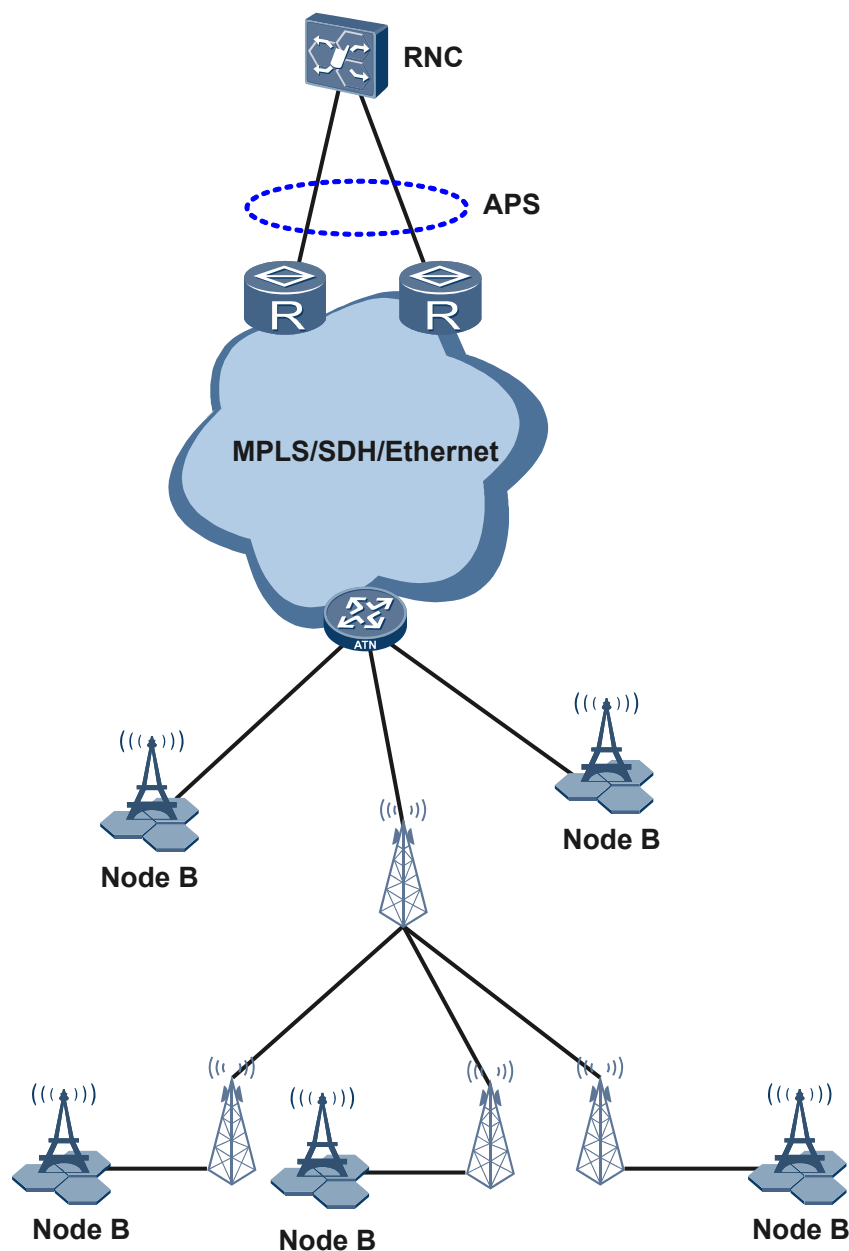
APS 协议利用复用段开销传递信号，保护方式分为 1+1 保护方式和 1:N 保护方式。

APS 基本原理

APS（Automatic Protection Switching，自动保护倒换）是 SDH（Synchronous Digital Hierarchy，同步数字体系）网络的一个重要特性。它是指使用一条保护链路为一条或多条工作链路提供保护。当工作链路上出现故障以后，原来在工作链路上传输的业务可以自动的倒换到保护链路上来，从而保障用户数据不被丢失，最大限度地提高了网络的可靠性。

如图 3-1 所示，SDH 作为一个支撑网络，为数据通信网络提供了组建大型高速网络的可能。比如 A 和 B 两地的数据网络通过光纤将业务复用到 SDH 的净负荷中，就可以实现 A 和 B 两地的连通。由于 SDH 网络本身具备 APS 自动保护功能，所以路由器上的 APS 特性可以用来保护路由器接入 SDH 网络的接入链路部分，即路由器到 SDH 的 ADM（Add/Drop Multiplex，分插复用器）设备或者 RNC（Radio Network Controller，无线网络控制器）之间的通道的安全。当路由器之间直接连接在一起时，也能够实现路由器间的 APS 保护功能。

图 3-1 APS 组网图



APS 协议利用复用段开销（MSOH，Multiplex Section Over Header）中的 K1、K2 字节来传递，K1 传递倒换请求信号，K2 传递倒换证实信号，从而达到倒换和回切的目的。具体字节的含义，请参考《HUAWEI NetEngine80E/40E 路由器特性描述 可靠性》中的“APS”，此处不赘述。

APS 保护方式

- 根据保护结构分，可以分为 1+1 保护和 1:N（当 N=1 时，为 1:1）保护。
 - 1+1 保护：发送端在工作和保护两个链路上发同样的信息（双发），接收端在正常情况下收工作链路上的业务。它具有切换时间短，可靠性高等优点，但是缺点的是信道利用率低（50%）。

- 1:1 保护：正常时，工作链路发主要业务，保护链路空闲，接收端从工作链路收主要业务。优点是信道利用率高，但是可靠性不如 1+1 保护。
- 按照倒回模式分，可以分为倒回模式和非倒回模式。

当工作链路出现故障后，原来在工作链路上传输的数据自动倒换到保护链路上，保护链路开始工作。

 - 倒回模式就是在工作链路的故障消除后，通过一段倒回等待时间（WTR, Wait-to-Restore）的稳定，将业务及时倒回原工作通道，以让出保护通道的一种机制。
 - 不倒回模式在故障消除后，仍然使用保护链路，直至保护链路故障或者有其他链路请求保护倒换时才将业务倒回的一种机制。仅 1+1 模式支持不倒回模式。
- 按照发生链路故障时，两端是否同时切换，可以分为单向倒换和双向倒换。
 - 单向倒换：当工作链路故障时，仅接收端切换选收保护链路的数据。仅 1+1 保护支持单向倒换。
 - 双向倒换：当工作链路故障时，发送端和接收端都切换到保护链路上。1:1 和 1+1 保护都支持双向倒换。
- 按照保护的层次，可以分为 4 个层级。其中，端口、子卡和单板级为单机 APS；设备级为 E-APS。
 - 端口级：工作接口和保护接口位于同一路由器的同一单板同一子卡上。
 - 子卡级：工作接口和保护接口位于同一路由器的同一单板的不同子卡上。
 - 单板级：工作接口和保护接口位于同一路由器的不同单板上。
 - 设备级：工作接口和保护接口位于不同的路由器。其中，配置了工作接口的路由器我们称为工作路由器，配置了保护接口的路由器我们称为保护路由器。工作路由器和保护路由器之间在一条带外通道上运行 PGP（Protect Group Protocol，保护组协议）交换控制信息。

3.1.2 NE80E/40E 支持的 APS 特性

NE80E/40E 支持的 APS 特性主要包括保护倒换模式、保护的工作接口、故障恢复回切的方式。

NE80E/40E 目前实现的 APS 保护功能：

- 支持 1+1 单向、1:1 双向、1+1 双向保护倒换模式。
- 支持基于 APS Group 的手工倒换。
- 支持基于 APS Group 的强制倒换。
- 支持基于 APS Group 的锁定功能。
- 支持接口级的 APS 保护倒换。
- 支持同板、跨板的 APS 保护倒换。
- 支持跨设备的 APS 保护倒换，即 E-APS。
- 支持将 APS Group 的工作接口和保护接口加入 Trunk 口，相关业务都将在 Trunk 口上配置。

3.2 配置单机 APS

一台设备通过两条链路与另一条设备相连，这两台设备均支持 APS，配置单机 APS 可以提高链路的可靠性。

3.2.1 建立配置任务

在进行单机 APS 配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

当配置路由器网络侧下行方向与 RNC 对接时，用户可以配置单机 APS 以实现对接入链路的保护倒换。

前置任务

在配置 APS 之前，需完成以下任务：

- 在路由器上配置接口，使其与 RNC（Radio Network Controller）之间的链路协议 Up。

数据准备

在配置单机 APS 之前，需准备以下数据：

序号	数据
1	APS Group 编号
2	APS Group 工作接口和保护接口的编号
3	（可选）APS Group 倒回等待时间

3.2.2 配置 APS Group 的工作接口

配置 APS 必须指定工作接口。

背景信息

请在需要配置 APS 功能的路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface interface-type interface-number** 或 **controller cpos cpos-number**，进入接口视图。



说明

只有 LPUF-10 上的 ATM 接口、CPOS 接口支持 APS 功能。

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

步骤 3 执行命令 **aps group group-id**，创建 APS Group 并将接口加入该组。

步骤 4 执行命令 **aps working**，指定接口为 APS Group 的工作接口。

----结束

3.2.3 配置 APS Group 的保护接口

保护接口和工作接口必须加入相同的 APS Group。

背景信息

请在需要配置 APS 功能的路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface interface-type interface-number** 或 **controller cpos cpos-number**，进入接口视图。



说明

只有 LPUF-10 上的 ATM 接口、CPOS 接口支持 APS 功能。

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

步骤 3 执行命令 **aps group group-id**，创建 APS Group 并将接口加入该组。



注意

保护接口和工作接口必须加入相同的 APS Group。

步骤 4 执行命令 **aps protect**，指定接口为 APS Group 的保护接口。

步骤 5 (可选) 执行命令 **aps signal-low-priority**，配置 APS 保护接口 K 字节中端口信号故障请求码的优先级为低优先级。

APS 保护接口进行对接时，会利用报文中的 K 字节进行协商，K 字节中的端口信号故障请求码优先级默认为高优先级，如果对端设备的优先级为低，需要配置此命令将本端的优先级配置为低方可进行对接。

----结束

3.2.4 (可选) 配置 APS Group 的工作模式

APS 自动保护倒换的模式只能在 APS Group 的在保护接口配置。

背景信息

请在 APS Group 的保护接口上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface interface-type interface-number** 或 **controller cpos cpos-number**，进入 APS Group 的保护接口视图。

步骤 3 执行命令 **aps mode { one2one bidirection | one-plus-one unidirection | one-plus-one bidirection }**，配置 APS 的工作模式。保护接口的 APS 的工作模式在接口 shutdown 和 undo shutdown 后生效。

- **one2one bidirection:**
 - 指定 APS 保护倒换模式为 1:1，即只有工作链路传送业务数据，保护链路留作备份。
 - 指定 APS 保护倒换模式为双向倒换，当端口发生故障时，即发送方和接收方都将业务数据倒换到保护链路上。
- **one-plus-one unidirection:**
 - 指定 APS 保护倒换模式为 1+1，即工作链路和保护链路都传送业务数据。
 - 指定 APS 保护倒换模式为单向倒换，当端口光纤发生单纤故障时，即只有接收方将业务数据倒换到保护链路上。
- **one-plus-one bidirection:**
 - 指定 APS 保护倒换模式为 1+1，即工作链路和保护链路都传送业务数据。
 - 指定 APS 保护倒换模式为双向倒换，当端口发生故障时，即发送方和接收方都将业务数据倒换到保护链路上。

----结束

3.2.5 （可选）配置 APS Group 的倒换模式

背景信息

请在 APS Group 的保护接口上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **interface interface-type interface-number** 或 **controller cpos cpos-number**，进入 APS Group 的保护接口视图。
- 步骤 3** 执行命令 **aps switch-command { lockout | force | manual }**，配置 APS Group 倒换命令。
- **lockout:** 指定 APS Group 进行保护锁定，业务被锁定在工作链路上。
 - **force:** 指定 APS Group 进行强制倒换，业务被强制倒换到保护链路上。
 - **manual:** 指定 APS Group 进行人工倒换，业务被人工倒换到保护链路上。

----结束

3.2.6 （可选）配置 APS Group 的倒回等待时间

倒回等待时间只能在 APS Group 的在保护接口配置。

背景信息

请在 APS Group 的保护接口上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number* 或 **controller cpos** *cpo-number*，进入 APS Group 的保护接口视图。

步骤 3 执行命令 **aps revert** *wtr-time*，配置 APS Group 的倒回等待时间。

wtr-time：整数形式，取值范围是 1 ~ 12，单位是分钟。

配置倒回等待时间时，需要注意以下事项：

- 若 APS 的工作模式为 1:1，则默认故障恢复后数据业务回切到工作接口上，倒回等待时间为 5 分钟。

 说明

NE80E/40E 系列中的 X1 和 X2 设备上的默认倒回等待时间为 5 分钟。

- 若 APS 的工作模式为 1+1，则默认故障恢复后数据业务不回切到工作接口上。可以运行此命令配置 APS Group 的倒回等待时间，故障恢复后，数据业务将在倒回等待时间后回切到工作接口上。

----结束

3.2.7 将 APS Group 成员加入 Trunk

工作接口和保护接口必须加入同一 trunk 链路。

背景信息

请在 APS Group 的工作接口和保护接口上分别进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface atm-trunk** *interface-number*，创建 Atm-trunk 接口并进入接口视图。

 说明

支持 APS 功能的接口有 ATM 接口、和 CPOS 接口，对应的 Trunk 接口分别是 Atm-trunk，和 Cpos-trunk。此处以 Atm-Trunk 为例说明配置操作。

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

步骤 3 执行命令 **quit**，返回系统视图。

步骤 4 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 5 执行命令 **atm-trunk** *trunk-id*，将接口加入 Trunk。



注意

APS Group 的工作接口和保护接口需要加入同一 trunk-id 的 Trunk 接口。

----结束

3.2.8 检查配置结果

单机 APS 配置完成后，您可以查看到 APS 组的工作模式、工作接口、回切时间和接口状态。

操作步骤

步骤 1 执行命令 **display aps group group-id**，可以查看 APS Group 的相关配置信息。

步骤 2 分别执行以下命令，查看各种接口类型的 Trunk 接口的信息。

 说明

ATM 接口在 NE80E/40E 系列中的 X1 和 X2 设备上不支持。

- 执行命令 **display atm-trunk trunk-id**，可以查看 ATM-trunk 的相关配置信息。
- 执行命令 **display cpos-trunk trunk-id**，可以查看 CPOS-Trunk 的相关配置信息。

----结束

任务示例

```
<HUAWEI> display aps group 1
APS Group 1: Atm1/0/1 working channel 1(Active)
              Atm1/0/2 protection channel 0(Inactive)
              Unidirectional, 1+1 mode, Revert time(10 minutes)
              No Request on Both Working and Protection Side
```

Group	Work-Channel	Protect-Channel	Wtr	W-State	P-State	Switch-Cmd	Switch-Result
1	Atm1/0/1	Atm1/0/2	10	ok	ok	NA	idle

total entry: 1

查看 Trunk 接口的配置信息。

```
<HUAWEI> display atm-trunk 1
Interface Atm-Trunk1's state information is:
Operate status: up      Number Of Up Port In Trunk: 2
```

PortName	Status	Active Status
Atm1/0/1	Up	Active
Atm1/0/2	Up	Inactive

查看 CPOS-Trunk 接口的状态信息。

```
<HUAWEI> display cpos-trunk 1
Interface Cpos-Trunk1's state information is:,
Operate status: up      Number Of Up Port In Trunk: 2
```

PortName	Status	Active Status
Cpos1/0/1	Up	Active
Cpos1/0/2	Up	Inactive

3.3 配置 E-APS

配置 E-APS 可以实现跨设备的 APS 倒换。

3.3.1 建立配置任务

在进行 E-APS 配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在路由器网络侧下行方向与 RNC 对接时，若 RNC 双归接入用户可以配置 E-APS。

前置任务

在配置 E-APS 之前，需完成以下任务：

- 在路由器上配置接口，使其与 RNC 之间的链路协议 Up。

数据准备

在配置 E-APS 之前，需准备以下数据：

序号	数据
1	APS Group 编号
2	APS Group 工作接口和保护接口的编号
3	（可选）APS Group 倒回等待时间
4	（可选）PGP 协议认证字符串
5	（可选）工作接口与保护接口间发送 APS 协商报文的时间间隔
6	（可选）APS 连接状态的保持时间

3.3.2 配置 APS Group 的工作接口

配置 APS 必须指定工作接口。

背景信息

请在需要配置 APS 功能的路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface interface-type interface-number** 或 **controller cpos cpos-number**，进入接口视图。

 说明

只有 LPUF-10 上的 ATM 接口、CPOS 接口支持 APS 功能。

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

步骤 3 执行命令 **aps group group-id**，创建 APS Group 并将接口加入该组。

步骤 4 执行命令 **aps working peer-ip local-ip**，指定接口为 APS Group 的工作接口。

- *peer-ip*：指定同一 APS Group 的保护接口所在路由器的 IP，一般是指该路由器上 Loopback 接口的 IP。
- *local-ip*：指定属于同一 APS Group 的工作接口所在本地 Router 的 IP 地址，一般是指该 Router 上 Loopback 接口的 IP 地址。

----结束

3.3.3 配置 APS Group 的保护接口

保护接口和工作接口必须加入相同的 APS Group。

背景信息

请在需要配置 APS 功能的路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface interface-type interface-number** 或 **controller cpos cpos-number**，进入接口视图。

 说明

只有 LPUF-10 上的 ATM 接口、CPOS 接口支持 APS 功能。

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

步骤 3 执行命令 **aps group group-id**，创建 APS Group 并将接口加入该组。



注意

保护接口和工作接口必须加入相同的 APS Group。

步骤 4 执行命令 **aps protect peer-ip local-ip**，指定接口为 APS Group 的保护接口。

- **peer-ip**: 指定同一 APS Group 的保护接口所在路由器的 IP，一般是指该路由器上 Loopback 接口的 IP。
- **local-ip**: 指定属于同一 APS Group 的工作接口所在本地 Router 的 IP 地址，一般是指该 Router 上 Loopback 接口的 IP 地址。

步骤 5 (可选) 执行命令 **aps signal-low-priority**，配置 APS 保护接口 K 字节中端口信号故障请求码的优先级为低优先级。

APS 保护接口进行对接时，会利用报文中的 K 字节进行协商，K 字节中的端口信号故障请求码优先级默认为高优先级，如果对端设备的优先级为低，需要配置此命令将本端的优先级配置为低方可进行对接。

----结束

3.3.4 配置 APS Group 的工作模式

APS 自动保护倒换的模式只能在 APS Group 的在保护接口配置。

背景信息

请在 APS Group 的保护接口上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number* 或 **controller cpos** *cpo-number*，进入接口视图。

步骤 3 执行命令 **aps mode** { **one2one bidirection** | **one-plus-one** { **bidirection** | **unidirection** } }，配置 APS 的工作模式。

在 shutdown 和 undo shutdown 保护接口后工作模式才生效。

● **one2one bidirection:**

- 指定 APS 保护倒换模式为 1:1，即只有工作链路传送业务数据，保护链路留作备份。
- 指定 APS 保护倒换模式为双向倒换，当端口发生故障时，即发送方和接收方都将业务数据倒换到保护链路上。

● **one-plus-one unidirection:**

- 指定 APS 保护倒换模式为 1+1，即工作链路和保护链路都传送业务数据。
- 指定 APS 保护倒换模式为单向倒换，当端口光纤发生单纤故障时，即只有接收方将业务数据倒换到保护链路上。

● **one-plus-one bidirection:**

- 指定 APS 保护倒换模式为 1+1，即工作链路和保护链路都传送业务数据。
- 指定 APS 保护倒换模式为双向倒换，当端口发生故障时，即发送方和接收方都将业务数据倒换到保护链路上。

 说明

one-plus-one bidirection 模式在 NE80E/40E 系列中的 X1 和 X2 设备上不支持。

 说明

配置 E-APS 时不支持 1+1 单向模式。

----结束

3.3.5 （可选）配置 APS Group 的倒换模式

背景信息

请在 APS Group 的保护接口上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number* 或 **controller cpos** *cpo-number*，进入 APS Group 的保护接口视图。

步骤 3 执行命令 **aps switch-command** { **lockout** | **force** | **manual** }，配置 APS Group 倒换命令。

- **lockout:** 指定 APS Group 进行保护锁定，业务被锁定在工作链路上。
- **force:** 指定 APS Group 进行强制倒换，业务被强制倒换到保护链路上。
- **manual:** 指定 APS Group 进行人工倒换，业务被人工倒换到保护链路上。

----结束

3.3.6 （可选）配置发送 APS 协商报文的时间间隔和保持连接状态的时间

APS 工作接口和保护接口的连接状态的保持时间建议配置大于等于 10 秒。

背景信息

请在 APS Group 的保护接口和工作接口上分别进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **interface interface-type interface-number** 或 **controller cpos cpos-number**，进入工作接口或保护接口视图。
- 步骤 3** 执行命令 **aps timers keep-alive-time hold-time**，配置工作接口与保护接口之间发送 APS 协商报文的时间间隔和连接状态的保持时间。
 - **keep-alive-time**：本端发送 APS 协商报文的时间间隔。整数形式，取值范围是 1 ~ 60，单位是秒。
 - **hold-time**：APS 连接状态的保持时间。整数形式，取值范围是 3 ~ 300，单位是秒。建议配置大于 10 秒。配置的 APS 连接状态的保持时间必须是发送 APS 协商报文的时间间隔的 3 倍及以上。

 说明

hold-time 在 NE80E/40E 系列中的 X1 和 X2 设备上支持的取值范围是 1 ~ 300，缺省值是 180。

----结束

3.3.7 （可选）配置 PGP 协议认证字符串

配置 E-APS 的两台设备通过该认证字符串来进行安全性检查，只有两端的认证字符串一致的情况下，才能建立正常的 PGP 协商，否则会协商失败。

背景信息

请在 APS Group 的保护接口和工作接口上分别进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **interface interface-type interface-number** 或 **controller cpos cpos-number**，进入工作接口或保护接口视图。
- 步骤 3** 执行命令 **aps authenticate string**，配置 PGP 协议认证字符串。



注意

配置 PGP 协议认证字符串之前必须先将接口指定为 E-APS 中 APS Group 的工作接口和保护接口。

保护接口和工作接口上的 PGP 协议认证字符串配置一致时才能建立正常的 PGP 协商。

----结束

3.3.8 （可选）配置 APS Group 的倒回等待时间

倒回等待时间只能在 APS Group 的保护接口配置。

背景信息

请在 APS Group 的保护接口上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface interface-type interface-number** 或 **controller cpos cpos-number**，进入 APS Group 的保护接口视图。

步骤 3 执行命令 **aps revert wtr-time**，配置 APS Group 的倒回等待时间。

wtr-time：整数形式，取值范围是 1 ~ 12，单位是分钟。

配置倒回等待时间时，需要注意以下事项：

- 若 APS 的工作模式为 1:1，则默认故障恢复后数据业务回切到工作接口上，倒回等待时间为 5 分钟。



NE80E/40E 系列中的 X1 和 X2 设备上的默认倒回等待时间为 5 分钟。

- 若 APS 的工作模式为 1+1，则默认故障恢复后数据业务不回切到工作接口上。可以运行此命令配置 APS Group 的倒回等待时间，故障恢复后，数据业务将在倒回等待时间后回切到工作接口上。

----结束

3.3.9 将 APS Group 成员加入 Trunk

工作接口和保护接口必须加入同一 trunk 链路。

背景信息

请在 APS Group 的工作接口和保护接口上分别进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface atm-trunk interface-number**，创建 Atm-trunk 接口并进入接口视图。



说明

支持 APS 功能的接口有 ATM 接口、和 CPOS 接口，对应的 Trunk 接口分别是 Atm-trunk，和 Cpos-trunk。此处以 Atm-Trunk 为例说明配置操作。

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

步骤 3 执行命令 **quit**，返回系统视图。

步骤 4 执行命令 **interface interface-type interface-number**，进入接口视图。

步骤 5 执行命令 **atm-trunk trunk-id**，将接口加入 Trunk。

----结束

3.3.10 检查配置结果

E-APS 配置完成后，您可以查看到 APS 组的工作模式、工作接口、回切时间和接口状态。

操作步骤

步骤 1 执行命令 **display aps group group-id**，可以查看 APS Group 的相关配置信息。

步骤 2 分别执行以下命令，查看各种接口类型的 Trunk 接口的信息。



说明

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

- 执行命令 **display atm-trunk trunk-id**，可以查看 ATM-trunk 的相关配置信息。
- 执行命令 **display cpos-trunk trunk-id**，可以查看 CPOS-Trunk 的相关配置信息。

----结束

任务示例

配置完 E-APS，在保护接口所在的路由器上执行命令 **display aps group group-id**，查看 APS Group 的相关配置信息。

```
<HUAWEI> display aps group 1
APS Group 1: APS working channel is 72.72.72.72
               Atm1/0/1 protection channel 0(Inactive)
               PGP authentication string: 111
               Bidirection, 1:1 mode, Revert time(1 minutes)
               KeepAlive Timer: 1(seconds), Hold Timer: 3(seconds)
               No Request on Both Working and Protection Side
```

Group	Work-Channel	Protect-Channel	Wtr	W-State	P-State	Switch-Cmd	Switch-Result
1	72.72.72.72	Atm1/0/1	1	ok	ok	NA	idle

查看 Trunk 接口的配置信息。

```
<HUAWEI> display atm-trunk 1
Interface Atm-Trunk1's state information is:
Operate status: up      Number Of Up Port In Trunk: 1
```

PortName	Status	Active Status
Atm1/0/1	Up	Active

3.4 配置举例

介绍 APS 的各种示例。配置示例中包括组网需求、配置注意事项和配置思路等。

背景信息

说明

手册中所使用的链路接口编号和链路类型以 NE40E-X8 为例，实际使用时以现网设备为准。

3.4.1 配置 CPOS 接口下基于 APS 的 TDM 功能

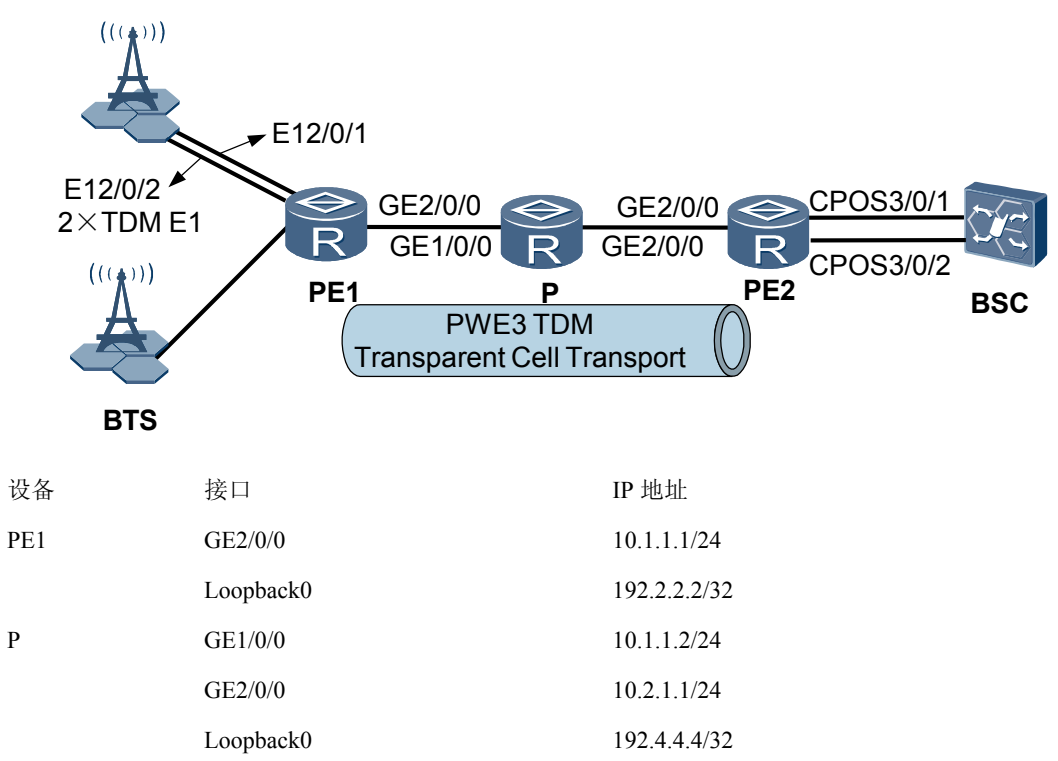
介绍一个 CPOS 接口下基于 APS 的 TDM 功能的配置示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

组网需求

在 2G RAN 上,基站 BTS 出 1—3 个 E1 接口与基站控制器 BSC 相连是最普遍的情形。部分无线运营商没有固网基础设施，租用固网运营商的 E1 专线，费用较高。通过部署 TDMoPSN 业务，即 TDM 业务透传应用于 2G RAN，利用简单、便宜的城域以太网和 TDM 业务透传技术实现同城区域内基站和基站控制器之间的业务传送。

如图 3-2 所示，BTS 和 PE1 之间通过 2 路 E1 链路接入。BSC 和路由器之间 PE2 采用两个 CPOS 接口接入，在 CPOS 接口上配置单机 APS 以提高数据传输的可靠性。在 E1 链路通道化串口下配置封装协议为 TDM。PE1 和 PE2 之间形成 PW 通路，透传 TDM 信元。

图 3-2 配置 TDMoPSN 组网图



PE2	GE2/0/0	10.2.1.2/24
	Loopback0	192.3.3.3/32

配置思路

在 PSN 网络中配置 PW 隧道来传输 TDM 业务时，按照如下顺序进行：

1. 在骨干网上运行 IGP 路由协议，使骨干网各设备能互通。
2. 在骨干网上配置 MPLS 基本能力，在 PE 设备上配置 MPLS L2VPN。且 PW 两端的 PE 之间要建立 MPLS LDP 远端对等体关系。
3. 配置 TDM 接口参数。
4. 配置 PW。
5. 在 PE 上创建 MPLS L2VC 连接。
6. 在 PE2 上配置单机 APS。

数据准备

为完成此配置例，需准备如下的数据：

- PW 两端的 L2VC ID（必须一致）
- 各个 PE 及 P 上的 MPLS LSR-ID
- 设置 PE 远端对等体的 IP 地址

操作步骤

步骤 1 在骨干网上运行 IGP 路由协议，使骨干网各设备能互通（略）。具体配置请参见配置文件

步骤 2 在骨干网上配置 MPLS 基本能力，在 PE 设备上配置 MPLS L2VPN。且 PW 两端的 PE 之间要建立 MPLS LDP 远端对等体关系（略）。具体配置请参见配置文件

建立动态 PW 才需要建立 MPLS LDP 远端对等体关系。

步骤 3 配置单机 APS



注意

要求与 PE2 相连的 BSC 设备也必须支持 APS 功能。

配置 PE2

```
[PE2] controller cpos 3/0/1
[PE2-Cpos3/0/1] aps group 1
[PE2-Cpos3/0/1] aps working
[PE2-Cpos3/0/1] quit
[PE2] controller cpos 3/0/2
[PE2-Cpos3/0/2] aps group 1
[PE2-Cpos3/0/2] aps protect
[PE2-Cpos3/0/2] aps mode one-plus-one unidirection
[PE2-Cpos3/0/2] quit
```

```
[PE2] interface cpos-trunk 1
[PE2-cpos-trunk1] quit
[PE2] controller cpos 3/0/1
[PE2-Cpos3/0/1] cpos-trunk 1
[PE2-Cpos3/0/1] quit
[PE2] controller cpos 3/0/2
[PE2-Cpos3/0/2] cpos-trunk 1
```

在 PE2 上分别执行命令 **display aps group**，查看 APS Group 的配置信息；执行命令 **display cpos-trunk** 查看 Cpos-trunk 接口的配置信息。

```
<PE2> display aps group 1
APS Group 1: Cpos 3/0/1 working channel 1(Active)
              Pos3/0/2 protection channel 0(Inactive)
              Unidirection, 1+1 mode, No Revert mode
              No Request on Both Working and Protection Side
```

```
-----
Group Work-Channel Protect-Channel Wtr W-State P-State Switch-Cmd Switch-Result
-----
1      Cpos 3/0/1   Cpos 3/0/2   NA    ok      ok      NA      idle
-----

total entry: 1
<PE2> display cpos-trunk 1
Interface Cpos-Trunk1's state information is:,
Operate status: up      Number Of Up Port In Trunk: 2
-----
PortName      Status      Active Status
Cpos3/0/1     Up          Active
Cpos3/0/2     Up          Inactive
```

步骤 4 配置 TDM 接口参数

1. 配置 PE1。

配置 PE1 上的 CE1 2/0/1 和 CE1 2/0/2 接口的参数，采用通道化模式。

```
[PE1] controller e1 2/0/1
[PE1-E1 2/0/1] using cel
[PE1-E1 2/0/1] channel-set 1 timeslot-list 1-15 ts0
[PE1-E1 2/0/1] quit
[PE1] controller e1 2/0/2
[PE1-E1 2/0/2] using cel
[PE1-E1 2/0/2] channel-set 1 timeslot-list 16-31 ts0
[PE1-E1 2/0/2] quit
```

2. 配置 PE2。

配置 PE2 上的 CPOS 接口参数。

```
[PE2] interface cpos-trunk 1
[PE2-Cpos-trunk1] e1 1 channel-set 1 timeslot-list 1-15 ts0
[PE2-Cpos-trunk1] e1 2 channel-set 2 timeslot-list 16-31 ts0
```

步骤 5 配置串口的封装协议为 TDM

1. 配置 PE1。

```
[PE1] interface serial2/0/1:1
[PE1-Serial2/0/1:0] link-protocol tdm
[PE1-Serial2/0/1:0] quit
[PE1] interface serial2/0/2:1
[PE1-Serial2/0/2:1] link-protocol tdm
[PE1-Serial2/0/2:1] quit
```

2. 配置 PE2。

```
[PE2] interface trunk-serial1/1:1
[PE2-Trunk-Serial1/1:1] link-protocol tdm
[PE2-Serial1/1:1] quit
[PE2] interface trunk-serial1/2:2
```

```
[PE2-Trunk-Serial1/2:2] link-protocol tdm
[PE2-Trunk-Serial1/2:2] quit
```

步骤6 配置 PW

1. 配置 PE1。

```
[PE1] pw-template lto3
[PE1-pw-template-lto3] peer-address 192.3.3.3
[PE1-pw-template-lto3] jitter-buffer depth 20
[PE1-pw-template-lto3] tdm-encapsulation-number 40
[PE1-pw-template-lto3] quit
[PE1] interface serial2/0/1:1
[PE1-Serial2/0/1:0] mpls l2vc pw-template lto3 100
[PE1] interface serial2/0/2:1
[PE1-Serial2/0/2:1] mpls l2vc pw-template lto3 200
```

2. 配置 PE2。

```
[PE2] pw-template 3tol
[PE2-pw-template-3tol] peer-address 192.2.2.2
[PE2-pw-template-3tol] jitter-buffer depth 20
[PE2-pw-template-3tol] tdm-encapsulation-number 40
[PE2-pw-template-3tol] quit
[PE2] interface trunk-serial1/1:1
[PE2-Trunk-Serial1/1:1] mpls l2vc pw-template 3tol 100
[PE2-Trunk-Serial1/1:1] undo shutdown
[PE2-Trunk-Serial1/1:1] quit
[PE2] interface trunk-serial1/2:2
[PE2-Trunk-Serial1/2:2] mpls l2vc pw-template 3tol 200
[PE2-Trunk-Serial1/2:2] undo shutdown
[PE2-Trunk-Serial1/2:2] quit
```

在 PE1 上执行命令 **display mpls l2vc** 查看 PW 的状态，其状态为 Up。

PE1 的显示。

```
<PE1> display mpls l2vc interface serial2/0/1:1
*client interface      : Serial2/0/1:1 is up
  session state        : up
  AC state              : up
  VC state              : up
  VC ID                 : 100
  VC type               : CESoPSN basic mode
  destination           : 192.3.3.3
  local group ID        : 0
  remote group ID       : 0
  local VC label        : 146432
  remote VC label       : 145287
  TDM encapsulation number : 40
  jitter-buffer         : 20
  idle-code             : FF
  rtp-header            : disable
  local AC OAM State    : up
  local PSN State       : up
  local forwarding state : forwarding
  local status code     : 0x0
  remote AC OAM state    : up
  remote PSN state      : up
  remote forwarding state : forwarding
  remote statuscode     : 0x0
  BFD for PW            : unavailable
  manual fault          : not set
  active state          : active
  forwarding entry      : not exist
  link state            : up
  local VC MTU          : 1500
  remote VC MTU         : 1500
  local VCCV            : alert lsp-ping bfd
  remote VCCV           : none
  local control word    : disable
  remote control word   : disable
```

```
tunnel policy name      : --
traffic behavior name   : --
PW template name        : --
primary or secondary    : primary
VC tunnel/token info    : 0 tunnels/tokens
create time             : 0 days, 4 hours, 48 minutes, 51 seconds
up time                 : 0 days, 3 hours, 43 minutes, 49 seconds
last change time        : 0 days, 0 hours, 39 minutes, 29 seconds
VC last up time         : 2008/12/26 12:02:49
VC total up time        : 0 days, 3 hours, 43 minutes, 49 seconds
CKey                    : 11
NKey                    : 10
```

步骤 7 检查配置结果

模拟 PE2 接入 BSC 侧故障

在接口 CPOS 3/0/1 上执行命令 **shutdown**。

```
[PE2] controller cpos 3/0/1
[PE2-Cpos3/0/1] shutdown
```

在 PE2 上分别执行命令 **display aps group 1**，查看 APS Group 的成员接口的状态信息，执行命令 **display cpos-trunk 1**，查看 CPOS-Trunk 成员接口的状态信息，可以看到保护接口 CPOS 3/0/2 的状态变为 Active。

```
[PE2] display aps group 1
APS Group 1: Cpos 3/0/1 working channel 1(Inactive)
              Pos3/0/2 protection channel 0(Active)
              Unidirection, 1+1 mode, No Revert mode
              No Request on Both Working and Protection Side
```

Group	Work-Channel	Protect-Channel	Wtr	W-State	P-State	Switch-Cmd	Switch-Result
1	Cpos 3/0/1	Cpos 3/0/2	NA	sf	ok	NA	switch

total entry: 1

```
<PE2> display cpos-trunk 1
Interface Cpos-Trunk1's state information is:,
Operate status: up      Number Of Up Port In Trunk: 2
```

PortName	Status	Active Status
Cpos3/0/1	Down	Inactive
Cpos3/0/2	Up	Active

在 PE1 上执行命令 **display mpls l2vc** 查看 PW 的状态，可以看到 PE2 上 CPOS3/0/1 接口的故障并未影响到 PW 的状态。

```
<PE1> display mpls l2vc interface serial2/0/1:1
*client interface      : Serial2/0/1:1 is up
  session state        : up
  AC state             : up
  VC state             : up
  VC ID               : 100
  VC type              : CESoPSN basic mode
  destination          : 192.3.3.3
  local group ID       : 0
  remote group ID      : 0
  local VC label       : 146432
  remote VC label      : 145287
  TDM encapsulation number : 40
  jitter-buffer        : 20
  idle-code            : FF
  rtp-header           : disable
  local AC OAM State   : up
  local PSN State      : up
  local forwarding state : forwarding
  local status code    : 0x0
```

```

remote AC OAM state      : up
remote PSN state        : up
remote forwarding state  : forwarding
remote statuscode       : 0x0
BFD for PW              : unavailable
manual fault            : not set
active state            : active
forwarding entry        : not exist
link state              : up
local VC MTU            : 1500
remote VC MTU           : 1500
local VCCV              : alert lsp-ping bfd
remote VCCV             : none
local control word      : disable
remote control word     : disable
tunnel policy name      : --
traffic behavior name   : --
PW template name       : --
primary or secondary    : primary
VC tunnel/token info    : 0 tunnels/tokens
create time             : 0 days, 4 hours, 48 minutes, 51 seconds
up time                 : 0 days, 4 hours, 02 minutes, 39 seconds
last change time        : 0 days, 0 hours, 39 minutes, 29 seconds
VC last up time         : 2008/12/26 12:02:49
VC total up time        : 0 days, 4 hours, 02 minutes, 39 seconds
CKey                    : 11
NKey                    : 10

```

----结束

配置文件

- PE1 的配置文件

```

#
sysname PE1
#
mpls lsr-id 192.2.2.2
mpls
#
mpls l2vpn
#
pw-template lto3
peer-address 192.3.3.3
jitter-buffer depth 20
tdm-encapsulation-number 40
#
mpls ldp
#
mpls ldp remote-peer 192.3.3.3
remote-ip 192.3.3.3
#
controller e1 2/0/1
using cel
channel-set 1 timeslot-list 1-15 ts0
undo shutdown
#
controller e1 2/0/2
using cel
channel-set 1 timeslot-list 16-31 ts0
undo shutdown
#
interface serial2/0/1:1
link-protocol tdm
mpls l2vc pw-template lto3 100
undo shutdown
#
interface serial2/0/2:1
link-protocol tdm

```

```
mpls l2vc pw-template lto3 200
undo shutdown
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 10.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 192.2.2.2 255.255.255.255
#
ospf 1
area 0.0.0.0
network 192.2.2.2 0.0.0.0
network 10.1.1.0 0.0.0.255
#
return
```

● PE2 的配置文件

```
#
sysname PE2
#
mpls lsr-id 192.3.3.3
mpls
#
mpls l2vpn
#
pw-template 3tol
peer-address 192.2.2.2
jitter-buffer depth 20
tdm-encapsulation-number 40
#
mpls ldp
#
mpls ldp remote-peer 192.2.2.2
remote-ip 192.2.2.2
#
cpos-trunk 1
el 1 channel-set 1 timeslot-list 1-15 ts0
code ami
el 2 channel-set 2 timeslot-list 16-31 ts0
#
interface serial1/1:1
link-protocol tdm
mpls l2vc pw-template 3tol 100
undo shutdown
#
interface serial1/2:2
link-protocol tdm
mpls l2vc pw-template 3tol 200
undo shutdown
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 10.2.2.2 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 192.3.3.3 255.255.255.255
#
ospf 1
area 0.0.0.0
network 192.3.3.3 0.0.0.0
network 10.2.2.0 0.0.0.255
#
return
```

● P 的配置文件


```
#
sysname P
#
mpls lsr-id 192.4.4.4
mpls
#
mpls ldp
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 10.2.2.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 192.4.4.4 255.255.255.255
#
ospf 1
area 0.0.0.0
network 192.4.4.4 0.0.0.0
network 10.1.1.0 0.0.0.255
network 10.2.2.0 0.0.0.255
#
return
```

3.4.2 配置 CPOS-Trunk 的 APS 保护倒换示例

以 CPOS-Trunk 汇聚多路中低端设备的 E1 链路的典型组网为背景，介绍如何在 CPOS 接口上配置 APS 实现保护倒换，配置 CPOS-Trunk 以实现路由器对各中低端设备业务的汇聚并能通过时隙唯一识别各中低端设备。配置示例包括组网需求、思路准备、操作步骤和配置文件。

组网需求



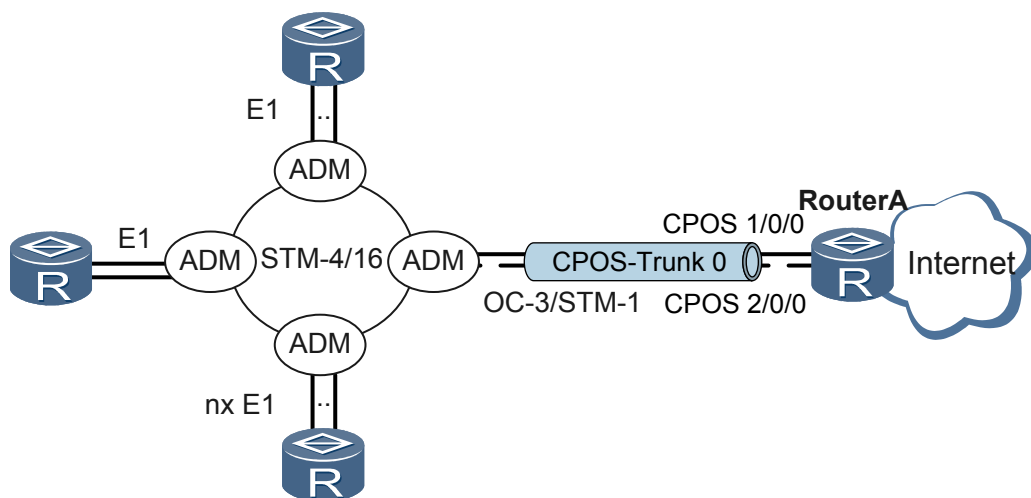
说明

手册中所使用的链路接口编号和链路类型以 NE40E-X8 为例，实际使用时以现网设备为准。

如图 3-3 所示，一些中低端设备通过一个或几个 E1 租用线接入到传输网。所有这些用户的带宽经过传输网汇聚到 RouterA 的 CPOS-Trunk，RouterA 通过时隙唯一识别各低端设备。RouterA 的 CPOS-Trunk 由 2 个 CPOS 接口组成，在 CPOS 接口上配置单机 APS 以提高数据传输的可靠性。

实际情况中，CPOS 接口与各低端设备之间可能经过不止一级传输网，各低端设备与传输网之间可能还需要其他的传输手段进行中继。

图 3-3 配置 CPOS-Trunk 的 APS 保护倒换组网图



配置思路

采用如下的思路配置：

1. 在两个 CPOS 接口间配置单机 APS，并将其加入同一个 CPOS-Trunk
2. 对 CPOS-Trunk 的 E1 通道的时隙进行捆绑，创建 Trunk-serial 接口，并将其加入 Global-MP-Group

数据准备

为完成此配置例，需准备如下的数据：

- 配置 APS 所需的参数。
- CPOS-Trunk 所需的参数。
- Global-MP-Group 接口的编号

操作步骤

步骤 1 配置单机 APS

1. 在 RouterA 上配置单机 APS 功能


```

<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] controller cpos 1/0/0
[RouterA-Cpos1/0/0] undo shutdown
[RouterA-Cpos1/0/0] aps group 1
[RouterA-Cpos1/0/0] aps working
[RouterA-Cpos1/0/0] quit
[RouterA] controller cpos 2/0/0
[RouterA-Cpos2/0/0] undo shutdown
[RouterA-Cpos2/0/0] aps group 1
[RouterA-Cpos2/0/0] aps protect
[RouterA-Cpos2/0/0] aps mode one-plus-one unidirection
[RouterA-Cpos2/0/0] quit
      
```
2. 在 RouterA 上创建 CPOS-Trunk，并加入成员接口


```

[RouterA] interface cpos-trunk 0
[RouterA-Cpos-Trunk0] quit
      
```

```
[RouterA] controller cpos 1/0/0
[RouterA-Cpos1/0/0] cpos-trunk 0
[RouterA-Cpos1/0/0] quit
[RouterA] controller cpos 2/0/0
[RouterA-Cpos2/0/0] cpos-trunk 0
[RouterA-Cpos2/0/0] quit
```

步骤 2 配置 CPOS-Trunk

1. 对 CPOS-Trunk 的 E1 通道的时隙进行捆绑

```
[RouterA] interface cpos-trunk 0
[RouterA-Cpos-Trunk0] e1 1 channel-set 1 timeslot-list 1-15
[RouterA-Cpos-Trunk0] e1 2 channel-set 2 timeslot-list 17-31
[RouterA-Cpos-Trunk0] quit
```

2. 创建一个 Global-Mp-Group

```
[RouterA] interface global-mp-group 0
[RouterA-Global-Mp-Group0] shutdown
[RouterA-Global-Mp-Group0] quit
```

3. 将 Trunk-Serial 加入 Global-Mp-Group 当中

```
[RouterA] interface Trunk-Serial0/1:1
[RouterA-Trunk-Serial0/1:1] shutdown
[RouterA-Trunk-Serial0/1:1] link-protocol ppp
[RouterA-Trunk-Serial0/1:1] ppp mp-global global-mp-group 0
[RouterA-Trunk-Serial0/1:1] quit
[RouterA] interface Trunk-Serial0/2:2
[RouterA-Trunk-Serial0/2:2] shutdown
[RouterA-Trunk-Serial0/2:2] link-protocol ppp
[RouterA-Trunk-Serial0/2:2] ppp mp-global global-mp-group 0
[RouterA-Trunk-Serial0/2:2] quit
```

4. 重启通道和 Global-Mp-Group

```
[RouterA] interface global-mp-group 0
[RouterA-Global-Mp-Group0] undo shutdown
[RouterA-Global-Mp-Group0] quit
[RouterA] interface Trunk-Serial0/1:1
[RouterA-Trunk-Serial0/1:1] undo shutdown
[RouterA-Trunk-Serial0/1:1] quit
[RouterA] interface Trunk-Serial0/2:2
[RouterA-Trunk-Serial0/2:2] undo shutdown
[RouterA-Trunk-Serial0/2:2] quit
```

步骤 3 检查配置结果

在 RouterA 上执行命令 **display aps group**，查看 APS 的配置信息，可以看到配置的工作接口与保护接口的信息，以及保护倒换时间。

```
[RouterA] display aps group 1
APS Group 1: Cpos1/0/0 working channel 1(Active)
              Cpos2/0/0 protection channel 0(Inactive)
              Unidirectional, 1+1 mode, Revert time(6 minutes)
              No Request on Both Working and Protection Side
```

```
-----
Group Work-Channel Protect-Channel Wtr W-State P-State Switch-Cmd Switch-Result
-----
1      Cpos1/0/0    Cpos2/0/0    6    ok      ok      NA      idle
-----
total entry: 1
```

执行命令 **display cpos-trunk** 查看 CPOS-Trunk 接口的配置信息，可以看到 CPOS-Trunk 里各成员接口的状态。

```
[RouterA] display cpos-trunk 0
Interface Cpos-Trunk0's state information is:
Operate status: up      Number Of Up Port In Trunk: 1
```

```
-----
PortName      Status      Active Status
-----
```

Cpos1/0/0	Up	Active
Cpos2/0/0	Up	Inactive

执行命令 **display ppp mp-global** 查看 Global-Mp-Group 的配置信息，可以看到 Global-Mp-Group 里 Trunk-Serial 的状态。

```
[RouterA] display ppp mp-global
Global-Mp-Group is Global-Mp-Group0
=====Sublinks status begin=====
Trunk-Serial0/1:1 physical UP, protocol UP
Trunk-Serial0/2:2 physical UP, protocol UP
=====Sublinks status end=====
```

----结束

配置文件

#

RouterA 的配置文件

```
#
sysname RouterA
#
controller Cpos1/0/0
undo shutdown
aps group 1
aps working
cpos-trunk 0
#
controller Cpos2/0/0
undo shutdown
aps group 1
aps protect
aps mode one-plus-one unidirection
cpos-trunk 0
#
interface Cpos-Trunk0
undo shutdown
el 1 channel-set 1 timeslot-list 1-15
el 2 channel-set 2 timeslot-list 17-31
#
interface Global-Mp-Group0
undo shutdown
#
interface Trunk-Serial0/1:1
undo shutdown
link-protocol ppp
ppp mp-global global-mp-group 0
#
interface Trunk-Serial0/2:2
undo shutdown
link-protocol ppp
ppp mp-global global-mp-group 0
#
return
```

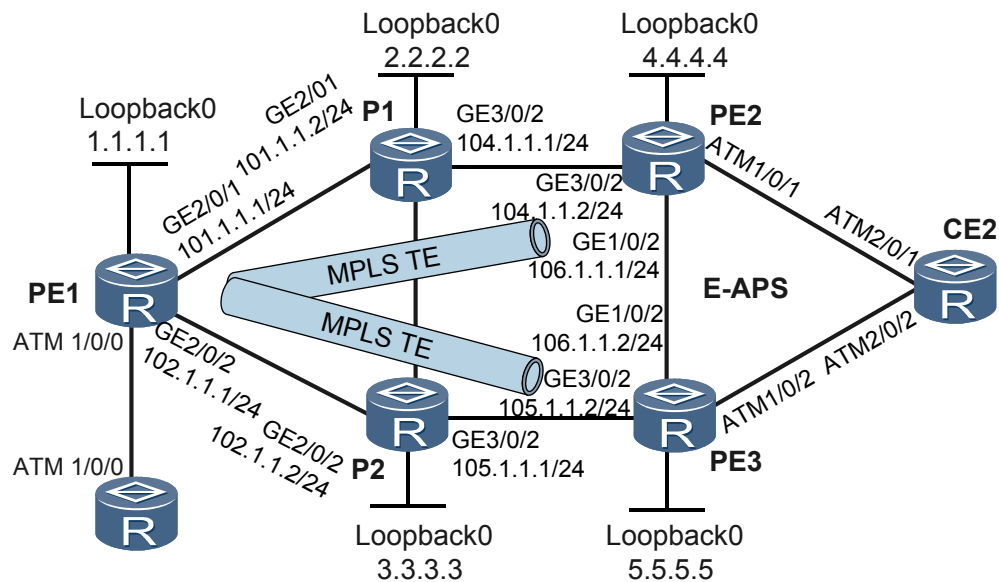
3.4.3 配置 PW Redundancy 与 E-APS 1:1 保护联动示例

介绍一个配置 PW Redundancy 与 E-APS 1:1 保护联动示例，结合配置组网图来理解业务的配置过程。配置示例包括组网需求、思路准备、操作步骤和配置文件。

组网需求

如图 3-4 所示，PE1 通过两条 PW 双归接入到 PE2 和 PE3，PW 由 MPLS TE 承载。AC 侧故障倒换通过 E-APS 进行，AC 侧倒换时会联动 PW 进行倒换，保证了 AC 侧故障发生时不造成网络数据丢失。

图 3-4 配置 PW Redundancy 与 APS 联动组网图



配置思路

采用如下的思路配置：

1. 配置 IP 地址和路由协议实现互通。
2. 配置 MPLS TE，建立隧道，并配置隧道的显式路径，保证流量按照指定路径进行转发。
3. 在 PE2 和 PE3 上配置 E-APS，在 CE2 上配置单机 APS。
4. PE1 上配置主备 PW 双归接入 PE2 和 PE3，PE2 和 PE3 上分别配置普通 PW 和 bypass PW。
5. 配置 BFD 会话检测 PW 链路。

数据准备

为完成此配置例，需准备如下的数据：

- 设备各接口的 IP 地址。
- 配置 MPLS TE 所需的参数以及隧道的显式路径、隧道策略等。
- 配置 E-APS 所需的参数。
- 配置 PW 所需的参数。
- 配置 BFD 会话检测 PW 链路的参数。

操作步骤

步骤 1 配置 IP 地址和 IGP 协议，实现 PE 之间的 IP 连通性

1. 配置各接口的 IP 地址

按图 3-4 所示配置各接口的 IP 地址和掩码，具体配置过程略。

2. 配置 IGP 路由协议，本例使用 IS-IS 协议。

配置 PE1。

```
[PE1] isis 1
[PE1-isis-1] is-level level-1
[PE1-isis-1] network-entity 1111.1111.1111.1111.00
[PE1-isis-1] graceful-restart
[PE1-isis-1] cost-style wide-compatible
[PE1-isis-1] timer spf 1 1 50
[PE1-isis-1] traffic-eng level-1-2
[PE1-isis-1] quit
[PE1] interface gigabitEthernet 2/0/1
[PE1-GigabitEthernet2/0/1] isis enable 1
[PE1-GigabitEthernet2/0/1] quit
[PE1] interface gigabitEthernet 2/0/2
[PE1-GigabitEthernet2/0/2] isis enable 1
[PE1-GigabitEthernet2/0/2] quit
[PE1] interface loopback 0
[PE1-LoopBack0] isis enable 1
[PE1-LoopBack0] quit
```

配置 P1。

```
[P1] isis 1
[P1-isis-1] is-level level-1
[P1-isis-1] network-entity 2222.2222.2222.2222.00
[P1-isis-1] graceful-restart
[P1-isis-1] cost-style wide-compatible
[P1-isis-1] timer spf 1 1 50
[P1-isis-1] traffic-eng level-1-2
[P1-isis-1] quit
[P1] interface gigabitEthernet 2/0/1
[P1-GigabitEthernet2/0/1] isis enable 1
[P1-GigabitEthernet2/0/1] quit
[P1] interface gigabitEthernet 3/0/2
[P1-GigabitEthernet3/0/2] isis enable 1
[P1-GigabitEthernet3/0/2] quit
[P1] interface loopback 0
[P1-LoopBack0] isis enable 1
[P1-LoopBack0] quit
```

配置 P2。

```
[P2] isis 1
[P2-isis-1] is-level level-1
[P2-isis-1] network-entity 3333.3333.3333.3333.00
[P2-isis-1] graceful-restart
[P2-isis-1] cost-style wide-compatible
[P2-isis-1] timer spf 1 1 50
[P2-isis-1] traffic-eng level-1-2
[P2-isis-1] quit
[P2] interface gigabitEthernet 2/0/2
[P2-GigabitEthernet2/0/2] isis enable 1
[P2-GigabitEthernet2/0/2] quit
[P2] interface gigabitEthernet 3/0/2
[P2-GigabitEthernet3/0/2] isis enable 1
[P2-GigabitEthernet3/0/2] quit
[P2] interface loopback 0
[P2-LoopBack0] isis enable 1
[P2-LoopBack0] quit
```

配置 PE2

```
[PE2] isis 1
[PE2-isis-1] is-level level-1
[PE2-isis-1] network-entity 4444.4444.4444.4444.00
[PE2-isis-1] graceful-restart
[PE2-isis-1] cost-style wide-compatible
[PE2-isis-1] timer spf 1 1 50
[PE2-isis-1] traffic-eng level-1-2
[PE2-isis-1] quit
[PE2] interface gigabitEthernet 3/0/2
[PE2-GigabitEthernet3/0/2] isis enable 1
[PE2-GigabitEthernet3/0/2] quit
[PE2] interface gigabitEthernet 1/0/2
[PE2-GigabitEthernet1/0/2] isis enable 1
[PE2-GigabitEthernet1/0/2] quit
[PE2] interface loopback 0
[PE2-LoopBack0] isis enable 1
[PE2-LoopBack0] quit
```

配置 PE3

```
[PE3] isis 1
[PE3-isis-1] is-level level-1
[PE3-isis-1] network-entity 5555.5555.5555.5555.00
[PE3-isis-1] graceful-restart
[PE3-isis-1] cost-style wide-compatible
[PE3-isis-1] timer spf 1 1 50
[PE3-isis-1] traffic-eng level-1-2
[PE3-isis-1] quit
[PE3] interface gigabitEthernet 3/0/2
[PE3-GigabitEthernet3/0/2] isis enable 1
[PE3-GigabitEthernet3/0/2] quit
[PE3] interface gigabitEthernet 1/0/2
[PE3-GigabitEthernet1/0/2] isis enable 1
[PE3-GigabitEthernet1/0/2] quit
[PE3] interface loopback 0
[PE3-LoopBack0] isis enable 1
[PE3-LoopBack0] quit
```

步骤 2 配置 MPLS TE

1. 使能 MPLS TE

配置 PE1。

```
[PE1] interface loopBack 0
[PE1-LoopBack0] ip address 1.1.1.1 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls
[PE1-mpls] mpls te
[PE1-mpls] quit
[PE1] interface gigabitEthernet 2/0/1
[PE1-GigabitEthernet2/0/1] mpls
[PE1-GigabitEthernet2/0/1] mpls te
[PE1-GigabitEthernet2/0/1] quit
[PE1] interface gigabitEthernet 2/0/2
[PE1-GigabitEthernet2/0/2] mpls
[PE1-GigabitEthernet2/0/2] mpls te
[PE1-GigabitEthernet2/0/2] quit
```

配置 P1。

```
[P1] interface loopBack 0
[P1-LoopBack0] ip address 2.2.2.2 32
[P1-LoopBack0] quit
[P1] mpls lsr-id 2.2.2.2
[P1] mpls
[P1-mpls] mpls te
```

```
[P1-mps] quit
[P1] interface gigabitethernet 2/0/1
[P1-GigabitEthernet2/0/1] mpls
[P1-GigabitEthernet2/0/1] mpls te
[P1-GigabitEthernet2/0/1] quit
[P1] interface gigabitethernet 3/0/2
[P1-GigabitEthernet3/0/2] mpls
[P1-GigabitEthernet3/0/2] mpls te
[P1-GigabitEthernet3/0/2] quit
```

配置 P2。

```
[P2] interface loopBack 0
[P2-LoopBack0] ip address 3.3.3.3 32
[P2-LoopBack0] quit
[P2] mpls lsr-id 3.3.3.3
[P2] mpls
[P2-mps] mpls te
[P2-mps] quit
[P2] interface gigabitethernet 2/0/2
[P2-GigabitEthernet2/0/2] mpls
[P2-GigabitEthernet2/0/2] mpls te
[P2-GigabitEthernet2/0/2] quit
[P2] interface gigabitethernet 3/0/2
[P2-GigabitEthernet3/0/2] mpls
[P2-GigabitEthernet3/0/2] mpls te
[P2-GigabitEthernet3/0/2] quit
```

配置 PE2

```
[PE2] interface loopBack 0
[PE2-LoopBack0] ip address 4.4.4.4 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 4.4.4.4
[PE2] mpls
[PE2-mps] mpls te
[PE2-mps] quit
[PE2] interface gigabitethernet 3/0/2
[PE2-GigabitEthernet3/0/2] mpls
[PE2-GigabitEthernet3/0/2] mpls te
[PE2-GigabitEthernet3/0/2] quit
```

配置 PE3

```
[PE3] interface loopBack 0
[PE3-LoopBack0] ip address 5.5.5.5 32
[PE3-LoopBack0] quit
[PE3] mpls lsr-id 5.5.5.5
[PE3] mpls
[PE3-mps] mpls te
[PE3-mps] quit
[PE3] interface gigabitethernet 3/0/2
[PE3-GigabitEthernet3/0/2] mpls
[PE3-GigabitEthernet3/0/2] mpls te
[PE3-GigabitEthernet3/0/2] quit
```

2. 配置隧道的显式路径

配置 PE1

```
[PE1] explicit-path path1
[PE1-explicit-path-path1] next hop 101.1.1.2
[PE1-explicit-path-path1] next hop 104.1.1.2
[PE1-explicit-path-path1] next hop 4.4.4.4
[PE1] explicit-path path2
[PE1-explicit-path-path2] next hop 102.1.1.2
[PE1-explicit-path-path2] next hop 105.1.1.2
[PE1-explicit-path-path2] next hop 5.5.5.5
```

配置 PE2


```
[PE2] explicit-path path
[PE2-explicit-path-path] next hop 104.1.1.1
[PE2-explicit-path-path] next hop 101.1.1.1
[PE2-explicit-path-path] next hop 1.1.1.1
```

配置 PE3

```
[PE3] explicit-path path
[PE3-explicit-path-path] next hop 105.1.1.1
[PE3-explicit-path-path] next hop 102.1.1.1
[PE3-explicit-path-path] next hop 1.1.1.1
```

3. 建立 TE 隧道

配置 PE1

```
[PE1] interface tunnel 1/0/0
[PE1-Tunnel1/0/0] ip address unnumbered interface LoopBack0
[PE1-Tunnel1/0/0] tunnel-protocol mpls te
[PE1-Tunnel1/0/0] destination 4.4.4.4
[PE1-Tunnel1/0/0] mpls te tunnel-id 1
[PE1-Tunnel1/0/0] mpls te path explicit-path path1
[PE1-Tunnel1/0/0] mpls te reserved-for-binding
[PE1-Tunnel1/0/0] mpls te commit
[PE1-Tunnel1/0/0] quit
[PE1] interface tunnel 2/0/0
[PE1-Tunnel2/0/0] ip address unnumbered interface LoopBack0
[PE1-Tunnel2/0/0] tunnel-protocol mpls te
[PE1-Tunnel2/0/0] destination 5.5.5.5
[PE1-Tunnel2/0/0] mpls te tunnel-id 2
[PE1-Tunnel2/0/0] mpls te path explicit-path path2
[PE1-Tunnel2/0/0] mpls te reserved-for-binding
[PE1-Tunnel2/0/0] mpls te commit
[PE1-Tunnel2/0/0] quit
[PE1] tunnel-policy ct1
[PE1-tunnel-policy-ct1] tunnel select-seq cr-lsp load-balance-number 1
[PE1-tunnel-policy-ct1] quit
[PE1] tunnel-policy ct2
[PE1-tunnel-policy-ct2] tunnel select-seq cr-lsp load-balance-number 1
[PE1-tunnel-policy-ct2] quit
```

配置 PE2

```
[PE2] interface tunnel 1/0/0
[PE2-Tunnel1/0/0] ip address unnumbered interface LoopBack0
[PE2-Tunnel1/0/0] tunnel-protocol mpls te
[PE2-Tunnel1/0/0] destination 1.1.1.1
[PE2-Tunnel1/0/0] mpls te tunnel-id 1
[PE2-Tunnel1/0/0] mpls te path explicit-path path
[PE2-Tunnel1/0/0] mpls te reserved-for-binding
[PE2-Tunnel1/0/0] mpls te commit
[PE2-Tunnel1/0/0] quit
[PE2] tunnel-policy ct
[PE2-tunnel-policy-ct] tunnel select-seq cr-lsp load-balance-number 1
[PE2-tunnel-policy-ct] quit
```

配置 PE3

```
[PE3] interface tunnel 1/0/0
[PE3-Tunnel1/0/0] ip address unnumbered interface LoopBack0
[PE3-Tunnel1/0/0] tunnel-protocol mpls te
[PE3-Tunnel1/0/0] destination 1.1.1.1
[PE3-Tunnel1/0/0] mpls te tunnel-id 2
[PE3-Tunnel1/0/0] mpls te path explicit-path path
[PE3-Tunnel1/0/0] mpls te reserved-for-binding
[PE3-Tunnel1/0/0] mpls te commit
[PE3-Tunnel1/0/0] quit
[PE3] tunnel-policy ct
[PE3-tunnel-policy-ct] tunnel select-seq cr-lsp load-balance-number 1
[PE3-tunnel-policy-ct] quit
```

步骤 3 配置 E-APS

1. 在 PE2、PE3 和 CE2 上配置 APS 功能。

配置 PE2

```
[PE2] interface atm 1/0/1
[PE2-Atm1/0/1] undo shutdown
[PE2-Atm1/0/1] aps group 1
[PE2-Atm1/0/1] aps working 5.5.5.5 4.4.4.4
[PE2-Atm1/0/1] aps timers 1 180
[PE2-Atm1/0/1] quit
```

配置 PE3

```
[PE3] interface atm 1/0/2
[PE3-Atm1/0/2] undo shutdown
[PE3-Atm1/0/2] aps group 1
[PE3-Atm1/0/2] aps protect 4.4.4.4 5.5.5.5
[PE3-Atm1/0/2] aps mode one2one bidirection
[PE3-Atm1/0/2] aps revert 5
[PE3-Atm1/0/2] aps timers 1 180
[PE3-Atm1/0/2] quit
```

配置 CE2

```
<HUAWEI> system-view
[HUAWEI] sysname CE2
[CE2] interface atm 2/0/1
[CE2-Atm2/0/1] aps group 1
[CE2-Atm2/0/1] aps working
[CE2-Atm2/0/1] quit
[CE2] interface atm 2/0/2
[CE2-Atm2/0/2] aps group 1
[CE2-Atm2/0/2] aps protect
[CE2-Atm2/0/2] aps mode one2one bidirection
[CE2-Atm2/0/2] aps revert 5
[CE2-Atm2/0/2] quit
```

2. 在 PE2、PE3 和 CE2 上创建 Atm-Trunk，并加入成员接口

配置 PE2

```
[PE2] interface atm-trunk 1
[PE2-Atm-Trunk1] quit
[PE2] interface atm 1/0/1
[PE2-Atm1/0/1] atm-trunk 1
```

配置 PE3

```
[PE3] interface atm-trunk 1
[PE3-Atm-Trunk1] quit
[PE3] interface atm 1/0/2
[PE3-Atm1/0/2] atm-trunk 1
```

配置 CE2

```
[CE2] interface atm-trunk 1
[CE2-Atm-Trunk1] quit
[CE2] interface atm 2/0/1
[CE2-Atm2/0/1] atm-trunk 1
[CE2-Atm2/0/1] quit
[CE2] interface atm 2/0/2
[CE2-Atm2/0/2] atm-trunk 1
```

步骤 4 配置 PW

- # 配置 PE1。

```
[PE1] mpls l2vpn
```

```
[PE1-l2vpn] quit
[PE1] pw-template pwt
[PE1-pw-template-pwt] control-word
[PE1-pw-template-pwt] quit
[PE1] interface atm 1/0/0
[PE1-Atm1/0/0] undo shutdown
[PE1-Atm1/0/0] quit
[PE1] interface atm 1/0/0.1 p2p
[PE1-Atm1/0/0.1] atm cell transfer
[PE1-Atm1/0/0.1] pvc 1/100
[PE1-atm-pvc-Atm1/0/0.1-1/100] quit
[PE1-Atm1/0/0.1] mpls l2vc 4.4.4.4 pw-template pwt 1 tunnel-policy ct1
[PE1-Atm1/0/0.1] mpls l2vc 5.5.5.5 pw-template pwt 2 tunnel-policy ct2 secondary
[PE1-Atm1/0/0.1] mpls l2vpn redundancy independent
[PE1-Atm1/0/0.1] mpls l2vpn stream-dual-receiving
[PE1-Atm1/0/0.1] quit
```

配置 PE2。

```
[PE2] mpls l2vpn
[PE2-l2vpn] quit
[PE2] pw-template pwt
[PE2-pw-template-pwt] control-word
[PE2-pw-template-pwt] quit
[PE2] interface atm-trunk 1.1 p2p
[PE2-Atm-Trunk1.1] pvc 1/100
[PE2-atm-pvc-Atm-trunk1.1-1/100] quit
[PE2-Atm-Trunk1.1] mpls l2vc 1.1.1.1 pw-template pwt 1 tunnel-policy ct
[PE2-Atm-Trunk1.1] mpls l2vc 5.5.5.5 3 bypass
[PE2-Atm-Trunk1.1] quit
```

配置 PE3。

```
[PE3] mpls l2vpn
[PE3-l2vpn] quit
[PE3] pw-template pwt
[PE3-pw-template-pwt] control-word
[PE3-pw-template-pwt] quit
[PE3] interface atm-trunk 1.1 p2p
[PE3-Atm-Trunk1.1] pvc 1/100
[PE3-atm-pvc-Atm-trunk1.1-1/100] quit
[PE3-Atm-Trunk1.1] mpls l2vc 1.1.1.1 pw-template pwt 2 tunnel-policy ct
[PE3-Atm-Trunk1.1] mpls l2vc 4.4.4.4 3 bypass
[PE3-Atm-Trunk1.1] quit
```

步骤 5 配置 BFD 会话检测 PW 链路

配置 PE1。

```
[PE1] bfd
[PE1-bfd] quit
[PE1] bfd bfd1 bind pw interface atm 1/0/0 remote-peer 4.4.4.4 pw-ttl auto-calculate
[PE1-bfd-session-bfd1] discriminator local 222
[PE1-bfd-session-bfd1] discriminator remote 111
[PE1-bfd-session-bfd1] quit
[PE1] bfd bfd2 bind pw interface atm 1/0/0 remote-peer 5.5.5.5 pw-ttl auto-calculate
[PE1-bfd-session-bfd2] discriminator local 444
[PE1-bfd-session-bfd2] discriminator remote 333
[PE1-bfd-session-bfd2] quit
```

配置 PE2。

```
[PE2] bfd
[PE2-bfd] quit
[PE2] bfd bfd bind pw interface atm 1/0/1 remote-peer 1.1.1.1 pw-ttl auto-calculate
[PE2-bfd-session-bfd] discriminator local 111
[PE2-bfd-session-bfd] discriminator remote 222
[PE2-bfd-session-bfd] quit
```

配置 PE3。

```
[PE3] bfd
[PE3-bfd] quit
[PE3] bfd bfd bind pw interface atm 1/0/2 remote-peer 1.1.1.1 pw-ttl auto-calculate
[PE3-bfd-session-bfd] discriminator local 333
[PE3-bfd-session-bfd] discriminator remote 444
[PE3-bfd-session-bfd] quit
```

步骤 6 检查配置结果

在 PE2 和 PE3 上执行命令 **display aps group**，查看 E-APS 的配置信息，执行命令 **display atm-trunk** 查看 Atm-trunk 接口的配置信息。

```
[PE2] display aps group 1
APS Group 1: Atm1/0/1 working channel 1(Active)
              APS protection channel is 5.5.5.5

-----
Group Work-Channel Protect-Channel Wtr W-State P-State Switch-Cmd Switch-Result
-----
1      Atm1/0/1      5.5.5.5      NA    ok      ok      NA      idle

[PE3] display aps group 1
APS Group 1: APS working channel is 4.4.4.4
              Atm1/0/2 protection channel 0(Inactive)
              Bidirection, 1:1 mode, Revert time(1 minutes)
              KeepAlive Timer: 1(seconds), Hold Timer: 3(seconds)
              No Request on Both Working and Protection Side

-----
Group Work-Channel Protect-Channel Wtr W-State P-State Switch-Cmd Switch-Result
-----
1      4.4.4.4      Atm1/0/2      1    ok      ok      NA      idle

[PE2] display atm-trunk 1
Interface Atm-Trunk1's state information is:
Operate status: up      Number Of Up Port In Trunk: 1

-----
PortName      Status      Active Status
Atm1/0/1      Up          Active
[PE3] display atm-trunk 1
Interface Atm-Trunk1's state information is:
Operate status: up      Number Of Up Port In Trunk: 1

-----
PortName      Status      Active Status
Atm1/0/2      Up          Inactive
```

----结束

配置文件

● PE1 的配置文件

```
#
sysname PE1
isis 1
 is-level level-1
 network-entity 1111.1111.1111.00
 graceful-restart
 cost-style wide-compatible
 timer spf 1 1 50
 traffic-eng level-1-2
 quit
#
interface gigabitEthernet 2/0/1
 isis enable 1
 mpls
 mpls te
 quit
interface gigabitEthernet 2/0/2
 isis enable 1
 mpls
```

```
mpls te
quit
#
interface loopBack 0
ip address 1.1.1.1 32
quit
mpls lsr-id 1.1.1.1
mpls
mpls te
quit
#
explicit-path path1
next hop 101.1.1.2
next hop 104.1.1.2
next hop 4.4.4.4
quit
explicit-path path2
next hop 102.1.1.2
next hop 105.1.1.2
next hop 5.5.5.5
quit
#
interface tunnel 1/0/0
ip address unnumbered interface LoopBack0
tunnel-protocol mpls te
destination 4.4.4.4
mpls te tunnel-id 1
mpls te path explicit-path path1
mpls te reserved-for-binding
mpls te commit
quit
interface tunnel 2/0/0
ip address unnumbered interface LoopBack0
tunnel-protocol mpls te
destination 5.5.5.5
mpls te tunnel-id 2
mpls te path explicit-path path2
mpls te reserved-for-binding
mpls te commit
quit
tunnel-policy ct1
tunnel select-seq cr-lsp load-balance-number 1
quit
tunnel-policy ct2
tunnel select-seq cr-lsp load-balance-number 1
quit
#
mpls l2vpn
quit
pw-template pwt
control-word
quit
interface atm 1/0/0
undo shutdown
quit
#
interface Atm1/0/0.1
atm cell transfer
pvc 1/100
mpls l2vc 4.4.4.4 pw-template pwt 1 tunnel-policy ct1
mpls l2vc 5.5.5.5 pw-template pwt 2 tunnel-policy ct2 secondary
mpls l2vpn redundancy independent
mpls l2vpn stream-dual-receiving
#
bfd
quit
bfd bfd1 bind pw interface atm 1/0/0 remote-peer 4.4.4.4 pw-ttl auto-calculate
discriminator local 222
discriminator remote 111
```

```
quit
bfd bfd2 bind pw interface atm 1/0/0 remote-peer 5.5.5.5 pw-ttl auto-calculate
discriminator local 444
discriminator remote 333
quit
#
return
```

● P1 的配置文件

```
isis 1
 is-level level-1
 network-entity 2222.2222.2222.00
 graceful-restart
 cost-style wide-compatible
 timer spf 1 1 50
 traffic-eng level-1-2
quit
#
interface gigabitEthernet 2/0/1
 isis enable 1
 mpls
 mpls te
quit
interface gigabitEthernet 3/0/2
 isis enable 1
 mpls
 mpls te
quit
interface loopBack 0
 ip address 2.2.2.2 32
quit
#
mpls lsr-id 2.2.2.2
mpls
 mpls te
quit
#
return
```

● P2 的配置文件

```
isis 1
 is-level level-1
 network-entity 3333.3333.3333.00
 graceful-restart
 cost-style wide-compatible
 timer spf 1 1 50
 traffic-eng level-1-2
quit
#
interface gigabitEthernet 2/0/2
 isis enable 1
 mpls
 mpls te
quit
interface gigabitEthernet 3/0/2
 isis enable 1
 mpls
 mpls te
quit
interface loopBack 0
 ip address 3.3.3.3 32
quit
#
mpls lsr-id 3.3.3.3
mpls
 mpls te
quit
#
return
```

● PE2 的配置文件

```
isis 1
 is-level level-1
 network-entity 4444.4444.4444.4444.00
 graceful-restart
 cost-style wide-compatible
 timer spf 1 1 50
 traffic-eng level-1-2
 quit
#
interface gigabitEthernet 3/0/2
 isis enable 1
 mpls
 mpls te
 quit
interface gigabitEthernet 1/0/2
 isis enable 1
 quit
interface loopBack 0
 ip address 4.4.4.4 32
 quit
#
mpls lsr-id 4.4.4.4
mpls
 mpls te
 quit
#
explicit-path path
 next hop 104.1.1.1
 next hop 101.1.1.1
 next hop 1.1.1.1
#
interface tunnel 1/0/0
 ip address unnumbered interface LoopBack0
 tunnel-protocol mpls te
 destination 1.1.1.1
 mpls te tunnel-id 1
 mpls te path explicit-path path
 mpls te reserved-for-binding
 mpls te commit
 quit
#
tunnel-policy ct
 tunnel select-seq cr-lsp load-balance-number 1
 quit
#
interface atm 1/0/1
 undo shutdown
 aps group 1
 aps working 5.5.5.5 4.4.4.4
 aps timers 1 180
 atm-trunk 1
 quit
#
interface atm-trunk 1
 quit
#
mpls l2vpn
 quit
pw-template pwt
 control-word
 quit
#
interface atm-trunk 1.1 p2p
 pvc 1/100
 quit
 mpls l2vc 1.1.1.1 pw-template pwt 1 tunnel-policy ct
 mpls l2vc 5.5.5.5 3 bypass
 quit
```

```
#
bfd
quit
bfd bfd bind pw interface atm 1/0/1 remote-peer 1.1.1.1 pw-ttl auto-calculate
discriminator local 111
discriminator remote 222
quit
#
return
```

● PE3 的配置文件

```
isis 1
 is-level level-1
 network-entity 5555.5555.5555.5555.00
 graceful-restart
 cost-style wide-compatible
 timer spf 1 1 50
 traffic-eng level-1-2
 quit
#
interface gigabitEthernet 3/0/2
 isis enable 1
 mpls
 mpls te
 quit
interface gigabitEthernet 1/0/2
 isis enable 1
 quit
interface loopBack 0
 ip address 5.5.5.5 32
 quit
#
mpls lsr-id 5.5.5.5
mpls
 mpls te
 quit
#
explicit-path path
 next hop 105.1.1.1
 next hop 102.1.1.1
 next hop 1.1.1.1
#
interface tunnel 1/0/0
 ip address unnumbered interface LoopBack0
 tunnel-protocol mpls te
 destination 1.1.1.1
 mpls te tunnel-id 1
 mpls te path explicit-path path
 mpls te reserved-for-binding
 mpls te commit
 quit
#
tunnel-policy ct
 tunnel select-seq cr-lsp load-balance-number 1
 quit
#
interface atm 1/0/2
 undo shutdown
 aps group 1
 aps aps protect 4.4.4.4 5.5.5.5
 aps mode one2one bidirection
 aps revert 5
 aps timers 1 180
 atm-trunk 1
 quit
#
interface atm-trunk 1
 quit
#
mpls l2vpn
```



```
quit
pw-template pwt
control-word
quit
#
interface atm-trunk 1.1 p2p
pvc 1/100
quit
mpls l2vc 1.1.1.1 pw-template pwt 1 tunnel-policy ct
mpls l2vc 4.4.4.4 3 bypass
quit
#
bfd
quit
bfd bfd bind pw interface atm 1/0/2 remote-peer 1.1.1.1 pw-ttl auto-calculate
discriminator local 333
discriminator remote 444
quit
#
return
```

4 VRRP 配置

关于本章

通过创建 VRRP 备份组，实现当主用设备出现故障时，由备用设备承担网路流量。

4.1 VRRP 简介

VRRP 是一种容错协议，通过物理设备和逻辑设备的分离，实现在多个出口网关之间选路。

4.2 配置 VRRP 备份组

通过配置主备备份方式或者是负载分担方式的 VRRP 备份组，实现局域网内的主机和外部网络的通信。

4.3 配置 VRRP 监视接口状态

通过配置 VRRP 备份组监视接口状态，实现接口故障时提供的备份功能。

4.4 配置 VRRP 快速切换（普通方式）

通过 VRRP 备份组监视 BFD 会话状态或者是 EFM 会话状态，实现 VRRP 快速切换的功能。

4.5 配置 VRRP 快速切换（使用 BFD Sampling）

通过配置 BFD Sampling 方式的 BFD 检测，解决 NPE 和 PE 之间无法直接建立 Link BFD 会话的问题。

4.6 配置管理 VRRP 忽略接口 Down 事件功能

通过配置管理 VRRP 忽略接口 Down 事件功能，解决 NPE 之间无法建立管理 VRRP 和 Peer BFD 的问题。

4.7 配置 VRRP 在 VLANIF 的应用

通过在 VLANIF 接口上配置 VRRP 备份组，实现 VRRP 的快速切换功能。

4.8 配置 VRRP 安全功能

在有可能受到安全威胁的网络中，可以配置 VRRP 报文的认证方式，从而避免设备受到非法的攻击。

4.9 配置 VRRP 平滑切换功能

通过配置 VRRP 平滑切换功能，解决因主备板倒换而引起的业务流量丢失问题。

4.10 调整优化 VRRP

可以调整 VRRP 备份组的参数来优化 VRRP 备份组的功能。

4.11 配置管理 VRRP 备份组

管理 VRRP 备份组可以绑定其它的业务备份组，并根据绑定关系，决定相关业务备份组的状态。它主要解决城域以太网中的主备双归属问题。

4.12 配置 VRRP 协议版本升级

通过将 VRRP 协议由版本 2 升级到版本 3，实现 VRRP 协议既支持 IPv6 网络也支持 IPv4 网络。

4.13 维护 VRRP

通过维护 VRRP，可以实现清除 VRRP 统计数据和监控 VRRP 的运行状况的目的。

4.14 配置举例

介绍使用 VRRP 提高可靠性的各种示例。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

4.1 VRRP 简介

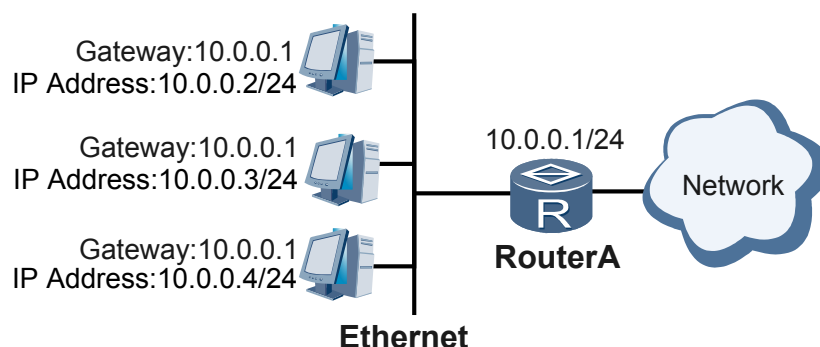
VRRP 是一种容错协议，通过物理设备和逻辑设备的分离，实现在多个出口网关之间选路。

4.1.1 VRRP 概述

VRRP 将一组路由器联合组成一台虚拟路由器，将网络内主机的缺省网关设置为该虚拟路由器的 IP 地址。

通常情况下，网络内部的所有主机都设置一条相同的缺省路由，指向出口网关（即图 4-1 中的路由器 RouterA），实现主机与外部网络的通信。当出口网关发生故障时，主机与外部网络的通信就会中断。

图 4-1 局域网缺省网关



配置多个出口网关是提高系统可靠性的常见方法，但需要解决如何在多个出口网关之间进行选路的问题。

VRRP 是 RFC3768 定义的一种容错协议，通过物理设备和逻辑设备的分离，实现在多个出口网关之间选路，很好地解决了上述问题。

在具有多播或广播能力的局域网（如以太网）中，VRRP 提供逻辑网关确保高利用度的传输链路，不仅能够解决因某网关设备故障带来的业务中断，而且无需修改路由协议的配置。

4.1.2 NE80E/40E 支持的 VRRP 特性

VRRP 包括：主备备份 VRRP、负载分担 VRRP、监视接口状态、VRRP 快速切换、虚拟 IP 地址 Ping 开关、VRRP 的安全功能、VRRP 平滑倒换功能和管理 VRRP。

主备备份 VRRP

这是 VRRP 提供 IP 地址备份功能的基本方式。主备备份方式需要建立一个虚拟路由器，该虚拟路由器包括一个 Master 设备和若干 Backup 设备，这些设备构成一个备份组。Master 设备和 Backup 设备在备份组中拥有不同的优先级，优先级最高的路由器作为 Master 设备。正常情况下，业务全部由 Master 设备承担。Master 设备出现故障时，Backup 设备接替工作。

负载分担 VRRP

负载分担方式是指建立两个或更多备份组，多台路由器同时承担业务。在这种模式下，VRRP 备份组的特性如下：

- NE80E/40E 中允许一台路由器加入多个备份组，在不同备份组中有不同的优先级。通过多虚拟路由器设置可以实现负载分担。
- 每个备份组都包括一个 Master 设备和若干 Backup 设备。
- 各备份组的 Master 可以不同。

监视接口状态

NE80E/40E 支持监控接口的状态，当接口状态变化时，路由器的优先级自动调整，从而使备份组中各路由器优选级高低顺序发生变化，VRRP 重新确定 Master 设备。

VRRP 快速切换

- NE80E/40E 实现双向转发检测 BFD（Bidirectional Forwarding Detection）机制，能够快速检测、监控网络中链路或者 IP 路由的连通状况，VRRP 通过监视 BFD 会话状态实现主备快速切换，最多可以配置 8 个 BFD Session，实现毫秒级别的主备切换。结合使用 BFD 会话的检测结果，可以加快 VRRP 主备倒换的速度。

VRRP 支持监视以下类型的 BFD Session

- 普通类型的 BFD Session
- Peer 类型的 BFD Session
- Link 类型的 BFD Session

VRRP 监视这三种类型的 BFD，功能有相同点，也有不同点。

- 相同点：
 - 三者都可实现链路或设备故障的检测。
 - VRRP 备份组都可通过 track BFD 会话来实现状态的毫秒级快速切换。
- 不同点：
 - VRRP 监视普通 BFD Session 功能是通过修改 VRRP 备份组的优先级来间接影响备份组状态的，它与监视接口状态的作用相同，只是速度更快。当被监视 BFD session 状态恢复时，路由器在备份组中的优先级将恢复原来的值。在 Backup 设备上配置 BFD 会话，BFD 会话要和 VRRP 备份组在同一接口。
 - VRRP 监视 Peer BFD 和 Link BFD 功能则不修改备份组优先级，而是直接影响备份组的状态。
 - Peer BFD 可以同时检测 NPE 近端和远端链路或设备故障，但它不能区分近端或远端故障；Link BFD 只能检测近端链路或设备故障。
- VRRP 可以监视 EFM。在城域以太网解决方案中，主备 NPE 之间和 NPE-UPE 之间都是通过 BFD 来实现链路检测和保护。但是如果 UPE 设备不支持 BFD，就无法使用 BFD 来保护链路。EFM 是慢检测协议，实现要求低，如果此时 UPE 支持 EFM，则 NPE-UPE 之间也可以使用 EFM 来替代。

使用 BFD Sampling 方式的 VRRP 快速切换

VRRP 通过监视 BFD 会话状态可以实现主备快速切换，但是有些特殊的网络组网环境，以及网络设备是否支持 BFD 功能等等，这些都限制了 VRRP 快速切换功能的实现。此时，可以使用 BFD Sampling 方式的 VRRP 快速切换。



说明

NPE 不再与 PE 之间建立 Link BFD 会话，而是直接与每个用户设备 CE 建立多个 Link BFD 会话，这种 BFD 检测方式称为 BFD Sampling。

管理 VRRP 忽略接口 Down 事件

根据 VRRP 协议中的规定，VRRP 有三种状态机：初始状态（Initialize）、活动状态（Master）、备份状态（Backup）。其中当 VRRP 收到接口 shutdown 的消息后，其状态会迁移到 Initialize 状态。

管理 VRRP 备份组配置在两台直连的设备上，VRRP 的心跳报文在两台直连设备得直连链路上传输。当其中一台设备出现故障时，对端设备的接口状态会变为 Down，管理 VRRP 备份组的状态会变为 Initialize，因此对端设备也就无法正常工作，为防止这种情况发生，使用管理 VRRP 忽略接口 Down 事件功能来实现 VRRP 快速切换，使得接口上 VRRP 的状态直接切换到 Master 状态，而不是 Initialize 状态。

虚拟 IP 地址 Ping 开关

VRRP 备份组使用虚拟 IP 地址，能够 Ping 通虚拟 IP 地址可以比较方便的监控虚拟路由器的工作情况，但是可能遭到 ICMP 攻击的隐患。在 NE80E/40E 中，提供了控制 Ping 通虚拟 IP 地址的开关命令，用户可以选择是否打开。

VRRP 的安全功能

对于安全程度不同的网络环境，可以在 VRRP 报头上设定不同的认证方式和认证字。

在一个安全的网络中，可以采用缺省设置：路由器对要发送的 VRRP 报文不进行任何认证处理，收到 VRRP 报文的路由器也不进行任何认证，认为收到的都是真实的、合法的 VRRP 报文。这种情况下，不需要设置认证字。

在有可能受到安全威胁的网络中，VRRP 提供了简单字符（Simple）认证方式和 MD5 认证方式。对于简单认证字方式，可以设置长度为 1～8 的认证字；对于 MD5 认证方式，明文长度范围是 1～8，密文长度为 24。

VRRP 平滑切换功能

配置 VRRP 平滑切换功能之前，在配置了 VRRP 备份组的网络中，在 Master 设备主备倒换期间，由于 Master 设备和 Backup 设备之间不能及时通信，在原 Master 设备发生主备倒换时，Backup 设备切换成 Master 设备。当原 Master 设备主备倒换完成后，如果其优先级高于原 Backup 设备，则它又会抢占成为 Master 设备。由于倒换过程中报文处理较为繁忙，Master 设备发送的免费 ARP 表项报文被阻塞或者处理异常，则必须等待后续报文刷新下游交换机 MAC 表项，在此期间将导致用户报文丢失。

配置 VRRP 平滑切换功能后，原 Master 设备发生主备倒换，则新的主备启动后，如果当前配置的优先级高于原 Backup 设备的优先级，则它会抢占成为 Master 设备。此时，将会保存当前配置的 VRRP 通告报文时间间隔，并对 Master 状态的 VRRP 通告报文时间间隔调整，然后以当前配置的平滑切换时间间隔发出 VRRP 通告报文。Backup 设备收到该报文后，将学习这个新的时间间隔。这样可以确保在 Master 设备主备倒换期间以及主备倒换完成后数据平滑期间 VRRP 备份组状态稳定，避免用户报文丢失。

使能了平滑切换功能后，学习功能优先于抢占功能，即如果收到的协议报文时间间隔和自己当前的不一致，并且报文中携带的优先级低于自己当前的配置优先级，这种情况 VRRP 首先考虑的是学习功能和重置定时器，而后才会考虑是否抢占。

VRRP 整机平滑倒换功能还依赖于系统本身，如果设备自身从主备倒换一开始系统便非常繁忙，无法调度 VRRP 模块运行的情况，VRRP 整机平滑倒换功能无效。

管理 VRRP

为了满足不同的业务需要，路由器之间可以运行多个 VRRP 备份组。如果每个 VRRP 备份组都需要维护自己的状态机，这样路由器之间就会存在大量的 VRRP 协议报文。为了简化协议操作，减少协议报文对带宽的占用，可以将其中一个 VRRP 备份组配置为管理备份组，其余成员备份组与管理备份组绑定，从而成员备份组的状态和管理备份组的状态保持一致。



说明

关于管理 VRRP 的具体配置，请参考《HUAWEI NetEngine80E/40E 路由器 配置指南-VPN》中的“VPLS 汇聚配置”。

VRRP6

VRRP6 是 VRRP for IPv6 的简称。它是一种容错协议，是对 VRRP 协议的扩展。它通过把几台路由设备联合组成一台虚拟的路由设备，并通过一定的机制保证当主机的下一跳设备出现故障时，及时将业务切换到其它设备，从而保持通讯的连续性和可靠性。

可以根据 VRRP6 和 VRRP for IPv4 所支持的功能，来查看它们的异同点。

VRRP6/VRRP for IPv4 支持的功能	VRRP6	VRRP for IPv4
主备备份 VRRP	是	是
负载分担 VRRP	是	是
监视接口状态	是	是
VRRP 快速切换	是	是
虚拟 IP 地址 Ping 开关	是	是
VRRP 的安全认证功能	否	是
VRRP 平滑倒换	否	是
管理 VRRP	是	是

4.2 配置 VRRP 备份组

通过配置主备备份方式或者是负载分担方式的 VRRP 备份组，实现局域网内的主机和外部网络的通信。

4.2.1 建立配置任务

在配置 VRRP 备份组功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

VRRP 备份组分主备备份方式和负载分担方式。

- 主备备份是 VRRP 提供的基本功能，其工作方式如下：
 - 仅有一个备份组。
 - 备份组内优先级最高的一台路由器作为 Master 设备，承担业务。
 - 除了 Master，其它路由器是备份组内的 Backup 设备，处于就绪监听状态。
 - 如果 Master 设备发生故障，Backup 设备将根据优先级选出一个新的 Master 设备提供路由服务。
- 负载分担是通过建立多个备份组的方式来分担网络流量，一台路由器可以属于多个备份组，其工作方式如下：
 - RouterA 作为备份组 1 的 Master，同时又是备份组 2 的 Backup。
 - RouterB 作为备份组 2 的 Master，同时又是备份组 1 的 Backup。
 - 网络内部分主机使用备份组 1 作网关，部分主机使用备份组 2 作为网关。

这样，既达到相互备份的目的，又可以分担网络流量。



说明

支持 VRRP 功能的接口包括 GigabitEthernet、Ethernet、VE（Virtual Ethernet）、Eth-Trunk、以太网子接口和 VLANIF。

前置任务

在配置 VRRP 备份组之前，需完成以下任务：

- 配置接口的网络层属性，使网络连通

数据准备

配置 VRRP 备份组之前，需要准备以下数据。

序号	数据
1	备份组 ID
2	备份组的虚拟 IP 地址
3	VRRP 备份组中各路由器的优先级

4.2.2 创建备份组并配置虚拟 IP 地址

通过创建备份组，实现局域网内的主机的缺省网关为该备份组的 IP 地址。

背景信息

请在备份组的各路由器上进行以下配置。

根据 VRRP 是基于 IPv4 还是 IPv6，选择执行如下步骤之一：

操作步骤

- 对于 VRRP for IPv4（VRRP）：
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **interface interface-type interface-number**，进入接口视图。
 3. 执行命令 **vrrp vrid virtual-router-id virtual-ip virtual-address**，创建备份组并配置虚拟 IP 地址。



- 各备份组之间的虚拟 IP 地址不能重复。
- 保证同一备份组的两端设备上配置相同的备份组 ID。
- 不同接口之间的备份组 ID 可以重复使用。

当指定第一个虚拟 IP 地址到 VRRP 备份组时，系统会创建这个备份组。以后再指定虚拟 IP 地址到这个备份组时，系统将这个地址添加到备份组的虚拟 IP 地址列表中。

对于网络中具有相同 VRRP 可靠性需求的用户，为了便于管理，并避免用户侧缺省网关地址随 VRRP 配置而改变，可以为同一个备份组配置多个虚拟 IP 地址，不同的虚拟 IP 地址为不同用户群服务，每个备份组最多可配置 16 个虚拟 IP 地址。

对于负载分担方式 VRRP 备份组，需要重复执行该步骤，在接口上配置多个备份组。至少需要在接口上配置两个备份组，各备份组之间以 VRID 区分。各备份组间的虚拟 IP 地址不能重复。



NE80E/40E，每个接口上最多可以配置 255 个备份组。



注意

在设备上同时配置 VRRP 和静态 ARP 时，需要注意：当在 Dot1q 终结子接口、QinQ 终结子接口或者 VLANIF 接口下配置 VRRP 时，不能将与这些接口相关的静态 ARP 表项对应的映射 IP 地址作为 VRRP 的虚拟地址。否则会生成错误的主机路由，影响设备之间的正常转发。

- 对于 VRRP for IPv6（VRRP6）：
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **interface interface-type interface-number**，进入接口视图。
 3. 执行命令 **vrrp6 vrid virtual-router-id virtual-ip virtual-ipv6-address [link-local]**，创建备份组并配置虚拟 IPv6 地址。



- 各备份组之间的虚拟 IP 地址不能重复。
- 保证同一备份组的两端设备上配置相同的备份组 ID。
- 不同接口之间的备份组 ID 可以重复使用。

link-local：指定 VRRP6 的虚拟 IPv6 地址为链路本地地址。链路本地地址前缀是 FE80 的 IPv6 地址，用于同一链路的相邻节点间通信，有效域仅限于本地链路。链路本地地址的报文永远不会被 IPv6 路由器转发。配置 VRRP6 的虚拟 IPv6 地址时，第一个虚拟 IPv6 地址必须是链路本地地址。

当指定第一个虚拟 IPv6 地址到 VRRP 备份组时，系统会创建这个备份组。以后再指定虚拟 IP 地址到这个备份组时，系统将这个地址添加到备份组的虚拟 IPv6 地址列表中。

对于负载分担方式 VRRP6 备份组，需要重复执行该步骤，在接口上配置多个备份组。至少需要在接口上配置两个备份组，各备份组之间以 VRID 区分。各备份组间的虚拟 IPv6 地址不能重复。

在配置 IPv6 VRRP 功能时，若用户需要配置一端为 IP 地址所有者，建议用户先配置 IP 地址所有者端的 VRRP 功能，再配置对端设备的 VRRP 功能，否则可能会出现地址冲突。若出现地址冲突，可以采用如下方式解决：

- 通过关闭 IPV6 地址冲突检查解决。
 - (1) 在配置 IP 地址所有者前，先在接口下配置命令 **ipv6 nd dad attempts value**，参数 *value* 值为 0，关闭 IPv6 的地址冲突检查。
 - (2) 配置 IP 地址所有者。
 - (3) 执行 **ipv6 nd dad attempts value**，参数 *value* 值为 1，打开 IPv6 的地址冲突检查。
- 通过重启接口解决。
 - (1) 在 IP 地址所有者所在接口视图下执行 **shutdown** 命令，关闭接口。
 - (2) 在 IP 地址所有者所在接口视图下执行 **undo shutdown** 命令，重启接口。

----结束

4.2.3 配置接口在备份组中的优先级

通过创建接口在备份组中的优先级，实现主用设备承担网络流量。

背景信息

主备备份方式只有一个备份组，不同路由器在该备份组中拥有不同优先级，优先级最高的成为 Master，其他均为 Backup 状态。

负载分担方式有两个或更多的备份组，VRRP 根据优先级来确定备份组中每台路由器的地位，各路由器在不同备份组中拥有不同的优先级。重复执行该步骤，保证各个 VRRP 备份组的 Master 分布在不同的路由器上。

请在备份组的各路由器接口上进行以下配置。

根据 VRRP 是基于 IPv4 还是 IPv6，选择执行如下步骤之一：

操作步骤

- 对于 VRRP for IPv4:
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **interface interface-type interface-number**，进入接口视图。
 3. 执行命令 **vrrp vrid virtual-router-id priority priority-value**，配置路由器在备份组中的优先级。

缺省情况下，优先级的取值是 100。优先级 0 是系统保留作为特殊用途的，优先级值 255 保留给 IP 地址所有者，IP 地址所有者的优先级不可配置。通过命令可以配置的优先级取值范围是 1 ~ 254。

- 对于 VRRP for IPv6:
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **interface interface-type interface-number**，进入接口视图。
 3. 执行命令 **vrrp6 vrid virtual-router-id priority priority-value**，配置路由器在备份组中的优先级。

缺省情况下，优先级的取值是 100。优先级 0 是系统保留作为特殊用途的，优先级值 255 保留给 IP 地址拥有者，IP 地址拥有者的优先级不可配置。通过命令可以配置的优先级取值范围是 1 ~ 254。

----结束

4.2.4 检查配置结果

通过查看 VRRP 备份组的状态等内容，来检查配置是否成功。

前提条件

已经完成 VRRP 备份组功能的所有配置。

操作步骤

- 使用 **display vrrp [interface interface-type interface-number [virtual-router-id]] [brief]** 命令查看 VRRP 备份组的状态信息。
- 使用 **display vrrp6 [interface interface-type interface-number [vrid virtual-router-id]] [brief]** 命令查看 VRRP6 备份组的状态信息和配置参数。

----结束

任务示例

对于主备备份方式，配置成功后，执行 **display vrrp** 命令，可以看到 VRRP 备份组的状态。

```
<HUAWEI> display vrrp
GigabitEthernet2/0/0 | Virtual Router 1
  State           : Master
  Virtual IP      : 10.1.1.111
  Master IP       : 10.1.1.1
  PriorityRun      : 120
  PriorityConfig   : 120
  MasterPriority   : 120
  Preempt         : YES      Delay Time   : 20
  TimerRun        : 1
  TimerConfig     : 1
  Auth Type       : NONE
  Virtual Mac     : 0000-5e00-0201
  Check TTL       : YES
  Config type     : normal-vrrp
  Config track link-bfd down-number : 0
  Create time     : 2010-06-22 17:32:56
  Last change time : 2010-06-22 17:33:00
```

对于负载分担方式，配置成功后，在路由器上执行 **display vrrp** 命令，可以看到路由器在不同备份组中的状态。

```
<HUAWEI> display vrrp
GigabitEthernet2/0/0 | Virtual Router 1
  State           : Master
  Virtual IP      : 10.1.1.111
```

```
Master IP      : 10.1.1.1
PriorityRun    : 120
PriorityConfig : 120
MasterPriority : 120
Preempt       : YES      Delay Time   : 0
TimerRun      : 1
TimerConfig   : 1
Auth Type     : NONE
Virtual Mac   : 0000-5e00-0201
Check TTL     : YES
Config type   : normal-vrrp
Config track link-bfd down-number : 0
Create time   : 2010-06-21 17:32:56
Last change time : 2010-06-21 17:33:00
GigabitEthernet2/0/0 | Virtual Router 2
State       : Backup
Virtual IP    : 10.1.1.112
Master IP     : 10.1.1.1
PriorityRun   : 100
PriorityConfig : 100
MasterPriority : 120
Preempt      : YES      Delay Time    : 0
TimerRun     : 1
TimerConfig  : 1
Auth Type    : NONE
Virtual Mac   : 0000-5e00-0102
Check TTL    : YES
Config type   : normal-vrrp
Config track link-bfd down-number : 0
Create time   : 2010-06-18 17:32:56
Last change time : 2010-06-18 17:33:00
```

配置成功后，在路由器上执行 **display vrrp6** 命令，查看 VRRP6 备份组的信息。

```
<HUAWEI> display vrrp6
GigabitEthernet1/0/0 | Virtual Router 1
State      : Master
Virtual IP  : FE80::1:2
Master IP   : FE80::218:82FF:FED3:2AF1
PriorityRun : 200
PriorityConfig : 200
MasterPriority : 200
Preempt    : YES      Delay Time : 0
TimerRun   : 100
TimerConfig : 100
Virtual Mac : 0000-5e00-0201
Uncheck hop limit : YES
Accept Mode : ON
Config type : normal-vrrp
Track If    : GigabitEthernet3/0/4   priority reduced : 70
IF State    : UP
Create time : 2010-06-23 17:32:56
Last change time : 2010-06-23 17:33:00
```

4.3 配置 VRRP 监视接口状态

通过配置 VRRP 备份组监视接口状态，实现接口故障时提供的备份功能。

4.3.1 建立配置任务

在配置 VRRP 备份组监视接口状态的功能之前，应了解其应用环境和数据准备，并需要配置 VRRP 备份组等前置任务。

应用环境

VRRP 具备监视接口状态的功能，即不仅在备份组所在的接口出现故障时提供备份功能，而且在路由器的某个其它端口出现故障时也提供备份功能。

监视接口状态的实现方式是：

1. 当被监视的接口 **Down** 时，这个路由器在备份组的优先级自动减低一个数额，致使备份组内其它的路由器的优先级高于这个路由器的优先级。
2. 优先级最高的路由器转变为 **Master**，完成主备切换。

前置任务

在配置 VRRP 监视接口状态之前，需完成以下任务：

- 配置接口的网络层属性，使网络连通
- 配置 VRRP 备份组

数据准备

在配置 VRRP 监视接口状态之前，需要准备以下数据。

序号	数据
1	备份组 ID
2	需要监视的接口和升高或降低的优先级

4.3.2 配置 VRRP 监视接口状态

通过在接口上配置 VRRP 备份组监视接口状态，可以实现 VRRP 主备快速切换的功能。

背景信息

可以在路由器其它接口不可用时进行备份

在欲监视的接口所在的路由器上进行如下配置。

根据 VRRP 是基于 IPv4 还是 IPv6，选择执行如下步骤之一：

操作步骤

- 对于 VRRP for IPv4：
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **interface interface-type interface-number**，进入接口视图。
 3. 执行命令 **vrrp vrid virtual-router-id track interface interface-type interface-number [increased value-increased | reduced value-reduced]**，监视指定接口的状态。
 - 缺省情况下，当被监视的接口变为 Down 时，优先级的数值降低 10。

- **increased value-increased:** 设置当被监视的接口状态变为 Down 时, 优先级增加的数值。取值范围是 1 ~ 255。由于只有 IP 地址拥有者的优先级是 255, 所以, 优先级最高可以达到 254。
- **reduced value-decreased:** 设置当被监视的接口状态变为 Down 时, 优先级降低的数值。取值范围 1 ~ 255。优先级最低可以降至 1。优先级 0 由系统保留为特殊用途, 当 Backup 设备收到的 VRRP 通告报文中的优先级值为 0, 则 Backup 设备会立即上升为 Master 设备。
- 如果 VRRP 同时监视 BFD 会话和监视接口, 则所监视的 BFD 会话和接口的总数最多为 8 个。
 - 如果配置 VRRP 监视 BFD 会话和接口时全部是增加优先级, 则当监视的 BFD 会话或接口全部 Down 时, Backup 端 VRRP 优先级的总和可以超过 Master 端的优先级。
 - 如果配置 VRRP 监视 BFD 会话和接口时不全部是增加优先级, 一个或其中几个 BFD 会话或接口 Down, VRRP 优先级重新增加计算就已经超过对端, 则其他 BFD 会话或接口 Down 时 VRRP 优先级增加就不会产生任何影响。



说明

一台路由器上最多可以配置监视 8 个接口。并且, 当路由器为 IP 地址拥有者时, 不允许对其配置监视接口。目前不能监视的接口有 Loopback、NULL、AUX 和 CPOS 接口。

● 对于 VRRP for IPv6:

1. 执行命令 **system-view**, 进入系统视图。
2. 执行命令 **interface interface-type interface-number**, 进入接口视图。
3. 执行命令 **vrrp6 vrid virtual-router-id track interface interface-type interface-number [increased value-increased | reduced value-reduced]**, 监视指定接口的状态。
 - 缺省情况下, 当被监视的接口变为 Down 时, 优先级的数值降低 10。
 - **increased value-increased:** 设置当被监视的接口状态变为 Down 时, 优先级增加的数值。取值范围是 1 ~ 255。由于只有 IP 地址拥有者的优先级是 255, 所以, 优先级最高可以达到 254。
 - **reduced value-reduced:** 设置当被监视的接口状态变为 Down 时, 优先级降低的数值。取值范围 1 ~ 255。优先级最低可以降至 1。优先级 0 由系统保留为特殊用途, 当 Backup 设备收到的 VRRP 通告报文中的优先级值为 0, 则 Backup 设备会立即上升为 Master 设备。
 - 配置 VRRP6 备份组监视接口状态时, 若被监视接口的地址配置了 IPv4 地址, IPv4 协议状态发生变化时, VRRP6 备份组会重新选举 Master。若 VRRP6 备份组监视的接口配置了 IPv6 地址, 接口的 IPv6 协议状态变化不会影响 VRRP6 备份组的状态。

----结束

4.3.3 检查配置结果

通过查看备份组所监视的接口及状态等内容, 来检查配置是否成功。

前提条件

已经完成 VRRP 监视接口状态功能的所有配置。

操作步骤

- 使用 **display vrrp** [interface interface-type interface-number [virtual-router-id]] [brief] 命令查看 VRRP 备份组的状态信息。
- 使用 **display vrrp6** [interface interface-type interface-number [vrid virtual-router-id]] [brief] 命令查看当前 VRRP6 备份组的状态信息和配置参数。

----结束

任务示例

执行 **display vrrp** 或者 **display vrrp6** 命令可以看到 Track IF 和 IF State 字段的信息，Track IF 显示所监视的接口类型和编号，IF State 显示所监视接口的状态是 UP 还是 DOWN。

```
<HUAWEI> display vrrp
GigabitEthernet2/0/0 | Virtual Router 1
  State           : Master
  Virtual IP      : 10.1.1.111
  Master IP       : 10.1.1.1
  PriorityRun      : 130
  PriorityConfig   : 130
  MasterPriority   : 130
  Preempt         : YES      Delay Time    : 0
  TimerRun        : 1
  TimerConfig     : 1
  Auth Type       : NONE
  Virtual Mac     : 0000-5e00-0201
  Check TTL       : YES
  Config type     : normal-vrrp
  Config track link-bfd down-number : 0
  Track IF        : GigabitEthernet2/0/1    priority reduced   : 10
  IF State        : UP
  Create time     : 2010-06-22 17:32:56
  Last change time : 2010-06-22 17:33:00
<HUAWEI> display vrrp6
GigabitEthernet1/0/0 | Virtual Router 1
  State           : Master
  Virtual IP      : FE80::1:2
  Master IP       : FE80::218:82FF:FED3:2AF1
  PriorityRun      : 200
  PriorityConfig   : 200
  MasterPriority   : 200
  Preempt         : YES      Delay Time    : 0
  TimerRun        : 100
  TimerConfig     : 100
  Virtual Mac     : 0000-5e00-0201
  Uncheck hop limit : YES
  Accept Mode     : ON
  Config type     : normal-vrrp
  Track If        : GigabitEthernet2/0/1    priority reduced   : 70
  IF State        : UP
  Create time     : 2010-06-21 17:32:56
  Last change time : 2010-06-21 17:33:00
```

4.4 配置 VRRP 快速切换（普通方式）

通过 VRRP 备份组监视 BFD 会话状态或者是 EFM 会话状态，实现 VRRP 快速切换的功能。

4.4.1 建立配置任务

在配置 VRRP 快速切换功能(普通方式)之前，应了解其应用环境和数据准备，并需要配置 VRRP 备份组、BFD 会话或者是 EFM OAM 等前置任务。

应用环境

使用 VRRP 监视 BFD 会话或者 EFM OAM 功能，在 BFD 会话或者是 EFM 会话状态改变后通知 VRRP 模块，实现 VRRP 快速切换。

一个 VRRP 备份组可以同时监视 Peer BFD、Link BFD 和 Normal BFD，同时也可以配置监视接口状态。一般情况下，一个 VRRP 备份组只监视一个 Peer BFD 或一个 Link BFD 的状态，但可以监视多个 Normal BFD 或多个接口状态。

同时配置监视多个 BFD 的情况下，各个配置相互独立，彼此没有影响。

VRRP 备份组监视 Normal BFD 时，当 BFD 状态变化时，通过修改备份组优先级改变主备状态，被监视的 BFD 会话状态恢复时，路由器在备份组中的优先级将恢复原来的值。VRRP 备份组监视 Peer BFD 和 Link BFD 时，当 BFD 状态变化时，不修改备份组优先级，直接影响备份组的状态。

说明

- 关于 EFM OAM 的具体信息，请参见《HUAWEI NetEngine80E/40E 路由器 配置指南-可靠性》中的“以太网 OAM 配置”。
- 关于 VRRP 备份组监视 Peer BFD、Link BFD 和 EFM OAM 的具体配置，请参见《HUAWEI NetEngine80E/40E 路由器 配置指南-VPN》中的“VPLS 汇聚配置”。

前置任务

在配置 VRRP 快速切换功能之前，需完成以下任务：

- 配置接口的网络层属性，使网络连通
- 配置 EFM OAM 基本功能
- 配置 VRRP 备份组
- 配置 BFD 会话，包括 Normal BFD 会话、Link BFD 会话或者 Peer BFD 会话

数据准备

在配置 VRRP 快速切换功能之前，需准备以下数据：

序号	数据
1	备份组 ID

4.4.2 监视 BFD 会话状态

使用 VRRP 备份组监视 BFD 会话，在 BFD 会话状态改变后通知 VRRP 备份组，实现 VRRP 备份组的快速切换。

背景信息

请在需要快速切换的 VRRP 设备上进行以下配置。

说明

- 在配置 VRRP 快速切换时，若 VRRP 监视 peer BFD 会话，则必须在两端设备上配置 peer BFD 会话，否则 VRRP 会产生振荡。
- 当一个 VRRP 备份组和管理 VRRP 绑定后，这个 VRRP 备份组就不能再通过监视任何类型的 BFD 的状态来实现快速倒换，此时该 VRRP 备份组的状态与管理 VRRP 保持一致。
- 在配置 VRRP 备份组监视 BFD 会话状态时：
 - 如果选择参数 **session-name** *bfd-configure-name*，只能绑定静态标识符自协商的 BFD 会话类型。
 - 如果选择参数 *session-id*，只能绑定静态的 BFD 会话类型。

根据 VRRP 是基于 IPv4 还是 IPv6，选择执行如下步骤之一：

操作步骤

- 对于 VRRP for IPv4:
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **interface** *interface-type interface-number* [*.subinterface-number*]，进入 VRRP 备份组所在的接口视图。
 3. 执行命令：
 - **vrrp vrid** *virtual-router-id* **track bfd-session** { *bfd-session-id* | **session-name** *bfd-configure-name* } [**increased** *value-increased* | **reduced** *value-reduced*]，监视普通 BFD Session 状态。

increased value-increased：设置当被监视的 BFD session 状态变为 Down 时，优先级增加的数值。取值范围是 1 ~ 255。由于只有 IP 地址拥有者的优先级是 255，所以，优先级最高可以达到 254。

reduced value-reduced：设置当被监视的 BFD session 状态变为 Down 时，优先级降低的数值。取值范围 1 ~ 255。优先级最低可以降至 1。优先级 0 由系统保留为特殊用途，当 Backup 设备收到的 VRRP 通告报文中的优先级值为 0，则 Backup 设备会立即上升为 Master 设备。缺省情况下，当被监视的 BFD session 变为 Down 时，优先级的数值降低 10。

在配置优先级增加值或减少值时，要注意在增加或减少优先级后备份组内 Backup 的优先级高于 Master，从而使 VRRP 状态快速切换。

如果 VRRP 同时监视 BFD 会话和监视接口，则所监视的 BFD 会话和接口的总数各为 8 个。

 - 如果配置 VRRP 监视 BFD 会话和接口时全部是增加优先级，则只有监视的 BFD 会话或接口全部 Down 时，Backup 端 VRRP 优先级的总和可以超过 Master 端的优先级。
 - 如果配置 VRRP 监视 BFD 会话和接口时不全部是增加优先级，一个或其中几个 BFD 会话或接口 Down，VRRP 优先级重新增加计算就已经超过对端，则其他 BFD 会话或接口 Down 时 VRRP 优先级增加就不会产生任何影响。
 - **vrrp vrid** *virtual-router-id* **track bfd-session** { *bfd-session-id* | **session-name** *bfd-configure-name* } [**peer** | **link**]，监视 Link BFD Session 或者 Peer BFD Session 状态。

当 Link BFD 的类型是如下几种时，在配置 VRRP 备份组监视 BFD 会话之前，必须使用 **process-pst** 命令来允许 BFD 会话修改端口状态表。否则管理 VRRP 监视的 Link BFD 会话的状态和 Link BFD 会话本身的状态不一致。

- BFD for 静态 LSP
- BFD for LDP LSP
- BFD for CR-LSP
- BFD for TE

● 对于 VRRP for IPv6:

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface interface-type interface-number[.subinterface-number]**，进入 VRRP 备份组所在的接口视图。
3. 执行命令：

- **vrrp6 vrid virtual-router-id track bfd-session { session-id | session-name bfd-configure-name } [increased value-increased | reduced value-reduced]**，配置 VRRP6 备份组监视普通 BFD 会话状态。

increased value-increased: 当被监视的 BFD 会话状态变为 Down 时，优先级增加的数值。整数形式，取值范围是 1 ~ 255。由于只有 IP 地址拥有者的优先级是 255，所以，优先级最高可以达到 254。

reduced value-reduced: 当被监视的 BFD 会话状态变为 Down 时，优先级降低的数值。整数形式，取值范围是 1 ~ 254。优先级最低可以降至 1。优先级 0 由系统保留为特殊用途，当 Backup 设备收到的 VRRP 通告报文中的优先级值为 0，则 Backup 设备会立即上升为 Master 设备。缺省情况下，优先级的数值降低 10。

 说明

在配置优先级值增加或者减少时，需要注意在增加或者减小优先级后，备份组内 Backup 的优先级高于 Master，从而使 VRRP6 备份组快速切换。

- **vrrp6 vrid virtual-router-id track bfd-session { session-id | session-name bfd-configure-name } [peer | link]**，配置 VRRP6 备份组监视 Link BFD 或者是 Peer BFD 会话的状态。

当 Link BFD 的类型是如下几种时，在配置 VRRP 备份组监视 BFD 会话之前，必须使用 **process-pst** 命令来允许 BFD 会话修改端口状态表。否则管理 VRRP 监视的 Link BFD 会话的状态和 Link BFD 会话本身的状态不一致。

- BFD for 静态 LSP
- BFD for LDP LSP
- BFD for CR-LSP
- BFD for TE

----结束

4.4.3 监视 BFD 会话状态

使用 VRRP 备份组监视 BFD 会话，在 BFD 会话状态改变后通知 VRRP 备份组，实现 VRRP 备份组的快速切换。

背景信息

请在需要快速切换的 VRRP 设备上进行以下配置。

 说明

- 在配置 VRRP 快速切换时，若 VRRP 监视 peer BFD 会话，则必须在两端设备上配置 peer BFD 会话，否则 VRRP 会产生振荡。
- 当一个 VRRP 备份组和管理 VRRP 绑定后，这个 VRRP 备份组就不能再通过监视任何类型的 BFD 的状态来实现快速倒换，此时该 VRRP 备份组的状态与管理 VRRP 保持一致。
- 在配置 VRRP 备份组监视 BFD 会话状态时：
 - 如果选择参数 **session-name bfd-configure-name**，只能绑定静态标识符自协商的 BFD 会话类型。
 - 如果选择参数 **session-id**，只能绑定静态的 BFD 会话类型。

根据 VRRP 是基于 IPv4 还是 IPv6，选择执行如下步骤之一：

操作步骤

- 对于 VRRP for IPv4：
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **interface interface-type interface-number[.subinterface-number]**，进入 VRRP 备份组所在的接口视图。
 3. 执行命令：
 - **vrrp vrid virtual-router-id track bfd-session { bfd-session-id | session-name bfd-configure-name } [increased value-increased | reduced value-reduced]**，监视普通 BFD Session 状态。

increased value-increased：设置当被监视的 BFD session 状态变为 Down 时，优先级增加的数值。取值范围是 1 ~ 255。由于只有 IP 地址拥有者的优先级是 255，所以，优先级最高可以达到 254。

reduced value-reduced：设置当被监视的 BFD session 状态变为 Down 时，优先级降低的数值。取值范围 1 ~ 255。优先级最低可以降至 1。优先级 0 由系统保留为特殊用途，当 Backup 设备收到的 VRRP 通告报文中的优先级值为 0，则 Backup 设备会立即上升为 Master 设备。缺省情况下，当被监视的 BFD session 变为 Down 时，优先级的数值降低 10。

在配置优先级增加值或减少值时，要注意在增加或减少优先级后备份组内 Backup 的优先级高于 Master，从而使 VRRP 状态快速切换。

如果 VRRP 同时监视 BFD 会话和监视接口，则所监视的 BFD 会话和接口的总数各为 8 个。

 - 如果配置 VRRP 监视 BFD 会话和接口时全部是增加优先级，则只有监视的 BFD 会话或接口全部 Down 时，Backup 端 VRRP 优先级的总和可以超过 Master 端的优先级。
 - 如果配置 VRRP 监视 BFD 会话和接口时不全部是增加优先级，一个或其中几个 BFD 会话或接口 Down，VRRP 优先级重新增加计算就已经超过对端，则其他 BFD 会话或接口 Down 时 VRRP 优先级增加就不会产生任何影响。
 - **vrrp vrid virtual-router-id track bfd-session { bfd-session-id | session-name bfd-configure-name } [peer | link]**，监视 Link BFD Session 或者 Peer BFD Session 状态。

当 Link BFD 的类型是如下几种时，在配置 VRRP 备份组监视 BFD 会话之前，必须使用 **process-pst** 命令来允许 BFD 会话修改端口状态表。否则管理 VRRP 监视的 Link BFD 会话的状态和 Link BFD 会话本身的状态不一致。

 - BFD for 静态 LSP

- BFD for LDP LSP
- BFD for CR-LSP
- BFD for TE

● 对于 VRRP for IPv6:

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface interface-type interface-number** [*subinterface-number*]，进入 VRRP 备份组所在的接口视图。
3. 执行命令:

- **vrrp6 vrid virtual-router-id track bfd-session** { *session-id* | **session-name** *bfd-configure-name* } [**increased value-increased** | **reduced value-reduced**]，配置 VRRP6 备份组监视普通 BFD 会话状态。

increased value-increased: 当被监视的 BFD 会话状态变为 Down 时，优先级增加的数值。整数形式，取值范围是 1 ~ 255。由于只有 IP 地址拥有者的优先级是 255，所以，优先级最高可以达到 254。

reduced value-reduced: 当被监视的 BFD 会话状态变为 Down 时，优先级降低的数值。整数形式，取值范围是 1 ~ 254。优先级最低可以降至 1。优先级 0 由系统保留为特殊用途，当 Backup 设备收到的 VRRP 通告报文中的优先级值为 0，则 Backup 设备会立即上升为 Master 设备。缺省情况下，优先级的数值降低 10。



说明

在配置优先级值增加或者减少时，需要注意在增加或者减小优先级后，备份组内 Backup 的优先级高于 Master，从而使 VRRP6 备份组快速切换。

- **vrrp6 vrid virtual-router-id track bfd-session** { *session-id* | **session-name** *bfd-configure-name* } [**peer** | **link**]，配置 VRRP6 备份组监视 Link BFD 或者是 Peer BFD 会话的状态。

当 Link BFD 的类型是如下几种时，在配置 VRRP 备份组监视 BFD 会话之前，必须使用 **process-pst** 命令来允许 BFD 会话修改端口状态表。否则管理 VRRP 监视的 Link BFD 会话的状态和 Link BFD 会话本身的状态不一致。

- BFD for 静态 LSP
- BFD for LDP LSP
- BFD for CR-LSP
- BFD for TE

----结束

4.4.4 监视 SPU-Group 状态

通过监视 SPU-Group 的状态，可以实现 VRRP 根据 SPU-Group 的状态调整优先级，进行主备切换。

背景信息

请在备份组的各路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

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

步骤 3 执行命令 **vrrp vrid virtual-router-id track spu-group spu-group-number reduced value-reduced**，配置 VRRP SPU-Group 状态。

----结束

4.4.5 检查配置结果

通过查看备份组所监视的 BFD 会话状态或者 EFM 会话状态等内容，来检查配置是否成功。

前提条件

已经完成 VRRP 快速切换功能的所有配置。

操作步骤

- 使用 **display vrrp [interface interface-type interface-number [virtual-router-id]]** 命令查看 VRRP 的状态信息。
- 使用 **display vrrp6 [interface interface-type interface-number [vrid virtual-router-id]] [brief]** 命令查看 VRRP6 备份组的状态信息和配置参数。

----结束

任务示例

执行命令 **display vrrp**，可以看到 VRRP 所监视的 BFD 会话状态是 Up。例如：

```
<HUAWEI> display vrrp
GigabitEthernet1/0/0.3 | Virtual Router 1
  State           : Backup
  Virtual IP      : 192.168.1.100
  Master IP       : 192.168.1.1
  PriorityRun      : 120
  PriorityConfig   : 120
  MasterPriority   : 130
  Preempt         : YES      Delay Time : 0
  TimerRun        : 1
  TimerConfig     : 1
  Auth Type       : NONE
  Check TTL       : YES
  Config type     : normal-vrrp
  Config track link-bfd down-number : 0
  Track BFD       : 1 Priority increased : 20
  BFD-session state : Up
  Create time     : 2010-06-22 17:32:56
  Last change time : 2010-06-22 17:33:00

GigabitEthernet1/0/0.2 | Virtual Router 2
  State           : Backup
  Virtual IP      : 192.168.2.254
  Master IP       : 192.168.2.1
  PriorityRun      : 100
  PriorityConfig   : 100
  MasterPriority   : 120
  Preempt         : yes      Delay time : 0
  TimerRun        : 1
  TimerConfig     : 1
  Auth Type       : NONE
  Check TTL       : YES
  Config type     : admin-vrrp
  Config track link-bfd down-number : 0
```

```
Track EFM          : GigabitEthernet2/0/0
EFM state          : up
Track BFD          : 2 type: peer
BFD-session state  : up
Create time        : 2010-06-23 17:32:56
Last change time   : 2010-06-23 17:33:00

GigabitEthernet1/0/0.1 | Virtual Router 1
State                  : Master
Virtual IP             : 192.168.1.254
Master IP              : 192.168.1.2
PriorityRun             : 120
PriorityConfig          : 120
MasterPriority          : 120
Preempt               : yes      Delay time : 0
TimerRun               : 1
TimerConfig            : 1
Auth Type              : NONE
Check TTL              : YES
Config type            : admin-vrrp
Config track link-bfd down-number : 0
Track BFD              : 4      type: link
BFD-session state     : up
Track BFD              : 1 type: peer
BFD-session state     : up
Create time            : 2010-06-24 17:32:56
Last change time       : 2010-06-24 17:33:00
<HUAWEI> display vrrp6
GigabitEthernet1/0/0 | Virtual Router 1
State                  : Master
Virtual IP             : FE80::1:2
Master IP : FE80::218:82FF:FED3:2AF1
PriorityRun             : 200
PriorityConfig          : 200
MasterPriority          : 180
Preempt                : YES      Delay Time : 0
TimerRun               : 100
TimerConfig            : 100
Virtual Mac            : 0000-5e00-0201
Uncheck hop limit      : YES
Accept Mode            : ON
Config type            : normal-vrrp
Track If               : GigabitEthernet3/1/4  priority reduced : 70
IF State               : UP
Track BFD              : 45 type : peer
BFD6-session state    : up
Create time            : 2010-06-25 17:32:56
Last change time       : 2010-06-25 17:33:00
```

4.5 配置 VRRP 快速切换（使用 BFD Sampling）

通过配置 BFD Sampling 方式的 BFD 检测，解决 NPE 和 PE 之间无法直接建立 Link BFD 会话的问题。

4.5.1 建立配置任务

在配置 VRRP 快速切换（使用 BFD Sampling）功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

VRRP 通过监视 BFD 会话状态可以实现主备快速切换，但是有些特殊的网络组网环境，以及网络设备是否支持 BFD 功能等等，这些都限制了 VRRP 快速切换功能的实现。

如图 4-2 所示，CE 通过 VPLS 汇聚网络接入 NPE 的 QinQ 终结子接口。

NPE 上配置管理 VRRP 和业务 VRRP，并通过管理 VRRP 监视 BFD 会话来完成 VRRP 主备快速切换。NPE 之间建立 Peer BFD 会话。但是，限制 VRRP 快速切换功能的原因可能有：

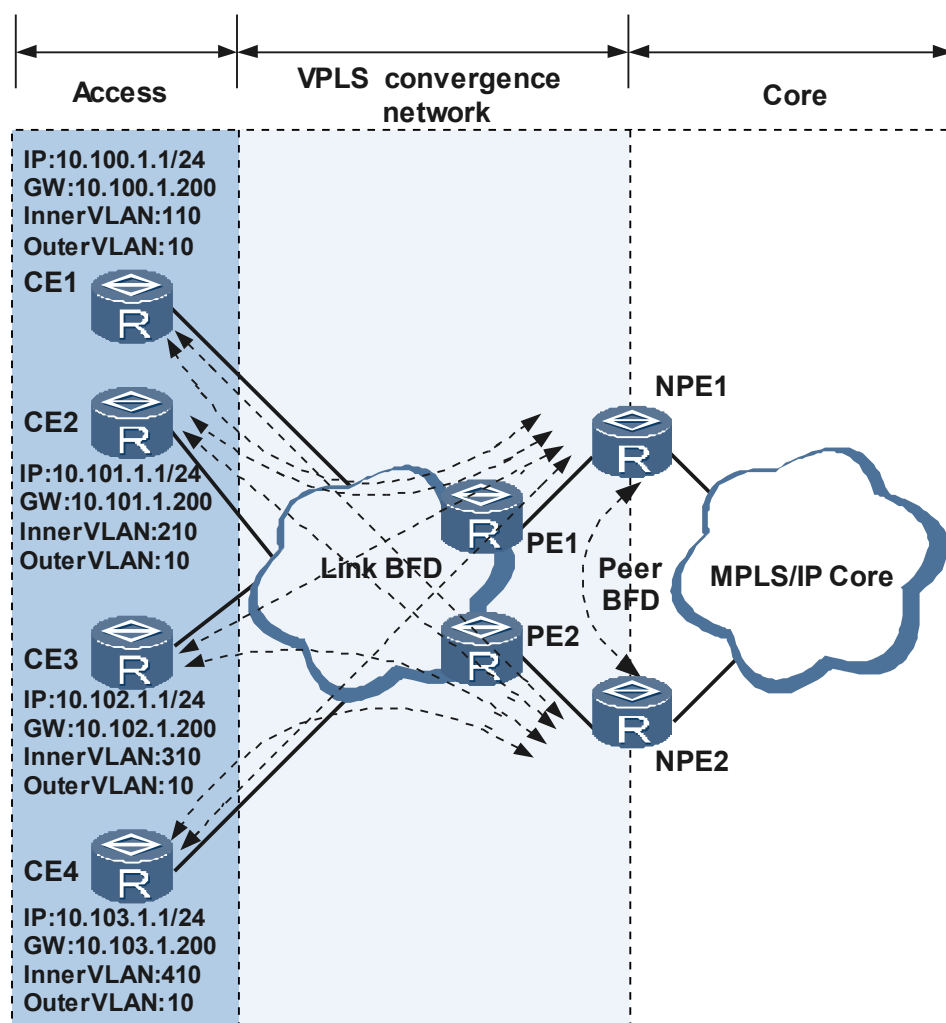
- VPLS 汇聚网络属于其他的运营商，因此 NPE1 与 PE1、NPE2 与 PE2 之间无法直接建立 Link BFD 会话。
- PE1 与 PE2 本身不支持 BFD 功能。

此时可以配置使用 BFD Sampling 方式的 VRRP 快速切换功能。

NPE 不再与 PE 之间建立 Link BFD 会话，而是直接与每个用户设备 CE 建立多个 Link BFD 会话，这种 BFD 检测方式称为 BFD Sampling。

这样，此时虽然 NPE 上 VRRP 不能够通过监视 NPE 与 PE 之间 BFD 会话状态来实现主备快速切换，但是仍可以通过监视 NPE 与 CE 之间的多个 Link BFD 会话状态来实现主备快速切换。

图 4-2 配置 VRRP 快速切换（使用 BFD Sampling）组网图



前置任务

在配置 VRRP 快速切换（使用 BFD Sampling）之前，需完成以下任务：

- 配置接口的网络层属性，使网络连通
- 配置 VRRP 备份组，包括业务 VRRP 与管理 VRRP
- 配置 BFD 会话，包括 Link BFD 会话和 Peer BFD 会话（其中 PE 与每个 CE 之间都要配置 BFD 会话）

数据准备

在配置 VRRP 快速切换（使用 BFD Sampling）之前，需要准备以下数据。

序号	数据
1	VRRP 备份组 ID、虚拟 IP 地址
2	VRRP 备份组中的优先级
3	BFD 会话的本地标识符和远端标识符

4.5.2 配置业务 VRRP 监视管理 VRRP 状态

管理 VRRP 备份组可以决定与其绑定的业务 VRRP 备份组的状态。

背景信息

请在需要快速切换的 VRRP 设备上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **interface interface-type interface-number[.subinterface-number]**，进入业务 VRRP 备份组所在的接口视图。
- 步骤 3** 执行命令 **vrrp vrid virtual-router-id1 track admin-vrrp interface interface-type interface-number vrid virtual-router-id2**，将业务 VRRP 备份组与管理 VRRP 备份组绑定。

业务 VRRP 备份组与管理 VRRP 备份组绑定之后，业务 VRRP 状态机就丧失了独立性，即会删除协议定时器、不再收发协议报文，通过直接拷贝管理 VRRP 备份组的状态来实现自己的状态机。一个业务 VRRP 备份组只能绑定到一个管理 VRRP 备份组。

 说明

一个接口上仅能配置一个业务 VRRP。

----结束

4.5.3 配置管理 VRRP 监视 BFD 会话状态

背景信息

请在需要快速切换的 VRRP 设备上进行以下配置。



说明

- 在配置 VRRP 快速切换时，若 VRRP 监视 peer BFD 会话，则必须在两端设备上配置 peer BFD 会话，否则 VRRP 会产生振荡。
- 当一个 VRRP 备份组和管理 VRRP 绑定后，这个 VRRP 备份组就不能再通过监视任何类型的 BFD 的状态来实现快速倒换，此时该 VRRP 备份组的状态与管理 VRRP 保持一致。
- 在配置 VRRP 备份组监视 BFD 会话状态时：
 - 如果选择参数 **session-name bfd-configure-name**，只能绑定静态标识符自协商的 BFD 会话类型。
 - 如果选择参数 **session-id**，只能绑定静态的 BFD 会话类型。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface interface-type interface-number[.subinterface-number]**，进入 VRRP 备份组所在的接口视图。

步骤 3 根据 BFD 类型的不同，可以使用不同的命令监视不同类型的 BFD 会话：

- **vrrp vrid virtual-router-id track bfd-session { bfd-session-id | session-name bfd-configure-name } [increased value-increased | reduced value-reduced]**，监视普通 BFD Session 状态。

increased value-increased: 设置当被监视的 BFD session 状态变为 Down 时，优先级增加的数值。取值范围是 1 ~ 255。优先级最高可以达到 254。只有 VRRP 备份组的状态为 Backup 时，该参数才生效。

reduced value-reduced: 设置当被监视的 BFD session 状态变为 Down 时，优先级降低的数值。取值范围 1 ~ 255。优先级最低可以降至 1。缺省情况下，当被监视的 BFD session 变为 Down 时，优先级的数值降低 10。

在配置优先级增加值或减少值时，要注意在增加或减少优先级后备份组内 Backup 的优先级高于 Master，从而使 VRRP 状态快速切换，这一点在使用缺省值时尤其要注意。

如果 VRRP 同时监视 BFD 会话和监视接口，所监视的 BFD 会话和接口的总数最多为 8 个。如果配置监视 BFD 会话和监视接口时全部是增加优先级，只有监视的 BFD 会话或接口全部 Down 时，VRRP 的优先级增加的总和可以超过 Master 端的优先级。如果一个或其中几个 BFD 会话或接口 Down，VRRP 优先级重新增加计算就已经超过对端，则其他 BFD 会话或接口 Down 时 VRRP 优先级增加就没有意义。

- **vrrp vrid virtual-router-id track bfd-session { bfd-session-id | session-name bfd-configure-name } [peer | link]**，监视 Link BFD Session 或者 Peer BFD Session 状态。

当 link BFD 的类型是如下几种时，必须配置 **process-pst** 命令来允许 BFD 会话修改端口状态表。否则管理 VRRP 监视的 link BFD 会话的状态和 link BFD 会话本身的状态不一致。

- BFD for 静态 LSP
- BFD for LDP LSP
- BFD for CR-LSP
- BFD for TE

对于本场景中，NPE 之间建立 Peer BFD 会话，但是 NPE 和 PE 之间不建立 Link BFD 会话，而是直接与每个用户设备 CE 建立多个 Link BFD 会话。NPE 通过监视这些 Link BFD 会话状态来实现主备快速切换。

----结束

4.5.4 配置管理 VRRP 切换的阈值

VRRP 备份组根据设置的、所监视 Link BFD 会话 Down 的个数，来实现快速切换。

背景信息

请在需要快速切换的 VRRP 设备上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **interface interface-type interface-number[.subinterface-number]**，进入管理 VRRP 备份组所在的接口视图。
- 步骤 3** 执行命令 **vrrp vrid virtual-router-id track link-bfd down-number down-number**，配置管理 VRRP 监视的 Link BFD 会话 Down 的数目。

当管理 VRRP 监视的 Link BFD 会话中，状态为 Down 的会话数目达到或者超过配置值时，管理 VRRP 进行主备快速切换。

----结束

4.5.5 配置管理 VRRP 状态变化和路由的联动功能

通过将 VRRP 状态和路由联动，解决上行流量和下行流量的不一致的问题。

背景信息

请在需要快速切换的 VRRP 设备上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **interface interface-type interface-number[.subinterface-number]**，进入管理 VRRP 备份组所在的接口视图。
- 步骤 3** 执行命令 **vrrp trigger route**，配置管理 VRRP 和路由的联动功能。

目前设备上，一个接口下可以配置多个 VRRP 备份组，可能有多多个不同的 VRRP 状态同时共存。那么在配置 VRRP 状态变化与路由联动的功能后，为了避免发生路由状态混乱，建议在该接口下只配置一个 VRRP 备份组。



说明

配置管理 VRRP 状态变化和路由的联动功能后:

- 对于 QinQ 终结子接口和 VLANIF 接口
 - 当 VRRP 的状态变成 Initialize 状态时, 设备会删除 VRRP 接口对应网段路由以及远端的主机路由。
 - 当 VRRP 的状态变成 Master 状态时, 设备会发布 VRRP 接口对应网段路由以及远端的主机路由。
- 对于其他类型的接口
 - 当 VRRP 的状态变成 Initialize 状态时, 设备会删除 VRRP 接口对应网段路由。
 - 当 VRRP 的状态变成 Master 状态时, 设备会发布 VRRP 接口对应网段路由。

----结束

4.5.6 检查配置结果

通过查看管理 VRRP 备份组所监视的 BFD 会话信息和 VRRP 备份组切换的阈值等内容, 来检查配置是否成功。

前提条件

已经完成 VRRP 快速切换（使用 BFD Sampling）功能的所有配置。

操作步骤

- 使用 **display vrrp [interface interface-type interface-number [virtual-router-id]]** 命令查看 VRRP 的状态信息。

----结束

任务示例

执行 **display vrrp** 命令, 可以看到管理 VRRP 所监视的 BFD 会话的状态是 Up, 此外还能看到管理 VRRP 切换的阈值是 2。

```
[HUAWEI] display vrrp interface gigabitethernet1/0/1.1
GigabitEthernet1/0/1.1 | Virtual Router 10
State                               : Master
Virtual IP                           : 10.1.1.1
Master IP                           : 10.1.1.2
PriorityRun                          : 120
PriorityConfig                       : 120
MasterPriority                       : 120
Preempt                             : YES          Delay Time : 0
TimerRun                            : 1
TimerConfig                         : 1
Auth Type                           : NONE
Virtual Mac                         : 0000-5e00-010a
Check TTL                           : YES
Config type                         : admin-vrrp
Config track link-bfd down-number : 2
Track BFD                           : link1          type: link
BFD-session state                   : UP
Track BFD                           : peer1          type: peer
BFD-session state                   : UP
Track BFD                           : link2          type: link
BFD-session state                   : UP
Track BFD                           : link3 type: link
BFD-session state                   : UP
Track BFD                           : link4 type: link
BFD-session state                   : UP
```

Create time : 2010-06-22 17:32:56
Last change time : 2010-06-22 17:33:00

4.6 配置管理 VRRP 忽略接口 Down 事件功能

通过配置管理 VRRP 忽略接口 Down 事件功能，解决 NPE 之间无法建立管理 VRRP 和 Peer BFD 的问题。

4.6.1 建立配置任务

在配置管理 VRRP 忽略接口 Down 事件功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

根据 VRRP 协议中的规定，VRRP 有三种状态机：初始状态（Initialize）、活动状态（Master）、备份状态（Backup）。其中当 VRRP 收到接口 shutdown 的消息后，其状态会迁移到初始状态。

如图 4-3 所示，CE 通过 VPLS 汇聚网络接入 NPE 的 QinQ 终结子接口。

NPE 上配置管理 VRRP 和业务 VRRP，并通过管理 VRRP 监视 BFD 会话来完成快速切换。NPE 之间建立 Peer BFD 会话。但是，限制 VRRP 快速切换功能的原因可能有：

- VPLS 汇聚网络中仅在 PE1 与 PE3 之间、PE2 与 PE3 之间存在 PW，根据 VPLS 水平分割的原则，NPE1 与 NPE2 之间无法建立管理 VRRP 和 Peer BFD。
- VPLS 汇聚网络属于其他的运营商，因此 NPE1 与 PE1、NPE2 与 PE2 之间无法建立 Link BFD。

此时可以使用管理 VRRP 忽略接口 Down 事件功能来实现 VRRP 快速切换。

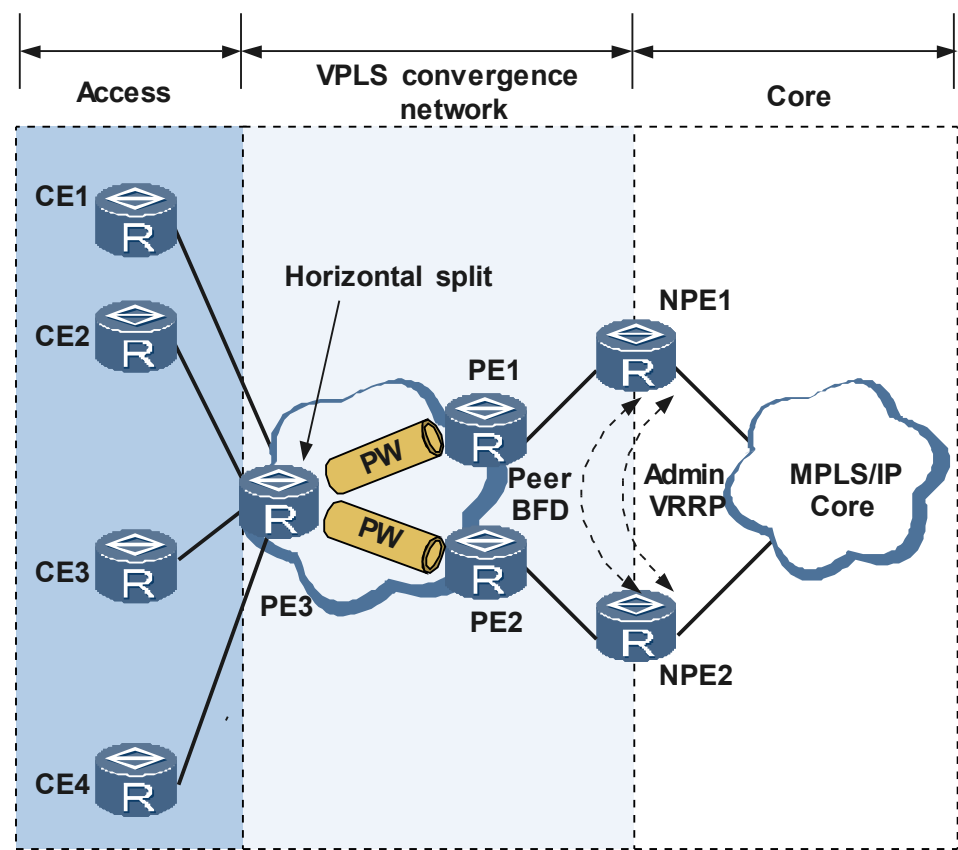
NPE1 和 NPE2 之间通过直连的链路，建立管理 VRRP 和 Peer BFD，而不是通过 VPLS 汇聚网络来建立。

当 VRRP 备份组所在接口变为 Down 状态时，接口上 VRRP 的状态直接切换到 Master 状态，而不是初始状态。

说明

在实际的组网中，由于 NPE1 和 NPE2 无法通过 VPLS 汇聚网络侧的接口建立 Peer BFD 会话和管理 VRRP，而是通过直连链路建立管理 VRRP 和 Peer BFD 会话，因此推荐 NPE 之间使用跨板的 Eth-Trunk 链路，以保证管理 VRRP 和 Peer BFD 会话状态的可靠性。

图 4-3 配置管理 VRRP 忽略接口 Down 事件功能组网图



前置任务

在配置管理 VRRP 忽略接口 Down 事件功能之前，需完成以下任务：

- 配置接口的网络层属性，使网络连通
- 配置 VRRP 备份组，包括业务 VRRP 与管理 VRRP
- 配置 BFD 会话，包括 Link BFD 会话或者 Peer BFD 会话（其中 PE 与每个 CE 之间都要配置 Link BFD 会话）

数据准备

在配置管理 VRRP 忽略接口 Down 事件功能之前，需要准备以下数据。

序号	数据
1	VRRP 备份组 ID、虚拟 IP 地址
2	VRRP 备份组中的优先级
3	BFD 会话的本地标识符和远端标识符

4.6.2 配置管理 VRRP 备份组

配置成员 VRRP 备份组与管理 VRRP 备份组绑定，实现成员 VRRP 备份组和管理 VRRP 备份组状态机的一致性。

背景信息

请在管理 VRRP 备份组所在的设备上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **interface interface-type interface-number[.subinterface-number]**，进入业务 VRRP 备份组所在的接口视图。
- 步骤 3** 执行命令 **vrrp vrid virtual-router-id virtual-ip virtual-address**，创建备份组并配置虚拟 IP 地址。
- 步骤 4** 执行命令 **vrrp vrid virtual-router-id priority priority-value**，配置 VRRP 备份组的优先级。
- 步骤 5** 执行命令 **admin-vrrp vrid virtual-router-id ignore-if-down**，配置该 VRRP 备份组为管理 VRRP 备份组。

对于图 4-3 中所示的场景，在 NPE1 非整机故障的情况下，建议不要在 NPE1 和 NPE2 直连的链路上使用 shutdown 命令，否则 NPE1 和 NPE2 上的管理 VRRP 会同时成为 Master 状态，进而造成业务中断。

除图 4-3 中介绍的场景之外的其他组网环境，不建议使用管理 VRRP 忽略接口 Down 事件功能，否则会造成设备上 VRRP 的协议状态机与 RFC 标准中规定的不一致。

----结束

4.6.3 配置业务 VRRP 监视管理 VRRP 状态

管理 VRRP 备份组可以决定与其绑定的业务 VRRP 备份组的状态。

背景信息

请在需要快速切换的 VRRP 设备上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **interface interface-type interface-number[.subinterface-number]**，进入业务 VRRP 备份组所在的接口视图。
- 步骤 3** 执行命令 **vrrp vrid virtual-router-id1 track admin-vrrp interface interface-type interface-number vrid virtual-router-id2**，将业务 VRRP 备份组与管理 VRRP 备份组绑定。

业务 VRRP 备份组与管理 VRRP 备份组绑定之后，业务 VRRP 状态机就丧失了独立性，即会删除协议定时器、不再收发协议报文，通过直接拷贝管理 VRRP 备份组的状态来实现自己的状态机。一个业务 VRRP 备份组只能绑定到一个管理 VRRP 备份组。



说明

一个接口上仅能配置一个业务 VRRP。

----结束

4.6.4 配置管理 VRRP 监视 BFD 会话状态

背景信息

请在需要快速切换的 VRRP 设备上进行以下配置。



说明

- 在配置 VRRP 快速切换时，若 VRRP 监视 peer BFD 会话，则必须在两端设备上配置 peer BFD 会话，否则 VRRP 会产生振荡。
- 当一个 VRRP 备份组和管理 VRRP 绑定后，这个 VRRP 备份组就不能再通过监视任何类型的 BFD 的状态来实现快速倒换，此时该 VRRP 备份组的状态与管理 VRRP 保持一致。
- 在配置 VRRP 备份组监视 BFD 会话状态时：
 - 如果选择参数 **session-name bfd-configure-name**，只能绑定静态标识符自协商的 BFD 会话类型。
 - 如果选择参数 **session-id**，只能绑定静态的 BFD 会话类型。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface interface-type interface-number[.subinterface-number]**，进入 VRRP 备份组所在的接口视图。

步骤 3 根据 BFD 类型的不同，可以使用不同的命令监视不同类型的 BFD 会话：

- **vrrp vrid virtual-router-id track bfd-session { bfd-session-id | session-name bfd-configure-name } [increased value-increased | reduced value-reduced]**，监视普通 BFD Session 状态。

increased value-increased：设置当被监视的 BFD session 状态变为 Down 时，优先级增加的数值。取值范围是 1 ~ 255。优先级最高可以达到 254。只有 VRRP 备份组的状态为 Backup 时，该参数才生效。

reduced value-reduced：设置当被监视的 BFD session 状态变为 Down 时，优先级降低的数值。取值范围 1 ~ 255。优先级最低可以降至 1。缺省情况下，当被监视的 BFD session 变为 Down 时，优先级的数值降低 10。

在配置优先级增加值或减少值时，要注意在增加或减少优先级后备份组内 Backup 的优先级高于 Master，从而使 VRRP 状态快速切换，这一点在使用缺省值时尤其要注意。

如果 VRRP 同时监视 BFD 会话和监视接口，所监视的 BFD 会话和接口的总数最多为 8 个。如果配置监视 BFD 会话和监视接口时全部是增加优先级，只有监视的 BFD 会话或接口全部 Down 时，VRRP 的优先级增加的总和可以超过 Master 端的优先级。如果一个或其中几个 BFD 会话或接口 Down，VRRP 优先级重新增加计算就已经超过对端，则其他 BFD 会话或接口 Down 时 VRRP 优先级增加就没有意义。

- **vrrp vrid virtual-router-id track bfd-session { bfd-session-id | session-name bfd-configure-name } [peer | link]**，监视 Link BFD Session 或者 Peer BFD Session 状态。

当 link BFD 的类型是如下几种时，必须配置 **process-pst** 命令来允许 BFD 会话修改端口状态表。否则管理 VRRP 监视的 link BFD 会话的状态和 link BFD 会话本身的状态不一致。

- BFD for 静态 LSP
- BFD for LDP LSP
- BFD for CR-LSP
- BFD for TE

对于本场景中，NPE 之间建立 Peer BFD 会话，但是 NPE 和 PE 之间不建立 Link BFD 会话，而是直接与每个用户设备 CE 建立多个 Link BFD 会话。NPE 通过监视这些 Link BFD 会话状态来实现主备快速切换。

----结束

4.6.5 配置管理 VRRP 切换的阈值

VRRP 备份组根据设置的、所监视 Link BFD 会话 Down 的个数，来实现快速切换。

背景信息

请在需要快速切换的 VRRP 设备上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **interface interface-type interface-number[.subinterface-number]**，进入管理 VRRP 备份组所在的接口视图。
- 步骤 3** 执行命令 **vrrp vrid virtual-router-id track link-bfd down-number down-number**，配置管理 VRRP 监视的 Link BFD 会话 Down 的数目。

当管理 VRRP 监视的 Link BFD 会话中，状态为 Down 的会话数目达到或者超过配置值时，管理 VRRP 进行主备快速切换。

----结束

4.6.6 配置管理 VRRP 状态变化和路由的联动功能

通过将 VRRP 状态和路由联动，解决上行流量和下行流量的不一致的问题。

背景信息

请在需要快速切换的 VRRP 设备上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **interface interface-type interface-number[.subinterface-number]**，进入管理 VRRP 备份组所在的接口视图。
- 步骤 3** 执行命令 **vrrp trigger route**，配置管理 VRRP 和路由的联动功能。

目前设备上，一个接口下可以配置多个 VRRP 备份组，可能有多组不同的 VRRP 状态同时共存。那么在配置 VRRP 状态变化与路由联动的功能后，为了避免发生路由状态混乱，建议在该接口下只配置一个 VRRP 备份组。



说明

配置管理 VRRP 状态变化和路由的联动功能后:

- 对于 QinQ 终结子接口和 VLANIF 接口
 - 当 VRRP 的状态变成 Initialize 状态时, 设备会删除 VRRP 接口对应网段路由以及远端的主机路由。
 - 当 VRRP 的状态变成 Master 状态时, 设备会发布 VRRP 接口对应网段路由以及远端的主机路由。
- 对于其他类型的接口
 - 当 VRRP 的状态变成 Initialize 状态时, 设备会删除 VRRP 接口对应网段路由。
 - 当 VRRP 的状态变成 Master 状态时, 设备会发布 VRRP 接口对应网段路由。

----结束

4.6.7 检查配置结果

通过查看管理 VRRP 备份组所监视的 BFD 会话信息和 VRRP 备份组切换的阈值等内容, 来检查配置是否成功。

前提条件

已经完成 VRRP 快速切换 (使用 BFD Sampling) 功能的所有配置。

操作步骤

- 使用 **display vrrp [interface interface-type interface-number [virtual-router-id]]** 命令查看 VRRP 的状态信息。

----结束

任务示例

执行 **display vrrp** 命令, 可以看到管理 VRRP 所监视的 BFD 会话的状态是 Up, 此外还能看到管理 VRRP 切换的阈值是 2。

```
[HUAWEI] display vrrp interface gigabitethernet1/0/1.1
GigabitEthernet1/0/1.1 | Virtual Router 10
State                               : Master
Virtual IP                          : 10.1.1.1
Master IP                           : 10.1.1.2
PriorityRun                          : 120
PriorityConfig                       : 120
MasterPriority                       : 120
Preempt                             : YES          Delay Time : 0
TimerRun                            : 1
TimerConfig                         : 1
Auth Type                           : NONE
Virtual Mac                         : 0000-5e00-010a
Check TTL                           : YES
Config type                          : admin-vrrp
Config track link-bfd down-number  : 2
Track BFD                           : link1          type: link
BFD-session state                   : UP
Track BFD                           : peer1          type: peer
BFD-session state                   : UP
Track BFD                           : link2          type: link
BFD-session state                   : UP
Track BFD                           : link3 type: link
BFD-session state                   : UP
Track BFD                           : link4 type: link
BFD-session state                   : UP
```

Create time : 2010-06-22 17:32:56
Last change time : 2010-06-22 17:33:00

4.7 配置 VRRP 在 VLANIF 的应用

通过在 VLANIF 接口上配置 VRRP 备份组，实现 VRRP 的快速切换功能。

4.7.1 建立配置任务

在配置 VRRP 在 VLANIF 的应用之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

VLANIF 支持 VRRP 功能。

前置任务

在配置 VRRP 在 VLANIF 的应用之前，需完成以下任务：

- 配置接口物理参数
- 配置接口的链路属性
- 配置 sub-VLAN
- 配置 super-VLAN

数据准备

在配置 VRRP 在 VLANIF 的应用之前，需要准备以下数据。

序号	数据
1	super-VLAN ID
2	sub-VLAN ID
3	备份组 ID
4	备份组的虚拟 IP 地址

4.7.2 配置 VLANIF 上的 VRRP

可以在 VLANIF 接口上创建 VRRP 备份组，实现当主用接口 Down 时，备用 VLANIF 接口承担网络流量。

背景信息

请在运行 VRRP for VLANIF 的设备上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。
- 步骤 3** 执行命令 **vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address*，创建备份组并配置虚拟 IP 地址。
- 步骤 4** 执行命令 **vrrp vrid** *virtual-router-id* **priority** *priority-value*，配置路由器在备份组中的优先级。

----结束

4.7.3 （可选）super-VLAN 中 VRRP 报文发送方式

可以根据需要在 VLANIF 接口上配置 super-VLAN 中的 VRRP 通告报文发送方式。

背景信息

请在配置 super-VLAN 的 VRRP 设备上以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
 - 步骤 2** 执行命令 **interface vlanif** *vlan-id*，进入 VLAN 接口视图。
 - 步骤 3** 执行命令 **vrrp advertise send-mode** { *sub-vlan-id* | **all** }，配置 VRRP 通告报文发送方式。
- 缺省情况下，super-VLAN 不向自己的 sub-VLAN 发送 VRRP 通告报文。

----结束

4.7.4 检查配置结果

通过查看 VRRP 备份组的状态等内容，来检查配置是否成功。

前提条件

已经完成 VRRP 在 VLANIF 的应用功能的所有配置。

操作步骤

- 步骤 1** 使用 **display vrrp** [**interface** *interface-type interface-number* [*virtual-router-id*]]命令查看 VRRP 的状态信息。

----结束

任务示例

配置成功后，使用 **display vrrp interface vlanif** 命令可以看到在 VLANIF 上建立的 VRRP 的状态。

```
<HUAWEI> display vrrp interface vlanif 40
Vlanif40 | Virtual Router 1
State           : Master
```

```
Virtual IP      : 100.1.1.111
Master IP      : 100.1.1.1
PriorityRun     : 120
PriorityConfig  : 120
MasterPriority  : 120
Preempt        : YES          Delay Time : 0
TimerRun       : 1
TimerConfig    : 1
Auth Type      : NONE
Virtual Mac    : 0000-5e00-0101
Check TTL      : YES
Config type    : normal-vrrp
Config track link-bfd down-number : 0
Create time    : 2010-06-22 17:32:56
Last change time : 2010-06-22 17:33:00
```

4.8 配置 VRRP 安全功能

在有可能受到安全威胁的网络中，可以配置 VRRP 报文的认证方式，从而避免设备受到非法的攻击。

4.8.1 建立配置任务

在配置 VRRP 安全功能之前，应了解其应用环境和数据准备，并需要配置 VRRP 备份组等前置任务。

应用环境

在一个安全的网络中，可以采用缺省设置：路由器对要发送的 VRRP 报文不进行任何认证处理，收到 VRRP 报文的路由器也不进行任何认证，认为收到的都是真实的、合法的 VRRP 报文。这种情况下，不需要设置认证字。

在有可能受到安全威胁的网络中，VRRP 提供了简单字符（Simple）认证方式和 MD5 认证方式。对于简单认证字方式，可以设置长度为 1～8 的认证字；对于 MD5 认证方式，明文长度范围是 1～8，密文长度为 24。

简单字符认证方式的工作过程主要包括：

- 发送方路由器将认证字填入到 VRRP 报文中。
- 接收方将收到的 VRRP 报文中的认证字与本地配置的认证字比较。如果相同，认为是真实的、合法的 VRRP 报文；如果不同，则认为是非法报文，丢弃，并向网管发送告警消息（Trap）。

MD5 认证方式的工作过程主要包括：

- 发送方路由器将认证字填入到 VRRP 报文中。
- 接收方将根据本地配置的认证字而形成摘要，将收到的 VRRP 报文中的摘要和形成的摘要进行比较，如果相同，认为是真实的、合法的 VRRP 报文；如果不同，则认为是非法报文，丢弃，并向网管发送告警消息（Trap）。

前置任务

在配置 VRRP 安全功能之前，需完成以下任务：

- 配置接口的网络层属性，使网络连通
- 配置 VRRP 备份组

数据准备

在配置 VRRP 安全功能之前，需要准备以下数据。

序号	数据
1	备份组 ID
2	备份组的虚拟 IP 地址
3	VRRP 报文安全认证字

4.8.2 配置 VRRP 报文认证方式

VRRP 报文有两种认证方式：简单字符认证方式和 MD5 认证方式。

背景信息

请在需要配置 VRRP 报文认证方式的路由器上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **interface interface-type interface-number**，进入接口视图。
- 步骤 3** 执行命令 **vrrp vrid virtual-router-id virtual-ip virtual-address**，创建备份组并配置虚拟 IP 地址。
- 步骤 4** （可选）执行命令 **vrrp vrid virtual-router-id priority priority-value**，配置路由器在备份组中的优先级。
- 步骤 5** 执行命令 **vrrp vrid virtual-router-id authentication-mode { simple key | md5 md5-key }**，配置 VRRP 报文认证方式。

同一 VRRP 备份组的认证方式必须相同，否则 Master 设备和 Backup 设备无法协商成功。

符号[^]#和\$@\$@用来识别变长密码，[^]#作为新密码的前缀和后缀，\$@\$@作为老密码的前缀和后缀，所以不支持以“\$@\$@”或“[^]#”同时作为明文密码的起始和结束字符。

----结束

4.8.3 检查配置结果

通过查看 VRRP 报文的认证方式和认证字等内容，来检查配置是否成功。

前提条件

已经完成 VRRP 安全功能的所有配置。

操作步骤

步骤 1 使用 **display vrrp [interface interface-type interface-number [virtual-router-id]]** 命令查看 VRRP 的状态信息。

----结束

任务示例

配置成功后，使用 **display vrrp** 可以看到报文认证方式。

```
<HUAWEI> display vrrp
GigabitEthernet1/0/0 | Virtual Router 1
  State           : Master
  Virtual IP      : 10.1.1.111
  Master IP       : 10.1.1.1
  PriorityRun      : 120
  PriorityConfig   : 120
  MasterPriority   : 120
  Preempt         : YES           Delay Time : 20
  TimerRun        : 1
  TimerConfig     : 1
  Auth Type       : MD5           Auth key  : >6M*PO438G/Q=^Q`MAF4<1!!
  Virtual Mac     : 0000-5e00-0101
  Check TTL       : YES
  Config type     : normal-vrrp
  Config track link-bfd down-number : 0
  Create time     : 2010-06-22 17:32:56
  Last change time : 2010-06-22 17:33:00
```

在以上显示信息中，可以看到“Auth Type”字段显示为“MD5”，“Auth key”字段显示为“>6M*PO438G/Q=^Q`MAF4<1!!”，即 VRRP 备份组 1 的报文认证方式为 MD5 认证，密文为“>6M\*PO438G/Q=^Q`MAF4<1!!”。

4.9 配置 VRRP 平滑倒换功能

通过配置 VRRP 平滑倒换功能，解决因主备板倒换而引起的业务流量丢失问题。

4.9.1 建立配置任务

在配置 VRRP 平滑倒换功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在配置了 VRRP 备份组的网络中，在 Master 设备主备倒换期间，由于 Master 和 Backup 之间不能及时通信，在原 Master 发生倒换时，Backup 切换成为 Master。当原 Master 倒换完成后，由于其优先级高于原 Backup，它又会抢占成为 Master。

由于倒换过程中系统过于繁忙，Master 端的 Hello 协议报文无法正常发送，而 Backup 端无法及时收到报文，会抢占成为 Master，引起链路切换，导致丢包。

在路由器上启用 VRRP 平滑倒换功能可以优化 VRRP 性能，改善对用户流量的影响。

前置任务

无

数据准备

在配置 VRRP 平滑倒换功能之前，需准备以下数据。

序号	数据
1	平滑倒换期间 Master 设备发送协议报文的时间间隔

4.9.2 配置 VRRP 平滑倒换功能

使能平滑倒换功能后，VRRP 备份组学习功能优先于抢占功能。从而 VRRP 备份组的状态不切换，业务流量不受影响。

背景信息

请在 VRRP 备份组的各路由器上进行以下配置

操作步骤

步骤 1 执行命令 **vrrp timer-advertise learning enable**，使能 VRRP 协议报文时间间隔学习功能。

默认情况下，该功能使能。

步骤 2 执行命令 **vrrp smooth-switching timer timer-value**，使能 VRRP 整机平滑倒换功能并配置平滑倒换期间 VRRP 报文中携带的时间间隔。

默认情况下，使能 VRRP 整机平滑倒换功能，并且 VRRP 报文携带的默认时间间隔为 100 秒。

配置该命令前必须确保已使能 VRRP 协议报文时间间隔学习功能。关闭 VRRP 协议报文时间间隔学习功能时，VRRP 整机平滑倒换功能也一起关闭。

说明

- 如果 Master 配置的广播报文发送时间间隔远大于 Backup 配置广播报文发送时间间隔，此时重启 Backup，接口恢复后，Backup 会重置自己的 masterdown 时间。当 masterdown 超时后，Master 可能远没有到达发送报文的时间，于是 Backup 就会超时成为 Master，从而出现双 Master。
- Master 在主备倒换期间发送平滑倒换报文是按照配置的时间间隔发送。如果 Master 配置的平滑倒换时间（如：1s）小于配置的 VRRP 广播报文时间间隔（如：10s），那么在主备倒换期间，会以 10s 的间隔发送 VRRP 报文，填充时间间隔为 1s，这样会导致对端 VRRP 状态不断振荡。

----结束

4.9.3 检查配置结果

通过查看 VRRP 备份组的状态等内容，来检查配置是否成功。

前提条件

已经完成 VRRP 平滑倒换功能的所有配置。

操作步骤

步骤 1 使用 **display vrrp [interface interface-type interface-number [virtual-router-id]]** 命令查看 VRRP 的状态信息。

----结束

任务示例

完成 VRRP 平滑倒换配置后，设备进行主备倒换。在设备主备倒换的过程中，VRRP 备份组的状态不切换，用户流量不受影响。主备倒换完成后，新主控板的所有 VRRP 配置和老主控板配置相同。

```
<HUAWEI> display vrrp
GigabitEthernet1/0/0 | Virtual Router 1
  State           : Master
  Virtual IP      : 10.10.10.158
  Master IP       : 10.10.10.1
  PriorityRun      : 180
  PriorityConfig   : 180
  MasterPriority   : 180
  Preempt         : YES      Delay Time : 0
  TimerRun        : 1
  TimerConfig     : 1
  Auth Type       : NONE
  Virtual Mac     : 0000-5e00-0101
  Check TTL       : YES
  Config type     : normal-vrrp
  Config track link-bfd down-number : 0
  Create time     : 2010-06-22 17:32:56
  Last change time : 2010-06-22 17:33:00
```

4.10 调整优化 VRRP

可以调整 VRRP 备份组的参数来优化 VRRP 备份组的功能。

4.10.1 建立配置任务

在调整优化 VRRP 功能之前，应了解其应用环境和数据准备，并需要配置 VRRP 备份组等前置任务。

应用环境

配置 VRRP 报文的相关参数可以优化备份组功能：

- 通过增大虚拟路由器发送 VRRP 通告报文的时间间隔，可以减轻协议报文造成的网络负荷。
- 对于 VRRP for IPv4，通过设置备份组内成员发送的 VRRP 通告报文时间间隔一致，可以避免同一备份组内出现多个 Master。
- VRRP 报文的通告时间间隔：
 - 对于 VRRP for IPv4，通过设置备份组内成员发送的 VRRP 通告报文时间间隔一致，可以避免同一备份组内出现多个 Master。
 - 对于 VRRP6，即使设置备份组内成员发送的 VRRP 通告报文的时间间隔不一致，同一备份组内也不会出现多个 Master。

- 通过配置备份组路由器的抢占方式和抢占延迟时间，可以加快或减慢主备设备之间的切换速度。
- 通过使能虚拟 IP 地址可达性测试开关，可以使用 Ping 功能检测网络的连通性。
- 通过禁止检测 VRRP 报文的跳数值，可以提高不同厂商设备的兼容性。

前置任务

在调整优化 VRRP 之前，需完成以下任务：

- 配置接口的网络层属性，使网络连通
- 配置 VRRP 备份组

数据准备

在调整优化 VRRP 之前，需要准备以下数据。

序号	数据
1	发送 VRRP 通告报文的时间间隔
2	备份组中路由器的抢占延迟时间
3	Master 发送免费 ARP 报文的超时时间

4.10.2 配置发送 VRRP 通告报文的时间间隔

通过增大虚拟路由器发送 VRRP 通告报文的时间间隔，可以减轻协议报文造成的网络负荷。

背景信息

Master 设备每隔一定时间向组内其他 Backup 设备发送 VRRP 通告报文，通知自己工作正常。如果 Backup 定时器超时后仍未收到 VRRP 通告报文，则优先级最高的 Backup 自动变成 Master。

请在需要调整 VRRP 通告报文时间间隔的路由器上进行以下配置。

根据 VRRP 是基于 IPv4 还是 IPv6，选择执行如下步骤之一：

操作步骤

- 对于 VRRP for IPv4：
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **interface interface-type interface-number**，进入接口视图。
 3. 执行命令 **vrrp vrid virtual-router-id timer advertise advertise-interval**，配置发送 VRRP 通告报文的间隔时间。

缺省情况下，发送 VRRP 通告报文的时间是 1 秒。在存在多个备份组的情况下，时间间隔太短会导致 VRRP 状态频繁倒换，可能需要增大时间间隔。
- 对于 VRRP6：

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface interface-type interface-number**，进入接口视图。
3. 执行命令 **vrrp6 vrid virtual-router-id timer advertise advertise-interval**，配置发送 VRRP6 通告报文的时间间隔。

缺省情况下，Master 设备发送 VRRP6 通告报文的时间间隔为 100 厘秒，即 1 秒。

----结束

4.10.3 设置备份组中路由器的抢占延迟时间

通过设置备份组中路由器的抢占延迟时间，可以加快或者减慢主备之间的切换速度。

背景信息

请在需要调整抢占延迟时间的 VRRP 备份组路由器上进行以下配置。

根据 VRRP 是基于 IPv4 还是 IPv6，选择执行如下步骤之一：

操作步骤

- 对于 VRRP for IPv4:

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface interface-type interface-number**，进入接口视图。
3. 执行命令 **vrrp vrid virtual-router-id preempt-mode timer delay delay-value**，配置备份组中路由器的抢占延迟时间。

缺省方式是抢占方式，延迟时间为 0，即立即抢占。立即抢占方式下，Backup 设备一旦发现自己的优先级比当前的 Master 的优先级高，就会成为 Master；相应地，原来的 Master 将会变成 Backup。设置抢占延迟时间，可以使 Backup 延迟一段时间成为 Master。

可以执行 **vrrp vrid virtual-router-id preempt-mode disable** 命令设置备份组中路由器采用非抢占方式。在非抢占方式下，一旦备份组中的某台路由器成为 Master，只要它没有出现故障，其它路由器即使随后被配置更高的优先级也不会成为 Master。

当 IP 地址拥有者故障恢复后，不会等待延时抢占，会立即切换到 Master。而延时抢占功能是指 Backup 设备切换到 Master 的等待时间，所以，IP 地址拥有者和延时抢占功能不相关。对于需要支持延时抢占功能的备份组，不能把 VRRP 备份组的主用设备配置成 IP 地址拥有者。

执行 **undo vrrp vrid virtual-router-id preempt-mode** 命令用来恢复缺省的抢占方式。

说明

在配置 VRRP 备份组内各路由器的延迟方式时，建议将 Backup 配置为立即抢占，即不延迟（延迟时间为 0），而将 Master 配置为抢占，并且配置一定的延迟时间。这样配置的目的是为了在网络环境不稳定时，为上下行链路的状态恢复一致性等待一定时间，以免出现双 Master 或由于双方频繁抢占导致用户设备学习到错误的 Master 设备地址。

- 对于 VRRP6:

1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
3. 执行命令 **vrrp6 vrid** *virtual-router-id* **preempt-mode timer delay** *delay-value*，配置备份组中路由器的抢占延迟时间。

缺省方式是抢占方式，延迟时间为 0，即立即抢占。立即抢占方式下，Backup 设备一旦发现自己的优先级比当前的 Master 的优先级高，就会成为 Master；相应地，原来的 Master 将会变成 Backup。设置抢占延迟时间，可以使 Backup 延迟一段时间成为 Master。

可以执行 **vrrp6 vrid preempt-mode disable** 命令设置备份组中路由器采用非抢占方式。在非抢占方式下，一旦备份组中的某台路由器成为 Master，只要它没有出现故障，其它路由器即使随后被配置更高的优先级也不会成为 Master。

当 IP 地址拥有者故障恢复后，不会等待延时抢占，会立即切换到 Master。而延时抢占功能是指 Backup 设备切换到 Master 的等待时间，所以，IP 地址拥有者和延时抢占功能不相关。对于需要支持延时抢占功能的备份组，不能把 VRRP 备份组的主用设备配置成 IP 地址拥有者。

执行 **undo vrrp6 vrid preempt-mode** 命令用来恢复缺省的抢占方式。

说明

在配置 VRRP 备份组内各路由器的延迟方式时，建议将 Backup 配置为立即抢占，即不延迟（延迟时间为 0），而将 Master 配置为抢占，并且配置一定的延迟时间。这样配置的目的是为了在网络环境不稳定时，为上下行链路的状态恢复一致性等待一定时间，以免出现双 Master 或由于双方频繁抢占导致用户设备学习到错误的 Master 设备地址。

----结束

4.10.4 使能虚拟地址可达性测试开关

通过使能虚拟 IP 地址可达性开关，可以使用 Ping 功能检测网络可达性。

背景信息

NE80E/40E 支持对虚拟 IP 地址的 Ping 功能，可用于：

- 检测备份组中的 Master 设备是否起作用。
- 检测是否能通过使用某虚拟 IP 地址作为默认网关与外部通信。

请在需要使能虚拟地址可达的路由器上进行以下配置。

该场景对于 VRRP for IPv4 和 VRRP6 同时有效。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vrrp virtual-ip ping enable**，使能虚拟地址可达性测试开关。

缺省情况下，该功能是打开的，Master 设备响应对本备份组虚拟 IP 地址的 Ping 报文。

能够 Ping 通虚拟 IP 地址，带来可能遭受 ICMP 攻击的隐患，可以执行 **undo vrrp virtual-ip ping enable** 命令来关闭虚拟地址可达性开关。

----结束

4.10.5 禁止检测 VRRP 报文的跳数

过禁止检测 VRRP 报文的跳数，可以提高不同厂商设备的兼容性。

背景信息

按照 RFC3768 定义，系统对收到的 VRRP 报文的跳数值进行检测，如果这个值不等于 255，报文将被丢弃。

在不同厂商的设备配合使用的组网环境中，检测 VRRP 报文的跳数值可能导致错误地丢弃报文。这时可以配置系统不检测 VRRP 报文的跳数值。

请在需要禁止检测 VRRP 报文的跳数的路由器上进行以下配置。

根据 VRRP 是基于 IPv4 还是 IPv6，选择执行如下步骤之一：

操作步骤

- 对于 VRRP for IPv4:
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **interface interface-type interface-number**，进入接口视图。
 3. 执行命令 **vrrp un-check ttl**，禁止检测 VRRP 报文的 TTL 值。
缺省情况下，检测 VRRP 报文的 TTL 值。可以执行 **undo vrrp un-check ttl** 命令来启动对 VRRP 报文 TTL 值的检测。
- 对于 VRRP6:
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **interface interface-type interface-number**，进入接口视图。
 3. 执行命令 **vrrp6 un-check hop-limit**，禁止检测 VRRP6 报文跳数值。
缺省情况下，检测 VRRP6 报文的跳数值。可以执行 **undo vrrp6 un-check hop-limit** 命令来启动对 VRRP6 报文跳数值的检测。

----结束

4.10.6 配置 Master 发送免费 ARP 报文的超时时间

通过调整 Master 设备发送免费 ARP 报文的时间间隔，可以减轻协议报文造成的网络负荷。

背景信息

请在需要配置发送免费 ARP 报文的路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vrrp gratuitous-arp timeout time**，配置 Master 发送免费 ARP 报文的超时时间。

Master 设备发送 ARP 报文时携带的是虚拟 MAC 地址。缺省情况下，Master 每隔 120 秒（2 分钟）发送一次免费 ARP 报文。

如果要恢复 Master 发送免费 ARP 报文的缺省超时时间，请在系统视图下执行 **undo vrrp gratuitous-arp timeout** 命令。

如果不需要发送免费 ARP 报文，请在系统视图下执行 **vrrp gratuitous-arp timeout disable** 命令。

----结束

4.10.7 检查配置结果

通过查看调整后的 VRRP 备份组的参数，来检查配置是否成功。

前提条件

已经完成调整优化 VRRP 功能的所有配置。

操作步骤

- 使用 **display vrrp [interface interface-type interface-number [virtual-router-id]] [brief]** 命令查看 VRRP 备份组的状态信息。
- 使用 **display vrrp6 [interface interface-type interface-number [vrid virtual-router-id]] [brief]** 查看当前 VRRP6 备份组的状态信息和配置参数。

----结束

任务示例

执行 **display vrrp** 命令，可以看到对 VRRP 的调整结果，例如，“TimerRun”和“TimerConfig”字段显示为“20”，将发送 VRRP 通告报文的时间调整为 20 秒（默认情况下为 1 秒）。

```
<HUAWEI> display vrrp
GigabitEthernet1/0/0 | Virtual Router 1
  State           : Master
  Virtual IP      : 100.1.1.111
  Master IP       : 10.1.1.1
  PriorityRun      : 120
  PriorityConfig   : 120
  MasterPriority   : 120
  Preempt         : YES      Delay Time : 0
  TimerRun        : 20
  TimerConfig      : 20
  Auth Type       : NONE
  Virtual Mac     : 0000-5e00-0201
  Check TTL       : YES
  Config type     : normal-vrrp
  Config track link-bfd down-number : 0
  Create time     : 2010-06-22 17:32:56
  Last change time : 2010-06-22 17:33:00
<HUAWEI> display vrrp6
GigabitEthernet1/0/0 | Virtual Router 1
  State           : Master
  Virtual IP      : FE80::1:2
  Master IP       : FE80::218:82FF:FED3:2AF1
  PriorityRun      : 200
  PriorityConfig   : 200
  MasterPriority   : 200
  Preempt         : YES      Delay Time : 0
  TimerRun        : 200
  TimerConfig     : 20
  Virtual Mac     : 0000-5e00-0201
  Uncheck hop limit : YES
```

```
Accept Mode      : ON
Config type      : normal-vrrp
Track If         : GigabitEthernet3/0/4   priority reduced : 70
IF State         : UP
Create time      : 2010-06-23 17:32:56
Last change time : 2010-06-23 17:33:00
```

4.11 配置管理 VRRP 备份组

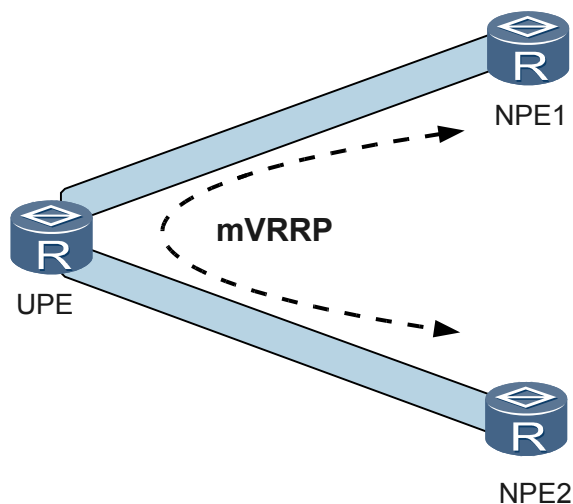
管理 VRRP 备份组可以绑定其它的业务备份组，并根据绑定关系，决定相关业务备份组的状态。它主要解决城域以太网中的主备双归属问题。

4.11.1 建立配置任务

在配置管理 VRRP 备份组功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

图 4-4 管理 VRRP 决定主备双归属



如图 4-4 所示，当城域以太网的汇聚层使用汇聚时，为了提高可靠性，通常部署双 NPE。NPE 之间通过运行管理 VRRP 来决定主备关系。

管理 VRRP 备份组从本质上讲就是普通的 VRRP 备份组，它与普通 VRRP 备份组的唯一区别在于：管理 VRRP 备份组可以绑定其他的业务备份组，并根据绑定关系，决定相关业务备份组的状态。

一个管理 VRRP 备份组可以绑定多个业务备份组，但它不能作为业务备份组与其他管理备份组进行绑定。

根据不同的应用场景，管理 VRRP 的绑定关系可分为：

- 成员 VRRP 备份组与管理 VRRP 备份组绑定：UPE 双归属到 NPE，NPE 之间运行 VRRP，通过配置 VRRP 的优先级来决定主用 NPE 和备用 NPE。为了满足不同的业务需要，NPE 之间可以运行多个 VRRP 备份组。

每个 VRRP 备份组都需要维护自己的状态机，这样 NPE 之间就会存在大量的 VRRP 协议报文。为了简化协议操作，减少协议报文对带宽的占用，可以将其中一个 VRRP 备份组配置为管理备份组，其余业务备份组与管理备份组进行绑定，并根据绑定管理直接决定业务备份组的状态。

- 业务接口与管理 VRRP 备份组绑定：如果 UPE 通过两条物理链路双归属到 NPE，可以配置业务接口与管理 VRRP 绑定来决定主用业务接口和备用业务接口。
- PW 与管理 VRRP 备份组绑定：如果 UPE 与 NPE 之间运行 VPLS，UPE 通过两条 PW 双归属到 NPE，此时可以配置 PW 与管理 VRRP 绑定来决定主用 PW 和备用 PW。

前置任务

在配置管理 VRRP 之前，需完成以下任务：

- 配置接口的网络层属性，使网络连通

数据准备

在配置管理 VRRP 备份组之前，需要准备以下数据。

序号	数据
1	管理 VRRP 和成员 VRRP 备份组 ID
2	管理 VRRP 和成员 VRRP 备份组虚拟 IP 地址
3	管理 VRRP 优先级
4	业务接口编号

4.11.2 配置管理 VRRP 备份组

每个 VRRP 备份组都要维护自己的状态机，配置管理 VRRP 备份组，可以减少协议报文对带宽的占用。

背景信息

请在管理 VRRP 备份组所在的路由器上进行以下配置。

根据 VRRP 是基于 IPv4 还是 IPv6，选择执行如下步骤之一：

操作步骤

- 对于 VRRP for IPv4：
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **interface interface-type interface-number**，进入接口视图。
 3. 执行命令 **vrrp vrid virtual-router-id virtual-ip virtual-address**，创建备份组并配置虚拟 IP 地址。
 4. 执行命令 **vrrp vrid virtual-router-id priority priority-value**，配置 VRRP 备份组的优先级。

5. 执行命令 **admin-vrrp vrid** *virtual-router-id* [**ignore-if-down**]，配置该 VRRP 备份组为管理 VRRP 备份组。
- 对于 VRRP for IPv6:
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
 3. 执行命令 **vrrp6 vrid** *virtual-router-id* **virtual-ip** *virtual-ipv6-address* [**link-local**]，创建备份组并配置虚拟 IPv6 地址。
 4. 执行命令 **vrrp6 vrid** *virtual-router-id* **priority** *priority-value*，配置备份组的优先级。
 5. 执行命令 **admin-vrrp6 vrid** *virtual-router-id* [**ignore-if-down**]，配置该备份组为管理 VRRP6 备份组。

----结束

4.11.3 （可选）配置成员 VRRP 备份组并将其与管理 VRRP 备份组绑定

配置成员 VRRP 备份组与管理 VRRP 备份组绑定，实现成员 VRRP 备份组和管理 VRRP 备份组状态机的一致性。

背景信息

请在需要将成员 VRRP 备份组与管理 VRRP 绑定的路由器上进行以下配置。

操作步骤

- 对于 VRRP for IPv4:
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **interface** *interface-type interface-number* [*.subinterface-number*]，进入运行成员 VRRP 备份组所在的接口视图。
 3. 执行命令 **vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address*，创建成员 VRRP 备份组并配置虚拟 IP 地址。

由于成员 VRRP 备份组的状态由管理 VRRP 备份组决定，因此，无需为成员 VRRP 备份组配置优先级。

4. 执行命令 **vrrp vrid** *virtual-router-id1* **track admin-vrrp interface** *interface-type interface-number* **vrid** *virtual-router-id2*，将成员 VRRP 备份组与管理 VRRP 备份组绑定。

成员 VRRP 备份组与管理 VRRP 备份组绑定之后，成员 VRRP 状态机就丧失了独立性，即会删除协议定时器、不再收发协议报文，通过直接拷贝管理备份组的状态来实现自己的状态机。成员 VRRP 备份组只能绑定到一个管理 VRRP 备份组。



说明

一个接口上仅能配置一个业务 VRRP。

- 对于 VRRP for IPv6:
 1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **interface** *interface-type interface-number* [*.subinterface-number*], 进入运行成员 VRRP6 备份组所在的接口视图。
3. 执行命令 **vrrp6 vrid** *virtual-router-id* **virtual-ip** *virtual-ipv6-address* [**link-local**], 创建成员 VRRP6 备份组并配置虚拟 IPv6 地址。

由于成员 VRRP6 备份组的状态由管理 VRRP6 备份组决定, 因此, 无需为成员 VRRP6 备份组配置优先级。

4. 执行命令 **vrrp6 vrid** *virtual-router-id1* **track admin-vrrp6 interface** *interface-type interface-number* **vrid** *virtual-router-id2*, 将成员 VRRP6 备份组与管理 VRRP6 备份组绑定。

成员 VRRP6 备份组与管理 VRRP6 备份组绑定之后, 成员 VRRP6 备份组的状态机就丧失了独立性, 即会删除协议定时器、不再收发协议报文, 通过直接拷贝管理 VRRP6 备份组的状态来实现自己的状态机。成员 VRRP6 备份组只能绑定到一个管理 VRRP6 备份组。



说明
一个接口上仅能配置一个业务 VRRP6。

----结束

4.11.4 (可选) 配置业务接口与管理 VRRP 备份组绑定

管理 VRRP 备份组可以通过监视接口的状态实现主备快速切换的功能。

背景信息

请在需要将业务接口与管理 VRRP 绑定的路由器上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**, 进入系统视图。
- 步骤 2** 执行命令 **interface** *interface-type interface-number* [*.subinterface-number*], 进入业务接口视图。
- 步骤 3** 执行命令 **track admin-vrrp interface** *interface-type interface-number* **vrid** *virtual-router-id*, 配置业务接口与管理 VRRP 备份组绑定。

----结束

4.11.5 (可选) 配置 VPLS 方式 PW 与管理 VRRP 备份组绑定

通过配置 PW 与管理 VRRP 备份组绑定, 实现 PW 和管理 VRRP 备份组的联动。

背景信息

请在需要将 PW 与管理 VRRP 绑定的路由器上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**, 进入系统视图。
- 步骤 2** 执行命令 **vsi** *vsi-name* **static**, 进入 VSI 视图。

步骤 3 执行命令 **pwsignal ldp**，进入 VSI-LDP 视图。

步骤 4 执行命令 **peer peer-address [negotiation-vc-id vc-id] track admin-vrrp interface interface-type interface-number vrid virtual-router-id**，配置 PW 与管理 VRRP 备份组绑定。

使用该命令配置 PW 与管理 VRRP 备份组绑定之前，Peer 必须已存在。

有关 PW 的具体配置请参考《HUAWEI NetEngine80E/40E 路由器 配置指南-VPN》中的“VPLS 配置”。

----结束

4.11.6 检查配置结果

通过查看管理 VRRP 备份组的所有绑定信息，来检查配置是否成功。

前提条件

已经完成管理 VRRP 备份组功能的所有配置。

操作步骤

- 使用 **display vrrp binding admin-vrrp [interface interface-type interface-number] [vrid virtual-router-id]**命令查看管理 VRRP 所有的绑定信息。
- 使用 **display vrrp binding admin-vrrp [interface interface-type1 interface-number1] [vrid virtual-router-id1] member-vrrp [interface interface-type2 interface-number2] [vrid virtual-router-id2]**命令查看管理 VRRP 备份组与成员 VRRP 备份组的绑定关系。
- 使用 **display vrrp binding admin-vrrp [interface interface-type1 interface-number1] [vrid virtual-router-id] member-interface [interface interface-type2 interface-number2]**命令查看管理 VRRP 备份组与成员业务接口的绑定关系。
- 使用 **display vrrp6 binding admin-vrrp6 [interface interface-type1 interface-number1] [vrid virtual-router-id1] member-vrrp [interface interface-type2 interface-number2] [vrid virtual-router-id2]**命令查看管理 VRRP6 备份组与成员 VRRP6 备份组的绑定关系。
- 使用以下命令查看管理 VRRP 备份组与成员 PW 的绑定关系：
 - **display vrrp binding admin-vrrp [interface interface-type1 interface-number1] [vrid virtual-router-id] member-pw**
 - **display vrrp binding admin-vrrp [interface interface-type1 interface-number1] [vrid virtual-router-id] member-pw vc interface interface-type2 interface-number2**
 - **display vrrp binding admin-vrrp [interface interface-type1 interface-number1] [vrid virtual-router-id] member-pw vsi vsi-name peer ip-address [negotiation-vc-id vc-id1]**
 - **display vrrp binding admin-vrrp [interface interface-type1 interface-number1] [vrid virtual-router-id] member-pw vc switch-vc peer ip-address vc-id2**
- 使用 **display vrrp admin-vrrp** 查看当前配置中所有管理 VRRP 的状态。

----结束

任务示例

配置完成后，执行 **display vrrp binding admin-vrrp** 命令可以看到管理 VRRP 所有的绑定信息，包括成员 VRRP、业务接口和成员 PW。

```
<HUAWEI> display vrrp binding admin-vrrp
Interface: GigabitEthernet2/0/0, admin-vrrp vrid: 6, state: Master
Member-vrrp number: 1
    Interface: GigabitEthernet2/0/0.1, vrid: 8, state: Master

Member-interface number: 1
    Interface: GigabitEthernet2/0/0.2, state: Up
```

4.12 配置 VRRP 协议版本升级

通过将 VRRP 协议由版本 2 升级到版本 3，实现 VRRP 协议既支持 IPv6 网络也支持 IPv4 网络。

4.12.1 建立配置任务

在配置 VRRP 协议版本功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

目前，VRRP 协议的版本号是 2。VRRP for IPv4 支持 VRRPv2 报文格式和 VRRPv3 报文格式，而 VRRP for IPv6 只支持 VRRPv3 报文格式。如果用户需要将 VRRP 协议的版本进行升级，则可以执行此配置。

前置任务

在配置 VRRP 协议版本升级之前，需完成以下任务：

- 设备安装完毕并加电启动正常
- 当前 VRRP 协议的版本号是 2

数据准备

配置 VRRP 协议版本升级之前，需要准备以下数据。

序号	数据
1	VRRP 协议的版本号

4.12.2 配置 VRRPv3 版本

通过配置 VRRPv3 版本，实现备份组既能接收版本 v2 的通告报文，也能接收版本 v3 的通告报文。

背景信息

请在备份组的各路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **vrrp version v3**，设置当前设备的 VRRP 协议版本号是 3。

步骤 3（可选）执行命令 **vrrp version-3 send-packet-mode { v2-only | v3-only | v2v3-both }**，设置 VRRPv3 发送通告报文的模式。

缺省情况下，VRRP 版本协议为 v2。切换到 v3 模式下，缺省的通告报文模式为 **v3-only**。

----结束

4.12.3 检查配置结果

通过查看 VRRP 协议的版本信息，检查配置是否成功。

前提条件

已经完成 VRRP 协议版本升级功能的所有配置。

操作步骤

- 使用 **display vrrp protocol-information** 命令查看 VRRP 协议的相关信息。

----结束

任务示例

配置成功后，执行 **display vrrp protocol-information** 命令，可以看到 VRRP 协议的版本是 **v3**，发送通告报文的模式是 **send v3 only**

```
<HUAWEI> display vrrp protocol-information
VRRP protocol information is shown as below:
      VRRP protocol version : v3
      Send advertisement packet mode : send v3 only
```

4.13 维护 VRRP

通过维护 VRRP，可以实现清除 VRRP 统计数据和监控 VRRP 的运行状况的目的。

4.13.1 监控 VRRP 运行状况

通过监控 VRRP 运行状况，可以了解运行过程中 VRRP 的相关信息。

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解 VRRP 的运行状况。

操作步骤

- 在任意视图下执行 **display vrrp [interface interface-type interface-number [virtual-router-id]] [brief]** 命令，查看当前 VRRP 备份组的状态信息和配置参数。

- 在任意视图下执行 **display vrrp6** [interface interface-type interface-number [vrid virtual-router-id]] [brief] 查看当前 VRRP6 备份组的状态信息和配置参数。

----结束

4.14 配置举例

介绍使用 VRRP 提高可靠性的各种示例。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

背景信息

说明

手册中所使用的链路接口编号和链路类型以 NE40E-X8 为例，实际使用时以现网设备为准。

4.14.1 配置主备备份 VRRP 示例

本示例中，通过配置主备备份方式的 VRRP 备份组，实现备份组中的主用设备分担网路流量。

组网需求

说明

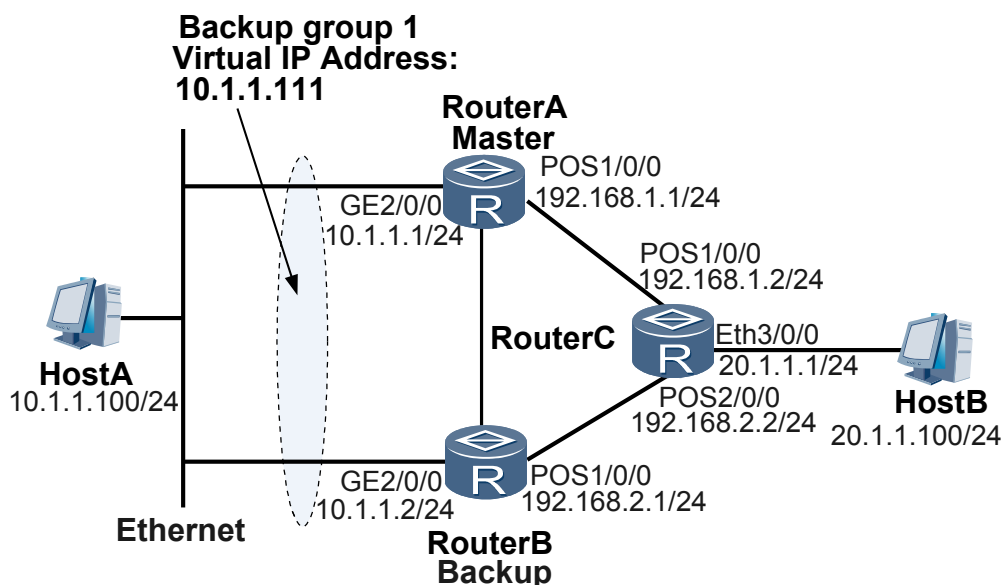
POS 接口特性在 NE80E/40E 系列中的 X1 和 X2 设备上不支持。

如图 4-5 所示。主机 HostA 通过缺省网关访问主机 HostB。

需求如下：

- RouterA 和 RouterB 组成 VRRP 备份组，作为 HostA 的缺省网关。
- 正常情况下，RouterA 承担网关工作；当 RouterA 出现故障时，RouterB 接替执行网关工作。
- RouterA 恢复后，能在 20 秒内抢占成为 Master。

图 4-5 配置主备备份 VRRP 组网图



配置思路

采用如下思路配置主备备份 VRRP：

1. 在 RouterA 的 GE2/0/0 接口下创建备份组 1，并配置 RouterA 在该备份组中具有高优先级，确保 RouterA 为 Master，配置抢占方式。
2. 在 RouterB 的 GE2/0/0 接口下创建备份组 1，使用缺省优先级。

数据准备

为完成此配置例，需准备如下的数据：

- VRRP 备份组 ID、虚拟 IP 地址
- 路由器在备份组中的优先级
- 抢占方式

操作步骤

步骤 1 配置设备之间的网络互连

设置主机 HostA 的缺省网关为 10.1.1.111，HostB 的缺省网关为 20.1.1.1。

在 RouterA、RouterB、RouterC 路由器之间采用 OSPF 协议进行互连。

步骤 2 配置 VRRP

在 RouterA 上，配置接口 IP 地址，创建备份组 1，并配置 RouterA 在该备份组中的优先级为 120（作为 Master）。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] undo shutdown
[RouterA-GigabitEthernet2/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet2/0/0] vrrp vrid 1 virtual-ip 10.1.1.111
[RouterA-GigabitEthernet2/0/0] vrrp vrid 1 priority 120
[RouterA-GigabitEthernet2/0/0] vrrp vrid 1 preempt-mode timer delay 20
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] quit
```

在 RouterB 上，配置接口 IP 地址，创建备份组 1，并配置 RouterB 在该备份组中的优先级为缺省值 100（作为 Backup）。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] undo shutdown
[RouterB-GigabitEthernet2/0/0] ip address 10.1.1.2 24
[RouterB-GigabitEthernet2/0/0] vrrp vrid 1 virtual-ip 10.1.1.111
[RouterB-GigabitEthernet2/0/0] quit
[RouterB] quit
```

步骤 3 检验配置结果

- 验证 VRRP 备份组能够正常提供网关功能

完成以上配置后，在主机 HostA 上能够 Ping 通 HostB，在 RouterA 上执行 **display vrrp** 命令可以看到 RouterA 的状态是 Master，在 RouterB 上执行 **display vrrp** 命令可以看到 RouterB 的状态是 Backup，如下所示。

```
<RouterA> display vrrp
```

```
GigabitEthernet2/0/0 | Virtual Router 1
state : Master
Virtual IP : 10.1.1.111
Master IP : 10.1.1.1
PriorityRun : 120
PriorityConfig : 120
MasterPriority : 120
Preempt : YES Delay Time : 20
TimerRun : 1
TimerConfig : 1
Auth Type : NONE
Virtual Mac : 0000-5e00-0101
Check TTL : YES
Config type : normal-vrrp
Create time : 2010-06-22 17:33:00
Last change time : 2010-06-22 17:33:06
<RouterB> display vrrp
GigabitEthernet2/0/0 | Virtual Router 1
state : Backup
Virtual IP : 10.1.1.111
Master IP : 10.1.1.1
PriorityRun : 100
PriorityConfig : 100
MasterPriority : 120
Preempt : YES Delay Time : 0
TimerRun : 1
TimerConfig : 1
Auth Type : NONE
Virtual Mac : 0000-5e00-0101
Check TTL : YES
Config type : normal-vrrp
Create time : 2010-06-22 17:33:00
Last change time : 2010-06-22 17:33:06
```

在 RouterA 和 RouterB 上执行 **display ip routing-table** 命令，RouterA 上可以看到路由表中有一条目的地址为虚拟 IP 地址的直连路由，而 RouterB 上该路由为 OSPF 路由。
RouterA 和 RouterB 上的显示信息如下。

```
<RouterA> display ip routing-table
Route Flags: R - relied, D - download to fib
-----
Routing Tables: Public
Destinations : 10 Routes : 10
Destination/Mask Proto Pre Cost Flags NextHop Interface
10.1.1.0/24 Direct 0 0 D 10.1.1.1 GigabitEthernet2/0/0
10.1.1.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
10.1.1.111/32 Direct 0 0 D 127.0.0.1 InLoopBack0
20.1.1.0/24 OSPF 10 2 D 192.168.1.2 Pos1/0/0
127.0.0.0/8 Direct 0 0 D 127.0.0.1 InLoopBack0
127.0.0.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
192.168.1.0/24 Direct 0 0 D 192.168.1.1 Pos1/0/0
192.168.1.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
192.168.1.2/32 Direct 0 0 D 192.168.1.2 Pos1/0/0
192.168.2.0/24 OSPF 10 2 D 10.1.1.2 GigabitEthernet2/0/0
<RouterB> display ip routing-table
Route Flags: R - relied, D - download to fib
-----
Routing Tables: Public
Destinations : 10 Routes : 10
Destination/Mask Proto Pre Cost Flags NextHop Interface
10.1.1.0/24 Direct 0 0 D 10.1.1.2 InLoopBack0
10.1.1.2/32 Direct 0 0 D 127.0.0.1 InLoopBack0
10.1.1.111/32 OSPF 10 2 D 10.1.1.1 InLoopBack0
20.1.1.0/24 OSPF 10 2 D 192.168.2.2 Pos1/0/0
127.0.0.0/8 Direct 0 0 D 127.0.0.1 InLoopBack0
127.0.0.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
192.168.1.0/24 OSPF 10 2 D 10.1.1.1 GigabitEthernet2/0/0
192.168.2.0/24 Direct 0 0 D 192.168.2.1 Pos1/0/0
192.168.2.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
```

```
192.168.2.2/32    Direct  0    0    D    192.168.2.2    Pos1/0/0
```

- 验证 RouterA 故障时 RouterB 能够成为 Master

对 RouterA 的 GE2/0/0 接口执行 **shutdown** 命令，模拟 RouterA 出现故障。

在 RouterB 上使用 **display vrrp** 命令查看 VRRP 状态信息，应能够看到 RouterB 的状态是 Master，如下。

```
<RouterB> display vrrp
GigabitEthernet2/0/0 | Virtual Router 1
  state           : Master
  Virtual IP      : 10.1.1.111
  Master IP       : 10.1.1.2
  PriorityRun      : 100
  PriorityConfig   : 100
  MasterPriority   : 100
  Preempt         : YES    Delay Time : 0
  TimerRun        : 1
  TimerConfig     : 1
  Auth Type       : NONE
  Virtual Mac     : 0000-5e00-0101
  Check TTL       : YES
  Config type     : normal-vrrp
  Create time     : 2010-06-22 17:33:00
  Last change time : 2010-06-22 17:33:06
```

- 验证 RouterA 恢复后能够抢占

对 RouterA 的 GE2/0/0 接口执行 **undo shutdown** 命令，GE2/0/0 接口恢复 UP 状态后，等待 20 秒，在 RouterA 上使用 **display vrrp** 命令查看 VRRP 状态信息，应能够看到 RouterA 的状态恢复成 Master。

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode timer delay 20
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
```



```
vrp vrid 1 virtual-ip 10.1.1.111
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.2.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
 network 192.168.2.0 0.0.0.255
 network 10.1.1.0 0.0.0.255
#
return
```

● RouterC 的配置文件

```
#
sysname RouterC
#
interface Ethernet3/0/0
 undo shutdown
 ip address 20.1.1.1 255.255.255.0
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.1.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.2.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
 network 192.168.1.0 0.0.0.255
 network 192.168.2.0 0.0.0.255
 network 20.1.1.0 0.0.0.255
#
return
```

4.14.2 配置负载分担 VRRP 示例

本示例中，通过配置负载分担方式的 VRRP 备份组，实现备份组中各台设备既相互备份，又分担网络流量。

组网需求



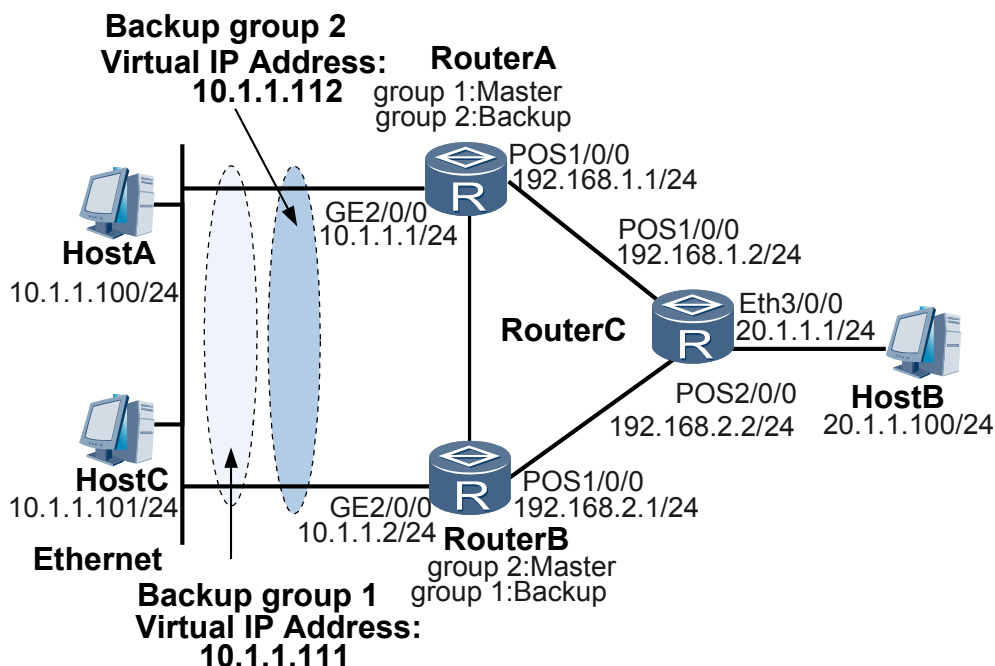
说明

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

如图 4-6 所示。

- RouterA 作为备份组 1 的 Master，兼任备份组 2 的 Backup。
- RouterB 作为备份组 2 的 Master，兼任备份组 1 的 Backup。
- 内部网络中的 HostA 使用备份组 1 作网关，HostC 主机使用备份组 2 作为网关，达到分担数据流而又相互备份的目的。

图 4-6 配置负载分担 VRRP 组网图



配置思路

采用如下思路配置负载分担 VRRP：

1. 在 RouterA 的 GE2/0/0 接口下创建 2 个备份组，RouterA 在备份组 1 中作为 Master，在备份组 2 中作为 Backup。
2. 在 RouterB 的 GE2/0/0 接口下创建 2 个备份组，RouterB 在备份组 1 中作为 Backup，在备份组 2 中作为 Master。

数据准备

为完成此配置例，需准备如下的数据：

- VRRP 备份组 ID、虚拟 IP 地址
- 路由器在备份组中的优先级

操作步骤

步骤 1 配置设备之间的网络互连

配置主机 HostA 的缺省网关为备份组 1 的虚拟 IP 地址 10.1.1.111，配置主机 HostB 的缺省网关为 20.1.1.1，配置主机 HostC 的缺省网关为备份组 2 的虚拟 IP 地址 10.1.1.112。

配置 RouterA、RouterB 和 RouterC 路由器之间运行 OSPF。

步骤 2 配置 VRRP 备份组

在 RouterA 上配置接口 GE2/0/0，创建备份组 1，并配置 RouterA 在备份组 1 中的优先级为 120（作为 Master）。创建备份组 2，并配置 RouterA 在备份组 2 中的优先级为缺省值 100（作为 Backup）。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] undo shutdown
[RouterA-GigabitEthernet2/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet2/0/0] vrrp vrid 1 virtual-ip 10.1.1.111
[RouterA-GigabitEthernet2/0/0] vrrp vrid 1 priority 120
[RouterA-GigabitEthernet2/0/0] vrrp vrid 2 virtual-ip 10.1.1.112
[RouterA-GigabitEthernet2/0/0] quit
```

在 RouterB 上配置接口 GE2/0/0，创建备份组 1，并配置 RouterB 在备份组 1 中的优先级为缺省值 100（作为 Backup）。创建备份组 2，并配置 RouterB 在备份组 2 中的优先级为 120（作为 Master）。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] undo shutdown
[RouterB-GigabitEthernet2/0/0] ip address 10.1.1.2 24
[RouterB-GigabitEthernet2/0/0] vrrp vrid 1 virtual-ip 10.1.1.111
[RouterB-GigabitEthernet2/0/0] vrrp vrid 2 virtual-ip 10.1.1.112
[RouterB-GigabitEthernet2/0/0] vrrp vrid 2 priority 120
[RouterB-GigabitEthernet2/0/0] quit
```

步骤 3 检验配置结果

完成以上配置后，网络中 HostA、HostC 主机分别能够 Ping 通 HostB。

在 HostA 和 HostC 上分别对 HostB 的地址进行 **tracert** 测试，可以看到 HostA 经过 RouterA 和 RouterC 到达 HostB，而 HostC 经过 RouterB 和 RouterC 到达 HostB。即，RouterA 和 RouterB 对内部网络来的流量进行负载分担。

```
<HostA> tracert 20.1.1.100
traceroute to 20.1.1.100 (20.1.1.100), max hops: 30, packet length: 40, press CTRL_C to break
 1  10.1.1.1      120ms  50 ms  60 ms
 2  192.168.1.2   100 ms  60 ms  60 ms
 3  20.1.1.100    130 ms  90 ms  90 ms
<HostC> tracert 20.1.1.100
traceroute to 20.1.1.100 (20.1.1.100), max hops: 30, packet length: 40, press CTRL_C to break
 1  10.1.1.2      30 ms  60 ms  40 ms
 2  192.168.2.2   90 ms  60 ms  60 ms
 3  20.1.1.100    70 ms  60 ms  90 ms
```

在 RouterA 上执行 **display vrrp** 命令，可以看到 RouterA 分别作为备份组 1 的 Master 和备份组 2 的 Backup。

```
<RouterA> display vrrp
GigabitEthernet2/0/0 | Virtual Router 1
  state           : Master
  Virtual IP      : 10.1.1.111
  Master IP       : 10.1.1.1
  PriorityRun      : 120
  PriorityConfig   : 120
  MasterPriority   : 120
  Preempt         : YES      Delay Time : 0
  TimerRun        : 1
  TimerConfig     : 1
  Auth Type       : NONE
  Virtual Mac     : 0000-5e00-0101
  Check TTL       : YES
  Config type     : normal-vrrp
GigabitEthernet2/0/0 | Virtual Router 2
  state           : Backup
  Virtual IP      : 10.1.1.112
  Master IP       : 10.1.1.2
  PriorityRun      : 100
  PriorityConfig   : 100
  MasterPriority   : 120
  Preempt         : YES      Delay Time : 0
  TimerRun        : 1
```

```
TimerConfig      : 1
Auth Type        : NONE
Virtual Mac       : 0000-5e00-0102
Check TTL         : YES
Config type       : normal-vrrp
```

----结束

配置文件

● RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 1 priority 120
 vrrp vrid 2 virtual-ip 10.1.1.112
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
return
```

● RouterB 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 2 virtual-ip 10.1.1.112
 vrrp vrid 2 priority 120
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.2.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
return
```

● RouterC 的配置文件

```
#
 sysname RouterC
#
interface Ethernet3/0/0
 undo shutdown
 ip address 20.1.1.1 255.255.255.0
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.1.2 255.255.255.0
```

```
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.2.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
#
return
```

4.14.3 配置多实例 VRRP 示例

本示例中，通过将不同 VPN 网络的 CE 设备的缺省网关设置为不同的值，可以实现 VRRP 备份组的负载分担，并实现同一个 VPN 网络内的主机相互通信。

组网需求



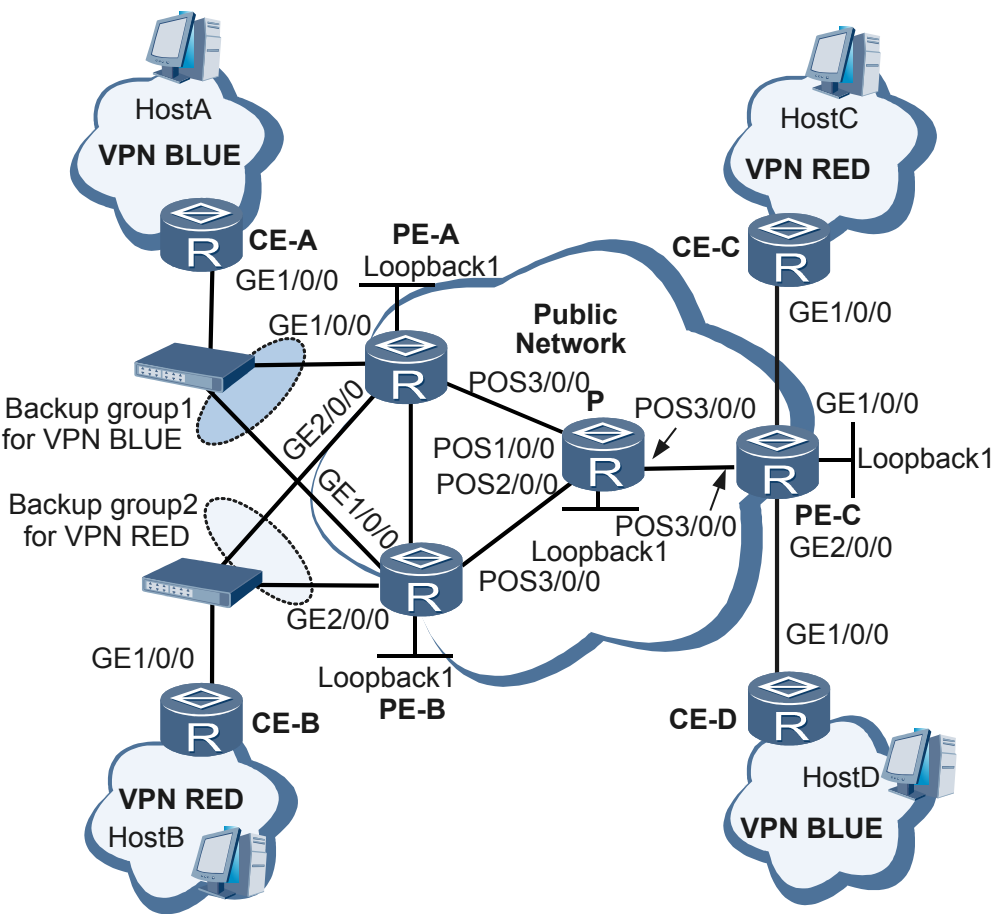
POS 接口特性在 NE80E/40E 系列中的 X1 和 X2 设备上不支持。

如图 4-7 所示，存在两个 VPN 网络 VPN RED 和 VPN BLUE，并已经按照表 4-1 要求进行 MPLS 和 VRRP 基本配置。

表 4-1 多实例 VRRP 的组网需求

项目	组网需求
备份组需求	● PE-A 和 PE-B 组成备份组 1 和备份组 2。其中，备份组 1 中 PE-A 为 Master，PE-B 为 Backup；备份组 2 中 PE-A 为 Backup，PE-B 为 Master。 ● CE-A 以 VRRP 备份组 1 的虚拟 IP 地址为自己的缺省网关。 ● CE-B 以 VRRP 备份组 2 的虚拟 IP 地址为自己的缺省网关。
CE 所属的 VPN 实例	● CE-A、CE-D 属于 VPN-BLUE 实例。 ● CE-B、CE-C 属于 VPN-RED 实例。
PE 上的接口所属 VPN 实例	● PE-A 上的 GE1/0/0 接口属于 VPN-BLUE 实例；GE2/0/0 接口属于 VPN-RED 实例。 ● PE-B 上的 GE1/0/0 接口属于 VPN-BLUE 实例；GE2/0/0 接口属于 VPN-RED 实例。 ● PE-C 上的 GE1/0/0 接口属于 VPN-RED 实例；GE2/0/0 接口属于 VPN-BLUE 实例。
路由协议和 MPLS	● 在公网上配置 OSPF，启动 MPLS 转发。 ● 在 CE-A、CE-B 上配置缺省路由，和 PE-A、PE-B 交换 VPN 路由。 ● 在 PE-A、PE-B、PE-C 之间建立 BGP Peer 传递 VPN 路由。

图 4-7 配置多实例 VRRP 组网图



设备	接口	IP 地址	所属实例
P	POS1/0/0	192.168.1.2/24	-
	POS2/0/0	192.168.2.2/24	-
	POS3/0/0	192.168.3.2/24	-
	Loopback1	4.4.4.4/32	-
PE-A	GE1/0/0	10.1.1.1/24	VPN-BLUE
	GE2/0/0	20.1.1.1/24	VPN-RED
	POS3/0/0	192.168.1.1/24	-
	Loopback1	1.1.1.1/32	-
PE-B	GE1/0/0	10.1.1.2/24	VPN-BLUE
	GE2/0/0	20.1.1.2/24	VPN-RED
	POS3/0/0	192.168.2.1/24	-
	Loopback1	2.2.2.2/32	-
PE-C	GE1/0/0	20.2.1.1/24	VPN-RED
	GE2/0/0	10.2.1.1/24	VPN-BLUE
	POS3/0/0	192.168.3.1/24	-
	Loopback1	3.3.3.3/32	-
CE-A	GE1/0/0	10.1.1.100/24	-
CE-B	GE1/0/0	20.1.1.100/24	-
CE-C	GE1/0/0	20.2.1.100/24	-
CE-D	GE1/0/0	10.2.1.100/24	-

配置思路

采用如下思路配置 VRRP 多实例：

1. 在 PE-A 和 PE-B 上配置备份组 1 和备份组 2。其中，备份组 1 中 PE-A 为 Master，PE-B 为 Backup；备份组 2 中 PE-A 为 Backup，PE-B 为 Master。
2. PE-A 和 PE-B 实现负载分担并互为备份。

数据准备

为完成此配置例，需准备如下的数据：

- VRRP 备份组 ID、虚拟 IP 地址
- 路由器在备份组中的优先级

操作步骤

步骤 1 在各 PE 间、PE 和 P 上配置 OSPF 路由协议，实现骨干网互通（略）

步骤 2 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP（略）

步骤 3 在各 PE 设备上配置 VPN 实例，将 CE 接入 PE（略）

步骤 4 在各 PE 之间建立 MP-IBGP 对等体连接（略）

步骤 5 在 CE-A 和 CE-B 上配置缺省路由（略）

步骤 1～步骤 5 中的配置，请参见《HUAWEI NetEngine80E/40E 路由器 配置指南-VPN》中“BGP MPLS IP VPN 配置”章节的描述，也可以参见本例的配置文件。

步骤 6 在 PE-A 和 PE-B 上配置多实例 VRRP

在 PE-A 上创建备份组 1，配置 PE-A 在备份组 1 中的优先级为 120（作为 Master）。

```
<PE-A> system-view
[PE-A] interface gigabitethernet 1/0/0
[PE-A-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.1.1.111
[PE-A-GigabitEthernet1/0/0] vrrp vrid 1 priority 120
[PE-A-GigabitEthernet1/0/0] quit
```

在 PE-A 上创建备份组 2，配置 PE-A 在备份组 2 中的优先级为缺省值（作为 Backup）。

```
[PE-A] interface gigabitethernet 2/0/0
[PE-A-GigabitEthernet2/0/0] vrrp vrid 2 virtual-ip 20.1.1.111
[PE-A-GigabitEthernet2/0/0] quit
```

在 PE-B 上创建备份组 1，PE-B 在备份组 1 中采用缺省优先级（作为 Backup）。

```
<PE-B> system-view
[PE-B] interface gigabitethernet 1/0/0
[PE-B-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.1.1.111
[PE-B-GigabitEthernet1/0/0] quit
```

在 PE-B 上创建备份组 2，配置 PE-B 在备份组 2 中的优先级为 120（作为 Master）。

```
[PE-B] interface gigabitethernet 2/0/0
[PE-B-GigabitEthernet2/0/0] vrrp vrid 2 virtual-ip 20.1.1.111
[PE-B-GigabitEthernet2/0/0] vrrp vrid 2 priority 120
```

```
[PE-B-GigabitEthernet2/0/0] quit
```

步骤 7 验证配置结果

在 PE-A 和 PE-B 上执行 **display ip routing-table vpn-instance vpn-instance-name** 命令，可以看到：PE-A 的 VPN 路由表中有一条目的地址为虚拟 IP 地址的路由，PE-B 上没有该路由。

PE-A 上的显示信息如下。

```
<PE-A> display ip routing-table vpn-instance VPN-BLUE
Route Flags: R - relied, D - download to fib
-----
Routing Tables: VPN-BLUE
      Destinations : 3          Routes : 3
Destination/Mask    Proto   Pre  Cost   Flags  NextHop         Interface
10.1.1.0/24         Direct  0    0       D      10.1.1.2         GigabitEthernet1/0/0
10.1.1.1/32         Direct  0    0       D      10.1.1.1         InLoopBack0
10.1.1.111/32       Direct  0    0       D      127.0.0.1        InLoopBack0
```

在 PE-A 和 PE-B 上使用支持多实例的 ping 命令。

```
<PE-A> ping -vpn-instance VPN-BLUE 10.1.1.111
PING 10.1.1.111: 56 data bytes, press CTRL_C to break
  Reply from 10.1.1.111: bytes=56 Sequence=1 ttl=255 time=6 ms
  Reply from 10.1.1.111: bytes=56 Sequence=2 ttl=255 time=1 ms
  Reply from 10.1.1.111: bytes=56 Sequence=3 ttl=255 time=1 ms
  Reply from 10.1.1.111: bytes=56 Sequence=4 ttl=255 time=1 ms
  Reply from 10.1.1.111: bytes=56 Sequence=5 ttl=255 time=1 ms

--- 10.1.1.111 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/2/6 ms
```

----结束

配置文件

● PE-A 的配置文件

```
#
sysname PE-A
#
ip vpn-instance VPN-BLUE
  ipv4-family
    route-distinguisher 100:1
    vpn-target 100:1 export-extcommunity
    vpn-target 100:1 import-extcommunity
#
ip vpn-instance VPN-RED
  ipv4-family
    route-distinguisher 200:1
    vpn-target 200:1 export-extcommunity
    vpn-target 200:1 import-extcommunity
#
mpls lsr-id 1.1.1.1
mpls
#
mpls ldp
#
interface GigabitEthernet1/0/0
  undo shutdown
  ip binding vpn-instance VPN-BLUE
  ip address 10.1.1.1 255.255.255.0
  vrrp vrid 1 virtual-ip 10.1.1.111
  vrrp vrid 1 priority 120
```



```
#
interface GigabitEthernet2/0/0
undo shutdown
ip binding vpn-instance VPN-RED
ip address 20.1.1.1 255.255.255.0
vrrp vrid 2 virtual-ip 20.1.1.111
#
interface Pos3/0/0
link-protocol ppp
undo shutdown
ip address 192.168.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 1.1.1.1 255.255.255.255
#
bgp 100
peer 3.3.3.3 as-number 100
peer 3.3.3.3 connect-interface LoopBack1
#
ipv4-family unicast
undo synchronization
peer 3.3.3.3 enable
#
ipv4-family vpnv4
policy vpn-target
peer 3.3.3.3 enable
#
ipv4-family vpn-instance VPN-BLUE
import-route direct
import-route static
#
ipv4-family vpn-instance VPN-RED
import-route direct
import-route static
#
ospf 1
area 0.0.0.0
network 192.168.1.0 0.0.0.255
network 1.1.1.1 0.0.0.0
#
ip route-static vpn-instance VPN-BLUE 0.0.0.0 0.0.0.0 10.1.1.100
ip route-static vpn-instance VPN-RED 0.0.0.0 0.0.0.0 20.1.1.100
#
return
```

● PE-B 的配置文件

```
#
sysname PE-B
#
ip vpn-instance VPN-BLUE
ipv4-family
route-distinguisher 100:1
vpn-target 100:1 export-extcommunity
vpn-target 100:1 import-extcommunity
#
ip vpn-instance VPN-RED
ipv4-family
route-distinguisher 200:1
vpn-target 200:1 export-extcommunity
vpn-target 200:1 import-extcommunity
#
mpls lsr-id 2.2.2.2
mpls
#
mpls ldp
#
interface GigabitEthernet1/0/0
undo shutdown
```

```
ip binding vpn-instance VPN-BLUE
ip address 10.1.1.2 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.111
#
interface GigabitEthernet2/0/0
undo shutdown
ip binding vpn-instance VPN-RED
ip address 20.1.1.2 255.255.255.0
vrrp vrid 2 virtual-ip 20.1.1.111
vrrp vrid 2 priority 120
#
interface Pos3/0/0
link-protocol ppp
undo shutdown
ip address 192.168.2.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 2.2.2.2 255.255.255.255
#
bgp 100
peer 3.3.3.3 as-number 100
peer 3.3.3.3 connect-interface LoopBack1
#
ipv4-family unicast
undo synchronization
peer 3.3.3.3 enable
#
ipv4-family vpnv4
policy vpn-target
peer 3.3.3.3 enable
#
ipv4-family vpn-instance VPN-BLUE
import-route direct
import-route static
#
ipv4-family vpn-instance VPN-RED
import-route direct
import-route static
#
ospf 1
area 0.0.0.0
network 192.168.2.0 0.0.0.255
network 2.2.2.2 0.0.0.0
#
ip route-static vpn-instance VPN-BLUE 0.0.0.0 0.0.0.0 10.1.1.100
ip route-static vpn-instance VPN-RED 0.0.0.0 0.0.0.0 20.1.1.100
#
return
```

4.14.4 配置 VRRP 快速切换功能示例

本示例中，通过配置 VRRP 备份组监视 BFD 会话，实现主用接口或者链路 Down 时，备用设备承担网络流量。

组网需求



说明

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

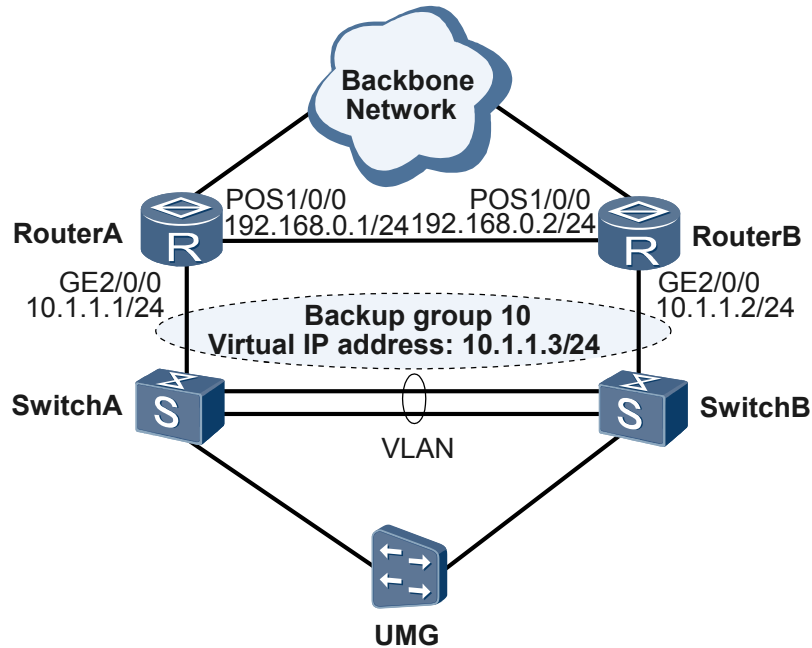
如图 4-8 所示，RouterA、RouterB、SwitchA、SwitchB 和通用媒体网关 UMG 设备组成一个简单的 NGN 承载网。

其中：

- UMG 通过交换机 SwitchA 和 SwitchB 双归属到 RouterA 和 RouterB。
- RouterA 和 RouterB 之间运行 VRRP，RouterA 作为 Master，RouterB 作为 Backup。

要求当 RouterA 发生故障、或 RouterA 与 RouterB 之间的 GE 链路故障时，VRRP 主备切换的时间不超过 1 秒，以实现承载网的快速收敛。

图 4-8 配置 VRRP 快速切换功能组网图



配置思路

采用如下思路实现 VRRP 快速切换：

1. 在 RouterA 和 RouterB 的 GE 接口上配置 BFD Session，同时实现对 RouterA 和下行链路 RouterA—SwitchA—SwitchB—RouterB 的监测。
2. 在作为 Backup 的 RouterB 上配置 VRRP 监视 BFD Session，一旦 BFD Session 的状态变为 Down，RouterB 的优先级增加 40，进行主备切换。

说明

- 本示例只介绍 RouterA 和 RouterB 上的配置。
- 如果只需要实现 RouterA 本身故障时的快速切换，上述配置思路的第一项可以改为在 RouterA 和 RouterB 直连的 POS 接口上配置 BFD Session，第二项不变。本示例不介绍这种配置。

数据准备

为完成此配置例，需准备如下的数据：

- 本地和对端的 BFD 会话标识符
- VRRP 备份组 ID、虚拟 IP 地址
- 路由器在备份组中的优先级

操作步骤

步骤 1 配置 BFD 基本功能

在 RouterA 上配置 BFD Session。

```
<RouterA> system-view
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] bfd atob bind peer-ip 10.1.1.2 interface gigabitethernet 2/0/0
[RouterA-bfd-session-atob] discriminator local 1
[RouterA-bfd-session-atob] discriminator remote 2
[RouterA-bfd-session-atob] min-rx-interval 50
[RouterA-bfd-session-atob] min-tx-interval 50
[RouterA-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
```

在 RouterB 上配置 BFD Session。

```
<RouterB> system-view
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] interface gigabitethernet2/0/0
[RouterB-GigabitEthernet2/0/0] ip address 10.1.1.2 24
[RouterB-GigabitEthernet2/0/0] quit
[RouterB] bfd btoa bind peer-ip 10.1.1.1 interface gigabitethernet 2/0/0
[RouterB-bfd-session-btoa] discriminator local 2
[RouterB-bfd-session-btoa] discriminator remote 1
[RouterB-bfd-session-btoa] min-rx-interval 50
[RouterB-bfd-session-btoa] min-tx-interval 50
[RouterB-bfd-session-btoa] commit
[RouterB-bfd-session-btoa] quit
```

配置完成后，在 RouterA 或 RouterB 上执行 **display bfd session** 命令，可以看到 BFD Session 会话的状态为 Up。以 RouterA 的显示为例。

```
[RouterA] display bfd session all
```

Local	Remote	PeerIPAddress	InterfaceName	State	Type
1	2	10.1.1.2	GigabitEthernet2/0/0	Up	S_IP_IF

Total UP/DOWN Session Number : 1/0

步骤 2 配置 VRRP 快速切换

创建备份组 10，配置 RouterA 在备份组 10 中的优先级为 160，为 Master。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] vrrp vrid 10 virtual-ip 10.1.1.3
[RouterA-GigabitEthernet2/0/0] vrrp vrid 10 priority 160
[RouterA-GigabitEthernet2/0/0] quit
```

创建备份组 10，配置 RouterB 在备份组 10 中的优先级为 140，为 Backup。

```
[RouterB] interface gigabitethernet2/0/0
[RouterB-GigabitEthernet2/0/0] vrrp vrid 10 virtual-ip 10.1.1.3
[RouterB-GigabitEthernet2/0/0] vrrp vrid 10 priority 140
```

在 Backup 侧配置监视 BFD Session 的状态，如果 BFD Session 状态变为 Down，RouterB 的 VRRP 优先级增加 40。

```
[RouterB-GigabitEthernet2/0/0] vrrp vrid 10 track bfd-session 2 increased 40
[RouterB-GigabitEthernet2/0/0] quit
```

配置完成后，在 RouterA 或 RouterB 上执行 **display vrrp** 命令，可以看到 RouterA 是 Master，RouterB 是 Backup。在 RouterB 上还能看到对 BFD Session 的监测设置以及 BFD Session 的当前状态。

```
[RouterA] display vrrp
GigabitEthernet2/0/0 | Virtual Router 10
  state           : Master
  Virtual IP      : 10.1.1.3
  Master IP       : 10.1.1.1
  PriorityRun      : 160
  PriorityConfig   : 160
  MasterPriority   : 160
  Preempt         : YES   Delay Time : 0
  TimerRun        : 1
  TimerConfig     : 1
  Auth Type       : NONE
  Virtual Mac     : 0000-5e00-0110
  Check TTL       : YES
  Config type     : normal-vrrp
  Create time     : 2010-06-22 17:32:56
  Last change time : 2010-06-22 17:33:00
[RouterB] display vrrp
GigabitEthernet2/0/0 | Virtual Router 10
  state           : Backup
  Virtual IP      : 10.1.1.3
  Master IP       : 10.1.1.2
  PriorityRun      : 140
  PriorityConfig   : 140
  MasterPriority   : 160
  Preempt         : YES   Delay Time : 0
  TimerRun        : 1
  TimerConfig     : 1
  Auth Type       : NONE
  Virtual Mac     : 0000-5e00-0110
  Check TTL       : YES
  Config type     : normal-vrrp
  Track BFD       : 2 Priority increased : 40
  BFD-Session State : UP
  Create time     : 2010-06-22 17:33:00
  Last change time : 2010-06-22 17:33:04
```

步骤 3 验证配置结果

对 RouterA 的接口 GE2/0/0 执行 **shutdown** 操作，模拟链路故障。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] shutdown
```

在 RouterB 上可以看到：VRRP 接收到 BFD 的故障报告后进行主备切换。

```
%May 10 15:48:30 2006 RouterB BFD/5/BFD:Slot=1;IO(1) BFD Session(Discr:2) FSM Change To Down(Detect)
%May 10 15:48:30 2006 RouterB VRRP/5/BfdWarning:
  Virtual Router 10 | BFD-SESSION 2 : BFD_STATE_UP --> BFD_STATE_DOWN
%May 10 15:48:30 2006 RouterB VRRP/5/StateWarning:
  GigabitEthernet2/0/0 | Virtual Router 10 : BACKUP --> MASTER
```

此时在 RouterA 上执行 **display vrrp** 命令，可以看到 RouterA 的状态变为 Initialize。

```
[RouterA] display vrrp
GigabitEthernet2/0/0 | Virtual Router 10
  state           : Initialize
  Virtual IP      : 10.1.1.3
  Master IP       : 10.1.1.1
  PriorityRun      : 160
  PriorityConfig   : 160
  MasterPriority   : 0
  Preempt         : YES   Delay Time : 0
  TimerRun        : 1
  TimerConfig     : 1
```

```
Auth Type      : NONE
Virtual Mac    : 0000-5e00-0110
Check TTL     : YES
Config type    : normal-vrrp
Create time    : 2010-06-22 17:32:56
Last change time : 2010-06-22 17:33:06
```

在 RouterB 上执行 **display vrrp** 命令，可以看到 RouterB 的状态切换成 Master，BFD Session 的状态变为 Down。

```
[RouterB] display vrrp
GigabitEthernet2/0/0 | Virtual Router 10
  state                : Master
  Virtual IP           : 10.1.1.3
  Master IP            : 10.1.1.2
  PriorityRun           : 180
  PriorityConfig        : 140
  MasterPriority        : 180
  Preempt              : YES      Delay Time : 0
  TimerRun              : 1
  TimerConfig          : 1
  Auth Type            : NONE
  Virtual Mac          : 0000-5e00-0110
  Check TTL            : YES
  Config type          : normal-vrrp
  Track BFD            : 2      Priority increased : 40
  BFD-Session State    : DOWN
  Create time          : 2010-06-22 17:33:00
  Last change time     : 2010-06-22 17:33:06
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 bfd
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 10 virtual-ip 10.1.1.3
 vrrp vrid 10 priority 160
#
 bfd atob bind peer-ip 10.1.1.2 interface gigabitethernet2/0/0
 discriminator local 1
 discriminator remote 2
 min-tx-interval 50
 min-rx-interval 50
 commit
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 bfd
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 10 virtual-ip 10.1.1.3
 vrrp vrid 10 priority 140
 vrrp vrid 10 track bfd-session 2 increased 40
#
```

```
bfd toa bind peer-ip 10.1.1.1 interface gigabitethernet2/0/0
discriminator local 2
discriminator remote 1
min-tx-interval 50
min-rx-interval 50
commit
#
return
```

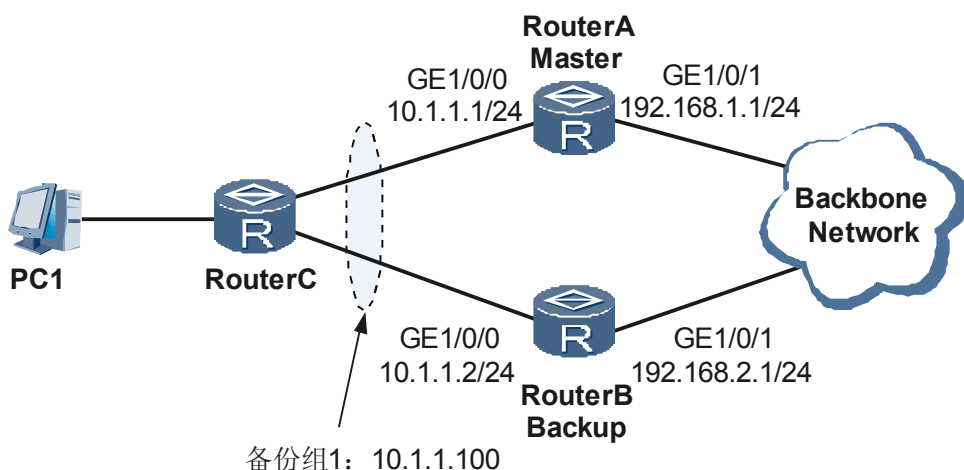
4.14.5 配置 VRRP 快速切换示例（使用单臂 ECHO 功能）

本示例中，通过在支持 BFD 功能的一端设备上配置单臂 ECHO 功能，实现快速检测和监控网络中的直连链路。

组网需求

如图 4-9 所示，RouterA 和 RouterB 支持 BFD 功能，RouterC 不支持 BFD 功能。为了快速检测 RouterA 与 RouterC 或者 RouterB 与 RouterC 之间的直连链路，需要使用 BFD 功能。此时，可以在 RouterA 上配置单臂 ECHO 功能的 BFD 会话，检测 RouterA 与 RouterC 之间的直连链路；在 RouterB 上配置单臂 ECHO 功能的 BFD 会话，检测 RouterB 与 RouterC 之间的直连链路。

图 4-9 配置 VRRP 快速切换示例（使用单臂 ECHO 功能的 BFD）组网图



配置思路

采用如下思路配置三层物理链路单跳检测：

1. 分别在 RouterA 和 RouterB 上配置单臂 ECHO 功能的 BFD 会话，检测 RouterA 与 RouterC、RouterB 与 RouterC 之间的直连链路；在 RouterA 和 RouterB 上配置 Peer BFD 会话，检测 RouterA 与 RouterB 之间的直连链路。
2. 在 RouterA 和 RouterB 上配置 VRRP 备份组。其中，RouterA 为 Master 设备，RouterB 为 Backup 设备。此 VRRP 备份组通过监视 BFD 会话的状态来实现快速切换。

数据准备

为完成此配置例，需要准备如下数据：

- BFD 会话的名称
- BFD 会话的标识符
- VRRP 备份组号
- VRRP 备份组的虚拟 IP 地址
- 设备在 VRRP 备份组中的优先级

操作步骤

步骤 1 RouterA、RouterB 和 RouterC 之间采用 OSPF 协议进行互连（略）。

步骤 2 配置 RouterA 和 RouterB 各接口的 IP 地址

配置 RouterA 的接口 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] undo shutdown
[RouterA-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] undo shutdown
[RouterA-GigabitEthernet1/0/1] ip address 192.168.1.1 24
[RouterA-GigabitEthernet1/0/1] quit
```

配置 RouterB 的接口 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] undo shutdown
[RouterB-GigabitEthernet1/0/0] ip address 10.1.1.2 24
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] undo shutdown
[RouterB-GigabitEthernet1/0/1] ip address 192.168.2.1 24
[RouterB-GigabitEthernet1/0/1] quit
```

步骤 3 在 RouterC 上配置 VLANIF 接口

```
<HUAWEI> system-view
[HUAWEI] sysname RouterC
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] undo shutdown
[RouterC-GigabitEthernet1/0/0] portswitch
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface gigabitethernet 2/0/0
[RouterC-GigabitEthernet2/0/0] undo shutdown
[RouterC-GigabitEthernet2/0/0] portswitch
[RouterC-GigabitEthernet2/0/0] quit
[HUAWEI] vlan 10
[HUAWEI-vlan10] port gigabitethernet 1/0/0
[HUAWEI-vlan10] port gigabitethernet 2/0/0
[HUAWEI-vlan10] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ip address 10.1.1.3 24
[HUAWEI-Vlanif10] quit
```

步骤 4 配置单臂 ECHO 功能的 BFD 会话

配置 RouterA。


```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atoc bind peer-ip 10.1.1.3 interface gigabitEthernet1/0/0 one-arm-echo
[RouterA-bfd-session-atoc] discriminator local 1
[RouterA-bfd-session-atoc] min-echo-rx-interval 100
[RouterA-bfd-session-atoc] commit
[RouterA-bfd-session-atoc] quit
```

配置 RouterB。

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bfd btoc bind peer-ip 10.1.1.3 interface gigabitEthernet1/0/0 one-arm-echo
[RouterB-bfd-session-atoc] discriminator local 2
[RouterB-bfd-session-atoc] min-echo-rx-interval 100
[RouterB-bfd-session-atoc] commit
[RouterB-bfd-session-atoc] quit
```

配置完成后，在 RouterA 或者 RouterB 上执行 **display bfd session all verbose** 命令，可以看到单臂 ECHO 功能的 BFD 会话的状态为 Up。以 RouterA 的显示为例。

```
[RouterA] display bfd session all verbose
```

Session MIndex : 256	(One Hop) State : Up	Name : atob
Local Discriminator : 1	Remote Discriminator : -	
Session Detect Mode : Asynchronous Mode Without Echo Function		
BFD Bind Type : Interface(GigabitEthernet1/0/0)		
Bind Session Type : Static		
Bind Peer IP Address : 10.1.1.3		
NextHop Ip Address : 10.1.1.3		
Bind Interface : GigabitEthernet1/0/0		
FSM Board Id : 0	TOS-EXP : 7	
Echo Rx Interval (ms) : 100		
Actual Tx Interval (ms): 1000	Actual Rx Interval (ms): 100	
Local Detect Multi : 3	Detect Interval (ms) : 3000	
Echo Passive : Disable	Acl Number : -	
Destination Port : 3784	TTL : 255	
Proc Interface Status : Disable	Process PST : Disable	
WTR Interval (ms) : -	Local Demand Mode : Disable	
Active Multi : 3		
Last Local Diagnostic : Control Detection Time Expired		
Bind Application : No Application Bind		
Session TX TmrID : 87	Session Detect TmrID : 88	
Session Init TmrID : -	Session WTR TmrID : -	
Session Echo Tx TmrID : -		
PDT Index : FSM-0 RCV-0 IF-0 TOKEN-0		
Session Description : -		

Total UP/DOWN Session Number : 1/0

步骤 5 配置 Peer BFD 功能。

配置 RouterA。

```
[RouterA] bfd peer bind peer-ip 10.1.1.2 interface gigabitEthernet1/0/0
[RouterA-bfd-session-peer] discriminator local 3
[RouterA-bfd-session-peer] discriminator remote 4
[RouterA-bfd-session-peer] commit
[RouterA-bfd-session-peer] quit
```

配置 RouterB。

```
[RouterB] bfd peer bind peer-ip 10.1.1.1 interface gigabitEthernet1/0/0
[RouterB-bfd-session-peer] discriminator local 4
[RouterB-bfd-session-peer] discriminator remote 3
[RouterB-bfd-session-peer] commit
```

```
[RouterB-bfd-session-peer] quit
```

配置完成后，在 RouterA 或者 RouterB 上执行 **display bfd session all verbose** 命令，可以看到 BFD 会话的状态为 Up。以 RouterA 的显示为例。

```
[RouterA] display bfd session all verbose
```

```
-----
Session MIndex : 16384      (One Hop) State : Up      Name : peer
-----
Local Discriminator      : 3      Remote Discriminator      : 4
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type            : Interface(GigabitEthernet1/0/0)
Bind Session Type        : Static
Bind Peer IP Address     : 10.1.1.2
NextHop Ip Address       : 10.1.1.2
Bind Interface           : GigabitEthernet1/0/0
FSM Board Id             : 0      TOS-EXP                  : 7
Min Tx Interval (ms)     : 10      Min Rx Interval (ms)    : 10
Actual Tx Interval (ms)  : 10      Actual Rx Interval (ms) : 10
Local Detect Multi       : 3      Detect Interval (ms)    : 30
Echo Passive             : Disable  Acl Number              : -
Destination Port         : 3784     TTL                     : 255
Proc Interface Status    : Disable  Process PST              : Disable
WTR Interval (ms)       : -
Active Multi             : 3
Last Local Diagnostic    : Control Detection Time Expired
Bind Application         : No Application Bind
Session TX TmrID         : -      Session Detect TmrID    : -
Session Init TmrID       : -      Session WTR TmrID       : -
Session Echo Tx TmrID    : -
PDT Index                : FSM-B030000 | RCV-0 | IF-B030000 | TOKEN-0
Session Description      : -
-----
```

```
Total UP/DOWN Session Number : 1/0
```

步骤6 配置管理 VRRP 备份组

在 RouterA 上配置备份组 1，RouterA 在备份组中的优先级为 160，确保 RouterA 为 Master 设备。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.1.1.100
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 priority 160
[RouterA-GigabitEthernet1/0/0] admin-vrrp vrid 1
[RouterA-GigabitEthernet1/0/0] quit
```

在 RouterB 上配置备份组 1，RouterB 在备份组中的优先级为 120，确保 RouterB 为 Backup 设备。

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.1.1.100
[RouterB-GigabitEthernet1/0/0] vrrp vrid 1 priority 140
[RouterB-GigabitEthernet1/0/0] admin-vrrp vrid 1
[RouterB-GigabitEthernet1/0/0] quit
```

配置完成后，在 RouterA 或者 RouterB 上执行 **display vrrp** 命令，可以看到 Router 是 Master 设备，RouterB 是 Backup 设备。

```
[RouterA] display vrrp
GigabitEthernet1/0/0 | Virtual Router 1
  State                : Master
  Virtual IP           : 10.1.1.100
  PriorityRun           : 160
  PriorityConfig        : 160
  MasterPriority        : 160
  Preempt              : YES      Delay Time : 0
  TimerRun             : 1
```

```
TimerConfig      : 1
Auth Type        : NONE
Virtual Mac      : 0000-5e00-0101
Check TTL        : YES
Config type      : normal-vrrp
Config track link-bfd down-number : 0
[RouterB] display vrrp
GigabitEthernet1/0/0 | Virtual Router 1
State            : Backup
Virtual IP       : 10.1.1.100
PriorityRun      : 120
PriorityConfig   : 120
MasterPriority   : 160
Preempt         : YES      Delay Time : 0
TimerRun        : 1
TimerConfig     : 1
Auth Type       : NONE
Virtual Mac     : 0000-5e00-0101
Check TTL       : YES
Config type     : normal-vrrp
Config track link-bfd down-number : 0
```

步骤 7 配置 VRRP 备份组监视 BFD 会话

配置 RouterA。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 track bfd-session 1 link
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 track bfd-session 3 peer
[RouterA-GigabitEthernet1/0/0] vrrp trigger route
[RouterA-GigabitEthernet1/0/0] quit
```

配置 RouterB。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 track bfd-session 2 link
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 track bfd-session 4 peer
[RouterA-GigabitEthernet1/0/0] vrrp trigger route
[RouterA-GigabitEthernet1/0/0] quit
```

步骤 8 验证配置结果

对 RouterA 的 GE1/0/0 执行 **shutdown** 操作，模拟链路故障。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] shutdown
[RouterA-GigabitEthernet1/0/0] quit
```

此时，在 RouterA 上执行 **display vrrp** 命令，可以看到 VRRP 备份组的状态变为 Initialize，BFD 会话的状态变为 Down。

```
[RouterA] display vrrp
GigabitEthernet1/0/0 | Virtual Router 1
State                : Initialize
Virtual IP           : 10.1.1.100
PriorityRun          : 160
PriorityConfig       : 160
MasterPriority       : 0
Preempt             : YES      Delay Time : 0
TimerRun            : 1
TimerConfig         : 1
Auth Type           : NONE
Virtual Mac         : 0000-5e00-0101
Check TTL           : YES
Config type         : normal-vrrp
Config track link-bfd down-number : 0
Track BFD           : 1      Type : link
BFD-session state   : DOWN
Track BFD           : 3      Type : peer
BFD-session state   : DOWN
```

此时，在 RouterB 上执行 **display vrrp** 命令，可以看到 VRRP 备份组的状态变为 Master，BFD 会话的状态变为 Down。

```
[RouterA] display vrrp
GigabitEthernet1/0/0 | Virtual Router 1
  State           : Master
  Virtual IP      : 10.1.1.100
  PriorityRun     : 170
  PriorityConfig  : 120
  MasterPriority  : 170
  Preempt        : YES      Delay Time : 0
  TimerRun       : 1
  TimerConfig    : 1
  Auth Type      : NONE
  Virtual Mac    : 0000-5e00-0101
  Check TTL      : YES
  Config type    : normal-vrrp
  Config track link-bfd down-number : 0
  Track BFD      : 2      Type : link
  BFD-session state : DOWN
  Track BFD      : 4      Tpye : peer
  BFD-session state : DOWN
```

----结束

配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
bfd
#
interface gigabitethernet 1/0/0
undo shutdown
ip address 10.1.1.1 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.100
vrrp vrid 1 priority 160
admin-vrrp vrid 1
vrrp vrid 1 track bfd-session 1 link
vrrp vrid 1 track bfd-session 3 peer
vrrp trigger route
#
interface gigabitethernet 1/0/1
undo shutdown
ip address 192.168.1.1 255.255.255.0
#
bfd atoc bind peer-ip 10.1.1.3 interface gigabitEthernet1/0/0 one-arm-echo
discriminator local 1
min-echo-rx-interval 100
commit
#
bfd peer bind peer-ip 10.1.1.2 interface gigabitEthernet1/0/0
discriminator local 3
discriminator remote 4
commit
#
ospf 1
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 192.168.1.0 0.0.0.255
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
```

```
bfd
#
interface gigabitethernet 1/0/0
undo shutdown
ip address 10.1.1.2 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.100
vrrp vrid 1 priority 140
admin-vrrp vrid 1
vrrp vrid 1 track bfd-session 2 link
vrrp vrid 1 track bfd-session 4 peer
vrrp trigger route
#
interface gigabitethernet 1/0/1
undo shutdown
ip address 192.168.2.1 255.255.255.0
#
bfd btoc bind peer-ip 10.1.1.3 interface gigabitEthernet1/0/0 one-arm-echo
discriminator local 2
min-echo-rx-interval 100
commit
#
bfd peer bind peer-ip 10.1.1.1 interface gigabitEthernet1/0/0
discriminator local 4
discriminator remote 3
commit
#
ospf 1
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 192.168.2.0 0.0.0.255
#
return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
interface Vlanif10
ip address 10.1.1.3 255.255.255.0
#
interface gigabitethernet 1/0/0
portswitch
undo shutdown
port default vlan 10
#
interface gigabitethernet 2/0/0
portswitch
undo shutdown
port default vlan 10
```

4.14.6 配置 VRRP 快速切换（使用 BFD Sampling）

本示例中，通过配置 BFD Sampling 方式的 BFD 检测，解决 NPE 和 PE 之间无法直接建立 Link BFD 会话的问题。

组网需求

说明

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

如图 4-10 所示。CE 通过 VPLS 汇聚网络接入 NPE 的 QinQ 终结子接口。

NPE 上配置管理 VRRP 和业务 VRRP，并通过管理 VRRP 监视 BFD 会话来完成快速切换。NPE 之间建立 Peer BFD 会话。

本例中，网络限制条件：

- VPLS 汇聚网络属于其他的运营商，因此 NPE1 与 PE1、NPE2 与 PE2 之间无法直接建立 Link BFD。
- PE1 与 PE2 本身不支持 BFD 功能。

此时可以配置使用 BFD Sampling 方式的 VRRP 快速切换功能。

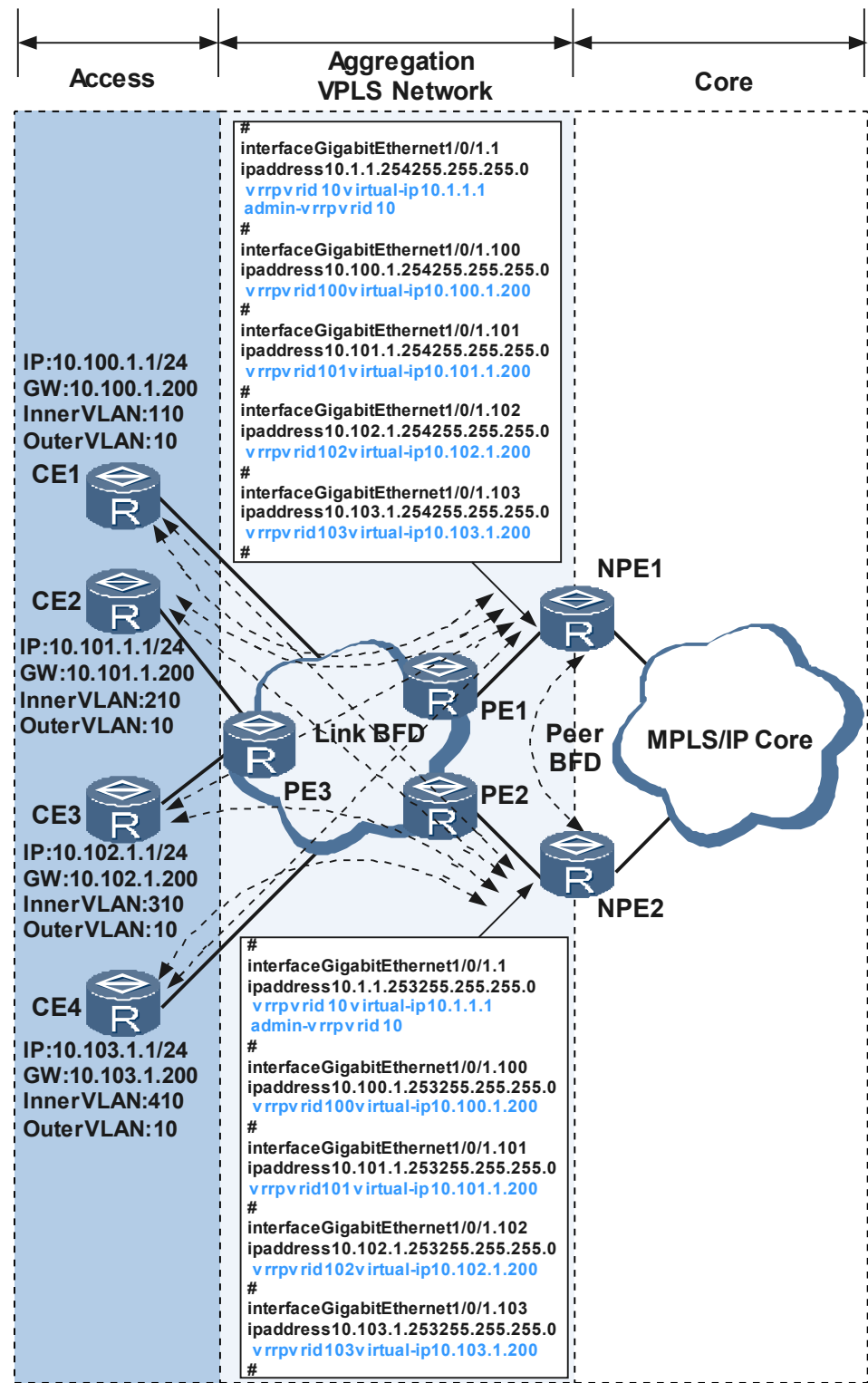
 说明

BFD Sampling: NPE 与所有的 CE 直接建立 Link BFD 的检测方式。

对于 NPE 而言：

- NPE1 和 NPE2 通过 VPLS 汇聚网络侧接口 GE1/0/1，建立管理 VRRP、业务 VRRP 和 Peer BFD。
- 每个 NPE 通过 VPLS 汇聚网络侧接口 GE1/0/1 与 CE 之间直接建立 4 个 Link BFD 会话，管理 VRRP 同时监视这 4 个 Link BFD 会话的状态。当管理 VRRP 监视的 Link BFD 会话有 2 条或者 2 条以上的 Link BFD 会话状态变为 Down，管理 VRRP 进行主备快速切换。

图 4-10 配置 VRRP 快速切换（使用 BFD Sampling）组网图



配置思路

采用如下的思路配置 VRRP 快速切换（使用 BFD Sampling）的基本功能：

1. 在 NPE 上配置 QinQ 终结子接口的基本功能。
2. 在 NPE 的 QinQ 终结子接口上配置管理 VRRP 和业务 VRRP，并将业务 VRRP 与管理 VRRP 绑定。
3. 配置 NPE 之间，NPE 与 CE 之间的 BFD 功能。
4. 配置管理 VRRP 通过 BFD Sampling 完成快速切换。

数据准备

为完成此配置例，需准备如下的数据：

- VRRP 备份组 ID、虚拟 IP 地址。
- VRRP 备份组中的优先级。

操作步骤

步骤 1 配置 QinQ 终结子接口的基本功能

 说明

以下仅给出 NPE 的配置步骤，[图 4-10](#) 中 CE 的 BFD 功能以及 VPLS 汇聚网络的配置步骤请参见《HUAWEI NetEngine80E/40E 路由器 配置指南-可靠性》和《HUAWEI NetEngine80E/40E 路由器 配置指南-VPN》中的相关内容。

配置 NPE1。

```
<HUAWEI> system-view
[HUAWEI] sysname NPE1
[NPE1] interface gigabitethernet1/0/1
[NPE1-GigabitEthernet1/0/1] mode user-termination
[NPE1-GigabitEthernet1/0/1] undo shutdown
[NPE1-GigabitEthernet1/0/1] quit
[NPE1] interface gigabitethernet1/0/1.1
[NPE1-GigabitEthernet1/0/1.1] control-vid 1 qinq-termination
[NPE1-GigabitEthernet1/0/1.1] qinq termination pe-vid 10 ce-vid 1 to 100
[NPE1-GigabitEthernet1/0/1.1] ip address 10.1.1.254 24
[NPE1-GigabitEthernet1/0/1.1] arp broadcast enable
[NPE1-GigabitEthernet1/0/1.1] quit
[NPE1] interface gigabitethernet1/0/1.100
[NPE1-GigabitEthernet1/0/1.100] control-vid 100 qinq-termination
[NPE1-GigabitEthernet1/0/1.100] qinq termination pe-vid 10 ce-vid 101 to 200
[NPE1-GigabitEthernet1/0/1.100] ip address 10.100.1.254 24
[NPE1-GigabitEthernet1/0/1.100] arp broadcast enable
[NPE1-GigabitEthernet1/0/1.100] quit
[NPE1] interface gigabitethernet1/0/1.101
[NPE1-GigabitEthernet1/0/1.101] control-vid 101 qinq-termination
[NPE1-GigabitEthernet1/0/1.101] qinq termination pe-vid 10 ce-vid 201 to 300
[NPE1-GigabitEthernet1/0/1.101] ip address 10.101.1.254 24
[NPE1-GigabitEthernet1/0/1.101] arp broadcast enable
[NPE1-GigabitEthernet1/0/1.101] quit
[NPE1] interface gigabitethernet1/0/1.102
[NPE1-GigabitEthernet1/0/1.102] control-vid 102 qinq-termination
[NPE1-GigabitEthernet1/0/1.102] qinq termination pe-vid 10 ce-vid 301 to 400
[NPE1-GigabitEthernet1/0/1.102] ip address 10.102.1.254 24
[NPE1-GigabitEthernet1/0/1.102] arp broadcast enable
[NPE1-GigabitEthernet1/0/1.102] quit
[NPE1] interface gigabitethernet1/0/1.103
[NPE1-GigabitEthernet1/0/1.103] control-vid 103 qinq-termination
[NPE1-GigabitEthernet1/0/1.103] qinq termination pe-vid 10 ce-vid 401 to 500
[NPE1-GigabitEthernet1/0/1.103] ip address 10.103.1.254 24
[NPE1-GigabitEthernet1/0/1.103] arp broadcast enable
[NPE1-GigabitEthernet1/0/1.103] quit
```

配置 NPE2。


```
<HUAWEI> system-view
[HUAWEI] sysname NPE2
[NPE2] interface gigabitethernet1/0/1
[NPE2-GigabitEthernet1/0/1] mode user-termination
[NPE2-GigabitEthernet1/0/1] undo shutdown
[NPE2-GigabitEthernet1/0/1] quit
[NPE2] interface gigabitethernet1/0/1.1
[NPE2-GigabitEthernet1/0/1.1] control-vid 1 qinq-termination
[NPE2-GigabitEthernet1/0/1.1] qinq termination pe-vid 10 ce-vid 1 to 100
[NPE2-GigabitEthernet1/0/1.1] ip address 10.1.1.253 24
[NPE2-GigabitEthernet1/0/1.1] arp broadcast enable
[NPE2-GigabitEthernet1/0/1.1] quit
[NPE2] interface gigabitethernet1/0/1.100
[NPE2-GigabitEthernet1/0/1.100] control-vid 100 qinq-termination
[NPE2-GigabitEthernet1/0/1.100] qinq termination pe-vid 10 ce-vid 101 to 200
[NPE2-GigabitEthernet1/0/1.100] ip address 10.100.1.253 24
[NPE2-GigabitEthernet1/0/1.100] arp broadcast enable
[NPE2-GigabitEthernet1/0/1.100] quit
[NPE2] interface gigabitethernet1/0/1.101
[NPE2-GigabitEthernet1/0/1.101] control-vid 101 qinq-termination
[NPE2-GigabitEthernet1/0/1.101] qinq termination pe-vid 10 ce-vid 201 to 300
[NPE2-GigabitEthernet1/0/1.101] ip address 10.101.1.253 24
[NPE2-GigabitEthernet1/0/1.101] arp broadcast enable
[NPE2-GigabitEthernet1/0/1.101] quit
[NPE2] interface gigabitethernet1/0/1.102
[NPE2-GigabitEthernet1/0/1.102] control-vid 102 qinq-termination
[NPE2-GigabitEthernet1/0/1.102] qinq termination pe-vid 10 ce-vid 301 to 400
[NPE2-GigabitEthernet1/0/1.102] ip address 10.102.1.253 24
[NPE2-GigabitEthernet1/0/1.102] arp broadcast enable
[NPE2-GigabitEthernet1/0/1.102] quit
[NPE2] interface gigabitethernet1/0/1.103
[NPE2-GigabitEthernet1/0/1.103] control-vid 103 qinq-termination
[NPE2-GigabitEthernet1/0/1.103] qinq termination pe-vid 10 ce-vid 401 to 500
[NPE2-GigabitEthernet1/0/1.103] ip address 10.103.1.253 24
[NPE2-GigabitEthernet1/0/1.103] arp broadcast enable
[NPE2-GigabitEthernet1/0/1.103] quit
```

说明

在 QinQ 终结子接口上配置 IP 地址后，建议配置 **arp broadcast enable** 命令，否则 QinQ 终结子接口之间无法 Ping 通。

完成此步配置后，NPE 上属于同一网段的 QinQ 终结子接口，通过 VPLS 网络，可以相互 Ping 通，从而说明 NPE 之间的链路工作正常。以 NPE1 和 NPE2 互相 Ping 为例。

管理 VRRP 所在的接口可以互相 Ping 通。

```
[NPE1] ping 10.1.1.253
PING 10.1.1.253: 56 data bytes, press CTRL_C to break
  Reply from 10.1.1.253: bytes=56 Sequence=1 ttl=255 time=160 ms
  Reply from 10.1.1.253: bytes=56 Sequence=2 ttl=255 time=90 ms
  Reply from 10.1.1.253: bytes=56 Sequence=3 ttl=255 time=160 ms
  Reply from 10.1.1.253: bytes=56 Sequence=4 ttl=255 time=180 ms
  Reply from 10.1.1.253: bytes=56 Sequence=5 ttl=255 time=120 ms

--- 10.1.1.253 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 90/142/180 ms
```

业务 VRRP 所在的接口可以互相 Ping 通。

```
[NPE1] ping 10.100.1.253
PING 10.100.1.253: 56 data bytes, press CTRL_C to break
  Reply from 10.100.1.253: bytes=56 Sequence=1 ttl=255 time=90 ms
  Reply from 10.100.1.253: bytes=56 Sequence=2 ttl=255 time=100 ms
  Reply from 10.100.1.253: bytes=56 Sequence=3 ttl=255 time=190 ms
  Reply from 10.100.1.253: bytes=56 Sequence=4 ttl=255 time=100 ms
  Reply from 10.100.1.253: bytes=56 Sequence=5 ttl=255 time=90 ms
```

```
--- 10.100.1.253 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 90/114/190 ms
```

此外，NPE 与属于同一网段 CE 也可以 Ping 通，从而说明 NPE 与 CE 之间的链路工作正常。以 NPE1、NPE2 与 CE1 互相 Ping 为例。

```
[NPE1] ping 10.100.1.1
PING 10.100.1.1: 56 data bytes, press CTRL_C to break
  Reply from 10.100.1.1: bytes=56 Sequence=1 ttl=255 time=180 ms
  Reply from 10.100.1.1: bytes=56 Sequence=2 ttl=255 time=160 ms
  Reply from 10.100.1.1: bytes=56 Sequence=3 ttl=255 time=150 ms
  Reply from 10.100.1.1: bytes=56 Sequence=4 ttl=255 time=150 ms
  Reply from 10.100.1.1: bytes=56 Sequence=5 ttl=255 time=120 ms

--- 10.100.1.1 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 120/152/180 ms
```

```
[NPE2] ping 10.100.1.1
PING 10.100.1.1: 56 data bytes, press CTRL_C to break
  Reply from 10.100.1.1: bytes=56 Sequence=1 ttl=255 time=190 ms
  Reply from 10.100.1.1: bytes=56 Sequence=2 ttl=255 time=120 ms
  Reply from 10.100.1.1: bytes=56 Sequence=3 ttl=255 time=130 ms
  Reply from 10.100.1.1: bytes=56 Sequence=4 ttl=255 time=100 ms
  Reply from 10.100.1.1: bytes=56 Sequence=5 ttl=255 time=70 ms

--- 10.100.1.1 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 70/122/190 ms
```

步骤 2 配置 QinQ 终结子接口的 VRRP 基本功能

配置 NPE1，其中在子接口 GE1/0/1.1 上配置管理 VRRP，其 VRID 是 10，其他子接口上配置业务 VRRP。

```
[NPE1] interface gigabitethernet1/0/1.1
[NPE1-GigabitEthernet1/0/1.1] qinq vrrp pe-vid 10 ce-vid 100
[NPE1-GigabitEthernet1/0/1.1] vrrp vrid 10 virtual-ip 10.1.1.1
[NPE1-GigabitEthernet1/0/1.1] vrrp vrid 10 priority 120
[NPE1-GigabitEthernet1/0/1.1] admin-vrrp vrid 10
[NPE1-GigabitEthernet1/0/1.1] quit
[NPE1] interface gigabitethernet1/0/1.100
[NPE1-GigabitEthernet1/0/1.100] qinq vrrp pe-vid 10 ce-vid 101
[NPE1-GigabitEthernet1/0/1.100] vrrp vrid 100 virtual-ip 10.100.1.200
[NPE1-GigabitEthernet1/0/1.100] quit
[NPE1] interface gigabitethernet1/0/1.101
[NPE1-GigabitEthernet1/0/1.101] qinq vrrp pe-vid 10 ce-vid 201
[NPE1-GigabitEthernet1/0/1.101] vrrp vrid 101 virtual-ip 10.101.1.200
[NPE1-GigabitEthernet1/0/1.101] quit
[NPE1] interface gigabitethernet1/0/1.102
[NPE1-GigabitEthernet1/0/1.102] qinq vrrp pe-vid 10 ce-vid 301
[NPE1-GigabitEthernet1/0/1.102] vrrp vrid 102 virtual-ip 10.102.1.200
[NPE1-GigabitEthernet1/0/1.102] quit
[NPE1] interface gigabitethernet1/0/1.103
[NPE1-GigabitEthernet1/0/1.103] qinq vrrp pe-vid 10 ce-vid 401
[NPE1-GigabitEthernet1/0/1.103] vrrp vrid 103 virtual-ip 10.103.1.200
[NPE1-GigabitEthernet1/0/1.103] quit
```

配置 NPE2，其中在子接口 GE1/0/1.1 上配置管理 VRRP，其 VRID 是 10，其他子接口上配置业务 VRRP。

```
[NPE2] interface gigabitethernet1/0/1.1
[NPE2-GigabitEthernet1/0/1.1] qinq vrrp pe-vid 10 ce-vid 100
[NPE2-GigabitEthernet1/0/1.1] vrrp vrid 10 virtual-ip 10.1.1.1
[NPE2-GigabitEthernet1/0/1.1] admin-vrrp vrid 10
[NPE2-GigabitEthernet1/0/1.1] quit
[NPE2] interface gigabitethernet1/0/1.100
[NPE2-GigabitEthernet1/0/1.100] qinq vrrp pe-vid 10 ce-vid 101
[NPE2-GigabitEthernet1/0/1.100] vrrp vrid 100 virtual-ip 10.100.1.200
[NPE2-GigabitEthernet1/0/1.100] quit
[NPE2] interface gigabitethernet1/0/1.101
[NPE2-GigabitEthernet1/0/1.101] qinq vrrp pe-vid 10 ce-vid 201
[NPE2-GigabitEthernet1/0/1.101] vrrp vrid 101 virtual-ip 10.101.1.200
[NPE2-GigabitEthernet1/0/1.101] quit
[NPE2] interface gigabitethernet1/0/1.102
[NPE2-GigabitEthernet1/0/1.102] qinq vrrp pe-vid 10 ce-vid 301
[NPE2-GigabitEthernet1/0/1.102] vrrp vrid 102 virtual-ip 10.102.1.200
[NPE2-GigabitEthernet1/0/1.102] quit
[NPE2] interface gigabitethernet1/0/1.103
[NPE2-GigabitEthernet1/0/1.103] qinq vrrp pe-vid 10 ce-vid 401
[NPE2-GigabitEthernet1/0/1.103] vrrp vrid 103 virtual-ip 10.103.1.200
[NPE2-GigabitEthernet1/0/1.103] quit
```

完成上述配置后，在 NPE 上执行 **display vrrp brief** 命令，可以看到：

NPE1 上：

- VRID 为 10 的 VRRP，“State”是 Master，“Type”是 Admin。
- 其他 VRID 的 VRRP，“Type”是 Normal。

```
[NPE1] display vrrp brief
VRID   State      Interface      Type      Virtual IP
-----
10     Master      GE1/0/1.1     Admin     10.1.1.1
100    Master      GE1/0/1.100   Normal    10.100.1.200
101    Master      GE1/0/1.101   Normal    10.101.1.200
102    Master      GE1/0/1.102   Normal    10.102.1.200
103    Master      GE1/0/1.103   Normal    10.103.1.200
```

NPE2 上：

- VRID 为 10 的 VRRP，“State”是 Backup，“Type”是 Admin。
- 其他 VRID 的 VRRP，“Type”是 Normal。

```
[NPE2] display vrrp brief
VRID   State      Interface      Type      Virtual IP
-----
10     Backup      GE1/0/1.1     Admin     10.1.1.1
100    Backup      GE1/0/1.100   Normal    10.100.1.200
101    Backup      GE1/0/1.101   Normal    10.101.1.200
102    Backup      GE1/0/1.102   Normal    10.102.1.200
103    Backup      GE1/0/1.103   Normal    10.103.1.200
```

步骤 3 配置业务 VRRP 与管理 VRRP 的绑定关系

配置 NPE1。

```
[NPE1] interface gigabitethernet1/0/1.100
[NPE1-GigabitEthernet1/0/1.100] vrrp vrid 100 track admin-vrrp interface gigabitethernet1/0/1.1
vrid 10 unflowdown
[NPE1-GigabitEthernet1/0/1.100] quit
[NPE1] interface gigabitethernet1/0/1.101
[NPE1-GigabitEthernet1/0/1.101] vrrp vrid 101 track admin-vrrp interface gigabitethernet1/0/1.1
vrid 10 unflowdown
[NPE1-GigabitEthernet1/0/1.101] quit
[NPE1] interface gigabitethernet1/0/1.102
[NPE1-GigabitEthernet1/0/1.102] vrrp vrid 102 track admin-vrrp interface gigabitethernet1/0/1.1
vrid 10 unflowdown
[NPE1-GigabitEthernet1/0/1.102] quit
[NPE1] interface gigabitethernet1/0/1.103
```

```
[NPE1-GigabitEthernet1/0/1.103] vrrp vrid 103 track admin-vrrp interface gigabitethernet1/0/1.1  
vrid 10 unflowdown  
[NPE1-GigabitEthernet1/0/1.103] quit
```

配置 NPE2。

```
[NPE2] interface gigabitethernet1/0/1.100  
[NPE2-GigabitEthernet1/0/1.100] vrrp vrid 100 track admin-vrrp interface gigabitethernet1/0/1.1  
vrid 10 unflowdown  
[NPE2-GigabitEthernet1/0/1.100] quit  
[NPE2] interface gigabitethernet1/0/1.101  
[NPE2-GigabitEthernet1/0/1.101] vrrp vrid 101 track admin-vrrp interface gigabitethernet1/0/1.1  
vrid 10 unflowdown  
[NPE2-GigabitEthernet1/0/1.101] quit  
[NPE2] interface gigabitethernet1/0/1.102  
[NPE2-GigabitEthernet1/0/1.102] vrrp vrid 102 track admin-vrrp interface gigabitethernet1/0/1.1  
vrid 10 unflowdown  
[NPE2-GigabitEthernet1/0/1.102] quit  
[NPE2] interface gigabitethernet1/0/1.103  
[NPE2-GigabitEthernet1/0/1.103] vrrp vrid 103 track admin-vrrp interface gigabitethernet1/0/1.1  
vrid 10 unflowdown  
[NPE2-GigabitEthernet1/0/1.103] quit
```

完成上述配置后，在 NPE 上执行 **display vrrp brief** 命令，可以看到：

NPE1 上：

- VRID 为 10 的 VRRP，“State”是 Master，“Type”是 Admin。
- 其他 VRID 的 VRRP，“State”是 Master，“Type”是 Member。

```
[NPE1] display vrrp brief
```

VRID	State	Interface	Type	Virtual IP
10	Master	GE1/0/1.1	Admin	10.1.1.1
100	Master	GE1/0/1.100	Member	10.100.1.200
101	Master	GE1/0/1.101	Member	10.101.1.200
102	Master	GE1/0/1.102	Member	10.102.1.200
103	Master	GE1/0/1.103	Member	10.103.1.200

NPE2 上：

- VRID 为 10 的 VRRP，“State”是 Backup，“Type”是 Admin。
- 其他 VRID 的 VRRP，“State”是 Backup，“Type”是 Member。

```
[NPE2] display vrrp brief
```

VRID	State	Interface	Type	Virtual IP
10	Backup	GE1/0/1.1	Admin	10.1.1.1
100	Backup	GE1/0/1.100	Member	10.100.1.200
101	Backup	GE1/0/1.101	Member	10.101.1.200
102	Backup	GE1/0/1.102	Member	10.102.1.200
103	Backup	GE1/0/1.103	Member	10.103.1.200

此时，业务 VRRP 已经与管理 VRRP 成功绑定，且状态正确。

步骤 4 配置 BFD 的基本功能

在 NPE 之间配置 Peer BFD；在 NPE 与每个 CE 之间配置 Link BFD。

配置 NPE1。

```
[NPE1] bfd  
[NPE1-bfd] quit  
[NPE1] bfd peer1 bind peer-ip 10.1.1.253 interface gigabitethernet1/0/1.1 source-ip 10.1.1.254 auto  
[NPE1-bfd-session-peer1] commit  
[NPE1-bfd-session-peer1] quit  
[NPE1] bfd link1 bind peer-ip 10.100.1.1 interface gigabitethernet1/0/1.100 source-ip 10.100.1.254  
auto
```

```
[NPE1-bfd-session-link1] commit
[NPE1-bfd-session-link1] quit
[NPE1] bfd link2 bind peer-ip 10.101.1.1 interface gigabitethernet1/0/1.101 source-ip 10.101.1.254
auto
[NPE1-bfd-session-link2] commit
[NPE1-bfd-session-link2] quit
[NPE1] bfd link3 bind peer-ip 10.102.1.1 interface gigabitethernet1/0/1.102 source-ip 10.102.1.254
auto
[NPE1-bfd-session-link3] commit
[NPE1-bfd-session-link3] quit
[NPE1] bfd link4 bind peer-ip 10.103.1.1 interface gigabitethernet1/0/1.103 source-ip 10.103.1.254
auto
[NPE1-bfd-session-link4] commit
[NPE1-bfd-session-link4] quit
```

配置 NPE2。

```
[NPE2] bfd
[NPE2-bfd] quit
[NPE2] bfd peer1 bind peer-ip 10.1.1.254 interface gigabitethernet1/0/1.1 source-ip 10.1.1.253 auto
[NPE2-bfd-session-peer1] commit
[NPE2-bfd-session-peer1] quit
[NPE2] bfd link1 bind peer-ip 10.100.1.1 interface gigabitethernet1/0/1.100 source-ip 10.100.1.253
auto
[NPE2-bfd-session-link1] commit
[NPE2-bfd-session-link1] quit
[NPE2] bfd link2 bind peer-ip 10.101.1.1 interface gigabitethernet1/0/1.101 source-ip 10.101.1.253
auto
[NPE2-bfd-session-link2] commit
[NPE2-bfd-session-link2] quit
[NPE2] bfd link3 bind peer-ip 10.102.1.1 interface gigabitethernet1/0/1.102 source-ip 10.102.1.253
auto
[NPE2-bfd-session-link3] commit
[NPE2-bfd-session-link3] quit
[NPE2] bfd link4 bind peer-ip 10.103.1.1 interface gigabitethernet1/0/1.103 source-ip 10.103.1.253
auto
[NPE2-bfd-session-link4] commit
[NPE2-bfd-session-link4] quit
```

完成上述配置且 CE 也正确配置 BFD 会话后，在 NPE 上使用 **display bfd configuration all** 命令查看 BFD 的配置，可以看到“Commit”为 True。

以 NPE1 的显示为例。

```
[NPE1] display bfd configuration all
```

CFG Name	CFG Type	LocalDiscr	MIndex	SessNum	Commit	AdminDown
peer1	S_AUTO_IF	8192	256	1	True	False
link1	S_AUTO_IF	8193	257	1	True	False
link2	S_AUTO_IF	8194	258	1	True	False
link3	S_AUTO_IF	8195	259	1	True	False
link4	S_AUTO_IF	8196	260	1	True	False

Total Commit/Uncommit CFG Number : 5/0

在 NPE 上使用 **display bfd session all** 命令查看 BFD 的状态，可以看到“State”为 Up。

以 NPE1 的显示为例。

```
[NPE1] display bfd session all
```

Local	Remote	PeerIpAddr	State	Type	InterfaceName
8192	8192	10.1.1.253	Up	S_AUTO_IF	GigabitEthernet1/0/1.1
8193	8192	10.100.1.1	Up	S_AUTO_IF	GigabitEthernet1/0/1.100
8194	8193	10.101.1.1	Up	S_AUTO_IF	GigabitEthernet1/0/1.101
8195	8194	10.102.1.1	Up	S_AUTO_IF	GigabitEthernet1/0/1.102
8196	8195	10.103.1.1	Up	S_AUTO_IF	GigabitEthernet1/0/1.103

Total UP/DOWN Session Number : 5/0

步骤 5 配置 VRRP 通过 BFD Sampling 完成快速切换的功能



因为普通业务 VRRP 已经与管理 VRRP 绑定，因此，对于 NPE 而言，VRRP 通过 BFD Sampling 完成快速切换的功能，只需要针对接口 GE1/0/1.1 上的管理 VRRP 配置即可。

配置 NPE1。

```
[NPE1] interface gigabitethernet1/0/1.1
[NPE1-GigabitEthernet1/0/1.1] vrrp vrid 10 track bfd-session session-name peer1 peer
[NPE1-GigabitEthernet1/0/1.1] vrrp vrid 10 track bfd-session session-name link1 link
[NPE1-GigabitEthernet1/0/1.1] vrrp vrid 10 track bfd-session session-name link2 link
[NPE1-GigabitEthernet1/0/1.1] vrrp vrid 10 track bfd-session session-name link3 link
[NPE1-GigabitEthernet1/0/1.1] vrrp vrid 10 track bfd-session session-name link4 link
[NPE1-GigabitEthernet1/0/1.1] vrrp vrid 10 track link-bfd down-number 2
[NPE1-GigabitEthernet1/0/1.1] vrrp trigger route
[NPE1-GigabitEthernet1/0/1.1] quit
```

配置 NPE2。

```
[NPE2] interface gigabitethernet1/0/1.1
[NPE2-GigabitEthernet1/0/1.1] vrrp vrid 10 track bfd-session session-name peer1 peer
[NPE2-GigabitEthernet1/0/1.1] vrrp vrid 10 track bfd-session session-name link1 link
[NPE2-GigabitEthernet1/0/1.1] vrrp vrid 10 track bfd-session session-name link2 link
[NPE2-GigabitEthernet1/0/1.1] vrrp vrid 10 track bfd-session session-name link3 link
[NPE2-GigabitEthernet1/0/1.1] vrrp vrid 10 track bfd-session session-name link4 link
[NPE2-GigabitEthernet1/0/1.1] vrrp vrid 10 track link-bfd down-number 2
[NPE2-GigabitEthernet1/0/1.1] vrrp trigger route
[NPE2-GigabitEthernet1/0/1.1] quit
```

完成上述配置后，在 NPE 上执行 **display vrrp interface** 命令，可以看到管理 VRRP 监视的 Link BFD 状态为 Down 的数目是 2，管理 VRRP 与 1 个 Peer BFD、4 个 Link BFD 绑定，并且 BFD 的状态都是 Up。

```
[NPE1] display vrrp interface gigabitethernet1/0/1.1
GigabitEthernet1/0/1.1 | Virtual Router 10
  State                : Master
  Virtual IP            : 10.1.1.1
  PriorityRun            : 120
  PriorityConfig         : 120
  MasterPriority         : 120
  Preempt               : YES          Delay Time : 0
  TimerRun              : 1
  TimerConfig           : 1
  Auth Type             : NONE
  Virtual Mac           : 0000-5e00-010a
  Check TTL             : YES
  Config type           : admin-vrrp
  Config track link-bfd down-number : 2
  Track BFD             : link1        type: link
  BFD-session state     : UP
  Track BFD             : link2        type: link
  BFD-session state     : UP
  Track BFD             : link3        type: link
  BFD-session state     : UP
  Track BFD             : link4        type: link
  BFD-session state     : UP
  Track BFD             : peer1       type: peer
  BFD-session state     : UP
  Create time           : 2010-06-22 17:33:00
  Last change time      : 2010-06-22 17:33:06
[NPE2] display vrrp interface gigabitethernet1/0/1.1
GigabitEthernet1/0/1.1 | Virtual Router 10
  State                : Backup
  Virtual IP            : 10.1.1.1
```

```
PriorityRun           : 100
PriorityConfig        : 100
MasterPriority        : 120
Preempt              : YES          Delay Time : 0
TimerRun             : 1
TimerConfig          : 1
Auth Type            : NONE
Virtual Mac          : 0000-5e00-010a
Check TTL            : YES
Config type          : admin-vrrp
Config track link-bfd down-number : 2
Track BFD            : link1        type: link
BFD-session state    : UP
Track BFD            : link2        type: link
BFD-session state    : UP
Track BFD            : link3        type: link
BFD-session state    : UP
Track BFD            : link4        type: link
BFD-session state    : UP
Track BFD            : peer1        type: peer
BFD-session state    : UP
Create time          : 2010-06-22 17:35:00
Last change time     : 2010-06-22 17:35:06
```

步骤 6 验证配置结果

完成上述配置后，正常情况下，在 NPE 上执行 **display vrrp brief** 命令，可以看到：
NPE1 上：

- VRID 为 10 的 VRRP，“State”是 Master，“Type”是 Admin。
- 其他 VRID 的 VRRP，“State”是 Master，“Type”是 Member。

```
[NPE1] display vrrp brief
VRID  State      Interface      Type      Virtual IP
-----
10    Master       GE1/0/1.1     Admin     10.1.1.1
100   Master       GE1/0/1.100   Member    10.100.1.200
101   Master       GE1/0/1.101   Member    10.101.1.200
102   Master       GE1/0/1.102   Member    10.102.1.200
103   Master       GE1/0/1.103   Member    10.103.1.200
```

NPE2 上：

- VRID 为 10 的 VRRP，“State”是 Backup，“Type”是 Admin。
- 其他 VRID 的 VRRP，“State”是 Backup，“Type”是 Member。

```
[NPE2] display vrrp brief
VRID  State      Interface      Type      Virtual IP
-----
10    Backup      GE1/0/1.1     Admin     10.1.1.1
100   Backup      GE1/0/1.100   Member    10.100.1.200
101   Backup      GE1/0/1.101   Member    10.101.1.200
102   Backup      GE1/0/1.102   Member    10.102.1.200
103   Backup      GE1/0/1.103   Member    10.103.1.200
```

在 NPE1 上 **shutdown** 接口 GE1/0/1.100，来模拟 NPE1 和 CE1 之间的故障。

```
[NPE1] interface gigabitethernet1/0/1.100
[NPE1-GigabitEthernet1/0/1.100] shutdown
[NPE1-GigabitEthernet1/0/1.100] quit
```

可以看到 NPE1 与 CE1 之间的 BFD 状态变为 Down。

```
[NPE1] display bfd session all
-----
Local  Remote PeerIpAddr      State      Type      InterfaceName
-----
8192   8192   10.1.1.253      Up         S_AUTO_IF  GigabitEthernet1/0/1.1
```

8193	0	10.100.1.1	Down	S_AUTO_IF	GigabitEthernet1/0/1.100
8194	8193	10.101.1.1	Up	S_AUTO_IF	GigabitEthernet1/0/1.101
8195	8194	10.102.1.1	Up	S_AUTO_IF	GigabitEthernet1/0/1.102
8196	8195	10.103.1.1	Up	S_AUTO_IF	GigabitEthernet1/0/1.103

Total UP/DOWN Session Number : 4/1

由于本例中，管理 VRRP 监视的 Link BFD 会话 Down 的数目是 2，即只有 2 条或者 2 条以上的 Link BFD 会话状态变为 Down，管理 VRRP 才会进行主备切换。

目前只有 1 条 BFD 的状态为 Down，因此管理 VRRP 不会进行主备切换。

NPE1 上：

- VRID 为 10 的 VRRP，“State”是 Master，“Type”是 Admin。
- VRID 为 100 的 VRRP，“State”变为 Initialize，“Type”是 Member。
- 其他 VRID 的 VRRP，“State”是 Master，“Type”是 Member。

```
[NPE1] display vrrp brief
```

VRID	State	Interface	Type	Virtual IP
10	Master	GE1/0/1.1	Admin	10.1.1.1
100	Initialize	GE1/0/1.100	Member	10.100.1.200
101	Master	GE1/0/1.101	Member	10.101.1.200
102	Master	GE1/0/1.102	Member	10.102.1.200
103	Master	GE1/0/1.103	Member	10.103.1.200

NPE2 上：

- VRID 为 10 的 VRRP，“State”是 Backup，“Type”是 Admin。
- 其他 VRID 的 VRRP，“State”是 Backup，“Type”是 Member。

```
[NPE2] display vrrp brief
```

VRID	State	Interface	Type	Virtual IP
10	Backup	GE1/0/1.1	Admin	10.1.1.1
100	Backup	GE1/0/1.100	Member	10.100.1.200
101	Backup	GE1/0/1.101	Member	10.101.1.200
102	Backup	GE1/0/1.102	Member	10.102.1.200
103	Backup	GE1/0/1.103	Member	10.103.1.200

在 NPE1 上继续 shutdown 接口 GE1/0/1.101，来模拟 NPE1 和 CE2 之间的故障。

```
[NPE1] interface gigabitethernet1/0/1.101
[NPE1-GigabitEthernet1/0/1.101] shutdown
[NPE1-GigabitEthernet1/0/1.101] quit
```

可以看到 NPE1 与 CE2 之间的 BFD 状态变为 Down。

```
[NPE1] display bfd session all
```

Local	Remote	PeerIpAddr	State	Type	InterfaceName
8192	8192	10.1.1.253	Up	S_AUTO_IF	GigabitEthernet1/0/1.1
8193	0	10.100.1.1	Down	S_AUTO_IF	GigabitEthernet1/0/1.100
8194	0	10.101.1.1	Down	S_AUTO_IF	GigabitEthernet1/0/1.101
8195	8194	10.102.1.1	Up	S_AUTO_IF	GigabitEthernet1/0/1.102
8196	8195	10.103.1.1	Up	S_AUTO_IF	GigabitEthernet1/0/1.103

Total UP/DOWN Session Number : 3/2

由于本例中，管理 VRRP 监视的 Link BFD 会话 Down 的数目是 2，即只有 2 条或者 2 条以上的 Link BFD 会话状态变为 Down，管理 VRRP 才会进行主备切换。

此时已经有 2 条 BFD 的状态为 Down，因此管理 VRRP 会进行主备切换。

NPE1 上：

- VRID 为 10 的 VRRP, “State” 是 Initialize, “Type” 是 Admin。
- 其他 VRID 的 VRRP, “State” 是 Initialize, “Type” 是 Member。

```
[NPE1] display vrrp brief
```

VRID	State	Interface	Type	Virtual IP
10	Initialize	GE1/0/1.1	Admin	10.1.1.1
100	Initialize	GE1/0/1.100	Member	10.100.1.200
101	Initialize	GE1/0/1.101	Member	10.101.1.200
102	Initialize	GE1/0/1.102	Member	10.102.1.200
103	Initialize	GE1/0/1.103	Member	10.103.1.200

NPE2 上:

- VRID 为 10 的 VRRP, “State” 是 Master, “Type” 是 Admin。
- 其他 VRID 的 VRRP, “State” 是 Master, “Type” 是 Member。

```
[NPE2] display vrrp brief
```

VRID	State	Interface	Type	Virtual IP
10	Master	GE1/0/1.1	Admin	10.1.1.1
100	Master	GE1/0/1.100	Member	10.100.1.200
101	Master	GE1/0/1.101	Member	10.101.1.200
102	Master	GE1/0/1.102	Member	10.102.1.200
103	Master	GE1/0/1.103	Member	10.103.1.200

在 NPE1 上 **undo shutdown** 接口 GE1/0/1.100 和接口 GE1/0/1.101, 来模拟 NPE1 和 CE1 之间、NPE1 和 CE2 之间的故障恢复。

可以看到 NPE1 与 CE1 之间、NPE1 与 CE2 之间的 BFD 状态重新变为 Up。

```
[NPE1] display bfd session all
```

Local	Remote	PeerIpAddr	State	Type	InterfaceName
8192	8192	10.1.1.253	Up	S_AUTO_IF	GigabitEthernet1/0/1.1
8193	8192	10.100.1.1	Up	S_AUTO_IF	GigabitEthernet1/0/1.100
8194	8193	10.101.1.1	Up	S_AUTO_IF	GigabitEthernet1/0/1.101
8195	8194	10.102.1.1	Up	S_AUTO_IF	GigabitEthernet1/0/1.102
8196	8195	10.103.1.1	Up	S_AUTO_IF	GigabitEthernet1/0/1.103

Total UP/DOWN Session Number : 5/0

NPE 上的 VRRP 状态恢复。

NPE1 上:

- VRID 为 10 的 VRRP, “State” 是 Master, “Type” 是 Admin。
- 其他 VRID 的 VRRP, “State” 是 Master, “Type” 是 Member。

```
[NPE1] display vrrp brief
```

VRID	State	Interface	Type	Virtual IP
10	Master	GE1/0/1.1	Admin	10.1.1.1
100	Master	GE1/0/1.100	Member	10.100.1.200
101	Master	GE1/0/1.101	Member	10.101.1.200
102	Master	GE1/0/1.102	Member	10.102.1.200
103	Master	GE1/0/1.103	Member	10.103.1.200

NPE2 上:

- VRID 为 10 的 VRRP, “State” 是 Backup, “Type” 是 Admin。
- 其他 VRID 的 VRRP, “State” 是 Backup, “Type” 是 Member。

```
[NPE2] display vrrp brief
```

VRID	State	Interface	Type	Virtual IP

10	Backup	GE1/0/1.1	Admin	10.1.1.1
100	Backup	GE1/0/1.100	Member	10.100.1.200
101	Backup	GE1/0/1.101	Member	10.101.1.200
102	Backup	GE1/0/1.102	Member	10.102.1.200
103	Backup	GE1/0/1.103	Member	10.103.1.200

----结束

配置文件

- NPE1 的配置文件

```
#
sysname NPE1
#
bfd
#
interface GigabitEthernet1/0/1
undo shutdown
mode user-termination
#
interface GigabitEthernet1/0/1.1
control-vid 1 qinq-termination
qinq termination pe-vid 10 ce-vid 1 to 100
qinq vrrp pe-vid 10 ce-vid 100
ip address 10.1.1.254 255.255.255.0
vrrp vrid 10 virtual-ip 10.1.1.1
admin-vrrp vrid 10
vrrp vrid 10 priority 120
vrrp vrid 10 track bfd-session session-name link1 link
vrrp vrid 10 track bfd-session session-name link2 link
vrrp vrid 10 track bfd-session session-name link3 link
vrrp vrid 10 track bfd-session session-name link4 link
vrrp vrid 10 track bfd-session session-name peer1 peer
vrrp vrid 10 track link-bfd down-number 2
vrrp trigger route
arp broadcast enable
#
interface GigabitEthernet1/0/1.100
control-vid 100 qinq-termination
qinq termination pe-vid 10 ce-vid 101 to 200
qinq vrrp pe-vid 10 ce-vid 101
ip address 10.100.1.254 255.255.255.0
vrrp vrid 100 virtual-ip 10.100.1.200
vrrp vrid 100 track admin-vrrp interface GigabitEthernet1/0/1.1 vrid 10 unflowdown
arp broadcast enable
#
interface GigabitEthernet1/0/1.101
control-vid 101 qinq-termination
qinq termination pe-vid 10 ce-vid 201 to 300
qinq vrrp pe-vid 10 ce-vid 201
ip address 10.101.1.254 255.255.255.0
vrrp vrid 101 virtual-ip 10.101.1.200
vrrp vrid 101 track admin-vrrp interface GigabitEthernet1/0/1.1 vrid 10 unflowdown
arp broadcast enable
#
interface GigabitEthernet1/0/1.102
control-vid 102 qinq-termination
qinq termination pe-vid 10 ce-vid 301 to 400
qinq vrrp pe-vid 10 ce-vid 301
ip address 10.102.1.254 255.255.255.0
vrrp vrid 102 virtual-ip 10.102.1.200
vrrp vrid 102 track admin-vrrp interface GigabitEthernet1/0/1.1 vrid 10 unflowdown
arp broadcast enable
#
interface GigabitEthernet1/0/1.103
control-vid 103 qinq-termination
qinq termination pe-vid 10 ce-vid 401 to 500
qinq vrrp pe-vid 10 ce-vid 401
```

```

ip address 10.103.1.254 255.255.255.0
vrrp vrid 103 virtual-ip 10.103.1.200
vrrp vrid 103 track admin-vrrp interface GigabitEthernet1/0/1.1 vrid 10 unflowdown
arp broadcast enable
#
bfd link1 bind peer-ip 10.100.1.1 interface GigabitEthernet1/0/1.100 source-ip 10.100.1.254
auto
commit
#
bfd link2 bind peer-ip 10.101.1.1 interface GigabitEthernet1/0/1.101 source-ip 10.101.1.254
auto
commit
#
bfd link3 bind peer-ip 10.102.1.1 interface GigabitEthernet1/0/1.102 source-ip 10.102.1.254
auto
commit
#
bfd link4 bind peer-ip 10.103.1.1 interface GigabitEthernet1/0/1.103 source-ip 10.103.1.254
auto
commit
#
bfd peer1 bind peer-ip 10.1.1.253 interface GigabitEthernet1/0/1.1 source-ip 10.1.1.254 auto
commit
#
return

```

● NPE2 的配置文件

```

#
sysname NPE2
#
bfd
#
interface GigabitEthernet1/0/1
undo shutdown
mode user-termination
#
interface GigabitEthernet1/0/1.1
control-vid 1 qinq-termination
qinq termination pe-vid 10 ce-vid 1 to 100
qinq vrrp pe-vid 10 ce-vid 100
ip address 10.1.1.253 255.255.255.0
vrrp vrid 10 virtual-ip 10.1.1.1
admin-vrrp vrid 10
vrrp vrid 10 track bfd-session session-name link1 link
vrrp vrid 10 track bfd-session session-name link2 link
vrrp vrid 10 track bfd-session session-name link3 link
vrrp vrid 10 track bfd-session session-name link4 link
vrrp vrid 10 track bfd-session session-name peer1 peer
vrrp vrid 10 track link-bfd down-number 2
vrrp trigger route
arp broadcast enable
#
interface GigabitEthernet1/0/1.100
control-vid 100 qinq-termination
qinq termination pe-vid 10 ce-vid 101 to 200
qinq vrrp pe-vid 10 ce-vid 101
ip address 10.100.1.253 255.255.255.0
vrrp vrid 100 virtual-ip 10.100.1.200
vrrp vrid 100 track admin-vrrp interface GigabitEthernet1/0/1.1 vrid 10 unflowdown
arp broadcast enable
#
interface GigabitEthernet1/0/1.101
control-vid 101 qinq-termination
qinq termination pe-vid 10 ce-vid 201 to 300
qinq vrrp pe-vid 10 ce-vid 201
ip address 10.101.1.253 255.255.255.0
vrrp vrid 101 virtual-ip 10.101.1.200
vrrp vrid 101 track admin-vrrp interface GigabitEthernet1/0/1.1 vrid 10 unflowdown
arp broadcast enable
#

```

```
interface GigabitEthernet1/0/1.102
 control-vid 102 qinq-termination
 qinq termination pe-vid 10 ce-vid 301 to 400
 qinq vrrp pe-vid 10 ce-vid 301
 ip address 10.102.1.253 255.255.255.0
 vrrp vrid 102 virtual-ip 10.102.1.200
 vrrp vrid 102 track admin-vrrp interface GigabitEthernet1/0/1.1 vrid 10 unflowdown
 arp broadcast enable
#
interface GigabitEthernet1/0/1.103
 control-vid 103 qinq-termination
 qinq termination pe-vid 10 ce-vid 401 to 500
 qinq vrrp pe-vid 10 ce-vid 401
 ip address 10.103.1.253 255.255.255.0
 vrrp vrid 103 virtual-ip 10.103.1.200
 vrrp vrid 103 track admin-vrrp interface GigabitEthernet1/0/1.1 vrid 10 unflowdown
 arp broadcast enable
#
bfd link1 bind peer-ip 10.100.1.1 interface GigabitEthernet1/0/1.100 source-ip 10.100.1.253
 auto
 commit
#
bfd link2 bind peer-ip 10.101.1.1 interface GigabitEthernet1/0/1.101 source-ip 10.101.1.253
 auto
 commit
#
bfd link3 bind peer-ip 10.102.1.1 interface GigabitEthernet1/0/1.102 source-ip 10.102.1.253
 auto
 commit
#
bfd link4 bind peer-ip 10.103.1.1 interface GigabitEthernet1/0/1.103 source-ip 10.103.1.253
 auto
 commit
#
bfd peer1 bind peer-ip 10.1.1.254 interface GigabitEthernet1/0/1.1 source-ip 10.1.1.253 auto
 commit
#
return
```

● PE1 的配置文件

```
#
 sysname PE1
#
 mpls lsr-id 3.3.3.3
 mpls
#
 mpls l2vpn
#
 vsi ldpl static
 pwsignal ldp
 vsi-id 100
 peer 4.4.4.4
 peer 5.5.5.5
#
 mpls ldp
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 200.1.34.3 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/1
 undo shutdown
#
interface GigabitEthernet1/0/1.1
 vlan-type dot1q 10
 l2 binding vsi ldpl
#
interface GigabitEthernet1/0/3
```

```
undo shutdown
ip address 200.1.35.3 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 3.3.3.3 255.255.255.255
#
ospf 1
area 0.0.0.0
network 3.3.3.3 0.0.0.0
network 200.1.34.0 0.0.0.255
network 200.1.35.0 0.0.0.255
#
return
```

● PE2 的配置文件

```
#
sysname PE2
#
mpls lsr-id 4.4.4.4
mpls
#
mpls l2vpn
#
vsi ldpl static
pwsignal ldp
vsi-id 100
peer 3.3.3.3
peer 5.5.5.5
#
mpls ldp
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 200.1.34.4 255.255.255.0
mpls
mpls ldp
#
interface GigabitEthernet1/0/1
undo shutdown
#
interface GigabitEthernet1/0/1.1
vlan-type dot1q 10
l2 binding vsi ldpl
#
interface GigabitEthernet1/0/4
undo shutdown
ip address 200.1.45.4 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 4.4.4.4 255.255.255.255
#
ospf 1
area 0.0.0.0
network 4.4.4.4 0.0.0.0
network 200.1.34.0 0.0.0.255
network 200.1.45.0 0.0.0.255
#
return
```

● PE3 的配置文件

```
#
sysname PE3
#
mpls lsr-id 5.5.5.5
mpls
#
```

```

mpls l2vpn
#
vsi ldp1 static
pwsignal ldp
vsi-id 100
peer 3.3.3.3
peer 4.4.4.4
#
mpls ldp
#
interface GigabitEthernet1/0/0
undo shutdown
#
interface GigabitEthernet1/0/0.1
vlan-type dot1q 10
l2 binding vsi ldp1
#
interface GigabitEthernet1/0/1
undo shutdown
ip address 200.1.35.5 255.255.255.0
mpls
mpls ldp
#
interface GigabitEthernet1/0/2
undo shutdown
ip address 200.1.45.5 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 5.5.5.5 255.255.255.255
#
ospf 1
area 0.0.0.0
network 5.5.5.5 0.0.0.0
network 200.1.35.0 0.0.0.255
network 200.1.45.0 0.0.0.255
#
return

```

● CE 的配置文件

```

#
sysname CE1
#
bfd
#
interface GigabitEthernet1/0/1
undo shutdown
mode user-termination
#
interface GigabitEthernet1/0/1.100
control-vid 100 qinq-termination
qinq termination pe-vid 10 ce-vid 110
ip address 10.100.1.1 255.255.255.0
arp broadcast enable
#
interface GigabitEthernet1/0/1.101
control-vid 101 qinq-termination
qinq termination pe-vid 10 ce-vid 210
ip address 10.101.1.1 255.255.255.0
arp broadcast enable
#
interface GigabitEthernet1/0/1.102
control-vid 102 qinq-termination
qinq termination pe-vid 10 ce-vid 310
ip address 10.102.1.1 255.255.255.0
arp broadcast enable
#
interface GigabitEthernet1/0/1.103
control-vid 103 qinq-termination

```

```
qinq termination pe-vid 10 ce-vid 410
ip address 10.103.1.1 255.255.255.0
arp broadcast enable
#
bfd link11 bind peer-ip 10.100.1.254 interface GigabitEthernet1/0/1.100 source-i
p 10.100.1.1 auto
commit
#
bfd link12 bind peer-ip 10.101.1.254 interface GigabitEthernet1/0/1.101 source-i
p 10.101.1.1 auto
commit
#
bfd link13 bind peer-ip 10.102.1.254 interface GigabitEthernet1/0/1.102 source-i
p 10.102.1.1 auto
commit
#
bfd link14 bind peer-ip 10.103.1.254 interface GigabitEthernet1/0/1.103 source-i
p 10.103.1.1 auto
commit
#
bfd link21 bind peer-ip 10.100.1.253 interface GigabitEthernet1/0/1.100 source-i
p 10.100.1.1 auto
commit
#
bfd link22 bind peer-ip 10.101.1.253 interface GigabitEthernet1/0/1.101 source-i
p 10.101.1.1 auto
commit
#
bfd link23 bind peer-ip 10.102.1.253 interface GigabitEthernet1/0/1.102 source-i
p 10.102.1.1 auto
commit
#
bfd link24 bind peer-ip 10.103.1.253 interface GigabitEthernet1/0/1.103 source-i
p 10.103.1.1 auto
commit
#
return
```

4.14.7 配置管理 VRRP 忽略接口 Down 事件功能

本示例中，通过配置管理 VRRP 忽略接口 Down 事件功能，解决 NPE 之间无法建立管理 VRRP 和 Peer BFD 的问题。

组网需求



说明

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

如图 4-11 所示。CE 通过 VPLS 汇聚网络接入 NPE 的 QinQ 终结子接口。

NPE 上配置管理 VRRP 和业务 VRRP，并通过管理 VRRP 监视 BFD 会话来完成快速切换。

本例中，网络限制条件：

- VPLS 汇聚网络属于其他的运营商，因此 NPE1 与 PE1、NPE2 与 PE2 之间无法直接建立 Link BFD。
- VPLS 汇聚网络中仅在 PE1 与 PE3 之间、PE1 与 PE2 之间存在 PW，根据 VPLS 水平分割的原则，NPE1 与 NPE2 之间无法建立管理 VRRP 和 Peer BFD。

此时可以使用管理 VRRP 忽略接口 Down 事件的功能来实现 VRRP 快速切换。

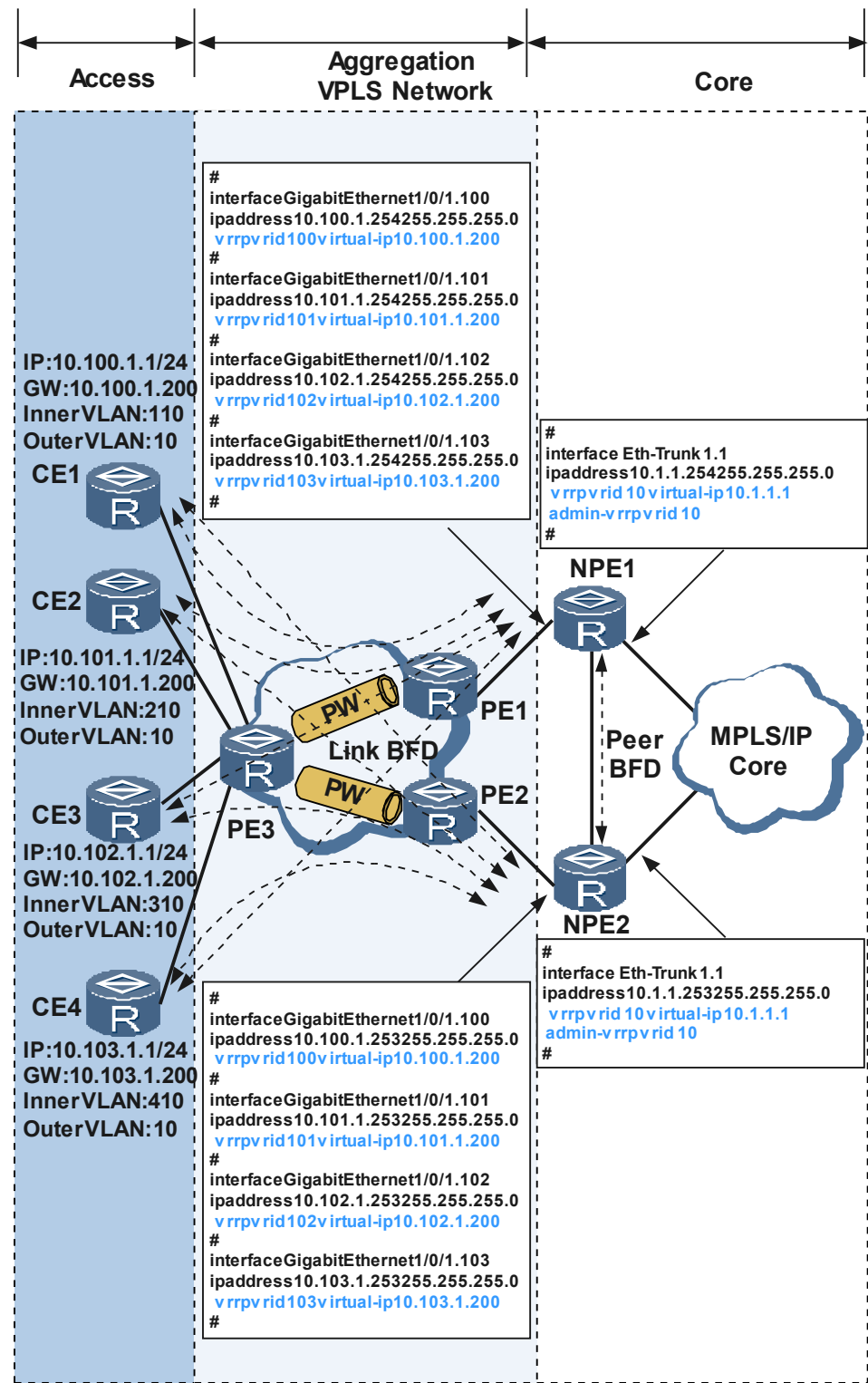
 说明

- BFD Samping: NPE 与所有的 CE 直接建立 Link BFD 的检测方式。
- 管理 VRRP 忽略接口 Down 事件: VRRP 备份组所在接口变为 Down 状态时, 接口上 VRRP 的状态不迁移到 Initialize 状态, 而是直接切换到 Master 状态。

对于 NPE 而言:

- NPE1 和 NPE2 通过直连链路 Eth-Trunk1, 建立管理 VRRP 和 Peer BFD。
- NPE1 和 NPE2 通过 VPLS 汇聚网络侧接口 GE1/0/1, 建立业务 VRRP。
- 每个 NPE 通过 VPLS 汇聚网络侧接口 GE1/0/1 与 CE 之间直接建立 4 个 Link BFD 会话, 管理 VRRP 同时监视这 4 个 BFD 会话的状态。当管理 VRRP 监视的 Link BFD 会话有 2 条或者 2 条以上的 Link BFD 会话状态变为 Down, 管理 VRRP 进行主备快速切换。

图 4-11 配置管理 VRRP 忽略接口 Down 事件功能组网图



配置思路

采用如下的思路配置管理 VRRP 忽略接口 Down 事件的基本功能：

1. 在 NPE 上配置 QinQ 终结子接口的基本功能。
2. 在 NPE 的 QinQ 终结子接口上配置管理 VRRP 和业务 VRRP，并将业务 VRRP 与管理 VRRP 绑定。
3. 配置 NPE 之间，NPE 与 CE 之间的 BFD 功能。
4. 配置管理 VRRP 通过 BFD Sampling 完成快速切换。

数据准备

为完成此配置例，需准备如下的数据：

- VRRP 备份组 ID、虚拟 IP 地址。
- VRRP 备份组中的优先级。

操作步骤

步骤 1 配置 NPE 之间的 Eth-Trunk 接口

 说明

以下仅给出 NPE 的配置步骤，[图 4-10](#) 中 CE 的 BFD 功能以及 VPLS 汇聚网络的配置步骤请参见《HUAWEI NetEngine80E/40E 路由器 配置指南-可靠性》和《HUAWEI NetEngine80E/40E 路由器 配置指南-VPN》中的相关内容。

配置 NPE1。

```
<HUAWEI> system-view
[HUAWEI] sysname NPE1
[NPE1] interface Eth-Trunk 1
[NPE1-Eth-Trunk1] quit
[NPE1] interface gigabitethernet1/0/2
[NPE1-GigabitEthernet1/0/2] undo shutdown
[NPE1-GigabitEthernet1/0/2] eth-trunk 1
[NPE1-GigabitEthernet1/0/2] quit
[NPE1] interface gigabitethernet2/0/1
[NPE1-GigabitEthernet2/0/1] undo shutdown
[NPE1-GigabitEthernet2/0/1] eth-trunk 1
[NPE1-GigabitEthernet2/0/1] quit
```

配置 NPE2。

```
<HUAWEI> system-view
[HUAWEI] sysname NPE2
[NPE2] interface Eth-Trunk 1
[NPE2-Eth-Trunk1] quit
[NPE2] interface gigabitethernet1/0/2
[NPE2-GigabitEthernet1/0/2] undo shutdown
[NPE2-GigabitEthernet1/0/2] eth-trunk 1
[NPE2-GigabitEthernet1/0/2] quit
[NPE2] interface gigabitethernet2/0/1
[NPE2-GigabitEthernet2/0/1] undo shutdown
[NPE2-GigabitEthernet2/0/1] eth-trunk 1
[NPE2-GigabitEthernet2/0/1] quit
```

步骤 2 配置 QinQ 终结子接口的基本功能

配置 NPE1。

```
[NPE1] interface eth-trunk 1
[NPE1-Eth-Trunk1] mode user-termination
[NPE1-Eth-Trunk1] undo shutdown
[NPE1-Eth-Trunk1] quit
[NPE1] interface eth-trunk 1.1
[NPE1-Eth-Trunk1.1] control-vid 1 qinq-termination
```

```
[NPE1-Eth-Trunk1.1] qinq termination pe-vid 10 ce-vid 1 to 100
[NPE1-Eth-Trunk1.1] ip address 10.1.1.254 24
[NPE1-Eth-Trunk1.1] arp broadcast enable
[NPE1-Eth-Trunk1.1] quit
[NPE1] interface gigabitethernet1/0/1
[NPE1-GigabitEthernet1/0/1] mode user-termination
[NPE1-GigabitEthernet1/0/1] undo shutdown
[NPE1-GigabitEthernet1/0/1] quit
[NPE1] interface gigabitethernet1/0/1.100
[NPE1-GigabitEthernet1/0/1.100] control-vid 100 qinq-termination
[NPE1-GigabitEthernet1/0/1.100] qinq termination pe-vid 10 ce-vid 101 to 200
[NPE1-GigabitEthernet1/0/1.100] ip address 10.100.1.254 24
[NPE1-GigabitEthernet1/0/1.100] arp broadcast enable
[NPE1-GigabitEthernet1/0/1.100] quit
[NPE1] interface gigabitethernet1/0/1.101
[NPE1-GigabitEthernet1/0/1.101] control-vid 101 qinq-termination
[NPE1-GigabitEthernet1/0/1.101] qinq termination pe-vid 10 ce-vid 201 to 300
[NPE1-GigabitEthernet1/0/1.101] ip address 10.101.1.254 24
[NPE1-GigabitEthernet1/0/1.101] arp broadcast enable
[NPE1-GigabitEthernet1/0/1.101] quit
[NPE1] interface gigabitethernet1/0/1.102
[NPE1-GigabitEthernet1/0/1.102] control-vid 102 qinq-termination
[NPE1-GigabitEthernet1/0/1.102] qinq termination pe-vid 10 ce-vid 301 to 400
[NPE1-GigabitEthernet1/0/1.102] ip address 10.102.1.254 24
[NPE1-GigabitEthernet1/0/1.102] arp broadcast enable
[NPE1-GigabitEthernet1/0/1.102] quit
[NPE1] interface gigabitethernet1/0/1.103
[NPE1-GigabitEthernet1/0/1.103] control-vid 103 qinq-termination
[NPE1-GigabitEthernet1/0/1.103] qinq termination pe-vid 10 ce-vid 401 to 500
[NPE1-GigabitEthernet1/0/1.103] ip address 10.103.1.254 24
[NPE1-GigabitEthernet1/0/1.103] arp broadcast enable
[NPE1-GigabitEthernet1/0/1.103] quit
```

配置 NPE2。

```
[NPE2] interface eth-trunk 1
[NPE2-Eth-Trunk1] mode user-termination
[NPE2-Eth-Trunk1] quit
[NPE2] interface eth-trunk 1.1
[NPE2-Eth-Trunk1.1] control-vid 1 qinq-termination
[NPE2-Eth-Trunk1.1] qinq termination pe-vid 10 ce-vid 1 to 100
[NPE2-Eth-Trunk1.1] ip address 10.1.1.253 24
[NPE2-Eth-Trunk1.1] arp broadcast enable
[NPE2-Eth-Trunk1.1] quit
[NPE2] interface gigabitethernet1/0/1
[NPE2-GigabitEthernet1/0/1] mode user-termination
[NPE2-GigabitEthernet1/0/1] undo shutdown
[NPE2-GigabitEthernet1/0/1] quit
[NPE2] interface gigabitethernet1/0/1.100
[NPE2-GigabitEthernet1/0/1.100] control-vid 100 qinq-termination
[NPE2-GigabitEthernet1/0/1.100] qinq termination pe-vid 10 ce-vid 101 to 200
[NPE2-GigabitEthernet1/0/1.100] ip address 10.100.1.253 24
[NPE2-GigabitEthernet1/0/1.100] arp broadcast enable
[NPE2-GigabitEthernet1/0/1.100] quit
[NPE2] interface gigabitethernet1/0/1.101
[NPE2-GigabitEthernet1/0/1.101] control-vid 101 qinq-termination
[NPE2-GigabitEthernet1/0/1.101] qinq termination pe-vid 10 ce-vid 201 to 300
[NPE2-GigabitEthernet1/0/1.101] ip address 10.101.1.253 24
[NPE2-GigabitEthernet1/0/1.101] arp broadcast enable
[NPE2-GigabitEthernet1/0/1.101] quit
[NPE2] interface gigabitethernet1/0/1.102
[NPE2-GigabitEthernet1/0/1.102] control-vid 102 qinq-termination
[NPE2-GigabitEthernet1/0/1.102] qinq termination pe-vid 10 ce-vid 301 to 400
[NPE2-GigabitEthernet1/0/1.102] ip address 10.102.1.253 24
[NPE2-GigabitEthernet1/0/1.102] arp broadcast enable
[NPE2-GigabitEthernet1/0/1.102] quit
[NPE2] interface gigabitethernet1/0/1.103
[NPE2-GigabitEthernet1/0/1.103] control-vid 103 qinq-termination
[NPE2-GigabitEthernet1/0/1.103] qinq termination pe-vid 10 ce-vid 401 to 500
[NPE2-GigabitEthernet1/0/1.103] ip address 10.103.1.253 24
```

```
[NPE2-GigabitEthernet1/0/1.103] arp broadcast enable
[NPE2-GigabitEthernet1/0/1.103] quit
```

说明

在 QinQ 终结子接口上配置 IP 地址后，建议配置 **arp broadcast enable** 命令，否则 QinQ 终结子接口之间无法 Ping 通。

完成此步配置后，NPE 上接口 Eth-Trunk1.1 的地址，可以相互 Ping 通，从而说明 NPE 之间的链路工作正常。以 NPE1 和 NPE2 互相 Ping 为例。

管理 VRRP 所在的接口可以互相 Ping 通。

```
[NPE1] ping 10.1.1.253
PING 10.1.1.253: 56 data bytes, press CTRL_C to break
  Reply from 10.1.1.253: bytes=56 Sequence=1 ttl=255 time=160 ms
  Reply from 10.1.1.253: bytes=56 Sequence=2 ttl=255 time=90 ms
  Reply from 10.1.1.253: bytes=56 Sequence=3 ttl=255 time=160 ms
  Reply from 10.1.1.253: bytes=56 Sequence=4 ttl=255 time=180 ms
  Reply from 10.1.1.253: bytes=56 Sequence=5 ttl=255 time=120 ms

--- 10.1.1.253 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 90/142/180 ms
```

由于 VPLS 汇聚网络的水平分割限制，NPE 上业务 VRRP 所在的接口无法互相 Ping 通。以 NPE1 的 GE1/0/1.100 为例。

```
[NPE1] ping 10.100.1.253
PING 10.100.1.253: 56 data bytes, press CTRL_C to break
  Request time out
  Request time out
  Request time out
  Request time out
  Request time out

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

此外，NPE 与属于同一网段 CE 也可以 Ping 通，从而说明 NPE 与 CE 之间的链路工作正常。以 NPE1、NPE2 与 CE1 互相 Ping 为例。

```
[NPE1] ping 10.100.1.1
PING 10.100.1.1: 56 data bytes, press CTRL_C to break
  Reply from 10.100.1.1: bytes=56 Sequence=1 ttl=255 time=180 ms
  Reply from 10.100.1.1: bytes=56 Sequence=2 ttl=255 time=160 ms
  Reply from 10.100.1.1: bytes=56 Sequence=3 ttl=255 time=150 ms
  Reply from 10.100.1.1: bytes=56 Sequence=4 ttl=255 time=150 ms
  Reply from 10.100.1.1: bytes=56 Sequence=5 ttl=255 time=120 ms

--- 10.100.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 120/152/180 ms
```

```
[NPE2] ping 10.100.1.1
PING 10.100.1.1: 56 data bytes, press CTRL_C to break
  Reply from 10.100.1.1: bytes=56 Sequence=1 ttl=255 time=190 ms
  Reply from 10.100.1.1: bytes=56 Sequence=2 ttl=255 time=120 ms
  Reply from 10.100.1.1: bytes=56 Sequence=3 ttl=255 time=130 ms
  Reply from 10.100.1.1: bytes=56 Sequence=4 ttl=255 time=100 ms
  Reply from 10.100.1.1: bytes=56 Sequence=5 ttl=255 time=70 ms

--- 10.100.1.1 ping statistics ---
```

```
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 70/122/190 ms
```

步骤3 配置 QinQ 终结子接口的 VRRP 基本功能

说明

- 对于本例中的场景，使用 **admin-vrrp** 命令配置管理 VRRP 时，一定需要使用关键字 **ignore-if-down**，当 VRRP 备份组所在接口变为 Down 状态时，接口上 VRRP 的状态直接切换到 Master 状态。
- 如果不使用关键字 **ignore-if-down**，当 NPE1 的接口 Eth-Trunk1.1 因为故障而变为 Down 状态后，对端 NPE2 的接口 Eth-Trunk1.1 也会相应地变为 Down 状态，配置在接口上的 VRRP 状态就会从 Backup 切换为 **Initialize**，这样就无法实现 NPE 之间管理 VRRP 的主备切换。
- 由于上述原因，对于本例中的场景，在非 NPE1 整机故障的情况下，建议不要在 NPE1 的接口 Eth-Trunk1.1 上使用 **shutdown** 命令，否则 NPE1 和 NPE2 上的管理 VRRP 会同时成为 Master 状态，进而造成业务中断。
- 除本例中介绍的场景之外的其他组网环境，不建议使用关键字 **ignore-if-down**，否则会造成设备上 VRRP 的协议状态机与 RFC 标准中规定的不一致。

#配置 NPE1，其中在 Eth-Trunk1.1 上配置管理 VRRP，其 VRID 是 10，接口 GE1/0/1 的子接口上配置业务 VRRP。

```
[NPE1] interface eth-trunk 1.1
[NPE1-Eth-Trunk1.1] qinq vrrp pe-vid 10 ce-vid 100
[NPE1-Eth-Trunk1.1] vrrp vrid 10 virtual-ip 10.1.1.1
[NPE1-Eth-Trunk1.1] vrrp vrid 10 priority 120
[NPE1-Eth-Trunk1.1] admin-vrrp vrid 10 ignore-if-down
[NPE1-Eth-Trunk1.1] quit
[NPE1] interface gigabitethernet1/0/1.100
[NPE1-GigabitEthernet1/0/1.100] qinq vrrp pe-vid 10 ce-vid 101
[NPE1-GigabitEthernet1/0/1.100] vrrp vrid 100 virtual-ip 10.100.1.200
[NPE1-GigabitEthernet1/0/1.100] quit
[NPE1] interface gigabitethernet1/0/1.101
[NPE1-GigabitEthernet1/0/1.101] qinq vrrp pe-vid 10 ce-vid 201
[NPE1-GigabitEthernet1/0/1.101] vrrp vrid 101 virtual-ip 10.101.1.200
[NPE1-GigabitEthernet1/0/1.101] quit
[NPE1] interface gigabitethernet1/0/1.102
[NPE1-GigabitEthernet1/0/1.102] qinq vrrp pe-vid 10 ce-vid 301
[NPE1-GigabitEthernet1/0/1.102] vrrp vrid 102 virtual-ip 10.102.1.200
[NPE1-GigabitEthernet1/0/1.102] quit
[NPE1] interface gigabitethernet1/0/1.103
[NPE1-GigabitEthernet1/0/1.103] qinq vrrp pe-vid 10 ce-vid 401
[NPE1-GigabitEthernet1/0/1.103] vrrp vrid 103 virtual-ip 10.103.1.200
[NPE1-GigabitEthernet1/0/1.103] quit
```

#配置 NPE2，其中在 Eth-Trunk1.1 上配置管理 VRRP，其 VRID 是 10，接口 GE1/0/1 的子接口上配置业务 VRRP。

```
[NPE2] interface eth-trunk 1.1
[NPE2-Eth-Trunk1.1] qinq vrrp pe-vid 10 ce-vid 100
[NPE2-Eth-Trunk1.1] vrrp vrid 10 virtual-ip 10.1.1.1
[NPE2-Eth-Trunk1.1] admin-vrrp vrid 10 ignore-if-down
[NPE2-Eth-Trunk1.1] quit
[NPE2] interface gigabitethernet1/0/1.100
[NPE2-GigabitEthernet1/0/1.100] qinq vrrp pe-vid 10 ce-vid 101
[NPE2-GigabitEthernet1/0/1.100] vrrp vrid 100 virtual-ip 10.100.1.200
[NPE2-GigabitEthernet1/0/1.100] quit
[NPE2] interface gigabitethernet1/0/1.101
[NPE2-GigabitEthernet1/0/1.101] qinq vrrp pe-vid 10 ce-vid 201
[NPE2-GigabitEthernet1/0/1.101] vrrp vrid 101 virtual-ip 10.101.1.200
[NPE2-GigabitEthernet1/0/1.101] quit
[NPE2] interface gigabitethernet1/0/1.102
[NPE2-GigabitEthernet1/0/1.102] qinq vrrp pe-vid 10 ce-vid 301
[NPE2-GigabitEthernet1/0/1.102] vrrp vrid 102 virtual-ip 10.102.1.200
[NPE2-GigabitEthernet1/0/1.102] quit
```

```
[NPE2] interface gigabitethernet1/0/1.103
[NPE2-GigabitEthernet1/0/1.103] qinq vrrp pe-vid 10 ce-vid 401
[NPE2-GigabitEthernet1/0/1.103] vrrp vrid 103 virtual-ip 10.103.1.200
[NPE2-GigabitEthernet1/0/1.103] quit
```

完成上述配置后，在 NPE 上执行 **display vrrp brief** 命令，可以看到：

NPE1 上：

- VRID 为 10 的 VRRP，“State”是 Master，“Type”是 Admin。
- 其他 VRID 的 VRRP，“State”是 Master，“Type”是 Normal。

```
[NPE1] display vrrp brief
VRID    State      Interface      Type      Virtual IP
-----
10      Master      Eth-Trunk1.1   Admin     10.1.1.1
100     Master      GE1/0/1.100    Normal    10.100.1.200
101     Master      GE1/0/1.101    Normal    10.101.1.200
102     Master      GE1/0/1.102    Normal    10.102.1.200
103     Master      GE1/0/1.103    Normal    10.103.1.200
```

NPE2 上：

- VRID 为 10 的 VRRP，“State”是 Backup，“Type”是 Admin。
- 其他 VRID 的 VRRP，“State”是 Master，“Type”是 Normal。

```
[NPE2] display vrrp brief
VRID    State      Interface      Type      Virtual IP
-----
10      Backup     Eth-Trunk1.1   Admin     10.1.1.1
100     Master     GE1/0/1.100    Normal    10.100.1.200
101     Master     GE1/0/1.101    Normal    10.101.1.200
102     Master     GE1/0/1.102    Normal    10.102.1.200
103     Master     GE1/0/1.103    Normal    10.103.1.200
```

 说明

由于 VPLS 汇聚网络水平分割的限制，NPE1 和 NPE2 上的业务 VRRP 之间无法交换 VRRP 协议报文，因此 NPE1 和 NPE2 上的业务 VRRP 状态均为 Master。

步骤 4 配置业务 VRRP 与管理 VRRP 的绑定关系

配置 NPE1。

```
[NPE1] interface gigabitethernet1/0/1.100
[NPE1-GigabitEthernet1/0/1.100] vrrp vrid 100 track admin-vrrp interface eth-trunk1.1 vrid 10
unflowdown
[NPE1-GigabitEthernet1/0/1.100] quit
[NPE1] interface gigabitethernet1/0/1.101
[NPE1-GigabitEthernet1/0/1.101] vrrp vrid 101 track admin-vrrp interface eth-trunk1.1 vrid 10
unflowdown
[NPE1-GigabitEthernet1/0/1.101] quit
[NPE1] interface gigabitethernet1/0/1.102
[NPE1-GigabitEthernet1/0/1.102] vrrp vrid 102 track admin-vrrp interface eth-trunk1.1 vrid 10
unflowdown
[NPE1-GigabitEthernet1/0/1.102] quit
[NPE1] interface gigabitethernet1/0/1.103
[NPE1-GigabitEthernet1/0/1.103] vrrp vrid 103 track admin-vrrp interface eth-trunk1.1 vrid 10
unflowdown
[NPE1-GigabitEthernet1/0/1.103] quit
```

配置 NPE2。

```
[NPE2] interface gigabitethernet1/0/1.100
[NPE2-GigabitEthernet1/0/1.100] vrrp vrid 100 track admin-vrrp interface eth-trunk1.1 vrid 10
unflowdown
[NPE2-GigabitEthernet1/0/1.100] quit
[NPE2] interface gigabitethernet1/0/1.101
[NPE2-GigabitEthernet1/0/1.101] vrrp vrid 101 track admin-vrrp interface eth-trunk1.1 vrid 10
```

```
unflowdown
[NPE2-GigabitEthernet1/0/1.101] quit
[NPE2] interface gigabitethernet1/0/1.102
[NPE2-GigabitEthernet1/0/1.102] vrrp vrid 102 track admin-vrrp interface eth-trunk1.1 vrid 10
unflowdown
[NPE2-GigabitEthernet1/0/1.102] quit
[NPE2] interface gigabitethernet1/0/1.103
[NPE2-GigabitEthernet1/0/1.103] vrrp vrid 103 track admin-vrrp interface eth-trunk1.1 vrid 10
unflowdown
[NPE2-GigabitEthernet1/0/1.103] quit
```

完成上述配置后，在 NPE 上执行 **display vrrp brief** 命令，可以看到：

NPE1 上：

- VRID 为 10 的 VRRP，“State”是 Master，“Type”是 Admin。
- 其他 VRID 的 VRRP，“State”是 Master，“Type”是 Member。

```
[NPE1] display vrrp brief
VRID   State   Interface      Type      Virtual IP
-----
10     Master   Eth-Trunk1.1   Admin     10.1.1.1
100    Master   GE1/0/1.100    Member    10.100.1.200
101    Master   GE1/0/1.101    Member    10.101.1.200
102    Master   GE1/0/1.102    Member    10.102.1.200
103    Master   GE1/0/1.103    Member    10.103.1.200
```

NPE2 上：

- VRID 为 10 的 VRRP，“State”是 Backup，“Type”是 Admin。
- 其他 VRID 的 VRRP，“State”是 Backup，“Type”是 Member。

```
[NPE2] display vrrp brief
VRID   State   Interface      Type      Virtual IP
-----
10     Backup   Eth-Trunk1.1   Admin     10.1.1.1
100    Backup   GE1/0/1.100    Member    10.100.1.200
101    Backup   GE1/0/1.101    Member    10.101.1.200
102    Backup   GE1/0/1.102    Member    10.102.1.200
103    Backup   GE1/0/1.103    Member    10.103.1.200
```

此时，业务 VRRP 已经与管理 VRRP 成功绑定，且状态正确。

说明

业务 VRRP 与管理 VRRP 绑定后，业务 VRRP 就不再发送 VRRP 协议报文，其状态与绑定的管理 VRRP 状态一致。

步骤 5 配置 BFD 的基本功能

在 NPE 之间配置 Peer BFD；在 NPE 与每个 CE 之间配置 Link BFD。

配置 NPE1。

```
[NPE1] bfd
[NPE1-bfd] quit
[NPE1] bfd peer1 bind peer-ip 10.1.1.253 interface eth-trunk 1.1 source-ip 10.1.1.254 auto
[NPE1-bfd-session-peer1] commit
[NPE1-bfd-session-peer1] quit
[NPE1] bfd link1 bind peer-ip 10.100.1.1 interface gigabitethernet1/0/1.100 source-ip 10.100.1.254
auto
[NPE1-bfd-session-link1] commit
[NPE1-bfd-session-link1] quit
[NPE1] bfd link2 bind peer-ip 10.101.1.1 interface gigabitethernet1/0/1.101 source-ip 10.101.1.254
auto
[NPE1-bfd-session-link2] commit
[NPE1-bfd-session-link2] quit
[NPE1] bfd link3 bind peer-ip 10.102.1.1 interface gigabitethernet1/0/1.102 source-ip 10.102.1.254
```

```
auto
[NPE1-bfd-session-link3] commit
[NPE1-bfd-session-link3] quit
[NPE1] bfd link4 bind peer-ip 10.103.1.1 interface gigabitethernet1/0/1.103 source-ip 10.103.1.254
auto
[NPE1-bfd-session-link4] commit
[NPE1-bfd-session-link4] quit
```

配置 NPE2。

```
[NPE2] bfd
[NPE2-bfd] quit
[NPE2] bfd peer1 bind peer-ip 10.1.1.254 interface eth-trunk 1.1 source-ip 10.1.1.253 auto
[NPE2-bfd-session-peer1] commit
[NPE2-bfd-session-peer1] quit
[NPE2] bfd link1 bind peer-ip 10.100.1.1 interface gigabitethernet1/0/1.100 source-ip 10.100.1.253
auto
[NPE2-bfd-session-link1] commit
[NPE2-bfd-session-link1] quit
[NPE2] bfd link2 bind peer-ip 10.101.1.1 interface gigabitethernet1/0/1.101 source-ip 10.101.1.253
auto
[NPE2-bfd-session-link2] commit
[NPE2-bfd-session-link2] quit
[NPE2] bfd link3 bind peer-ip 10.102.1.1 interface gigabitethernet1/0/1.102 source-ip 10.102.1.253
auto
[NPE2-bfd-session-link3] commit
[NPE2-bfd-session-link3] quit
[NPE2] bfd link4 bind peer-ip 10.103.1.1 interface gigabitethernet1/0/1.103 source-ip 10.103.1.253
auto
[NPE2-bfd-session-link4] commit
[NPE2-bfd-session-link4] quit
```

完成上述配置且 CE 也正确配置 BFD 会话后，在 NPE 上使用 **display bfd configuration all** 命令查看 BFD 的配置，可以看到“Commit”为 True。

以 NPE1 的显示为例。

```
[NPE1] display bfd configuration all
```

CFG Name	CFG Type	LocalDiscr	MIndex	SessNum	Commit	AdminDown
peer1	S_AUTO_IF	8192	4096	1	True	False
link1	S_AUTO_IF	8193	4097	1	True	False
link2	S_AUTO_IF	8194	4098	1	True	False
link3	S_AUTO_IF	8195	4099	1	True	False
link4	S_AUTO_IF	8196	4100	1	True	False

Total Commit/Uncommit CFG Number : 5/0

在 NPE 上使用 **display bfd session all** 命令查看 BFD 的状态，可以看到“State”为 Up。

以 NPE1 的显示为例。

```
[NPE1] display bfd session all
```

Local	Remote	PeerIpAddr	State	Type	InterfaceName
8192	8192	10.1.1.253	Up	S_AUTO_IF	Eth-Trunk1.1
8193	8192	10.100.1.1	Up	S_AUTO_IF	GigabitEthernet1/0/1.100
8194	8193	10.101.1.1	Up	S_AUTO_IF	GigabitEthernet1/0/1.101
8195	8194	10.102.1.1	Up	S_AUTO_IF	GigabitEthernet1/0/1.102
8196	8195	10.103.1.1	Up	S_AUTO_IF	GigabitEthernet1/0/1.103

Total UP/DOWN Session Number : 5/0

步骤 6 配置 VRRP 通过 BFD Sampling 完成快速切换的功能



说明

因为业务 VRRP 已经与管理 VRRP 绑定，因此，对于 NPE 而言，VRRP 通过 BFD Sampling 完成快速切换的功能，只需要针对接口 Eth-Trunk1.1 上的管理 VRRP 配置即可。

配置 NPE1。

```
[NPE1] interface eth-trunk 1.1
[NPE1-Eth-Trunk1.1] vrrp vrid 10 track bfd-session session-name peer1 peer
[NPE1-Eth-Trunk1.1] vrrp vrid 10 track bfd-session session-name link1 link
[NPE1-Eth-Trunk1.1] vrrp vrid 10 track bfd-session session-name link2 link
[NPE1-Eth-Trunk1.1] vrrp vrid 10 track bfd-session session-name link3 link
[NPE1-Eth-Trunk1.1] vrrp vrid 10 track bfd-session session-name link4 link
[NPE1-Eth-Trunk1.1] vrrp vrid 10 track link-bfd down-number 2
[NPE1-Eth-Trunk1.1] vrrp trigger route
[NPE1-Eth-Trunk1.1] quit
```

配置 NPE2。

```
[NPE2] interface eth-trunk 1.1
[NPE2-Eth-Trunk1.1] vrrp vrid 10 track bfd-session session-name peer1 peer
[NPE2-Eth-Trunk1.1] vrrp vrid 10 track bfd-session session-name link1 link
[NPE2-Eth-Trunk1.1] vrrp vrid 10 track bfd-session session-name link2 link
[NPE2-Eth-Trunk1.1] vrrp vrid 10 track bfd-session session-name link3 link
[NPE2-Eth-Trunk1.1] vrrp vrid 10 track bfd-session session-name link4 link
[NPE2-Eth-Trunk1.1] vrrp vrid 10 track link-bfd down-number 2
[NPE2-Eth-Trunk1.1] vrrp trigger route
[NPE2-Eth-Trunk1.1] quit
```

完成上述配置后，在 NPE 上执行 **display vrrp interface** 命令，可以看到管理 VRRP 已经与 1 个 Peer BFD、4 个 Link BFD 绑定，并且 BFD 的状态都是 Up。

```
[NPE1] display vrrp interface eth-trunk 1.1
Eth-Trunk1.1 | Virtual Router 10
  State           : Master
  Virtual IP      : 10.1.1.1
  PriorityRun     : 120
  PriorityConfig  : 120
  MasterPriority  : 120
  Preempt        : YES      Delay Time : 0
  TimerRun       : 1
  TimerConfig    : 1
  Auth Type      : NONE
  Virtual Mac    : 0000-5e00-010a
  Check TTL      : YES
  Config type    : admin-vrrp
  Config track link-bfd down-number : 2
  Track BFD      : link1      type : link
  BFD-session state : UP
  Track BFD      : link2      type : link
  BFD-session state : UP
  Track BFD      : link3      type : link
  BFD-session state : UP
  Track BFD      : link4      type : link
  BFD-session state : UP
  Track BFD      : peer1      type : peer
  BFD-session state : UP
  Create time    : 2010-06-22 17:33:00
  Last change time : 2010-06-22 17:33:06
[NPE2] display vrrp interface eth-trunk 1.1
Eth-Trunk1.1 | Virtual Router 10
  State           : Backup
  Virtual IP      : 10.1.1.1
  PriorityRun     : 100
  PriorityConfig  : 100
  MasterPriority  : 120
  Preempt        : YES      Delay Time : 0
  TimerRun       : 1
  TimerConfig    : 1
```

```
Auth Type          : NONE
Virtual Mac        : 0000-5e00-010a
Check TTL          : YES
Config type        : admin-vrrp
Config track link-bfd down-number : 2
Track BFD          : link1          type : link
BFD-session state  : UP
Track BFD          : link2          type : link
BFD-session state  : UP
Track BFD          : link3          type : link
BFD-session state  : UP
Track BFD          : link4          type : link
BFD-session state  : UP
Track BFD          : peer1          type : peer
BFD-session state  : UP
Create time        : 2010-06-22 17:35:00
Last change time   : 2010-06-22 17:35:06
```

步骤 7 验证配置结果

完成上述配置后，正常情况下，在 NPE 上执行 **display vrrp brief** 命令，可以看到：

NPE1 上：

- VRID 为 10 的 VRRP，“State”是 Master，“Type”是 Admin。
- 其他 VRID 的 VRRP，“State”是 Master，“Type”是 Member。

```
[NPE1] display vrrp brief
VRID  State      Interface      Type      Virtual IP
-----
10     Master      Eth-Trunk1.1   Admin     10.1.1.1
100    Master      GE1/0/1.100    Member    10.100.1.200
101    Master      GE1/0/1.101    Member    10.101.1.200
102    Master      GE1/0/1.102    Member    10.102.1.200
103    Master      GE1/0/1.103    Member    10.103.1.200
```

NPE2 上：

- VRID 为 10 的 VRRP，“State”是 Backup，“Type”是 Admin。
- 其他 VRID 的 VRRP，“State”是 Backup，“Type”是 Member。

```
[NPE2] display vrrp brief
VRID  State      Interface      Type      Virtual IP
-----
10     Backup      Eth-Trunk1.1   Admin     10.1.1.1
100    Backup      GE1/0/1.100    Member    10.100.1.200
101    Backup      GE1/0/1.101    Member    10.101.1.200
102    Backup      GE1/0/1.102    Member    10.102.1.200
103    Backup      GE1/0/1.103    Member    10.103.1.200
```

在 NPE1 上 **shutdown** 接口 GE1/0/1.100，来模拟 NPE1 和 CE1 之间的故障。

```
[NPE1] interface gigabitethernet1/0/1.100
[NPE1-GigabitEthernet1/0/1.100] shutdown
[NPE1-GigabitEthernet1/0/1.100] quit
```

可以看到 NPE1 与 CE1 之间的 BFD 状态变为 Down。

```
[NPE1] display bfd session all
-----
Local  Remote  PeerIpAddr  State  Type      InterfaceName
-----
8192   8192    10.1.1.253  Up     S_AUTO_IF Eth-Trunk1.1
8193   0        10.100.1.1  Down   S_AUTO_IF GigabitEthernet1/0/1.100
8194   8193    10.101.1.1  Up     S_AUTO_IF GigabitEthernet1/0/1.101
8195   8194    10.102.1.1  Up     S_AUTO_IF GigabitEthernet1/0/1.102
8196   8195    10.103.1.1  Up     S_AUTO_IF GigabitEthernet1/0/1.103
-----
Total UP/DOWN Session Number : 4/1
```

由于本例中，管理 VRRP 监视的 Link BFD 会话 Down 的数目是 2，即只有 2 条或者 2 条以上的 Link BFD 会话状态变为 Down，管理 VRRP 才会进行主备切换。

目前只有 1 条 BFD 的状态为 Down，因此管理 VRRP 不会进行主备切换。

NPE1 上：

- VRID 为 10 的 VRRP，“State”是 Master，“Type”是 Admin。
- VRID 为 100 的 VRRP，“State”变为 Initialize，“Type”是 Member。
- 其他 VRID 的 VRRP，“State”是 Master，“Type”是 Member。

```
[NPE1] display vrrp brief
```

VRID	State	Interface	Type	Virtual IP
10	Master	Eth-Trunk1.1	Admin	10.1.1.1
100	Initialize	GE1/0/1.100	Member	10.100.1.200
101	Master	GE1/0/1.101	Member	10.101.1.200
102	Master	GE1/0/1.102	Member	10.102.1.200
103	Master	GE1/0/1.103	Member	10.103.1.200

NPE2 上：

- VRID 为 10 的 VRRP，“State”是 Backup，“Type”是 Admin。
- 其他 VRID 的 VRRP，“State”是 Backup，“Type”是 Member。

```
[NPE2] display vrrp brief
```

VRID	State	Interface	Type	Virtual IP
10	Backup	Eth-Trunk1.1	Admin	10.1.1.1
100	Backup	GE1/0/1.100	Member	10.100.1.200
101	Backup	GE1/0/1.101	Member	10.101.1.200
102	Backup	GE1/0/1.102	Member	10.102.1.200
103	Backup	GE1/0/1.103	Member	10.103.1.200

在 NPE1 上继续 shutdown 接口 GE1/0/1.101，来模拟 NPE1 和 CE2 之间的故障。

```
[NPE1] interface gigabitethernet1/0/1.101
[NPE1-GigabitEthernet1/0/1.101] shutdown
[NPE1-GigabitEthernet1/0/1.101] quit
```

可以看到 NPE1 与 CE2 之间的 BFD 状态变为 Down。

```
[NPE1] display bfd session all
```

Local	Remote	PeerIpAddr	State	Type	InterfaceName
8192	8192	10.1.1.253	Up	S_AUTO_IF	Eth-Trunk1.1
8193	0	10.100.1.1	Down	S_AUTO_IF	GigabitEthernet1/0/1.100
8194	0	10.101.1.1	Down	S_AUTO_IF	GigabitEthernet1/0/1.101
8195	8194	10.102.1.1	Up	S_AUTO_IF	GigabitEthernet1/0/1.102
8196	8195	10.103.1.1	Up	S_AUTO_IF	GigabitEthernet1/0/1.103

Total UP/DOWN Session Number : 3/2

由于本例中，管理 VRRP 监视的 Link BFD 会话 Down 的数目是 2，即只有 2 条或者 2 条以上的 Link BFD 会话状态变为 Down，管理 VRRP 才会进行主备切换。

此时已经有 2 条 BFD 的状态为 Down，因此管理 VRRP 会进行主备切换。

NPE1 上：

- VRID 为 10 的 VRRP，“State”是 Initialize，“Type”是 Admin。
- 其他 VRID 的 VRRP，“State”是 Initialize，“Type”是 Member。

```
[NPE1] display vrrp brief
```

VRID	State	Interface	Type	Virtual IP

```
-----
10    Initialize Eth-Trunk1.1    Admin    10.1.1.1
100   Initialize GE1/0/1.100     Member   10.100.1.200
101   Initialize GE1/0/1.101     Member   10.101.1.200
102   Initialize GE1/0/1.102     Member   10.102.1.200
103   Initialize GE1/0/1.103     Member   10.103.1.200
-----
```

NPE2 上:

- VRID 为 10 的 VRRP, “State” 是 Master, “Type” 是 Admin。
- 其他 VRID 的 VRRP, “State” 是 Master, “Type” 是 Member。

```
[NPE2] display vrrp brief
VRID   State      Interface      Type      Virtual IP
-----
10     Master      Eth-Trunk1.1   Admin     10.1.1.1
100    Master      GE1/0/1.100    Member    10.100.1.200
101    Master      GE1/0/1.101    Member    10.101.1.200
102    Master      GE1/0/1.102    Member    10.102.1.200
103    Master      GE1/0/1.103    Member    10.103.1.200
-----
```

在 NPE1 上 **undo shutdown** 接口 GE1/0/1.100 和接口 GE1/0/1.101, 来模拟 NPE1 和 CE1 之间、NPE1 和 CE2 之间的故障恢复。

```
[NPE1] interface gigabitethernet1/0/1.100
[NPE1-GigabitEthernet1/0/1.100] undo shutdown
[NPE1-GigabitEthernet1/0/1.100] quit
[NPE1] interface gigabitethernet1/0/1.101
[NPE1-GigabitEthernet1/0/1.101] undo shutdown
[NPE1-GigabitEthernet1/0/1.101] quit
```

可以看到 NPE1 与 CE1 之间、NPE1 与 CE2 之间的 BFD 状态重新变为 Up。

```
[NPE1] display bfd session all
-----
Local  Remote PeerIpAddr    State    Type      InterfaceName
-----
8192   8192   10.1.1.253    Up       S_AUTO_IF Eth-Trunk1.1
8193   8192   10.100.1.1    Up       S_AUTO_IF GigabitEthernet1/0/1.100
8194   8193   10.101.1.1    Up       S_AUTO_IF GigabitEthernet1/0/1.101
8195   8194   10.102.1.1    Up       S_AUTO_IF GigabitEthernet1/0/1.102
8196   8195   10.103.1.1    Up       S_AUTO_IF GigabitEthernet1/0/1.103
-----

Total UP/DOWN Session Number : 5/0
```

NPE 上的 VRRP 状态恢复。

NPE1 上:

- VRID 为 10 的 VRRP, “State” 是 Master, “Type” 是 Admin。
- 其他 VRID 的 VRRP, “State” 是 Master, “Type” 是 Member。

```
[NPE1] display vrrp brief
VRID   State      Interface      Type      Virtual IP
-----
10     Master      Eth-Trunk1.1   Admin     10.1.1.1
100    Master      GE1/0/1.100    Member    10.100.1.200
101    Master      GE1/0/1.101    Member    10.101.1.200
102    Master      GE1/0/1.102    Member    10.102.1.200
103    Master      GE1/0/1.103    Member    10.103.1.200
-----
```

NPE2 上:

- VRID 为 10 的 VRRP, “State” 是 Backup, “Type” 是 Admin。
- 其他 VRID 的 VRRP, “State” 是 Backup, “Type” 是 Member。

```
[NPE2] display vrrp brief
VRID   State      Interface      Type      Virtual IP
-----
```

```
-----
10    Backup    Eth-Trunk1.1    Admin    10.1.1.1
100   Backup    GE1/0/1.100      Member   10.100.1.200
101   Backup    GE1/0/1.101      Member   10.101.1.200
102   Backup    GE1/0/1.102      Member   10.102.1.200
103   Backup    GE1/0/1.103      Member   10.103.1.200
```

----结束

配置文件

- NPE1 的配置文件

```
#
sysname NPE1
#
bfd
#
interface Eth-Trunk1
mode user-termination
#
interface Eth-Trunk1.1
control-vid 1 qinq-termination
qinq termination pe-vid 10 ce-vid 1 to 100
qinq vrrp pe-vid 10 ce-vid 100
ip address 10.1.1.254 255.255.255.0
vrrp vrid 10 virtual-ip 10.1.1.1
admin-vrrp vrid 10 ignore-if-down
vrrp vrid 10 priority 120
vrrp vrid 10 track bfd-session session-name link1 link
vrrp vrid 10 track bfd-session session-name link2 link
vrrp vrid 10 track bfd-session session-name link3 link
vrrp vrid 10 track bfd-session session-name link4 link
vrrp vrid 10 track bfd-session session-name peer1 peer
vrrp vrid 10 track link-bfd down-number 2
vrrp trigger route
arp broadcast enable
#
interface GigabitEthernet1/0/1
undo shutdown
mode user-termination
#
interface GigabitEthernet1/0/1.100
control-vid 100 qinq-termination
qinq termination pe-vid 10 ce-vid 101 to 200
qinq vrrp pe-vid 10 ce-vid 101
ip address 10.100.1.254 255.255.255.0
vrrp vrid 100 virtual-ip 10.100.1.200
vrrp vrid 100 track admin-vrrp interface Eth-Trunk1.1 vrid 10 unflowdown
arp broadcast enable
#
interface GigabitEthernet1/0/1.101
control-vid 101 qinq-termination
qinq termination pe-vid 10 ce-vid 201 to 300
qinq vrrp pe-vid 10 ce-vid 201
ip address 10.101.1.254 255.255.255.0
vrrp vrid 101 virtual-ip 10.101.1.200
vrrp vrid 101 track admin-vrrp interface Eth-Trunk1.1 vrid 10 unflowdown
arp broadcast enable
#
interface GigabitEthernet1/0/1.102
control-vid 102 qinq-termination
qinq termination pe-vid 10 ce-vid 301 to 400
qinq vrrp pe-vid 10 ce-vid 301
ip address 10.102.1.254 255.255.255.0
vrrp vrid 102 virtual-ip 10.102.1.200
vrrp vrid 102 track admin-vrrp interface Eth-Trunk1.1 vrid 10 unflowdown
arp broadcast enable
#
```

```
interface GigabitEthernet1/0/1.103
 control-vid 103 qinq-termination
 qinq termination pe-vid 10 ce-vid 401 to 500
 qinq vrrp pe-vid 10 ce-vid 401
 ip address 10.103.1.254 255.255.255.0
 vrrp vrid 103 virtual-ip 10.103.1.200
 vrrp vrid 103 track admin-vrrp interface Eth-Trunk1.1 vrid 10 unflowdown
 arp broadcast enable
#
interface GigabitEthernet1/0/2
 undo shutdown
 eth-trunk 1
#
interface GigabitEthernet2/0/1
 undo shutdown
 eth-trunk 1
#
bfd link1 bind peer-ip 10.100.1.1 interface GigabitEthernet1/0/1.100 source-ip 10.100.1.254
 auto
 commit
#
bfd link2 bind peer-ip 10.101.1.1 interface GigabitEthernet1/0/1.101 source-ip 10.101.1.254
 auto
 commit
#
bfd link3 bind peer-ip 10.102.1.1 interface GigabitEthernet1/0/1.102 source-ip 10.102.1.254
 auto
 commit
#
bfd link4 bind peer-ip 10.103.1.1 interface GigabitEthernet1/0/1.103 source-ip 10.103.1.254
 auto
 commit
#
bfd peer1 bind peer-ip 10.1.1.253 interface Eth-Trunk1.1 source-ip 10.1.1.254 auto
 commit
#
return
```

● NPE2 的配置文件

```
#
 sysname NPE2
#
 bfd
#
interface Eth-Trunk1
 mode user-termination
#
interface Eth-Trunk1.1
 control-vid 1 qinq-termination
 qinq termination pe-vid 10 ce-vid 1 to 100
 qinq vrrp pe-vid 10 ce-vid 100
 ip address 10.1.1.253 255.255.255.0
 vrrp vrid 10 virtual-ip 10.1.1.1
 admin-vrrp vrid 10 ignore-if-down
 vrrp vrid 10 track bfd-session session-name link1 link
 vrrp vrid 10 track bfd-session session-name link2 link
 vrrp vrid 10 track bfd-session session-name link3 link
 vrrp vrid 10 track bfd-session session-name link4 link
 vrrp vrid 10 track bfd-session session-name peer1 peer
 vrrp vrid 10 track link-bfd down-number 2
 vrrp trigger route
 arp broadcast enable
#
interface GigabitEthernet1/0/1
 undo shutdown
 mode user-termination
#
interface GigabitEthernet1/0/1.100
 control-vid 100 qinq-termination
 qinq termination pe-vid 10 ce-vid 101 to 200
```

```

qinq vrrp pe-vid 10 ce-vid 101
ip address 10.100.1.253 255.255.255.0
vrrp vrid 100 virtual-ip 10.100.1.200
vrrp vrid 100 track admin-vrrp interface Eth-Trunk1.1 vrid 10 unflowdown
arp broadcast enable
#
interface GigabitEthernet1/0/1.101
control-vid 101 qinq-termination
qinq termination pe-vid 10 ce-vid 201 to 300
qinq vrrp pe-vid 10 ce-vid 201
ip address 10.101.1.253 255.255.255.0
vrrp vrid 101 virtual-ip 10.101.1.200
vrrp vrid 101 track admin-vrrp interface Eth-Trunk1.1 vrid 10 unflowdown
arp broadcast enable
#
interface GigabitEthernet1/0/1.102
control-vid 102 qinq-termination
qinq termination pe-vid 10 ce-vid 301 to 400
qinq vrrp pe-vid 10 ce-vid 301
ip address 10.102.1.253 255.255.255.0
vrrp vrid 102 virtual-ip 10.102.1.200
vrrp vrid 102 track admin-vrrp interface Eth-Trunk1.1 vrid 10 unflowdown
arp broadcast enable
#
interface GigabitEthernet1/0/1.103
control-vid 103 qinq-termination
qinq termination pe-vid 10 ce-vid 401 to 500
qinq vrrp pe-vid 10 ce-vid 401
ip address 10.103.1.253 255.255.255.0
vrrp vrid 103 virtual-ip 10.103.1.200
vrrp vrid 103 track admin-vrrp interface Eth-Trunk1.1 vrid 10 unflowdown
arp broadcast enable
#
interface GigabitEthernet1/0/2
undo shutdown
eth-trunk 1
#
interface GigabitEthernet2/0/1
undo shutdown
eth-trunk 1
#
bfd link1 bind peer-ip 10.100.1.1 interface GigabitEthernet1/0/1.100 source-ip 10.100.1.253
auto
commit
#
bfd link2 bind peer-ip 10.101.1.1 interface GigabitEthernet1/0/1.101 source-ip 10.101.1.253
auto
commit
#
bfd link3 bind peer-ip 10.102.1.1 interface GigabitEthernet1/0/1.102 source-ip 10.102.1.253
auto
commit
#
bfd link4 bind peer-ip 10.103.1.1 interface GigabitEthernet1/0/1.103 source-ip 10.103.1.253
auto
commit
#
bfd peer1 bind peer-ip 10.1.1.254 interface Eth-Trunk1.1 source-ip 10.1.1.253 auto
commit
#
return

```

● PE1 得配置文件

```

#
sysname PE1
#
mpls lsr-id 3.3.3.3
mpls
#
mpls l2vpn

```

```
#
vsi ldp1 static
 pwsignal ldp
  vsi-id 100
  peer 5.5.5.5
#
mpls ldp
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 200.1.34.3 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/1
 undo shutdown
#
interface GigabitEthernet1/0/1.1
 vlan-type dot1q 10
 l2 binding vsi ldp1
#
interface GigabitEthernet1/0/3
 undo shutdown
 ip address 200.1.35.3 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 200.1.34.0 0.0.0.255
  network 200.1.35.0 0.0.0.255
#
return
```

● PE2 的配置文件

```
#
sysname PE2
#
mpls lsr-id 4.4.4.4
mpls
#
mpls l2vpn
#
vsi ldp1 static
 pwsignal ldp
  vsi-id 100
  peer 5.5.5.5
#
mpls ldp
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 200.1.34.4 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/1
 undo shutdown
#
interface GigabitEthernet1/0/1.1
 vlan-type dot1q 10
 l2 binding vsi ldp1
#
interface GigabitEthernet1/0/4
 undo shutdown
 ip address 200.1.45.4 255.255.255.0
```



```
mpls
mpls ldp
interface LoopBack1
ip address 4.4.4.4 255.255.255.255
#
ospf 1
area 0.0.0.0
network 4.4.4.4 0.0.0.0
network 200.1.34.0 0.0.0.255
network 200.1.45.0 0.0.0.255
#
return
```

● PE3 的配置文件

```
#
sysname PE3
#
mpls lsr-id 5.5.5.5
mpls
#
mpls l2vpn
#
vsi ldp1 static
pwsignal ldp
vsi-id 100
peer 3.3.3.3
peer 4.4.4.4
#
mpls ldp
#
interface GigabitEthernet1/0/0
undo shutdown
#
interface GigabitEthernet1/0/0.1
vlan-type dot1q 10
l2 binding vsi ldp1
#
interface GigabitEthernet1/0/1
undo shutdown
ip address 200.1.35.5 255.255.255.0
mpls
mpls ldp
#
interface GigabitEthernet1/0/2
undo shutdown
ip address 200.1.45.5 255.255.255.0
mpls
mpls ldp
#
ip address 5.5.5.5 255.255.255.255
#
ospf 1
area 0.0.0.0
network 5.5.5.5 0.0.0.0
network 200.1.35.0 0.0.0.255
network 200.1.45.0 0.0.0.255
#
return
```

● CE 的配置文件

```
#
sysname CE1
#
bfd
#
interface GigabitEthernet1/0/1
undo shutdown
mode user-termination
#
interface GigabitEthernet1/0/1.100
```

```
control-vid 100 qinq-termination
qinq termination pe-vid 10 ce-vid 110
ip address 10.100.1.1 255.255.255.0
arp broadcast enable
#
interface GigabitEthernet1/0/1.101
control-vid 101 qinq-termination
qinq termination pe-vid 10 ce-vid 210
ip address 10.101.1.1 255.255.255.0
arp broadcast enable
#
interface GigabitEthernet1/0/1.102
control-vid 102 qinq-termination
qinq termination pe-vid 10 ce-vid 310
ip address 10.102.1.1 255.255.255.0
arp broadcast enable
#
interface GigabitEthernet1/0/1.103
control-vid 103 qinq-termination
qinq termination pe-vid 10 ce-vid 410
ip address 10.103.1.1 255.255.255.0
arp broadcast enable
#
bfd link11 bind peer-ip 10.100.1.254 interface GigabitEthernet1/0/1.100 source-i
p 10.100.1.1 auto
commit
#
bfd link12 bind peer-ip 10.101.1.254 interface GigabitEthernet1/0/1.101 source-i
p 10.101.1.1 auto
commit
#
bfd link13 bind peer-ip 10.102.1.254 interface GigabitEthernet1/0/1.102 source-i
p 10.102.1.1 auto
commit
#
bfd link14 bind peer-ip 10.103.1.254 interface GigabitEthernet1/0/1.103 source-i
p 10.103.1.1 auto
commit
#
bfd link21 bind peer-ip 10.100.1.253 interface GigabitEthernet1/0/1.100 source-i
p 10.100.1.1 auto
commit
#
bfd link22 bind peer-ip 10.101.1.253 interface GigabitEthernet1/0/1.101 source-i
p 10.101.1.1 auto
commit
#
bfd link23 bind peer-ip 10.102.1.253 interface GigabitEthernet1/0/1.102 source-i
p 10.102.1.1 auto
commit
#
bfd link24 bind peer-ip 10.103.1.253 interface GigabitEthernet1/0/1.103 source-i
p 10.103.1.1 auto
commit
#
return
```

4.14.8 配置 VRRP 在 VLANIF 中的应用示例

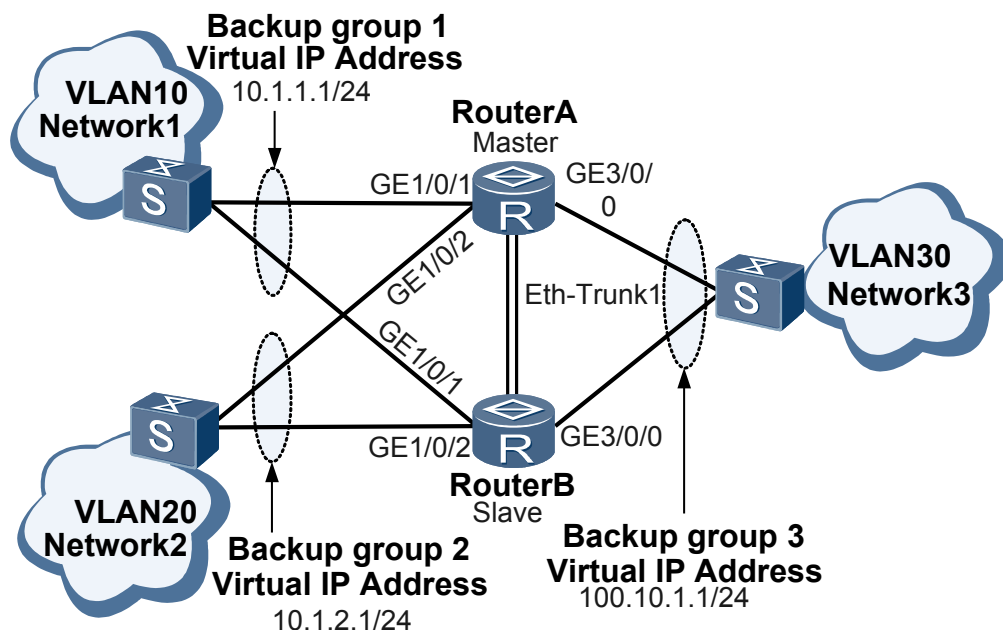
本示例中，通过在 VLANIF 接口上创建 VRRP 备份组，实现 VRRP 的快速切换。

组网需求

如图 4-12 所示，具体组网需求如下：

- RouterA 和 RouterB 两台路由器以主备备份方式工作，其中 RouterA 作为主用，RouterB 作为备用。
- Network1 所属 VLAN10；Network2 所属 VLAN20。两台路由器分别通过 LAN Switch 连接各个网络。
- Network1 对应的备份组虚拟 IP 地址为 10.1.1.1；Network2 对应的备份组虚拟 IP 地址为 10.1.2.1；Network3 对应的备份组虚拟 IP 地址为 100.10.1.1。

图 4-12 VLANIF 支持 VRRP 组网图



RouterA 和 RouterB 分别通过接口 GE1/0/1 连接 Network1，通过 GE1/0/2 连接 Network2，通过 GE3/0/0 连接 Network3。

RouterA 和 RouterB 之间通过 Eth-Trunk1 连接，包含成员端口 GE2/0/0、GE2/0/1。

配置思路

采用如下思路实现 VRRP 快速切换：

1. 配置路由器接口的 IP 地址。
2. 配置 MSTP。
3. 创建 VRRP 备份组并配置优先级。

数据准备

为完成此配置例，需准备如下的数据：

- 物理接口和 VLANIF 接口的 IP 地址。
- RouterA 和 RouterB 的域名 RG1。
- VRRP 备份组 ID、虚拟 IP 地址。

- VRRP 备份组的优先级。

操作步骤

步骤 1 对路由器 RouterA、RouterB 进行接口 IP 地址的配置

以 RouterA 为例。创建 VLAN10、VLAN20，将 GE1/0/1 加入 VLAN10，将 GE1/0/2 加入 VLAN20。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] undo shutdown
[RouterA-GigabitEthernet1/0/1] portswitch
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] undo shutdown
[RouterA-GigabitEthernet1/0/2] portswitch
[RouterA-GigabitEthernet1/0/2] quit
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] undo shutdown
[RouterA-GigabitEthernet3/0/0] ip address 100.10.1.2 255.255.255.0
[RouterA-GigabitEthernet3/0/0] quit
[RouterA] vlan 10
[RouterA-vlan10] port gigabitethernet 1/0/1
[RouterA-vlan10] quit
[RouterA] interface vlanif10
[RouterA-vlanif10] ip address 10.1.1.2 255.255.255.0
[RouterA-vlanif10] quit
[RouterA] vlan 20
[RouterA-vlan20] port gigabitethernet 1/0/2
[RouterA-vlan20] quit
[RouterA] interface vlanif20
[RouterA-vlanif20] ip address 10.1.2.2 255.255.255.0
[RouterA-vlanif20] quit
```

配置 RouterA 和 RouterB 通过 Eth-Trunk 连接。

```
[RouterA] interface eth-trunk1
[RouterA-Eth-Trunk1] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] undo shutdown
[RouterA-GigabitEthernet2/0/0] eth-trunk1
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] undo shutdown
[RouterA-GigabitEthernet2/0/1] eth-trunk1
[RouterA-GigabitEthernet2/0/1] quit
[RouterA] interface eth-trunk1
[RouterA-Eth-Trunk1] portswitch
[RouterA-Eth-Trunk1] port link-type trunk
[RouterA-Eth-Trunk1] port trunk allow-pass vlan 10 20
[RouterA-Eth-Trunk1] quit
```

RouterB 的配置同 RouterA。

步骤 2 配置 MSTP

配置 RouterA 的 MST 域。

```
[RouterA] stp region-configuration
[RouterA-mst-region] region-name RG1
[RouterA-mst-region] instance 1 vlan 10
[RouterA-mst-region] instance 2 vlan 20
```

激活域配置。

```
[RouterA-mst-region] active region-configuration
```

```
[RouterA-mst-region] quit

# 配置 RouterA 的优先级，确保 RouterA 为根桥。

[RouterA] stp instance 1 priority 0

# 启动 MSTP 功能。

[RouterA] interface Eth-Trunk1
[RouterA-Eth-Trunk1] stp enable
[RouterA-Eth-Trunk1] quit
[RouterA] interface GigabitEthernet1/0/1
[RouterA-GigabitEthernet1/0/1] stp enable
[RouterA-GigabitEthernet1/0/1] quit
```

RouterB 的配置同 RouterA。

步骤 3 对路由器 RouterA、RouterB 进行备份组的配置

以 RouterA 为例。配置 RouterA 各接口的 VRRP 备份组。

```
[RouterA] interface vlanif10
[RouterA-vlanif10] vrrp vrid 1 virtual-ip 10.1.1.1
[RouterA-vlanif10] vrrp vrid 1 priority 130
[RouterA-vlanif10] quit
[RouterA] interface vlanif20
[RouterA-vlanif20] vrrp vrid 2 virtual-ip 10.1.2.1
[RouterA-vlanif20] vrrp vrid 2 priority 130
[RouterA-vlanif20] quit
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] vrrp vrid 3 virtual-ip 100.10.1.1
[RouterA-GigabitEthernet3/0/0] vrrp vrid 3 priority 130
[RouterA-GigabitEthernet3/0/0] quit
```

RouterB 的配置同 RouterA。

步骤 4 验证配置结果

分别在 RouterA 和 RouterB 上使用 **display vrrp** 命令查看 VRRP 备份组的信息。

```
[RouterA] display vrrp
Vlanif20 | Virtual Router 2
State           : Master
Virtual IP       : 10.1.2.1
Master IP        : 10.1.2.2
PriorityRun      : 130
PriorityConfig   : 130
MasterPriority   : 130
Preempt         : YES      Delay Time : 0
TimerRun        : 1
TimerConfig     : 1
Auth Type       : NONE
Virtual Mac      : 0000-5e00-0102
Check TTL       : YES
Config type     : normal-vrrp
Create time     : 2010-06-22 17:33:00
Last change time : 2010-06-22 17:33:06
Vlanif10 | Virtual Router 1
State           : Master
Virtual IP       : 10.1.1.1
Master IP        : 10.1.1.2
PriorityRun      : 130
PriorityConfig   : 130
MasterPriority   : 130
Preempt         : YES      Delay Time : 0
TimerRun        : 1
TimerConfig     : 1
Auth Type       : NONE
Virtual Mac      : 0000-5e00-0101
```

```
Check TTL      : YES
Config type    : normal-vrrp
Create time    : 2010-06-22 17:32:00
Last change time : 2010-06-22 17:33:06
<RouterB> display vrrp
Vlanif20 | Virtual Router 2
State      : Backup
Virtual IP  : 10.1.2.1
Master IP   : 10.1.2.3
PriorityRun : 100
PriorityConfig : 100
MasterPriority : 130
Preempt    : YES      Delay Time : 0
TimerRun   : 1
TimerConfig : 1
Auth Type  : NONE
Virtual Mac : 0000-5e00-0102
Check TTL  : YES
Config type : normal-vrrp
Create time : 2010-06-22 17:35:00
Last change time : 2010-06-22 17:35:06
Vlanif10 | Virtual Router 1
State      : Backup
Virtual IP  : 10.1.1.1
Master IP   : 10.1.1.3
PriorityRun : 100
PriorityConfig : 100
MasterPriority : 130
Preempt    : YES      Delay Time : 0
TimerRun   : 1
TimerConfig : 1
Auth Type  : NONE
Virtual Mac : 0000-5e00-0101
Check TTL  : YES
Config type : normal-vrrp
Create time : 2010-06-22 17:34:00
Last change time : 2010-06-22 17:34:06
```

对 RouterA 的接口 VLANIF10 执行 **shutdown** 操作，模拟链路故障。

```
[RouterA] interface vlanif10
[RouterA-Vlanif10] shutdown
[RouterA-Vlanif10] quit
```

此时在 RouterA 上执行 **display vrrp** 命令，可以看到 RouterA 在备份组 1 中的状态变为 **Initialize**。

```
[RouterA] display vrrp
Vlanif20 | Virtual Router 2
State      : Master
Virtual IP  : 10.1.2.1
Master IP   : 10.1.2.2
PriorityRun : 130
PriorityConfig : 130
MasterPriority : 130
Preempt    : YES      Delay Time : 0
TimerRun   : 1
TimerConfig : 1
Auth Type  : NONE
Virtual Mac : 0000-5e00-0102
Check TTL  : YES
Config type : normal-vrrp
Create time : 2010-06-22 17:33:00
Last change time : 2010-06-22 17:33:06
Vlanif10 | Virtual Router 1
State      : Initialize
Virtual IP  : 10.1.1.1
Master IP   : 10.1.1.2
PriorityRun : 130
PriorityConfig : 130
```

```
MasterPriority : 0
Preempt       : YES    Delay Time : 0
TimerRun      : 1
TimerConfig   : 1
Auth Type     : NONE
Virtual Mac    : 0000-5e00-0101
Check TTL     : YES
Config type   : normal-vrrp
Create time    : 2010-06-22 17:36:00
Last change time : 2010-06-22 17:36:06
```

在 RouterB 上执行 **display vrrp** 命令，可以看到 RouterB 在备份组 1 中的状态切换成 Master。

```
[RouterB] display vrrp
Vlanif20 | Virtual Router 2
State      : Backup
Virtual IP  : 10.1.2.1
Master IP   : 10.1.2.3
PriorityRun  : 100
PriorityConfig : 100
MasterPriority : 130
Preempt     : YES    Delay Time : 0
TimerRun    : 1
TimerConfig : 1
Auth Type   : NONE
Virtual Mac  : 0000-5e00-0102
Check TTL   : YES
Config type  : normal-vrrp
Create time  : 2010-06-22 17:35:00
Last change time : 2010-06-22 17:35:06
Vlanif10 | Virtual Router 1
State      : Master
Virtual IP  : 10.1.1.1
Master IP   : 10.1.1.3
PriorityRun  : 100
PriorityConfig : 100
MasterPriority : 100
Preempt     : YES    Delay Time : 0
TimerRun    : 1
TimerConfig : 1
Auth Type   : NONE
Virtual Mac  : 0000-5e00-0101
Check TTL   : YES
Config type  : normal-vrrp
Create time  : 2010-06-22 17:37:00
Last change time : 2010-06-22 17:37:06
```

----结束

配置文件

● RouterA 的配置文件

```
#
sysname RouterA
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 20
#
interface GigabitEthernet3/0/0
undo shutdown
```

```

ip address 100.10.1.2 255.255.255.0
vrrp vrid 3 virtual-ip 100.10.1.1
vrrp vrid 3 priority 130
#
interface GigabitEthernet2/0/0
undo shutdown
eth-trunk 1
#
interface GigabitEthernet2/0/1
undo shutdown
eth-trunk 1
#
interface Vlanif10
ip address 10.1.1.3 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.1
vrrp vrid 1 priority 130
#
interface vlanif20
undo shutdown
ip address 10.1.2.2 255.255.255.0
vrrp vrid 2 virtual-ip 10.1.2.1
vrrp vrid 2 priority 130
#
return
#
interface eth-trunk1
undo shutdown
port link-type trunk
port trunk allow-pass vlan 10 20
#
stp region-configuration
region-name RG1
instance 1 vlan 10
instance 2 vlan 20
active region-configuration
#
Return

```

● RouterB 的配置文件

```

#
sysname RouterB
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port default vlan 10
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port default vlan 20
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 100.10.1.2 255.255.255.0
vrrp vrid 3 virtual-ip 100.10.1.1
vrrp vrid 3 priority 100
#
interface GigabitEthernet2/0/0
undo shutdown
eth-trunk 1
#
interface GigabitEthernet2/0/1
undo shutdown
eth-trunk 1
#
interface vlanif10
undo shutdown
ip address 10.1.1.3 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.1

```



```
vrrp vrid 1 priority 100
#
interface vlanif20
undo shutdown
ip address 10.1.2.3 255.255.255.0
vrrp vrid 2 virtual-ip 10.1.2.1
vrrp vrid 1 priority 100
#
return
#
interface eth-trunk1
undo shutdown
port link-type trunk
port trunk allow-pass vlan 10 20
#
stp region-configuration
region-name RG1
instance 1 vlan 10
instance 2 vlan 20
active region-configuration
#
return
```

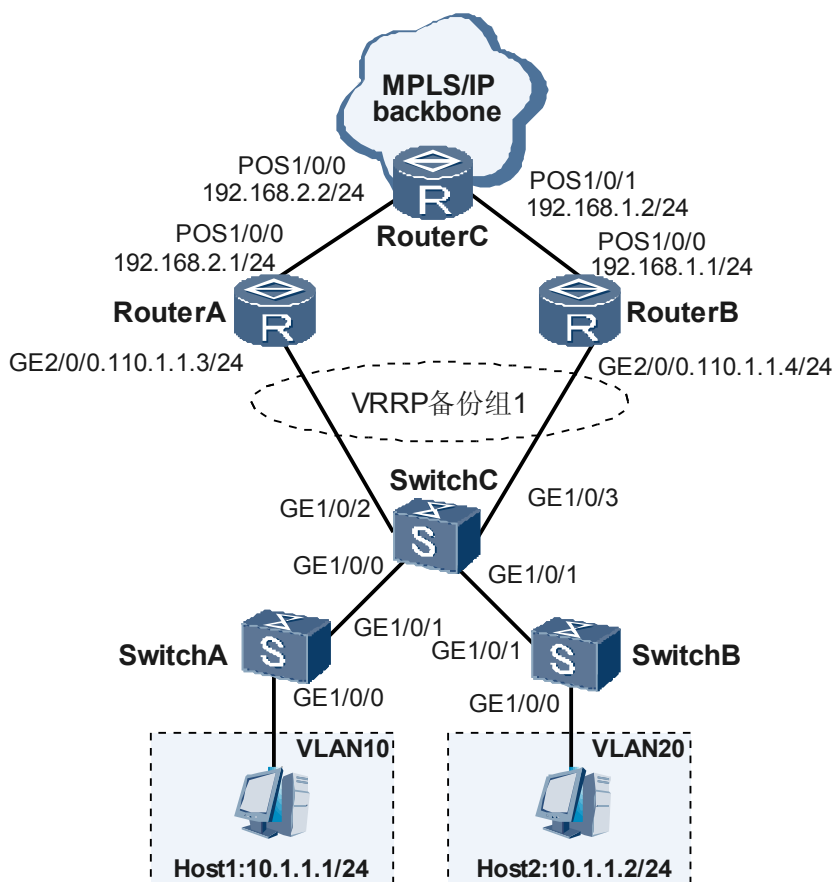
4.14.9 配置 QinQ 终结子接口支持 VRRP 示例（控制免费 ARP 报文方式）

VLAN 用户的缺省网关为 VRRP 备份组。通过控制 Master 设备发送免费 ARP 报文的数量，从而降低 Master 设备的负荷。

组网需求

如图 4-13 所示，VLAN10 和 VLAN20 的用户通过缺省网关访问 ISP 的网络。缺省网关为 VRRP 备份组 1 的虚拟 IP 地址。RouterA 为 Master 设备。正常情况下，RouterA 会根据 QinQ 终结子接口的内外层 Tag 发送免费 ARP 报文。由于内层 Tag 有两个（10 和 20），所以 RouterA 会发送两个免费 ARP 报文来刷新下游交换机的 MAC 表项，从而加重 RouterA 的负担。本示例就是要通过在指定内层 Tag 的 VLAN 内发送免费 ARP 报文，使得在 RouterA 上，对于 VLAN10 和 VLAN20，系统只发送一个免费 ARP 报文，来降低对 RouterA 的负荷。

图 4-13 配置 QinQ 终结子接口支持 VRRP 组网图（控制免费 ARP 报文方式）



配置思路

采用如下的思路配置 QinQ 终结子接口支持 VRRP（控制免费 ARP 报文方式）的基本功能：

1. 配置 RouterA 和 RouterB 的接口模式为用户终结模式。
2. 配置 IGP，使得 RouterA、RouterB 和 RouterC 设备之间可以互通。
3. 配置 RouterA 和 RouterB 的 QinQ 终结子接口。
4. 在 RouterA 的 GE2/0/0 子接口 GE2/0/0.1 上配置 VRRP 备份组 1，确保 RouterA 为 Master 设备；在 RouterB 上配置 VRRP 备份组 1，确保 RouterB 为 Backup 设备。
5. 配置 SwitchC 的 QinQ 功能，使 SwitchC 发送到 RouterA 和 RouterB 的报文带有两层 Tag
6. 配置各 Switch 的基本二层转发功能。

数据准备

为完成此配置例，需准备如下的数据：

- VRRP 备份组号、虚拟 IP 地址、路由器在备份组中的优先级。
- QinQ 终结子接口终结的 Tag 值。

操作步骤

步骤 1 配置接口的模式为用户终结模式

配置 RouterA。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] mode user-termination
[RouterA-GigabitEthernet2/0/0] undo shutdown
[RouterA-GigabitEthernet2/0/0] quit
```

配置 RouterB。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] mode user-termination
[RouterB-GigabitEthernet2/0/0] undo shutdown
[RouterB-GigabitEthernet2/0/0] quit
```

步骤 2 配置设备之间的网络互连，本例采用 OSPF。

配置 RouterA。

```
[RouterA] interface pos 1/0/0
[RouterA-Pos1/0/0] undo shutdown
[RouterA-Pos1/0/0] ip address 192.168.2.1 24
[RouterA-Pos1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0.1
[RouterA-GigabitEthernet2/0/0.1] undo shutdown
[RouterA-GigabitEthernet2/0/0.1] ip address 10.1.1.3 24
[RouterA-GigabitEthernet2/0/0.1] quit
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

配置 RouterB。

```
[RouterB] interface pos 1/0/0
[RouterB-Pos1/0/0] undo shutdown
[RouterB-Pos1/0/0] ip address 192.168.1.1 24
[RouterB-Pos1/0/0] quit
[RouterB] interface gigabitethernet 2/0/0.1
[RouterB-GigabitEthernet2/0/0.1] undo shutdown
[RouterB-GigabitEthernet2/0/0.1] ip address 10.1.1.4 24
[RouterB-GigabitEthernet2/0/0.1] quit
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

配置 RouterC。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterC
[RouterC] interface pos 1/0/0
[RouterC-Pos1/0/0] undo shutdown
[RouterC-Pos1/0/0] ip address 192.168.2.2 24
[RouterC-Pos1/0/0] quit
[RouterC] interface pos 1/0/1
[RouterC-Pos1/0/1] undo shutdown
[RouterC-Pos1/0/1] ip address 192.168.1.2 24
```

```
[RouterC-Pos1/0/1] quit
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[Router3-ospf-1] quit
```

完成此步骤后，RouterA 和 RouterB 相互之间有 OSPF 协议发现的到对方 IP 的路由，并能互相 Ping 通。

以 RouterA 的显示为例。

```
[RouterA] display ip routing-table
Route Flags: R - relied, D - download to fib
-----
Routing Tables: Public
        Destinations : 10          Routes : 11

Destination/Mask    Proto Pre  Cost   Flags NextHop         Interface
-----
10.1.1.0/24        Direct 0     0       D 10.1.1.1       GigabitEthernet2/0/0.1
10.1.1.3/32        Direct 0     0       D 127.0.0.1      InLoopBack0
127.0.0.0/8        Direct 0     0       D 127.0.0.1      InLoopBack0
127.0.0.1/32       Direct 0     0       D 127.0.0.1      InLoopBack0
192.168.1.0/24     OSPF   10    2       D 192.168.2.2    Pos1/0/0
192.168.2.0/24     Direct 0     0       D 192.168.2.1    Pos1/0/0
192.168.2.1/32     Direct 0     0       D 127.0.0.1      InLoopBack0
192.168.2.2/32     Direct 0     0       D 192.168.2.2    Pos1/0/0
```

RouterA 和 RouterB 之间可以相互 Ping 通。

```
[RouterA] ping 192.168.1.1
PING 192.168.1.1: 56 data bytes, press CTRL_C to break
  Reply from 192.168.1.1: bytes=56 Sequence=1 ttl=254 time=110 ms
  Reply from 192.168.1.1: bytes=56 Sequence=2 ttl=254 time=60 ms
  Reply from 192.168.1.1: bytes=56 Sequence=3 ttl=254 time=90 ms
  Reply from 192.168.1.1: bytes=56 Sequence=4 ttl=254 time=90 ms
  Reply from 192.168.1.1: bytes=56 Sequence=5 ttl=254 time=90 ms
--- 192.168.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 60/88/110 ms
```

步骤 3 配置 QinQ 终结子接口支持 VRRP

配置 RouterA，确保 RouterA 为 Master 设备。

```
[RouterA] interface gigabitethernet 2/0/0.1
[RouterA-GigabitEthernet2/0/0.1] control-vid 1 qinq-termination
[RouterA-GigabitEthernet2/0/0.1] qinq termination pe-vid 100 ce-vid 10 to 20
[RouterA-GigabitEthernet2/0/0.1] qinq vrrp pe-vid 100 ce-vid 10
[RouterA-GigabitEthernet2/0/0.1] vrrp vrid 1 virtual-ip 10.1.1.100
[RouterA-GigabitEthernet2/0/0.1] vrrp vrid 1 priority 120
[RouterA-GigabitEthernet2/0/0.1] vrrp arp send-mode simple
[RouterA-GigabitEthernet2/0/0.1] quit
```

配置 RouterB，确保 RouterB 为 Backup 设备。

```
[RouterB] interface gigabitethernet 2/0/0.1
[RouterB-GigabitEthernet2/0/0.1] control-vid 1 qinq-termination
[RouterB-GigabitEthernet2/0/0.1] qinq termination pe-vid 100 ce-vid 10 to 20
[RouterB-GigabitEthernet2/0/0.1] qinq vrrp pe-vid 100 ce-vid 10
[RouterB-GigabitEthernet2/0/0.1] vrrp vrid 1 virtual-ip 10.1.1.100
[RouterB-GigabitEthernet2/0/0.1] vrrp arp send-mode simple
[RouterB-GigabitEthernet2/0/0.1] quit
```

完成此步骤后，RouterA 和 RouterB 的终结子接口 GE2/0/0.1 的状态变为 Up，RouterC 上生成去往 10.1.1.0/24 网段的路由。以 RouterC 的显示为例。

```
[RouterC] display ip routing-table
Route Flags: R - relied, D - download to fib

-----
Routing Tables: Public
      Destinations : 12          Routes : 14

Destination/Mask    Proto Pre  Cost    Flags NextHop          Interface
-----
10.1.1.0/24        OSPF  10    2        D  192.168.1.1        Pos1/0/1
10.1.1.100/32       OSPF  10    2        D  192.168.2.1        Pos1/0/0
127.0.0.0/8         Direct 0     0        D  127.0.0.1          InLoopBack0
127.0.0.1/32        Direct 0     0        D  127.0.0.1          InLoopBack0
192.168.1.0/24       Direct 0     0        D  192.168.1.2        Pos1/0/1
192.168.1.1/32       Direct 0     0        D  192.168.1.1        Pos1/0/1
192.168.1.2/32       Direct 0     0        D  127.0.0.1          InLoopBack0
192.168.2.0/24       Direct 0     0        D  192.168.2.2        Pos1/0/0
192.168.2.1/32       Direct 0     0        D  192.168.2.1        Pos1/0/0
192.168.2.2/32       Direct 0     0        D  127.0.0.1          InLoopBack0
```

步骤4 配置二层转发功能

配置 SwitchA。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 1/0/0
[SwitchA-vlan10] quit
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port trunk allow-pass vlan 10
[SwitchA-GigabitEthernet1/0/1] undo shutdown
[SwitchA-GigabitEthernet1/0/1] quit
```

配置 SwitchB。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchB
[SwitchB] vlan 20
[SwitchB-vlan20] port gigabitethernet 1/0/0
[SwitchB-vlan20] quit
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port trunk allow-pass vlan 20
[SwitchB-GigabitEthernet1/0/1] undo shutdown
[SwitchB-GigabitEthernet1/0/1] quit
```

步骤5 配置 QinQ 功能，使 SwitchC 上送到 RouterA 和 RouterB 的报文带有两层 Tag

配置 SwitchC。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchC
[SwitchC] vlan 100
[SwitchC-vlan100] quit
[SwitchC] interface gigabitethernet 1/0/0
[SwitchC-GigabitEthernet1/0/0] undo shutdown
[SwitchC-GigabitEthernet1/0/0] port vlan-stacking vlan 10 stack-vlan 100
[SwitchC-GigabitEthernet1/0/0] quit
[SwitchC] interface gigabitethernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] undo shutdown
[SwitchC-GigabitEthernet1/0/1] port vlan-stacking vlan 20 stack-vlan 100
[SwitchC-GigabitEthernet1/0/1] quit
[SwitchC] interface gigabitethernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] undo shutdown
[SwitchC-GigabitEthernet1/0/2] port trunk allow-pass vlan 100
[SwitchC-GigabitEthernet1/0/2] quit
[SwitchC] interface gigabitethernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] undo shutdown
[SwitchC-GigabitEthernet1/0/3] port trunk allow-pass vlan 100
[SwitchC-GigabitEthernet1/0/3] quit
```



说明

如果设备不支持 **port vlan-stacking** 命令，也可以在接口上使用 **port link-type dot1q-tunnel** 和 **port default vlan** 来配置 QinQ 功能。

步骤6 验证配置结果

- 完成以上配置后，在 RouterA 上执行 **display vrrp** 命令可以看到 RouterA 在备份组 1 的状态为 Master；在 RouterB 上执行 **display vrrp** 命令可以看到 RouterB 在备份组 1 中的状态为 Backup。

```
[RouterA] display vrrp
GigabitEthernet2/0/0.1 | Virtual Router 1
  state           : Master
  Virtual IP      : 10.1.1.100
  PriorityRun      : 120
  PriorityConfig   : 120
  MasterPriority   : 120
  Preempt         : YES          Delay Time : 0
  Timer           : 1
  Auth Type       : NONE
  Virtual Mac     : 0000-5e00-0101
  Check TTL       : YES
  Config type     : normal-vrrp
Config track link-bfd down-number : 0
  Create time     : 2010-07-09 17:32:56
  Last change time : 2010-07-09 17:33:00
```

```
[RouterB] display vrrp
GigabitEthernet2/0/0.1 | Virtual Router 1
  state           : Backup
  Virtual IP      : 10.1.1.100
  PriorityRun      : 100
  PriorityConfig   : 100
  MasterPriority   : 120
  Preempt         : YES          Delay Time : 0
  Timer           : 1
  Auth Type       : NONE
  Virtual Mac     : 0000-5e00-0101
  Check TTL       : YES
  Config type     : normal-vrrp
Config track link-bfd down-number 0
  Create time     : 2010-07-09 17:33:06
  Last change time : 2010-07-09 17:33:10
```

- 验证 RouterA 故障时 RouterB 能够成为 Master 设备。

对 RouterA 的 GE2/0/0.1 接口执行 **shutdown** 命令，模拟 RouterA 出现故障。

在 RouterA 和 RouterB 分别使用 **display vrrp** 命令查看 VRRP 状态信息，可以看到 RouterA 的状态是 Initialize，RouterB 的状态是 Master。

```
[RouterA] display vrrp
GigabitEthernet2/0/0.1 | Virtual Router 1
  state           : Initialize
  Virtual IP      : 10.1.1.100
  PriorityRun      : 120
  PriorityConfig   : 120
  MasterPriority   : 0
  Preempt         : YES          Delay Time : 0
  Timer           : 1
  Auth Type       : NONE
  Virtual Mac     : 0000-5e00-0101
  Check TTL       : YES
  Config type     : normal-vrrp
Config track link-bfd down-number : 0
  Create time     : 2010-07-09 17:32:56
  Last change time : 2010-07-09 17:33:30
[RouterB] display vrrp
GigabitEthernet2/0/0.1 | Virtual Router 1
  state           : Master
  Virtual IP      : 10.1.1.100
```

```
PriorityRun      : 100
PriorityConfig   : 100
MasterPriority   : 100
Preempt         : YES      Delay Time : 0
Timer           : 1
Auth Type       : NONE
Virtual Mac     : 0000-5e00-0101
Check TTL       : YES
Config type     : normal-vrrp
Config track link-bfd down-number 0
Create time     : 2010-07-09 17:33:06
Last change time : 2010-07-09 17:33:40
```

----结束

配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
interface GigabitEthernet2/0/0
undo shutdown
mode user-termination
#
interface GigabitEthernet2/0/0.1
undo shutdown
control-vid 1 qinq-termination
qinq termination pe-vid 100 ce-vid 10 to 20
qinq vrrp pe-vid 100 ce-vid 10
ip address 10.1.1.3 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.100
vrrp vrid 1 priority 120
vrrp arp send-mode simple
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 192.168.2.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 192.168.2.0 0.0.0.255
network 10.1.1.0 0.0.0.255
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
interface GigabitEthernet2/0/0
undo shutdown
mode user-termination
#
interface GigabitEthernet2/0/0.1
undo shutdown
control-vid 1 qinq-termination
qinq termination pe-vid 100 ce-vid 10 to 20
qinq vrrp pe-vid 100 ce-vid 10
ip address 10.1.1.4 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.100
vrrp arp send-mode simple
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 192.168.1.1 255.255.255.0
```

```
#
ospf 1
 area 0.0.0.0
   network 192.168.1.0 0.0.0.255
   network 10.1.1.0 0.0.0.255
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.2.2 255.255.255.0
#
interface Pos1/0/1
 link-protocol ppp
 undo shutdown
 ip address 192.168.1.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
   network 192.168.1.0 0.0.0.255
   network 192.168.2.0 0.0.0.255
#
return
```

- SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 100
#
interface GigabitEthernet1/0/0
 undo shutdown
 port vlan-stacking vlan 10 stack-vlan 100
#
interface GigabitEthernet1/0/1
 undo shutdown
 port vlan-stacking vlan 20 stack-vlan 100
#
interface GigabitEthernet1/0/2
 undo shutdown
 port trunk allow-pass vlan 100
#
interface GigabitEthernet1/0/3
 undo shutdown
 port trunk allow-pass vlan 100
#
return
```

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10
#
interface GigabitEthernet1/0/0
 undo shutdown
 port default vlan 10
#
interface GigabitEthernet1/0/1
 undo shutdown
 port trunk allow-pass vlan 10
#
return
```


● SwitchB 的配置文件

```
#
sysname SwitchB
#
vlan batch 20
#
interface GigabitEthernet1/0/0
undo shutdown
port default vlan 20
#
interface GigabitEthernet1/0/1
undo shutdown
port trunk allow-pass vlan 20
#
return
```

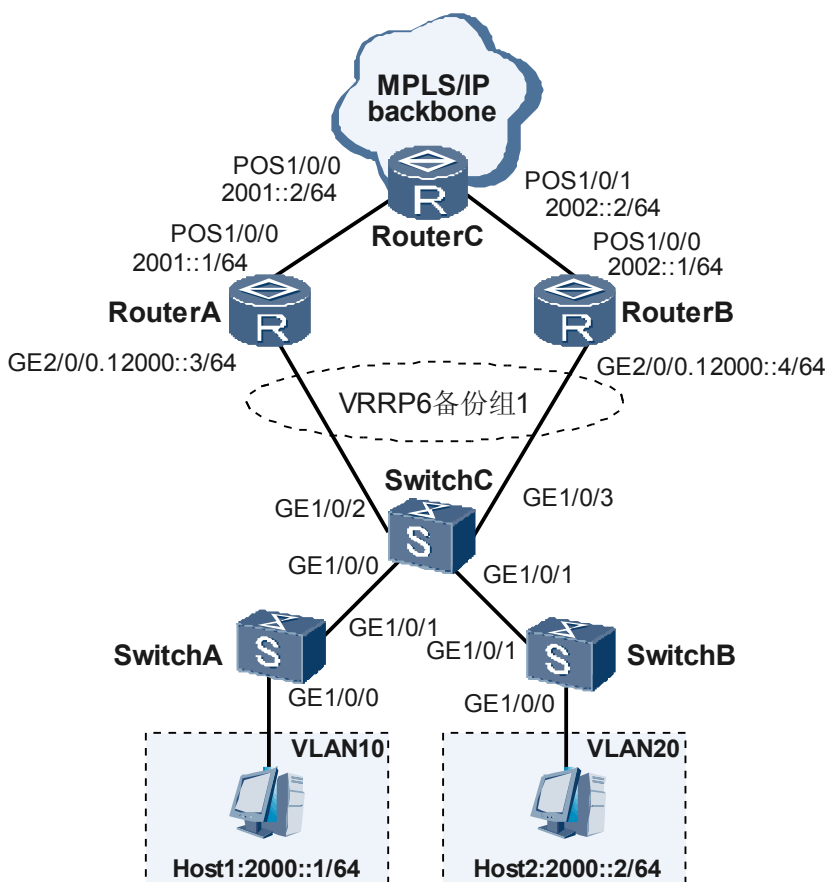
4.14.10 配置 QinQ 终结子接口支持 VRRP6 示例（控制 ND 报文方式）

VLAN 用户的缺省网关为 VRRP6 备份组。通过命令行控制 Master 设备发送 ND 报文的数量，从而降低 Master 设备的负荷。

组网需求

如图 4-14 所示，VLAN10 和 VLAN20 的用户通过缺省网关访问 ISP 的网络。缺省网关为 VRRP6 备份组 1 的虚拟 IP 地址。RouterA 为 Master 设备。正常情况下，RouterA 会根据 QinQ 终结子接口的内外层 Tag 发送 ND 报文。由于内层 Tag 有两个（10 和 20），所以 RouterA 会发送两个 ND 报文来刷新下游交换机的 MAC 表项，从而加重 RouterA 的负担。本示例就是要通过在指定内层 Tag 的 VLAN 内发送 ND 报文，使得在 RouterA 上，对于 VLAN10 和 VLAN20，系统只发送一个 ND 报文，来降低对 RouterA 的负荷。

图 4-14 配置 QinQ 终结子接口支持 VRRP6 组网图（控制 ND 报文方式）



配置思路

采用如下的思路配置 QinQ 终结子接口支持 VRRP6（控制 ND 报文方式）的基本功能：

1. 配置 RouterA 和 RouterB 的接口模式为用户终结模式。
2. 配置 IGP，使得 RouterA、RouterB 和 RouterC 设备之间可以互通。
3. 配置 RouterA 和 RouterB 的 QinQ 终结子接口。
4. 在 RouterA 的 GE2/0/0.1 子接口 GE2/0/0.1 上配置 VRRP6 备份组 1，确保 RouterA 为 Master 设备；在 RouterB 上配置 VRRP6 备份组 1，确保 RouterB 为 Backup 设备。
5. 配置 SwitchC 的 QinQ 功能，使 SwitchC 发送到 RouterA 和 RouterB 的报文带有两层 Tag
6. 配置各 Switch 的基本二层转发功能。

数据准备

为完成此配置例，需准备如下的数据：

- VRRP6 备份组号、虚拟 IPv6 地址、路由器在备份组中的优先级。
- QinQ 终结子接口终结的 Tag 值。

操作步骤

步骤 1 配置接口的模式为用户终结模式

配置 RouterA。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] mode user-termination
[RouterA-GigabitEthernet2/0/0] undo shutdown
[RouterA-GigabitEthernet2/0/0] quit
```

配置 RouterB。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] mode user-termination
[RouterB-GigabitEthernet2/0/0] undo shutdown
[RouterB-GigabitEthernet2/0/0] quit
```

步骤 2 配置设备之间的网络互连，本例采用 OSPFv3。

配置 RouterA。

```
[RouterA] ipv6
[RouterA] ospfv3
[RouterA-ospfv3-1] router-id 1.1.1.1
[RouterA-ospfv3-1] quit
[RouterA] interface pos 1/0/0
[RouterA-Pos1/0/0] undo shutdown
[RouterA-Pos1/0/0] ipv6 enable
[RouterA-Pos1/0/0] ipv6 address 2001::1 64
[RouterA-Pos1/0/0] ospfv3 1 area 0
[RouterA-Pos1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0.1
[RouterA-GigabitEthernet2/0/0.1] undo shutdown
[RouterA-GigabitEthernet2/0/0.1] ipv6 enable
[RouterA-GigabitEthernet2/0/0.1] ipv6 address 2000::3 64
[RouterA-GigabitEthernet2/0/0.1] ospfv3 1 area 0
[RouterA-GigabitEthernet2/0/0.1] quit
```

配置 RouterB。

```
[RouterB] ipv6
[RouterB] ospfv3
[RouterB-ospfv3-1] router-id 2.2.2.2
[RouterB-ospfv3-1] quit
[RouterB] interface pos 1/0/0
[RouterB-Pos1/0/0] undo shutdown
[RouterB-Pos1/0/0] ipv6 enable
[RouterB-Pos1/0/0] ipv6 address 2002::1 64
[RouterB-Pos1/0/0] ospfv3 1 area 0
[RouterB-Pos1/0/0] quit
[RouterB] interface gigabitethernet 2/0/0.1
[RouterB-GigabitEthernet2/0/0.1] undo shutdown
[RouterB-GigabitEthernet2/0/0.1] ipv6 enable
[RouterB-GigabitEthernet2/0/0.1] 2000::4 64
[RouterB-GigabitEthernet2/0/0.1] ospfv3 1 area 0
[RouterB-GigabitEthernet2/0/0.1] quit
```

配置 RouterC。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterC
[RouterC] ipv6
[RouterC] ospfv3
[RouterC-ospfv3-1] router-id 3.3.3.3
```

```
[RouterC-ospfv3-1] quit
[RouterC] interface pos 1/0/0
[RouterC-Pos1/0/0] undo shutdown
[RouterC-Pos1/0/0] ipv6 enable
[RouterC-Pos1/0/0] 2001::2 64
[RouterC-Pos1/0/0] ospfv3 1 area 0
[RouterC-Pos1/0/0] quit
[RouterC] interface pos 1/0/1
[RouterC-Pos1/0/1] undo shutdown
[RouterC-Pos1/0/1] ipv6 enable
[RouterC-Pos1/0/1] 2002::2 64
[RouterC-Pos1/0/1] ospfv3 1 area 0
[RouterC-Pos1/0/1] quit
```

完成此步骤后，RouterA 和 RouterB 相互之间有 OSPFv3 协议发现的到对方的路由，并应能互相 Ping 通。

以 RouterA 的显示为例。

```
[RouterA] display ospfv3 routing
OSPFv3 Process (1)
  Destination                                     Metric
  Next-hop
  2000::/64                                       1
    directly connected, GigabitEthernet2/0/0.1
  2001::/64                                       1
    directly connected, Pos1/0/0
  2002::/64                                       2
    via FE80::217D:7E4B:5888:1, Pos1/0/1
[RouterA] ping ipv6 2002::2
PING 2002::2 : 56 data bytes, press CTRL_C to break
  Reply from 2002::2:
    bytes=56 Sequence=1 hop limit=64  time = 14 ms
  Reply from 2002::2:
    bytes=56 Sequence=2 hop limit=64  time = 14 ms
  Reply from 2002::2:
    bytes=56 Sequence=3 hop limit=64  time = 13 ms
  Reply from 2002::2:
    bytes=56 Sequence=4 hop limit=64  time = 14 ms
  Reply from 2002::2:
    bytes=56 Sequence=5 hop limit=64  time = 13 ms

--- 2002::2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 13/13/14 ms
```

步骤 3 配置 QinQ 终结子接口支持 VRRP6

配置 RouterA，确保 RouterA 为 Master 设备。

```
[RouterA] interface gigabitethernet 2/0/0.1
[RouterA-GigabitEthernet2/0/0.1] control-vid 1 qinq-termination
[RouterA-GigabitEthernet2/0/0.1] qinq termination pe-vid 100 ce-vid 10 to 20
[RouterA-GigabitEthernet2/0/0.1] qinq vrrp pe-vid 100 ce-vid 10
[RouterA-GigabitEthernet2/0/0.1] vrrp6 vrid 1 virtual-ip FE80::1 link-local
[RouterA-GigabitEthernet2/0/0.1] vrrp6 vrid 1 virtua-ip 2000::100
[RouterA-GigabitEthernet2/0/0.1] vrrp6 vrid 1 priority 120
[RouterA-GigabitEthernet2/0/0.1] vrrp6 nd send-mode simple
[RouterA-GigabitEthernet2/0/0.1] quit
```

配置 RouterB，确保 RouterB 为 Backup 设备。

```
[RouterB] interface gigabitethernet 2/0/0.1
[RouterB-GigabitEthernet2/0/0.1] control-vid 1 qinq-termination
[RouterB-GigabitEthernet2/0/0.1] qinq termination pe-vid 100 ce-vid 10 to 20
[RouterB-GigabitEthernet2/0/0.1] qinq vrrp pe-vid 100 ce-vid 10
[RouterB-GigabitEthernet2/0/0.1] vrrp6 vrid 1 virtual-ip FE80::1 link-local
```

```
[RouterB-GigabitEthernet2/0/0.1] vrrp6 vrid 1 virtua-ip 2000::100
[RouterB-GigabitEthernet2/0/0.1] vrrp6 nd send-mode simple
[RouterB-GigabitEthernet2/0/0.1] quit
```

步骤 4 配置二层转发功能

配置 SwitchA。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 1/0/0
[SwitchA-vlan10] quit
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port trunk allow-pass vlan 10
[SwitchA-GigabitEthernet1/0/1] undo shutdown
[SwitchA-GigabitEthernet1/0/1] quit
```

配置 SwitchB。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchB
[SwitchB] vlan 20
[SwitchB-vlan20] port gigabitethernet 1/0/0
[SwitchB-vlan20] quit
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port trunk allow-pass vlan 20
[SwitchB-GigabitEthernet1/0/1] undo shutdown
[SwitchB-GigabitEthernet1/0/1] quit
```

步骤 5 配置 QinQ 功能，使 SwitchC 上送到 RouterA 和 RouterB 的报文带有两层 Tag

配置 SwitchC。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchC
[SwitchC] vlan 100
[SwitchC-vlan100] quit
[SwitchC] interface gigabitethernet 1/0/0
[SwitchC-GigabitEthernet1/0/0] undo shutdown
[SwitchC-GigabitEthernet1/0/0] port vlan-stacking vlan 10 stack-vlan 100
[SwitchC-GigabitEthernet1/0/0] quit
[SwitchC] interface gigabitethernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] undo shutdown
[SwitchC-GigabitEthernet1/0/1] port vlan-stacking vlan 20 stack-vlan 100
[SwitchC-GigabitEthernet1/0/1] quit
[SwitchC] interface gigabitethernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] undo shutdown
[SwitchC-GigabitEthernet1/0/2] port trunk allow-pass vlan 100
[SwitchC-GigabitEthernet1/0/2] quit
[SwitchC] interface gigabitethernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] undo shutdown
[SwitchC-GigabitEthernet1/0/3] port trunk allow-pass vlan 100
[SwitchC-GigabitEthernet1/0/3] quit
```

 说明

如果设备不支持 **port vlan-stacking** 命令，也可以在接口上使用 **port link-type dot1q-tunnel** 和 **port default vlan** 来配置 QinQ 功能。

步骤 6 验证配置结果

- 完成以上配置后，在 RouterA 上执行 **display vrrp6** 命令可以看到 RouterA 在备份组 1 的状态为 Master；在 RouterB 上执行 **display vrrp6** 命令可以看到 RouterB 在备份组 1 中的状态为 Backup。

```
[RouterA] display vrrp6
GigabitEthernet2/0/0.1 | Virtual Router 1
      State                : Master
      Virtual IP            : FE80::1
```

```

                2000::100
PriorityRun      : 120
PriorityConfig   : 120
MasterPriority   : 120
Preempt         : YES      Delay Time : 0
TimerRun        : 100
TimerConfig     : 100
Virtual Mac     : 0000-5e00-0201
Uncheck hop limit : YES
Accept Mode     : ON
Config type     : normal-vrrp
Create time     : 2010-07-09 17:10:56
Last change time : 2010-07-09 17:11:00
[RouterB] display vrrp6
GigabitEthernet2/0/0.1 | Virtual Router 1
State           : Backup
Virtual IP      : FE80::2
                2000::100
PriorityRun      : 100
PriorityConfig   : 100
MasterPriority   : 120
Preempt         : YES      Delay Time : 0
TimerRun        : 100
TimerConfig     : 100
Virtual Mac     : 0000-5e00-0201
Uncheck hop limit : YES
Accept Mode     : ON
Config type     : normal-vrrp
Create time     : 2010-07-09 17:11:24
Last change time : 2010-07-09 17:11:28
```

- 验证 RouterA 故障时 RouterB 能够成为 Master 设备。

对 RouterA 的 GE2/0/0.1 接口执行 **shutdown** 命令，模拟 RouterA 出现故障。

在 RouterA 和 RouterB 分别使用 **display vrrp6** 命令查看 VRRP 状态信息，可以看到 RouterA 的状态是 Initialize，RouterB 的状态是 Master。

```

[RouterA] display vrrp6
GigabitEthernet1/0/0 | Virtual Router 1
State           : Initialize
Virtual IP      : FE80::1
                2000::100
PriorityRun      : 120
PriorityConfig   : 120
MasterPriority   : 0
Preempt         : YES      Delay Time : 0
TimerRun        : 100
TimerConfig     : 100
Virtual Mac     : 0000-5e00-0201
Uncheck hop limit : YES
Accept Mode     : ON
Config type     : normal-vrrp
Create time     : 2010-07-09 17:10:56
Last change time : 2010-07-09 17:12:06
[RouterB] display vrrp6
GigabitEthernet2/0/0.1 | Virtual Router 1
State           : Master
Virtual IP      : FE80::2
                2000::100
PriorityRun      : 100
PriorityConfig   : 100
MasterPriority   : 100
Preempt         : YES      Delay Time : 0
TimerRun        : 100
TimerConfig     : 100
Virtual Mac     : 0000-5e00-0201
Uncheck hop limit : YES
Accept Mode     : ON
Config type     : normal-vrrp
```

Create time : 2010-07-09 17:11:24
Last change time : 2010-07-09 17:12:34

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
ipv6
#
ospfv3 1
 router-id 1.1.1.1
#
interface GigabitEthernet2/0/0
 undo shutdown
 mode user-termination
#
interface GigabitEthernet2/0/0.1
 undo shutdown
 ipv6 enable
 ipv6 address 2000::3/64
 control-vid 1 qinq-termination
 qinq termination pe-vid 100 ce-vid 10 to 20
 qinq vrrp pe-vid 100 ce-vid 10
 vrrp6 vrid 1 virtual-ip FE80::1 link-local
 vrrp6 vrid 1 virtua-ip 2000::100
 vrrp vrid 1 priority 120
 vrrp6 nd send-mode simple
 ospfv3 1 area 0
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ipv6 enable
 ipv6 address 2001::1/64
 ospfv3 1 area 0
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
ipv6
#
ospfv3 1
 router-id 2.2.2.2
#
interface GigabitEthernet2/0/0
 undo shutdown
 mode user-termination
#
interface GigabitEthernet2/0/0.1
 undo shutdown
 undo shutdown
 ipv6 enable
 ipv6 address 2000::4 64/64
 control-vid 1 qinq-termination
 qinq termination pe-vid 100 ce-vid 10 to 20
 qinq vrrp pe-vid 100 ce-vid 10
 vrrp6 vrid 1 virtual-ip FE80::1 link-local
 vrrp6 vrid 1 virtua-ip 2000::100
 vrrp6 nd send-mode simple
 ospfv3 1 area 0
#
```

```
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ipv6 enable
 ipv6 address 2002::1/64
 ospfv3 1 area 0
#
return
```

● RouterC 的配置文件

```
#
 sysname RouterC
#
ipv6
#
ospfv3 1
 router-id 3.3.3.3
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ipv6 enable
 2001::2/64
 ospfv3 1 area 0
#
interface Pos1/0/1
 link-protocol ppp
 undo shutdown
 ipv6 enable
 2002::2/64
 ospfv3 1 area 0
#
return
```

● SwitchC 的配置文件

```
#
 sysname SwitchC
#
 vlan batch 100
#
interface GigabitEthernet1/0/0
 undo shutdown
 port vlan-stacking vlan 10 stack-vlan 100
#
interface GigabitEthernet1/0/1
 undo shutdown
 port vlan-stacking vlan 20 stack-vlan 100
#
interface GigabitEthernet1/0/2
 undo shutdown
 port trunk allow-pass vlan 100
#
interface GigabitEthernet1/0/3
 undo shutdown
 port trunk allow-pass vlan 100
#
return
```

● SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10
#
interface GigabitEthernet1/0/0
 undo shutdown
 port default vlan 10
#
interface GigabitEthernet1/0/1
```



```
undo shutdown
port trunk allow-pass vlan 10
#
return
```

● SwitchB 的配置文件

```
#
sysname SwitchB
#
vlan batch 20
#
interface GigabitEthernet1/0/0
undo shutdown
port default vlan 20
#
interface GigabitEthernet1/0/1
undo shutdown
port trunk allow-pass vlan 20
#
return
```

4.14.11 配置主备备份 VRRP6 示例

组网需求



说明

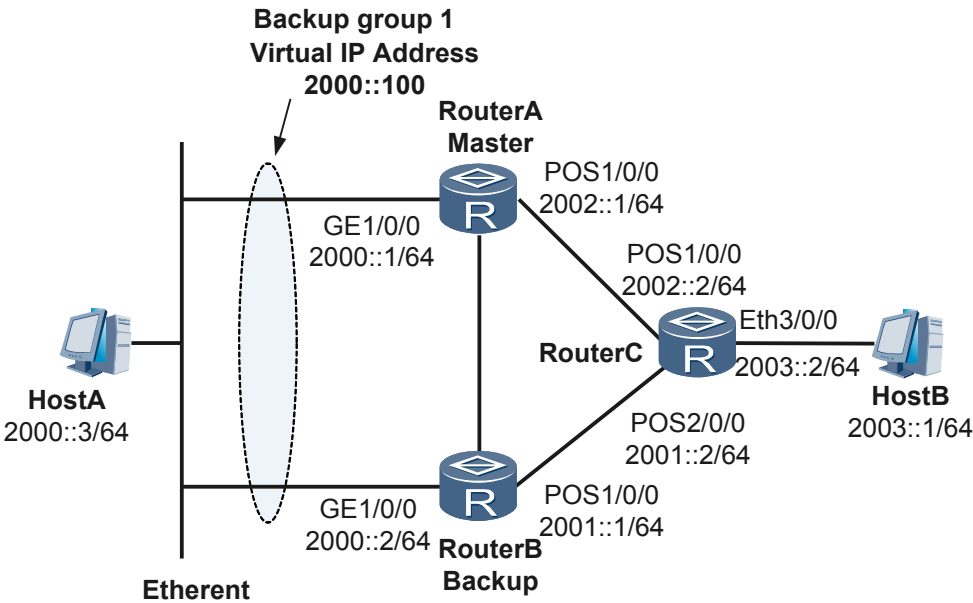
POS 接口特性在 NE80E/40E 系列中的 X1 和 X2 设备上不支持。

如图 4-15 所示，主机 HostA 通过缺省网关 2000::100 访问主机 HostB。

需求如下：

- RouterA 和 RouterB 组成备份组 1，该备份组的虚拟 IPv6 地址作为 HostA 的缺省网关。
- 正常情况下，RouterA 承担网关工作。当 RouterA 出现故障时，RouterB 接替网关执行工作。
- RouterA 故障恢复后，能够在 20 秒内抢占成为 Master 设备。

图 4-15 配置主备备份 VRRP6 组网图



配置思路

采用如下思路配置主备备份 VRRP6:

1. 在 RouterA 的接口 GE1/0/0 下创建备份组 1，并配置 RouterA 在该备份组中具有最高优先级，确保 RouterA 为 Master 设备，且采用抢占方式。
2. 在 RouterB 的接口 GE1/0/0 下创建备份组 1，使用缺省优先级 100，确保 RouterB 在该备份组中为 Backup 设备。

数据准备

为完成此配置例，需准备如下的数据：

- 各个接口的 IPv6 地址。
- 备份组的 ID 和虚拟 IPv6 地址。
- 路由器在备份组中的优先级。

操作步骤

步骤 1 配置主机（略）

配置主机 HostA 的缺省网关为 2000::100，HostB 的缺省网关为 2003::2。

步骤 2 在 RouterA、RouterB 和 RouterC 之间采用 OSPFv3 协议进行互连（略）

步骤 3 配置 VRRP6 备份组

在 RouterA 上配置接口 GE1/0/0 的 IPv6 地址。在接口 GE1/0/0 上创建 VRRP6 备份组 1，并配置 RouterA 在该备份组中的优先级为 120，确保 RouterA 为 Master 设备。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] ipv6
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] undo shutdown
[RouterA-GigabitEthernet1/0/0] ipv6 enable
[RouterA-GigabitEthernet1/0/0] ipv6 address 2000::1 64
[RouterA-GigabitEthernet1/0/0] vrrp6 vrid 1 virtual-ip FE80::1 link-local
[RouterA-GigabitEthernet1/0/0] vrrp6 vrid 1 virtual-ip 2000::100
[RouterA-GigabitEthernet1/0/0] vrrp6 vrid 1 priority 120
[RouterA-GigabitEthernet1/0/0] vrrp6 vrid 1 preempt-mode timer delay 20
[RouterA-GigabitEthernet1/0/0] quit
```

在 RouterB 上配置接口 GE1/0/0 的 IPv6 地址。在接口 GE1/0/0 上创建 VRRP6 备份组 1，并使用缺省优先级 100，确保 RouterA 为 Backup 设备。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] ipv6
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] undo shutdown
[RouterB-GigabitEthernet1/0/0] ipv6 enable
[RouterB-GigabitEthernet1/0/0] ipv6 address 2000::2 64
[RouterB-GigabitEthernet1/0/0] vrrp6 vrid 1 virtual-ip FE80::1 link-local
[RouterB-GigabitEthernet1/0/0] vrrp6 vrid 1 virtual-ip 2000::100
[RouterB-GigabitEthernet1/0/0] quit
```

步骤 4 检验配置结果

完成上述配置后，主机 HostA 能够 Ping 通主机 HostB。在 RouterA 上使用 **display vrrp6** 命令，可以看到 Router 在该备份组中的状态为 Master；在 RouterB 上使用 **display vrrp6** 命令可以看到 RouterB 在该备份组中的状态为 Backup。

```
<RouterA> display vrrp6
GigabitEthernet1/0/0 | Virtual Router 1
      State           : Master
      Virtual IP       : FE80::1
                        2000::100
      PriorityRun      : 120
      PriorityConfig    : 120
      MasterPriority    : 120
      Preempt          : YES      Delay Time : 20
      TimerRun         : 100
      TimerConfig      : 100
      Virtual Mac      : 0000-5e00-0201
      Uncheck hop limit : YES
      Accept Mode      : ON
      Config type      : normal-vrrp
```

```
<RouterB> display vrrp6
GigabitEthernet1/0/0 | Virtual Router 1
      State           : Backup
      Virtual IP       : FE80::1
                        2000::100
      PriorityRun      : 100
      PriorityConfig    : 100
      MasterPriority    : 120
      Preempt          : YES      Delay Time : 0
      TimerRun         : 100
      TimerConfig      : 100
      Virtual Mac      : 0000-5e00-0201
      Uncheck hop limit : YES
      Accept Mode      : ON
      Config type      : normal-vrrp
```

对 RouterA 的接口 GE1/0/0 执行 **shutdown** 操作，模拟 RouterA 出现故障。

在 RouterA 上使用 **display vrrp6** 命令，可以看到 Router 在该备份组中的状态为 Initialize；在 RouterB 上使用 **display vrrp6** 命令可以看到 RouterB 在该备份组中的状态为 Master。

```
<RouterA> display vrrp6
GigabitEthernet1/0/0 | Virtual Router 1
      State           : Initialize
      Virtual IP       : FE80::1
                        2000::100
      PriorityRun      : 120
      PriorityConfig    : 120
      MasterPriority    : 100
      Preempt          : YES      Delay Time : 20
      TimerRun         : 100
      TimerConfig      : 100
      Virtual Mac      : 0000-5e00-0201
      Uncheck hop limit : YES
      Accept Mode      : ON
      Config type      : normal-vrrp
```

```
<RouterB> display vrrp6
GigabitEthernet1/0/0 | Virtual Router 1
      State           : Master
      Virtual IP       : FE80::1
                        2000::100
      PriorityRun      : 100
      PriorityConfig    : 100
      MasterPriority    : 100
      Preempt          : YES      Delay Time : 0
      TimerRun         : 100
      TimerConfig      : 100
      Virtual Mac      : 0000-5e00-0201
```

```
Uncheck hop limit : YES
Accept Mode       : ON
Config type       : normal-vrrp
```

对 RouterA 的接口 GE1/0/0 执行 **undo shutdown** 操作。在接口 GE1/0/0 恢复 Up 后，等待 20 秒，在 RouterA 上使用 **display vrrp6** 命令查看 VRRP6 备份组的状态信息，应该可以看到 RouterA 在该备份组中的状态恢复成 Master。

```
<RouterA> display vrrp6
GigabitEthernet1/0/0 | Virtual Router 1
      State           : Master
      Virtual IP       : FE80::1
                        2000::100
      PriorityRun       : 120
      PriorityConfig    : 120
      MasterPriority    : 120
      Preempt          : YES      Delay Time : 20
      TimerRun         : 100
      TimerConfig      : 100
      Virtual Mac      : 0000-5e00-0201
      Uncheck hop limit : YES
      Accept Mode      : ON
      Config type      : normal-vrrp
```

----结束

配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
ipv6
#
ospfv3 1
router-id 1.1.1.1
#
interface GigabitEthernet1/0/0
undo shutdown
ipv6 enable
ipv6 address 2000::1/64
vrrp6 vrid 1 virtual-ip FE80::1 link-local
vrrp6 vrid 1 virtual-ip 2000::100
vrrp6 vrid 1 priority 120
vrrp6 vrid 1 preempt-mode timer delay 20
ospfv3 1 area 0.0.0.0
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ipv6 enable
ipv6 address 2002::1/64
ospfv3 1 area 0.0.0.0
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
ipv6
#
ospfv3 1
router-id 2.2.2.2
#
interface GigabitEthernet1/0/0
undo shutdown
ipv6 enable
```

```
ipv6 address 2000::2/64
vrrp6 vrid 1 virtual-ip FE80::1 link-local
vrrp6 vrid 1 virtual-ip 2000::100
ospfv3 1 area 0.0.0.0
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ipv6 enable
 ipv6 address 2001::1/64
 ospfv3 1 area 0.0.0.0
#
return
```

● RouterC 的配置文件

```
#
 sysname RouterC
#
 ipv6
#
 ospfv3 1
  router-id 3.3.3.3
#
 interface Ethernet3/0/0
  undo shutdown
  ipv6 enable
  ipv6 address 2003::2/64
  ospfv3 1 area 0.0.0.0
#
 interface Pos1/0/0
  link-protocol ppp
  undo shutdown
  ipv6 enable
  ipv6 address 2002::2
  ospfv3 1 area 0.0.0.0
#
 interface Pos2/0/0
  link-protocol ppp
  undo shutdown
  ipv6 enable
  ipv6 address 2001::2/64
  ospfv3 1 area 0.0.0.0
#
return
```

4.14.12 配置负载分担 VRRP6 示例

组网需求



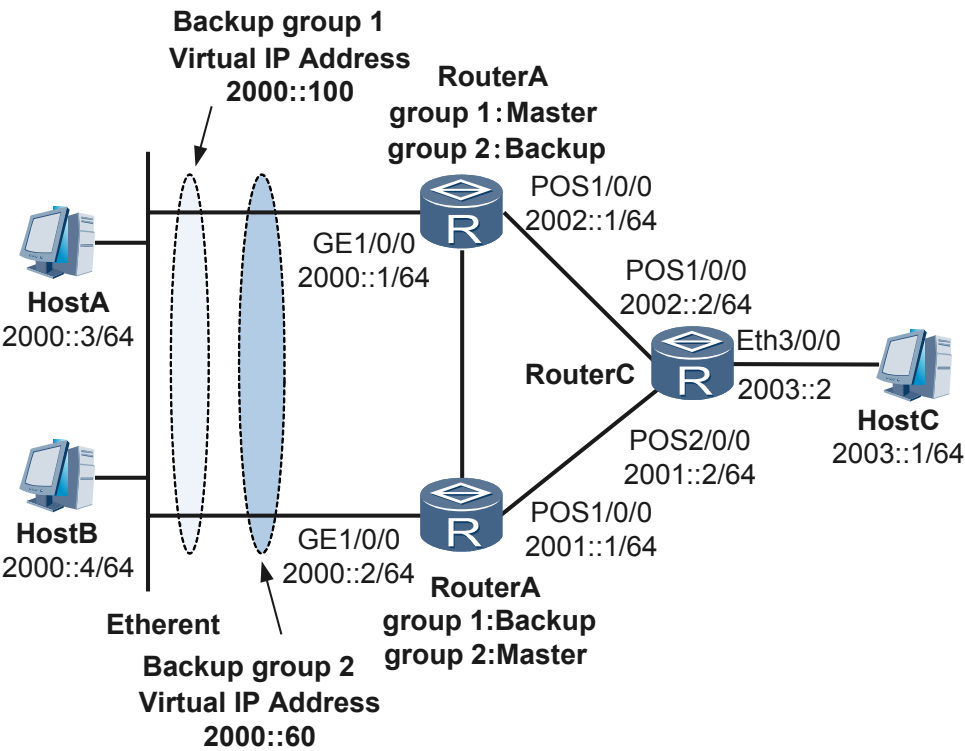
说明

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

如图 4-16 所示。

- RouterA 作为备份组 1 的 Master 设备，同时兼任备份组 2 的 Backup 设备。
- RouterB 作为备份组 2 的 Master 设备，同时兼任备份组 1 的 Backup 设备。
- 局域网中的主机 HostA 使用备份组 1 的虚拟 IPv6 地址作为网关，HostB 使用备份组 2 的虚拟 IPv6 地址作为网关，达到分担数据流而又相互备份的目的。

图 4-16 配置负载分担 VRRP6 组网图



配置思路

采用如下思路配置负载分担 VRRP6 备份组：

1. 在 RouterA 的接口 GE1/0/0 下创建备份组 1 和备份组 2。其中，RouterA 在备份组 1 中作为 Master 设备，在备份组 2 中作为 Backup 设备。
2. 在 RouterB 的接口 GE1/0/0 下创建备份组 1 和备份组 2。其中，RouterB 在备份组 1 中作为 Backup 设备，在备份组 2 中作为 Master 设备。

数据准备

为完成此配置例，需准备如下的数据：

- 各个接口的 IPv6 地址
- 备份组的 ID 和虚拟 IPv6 地址
- 路由器在备份组中的优先级

操作步骤

步骤 1 配置主机

配置主机 HostA 的缺省网关为备份组 1 的虚拟 IPv6 地址 2000::100，主机 HostB 的缺省网关为备份组 2 的 IPv6 地址 2000::60，主机 HostC 的缺省网关为 2003::2。

步骤 2 在 RouterA、RouterB 和 RouterC 之间采用 OSPFv3 协议进行互连（略）

步骤 3 配置 VRRP6 备份组

在 RouterA 上配置接口 GE1/0/0 的 IPv6 地址。在接口 GE1/0/0 上创建备份组 1 和备份组 2，并配置 RouterA 在备份组 1 中的优先级为 120，确保 RouterA 为 Master 设备；在备份组 2 中的优先级使用缺省值 100，确保 RouterA 为 Backup 设备。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] ipv6
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] undo shutdown
[RouterA-GigabitEthernet1/0/0] ipv6 enable
[RouterA-GigabitEthernet1/0/0] ipv6 address 2000::1 64
[RouterA-GigabitEthernet1/0/0] vrrp6 vrid 1 virtual-ip FE80::1 link-local
[RouterA-GigabitEthernet1/0/0] vrrp6 vrid 1 virtual-ip 2000::100
[RouterA-GigabitEthernet1/0/0] vrrp6 vrid 1 priority 120
[RouterA-GigabitEthernet1/0/0] vrrp6 vrid 2 virtual-ip FE80::2 link-local
[RouterA-GigabitEthernet1/0/0] vrrp6 vrid 2 virtual-ip 2000::60
[RouterA-GigabitEthernet1/0/0] quit
```

在 RouterB 上配置接口 GE1/0/0 的 IPv6 地址。在接口 GE1/0/0 上创建备份组 1 和备份组 2，并配置 RouterB 在备份组 1 中的优先级使用缺省值，确保 RouterB 为 Backup 设备；在备份组 2 中的优先级为 120，确保 RouterB 为 Master 设备。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] ipv6
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] undo shutdown
[RouterB-GigabitEthernet1/0/0] ipv6 enable
[RouterB-GigabitEthernet1/0/0] ipv6 address 2000::2 64
[RouterB-GigabitEthernet1/0/0] vrrp6 vrid 1 virtual-ip FE80::1 link-local
[RouterB-GigabitEthernet1/0/0] vrrp6 vrid 1 virtual-ip 2000::100
[RouterB-GigabitEthernet1/0/0] vrrp6 vrid 2 virtual-ip FE80::2 link-local
[RouterB-GigabitEthernet1/0/0] vrrp6 vrid 2 virtual-ip 2000::60
[RouterB-GigabitEthernet1/0/0] vrrp6 vrid 2 priority 120
[RouterB-GigabitEthernet1/0/0] quit
```

步骤 4 检查配置结果

完成上述配置后，网络中的 HostA 和 HostB 分别能够 Ping 通 HostC。在 RouterA 上使用 **display vrrp6** 命令，可以看到创建了两个备份组，备份组 1 和备份组 2。其中，RouterA 在备份组 1 中作为 Master 设备，在备份组 2 中作为 Backup 设备。

```
<RouterA> display vrrp6
GigabitEthernet1/0/0 | Virtual Router 1
      State           : Master
      Virtual IP       : FE80::1
                        2000::100
      PriorityRun      : 120
      PriorityConfig    : 120
      MasterPriority    : 120
      Preempt          : YES      Delay Time : 0
      TimerRun         : 100
      TimerConfig      : 100
      Virtual Mac      : 0000-5e00-0201
      Uncheck hop limit : YES
      Accept Mode      : ON
      Config type      : normal-vrrp
GigabitEthernet1/0/0 | Virtual Router 2
      State           : Backup
      Virtual IP       : FE80::2
                        2000::60
      PriorityRun      : 100
      PriorityConfig    : 100
      MasterPriority    : 120
      Preempt          : YES      Delay Time : 0
```

```
TimerRun      : 100
TimerConfig   : 100
Virtual Mac   : 0000-5e00-0102
Uncheck hop limit : YES
Accept Mode   : ON
Config type   : normal-vrrp
```

在 RouterB 上使用 **display vrrp6** 命令，可以查看创建了两个备份组，备份组 1 和备份组 2。其中，RouterA 在备份组 1 中作为 Backup 设备，RouterB 在备份组 2 中作为 Master 设备。

```
<RouterA> display vrrp6
GigabitEthernet1/0/0 | Virtual Router 1
    State      : Backup
    Virtual IP  : FE80::1
                  2000::100
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 120
    Preempt     : YES      Delay Time : 0
    TimerRun    : 100
    TimerConfig : 100
    Virtual Mac : 0000-5e00-0201
    Uncheck hop limit : YES
    Accept Mode : ON
    Config type : normal-vrrp
GigabitEthernet1/0/0 | Virtual Router 2
    State      : Master
    Virtual IP  : FE80::2
                  2000::60
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt     : YES      Delay Time : 0
    TimerRun    : 100
    TimerConfig : 100
    Virtual Mac : 0000-5e00-0102
    Uncheck hop limit : YES
    Accept Mode : ON
    Config type : normal-vrrp
```

----结束

配置文件

● RouterA 的配置文件

```
#
sysname RouterA
#
ipv6
#
ospfv3 1
router-id 1.1.1.1
#
interface GigabitEthernet1/0/0
undo shutdown
ipv6 enable
ipv6 address 2000::1/64
vrrp6 vrid 1 virtual-ip FE80::1 link-local
vrrp6 vrid 1 virtual-ip 2000::100
vrrp6 vrid 1 priority 120
vrrp6 vrid 2 virtual-ip FE80::2 link-local
vrrp6 vrid 2 virtual-ip 2000::60
ospfv3 1 area 0.0.0.0
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
```



```
        ipv6 enable
        ipv6 address 2002::1/64
        ospfv3 1 area 0.0.0.0
    #
return
```

● RouterB 的配置文件

```
#
sysname RouterB
#
ipv6
#
ospfv3 1
router-id 1.1.1.1
#
interface GigabitEthernet1/0/0
undo shutdown
ipv6 enable
ipv6 address 2000::2/64
vrrp6 vrid 1 virtual-ip FE80::1 link-local
vrrp6 vrid 1 virtual-ip 2000::100
vrrp6 vrid 2 virtual-ip FE80::2 link-local
vrrp6 vrid 2 virtual-ip 2000::60
vrrp6 vrid 2 priority 120
ospfv3 1 area 0.0.0.0
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ipv6 enable
ipv6 address 2001::1/64
ospfv3 1 area 0.0.0.0
#
return
```

● RouterC 的配置文件

```
#
sysname RouterC
#
ipv6
#
ospfv3 1
router-id 3.3.3.3
#
interface Ethernet3/0/0
undo shutdown
ipv6 enable
ipv6 address 2003::2/64
ospfv3 1 area 0.0.0.0
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ipv6 enable
ipv6 address 2002::2
ospfv3 1 area 0.0.0.0
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ipv6 enable
ipv6 address 2001::2/64
ospfv3 1 area 0.0.0.0
#
return
```

5 BFD 配置

关于本章

通过创建 BFD 会话，可以实现快速检测网络中链路故障。

5.1 BFD 简介

BFD 检测机制可以快速检测到与相邻设备间的通信故障，减小设备故障对业务的影响。

5.2 配置 BFD 单跳检测

通过配置 BFD 单跳检测，实现快速检测和监控网络中的直连链路。

5.3 配置 BFD 被动回声功能

通过配置 BFD 被动回声功能，实现与网络中支持回声功能的设备互通。它只能应用于 BFD 单跳检测。

5.4 配置 BFD 状态与接口状态联动

通过配置 BFD 状态与接口状态联动，触发路由快速收敛。它只能应用于缺省组播 IP 地址检测的单跳 BFD 会话中。

5.5 配置 BFD 状态与子接口状态联动

通过配置 BFD 状态与子接口状态联动，触发路由快速收敛。它只能应用于缺省组播 IP 地址检测的单跳 BFD 会话中。

5.6 配置 BFD 修改端口状态表

通过配置 BFD 修改端口状态表，实现 BFD 会话更加快速的检测链路的故障。它只能应用在 BFD 单跳检测中。

5.7 配置 BFD 多跳检测

配置 BFD 多跳检测，实现快速检测和监控网络中的多跳路径。

5.8 配置静态标识符自协商 BFD

通过配置静态标识符自协商 BFD，实现与采用动态建立 BFD 会话的设备互通。它主要应用在静态路由中。

5.9 配置 BFD 会话延迟 UP 功能

特殊场景中，通过配置 BFD 会话延迟 UP 功能，避免由于路由协议 UP 晚于接口 UP 而导致的流量丢失问题。

5.10 配置单臂 ECHO 功能

通过配置单臂 ECHO 功能，实现快速检测和监控网络中的直连链路。

5.11 调整 BFD 检测参数

通过调整 BFD 检测参数，实现 BFD 会话更好、更快速的检测和监控网络中的链路。

5.12 配置全局多跳端口号功能

通过配置全局多跳端口号功能，实现同以前版本的设备或者其它厂商的设备互通。

5.13 配置全局 TTL 功能

通过配置全局 TTL 功能，实现和以前版本的设备互通。

5.14 配置 Trap 消息定时器的时间间隔

通过配置 Trap 消息定时器的时间间隔，实现对 BFD 的告警信息进行抑制。

5.15 维护 BFD

通过维护 BFD，可以实现清除 BFD 统计数据和监控 BFD 的运行状况的目的。

5.16 配置举例

介绍 BFD 快速检测链路的各种示例。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

5.1 BFD 简介

BFD 检测机制可以快速检测到与相邻设备间的通信故障，减小设备故障对业务的影响。

5.1.1 BFD 概述

BFD 是一套全网统一的检测机制，用于快速检测、监控网络中链路或者 IP 路由的转发连通状况。

在现有网络中，通常采用以下几种方法检测链路故障：

- 通过硬件检测信号，如 SDH 告警，检测链路硬件故障。它的优点是可以很快的发现故障。
- 如果无法通过硬件信号检测故障，通常采用路由协议的 Hello 报文机制。

存在的问题如下：

- 并不是所有的介质都能够提供硬件检测。
- 路由协议的 Hello 报文机制检测到故障所需时间比较长，超过 1 秒钟。当数据达到吉比特速率级时，在此检测时间内，大量数据将会丢失。
- 在小型三层网络中，如果没有部署路由协议，则无法使用路由协议的 Hello 报文机制来检测故障。这对系统间互联互通定位故障造成困难。

BFD 就是为解决上述三个问题而产生的。

BFD 提供如下功能：

- 对相邻转发引擎之间的通道故障提供轻负荷、短持续时间的检测。
- 用单一的机制对任何介质、任何协议层进行实时检测，并支持不同的检测时间与开销。

5.1.2 NE80E/40E 支持的 BFD 特性

BFD 特性包括：会话建立方式、两种检测模式、单跳检测和多跳检测、被动回声功能、会话状态与接口状态联动、动态改变参数、BFD 绑定 VPN 实例、BFD for VRRP、BFD for 静态路由、BFD for 路由协议、BFD 触发快速重路由、BFD for IS-IS、BFD for LSP、BFD for PW、BFD for VSI PW 和 BFD for PIM。

作为一种全网统一的检测机制，BFD 可以为多种协议所用。

本节简单介绍 NE80E/40E 中 BFD 提供的的应用支持。

NE80E/40E 支持的 BFD 会话建立方式

BFD 使用本地标识符（Local Discriminator）和远端标识符（Remote Discriminator）区分同一对系统之间的多个 BFD 会话。按照本地标识符和远端标识符创建方式的差异区分，NE80E/40E 支持以下 BFD 会话类型：

- 手工指定标识符的静态 BFD 会话
- 标识符自协商的静态 BFD 会话
- 协议触发的动态 BFD 会话

协议触发的动态 BFD 会话的实现方式是：

- 动态分配本端标识符
- 自学习远端标识符

 说明

目前 NE80E/40E 支持 OSPF、BGP、IS-IS、MPLS、MPLS LDP、RSVP-TE、PWE3、PIM 协议动态触发创建 BFD 会话。

当建立 BFD 会话的两端采用的创建标识符的方式不同时：

- 如果本端采用手工指定标识符，则对端也必须手工指定标识符。
- 如果本端采用静态标识符自协商，则对端既可以配置静态标识符自协商，也可以配置动态 BFD。
- 当本端既配置了静态标识符自协商 BFD，又配置了动态 BFD 时，将按如下原则处理：
 - 如果动态 BFD 和静态标识符自协商 BFD 共用同一个配置属性四元组（源地址、目的地址、出接口、VPN 索引），将采用动态会话共享会话的流程，将静态标识符自协商类型和动态会话共用。
 - 如果先配置了动态 BFD（此时的配置名称为 DYN_本端标识符），然后再配置标识符自协商的静态 BFD，将更新配置名称为静态 BFD 名称。
 - 共用会话的参数采用共用会话的最小值。

目前支持的动态共用会话包括：BFD for OSPF、BFD for IS-IS、BFD for BGP、BFD for PIM、BFD for RSVP-TE。

检测模式

NE80E/40E 实现 BFD 异步检测模式。

异步模式：

各系统间按照协商好的周期发送 BFD 控制报文，如果某个系统在检测时间内没有收到对端发来的 BFD 控制报文，置会话为 Down。

单跳检测和多跳检测

NE80E/40E 支持 BFD 单跳检测和多跳检测。单跳检测和多跳检测用来检测 IP 路由的连通性。本节主要介绍单跳检测的支持情况。

NE80E/40E 支持对以下类型链路的 BFD 单跳检测：

 说明

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

- 三层物理接口
- 以太网接口（包括 Eth-Trunk 子接口）：

对于一个物理以太网口有多个子接口的情况，BFD 会话可以独立建立在各个子接口上和此物理以太网口上。
- QinQ 终结子接口和 Dot1q 终结子接口
- IP-Trunk
 - IP-Trunk 链路
 - IP-Trunk 成员链路

检测 IP-Trunk 成员口与检测 IP-Trunk 口的 BFD 会话互相独立，可同时检测。

- Eth-Trunk
 - 二层 Eth-Trunk 链路
 - 二层 Eth-Trunk 成员链路
 - 三层 Eth-Trunk 链路
 - 三层 Eth-Trunk 成员链路

检测 Trunk 成员口与检测 Trunk 口的 BFD 会话互相独立，可同时检测。



说明

- IP-Trunk 和 Eth-Trunk 都由多条成员链路组成，用于提供大带宽或增强可靠性。
- 只有处于 UP 状态的成员链路条数达到一定数目时，相应的 Trunk 才能保持 UP 状态。
- IP-Trunk 的具体配置信息请参考《HUAWEI NetEngine80E/40E 路由器 配置指南-广域网接入》，Eth-Trunk 的具体配置信息请参考《HUAWEI NetEngine80E/40E 路由器 配置指南-局域网与城域网接入》。
- VLANIF
 - VLAN 以太成员链路
 - VLANIF 接口

检测 VLANIF 与检测 VLANIF 成员口的 BFD 会话相互独立，可同时检测。

单臂回声功能

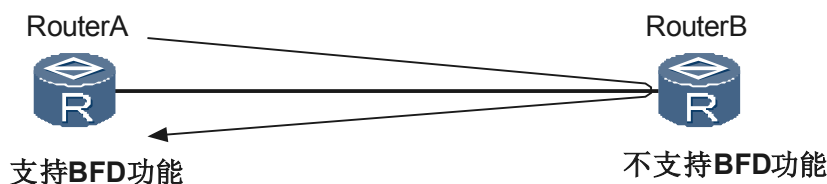
在两台直接相连的设备中，其中，一台设备支持 BFD 功能，另一台设备不支持 BFD 功能，只支持基本的网络层转发。为了能够快速检测这两台设备之间的故障，可以在支持 BFD 功能的设备上创建单臂回声功能的 BFD 会话。支持 BFD 功能的设备主动发起回声请求功能，不支持 BFD 功能的设备接收到该报文后直接将其环回，从而实现转发链路的连通性检测功能。



说明

单臂回声功能只适用于单跳 BFD 会话中。

图 5-1 单臂回声功能组网示意图



如图 5-1 所示，RouterA 支持 BFD 功能，RouterB 不支持 BFD 功能。在 RouterA 上配置单臂回声功能的 BFD 会话，检测 RouterA 到 RouterB 之间的单跳路径。RouterB 接收到 RouterA 发送的 BFD 报文后，直接在网络层将该报文环回，从而快速检测 RouterA 和 RouterB 之间的直连链路的连通性。

BFD 会话状态与接口状态联动

当直连链路中间存在传输设备时，与接口本身的链路协议故障检测机制相比，BFD 能够更快地检测到链路故障。另外对于 Trunk 或 VLANIF 等逻辑接口来说，链路协议状态是由其成员接口的链路协议状态决定的。

因此，为了将 BFD 检测结果更快地通告到应用程序，在接口管理模块中，对每个接口增加了一个属性，即 BFD 状态，指的是与该接口绑定的 BFD 会话的状态（对于子接口来说，也可能是与其主接口绑定的 BFD 会话的状态），系统根据接口的链路状态、协议状态和 BFD 状态决定接口的状态，并将结果通告给应用程序。

BFD 会话状态与接口状态联动功能是指当 BFD 会话的状态变化时，直接修改 IFNET 模块中接口的 BFD 状态。该功能是针对绑定出接口、且使用缺省组播地址进行检测的单跳 BFD 会话的，包括两个方面：

- BFD 会话状态与其绑定的接口状态联动

- 当 BFD 会话状态变为 Down 时，与其绑定的接口的 BFD 状态变为 Down，然后将接口状态通告给接口上的应用。

对于检测 Trunk 成员口或者 VLAN 成员口的 BFD 会话来说，状态变为 Down 时，Trunk 成员口或者 VLAN 成员口的链路协议状态会随之变化，从而加快 Trunk 接口或者 VLAN 成员口的链路协议状态改变，加速 Trunk 接口或者 VLANIF 接口的路由收敛。

 说明

对于成员口在不同接口板上的 Trunk，在配置 Bfd 会话检测 Trunk 成员口之间的链路时，需要在会话中同时配置 process-pst 命令与接口联动；否则某些场景下(如重启 Trunk 成员口所在板)可能会引起流量丢失。

- 当 BFD 会话的状态变为 Up 时，与其绑定的接口的 BFD 状态变为 Up。

该功能的主要目的是将 BFD 检测结果更快地通告给应用程序。

- BFD 会话状态与绑定接口的子接口状态联动

BFD 会话绑定的接口必须是主接口。

- 当 BFD 会话的状态变为 Down 时，与其绑定的接口及其所有子接口的 BFD 状态都变为 Down，然后通告给子接口上的应用程序。

对于子接口上配置业务（如 L2VPN）来说，可以直接使用 BFD 会话的检测结果。

- 当 BFD 会话的状态恢复为 Up 时，与其绑定的接口及其所有子接口的 BFD 状态都变为 Up。

该功能的主要目的是节约系统的会话资源，为更多的应用提供可靠性保障。主要使用在子接口上配置大量业务同时对可靠性要求高的组网方案中，如大规模的城域以太网。

动态改变 BFD 参数

BFD 会话建立后，用户可以改变 BFD 的相关配置参数，例如最小发送间隔、最小接收间隔、检测模式等，不影响会话的当前状态。

BFD 绑定 VPN 实例

NE80E/40E 支持 BFD 会话绑定到 VPN 实例，实现 BFD 控制报文在指定 VPN 发送。

BFD for VRRP

使用 BFD 检测、监控网络中链路或者 IP 路由的转发连通状况，触发 VRRP 快速切换。



说明

BFD for VRRP 的具体配置请参考“VRRP 配置”。

BFD for 静态路由

静态路由自身没有检测机制，当网络发生故障时需要管理员介入。

使用 BFD for 静态路由特性，可以利用 BFD 会话检测对公网 IPv4 静态路由的状态。路由管理系统根据 BFD 会话的状态决定静态路由是否可用。



说明

BFD for 静态路由的具体配置请参考《HUAWEI NetEngine80E/40E 路由器 配置指南 IP 路由》中的“静态路由配置”。

BFD for 路由协议

BFD 使用本地标识符（Local Discriminator）和远端标识符（Remote Discriminator）区分同一对系统之间的多个 BFD 会话。IS-IS 协议支持动态和静态方式建立 BFD 会话，BGP 协议和 OSPF 协议支持动态建立 BFD 会话。

路由协议动态触发建立 BFD 会话的实现方式是：

- 动态分配本地标识符
- 自学习远端标识符

当路由协议邻居建立成功时，路由协议通过路由管理模块通知 BFD 建立会话，对路由协议的邻居关系进行快速检测。BFD 会话的检测参数由路由协议设置。

当 BFD 会话检测到故障时，状态变为 Down，BFD 通过路由管理模块触发路由收敛。



说明

一般的路由协议基于 Hello 报文的 KeepAlive 机制，只能实现秒级检测，而 BFD 检测是毫秒级，采用 10ms 检测周期，3 倍检测间隔时，可以在 50ms 内通报协议故障，因此能够提高路由的收敛速度。

当邻居状态不可达时，路由协议通过路由管理模块通知 BFD 删除相应会话。

BFD 触发快速重路由

- BFD for LDP FRR
对于 MPLS 采用软件转发的产品，可以通过 BFD 检测被保护的接口，触发 LDP FRR 切换。
- BFD for IP FRR 以及 BFD for VPN FRR
在 NE80E/40E 中，通过 BFD 检测故障的上报，可以触发 IP FRR 以及 VPN FRR。
- BFD 能够为 VPN FRR、TE FRR、VLL FRR 等各种基于 MPLS 网络的应用提供可靠性，达到业务保护的目的。

BFD for IS-IS

NE80E/40E 支持使用静态配置的 BFD 会话对 IS-IS 邻居关系进行检测。

通过 BFD 检测 IS-IS 邻居节点间的链路故障，快速报告给 IS-IS 协议，从而触发 IS-IS 路由快速收敛。

 说明

- 由于 ISIS 只能建立单跳邻居，BFD 只对 IS-IS 邻居间的单跳链路进行检测。
- BFD for IS-IS 的具体配置请参考《HUAWEI NetEngine80E/40E 路由器 配置指南 IP 路由》中的“IS-IS 配置”。

BFD for LSP

BFD 可以用来检测 MPLS LSP 转发路径上数据平面的故障，同时 BFD 的报文格式是固定的，非常适合在硬件上实现和穿越防火墙。因此用 BFD 检测 MPLS LSP 数据平面的故障具有以下优势：

- 反向只要求 IP 路由可达
- 快速检测
- 支持大规模 LSP 的故障检测

检测 MPLS LSP 的连通性时，BFD 会话协商有两种方式：

- 静态配置 BFD：通过手工配置 BFD 的本地标识符和远端标识符，由 BFD 本身的协商机制建立会话。
- 动态创建 BFD 会话：通过在 LSP Ping 报文中携带 BFD Discriminator TLV 进行会话协商。

静态方式下，目前的 NE80E/40E 中，BFD 能够检测的 LSP 类型有：

- 静态 LSP
- LDP LSP
- TE：Tunnel、与 Tunnel 绑定的静态 CR-LSP、基于 RSVP 的动态 CR-LSP。BFD 能够检测信令协议为 CR-Static 和 RSVP-TE 的 TE 隧道，并且能够检测与 TE 隧道绑定的主用 LSP

动态方式下，BFD 支持的转发路径有：

- LDP LSP
- RSVP-LSP

目前动态 BFD 会话只能检测 RSVP-LSP，不能检测基于其他信令协议的 TE LSP，且不能检测 TE Tunnel。

由于 BFD 检测 LSP 和 TE 这些单向链路时，反向链路只要求 IP 路由可达即可。因此，反向链路可以是 IP、LSP 或 TE 隧道。

 说明

- BFD 检测静态 LSP、LDP LSP 的配置，请参考《HUAWEI NetEngine80E/40E 路由器 配置指南 MPLS》中的“MPLS 基本配置”。
- BFD 检测 MPLS TE 的配置，请参考《HUAWEI NetEngine80E/40E 路由器 配置指南 MPLS》中的“MPLS TE 配置”。

BFD for PW

BFD 能够对本地和远端的 PE 之间的 PW 链路进行快速故障检测，以支持 VLL FRR，减少链路故障给业务带来的影响。NE80E/40E 支持以静态（手工配置标识符）方式和动态方式建立 BFD for PW 会话。

NE80E/40E 通过将 BFD 和 VCCV Ping 结合的方式，实现动态 BFD 检测 PW 的连通性。从而引导承载的上层业务快速切换，达到保护业务的目的。

 说明

BFD 检测 PW 的配置，请参考《HUAWEI NetEngine80E/40E 路由器 配置指南 VPN》中的“PWE3 配置”。

BFD for PIM

NE80E/40E 支持 PIM 邻居之间动态创建 BFD 会话检测邻居之间的链路状态，一旦有故障，BFD 会把结果直接通告给 PIM。

 说明

BFD 检测 PIM 的配置，请参见《HUAWEI NetEngine80E/40E 路由器 配置指南-IP 组播》。

 注意

以上 BFD 会话在选板时按照 LDP，TE，PIM，路由的出接口来选板，BFD 会话会下发到这些出接口所在单板，如果出接口为多端口逻辑接口，例如 Eth-Trunk 接口下的子接口跨不同业务板时，则在出口板进行随即选择。在拔没有业务接口的接口板时，如果 BFD 会话在该接口板上，可能会导致业务切换。因此，建议在拔板之前先使用 display bfd session all verbose 命令查看，明确在接口板上有哪些会话。如果有，进入 BFD 会话视图下，将会话 shutdown 之后再拔板。拔板之后可以再重新创建会话。

BFD6

BFD6 是 BFD for IPv6 的简称。它和 BFD 的功能相同，用于检测系统之间的通信故障，并在故障出现时通知上层应用。

可以根据 BFD6 和 BFD for IPv4 所支持的功能，来查看它们的异同点。

BFD6/BFD for IPv4 支持的特性	BFD6	BFD for IPv4
IP 链路	是	是
单臂 ECHO	否	是
静态路由	是	是
OSPF	否	是
OSPFv3	是	否
BGP	是	是
ISIS	是	是
PIM	是	是
PST	是	是
PIS	否	是

BFD6/BFD for IPv4 支持的特性	BFD6	BFD for IPv4
PW	否	是
TE	否	是
LSP	否	是

5.2 配置 BFD 单跳检测

通过配置 BFD 单跳检测，实现快速检测和监控网络中的直连链路。

5.2.1 建立配置任务

在配置 BFD 单跳检测功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如果需要快速检测和监控网络中的直连链路，可以配置 BFD 单跳检测。

前置任务

在配置 BFD 单跳检测之前，需完成以下任务：

- 正确连接各接口
- 对于三层接口，正确配置接口 IP 地址

数据准备

在配置 BFD 单跳检测功能之前，需要准备以下数据。

序号	数据
1	BFD 配置名
2	BFD 检测的直连链路的对端 IP 地址、本端接口名称和编号。如果检测链路的物理层状态，还需要准备 BFD 使用的缺省组播地址。
3	BFD 会话参数：本地、远端标识符

5.2.2 使能全局 BFD 功能

只有全局使能 BFD 功能后，才能进行 BFD 的相关配置。

背景信息

如果对没有 IP 地址的三层物理接口或二层接口进行 BFD 单跳检测，需要配置缺省组播 IP 地址。

在需要检测的链路两端路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd**，使能全局 BFD 功能并进入 BFD 全局视图。

步骤 3（可选）执行命令 **default-ip-address ip-address**，配置 BFD 缺省组播 IP 地址。

缺省情况下，BFD 使用组播地址 224.0.0.184。

 说明

- BFD6 暂不支持组播地址检测，因此该命令仅对 IPv4 有效。
- 如果 BFD 检测路径上存在重叠的 BFD 会话，例如，三层接口通过具有 BFD 功能的二层交换设备连接，不同 BFD 会话所在的设备必须配置不同的缺省组播 IP 地址，以避免 BFD 报文被错误地转发。

----结束

5.2.3 建立 BFD 会话

通过在直连链路两端建立 BFD 会话，可以快速检测直连链路的故障。

背景信息

在需要检测的链路两端路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 根据 BFD 检测链路类型的不同，选择执行如下步骤之一：

- 基于 IPv4 链路：根据需求选择不同的命令选项创建 BFD 会话。
 - 对于有 IP 地址的三层接口，执行命令：
bfd cfg-name bind peer-ip peer-ip [vpn-instance vpn-instance-name] interface interface-type interface-number [source-ip source-ip]
 - 在第一次创建单跳 BFD 会话时，必须绑定对端 IP 地址和本端相应接口，且创建后不可修改。
 - 在创建 BFD 配置项时，系统只检查 IP 地址是否符合 IP 地址格式，不检查其正确性。绑定错误的对端 IP 地址或源 IP 地址都将导致 BFD 会话无法建立。
 - 当 BFD 与单播逆向路径转发 URPF（Unicast Reverse Path Forwarding）特性一起应用时，由于 URPF 会对接收到的报文进行源 IP 地址检查，用户在创建 BFD 绑定时，需要使用 **source-ip** 选项手工指定正确的源 IP 地址，以免 BFD 报文被错误地丢弃。
 - 对于二层接口和没有 IP 地址的三层物理成员接口，执行命令：

```
bfd cfg-name bind peer-ip default-ip interface interface-type interface-number  
[ source-ip source-ip ]
```

- 基于 IPv6 链路:

执行命令 **bfd** *cfg-name* **bind peer-ipv6 peer-ipv6** [**vpn-instance** *vpn-instance-name*] **interface** *interface-type interface-number* [**source-ipv6** *source-ipv6*] 命令，配置 BFD6 会话的绑定信息。

- 在第一次创建单跳 BFD6 会话时，必须绑定对端 IPv6 地址和本端相应接口，且创建后不可修改。
- 在创建 BFD6 配置项时，系统只检查 IPv6 地址是否符合 IP 地址格式，不检查其正确性。绑定错误的对端 IPv6 地址或源 IPv6 地址都将导致 BFD6 会话无法建立。

步骤 3 配置标识符:

- 执行命令 **discriminator local** *discr-value*，配置本地标识符。
- 执行命令 **discriminator remote** *discr-value*，配置远端标识符。

说明

- BFD 会话两端设备的本地标识符和远端标识符需要分别对应，即本端的本地标识符与对端的远端标识符相同，否则会话无法正确建立。并且，本地标识符和远端标识符配置成功后不可修改。
- 对于绑定缺省组播地址的 BFD 会话，一个 BFD 会话的本地标识符和远端标识符不能相同。

步骤 4 执行命令 **commit**，提交配置。

说明

在创建单跳 BFD 会话时，配置完必要的参数（例如本地标识符和远端标识符）后，必须执行 **commit** 命令才能成功创建会话。

----结束

5.2.4 检查配置结果

通过查看 BFD 会话的类型和状态等内容，来检查配置是否成功。

前提条件

已经完成 BFD 单跳检测功能的所有配置。

背景信息

说明

只有配置完 BFD 会话参数并成功建立会话后，才能查看到 BFD 会话统计信息和 BFD 会话信息。

操作步骤

- 使用 **display bfd configuration** { **all** | **static** [**name** *cfg-name*] | **discriminator local-discr-value** | **dynamic** | **peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] } [**verbose**] 命令查看 BFD 配置信息。
- 使用 **display bfd configuration** { **all** | **static** | **peer-ipv6** *peer-ipv6* [**vpn-instance** *vpn-instance-name*] } [**verbose**] 命令查看 BFD6 配置信息。
- 使用 **display bfd interface** [*interface-type interface-number*] 命令查看 BFD 接口信息。

- 使用 **display bfd session** { **all** | **discriminator** *discr-value* | **dynamic** | **peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] | **static** } [**verbose**] [**slot** *slot-id*] 命令查看 BFD 会话信息。
- 使用 **display bfd session** { **all** | **static** | **peer-ipv6** *peer-ipv6* [**vpn-instance** *vpn-instance-name*] } [**verbose**] [**slot** *slot-id*] 命令查看 BFD6 会话信息。
- 使用 **display bfd statistics** [**slot** *slot-id*] 命令查看 BFD 全局统计信息。
- 使用 **display bfd statistics session** { **all** | **static** | **dynamic** | **discriminator** *discr-value* | **peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] } [**slot** *slot-id*] 命令查看 BFD 会话统计信息。
- 使用 **display bfd statistics session** { **all** | **static** | **peer-ipv6** *peer-ipv6* [**vpn-instance** *vpn-instance-name*] } [**slot** *slot-id*] 查看 BFD6 会话的统计信息。

----结束

任务示例

配置成功后，使用 **display bfd session all verbose** 命令可以查看 BFD 会话的详细信息。

```
<HUAWEI> display bfd session all verbose
-----
Session MIndex : 256          (One Hop) State : Up          Name : aa
-----
Local Discriminator      : 11          Remote Discriminator   : 22
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type           : Interface(GigabitEthernet1/0/0)
Bind Session Type        : Static
Bind Peer Ip Address     : 224.0.0.184
Bind Peer Ip Address     : 2001:1001:1002:1003:1004:1005:1006:1007
NextHop Ip Address       : 224.0.0.184
NextHop Ip Address       : 2001:1001:1002:1003:1004:1005:1006:1007
Bind Interface           : GigabitEthernet1/0/0
FSM Board Id            : 1
TOS-EXP                  : 7
Min Tx Interval (ms)    : 10          Min Rx Interval (ms)   : 10
Actual Tx Interval (ms) : 10          Actual Rx Interval (ms) : 10
Local Detect Multi       : 3          Detect Interval (ms)   : 30
Echo Passive             : Disable     Acl Number              : -
Destination Port         : 3784        TTL                      : 255
Proc interface status    : Disable     Process PST              : Disable
WTR Interval (ms)        : --
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    : -
PDT Index                : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description      : -
-----
Total UP/DOWN Session Number : 1/0
```

可以看见，建立一个单跳（One Hop）BFD 会话，状态为 Up。

5.3 配置 BFD 被动回声功能

通过配置 BFD 被动回声功能，实现与网络中支持回声功能的设备互通。它只能应用于 BFD 单跳检测。

5.3.1 建立配置任务

在配置 BFD 被动回声功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

BFD 被动回声功能只适用于 BFD 单跳会话。
当网络中有支持回声功能的设备时，需要配置 BFD 被动回声功能，以和其他设备兼容。

图 5-2 BFD 被动回声功能应用场景



如图 5-2 所示，需要在 RouterA 上使能被动回声功能。

前置任务

在配置 BFD 被动回声功能之前，需完成以下任务：

- 全局使能 BFD
- （可选）建立 ACL

说明

BFD 回声报文在对端是通过 ICMP 重定向的方式来环回的，在封装 BFD 回声报文的 IP 报文中，目的地址和源地址都是本端出接口的 IP 地址。因此，在 ACL 规则中，除允许对端的源地址以外，还必须允许本端的源地址。

数据准备

在配置 BFD 被动回声功能之前，需要准备以下数据。

序号	数据
1	（可选）ACL 号码

5.3.2 配置 BFD 被动回声功能

特殊场景中，与网络中支持回声功能的设备互通时，可以配置 BFD 被动回声功能。

背景信息

在需要启用被动回声功能的路由器上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd**，进入 BFD 视图。

步骤 3 执行命令 **echo-passive { all | acl basic-acl-number }**，使能 BFD 被动回声功能。

- **all**：使能所有 BFD 会话的被动回声功能。
- **acl**：使能符合 ACL 的 BFD 会话的被动回声功能。在 ACL 中，除 permit 对端的源地址以外，还必须 permit 本端的源地址。

说明

如果在 BFD 会话已经协商 UP 之后创建 ACL 规则或者修改已有的 ACL 规则，新的 ACL 规则只有在 BFD 会话状态由 Down 变为 Up 或者修改了 BFD 会话参数之后才可以生效。

----结束

5.3.3 检查配置结果

通过查看 BFD 会话的类型、状态和被动回声是否使能等内容，来检查配置是否成功。

前提条件

已经完成 BFD 被动回声功能的所有配置。

操作步骤

步骤 1 使用 **display bfd session { all | static | dynamic | discriminator discr-value | peer-ip peer-ip [vpn-instance vpn-instance-name] } verbose [slot slot-id]** 命令查看 BFD 会话信息。

----结束

任务示例

查看所有 BFD 会话的详细信息。

```
<HUAWEI> display bfd session all verbose
```

Session MIndex : 256	(One Hop) State : Up	Name : aa
Local Discriminator : 11	Remote Discriminator : 22	
Session Detect Mode : Asynchronous Mode Without Echo Function		
BFD Bind Type : Interface(GigabitEthernet1/0/0)		
Bind Session Type : Static		
Bind Peer Ip Address : 224.0.0.184		
NextHop Ip Address : 224.0.0.184		
Bind Interface : GigabitEthernet1/0/0		
FSM Board Id : 1	TOS-EXP : 7	
Min Tx Interval (ms) : 10	Min Rx Interval (ms) : 10	
Actual Tx Interval (ms) : 10	Actual Rx Interval (ms) : 10	
Local Detect Multi : 3	Detect Interval (ms) : 30	
Echo Passive : Enable	Acl Number : --	
Destination Port : 3784	TTL : 255	
Proc interface status : Disable	Process PST : Disable	
WTR Interval (ms) : --		
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 : --		

PDT Index : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description : --

可以看到 **Echo Passive** 字段的值为“Enable”，表示该 BFD 会话已经启动了被动回声功能；如果该字段值是“Disable”，表示该 BFD 会话没有启动被动回声功能。会话能够启动被动回声功能的条件是：全局被动 Echo 功能已经使能，匹配 ACL 规则（如果配置了 ACL），并且对端已经启动了 Echo 功能。

5.4 配置 BFD 状态与接口状态联动

通过配置 BFD 状态与接口状态联动，触发路由快速收敛。它只能应用于缺省组播 IP 地址检测的单跳 BFD 会话中。

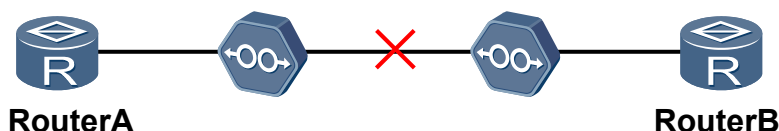
5.4.1 建立配置任务

在配置 BFD 状态与接口状态联动功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

当链路中间存在传输设备时，虽然三层仍是直连，但由于实际物理线路分段，一旦链路故障，两端设备需要比较长的时间才能检测到，导致直连路由失效慢，网络中断时间长。

图 5-3 两端路由器间存在传输设备



为解决上述问题，NE80E/40E 实现 BFD 状态与接口状态联动，使 BFD 会话状态的变化能够影响接口的协议状态，触发路由快速收敛。

配置 BFD 状态与接口状态联动后，当 BFD 会话检测到故障进入 Down 状态时，相应的接口状态变为 BFD_Down。在这种状态下，该接口的直连路由在路由表中被取消，但 BFD 报文的转发不受影响。

前置任务

在配置 BFD 状态与接口状态联动之前，需完成以下任务：

- **配置 BFD 单跳检测**

📖 说明

需要注意，能够实现 BFD 状态与接口状态联动的会话，必须是绑定缺省组播 IP 地址的单跳 BFD 会话，即，使用命令 **bfd cfg-name bind peer-ip default-ip interface interface-type interface-number [source-ip source-ip]** 创建 BFD 会话。

数据准备

在配置 BFD 状态与接口状态联动之前，需要准备以下数据。

序号	数据
1	BFD 配置名

5.4.2 配置 BFD 状态与接口状态联动

通过配置 BFD 与接口状态联动，可以使 BFD 会话状态的变化影响接口的协议状态，触发路由快速收敛。

背景信息

在需要进行 BFD 状态与接口状态联动的路由器上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd cfg-name**，进入 BFD 会话视图。

步骤 3 执行命令 **process-interface-status**，配置当前 BFD 会话与其绑定接口状态联动。

缺省情况下，BFD 会话不与绑定的接口状态联动，即 BFD 会话状态的变化不修改接口状态。

步骤 4 执行命令 **commit**，提交配置。

 说明

- 用命令行配置 **process-interface-status** 命令后，在 **commit** 时 BFD 会话不会立即将 BFD 状态上报给接口（在 **commit** 时 BFD 会话可能还没有建立或者还没有协商 UP），以免把错误的状态信息上报给接口，导致接口状态错误。在 **commit** 之后，如果 BFD 的状态发生变化，就会通告接口。以保证 BFD 的状态与接口状态联动。
- 当配置文件中存在 **process-interface-status** 命令时，在整机重启后，考虑到接口的初始状态一定是 Down，所以配置了 **process-interface-status** 命令的 BFD 会上报一个 Down 状态给接口。
- 使用接口状态联动必须保证两台路由器之间的 BFD 配置是正确和对称的。如果发现本端接口的 BFD 状态是 Down，需要检查一下对端 BFD 配置是否正确，是否被 **shutdown**。
- 如果组网中有需要 BFD 立即同步状态给接口，可以在保证两端路由器配置正确的情况下，**shutdown** 和 **undo shutdown** BFD 会话。BFD 在 **undo shutdown** 的时候会启动一个检测定时器，如果在定时器超时之前能够协商 UP，则上报 UP 给接口，否则认为链路有故障，因而在定时器超时后上报检测 Down 给接口。这样可以实现 BFD 与接口状态的实时同步。

----结束

5.4.3 检查配置结果

通过查看 BFD 会话与接口状态的联动标识等内容，来检查配置是否成功。

前提条件

已经完成 BFD 状态与接口状态联动功能的所有配置。

操作步骤

- 使用 **display bfd session** { all | discriminator *discr-value* | dynamic | peer-ip *peer-ip* [vpn-instance *vpn-instance-name*] | static } [verbose] [slot *slot-id*] 命令查看 BFD 会话信息。
- 使用 **display bfd session** { all | static | peer-ipv6 *peer-ipv6* [vpn-instance *vpn-instance-name*] } [verbose] [slot *slot-id*] 命令查看 BFD6 会话信息。

----结束

任务示例

配置成功后，执行上述命令，可以看到输出信息中相应会话的“Proc interface status”字段显示为“Enable”。

```
<HUAWEI> display bfd session all verbose
```

```
-----
Session MIndex : 256          (One Hop) State : Up          Name : test
-----
Local Discriminator      : 22          Remote Discriminator      : 11
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type           : Interface(GigabitEthernet2/0/0)
Bind Session Type        : Static
Bind Peer Ip Address     : 224.0.0.184
NextHop Ip Address       : 224.0.0.184
Bind Interface           : GigabitEthernet2/0/0
FSM Board Id            : 2            TOS-EXP                    : 7
Min Tx Interval (ms)     : 10          Min Rx Interval (ms)      : 10
Actual Tx Interval (ms)  : 10          Actual Rx Interval (ms)   : 10
Local Detect Multi       : 3            Detect Interval (ms)      : 30
Echo Passive             : Disable      Acl Number                 : --
Destination Port         : 3784         TTL                        : 255
Proc interface status    : Enable        Process PST                 : Disable
WTR Interval (ms)        : --
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    : --
PDT Index                : FSM-0 | RCV-0 | IF-0 | TOKEN-0
Session Description      : --
-----
Total UP/DOWN Session Number : 1/0
```

5.5 配置 BFD 状态与子接口状态联动

通过配置 BFD 状态与子接口状态联动，触发路由快速收敛。它只能应用于缺省组播 IP 地址检测的单跳 BFD 会话中。

5.5.1 建立配置任务

在配置 BFD 状态与子接口状态联动功能之前，应了解其应用环境和数据准备，并需要配置 BFD 单跳检测等前置任务。

应用环境

在子接口上配置大量业务、对可靠性要求高的组网环境中，需要建立 BFD 会话检测主接口链路的连通性，并配置 BFD 状态与子接口状态联动功能，以提高子接口上业务的可靠性，同时节约会话资源。

前置任务

在配置 BFD 会话状态与子接口状态联动之前，需要完成以下任务：

- 全局使能 BFD。
- 建立单跳 BFD 会话，该 BFD 会话必须绑定主接口、且使用缺省组播地址检测。
- BFD 会话已经建立并且状态为 Up。

数据准备

在配置 BFD 会话状态与子接口状态联动之前，需要准备以下数据。

序号	数据
1	BFD 会话配置名

5.5.2 配置 BFD 会话状态与子接口状态联动

通过配置 BFD 与子接口状态联动，可以使 BFD 会话状态的变化影响接口的协议状态，触发路由快速收敛。

背景信息

在需要快速感知链路故障的路由器上进行如下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **bfd cfg-name**，进入 BFD 会话视图。
- 步骤 3** 执行命令 **process-interface-status sub-if**，配置 BFD 会话状态与子接口状态联动功能。
- 步骤 4** 执行命令 **commit**，提交配置。

当 BFD 会话状态变为 Down 时，与会话绑定的主接口及其子接口的 BFD 状态都会变为 Down。



说明

- 配置 **process-interface-status** 命令后，在 **commit** 时 BFD 会话不会立即将 BFD 状态上报给接口（在 **commit** 时 BFD 会话可能还没有建立或者还没有协商 UP），以免把错误的状态信息上报给接口，导致接口状态错误。在 **commit** 之后，如果 BFD 的状态发生变化，就会通告接口。以保证 BFD 的状态与接口状态联动。
- 如果组网中有需要 BFD 立即同步状态给接口，可以在保证两端路由器配置正确的情况下，**shutdown** 和 **undo shutdown** BFD 会话。BFD 在 **undo shutdown** 的时候会启动一个检测定时器，如果在定时器超时之前能够协商 UP，则上报 UP 给接口，否则认为链路有故障，因而在定时器超时后上报检测 Down 给接口。这样可以实现 BFD 与接口状态的实时同步。
- 当配置文件中存在 **process-interface-status** 命令时，在整机重启后，考虑到接口的初始状态一定是 Down 的，所以配置了 **process-interface-status** 命令的 BFD 会上报一个 Down 状态给接口。
- 使用接口状态联动必须保证两台路由器之间的 BFD 配置是正确和对称的。如果发现本端接口的 BFD 状态是 Down，需要检查一下对端 BFD 配置是否正确，是否被 **shutdown**。

----结束

5.5.3 检查配置结果

通过查看 BFD 会话与子接口状态的联动标识等内容，来检查配置是否成功。

前提条件

已经完成 BFD 状态与子接口状态联动功能的所有配置。

操作步骤

- 使用 **display bfd session { all | static | dynamic | discriminator *discr-value* | peer-ip *peer-ip* [vpn-instance *vpn-instance-name*] } verbose [slot *slot-id*]** 命令查看 BFD 会话信息。
- 使用 **display bfd session { all | static | peer-ipv6 *peer-ipv6* [vpn-instance *vpn-instance-name*] } [verbose] [slot *slot-id*]** 命令查看 BFD6 会话信息。

----结束

任务示例

执行 **display bfd session all verbose** 命令。

<HUAWEI> **display bfd session all verbose**

Session MIndex : 256		(One Hop) State : Up	Name : aa
Local Discriminator	: 11	Remote Discriminator	: 22
Session Detect Mode	: Asynchronous Mode Without Echo Function		
BFD Bind Type	: Interface(GigabitEthernet1/2/0)		
Bind Session Type	: Static		
Bind Peer Ip Address	: 224.0.0.184		
NextHop Ip Address	: 224.0.0.184		
Bind Interface	: GigabitEthernet1/2/0		
FSM Board Id	: 1	TOS-EXP	: 7
Min Tx Interval (ms)	: 10	Min Rx Interval (ms)	: 10
Actual Tx Interval (ms)	: 10	Actual Rx Interval (ms)	: 10
Local Detect Multi	: 3	Detect Interval (ms)	: 30
Echo Passive	: Disable	Acl Number	: --
Destination Port	: 3784	TTL	: 255
Proc interface status	: Enable(Sub-If)	Process PST	: Disable
WTR Interval (ms)	: --		
Active Multi	: 3		

```
Last Local Diagnostic : --
Bind Application       : No Application Bind
Session TX TmrID      : --           Session Detect TmrID   : --
Session Init TmrID    : --           Session WTR TmrID    : --
Session Echo Tx TmrID : --
PDT Index              : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description    : --
```

Proc interface status 字段的值是“Enable(Sub-If)”，表示 BFD 会话 aa 的状态关联主接口及其子接口的状态。

5.6 配置 BFD 修改端口状态表

通过配置 BFD 修改端口状态表，实现 BFD 会话更加快速的检测链路的故障。它只能应用在 BFD 单跳检测中。

5.6.1 建立配置任务

在配置 BFD 修改端口状态表功能之前，应了解其应用环境和数据准备，并需要配置 BFD 单跳检测等前置任务。

应用环境

如果允许 BFD 修改端口状态表 PST（Port State Table），当 BFD 检测到接口状态变为 Down 时，将更改 PST 中相应表项。这样，其他上层应用协议就能够通过 PST 了解接口是否发生故障。

目前，对于 NE80E/40E，基于 BFD 检测的 LDP FRR 和 IP FRR 需要通过 PST 来感知 BFD 检测结果。

对于不通过 PST 来感知 BFD 检测故障的应用，不需要配置 `process-pst` 命令。

说明

- LDP FRR 的介绍请参考《HUAWEI NetEngine80E/40E 路由器 配置指南 MPLS》中的“MPLS 基本配置”。
- IP FRR 有两类：公网 IP FRR 和私网 IP FRR。公网 IP FRR 介绍请参考《HUAWEI NetEngine80E/40E 路由器 配置指南 IP 路由》中的“路由策略配置”，私网 IP FRR 介绍请参考《HUAWEI NetEngine80E/40E 路由器 配置指南 VPN》中的“BGP MPLS IP VPN 配置”。

前置任务

在配置 BFD 修改端口状态表之前，需完成以下任务：

- [5.2 配置 BFD 单跳检测](#)

说明

BFD 修改 PST 需要与 BFD 单跳检测配合使用。

数据准备

在配置 BFD 修改端口状态表之前，需要准备以下数据。

序号	数据
1	BFD 会话的配置名

5.6.2 使能 BFD 修改端口状态表

对于通过 PST 来感知 BFD 检测故障的应用，可以配置 BFD 修改端口状态表。

背景信息

在需要通过 PST 了解 BFD 检测结果的路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd cfg-name**，进入 BFD 会话视图。

步骤 3 执行命令 **process-pst**，允许 BFD 修改端口状态表 PST。

缺省情况下，BFD 不修改端口状态表。

 说明

在创建完 BFD 会话后，如果需要修改会话参数（命令包括 **process-pst**、**process-interface-status**、**min-tx-interval**、**min-rx-interval**、**detect-multiplier**、**tos-exp**、**wtr**、**description**），可以执行相关命令即可立即生效，不需要再执行 **commit** 操作。

当检测 Trunk 成员口或者 VLAN 成员口上的 BFD 会话允许 BFD 修改端口状态表并且其主接口上也配置了 BFD 会话时，必须为检测主接口的 BFD 会话配置等待恢复时间 WTR（Wait to Recovery），以避免成员口加入或者退出主接口的时候导致主接口的 BFD 会话震荡。

配置 BFD 等待恢复时间请参见 [5.11.3 配置 BFD 等待恢复时间](#)。

步骤 4 执行命令 **commit**，提交配置。

----结束

5.6.3 检查配置结果

通过查看端口状态表是否使能等内容，来检查配置是否成功。

前提条件

已经完成 BFD 修改端口状态表功能的所有配置。

操作步骤

- 使用 **display bfd session { all | discriminator discr-value | dynamic | peer-ip peer-ip [vpn-instance vpn-instance-name] | static } [verbose] [slot slot-id]** 命令查看 BFD 会话信息。

- 使用 **display bfd session { all | static | peer-ipv6 peer-ipv6 [vpn-instance vpn-instance-name] } [verbose] [slot slot-id]** 命令查看 BFD6 会话信息。

----结束

任务示例

配置成功后，执行上述命令，可以看到输出信息中相应会话的“Process PST”字段显示为“Enable”。

```
<HUAWEI> display bfd session all verbose
-----
Session MIndex : 256          (One Hop) State : Up          Name : test
-----
Local Discriminator      : 22          Remote Discriminator : 11
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type           : Interface(GigabitEthernet2/0/0)
Bind Session Type        : Static
Bind Peer Ip Address     : 10.100.10.2
NextHop Ip Address       : 10.100.10.2
Bind Interface           : GigabitEthernet2/0/0
FSM Board Id            : 2            TOS-EXP                : 7
Min Tx Interval (ms)    : 10           Min Rx Interval (ms)   : 10
Actual Tx Interval (ms) : 10           Actual Rx Interval (ms): 10
Local Detect Multi       : 3            Detect Interval (ms)   : 30
Echo Passive             : Disable       Acl Number              : --
Destination Port         : 3784          TTL                      : 255
Proc interface status    : Disable       Process PST              : Enable
WTR Interval (ms)       : --
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    : --
PDT Index                : FSM-0 | RCV-0 | IF-0 | TOKEN-0
Session Description      : --
-----
Total UP/DOWN Session Number : 1/0
```

5.7 配置 BFD 多跳检测

配置 BFD 多跳检测，实现快速检测和监控网络中的多跳路径。

5.7.1 建立配置任务

在配置 BFD 多跳检测功能之前，应了解其应用环境和数据准备。

应用环境

如果需要快速检测和监控 IP 路由的转发连通状况，可以配置 BFD 多跳检测。

前置任务

在配置 BFD 多跳检测之前，需完成以下任务：

- 正确连接各接口并配置 IP 地址
- 配置路由协议，保证网络层可达

数据准备

在配置 BFD 多跳检测功能之前，需要准备以下数据。

序号	数据
1	对端 IP 地址
2	BFD 配置名
3	BFD 会话参数：本地、远端标识符
4	BFD 检测模式：异步模式或查询模式。如果采用查询模式，还需要确定查询周期

5.7.2 使能全局 BFD 功能

只有全局使能 BFD 功能后，才能进行 BFD 的相关配置。

背景信息

在需要建立 BFD 会话的路由器上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **bfd**，使能全局 BFD 功能并进入 BFD 全局视图。
- 结束

5.7.3 建立 BFD 会话

通过在多跳路径两端建立 BFD 会话，可以快速检测多跳路径的故障。

背景信息

在需要建立 BFD 会话的路由器上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 根据 BFD 是检测链路类型的不同，选择执行如下步骤之一：
- 基于 IPv4 链路：
执行命令 **bfd cfg-name bind peer-ip peer-ip [vpn-instance vpn-instance-name] [source-ip source-ip]**，创建 BFD 会话。
 - 在第一次创建 BFD 会话时，必须绑定对端的 IP 地址，且创建后不可修改。
 - 在创建 BFD 配置项时，系统只检查 IP 地址是否符合 IP 地址格式，不检查其正确性。绑定错误的对端 IP 地址或源 IP 地址都将导致 BFD 会话无法建立。

- 当 BFD 与单播逆向路径转发 URPF（Unicast Reverse Path Forwarding）特性一起应用时，由于 URPF 会对接收到的报文进行源 IP 地址检查，用户在创建 BFD 绑定时，需要使用 `source-ip` 选项手工指定正确的 BFD 报文的源 IP 地址，以免 BFD 报文被错误地丢弃。

- 基于 IPv6 链路：

执行命令 **bfd** *cfg-name* **bind peer-ipv6** *peer-ipv6* [**vpn-instance** *vpn-instance-name*] [**source-ipv6** *ipv6-address*]，创建 BFD6 会话。

- 在创建 BFD6 会话时，必须绑定对端的 IPv6 地址，且创建后不可修改。
- 在创建 BFD6 会话时，如果指定的对端 IPv6 地址是本地链路地址，则必须绑定接口，即只能创建单跳 BFD 会话，否则会给出错误信息。
- 在创建 BFD6 配置项时，系统只检查 IPv6 地址是否符合 IPv6 地址格式，不检查其正确性。绑定错误的对端 IPv6 地址或源 IPv6 地址都将导致 BFD6 会话无法建立。

步骤 3 配置标识符：

- 执行命令 **discriminator local** *discr-value*，配置本地标识符。
- 执行命令 **discriminator remote** *discr-value*，配置远端标识符。

 说明

BFD 会话两端设备的本地标识符和远端标识符需要分别对应，即，本端的本地标识符与对端的远端标识符相同，否则会话无法正确建立。并且，本地标识符和远端标识符配置成功后不可修改。

步骤 4 执行命令 **commit**，提交配置。

 说明

在创建 BFD 会话时，配置完必要的参数（例如本地标识符和远端标识符）后，必须执行 **commit** 命令才能成功创建会话。

----结束

5.7.4 检查配置结果

通过查看 BFD 会话的类型和状态等，来检查是否配置成功。

前提条件

已经完成 BFD 多跳检测功能的所有配置。

背景信息

 说明

只有配置完 BFD 会话参数并成功建立会话后，才能查看到 BFD 会话统计信息和 BFD 会话信息。

操作步骤

- 使用 **display bfd configuration** { **all** | **static** [**name** *cfg-name*] | **discriminator local** *discr-value* | **dynamic** | **peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] } [**verbose**] 命令查看 BFD 配置信息。
- 使用 **display bfd configuration** { **all** | **static** | **peer-ipv6** *peer-ipv6* [**vpn-instance** *vpn-instance-name*] } [**verbose**] 命令查看 BFD6 配置信息。

- 使用 **display bfd session** { all | discriminator *discr-value* | dynamic | peer-ip *peer-ip* [vpn-instance *vpn-instance-name*] | static } [verbose] [slot *slot-id*]命令查看 BFD 会话信息。
- 使用 **display bfd session** { all | static | peer-ipv6 *peer-ipv6* [vpn-instance *vpn-instance-name*] } [verbose] [slot *slot-id*]命令查看 BFD6 会话信息。
- 使用 **display bfd statistics** [slot *slot-id*]命令查看 BFD 全局统计信息。
- 使用 **display bfd statistics session** { all | static | discriminator *discr-value* | peer-ip *peer-ip* [vpn-instance *vpn-instance-name*] } [slot *slot-id*]命令查看 BFD 会话统计信息。
- 使用 **display bfd statistics session** {all | static | peer-ipv6 *peer-ipv6* [vpn-instance *vpn-instance-name*] } [slot *slot-id*]查看 BFD6 会话的统计信息。

----结束

任务示例

配置成功后，执行 **display bfd session all verbose** 命令。

```
<RouterA> display bfd session all verbose
-----
Session MIndex : 256          (Multi Hop) State : Up          Name : atoc
-----
Local Discriminator      : 10          Remote Discriminator   : 20
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type           : Peer Ip Address
Bind Session Type        : Static
Bind Peer Ip Address     : 10.2.1.2
Bind Interface           : --
FSM Board Id            : 1
Min Tx Interval (ms)     : 10          Min Rx Interval (ms)    : 10
Actual Tx Interval (ms) : 10          Actual Rx Interval (ms) : 10
Local Detect Multi       : 3           Detect Interval (ms)    : 3000
Echo Passive             : Disable      Acl Number              : --
Destination Port         : 3784         TTL                      : 255
Proc interface status    : Disable      Process PST              : Enable
WTR Interval (ms)        : --
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      : --
PDT Index                : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description      : --
-----
Total UP/DOWN Session Number : 1/0
```

可以看到建立了一个多跳（Multi Hop）的 BFD Session，且状态为 Up。

5.8 配置静态标识符自协商 BFD

通过配置静态标识符自协商 BFD，实现与采用动态建立 BFD 会话的设备互通。它主要应用在静态路由中。

5.8.1 建立配置任务

在配置静态标识符自协商 BFD 功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如果对端设备采用动态 BFD，而本端设备既要与之互通，又要能够实现静态路由 Track BFD，此时必须配置静态标识符自协商 BFD。

前置任务

在配置静态标识符自协商 BFD 之前，需完成以下任务：

- 正确连接各接口
- 对于三层接口，正确配置接口 IP 地址

数据准备

在配置静态标识符自协商 BFD 之前，需要准备以下数据。

序号	数据
1	BFD 配置名
2	BFD 检测链路的本端和对端 IP 地址、本端接口名称和编号

5.8.2 使能全局 BFD 功能

只有全局使能 BFD 功能后，才能进行 BFD 的相关配置。

背景信息

在需要使用静态标识符自协商 BFD 检测链路的路由器上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **bfd**，使能全局 BFD 功能并进入 BFD 全局视图。

----结束

5.8.3 建立 BFD 会话

通过在两端建立静态标识符自协商 BFD 会话，可以快速检测链路故障。

背景信息

在需要使用静态标识符自协商 BFD 检测链路的路由器上进行以下配置。

根据 BFD 是基于 IPv4 还是 IPv6，选择执行如下步骤之一：

操作步骤

- 基于 IPv4 的 BFD：

1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **bfd cfg-name bind peer-ip ip-address [vpn-instance vpn-instance-name] [interface interface-type interface-number] source-ip ip-address auto**，创建静态标识符自协商 BFD 会话。
 - 必须配置源地址。
 - 必须指定明确的对端 IP 地址，不能使用组播 IP 地址。
 3. 执行命令 **commit**，提交配置。
- 基于 BFD6:
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **bfd cfg-name bind peer-ipv6 peer-ipv6 [vpn-instance vpn-instance-name] [interface interface-type interface number] source-ipv6 ipv6-address auto**，创建静态标识符自协商 BFD 会话。
 - 必须配置源地址。
 - 必须指定明确的对端 IPv6 地址。
 3. 执行命令 **commit**，提交配置。

----结束

5.8.4 检查配置结果

通过查看 BFD 会话的建立类型等内容，来检查配置是否成功。

前提条件

已经完成静态标识符自协商 BFD 功能的所有配置。

操作步骤

- 使用 **display bfd session { all | static | dynamic | discriminator discr-value | peer-ip peer-ip [vpn-instance vpn-instance-name] } verbose [slot slot-id]**命令查看 BFD 会话信息。
- 使用 **display bfd session { all | static | peer-ipv6 peer-ipv6 [vpn-instance vpn-instance-name] } [verbose] [slot slot-id]**命令查看 BFD6 会话信息。Active Multi : 3

----结束

任务示例

查看所有 BFD 会话的详细信息。

```
<HUAWEI> display bfd session all verbose
```

```
-----
Session MIndex : 16385      (One Hop) State : Up      Name : auto
-----
Local Discriminator      : 8193      Remote Discriminator      : 8192
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type            : Interface(GigabitEthernet2/0/1)
Bind Session Type        : Static_Auto
Bind Peer IP Address     : 192.168.1.2
NextHop Ip Address       : 192.168.1.2
Bind Interface           : GigabitEthernet2/0/1
Bind Source IP Address   : 192.168.1.1
FSM Board Id            : 2          TOS-EXP              : 7
-----
```

```
Min Tx Interval (ms) : 10           Min Rx Interval (ms) : 10
Actual Tx Interval (ms): 10         Actual Rx Interval (ms): 10
Local Detect Multi : 3              Detect Interval (ms) : 30
Echo Passive : Disable              Acl Number : -
Destination Port : 3784             TTL : 255
Proc Interface Status : Disable     Process PST : Disable
WTR Interval (ms) : -

Last Local Diagnostic : No Diagnostic
Bind Application : AUTO
Session TX TmrID : -                Session Detect TmrID : -
Session Init TmrID : -              Session WTR TmrID : -
Session Echo Tx TmrID : -
PDT Index : FSM-3010000 | RCV-0 | IF-3010000 | TOKEN-0
Session Description : -

-----
Total UP/DOWN Session Number : 1/0
```

可以看到建立了一个会话类型为 **Static_Auto** 的 BFD 会话，该会话的本端和远端标识符分别为 8193 和 8192，这是通过自协商方式获得的。

5.9 配置 BFD 会话延迟 UP 功能

特殊场景中，通过配置 BFD 会话延迟 UP 功能，避免由于路由协议 UP 晚于接口 UP 而导致的流量丢失问题。

5.9.1 建立配置任务

在配置 BFD 会话延迟 UP 功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

由于在实际组网环境中一些设备只根据 BFD 是否 UP 启动流量切换，而路由协议 UP 晚于接口 UP，这样可能导致流量回切时查不到路由，从而丢失流量。因此，需要弥补路由晚于接口 UP 的时间差。

前置任务

在配置 BFD 会话延迟 UP 功能之前，需完成以下任务：

- 路由器需要处于正常运转状态

数据准备

在配置 BFD 会话延迟 UP 功能之前，需要准备以下数据。

序号	数据
1	延迟 UP 的时间

5.9.2 配置 BFD 会话延迟 UP 功能

通过配置 BFD 会话延迟 UP 功能，可以避免特殊场景中的流量丢失问题。

背景信息

在需要 BFD 会话延迟 UP 的路由器上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **bfd**，对本节点使能全局 BFD 能力并进入 BFD 视图。
- 步骤 3** 执行命令 **delay-up seconds**，配置 BFD 会话延迟 UP 的时间。
- 缺省情况下，BFD 会话延迟 UP 的时间是 0 秒。

----结束

5.9.3 检查配置结果

通过查看当前延迟 UP 定时器等内容，来检查配置是否成功。

前提条件

已经完成 BFD 会话延迟 UP 功能的所有配置。

操作步骤

- 步骤 1** 使用 **display bfd statistics [slot slot-id]**命令查看 BFD 全局统计信息。

----结束

任务示例

配置完成后，将路由器整机重启。在重启完成后进入配置恢复时，执行 **display bfd statistics** 命令。

```
<HUAWEI> display bfd statistics
Current Display Board Number : Main ; Current Product Register Type:
IP Multihop Destination Port : 3784
Total Up/Down Session Number : 0/1
Current Session Number :
    Static session      : 0          Dynamic session      : 0
    E_Dynamic session   : 0          STATIC_AUTO session : 1
    LDP_LSP session     : 0          STATIC_LSP session  : 0
    TE_TUNNEL session   : 0          TE_LSP session       : 0
    PW session          : 0          IP session           : 1

-----
PAF/LCS Name                Maxnum      Minnum      Create
-----
BFD_CFG_NUM                  8192         1           1
BFD_IF_NUM                    512          1           1
BFD_SESSION_NUM              8192         1           1
BFD_IO_SESSION_NUM           512          1           0
BFD_PER_TUNNEL_CFG_NUM       16           1           0
-----
IO Board Current Created Session Statistics Information : (slot/number)
-----
0 /0    1 /0    2 /1    3 /0    4 /0    5 /0    6 /0    7 /0
8 /0    9 /0   10/0   11/0   12/0   13/0   14/0   15/0
16/0   17/0   18/0   19/0   20/0   21/0   22/0   23/0
24/0   25/0   26/0   27/0   28/0   29/0   30/0   31/0
32/0   33/0   34/0   35/0   36/0   37/0
```

```
-----
Current Total Used Discriminator Num           : 1
-----
10 Board Reserved Sessions Number Information : (slot/number)
-----
0 /0    1 /0    2 /0    3 /0    4 /0    5 /0    6 /0    7 /0
8 /0    9 /0   10 /0   11 /0   12 /0   13 /0   14 /0   15 /0
16 /0   17 /0   18 /0   19 /0   20 /0   21 /0   22 /0   23 /0
24 /0   25 /0   26 /0   27 /0   28 /0   29 /0   30 /0   31 /0
32 /0   33 /0   34 /0   35 /0   36 /0   37 /0
-----
BFD HA Information :
-----
Core Current HA Status           : Normal
Shell Current HA Status          : Normal
-----
BFD for LSP Information :
-----
Ability of auto creating BFD session on egress : Disable
Period of LSP Ping                : 60
System Session Delay Up Timer      : OFF
-----
```

可以看到显示信息中有一个字段 **System Session Delay Up Timer**，显示当前延迟 UP 定时器的状态，OFF 表示系统处于正常状态；×s 表明 X 秒后系统恢复正常，BFD 会话可以 UP。

5.10 配置单臂 ECHO 功能

通过配置单臂 ECHO 功能，实现快速检测和监控网络中的直连链路。

5.10.1 建立配置任务

在配置单臂 ECHO 功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在两台直接相连的设备中，其中，一台设备支持 BFD 功能，另一台设备不支持 BFD 功能。此时，为了能够更加快速的检测链路故障，可以在支持 BFD 功能的设备上创建单臂 ECHO 功能的 BFD 会话。不支持 BFD 功能的设备接收到该 BFD 报文后，直接将该报文环回。从而达到快速检测链路的目的。

前置任务

在配置单臂 ECHO 功能之前，需完成以下任务：

- 正确连接各接口
- 对于三层接口，正确配置接口 IP 地址

数据准备

在配置单臂 ECHO 功能之前，需要准备以下数据。

序号	数据
1	BFD 会话的名称
2	报文的最小接收间隔

5.10.2 使能全局 BFD 功能

只有全局使能 BFD 能力后，才能进行 BFD 的相关配置。

背景信息

在支持 BFD 功能的一端设备上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **bfd**，使能全局 BFD 功能并进入 BFD 视图。
- 结束

5.10.3 建立 BFD 会话

通过在支持 BFD 功能的设备上建立 BFD 会话，实现单方面的快速检测直连链路的目的。

背景信息

在支持 BFD 功能的一端设备上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **bfd cfg-name bind peer-ip peer-ip [vpn-instance vpn-instance-name] interface interface-type interface-number [source-ip source-ip] one-arm-echo**，创建单臂 ECHO 功能的 BFD 会话。
-  说明
- 单臂 ECHO 功能的 BFD 会话只能应用的单跳检测中。
- 步骤 3** 执行命令 **discriminator local discr-value**，配置单臂 ECHO 功能的 BFD 会话的标识符。
- 由于只能在支持 BFD 功能的一端设备上配置单臂 ECHO 功能，所以，配置单臂 ECHO 功能的 BFD 会话时，只需要配置本地标识符，无需配置远端标识符。
- 步骤 4** （可选）执行命令 **min-echo-rx-interval**，配置单臂 ECHO 功能的 BFD 会话的最小接收时间。
- 缺省情况下，单臂 ECHO 功能的 BFD 会话的最小接收间隔为 10 毫秒。
- 步骤 5** 执行命令 **commit**，提交配置。



说明

在创建单臂 ECHO 功能的 BFD 会话时，配置完必要的参数（例如，会话的标识符）后，必须执行 **commit** 命令才能成功创建会话。

----结束

5.10.4 检查配置结果

通过查看单臂 ECHO 功能的 BFD 会话的类型和状态等内容，来检查配置是否成功。

前提条件

已经完成单臂 ECHO 功能的所有配置。

操作步骤

- 使用 **display bfd configuration { all | static [name cfg-name] | discriminator local-dscr-value | dynamic | peer-ip peer-ip [vpn-instance vpn-instance-name] } [verbose]** 命令查看 BFD 配置信息。
- 使用 **display bfd interface [interface-type interface-number]** 命令查看 BFD 接口信息。
- 使用 **display bfd session { all | discriminator dscr-value | dynamic | peer-ip peer-ip [vpn-instance vpn-instance-name] | static } [verbose] [slot slot-id]** 命令查看 BFD 会话信息。
- 使用 **display bfd statistics session { all | static | dynamic | discriminator dscr-value | peer-ip peer-ip [vpn-instance vpn-instance-name] } [slot slot-id]** 命令查看 BFD 会话统计信息。

----结束

任务示例

配置成功后，使用 **display bfd session all verbose** 命令可以查看单臂 ECHO 功能的 BFD 会话的详细信息。

<HUAWEI> **display bfd session all verbose**

Session MIndex : 256		(One Hop) State : Up	Name : atob
Local Discriminator	: 1	Remote Discriminator	: -
Session Detect Mode	: Asynchronous One-arm-echo Mode		
BFD Bind Type	: Interface(gigabitEthernet1/0/0)		
Bind Session Type	: Static		
Bind Peer IP Address	: 10.1.1.2		
NextHop Ip Address	: 10.1.1.2		
Bind Interface	: EigabitEthernet1/0/0		
FSM Board Id	: 0	TOS-EXP	: 7
Echo Rx Interval (ms)	: 100		
Actual Tx Interval (ms)	: 1000	Actual Rx Interval (ms)	: 1000
Local Detect Multi	: 3	Detect Interval (ms)	: 3000
Echo Passive	: Disable	Acl Number	: -
Destination Port	: 3784	TTL	: 255
Proc Interface Status	: Disable	Process PST	: Disable
WTR Interval (ms)	: -	Local Demand Mode	: Disable
Active Multi	: 3		
Last Local Diagnostic	: Control Detection Time Expired		
Bind Application	: No Application Bind		
Session TX TmrID	: 87	Session Detect TmrID	: 88
Session Init TmrID	: -	Session WTR TmrID	: -
Session Echo Tx TmrID	: -		

PDT Index

: FSM-0 | RCV-0 | IF-0 | TOKEN-0

Session Description

: -

Total UP/DOWN Session Number : 1/0

由以上信息可知，建立了一个单跳（One Hop）的 BFD 会话，状态为 Up。

5.11 调整 BFD 检测参数

通过调整 BFD 检测参数，实现 BFD 会话更好、更快速的检测和监控网络中的链路。

5.11.1 建立配置任务

在调整 BFD 检测参数功能之前，应了解其应用环境和数据准备，并需要配置 BFD 会话等前置任务。

应用环境

在建立 BFD 会话时，可以根据网络状况和性能需求，调整设备的 BFD 报文发送间隔、接收间隔以及本地检测倍数。

用户可以通过配置 BFD 会话的等待恢复时间 WTR（Wait to Recovery），来避免 BFD 会话震荡导致的 BFD 应用在主备之间频繁切换。

用户还可以通过配置 BFD 会话的描述信息对 BFD 会话监视的链路进行简单描述，方便用户识别不同的 BFD 会话。

通常情况下，使用系统的缺省配置即可。

前置任务

在调整 BFD 检测参数之前，需完成以下任务：

- 完成 BFD 会话的创建

数据准备

在调整 BFD 检测参数之前，需要准备以下数据。

序号	数据
1	BFD 配置名
2	BFD 报文的本地发送间隔、接收间隔
3	BFD 报文的本地检测倍数

5.11.2 调整 BFD 检测时间

通过调整 BFD 的检测时间，使 BFD 会话更好的监控网络中的链路。

背景信息

请在路由器上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **bfd cfg-name**，进入 BFD 会话视图。
- 步骤 3** 执行命令 **min-tx-interval interval**，配置发送间隔。
- 缺省情况下，最小发送间隔是 10 毫秒。
- 步骤 4** 执行命令 **min-rx-interval interval**，配置接收间隔。
- 缺省情况下，最小接收间隔是 10 毫秒。
- 步骤 5** 执行命令 **detect-multiplier multiplier**，配置本地检测倍数。
- 缺省情况下，本地检测倍数为 3。

说明

在创建完 BFD 会话后，如果需要修改会话参数（命令包括 **process-pst**、**process-interface-status**、**min-tx-interval**、**min-rx-interval**、**detect-multiplier**、**tos-exp**、**wtr**、**description**），可以执行相关命令即可立即生效，不需要再执行 **commit** 操作。

----结束

后续处理

为降低对系统资源的占用，一旦检测到 BFD 会话 Down，系统自动将本端的发送间隔和接收间隔调整为大于 1000 毫秒的一个随机值，当 BFD 会话的状态重新变为 Up 后，再恢复成用户配置的间隔时间。

说明

BFD 本身可以应用于各种通信设备，为满足快速检测的需求，BFD 草案规定发送间隔和接收间隔的时间单位是微秒。但限于目前的设备处理能力，大部分厂商的设备在配置 BFD 时只能达到毫秒级，在进行内部处理时再转换到微秒级。

5.11.3 配置 BFD 等待恢复时间

通过配置 BFD 会话的等待恢复时间，可以避免因 BFD 会话振荡而导致的应用在主备设备之间频繁切换。

背景信息

如果 BFD 会话发生震荡，使用 BFD 的应用将在主备之间频繁切换。为避免这种情况的发生，可以配置 BFD 会话的等待恢复时间。当 BFD 会话从 Down 变为 Up 时，BFD 等待 WTR 超时后才将这个变化通知给上层应用。

请在路由器上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd cfg-name**，进入 BFD 会话视图。

步骤 3 执行命令 **wtr wtr-value**，配置等待恢复时间。

缺省情况下，等待恢复时间 WTR 为 0，即不等待。

 说明

- BFD 会话是单向的。因此，如果使用 WTR，用户需要手工在两端配置相同的 WTR。否则，当一端会话状态变化时，两端应用程序感知到的 BFD 会话状态将不一致。
- 在创建完 BFD 会话后，如果需要修改会话参数（命令包括 **process-pst**、**process-interface-status**、**min-tx-interval**、**min-rx-interval**、**detect-multiplier**、**tos-exp**、**wtr**、**description**），可以执行相关命令即可立即生效，不需要再执行 **commit** 操作。

----结束

5.11.4 配置 BFD 会话的描述信息

通过配置 BFD 会话的描述信息，识别不同的 BFD 会话。

背景信息

 说明

description 命令只对静态配置的 BFD 会话有效，对于动态配置的 BFD 会话和静态标识符自协商 BFD 会话无效。

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd cfg-name**，进入 BFD 会话视图。

步骤 3 执行命令 **description description**，配置 BFD 会话的描述信息。

description 是字符串类型，长度范围是 1 ~ 51。

缺省情况下，BFD 会话的描述信息是空。

可以执行 **undo description** 命令来删除 BFD 会话的描述信息。

 说明

在创建完 BFD 会话后，如果需要修改会话参数（命令包括 **process-pst**、**process-interface-status**、**min-tx-interval**、**min-rx-interval**、**detect-multiplier**、**tos-exp**、**wtr**、**description**），可以执行相关命令即可立即生效，不需要再执行 **commit** 操作。

----结束

5.11.5 检查配置结果

通过查看调整后的 BFD 检测参数，来检查配置是否成功。

前提条件

已经完成调整 BFD 检测参数功能的所有配置。

背景信息



说明

只有配置完 BFD 会话参数并成功建立会话后，才能查看到 BFD 会话信息。

操作步骤

- 使用 **display bfd configuration** { all | static [name *cfg-name*] | discriminator *local-dscr-value* | dynamic | peer-ip *peer-ip* [vpn-instance *vpn-instance-name*] } [verbose] 命令查看 BFD 配置信息。
- 使用 **display bfd configuration** { all | static | peer-ipv6 *peer-ipv6* [vpn6-instance *vpn6-instance-name*] | peer-ipv4 *peer-ipv4* [vpn-instance *vpn-instance-name*] } [verbose] 命令查看 BFD6 配置信息。
- 使用 **display bfd session** { all | discriminator *discr-value* | dynamic | peer-ip *peer-ip* [vpn-instance *vpn-instance-name*] | static } [verbose] [slot *slot-id*] 命令查看 BFD 会话信息。
- 使用 **display bfd session** { all | static | peer-ipv6 *peer-ipv6* [vpn-instance *vpn-instance-name*] | peer-ipv4 *peer-ipv4* [vpn-instance *vpn-instance-name*] } [verbose] [slot *slot-id*] 命令查看 BFD6 会话信息。

----结束

任务示例

配置完成后，执行 **display bfd session all verbose**。

```
<HUAWEI> display bfd session all verbose
```

```
-----
Session MIndex : 256          (One Hop) State : Up          Name : aa
-----
Local Discriminator      : 10          Remote Discriminator : 20
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type           : Interface(GigabitEthernet1/2/0)
Bind Session Type        : Static
Bind Peer Ip Address     : 10.1.1.2
NextHop Ip Address       : 10.1.1.2
Bind Interface           : GigabitEthernet1/2/0
FSM Board Id            : 6            TOS-EXP                : 7
Min Tx Interval (ms)     : 500          Min Rx Interval (ms)    : 500
Actual Tx Interval (ms)  : 500          Actual Rx Interval (ms) : 500
Local Detect Multi       : 3            Detect Interval (ms)    : 30
Echo Passive             : Disable       Acl Number              : --
Destination Port         : 3784          TTL                     : 255
Proc interface status    : Disable       Process PST              : Enable
WTR Interval (ms)        : 60000
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    : -
PDT Index                : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description      : RouterA_to_RouterB
-----
Total UP/DOWN Session Number : 1/0
```

可以看出 BFD 最小发送间隔（Min Tx Interval）为 500 毫秒，最小接收间隔（Min Rx Interval）为 500 毫秒。BFD 等待恢复时间（WTR Interval）为 60000 毫秒。BFD 会话描述信息（Session Description）为“RouterA_to_RouterB”。

5.12 配置全局多跳端口号功能

通过配置全局多跳端口号功能，实现同以前版本的设备或者其它厂商的设备互通。

5.12.1 建立配置任务

在配置全局多跳端口号功能之前，应了解此特性的应用环境、配置此特性的前置任务和
数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

BFD 控制报文封装在 UDP 报文中传送，源端口号的取值范围是 49152 ~ 65535，目的
端口号的取值范围是 3784 或 4784。BFD 草案规定，多跳 BFD 报文的目的端口号是
4784。而 NE80E/40E 早期版本使用 3784 作为多跳 BFD 控制报文的目的端口号。

可以根据需要配置全局多跳端口号功能：

- 同以前版本的设备互通时，使用 3784 作为多跳 BFD 会话报文的目的端口号。
- 同其他厂商的设备互通时，使用 4784 作为多跳 BFD 会话报文的目的端口号。

前置任务

在配置全局多跳端口号功能之前，需完成以下任务：

- 设备安装完毕并加电启动正常。
- 正确连接各接口。

数据准备

在配置全局多跳端口号功能之前，需要准备以下数据。

序号	数据
1	设备的名称。

5.12.2 配置全局多跳端口号

可以根据不同版本的设备和其它厂商设备的不同来配置全局多跳端口号功能。

背景信息

在需要配置全局多跳端口号的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd**，使能本节点的全局 BFD 功能并进入 BFD 全局视图。

步骤 3 执行命令 **multi-hop destination-port { 3784 | 4784 }**，配置全局多跳端口号。

 说明

如果使用 3784 作为多跳 BFD 会话报文的目的端口，则可以使用 4784 作为多跳 BFD 会话报文的目的端口进行互通，同时 3784 侧可以自动更新此多跳 BFD 会话的目的端口。若需要将 4784 侧的多跳 BFD 会话报文的目的端口号修改为 3784，则需要先在 4784 侧 **shutdown**BFD 会话，并在两端执行 **multi-hop destination-port 3784** 命令，然后在 **undo shutdown**BFD 会话。

----结束

5.12.3 检查配置结果

通过查看目的端口号和 TTL 等内容，来检查配置是否成功。

前提条件

已经完成全局多跳端口号功能的所有配置。

背景信息

 说明

只有配置完 BFD 会话参数并成功建立会话后，才能查看到 BFD 会话统计信息和 BFD 会话信息。

操作步骤

- 使用 **display bfd session { all | discriminator *discr-value* | dynamic | peer-ip *peer-ip* [vpn-instance *vpn-instance-name*] | static } [verbose] [slot *slot-id*]** 命令查看 BFD 会话信息。
- 使用 **display bfd statistics [slot *slot-id*]** 命令查看 BFD 全局统计信息。

----结束

任务示例

```
<HUAWEI> display bfd session all verbose
```

```
-----
Session MIndex : 16384      (Multi Hop) State : Up      Name : test
-----
Local Discriminator      : 111      Remote Discriminator : 222
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type           : Interface(GigabitEthernet1/0/0)
Bind Session Type       : Static
Bind Peer IP Address     : 100.1.1.2
NextHop Ip Address      : 100.1.1.2
Bind Interface          : GigabitEthernet1/0/0
FSM Board Id            : 6          TOS-EXP              : 6
Min Tx Interval (ms)    : 10          Min Rx Interval (ms) : 10
Actual Tx Interval (ms): 10          Actual Rx Interval (ms): 10
Local Detect Multi      : 3          Detect Interval (ms) : 30
Echo Passive           : Disable     Acl Number           : -
Destination Port       : 3784      TTL                  : 254
Proc Interface Status   : Disable     Process PST           : Disable
WTR Interval (ms)      : -
Active Multi           : 3
Last Local Diagnostic   : Control Detection Time Expired
Bind Application        : No Application Bind
Session TX TmrID       : -          Session Detect TmrID  : -
Session Init TmrID     : -          Session WTR TmrID     : -
Session Echo Tx TmrID  : -
PDT Index              : FSM-B030000 | RCV-0 | IF-B030000 | TOKEN-0
Session Description     : -
```


可以看到，多跳 BFD 报文的目的端口号（Destination Port）为 3784。

5.13 配置全局 TTL 功能

通过配置全局 TTL 功能，实现和以前版本的设备互通。

5.13.1 建立配置任务

在配置全局 TTL 功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

使用某些不同版本的设备进行互通时，BFD 会话双方 TTL 设置及检测方法不一致，会导致报文被丢弃。为使得使用不同 NE80E/40E 版本的设备能够互通，并考虑后续版本升级以及和其他厂商的设备互通，此时可以配置全局 TTL 功能。

前置任务

在配置全局 TTL 功能之前，需完成以下任务：

- 正确连接各接口。
- 对于三层接口，正确配置接口 IP 地址。

数据准备

在配置全局 TTL 功能之前，需要准备以下数据。

序号	数据
1	接口名称和编号。

5.13.2 配置全局 TTL

和以前版本的设备互通时，可以根据 TTL 值判断单跳和多跳 BFD 会话。

背景信息

在需要配置 TTL 的设备上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **bfd**，使能本节点的全局 BFD 功能并进入 BFD 全局视图。
- 步骤 3** 执行命令 **peer-ip peer-ip mask-length ttl { single-hop | multi-hop } ttl-value**，配置 BFD 报文的生存时间。



说明

缺省情况下，对于静态类会话，单跳 BFD 报文的生存时间为 255，多跳 BFD 报文的生存时间为 254；对于动态类会话，单跳 BFD 报文的生存时间为 255，多跳 BFD 报文的生存时间为 253。

----结束

5.13.3 检查配置结果

通过查看全局 TTL 信息等内容，来检查配置是否成功。

前提条件

已经完成全局 TTL 功能的所有配置。

操作步骤

- 使用 **display bfd session** { **all** | **discriminator** *discr-value* | **dynamic** | **peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] | **static** } [**verbose**] [**slot** *slot-id*] 命令查看 BFD 会话信息。
- 使用 **display bfd ttl** [**slot** *slot-id*] 命令查看配置的全局 TTL 信息。

----结束

任务示例

配置成功后，使用 **display bfd ttl** 命令可以查看配置的全局 TTL 信息。

```
<HUAWEI> display bfd ttl
```

Peer IP	Mask	Type	Value
1.1.1.0	24	Single-hop	255

5.14 配置 Trap 消息定时器的时间间隔

通过配置 Trap 消息定时器的时间间隔，实现对 BFD 的告警信息进行抑制。

5.14.1 建立配置任务

在配置 Trap 消息定时器的时间间隔功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如果 BFD 使能了 SNMP 告警，则在网管侧将会接收到 BFD 会话的 Up 或 Down 消息。此时如果 BFD 会话振荡，则网管侧将会接收到大量的告警信息，因此，需要对 BFD 的 Trap 消息进行抑致。通过配置发送 Trap 消息定时器的时间间隔可以实现对 BFD 的告警信息进行抑制。

前置任务

在配置 TRAP 消息定时器的时间间隔功能之前，需完成以下任务：

- 全局使能 BFD 功能

数据准备

在配置 Trap 消息定时器的时间间隔之前，需要准备以下数据。

序号	数据
1	发送 Trap 消息定时器的时间间隔

5.14.2 配置发送告警消息定时器的时间间隔

BFD 会话震荡时，网管侧会收到大量的告警信息，此时可以配置发送告警消息定时器的时间间隔对告警信息进行抑致。

背景信息

请在需要配置发送告警消息定时器的时间间隔路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd**，使能 BFD 全局能力并进入 BFD 全局视图。

步骤 3 执行命令 **snmp-agent bfd trap-interval interval**，设置发送 TRAP 消息定时器的时间间隔。

缺省情况下，发送 TRAP 消息定时器的时间间隔是 120 秒。

----结束

5.14.3 检查配置结果

通过查看 Trap 消息定时器的时间间隔等内容，来检查配置是否成功。

前提条件

已经完成 TRAP 消息定时器的时间间隔功能的所有配置。

操作步骤

- 使用 **display current-configuration configuration bfd** 命令查看 BFD 的告警功能。

----结束

任务示例

使用 **display current-configuration configuration bfd** 命令可以看到发送 TRAP 消息定时器的时间间隔是 300 秒。

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

```
snmp-agent bfd trap-interval 300
#
return
```

5.15 维护 BFD

通过维护 BFD，可以实现清除 BFD 统计数据和监控 BFD 的运行状况的目的。

5.15.1 清除 BFD 的统计数据

在查看一段时间内的 BFD 的统计信息之前，建议清除 BFD 的统计信息。

背景信息



注意

清除 BFD 的统计信息后，以前的信息将无法恢复，务必仔细确认。

操作步骤

- 步骤 1** 在确认需要清除 BFD 的统计信息后，请在用户视图下执行 **reset bfd statistics** { **all** [**slot slot-id**] | **discriminator** *discr-value* } 命令。

----结束

5.15.2 监控 BFD 运行状况

通过监控 BFD 运行状况，可以了解运行过程中 BFD 的相关信息。

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解 BFD 的运行状况。

操作步骤

- 在任意视图下执行 **display bfd configuration** { **all** | **static** [**name** *cfg-name*] | **discriminator** *local-discr-value* | **dynamic** | **peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] } [**verbose**] 命令，查看 BFD 会话配置信息。
- 在任意视图下执行 **display bfd configuration** { **all** | **static** | **peer-ipv6** *peer-ipv6* [**vpn-instance** *vpn-instance-name*] } [**verbose**] 命令查看 BFD6 配置信息。
- 在任意视图下执行 **display bfd interface** [*interface-type* *interface-number*] 命令，查看使能 BFD 的接口信息。
- 在任意视图下执行 **display bfd session** { **all** | **static** | **dynamic** | **discriminator** *discr-value* | **peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] } [**verbose**] [**slot** *slot-id*] 命令，查看 BFD 会话信息。
- 在任意视图下执行 **display bfd session** { **all** | **static** | **peer-ipv6** *peer-ipv6* [**vpn-instance** *vpn-instance-name*] } [**verbose**] [**slot** *slot-id*] 命令查看 BFD6 会话信息。

- 在任意视图下执行 **display bfd statistics** [slot slot-id] 命令，查看 BFD 全局统计信息。
- 在任意视图下执行 **display bfd statistics session** { all | static | dynamic | discriminator discr-value | peer-ip peer-ip [vpn-instance vpn-instance-name] } [slot slot-id] 命令，查看 BFD 会话的统计信息。
- 在任意视图下执行 **display bfd statistics session** { all | static | peer-ipv6 peer-ipv6 [vpn-instance vpn-instance-name] } [slot slot-id] 查看 BFD6 会话的统计信息。

----结束

5.16 配置举例

介绍 BFD 快速检测链路的各种示例。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

背景信息



说明

手册中所使用的链路接口编号和链路类型以 NE40E-X8 为例，实际使用时以现网设备为准。

5.16.1 配置三层物理链路单跳检测示例

本示例中，通过配置三层物理链路单跳检测，实现快速检测和监控网络中的直连链路。

组网需求

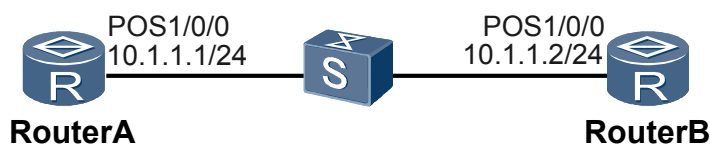


说明

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

如图 5-4 所示，使用 BFD 异步模式检测 RouterA、RouterB 之间的直连链路。

图 5-4 配置三层物理链路单跳检测组网图



配置思路

采用如下思路配置三层物理链路单跳检测：

1. 在 RouterA 上配置 BFD Session，检测 RouterA 到 RouterB 的直连链路。
2. 在 RouterB 上配置 BFD Session，检测 RouterB 到 RouterA 的直连链路。

数据准备

为完成此配置例，需要准备如下数据：

- BFD 检测的对端 IP 地址
- 发送和接收 BFD 控制报文的本端接口
- BFD Session 的本地标识符和远端标识符

 说明

BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数等都使用缺省值。

操作步骤

步骤 1 配置 RouterA 和 RouterB 的直连接口 IP 地址

配置 RouterA 的接口 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] interface pos 1/0/0
[RouterA-Pos1/0/0] undo shutdown
[RouterA-Pos1/0/0] ip address 10.1.1.1 24
[RouterA-Pos1/0/0] quit
```

配置 RouterB 的接口 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] interface pos 1/0/0
[RouterB-Pos1/0/0] undo shutdown
[RouterB-Pos1/0/0] ip address 10.1.1.2 24
[RouterB-Pos1/0/0] quit
```

步骤 2 配置 BFD 单跳检测

在 RouterA 上使能 BFD，并配置与 RouterB 之间的 BFD Session。需要在 BFD Session 中绑定接口。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atob bind peer-ip 10.1.1.2 interface pos 1/0/0
[RouterA-bfd-session-atob] discriminator local 1
[RouterA-bfd-session-atob] discriminator remote 2
[RouterA-bfd-session-atob] min-tx-interval 10
[RouterA-bfd-session-atob] min-rx-interval 10
[RouterA-bfd-session-atob] wtr 5
[RouterA-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
```

在 RouterB 上使能 BFD，并配置与 RouterA 之间的 BFD Session。需要在 BFD Session 中绑定接口。

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bfd atob bind peer-ip 10.1.1.1 interface pos 1/0/0
[RouterB-bfd-session-atob] discriminator local 2
[RouterB-bfd-session-atob] discriminator remote 1
[RouterB-bfd-session-btoa] min-tx-interval 10
[RouterB-bfd-session-btoa] min-rx-interval 10
[RouterB-bfd-session-btoa] wtr 5
[RouterB-bfd-session-atob] commit
[RouterB-bfd-session-atob] quit
```

步骤 3 验证配置结果

配置完成后，在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令，可以看到建立了一个单跳（one hop）的 BFD Session，且状态为 Up。

以 RouterA 上的显示为例。

```
<RouterA> display bfd session all verbose
-----
Session MIndex : 256      (One Hop) State : Up      Name : atob
-----
Local Discriminator      : 1          Remote Discriminator : 2
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type            : Interface(Pos1/0/0)
Bind Session Type        : Static
Bind Peer Ip Address     : 10.1.1.2
NextHop Ip Address       : 10.1.1.2
Bind Interface           : Pos1/0/0
FSM Board Id             : 1          TOS-EXP                : 7
Min Tx Interval (ms)     : 10         Min Rx Interval (ms)   : 10
Actual Tx Interval (ms)  : 10         Actual Rx Interval (ms): 10
Local Detect Multi       : 3          Detect Interval (ms)   : 30
Echo Passive             : Disable     Acl Number             : --
Destination Port         : 3784        TTL                    : 255
Proc interface status    : Disable     Process PST             : Disable
WTR Interval (ms)        : 300000
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    : --
PDT Index                : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description      : --
-----

Total UP/DOWN Session Number : 1/0
```

----结束

配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
bfd
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.1 255.255.255.0
#
bfd atob bind peer-ip 10.1.1.2 interface Pos1/0/0
discriminator local 1
discriminator remote 2
wtr 5
commit
#
return
```
- RouterB 的配置文件

```
#
sysname RouterB
#
bfd
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.2 255.255.255.0
#
bfd btoa bind peer-ip 10.1.1.1 interface Pos1/0/0
discriminator local 2
discriminator remote 1
wtr 5
```

```
commit
#
return
```

5.16.2 配置 IP-Trunk 成员链路单跳检测示例

本示例中，通过在 IP-Trunk 成员接口上创建 BFD 单跳会话，实现 BFD 会话检测 IP-Trunk 成员接口之间的直连链路。

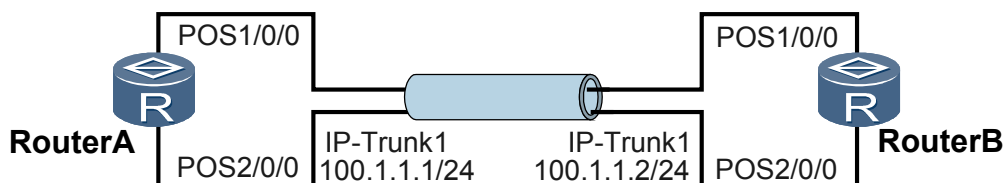
组网需求

 说明

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

如图 5-5 所示，路由器 RouterA、RouterB 之间使用两条 POS 链路组成一条 IP-Trunk。要求对成员链路 POS1/0/0 进行 BFD 检测。

图 5-5 配置 IP-Trunk 成员链路单跳检测组网图



配置思路

采用如下的思路配置 IP-Trunk 成员链路单跳检测：

1. 创建 IP-Trunk 接口。
2. 对指定的成员链路配置 BFD 单跳检测。

数据准备

为完成此配置例，需准备如下的数据：

- BFD 检测的对端 IP 地址，即对端 IP-Trunk 的 IP 地址
- 发送和接收 BFD 控制报文的本端成员链路接口
- BFD Session 的本地标识符和远端标识符

 说明

BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数等都使用缺省值。

操作步骤

步骤 1 配置 IP-Trunk 接口

在 RouterA 上创建 IP-Trunk 接口，并配置 IP-Trunk 的 UP 链路下限阈值为 1。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] interface ip-trunk 1
```



```
[RouterA-Ip-Trunk1] undo shutdown
[RouterA-Ip-Trunk1] ip address 100.1.1.1 255.255.255.0
[RouterA-Ip-Trunk1] least active-linknumber 1
[RouterA-Ip-Trunk1] quit
[RouterA] interface pos 1/0/0
[RouterA-Pos1/0/0] undo shutdown
[RouterA-Pos1/0/0] link-protocol hdlc
[RouterA-Pos1/0/0] ip-trunk 1
[RouterA-Pos1/0/0] quit
[RouterA] interface pos 2/0/0
[RouterA-Pos2/0/0] undo shutdown
[RouterA-Pos2/0/0] link-protocol hdlc
[RouterA-Pos2/0/0] ip-trunk 1
[RouterA-Pos2/0/0] quit
```

在 RouterB 上创建 IP-Trunk 接口，并配置 IP-Trunk 的 UP 链路下限阈值为 1。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] interface ip-trunk 1
[RouterB-Ip-Trunk1] undo shutdown
[RouterB-Ip-Trunk1] ip address 100.1.1.2 255.255.255.0
[RouterB-Ip-Trunk1] least active-linknumber 1
[RouterB-Ip-Trunk1] quit
[RouterB] interface pos 1/0/0
[RouterB-Pos1/0/0] undo shutdown
[RouterB-Pos1/0/0] link-protocol hdlc
[RouterB-Pos1/0/0] ip-trunk 1
[RouterB-Pos1/0/0] quit
[RouterB] interface pos 2/0/0
[RouterB-Pos2/0/0] undo shutdown
[RouterB-Pos2/0/0] link-protocol hdlc
[RouterB-Pos2/0/0] ip-trunk 1
[RouterB-Pos2/0/0] quit
```

配置完成后，在 RouterA 或 RouterB 上执行 **display interface ip-trunk** 命令，可以看到 IP-Trunk 状态为 UP。

以 RouterA 的显示为例。

```
[RouterA] display interface ip-trunk 1
Ip-Trunk1 current state : UP
Line protocol current state : UP
Last line protocol up time: 2007-11-12, 10:18:09
Description : Ip-Trunk1 Interface, Route Port
Route Port,Hash arithmetic : According to flow,Maximal BW: 5G, Current BW: 5G, The Maximum Transmit
Unit is 4470
Internet Address is 100.1.1.1/24 Link layer protocol is nonstandard HDLC

Physical is IP_TRUNK
  Last 300 seconds input rate 192 bits/sec, 0 packets/sec
  Last 300 seconds output rate 24 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: 69 packets,13465 bytes,
        0 errors,71 drops,
  Output:45 packets,1170 bytes,
        0 errors,0 drops
  Input bandwidth utilization : 0.01%
  Output bandwidth utilization : 0.01%
```

PortName	Status	Weight
Pos2/0/0	UP	1
Pos2/0/3	UP	1

```
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 2
```

RouterA 和 RouterB 的 IP-Trunk 接口能够互相 Ping 通。

```
[RouterA] ping -a 100.1.1.1 100.1.1.2
PING 100.1.1.2: 56 data bytes, press CTRL_C to break
  Reply from 100.1.1.2: bytes=56 Sequence=1 ttl=255 time=310 ms
  Reply from 100.1.1.2: bytes=56 Sequence=2 ttl=255 time=30 ms
  Reply from 100.1.1.2: bytes=56 Sequence=3 ttl=255 time=50 ms
  Reply from 100.1.1.2: bytes=56 Sequence=4 ttl=255 time=40 ms
  Reply from 100.1.1.2: bytes=56 Sequence=5 ttl=255 time=40 ms
--- 100.1.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 30/94/310 ms
```

步骤2 配置对 IP-Trunk 的 BFD 单跳检测

在 RouterA 上配置 BFD Session，绑定成员链路接口 POS1/0/0。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd to_Link1 bind peer-ip default-ip interface pos 1/0/0
[RouterA-bfd-session-to_Link1] discriminator local 10
[RouterA-bfd-session-to_Link1] discriminator remote 20
[RouterA-bfd-session-to_Link1] wtr 5
[RouterA-bfd-session-to_Link1] commit
[RouterA-bfd-session-to_Link1] quit
```

在 RouterB 上配置 BFD Session，绑定成员链路接口 POS1/0/0。

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bfd to_Link1 bind peer-ip default-ip interface pos 1/0/0
[RouterB-bfd-session-to_Link1] discriminator local 20
[RouterB-bfd-session-to_Link1] discriminator remote 10
[RouterB-bfd-session-to_Link1] wtr 5
[RouterB-bfd-session-to_Link1] commit
[RouterB-bfd-session-to_Link1] quit
```

步骤3 验证配置结果

配置完成后，在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令，可以看到建立了一个单跳（one hop）的 BFD Session，且状态为 Up。

以 RouterA 上的显示为例。

```
[RouterA] display bfd session all verbose
```

Session MIndex : 256	(One Hop) State : Up	Name : to_link1
Local Discriminator	: 10	Remote Discriminator : 20
Session Detect Mode	: Asynchronous Mode Without Echo Function	
BFD Bind Type	: Interface(Pos1/0/0)	
Bind Session Type	: Static	
Bind Peer Ip Address	: 224.0.0.184	
NextHop Ip Address	: 224.0.0.184	
Bind Interface	: Pos1/0/0	
FSM Board Id	: 1	TOS-EXP : 7
Min Tx Interval (ms)	: 10	Min Rx Interval (ms) : 10
Actual Tx Interval (ms)	: 10	Actual Rx Interval (ms): 10
Local Detect Multi	: 3	Detect Interval (ms) : 30
Echo Passive	: Disable	Acl Number : --
Destination Port	: 3784	TTL : 255
Proc interface status	: Disable	Process PST : Disable
WTR Interval (ms)	: -- 300000	
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 : --
PDT Index	: FSM-0 RCV-0 IF-0 TOKEN-0	

```
Session Description      : --
```

```
-----  
Total UP/DOWN Session Number : 1/0
```

对 RouterA 的 POS1/0/0 接口执行 **shutdown** 操作，模拟链路故障。

```
[RouterA] interface pos 1/0/0  
[RouterA-Pos1/0/0] shutdown  
[RouterA-Pos1/0/0] quit
```

在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令和 **display interface ip-trunk** 命令，可以看到 BFD Session 状态为 Down，但 IP-Trunk 的状态仍然为 UP。

```
[RouterA] display bfd session all verbose
```

```
-----  
Session MIndex : 256      (One Hop) State : Down      Name : to_link1  
-----  
Local Discriminator      : 10      Remote Discriminator : 20  
Session Detect Mode      : Asynchronous Mode Without Echo Function  
BFD Bind Type            : Interface(Pos1/0/0)  
Bind Session Type        : Static  
Bind Peer Ip Address     : 224.0.0.184  
NextHop Ip Address       : 224.0.0.184  
Bind Interface           : Pos1/0/0  
FSM Board Id             : 1      TOS-EXP              : 7  
Min Tx Interval (ms)    : 10      Min Rx Interval (ms) : 10  
Actual Tx Interval (ms) : 10      Actual Rx Interval (ms) : 10  
Local Detect Multi       : 3      Detect Interval (ms) : 30  
Echo Passive             : Disable Acl Number             : --  
Destination Port         : 3784    TTL                  : 255  
Proc interface status    : Disable Process PST           : Disable  
WTR Interval (ms)        : 300000  
Active Multi             : 3  
Last Local Diagnostic    : Control Detection Time Expired  
Bind Application          : No Application Bind  
Session TX TmrID         : --      Session Detect TmrID : --  
Session Init TmrID       : --      Session WTR TmrID   : --  
PDT Index                 : FSM-0|RCV-0|IF-0|TOKEN-0  
Session Description      : --  
-----
```

```
Total UP/DOWN Session Number : 1/0
```

```
[RouterA] display interface ip-trunk 1
```

```
Ip-Trunk1 current state : UP
```

```
Line protocol current state : UP
```

```
Last line protocol up time: 2009-11-12, 11:22:19
```

```
Description : Ip-Trunk1 Interface, Route Port
```

```
Route Port,Hash arithmetic : According to flow,Maximal BW: 5G, Current BW: 5G, The Maximum Transmit  
Unit is 4470
```

```
Internet Address is 100.1.1.1/24 Link layer protocol is nonstandard HDLC
```

```
Physical is IP_TRUNK
```

```
Last 300 seconds input rate 192 bits/sec, 0 packets/sec  
Last 300 seconds output rate 24 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: 69 packets,13465 bytes,  
      0 errors,71 drops,  
Output:45 packets,1170 bytes,  
      0 errors,0 drops  
Input bandwidth utilization : 0.01%  
Output bandwidth utilization : 0.01%
```

```
-----  
PortName      Status      Weight  
-----  
Pos1/0/0      DOWN        1  
Pos2/0/0      UP          1  
-----
```

The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 1

----结束

配置文件

● RouterA 的配置文件

```
#
 sysname RouterA
#
 bfd
#
 interface Ip-Trunk1
  undo shutdown
  ip address 100.1.1.1 255.255.255.0
#
 interface Pos1/0/0
  link-protocol hdlc
  undo shutdown
  ip-trunk 1
#
 interface Pos2/0/0
  link-protocol hdlc
  undo shutdown
  ip-trunk 1
#
 bfd to_Link1 bind peer-ip default-ip interface pos 1/0/0
  discriminator local 10
  discriminator remote 20
  wtr 5
 commit
#
 return
```

● RouterB 的配置文件

```
#
 sysname RouterB
#
 bfd
#
 interface Ip-Trunk1
  undo shutdown
  ip address 100.1.1.2 255.255.255.0
#
 interface Pos1/0/0
  link-protocol hdlc
  undo shutdown
  ip-trunk 1
#
 interface Pos2/0/0
  link-protocol hdlc
  undo shutdown
  ip-trunk 1
#
 bfd to_Link1 bind peer-ip default-ip interface pos 1/0/0
  discriminator local 20
  discriminator remote 10
  wtr 5
 commit
#
 return
```

5.16.3 配置 IP-Trunk 单跳检测示例

本示例中，通过在 IP-Trunk 接口上建立 BFD 单跳会话，实现 BFD 会话检测 IP-Trunk 接口之间的直连链路。

组网需求

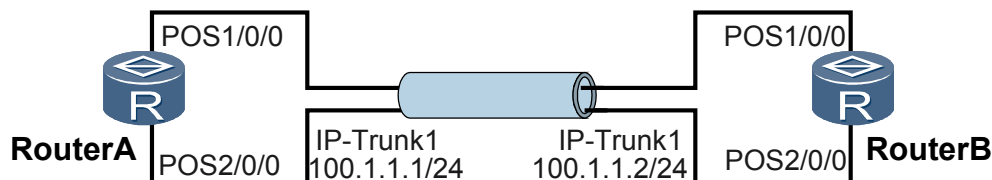
说明

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

如图 5-6 所示：路由器 RouterA、RouterB 之间使用两条 POS 链路组成一条 IP-Trunk。

对 IP-Trunk 链路进行检测。

图 5-6 配置 IP-Trunk 单跳检测组网图



配置思路

采用如下的思路配置 IP-Trunk 单跳检测：

1. 创建 IP-Trunk 接口。
2. 对 IP-Trunk 链路配置 BFD 单跳检测。

数据准备

为完成此配置例，需准备如下的数据：

- BFD 检测的对端 IP 地址，即 IP-Trunk 的 IP 地址
- 发送和接收 BFD 控制报文的本端 IP-Trunk 接口
- BFD Session 的本地标识符和远端标识符

说明

BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数等都使用缺省值。

操作步骤

步骤 1 配置 IP-Trunk 接口

在 RouterA 上创建 IP-Trunk 接口，并配置 IP-Trunk 的 UP 链路下限阈值为 1。

说明

缺省情况下，IP-Trunk 的 Up 链路下限阈值为 1。在其它的组网环境中，用户可以根据实际需要进行配置。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] interface ip-trunk 1
[RouterA-Ip-Trunk1] undo shutdown
[RouterA-Ip-Trunk1] ip address 100.1.1.1 255.255.255.0
[RouterA-Ip-Trunk1] least active-linknumber 1
[RouterA-Ip-Trunk1] quit
[RouterA] interface pos 1/0/0
[RouterA-Pos1/0/0] undo shutdown
```

```
[RouterA-Pos1/0/0] link-protocol hdlc
[RouterA-Pos1/0/0] ip-trunk 1
[RouterA-Pos1/0/0] quit
[RouterA] interface pos 2/0/0
[RouterA-Pos2/0/0] undo shutdown
[RouterA-Pos2/0/0] link-protocol hdlc
[RouterA-Pos2/0/0] ip-trunk 1
[RouterA-Pos2/0/0] quit
```

在 RouterB 上创建 IP-Trunk 接口，并配置 IP-Trunk 的 UP 链路下限阈值为 1。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] interface ip-trunk 1
[RouterB-Ip-Trunk1] undo shutdown
[RouterB-Ip-Trunk1] ip address 100.1.1.2 255.255.255.0
[RouterB-Ip-Trunk1] least active-linknumber 1
[RouterB-Ip-Trunk1] quit
[RouterB] interface pos 1/0/0
[RouterB-Pos1/0/0] undo shutdown
[RouterB-Pos1/0/0] link-protocol hdlc
[RouterB-Pos1/0/0] ip-trunk 1
[RouterB-Pos1/0/0] quit
[RouterB] interface pos 2/0/0
[RouterB-Pos2/0/0] undo shutdown
[RouterB-Pos2/0/0] link-protocol hdlc
[RouterB-Pos2/0/0] ip-trunk 1
[RouterB-Pos2/0/0] quit
```

配置完成后，在 RouterA 或 RouterB 上执行 **display interface ip-trunk** 命令，可以看到接口状态为 UP。

以 RouterA 的显示为例。

```
[RouterA] display interface ip-trunk 1
Ip-Trunk1 current state : UP
Line protocol current state : UP
Last line protocol up time: 2007-11-13, 10:18:19
Description : Ip-Trunk1 Interface, Route Port
Route Port,Hash arithmetic : According to flow,Maximal BW: 5G, Current BW: 5G, The Maximum Transmit
Unit is 4470
Internet Address is 100.1.1.1/24 Link layer protocol is nonstandard HDLC
```

```
Physical is IP_TRUNK
  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 errors,0 drops,
  Output:0 packets,0 bytes,
        0 errors,0 drops
  Input bandwidth utilization : 0.01%
  Output bandwidth utilization : 0.01%
```

PortName	Status	Weight
Pos1/0/0	UP	1
Pos2/0/0	UP	1

```
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 2
```

RouterA 和 RouterB 的 IP-Trunk 接口能够互相 Ping 通。

以 RouterA 的结果为例。

```
[RouterA] ping 100.1.1.2
PING 100.1.1.2: 56 data bytes, press CTRL_C to break
```

```
Reply from 100.1.1.2: bytes=56 Sequence=1 ttl=255 time=220 ms
Reply from 100.1.1.2: bytes=56 Sequence=2 ttl=255 time=30 ms
Reply from 100.1.1.2: bytes=56 Sequence=3 ttl=255 time=10 ms
Reply from 100.1.1.2: bytes=56 Sequence=4 ttl=255 time=30 ms
Reply from 100.1.1.2: bytes=56 Sequence=5 ttl=255 time=40 ms
--- 100.1.1.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 10/66/220 ms
```

步骤 2 配置对 IP-Trunk 的 BFD 单跳检测

在 RouterA 上使能 BFD，并配置与 RouterB 之间的 BFD Session。需要在 BFD Session 中绑定 IP-Trunk 接口。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atob bind peer-ip 100.1.1.2 interface ip-trunk 1
[RouterA-bfd-session-atob] discriminator local 10
[RouterA-bfd-session-atob] discriminator remote 20
[RouterA-bfd-session-atob] wtr 5
[RouterA-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
```

在 RouterB 上使能 BFD，并配置与 RouterA 之间的 BFD Session。需要在 BFD Session 中绑定 IP-Trunk 接口。

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bfd btoa bind peer-ip 100.1.1.1 interface ip-trunk 1
[RouterB-bfd-session-btoa] discriminator local 20
[RouterB-bfd-session-btoa] discriminator remote 10
[RouterB-bfd-session-btoa] wtr 5
[RouterB-bfd-session-btoa] commit
[RouterB-bfd-session-btoa] quit
```

步骤 3 验证配置结果

配置完成后，在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令，可以看到建立了一个单跳（one hop）的 BFD Session，且状态为 Up。

以 RouterA 上的显示为例。

```
[RouterA] display bfd session all verbose
```

Session MIndex : 256	(One Hop) State : Up	Name : atob
Local Discriminator	: 10	Remote Discriminator : 20
Session Detect Mode	: Asynchronous Mode Without Echo Function	
BFD Bind Type	: Interface(Ip-Trunk 1)	
Bind Session Type	: Static	
Bind Peer Ip Address	: 100.1.1.2	
NextHop Ip Address	: 100.1.1.2	
Bind Interface	: Ip-Trunk 1	
FSM Board Id	: 1	TOS-EXP : 7
Min Tx Interval (ms)	: 10	Min Rx Interval (ms) : 10
Actual Tx Interval (ms)	: 10	Actual Rx Interval (ms): 10
Local Detect Multi	: 3	Detect Interval (ms) : 30
Echo Passive	: Disable	Acl Number : --
Destination Port	: 3784	TTL : 255
Proc interface status	: Disable	Process PST : Disable
WTR Interval (ms)	: 300000	
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 : --

```
PDT Index          : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description : --
```

```
-----
Total UP/DOWN Session Number : 1/0
```

对 RouterA 的 POS1/0/0 接口执行 **shutdown** 操作，模拟链路故障。

```
[RouterA] interface pos 1/0/0
[RouterA-Pos1/0/0] shutdown
[RouterA-Pos1/0/0] quit
```

在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令和 **display interface ip-trunk** 命令，可以看到 BFD Session 的状态和 IP-Trunk 接口的状态仍为 Up。

```
[RouterA] display bfd session all verbose
```

```
-----
Session MIndex : 256          (One Hop) State : Up          Name : atob
-----
Local Discriminator      : 10          Remote Discriminator : 20
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type           : Interface(Ip-Trunk 1)
Bind Session Type        : Static
Bind Peer Ip Address     : 100.1.1.2
NextHop Ip Address       : 100.1.1.2
Bind Interface           : Ip-Trunk 1
FSM Board Id            : 1            TOS-EXP                : 7
Min Tx Interval (ms)    : 10          Min Rx Interval (ms)   : 10
Actual Tx Interval (ms) : 10          Actual Rx Interval (ms): 10
Local Detect Multi       : 3            Detect Interval (ms)   : 30
Echo Passive             : Disable      Acl Number              : --
Destination Port         : 3784         TTL                     : 255
Proc interface status    : Disable      Process PST              : Disable
WTR Interval (ms)        : 300000
Active Multi              : 3
Last Local Diagnostic    : Control Detection Time Expired
Bind Application         : No Application Bind
Session TX TmrID         : --          Session Detect TmrID   : --
Session Init TmrID       : --          Session WTR TmrID      : --
PDT Index                : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description      : --
-----
```

```
Total UP/DOWN Session Number : 1/0
```

```
[RouterA] display interface ip-trunk 1
Ip-Trunk1 current state : UP
Line protocol current state : UP
Last line protocol up time: 2007-11-14, 10:12:45
Description : Ip-Trunk1 Interface, Route Port
Route Port,Hash arithmetic : According to flow,Maximal BW: 5G, Current BW: 5G, The Maximum Transmit
Unit is 4470
Internet Address is 100.1.1.1/24 Link layer protocol is nonstandard HDLC
```

```
Physical is IP_TRUNK
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 errors,0 drops,
Output:0 packets,0 bytes,
      0 errors,0 drops
Input bandwidth utilization : 0.01%
Output bandwidth utilization : 0.01%
```

```
-----
PortName          Status          Weight
-----
Pos1/0/0          DOWN              1
Pos2/0/0          UP                1
-----
```

```
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 1
```


对 RouterA 的 POS2/0/0 接口也执行 **shutdown** 操作，模拟链路故障。

```
[RouterA] interface pos 2/0/0
[RouterA-Pos2/0/0] shutdown
[RouterA-Pos2/0/0] quit
```

在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令和 **display interface ip-trunk** 命令，可以看到 BFD Session 的状态和 IP-Trunk 接口的状态都变为 Down。

```
[RouterA] display bfd session all verbose
```

```
-----
Session MIndex : 256          (One Hop) State : Down          Name : atob
-----
Local Discriminator      : 10          Remote Discriminator   : 20
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type           : Interface(Ip-Trunk 1)
Bind Session Type        : Static
Bind Peer Ip Address     : 100.1.1.2
NextHop Ip Address       : 100.1.1.2
Bind Interface           : Ip-Trunk 1
FSM Board Id            : 1           TOS-EXP                  : 7
Min Tx Interval (ms)    : 10          Min Rx Interval (ms)    : 10
Actual Tx Interval (ms) : 10          Actual Rx Interval (ms) : 10
Local Detect Multi       : 3           Detect Interval (ms)    : 30
Echo Passive             : Disable     Acl Number              : --
Destination Port         : 3784        TTL                     : 255
Proc interface status    : Disable     Process PST              : Disable
WTR Interval (ms)       : 300000
Active Multi             : 3
Last Local Diagnostic    : Control Detection Time Expired
Bind Application         : No Application Bind
Session TX TmrID         : --          Session Detect TmrID    : --
Session Init TmrID       : --          Session WTR TmrID      : --
PDT Index                : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description      : --
-----
```

```
Total UP/DOWN Session Number : 1/0
[RouterA] display interface ip-trunk 1
Ip-Trunk1 current state : Down
Line protocol current state : Down
Last line protocol up time: 2007-11-15, 12:12:19
Description : Ip-Trunk1 Interface, Route Port
Route Port,Hash arithmetic : According to flow,Maximal BW: 5G, Current BW: 5G, T,he Maximum Transmit
Unit is 4470
Internet Address is 100.1.1.1/24 Link layer protocol is nonstandard HDLC

Physical is IP_TRUNK
  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 errors,0 drops,
  Output:0 packets,0 bytes,
        0 errors,0 drops
  Input bandwidth utilization : 0.01%
  Output bandwidth utilization : 0.01%
```

PortName	Status	Weight
Pos1/0/0	DOWN	1
Pos2/0/0	DOWN	1

```
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 0
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 bfd
#
interface Ip-Trunk1
 undo shutdown
 ip address 100.1.1.1 255.255.255.0
#
interface Pos1/0/0
 link-protocol hdlc
 undo shutdown
 ip-trunk 1
#
interface Pos2/0/0
 link-protocol hdlc
 undo shutdown
 ip-trunk 1
#
bfd atob bind peer-ip 100.1.1.2 interface ip-trunk 1
 discriminator local 10
 discriminator remote 20
 wtr 5
commit
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 bfd
#
interface Ip-Trunk1
 undo shutdown
 ip address 100.1.1.2 255.255.255.0
#
interface Pos1/0/0
 link-protocol hdlc
 undo shutdown
 ip-trunk 1
#
interface Pos2/0/0
 link-protocol hdlc
 undo shutdown
 ip-trunk 1
#
bfd btoa bind peer-ip 100.1.1.1 interface ip-trunk 1
 discriminator local 20
 discriminator remote 10
 wtr 5
commit
#
return
```

5.16.4 配置三层 Eth-Trunk 成员链路单跳检测示例

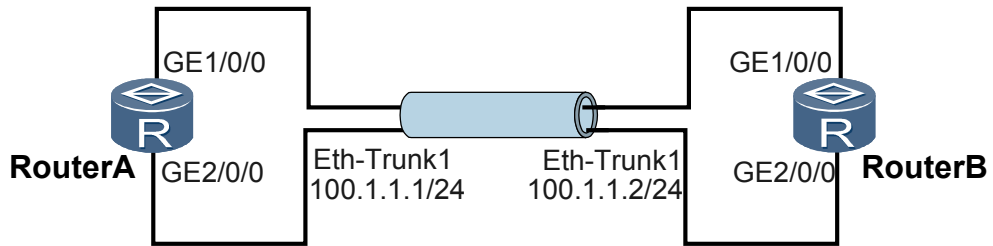
本示例中，通过在 Eth-Trunk 成员接口上创建 BFD 单跳会话，实现 BFD 会话检测 Eth-Trunk 成员接口之间的直连链路。

组网需求

如图 5-7 所示，路由器 RouterA、RouterB 之间使用两条 GE 链路组成一条 Eth-Trunk。

要求对成员链路 GE1/0/0 进行 BFD 检测。

图 5-7 配置三层 Eth-Trunk 成员链路单跳检测组网图



配置思路

采用如下的思路配置 Eth-Trunk 成员链路单跳检测：

1. 创建 Eth-Trunk 接口。
2. 对指定成员链路配置 BFD 单跳检测。

数据准备

为完成此配置例，需准备如下的数据：

- BFD 检测的对端 IP 地址，即 Eth-Trunk 的 IP 地址
- 发送和接收 BFD 控制报文的本端成员链路接口
- BFD Session 的本地标识符和远端标识符

说明

BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数等都使用缺省值。

操作步骤

步骤 1 配置 Eth-Trunk 接口

在 RouterA 上创建 Eth-Trunk 接口。

```

<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] interface eth-trunk 1
[RouterA-Eth-Trunk1] undo shutdown
[RouterA-Eth-Trunk1] ip address 100.1.1.1 24
[RouterA-Eth-Trunk1] least active-linknumber 1
[RouterA-Eth-Trunk1] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] undo shutdown
[RouterA-GigabitEthernet1/0/0] eth-trunk 1
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] undo shutdown
[RouterA-GigabitEthernet2/0/0] eth-trunk 1
[RouterA-GigabitEthernet2/0/0] quit

```

在 RouterB 上创建 Eth-Trunk 接口。

```

<HUAWEI> system-view

```

```
[HUAWEI] sysname RouterB
[RouterB] interface eth-trunk 1
[RouterB-Eth-Trunk1] undo shutdown
[RouterB-Eth-Trunk1] ip address 100.1.1.2 24
[RouterB-Eth-Trunk1] least active-linknumber 1
[RouterB-Eth-Trunk1] quit
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] undo shutdown
[RouterB-GigabitEthernet1/0/0] eth-trunk 1
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] undo shutdown
[RouterB-GigabitEthernet2/0/0] eth-trunk 1
[RouterB-GigabitEthernet2/0/0] quit
```

配置完成后，在 RouterA 或 RouterB 上执行 **display interface eth-trunk** 命令，可以看到接口状态为 UP。

以 RouterA 的显示为例。

```
[RouterA] display interface eth-trunk 1
Eth-Trunk1 current state : UP
Line protocol current state : UP
Last line protocol up time: 2007-11-10, 11:35:19
Current system time: 2010-08-30 18:02:12
Description: Eth-Trunk1 Interface
Route Port,Hash arithmetic : According to flow,Maximal BW: 4G, Current BW: 4G, The Maximum Transmit
Unit is 1500
Internet Address is 100.1.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc90-5851
Physical is ETH_TRUNK
  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 drops
  Output:0 packets,0 bytes
    0 unicast,0 broadcast,0 multicast
    0 errors,0 drops
  Input bandwidth utilization : 0.00%
  Output bandwidth utilization : 0.01%
```

PortName	Status	Weight
GigabitEthernet1/0/0	UP	1
GigabitEthernet2/0/0	UP	1

```
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 2
```

RouterA 和 RouterB 的 Eth-Trunk 接口能够互相 Ping 通。

```
[RouterA] ping -a 100.1.1.1 100.1.1.2
PING 100.1.1.2: 56 data bytes, press CTRL_C to break
  Reply from 100.1.1.2: bytes=56 Sequence=1 ttl=255 time=31 ms
  Reply from 100.1.1.2: bytes=56 Sequence=2 ttl=255 time=31 ms
  Reply from 100.1.1.2: bytes=56 Sequence=3 ttl=255 time=62 ms
  Reply from 100.1.1.2: bytes=56 Sequence=4 ttl=255 time=62 ms
  Reply from 100.1.1.2: bytes=56 Sequence=5 ttl=255 time=62 ms
--- 100.1.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 31/49/62 ms
```

步骤 2 配置对三层 Eth-Trunk 成员链路的 BFD 单跳检测

在 RouterA 上配置 BFD Session，绑定成员链路接口 GE1/0/0。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd to_link1 bind peer-ip default-ip interface gigabitethernet 1/0/0
[RouterA-bfd-session-to_link1] discriminator local 10
[RouterA-bfd-session-to_link1] discriminator remote 11
[RouterA-bfd-session-to_link1] wtr 5
[RouterA-bfd-session-to_link1] commit
[RouterA-bfd-session-to_link1] quit
```

在 RouterB 上配置 BFD Session，绑定成员链路接口 GE1/0/0。

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bfd to_link1 bind peer-ip default-ip interface gigabitethernet 1/0/0
[RouterB-bfd-session-to_link1] discriminator local 11
[RouterB-bfd-session-to_link1] discriminator remote 10
[RouterB-bfd-session-to_link1] wtr 5
[RouterB-bfd-session-to_link1] commit
[RouterB-bfd-session-to_link1] quit
```

步骤3 验证配置结果

配置完成后，在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令，可以看到建立了 1 个单跳（one hop）的 BFD Session，且状态为 Up。

以 RouterA 上的显示为例。

```
[RouterA] display bfd session all verbose
```

Session MIndex : 256	(One Hop) State : Up	Name : to_link1
Local Discriminator : 10	Remote Discriminator : 11	
Session Detect Mode : Asynchronous Mode Without Echo Function		
BFD Bind Type : Interface(GigabitEthernet1/0/0)		
Bind Session Type : Static		
Bind Peer Ip Address : 224.0.0.184		
NextHop Ip Address : 224.0.0.184		
Bind Interface : GigabitEthernet1/0/0		
FSM Board Id : 1	TOS-EXP : 7	
Min Tx Interval (ms) : 10	Min Rx Interval (ms) : 10	
Actual Tx Interval (ms) : 10	Actual Rx Interval (ms) : 10	
Local Detect Multi : 3	Detect Interval (ms) : 30	
Echo Passive : Disable	Acl Number : --	
Destination Port : 3784	TTL : 255	
Proc interface status : Disable	Process PST : Disable	
WTR Interval (ms) : 300000		
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 : --	
PDT Index : FSM-0 RCV-0 IF-0 TOKEN-0		
Session Description : --		

Total UP/DOWN Session Number : 1/0

对 RouterA 的 GE1/0/0 接口执行 **shutdown** 命令，模拟链路故障。BFD 会话 Down，但 Eth-Trunk 的状态仍为 Up。

```
[RouterA] display bfd session all verbose
```

Session MIndex : 256	(One Hop) State : Down	Name : to_link1
Local Discriminator : 10	Remote Discriminator : 11	
Session Detect Mode : Asynchronous Mode Without Echo Function		
BFD Bind Type : Interface(GigabitEthernet1/0/0)		
Bind Session Type : Static		
Bind Peer Ip Address : 224.0.0.184		
NextHop Ip Address : 224.0.0.184		

```
Bind Interface      : GigabitEthernet1/0/0
FSM Board Id       : 1                      TOS-EXP           : 7
Min Tx Interval (ms) : 10                   Min Rx Interval (ms) : 10
Actual Tx Interval (ms) : 10                 Actual Rx Interval (ms) : 10
Local Detect Multi   : 3                   Detect Interval (ms) : 30
Echo Passive         : Disable              Acl Number         : --
Destination Port     : 3784                 TTL                 : 255
Proc interface status : Disable             Process PST         : Disable
WTR Interval (ms)    : 300000
Active Multi         : 3
Last Local Diagnostic : Control Detection Time Expired
Bind Application     : No Application Bind
Session TX TmrID     : --                   Session Detect TmrID : --
Session Init TmrID   : --                   Session WTR TmrID    : --
PDT Index            : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description   : --
```

```
-----
Total UP/DOWN Session Number : 1/0
[RouterA] display interface eth-trunk 1
Eth-Trunk1 current state : UP
Line protocol current state : UP
Last line protocol up time: 2007-11-16, 11:22:19
Current system time: 2010-08-30 18:04:12
Description: Eth-Trunk1 Interface
Route Port,Hash arithmetic : According to flow,Maximal BW: 4G, Current BW: 4G, The Maximum Transmit
Unit is 1500
Internet Address is 100.1.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc90-5851
Physical is ETH_TRUNK
  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 drops
  Output:0 packets,0 bytes
        0 unicast,0 broadcast,0 multicast
        0 errors,0 drops
  Input bandwidth utilization : 0.00%
  Output bandwidth utilization : 0.01%
```

PortName	Status	Weight
GigabitEthernet1/0/0	DOWN	1
GigabitEthernet2/0/0	UP	1

```
-----
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 1
```

----结束

配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
bfd
#
interface Eth-Trunk1
undo shutdown
ip address 100.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
undo shutdown
eth-trunk 1
#
```

```
interface GigabitEthernet2/0/0
 undo shutdown
 eth-trunk 1
#
bfd to_link1 bind peer-ip default-ip interface GigabitEthernet 1/0/0
 discriminator local 10
 discriminator remote 11
 wtr 5
 commit
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
bfd
#
interface Eth-Trunk1
 undo shutdown
 ip address 100.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/0
 undo shutdown
 eth-trunk 1
#
interface GigabitEthernet2/0/0
 undo shutdown
 eth-trunk 1
#
bfd to_link1 bind peer-ip default-ip interface GigabitEthernet 1/0/0
 discriminator local 11
 discriminator remote 10
 wtr 5
 commit
#
return
```

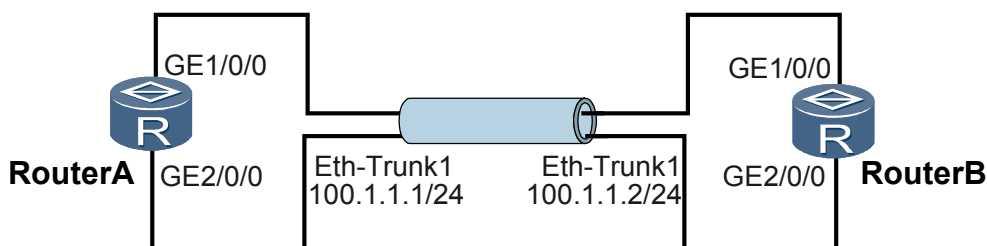
5.16.5 配置三层 Eth-Trunk 单跳检测示例

本示例中，通过在 Eth-Trunk 接口上创建 BFD 单跳会话，实现 BFD 会话检测 Eth-Trunk 接口之间的直连链路。

组网需求

如图 5-8 所示：路由器 RouterA、RouterB 之间使用两条 GE 链路组成一条 Eth-Trunk。对 Eth-Trunk 链路进行检测。

图 5-8 配置三层 Eth-Trunk 单跳检测组网图



配置思路

采用如下的思路配置 Eth-Trunk 单跳检测：

1. 创建 Eth-Trunk 接口。
2. 对 Eth-Trunk 链路配置 BFD 单跳检测。

数据准备

为完成此配置例，需准备如下的数据：

- BFD 检测的对端 IP 地址，即 Eth-Trunk 的 IP 地址
- 发送和接收 BFD 控制报文的本端 Eth-Trunk 接口
- BFD Session 的本地标识符和远端标识符



说明

BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数等都使用缺省值。

操作步骤

步骤 1 配置 Eth-Trunk 接口

在 RouterA 上创建 Eth-Trunk 接口，并配置 Eth-Trunk 的 UP 链路下限阈值为 1。



说明

缺省情况下，Eth-Trunk 的 Up 链路下限阈值为 1。在其它的组网环境中，用户可以根据实际需要进行配置。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] interface eth-trunk 1
[RouterA-Eth-Trunk1] undo shutdown
[RouterA-Eth-Trunk1] ip address 100.1.1.1 24
[RouterA-Eth-Trunk1] least active-linknumber 1
[RouterA-Eth-Trunk1] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] undo shutdown
[RouterA-GigabitEthernet1/0/0] eth-trunk 1
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] undo shutdown
[RouterA-GigabitEthernet2/0/0] eth-trunk 1
[RouterA-GigabitEthernet2/0/0] quit
```

在 RouterB 上创建 Eth-Trunk 接口，并配置 Eth-Trunk 的 UP 链路下限阈值为 1。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] interface eth-trunk 1
[RouterB-Eth-Trunk1] undo shutdown
[RouterB-Eth-Trunk1] ip address 100.1.1.2 24
[RouterB-Eth-Trunk1] least active-linknumber 1
[RouterB-Eth-Trunk1] quit
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] undo shutdown
[RouterB-GigabitEthernet1/0/0] eth-trunk 1
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] undo shutdown
[RouterB-GigabitEthernet2/0/0] eth-trunk 1
[RouterB-GigabitEthernet2/0/0] quit
```


配置完成后，在 RouterA 或 RouterB 上执行 **display interface eth-trunk** 命令，可以看到接口状态为 UP。

以 RouterA 的显示为例。

```
[RouterA] display interface eth-trunk 1
Eth-Trunk1 current state : UP
Line protocol current state : UP
Last line protocol up time: 2007-11-13, 10:19:19
Description: Eth-Trunk1 Interface
Route Port, Hash arithmetic : According to flow, Maximal BW: 4G, Current BW: 4G, The Maximum Transmit
Unit is 1500
Internet Address is 100.1.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc90-5851
Physical is ETH_TRUNK
  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 drops
  Output: 0 packets, 0 bytes
    0 unicast, 0 broadcast, 0 multicast
    0 errors, 0 drops
  Input bandwidth utilization : 0.00%
  Output bandwidth utilization : 0.01%
```

PortName	Status	Weight
GigabitEthernet1/0/0	UP	1
GigabitEthernet2/0/0	UP	1

```
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 2
```

RouterA 和 RouterB 的 Eth-Trunk 接口能够互相 Ping 通。

```
[RouterA] ping -a 100.1.1.1 100.1.1.2
PING 100.1.1.2: 56 data bytes, press CTRL_C to break
  Reply from 100.1.1.2: bytes=56 Sequence=1 ttl=255 time=31 ms
  Reply from 100.1.1.2: bytes=56 Sequence=2 ttl=255 time=31 ms
  Reply from 100.1.1.2: bytes=56 Sequence=3 ttl=255 time=62 ms
  Reply from 100.1.1.2: bytes=56 Sequence=4 ttl=255 time=62 ms
  Reply from 100.1.1.2: bytes=56 Sequence=5 ttl=255 time=62 ms
--- 100.1.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 31/49/62 ms
```

步骤2 配置对三层 Eth-Trunk 链路的 BFD 单跳检测

在 RouterA 上使能 BFD，并配置与 RouterB 之间的 BFD Session。需要在 BFD Session 中绑定 Eth-Trunk 接口。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atob bind peer-ip 100.1.1.2 interface eth-trunk 1
[RouterA-bfd-session-atob] discriminator local 10
[RouterA-bfd-session-atob] discriminator remote 20
[RouterA-bfd-session-atob] wtr 5
[RouterA-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
```

在 RouterB 上使能 BFD，并配置与 RouterA 之间的 BFD Session。需要在 BFD Session 中绑定 Eth-Trunk 接口。

```
[RouterB] bfd
```

```
[RouterB-bfd] quit
[RouterB] bfd btoa bind peer-ip 100.1.1.1 interface eth-trunk 1
[RouterB-bfd-session-btoa] discriminator local 20
[RouterB-bfd-session-btoa] discriminator remote 10
[RouterB-bfd-session-btoa] wtr 5
[RouterB-bfd-session-btoa] commit
[RouterB-bfd-session-btoa] quit
```

步骤3 验证配置结果

配置完成后，在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令，可以看到建立了一个单跳（one hop）的 BFD Session，且状态为 Up。

以 RouterA 上的显示为例。

```
[RouterA] display bfd session all verbose
```

```
-----
Session MIndex : 256          (One Hop) State :Up          Name : atob
-----
Local Discriminator      : 10          Remote Discriminator : 20
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type            : Interface(Eth-Trunk1)
Bind Session Type        : Static
Bind Peer Ip Address     : 100.1.1.2
NextHop Ip Address       : 100.1.1.2
Bind Interface           : Eth-Trunk1
FSM Board Id             : 1           TOS-EXP                : 7
Min Tx Interval (ms)     : 10          Min Rx Interval (ms)   : 10
Actual Tx Interval (ms)  : 10          Actual Rx Interval (ms): 10
Local Detect Multi       : 3           Detect Interval (ms)   : 30
Echo Passive             : Disable      Acl Number             : --
Destination Port         : 3784         TTL                    : 255
Proc interface status    : Disable      Process PST             : Disable
WTR Interval (ms)        : --
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      : --
PDT Index               : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description      : --
-----
Total UP/DOWN Session Number : 1/0
```

对 RouterA 的 GE1/0/0 接口执行 **shutdown** 操作，模拟链路故障。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] shutdown
[RouterA-GigabitEthernet1/0/0] quit
```

在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令和 **display interface eth-trunk** 命令，可以看到 BFD Session 的状态和 Eth-Trunk 接口的状态仍为 Up。

```
[RouterA] display bfd session all verbose
```

```
-----
Session MIndex : 256          (One Hop) State : Up          Name : atob
-----
Local Discriminator      : 10          Remote Discriminator : 20
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type            : Interface(Eth-Trunk1)
Bind Session Type        : Static
Bind Peer Ip Address     : 100.1.1.2
NextHop Ip Address       : 100.1.1.2
Bind Interface           : Eth-Trunk1
FSM Board Id             : 1           TOS-EXP                : 7
Min Tx Interval (ms)     : 10          Min Rx Interval (ms)   : 10
Actual Tx Interval (ms)  : 10          Actual Rx Interval (ms): 10
Local Detect Multi       : 3           Detect Interval (ms)   : 30
Echo Passive             : Disable      Acl Number             : --
```

```
Destination Port      : 3784          TTL           : 255
Proc interface status : Disable       Process PST    : Disable
WTR Interval (ms)    : --
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    : --
PDT Index             : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description   : --
```

Total UP/DOWN Session Number : 1/0

[RouterA] **display interface eth-trunk 1**

Eth-Trunk1 current state : **UP**

Line protocol current state : UP

Last line protocol up time: 2007-11-11, 11:09:19

Description: Eth-Trunk1 Interface

Route Port, Hash arithmetic : According to flow, Maximal BW: 4G, Current BW: 4G, The Maximum Transmit Unit is 1500

Internet Address is 100.1.1.1/24

IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc90-5851

Physical is ETH_TRUNK

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 drops

Output: 0 packets, 0 bytes

0 unicast, 0 broadcast, 0 multicast

0 errors, 0 drops

Input bandwidth utilization : 0.00%

Output bandwidth utilization : 0.01%

PortName	Status	Weight
GigabitEthernet1/0/0	DOWN	1
GigabitEthernet2/0/0	UP	1

The Number of Ports in Trunk : 2

The Number of UP Ports in Trunk : 1

对 RouterA 的 GE2/0/0 接口也执行 **shutdown** 操作，模拟链路故障。

在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令和 **display interface eth-trunk** 命令，可以看到 BFD Session 的状态和 Eth-Trunk 接口的状态都变为 Down。

以 RouterA 上的显示为例。

[RouterA] **display bfd session all verbose**

Session MIndex : 256 (One Hop) State : **Down** Name : atob

Local Discriminator	: 10	Remote Discriminator	: 20
Session Detect Mode	: Asynchronous Mode Without Echo Function		
BFD Bind Type	: Interface(Eth-Trunk1)		
Bind Session Type	: Static		
Bind Peer Ip Address	: 100.1.1.2		
NextHop Ip Address	: 100.1.1.2		
Bind Interface	: Eth-Trunk1		
FSM Board Id	: 1	TOS-EXP	: 7
Min Tx Interval (ms)	: 10	Min Rx Interval (ms)	: 10
Actual Tx Interval (ms)	: 10	Actual Rx Interval (ms)	: 10
Local Detect Multi	: 3	Detect Interval (ms)	: 30
Echo Passive	: Disable	Acl Number	: --
Destination Port	: 3784	TTL	: 255
Proc interface status	: Disable	Process PST	: Disable
WTR Interval (ms)	: --		

```
Active Multi          : 3
Last Local Diagnostic : Control Detection Time Expired
Bind Application      : No Application Bind
Session TX TmrID      : --
Session Init TmrID    : --
PDT Index             : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description   : --

-----
Total UP/DOWN Session Number : 1/0
[RouterA] display interface eth-trunk 1
Eth-Trunk1 current state : Down
Line protocol current state : Down
Last line protocol up time: 2007-11-10, 09:12:19
Description: Eth-Trunk1 Interface
Route Port,Hash arithmetic : According to flow,Maximal BW: 4G, Current BW: 4G, The Maximum Transmit
Unit is 1500
Internet Address is 100.1.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc90-5851
Physical is ETH_TRUNK
  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 drops
  Output:0 packets,0 bytes
        0 unicast,0 broadcast,0 multicast
        0 errors,0 drops
  Input bandwidth utilization : 0.00%
  Output bandwidth utilization : 0.01%

-----
PortName              Status      Weight
-----
GigabitEthernet1/0/0  DOWN      1
GigabitEthernet2/0/0  DOWN      1
-----

The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 0
```

----结束

配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
bfd
#
interface Eth-Trunk1
undo shutdown
ip address 100.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
undo shutdown
eth-trunk 1
#
interface GigabitEthernet2/0/0
undo shutdown
eth-trunk 1
#
bfd atob bind peer-ip 100.1.1.2 interface Eth-Trunk 1
discriminator local 10
discriminator remote 20
wtr 5
commit
#
```

```
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
bfd
#
interface Eth-Trunk1
undo shutdown
ip address 100.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/0
undo shutdown
eth-trunk 1
#
interface GigabitEthernet2/0/0
undo shutdown
eth-trunk 1
#
bfd toa bind peer-ip 100.1.1.1 interface Eth-Trunk 1
discriminator local 20
discriminator remote 10
wtr 5
commit
#
return
```

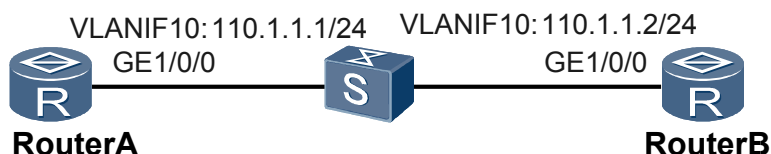
5.16.6 配置 VLANIF 接口单跳检测示例

本示例中，通过在 VLANIF 接口上创建单跳 BFD 会话，实现 BFD 会话检测 VLANIF 接口之间的直连链路。

组网需求

如图 5-9 所示，RouterA 和 RouterB 之间有一条以太网链路。其中 RouterA 的 GE1/0/0 接口和 RouterB 的 GE1/0/0 接口属于同一个 VLAN。建立单跳 BFD 会话对 VLANIF 接口进行检测。

图 5-9 配置 VLANIF 接口单跳检测组网图



配置思路

采用如下的思路配置 VLANIF 接口单跳检测：

1. 配置基于端口的 VLAN。
2. 在 VLANIF 接口上配置 BFD 单跳检测。

数据准备

为完成此配置例，需准备如下的数据：

- BFD 检测的对端 IP 地址，即对端 VLANIF 接口的 IP 地址
- 发送和接收 BFD 控制报文的本端 VLANIF 接口
- BFD Session 的本地标识符和远端标识符

 说明

BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数等都使用缺省值。

操作步骤

步骤 1 配置 VLAN10

在 RouterA 上配置 VLAN10。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] undo shutdown
[RouterA-GigabitEthernet1/0/0] portswitch
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] vlan 10
[RouterA-vlan10] port gigabitethernet 1/0/0
[RouterA-vlan10] quit
[RouterA] interface vlanif 10
[RouterA-Vlanif10] undo shutdown
[RouterA-Vlanif10] ip address 110.1.1.1 24
[RouterA-Vlanif10] quit
```

在 RouterB 上配置 VLAN10。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] undo shutdown
[RouterB-GigabitEthernet1/0/0] portswitch
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] vlan 10
[RouterB-vlan10] port gigabitethernet 1/0/0
[RouterB-vlan10] quit
[RouterB] interface vlanif 10
[RouterB-Vlanif10] undo shutdown
[RouterB-Vlanif10] ip address 110.1.1.2 24
[RouterB-Vlanif10] quit
```

配置完成后，在 RouterA 或 RouterB 上执行 **display interface vlanif** 命令，可以看到接口状态为 UP。

以 RouterA 的显示为例。

```
[RouterA] display interface vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Last line protocol up time: 2007-11-14, 10:45:35
Current system time: 2010-08-30 18:13:11
Description: Vlanif10 Interface
Route Port, The Maximum Transmit Unit is 1500
Internet Address is 110.1.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc50-c43d
Physical is VLANIF
  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
  Output: 0 packets, 0 bytes
    0 unicast, 0 broadcast, 0 multicast
  Input bandwidth utilization : --
  Output bandwidth utilization : --
```

RouterA 和 RouterB 的 VLANIF 接口能够互相 Ping 通。

```
[RouterA] ping -a 110.1.1.1 110.1.1.2
PING 110.1.1.2: 56 data bytes, press CTRL_C to break
  Reply from 110.1.1.2: bytes=56 Sequence=1 ttl=255 time=31 ms
  Reply from 110.1.1.2: bytes=56 Sequence=2 ttl=255 time=31 ms
  Reply from 110.1.1.2: bytes=56 Sequence=3 ttl=255 time=62 ms
  Reply from 110.1.1.2: bytes=56 Sequence=4 ttl=255 time=62 ms
  Reply from 110.1.1.2: bytes=56 Sequence=5 ttl=255 time=62 ms
--- 110.1.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 31/49/62 ms
```

步骤 2 配置对 VLANIF 的 BFD 单跳检测

在 RouterA 上使能 BFD，并配置与 RouterB 之间的 BFD Session。需要在 BFD Session 中绑定 VLANIF 接口。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atob bind peer-ip 110.1.1.2 interface vlanif 10
[RouterA-bfd-session-atob] discriminator local 10
[RouterA-bfd-session-atob] discriminator remote 20
[RouterA-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
```

在 RouterB 上使能 BFD，并配置与 RouterA 之间的 BFD Session。需要在 BFD Session 中绑定 VLANIF 接口。

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bfd btoa bind peer-ip 110.1.1.1 interface vlanif 10
[RouterB-bfd-session-btoa] discriminator local 20
[RouterB-bfd-session-btoa] discriminator remote 10
[RouterB-bfd-session-btoa] commit
[RouterB-bfd-session-btoa] quit
```

步骤 3 验证配置结果

以 RouterA 上的显示为例。

```
[RouterA] display bfd session all verbose
```

Session MIndex : 256	(One Hop) State : Up	Name : atob
Local Discriminator	: 10	Remote Discriminator : 20
Session Detect Mode	: Asynchronous Mode Without Echo Function	
BFD Bind Type	: Interface(Vlanif10)	
Bind Session Type	: Static	
Bind Peer Ip Address	: 110.1.1.2	
NextHop Ip Address	: 110.1.1.2	
Bind Interface	: Vlanif10	
FSM Board Id	: 1	TOS-EXP : 7
Min Tx Interval (ms)	: 10	Min Rx Interval (ms) : 10
Actual Tx Interval (ms)	: 10	Actual Rx Interval (ms): 10
Local Detect Multi	: 3	Detect Interval (ms) : 30
Echo Passive	: Disable	Acl Number : --
Destination Port	: 3784	TTL : 255
Proc interface status	: Disable	Process PST : Disable
WTR Interval (ms)	: --	
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 : --
PDT Index	: FSM-0 RCV-0 IF-0 TOKEN-0	
Session Description	: --	

Total UP/DOWN Session Number : 1/0

对 RouterA 的 GE1/0/0 接口执行 **shutdown** 操作，模拟链路故障。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] shutdown
[RouterA-GigabitEthernet1/0/0] quit
```

在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令，可以看到 BFD Session 的状态变为 Down。

以 RouterA 上的显示为例。

```
[RouterA] display bfd session all verbose
```

Session MIndex : 256 (One Hop) State : **Down** Name : atob

Local Discriminator	: 10	Remote Discriminator	: 20
Session Detect Mode	: Asynchronous Mode Without Echo Function		
BFD Bind Type	: Interface(Vlanif10)		
Bind Session Type	: Static		
Bind Peer Ip Address	: 110.1.1.2		
NextHop Ip Address	: 110.1.1.2		
Bind Interface	: Vlanif10		
FSM Board Id	: 1	TOS-EXP	: 7
Min Tx Interval (ms)	: 10	Min Rx Interval (ms)	: 10
Actual Tx Interval (ms)	: 10	Actual Rx Interval (ms)	: 10
Local Detect Multi	: 3	Detect Interval (ms)	: 30
Echo Passive	: Disable	Acl Number	: --
Destination Port	: 3784	TTL	: 255
Proc interface status	: Disable	Process PST	: Disable
WTR Interval (ms)	: --		
Active Multi	: 3		
Last Local Diagnostic	: Control Detection Time Expired		
Bind Application	: No Application Bind		
Session TX TmrID	: --	Session Detect TmrID	: --
Session Init TmrID	: --	Session WTR TmrID	: --
PDT Index	: FSM-0 RCV-0 IF-0 TOKEN-0		
Session Description	: --		

Total UP/DOWN Session Number : 0/1

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 vlan batch 10
#
 bfd
#
 interface Vlanif10
 undo shutdown
 ip address 110.1.1.1 255.255.255.0
#
 interface GigabitEthernet1/0/0
 undo shutdown
 portswitch
 port default vlan 10
#
 bfd atob bind peer-ip 110.1.1.2 interface vlanif 10
 discriminator local 10
 discriminator remote 20
 commit
```



```
#
return

● RouterB 的配置文件

#
sysname RouterB
#
vlan batch 10
#
bfd
#
interface Vlanif10
undo shutdown
ip address 110.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/0
undo shutdown
portswitch
port default vlan 10
#
bfd toa bind peer-ip 110.1.1.1 interface vlanif 10
discriminator local 20
discriminator remote 10
commit
#
Return
```

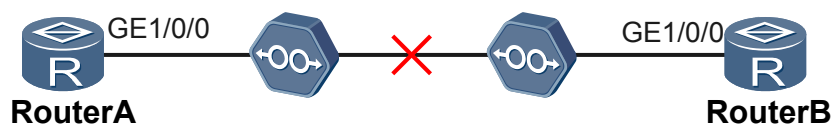
5.16.7 配置 BFD 状态与接口状态联动示例

本示例中，通过配置 BFD 状态与接口状态联动，触发路由快速收敛。

组网需求

如图 5-10 所示，链路中间存在传输设备。当传输设备之间的链路出现故障时，RouterA 和 RouterB 需要较长的时间才能检测到链路故障，导致路由失效慢，网络终端时间较长。通过配置 BFD 会话状态和接口状态联动，实现 RouterA 的 GE1/0/0 接口和 RouterB 的 GE1/0/0 接口之间的 BFD 会话状态的变化能够影响接口的协议状态，从而触发路由的快速收敛。

图 5-10 配置 BFD 状态与接口状态联动



配置思路

采用如下思路配置 BFD 状态与接口状态联动：

1. 在 RouterA 上配置 BFD Session
2. 在 RouterB 上配置 BFD Session
3. 在 RouterA 上 BFD Session UP 以后配置 BFD 状态与接口状态联动
4. 在 RouterB 上 BFD Session UP 以后配置 BFD 状态与接口状态联动

数据准备

为完成此配置例，需要准备如下数据：

- BFD 检测的对端 IP 地址
- 发送和接收 BFD 控制报文的本端接口
- BFD Session 的本地标识符和远端标识符

 说明

BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数等都使用缺省值。

操作步骤

步骤 1 配置 RouterA 和 RouterB 的直连接口 IP 地址

配置 RouterA 的接口 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] undo shutdown
[RouterA-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
```

配置 RouterB 的接口 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] undo shutdown
[RouterB-GigabitEthernet1/0/0] ip address 10.1.1.2 24
[RouterB-GigabitEthernet1/0/0] quit
```

步骤 2 配置 BFD 单跳检测

在 RouterA 上使能 BFD，配置与 RouterB 之间的 BFD Session。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atob bind peer-ip default-ip interface gigabitethernet 1/0/0
[RouterA-bfd-session-atob] discriminator local 10
[RouterA-bfd-session-atob] discriminator remote 20
[RouterA-bfd-session-atob] min-tx-interval 10
[RouterA-bfd-session-atob] min-rx-interval 10
[RouterA-bfd-session-atob] wtr 5
[RouterA-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
```

在 RouterB 上使能 BFD，并配置与 RouterA 之间的 BFD Session。

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bfd btoa bind peer-ip default-ip interface gigabitethernet 1/0/0
[RouterB-bfd-session-btoa] discriminator local 20
[RouterB-bfd-session-btoa] discriminator remote 10
[RouterB-bfd-session-btoa] min-tx-interval 10
[RouterB-bfd-session-btoa] min-rx-interval 10
[RouterB-bfd-session-btoa] wtr 5
[RouterB-bfd-session-btoa] commit
[RouterB-bfd-session-btoa] quit
```

配置完成后，在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令，可以看到建立了一个单跳（one hop）的 BFD Session，状态为 Up。以 RouterA 为例：

```
[RouterA] display bfd session all verbose
```

```
-----
Session MIndex : 16384      (One Hop) State : Up      Name : atob
-----
Local Discriminator      : 10          Remote Discriminator : 20
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type            : Interface(GigabitEthernet1/0/0)
Bind Session Type        : Static
Bind Peer Ip Address     : 224.0.0.184
NextHop Ip Address       : 224.0.0.184
Bind Interface           : GigabitEthernet1/0/0
FSM Board Id             : 3          TOS-EXP              : 7
Min Tx Interval (ms)     : 10          Min Rx Interval (ms) : 10
Actual Tx Interval (ms)  : 10          Actual Rx Interval (ms): 10
Local Detect Multi        : 3          Detect Interval (ms)  : 30
Echo Passive             : Disable     Acl Number            : --
Destination Port         : 3784        TTL                   : 255
Proc interface status    : Disable     Process PST            : Disable
WTR Interval (ms)        : 300000
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     : --
PDT Index                 : FSM-5000000|RCV-0|IF-0|TOKEN-0
Session Description       : --
-----

Total UP/DOWN Session Number : 1/0
```

步骤 3 配置 BFD 状态与接口状态联动

在 RouterA 上配置 BFD 状态与接口状态联动。

```
[RouterA] bfd atob
[RouterA-bfd-session-atob] process-interface-status
[RouterA-bfd-session-atob] process-pst
[RouterA-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
```

在 RouterB 上配置 BFD 状态与接口状态联动。

```
[RouterB] bfd btoa
[RouterB-bfd-session-btoa] process-interface-status
[RouterA-bfd-session-atob] process-pst
[RouterB-bfd-session-btoa] commit
[RouterB-bfd-session-btoa] quit
```

步骤 4 验证配置结果

配置完成后，在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令，看到“Proc interface status”字段显示为“Enable”。

以 RouterA 上的显示为例。

```
[RouterA] display bfd session all verbose
-----
Session MIndex : 16384      (One Hop) State : Up      Name : atob
-----
Local Discriminator      : 10          Remote Discriminator : 20
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type            : Interface(GigabitEthernet1/0/0)
Bind Session Type        : Static
Bind Peer Ip Address     : 224.0.0.184
NextHop Ip Address       : 224.0.0.184
Bind Interface           : GigabitEthernet1/0/0
FSM Board Id             : 3          TOS-EXP              : 7
Min Tx Interval (ms)     : 10          Min Rx Interval (ms) : 10
Actual Tx Interval (ms)  : 10          Actual Rx Interval (ms): 10
Local Detect Multi        : 3          Detect Interval (ms)  : 30
Echo Passive             : Disable     Acl Number            : --
```

```
Destination Port      : 3784          TTL          : 255
Proc interface status : Enable        Process PST   : Disable
WTR Interval (ms)    : 300000
Active Multi         : 3
Last Local Diagnostic : No Diagnostic
Bind Application      : IFNET
Session TX TmrID     : --             Session Detect TmrID : --
Session Init TmrID   : --             Session WTR TmrID   : --
PDT Index            : FSM-5000000|RCV-0|IF-0|TOKEN-0
Session Description   : --
```

Total UP/DOWN Session Number : 1/0

对 RouterB 的 GE1/0/0 接口执行 **shutdown** 操作，BFD 会话的状态变为 Down:

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] shutdown
[RouterB-GigabitEthernet1/0/0] quit
```

在 RouterA 上执行 **display bfd session all verbose** 命令和 **display interface gigabitethernet 1/0/0** 命令，可以看到 BFD Session 状态为 Down，GE1/0/0 接口的状态为 UP（BFD status down）。

```
[RouterA] display bfd session all verbose
```

```
-----
Session MIndex : 16384      (One Hop) State : Down      Name : atob
-----
Local Discriminator      : 10          Remote Discriminator : 20
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type            : Interface(GigabitEthernet1/0/0)
Bind Session Type        : Static
Bind Peer Ip Address     : 224.0.0.184
NextHop Ip Address       : 224.0.0.184
Bind Interface           : GigabitEthernet1/0/0
FSM Board Id             : 3           TOS-EXP              : 7
Min Tx Interval (ms)     : 10          Min Rx Interval (ms) : 10
Actual Tx Interval (ms)  : 10          Actual Rx Interval (ms): 10
Local Detect Multi       : 3           Detect Interval (ms) : 30
Echo Passive             : Disable      Acl Number            : --
Destination Port         : 3784         TTL                   : 255
Proc interface status    : Enable        Process PST           : Disable
WTR Interval (ms)       : 300000
Active Multi             : 3
Last Local Diagnostic    : Neighbor Signaled Session Down
Bind Application         : IFNET
Session TX TmrID        : --             Session Detect TmrID : --
Session Init TmrID      : --             Session WTR TmrID   : --
PDT Index                : FSM-5000000|RCV-0|IF-0|TOKEN-0
Session Description      : --
```

Total UP/DOWN Session Number : 1/0

```
[RouterA] display interface gigabitethernet 1/0/0
GigabitEthernet1/0/0 current state : UP
Line protocol current state : UP(BFD status down)
Last line protocol up time: 2008-10-16 09:25:17
Description : GigabitEthernet1/0/0 Interface, Route Port
The Maximum Transmit Unit is 1500 bytes
Internet Address is 10.1.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fcc7-565a
The Vendor PN is HFBR-5710L
Port BW: 1G, Transceiver max BW: 1G, Transceiver Mode: MultiMode
WaveLength: 850nm, Transmission Distance: 550m
Loopback:none, full-duplex mode, negotiation: disable, Pause Flowcontrol:Send and Receive Enable
Last physical up time   : 2008-10-16 09:18:48
Last physical down time : 2008-10-16 09:18:42
Current system time: 2010-08-30 18:02:12
Statistics last cleared:never
Last 300 seconds input rate: 56 bits/sec, 0 packets/sec
```

```
Last 300 seconds output rate: 88 bits/sec, 0 packets/sec
Input: 420904 bytes, 5802 packets
Output: 1250456 bytes, 13926 packets
Input:
  Unicast: 461 packets, Multicast: 5331 packets
  Broadcast: 10 packets, Jumbo: 0 packets
  CRC: 3 packets, Symbol: 0 packets
  Overrun: 0 packets, InRangeLength: 0 packets
  LongPacket: 0 packets, Jabber: 0 packets, Alignment: 0 packets
  Fragment: 0 packets, Undersized Frame: 0 packets
  RxPause: 0 packets
Output:
  Unicast: 8622 packets, Multicast: 5293 packets
  Broadcast: 11 packets, Jumbo: 0 packets
  Lost: 0 packets, Overflow: 0 packets, Underrun: 0 packets
  TxPause: 0 packets
Unknown Vlan: 0 packets
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 bfd
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
bfd atob bind peer-ip default-ip interface GigabitEthernet1/0/0
 discriminator local 10
 discriminator remote 20
 wtr 5
 process-pst
 process-interface-status
 commit
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 bfd
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
bfd btoa bind peer-ip default-ip interface GigabitEthernet1/0/0
 discriminator local 20
 discriminator remote 10
 wtr 5
 process-pst
 process-interface-status
 commit
#
return
```

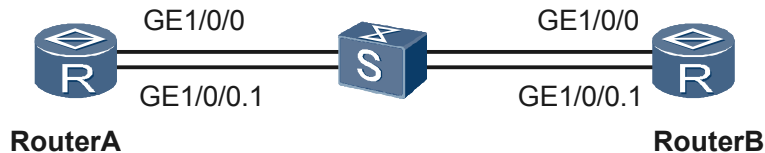
5.16.8 配置 BFD 状态与子接口状态联动示例

本示例中，通过 BFD 状态与子接口状态联动功能，提高子接口业务上的可靠性。

组网需求

如图 5-11 所示，在大规模城域以太网等组网环境中，子接口上需要配置大量 VLAN 业务，对可靠性要求也很高，这时可以建立 BFD 会话检测主接口链路的连通性，并配置 BFD 状态与子接口状态联动功能，以提高子接口上业务的可靠性，同时节约会话资源。

图 5-11 配置 BFD 状态与子接口状态联动



配置思路

采用如下思路配置 BFD 状态与子接口状态联动：

1. 在 RouterA 上配置 BFD Session。
2. 在 RouterB 上配置 BFD Session。
3. 在 RouterA 上 BFD Session UP 以后配置 BFD 状态与子接口状态联动。
4. 在 RouterB 上 BFD Session UP 以后配置 BFD 状态与子接口状态联动。

数据准备

为完成此配置例，需要准备如下数据：

- BFD 检测的对端主接口 IP 地址
- 发送和接收 BFD 控制报文的本端接口
- BFD Session 的本地标识符和远端标识符

说明

BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数等都使用缺省值。

操作步骤

步骤 1 配置 RouterA 和 RouterB 的主接口 IP 地址，并创建子接口。

配置 RouterA 的接口 IP 地址，并创建子接口。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] undo shutdown
[RouterA-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 1/0/0.1
[RouterA-GigabitEthernet1/0/0.1] undo shutdown
[RouterA-GigabitEthernet1/0/0.1] ip address 11.1.1.1 24
[RouterA-GigabitEthernet1/0/0.1] vlan-type dot1q 10
[RouterA-GigabitEthernet1/0/0.1] quit
```

配置 RouterB 的接口 IP 地址，并创建子接口。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] undo shutdown
[RouterB-GigabitEthernet1/0/0] ip address 10.1.1.2 24
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 1/0/0.1
[RouterB-GigabitEthernet1/0/0.1] undo shutdown
[RouterB-GigabitEthernet1/0/0.1] ip address 11.1.1.2 24
[RouterB-GigabitEthernet1/0/0.1] vlan-type dot1q 10
[RouterB-GigabitEthernet1/0/0.1] quit
```

步骤2 配置 BFD 单跳检测

在 RouterA 上使能 BFD，配置与 RouterB 之间的 BFD Session，绑定主接口。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atob bind peer-ip default-ip interface gigabitethernet 1/0/0
[RouterA-bfd-session-atob] discriminator local 10
[RouterA-bfd-session-atob] discriminator remote 20
[RouterA-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
```

在 RouterB 上使能 BFD，并配置与 RouterA 之间的 BFD Session，绑定主接口。

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bfd btoa bind peer-ip default-ip interface gigabitethernet 1/0/0
[RouterB-bfd-session-btoa] discriminator local 20
[RouterB-bfd-session-btoa] discriminator remote 10
[RouterB-bfd-session-btoa] commit
[RouterB-bfd-session-btoa] quit
```

配置完成后，在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令，可以看到建立了一个单跳（one hop）的 BFD Session，状态为 Up。以 RouterA 为例：

```
[RouterA] display bfd session all verbose
```

Session MIndex : 16384	(One Hop) State :Up	Name : atob
Local Discriminator : 10	Remote Discriminator : 20	
Session Detect Mode : Asynchronous Mode Without Echo Function		
BFD Bind Type : Interface(GigabitEthernet1/0/0)		
Bind Session Type : Static		
Bind Peer Ip Address : 224.0.0.184		
NextHop Ip Address : 224.0.0.184		
Bind Interface : GigabitEthernet1/0/0		
FSM Board Id : 3	TOS-EXP : 7	
Min Tx Interval (ms) : 10	Min Rx Interval (ms) : 10	
Actual Tx Interval (ms) : 10	Actual Rx Interval (ms) : 10	
Local Detect Multi : 3	Detect Interval (ms) : 30	
Echo Passive : Disable	Acl Number : --	
Destination Port : 3784	TTL : 255	
Proc interface status : Disable	Process PST : Disable	
WTR Interval (ms) : --		
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 : --		
PDT Index : FSM-5000000 RCV-0 IF-0 TOKEN-0		
Session Description : --		

Total UP/DOWN Session Number : 1/0

步骤3 配置 BFD 状态与子接口状态联动

在 RouterA 上配置 BFD 状态与子接口状态联动。

```
[RouterA] bfd atob
[RouterA-bfd-session-atob] process-interface-status sub-if
[RouterA-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
```

在 RouterB 上配置 BFD 状态与子接口状态联动。

```
[RouterB] bfd btoa
[RouterB-bfd-session-btoa] process-interface-status sub-if
[RouterB-bfd-session-btoa] commit
[RouterB-bfd-session-btoa] quit
```

步骤 4 验证配置结果

配置完成后，在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令，看到“Proc interface status”字段显示为“Enable (Sub-If)”。

以 RouterA 上的显示为例。

```
[RouterA] display bfd session all verbose
```

```
-----
Session MIndex : 16384      (One Hop) State : Up      Name : atob
-----
Local Discriminator      : 10      Remote Discriminator      : 20
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type            : Interface(GigabitEthernet1/0/0)
Bind Session Type        : Static
Bind Peer Ip Address     : 224.0.0.184
NextHop Ip Address       : 224.0.0.184
Bind Interface            : GigabitEthernet1/0/0
FSM Board Id             : 3      TOS-EXP                      : 7
Min Tx Interval (ms)     : 10      Min Rx Interval (ms)     : 10
Actual Tx Interval (ms)  : 10      Actual Rx Interval (ms)  : 10
Local Detect Multi       : 3      Detect Interval (ms)     : 30
Echo Passive             : Disable  Acl Number                : --
Destination Port         : 3784     TTL                        : 255
Proc interface status    : Enable (Sub-If)  Process PST                : Disable
WTR Interval (ms)       : --
Active Multi             : 3
Last Local Diagnostic    : No Diagnostic
Bind Application         : IFNET
Session TX TmrID         : --      Session Detect TmrID      : --
Session Init TmrID       : --      Session WTR TmrID        : --
Session Echo Tx TmrID    : --
PDT Index                : FSM-5000000|RCV-0|IF-0|TOKEN-0
Session Description      : --
-----
```

```
Total UP/DOWN Session Number : 1/0
```

对 RouterB 的 GE1/0/0 接口执行 **shutdown** 操作，BFD 会话状态变为 Down:

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] shutdown
[RouterB-GigabitEthernet1/0/0] quit
```

在 RouterA 上执行 **display bfd session all verbose** 命令和 **display interface gigabitethernet 1/0/0.1** 命令，可以看到 BFD Session 状态为 Down，GE1/0/0.1 接口的状态为 UP（Main BFD status down）。

```
[RouterA] display bfd session all verbose
```

```
-----
Session MIndex : 16384      (One Hop) State : Down      Name : atob
-----
Local Discriminator      : 10      Remote Discriminator      : 20
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type            : Interface(GigabitEthernet1/0/0)
Bind Session Type        : Static
Bind Peer Ip Address     : 224.0.0.184
Bind Interface            : GigabitEthernet1/0/0
-----
```



```
FSM Board Id      : 3          TOS-EXP          : 7
Min Tx Interval (ms) : 10       Min Rx Interval (ms) : 10
Actual Tx Interval (ms): 10     Actual Rx Interval (ms): 10
Local Detect Multi  : 3         Detect Interval (ms) : 30
Echo Passive       : Disable    Acl Number       : --
Destination Port    : 3784      TTL               : 255
Proc interface status : Disable  Process PST       : Disable
WTR Interval (ms)   : --
Active Multi        : 3
Last Local Diagnostic : Neighbor Signaled Session Down
Bind Application     : IFNET
Session TX TmrID     : --       Session Detect TmrID : --
Session Init TmrID   : --       Session WTR TmrID    : --
Session Echo Tx TmrID : --
PDT Index            : FSM-5000000|RCV-0|IF-0|TOKEN-0
Session Description   : --
-----
Total UP/DOWN Session Number : 1/0
[RouterA] display interface gigabitethernet 1/0/0.1
GigabitEthernet1/0/0.1 current state : UP
Line protocol current state : UP(Main BFD status down)
Last line protocol up time: 2007-11-13, 11:12:49
Route Port, The Maximum Transmit Unit is 1500
Internet Address is 11.1.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fcc7-565a
Encapsulation dot1q Virtual LAN, Vlan number 1
Current system time: 2010-08-30 18:02:12
Statistics last cleared:never
  Last 300 seconds input rate 0 bytes/sec, 0 packets/sec
  Last 300 seconds output rate 0 bytes/sec, 0 packets/sec
  Input: 0 packets, 0 bytes,
         0 unicast, 0 broadcast, 0 multicast
         0 errors, 0 drops
  Output: 0 packets, 0 bytes,
         0 unicast, 0 broadcast, 0 multicast
         0 errors, 0 drops
```

----结束

配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
bfd
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 10
ip address 11.1.1.1 255.255.255.0
#
bfd atob bind peer-ip 10.1.1.2 interface GigabitEthernet1/0/0
discriminator local 10
discriminator remote 20
wtr 5
process-interface-status sub-if
commit
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
```

```
#
bfd
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 11.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 10
ip address 10.1.1.2 255.255.255.0
#
bfd toa bind peer-ip 10.1.1.1 interface GigabitEthernet1/0/0
discriminator local 20
discriminator remote 10
wtr 5
process-interface-status sub-if
commit
#
return
```

5.16.9 配置 BFD 多跳检测示例

本示例中，通过在多跳路径的两端建立 BFD 会话，实现 BFD 会话快速检测网络中多跳路径的链路。

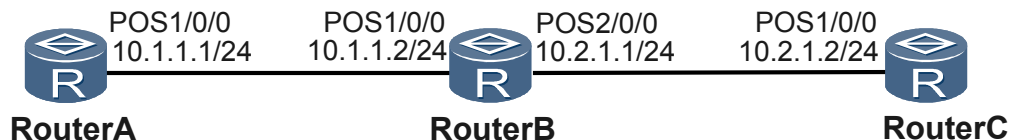
组网需求

 说明

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

如图 5-12 所示，使用 BFD 异步模式检测 RouterA、RouterC 之间的多跳路径。

图 5-12 配置 BFD 多跳检测组网图



配置思路

采用如下思路配置 BFD：

1. 在 RouterA 上配置 BFD Session，检测 RouterA 到 RouterC 的多跳路径。
2. 在 RouterC 上配置 BFD Session，检测 RouterC 到 RouterA 的多跳路径。

数据准备

为完成此配置例，需要准备如下数据：

- BFD 检测的对端 IP 地址
- BFD Session 的本地标识符和远端标识符

 说明

BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数等都使用缺省值。

操作步骤

步骤 1 配置 RouterA、RouterB、RouterC 相互路由可达

本案例采用静态路由，具体配置过程略。

步骤 2 配置 RouterA 和 RouterC 之间的多跳路由检测

在 RouterA 上配置与 RouterC 之间的 BFD Session。不需要绑定接口。

```
<RouterA> system-view
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atoc bind peer-ip 10.2.1.2
[RouterA-bfd-session-atoc] discriminator local 10
[RouterA-bfd-session-atoc] discriminator remote 20
[RouterA-bfd-session-atoc] wtr 10
[RouterA-bfd-session-atoc] commit
[RouterA-bfd-session-atoc] quit
```

在 RouterC 上配置与 RouterA 之间的 BFD Session。不需要绑定接口。

```
<RouterC> system-view
[RouterC] bfd
[RouterC-bfd] quit
[RouterC] bfd ctoa bind peer-ip 10.1.1.1
[RouterC-bfd-session-ctoa] discriminator local 20
[RouterC-bfd-session-ctoa] discriminator remote 10
[RouterC-bfd-session-ctoa] wtr 10
[RouterC-bfd-session-ctoa] commit
[RouterC-bfd-session-ctoa] quit
```

步骤 3 验证配置结果

配置完成后，在 RouterA 和 RouterC 上执行 **display bfd session all verbose** 命令，可以看到建立了一个多跳（Multi Hop）的 BFD Session，且状态为 Up。

以 RouterA 上的显示为例。

```
<RouterA> display bfd session all verbose
```

Session MIndex : 256	(Multi Hop) State :Up	Name : atoc
Local Discriminator : 10	Remote Discriminator : 20	
Session Detect Mode : Asynchronous Mode Without Echo Function		
BFD Bind Type : Peer Ip Address		
Bind Session Type : Static		
Bind Peer Ip Address : 10.2.1.2		
Bind Interface : --		
FSM Board Id : 1	TOS-EXP : 7	
Min Tx Interval (ms) : 10	Min Rx Interval (ms) : 10	
Actual Tx Interval (ms) : 10	Actual Rx Interval (ms) : 10	
Local Detect Multi : 3	Detect Interval (ms) : 30	
Echo Passive : Disable	Acl Number : --	
Destination Port : 3784	TTL : 254	
Proc interface status : Disable	Process PST : Disable	
WTR Interval (ms) : -- 600000		
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 : --	
PDT Index : FSM-0 RCV-0 IF-0 TOKEN-0		
Session Description : --		

Total UP/DOWN Session Number : 1/0

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 bfd
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
 bfd atoc bind peer-ip 10.2.1.2
 discriminator local 10
 discriminator remote 20
 wtr 10
 commit
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.2.1.1 255.255.255.0
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
 bfd
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.2.1.2 255.255.255.0
#
 bfd ctoa bind peer-ip 10.1.1.1
 discriminator local 20
 discriminator remote 10
 wtr 10
 commit
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

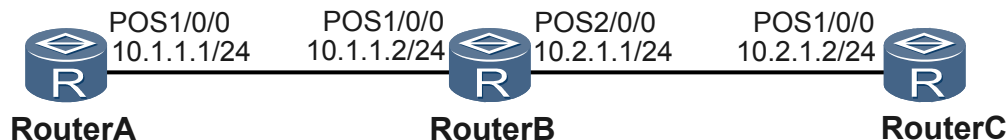
5.16.10 配置 BFD 查询模式示例

本示例中，使 BFD 工作的查询模式下，防止周期性发送 BFD 报文的开销影响到系统的正常运行。

组网需求

如图 5-13 所示，使用 BFD 查询模式检测 RouterA、RouterC 之间的多跳路径。

图 5-13 配置 BFD 多跳检测组网图



配置思路

采用如下思路配置 BFD：

1. 在 RouterA 上配置 BFD Session，检测 RouterA 到 RouterC 的多跳路径。
2. 在 RouterC 上配置 BFD Session，检测 RouterC 到 RouterA 的多跳路径。

说明

查询模式与异步模式的配置基本相同，唯一的区别在于，如果采用查询模式，需要在 BFD 会话视图下配置 **demand** 命令。

数据准备

为完成此配置例，需要准备如下数据：

- BFD 检测的对端 IP 地址
- BFD Session 的本地标识符和远端标识符
- 查询序列发送间隔

BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数等都使用缺省值。

操作步骤

步骤 1 配置 RouterA、RouterB、RouterC 相互路由可达

本案例采用静态路由，具体配置过程略。

步骤 2 配置 RouterA 和 RouterC 之间的多跳路由检测

在 RouterA 上配置与 RouterC 之间的 BFD Session。不需要绑定接口。

```
<RouterA> system-view
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atoc bind peer-ip 10.2.1.2
[RouterA-bfd-session-atoc] discriminator local 10
[RouterA-bfd-session-atoc] discriminator remote 20
```

配置采用查询模式，每隔 1 分钟发送一次查询序列。

```
[RouterA-bfd-session-atoc] demand
[RouterA-bfd-session-atoc] demand timer 60000
[RouterA-bfd-session-atoc] commit
[RouterA-bfd-session-atoc] quit
```

在 RouterC 上配置与 RouterA 之间的 BFD Session。不需要绑定接口。

```
<RouterC> system-view
[RouterC] bfd
[RouterC-bfd] quit
[RouterC] bfd ctoa bind peer-ip 10.1.1.1
[RouterC-bfd-session-ctoa] discriminator local 20
[RouterC-bfd-session-ctoa] discriminator remote 10
```

配置采用查询模式。

```
[RouterC-bfd-session-ctoa] demand
[RouterC-bfd-session-ctoa] commit
[RouterC-bfd-session-ctoa] quit
```

步骤 3 验证配置结果

配置完成后，在 RouterA 和 RouterC 上执行 **display bfd session all verbose** 命令，可以看到建立了一个多跳（Multi Hop）的 BFD Session，检测模式为“Demand Mode Without Echo Function”，会话处于 UP 状态。

以 RouterA 上的显示为例。

```
<RouterA> display bfd session all verbose
```

Session MIndex : 256	(Multi Hop) State : Up	Name : atoc

Local Discriminator	: 10	Remote Discriminator	: 20
Session Detect Mode	: Demand Mode Without Echo Function		
BFD Bind Type	: Peer Ip Address		
Bind Session Type	: Static		
Bind Peer Ip Address	: 10.2.1.2		
NextHop Ip Address	: 10.2.1.2		
Bind Interface	: --		
FSM Board Id	: 1	TOS-EXP	: 7
Min Tx Interval (ms)	: 10	Min Rx Interval (ms)	: 10
Actual Tx Interval (ms)	: 10	Actual Rx Interval (ms)	: 10
Local Detect Multi	: 3	Detect Interval (ms)	: 30
Echo Passive	: Disable	Acl Number	: --
Destination Port	: 3784	TTL	: 254
Proc interface status	: Disable	Process PST	: Disable
WTR Interval (ms)	: --		
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	: --
PDT Index	: FSM-0 RCV-0 IF-0 TOKEN-0		
Session Description	: --		

Total UP/DOWN Session Number : 1/0

----结束

配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
bfd
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.1 255.255.255.0
#
```

```
bfd atoc bind peer-ip 10.2.1.2
discriminator local 10
discriminator remote 20
demand
demand timer 60000
commit
#
ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.2 255.255.255.0
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 10.2.1.1 255.255.255.0
#
return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
bfd
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.2.1.2 255.255.255.0
#
bfd ctoa bind peer-ip 10.1.1.1
discriminator local 20
discriminator remote 10
demand
commit
#
ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

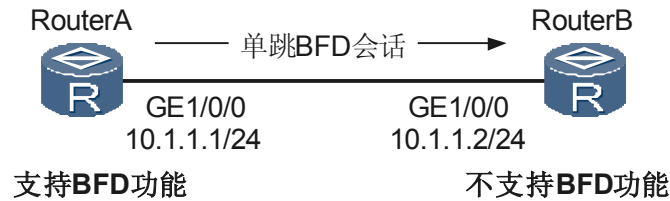
5.16.11 配置单臂 ECHO 功能示例

本示例中，通过在支持 BFD 功能的一端设备上配置单臂 ECHO 功能，实现快速检测和监控网络中的直连链路。

组网需求

如图 5-14 所示，RouterA 支持 BFD 功能，RouterB 不支持 BFD 功能。为了快速检测和监控 RouterA 和 RouterB 之间的直连链路，可以在 RouterA 上配置单臂 ECHO 功能的 BFD 会话。RouterB 接收到 RouterA 发送的 BFD 报文后，直接将该报文环回，进而快速检测链路。

图 5-14 配置单臂 ECHO 功能组网图



配置思路

采用如下思路配置三层物理链路单跳检测：

1. 在 RouterA 上配置 BFD 会话，检测 RouterA 到 RouterB 的直连链路。

数据准备

为完成此配置例，需要准备如下数据：

- 单臂 ECHO 功能的 BFD 会话检测的对端 IP 地址
- 单臂 ECHO 功能的 BFD 会话的标识符
- 单臂 ECHO 功能的 BFD 报文的最小接收间隔

操作步骤

步骤 1 配置 RouterA 和 RouterB 的直连接口 IP 地址

配置 RouterA 的接口 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] undo shutdown
[RouterA-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
```

配置 RouterB 的接口 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] undo shutdown
[RouterB-GigabitEthernet1/0/0] ip address 10.1.1.2 24
[RouterB-GigabitEthernet1/0/0] quit
```

步骤 2 配置单臂 ECHO 功能的 BFD 会话

配置 RouterA。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atob bind peer-ip 10.1.1.2 interface gigabitEthernet1/0/0 one-arm-echo
[RouterA-bfd-session-atob] discriminator local 1
[RouterA-bfd-session-atob] min-echo-rx-interval 100
[RouterA-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
```


步骤 3 验证配置结果

配置完成后，在 RouterA 上执行 **display bfd session all verbose** 命令，可以看到建立了一个单跳（one hop）的 BFD 会话，且状态为 Up。

```
<RouterA> display bfd session all verbose
-----
Session MIndex : 256      (One Hop) State : Up      Name : atob
-----
Local Discriminator      : 1      Remote Discriminator      : -
Session Detect Mode      : Asynchronous One-arm-echo Mode
BFD Bind Type            : Interface(gigabitEthernet1/0/0)
Bind Session Type        : Static
Bind Peer IP Address     : 10.1.1.2
NextHop Ip Address       : 10.1.1.2
Bind Interface           : EigabitEthernet1/0/0
FSM Board Id            : 0      TOS-EXP                  : 7
Echo Rx Interval (ms)    : 100
Actual Tx Interval (ms)  : 1000      Actual Rx Interval (ms): 1000
Local Detect Multi        : 3      Detect Interval (ms)    : 3000
Echo Passive             : Disable   Acl Number              : -
Destination Port         : 3784      TTL                     : 255
Proc Interface Status    : Disable   Process PST              : Disable
WTR Interval (ms)        : -      Local Demand Mode       : Disable
Active Multi             : 3
Last Local Diagnostic    : Control Detection Time Expired
Bind Application         : No Application Bind
Session TX TmrID         : 87      Session Detect TmrID    : 88
Session Init TmrID       : -      Session WTR TmrID       : -
Session Echo Tx TmrID    : -
PDT Index                : FSM-0 | RCV-0 | IF-0 | TOKEN-0
Session Description      : -
-----

Total UP/DOWN Session Number : 1/0
```

----结束

配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
bfd
#
interface gigabitethernet 1/0/0
undo shutdown
ip address 10.1.1.1 255.255.255.0
#
bfd atob bind peer-ip 10.1.1.2 interface gigabitEthernet1/0/0 one-arm-echo
discriminator local 1
commit
#
return
```
- RouterB 的配置文件

```
#
sysname RouterB
#
interface gigabitethernet 1/0/0
undo shutdown
ip address 10.1.1.2 255.255.255.0
#
return
```

5.16.12 配置 BFD 检测 VPN 路由示例

本示例中，通过在 VPN 的私网接口上配置 BFD 会话，实现 BFD 会话检测 VPN 路由。

组网需求

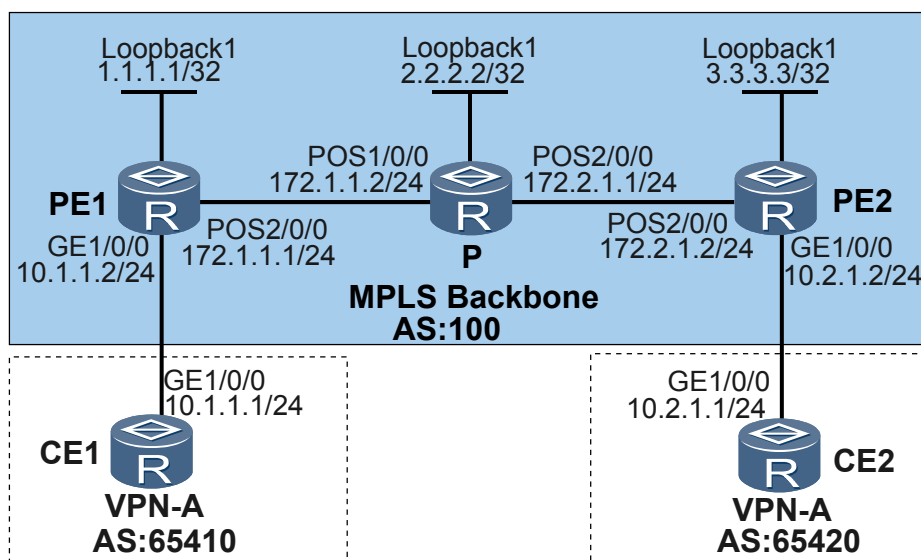
 说明

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

如图 5-15 所示：

- CE1 和 CE2 属于 VPN-A，分别通过 PE1 和 PE2 接入 MPLS 骨干网。
- PE1 和 PE2 的 GE1/0/0 接口与 VPNA 绑定。
- 使用 BFD 异步模式检测 PE1 和 PE2 之间的 VPN 路由。

图 5-15 配置 BFD 检测 VPN 路由组网图



配置思路

采用如下思路配置 BFD：

1. 在 PE1 上配置 BFD Session，检测 PE1 到 PE2 的多跳路径。
2. 在 PE2 上配置 BFD Session，检测 PE2 到 PE1 的多跳路径。

数据准备

为完成此配置例，需要准备如下的数据：

- BFD 检测的对端 IP 地址
- BFD Session 的本地标识符和远端标识符

 说明

BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数等都使用缺省值。

操作步骤

步骤 1 配置各接口的 IP 地址（略）

步骤 2 配置 MPLS 骨干网，使 PE1 和 PE2 互通（略）

步骤 3 配置 VPN 实例（略）

步骤 4 配置 PE1 和 PE2 相互 VPN 路由可达(略)

配置完成后，PE1 可以 Ping 通 PE2 的 GE1/0/0 接口 IP 地址。

```
<PE1> ping -vpn-instance vpna 10.2.1.2
PING 10.2.1.2: 56 data bytes, press CTRL_C to break
  Reply from 10.2.1.2: bytes=56 Sequence=1 ttl=254 time=60 ms
  Reply from 10.2.1.2: bytes=56 Sequence=2 ttl=254 time=50 ms
  Reply from 10.2.1.2: bytes=56 Sequence=3 ttl=254 time=50 ms
  Reply from 10.2.1.2: bytes=56 Sequence=4 ttl=254 time=60 ms
  Reply from 10.2.1.2: bytes=56 Sequence=5 ttl=254 time=50 ms
--- 10.2.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 50/54/60 ms
```

步骤 5 配置 PE1 和 PE2 之间 VPN 路由检测

在 PE1 上配置与 PE2 之间的 BFD Session，绑定 VPN 实例。

```
<PE1> system-view
[PE1] bfd
[PE1-bfd] quit
[PE1] bfd lto2_vpn bind peer-ip 10.2.1.2 vpn-instance vpna
[PE1-bfd-session-lto2_vpn] discriminator local 12
[PE1-bfd-session-lto2_vpn] discriminator remote 21
[PE1-bfd-session-lto2_vpn] wtr 5
[PE1-bfd-session-lto2_vpn] commit
```

在 PE2 上配置与 PE1 之间的 BFD Session，需要绑定 VPN 实例。

```
<PE2> system-view
[PE2] bfd
[PE2-bfd] quit
[PE2] bfd 2tol_vpn bind peer-ip 10.1.1.2 vpn-instance vpna
[PE2-bfd-session-2tol_vpn] discriminator local 21
[PE2-bfd-session-2tol_vpn] discriminator remote 12
[PE2-bfd-session-2tol_vpn] wtr 5
[PE2-bfd-session-2tol_vpn] commit
```

步骤 6 验证配置结果

配置完成后，在 PE1 和 PE2 上执行 **display bfd session peer-ip** 命令，可以看到建立了一个多跳（Multi Hop）的 BFD Session，且状态为 Up。

以 PE1 上的显示为例。

```
<PE1> display bfd session peer-ip 10.2.1.2 vpn-instance vpna verbose
```

Session MIndex : 256	(Multi Hop) State : Up	Name : lto2_vpn
Local Discriminator	: 12	Remote Discriminator : 21
Session Detect Mode	: Asynchronous Mode Without Echo Function	
BFD Bind Type	: Peer Ip Address	
Bind Session Type	: Static	
Bind Peer Ip Address	: 10.2.1.2	
NextHop Ip Address	: 10.2.1.2	
Bind Interface	: --	
Vpn Instance Name	: vpna	

```
FSM Board Id      : 6          TOS-EXP      : 7
Min Tx Interval (ms) : 10       Min Rx Interval (ms) : 10
Actual Tx Interval (ms): 10     Actual Rx Interval (ms): 10
Local Detect Multi  : 3         Detect Interval (ms) : 30
Echo Passive       : Disable    Acl Number    : --
Destination Port    : 3784      TTL            : 254
Proc interface status : Disable  Process PST    : Disable
WTR Interval (ms)   : -- 300000
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   : --
PDT Index            : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description   : --
```

Total UP/DOWN Session Number : 1/0

----结束

配置文件

- PE1 的配置文件

```
#
 sysname PE1
#
ip vpn-instance vpna
 ipv4-family
  route-distinguisher 100:1
  vpn-target 111:1 export-extcommunity
  vpn-target 111:1 import-extcommunity
#
 mpls lsr-id 1.1.1.1
 mpls
#
 mpls ldp
#
 bfd
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip binding vpn-instance vpna
 ip address 10.1.1.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 172.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
bfd lto2_vpn bind peer-ip 10.2.1.2 vpn-instance vpna
 discriminator local 12
 discriminator remote 21
 wtr 5
 commit
#
bgp 100
 peer 3.3.3.3 as-number 100
 peer 3.3.3.3 connect-interface LoopBack1
#
 ipv4-family unicast
  undo synchronization
  peer 3.3.3.3 enable
#
```

```

ipv4-family vpnv4
 policy vpn-target
 peer 3.3.3.3 enable
#
ipv4-family vpn-instance vpna
 peer 10.1.1.1 as-number 65410
 import-route direct
#
ospf 100
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 172.1.1.0 0.0.0.255
#
return

```

● PE2 的配置文件

```

#
sysname PE2
#
ip vpn-instance vpna
 ipv4-family
  route-distinguisher 200:1
  vpn-target 111:1 export-extcommunity
  vpn-target 111:1 import-extcommunity
#
mpls lsr-id 3.3.3.3
mpls
#
mpls ldp
#
bfd
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 172.2.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip binding vpn-instance vpna
 ip address 10.2.1.2 255.255.255.0
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
bfd 2to1_vpn bind peer-ip 10.1.1.2 vpn-instance vpna
 discriminator local 21
 discriminator remote 12
 wtr 5
 commit
#
bgp 100
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 connect-interface LoopBack1
#
ipv4-family unicast
 undo synchronization
 peer 1.1.1.1 enable
#
ipv4-family vpnv4
 policy vpn-target
 peer 1.1.1.1 enable
#
ipv4-family vpn-instance vpn1
 peer 10.2.1.1 as-number 65420
 import-route direct
#
ospf 100

```

```

        area 0.0.0.0
        network 3.3.3.3 0.0.0.0
        network 172.2.1.0 0.0.0.255
    #
    return

```

● P 的配置文件

```

#
sysname P
#
mpls lsr-id 2.2.2.2
mpls
#
mpls ldp
#
interface Pos1/0/0
    link-protocol ppp
    undo shutdown
    ip address 172.1.1.2 255.255.255.0
    mpls
    mpls ldp
#
interface Pos2/0/0
    link-protocol ppp
    undo shutdown
    ip address 172.2.1.1 255.255.255.0
    mpls
    mpls ldp
#
interface LoopBack1
    ip address 2.2.2.2 255.255.255.255
#
ospf 100
    area 0.0.0.0
    network 172.1.1.0 0.0.0.255
    network 172.2.1.0 0.0.0.255
    network 2.2.2.2 0.0.0.0
#
return

```

● CE1 的配置文件

```

#
sysname CE1
#
interface GigabitEthernet1/0/0
    undo shutdown
    ip address 10.1.1.1 255.255.255.0
#
bgp 65410
    peer 10.1.1.2 as-number 100
#
    ipv4-family unicast
        import-route direct
        peer 10.1.1.2 enable
#
return

```

● CE2 的配置文件

```

#
sysname CE2
#
interface GigabitEthernet1/0/0
    undo shutdown
    ip address 10.2.1.1 255.255.255.0
#
bgp 65420
    peer 10.2.1.2 as-number 100
#
    ipv4-family unicast

```

```
import-route direct
peer 10.2.1.2 enable
#
return
```

5.16.13 配置 Dot1q 终结子接口支持 BFD 示例

从典型的应用场景描述了 Dot1q 终结子接口支持 BFD 后，如何保证发送带有一层 Tag 报文的终端用户与网络的联系可靠、稳定。

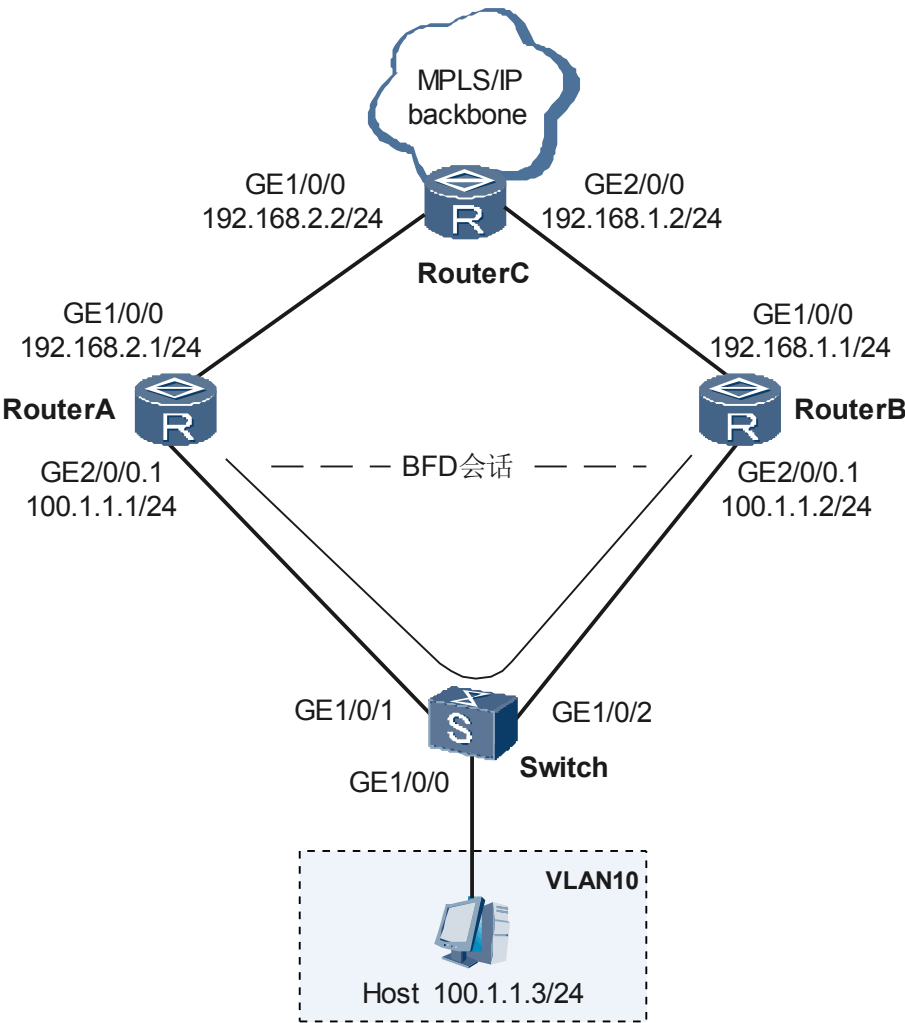
组网需求

如图 5-16 所示，VLAN10 的用户通过缺省网关访问 ISP 网络。其中，RouterA 的 GE2/0/0.1 为 Dot1q 终结子接口，RouterB 的 GE2/0/0.1 为 Dot1q 终结子接口。

需求如下：

- 在 RouterA 和 RouterB 上配置 BFD 会话，检测他们之间的链路。
- 在 RouterA 上配置 VRRP 备份组 1，使其为 Master 设备；在 RouterB 上配置 VRRP 备份组 1，使其为 Backup 设备。
- 分别在 RouterA 和 RouterB 上配置 VRRP 备份组 1 监视 BFD 会话。

图 5-16 配置 Dot1q 终结子接口支持 BFD 组网图



配置思路

采用如下的思路配置 Dot1q 终结子接口支持 BFD 的基本功能：

1. 配置 RouterA 和 RouterB 的接口模式为用户终结模式。
2. 配置 IGP，使得 RouterA、RouterB 和 RouterC 设备之间可以互通。
3. 配置 Switch 二层转发功能。
4. 配置 RouterA 和 RouterB 的 Dot1q 终结子接口。
5. 在 RouterA 和 RouterB 上创建 BFD 会话，检测 RouterA 和 RouterB 之间的链路。
6. 分别在 RouterA 和 RouterB 的 GE2/0/0.1 接口上创建 VRRP 备份组 1，确保 RouterA 为 Master 设备，RouterB 为 Backup 设备。

数据准备

为完成此配置例，需准备如下的数据：

- Dot1q 终结子接口终结的 Tag 值
- BFD 会话的名称
- VRRP 备份组号、虚拟 IP 地址

操作步骤

步骤 1 配置接口的模式为用户终结模式

配置 RouterA。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] undo shutdown
[RouterA-GigabitEthernet2/0/0] mode user-termination
[RouterA-GigabitEthernet2/0/0] quit
```

配置 RouterB。

```
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] undo shutdown
[RouterB-GigabitEthernet2/0/0] mode user-termination
[RouterB-GigabitEthernet2/0/0] quit
```

步骤 2 配置设备之间的网络互连

如图 5-16 所示，配置各设备接口的 IP 地址。配置 RouterA、RouterB 和 RouterC 之间的 IGP，本例采用 OSPF。

配置 RouterA。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] undo shutdown
[RouterA-GigabitEthernet1/0/0] ip address 192.168.2.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0.1
[RouterA-GigabitEthernet2/0/0.1] undo shutdown
[RouterA-GigabitEthernet2/0/0.1] ip address 100.1.1.1 24
[RouterA-GigabitEthernet2/0/0.1] quit
[RouterA] ospf 1
[RouterA-ospf-1] area 0
```



```
[RouterA-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

配置 RouterB。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] undo shutdown
[RouterB-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 2/0/0.1
[RouterB-GigabitEthernet2/0/0.1] undo shutdown
[RouterB-GigabitEthernet2/0/0.1] ip address 100.1.1.2 24
[RouterB-GigabitEthernet2/0/0.1] quit
[RouterB] ospf 1
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

配置 RouterC。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterC
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] undo shutdown
[RouterC-GigabitEthernet1/0/0] ip address 192.168.2.2 24
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface gigabitethernet 2/0/0
[RouterC-GigabitEthernet2/0/0] undo shutdown
[RouterC-GigabitEthernet2/0/0] ip address 192.168.1.2 24
[RouterC-GigabitEthernet2/0/0] quit
[RouterC] ospf 1
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

配置完成后，RouterA 和 RouterB 相互之间有 OSPF 协议发现到对端 IP 的路由，并能互相 Ping 通。

以 RouterA 的显示为例。

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 17          Routes : 17

Destination/Mask    Proto Pre  Cost      Flags NextHop         Interface
192.168.2.0/24      Direct 0     0          D    192.168.2.1      GigabitEthernet1/0/0
192.168.2.1/32      Direct 0     0          D    127.0.0.1         InLoopBack0
192.168.1.0/24      OSPF   10     2          D    192.168.2.2      GigabitEthernet1/0/0
100.1.1.0/24        Direct 0     0          D    100.1.1.1         GigabitEthernet2/0/0.1
100.1.1.1/32        Direct 0     0          D    127.0.0.1         InLoopBack0
127.0.0.0/8         Direct 0     0          D    127.0.0.1         InLoopBack0
127.0.0.1/32        Direct 0     0          D    127.0.0.1         InLoopBack0
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 17          Routes : 17

Destination/Mask    Proto Pre  Cost      Flags NextHop         Interface
192.168.2.0/24      Direct 0     0          D    192.168.2.1      GigabitEthernet1/0/0
```

```
192.168.2.1/32 Direct 0 0 D 127.0.0.1 GigabitEthernet1/0/0
192.168.1.0/24 OSPF 10 2 D 192.168.2.2 GigabitEthernet1/0/0
100.1.1.0/24 Direct 0 0 D 100.1.1.1 GigabitEthernet2/0/0.1
100.1.1.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
127.0.0.0/8 Direct 0 0 D 127.0.0.1 InLoopBack0
127.0.0.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
[RouterA] ping 192.168.1.1
PING 192.168.1.1: 56 data bytes, press CTRL_C to break
  Reply from 192.168.1.1: bytes=56 Sequence=1 ttl=254 time=7 ms
  Reply from 192.168.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
  Reply from 192.168.1.1: bytes=56 Sequence=3 ttl=254 time=5 ms
  Reply from 192.168.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
  Reply from 192.168.1.1: bytes=56 Sequence=5 ttl=254 time=8 ms

--- 192.168.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/4/8 ms
```

步骤 3 配置 Switch 二层转发功能

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan 10
[Switch-vlan10] port gigabitethernet 1/0/0
[Switch-vlan10] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] undo shutdown
[Switch-GigabitEthernet1/0/1] port trunk allow-pass vlan 10
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] undo shutdown
[Switch-GigabitEthernet1/0/2] port trunk allow-pass vlan 10
[Switch-GigabitEthernet1/0/2] quit
```

步骤 4 配置 Dot1q 终结子接口

配置 RouterA。

```
[RouterA] interface gigabitethernet 2/0/0.1
[RouterA-GigabitEthernet2/0/0.1] control-vid 1 dot1q-termination
[RouterA-GigabitEthernet2/0/0.1] dot1q termination vid 10
```

配置 RouterB。

```
[RouterB] interface gigabitethernet 2/0/0.1
[RouterB-GigabitEthernet2/0/0.1] control-vid 1 dot1q-termination
[RouterB-GigabitEthernet2/0/0.1] dot1q termination vid 10
```

步骤 5 配置 BFD 会话

配置 RouterA。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atob bind peer-ip default-ip interface gigabitethernet 2/0/0.1
[RouterA-bfd-session-atob] discriminator local 1
[RouterA-bfd-session-atob] discriminator remote 2
[RouterA-bfd-session-atob] dot1q vid 10
[RouterA-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
```

配置 RouterB。

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bfd atob bind peer-ip default-ip interface gigabitethernet 2/0/0.1
[RouterB-bfd-session-atob] discriminator local 2
[RouterB-bfd-session-atob] discriminator remote 1
```

```
[RouterB-bfd-session-atob] dot1q vid 10
[RouterB-bfd-session-atob] commit
[RouterB-bfd-session-atob] quit
```

完成配置后, 执行 **display bfd session all verbose** 命令, 可以查看到 BFD 会话的状态为 Up。以 RouterA 的显示为例。

```
[RouterA] display bfd session all verbose
```

Session MIndex : 16384	(One Hop) State : Up	Name : atob
Local Discriminator	: 1	Remote Discriminator : 2
Session Detect Mode	: Asynchronous Mode Without Echo Function	
BFD Bind Type	: Interface(GigabitEthernet2/0/0.1)	
Bind Session Type	: Static	
Bind Peer IP Address	: 224.0.0.184	
NextHop Ip Address	: 224.0.0.184	
Bind Interface	: GigabitEthernet2/0/0.1	
FSM Board Id	: 6	TOS-EXP : 7
Min Tx Interval (ms)	: 10	Min Rx Interval (ms) : 10
Actual Tx Interval (ms)	: 10	Actual Rx Interval (ms): 10
Local Detect Multi	: 3	Detect Interval (ms) : 30
Echo Passive	: Disable	Acl Number : -
Destination Port	: 3784	TTL : 255
Proc Interface Status	: Disable	Process PST : Disable
WTR Interval (ms)	: -	
Active Multi	: 3	
Last Local Diagnostic	: Control Detection Time Expired	
Bind Application	: No Application Bind	
Session TX TmrID	: -	Session Detect TmrID : -
Session Init TmrID	: -	Session WTR TmrID : -
Session Echo Tx TmrID	: -	
PDT Index	: FSM-B030000 RCV-0 IF-B030000 TOKEN-0	
Session Description	: -	

Total UP/DOWN Session Number : 1/0

步骤 6 配置 VRRP 备份组 1 监视 BFD 会话

配置 RouterA。

```
[RouterA] interface gigabitethernet 2/0/0.1
[RouterA-GigabitEthernet2/0/0.1] dot1q vrrp vid 10
[RouterA-GigabitEthernet2/0/0.1] vrrp vrid 1 virtual 100.1.1.100
[RouterA-GigabitEthernet2/0/0.1] vrrp vrid 1 priority 160
[RouterA-GigabitEthernet2/0/0.1] vrrp vrid 1 track bfd-session 1
[RouterA-GigabitEthernet2/0/0.1] arp broadcast enable
[RouterA-GigabitEthernet2/0/0.1] quit
```

配置 RouterB。

```
[RouterB] interface gigabitethernet 2/0/0.1
[RouterB-GigabitEthernet2/0/0.1] dot1q vrrp vid 10
[RouterB-GigabitEthernet2/0/0.1] vrrp vrid 1 virtual 100.1.1.100
[RouterB-GigabitEthernet2/0/0.1] vrrp vrid 1 track bfd-session 2
[RouterB-GigabitEthernet2/0/0.1] arp broadcast enable
[RouterB-GigabitEthernet2/0/0.1] quit
```

步骤 7 验证配置结果

执行 **display vrrp** 命令, 可以查看到 VRRP 备份组监视的 BFD 会话的状态为 Up。以 RouterA 的显示为例。

```
[RouterA] display vrrp
GigabitEthernet1/0/0 | Virtual Router 1
      State           : Master
      Virtual IP       : 100.1.1.100
      PriorityRun       : 160
      PriorityConfig    : 160
```

```
MasterPriority      : 160
Preempt            : YES      Delay Time : 0
TimerRun           : 1
TimerConfig        : 1
Virtual Mac        : 0000-5e00-0101
Check TTL          : YES
Config type        : normal-vrrp
Config track link-bfd down-number : 0
Track BFD          : 1
BFD-session state  : UP
Priority reduced    : 10
```

----结束

配置文件

● RouterA 的配置文件

```
#
sysname RouterA
#
bfd
#
interface GigabitEthernet 1/0/0
undo shutdown
ip address 192.168.2.1 24
#
interface GigabitEthernet2/0/0
undo shutdown
mode user-termination
#
interface GigabitEthernet2/0/0.1
undo shutdown
control-vid 1 dot1q-termination
dot1q termination vid 10
dot1q vrrp vid 10
ip address 100.1.1.1 24
vrrp vrid 1 virtual 100.1.1.100
vrrp vrid 1 priority 160
vrrp vrid 1 track bfd-session 1
arp broadcast enable
#
bfd atob bind peer-ip default-ip interface gigabitethernet 2/0/0.1
discriminator local 1
discriminator remote 2
dot1q vid 10
commit
#
ospf 1
area 0.0.0.0
network 192.168.2.0 0.0.0.255
network 100.1.1.0 0.0.0.255
#
return
```

● RouterB 的配置文件

```
#
sysname RouterB
#
bfd
#
interface GigabitEthernet 1/0/0
undo shutdown
ip address 192.168.1.1 24
#
interface GigabitEthernet2/0/0
undo shutdown
mode user-termination
#
interface GigabitEthernet2/0/0.1
```

```
undo shutdown
control-vid 1 dot1q-termination
dot1q termination vid 10
dot1q vrrp vid 10
ip address 100.1.1.2 24
vrrp vrid 1 virtual 100.1.1.100
vrrp vrid 1 track bfd-session 2
arp broadcast enable
#
bfd atob bind peer-ip default-ip interface gigabitethernet 2/0/0.1
discriminator local 2
discriminator remote 1
dot1q vid 10
commit
#
ospf 1
area 0.0.0.0
network 192.168.1.0 0.0.0.255
network 100.1.1.0 0.0.0.255
#
return
```

- RouterC 的配置文件

```
#
sysname RouterC
#
bfd
#
interface GigabitEthernet 1/0/0
undo shutdown
ip address 192.168.2.2 24
#
interface GigabitEthernet 2/0/0
undo shutdown
ip address 192.168.1.2 24
#
ospf 1
area 0.0.0.0
network 192.168.1.0 0.0.0.255
network 192.168.2.0 0.0.0.255
#
return
```

- Switch 的配置文件

```
#
sysname Switch
#
vlan batch 10
#
interface GigabitEthernet1/0/0
undo shutdown
port default vlan 10
#
interface GigabitEthernet1/0/1
undo shutdown
port trunk allow-pass vlan 10
#
interface GigabitEthernet1/0/2
undo shutdown
port trunk allow-pass vlan 10
#
return
```

5.16.14 配置 QinQ 终结子接口支持 BFD 示例

从典型的应用场景描述了 QinQ 终结子接口支持 BFD 后，如何保证发送带有两层 Tag 报文的终端用户与网络的联系可靠、稳定。

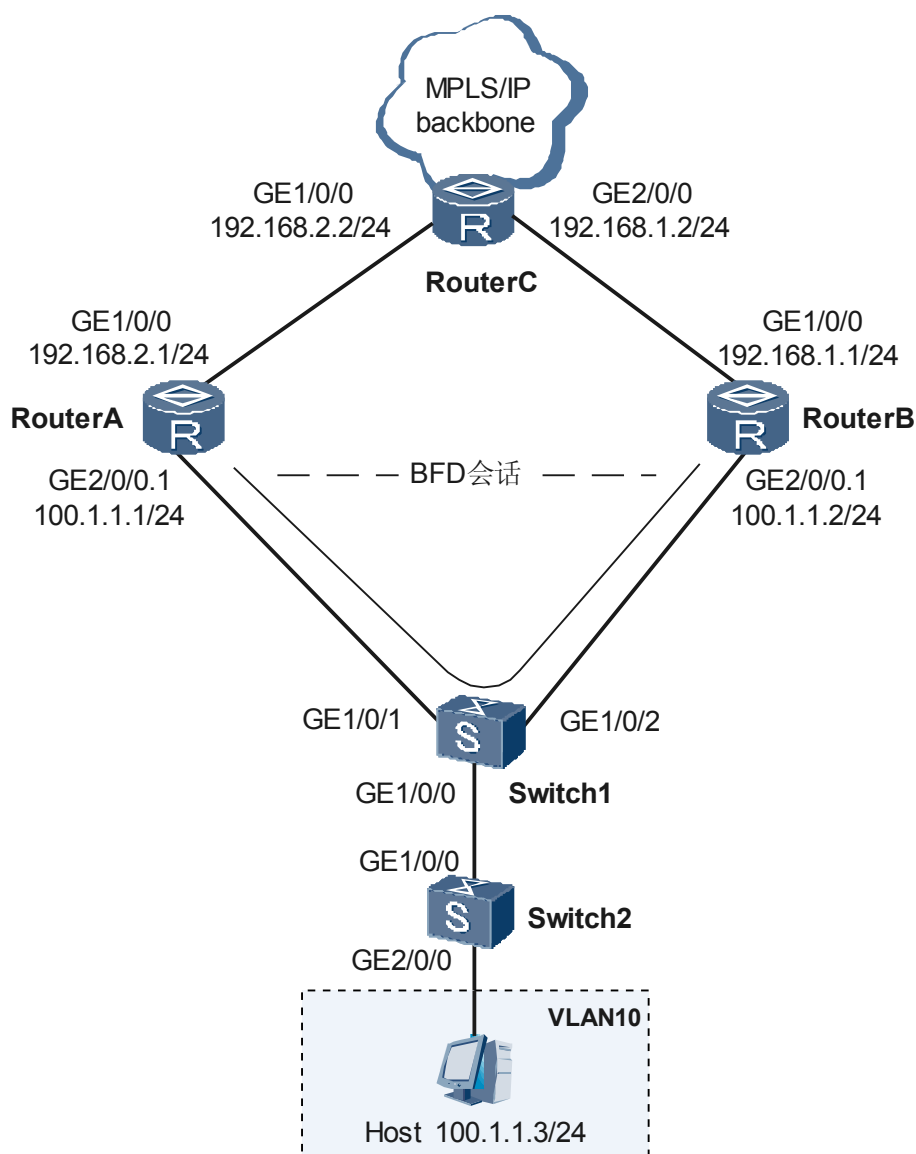
组网需求

如图 5-17 所示，VLAN10 的用户通过缺省网关访问 ISP 网络。其中，RouterA 的 GE2/0/0.1 为 QinQ 终结子接口，RouterB 的 GE2/0/0.1 为 QinQ 终结子接口。

需求如下：

- 在 RouterA 和 RouterB 上配置 BFD 会话，检测他们之间的链路。
- 在 RouterA 上配置 VRRP 备份组 1，使其为 Master 设备；在 RouterB 上配置 VRRP 备份组 1，使其为 Backup 设备。
- 分别在 RouterA 和 RouterB 上配置 VRRP 备份组 1 监视 BFD 会话。

图 5-17 配置 QinQ 终结子接口支持 BFD 组网图



配置思路

采用如下的思路配置 QinQ 终结子接口支持 BFD 的基本功能：

1. 配置 RouterA 和 RouterB 的接口模式为用户终结模式。
2. 配置 IGP，使得 RouterA、RouterB 和 RouterC 设备之间可以互通。
3. 配置 Switch2 的二层转发功能。
4. 配置 Switch1 的 QinQ 功能。
5. 配置 RouterA 和 RouterB 的 QinQ 终结子接口。
6. 在 RouterA 和 RouterB 上创建 BFD 会话，检测 RouterA 和 RouterB 之间的链路。
7. 分别在 RouterA 和 RouterB 的 GE2/0/0.1 接口上创建 VRRP 备份组 1，确保 RouterA 为 Master 设备，RouterB 为 Backup 设备。

数据准备

为完成此配置例，需准备如下的数据：

- BFD 会话的名称
- VRRP 备份组号、虚拟 IP 地址
- QinQ 终结子接口终结的 Tag 值

操作步骤

步骤 1 配置接口的模式为用户终结模式

配置 RouterA。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] undo shutdown
[RouterA-GigabitEthernet2/0/0] mode user-termination
[RouterA-GigabitEthernet2/0/0] quit
```

配置 RouterB。

```
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] undo shutdown
[RouterB-GigabitEthernet2/0/0] mode user-termination
[RouterB-GigabitEthernet2/0/0] quit
```

步骤 2 配置设备之间的网络互连

如图 5-17 所示，配置各设备接口的 IP 地址。配置 RouterA、RouterB 和 RouterC 之间的 IGP，本例采用 OSPF。

配置 RouterA。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] undo shutdown
[RouterA-GigabitEthernet1/0/0] ip address 192.168.2.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0.1
[RouterA-GigabitEthernet2/0/0.1] undo shutdown
[RouterA-GigabitEthernet2/0/0.1] ip address 100.1.1.1 24
[RouterA-GigabitEthernet2/0/0.1] quit
[RouterA] ospf 1
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

配置 RouterB。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] undo shutdown
[RouterB-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 2/0/0.1
[RouterB-GigabitEthernet2/0/0.1] undo shutdown
[RouterB-GigabitEthernet2/0/0.1] ip address 100.1.1.2 24
[RouterB-GigabitEthernet2/0/0.1] quit
[RouterB] ospf 1
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

配置 RouterC。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterC
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] undo shutdown
[RouterC-GigabitEthernet1/0/0] ip address 192.168.2.2 24
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface gigabitethernet 2/0/0
[RouterC-GigabitEthernet2/0/0] undo shutdown
[RouterC-GigabitEthernet2/0/0] ip address 192.168.1.2 24
[RouterC-GigabitEthernet2/0/0] quit
[RouterC] ospf 1
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

配置完成后，RouterA 和 RouterB 相互之间有 OSPF 协议发现到对端 IP 的路由，并能互相 Ping 通。

以 RouterA 的显示为例。

```
[RouterA] display ip routing-table
```

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

Routing Tables: Public

Destinations : 17 Routes : 17

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
192.168.2.0/24	Direct	0	0	D	192.168.2.1	GigabitEthernet1/0/0
192.168.2.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
192.168.1.0/24	OSPF	10	2	D	192.168.2.2	GigabitEthernet1/0/0
100.1.1.0/24	Direct	0	0	D	100.1.1.1	GigabitEthernet2/0/0.1
100.1.1.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0

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

Routing Tables: Public

Destinations : 17 Routes : 17

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
192.168.2.0/24	Direct	0	0	D	192.168.2.1	GigabitEthernet1/0/0
192.168.2.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet1/0/0
192.168.1.0/24	OSPF	10	2	D	192.168.2.2	GigabitEthernet1/0/0
100.1.1.0/24	Direct	0	0	D	100.1.1.1	GigabitEthernet2/0/0.1
100.1.1.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0

```
[RouterA] ping 192.168.1.1
```



```
PING 192.168.1.1: 56 data bytes, press CTRL_C to break
  Reply from 192.168.1.1: bytes=56 Sequence=1 ttl=254 time=7 ms
  Reply from 192.168.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
  Reply from 192.168.1.1: bytes=56 Sequence=3 ttl=254 time=5 ms
  Reply from 192.168.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
  Reply from 192.168.1.1: bytes=56 Sequence=5 ttl=254 time=8 ms

--- 192.168.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/4/8 ms
```

步骤 3 配置 Switch2 的二层转发功能

```
<HUAWEI> system-view
[HUAWEI] sysname Switch2
[Switch2] vlan 10
[Switch2-vlan10] port gigabitethernet 2/0/0
[Switch2-vlan10] quit
[Switch2] interface gigabitethernet 1/0/0
[Switch2-GigabitEthernet1/0/0] undo shutdown
[Switch2-GigabitEthernet1/0/0] port trunk allow-pass vlan 10
[Switch2-GigabitEthernet1/0/0] quit
```

步骤 4 配置 QinQ 功能，使 Switch2 上送到 RouterA 和 RouterB 的报文带有两层 Tag。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch1
[Switch1] vlan 100
[Switch1-vlan100] quit
[Switch1] interface gigabitethernet 1/0/0
[Switch1-GigabitEthernet1/0/0] port vlan-stacking vlan 10 stack-vlan 100
[Switch1-GigabitEthernet1/0/0] undo shutdown
[Switch1-GigabitEthernet1/0/0] quit
[Switch1] interface gigabitethernet 1/0/1
[Switch1-GigabitEthernet1/0/1] port trunk allow-pass vlan 100
[Switch1-GigabitEthernet1/0/1] undo shutdown
[Switch1-GigabitEthernet1/0/1] quit
[Switch1] interface gigabitethernet 1/0/2
[Switch1-GigabitEthernet1/0/2] port trunk allow-pass vlan 100
[Switch1-GigabitEthernet1/0/2] undo shutdown
[Switch1-GigabitEthernet1/0/2] quit
```

步骤 5 配置 QinQ 终结子接口

配置 RouterA。

```
[RouterA] interface gigabitethernet 2/0/0.1
[RouterA-GigabitEthernet2/0/0.1] control-vid 1 qinq-termination
[RouterA-GigabitEthernet2/0/0.1] qinq termination pe-vid 100 ce-vid 10
```

配置 RouterB。

```
[RouterB] interface gigabitethernet 2/0/0.1
[RouterB-GigabitEthernet2/0/0.1] control-vid 1 qinq-termination
[RouterB-GigabitEthernet2/0/0.1] qinq termination pe-vid 100 ce-vid 10
```

步骤 6 配置 BFD 会话

配置 RouterA。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atob bind peer-ip default-ip interface gigabitethernet 2/0/0.1
[RouterA-bfd-session-atob] discriminator local 1
[RouterA-bfd-session-atob] discriminator remote 2
[RouterA-bfd-session-atob] qinq pe-vid 100 ce-vid 10
[RouterA-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
```

配置 RouterB。

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bfd atob bind peer-ip default-ip interface gigabitethernet 2/0/0.1
[RouterB-bfd-session-atob] discriminator local 2
[RouterB-bfd-session-atob] discriminator remote 1
[RouterB-bfd-session-atob] qinq pe-vid 100 ce-vid 10
[RouterB-bfd-session-atob] commit
[RouterB-bfd-session-atob] quit
```

完成配置后，执行 **display bfd session all verbose** 命令，可以查看到 BFD 会话的状态为 Up。以 RouterA 的显示为例。

```
[RouterA] display bfd session all verbose
```

```
-----
Session MIndex : 16384      (One Hop) State : Up      Name : atob
-----
Local Discriminator      : 1      Remote Discriminator      : 2
Session Detect Mode      : Asynchronous Mode Without Echo Function
BFD Bind Type           : Interface(GigabitEthernet2/0/0.1)
Bind Session Type       : Static
Bind Peer IP Address    : 224.0.0.184
NextHop Ip Address      : 224.0.0.184
Bind Interface          : GigabitEthernet2/0/0.1
FSM Board Id           : 6      TOS-EXP                   : 7
Min Tx Interval (ms)    : 10      Min Rx Interval (ms)    : 10
Actual Tx Interval (ms) : 10      Actual Rx Interval (ms) : 10
Local Detect Multi      : 3      Detect Interval (ms)    : 30
Echo Passive           : Disable  Acl Number              : -
Destination Port        : 3784    TTL                      : 255
Proc Interface Status   : Disable  Process PST              : Disable
WTR Interval (ms)      : -
Active Multi            : 3
Last Local Diagnostic    : Control Detection Time Expired
Bind Application        : No Application Bind
Session TX TmrID        : -      Session Detect TmrID    : -
Session Init TmrID      : -      Session WTR TmrID       : -
Session Echo Tx TmrID   : -
PDT Index               : FSM-B030000 | RCV-0 | IF-B030000 | TOKEN-0
Session Description     : -
-----
```

Total UP/DOWN Session Number : 1/0

步骤 7 配置 VRRP 备份组 1 监视 BFD 会话

配置 RouterA。

```
[RouterA] interface gigabitethernet 2/0/0.1
[RouterA-GigabitEthernet2/0/0.1] qinq vrrp pe-vid 100 ce-vid 10
[RouterA-GigabitEthernet2/0/0.1] vrrp vrid 1 virtual 100.1.1.100
[RouterA-GigabitEthernet2/0/0.1] vrrp vrid 1 priority 160
[RouterA-GigabitEthernet2/0/0.1] vrrp vrid 1 track bfd-session 1
[RouterA-GigabitEthernet2/0/0.1] arp broadcast enable
[RouterA-GigabitEthernet2/0/0.1] quit
```

配置 RouterB。

```
[RouterB] interface gigabitethernet 2/0/0.1
[RouterB-GigabitEthernet2/0/0.1] qinq vrrp pe-vid 100 ce-vid 10
[RouterB-GigabitEthernet2/0/0.1] vrrp vrid 1 virtual 100.1.1.100
[RouterB-GigabitEthernet2/0/0.1] vrrp vrid 1 track bfd-session 2
[RouterB-GigabitEthernet2/0/0.1] arp broadcast enable
[RouterB-GigabitEthernet2/0/0.1] quit
```

步骤 8 验证配置结果

执行 **display vrrp** 命令，可以查看到 VRRP 备份组监视的 BFD 会话的状态为 Up。以 RouterA 的显示为例。

```
[RouterA] display vrrp
GigabitEthernet1/0/0 | Virtual Router 1
      State           : Master
      Virtual IP       : 100.1.1.100
      PriorityRun      : 160
      PriorityConfig    : 160
      MasterPriority    : 160
      Preempt          : YES      Delay Time : 0
      TimerRun         : 1
      TimerConfig      : 1
      Virtual Mac      : 0000-5e00-0101
      Check TTL        : YES
      Config type      : normal-vrrp
Config track link-bfd down-number : 0
      Track BFD        : 1          Priority reduced : 10
      BFD-session state : UP
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
bfd
#
interface GigabitEthernet 1/0/0
 undo shutdown
 ip address 192.168.2.1 24
#
interface GigabitEthernet2/0/0
 undo shutdown
 mode user-termination
#
interface GigabitEthernet2/0/0.1
 undo shutdown
 control-vid 1 qinq-termination
 qinq termination pe-vid 100 ce-vid 10
 qinq vrrp pe-vid 100 ce-vid 10
 ip address 100.1.1.1 24
 vrrp vrid 1 virtual 100.1.1.100
 vrrp vrid 1 priority 160
 vrrp vrid 1 track bfd-session 1
 arp broadcast enable
#
bfd atob bind peer-ip default-ip interface gigabitethernet 2/0/0.1
 discriminator local 1
 discriminator remote 2
 qinq pe-vid 100 ce-vid 10
 commit
#
ospf 1
 area 0.0.0.0
 network 192.168.2.0 0.0.0.255
 network 100.1.1.0 0.0.0.255
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
bfd
#
interface GigabitEthernet 1/0/0
 undo shutdown
 ip address 192.168.1.1 24
```

```
#
interface GigabitEthernet2/0/0
 undo shutdown
 mode user-termination
#
interface GigabitEthernet2/0/0.1
 undo shutdown
 control-vid 1 qinq-termination
 qinq termination pe-vid 100 ce-vid 10
 qinq vrrp pe-vid 100 ce-vid 10
 ip address 100.1.1.2 24
 vrrp vrid 1 virtual 100.1.1.100
 vrrp vrid 1 track bfd-session 2
 arp broadcast enable
#
bfd atob bind peer-ip default-ip interface gigabitethernet 2/0/0.1
 discriminator local 2
 discriminator remote 1
 qinq pe-vid 100 ce-vid 10
 commit
#
ospf 1
 area 0.0.0.0
 network 192.168.1.0 0.0.0.255
 network 100.1.1.0 0.0.0.255
#
return
```

● RouterC 的配置文件

```
#
 sysname RouterC
#
bfd
#
interface GigabitEthernet 1/0/0
 undo shutdown
 ip address 192.168.2.2 24
#
interface GigabitEthernet 2/0/0
 undo shutdown
 ip address 192.168.1.2 24
#
ospf 1
 area 0.0.0.0
 network 192.168.1.0 0.0.0.255
 network 192.168.2.0 0.0.0.255
#
return
```

● Switch1 的配置文件

```
#
 sysname Switch1
#
vlan batch 100
#
interface GigabitEthernet1/0/0
 undo shutdown
 port vlan-stacking vlan 10 stack-vlan 100
#
interface GigabitEthernet1/0/1
 undo shutdown
 port trunk allow-pass vlan 100
#
interface GigabitEthernet1/0/2
 undo shutdown
 port trunk allow-pass vlan 100
#
return
```

- Switch2 的配置文件

```
#
sysname Switch2
#
vlan batch 10
#
interface GigabitEthernet2/0/0
undo shutdown
port default vlan 10
#
interface GigabitEthernet1/0/0
undo shutdown
port trunk allow-pass vlan 10
#
return
```

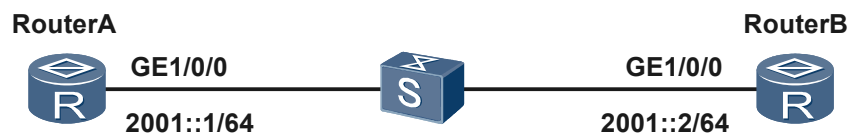
5.16.15 配置三层物理链路单跳检测示例（BFD6）

本示例中，通过配置三层物理链路单跳检测（BFD6），实现快速检测和监控网络中的直连 IPv6 链路。

组网需求

如图 5-18 所示，使用 BFD 异步模式检测 RouterA 和 RouterB 之间的直连链路。

图 5-18 配置三层物理链路单跳检测（BFD6）组网图



配置思路

采用如下思路配置三层物理链路单跳检测（BFD6）：

1. 在 RouterA 上配置 BFD6 会话，检测 RouterA 到 RouterB 的直连链路。
2. 在 RouterB 上配置 BFD6 会话，检测 RouterB 到 RouterA 的直连链路。

数据准备

为完成此配置例，需要准备如下数据：

- BFD6 会话检测的对端 IPv6 地址
- 发送和接收 BFD 控制报文的本端接口
- BFD6 会话的本地标识符和远端标识符

📖 说明

BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数等都使用缺省值。

操作步骤

步骤 1 配置 RouterA 和 RouterB 的直连接口 IPv6 地址

配置 RouterA 的接口 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] ipv6
[RouterA] interface GigabitEthernet 1/0/0
[RouterA-GigabitEthernet1/0/0] undo shutdown
[RouterA-GigabitEthernet1/0/0] ipv6 enable
[RouterA-GigabitEthernet1/0/0] ipv6 address 2001::1 64
[RouterA-GigabitEthernet1/0/0] quit
```

配置 RouterB 的接口 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] ipv6
[RouterB] interface GigabitEthernet 1/0/0
[RouterB-GigabitEthernet1/0/0] undo shutdown
[RouterB-GigabitEthernet1/0/0] ipv6 enable
[RouterB-GigabitEthernet1/0/0] ipv6 address 2001:2 64
[RouterB-GigabitEthernet1/0/0] quit
```

步骤 2 配置 BFD 单跳检测



说明

IP-Trunk、Eth-Trunk 和 VLANIF 接口也可以配置 BFD 单跳检测，配置的步骤和方法与本示例相同。

在 RouterA 上使能 BFD 功能，并配置与 RouterB 之间的 BFD 会话。需要在 BFD6 会话中绑定出接口。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atob bind peer-ipv6 2001::2 interface GigabitEthernet 1/0/0
[RouterA-bfd-session-atob] discriminator local 1
[RouterA-bfd-session-atob] discriminator remote 2
[RouterA-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
```

在 RouterB 上使能 BFD 功能，并配置与 RouterA 之间的 BFD6 会话。需要在 BFD6 会话中绑定出接口。

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bfd atob bind peer-ipv6 2001::1 interface GigabitEthernet 1/0/0
[RouterB-bfd-session-btoa] discriminator local 2
[RouterB-bfd-session-btoa] discriminator remote 1
[RouterB-bfd-session-btoa] commit
[RouterB-bfd-session-btoa] quit
```

步骤 3 验证配置结果

配置完成后，在 RouterA 和 RouterB 上执行 **display bfd session all verbose** 命令，可以看到建立了一个单跳（one hop）的 BFD6 会话，且状态为 Up。

以 RouterA 上的显示结果为例。

```
<RouterA> display bfd session all verbose
```

Session MIndex : 256	(One Hop) State : Up	Name : atob
Local Discriminator	: 1	Remote Discriminator : 2
Session Detect Mode	: Asynchronous Mode Without Echo Function	
BFD Bind Type	: Interface(GigabitEthernet1/0/0)	
Bind Session Type	: Static	
Bind Peer Ip Address	: 2001::2	
NextHop Ip Address	: 2001::2	
Bind Interface	: GigabitEthernet1/0/0	

```
FSM Board Id      : 1          TOS-EXP      : 7
Min Tx Interval (ms) : 1000    Min Rx Interval (ms) : 1000
Actual Tx Interval (ms): -      Actual Rx Interval (ms): -
Local Detect Multi  : 3        Detect Interval (ms) : -
Echo Passive       : Disable    Acl Number    : --
Destination Port    : 3784      TTL           : 255
Proc interface status : Disable Process PST      : Disable
WTR Interval (ms)   : --
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 : --
PDT Index           : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description  : --
```

Total UP/DOWN Session Number : 1/0

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 ipv6
#
 bfd
#
 interface GigabitEthernet1/0/0
 undo shutdown
 ipv6 enable
 ipv6 address 2001::1/64
#
 bfd atob bind peer-ipv6 2001::2 interface GigabitEthernet1/0/0
 discriminator local 1
 discriminator remote 2
 commit
#
 return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 ipv6
#
 bfd
#
 interface GigabitEthernet1/0/0
 undo shutdown
 ipv6 enable
 ipv6 address 2001::2/64
#
 bfd btoa bind peer-ipv6 2001::1 interface GigabitEthernet1/0/0
 discriminator local 2
 discriminator remote 1
 commit
#
 return
```

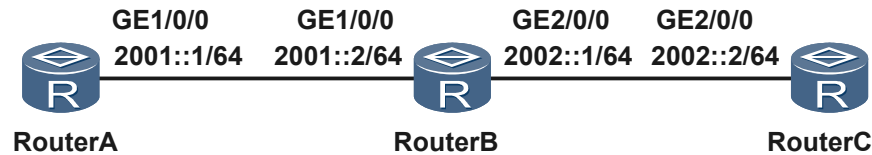
5.16.16 配置 BFD 多跳检测示例（BFD6）

本示例中，通过在多跳路径的两端建立 BFD6 会话，实现 BFD6 会话快速检测网络中多跳路径的链路。

组网需求

如图 5-19 所示，使用 BFD 异步模式检测 RouterA 和 RouterC 之间的多跳路径。

图 5-19 配置 BFD 多跳检测（BFD6）组网图



配置思路

采用如下思路配置 BFD 多跳检测（BFD6）：

1. 在 RouterA 上配置会话，检测 RouterA 到 RouterC 的多跳路径。
2. 在 RouterC 上配置 BFD 会话，检测 RouterC 到 RouterA 的多跳路径。

数据准备

为完成此配置例，需要准备如下数据：

- BFD6 会话检测的对端 IPv6 地址
- 发送和接收 BFD 控制报文的本端接口
- BFD6 会话的本地标识符和远端标识符

说明

BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数等都使用缺省值。

操作步骤

步骤 1 RouterA、RouterB 和 RouterC 之间采用 OSPFv3 协议进行互连（略）

步骤 2 配置 RouterA、RouterB、RouterC 接口的 IPv6 地址。

配置 RouterA 的接口 IPv6 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] ipv6
[RouterA] interface GigabitEthernet 1/0/0
[RouterA-GigabitEthernet1/0/0] undo shutdown
[RouterA-GigabitEthernet1/0/0] ipv6 enable
[RouterA-GigabitEthernet1/0/0] ipv6 address 2001::1 64
[RouterA-GigabitEthernet1/0/0] quit
```

配置 RouterB 的接口 IPv6 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] ipv6
[RouterB] interface GigabitEthernet 1/0/0
[RouterB-GigabitEthernet1/0/0] undo shutdown
[RouterB-GigabitEthernet1/0/0] ipv6 enable
[RouterB-GigabitEthernet1/0/0] ipv6 address 2001::2 64
[RouterBA-GigabitEthernet1/0/0] quit
```



```
[RouterB] interface GigabitEthernet 2/0/0
[RouterB-GigabitEthernet2/0/0] undo shutdown
[RouterB-GigabitEthernet2/0/0] ipv6 enable
[RouterB-GigabitEthernet2/0/0] ipv6 address 2002::1 64
[RouterB-GigabitEthernet2/0/0] quit
```

配置 RouterC 的接口 IPv6 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterC
[RouterC] ipv6
[RouterA] interface GigabitEthernet 2/0/0
[RouterA-GigabitEthernet2/0/0] undo shutdown
[RouterA-GigabitEthernet2/0/0] ipv6 enable
[RouterA-GigabitEthernet2/0/0] ipv6 address 2002::2 64
[RouterA-GigabitEthernet2/0/0] quit
```

步骤 3 配置 RouterA 和 RouterC 之间的多跳路由检测

在 RouterA 上配置与 RouterC 之间的 BFD6 会话。不需要绑定出接口。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atoc bind peer-ipv6 2002::2
[RouterA-bfd-session-atoc] discriminator local 10
[RouterA-bfd-session-atoc] discriminator remote 20
[RouterA-bfd-session-atoc] commit
[RouterA-bfd-session-atoc] quit
```

在 RouterC 上配置与 RouterA 之间的 BFD6 会话。不需要绑定出接口。

```
[RouterC] bfd
[RouterC-bfd] quit
[RouterC] bfd ctoa bind peer-ipv6 2001::1
[RouterC-bfd-session-ctoa] discriminator local 20
[RouterC-bfd-session-ctoa] discriminator remote 10
[RouterC-bfd-session-ctoa] commit
[RouterC-bfd-session-ctoa] quit
```

步骤 4 验证配置结果

配置完成后，在 RouterA 和 RouterC 上执行 **display bfd session all verbose** 命令，可以看到建立了一个多跳（Multi Hop）的 BFD6 会话，且状态为 Up。

以 RouterA 上的显示结果为例。

```
<RouterA> display bfd session all verbose
```

Session MIndex : 256	(Multi Hop) State :Up	Name : atoc
Local Discriminator : 10	Remote Discriminator : 20	
Session Detect Mode : Asynchronous Mode Without Echo Function		
BFD Bind Type : Peer Ip Address		
Bind Session Type : Static		
Bind Peer Ip Address : 2002::2		
Bind Interface : --		
FSM Board Id : 1	TOS-EXP : 7	
Min Tx Interval (ms) : 1000	Min Rx Interval (ms) : 1000	
Actual Tx Interval (ms) : --	Actual Rx Interval (ms) : --	
Local Detect Multi : 3	Detect Interval (ms) : --	
Echo Passive : Disable	Acl Number : --	
Destination Port : 4784	TTL : 254	
Proc interface status : Disable	Process PST : Disable	
WTR Interval (ms) : --		
Last Local Diagnostic : No Diagnostic		
Bind Application : No Application Bind		
Session TX TmrID : --	Session Detect TmrID : --	
Session Init TmrID : --	Session WTR TmrID : --	
PDT Index : FSM-0 RCV-0 IF-0 TOKEN-0		

Session Description : --

Total UP/DOWN Session Number : 1/0

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 ipv6
#
 bfd
#
 ospfv3 1
  router-id 1.1.1.1
#
 interface GigabitEthernet1/0/0
  undo shutdown
  ipv6 enable
  ipv6 address 2001::1/64
  ospfv3 1 area 0.0.0.0
#
 bfd atoc bind peer-ipv6 2002::2
  discriminator local 10
  discriminator remote 20
 commit
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 ipv6
#
 bfd
#
 ospfv3 1
  router-id 1.1.1.1
#
 interface GigabitEthernet1/0/0
  undo shutdown
  ipv6 enable
  ipv6 address 2001::2/64
  ospfv3 1 area 0.0.0.0
#
 interface GigabitEthernet2/0/0
  undo shutdown
  ipv6 enable
  ipv6 address 2002::1
  ospfv3 1 area 0.0.0.0
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
 ipv6
#
 bfd
#
 ospfv3 1
  router-id 1.1.1.1
#
```

```
interface GigabitEthernet2/0/0
undo shutdown
ipv6 enable
ipv6 address 2002::2
ospfv3 1 area 0.0.0.0
#
bfd ctoa bind peer-ipv6 2001::1
discriminator local 20
discriminator remote 10
commit
#
return
```

6 GR 配置

关于本章

通过 GR 的各种配置，提高系统的高可用性。

6.1 GR 简介

GR 是 IETF 针对 IP/MPLS 转发相关的协议进行扩展，实现协议重启时转发不中断的功能，使系统进行主备倒换时控制层协议的震荡在一定程度上得到限制。

6.2 配置系统级 GR

系统级 GR 是将冗余备份、GR 和 HSB 技术结合在一起的、提高设备高可用性的一项技术。

6.3 维护 HA

通过维护 HA，实现监控 HA 的运行状况。

6.4 配置举例

介绍了一种 GR 的配置示例。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

6.1 GR 简介

GR 是 IETF 针对 IP/MPLS 转发相关的协议进行扩展，实现协议重启时转发不中断的功能，使系统进行主备倒换时控制层协议的震荡在一定程度上得到限制。

6.1.1 HA 概述

实现 HA 高可用性的主要技术有：冗余备份技术、HSB 技术和 GR 技术。

在实际网络中，总是避免不了各种非技术因素造成网络故障和服务中断。因此，提高系统的容错能力、提高故障恢复速度、降低故障对业务的影响，是提高系统可用性的可行方法。

高可用性 HA（High Availability）是指一个设备具有很高的可靠性。

通常使用平均修复时间 MTTR（Mean Time to Repair）和平均故障间隔时间 MTBF（Mean Time Between Failure）这两个指标来评价设备的可靠性。

- **MTTR：**指一个组件或设备从故障到恢复正常所需的平均时间。

广义的 MTTR 涉及备件管理、客户服务等，是设备维护的一项重要指标。

以下为 MTTR 的计算公式：

$$\text{MTTR} = \text{故障检测时间} + \text{单板更换时间} + \text{系统初始化时间} + \text{链路恢复时间} + \text{路由覆盖时间} + \text{转发恢复时间}$$

上述各项的值越小，MTTR 也就越小，设备的可靠性也就越高。

在电信行业，99.999%的可用度意味着设备因故障导致的业务中断时间平均每年不得超过 5 分钟。

- **MTBF：**指一个组件或设备的无故障运行平均时间，通常以小时为单位。

系统发生故障时进行主备倒换是提供系统可用性的一种重要方式。

主备倒换会导致数据丢失。大部分丢失的数据可通过 HSB（Hot Standby）提供的数据平滑过程恢复，对于无法恢复的数据，必须通过 GR（Graceful Restart）功能修复。

冗余备份技术

对系统中关键组件进行冗余备份是提供系统容错能力的主要方法。

冗余备份方式有 1+1 备份和 n+1 备份。

- **1+1 备份方式：**两个组件必须互为镜像（mirror）。当主用组件发生故障时，备用组件可以立即接管当前任务，从而保证系统业务不中断。
- **n+1 备份方式：**系统通过 n 个相似的组件来提供某项服务，由另外一个组件作为这 n 个组件的备份。当 n 个中的某一个组件发生故障时，备份组件接管故障组件的任务，业务仍然可以继续运行。

目前路由器提供的硬件备份功能如下：

- 交换网板之间形成 3+1 备份
- 各主控板（简称为主板）之间形成 1+1 备份
- 各业务处理板之间形成 1+1 备份或 n+1 备份

- 各电源之间形成 1+1 备份
- 各制冷风扇之间形成 n+1 备份

主控板的 1+1 备份，即双主控板，是系统进行主备倒换的前提条件。

HSB 技术

HSB（Hot Standby）是提供热备份的一个关键技术。

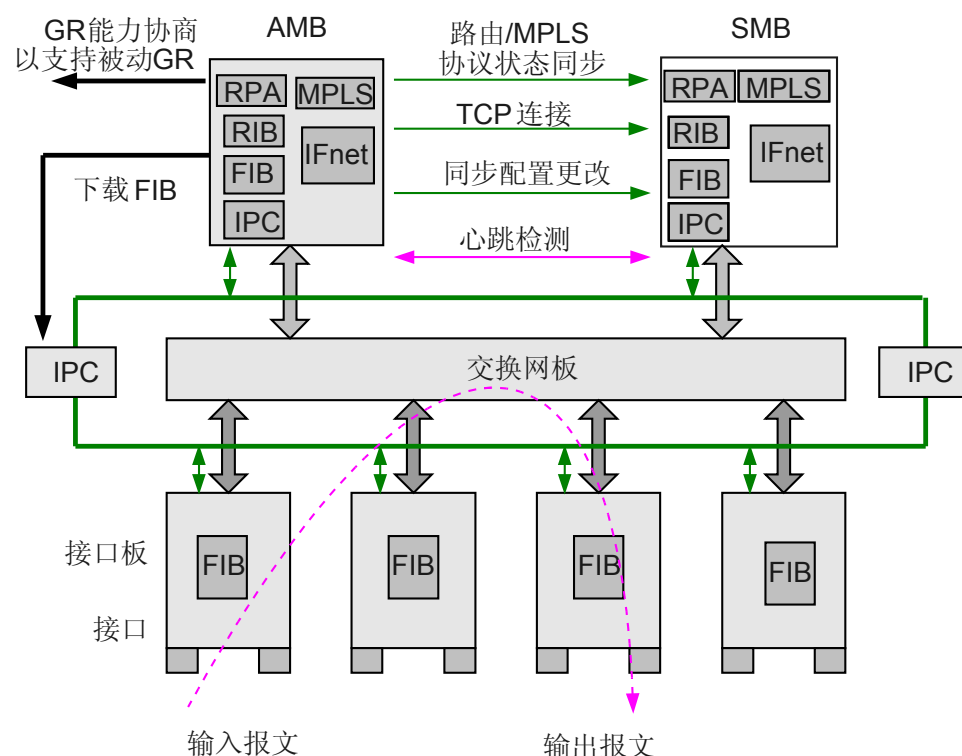
HSB 相关部件和术语如下：

- AMB（Active Main Board）：主用主板，路由器两块主板中处于主用状态的板。
- SMB（Standby Main Board）：备用主板，路由器两块主板中处于备用状态的板。
- HA Channel：主用主板与备用主板之间进行通信的通道。
- Switchover：主备板切换，即由管理员或严重故障触发引起的主板切换动作。在此过程中，原主用主板会被复位而变成备用主板。
- Smooth：数据平滑过程，即当备用主板切换成主用主板后，新主用主板上不同模块之间的数据可能不一致，此时需要进行数据同步操作使其一致。

HSB 的功能是将系统的静态和动态配置信息从 AMB 备份到 SMB。

AMB 和 SMB 之间的基本机制如图 6-1 所示。

图 6-1 HSB 的基本机制



当系统重启时，主用主板 AMB 将其静态配置信息备份到备用主板 SMB 上，并在备用主板上重新执行。

在系统正常运行时，AMB 上的任何数据变化（包括静态和动态的数据变化）都会备份到 SMB。需要注意，AMB 可将路由信息从数据层面下载到接口板，SMB 却不能、也无法从接口板接收任何信息。

备用主板 SMB 切换成主用主板 AMB 后进入平滑运行阶段。切换后，主用主板 AMB 上的所有数据都已备份，因此，该系统与其它路由器间的会话不受影响，其它路由器也不会察觉该路由器的切换。因此，热备份 HSB 切换是一个自包含过程。

实现 HSB 的硬件/软件需求如下：

- 支持双主控，互为备份
- AMB 和 SMB 之间存在一条物理通信通道
- 硬件或软件支持 AMB 心跳检测

HSB 支持的应用有：

- 支持 AMB 到 SMB 的静态配置数据备份
- 支持 AMB 到 SMB 的协议状态数据动态备份和更新
- 支持协议 GR 能力
- 支持模块间的数据平滑

GR 技术

IETF 针对 IP/MPLS 转发相关的协议（如 OSPF、IS-IS、BGP、LDP 和 RSVP）进行扩展，实现协议重启时转发不中断的功能，使系统进行主备切换时控制层协议的震荡在一定程度上得到限制。这一系列标准统称为各个协议的 Graceful Restart 扩展，简称 GR。GR 目前已经被广泛的使用在主备倒换和系统升级方面。

系统能够进行 GR 的前提条件是转发和控制分离，即路由器有主控板和接口板，接口板处理转发任务。当系统进行协议重启或者主备倒换时，不复位接口板，接口板继续转发数据，从而实现整个系统不间断地转发报文。

由此可以看出，系统实现不间断转发的必要条件是在 GR Time 时间内网络拓扑和接口状态不发生变化，否则系统将退出 GR 过程，转发也将中断。

GR 相关概念有：

- 角色
 - GR Restarter: GR 重启路由器，指路由协议使能了 GR 能力，并且具有双主控板，能够在主备倒换的时候通知邻居，请求邻居保持与自己的邻接关系。
 - GR Helper: GR Restarter 的邻居，至少能够识别 GR 信令，在 GR Restarter 进行主备倒换时保持和 GR Restarter 的邻接关系不变，协助 GR Restarter 进行网络拓扑关系的恢复。

说明

GR Restarter 与 GR Helper 的作用是相互的。在 GR Helper 使能 GR 能力的情况下，GR Restarter 与 GR Helper 的位置和作用可以互换。

- 会话和定时器
 - GR Session: 有 GR 能力的会话，是 GR Restarter 和 GR Helper 之间通过 GR 能力协商建立的会话关系。
 - GR Time: 是 GR Helper 发现 GR Restarter Down 后，保持路由信息不删除的时间，可以看作从 GR 过程开始到结束这一段时间。



说明

各协议 GR 实现机制不一致，GR Time 具体的名称和取值方法请参见《HUAWEI NetEngine80E/40E 路由器 配置指南 IP 路由》和《HUAWEI NetEngine80E/40E 路由器 配置指南 MPLS》。

管理员或故障都可触发 GR Restarter 进行协议重启或主备倒换。

下面介绍系统进行主备倒换时 GR 的工作过程。

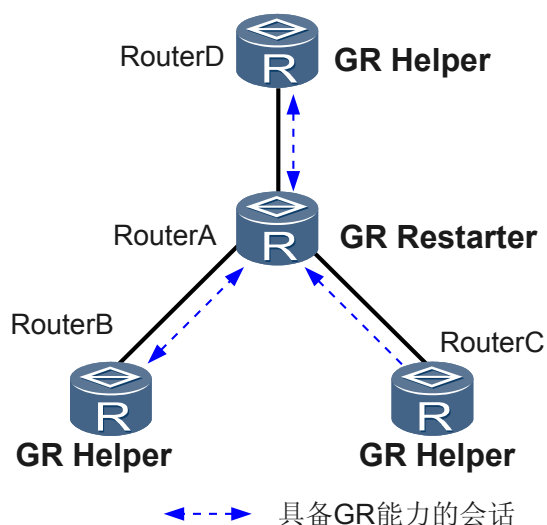


说明

一旦网络拓扑和接口状态发生变化，系统将退出 GR 过程。下面的描述假设 GR 过程中网络拓扑和接口状态均不发生变化。

1. Restarter 和 GR Helper 之间进行 GR 能力协商，建立会话。

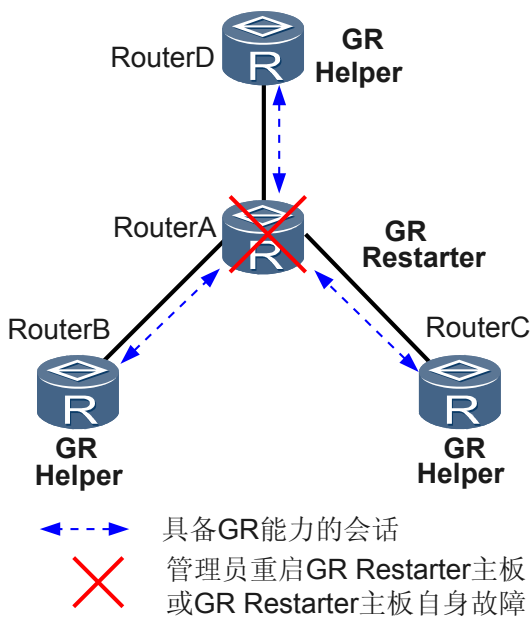
图 6-2 在 GR Restarter 与 GR Helper 间建立会话



RouterA 作为 GR Restarter，RouterB、RouterC 和 RouterD 分别是 RouterA 的 GR Helper 邻居，在 GR Restarter 和 GR Helper 之间建立起有 GR 能力的会话。

2. Restarter 进行主备倒换

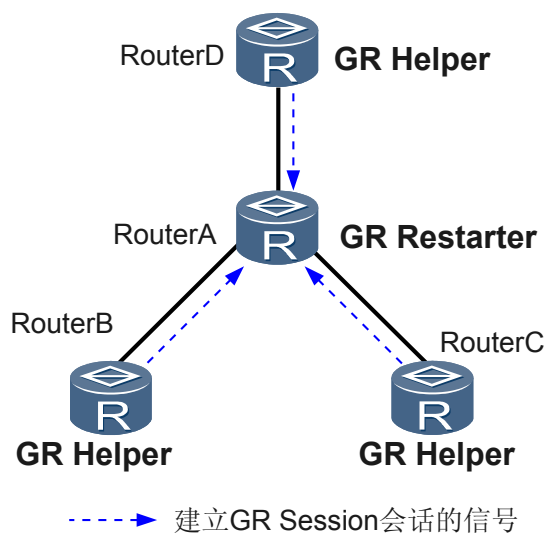
图 6-3 GR Restarter 的主备倒换过程



GR Helper 发现 GR Restarter 故障，继续保持和 GR Restarter 的邻接关系，在 GR Time 超时之前，仍保留与 GR Restarter 相关的路由。

3.启动后，GR Restarter 向邻居发送信号

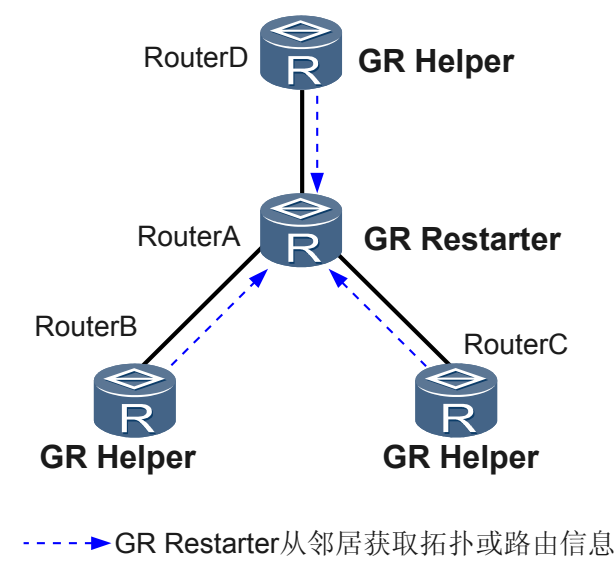
图 6-4 GR Restarter 主备倒换完毕后向邻居发送信号



Restarter 备板启动，向邻居 GR Helper 发送信号，重新建立会话。

4. Restarter 从邻居获取拓扑或路由信息

图 6-5 GR Restarter 从邻居获取拓扑或路由信息



GR Restarter 从邻居获取拓扑和路由信息后，重新计算路由表，并老化旧路由。

至此，GR Restarter 完成主备切换过程，并且在主备倒换期间转发不中断。

GR 与 HSB 的比较

表 6-1 GR 与 HSB 的比较

特性	优点	缺点
GR	● 简单易实现，无须对现有软件做大的改动 ● 无须备份协议的状态信息 ● 仅少量信息需要从 AMB 备份到 SMB，包括配置修改或更新的信息和事件、接口状态变化信息，及主板重启后可从邻居获得拓扑或路由信息 ● 发生主板切换时，中断转发业务的概率很低 ● 正常情况下，网络收敛迅速	● 互通问题：部分 GR 的规范还是草案，不同厂商可能采用不同的实现方式 ● 同时崩溃问题：如果 GR 路由器和其邻居同时崩溃，GR 无法正常工作 ● 较长的路由收敛时间：当处于 DOWN 状态的 GR 路由器永远不能恢复时，其邻居却误推测它会再次恢复而保留其相关路由和拓扑信息，直到 Recovery 定时器超时。与普通的无 GR 能力路由器的网络相比，整个网络的路由收敛时间延长 ● 恢复过程依赖于邻居路由器：由于 GR 协议的非独立特性，邻居路由器必须也支持 GR 能力

特性	优点	缺点
HSB	● HSB 路由器主板切换不会影响转发业务、路由进程 ● 路由和拓扑信息不会在切换时丢失，协议会话不会中断 ● HSB 路由器主备板之间的切换相对独立 ● 不需要邻居路由器的支持 ● 不存在兼容性问题 ● 切换不会影响邻居 ● 网络路由收敛比 GR 路由器更迅速	● 比 GR 更难实现：需要备份更多信息，包括协议状态、会话、路由、策略以及更新信息 ● 占用更多通信通道带宽：需要支持 AMB 和 SMB 之间的 TCP 备份 ● BGP/LDP 会话热备份依靠 TCP 连接。如果不希望邻居察觉到发生的切换，必须将 TCP 链路状态从 AMB 备份到 SMB；需要对不断变化的 TCP 链路状态进行备份

6.1.2 NE80E/40E 中的 GR 特性

GR 特性主要包括系统级 GR。系统级 GR 是将冗余备份、GR 和 HSB 相结合的一种技术，在设备进行主备倒换时不中断转发，降低对业务的影响，从而获得设备高可用性。

目前 NE80E/40E 支持以下 GR 特性：

- MPLS LDP（DU 或 DOD）
- OSPF（IPv4）
- IS-IS（IPv4/IPv6）
- BGP（IPv4/IPv6）、VPNv4 BGP 以及带标签路由 BGP
- RSVP
- PIM-SM 和 PIM-SSM
- OSPFv3
- RIP
- L3VPN
- Martini 方式的 VLL、PWE3 和 Martini 方式的 VPLS。

NE80E/40E 系统融合了 GR 和 HSB 的优点实现高可用性。实现方法是：

- 通过冗余备份技术，提供主控板的 1+1 备份。
- 通过 HSB 技术，将静态配置信息从 AMB 备份到 SMB，同时备份没有 GR 能力的协议的状态信息。
- 对于有 GR 能力扩展的协议，通过 GR 功能，借助邻居的帮助恢复协议状态信息。

这种融合双主控、GR 和 HSB 功能的 HA 特性称为系统级 GR，其功能是减小主备板倒换对报文转发的影响。

满足以下条件的路由器可以进行系统级 GR 的过程。

- 具备双主控板
- BGP、OSPF、IS-IS 和 LDP 协议支持 GR 功能

- 支持 HSB



说明

当路由器只支持 GR 不支持热备份 HSB 时，路由器可被用做 GR Helper，支持其他路由器的 GR 过程。

6.2 配置系统级 GR

系统级 GR 是将冗余备份、GR 和 HSB 技术结合在一起的、提高设备高可用性的一项技术。

6.2.1 建立配置任务

在配置系统级 GR 功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在以下情况下，使用系统级 GR 功能：

- 系统故障触发主备倒换
- 软件升级或系统维护时网络管理员手动触发主备倒换

为了确保主备板切换后业务不受影响，需要在主备板之间实现配置信息同步。目前有两种同步方式：自动同步、手动同步。

前置任务

在配置系统级 GR 之前，需完成以下任务：

- 配置各协议基本功能
- 配置各协议 GR 功能



说明

OSPF GR、IS-IS GR 和 BGP GR 的详细配置请参见《HUAWEI NetEngine80E/40E 路由器配置指南-IP 路由》，LDP GR 的详细配置请参见《HUAWEI NetEngine80E/40E 路由器配置指南-MPLS》。

数据准备

在配置系统级 GR 之前，需准备以下数据：

序号	数据
1	备用板的缺省槽位号

6.2.2 （可选）设置缺省的备板槽位号

此配置用来设置系统重启时缺省的备用板槽号。

背景信息

在同时存在两块主板的情况下，当系统重新启动时，将根据一定的规则裁决出哪块板作为备用板。可以通过本节的命令设置缺省的备板槽位号。

在 GR Restarter 路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **slave default slot-id**，配置备用板的缺省槽位号。

----结束

6.2.3 使能主备板配置数据自动同步功能

此配置用来在主用板写配置时自动的将配置数据同步到备用板。

背景信息

在 GR Restarter 路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **slave auto-update config**，使能主备板配置数据自动同步功能。

如果在主用板上执行命令 **save** 保存配置，系统自动将配置信息同步到备用板，实现主用板与备用板上的配置文件同步。

缺省情况下，主备板配置数据自动同步功能是打开的。

如果要关闭主备板配置数据自动同步功能，请执行命令 **undo slave auto-update config**。

----结束

6.2.4 使能强制主备倒换功能

使能主备倒换功能后，实现主用板和备用板的切换。

背景信息

在 GR Restarter 路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **slave switchover enable**，使能系统的强制主备倒换功能。

使能该功能后，可以手工执行 **slave switchover** 命令进行强制主备倒换。

缺省情况下，强制主备倒换功能是使能的。

如果要关闭系统的强制主备倒换功能，请执行命令 **slave switchover disable**。

----结束

6.2.5 （可选）重启备板

备板的软件版本升级后，可以使用此配置进行备板重启。

背景信息

当进行软件版本在线升级的任务时，会在主控板正常工作的情况下对备板进行软件版本升级，需要重新启动备板，待备板就绪后才能执行主备板切换。

在 GR Restarter 路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **slave restart**，重启备板。

----结束

6.2.6 检查配置结果

通过查看主备板状态内容，来检查配置是否成功。

前提条件

已经完成系统级 GR 功能的所有配置。

操作步骤

步骤 1 使用 **display switchover state** 查看主用板/备用板状态。

----结束

6.3 维护 HA

通过维护 HA，实现监控 HA 的运行状况。

6.3.1 监控 HA 运行状况

通过监控 HA 运行状况，可以了解运行过程中 HA 的相关信息。

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解 HA 的运行状况。

操作步骤

步骤 1 在任意视图下执行 **display switchover state** 命令，了解指定槽号的主用板/备用板备份状态的运行情况。

----结束

6.4 配置举例

介绍了一种 GR 的配置示例。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

背景信息

 说明

手册中所使用的链路接口编号和链路类型以 NE40E-X8 为例，实际使用时以现网设备为准。

6.4.1 配置系统级 GR 示例

本示例中，通过使能设备的 GR 能力，实现当设备出现故障而进行主备倒换时，转发不中断。

组网需求

 说明

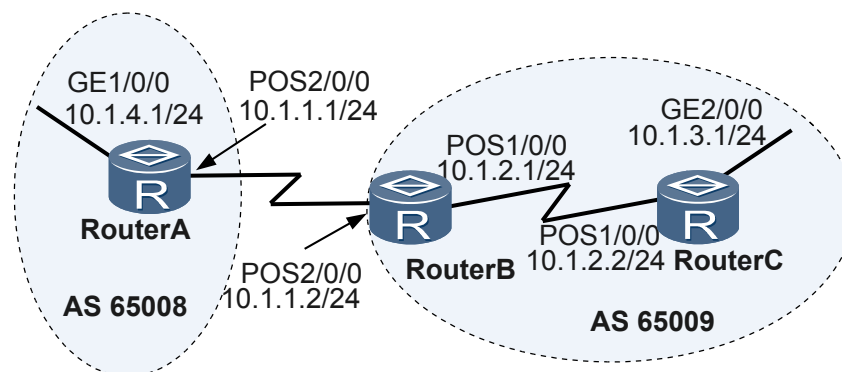
POS 接口特性在 NE80E/40E 系列中的 X1 和 X2 设备上不支持。

如图 6-6 所示。

- 在 AS65009 内使用 OSPF 作为 IGP 协议，RouterA 和 RouterB 建立 EBGP 连接，RouterC 为 AS 内部的一台非 BGP 路由器。
- RouterB 为双主控设备，主用板和备用板间形成备份关系，且支持 HSB，即主备板配置信息热备份功能。
- RouterA 上启用 BGP GR、RouterB 上启用 OSPF GR 和 BGP GR，RouterC 上启用 OSPF GR。

要求当 RouterB 由于系统故障或者管理员系统维护而进行主备板倒换时，转发不中断，即现网业务不受影响。

图 6-6 配置系统级 GR 组网图



配置思路

采用如下思路配置系统级 GR：

1. 在 RouterA 上使能 BGP 的 GR 能力，在 RouterB 上使能 OSPF、BGP 的 GR 能力，在 RouterC 上使能 OSPF 的 GR 能力，并配置 GR 参数。
2. 在 RouterB 上配置主备板配置信息同步功能。

数据准备

为完成此配置示例，需要准备如下数据：

- 各接口的 IP 地址
- OSPF、BGP 相关参数
- GR 参数

操作步骤

步骤 1 配置各接口的 IP 地址（略）

步骤 2 配置 OSPF、BGP 的基本功能（略）

步骤 3 配置 OSPF GR 功能

使能 RouterB 的 OSPF 协议本地链路信令能力和带外同步能力。RouterC 上的配置和 RouterB 完全相同。

```
[RouterB] ospf 100
[RouterB-ospf-100] opaque-capability enable
```

使能 RouterB 的 OSPF GR 能力。RouterC 上的配置和 RouterB 相同。

```
[RouterB-ospf-100] graceful-restart
[RouterB-ospf-100] graceful-restart period 600
```

步骤 4 配置 BGP GR 功能

使能 RouterB 的 BGP GR 能力。

```
[RouterB] bgp 65009
[RouterB-bgp] graceful-restart
[RouterB-bgp] graceful-restart timer restart 600
[RouterB-bgp] graceful-restart timer wait-for-rib 600
```

使能 RouterA 的 BGP GR 能力。

```
[RouterA] bgp 65008
[RouterA-bgp] graceful-restart
[RouterA-bgp] graceful-restart timer restart 600
[RouterA-bgp] graceful-restart timer wait-for-rib 600
```

步骤 5 配置主备板倒换参数

指定缺省的备板槽位号

```
<RouterB> system-view
[RouterB] slave default 17
```

使能 RouterB 的强制主备倒换功能。


```
<RouterB> system-view
[RouterB] slave switchover enable

# 使能主备板配置信息自动同步功能。

<RouterB> system-view
[RouterB] slave auto-update config
[RouterB] quit
<RouterB> save
```

步骤6 检验配置结果

在 RouterB 上强制执行主备倒换。

```
[RouterB] slave switchover
Caution!!! Confirm switch slave to master[Y/N]?y
```

立即在路由器 RouterC 和 RouterA 上执行 **display fib** 命令，可以看到和 RouterB 相关的转发表项依然存在，转发不中断，业务传输不受影响。

```
<RouterC> display fib
FIB Table:
Total number of Routes : 9
Destination/Mask  Nexthop      Flag TimeStamp      Interface      TunnelID
127.0.0.1/32      127.0.0.1      HU   t[42]              InLoop0        0x0
127.0.0.0/8       127.0.0.1      U    t[42]              InLoop0        0x0
10.1.2.2/32       127.0.0.1      HU   t[561]             InLoop0        0x0
10.1.2.0/24       10.1.2.2      U    t[561]             Pos1/0/0       0x0
10.1.2.1/32       10.1.2.1      HU   t[561]             Pos1/0/0       0x0
10.1.3.1/32       127.0.0.1      HU   t[578]             InLoop0        0x0
10.1.3.0/24       10.1.3.1      U    t[578]             GE1/0/0        0x0
3.3.3.3/32        127.0.0.1      HU   t[724]             InLoop0        0x0
10.1.4.0/24       10.1.2.1      DGU  t[1422]            Pos1/0/0       0x0

<RouterA> display fib
FIB Table:
Total number of Routes : 10
Destination/Mask  Nexthop      Flag TimeStamp      Interface      TunnelID
127.0.0.1/32      127.0.0.1      HU   t[28]              InLoop0        0x0
127.0.0.0/8       127.0.0.1      U    t[28]              InLoop0        0x0
10.1.4.1/32       127.0.0.1      HU   t[28]              InLoop0        0x0
10.1.4.0/24       10.1.4.1      U    t[28]              GE1/0/0        0x0
10.1.1.1/32       127.0.0.1      HU   t[444]             InLoop0        0x0
10.1.1.0/24       10.1.1.1      U    t[444]             Pos2/0/0       0x0
10.1.1.2/32       10.1.1.2      HU   t[444]             Pos2/0/0       0x0
10.1.2.0/24       10.1.1.2      DGU  t[1402]            Pos2/0/0       0x0
10.1.3.0/24       10.1.1.2      DGU  t[1402]            Pos2/0/0       0x0
1.1.1.1/32        127.0.0.1      HU   t[2060]            InLoop0        0x0
```

----结束

配置文件

● RouterA 的配置文件

```
#
sysname RouterA
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.4.1 255.255.255.0
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.1 255.255.255.0
#
interface LoopBack1
ip address 1.1.1.1 255.255.255.255
#
```

```
bgp 65008
router-id 1.1.1.1
graceful-restart
graceful-restart timer restart 600
peer 10.1.1.2 as-number 65009
#
ipv4-family unicast
undo synchronization
network 10.1.4.0 255.255.255.0
peer 10.1.1.2 enable
#
return
```

● RouterB 的配置文件

```
#
sysname RouterB
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.2 255.255.255.0
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.2.1 255.255.255.0
#
interface LoopBack1
ip address 2.2.2.2 255.255.255.255
#
bgp 65009
router-id 2.2.2.2
graceful-restart
graceful-restart timer restart 600
peer 10.1.1.1 as-number 65008
#
ipv4-family unicast
undo synchronization
import-route ospf 100
peer 10.1.1.1 enable
#
#
ospf 100
import-route bgp
opaque-capability enable
graceful-restart period 600
area 0.0.0.0
network 10.1.2.0 0.0.0.255
#
return
```

● RouterC 的配置文件

```
#
sysname RouterC
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 10.1.3.1 255.255.255.0
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.2.2 255.255.255.0
#
interface LoopBack1
ip address 3.3.3.3 255.255.255.255
#
ospf 100
opaque-capability enable
graceful-restart period 600
```

```
area 0.0.0.0
network 10.1.3.0 0.0.0.255
network 10.1.2.0 0.0.0.255
#
return
```

7 NSR 配置

关于本章

NSR 可以提高系统的高可用性。

[7.1 NSR 简介](#)

介绍 NSR 的实现方式和相关技术。

[7.2 配置 NSR](#)

通过配置 NSR，实现主备倒换过程中路由和转发的不中断。

7.1 NSR 简介

介绍 NSR 的实现方式和相关技术。

7.1.1 NSR 概述

NSR 是在有主用主控板和备用主控板的设备上主用主控板发生故障时不影响邻居关系的一种可靠性技术。

NSF（Non-Stopping Forwarding，不间断转发）和 NSR（Non-Stopping Routing，不间断路由）是高可靠性的两个解决方案。

- NSF：通过协议的 GR 机制，支持系统主备倒换时，转发业务不中断。
 - 当由于某种原因系统发生故障时，在系统重启过程中，转发业务不中断
 - 系统恢复后，设备能够重新建立邻居关系，从邻居处获取路由信息并重建路由表

关于 GR 的具体配置，请参见《HUAWEI NetEngine80E/40E 路由器 配置指南-可靠性》中的“GR 配置”。

- NSR：通过协议备份机制，实现主备控制板倒换时控制平面（路由）和转发平面均不中断。

在设备发生倒换的过程中，路由处理不中断，因为：

- 邻居和拓扑信息不丢失
- 邻居关系不中断

这种方式的优点有：

- 不依赖也不影响对端设备，没有互通问题
- 路由的收敛速度要比 NSF 快

表 7-1 NSR 与 NSF 的比较

特性	优点	缺点
NSF	● 从主用主控板到备用主控板需要备份的信息少： - 配置信息的变化 - 接口状态信息 - 邻居、协议状态、收发报文信息、路由、拓扑信息 ● 系统倒换过程中，转发平面仍然能够提供转发服务： - 在协议 GR 的过程中，路由、拓扑可能发生变化，导致转发错误。但是这种情况发生的可能性较小	● 互通问题：标准不成熟，不同厂商可能采用不同的实现方式 ● 依赖邻居状态：GR 依赖邻居协助。如果软件缺陷导致所有设备同时发生故障，NSF 不能正常工作 ● 路由协议收敛速度慢：如果 NSF 设备故障后永远不能正常启动，对端设备仍然会错误的认为它过一段时间能够启动，一直到恢复时间结束，然后才会删除从它学到的路由信息，这段时间内邻居路由的正确性无法保证

特性	优点	缺点
NSR	● 控制平面发生故障时，转发平面仍然能够提供转发服务 ● 设备发生倒换时，路由处理不中断 - 路由和拓扑信息不丢失 - 邻居关系不中断 ● 倒换只与自身相关 - 不依赖也不影响对端设备，没有互通问题 - 路由收敛速度比 NSF 快	● 需要更多的带宽：消耗更多的系统资源

NSR 与 GR

在主备倒换端，系统支持 NSR 和 GR 两种不同的 HA 保护，他们是互斥的。即，对于一个特定协议，系统倒换后，只能采用 NSR 或 GR 两种处理方式的一种。设备在部署 NSR 时，仍然可以支持 GR Helper 的功能，以支持自己的邻居 GR 过程，最大可能的保证用户全网网络节点业务的高可靠性。

7.1.2 NE80E/40E 支持的 NSR 特性

您可以了解到支持 NSR 功能的协议有哪些。

目前，支持 NSR 功能的协议有：

- ISIS
- OSPF
- OSPFv3
- BGP
- BGP4+
- PIM
- MSDP
- MVPN
- IPv4/IPv6 L3VPN
- RSVP
- LDP
- BFD
- VRRP

7.2 配置 NSR

通过配置 NSR，实现主备倒换过程中路由和转发的不中断。

7.2.1 建立配置任务

在配置系统级 NSR 功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

在以下情况下，使用系统级 NSR 功能：

- 系统故障触发主备倒换
- 软件升级或系统维护时网络管理员手动触发主备倒换

NSR 对系统可靠性要求很高。要求当系统控制平面发生故障后，不依赖于邻居就能将控制平面平滑切换到备用平面，路由不间断。

使用 NSR 特性有如下限制：

- 系统倒换后的平滑时间不是关键的性能指标。NSR 不会针对系统倒换后的平滑时间进行优化设计，全部采用全平滑的方式。
- 由于采用备份稳态邻居的方案，可能会导致对端设备认为已经建立的邻居关系在倒换过后重新建立。这种情况下邻居设备会感知倒换的发生。对于这种临界情况下倒换瞬间建立的邻居关系，还没有更新报文发生，邻居重新建立不会导致业务发生任何中断。
- 对于单主控的系统，不能使用 NSR 实现高可靠性。
- 如果在批量备份之前主用进程发生故障，备用进程的状态是不可预知的，没有进入可以倒换的状态，不能够承担主用进程的角色，此时使用 NSF 技术。
- 使能了 NSR 的系统不支持系统级 GR。

前置任务

无

数据准备

无

7.2.2 使能 NSR 功能

使能 NSR 功能后，在设备主备倒换的过程中，路由和转发的不中断。

背景信息

在要求高可靠性的设备上以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **switchover mode nonstop-routing**，使能 NSR 功能。

----结束

7.2.3 检查配置结果

通过查看备倒换后的路由信息，来检查配置是否成功。

前提条件

已经完成 NSR 功能的所有配置。

操作步骤

- 使用 **display ip routing-table [verbose]**命令，查看主备倒换后的路由信息。
- 使用 **display fib verbose** 命令，查看主备倒换后的转发信息。

----结束

任务示例

在配置成功备用主控板重启完毕后，执行上面的命令，应能得到如下的结果：

- 备用主控板上查看邻居信息只有 Up 状态，没有 Init 状态，Up 时与主用主控板一致
- 备用主控板上查看的接口信息、LSDB 信息和路由信息与主用主控板一致

8 以太网 OAM 配置

关于本章

通过对以太网 OAM 的介绍和各种配置，实现链路级以太网 OAM 和网络级以太网 OAM 链路的检测，提高网络可靠性。它主要应用在城域网中。

8.1 以太网 OAM 简介

以太网 OAM 技术是分层实现的，可分为链路级以太网 OAM 和网络级以太网 OAM。

8.2 配置 EFM OAM 基本功能

通过配置 EFM OAM 基本功能，检测两直连设备之间链路的连通性。

8.3 配置 EFM OAM 链路监控

通过配置 EFM OAM 误帧、误码和误帧秒检测，能够更好的检测和发现链路层的故障。

8.4 配置物理链路丢包率检测

可以检测物理链路的丢包率，以使用户能够采取有效的措施来保证链路更好的工作。

8.5 配置 EFM OAM 和接口联动

一旦 EFM OAM 和接口联动后，可能对业务产生很大影响，例如二三层业务全部被阻塞。

8.6 配置以太网 CFM 基本功能

通过配置以太网 CFM 基本功能，实现端到端的连通性故障检测、故障通告、故障判定和故障定位功能。

8.7 配置以太网 CFM 的相关参数

通过对以太网 CFM 的相关参数进行调整，在以太网中更好的实现端到端的连通性故障检测。

8.8 配置以太网的故障确认

通过发送测试报文和接收应答报文来检测两台设备之间链路的连通性。

8.9 配置以太网的故障定位

通过发送测试报文和接收应答报文来定位两台设备之间链路的连通性故障。

8.10 配置以太网 CFM 和接口联动

以太网 CFM 与接口联动功能主要用于 LACP 静态链路聚合组或手工 1:1 主备模式链路聚合的活动链路快速故障检测和触发保护倒换。

8.11 配置 EFM OAM 和以太网 CFM 之间的联动

通过配置 EFM OAM 和以太网 CFM 之间的联动，实现故障相互传递。

8.12 配置以太网 CFM 和 VPLS 的组合应用

通过配置 CFM 和 VPLS 的组合应用，实现在 VPLS 场景中端到端的连通性故障检测、故障通告、故障判定和故障定位功能。

8.13 配置以太网 CFM 和 VLL 的组合应用（使用 QinQ 终结子接口）

PE 设备将带有两层 Tag 的报文接入 VLL 网络中，为了提高网络的可靠性，可通过在 PE 设备 AC 侧配置 QinQ 终结子接口绑定 L2VC，再部署 CFM 功能。

8.14 配置以太网 CFM 和 VPLS 的组合应用（使用 QinQ 终结子接口）

PE 设备将带有两层 Tag 的报文接入 VPLS 网络中，为了提高网络的可靠性，可通过在 PE 设备 AC 侧配置 QinQ 终结子接口绑定 VSI 接入 VPLS 网络，再部署 CFM 功能。

8.15 配置 ETH OAM 和 MPLS OAM/BFD 组合应用

通过配置 ETH OAM 和 MPLS OAM/BFD 的组合应用，实现故障信息的传递功能。

8.16 配置以太网 CFM 和组播 VLAN 1+1 保护功能

以太网 CFM 可用于工作 VLAN 和保护 VLAN 的连通性故障检测，以及触发保护倒换，从而实现组播 1+1 保护功能。

8.17 维护以太网 OAM

通过维护以太网 OAM，可以实现清除 CCM 消息统计数据、监控以太网 OAM 的运行状况。

8.18 配置举例

介绍 BFD 快速检测链路的各种示例。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

8.1 以太网 OAM 简介

以太网 OAM 技术是分层实现的，可分为链路级以太网 OAM 和网络级以太网 OAM。

8.1.1 以太网 OAM 概述

以太网 OAM 是能够有效提高以太网的网络管理能力和维护能力，保障网络的稳定运行。它主要应用在以太网中。

产生背景

以太网技术自诞生起，以其简单易用、价格低廉的特点逐步成为局域网的主导技术。近年来，随着千兆、万兆以太网技术的相继应用，以太网已经向城域网和广域网方向扩展。

由于以太网最初主要应用于局域网，相对于城域网和广域网，局域网对可靠性、稳定性要求都较低，因此以太网一直缺乏运行维护管理机制，这一点已成为以太网作为运营网络的严重障碍。因此，在以太网上实现 OAM（Operations Administration and Maintenance）成为一个必然的发展趋势。

主要功能

以太网 OAM 主要功能可分为以下两部分：

- 故障管理
 - 通过定时或手动发送检测报文来探测网络的连通性。
 - 提供类似 IP 网络中的 Ping（Packet Internet Groper）和 Traceroute 的功能，对以太网进行故障确认和故障定位。
 - 和保护倒换协议配合，当检测到连通性故障后触发保护倒换，以实现网络业务中断小于等于 50 毫秒的运营级可靠性目标。
- 性能管理

性能管理主要是指对网络中的丢包、时延、抖动进行衡量，也包括对网络中各类流量进行统计。性能管理通常在用户接入点实施。有了性能管理工具，运营商可通过网管监测网络运行情况、定位故障，确认网络转发能力是否符合与用户签订的 SLA（Service Level Agreement）。

以太网 OAM 能够有效提高以太网的网络管理和维护能力，保障网络的稳定运行。

8.1.2 NE80E/40E 支持的以太网 OAM

以太网 OAM 包括：EFM OAM、以太网 CFM、故障联动和 EFM OAM 扩展。

EFM OAM

802.3ah（Ethernet in the First Mile，简称 EFM）主要定义用于用户接入部分的以太网物理层规范，以及接入部分的以太网 OAM。主要用于最后一公里的链路检测。是链路级的 OAM。NE80E/40E 设备的 EFM OAM 功能包括：

- 对端发现

对端发现是指当 NE80E/40E 的某个接口和对端接口使能了 EFM OAM 功能时，该接口和对端接口通过发送和响应慢速协议帧 OAMPDU（OAM Protocol Data Unit）来协商确定双方的 EFM OAM 配置是否匹配。如果双方的 EFM OAM 配置匹配，则双方进入 EFM OAM 握手阶段。在握手阶段，双方通过定时发送 OAMPDU 维持邻居关系。正常情况下，OAMPDU 的发送时间间隔为 1 秒。

- 链路监控

链路监控是指如果接口检测到误帧越限事件、误码越限事件或误帧秒越限事件，则该接口通过向对端设备发送事件通告 OAMPDU 来通告故障。其中：

- 误帧越限事件是指在设定的观察时长内，接口检测到的误帧数量达到或超过设定的阈值。
- 误码越限事件是指在设定的观察时长内，接口检测到的误码数量达到或超过设定的阈值。
- 误帧秒越限事件是指在设定的观察时长内，接口检测到的误帧秒数量达到或超过设定的阈值。

其中，误帧秒是指将设定的观察时长划分为若干个以 1 秒为单位的时间段，如果在某个时间段内检测到了至少一个误帧，则该时间段称为一个误帧秒。

- 故障通告

故障通告是指当本端发生报文错误越限事件或严重故障事件后，本端发送故障消息通告对端设备，同时将故障事件记入日志并上报给网管系统。

- 系统重新启动
- 接口板复位
- 物理链路故障
- 协议报文超时
- OAM 管理模块传递的故障

对端设备接到通知消息后，将消息中携带的故障事件记入日志，并上报给网管系统。

- 远端环回

远端环回是指当本端向对端发送除 EFM OAM 协议报文外的所有其它报文时，对端（远端）接收到报文后不按照报文的目地址进行转发，而是将报文从接收端口再发回给本端。远端环回功能可用于定位链路故障和测试链路质量。

每个具备 EFM OAM 功能的接口都有一个工作模式属性。EFM OAM 工作模式共包括两种：主动模式和被动模式。对端发现和远端环回都只能由主动模式的接口发起。

以太网 CFM

802.1ag（Connectivity Fault Management，简称 CFM）定义了基于以太网承载网络的连接检测的 OAM 功能，包括 CC/LB/LT，适用于大规模组网的端到端场景，是网络级的 OAM。

现如今，802.1ag 协议分为 draft7 草案版本和 standard2007 标准版本，两者主要如表 8-1 所示。

表 8-1 802.1 协议 draft7 版本和 standard2007 版本的区别

特性	draft7	standard2007	备注
MD (Maintenance Domain)	支持	支持	标准版本和草案实现的功能、配置一样
默认 MD (Default Maintenance Domain)	不支持	支持	-
MA (Maintenance Association)	支持	支持	标准版本和草案实现的功能、配置一样
MEP (Maintenance association End Point)	支持	支持	标准版本和草案实现的功能、配置一样
RMEP (Remote Maintenance association End Point)	支持	支持	标准版本和草案实现的功能、配置一样
MIP (Maintenance association Intermediate Point)	支持	支持	标准版本和草案中 MIP 节点的生成规则是一样的，分为：default 型、explicit 型和 none 型。不同的是： ● 草案中，MIP 节点是基于端口创建。 ● 标准版本中，MIP 节点是基于 MD 或默认 MD 创建。
MP (Maintenance Point)	支持	支持	标准版本和草案实现的功能、配置一样

- 基本概念

- MD

维护域 MD (Maintenance Domain) 是指对其实施以太网 CFM 管理的一个网络或一个网络的一部分。一个 MD 由一个统一的 ISP (Internet Service Provider) 进行管理。

- 默认 MD

802.1ag2007 标准版本规定，每台设备上可配置一个默认 MD。默认 MD 的级别必须高于本设备配置 MEP 节点所有 MD 的级别，和高优先级 MD 的级别相等，用于高级别 CCM 报文穿越，创建 MIP 节点回复 LTR 报文。

- MA

维护联盟 MA（Maintenance Association）是 MD 的一部分。一个 MD 可以划分成一个或多个 MA。在 NE80E/40E 设备上，每个 MA 可以对应一个 VLAN 或 VSI。以太网 CFM 对每个 MA 分别进行连通性故障检测。

- MEP

维护联盟边缘节点 MEP（Maintenance association End Point）是 MA 的边缘节点。

对于运行以太网 CFM 的网络中的任意一台设备，该设备上的 MEP 称为本地 MEP，同一 MA 内其它设备上的 MEP 对本设备而言称为远端维护联盟边缘节点 RMEP（Remote Maintenance association End Point）。



注意

- 一个 Trunk 上只支持配置一个 MEP，Trunk 上存在多个子接口也只能配置一个 MEP。
- 设备在运行过程中，不支持热插拔。

- MIP

维护联盟内部节点 MIP（Maintenance association Intermediate Point）是 MA 的内部节点。

草案中，MIP 位于设备的接口上，是设备按规则自动创建的。

标准版本中，MIP 节点基于 MD 和默认 MD 按规则自动创建。

● 连通性故障检测

以太网 CFM 将整个网络划分成一个或多个 MD，将每个 MD 又划分成一个或多个 MA，通过同一 MA 的 MEP 之间定时互发 CCM（Continuity Check Message）消息来检测该 MA 内以太网的连通性。

● 故障确认

- 802.1ag MAC Ping

802.1ag MAC Ping 与 Ping 类似，通过发送测试报文和接收应答报文来检测从本设备到目的设备是否可达。802.1ag MAC Ping 在同一个 MA 内进行，由 MEP 发起，目的节点可以是 MEP 或 MIP。

- 通用 GMAC ping

通用 Gmac ping 和 802.1ag MAC Ping 原理相似，但是通用 Gmac ping 不需要由 MEP 发起，目的节点也不需要是 MEP 或 MIP，即在源设备、中间设备和目的设备上均不需要配置 MD、MA 和 MEP 就可以进行通用 Gmac ping。

- PBB-TE Ping

PBB-TE Ping（Provider Backbone Bridge-Traffic Engineering Ping）用来检测 PBB-TE Tunnel 的连通性。

● 故障定位

- 802.1ag MAC Trace

802.1ag MAC Trace 与 Traceroute（或 Tracert）类似，通过发送测试报文和接收应答报文来检测从本设备到目的设备的路径或定位故障点。802.1ag MAC Trace 在同一个 MA 内进行，由 MEP 发起，目的节点可以是 MEP 或 MIP。

- 通用 GMAC trace

通用 Gmac trace 和 802.1ag MAC Trace 原理相似，但是通用 Gmac trace 不需要由 MEP 发起，中间节点和目的节点也不需要是 MEP 或 MIP，即在源设备、中间设

备和目的设备上均不需要配置 MD、MA 和 MEP 就可以进行通用 Gmac trace，所有中间设备均回应 LTR（Linktrace Reply）消息。

- PBB-TE MAC Trace

PBB-TE Trace 用来定位 PBB-TE Tunnel 的连通性故障。PBB-TE Trace 由 PBB-TE Tunnel 的一端发起，目的地是该 PBB-TE Tunnel 的另一端。

故障联动

- EFM OAM 与接口联动

EFM OAM 与接口联动是指当 EFM OAM 检测到链路连通性故障后，接口下除 EFM 协议报文外的所有其他报文都无法被转发，二三层业务将全部被阻塞。因此，一旦启用 EFM OAM 和当前接口联动功能，将可能对业务产生很大影响。如果当前接口通过 EFM OAM 检测到链路连通性故障恢复，则恢复该接口的所有转发报文，并通知该接口上的所有二三层业务作相应处理。

此外，请务必确保两端 EFM OAM 协议状态变为 detect 之后再配置 EFM OAM 和当前接口联动功能。

- 以太网 CFM 与接口联动

以太网 CFM 与接口联动是如果某个 MA 内的 MEP 检测到和指定 RMEP 之间有连通性故障，OAM 管理模块对该 MEP 所在接口进行闪断处理，即先关闭该接口 7 秒，然后再打开该接口。

- EFM OAM 和 PBB-TE 业务实例联动

EFM OAM 和 PBB-TE 业务实例联动是指 EFM OAM 模块检测到故障后，通过和自己建立联动关系的业务实例所绑定的 PBB-TE Tunnel 将故障消息传递到隧道的另一端。

- 以太网 CFM 和 PBB-TE 业务实例联动

以太网 CFM 和 PBB-TE 业务实例联动是指以太网 CFM 模块检测到故障后，通过和自己建立联动关系的业务实例所绑定的 PBB-TE Tunnel 将故障消息传递到隧道的另一端。

- 以太网 CFM 和 EFM OAM 联动

以太网 CFM 和 EFM OAM 联动是指 MA 内检测到故障后，OAM 管理模块通过接口将故障传递到 EFM OAM 的对端；EFM OAM 模块检测到故障后，OAM 管理模块通过接口将故障传递到 MA。

- 以太网 CFM 向 EFM OAM 传递故障
- EFM OAM 向以太网 CFM 传递故障
- 以太网 CFM 和 EFM OAM 双向传递故障

- 以太网 CFM 和以太网 CFM 联动

以太网 CFM 和以太网 CFM 联动是指 MA 内检测到故障后，OAM 管理模块通过绑定关系将该故障传递到另一侧的 MA。

- 某侧以太网 CFM 向另一侧以太网 CFM 传递故障
- 两侧以太网 CFM 双向传递故障

- 以太网 CFM 和 BFD 联动

以太网 CFM 和 BFD 联动是指 MA 内检测到故障后，OAM 管理模块通过绑定关系将该故障传递到另一侧的 BFD；BFD 检测到故障后，通过绑定关系将故障传递到 MA。

- 以太网 CFM 向 BFD 传递故障

- BFD 向以太网 CFM 传递故障
- 以太网 CFM 和 BFD 双向传递故障
- 以太网 CFM 和 MPLS OAM 联动

以太网 CFM 和 MPLS OAM 联动是指 MA 内检测到故障后，OAM 管理模块通过绑定关系将该故障传递到 MPLS OAM；MPLS OAM 检测到故障后，OAM 管理模块通过绑定关系将故障传递到 MA。

 - 以太网 CFM 向 MPLS OAM 传递故障
 - MPLS OAM 向以太网 CFM 传递故障
- EFM OAM 和 BFD 联动

EFM OAM 和 BFD 联动是指 EFM OAM 检测到故障后，OAM 管理模块通过接口将该故障传递到另一侧的 BFD；BFD 检测到故障后，通过接口将故障传递到 EFM OAM。

 - EFM OAM 向 BFD 传递故障
 - BFD 向 EFM OAM 传递故障
 - EFM OAM 和 BFD 双向传递故障
- EFM OAM 和 MPLS OAM 联动

EFM OAM 和 MPLS OAM 联动是指 EFM OAM 检测到故障后，OAM 管理模块通过接口将该故障传递到 MPLS OAM；MPLS OAM 检测到故障后，OAM 管理模块通过接口将故障传递到 EFM OAM。

 - EFM OAM 向 MPLS OAM 传递故障
 - MPLS OAM 向 EFM OAM 传递故障

EFM OAM 扩展

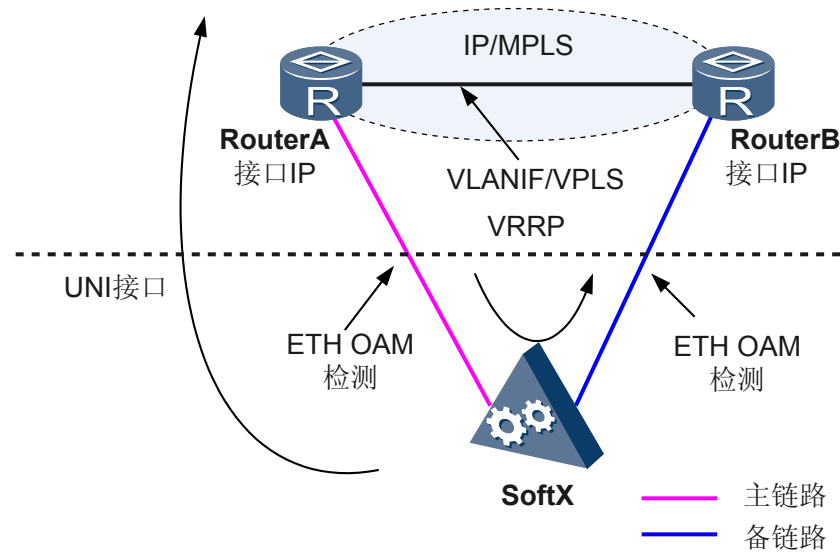
对于 IP 业务设备来说，为保证业务的可靠性，一般采用主备冗余方式接入到 IP 网络。当前主流设计中，IP 业务设备主要通过 VRRP 方式接入路由器，但这种方式当初是为 PC 终端设计，所以在可靠性和性能上不能满足电信级的业务的需求。

EFM OAM 作为一种检测机制，既可以接入三层网络（IP/MPLS），也可以接入二层网络（PBT-TE/T-MPLS/VPLS），目前被各厂商设备认可。EFM OAM 扩展即在 EFM OAM 原有功能的基础上扩展了主备控制功能。

为了满足电信级业务的接入需要，EFM OAM 扩展了原有的 EFM 的检测功能和通告功能。在 EFM OAM 的信息报文中携带主备状态标志，在路由器侧根据接收到的报文的主备状态标志来控制接入链路的状态，通过与接口联动、与静态路由联动来影响业务流量的走向，并且在主用链路出现故障时实现自动倒换，使接入网络达到电信级的可靠性。

- **图 8-1** 是 EFM OAM 扩展 FOR VRRP 场景图。

图 8-1 EFM OAM 扩展 FOR VRRP 场景



SoftX 上使用两块物理板卡上的接口，作为主备接口，主备接口板上配置同一个 IP 地址，正常情况下主接口板上 IP 有效。SoftX 业务双归接入路由器网关 RouterA 和 RouterB。

RouterA 和 RouterB 之间的链路配置有两种选择：

- VLANIF 方式：
 - 路由器下行口为二层口，加入到 VLAN，使两台设备处于同一个广播域。
 - 配置 VLANIF 接口。
- VPLS 方式：
 - 配置 PW，路由器下行口作为 AC 侧接入 VPLS。
 - 路由器之间配置 L2VE 口，绑定与 AC 口同一个 VSI。
 - 配置 L3VE 口，在 L3VE 口上创建 VRRP，与 L2VE 形成 VE-GROUP。这样就可以通过 VPLS 使两台路由器处于同一个广播域。

SoftX 通过 EFM OAM 扩展功能对连接 RouterA 和 RouterB 的链路分别进行故障检测。

在 VLANIF 接口上配置 VRRP 备份组。VRRP 备份组的虚拟 IP 地址与 IP 业务设备的 IP 地址处于同一网段。RouterA 和 RouterB 下行口为普通以太网口。配置 VRRP 以 reduce 方式 track 下行口。配置 EFM OAM 扩展与接口联动。

正常情况下，SoftX 首先计算出链路主备，用户流量从主用链路上传输，备用链路禁止流量收发处理。SoftX 通过 EFM OAM 扩展报文将链路主备信息通知给设备 RouterA 和 RouterB 下行口。由于主备路由器配置了 VRRP 以 reduce 方式 track 接口，同时配置 EFM OAM 扩展与接口联动。所以收到备用消息的路由器会降低优先级，而收到主用消息的路由器会恢复优先级，以保证 VRRP 的主备状态与下行口主备状态一致。

- 下行口链路故障切换和回切：当 IP 业务设备与路由器之间检测到 EFM OAM 故障，IP 业务设备进行主备链路切换，从原备用接口发送免费 ARP 报文给设备，然后在发送的 EFM OAM 扩展报文中携带新主备链路信息。

1. 如果 Router2 先收到免费 ARP 报文，处理流程如下：

- Router2 刷新 MAC 表项和 ARP 表项，并生成到 SoftX 的主机路由，同时将免费 ARP 广播到 RouterA，RouterA 同样进行 ARP 表项刷新，同时刷新到 SoftX 的路由出接口。

这样，从 RouterA 过来的回程流量将会经过 RouterB，RouterB 查 MAC 表发送到 IP 业务设备。此时下行流量将通过 RouterB 转发，但此时 RouterB 为备用，所以下行流量将被丢弃。

- 然后 RouterB 又收到主用 EFM OAM 报文，对外发布路由，恢复 VRRP 优先级，并切换为主用链路。返程流量将直接回到 RouterB 上。
- RouterA 检测到 EFM OAM 故障后立即撤消路由，降低 VRRP 优先级，链路切换为备用，上下行流量均被阻塞。

2. 如果 RouterB 先收到 EFM OAM 主用报文，处理流程如下：

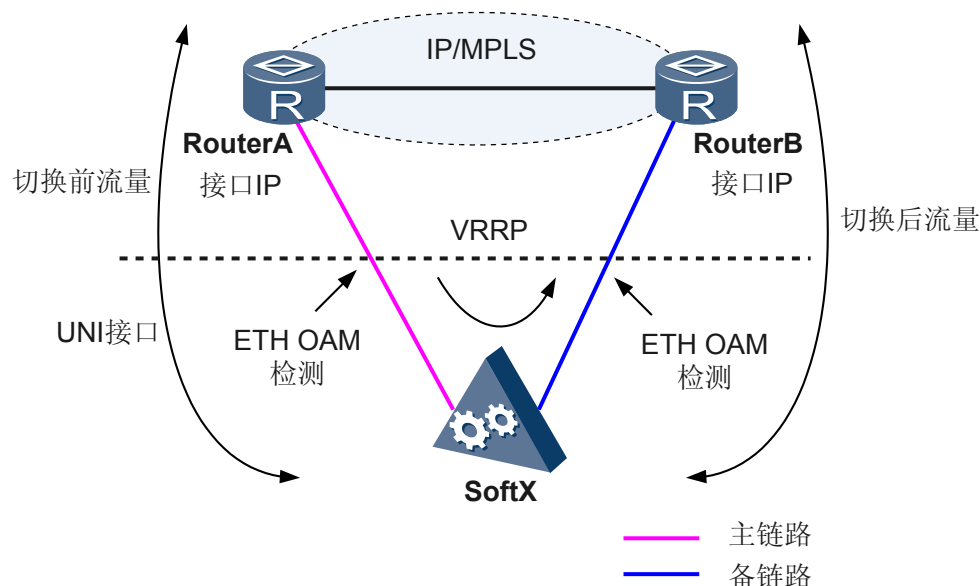
- Router2 对外发布静态路由，取消链路阻塞状态，链路恢复正常。恢复 VRRP 优先级，VRRP 切换为主用链路，上下行流量将会引到 RouterB 上，同时向 RouterA 和 IP 业务设备发送免费 ARP 报文。
- RouterA 检测到 EFM OAM 故障后撤消静态路由，降低 VRRP 优先级，VRRP 切换为备用链路，同时阻塞下行口的业务流量。学习收到的免费 ARP 报文，生成经过 RouterB 到 IP 业务设备路由，将下行流量引导 RouterB 上。

当链路故障恢复后，IP 业务设备从恢复的链路上通知对端路由器备用状态，不发送免费 ARP 报文，不进行流量回切，所以没有流量回切问题。

- 上行链路故障切换和回切：RouterA 上行链路故障时，将会导致路由在远端 PE 设备收敛。回程流量从 RouterA 上迂回到 RouterB，从 IP 业务设备发出的流量将会因为 RouterA 启用了到 RouterB 的路由而通过 RouterB 上行。

- 图 8-2 是 EFM OAM 扩展 FOR 静态路由场景。

图 8-2 EFM OAM 扩展 For 静态路由



SoftX 上主备接口板上配置同一个 IP 地址；RouterA 和 RouterB 上与 IP 业务设备连接的接口上配置同一个 IP 地址，而且与 IP 业务设备同一网段。SoftX 上再配置一个业务 IP，用于业务传输。路由器上配置到业务 IP 的静态路由。RouterA 和

RouterB 之间为 PE 连接。路由器下行口可以为普通以太网口、设备之间连接链路为普通以太网链路、ETH-TRUNK 链路。

IP 业务设备扩展 EFM OAM 协议，通过 EFM OAM 扩展协议对路由器发布主备用信息，路由器上配置静态路由 track EFM OAM 扩展接口，主用路由器对外发布到业务 IP 的静态路由；备用路由器对外不发布路由。如果 EFM OAM 扩展检测到故障则作与备用链路相同的处理。

路由收敛稳定后上行流量和下行流量都从主用链路上走。RouterA 为主用路由器，RouterB 为备用路由器。

- 下行口链路故障切换和回切：

当 IP 业务设备主用链路故障时，IP 业务设备进行链路切换，主用 EFM OAM 扩展报文发送到 RouterB 上，RouterB 收到后切换为主设备，对外发布经 RouterB 到业务 IP 的路由；RouterA 通过 EFM OAM 进行故障检测后切换为备用设备，撤销到业务 IP 的路由。

当链路故障恢复后 IP 业务设备对 RouterA 发布 EFM OAM 备用信息，但不进行流量切换。RouterA 不发布路由。

- 上行口链路故障和回切：RouterA 上行链路故障时，将会导致路由在远端 PE 设备上收敛，回程流量从 RouterB 上迂回到 RouterA，从 IP 业务设备发出的流量会经由 RouterA 到 RouterB 的上行路由，通过 RouterB 传输到远端 PE。

8.2 配置 EFM OAM 基本功能

通过配置 EFM OAM 基本功能，检测两直连设备之间链路的连通性。

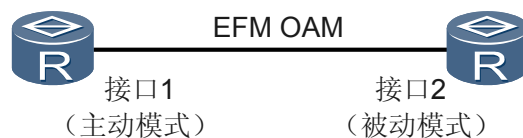
8.2.1 建立配置任务

在配置 EFM OAM 基本功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 8-3 所示，当需要检测两直连设备之间链路的连通性时，可执行本配置任务。

图 8-3 配置 EFM OAM 基本功能



前置任务

无

数据准备

在配置 EFM OAM 基本功能之前，需要准备以下数据。

序号	数据
1	(可选) EFM OAM 协议报文的最大尺寸

8.2.2 全局使能 EFM OAM 功能

全局使能 EFM OAM 功能是所有使用 EFM OAM 功能的前提条件。

背景信息

请在链路两端设备上以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **efm enable**，全局使能 EFM OAM 功能。

缺省情况下，EFM OAM 功能处于全局禁止状态。

----结束

8.2.3 配置接口的 EFM OAM 工作模式

EFM OAM 工作模式是具备 EFM OAM 接口的一个属性，包括两种模式：主动模式和被动模式。

背景信息

 说明

只能在 EFM OAM 功能全局使能后，接口的 EFM OAM 功能使能前，配置接口的 EFM OAM 工作模式。在接口的 EFM OAM 功能使能后，设备不允许再改变接口的 EFM OAM 工作模式。

请在链路两端设备上以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface interface-type interface-number**，进入链路两端接口的接口视图。

步骤 3 执行命令 **efm mode { active | passive }**，配置接口的 EFM OAM 工作模式。

缺省情况下，接口的 EFM OAM 工作模式是主动模式。

应将链路两端中至少一端的接口配置为主动模式。配置为主动模式的接口，在使能了接口的 EFM OAM 功能后，会主动发起 EFM OAM 对端发现。而配置为被动模式的接口则不会主动发起 EFM OAM 对端发现过程，而是等待对端发送的协议报文。如果两端都配置成为主动模式，链路检测也可以进行；如果两端都配置成为被动模式，则链路检测无法进行。

----结束

8.2.4 （可选）配置 EFM OAM 协议报文的最大尺寸

可以在接口上配置 EFM OAM 协议报文的最大尺寸。在当前接口上，超过此尺寸的 EFM OAM 协议报文被作为非法报文丢弃。

背景信息

请在链路两端设备上以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface interface-type interface-number**，进入链路两端接口的接口视图。

步骤 3 执行命令 **efm packet max-size size**，配置 EFM OAM 协议报文的最大尺寸。

缺省情况下，接口的 EFM OAM 协议报文的最大尺寸是 128 字节。

如果将链路两端接口的 EFM OAM 协议报文最大尺寸参数配置为不同的值，两端接口在发现阶段通过协商确定此参数值。协商的结果是取配置值较小的一端的配置值。

----结束

8.2.5 （可选）配置 EFM OAM 协议报文接收超时时间

需要调整 EFM OAM 连通性故障检测所需时间时，可以配置 EFM AOM 协议报文接收超时时间。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface interface-type interface-number**，进入链路两端接口的接口视图。

步骤 3 执行命令 **efm timeout timeout-value**，配置 EFM 协议报文接收超时时间。

缺省情况下，接口的 EFM OAM 协议报文接收超时时间是 5000ms。

链路两端接口的 EFM 协议报文接收超时时间必须配置成相同值，否则可能导致会话无法协商成功，或者出现会话震荡。

 说明

只有在全局使能 EFM OAM 功能后，接口使能 EFM OAM 功能之前，配置接口接收 EFM OAM 协议报文的超时时间。

----结束

8.2.6 使能接口的 EFM OAM 功能

只有使能两端端口的 EFM OAM 功能后，才开始点到点的 EFM 链路检测。

背景信息

请在链路两端设备上以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface interface-type interface-number**，进入链路两端接口的接口视图。

步骤 3 执行命令 **efm enable**，使能接口的 EFM OAM 功能。

缺省情况下，接口的 EFM OAM 功能处于禁止状态。

----结束

8.2.7 检查配置结果

通过查看 EFM OAM 配置信息等内容，来检查配置是否成功。

前提条件

已经完成 EFM OAM 基本功能的所有配置。

操作步骤

- 使用 **display efm { all | interface interface-type interface-number }** 命令查看接口的 EFM OAM 配置信息。
- 使用 **display efm session { all | interface interface-type interface-number }** 命令查看接口的 EFM OAM 协议状态。

----结束

任务示例

执行命令 **display efm**，可以查看本端接口的所有 EFM OAM 配置和对端接口的部分 EFM OAM 配置。

```
<HUAWEI> display efm interface gigabitethernet2/0/1
```

Item	Value
Interface:	GigabitEthernet2/0/1
EFM Enable Flag:	enable
Mode:	active
OAMPDU MaxSize:	128
OAMPDU Timeout:	3000
ErrCodeNotification:	disable
ErrCodePeriod:	1
ErrCodeThreshold:	1
ErrFrameNotification:	disable
ErrFramePeriod:	1
ErrFrameThreshold:	1
ErrFrameSecondNotification:	disable
ErrFrameSecondPeriod:	60
ErrFrameSecondThreshold:	1
Hold Up Time:	0
ThresholdEvtTriggerErrDown:	disable
TriggerIfDown:	disable
TriggerMacRenew:	disable
Remote MAC:	00e0-fc7f-724f
Remote EFM Enable Flag:	enable
Remote Mode:	passive
Remote MaxSize:	128
Remote State:	--

如果配置正确，两端接口成功协商后进入握手阶段，此时执行 **display efm session** 命令，可看到接口的 EFM OAM 协议状态为 **detect**。

```
<HUAWEI> display efm session interface gigabitethernet2/0/1
Interface           EFM State           Loopback Timeout
-----
GigabitEthernet2/0/1  detect              --
```

8.3 配置 EFM OAM 链路监控

通过配置 EFM OAM 误帧、误码和误帧秒检测，能够更好的检测和发现链路层的故障。

8.3.1 建立配置任务

在配置 EFM OAM 链路监控功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

链路监控用于在各种情况下检测和发现链路层的故障。链路监控使用事件通知的 OAMPDU，当链路故障发生时，本地链路监控到故障后通过事件的方式通知远端的 OAM 实体。

前置任务

在配置 EFM OAM 链路监控之前，需完成以下任务：

- **配置 EFM OAM 基本功能**

数据准备

在配置 EFM OAM 链路监控之前，需要准备以下数据。

序号	数据
1	（可选）EFM OAM 误帧检测观察时长、阈值
2	（可选）EFM OAM 误码检测观察时长、阈值
3	（可选）EFM OAM 误帧秒检测观察时长、阈值

8.3.2 （可选）配置 EFM OAM 误帧检测

误帧是指 1 秒钟内错误的帧数。当 EFM OAM 误帧检测上报功能使能后，如果在设置的观察时长内，接口检测到的误帧数量达到或者超过门限值，那么设备将产生误帧超限事件，并通告对端设备。

背景信息

请在链路一端或两端设备上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **interface interface-type interface-number**，进入链路两端接口的接口视图。
- 步骤 3** 执行命令 **efm error-frame period period**，配置接口的 EFM OAM 误帧检测观察时长。
- 缺省情况下，接口的 EFM OAM 误帧检测观察时长是 1 秒。
- 步骤 4** 执行命令 **efm error-frame threshold threshold**，配置接口的 EFM OAM 误帧检测门限。
- 缺省情况下，接口的 EFM OAM 误帧检测门限是 1。
- 步骤 5** 执行命令 **efm error-frame notification enable**，使能接口的 EFM OAM 误帧检测上报功能。
- 缺省情况下，接口的 EFM OAM 误帧检测上报功能处于禁止状态。
- 结束

8.3.3 （可选）配置 EFM OAM 误码检测

误码是指 1 秒钟内错误的编码数。当 EFM OAM 误码检测上报功能使能后，如果在设置的观察时长内，接口检测到的误码数量达到或者超过门限值，那么设备将产生误码超限事件，并通告对端设备。

背景信息

请在链路一端或两端设备上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **interface interface-type interface-number**，进入链路两端接口的接口视图。
- 步骤 3** 执行命令 **efm error-code period period**，配置接口的 EFM OAM 误码检测观察时长。
- 缺省情况下，接口的 EFM OAM 误码检测观察时长是 1 秒。
- 步骤 4** 执行命令 **efm error-code threshold threshold**，配置接口的 EFM OAM 误码检测门限。
- 缺省情况下，接口的 EFM OAM 误码检测门限是 1。
- 步骤 5** 执行命令 **efm error-code notification enable**，使能接口的 EFM OAM 误码检测上报功能。
- 缺省情况下，接口的 EFM OAM 误码检测上报功能处于禁止状态。
- 结束

8.3.4 （可选）配置 EFM OAM 误帧秒检测

当 EFM OAM 误帧秒检测上报功能使能后，如果在设置的观察时长内，接口检测到的误帧秒数量达到或者超过门限值，那么设备将产生误帧秒超限事件，并通告对端设备。

背景信息

误帧秒是指将设定的观察时长划分为若干个以 1 秒为单位的时间段，如果在某个时间段内检测到了至少一个误帧，则该时间段称为一个误帧秒。即指定 M 秒数下有错误帧的时间数。

请在链路一端或两端设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface interface-type interface-number**，进入链路两端接口的接口视图。

步骤 3 执行命令 **efm error-frame-second period period**，配置接口的 EFM OAM 误帧秒检测观察时长。

缺省情况下，接口的 EFM OAM 误帧秒检测观察时长是 60 秒。

步骤 4 执行命令 **efm error-frame-second threshold threshold**，配置接口的 EFM OAM 误帧秒检测门限。

缺省情况下，接口的 EFM OAM 误帧秒检测门限是 1。

步骤 5 执行命令 **efm error-frame-second notification enable**，使能接口的 EFM OAM 误帧秒检测上报功能。

缺省情况下，接口的 EFM OAM 误帧秒检测上报功能处于禁止状态。

----结束

8.3.5 检查配置结果

通过查看 EFM OAM 配置信息等内容，来检查配置是否成功。

前提条件

已经完成 EFM OAM 链路监控功能的所有配置。

操作步骤

- 使用 **display efm { all | interface interface-type interface-number }** 命令查看接口的 EFM OAM 配置信息。
- 使用 **display efm session { all | interface interface-type interface-number }** 命令查看接口的 EFM OAM 协议状态。

----结束

任务示例

执行命令 **display efm**，可以查看接口的 EFM OAM 链路监控配置。

```
<HUAWEI> display efm interface gigabitethernet1/0/0
  Item                               Value
-----
Interface:                           GigabitEthernet1/0/0
EFM Enable Flag:                       enable
Mode:                                  active
```

```
OAM PDU MaxSize: 128
OAM PDU Timeout: 3000
ErrCodeNotification: enable
ErrCodePeriod: 1
ErrCodeThreshold: 1
ErrFrameNotification: enable
ErrFramePeriod: 1
ErrFrameThreshold: 1
ErrFrameSecondNotification: enable
ErrFrameSecondPeriod: 60
ErrFrameSecondThreshold: 1
Hold Up Time: 0
ThresholdEvtTriggerErrDown: enable
TriggerIfDown: disable
TriggerMacRenew: disable
RemoteMAC: 00e0-fc7f-7258
Remote EFM Enable Flag: enable
Remote Mode: passive
Remote MaxSize: 128
Remote State: --
```

8.4 配置物理链路丢包率检测

可以检测物理链路的丢包率，以使用户能够采取有效的措施来保证链路更好的工作。

8.4.1 建立配置任务

在配置物理链路丢包率检测功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

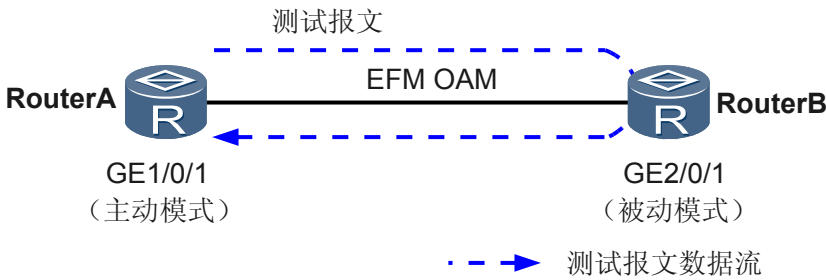


EFM OAM 远端环回影响业务数据的正常转发，请在不需转发业务数据的链路上配置。

当需要检测某段链路的丢包率时，可执行本配置任务。

例如：如图 8-4 所示，在 RouterA 和 RouterB 之间配置 EFM OAM，在 RouterA 的接口 GE1/0/1 上配置远端环回。然后从 RouterA 向 RouterB 发送测试报文，在 RouterA 上观察测试报文的返回情况，从而得到链路的丢包率。

图 8-4 测试链路丢包率



前置任务

在测试链路丢包率之前，需完成以下任务：

- [配置 EFM OAM 基本功能](#)

数据准备

在测试链路丢包率之前，需要准备以下数据。

序号	数据
1	远端环回的超时时间
2	测试报文的目的 MAC 地址、所属 VLAN、测试报文的出接口、测试报文的大小、数量、发送速率

8.4.2 配置 EFM OAM 远端环回

EFM OAM 远端环回可用来定位远端故障和测试链路质量。

背景信息

EFM OAM 远端环回功能为用户提供了一种测试链路性能的手段，其具体的实现过程为

1. 主动模式下的 OAM 实体向对端设备发起远端环回请求。
2. 手动或者自动取消发起端设备的远端环回功能。

操作步骤

步骤 1 请在主动模式的发起端设备上配置远端环回请求功能。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface interface-type interface-number**，进入接口视图。
3. 执行命令 **efm loopback start [timeout timeout]**，配置接口发起 EFM OAM 远端环回。

缺省情况下，远端环回的超时时间是 20 分钟。到达此时间，远端环回自动取消。如果需要使某链路一直处于远端环回状态，可将超时时间设置为 0。

只有在两端的 EFM OAM 协议处于 detect 状态，本端的 EFM OAM 工作模式为主动模式时，远端环回才能成功进行。可使用 **display efm session** 命令查询本端和对端之间 EFM OAM 协议是否处于 detect 状态。

4. 执行命令 **efm loopback action discard**，配置接口丢弃返回的报文。

缺省情况下，接口丢弃返回的报文。

----结束

8.4.3 发送测试报文

发送的测试报文是为测试链路的丢包率构造的一种以太类型的报文。它可与 EFM OAM 远端环回功能配合使用，来测试链路的丢包率。

背景信息

在链路两端设备当中主动模式接口所在设备上以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **test-packet start** [**mac** *mac-address*] [**vlan** *vlan-id*] { **interface** *interface-type interface-number* | **service-instance** *instance-name* } [**-c** *count* | **-p** *speed* | **-s** *size*] *，发送测试报文。

缺省情况下，测试报文的大小是 64 字节，发送速率是 1Mbit/s，发送数量是 5 个。

测试报文的出接口应配置为连接被测链路的接口。

----结束

后续处理

在发送测试报文进行过程中，不能修改发送测试报文的参数。

如需终止发送测试报文，可按<Ctrl+C>快捷键。

8.4.4 查看测试报文的返回统计

通过查看测试报文的返回统计来计算链路的丢包率。

背景信息

在链路两端设备当中主动模式接口所在设备上以下配置。

操作步骤

步骤 1 执行命令 **display test-packet result**，查看测试报文的返回统计。

display test-packet result 命令的显示信息包括：

- 发送测试报文的个数
- 接收报文的个数
- 丢弃报文的个数
- 发送报文的总字节数
- 接收报文的总字节数
- 丢弃报文的总字节数
- 发送开始时间
- 发送结束时间

根据以上数据可计算链路的丢包率。

----结束

8.4.5 （可选）手动取消 EFM OAM 远端环回

EFM OAM 远端环回既可以超时自动取消也可以手动取消。

背景信息

在链路两端设备当中主动模式接口所在设备上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **interface interface-type interface-number**，进入接口视图。
- 步骤 3** 执行命令 **efm loopback stop**，配置接口取消 EFM OAM 远端环回。

为避免由于用户忘记停止 EFM OAM 远端环回而造成链路长时间无法正常转发业务数据，NE80E/40E 设备的 EFM OAM 远端环回具有超时自动取消功能。缺省情况下，远端环回的超时时间是 20 分钟，到达此时间，远端环回自动取消。如果需要手工取消远端环回，可执行以上配置步骤。

----结束

8.4.6 检查配置结果

通过查看远端环回状态等内容，来检查配置是否成功。

前提条件

已经完成物理链路丢包率检测功能的所有配置。

操作步骤

- 步骤 1** **display efm session { all | interface interface-type interface-number }** 命令查看接口的 EFM OAM 协议状态。

----结束

任务示例

配置 EFM OAM 远端环回成功后，在链路两端设备当中主动模式接口所在设备上执行 **display efm session** 命令，可以看到主动模式接口的 EFM OAM 协议状态为 Loopback (control)，即远端环回状态（且为远端环回的发起方）。

```
<RouterA> display efm session interface gigabitethernet 1/0/1
  Interface          EFM State          Loopback Timeout
  -----
  GigabitEthernet1/0/1    Loopback(control)    20
```

配置 EFM OAM 远端环回成功后，在链路两端设备当中被动模式接口所在设备上执行 **display efm session** 命令，可以看到被动模式接口的 EFM OAM 协议状态为 Loopback(be controlled)，即远端环回状态（且为远端环回的响应方）。

```
<RouterB> display efm session interface gigabitethernet 2/0/1
  Interface          EFM State          Loopback Timeout
  -----
  GigabitEthernet2/0/8    Loopback(be controlled)  --
```

在远端环回自动取消或手动取消后，在链路两端中任一端设备上执行 **display efm session** 命令，可以看到链路两端接口的 EFM OAM 协议状态为 Detect 或 Discovery，即握手状态或对端发现状态。

```
<RouterA> display efm session interface gigabitethernet 1/0/1
```

Interface	EFM State	Loopback Timeout
GigabitEthernet2/0/8	detect	--

8.5 配置 EFM OAM 和接口联动

一旦 EFM OAM 和接口联动后，可能对业务产生很大影响，例如二三层业务全部被阻塞。

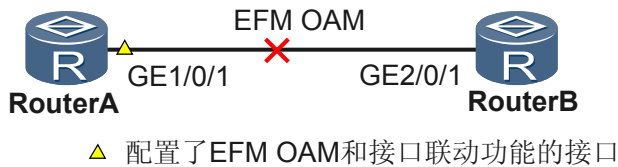
8.5.1 建立配置任务

在配置 EFM OAM 和接口联动功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 8-5 所示，两台设备之间配置了 EFM OAM 功能，并配置了 EFM OAM 和 RouterA 的接口 GE1/0/1 联动。在 RouterA 上，当 EFM OAM 模块检测到和 RouterB 之间有连通性故障时，接口 GE1/0/1 下除 EFM 协议报文外的所有其他报文都无法被转发，二三层业务将全部被阻塞。因此，一旦启用 EFM OAM 和当前接口联动功能，将可能对业务产生很大影响。如果当前接口通过 EFM OAM 检测到链路连通性故障恢复，则恢复该接口的所有转发报文，并通知该接口上的所有二三层业务作相应处理。

图 8-5 EFM OAM 和接口联动示意图



前置任务

在配置 EFM OAM 和接口联动之前，需完成以下任务：

- **配置 EFM OAM 基本功能**

数据准备

在配置 EFM OAM 和接口联动前，需要准备以下数据。

序号	数据
1	接口的类型和编号
2	（可选）故障状态的保持时间

8.5.2 配置 EFM OAM 和接口联动

通过在物理端口上绑定 EFM OAM，实现当 EFM OAM 检测到故障后，OAM Manager 管理模块通知与其绑定的接口管理模块做故障处理。

背景信息

使能 EFM OAM 和接口联动功能后，当该接口收到携带链路故障状态标记的 OAM PDU 控制请求报文时，就调整其接口状态。

在链路一端或两端设备上进行以下配置。

操作步骤

- 错误事件和接口联动：阻塞端口

阻塞端口：指除了 EFM 协议报文外，其他流量全部中断，适用于存在主备链路的网络中，链路故障恢复后，系统可自动回切的场景。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface interface-type interface-number**，进入链路一端接口的接口视图。
3. 执行命令 **efm trigger if-down**，配置 EFM OAM 和接口联动。

缺省情况下，接口不和 EFM OAM 联动。

当前接口必须已使用 **efm enable** 命令使能了 EFM OAM。

如果使能了 EFM OAM 和当前接口联动功能，当 EFM OAM 检测到链路连通性故障后，接口下除 EFM 协议报文外的所有其他报文都无法被转发，二三层业务将全部被阻塞。因此，一旦启用 EFM OAM 和当前接口联动功能，将可能对业务产生很大影响。如果当前接口通过 EFM OAM 检测到链路连通性故障恢复，则恢复该接口的所有转发报文，并通知该接口上的所有二三层业务作相应处理。

此外，请务必确保两端 EFM OAM 协议状态变为 detect 之后再配置 EFM OAM 和当前接口联动功能。

如果由于人为误操作导致二三层业务被阻塞，可通过在接口视图下执行命令 **undo efm trigger if-down** 恢复业务。

----结束

8.5.3 检查配置结果

通过查看 TriggerIfDown 等内容，来检查配置是否成功。

前提条件

已经完成 EFM OAM 和接口联动功能的所有配置。

操作步骤

- 步骤 1** 使用 **display efm { all | interface interface-type interface-number }** 命令查看接口的 EFM OAM 配置信息。

----结束

任务示例

如果接口和 EFM OAM 联动功能配置成功，执行 **display efm** 命令，可以看到 TriggerIfDown 项目的值为 enable。

```
<HUAWEI> display efm interface gigabitethernet 1/0/1
Item                                     Value
-----
Interface:                             GigabitEthernet1/0/1
EFM Enable Flag:                         enable
Mode:                                    active

OAMPDU MaxSize:                         128
OAMPDU Timeout:                         3000
ErrCodeNotification:                    disable
ErrCodePeriod:                          1
ErrCodeThreshold:                       1
ErrFrameNotification:                    disable
ErrFramePeriod:                          1
ErrFrameThreshold:                       1
ErrFrameSecondNotification:              disable
ErrFrameSecondPeriod:                    60
ErrFrameSecondThreshold:                  1
Hold Up Time:                            0
ThresholdEvtTriggerErrDown:              enable
TriggerIfDown:                           enable
TriggerMacRenew:                         disable
Remote MAC:                              0018-8200-0001
Remote EFM Enable Flag:                  enable
Remote Mode:                             passive
Remote MaxSize:                          128

Remote State:                            --
```

8.6 配置以太网 CFM 基本功能

通过配置以太网 CFM 基本功能，实现端到端的连通性故障检测、故障通告、故障判定和故障定位功能。

8.6.1 建立配置任务

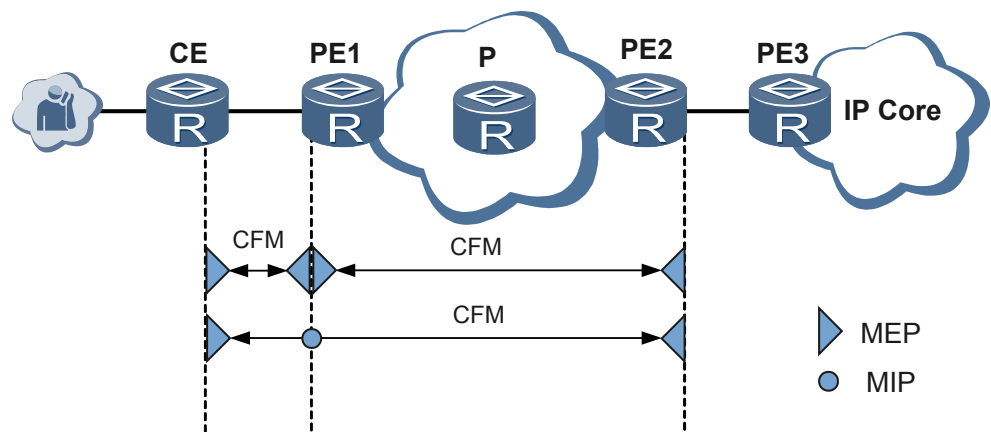
在配置以太网 CFM 基本功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

CFM 主要用于检测端到端链路或者直连链路的连通性。

如图 8-6 所示，可以在二层网络中部署 CFM 检测 CE 到 PE1 之间链路、PE1 到 PE2 之间网络或者 CE 到 PE2 之间链路的连通性。

图 8-6 CFM 基本功能示意图



如果需要在以太网中实现端到端的连通性自动检测功能，在执行本配置任务前需先进行以下规划工作：

- 根据网络设备所属的 ISP（Internet Service Provider）划分 MD，把由相同 ISP 管理的所有具备以太网 CFM 功能的设备划分在同一个 MD 内。
每台设备上可配置一个默认 MD，用于高级别 CCM 报文穿越，创建 MIP 节点回复 LTR 报文。
- 根据业务实例划分 MA。每个 MA 关联一个 VLAN。通常一个 VLAN 对应一个业务实例。通过划分 MA 可实现对传输某个业务实例的网络的连通性故障检测。
- 确定哪些设备的哪些接口位于 MA 的边缘位置，即需要在哪些设备的哪些接口上配置 MEP。

在直连链路上实现连通性自动检测功能时：

- 应将两端设备配置在同一个 MD 的同一个 MA 中；
- MA 可以关联 VLAN 也可以不关联 VLAN；
- MEP 应配置在直连链路两端的接口上。

前置任务

无

数据准备

在配置以太网 CFM 基本功能之前，需要准备以下数据。

序号	数据
1	MD 的名称和级别
2	（可选）默认 MD 的名称和级别
3	MA 的名称、MA 关联的 VLAN 的 ID
4	MEP 的 ID、MEP 所在接口的名称、MEP 的类型
5	（可选）RMEP 的 ID、RMEP 所在接口的 MAC 地址

序号	数据
6	MIP 的生成规则
7	MA 内 MEP 发送或探测 CCM 消息的时间间隔
8	(可选) 指定 VLAN ID

8.6.2 切换版本

802.1ag 协议分为 draft7 草案版本和 standard2007 标准版本，设备可以在这 2 个版本之间进行切换。

背景信息

缺省情况下，设备启用的是 802.1ag 协议 draft7 草案版本。如果需要使用 standard2007 标准版本，在所有需要切换版本的 NE80E/40E 设备上以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm version { draft7 | standard }**，切换版本。

 说明

整网中的设备使用的版本必须一致，要么都是 draft7 草案版本要么都是 standard2007 标准版本，两个版本不能混用。

----结束

8.6.3 全局使能以太网 CFM 功能

全局使能以太网 CFM 功能是配置和使用所有 CFM 功能的前提条件。

背景信息

在所有需要实施以太网 CFM 管理的 NE80E/40E 设备上以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm enable**，全局使能以太网 CFM 功能。

缺省情况下，NE80E/40E 设备的 CFM 功能处于全局禁止状态。

----结束

8.6.4 创建 MD

MD 是指对其实施以太网 CFM 管理的一个网络或一个网络的一部分，一个 MD 由一个统一的 ISP 进行管理。

背景信息

在所有需要实施以太网 CFM 管理的 NE80E/40E 设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md md-name [format { no-md-name | dns dns-md-format-name | mac-address mac-md-format-name | string string-md-format-name }] [level level]**，创建 MD 并进入 MD 视图。

缺省情况下，MD 的级别是 0，即最低级别。

参数 **format**、**no-md-name**、**dns dns-md-format-name**、**mac-address mac-md-format-name** 和 **string string-md-format-name** 仅在 802.1ag 标准版本中支持。

如果需要创建多个 MD，请重复执行步骤 2。一台设备最多可创建 64 个 MD。

 说明

低级别 MD 的 802.1ag 协议报文进入高级别的 MD 或级别相同的后被丢弃，高级别 MD 的 802.1ag 协议报文可以穿越低级别的 MD。

----结束

8.6.5 （可选）创建默认 MD

默认 MD 的级别必须高于本设备配置 MEP 节点所有 MD 的级别，和高优先级 MD 的级别相等，用于高级别 CCM 报文穿越，

背景信息

在所有需要实施以太网 CFM 管理的 NE80E/40E 设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm default md [level level]**，创建默认 MD 并进入默认 MD 视图。

缺省情况下，默认 MD 的级别是 7，即最高级别。

每台设备上只能创建一个默认 MD。

 说明

默认 MD 的级别必须高于本设备配置 MEP 节点所有 MD 的级别，和高优先级 MD 的级别相等，用于高级别 CCM 报文穿越，创建 MIP 节点回复 LTR 报文。

----结束

8.6.6 创建 MA

一个 MD 可以划分成一个或多个 MA。以太网 CFM 对每个 MA 分别进行连通性故障检测。

背景信息

在所有需要实施以太网 CFM 管理的 NE80E/40E 设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md md-name**，进入 MD 视图。

步骤 3 执行命令 **ma ma-name [format { icc-based iccbased-ma-format-name | string ma-format-name }]**，创建 MA 并进入 MA 视图。

同一个 MD 内，最多可创建 4k 个 MA。一台 NE80E/40E 设备上，最多可创建 4k 个 MA。

一个或多个 MA 可对应一个 VLAN。

步骤 4（可选）执行命令 **map vlan vlan-id**，配置 MA 关联 VLAN。

 说明

- 缺省情况下，MA 未和任何 VLAN 建立关联关系。
- 以太网 CFM 对每个 MA 分别进行连通性故障检测。配置某个 MA 和 1 个 VLAN 关联，可实现对该 VLAN 内的网络的连通性故障检测。
- 如果某 MA 用于两个直连设备之间的连通性故障检测，则该 MA 可以不关联 VLAN，否则该 MA 应关联 VLAN。

----结束

8.6.7 创建 MEP

MEP 是 MA 的边缘节点，它位于设备的接口上，需要手工创建。

背景信息

在 MA 内创建 MEP 时，对该 MA 是否关联 VLAN 和 MEP 所在接口的配置要求如下：

- 在创建 inward 型的 MEP 时，要求该 MA 必须已经关联了 VLAN，且指定的 MEP 所在接口必须已经加入该 VLAN。inward 型 MEP 发出的 802.1ag 协议报文通过当前 MA 关联 VLAN 内的所有接口（除 MEP 所在接口）向外发送，即在当前 MA 关联的 VLAN 内广播。
- 在创建 outward 型的 MEP 时，不要求该 MA 必须关联 VLAN，但是如果该 MA 已经关联了 VLAN，则指定的 MEP 所在接口必须已经加入该 VLAN。outward 型 MEP 发出的协议报文直接通过该 MEP 所在的接口向外发送。
- 在创建 VLAN 类型的 MEP 时，要求该 MA 必须已经关联了 VLAN。

在同一台设备的同一个 MA 内，对创建 MEP 的数量和类型要求如下：

- VLAN 型 MEP 和接口型 MEP 不能同时存在，inward 接口型 MEP 和 outward 接口型 MEP 不能同时存在。
- 只能创建 1 个 outward 接口型 MEP，可以创建多个 inward 接口型 MEP，但是同一个接口上只能创建 1 个 inward 接口型 MEP。
- 只能创建 1 个 VLAN 型的 MEP。



注意

- 一个 Trunk 上只支持配置一个 MEP，Trunk 上存在多个子接口也只能配置一个 MEP。
- 设备在运行过程中，不支持热插拔。

在所有 MA 的所有边缘设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md md-name**，进入 MD 视图。

步骤 3 执行命令 **ma ma-name**，进入 MA 视图。

步骤 4 执行以下命令创建 MEP。

- **mep mep-id mep-id interface** { *interface-type interface-number* | *interface-type interface-number.subnumber* } [**vlan vlan-id**] { **inward** | **outward** } 命令形式用来创建接口型 MEP。
- **mep mep-id mep-id vlan** 命令形式用来创建 VLAN 型 MEP。



说明
在 NE80E/40E 设备上，目前 VLAN 型 MEP 只用于组播 VLAN 的连通性故障检测，在其它连通性故障检测应用场景均需使用接口型 MEP。

----结束

后续处理

如需：

- 在同 1 个 MA 内创建多个 MEP，请重复执行步骤 4。
- 在多个 MA 内创建 MEP，请重复执行步骤 3 ~ 步骤 4。
- 在多个 MD 内创建 MEP，请重复执行步骤 2 ~ 步骤 4。

8.6.8 配置 RMEP

同一个 MA 内，其它设备上的 MEP 对本设备而言称为 RMEP。通过配置 RMEP，在同一个 MA 内实现和某个 RMEP 的连通性故障检测。

背景信息

如果需要检测本设备到某 RMEP 的连通性，则首先需要在本设备上配置该 RMEP。

在所有 MA 的所有边缘设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md md-name**，进入 MD 视图。

步骤 3 执行命令 **ma ma-name**，进入 MA 视图。

步骤 4 执行命令 **remote-mep mep-id mep-id [mac mac-address]**，配置当前 MA 内的 RMEP。

----结束

后续处理

如需：

- 在同 1 个 MA 内配置多个 RMEP，请重复执行步骤 4。
- 在多个 MA 内配置 RMEP，请重复执行步骤 2 ~ 步骤 4。
- 在多个 MD 内配置 RMEP，请重复执行步骤 3 ~ 步骤 4。

8.6.9（可选）配置 MIP 生成规则

MIP 是 MA 的内部节点。各个 MEP 定期以组播的方式发送 CCM 报文。为了确定故障的位置，需要用 MIP 节点来定位。

背景信息

如今，802.1ag 协议分为 draft7 草案版本和 standard2007 标准版本，两个版本的 MIP 节点创建规则一样，但不同的是：

- draft7 版本中，MIP 节点是基于接口按创建规则自动生成。
- standard 版本中，MIP 节点是基于 MD 或默认 MD 按创建规则自动生成。

在所有需要实施以太网 CFM 管理的 NE80E/40E 设备上以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 配置 MIP 生成规则

以下两个版本 MIP 配置规则，任选其一，不可以同时配置。

- 配置 draft7 草案中的 MIP 生成规则。

执行命令 **mip create-type { default | explicit | none } [interface interface-type interface-number]**，配置 draft7 草案中 MIP 生成规则。

- 配置 standard2007 标准版本中的 MIP 生成规则。

1. 执行命令 **cfm md md-name**，进入 MD 视图。

或者，执行命令 **cfm default md [level level]**，进入默认 MD 视图。

两种视图任选其一即可。

2. 执行命令 **mip create-type { default | explicit | none }**，配置 standard2007 标准版本中 MIP 生成规则。

缺省情况下，MIP 生成规则为 **none**。如果为：

- **default**：如果在指定 MD 或默认 MD 所属端口没有更高级别的 MEP，并且没有更低级别的 MIP，则可以在指定端口创建 MIP 节点。

- **explicit**: 如果在指定 MD 或默认 MD 所属端口没有更低级的 MEP 节点, 则不能创建 MIP; 如果指定 MD 或默认 MD 所属端口没有更高级别的 MEP, 并且没有更低级别的 MIP, 则可以创建 MIP 节点。
- **none**: 在指定 MD 或默认 MD 所属端口上不能创建 MIP 节点。

配置了 MIP 的生成规则为 **default** 类型或 **explicit** 类型后, 设备会根据规则自动创建 MIP。

MIP 的级别由生成规则以及生成其的 MD 的级别决定。

----结束

8.6.10 配置 CC 检测

通过配置 CC 检测, 实现以太网 CFM 通过 MEP 之间定期发送 CCM 来检测各 MEP 之间的连通性。

背景信息

在所有 MA 的所有边缘设备 (即 MEP 所在设备) 上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**, 进入系统视图。

步骤 2 执行命令 **cfm md md-name**, 进入 MD 视图。

步骤 3 执行命令 **ma ma-name**, 进入 MA 视图。

步骤 4 执行命令 **ccm-interval interval**, 配置本设备上当前 MA 内 MEP 发送或探测 CCM 消息的时间间隔。

缺省情况下, MA 内 MEP 发送或探测 CCM 消息的时间间隔是 1 秒。

如果某 MA 内:

- 已使用 **mep ccm-send enable** 命令使能了 CCM 消息发送功能
- 或已使用 **remote-mep ccm-receive enable** 命令使能了 CCM 消息接收功能

则不允许修改该 MA 内发送或探测 CCM 消息的时间间隔。如要修改, 需先使用对应的 **undo** 命令禁止以上功能。

步骤 5 执行命令 **mep ccm-send [mep-id mep-id] enable**, 使能 MEP 的 CCM 消息发送功能。

缺省情况下, MEP 的 CCM 消息发送功能处于禁止状态。

如果不指定 **mep-id mep-id** 参数, 则表示使能本设备上当前 MA 内所有 MEP 的 CCM 消息发送功能。

步骤 6 执行命令 **remote-mep ccm-receive [mep-id mep-id] enable**, 使能本设备上当前 MA 内本地 MEP 接收同一 MA 内的 RMEP 发送的 CCM 消息功能。

缺省情况下, 本地 MEP 不接收 RMEP 发送的 CCM 消息。

当在本端设备上使能了接收某个 RMEP 发送的 CCM 消息后, 如果通过 CC 探测发现本端与该 RMEP 之间出现连通性故障, 则本端设备上提示 RMEP 连通性告警。

如果不指定 **mep-id** *mep-id* 参数，则表示使能本设备当前 MA 内接收所有 RMEP 发送的 CCM 消息功能。

----结束

后续处理

如需：

- 在多个 MA 内配置 CC 检测，请重复执行步骤 3 ～步骤 6。
- 在多个 MD 内配置 CC 检测，请重复执行步骤 2 ～步骤 6。

8.6.11 （可选）创建指定 VLAN

通过将 VLAN 和默认 MD 相关联，指定 VLAN 内的所有接口将按照默认 MD 配置的 MIP 生成规则生成 MIP 节点。

背景信息

请在需要配置指定 VLAN 的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm default md** [*level level*]，创建默认 MD 并进入默认 MD 视图。

步骤 3 执行命令 **vlan** { *vlan-id1* [*to vlan-id2*] } <1-10>，创建指定 VLAN。

----结束

8.6.12 检查配置结果

通过查看 MD、MA、MEP 和 MIP 等内容，来检查配置是否成功。

前提条件

已经完成以太网 CFM 基本功能的所有配置。

操作步骤

- 使用 **display cfm md** [*md-name*] 命令查看 MD 的配置信息。
- 使用 **display cfm ma** [**md** *md-name*] [**ma** *ma-name*] 命令查看 MA 的详细信息。
- 使用 **display cfm mep** [**md** *md-name*] [**ma** *ma-name*] [**mep-id** *mep-id*] 命令查看 MEP 的详细信息。
- 使用 **display cfm remote-mep** [**md** *md-name*] [**ma** *ma-name*] [**mep-id** *mep-id*] 命令查看 RMEP 的详细信息。
- 使用 **display mip create-type** [**interface** *interface-type interface-number*] 命令查看 MIP 的创建规则。
- 使用 **display cfm mip** [**interface** *interface-type interface-number*] [**level** *level*] 命令查看 MIP 的信息。
- 使用 **display cfm default md** 命令查看默认 MD 的配置信息。

- 使用 **display cfm error-info** [interface interface-type interface-number] [vlan vlanid | vsi vsi-name] [error-type { ccm-interval-error | maid-error | mac-error | cfm-leak }] 命令查看符合指定条件的配置错误信息。
- 使用 **display cfm mp-info** [interface interface-type interface-number [level md-level] [inward | outward] [vlan vlanid | vsi vsi-name | no-associated-vlan]] 命令查看指定接口、VLAN 或 VSI 上的 CFM 管理对象的信息。
- 使用 **display oam global configuration** 命令查看以太网 CFM 的 MP 的 MAC 地址模式。

----结束

任务示例

不同的版本上，执行命令 **display cfm md**，显示信息是不一样的。

draft7 版本中，如果 MD 创建成功，执行命令 **display cfm md**，可以看到该 MD 和该 MD 的级别。

```
<HUAWEI> display cfm md
The total number of MDs is 2
MD-Name          Level
-----
md2               7
md3               3
```

standard2007 版本中，如果 MD 创建成功，执行命令 **display cfm md**，可以看到该 MD 的名称、MD 名称参数输入类型、MD 级别、MIP 生成规则和 Sender ID TLV 类型等信息。

```
<HUAWEI> display cfm md mdcustomer
The total number of MDs is : 1
-----
MD Name           : md
MD Name Format     : string
Level             : 0
MIP Create-type   : none
SenderID TLV-type : defer
MA list           :
    MA Name        : ma
    MA Name Format  : string
    Interval       : 1000
    Vlan ID        : 2
    VSI Name       : --
    L2VC ID        : --
```

如果 MA 创建成功，执行命令 **display cfm ma**，可以看到该 MA 的信息。

```
<HUAWEI> display cfm ma md md1
The total number of MAs is 2:
MD Name           : md1
MD Name Format     : string
Level             : 7
MIP Create-type   : none
SenderID TLV-type : Defer
MA Name           : mal
MA Name Format     : string
Interval          : 10ms
Priority           : 4
Vlan ID           : 7
VSI Name          : --
L2VC ID           : --
MEP Number        : 2
RMEP Number       : 3
Suppressing Alarms : No
```

```
Sending Ais Packet : No
MD Name           : md1
MD Name Format     : string
Level             : 7
MIP Create-type   : none
SenderID TLV-type : Defer
MA Name           : ma2
MA Name Format     : string
Interval          : 10ms
Priority           : 5
Vlan ID           : 8
VSI Name          : --
L2VC ID           : --
MEP Number        : 1
RMEP Number       : 4
Suppressing Alarms : No
Sending Ais Packet : No
```

如果 MEP 创建成功，执行命令 **display cfm mep**，可以看到该 MEP 的信息。

```
<HUAWEI> display cfm mep
The total number of MEPs is 2
MD Name           : md2
MD Name Format     : string
Level             : 7
MA Name           : ma3
MA Name Format     : string
MEP ID            : 40
Vlan ID           : 10
VSI Name          : --
Interface Name     : GigabitEthernet1/0/1
CCM Send          : enabled
Direction         : outward
MD Name           : md3
MD Name Format     : string
Level             : 3
MA Name           : ma1
MA Name Format     : string
MEP ID            : 100
Vlan ID           : 20
VSI Name          : --
Interface Name     : GigabitEthernet2/0/1
CCM Send          : enabled
Direction         : outward
```

如果 RMEP 配置成功，执行命令 **display cfm remote-mep**，可以看到该 RMEP 的信息。

```
<HUAWEI> display cfm remote-mep
The total number of RMEPs is 2
MD Name           : md2
Level             : 7
MA Name           : ma3
RMEP ID           : 110
Vlan ID           : 20
VSI Name          : --
MAC               : 0000-0121-0222
CCM Receive       : enabled
Trigger-If-Down   : disabled
CFM Status        : up
MD Name           : md2
Level             : 4
MA Name           : ma3
RMEP ID           : 30
Vlan ID           : --
VSI Name          : --
MAC               : --
CCM Receive       : enabled
Trigger-If-Down   : disabled
CFM Status        : up
```

执行命令 **display mip create-type**，可查看 MIP 的创建规则，验证 MIP 创建规则配置是否正确。

```
<HUAWEI> display mip create-type interface ethernet1/0/1
Interface Name      MIP Create-Type  MIP Create-Type On Interface
-----
GigabitEthernet1/0/1  none            --
```

执行命令 **display cfm mip**，可查看 MIP 的信息。

```
<HUAWEI> display cfm mip
Interface Name      Level      MAC
-----
GigabitEthernet2/0/8  0          0018-82e2-377f
```

执行 **display cfm default md** 命令，可以查看默认 MD 的级别、MIP 生成规则、Sender ID TLV 类型及关联了默认 MD 的 VLAN 列表。

```
<HUAWEI> display cfm default md
Level  MIP Create-type  SenderID TLV-type  VLAN List
-----
7      default        Defer              100 to 200 2049
```

执行 **display cfm error-info** 命令，可以查看符合指定条件的配置错误信息。

```
<HUAWEI> display cfm error-info interface gigabitethernet1/0/2 error-type cfm-leak
The total number of Errors is : 1
-----
Interface      : gigabitethernet1/0/2
VLAN ID       : 100
VSI Name      : --
Error Type    : ccm-interval-error cfm-leak
MD Name       : mdl
MA Name       : mal
Level        : 3
MEP ID       : 10
CCM-Interval  : 20
MAC Address   : 0018-8247-b977
```

执行 **display cfm mp-info** 命令，可以查看指定接口、VLAN 或 VSI 上的 CFM 管理对象的信息。

```
<HUAWEI> display cfm mp-info interface gigabitethernet 1/0/1 level 6 inward vlan 300
MD Name          : mdl
MD Name Format    : string
Level           : 6
MA Name          : mal
MEP ID           : 10
VLAN ID          : 300
VSI Name         : --
Interface Name   : gigabitethernet 1/0/1
CCM Send         : enable
Direction       : inward
MAC Address      : 0018-8247-b977
MEP Pe-vid      : --
MEP Ce-vid      : --
MEP Vid         : --
Alarm Status     : none
```

执行 **display oam global configuration** 命令，可以查看以太网 CFM 的 MP 的 MAC 地址模式。

```
<HUAWEI> display oam global configuration
global conf      value
-----
cfm status       enabled
ping mac status  disabled
trace mac status disabled
cfm mac-tunnel mip trace status disabled
```

efm status	disabled
cfm protocol	standard
cfm mp-address-model	individual

8.7 配置以太网 CFM 的相关参数

通过对以太网 CFM 的相关参数进行调整，在以太网中更好的实现端到端的连通性故障检测。

8.7.1 建立配置任务

在配置以太网 CFM 相关参数之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如果在以太网中已经启动故障连通性检测功能，可以对相关检测参数进行调整。根据应用环境的不同，可以选择以下参数进行调整：

- RMEP 激活时间

当在本端设备上使能接收某个 RMEP 发送的 CCM 消息功能后，

- 如果通过 CC 探测发现本端 MEP 与该 RMEP 之间出现连通性故障，则本端设备上提示 RMEP 连通性告警。
- 如果本端 MEP 与 RMEP 之间物理连通正常，但是由于对端设备没有及时配置 MEP 或者 MEP 配置延后，此时进行 CC 探测，若本端 MEP 连续 3 个 CCM 发送周期没有接收到远端 MEP 发送的 CCM 消息，则认为和远端 MEP 之间发生了连通性故障，在本端设备上提示 RMEP 连通性告警。

可以看出，此告警为误告警。为了解决这个问题，提出了 RMEP 激活时间这个概念。

若设备配置了 RMEP 激活时间，当在本端设备上使能接收某个 RMEP 发送的 CCM 消息功能后，等待配置的 RMEP 激活时间到达后，本端设备开始接收 CCM 报文。也就是说 RMEP 激活时间是预留给用户对远端 MEP 配置的时间。

如果配置的 RMEP 激活时间到达后，本端设备上的 MEP 连续 3 个 CCM 周期内没有收到 CCM 报文，则认为 MEP 之间发生了连通性故障，本端设备上才提示 RMEP 连通性告警。

- 告警产生和恢复的防抖时间

对于每个 MA 下的所有 RMEP 有两个定时器，分别是：

- 一个是告警产生定时器，周期是用户配置的告警产生防抖时间；
- 另一个是告警恢复定时器，周期是用户配置的告警恢复防抖时间。

当 RMEP 检测到告警时，告警定时器开始启动，等到定时器的时间到，上报告警；当每 RMEP 检测到告警恢复时，告警恢复定时器开始启动，等到定时器时间到，上报告警恢复。

如果 RMEP 频繁的检测到告警和告警恢复信号，那么就会产生告警振荡。

通过配置告警产生和恢复的防抖时间可以抑制告警振荡。

- 指定 VLAN 或 VLAN 链表

指定 VLAN 内的所有接口将按照默认 MD 配置的 MIP 生成规则生成 MIP 节点。

前置任务

无

数据准备

在配置以太网 CFM 检测参数之前，需要准备以下数据。

序号	数据
1	(可选) RMEP 激活时间
2	(可选) 告警恢复的防抖时间
3	(可选) 告警产生的防抖时间

8.7.2 (可选) 配置 RMEP 激活时间

RMEP 激活时间是预留给用户对远端 MEP 配置的时间。通过配置 RMEP 的激活时间，实现在配置的 RMEP 激活时间到达后，本端设备开始接收 CCM 报文。

背景信息

在所有 MA 的所有边缘设备上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **cfm md md-name**，进入 MD 视图。
- 步骤 3** 执行命令 **ma ma-name**，进入 MA 视图。
- 步骤 4** 执行命令 **active time time**，配置 RMEP 激活时间。
- 结束

8.7.3 (可选) 配置告警恢复防抖时间

通过配置告警恢复防抖时间可以抑制告警振荡。

背景信息

请在需要配置告警恢复防抖时间的设备上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **cfm md md-name**，进入 MD 视图。
- 步骤 3** 执行命令 **ma ma-name**，进入 MA 视图。

步骤 4 执行命令 **alarm finish time** *time*，配置告警恢复防抖时间。

----结束

8.7.4 （可选）配置告警产生防抖时间

通过配置告警产生防抖时间可以抑制告警振荡。

背景信息

请在需要配置告警产生的防抖时间的设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md** *md-name*，进入 MD 视图。

步骤 3 执行命令 **ma** *ma-name*，进入 MA 视图。

步骤 4 执行命令 **alarm occur time** *time*，配置告警产生的防抖时间。

----结束

8.8 配置以太网的故障确认

通过发送测试报文和接收应答报文来检测两台设备之间链路的连通性。

8.8.1 建立配置任务

在配置以太网的故障确认之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用场景

当需要手动检测两台设备之间链路的连通性时，可通过发送测试报文和接收应答报文来检测从本设备到目的设备是否可达。根据被测链路的类型，可分为以下三种场景：

- 当需要在配置了 MD、MA、MEP 的网络中，检测同一 MA 内的 MEP 之间或 MEP 和 MIP 之间的连通性时，可执行 802.1ag MAC Ping。
- 当需要在未配置 MD、MA、MEP 的网络中，检测两台设备之间的连通性时，可执行通用 Gmac ping。
- 当需要检测 PBB-TE Tunnel 的连通性时，可执行 PBB-TE MAC Ping。

前置任务

在执行 802.1ag MAC Ping 之前，需完成以下任务：

- **配置以太网 CFM 基本功能**

执行通用 Gmac ping 和 PBB-TE MAC Ping 之前无前置任务。

数据准备

在手动检测以太网的连通性前，需要准备以下数据。

序号	数据
1	(可选) 目的 MEP 的 MAC 地址或 ID
2	(可选) 目的 MIP 的 MAC 地址
3	(可选) 发送 MAC Ping 报文的个数、大小、超时时间、出接口
4	(可选) 目的节点所属 VLAN
5	(可选) PBB-TE Tunnel 的名称

8.8.2 (可选) 执行 802.1ag MAC Ping

通过执行 802.1ag MAC Ping，检测同一 MA 内的 MEP 之间或 MEP 和 MIP 之间的连通性。

背景信息

802.1ag MAC Ping 与 Ping 类似，通过发送测试报文和接收应答报文来检测从本设备到目的设备是否可达。同时还可以在发送端计算 Ping 操作的时间，以分析网络性能。

操作步骤

步骤 1 在被测链路的任意一端 NE80E/40E 设备上进行以下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cfm md md-name**，进入 MD 视图。
3. 执行命令 **ma ma-name**，进入 MA 视图。
4. 执行命令 **ping mac-8021ag mep mep-id mep-id { mac mac-address | remote-mep mep-id mep-id } [-c count | interface interface-type interface-number | -s packet-size | -t timeout] [-p priority-value] ***，检测和指定 RMEP 或 MIP 之间的连通性。

进行 802.1ag MAC Ping 操作时：

- 当前 MA 必须已关联了 VLAN。
- 当前 MA 必须已配置了 MEP。
- 如果指定出接口，则该接口不能是配置了 inward 型 MEP 的接口。该接口必须加入指定 VLAN 并关联了相应的 MA。
- 如果目的节点是 RMEP，可选用参数 **mac mac-address**，也可选用参数 **remote-mep mep-id mep-id**。如果选用参数 **remote-mep mep-id mep-id**，则该 RMEP 在当前设备上必须已使用 **remote-mep** 命令创建，且创建时指定了该 RMEP 的 MAC 地址。
- 如果目的节点是 MIP，请选用参数 **mac mac-address**。

链路上的中间设备只是用来转发 LBM 和 LBR 报文，所以中间设备上均不需要配置 MD、MA 和 MEP。

----结束

8.8.3 （可选）执行通用 Gmac ping

通过执行通用 Gmac ping，检测两台设备之间的连通性。

背景信息

在被测链路的两端 NE80E/40E 设备上执行步骤 1～步骤 2，在任意一端 NE80E/40E 设备上执行步骤 3。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ping mac enable**，全局使能通用 Gmac ping 功能。

缺省情况下，通用 Gmac ping 功能处于禁止状态。

当通用 Gmac ping 功能处于使能状态时：

- 在 NE80E/40E 设备上可以进行通用 Gmac ping 操作；
- NE80E/40E 设备对接收到的通用 Gmac ping 报文进行回复。

步骤 3 执行命令 **ping mac mac-address vlan vlan-id [interface interface-type interface-number | -c count | -s packetsize | -t timeout | -p priority-value] ***，检测和对端设备之间的连通性。

通用 Gmac ping 不需要由 MEP 发起，目的节点也不需要是 MEP 或 MIP，即在源设备、中间设备和目的设备上均不需要配置 MD、MA 和 MEP 就可以进行通用 Gmac ping。

两台设备上必须配置 802.1ag 协议的相同版本。如果本端设备上配置 Draft7 草案版本，对端设备上配置 standard2007 标准版本，此时用户使用 **ping mac** 命令检测这两台设备之间的连通性时，则本端设备无法 ping 通对端设备。

----结束

8.9 配置以太网的故障定位

通过发送测试报文和接收应答报文来定位两台设备之间链路的连通性故障。

8.9.1 建立配置任务

在配置以太网的故障定认之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用场景

当需要定位两台设备之间链路的连通性故障时，可通过发送测试报文和接收应答报文来检测从本设备到目的设备的路径或定位故障点。根据被检测链路的类型，分为以下三种场景

- 当需要在配置了 MD、MA、MEP 的网络中，定位同一 MA 内的 MEP 之间或 MEP 和 MIP 之间的连通性故障时，可执行 802.1ag MAC Trace。
- 当需要在未配置 MD、MA、MEP 的网络中，定位两台设备之间的连通性故障时，可执行通用 Gmac trace。

- 当需要定位 PBB-TE Tunnel 的连通性故障时，可执行 PBB-TE MAC Trace。

前置任务

在执行 802.1ag MAC Trace 之前，需完成以下任务：

- [配置以太网 CFM 基本功能](#)

执行通用 Gmac trace 和 PBB-TE MAC Trace 之前无前置任务。

数据准备

在定位以太网的连通性故障前，需要准备以下数据。

序号	数据
1	（可选）目的 MEP 的 MAC 地址或 ID
2	（可选）目的 MIP 的 MAC 地址
3	（可选）发送 MAC Trace 报文出接口
4	（可选）等待应答报文的超时时间
5	（可选）最大跟踪跳数
6	（可选）目的节点所属 VLAN
7	（可选）PBB-TE Tunnel 的名称

8.9.2 （可选）执行 802.1ag MAC Trace

通过执行 802.1ag MAC Trace，定位同一 MA 内的 MEP 之间或 MEP 和 MIP 之间的连通性故障。

背景信息

802.1ag MAC Trace 与 Traceroute（或 Tracert）类似，通过发送测试报文和接收应答报文来检测从本设备到目的设备的路径或定位故障点。

操作步骤

步骤 1 在被测链路的任意一端 NE80E/40E 设备上进行以下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cfm md md-name**，进入 MD 视图。
3. 执行命令 **ma ma-name**，进入 MA 视图。
4. 执行命令 **trace mac-8021ag mep mep-id mep-id { mac mac-address | remote-mep mep-id mep-id } [md md-name ma ma-name] [interface interface-type interface-number | -t timeout | ttl ttl] ***，定位和对端设备之间的连通性故障。

进行 802.1ag MAC Trace 操作时：

- 当前 MA 必须已关联了 VLAN。
- 当前 MA 必须已配置了 MEP。
- 如果指定出接口，则该接口不能是配置了 inward 型 MEP 的接口。该接口必须加入 VLAN 并关联 MA。
- 如果目的节点是 RMEP，可选用参数 **mac mac-address**，也可选用参数 **remote-mep mep-id mep-id**。如果选用参数 **remote-mep mep-id mep-id**，则该 RMEP 在当前设备上必须已使用 **remote-mep** 命令创建，且创建时指定了该 RMEP 所在设备的桥 MAC 地址。
- 如果目的节点是 MIP，请选用参数 **mac mac-address**。
- 如果 MAC 地址表中不存在目的节点对应的转发表项，则必须指定 **interface interface-type interface-number** 参数。

----结束

8.9.3 （可选）执行通用 Gmac trace

通过执行通用 Gmac ping，定位两台设备之间的连通性故障。

背景信息

在被测链路两端和中间 NE80E/40E 设备上都需要进行配置。

操作步骤

步骤 1 配置两端和中间设备

在被测链路的两端和中间 NE80E/40E 设备上进行以下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **trace mac enable**，全局使能通用 Gmac trace 功能。

缺省情况下，通用 Gmac trace 功能处于禁止状态。

只有当通用 Gmac trace 功能处于使能状态时：

- 在 NE80E/40E 设备上才能进行通用 Gmac trace 操作；
- NE80E/40E 设备才对接收到的通用 Gmac trace 报文进行回复。

步骤 2 执行 Gmac trace 探测

在被测链路的任意一端 NE80E/40E 设备上执行 MAC Trace 探测。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **trace mac mac-address vlan vlan-id [interface interface-type interface-number | -t timeout] ***，定位和对端设备之间的连通性故障。

通用 Gmac trace 不需要由 MEP 发起，中间节点和目的节点也不需要是 MEP 或 MIP，即在源设备、中间设备和目的设备上均不需要配置 MD、MA 和 MEP 就可以进行通用 Gmac trace，所有中间设备均回应 LTR 消息。

两台设备上必须配置 802.1ag 协议的相同版本。如果本端设备上配置 Draft7 草案版本，对端设备上配置 standard2007 标准版本，此时用户使用 **trace mac** 命令定位这两台设备之间的连通性故障时，则无法定位成功。

----结束

8.10 配置以太网 CFM 和接口联动

以太网 CFM 与接口联动功能主要用于 LACP 静态链路聚合组或手工 1:1 主备模式链路聚合的活动链路快速故障检测和触发保护倒换。

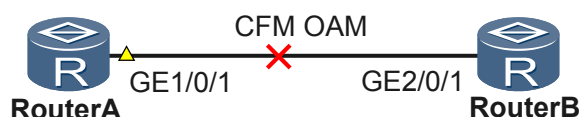
8.10.1 建立配置任务

在配置以太网 CFM 和接口联动功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

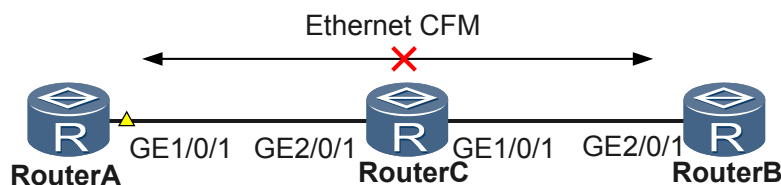
当配置了以太网 CFM 和接口联动后，如果指定 MA 内的 MEP 检测到和指定 RMEP 之间有连通性故障，OAM 管理模块对该 MEP 所在接口进行闪断处理（即先关闭该接口，然后再打开该接口），以使其它模块感知到该故障。

图 8-7 以太网 CFM 和接口联动应用场景（一）



▲ 配置了以太网CFM和接口联动功能的接口

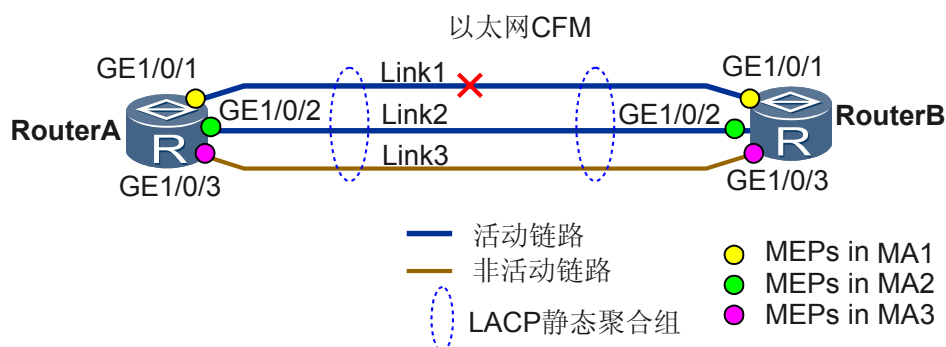
图 8-8 以太网 CFM 和接口联动应用场景（二）



▲ 配置了以太网CFM和接口联动功能的接口

图 8-7 和图 8-8 中，CFM 分别用于直连链路和多跳链路检测。两台设备 RouterA 和 RouterB 之间配置了以太网 CFM 功能，并配置了 CFM 和 RouterA 的接口 GE1/0/1 联动。在 RouterA 上，当 CFM OAM 模块检测到和 RouterB 之间有连通性故障时，OAM 管理模块对接口 GE1/0/1 进行闪断，即先关闭该接口再打开该接口，以使 RouterA 的其它接口感知到此故障。

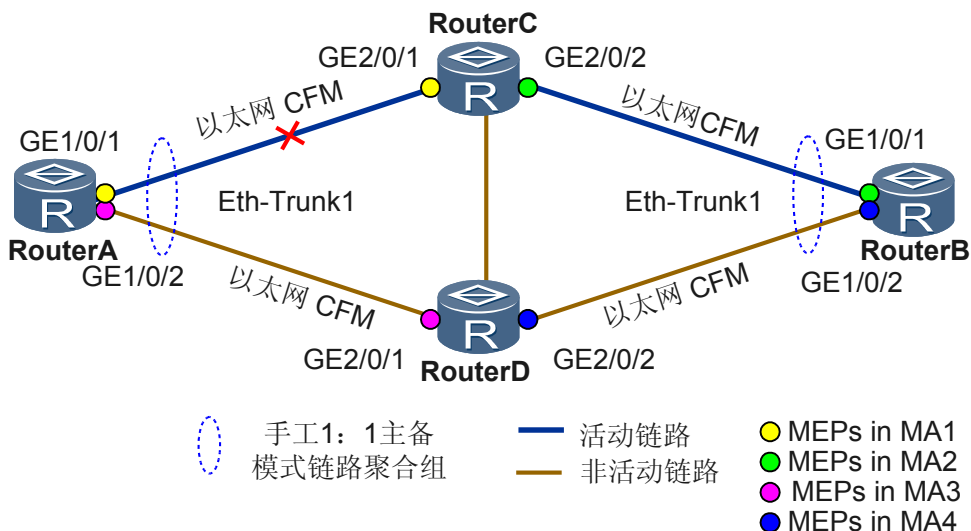
图 8-9 以太网 CFM 和接口联动应用场景（三）



RouterA 和 RouterB 配置了 LACP 静态链路聚合组。在 RouterA 和 RouterB 上配置以太网 CFM 功能：使 RouterA 和 RouterB 属于同一 MD；在链路聚合组的所有成员接口上配置 MEP，并使同一条链路两端接口上的 MEP 属于同一个 MA，不同链路两端接口上的 MEP 属于不同 MA。通过同一链路两端的 MEP 互发 CCM 消息检测链路的连通性。并配置以太网 CFM 和接口联动。

当 Link1 出现连通性故障时，RouterA 和 RouterB 的 OAM 管理模块分别对自己的 GE1/0/1 接口进行闪断。于是，LACP 模块就可以感知到 Link1 出现故障，并将通过该链路转发的业务数据切换到非活动链路 Link3 上转发。在这种情况下，保护倒换时间可达到小于等于 50 毫秒，可满足电信级网络的要求。

图 8-10 以太网 CFM 和接口联动应用场景（四）



RouterA 和 RouterB 配置了手工 1：1 主备模式链路聚合组。在 RouterA 和 RouterC、RouterA 和 RouterD、RouterB 和 RouterC、RouterB 和 RouterD 之间分别配置以太网 CFM，并在 RouterA 上配置以太网 CFM 和接口 GE1/0/1、GE1/0/2 联动，在 RouterB 上配置以太网 CFM 和接口 GE1/0/1、GE1/0/2 联动。

当 RouterA 和 RouterC 之间的链路出现连通性故障时，以太网 CFM 模块检测到该故障并通知 OAM 管理模块。OAM 管理模块对 GE1/0/1 接口进行闪断，以使链路聚合组感

知到该故障并将业务数据切换到非活动链路转发。其它链路的连通性故障的处理过程和以上 RouterA 和 RouterC 之间的链路故障处理过程类似。在这种情况下，保护倒换时间可达到小于等于 50 毫秒，可满足电信级网络的要求。

前置任务

在配置以太网 CFM 和接口联动之前，需完成以下任务：

- 配置链路聚合组
- [8.6 配置以太网 CFM 基本功能](#)

数据准备

在配置以太网 CFM 和接口联动前，需要准备以下数据。

序号	数据
1	接口的类型和编号
2	MD 的名称、MA 的名称、RMEP 的 ID

8.10.2 配置以太网 CFM 和接口联动

可以配置以太网 CFM 和接口联动，实现指定 MA 内的 MEP 检测到和指定 RMEP 之间有连通性故障，OAM 管理模块对该 MEP 所在接口先关闭，然后在打开，以使其它模块感知到该故障。

背景信息

在配置了静态 LACP 聚合组的 NE80E/40E 设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface interface-type interface-number**，进入链路聚合组成员接口的接口视图。

步骤 3 执行命令 **cfm md md-name ma ma-name remote-mep mep-id mep-id trigger if-down**，配置以太网 CFM 和接口联动。

缺省情况下，接口不和以太网 CFM 联动。

使用 **cfm md md-name ma ma-name remote-mep mep-id mep-id trigger if-down** 命令配置以太网 CFM 和当前接口联动时，指定 MA 内必须已创建 outward 型的 MEP，且该 MEP 所在接口为当前接口。

每个接口仅支持和一个 RMEP 绑定，如果要改变接口和 MA 及 RMEP 的对应联动关系，需先删除原有的配置，再重新进行配置。

如果链路聚合组有多个成员接口，请重复执行步骤 2～步骤 3，配置以太网 CFM 和所有成员接口联动。

----结束

8.10.3 检查配置结果

通过查看 Trigger-If-down 字段等内容，来检查配置是否成功。

前提条件

已经完成以太网 CFM 和接口联动功能的所有配置。

操作步骤

步骤 1 使用 **display cfm remote-mep** [md md-name [ma ma-name [mep-id mep-id]]] 命令查看 RMEP 的详细信息。

----结束

任务示例

如果以太网 CFM 和接口联动配置成功，执行 **display cfm remote-mep** 命令，可以看到对应 RMEP 的 Trigger If-down 字段显示为 enable。

```
<HUAWEI> display cfm remote-mep
The total number of RMEPs is : 1
The status of RMEPS : 0 up, 1 down, 0 disable
```

```
-----
MD Name       : md110
Level         : 0
MA Name       : ma110
RMEP ID       : 2
Vlan ID       : --
VSI Name      : --
L2VC ID       : 110 tagged
MAC           : 0025-9eb1-bce6
CCM Receive   : enabled
Trigger-If-Down : disabled
CFM Status    : down
Alarm Status   : RemoteAlarm
```

8.11 配置 EFM OAM 和以太网 CFM 之间的联动

通过配置 EFM OAM 和以太网 CFM 之间的联动，实现故障相互传递。

8.11.1 建立配置任务

在配置配置 EFM OAM 和以太网 CFM 之间的联动功能之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

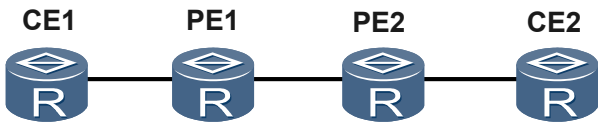
应用环境

802.3ah 协议针对以太网最后一公里，主要用于 CE 和 PE 之间直连链路的检测。802.1ag 协议针对一组业务或一些特定的网络设备，主要用于对网络的故障检测：

- CE 和 CE
- PE 和 PE
- CE 和 PE

如图 8-11 所示，在 CE1 和 PE1、CE2 和 PE2 之间配置 EFM OAM 或以太网 CFM，在 PE1 和 PE2 之间配置以太网 CFM，通过配置 ETH OAM 之间的联动，当 CE1 和 PE1 之间的链路发生故障时，通过以太网 CFM 向对端的 CE2 发出故障告警。

图 8-11 ETH OAM 联动示意图



前置任务

在配置 ETH OAM 联动之前，需完成以下任务：

- 配置 EFM OAM 基本功能
- 配置以太网 CFM 基本功能

数据准备

在配置 ETH OAM 联动功能之前，需要准备以下数据。

序号	数据
1	联动的接口和编号
2	MD 的名称和 MA 的名称

8.11.2 配置 ETH OAM 联动

可以根据实际需求选择故障的传递方式。

背景信息

在 CE 设备上进行如下配置。

操作步骤

- 步骤 1 执行命令 `system-view`，进入系统视图。
- 步骤 2 执行命令 `oam-mgr`，进入 OAM 管理视图。
- 步骤 3 请根据实际情况选择以下配置。
 - 执行命令 `oam-bind cfm md md-name ma ma-name efm interface interface-type interface-number`，配置 EFM OAM 和以太网 CFM 双向故障传递。
 - 执行命令 `oam-bind ingress efm interface interface-type interface-number egress cfm md md-name ma ma-name`，配置 EFM OAM 向以太网 CFM 传递故障。

- 执行命令 **oam-bind ingress cfm md md-name ma ma-name egress efm interface interface-type interface-number**，配置以太网 CFM 向 EFM OAM 传递故障。
- 执行命令 **oam-bind ingress cfm md md-name1 ma ma-name1 egress cfm md md-name2 ma ma-name2**，配置某一侧以太网 CFM 向另一侧以太网 CFM 传递故障。
- 执行命令 **oam-bind cfm md md-name1 ma ma-name1 cfm md md-name2 ma ma-name2**，配置两侧以太网 CFM 双向传递故障。

 说明

在配置 ETH OAM 和其它功能模块联动后，

- 如果去使能端口的 EFM 功能，则会导致和 EFM 的联动功能被删除。
- 如果删除 MA 或 MD，则会导致和 CFM 的联动功能被删除。

----结束

8.11.3 检查配置结果

通过查看以太网 CFM 是否向对端发送故障告警，来检查配置是否成功。

操作步骤

- 完成上述配置后，CE1 和 PE1 之间 ETH OAM 检测到的故障，可以通过以太网 CFM 通告给 CE2 和 PE2 之间的 OAM。

----结束

8.12 配置以太网 CFM 和 VPLS 的组合应用

通过配置 CFM 和 VPLS 的组合应用，实现在 VPLS 场景中端到端的连通性故障检测、故障通告、故障判定和故障定位功能。

8.12.1 建立配置任务

在配置以太网 CFM 和 VPLS 的组合应用之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 8-12 所示，PE1 和 PE2 之间运行 VPLS。在该组网中，分别存在 CE 到 CE、CE 到 PE、PE 到 PE 的维护域。CE 与 CE 之间、CE 与 PE 之间运行 CFM OAM，通过互发 CCM 消息进行连通性检测。可以进行 MAC Ping/Trace 操作，检测目的设备的可达性/或者定位故障点；PE 与 PE 之间运行 VPLS OAM，以对 VPLS 网络的连通性进行检测。

图 8-12 以太网 CFM 和 VPLS 的组合应用示意图



前置任务

配置以太网 CFM 和 VPLS 组合应用之前，需要完成以下任务：

- 配置 Martini 方式 VPLS
- 配置以太网基本功能

数据准备

在配置以太网 CFM 和 VPLS 组合应用之前，需要准备以下数据。

序号	数据
1	VSI 的名称和 ID
2	MD 的名称和 MA 的名称对等体的 IP 地址及建立对等体时使用的隧道策略
3	绑定 VSI 的接口
4	发送的检测报文类型
5	MD 的名称和 MA 的名称

8.12.2 在 PE 和 PE 之间配置基于 VPLS 的以太网 CFM 功能

通过在 PE 之间配置以太网 CFM 功能，实现 PE 之间的连通性故障检测、故障通告、故障判定和故障定位功能。

背景信息

 说明

- 在 PE 和 PE 之间如果要配置 802.1ag MAC Trace 来检测 PE 之间的连通性故障，不能指定发送 Trace 报文的出接口。
- 当前的 MA 必须和 VSI 关联，MEP 是 inward 类型。

在 PE 设备上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **cfm md md-name [level level]**，创建 MD 并进入 MD 视图。
- 步骤 3** 执行命令 **ma ma-name**，创建 MA 并进入 MA 视图。
- 步骤 4** 执行命令 **map vsi vsi-name**，配置 MA 关联 VSI。
- 步骤 5** 执行命令 **mep mep-id mep-id interface { interface-type interface-number | interface-type interface-number.subnumber } inward**，在 PE 设备的 AC 侧接口上创建 inward 类型 MEP。
- 步骤 6** 执行命令 **remote-mep mep-id mep-id [mac mac-address]**，配置当前 MA 内的 RMEP。

步骤 7 执行命令 **mep ccm-send [mep-id mep-id] enable**，使能 MEP 的 CCM 消息发送功能。

步骤 8 执行命令 **remote-mep ccm-receive [mep-id mep-id] enable**，使能本设备上当前 MA 内本地 MEP 接收同一 MA 内的 RMEP 发送的 CCM 消息功能。

----结束

8.12.3 在 CE 和本端 PE 之间配置以太网 CFM 功能

通过在 CE 和本端 PE 之间配置以太网 CFM 功能，实现 CE 和本端 PE 之间的连通性故障检测、故障通告、故障判定和故障定位功能。

操作步骤

- 在 PE 设备上以下配置。

 说明

在 PE 上配置 MA，必须和 VSI 关联，MEP 是 outward 类型。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cfm md md-name [level level]**，创建 MD 并进入 MD 视图。
3. 执行命令 **ma ma-name**，创建 MA 并进入 MA 视图。
4. 执行命令 **map vsi vsi-name**，配置 MA 关联 VSI。
5. 执行命令 **mep mep-id mep-id interface { interface-type interface-number | interface-type interface-number.subnumber } outward**，创建 outward 类型 MEP。
6. 执行命令 **remote-mep mep-id mep-id [mac mac-address]**，配置当前 MA 内的 RMEP。
7. 执行命令 **mep ccm-send [mep-id mep-id] enable**，使能 MEP 的 CCM 消息发送功能。
8. 执行命令 **remote-mep ccm-receive [mep-id mep-id] enable**，使能本设备上当前 MA 内本地 MEP 接收同一 MA 内的 RMEP 发送的 CCM 消息功能。

- 在 CE 设备上以下配置。

 说明

在 CE 上配置 MA，必须和 VLAN 关联，MEP 是 outward 类型。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cfm md md-name [level level]**，创建 MD 并进入 MD 视图。
3. 执行命令 **ma ma-name**，创建 MA 并进入 MA 视图。
4. 执行命令 **map vlan vlan-id**，配置 MA 关联 VLAN。
5. 执行命令 **mep mep-id mep-id interface { interface-type interface-number | interface-type interface-number.subnumber } outward**，创建 outward 类型 MEP。
6. 执行命令 **remote-mep mep-id mep-id [mac mac-address]**，配置当前 MA 内的 RMEP。
7. 执行命令 **mep ccm-send [mep-id mep-id] enable**，使能 MEP 的 CCM 消息发送功能。
8. 执行命令 **remote-mep ccm-receive [mep-id mep-id] enable**，使能本设备上当前 MA 内本地 MEP 接收同一 MA 内的 RMEP 发送的 CCM 消息功能。

----结束

8.12.4 在 CE 和对端 PE 之间配置以太网 CFM 功能

通过在 CE 和对端 PE 之间配置以太网 CFM 功能，实现 CE 和本端 PE 之间的连通性故障检测、故障通告、故障判定和故障定位功能。

背景信息

具体配置和[在 CE 和本端 PE 之间配置以太网 CFM 功能](#)的配置类似。

说明

- 在 PE 上配置 MA，必须和 VSI 关联，MEP 是 inward 类型。
- 在 CE 上配置 MA，必须和 VLAN 关联，MEP 是 outward 类型。
- 中间节点设备需要配置 MIP 生成规则。

8.12.5 检查配置结果

通过查看 MD、MA、MEP 和 MIP 等内容，来检查配置是否成功。

操作步骤

- 完成上述配置后，在 PE 或 CE 上执行 **display cfm mep** 命令和 **display cfm remote-mep** 命令，可以看到以太网 CFM 已经建立成功。以太网 CFM 能够快速检测到 PE 和 PE 之间、CE 和 PE 之间的故障，并通知给网管系统。

----结束

8.13 配置以太网 CFM 和 VLL 的组合应用（使用 QinQ 终结子接口）

PE 设备将带有两层 Tag 的报文接入 VLL 网络中，为了提高网络的可靠性，可通过在 PE 设备 AC 侧配置 QinQ 终结子接口绑定 L2VC，再部署 CFM 功能。

8.13.1 建立配置任务

配置以太网 CFM（Connectivity Fault Management）和 VLL 的组合应用前，务必确认 PE 设备收到的报文带有一层 Tag 还是两层 Tag。若 PE 设备收到的报文带有一层 Tag，可使用普通子接口/Dot1q 终结子接口接入网络。若 PE 设备收到的报文带有两层 Tag，则使用 QinQ 终结子接口绑定 L2VC 接入网络。本节重点描述 PE 收到带有两层 Tag 报文的场景。

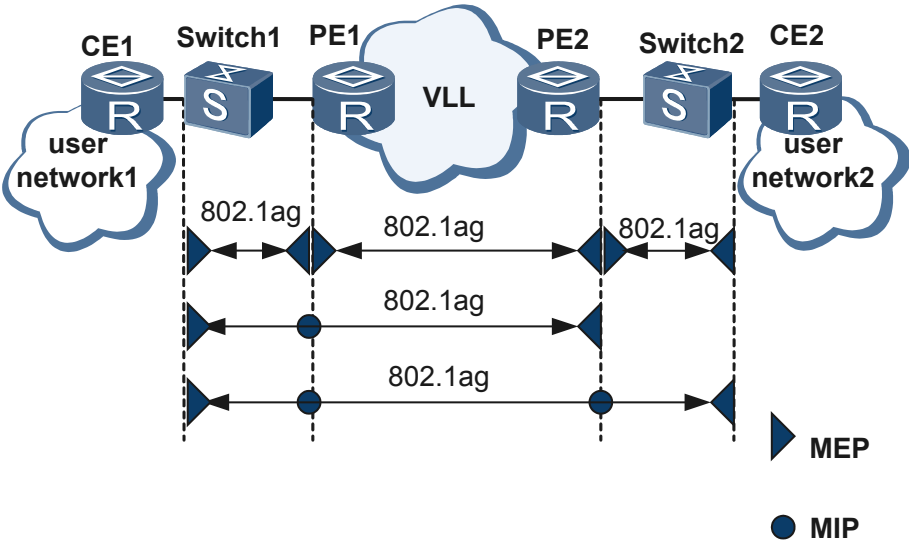
应用环境

如[图 8-13](#)所示，MA 分别如下：

- PE 与 PE 之间
- Switch 与本端 PE 之间
- Switch 与对端 PE 之间
- Switch 与 Switch 之间

同一个 MA 内的 MEP 之间通过互发 CCM 消息进行连通性检测，可以进行 MAC Ping/Trace 操作，进行故障确认、定位。

图 8-13 以太网 CFM 和 VLL 的组合应用示意图



PE1 和 PE2 之间运行 VLL。PE 收到的报文带有两层 Tag。若需要对 PE 之间进行连通性检测，可在 PE 设备 AC 侧接口上配置 QinQ 终结子接口绑定 L2VC，然后在 PE 间部署 CFM 功能。

前置任务

配置以太网 CFM 和 VLL 的组合应用（使用 QinQ 终结子接口）之前，需要完成以下任务：

- 配置 Martini 方式 VLL
具体配置可参见《HUAWEI NetEngine80E/40E 路由器 配置指南-VPN》中的 VLL 配置。
- 配置 QinQ 终结子接口接入 VLL
具体配置可参见《HUAWEI NetEngine80E/40E 路由器 配置指南-局域网与城域网接入》中的 QinQ 配置。
- 配置以太网 CFM 基本功能

数据准备

在配置以太网 CFM 和 VLL 的组合应用（使用 QinQ 终结子接口）之前，需要准备以下数据。

序号	数据
1	L2VC 的目的地址和 VC ID
2	绑定 L2VC 的接口
3	MD 的名称和 MA 的名称
4	MEP 的 ID、MEP 所在接口的名称、MEP 的类型

序号	数据
5	(可选) RMEP 的 ID、RMEP 所在接口的 MAC 地址
6	MA 内 MEP 发送 CCM 消息的时间间隔

8.13.2 在 PE 和 PE 之间配置基于 VLL 的以太网 CFM 功能

以太网 CFM 实现端到端的连通性故障检测、故障通知、故障确认和故障定位功能。可用于监测整个网络的连通性，定位网络的连通性故障，提高网络的可靠性。

背景信息

-  说明
- 在 PE 间配置 802.1ag MAC Trace 功能检测 PE 之间的连通性时，不能指定发送 Trace 报文的出口。
 - 当前的 MA 必须和 L2VC 关联，并且 MEP 是 inward 类型。
- 在 PE 设备上进行以下配置。

操作步骤

- 步骤 1** 执行命令 `system-view`，进入系统视图。
- 步骤 2** 执行命令 `cfm md md-name [ level level ]`，创建 MD 并进入 MD 视图。
- 步骤 3** 执行命令 `ma ma-name`，创建 MA 并进入 MA 视图。
- 步骤 4** 执行命令 `map mpls l2vc vc-id { raw | tagged }`，配置 L2VC 关联 MA。

-  说明
- 802.1ag 不支持 MA 关联备份 VC。
- 将接口设置为 `raw` 或 `tagged` 的类型，接口对报文的处理方式也不同。如表 8-2 和表 8-3 所示。

表 8-2 报文入接口处理

入接口类型	raw 封装方式（以太封装方式）	tagged 封装方式（VLAN 封装方式）
Dot1q 子接口	剥掉一层 Tag	不做处理，保留 Tag
Dot1q 终结子接口	剥掉一层 Tag	不做处理，保留 Tag
QinQ 终结子接口（对称方式）	剥掉外层 Tag	不处理，两层 Tag 都保留
QinQ 终结子接口（非对称方式）	两层 Tag 都剥掉	剥掉两层 Tag，再添加一层 Tag

表 8-3 报文出接口处理

出接口类型	raw 封装方式（以太封装方式）	tagged 封装方式（VLAN 封装方式）
Dot1q 子接口	添加一层 Tag	替换为出接口封装的 Tag
Dot1q 终结子接口	添加一层 Tag	替换为出接口封装的 Tag
QinQ 终结子接口（对称方式）	添加外层 Tag	替换外层 Tag 为出接口封装的 Tag
QinQ 终结子接口（非对称方式）	添加两层 Tag	剥掉外层 Tag，再添加出接口封装的两层 Tag

步骤 5 执行命令 **mep mep-id mep-id interface { interface-type interface-number | interface-type interface-number.subnumber } pe-vid pe-vid ce-vid ce-vid inward**，在 PE 设备 AC 侧绑定 L2VC 的接口上创建 inward 类型 MEP。

步骤 6 执行命令 **remote-mep mep-id mep-id [mac mac-address]**，配置当前 MA 内的 RMEP。

步骤 7 执行命令 **mep ccm-send [mep-id mep-id] enable**，使能 MEP 的 CCM 消息发送功能。

步骤 8 执行命令 **remote-mep ccm-receive [mep-id mep-id] enable**，使能本设备上当前 MA 内本地 MEP 接收同一 MA 内的 RMEP 发送的 CCM 消息功能。

----结束

8.13.3 在 Switch 和本端 PE 之间配置以太网 CFM 功能

Switch 和本端 PE 之间运行 CFM，通过互发 CCM 消息进行连通性检测。

操作步骤

- 在 PE 设备上以下配置。

 说明

在 PE 上配置 MA，必须和 L2VC 关联，MEP 是 outward 类型。

- 执行命令 **system-view**，进入系统视图。
- 执行命令 **cfm md md-name [level level]**，创建 MD 并进入 MD 视图。
- 执行命令 **ma ma-name**，创建 MA 并进入 MA 视图。
- 执行命令 **map mpls l2vc vc-id { raw | tagged }**，配置 L2VC 关联 MA。

 说明

802.lag 不支持 MA 关联备份 VC。

将接口设置为 **raw** 或 **tagged** 的类型，接口对报文的处理方式也不同。如表 8-4 和表 8-5 所示。

表 8-4 报文入接口处理

入接口类型	raw 封装方式（以太封装方式）	tagged 封装方式（VLAN 封装方式）
Dot1q 子接口	剥掉一层 Tag	不做处理，保留 Tag
Dot1q 终结子接口	剥掉一层 Tag	不做处理，保留 Tag
QinQ 终结子接口（对称方式）	剥掉外层 Tag	不处理，两层 Tag 都保留
QinQ 终结子接口（非对称方式）	两层 Tag 都剥掉	剥掉两层 Tag，再添加一层 Tag

表 8-5 报文出接口处理

出接口类型	raw 封装方式（以太封装方式）	tagged 封装方式（VLAN 封装方式）
Dot1q 子接口	添加一层 Tag	替换为出接口封装的 Tag
Dot1q 终结子接口	添加一层 Tag	替换为出接口封装的 Tag
QinQ 终结子接口（对称方式）	添加外层 Tag	替换外层 Tag 为出接口封装的 Tag
QinQ 终结子接口（非对称方式）	添加两层 Tag	剥掉外层 Tag，再添加出接口封装的两层 Tag

5. 执行命令 **mep mep-id mep-id interface { interface-type interface-number | interface-type interface-number.subnumber } pe-vid pe-vid ce-vid ce-vid outward**，在 PE 设备 AC 侧，配置 QinQ 终结子接口绑定 L2VC 的接口上创建 outward 类型 MEP。
 6. 执行命令 **remote-mep mep-id mep-id [mac mac-address]**，配置当前 MA 内的 RMEP。
 7. 执行命令 **mep ccm-send [mep-id mep-id] enable**，使能 MEP 的 CCM 消息发送功能。
 8. 执行命令 **remote-mep ccm-receive [mep-id mep-id] enable**，使能本设备上当前 MA 内本地 MEP 接收同一 MA 内的 RMEP 发送的 CCM 消息功能。
- Switch 设备上的具体配置请参见该型号交换机的相关配置手册。

----结束

8.13.4 在 Switch 和对端 PE 之间配置以太网 CFM 功能

Switch 和对端 PE 之间运行 CFM，通过互发 CCM 消息进行连通性检测，可以进行 MAC Ping/Trace 操作，进行性能测试。

背景信息

具体配置和在 Switch 和本端 PE 之间配置以太网 CFM 功能的配置类似。



说明

- 在对端 PE 上配置 MA，必须和 L2VC 关联，MEP 是 inward 类型。
- Switch 设备上的具体配置请参见该型号交换机的相关配置手册。
- 中间节点设备需要配置 MIP 生成规则。

MIP 生成规则请参见 [\(可选\) 配置 MIP 生成规则](#)

8.13.5 检查配置结果

以太网 CFM 和 VLL 的组合应用（使用 QinQ 终结子接口）配置成功后，您可以查看到指定 MD 和 MA 内的 MEP 和 RMEP 的信息、不同 MA 之间的 CFM 状态等内容。

前提条件

已经完成以太网 CFM 和 VLL 的组合应用（使用 QinQ 终结子接口）的所有配置。

操作步骤

- 执行命令 **display cfm md** [*md-name*]，查看 MD 的配置信息。
- 执行命令 **display cfm ma** [**md** *md-name* [**ma** *ma-name*]]，查看 MA 的详细信息。
- 执行命令 **display cfm mep** [**md** *md-name* [**ma** *ma-name* [**mep-id** *mep-id*]]]，查看 MEP 的详细信息。
- 执行命令 **display cfm remote-mep** [**md** *md-name* [**ma** *ma-name* [**mep-id** *mep-id*]]]，查看 RMEP 的详细信息。
- 执行命令 **display mip create-type** [**interface** *interface-type* *interface-number*]，查看 MIP 的创建规则。
- 执行命令 **display cfm mip** [**interface** *interface-type* *interface-number* | **level** *level*]，查看 MIP 的信息。



说明

MIP 成功配置后，才能执行命令 **display mip create-type** 和 **display cfm mip** 查看 MIP 的相关配置，否则不显示 MIP 的详细信息。

----结束

任务示例

Standard2007 标准版本中，如果 MD 创建成功，执行命令 **display cfm md**，可以看到该 MD 的名称、MD 名称参数输入类型、MD 级别、MIP 生成规则和 Sender ID TLV 类型等信息。

```
<HUAWEI> display cfm md mdcustomer
MD Name           : mdcustomer
MD Name Format     : string
Level             : 2
MIP Create-type    : none
SenderID TLV-type  : defer
MA list            :
    MA Name        : mdcustomer1
    MA Name Format  : string
    Interval       : 1000
    Vlan ID        : --
    L2VC ID        : 11
```

如果 MA 创建成功，执行命令 **display cfm ma**，可以看到该 MA 的信息。

```
<HUAWEI> display cfm ma md mdcustomer
```



```
The total number of MAs is : 1
```

```
-----
MD Name           : mdcustomer
MD Name Format     : string
Level             : 4
MIP Create-type   : none
SenderID TLV-type : defer
MA Name           : mdcustomer1
MA Name Format     : string
Interval          : 1000
Priority           : 6
Vlan ID           : --
VSI Name          : vsil
L2VC ID           : 11
MEP Number        : 1
RMEP Number       : 1
Suppressing Alarms : No
Sending Ais Packet : No
```

如果 MEP 创建成功，执行命令 **display cfm mep**，可以看到该 MEP 的信息。

```
<HUAWEI> display cfm mep
The total number of MEPs is : 1
```

```
-----
MD Name           : mdcustomer
MD Name Format     : string
Level             : 4
MA Name           : mdcustomer1
MA Name Format     : string
MEP ID            : 4
Vlan ID           : --
L2VC ID           : 11
Interface Name     : GigabitEthernet1/0/2.1
CCM Send          : enabled
Direction         : inward
MAC Address        : 0018-82a0-23a7
```

如果 RMEP 配置成功，执行命令 **display cfm remote-mep**，可以看到该 RMEP 的信息。

```
<HUAWEI> display cfm remote-mep
The total number of RMEPs is : 1
The status of RMEPS : 1 up, 0 down
```

```
-----
MD Name           : mdcustomer
Level             : 4
MA Name           : mdcustomer1
RMEP ID           : 3
Vlan ID           : --
L2VC ID           : 11
MAC               : 0018-82aa-12ed
CCM Receive       : enabled
Trigger-If-Down   : disabled
CFM Status        : up
```

8.14 配置以太网 CFM 和 VPLS 的组合应用（使用 QinQ 终结子接口）

PE 设备将带有两层 Tag 的报文接入 VPLS 网络中，为了提高网络的可靠性，可通过在 PE 设备 AC 侧配置 QinQ 终结子接口绑定 VSI 接入 VPLS 网络，再部署 CFM 功能。

8.14.1 建立配置任务

配置以太网 CFM（Connectivity Fault Management）和 VPLS 的组合应用前，务必确认 PE 设备收到的报文带有一层 Tag 还是两层 Tag。若 PE 设备收到的报文带有一层 Tag，

可使用普通子接口接入网络。若 PE 设备收到的报文带有两层 Tag，则使用 QinQ 终结子接口绑定 VSI 接入网络。本节重点描述 PE 收到带有两层 Tag 报文的场景。

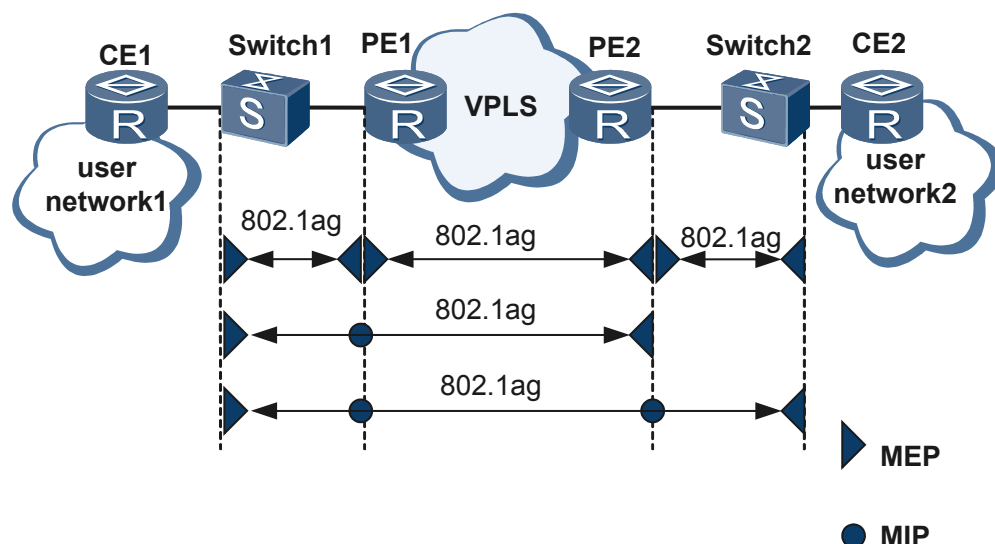
应用环境

如图 8-14 所示，MA 分别如下所示：

- PE 与 PE 之间
- Switch 与本端 PE 之间
- Switch 与对端 PE 之间
- Switch 与 Switch 之间

同一个 MA 内的 MEP 之间通过互发 CCM 消息进行连通性检测，可以进行 MAC Ping/Trace 操作，进行故障确认、定位。

图 8-14 以太网 CFM 和 VPLS 的组合应用示意图 1



PE1 和 PE2 之间运行 VPLS。PE 收到的报文带有两层 Tag。若需要对 PE 之间进行连通性检测，可在 PE 设备 AC 侧接口上配置 QinQ 终结子接口绑定 VSI 接入 VPLS，然后在 PE 间部署 CFM 功能。

前置任务

配置以太网 CFM 和 VPLS 的组合应用（使用 QinQ 终结子接口）之前，需要完成以下任务：

- 配置 Martini 方式 VPLS
具体配置可参见《NE80E/40E 配置指南-VPN》中的 VPLS 配置。
- 配置 QinQ 终结子接口接入 VPLS
具体配置可参见《NE80E/40E 配置指南-局域网与城域网接入》中的 QinQ 配置。
- **配置以太网 CFM 基本功能**

数据准备

在配置以太网 CFM 和 VPLS 的组合应用（使用 QinQ 终结子接口）之前，需要准备以下数据。

序号	数据
1	VSI 的名称和 ID
2	绑定 VSI 的接口
3	MD 的名称和 MA 的名称
4	MEP 的 ID、MEP 所在接口的名称、MEP 的类型
5	（可选）RMEP 的 ID、RMEP 所在接口的 MAC 地址
6	MA 内 MEP 发送 CCM 消息的时间间隔

8.14.2 在 PE 和 PE 之间配置基于 VPLS 的以太网 CFM 功能

以太网 CFM 针对网络实现端到端的连通性故障检测、故障通知、故障确认和故障定位功能。可用于监测整个网络的连通性，定位网络的连通性故障，提高网络的可靠性。

背景信息

 说明

- 在 PE 和 PE 之间如果要配置 802.1ag MAC Trace 来检测 PE 之间的连通性故障，不能指定发送 Trace 报文的出接口。
- 当前的 MA 必须和 VSI 关联，MEP 是 inward 类型。

在 PE 设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md md-name [level level]**，创建 MD 并进入 MD 视图。

步骤 3 执行命令 **ma ma-name**，创建 MA 并进入 MA 视图。

步骤 4 执行命令 **map vsi vsi-name**，配置 MA 关联 VSI。

步骤 5 执行命令 **mep mep-id mep-id interface { interface-type interface-number | interface-type interface-number.subnumber } pe-vid pe-vid ce-vid ce-vid inward**，在 PE 设备的 AC 侧接口上创建 inward 类型 MEP。

步骤 6 执行命令 **remote-mep mep-id mep-id [mac mac-address]**，配置当前 MA 内的 RMEP。

步骤 7 执行命令 **mep ccm-send [mep-id mep-id] enable**，使能 MEP 的 CCM 消息发送功能。

步骤 8 执行命令 **remote-mep ccm-receive [mep-id mep-id] enable**，使能本设备上当前 MA 内本地 MEP 接收同一 MA 内的 RMEP 发送的 CCM 消息功能。

----结束

8.14.3 在 Switch 和本端 PE 之间配置以太网 CFM 功能

Switch 和本端 PE 之间运行 CFM，通过互发 CCM 消息进行连通性检测。

操作步骤

- 在 PE 设备上进行以下配置。

 说明

在 PE 上配置 MA，必须和 VSI 关联，MEP 是 outward 类型。

1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **cfm md md-name [level level]**，创建 MD 并进入 MD 视图。
 3. 执行命令 **ma ma-name**，创建 MA 并进入 MA 视图。
 4. 执行命令 **map vsi vsi-name**，配置 MA 关联 VSI。
 5. 执行命令 **mep mep-id mep-id interface { interface-type interface-number | interface-type interface-number.subnumber } pe-vid pe-vid ce-vid ce-vid outward**，在 PE 设备 AC 侧，配置 QinQ 终结子接口绑定 VSI 的接口上创建 outward 类型 MEP。
 6. 执行命令 **remote-mep mep-id mep-id [mac mac-address]**，配置当前 MA 内的 RMEP。
 7. 执行命令 **mep ccm-send [mep-id mep-id] enable**，使能 MEP 的 CCM 消息发送功能。
 8. 执行命令 **remote-mep ccm-receive [mep-id mep-id] enable**，使能本设备上当前 MA 内本地 MEP 接收同一 MA 内的 RMEP 发送的 CCM 消息功能。
- Switch 设备上的具体配置请参见该型号交换机的相关配置手册。

----结束

8.14.4 在 Switch 和对端 PE 之间配置以太网 CFM 功能

Switch 和对端 PE 之间运行 CFM，通过互发 CCM 消息进行连通性检测，可以进行 MAC Ping/Trace 操作，进行性能测试。

背景信息

具体配置和[在 Switch 和本端 PE 之间配置以太网 CFM 功能](#)的配置类似。

 说明

- 在对端 PE 上配置 MA，必须和 VSI 关联，MEP 是 inward 类型。
- Switch 设备上的具体配置请参见该型号交换机的相关配置手册。
- 中间节点设备需要配置 MIP 生成规则。

MIP 生成规则请参见 [\(可选\)配置 MIP 生成规则](#)

8.14.5 检查配置结果

以太网 CFM 和 VPLS 的组合应用（使用 QinQ 终结子接口）配置成功后，您可以查看到指定 MD 和 MA 内的 MEP 和 RMEP 的信息、不同 MA 之间的 CFM 状态等内容。

前提条件

已经完成以太网 CFM 和 VPLS 的组合应用（使用 QinQ 终结子接口）的所有配置。

操作步骤

- 执行命令 **display cfm md** [*md-name*], 查看 MD 的配置信息。
- 执行命令 **display cfm ma** [**md** *md-name* [**ma** *ma-name*]], 查看 MA 的详细信息。
- 执行命令 **display cfm mep** [**md** *md-name* [**ma** *ma-name* [**mep-id** *mep-id*]]], 查看 MEP 的详细信息。
- 执行命令 **display cfm remote-mep** [**md** *md-name* [**ma** *ma-name* [**mep-id** *mep-id*]]], 查看 RMEP 的详细信息。
- 执行命令 **display mip create-type** [**interface** *interface-type* *interface-number*], 查看 MIP 的创建规则。
- 执行命令 **display cfm mip** [**interface** *interface-type* *interface-number* | **level** *level*], 查看 MIP 的信息。



说明
MIP 成功配置后, 才能执行命令 **display mip create-type** 和 **display cfm mip** 查看 MIP 的相关配置, 否则不显示 MIP 的详细信息。

----结束

任务示例

Standard2007 标准版本中, 如果 MD 创建成功, 执行命令 **display cfm md**, 可以看到该 MD 的名称、MD 名称参数输入类型、MD 级别、MIP 生成规则和 Sender ID TLV 类型等信息。

```
<HUAWEI> display cfm md mdcustomer
MD Name          : mdcustomer
MD Name Format    : string
Level            : 2
MIP Create-type   : none
SenderID TLV-type : defer
MA list          :
                  MA Name          : mdcustomer1
                  MA Name Format    : string
                  Interval         : 1000
                  Vlan ID          : --
                  VSI Name         : vsil
```

如果 MA 创建成功, 执行命令 **display cfm ma**, 可以看到该 MA 的信息。

```
<HUAWEI> display cfm ma md mdcustomer
The total number of MAs is : 1
-----
MD Name          : mdcustomer
MD Name Format    : string
Level            : 4
MIP Create-type   : none
SenderID TLV-type : defer
MA Name          : mdcustomer1
MA Name Format    : string
Interval         : 1000
Priority          : 6
Vlan ID          : --
VSI Name         : vsil
L2VC ID          : --
MEP Number       : 1
RMEP Number      : 1
Suppressing Alarms : No
Sending Ais Packet : No
```

如果 MEP 创建成功, 执行命令 **display cfm mep**, 可以看到该 MEP 的信息。

```
<HUAWEI> display cfm mep
The total number of MEPs is : 2
-----
MD Name           : mdcustomer
MD Name Format     : string
Level             : 4
MA Name           : mdcustomer1
MA Name Format     : string
MEP ID            : 4
Vlan ID           : --
VSI Name          : vsil
Interface Name     : GigabitEthernet1/0/2.1
CCM Send          : enabled
Direction         : inward
MAC Address       : 0018-82a0-23a7

MD Name           : four
MD Name Format     : string
Level             : 2
MA Name           : four
MA Name Format     : string
MEP ID            : 7
Vlan ID           : --
VSI Name          : vsil
Interface Name     : GigabitEthernet1/0/2.1
CCM Send          : enabled
Direction         : outward
MAC Address       : 0018-82a0-23a7
```

如果 RMEP 配置成功，执行命令 **display cfm remote-mep**，可以看到该 RMEP 的信息。

```
<HUAWEI> display cfm remote-mep
The total number of RMEPs is : 2
The status of RMEPS : 1 up, 1 down
-----
MD Name           : mdcustomer
Level             : 4
MA Name           : mdcustomer1
RMEP ID           : 3
Vlan ID           : --
VSI Name          : vsil
MAC               : 0018-82aa-12ed
CCM Receive       : enabled
Trigger-If-Down   : disabled
CFM Status        : down

MD Name           : four
Level             : 2
MA Name           : four
RMEP ID           : 8
Vlan ID           : --
VSI Name          : vsil
MAC               : 0018-828a-f7c4
CCM Receive       : enabled
Trigger-If-Down   : disabled
CFM Status        : up
```

8.15 配置 ETH OAM 和 MPLS OAM/BFD 组合应用

通过配置 ETH OAM 和 MPLS OAM/BFD 的组合应用，实现故障信息的传递功能。

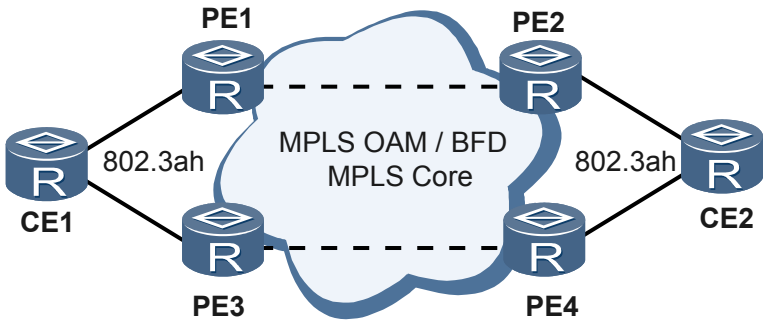
8.15.1 建立配置任务

在配置 ETH OAM 和 MPLS OAM/BFD 组合应用之前，应了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 8-15 所示，CE 双归方式接入到 PE，PE 之间为 MPLS 网络，为了实现端到端链路故障检测，在 PE 之间的 MPLS LSP 或 VLL 上配置 MPLS OAM 或 BFD，在 CE 和 PE 之间配置以太网 OAM。当核心网侧的 MPLS OAM/BFD 检测到故障时，通过 PE 设备通知以太网 OAM 机制，使 CE 设备切换到备份路径。

图 8-15 ETH OAM 和 MPLS OAM/BFD 联动示意图



前置任务

配置 ETH OAM 和 MPLS OAM/BFD 组合应用之前，需要完成以下任务：

- 配置 Martini 方式 VLL FRR
- 配置 BFD 会话
- 配置 MPLS OAM

数据准备

在配置 ETH OAM 和 MPLS OAM/BFD 组合应用之前，需要准备以下数据。

序号	数据
1	联动的接口和编号
2	MD 的名称和 MA 的名称
3	各路由器的接口和 IP 地址、隧道的接口名和隧道 ID
4	发送的检测报文类型
5	被检测 LSP 和反向通道各自的入节点和出节点
6	BFD 名称
7	BFD 会话参数

8.15.2 配置 ETH OAM 功能

可以在 CE 和 PE 之间配置 ETH OAM 功能来检测他们之间的连通性故障。

前提条件

在 CE 和 PE 之间配置 ETH OAM 功能，具体配置请参考配置 EFM OAM 基本功能和配置以太网 CFM 基本功能。

8.15.3 配置 ETH OAM 和 MPLS OAM/BFD 的联动

ETH OAM 和 MPLS OAM/BFD 之间可以进行故障传递。

背景信息

在 PE 设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **oam-mgr**，进入 OAM 管理视图。

步骤 3 请根据实际情况选择如下配置：

- 执行命令 **oam-bind ingress cfm md md-name ma ma-name egress bfd-session bfd-session-id**，配置以太网 CFM 向 BFD 传递故障。
- 执行命令 **oam-bind ingress bfd-session bfd-session-id egress cfm md md-name ma ma-name**，配置 BFD 向以太网 CFM 传递故障。
- 执行命令 **oam-bind cfm md md-name ma ma-name bfd-session bfd-session-id**，配置以太网 CFM 与 BFD 双向传递故障。
- 执行命令 **oam-bind ingress efm interface interface-type interface-number egress bfd-session bfd-session-id**，配置 EFM OAM 向 BFD 传递故障。
- 执行命令 **oam-bind ingress bfd-session bfd-session-id egress efm interface interface-type interface-number**，配置 BFD 向 EFM OAM 传递故障。
- 执行命令 **oam-bind efm interface interface-type interface-number bfd-session bfd-session-id**，配置 EFM OAM 与 BFD 双向传递故障。
- 执行命令 **oam-bind ingress cfm md md-name ma ma-name egress mpls oam interface tunnel tunnel-number**，配置以太网 CFM 向 MPLS OAM 传递故障。
- 执行命令 **oam-bind ingress mpls oam { lsp-name lsp-name | lsr-id lsr-id tunnel-id tunnel-id } egress cfm md md-name ma ma-name**，配置 MPLS OAM 向以太网 CFM 传递故障。
- 执行命令 **oam-bind ingress efm interface interface-type interface-number egress mpls oam interface tunnel tunnel-number**，配置 EFM OAM 向 MPLS OAM 传递故障。
- 执行命令 **oam-bind ingress mpls oam { lsp-name lsp-name | lsr-id ingress-lsr-id tunnel-id tunnel-id } egress efm interface interface-type interface-number**，配置 MPLS OAM 向 EFM OAM 传递故障。

----结束

8.15.4 检查配置结果

通过查看 CE 是否切换到了备份路径上，来检查配置是否成功。

前提条件

完成上述配置后，PE1 和 PE2 之间 MPLS OAM/BFD 检测到故障，可以通过 EFM OAM 和 CFM 通告给 CE1，使 CE1 切换到备份路径。

8.16 配置以太网 CFM 和组播 VLAN 1+1 保护功能

以太网 CFM 可用于工作 VLAN 和保护 VLAN 的连通性故障检测，以及触发保护倒换，从而实现组播 1+1 保护功能。

背景信息

具体的配置和介绍请参见《HUAWEI NetEngine80E/40E 路由器 配置指南-IP 组播》的“二层组播配置。”

8.17 维护以太网 OAM

通过维护以太网 OAM，可以实现清除 CCM 消息统计数据、监控以太网 OAM 的运行状况。

8.17.1 清除错误 CCM 消息统计信息

在查看一段时间内的 CCM 的统计信息之前，建议清除 BFD 的统计信息。

背景信息



注意

清除错误 CCM 消息统计信息后，以前的信息将无法恢复，务必仔细确认。

操作步骤

步骤 1 在确认需要清除错误 CCM 消息统计信息后，请在用户视图下执行 **reset cfm error-packet receive statistics [md md-name [ma ma-name [remote-mep mep-id mep-id]]]** 命令。

----结束

8.17.2 监控以太网 OAM 运行状况

通过监控以太网运行状况，可以了解运行过程中以太网 OAM 的相关信息。

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解以太网 OAM 的运行状况。

操作步骤

- 在任意视图下执行 **display oam global configuration** 命令，查看当前设备的以太网 OAM 全局配置。
- 在任意视图下执行 **display cfm error-packet statistics [md md-name [ma ma-name [remote-mep mep-id mep-id]]]**命令，查看当前设备接收错误 CCM 消息的统计信息。
- 在任意视图下执行 **display cfm mep [md md-name [ma ma-name [mep-id mep-id]]]**命令，查看 MEP 的信息。
- 在任意视图下执行 **display cfm mip [interface interface-type interface-number | level level]**命令，查看 MIP 的信息。
- 在任意视图下执行 **display cfm remote-mep [md md-name ma ma-name mep-id mep-id | [md md-name [ma ma-name [mep-id mep-id]]]]**命令，查看 RMEP 的信息。
- 在任意视图下执行 **display efm session { all | interface interface-type interface-number }**命令，查看指定接口和对端的 EFM OAM 会话信息。

----结束

8.18 配置举例

介绍 BFD 快速检测链路的各种示例。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

背景信息



说明

手册中所使用的链路接口编号和链路类型以 NE40E-X8 为例，实际使用时以现网设备为准。

8.18.1 配置 EFM OAM 示例

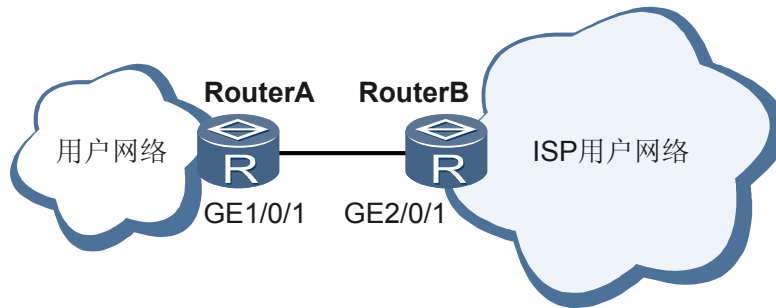
本示例中，通过在 CE 和 UPE 上配置 EFM OAM 功能，检测这两台设备之间的链路连通性。

组网需求

如图 8-16 所示，某用户网络通过 RouterA 和 RouterB 设备连接到 ISP 网络上。其中，RouterA 是 CE 设备，RouterB 是 UPE 设备。要求：

- 实现 RouterA 和 RouterB 之间连通性故障自动检测功能，并且如检测到连通性故障 RouterA 设备和 RouterB 设备上产生报警信息。
- RouterB 监测本设备上的接口 GE2/0/1 的误帧、误码和误帧秒，如误帧、误码和误帧秒超过设定的门限值则 RouterB 设备上产生报警信息。

图 8-16 配置 EFM OAM 示例组网图



配置思路

采用如下的思路配置 EFM OAM：

1. 全局使能 RouterA 和 RouterB 的 EFM OAM 功能。
2. 配置 RouterA 的接口 GE1/0/1 的 EFM OAM 工作模式为被动模式。
3. 在 RouterB 上配置接口 GE2/0/1 的误帧、误码、误帧秒检测功能。
4. 使能 RouterB 的接口 GE2/0/1 和 RouterA 的接口 GE1/0/1 的 EFM OAM 功能。

数据准备

为完成此配置例，需准备如下的数据：

- RouterB 上接口 GE2/0/1 的误帧观察时长为 5 秒，门限为 5。
- RouterB 上接口 GE2/0/1 的误码观察时长为 5 秒，门限为 5。
- RouterB 上接口 GE2/0/1 的误帧秒观察时长为 120 秒，门限为 5。

操作步骤

步骤 1 全局使能 EFM OAM 功能

全局使能 RouterA 的 EFM OAM 功能。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] efm enable
```

全局使能 RouterB 的 EFM OAM 功能。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] efm enable
```

步骤 2 配置 RouterA 的接口 GE1/0/1 的 EFM OAM 工作模式为被动模式

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] efm mode passive
```

步骤 3 在 RouterB 上配置接口 GE2/0/1 的误帧、误码、误帧秒检测功能

在 RouterB 上配置接口 GE2/0/1 的误帧检测功能。

```
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] efm error-frame period 5
```

```
[RouterB-GigabitEthernet2/0/1] efm error-frame threshold 5
[RouterB-GigabitEthernet2/0/1] efm error-frame notification enable

# 在 RouterB 上配置接口 GE2/0/1 的误码检测功能。

[RouterB-GigabitEthernet2/0/1] efm error-code period 5
[RouterB-GigabitEthernet2/0/1] efm error-code threshold 5
[RouterB-GigabitEthernet2/0/1] efm error-code notification enable

# 在 RouterB 上配置接口 GE2/0/1 的误帧秒检测功能。

[RouterB-GigabitEthernet2/0/1] efm error-frame-second period 120
[RouterB-GigabitEthernet2/0/1] efm error-frame-second threshold 5
[RouterB-GigabitEthernet2/0/1] efm error-frame-second notification enable
```

步骤 4 使能 RouterB 的接口 GE2/0/1 和 RouterA 的接口 GE1/0/1 的 EFM OAM 功能

```
# 使能 RouterA 的接口 GE1/0/1 的 EFM OAM 功能。

[RouterA-GigabitEthernet1/0/1] efm enable
[RouterA-GigabitEthernet1/0/1] quit

# 使能 RouterB 的接口 GE2/0/1 的 EFM OAM 功能。

[RouterB-GigabitEthernet2/0/1] efm enable
[RouterB-GigabitEthernet2/0/1] quit
```

步骤 5 检查配置结果

如果 RouterA 和 RouterB 的 EFM OAM 配置正确，接口 GE2/0/1 和接口 GE1/0/1 成功协商后进入握手阶段，此时在 RouterA 或 RouterB 上执行 **display efm session** 命令，可看到接口 GE2/0/1 或接口 GE1/0/1 的 EFM OAM 协议状态为 detect。

```
[RouterB] display efm session interface gigabitethernet 2/0/1
Interface          EFM State          Loopback Timeout
-----
GigabitEthernet2/0/1  detect              --
```

如果 RouterB 上接口 GE2/0/1 的误帧、误码、误帧秒检测功能配置正确，执行命令 **display efm**，接口的 EFM OAM 配置信息如下：

```
[RouterB] display efm interface gigabitethernet 2/0/1
Item              Value
-----
Interface:        GigabitEthernet2/0/1
EFM Enable Flag:  enable
Mode:             active
OAMPDU MaxSize:   128
OAMPDU Timeout:   5000
ErrCodeNotification: enable
ErrCodePeriod:    5
ErrCodeThreshold: 5
ErrFrameNotification: enable
ErrFramePeriod:   5
ErrFrameThreshold: 5
ErrFrameSecondNotification: enable
ErrFrameSecondPeriod: 120
ErrFrameSecondThreshold: 5
Hold Up Time:     0
ThresholdEvtTriggerErrDown: disable
TriggerIfDown:    disable
Remote MAC:       0010-0010-0010
Remote EFM Enable Flag: enable
Remote Mode:      passive
Remote MaxSize:   128
Remote State:     --
```

----结束

配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
efm enable
#
interface GigabitEthernet1/0/1
  efm mode passive
  efm enable
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
efm enable
#
interface GigabitEthernet2/0/1
  efm enable
  efm error-frame period 5
  efm error-frame threshold 5
  efm error-frame notification enable
  efm error-frame-second period 120
  efm error-frame-second threshold 5
  efm error-frame-second notification enable
  efm error-code period 5
  efm error-code threshold 5
  efm error-code notification enable
#
return
```

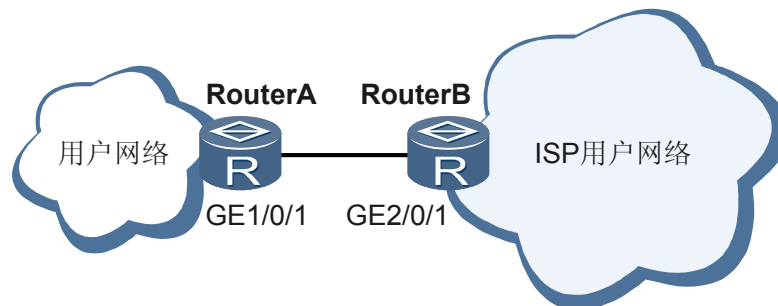
8.18.2 配置链路丢包率检测示例

本示例中，通过在 CE 和 UPE 上配置 EFM OAM 功能，可以检测物理链路的丢包率，以使用户能够采取有效的措施来保证链路更好的工作。

组网需求

如图 8-17 所示，某用户网络准备通过 RouterA 和 RouterB 连接到 ISP 网络上。其中，RouterA 是 CE 设备，RouterB 是 UPE 设备。由于 RouterA 和 RouterB 之间的链路是一条新搭建的链路，在正式启用前，ISP 需要在 RouterB 上对该链路进行丢包率测试。

图 8-17 测试链路丢包率示例组网图



配置思路

采用如下的思路测试链路丢包率：

1. 在 RouterA 和 RouterB 上配置 EFM OAM 基本功能，并将 RouterA 的接口 GE1/0/1 的 EFM OAM 工作模式配置为被动模式。
2. 在 RouterB 上配置 EFM OAM 远端环回。
3. 从 RouterB 向 RouterA 发送测试报文。
4. 在 RouterB 上查看测试报文的返回情况。

数据准备

为完成此配置例，需准备如下的数据：

- EFM OAM 远端环回的超时时间
- 测试报文的大小、数量和发送速率

操作步骤

步骤 1 配置 EFM OAM 基本功能

全局使能 RouterB 的 EFM OAM 功能。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] efm enable
```

全局使能 RouterA 的 EFM OAM 功能。

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] efm enable
```

配置 RouterA 的 GE1/0/1 接口的 EFM OAM 工作模式为被动模式。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] efm mode passive
```

使能 RouterA 上接口 GE1/0/1 的 EFM OAM 功能。

```
[RouterA-GigabitEthernet1/0/1] efm enable
[RouterA-GigabitEthernet1/0/1] quit
```

使能 RouterB 上接口 GE2/0/1 的 EFM OAM 功能。

```
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] efm enable
[RouterB-GigabitEthernet2/0/1] quit
```

检查配置结果。

如果 RouterA 和 RouterB 的 EFM OAM 配置正确，接口 GE2/0/1 和接口 GE1/0/1 成功协商后进入握手阶段，此时在 RouterA 或 RouterB 上执行 **display efm session** 命令，可看到接口 GE2/0/1 或接口 GE1/0/1 的 EFM OAM 协议状态为 detect。

```
[RouterB] display efm session interface gigabitethernet 2/0/1
  Interface          EFM State          Loopback Timeout
-----
GigabitEthernet2/0/1  detect              --
```

步骤 2 配置 EFM OAM 远端环回

在 RouterB 上配置 EFM OAM 远端环回。

```
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] efm loopback start
[RouterB-GigabitEthernet2/0/1] quit
```

检查配置结果。

配置 EFM OAM 远端环回成功后，在 RouterB 上执行 **display efm session** 命令，可以看到接口 GE2/0/1 的 EFM OAM 协议状态为 Loopback(control)，即远端环回状态（且为远端环回的发起方）。

```
[RouterB] display efm session interface gigabitethernet2/0/1
Interface          EFM State          Loopback Timeout
-----
GigabitEthernet2/0/1  Loopback(control)  20
```

配置 EFM OAM 远端环回成功后，在 RouterA 上执行 **display efm session** 命令，可以看到接口 GE1/0/1 的 EFM OAM 协议状态为 Loopback(be controlled)，即远端环回状态（且为远端环回的响应方）。

```
[RouterA] display efm session interface gigabitethernet1/0/1
Interface          EFM State          Loopback Timeout
-----
GigabitEthernet1/0/1  Loopback(be controlled)  --
```

配置 EFM OAM 远端环回成功后，在 RouterB 上执行 **display efm session** 命令，可以看到接口对远端环回的处理方式。

```
[RouterB] display efm session interface gigabitethernet2/0/1
Item                Value
-----
Interface:           GigabitEthernet2/0/1
EFM Enable Flag:     enable
Mode:                active

OAMPDU MaxSize:      128
OAMPDU Timeout:      3000
ErrCodeNotification: disable
ErrCodePeriod:       1
ErrCodeThreshold:    1
ErrFrameNotification: disable
ErrFramePeriod:      1
ErrFrameThreshold:   1
ErrFrameSecondNotification: disable
ErrFrameSecondPeriod: 60
ErrFrameSecondThreshold: 1
Hold Up Time:        0
ThresholdEvtTriggerErrDown: --
TriggerIfDown:       disable
TriggerMacRenew:     disable
Remote MAC:          00e0-c97e-a500
Remote EFM Enable Flag: enable
Remote Mode:         active
Remote MaxSize:      128

Remote State:        --
```

步骤 3 从 RouterB 向 RouterA 发送测试报文

```
[RouterB] test-packet start interface gigabitethernet 2/0/1
please waiting..
Info: The test is complete.
```

步骤 4 在 RouterB 上查看测试报文的返回情况

```
[RouterB] display test-packet result
TestResult          Value
-----
```

```
PacketsSend :          5
PacketsReceive :       5
PacketsLost :          0
BytesSend :            320
BytesReceive :         320
BytesLost :            0
StartTime :            07-06-2007 09:41:41
EndTime :              07-06-2007 09:41:41
```

根据以上数据可计算链路的丢包率。

步骤 5 取消 EFM OAM 远端环回

```
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] efm loopback stop
[RouterB-GigabitEthernet2/0/1] quit
```

说明

缺省情况下，远端环回的超时时间是 20 分钟，到达此时间，远端环回自动停止。如果需要提前取消远端环回，可执行以上步骤。

步骤 6 检查配置结果

在远端环回自动取消或手动取消后，在 RouterA 或 RouterB 上执行 **display efm session** 命令，可以看到链路两端接口的 EFM OAM 协议状态为 Detect 或 Discovery，即握手状态或对端发现状态。例如：

```
[RouterB] display efm session interface gigabitethernet2/0/1
Interface          EFM State          Loopback Timeout
-----
GigabitEthernet2/0/1  detect              --
```

----结束

配置文件

● RouterA 的配置文件

```
#
sysname RouterA
#
 efm enable
#
interface GigabitEthernet1/0/1
 efm mode passive
 efm enable
#
return
```

● RouterB 的配置文件

```
#
sysname RouterB
#
 efm enable
#
interface GigabitEthernet2/0/1
 efm enable
#
return
```

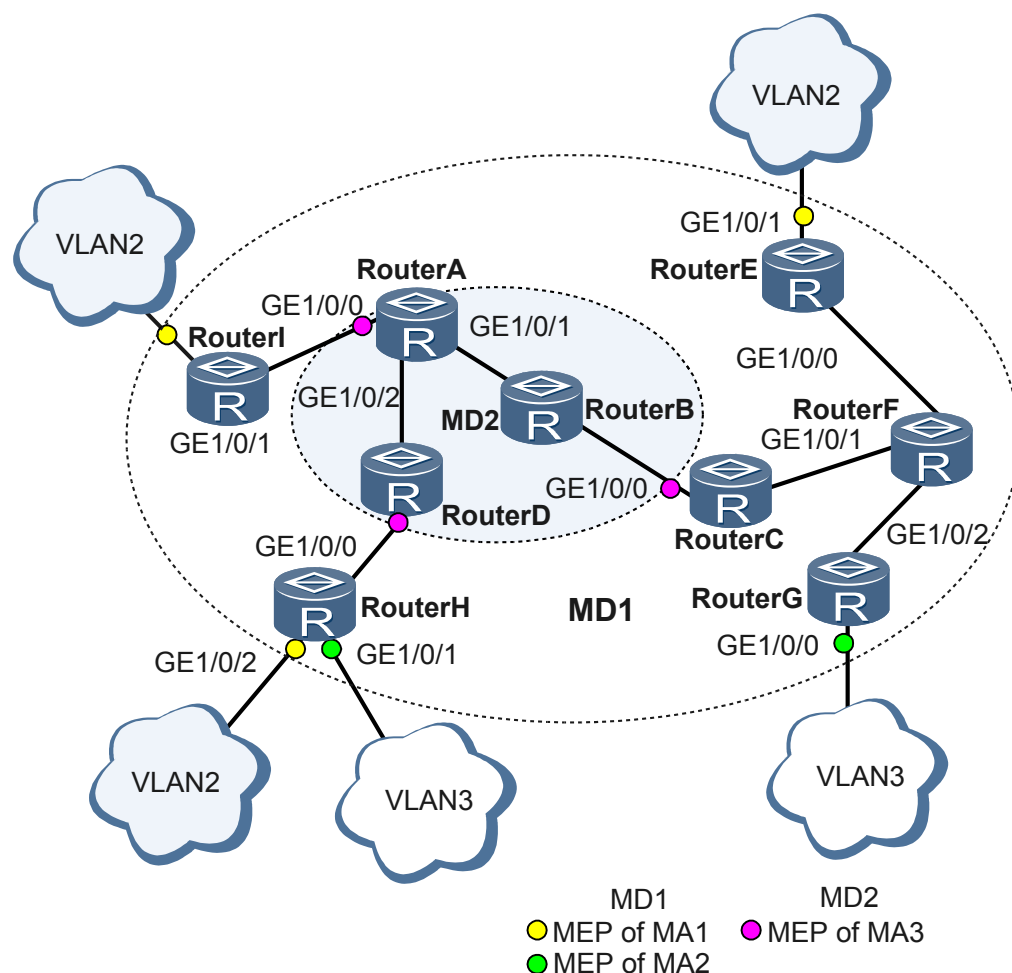
8.18.3 配置以太网 CFM 基本功能示例

本示例中，通过配置以太网 CFM 基本功能，实现端到端的连通性故障检测功能。

组网需求

如图 8-18 所示的以太网由两个 ISP 管理，其中 RouterA、RouterB、RouterD 由 ISP1 管理，RouterC、RouterE、RouterF、RouterG、RouterH、RouterI 由 ISP2 管理。要求在该网络中实现连通性故障检测功能。

图 8-18 配置以太网 CFM 基本功能示例组网图



配置思路

采用如下的思路配置以太网 CFM 基本功能：

1. 创建 VLAN，并将相关接口加入对应的 VLAN。
2. 在所有设备上创建 MD1，MD1 的级别为 6。
3. 在除 RouterG 外的所有设备上的 MD1 下创建并配置 MA1。（MA1 和 VLAN2 关联。）
4. 在除 RouterE、RouterI 外的所有设备上的 MD1 下创建并配置 MA2。（MA2 和 VLAN3 关联。）
5. 在 RouterA、RouterB、RouterC、RouterD 上创建 MD2，MD2 的级别为 4；并在 MD2 下创建并配置 MA3。（MA3 和 VLAN4 关联。）

6. 在 RouterI、RouterH、RouterE 上的 MD1 的 MA1 下创建 MEP 和 RMEP。
7. 在 RouterH、RouterG 上的 MD1 的 MA2 下配置 MEP 和 RMEP。
8. 在 RouterA、RouterC、RouterD 上的 MD2 的 MA3 下配置 MEP 和 RMEP。
9. 使能 CCM 消息的发送和接收功能。

数据准备

为完成此配置例，需准备如下的数据。

- MD1 的级别为 6
- MD2 的级别为 4

操作步骤

步骤 1 创建 VLAN，并将相关接口加入对应的 VLAN（略）

步骤 2 创建 MD1

在 RouterA 上创建 MD1。

```
<RouterA> system-view
[RouterA] cfm enable
Info: Operation succeeded.
[RouterA] cfm md md1 level 6
```

在 RouterB、RouterC、RouterD、RouterE、RouterF、RouterG、RouterH、RouterI 上创建 MD1。

略。与在 RouterA 上创建 MD1 的方法类似，此处不再赘述。

步骤 3 在除 RouterG 外的所有设备上的 MD1 下创建并配置 MA1

在 RouterA 上的 MD1 下创建并配置 MA1。

```
[RouterA-md-md1] ma ma1
[RouterA-md-md1-ma-ma1] map vlan 2
[RouterA-md-md1-ma-ma1] quit
```

在 RouterB、RouterC、RouterD、RouterE、RouterF、RouterH、RouterI 上的 MD1 下创建并配置 MA1。

略。与在 RouterA 上的 MD1 下创建并配置 MA1 的方法类似，此处不再赘述。

步骤 4 在除 RouterE、RouterI 外的所有设备上的 MD1 下创建并配置 MA2

在 RouterA 上的 MD1 下创建并配置 MA2。

```
[RouterA-md-md1] ma ma2
[RouterA-md-md1-ma-ma2] map vlan 3
[RouterA-md-md1-ma-ma2] quit
[RouterA-md-md1] quit
```

在 RouterB、RouterC、RouterD、RouterF、RouterG、RouterH 上的 MD1 下创建并配置 MA2。

略。与在 RouterA 上的 MD1 下创建并配置 MA2 的方法类似，此处不再赘述。

步骤 5 在 RouterA、RouterB、RouterC、RouterD 上创建 MD2，并在 MD2 下创建并配置 MA3

在 RouterA 上创建 MD2，并在 MD2 下创建并配置 MA3。

```
[RouterA] cfm md md2 level 4
[RouterA-md-md2] ma ma3
[RouterA-md-md2-ma-ma3] map vlan 4
[RouterA-md-md2-ma-ma3] quit
[RouterA-md-md2] quit
```

在 RouterB、RouterC、RouterD 上创建 MD2，并在 MD2 下创建并配置 MA3。

略。与在 RouterA 上创建 MD2，并在 MD2 下创建并配置 MA3 的方法类似，此处不再赘述。

步骤 6 在 RouterE、RouterH、RouterI 上的 MD1 的 MA1 下配置 MEP 和 RMEP

在 RouterE 上的 MD1 的 MA1 下配置 MEP。

```
[RouterE] cfm md md1
[RouterE-md-md1] ma ma1
[RouterE-md-md1-ma-ma1] mep mep-id 3 interface gigabitethernet 1/0/1 inward
```

在 RouterH 上的 MD1 的 MA1 下配置 MEP。

```
[RouterH] cfm md md1
[RouterH-md-md1] ma ma1
[RouterH-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet 1/0/2 inward
```

在 RouterI 上的 MD1 的 MA1 下配置 MEP。

```
[RouterI] cfm md md1
[RouterI-md-md1] ma ma1
[RouterI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 1/0/1 inward
```

在 RouterE 上的 MD1 的 MA1 下配置 RMEP。

```
[RouterE-md-md1-ma-ma1] remote-mep mep-id 1
[RouterE-md-md1-ma-ma1] remote-mep mep-id 2
```

在 RouterH 上的 MD1 的 MA1 下配置 RMEP。

```
[RouterH-md-md1-ma-ma1] remote-mep mep-id 1
[RouterH-md-md1-ma-ma1] remote-mep mep-id 3
```

在 RouterI 上的 MD1 的 MA1 下配置 RMEP。

```
[RouterI-md-md1-ma-ma1] remote-mep mep-id 2
[RouterI-md-md1-ma-ma1] remote-mep mep-id 3
```

步骤 7 在 RouterH、RouterG 上的 MD1 的 MA2 下配置 MEP 和 RMEP

在 RouterH 上的 MD1 的 MA2 下配置 MEP。

```
[RouterH] cfm md md1
[RouterH-md-md1] ma ma2
[RouterH-md-md1-ma-ma2] mep mep-id 1 interface gigabitethernet 1/0/1 inward
```

在 RouterG 上的 MD1 的 MA2 下配置 MEP。

```
[RouterG] cfm md md1
[RouterG-md-md1] ma ma2
[RouterG-md-md1-ma-ma2] mep mep-id 2 interface gigabitethernet 1/0/0 inward
```

在 RouterH 上的 MD1 的 MA2 下配置 RMEP。

```
[RouterH-md-md1-ma-ma2] remote-mep mep-id 2
```

在 RouterG 上的 MD1 的 MA2 下配置 RMEP。

```
[RouterG-md-md1-ma-ma2] remote-mep mep-id 1
```

步骤 8 在 RouterA、RouterC、RouterD 上的 MD2 的 MA3 下配置 MEP 和 RMEP

在 RouterA 上的 MD2 的 MA3 下配置 MEP。

```
[RouterA] cfm md md2
[RouterA-md-md2] ma ma3
[RouterA-md-md2-ma-ma3] mep mep-id 1 interface gigabitethernet 1/0/0 inward
```

在 RouterC 上的 MD2 的 MA3 下配置 MEP。

```
[RouterC] cfm md md2
[RouterC-md-md2] ma ma3
[RouterC-md-md2-ma-ma3] mep mep-id 2 interface gigabitethernet 1/0/1 outward
```

在 RouterD 上的 MD2 的 MA3 下配置 MEP。

```
[RouterD] cfm md md2
[RouterD-md-md2] ma ma3
[RouterD-md-md2-ma-ma3] mep mep-id 3 interface gigabitethernet 1/0/0 inward
```

在 RouterA 上的 MD2 的 MA3 下配置 RMEP。

```
[RouterA-md-md2-ma-ma3] remote-mep mep-id 2
[RouterA-md-md2-ma-ma3] remote-mep mep-id 3
```

在 RouterC 上的 MD2 的 MA3 下配置 RMEP。

```
[RouterC-md-md2-ma-ma3] remote-mep mep-id 1
[RouterC-md-md2-ma-ma3] remote-mep mep-id 3
```

在 RouterD 上的 MD2 的 MA3 下配置 RMEP。

```
[RouterD-md-md2-ma-ma3] remote-mep mep-id 1
[RouterD-md-md2-ma-ma3] remote-mep mep-id 2
```

步骤 9 使能 CCM 消息的发送和接收功能

在 RouterA 上使能所有 MEP 的 CCM 消息发送功能。

```
[RouterA-md-md2-ma-ma3] mep ccm-send enable
```

在 RouterA 上使能接收所有 RMEP 发送的 CCM 消息功能。

```
[RouterA-md-md2-ma-ma3] remote-mep ccm-receive enable
```

在 RouterB、RouterC、RouterD、RouterE、RouterF、RouterG、RouterH、RouterI 上使能所有 MEP 的 CCM 消息发送功能，并使能接收所有 RMEP 发送的 CC 报文功能。

略。与在 RouterA 上使能所有 MEP 的 CCM 消息发送功能和使能接收所有 RMEP 发送的 CCM 消息功能的配置方法类似，此处不再赘述。

----结束

配置文件

● RouterA 的配置文件

```
#
sysname RouterA
#
vlan batch 2 to 4
#
cfm enable
#
interface GigabitEthernet1/0/0
portswitch
port trunk allow-pass vlan 2 to 4
#
```

```
interface GigabitEthernet1/0/1
 portswitch
 port trunk allow-pass vlan 2 to 4
#
interface GigabitEthernet1/0/2
 portswitch
 port trunk allow-pass vlan 2 to 4
#
 cfm md md1 level 6
  ma ma1
   map vlan 2
  ma ma2
   map vlan 3
#
 cfm md md2 level 4
  ma ma3
   map vlan 4
  mep mep-id 1 interface gigabitethernet 1/0/0 inward
  mep ccm-send mep-id 1 enable
  remote-mep mep-id 2
  remote-mep ccm-receive mep-id 2 enable
  remote-mep mep-id 3
  remote-mep ccm-receive mep-id 3 enable
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
vlan batch 2 to 4
#
 cfm enable
#
interface GigabitEthernet1/0/0
 portswitch
 port trunk allow-pass vlan 2 to 4
#
interface GigabitEthernet1/0/1
 portswitch
 port trunk allow-pass vlan 2 to 4
#
 cfm md md1 level 6
  ma ma1
   map vlan 2
  ma ma2
   map vlan 3
#
 cfm md md2 level 4
  ma ma3
   map vlan 4
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
vlan batch 2 to 4
#
 cfm enable
#
interface GigabitEthernet1/0/0
 portswitch
 port trunk allow-pass vlan 2 to 4
#
interface GigabitEthernet1/0/1
 portswitch
 port trunk allow-pass vlan 2 to 4
#
```

```

cfm md md1 level 6
  ma ma1
  map vlan 2
  ma ma2
  map vlan 3
#
cfm md md2 level 4
  ma ma3
  map vlan 4
  mep mep-id 2 interface gigabitethernet 1/0/0 outward
  mep ccm-send mep-id 2 enable
  remote-mep mep-id 1
  remote-mep ccm-receive mep-id 1 enable
  remote-mep mep-id 3
  remote-mep ccm-receive mep-id 3 enable
#
return

```

● RouterD 的配置文件

```

#
sysname RouterD
#
vlan batch 2 to 4
#
cfm enable
#
interface GigabitEthernet1/0/0
  portswitch
  port trunk allow-pass vlan 2 to 4
#
interface GigabitEthernet1/0/2
  portswitch
  port trunk allow-pass vlan 2 to 4
#
cfm md md1 level 6
  ma ma1
  map vlan 2
  ma ma2
  map vlan 3
#
cfm md md2 level 4
  ma ma3
  map vlan 4
  mep mep-id 3 interface gigabitethernet 1/0/0 inward
  mep ccm-send mep-id 3 enable
  remote-mep mep-id 1
  remote-mep ccm-receive mep-id 1 enable
  remote-mep mep-id 2
  remote-mep ccm-receive mep-id 2 enable
#
return

```

● RouterE 的配置文件

```

#
sysname RouterE
#
vlan batch 2
#
cfm enable
#
interface GigabitEthernet1/0/0
  portswitch
  port trunk allow-pass vlan 2
#
interface GigabitEthernet1/0/1
  portswitch
  port trunk allow-pass vlan 2
#
cfm md md1 level 6
  ma ma1

```

```

        map vlan 2
        mep mep-id 3 interface gigabitethernet 1/0/1 inward
        mep ccm-send mep-id 3 enable
        remote-mep mep-id 1
        remote-mep ccm-receive mep-id 1 enable
        remote-mep mep-id 2
        remote-mep ccm-receive mep-id 2 enable
    #
    return

```

● RouterF 的配置文件

```

#
sysname RouterF
#
vlan batch 2 to 3
#
cfm enable
#
interface GigabitEthernet1/0/0
    portswitch
    port trunk allow-pass vlan 2
#
interface GigabitEthernet1/0/1
    portswitch
    port trunk allow-pass vlan 2 to 3
#
interface GigabitEthernet1/0/2
    portswitch
    port trunk allow-pass vlan 3
#
cfm md md1 level 6
    ma ma1
    map vlan 2
    ma ma2
    map vlan 3
#
return

```

● RouterG 的配置文件

```

#
sysname RouterG
#
vlan batch 3
#
cfm enable
#
interface GigabitEthernet1/0/0
    portswitch
    port trunk allow-pass vlan 3
#
interface GigabitEthernet1/0/2
    portswitch
    port trunk allow-pass vlan 3
#
cfm md md1 level 6
    ma ma2
    map vlan 3
    mep mep-id 2 interface gigabitethernet 1/0/0 inward
    mep ccm-send mep-id 2 enable
    remote-mep mep-id 1
    remote-mep ccm-receive mep-id 1 enable
#
return

```

● RouterH 的配置文件

```

#
sysname RouterH
#
vlan batch 2 to 3

```

```
#
cfm enable
#
interface GigabitEthernet1/0/0
 portswitch
 port trunk allow-pass vlan 2 to 3
#
interface GigabitEthernet1/0/1
 portswitch
 port trunk allow-pass vlan 3
#
interface GigabitEthernet1/0/2
 portswitch
 port trunk allow-pass vlan 2
#
cfm md mdl level 6
 ma ma1
  map vlan 2
  mep mep-id 2 interface gigabitethernet 1/0/2 inward
  mep ccm-send mep-id 2 enable
  remote-mep mep-id 1
  remote-mep ccm-receive mep-id 1 enable
  remote-mep mep-id 3
  remote-mep ccm-receive mep-id 3 enable
 ma ma2
  map vlan 3
  mep mep-id 1 interface gigabitethernet 1/0/1 inward
  mep ccm-send mep-id 1 enable
  remote-mep mep-id 2
  remote-mep ccm-receive mep-id 2 enable
#
return
```

- RouterI 的配置文件

```
#
sysname RouterI
#
vlan batch 2
#
cfm enable
#
interface GigabitEthernet1/0/0
 portswitch
 port trunk allow-pass vlan 2
#
interface GigabitEthernet1/0/1
 portswitch
 port trunk allow-pass vlan 2
#
cfm md mdl level 6
 ma ma1
  map vlan 2
  mep mep-id 1 interface gigabitethernet 1/0/1 inward
  mep ccm-send mep-id 1 enable
  remote-mep mep-id 2
  remote-mep ccm-receive mep-id 2 enable
  remote-mep mep-id 3
  remote-mep ccm-receive mep-id 3 enable
#
return
```

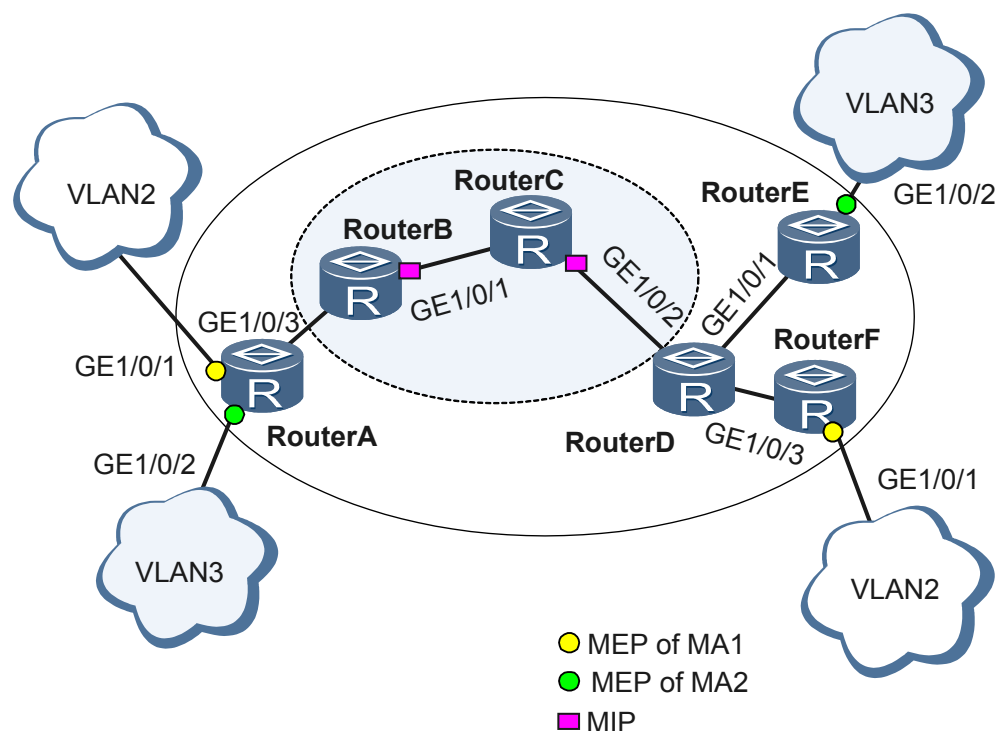
8.18.4 配置以太网 CFM 默认 MD 功能示例

本示例中，可以在低级别的 MD 设备上配置默认 MD，高级别 MD 能感知低级别 MD 中拓扑结构的变化。

组网需求

如图 8-19 所示的以太网由两个 ISP 管理，其中 RouterB 和 RouterC 由 ISP1 管理，RouterA、RouterD、RouterE 和 RouterF 由 ISP2 管理。通过在低级别的 MD 设备上配置默认 MD 实现网络中连通性故障检测功能。

图 8-19 配置以太网 CFM 默认 MD 功能示例组网图



配置思路

采用如下的思路配置以太网 CFM 默认 MD 功能：

1. 将版本切换为标准版本。
2. 创建 VLAN，并将相关接口加入对应的 VLAN。
3. 在除 RouterB、RouterC 外的所有设备上创建 MD1，MD1 的级别为 6。
在 RouterB、RouterC 设备上创建 MD2，MD2 的级别为 4。
4. 在 RouterB、RouterC 上创建默认 MD，默认 MD 级别为 6，关联 VLAN2 和 VLAN3，MIP 创建规则为 default。
5. 在除 RouterE 外的所有设备上的 MD1 下创建并配置 MA1。（MA1 和 VLAN2 关联。）
在除 RouterF 外的所有设备上的 MD1 下创建并配置 MA2。（MA2 和 VLAN3 关联。）
6. 在 RouterA、RouterF 上的 MD1 的 MA1 下创建 MEP 和 RMEP。
在 RouterA、RouterE 上的 MD1 的 MA2 下配置 MEP 和 RMEP。
7. 使能 CCM 消息的发送和接收功能。

数据准备

为完成此配置例，需准备如下的数据。

- 接口所属 VLAN ID 的范围
- MD1 的级别为 6
- MD2 的级别为 4
- 默认 MD 的级别为 6

操作步骤

步骤 1 切换版本



说明

缺省情况下，设备启用的是 draft7 草案版本。

在 RouterA 上，将版本切换为标准版本。

```
<RouterA> system-view
[RouterA] cfm version standard
Warning: Warning: CFM will be disabled before the version of CFM is changed, and
all information about the MD will be deleted . Continue?[Y/N]:y
Info: Succeeded in changing the version of CFM.
```

在 RouterB、RouterC、RouterD、RouterE、RouterF 上，将版本切换为标准版本。

略。与在 RouterA 上切换版本的方法类似，此处不再赘述。



说明

整网中的设备使用的版本必须一致，要么都是 draft7 版本要么都是 standard 标准版本，两个版本不能混用。

步骤 2 创建 VLAN，并将相关接口加入对应的 VLAN（略）

步骤 3 创建 MD1

在 RouterA 上创建 MD1。

```
<RouterA> system-view
[RouterA] cfm enable
Info: Enable the CFM successfully!
[RouterA] cfm md md1 level 6
[RouterA] quit
```

在 RouterD、RouterE、RouterF 上创建 MD1。

略。与在 RouterA 上创建 MD1 的方法类似，此处不再赘述。

步骤 4 创建 MD2

在 RouterB 上创建 MD2。

```
<RouterB> system-view
[RouterB] cfm enable
Info: Enable the CFM successfully!
[RouterB] cfm md md2 level 4
[RouterB] quit
```

在 RouterC 上创建 MD2。

略。与在 RouterB 上创建 MD2 的方法类似，此处不再赘述。

步骤 5 在 RouterB、RouterC 上创建默认 MD，并关联 VLAN2 和 VLAN3

在 RouterB 上创建默认 MD 并关联 VLAN2 和 VLAN3。

```
<RouterB> system-view
[RouterB] cfm default md level 6
[RouterB-default-md] vlan 2 to 3
[RouterB-default-md] quit
```

在 RouterC 上创建默认 MD，并关联 VLAN2 和 VLAN3。

略。与在 RouterB 上创建默认 MD 的方法类似，此处不再赘述。

步骤 6 在 RouterB、RouterC 上配置默认 MD 内的 MIP 生成规则

在 RouterB 上配置默认 MD 内的 MIP 生成规则。

```
<RouterB> system-view
[RouterB] cfm default md
[RouterB-default-md] mip create-type default
[RouterB-default-md] quit
```

在 RouterC 上配置默认 MD 内的 MIP 生成规则。

略。与在 RouterB 上配置默认 MD 内的 MIP 生成规则的方法类似，此处不再赘述。

步骤 7 在除 RouterB、RouterC 外的所有设备上的 MD1 下创建并配置 MA1

在 RouterA 上的 MD1 下创建并配置 MA1。

```
[RouterA] cfm md md1
[RouterA-md-md1] ma ma1
[RouterA-md-md1-ma-ma1] map vlan 2
[RouterA-md-md1-ma-ma1] quit
```

在 RouterD、RouterF 上的 MD1 下创建并配置 MA1。

略。与在 RouterA 上的 MD1 下创建并配置 MA1 的方法类似，此处不再赘述。

步骤 8 在除 RouterB、RouterC 外的所有设备上的 MD1 下创建并配置 MA2

在 RouterA 上的 MD1 下创建并配置 MA2。

```
[RouterA-md-md1] ma ma2
[RouterA-md-md1-ma-ma2] map vlan 3
[RouterA-md-md1-ma-ma2] quit
[RouterA-md-md1] quit
```

在 RouterD、RouterE 上的 MD1 下创建并配置 MA2。

略。与在 RouterA 上的 MD1 下创建并配置 MA2 的方法类似，此处不再赘述。

步骤 9 在 RouterA、RouterF 上的 MD1 的 MA1 下配置 MEP 和 RMEP

在 RouterA 上的 MD1 的 MA1 下配置 MEP。

```
[RouterA] cfm md md1
[RouterA-md-md1] ma ma1
[RouterA-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet 1/0/1 inward
```

在 RouterF 上的 MD1 的 MA1 下配置 MEP。

```
[RouterF] cfm md md1
[RouterF-md-md1] ma ma1
[RouterF-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 1/0/1 inward
```

在 RouterA 上的 MD1 的 MA1 下配置 RMEP。

```
[RouterA-md-md1-ma-ma1] remote-mep mep-id 1
```

在 RouterF 上的 MD1 的 MA1 下配置 RMEP。

```
[RouterF-md-md1-ma-ma1] remote-mep mep-id 2
```

步骤 10 在 RouterA、RouterE 上的 MD1 的 MA2 下配置 MEP 和 RMEP

在 RouterA 上的 MD1 的 MA2 下配置 MEP。

```
[RouterA] cfm md md1
```

```
[RouterA-md-md1] ma ma2
```

```
[RouterA-md-md1-ma-ma2] mep mep-id 1 interface gigabitethernet 1/0/2 inward
```

在 RouterE 上的 MD1 的 MA2 下配置 MEP。

```
[RouterE] cfm md md1
```

```
[RouterE-md-md1] ma ma2
```

```
[RouterE-md-md1-ma-ma2] mep mep-id 2 interface gigabitethernet 1/0/2 inward
```

在 RouterA 上的 MD1 的 MA2 下配置 RMEP。

```
[RouterA-md-md1-ma-ma2] remote-mep mep-id 2
```

在 RouterE 上的 MD1 的 MA2 下配置 RMEP。

```
[RouterE-md-md1-ma-ma2] remote-mep mep-id 1
```

步骤 11 使能 CCM 消息的发送和接收功能

在 RouterA 上使能所有 MEP 的 CCM 消息发送功能。

```
[RouterA-md-md1-ma-ma2] mep ccm-send enable
```

在 RouterA 上使能接收所有 RMEP 发送的 CCM 消息功能。

```
[RouterA-md-md1-ma-ma2] remote-mep ccm-receive enable
```

在 RouterE、RouterF 使能所有 MEP 的 CCM 消息发送功能，并使能接收所有 RMEP 发送的 CC 报文功能。

略。与在 RouterA 上使能所有 MEP 的 CCM 消息发送功能和使能接收所有 RMEP 发送的 CCM 消息功能的配置方法类似，此处不再赘述。

步骤 12 检查配置结果

经过以上配置，在网络稳定后，执行以下操作，验证配置结果。以 RouterA 和 RouterB 为例。

- 在 RouterB 上执行 **display cfm default md** 命令，查看结果如下：

```
[RouterB] display cfm default md
```

Level	MIP Create-type	SenderID	TLV-type	VLAN List

6	default	Defer	2 to 3	

可以看到 RouterB 上配置了级别为 6 的默认 MD 并关联了 VLAN2 和 VLAN3，MIP 节点的生成规则为 default。

- 在 RouterA 上执行 802.1ag MAC Trace 操作，可以看到 RouterA 和 RouterE 之间没有发生连通性故障，802.1ag MAC Trace 操作执行成功。查看结果如下：

```
<RouterA> system
```

```
[RouterA] cfm md md1
```

```
[RouterA-md-md1] ma ma1
```

```
[RouterA-md-md1-ma-ma1] trace mac-8021ag mac aa99-6600-5600
```

Tracing the route to aa99-6600-5600 over a maximum of 255 hops:

Hops	Mac	Ingress	Ingress Action	Relay Action

	Forwarded	Egress	Egress Action	Is mep
1	2155-2201-3302	gigabitethernet1/0/3	IngOK	
RlyFDB				
	Forwarded	gigabitethernet1/0/1	EgrOK	No
2	5522-1101-5503	gigabitethernet1/0/1	IngOK	
RlyFDB				
	Forwarded	gigabitethernet1/0/2	EgrOk	No
3	2234-6432-3344	gigabitethernet1/0/2	IngOK	
RlyFDB				
	Forwarded	gigabitethernet1/0/3	EgrOk	No
4	4323-5332-5522	gigabitethernet1/0/3	IngOK	
RlyFDB				
	Forwarded	gigabitethernet1/0/1	EgrOk	No
5	aa99-6600-5600	gigabitethernet1/0/1	IngOK	
RlyHit				
	Not Forwarded			Yes
Info: Succeed in tracing the destination address aa99-6600-5600.				

----结束

配置文件

- RouterA 的配置文件的配置内容

```
#
sysname RouterA
#
vlan batch 2 to 3
#
cfm version standard
cfm enable
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port trunk allow-pass vlan 2
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port trunk allow-pass vlan 3
#
interface GigabitEthernet1/0/3
undo shutdown
portswitch
port trunk allow-pass vlan 2 to 3
#
cfm md md1 level 6
ma ma1
map vlan 2
mep mep-id 2 interface gigabitethernet 1/0/1 inward
mep ccm-send mep-id 2 enable
remote-mep mep-id 1
remote-mep ccm-receive mep-id 1 enable
ma ma2
map vlan 3
mep mep-id 1 interface gigabitethernet 1/0/2 inward
mep ccm-send mep-id 1 enable
remote-mep mep-id 2
remote-mep ccm-receive mep-id 2 enable
#
return
```
- RouterB 的配置文件的配置内容

```
#
sysname RouterB
#
vlan batch 2 to 3
#
```

```

cfm version standard
cfm enable
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port trunk allow-pass vlan 2 to 3
#
interface GigabitEthernet1/0/3
undo shutdown
portswitch
port trunk allow-pass vlan 2 to 3
#
cfm md md2 level 4
#
cfm default md level 6
mip create-type default
vlan 2 to 3
#
return

```

● RouterC 的配置文件

```

#
sysname RouterC
#
vlan batch 2 to 3
#
cfm version standard
cfm enable
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port trunk allow-pass vlan 2 to 3
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port trunk allow-pass vlan 2 to 3
#
cfm md md2 level 4
#
cfm default md level 6
mip create-type default
vlan 2 to 3
#
return

```

● RouterD 的配置文件

```

#
sysname RouterD
#
vlan batch 2 to 3
#
cfm version standard
cfm enable
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port trunk allow-pass vlan 2 to 3
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port trunk allow-pass vlan 2 to 3
#
interface GigabitEthernet1/0/3
undo shutdown
portswitch

```

```
port trunk allow-pass vlan 2 to 3
#
cfm md md1 level 6
ma ma1
map vlan 2
ma ma2
map vlan 3
#
return
```

● RouterE 的配置文件

```
#
sysname RouterE
#
vlan batch 3
#
cfm version standard
cfm enable
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port trunk allow-pass vlan 3
#
interface GigabitEthernet1/0/2
undo shutdown
portswitch
port trunk allow-pass vlan 3
#
cfm md md1 level 6
ma ma2
map vlan 3
mep mep-id 2 interface gigabitethernet 1/0/2 inward
mep ccm-send mep-id 2 enable
remote-mep mep-id 1
remote-mep ccm-receive mep-id 1 enable
#
return
```

● RouterF 的配置文件

```
#
sysname RouterF
#
vlan batch 2
#
cfm version standard
cfm enable
#
interface GigabitEthernet1/0/1
undo shutdown
portswitch
port trunk allow-pass vlan 2
#
interface GigabitEthernet1/0/3
undo shutdown
portswitch
port trunk allow-pass vlan 2
#
cfm md md1 level 6
ma ma1
map vlan 2
mep mep-id 1 interface gigabitethernet 1/0/1 inward
mep ccm-send mep-id 1 enable
remote-mep mep-id 2
remote-mep ccm-receive mep-id 2 enable
#
return
```

8.18.5 配置以太网 CFM 和接口联动示例

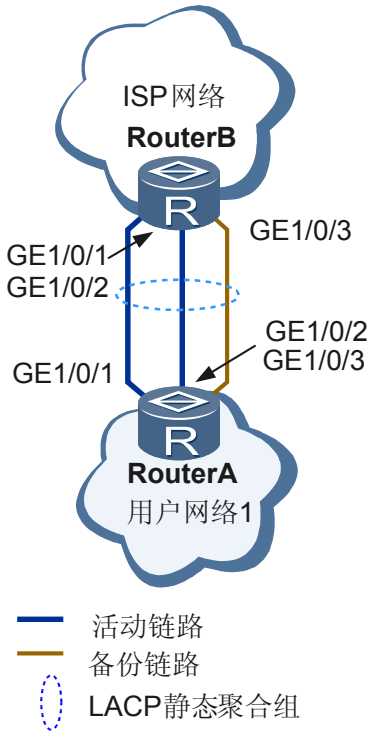
本示例中，通过配置以太网 CFM 和接口联动，实现 CE 和 UPE 之间的链路出现故障时，LACP 能够感知该故障。

组网需求

在如图 8-20 所示的网络中，用户网络通过 RouterA 和 RouterB 接入到 ISP 网络中。其中 RouterA 是 CE 设备，RouterB 是 UPE 设备。要求：

- 用户网络到 ISP 网络的接入带宽为 2000Mbit/s，并需要提供备份接入链路。
- 在用户网络和 ISP 网络之间的工作链路出现故障时，LACP 在 50ms 内感知到该故障，并停止通过该工作链路转发数据。

图 8-20 配置以太网 CFM 和接口联动示例组网图



配置思路

采用如下的思路配置静态 LACP 聚合组快速故障检测功能：

1. 在 RouterA 和 RouterB 上分别配置包括 3 个成员接口的静态 LACP 聚合组，3 个成员接口均为 GE 接口。
2. 在 RouterA 和 RouterB 上分别配置以太网 CFM 功能。为满足 50ms 内感知到连通性故障的要求，将各 MA 内发送和探测 CCM 消息的时间间隔配置为 10ms。
3. 在 RouterA 和 RouterB 上分别配置静态 LACP 聚合组成员接口和以太网 CFM 联动功能。

数据准备

为完成此配置例，需准备如下的数据。

- 在 RouterA 和 RouterB 上静态 LACP 聚合组的编号均为 2。
- 在 RouterB 上静态 LACP 聚合组的 3 个成员接口的名称分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2 和 GigabitEthernet1/0/3。
- 在 RouterA 上静态 LACP 聚合组的 3 个成员接口的名称分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2 和 GigabitEthernet1/0/3。

操作步骤

步骤 1 配置静态 LACP 聚合组

略。详细配置请参见《HUAWEI NetEngine80E/40E 路由器 配置指南-局域网与城域网接入》。

步骤 2 配置以太网 CFM 功能

在 RouterA 上全局使能以太网 CFM。

```
[RouterA] cfm enable
```

在 RouterA 上创建 MD、MA、MEP 和 RMEP

```
[RouterA] cfm md md1
[RouterA-md-md1] ma ma1
[RouterA-md-md1-ma-ma1] ccm-interval 10
[RouterA-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet 1/0/1 outward
[RouterA-md-md1-ma-ma1] remote-mep mep-id 1
[RouterA-md-md1-ma-ma1] mep ccm-send enable
[RouterA-md-md1-ma-ma1] remote-mep ccm-receive enable
[RouterA-md-md1-ma-ma1] quit
[RouterA-md-md1] ma ma2
[RouterA-md-md1-ma-ma2] ccm-interval 10
[RouterA-md-md1-ma-ma2] mep mep-id 4 interface gigabitethernet 1/0/2 outward
[RouterA-md-md1-ma-ma2] remote-mep mep-id 3
[RouterA-md-md1-ma-ma2] mep ccm-send enable
[RouterA-md-md1-ma-ma2] remote-mep ccm-receive enable
[RouterA-md-md1-ma-ma2] quit
[RouterA-md-md1] ma ma3
[RouterA-md-md1-ma-ma3] ccm-interval 10
[RouterA-md-md1-ma-ma3] mep mep-id 6 interface gigabitethernet 1/0/3 outward
[RouterA-md-md1-ma-ma3] remote-mep mep-id 5
[RouterA-md-md1-ma-ma3] mep ccm-send enable
[RouterA-md-md1-ma-ma3] remote-mep ccm-receive enable
[RouterA-md-md1-ma-ma3] quit
[RouterA-md-md1] quit
```

在 RouterB 上全局使能以太网 CFM。

```
[RouterB] cfm enable
```

在 RouterB 上创建 MD、MA、MEP 和 RMEP

```
[RouterB] cfm md md1
[RouterB-md-md1] ma ma1
[RouterB-md-md1-ma-ma1] ccm-interval 10
[RouterB-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 1/0/1 outward
[RouterB-md-md1-ma-ma1] remote-mep mep-id 2
[RouterB-md-md1-ma-ma1] mep ccm-send enable
[RouterB-md-md1-ma-ma1] remote-mep ccm-receive enable
[RouterB-md-md1-ma-ma1] quit
[RouterB-md-md1] ma ma2
[RouterB-md-md1-ma-ma2] ccm-interval 10
```

```
[RouterB-md-md1-ma-ma2] mep mep-id 3 interface gigabitethernet 1/0/2 outward
[RouterB-md-md1-ma-ma2] remote-mep mep-id 4
[RouterB-md-md1-ma-ma2] mep ccm-send enable
[RouterB-md-md1-ma-ma2] remote-mep ccm-receive enable
[RouterB-md-md1-ma-ma2] quit
[RouterB-md-md1] ma ma3
[RouterB-md-md1-ma-ma3] ccm-interval 10
[RouterB-md-md1-ma-ma3] mep mep-id 5 interface gigabitethernet 1/0/3 outward
[RouterB-md-md1-ma-ma3] remote-mep mep-id 6
[RouterB-md-md1-ma-ma3] mep ccm-send enable
[RouterB-md-md1-ma-ma3] remote-mep ccm-receive enable
[RouterB-md-md1-ma-ma3] quit
[RouterB-md-md1] quit
[RouterB] quit
```

检查配置结果。

RouterA 和 RouterB 上的以太网 CFM 功能配置成功后，在 RouterA 或 RouterB 上执行 **display cfm mep** 命令和 **display cfm remote-mep** 命令，显示结果如下：

```
[RouterB] display cfm mep md md1
MD Name          : md1
MD Name Format    : string
Level            : 0
MA Name          : ma1
MA Name Format    : string
MEP ID           : 1
Vlan ID          : --
VSI Name         : --
Interface Name    : GigabitEthernet1/0/1
CCM Send         : enabled
Direction        : outward
MD Name          : md1
MD Name Format    : string
Level            : 0
MA Name          : ma2
MA Name Format    : string
MEP ID           : 3
Vlan ID          : --
VSI Name         : --
Interface Name    : GigabitEthernet1/0/2
CCM Send         : enabled
Direction        : outward
MD Name          : md1
MD Name Format    : string
Level            : 0
MA Name          : ma3
MA Name Format    : string
MEP ID           : 5
Vlan ID          : --
VSI Name         : --
Interface Name    : GigabitEthernet1/0/3
CCM Send         : enabled
Direction        : outward
[RouterB] display cfm remote-mep md md1
The total number of RMEPs is 3
The status of RMEPs : 3 up, 0 down
```

```
-----
MD Name          : md1
Level            : 0
MA Name          : ma1
RMEP ID          : 2
Vlan ID          : --
VSI Name         : --
MAC              : --
CCM Receive      : enabled
Trigger-If-Down  : disabled
CFM Status       : up
MD Name          : md1
```

```
Level          : 0
MA Name        : ma2
RMEP ID        : 4
Vlan ID        : --
VSI Name       : --
MAC            : --
CCM Receive    : enabled
Trigger-If-Down : disabled
CFM Status     : up
MD Name        : md1
Level          : 0
MA Name        : ma3
RMEP ID        : 6
Vlan ID        : --
VSI Name       : --
MAC            : --
CCM Receive    : enabled
Trigger-If-Down : disabled
CFM Status     : up
```

步骤 3 配置静态 LACP 聚合组成员接口和以太网 CFM 联动功能

在 RouterA 上配置 Eth-Trunk2 的成员接口和以太网 CFM 联动。

```
[RouterA] interface gigabitethernet1/0/1
[RouterA-GigabitEthernet1/0/1] cfm md md1 ma ma1 remote-mep mep-id 1 trigger if-down
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet1/0/2
[RouterA-GigabitEthernet1/0/2] cfm md md1 ma ma2 remote-mep mep-id 3 trigger if-down
[RouterA-GigabitEthernet1/0/2] quit
[RouterA] interface gigabitethernet1/0/3
[RouterA-GigabitEthernet1/0/3] cfm md md1 ma ma3 remote-mep mep-id 5 trigger if-down
[RouterA-GigabitEthernet1/0/3] quit
```

在 RouterB 上配置 Eth-Trunk2 的成员接口和以太网 CFM 联动。

```
[RouterB] interface gigabitethernet1/0/1
[RouterB-GigabitEthernet1/0/1] cfm md md1 ma ma1 remote-mep mep-id 2 trigger if-down
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet1/0/2
[RouterB-GigabitEthernet1/0/2] cfm md md1 ma ma2 remote-mep mep-id 4 trigger if-down
[RouterB-GigabitEthernet1/0/2] quit
[RouterB] interface gigabitethernet1/0/3
[RouterB-GigabitEthernet1/0/3] cfm md md1 ma ma3 remote-mep mep-id 6 trigger if-down
[RouterB-GigabitEthernet1/0/3] quit
```

检查配置结果。

配置接口和以太网 CFM 联动功能成功后，在 RouterA 或 RouterB 上执行 **display cfm remote-mep** 命令，在显示信息中 Trigger-If-down 项目的值应为 enable。例如：

```
[RouterB] display cfm remote-mep md md1
The total number of RMEPs is 3
MD Name          : md1
Level            : 0
MA Name          : ma1
RMEP ID          : 2
Vlan ID          : --
VSI Name         : --
MAC              : --
CCM Receive      : enabled
Trigger-If-Down  : enabled
CFM Status       : up
MD Name          : md1
Level            : 0
MA Name          : ma2
RMEP ID          : 4
Vlan ID          : --
VSI Name         : --
```

```
MAC                : --
CCM Receive        : enabled
Trigger-If-Down    : enabled
CFM Status         : up
MD Name            : md1
Level              : 0
MA Name            : ma3
RMEP ID            : 6
Vlan ID            : --
VSI Name           : --
MAC                : --
CCM Receive        : enabled
Trigger-If-Down    : enabled
CFM Status         : up
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 cfm enable
#
interface Eth-Trunk2
 portswitch
 mode lacp-static
#
interface GigabitEthernet1/0/1
 eth-trunk 2
 cfm md md1 ma ma1 remote-mep mep-id 1 trigger if-down
#
interface GigabitEthernet1/0/2
 eth-trunk 2
 cfm md md1 ma ma2 remote-mep mep-id 3 trigger if-down
#
interface GigabitEthernet1/0/3
 eth-trunk 2
 cfm md md1 ma ma3 remote-mep mep-id 5 trigger if-down
#
 cfm md md1
  ma ma1
   ccm-interval 10
   mep mep-id 2 interface GigabitEthernet1/0/1 outward
   mep ccm-send mep-id 2 enable
   remote-mep mep-id 1
   remote-mep ccm-receive mep-id 1 enable
  ma ma2
   ccm-interval 10
   mep mep-id 4 interface GigabitEthernet1/0/2 outward
   mep ccm-send mep-id 4 enable
   remote-mep mep-id 3
   remote-mep ccm-receive mep-id 3 enable
  ma ma3
   ccm-interval 10
   mep mep-id 6 interface GigabitEthernet1/0/3 outward
   mep ccm-send mep-id 6 enable
   remote-mep mep-id 5
   remote-mep ccm-receive mep-id 5 enable
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 lacp priority 100
```

```
#
 cfm enable
#
interface Eth-Trunk2
 portswitch
 mode lacp-static
 max bandwidth-affected-linknumber 2
#
interface GigabitEthernet1/0/1
 eth-trunk 2
 lacp priority 2000
 cfm md md1 ma ma1 remote-mep mep-id 2 trigger if-down
#
interface GigabitEthernet1/0/2
 eth-trunk 2
 lacp priority 2000
 cfm md md1 ma ma2 remote-mep mep-id 4 trigger if-down
#
interface GigabitEthernet1/0/3
 eth-trunk 2
 cfm md md1 ma ma3 remote-mep mep-id 6 trigger if-down
#
 cfm md md1
  ma ma1
   ccm-interval 10
   mep mep-id 1 interface GigabitEthernet1/0/1 outward
   mep ccm-send mep-id 1 enable
   remote-mep mep-id 2
   remote-mep ccm-receive mep-id 2 enable
  ma ma2
   ccm-interval 10
   mep mep-id 3 interface GigabitEthernet1/0/2 outward
   mep ccm-send mep-id 3 enable
   remote-mep mep-id 4
   remote-mep ccm-receive mep-id 4 enable
  ma ma3
   ccm-interval 10
   mep mep-id 5 interface GigabitEthernet1/0/3 outward
   mep ccm-send mep-id 5 enable
   remote-mep mep-id 6
   remote-mep ccm-receive mep-id 6 enable
#
return
```

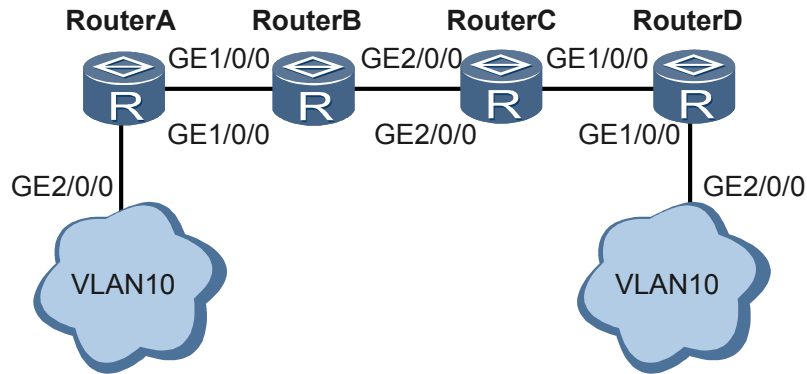
8.18.6 配置 EFM OAM 和以太网 CFM 联动示例

本示例中，通过配置 EFM OAM 和以太网 CFM 联动功能，实现故障信息的传递。

组网需求

如图 8-21 所示，为了实现端到端链路故障检测，在 RouterA 和 RouterB 之间配置 EFM OAM，在 RouterB 与 RouterC 之间配置以太网 CFM，RouterC 与 RouterD 之间配置 EFM OAM。当 RouterA 与 RouterB 之间有链路故障发生时，触发以太网 CFM 向远端 RouterD 设备发故障告警。当 RouterC 与 RouterD 之间有链路故障发生时，触发以太网 CFM 向远端 RouterA 设备发故障告警。

图 8-21 配置 EFM 和 CFM 联动示例组网图



配置思路

采用如下的思路配置 EFM OAM 和以太网 CFM 联动功能：

1. 创建 VLAN，并将相关接口加入对应的 VLAN。
2. 在 RouterA 和 RouterB 之间配置 EFM OAM 功能。
3. 在 RouterB 和 RouterC 之间配置以太网 CFM 功能。
4. 在 RouterC 和 RouterD 之间配置 EFM OAM 功能。
5. 在 RouterB 和 RouterC 上配置 EFM OAM 和以太网 CFM 的联动功能。

操作步骤

步骤 1 创建 VLAN10，并将相关接口加入对应的 VLAN。

步骤 2 配置 RouterA 和 RouterB 的 EFM OAM 功能。

配置 RouterA。

```
[RouterA] efm enable
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] efm mode passive
[RouterA-GigabitEthernet1/0/0] efm enable
[RouterA-GigabitEthernet1/0/0] quit
```

配置 RouterB。

```
[RouterB] efm enable
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] efm enable
[RouterB-GigabitEthernet1/0/0] quit
```

步骤 3 配置 RouterB 和 RouterC 之间的以太网 CFM 功能。

配置 RouterB。

```
[RouterB] cfm enable
[RouterB] cfm md mdl
[RouterB-md-mdl] ma ma1
[RouterB-md-mdl-ma-ma1] map vlan 10
[RouterB-md-mdl-ma-ma1] mep mep-id 1 interface gigabitethernet 2/0/0 outward
[RouterB-md-mdl-ma-ma1] remote-mep mep-id 2
[RouterB-md-mdl-ma-ma1] mep ccm-send enable
[RouterB-md-mdl-ma-ma1] remote-mep ccm-receive enable
```

```
[RouterB-md-md1-ma-mal] return
```

配置 RouterC。

```
[RouterC] cfm enable
[RouterC] cfm md md1
[RouterC-md-md1] ma mal
[RouterC-md-md1-ma-mal] map vlan 10
[RouterC-md-md1-ma-mal] mep mep-id 2 interface gigabitethernet 2/0/0 outward
[RouterC-md-md1-ma-mal] remote-mep mep-id 1
[RouterC-md-md1-ma-mal] mep ccm-send enable
[RouterC-md-md1-ma-mal] remote-mep ccm-receive enable
[RouterC-md-md1-ma-mal] return
```

步骤 4 配置 RouterC 和 RouterD 之间的 EFM OAM 功能。

配置 RouterC。

```
[RouterC] efm enable
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] efm enable
[RouterC-GigabitEthernet1/0/0] quit
```

配置 RouterD。

```
[RouterD] efm enable
[RouterD] interface gigabitethernet 1/0/0
[RouterD-GigabitEthernet1/0/0] efm mode passive
[RouterD-GigabitEthernet1/0/0] efm enable
[RouterD-GigabitEthernet1/0/0] quit
```

步骤 5 配置 EFM OAM 和以太网 CFM 的联动。

配置 RouterA 与 RouterB 之间的 EFM OAM 和 RouterB 与 RouterC 之间的以太网 CFM 的双向联动。

```
[RouterB] oam-mgr
[RouterB-oam-mgr] oam-bind cfm md md1 ma mal efm interface gigabitethernet 1/0/0
```

配置 RouterB 与 RouterC 之间的以太网 CFM 和 RouterC 与 RouterD 之间的 EFM OAM 的双向联动。

```
[RouterC] oam-mgr
[RouterC-oam-mgr] oam-bind cfm md md1 ma mal efm interface gigabitethernet 1/0/0
```

步骤 6 检查配置结果。

完成上述配置后，RouterA 和 RouterB 之间 EFM OAM 检测到的故障，可以通过以太网 CFM 通告给 RouterC 和 RouterD 之间的 EFM OAM。

----结束

配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
vlan batch 10
#
efm enable
#
interface GigabitEthernet1/0/0
portswitch
port trunk allow-pass vlan 10
efm mode passive
efm enable
```

```
#
interface GigabitEthernet2/0/0
 portswitch
 port trunk allow-pass vlan 10
#
return
```

● RouterB 的配置文件

```
#
sysname RouterB
#
vlan batch 10
#
efm enable
#
cfm enable
#
interface GigabitEthernet1/0/0
 portswitch
 port trunk allow-pass vlan 10
 efm enable
#
interface GigabitEthernet2/0/0
 portswitch
 port trunk allow-pass vlan 10
#
 cfm md mdl
 ma mal
 map vlan 10
 mep mep-id 1 interface gigabitethernet 2/0/0 outward
 mep ccm-send enable
 remote-mep mep-id 2
 remote-mep ccm-receive enable
#
 oam-mgr
 oam-bind cfm md mdl ma mal efm interface gigabitethernet 1/0/0
#
return
```

● RouterC 配置文件

```
#
sysname RouterC
#
vlan batch 10
#
efm enable
#
cfm enable
#
interface GigabitEthernet2/0/0
 portswitch
 port trunk allow-pass vlan 10
 efm enable
#
interface GigabitEthernet1/0/0
 portswitch
 port trunk allow-pass vlan 10
#
 cfm md mdl
 ma mal
 map vlan 10
 mep mep-id 2 interface gigabitethernet 1/0/0 outward
 mep ccm-send enable
 remote-mep mep-id 1
 remote-mep ccm-receive enable
#
 oam-mgr
 oam-bind cfm md mdl ma mal efm interface gigabitethernet 1/0/0
#
```



```
return
```

● RouterD 配置文件

```
#
sysname RouterD
#
vlan batch 10
#
efm enable
#
interface GigabitEthernet1/0/0
portswitch
port trunk allow-pass vlan 10
efm mode passive
efm enable
#
interface GigabitEthernet2/0/0
portswitch
port trunk allow-pass vlan 10
#
return
```

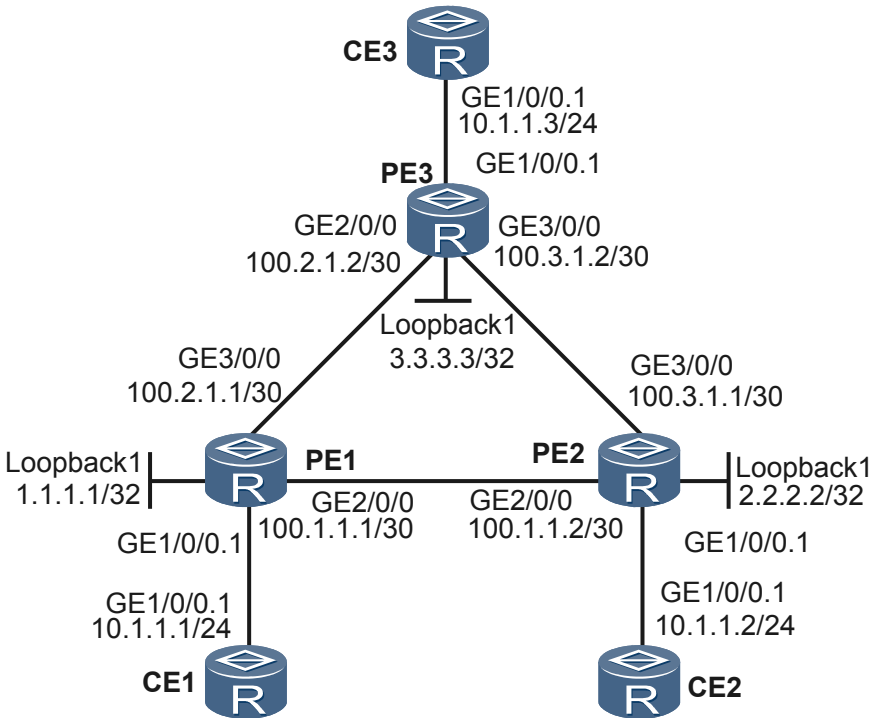
8.18.7 配置基于 VPLS 的以太网 CFM 示例

本示例中，通过配置基于 VPLS 的以太网功能，检测 PE 之间的连通性故障。

组网需求

如图 8-22 所示，骨干网采用 Maritini 方式的 VPLS，使用 LDP 作为信令建立 PW。在 PE 上部署基于 VPLS 的以太网 CFM，用于快速检测 PE 之间的 VPLS 连通性。

图 8-22 配置基于 VPLS 的以太网 CFM 组网图



配置思路

采用如下的思路配置基于 VPLS 的以太网 CFM 的基本功能：

1. 在骨干网上运行 IGP 路由协议，使骨干网各路由器能互通。
2. 在骨干网上配置路由协议实现互通，并使能 MPLS 基本能力。
3. 在 PE 之间建立 LSP 隧道。
4. 在 PE 上使能 MPLS L2VPN。
5. 在 PE 上创建 VSI，并将 VSI 与 AC 接口进行绑定。
6. 在 PE 上配置基于 VPLS 的以太网 CFM。

数据准备

为完成此配置例，需准备如下的数据：

- 接口的 IP 地址。
- 各个 PE 上的 MPLS LSR-ID。
- PE1、PE2 和 PE3 上的 VSI 名称和 VSI-ID。
- 绑定 VSI 的接口。
- 以太网 CFM 中 MD 的名称和级别、MA 的名称和 MEP 的 ID、MEP 所在接口的名称、MEP 的类型。

操作步骤

步骤 1 配置各接口 IP 地址

配置 PE1。

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] interface loopback 1
[PE1-LoopBack1] ip address 1.1.1.1 32
[PE1-LoopBack1] quit
[PE1] interface gigabitethernet 2/0/0
[PE1-GigabitEthernet2/0/0] ip address 100.1.1.1 30
[PE1-GigabitEthernet2/0/0] undo shutdown
[PE1-GigabitEthernet2/0/0] quit
[PE1] interface gigabitethernet 3/0/0
[PE1-GigabitEthernet3/0/0] ip address 100.2.1.1 30
[PE1-GigabitEthernet3/0/0] undo shutdown
[PE1-GigabitEthernet3/0/0] quit
```

配置 PE2。

```
<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] interface LoopBack 1
[PE2-LoopBack1] ip address 2.2.2.2 32
[PE2-LoopBack1] quit
[PE2] interface gigabitethernet 2/0/0
[PE2-GigabitEthernet2/0/0] ip address 100.1.1.2 30
[PE2-GigabitEthernet2/0/0] undo shutdown
[PE2-GigabitEthernet2/0/0] quit
[PE2] interface gigabitethernet 3/0/0
[PE2-GigabitEthernet3/0/0] ip address 100.3.1.1 30
[PE2-GigabitEthernet3/0/0] undo shutdown
[PE2-GigabitEthernet3/0/0] quit
```

配置 PE3。

```
<HUAWEI> system-view
[HUAWEI] sysname PE3
[PE3] interface loopback 1
[PE3-LoopBack1] ip address 3.3.3.3 32
[PE3-LoopBack1] quit
[PE3] interface gigabitethernet 2/0/0
[PE3-GigabitEthernet2/0/0] ip address 100.2.1.2 30
[PE3-GigabitEthernet2/0/0] undo shutdown
[PE3-GigabitEthernet2/0/0] quit
[PE3] interface gigabitethernet 3/0/0
[PE3-GigabitEthernet3/0/0] ip address 100.3.1.2 30
[PE3-GigabitEthernet3/0/0] undo shutdown
[PE3-GigabitEthernet3/0/0] quit
```

步骤 2 配置 MPLS 骨干网的 IGP，本示例中使用 OSPF



说明

配置 OSPF 时，注意需要发布 PE 的 32 位 Loopback 接口地址。

配置 PE1。

```
[PE1] ospf 1
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.3
[PE1-ospf-1-area-0.0.0.0] network 100.2.1.0 0.0.0.3
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

配置 PE2。

```
[PE2] ospf 1
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.3
[PE2-ospf-1-area-0.0.0.0] network 100.3.1.0 0.0.0.3
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

配置 PE3。

```
[PE3] ospf 1
[PE3-ospf-1] area 0
[PE3-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] network 100.2.1.0 0.0.0.3
[PE3-ospf-1-area-0.0.0.0] network 100.3.1.0 0.0.0.3
[PE3-ospf-1-area-0.0.0.0] quit
[PE3-ospf-1] quit
```

完成此步骤后，PE1 和 PE2、PE1 和 PE3 之间通过 OSPF 协议发现的对方 Loopback1 的 IP 路由。

以 PE1 的显示为例：

```
[PE1] display ip routing-table
```

Route Flags: R - relied, D - download to fib

Routing Tables: Public

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
Destinations : 12 Routes : 13						
1.1.1.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
2.2.2.2/32	OSPF	10	2	D	100.1.1.2	GigabitEthernet2/0/0
3.3.3.3/32	OSPF	10	2	D	100.2.1.2	GigabitEthernet3/0/0
100.1.1.0/30	Direct	0	0	D	100.1.1.1	GigabitEthernet2/0/0
100.1.1.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0/0/0
100.1.1.2/32	Direct	0	0	D	100.1.1.2	GigabitEthernet2/0/0
100.3.1.0/30	OSPF	10	2	D	100.1.1.2	GigabitEthernet2/0/0
	OSPF	10	2	D	100.2.1.2	GigabitEthernet3/0/0
100.2.1.0/30	Direct	0	0	D	100.2.1.1	GigabitEthernet3/0/0

100.2.1.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0/0/0
100.2.1.2/32	Direct	0	0	D	100.2.1.2	Gigabitethernet3/0/0
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0

步骤 3 在 MPLS 骨干网上使能 MPLS 基本能力和 LDP

```
# 配置 PE1。

[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface gigabitethernet 2/0/0
[PE1-Gigabitethernet2/0/0] mpls
[PE1-Gigabitethernet2/0/0] mpls ldp
[PE1-Gigabitethernet2/0/0] quit
[PE1] interface gigabitethernet 3/0/0
[PE1-Gigabitethernet3/0/0] mpls
[PE1-Gigabitethernet3/0/0] mpls ldp
[PE1-Gigabitethernet3/0/0] quit
```

```
# 配置 PE2。

[PE2] mpls lsr-id 2.2.2.2
[PE2] mpls
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface gigabitethernet2/0/0
[PE2-Gigabitethernet2/0/0] mpls
[PE2-Gigabitethernet2/0/0] mpls ldp
[PE2-Gigabitethernet2/0/0] quit
[PE2] interface gigabitethernet3/0/0
[PE2-Gigabitethernet3/0/0] mpls
[PE2-Gigabitethernet3/0/0] mpls ldp
[PE2-Gigabitethernet3/0/0] quit
```

```
# 配置 PE3。

[PE3] mpls lsr-id 3.3.3.3
[PE3] mpls
[PE3-mpls] quit
[PE3] mpls ldp
[PE3-mpls-ldp] quit
[PE3] interface gigabitethernet 2/0/0
[PE3-Gigabitethernet2/0/0] mpls
[PE3-Gigabitethernet2/0/0] mpls ldp
[PE3-Gigabitethernet2/0/0] quit
[PE3] interface gigabitethernet 3/0/0
[PE3-Gigabitethernet3/0/0] mpls
[PE3-Gigabitethernet3/0/0] mpls ldp
[PE3-Gigabitethernet3/0/0] quit
```

上述配置完成后，PE 之间应能建立 LDP 会话，执行 **display mpls ldp session** 命令可以看到显示结果中 Status 项为“Operational”。

以 PE1 的显示为例：

```
[PE1] display mpls ldp session
      LDP Session(s) in Public Network
-----
Peer-ID           Status      LAM  SsnRole  SsnAge      KA-Sent/Rcv
-----
2.2.2.2:0         Operational DU   Passive 000:00:02  10/10
3.3.3.3:0         Operational DU   Passive 000:00:02  9/9
-----
TOTAL: 2 session(s) Found.
```

LAM : Label Advertisement Mode SsnAge Unit : DDD:HH:MM

 说明

如果 PE 之间非直连，还需要使用 **mpls ldp remote-peer** 和 **remote-ip** 命令，在 PE 之间建立远端 LDP 会话。

步骤 4 在 PE 上使能 MPLS L2VPN

配置 PE1。

```
[PE1] mpls l2vpn  
[PE1-l2vpn] quit
```

配置 PE2。

```
[PE2] mpls l2vpn  
[PE2-l2vpn] quit
```

配置 PE3。

```
[PE3] mpls l2vpn  
[PE3-l2vpn] quit
```

步骤 5 创建 VSI，指定 VSI 的信令为 LDP

配置 PE1。

```
[PE1] vsi ldpl static  
[PE1-vsi-ldpl] pwsignal ldp  
[PE1-vsi-ldpl-ldp] vsi-id 2  
[PE1-vsi-ldpl-ldp] peer 2.2.2.2  
[PE1-vsi-ldpl-ldp] peer 3.3.3.3
```

配置 PE2。

```
[PE2] vsi ldpl static  
[PE2-vsi-ldpl] pwsignal ldp  
[PE2-vsi-ldpl-ldp] vsi-id 2  
[PE2-vsi-ldpl-ldp] peer 1.1.1.1  
[PE2-vsi-ldpl-ldp] peer 3.3.3.3
```

配置 PE3。

```
[PE3] vsi ldpl static  
[PE3-vsi-ldpl] pwsignal ldp  
[PE3-vsi-ldpl-ldp] vsi-id 2  
[PE3-vsi-ldpl-ldp] peer 1.1.1.1  
[PE3-vsi-ldpl-ldp] peer 2.2.2.2
```

步骤 6 配置 VSI 与 AC 接口绑定，并将 CE 接入 PE。

配置 PE1。

```
[PE1] interface gigabitethernet 1/0/0.1  
[PE1-GigabitEthernet1/0/0.1] vlan-type dot1q 10  
[PE1-GigabitEthernet1/0/0.1] l2 binding vsi ldpl  
[PE1-GigabitEthernet1/0/0.1] undo shutdown  
[PE1-GigabitEthernet1/0/0.1] quit
```

配置 PE2。

```
[PE2] interface gigabitethernet 1/0/0.1  
[PE2-GigabitEthernet1/0/0.1] vlan-type dot1q 10  
[PE2-GigabitEthernet1/0/0.1] l2 binding vsi ldpl  
[PE2-GigabitEthernet1/0/0.1] undo shutdown  
[PE2-GigabitEthernet1/0/0.1] quit
```

配置 PE3。

```
[PE3] interface gigabitethernet 1/0/0.1
[PE3-GigabitEthernet1/0/0.1] vlan-type dot1q 10
[PE3-GigabitEthernet1/0/0.1] l2 binding vsi ldp1
[PE3-GigabitEthernet1/0/0.1] undo shutdown
[PE3-GigabitEthernet1/0/0.1] quit

# 配置 CE1。

<HUAWEI> system-view
[HUAWEI] sysname CE1
[CE1] interface gigabitethernet 1/0/0.1
[CE1-GigabitEthernet1/0/0.1] vlan-type dot1q 10
[CE1-GigabitEthernet1/0/0.1] ip address 10.1.1.1 24
[CE1-GigabitEthernet1/0/0.1] undo shutdown
[CE1-GigabitEthernet1/0/0.1] quit

# 配置 CE2。

<HUAWEI> system-view
[HUAWEI] sysnameCE2
[CE2] interface gigabitethernet 1/0/0.1
[CE2-GigabitEthernet1/0/0.1] vlan-type dot1q 10
[CE2-GigabitEthernet1/0/0.1] ip address 10.1.1.2 24
[CE2-GigabitEthernet1/0/0.1] undo shutdown
[CE2-GigabitEthernet1/0/0.1] quit

# 配置 CE3。

<HUAWEI> system-view
[HUAWEI] sysnameCE3
[CE3] interface gigabitethernet 1/0/0.1
[CE3-GigabitEthernet1/0/0.1] vlan-type dot1q 10
[CE3-GigabitEthernet1/0/0.1] ip address 10.1.1.3 24
[CE3-GigabitEthernet1/0/0.1] undo shutdown
[CE3-GigabitEthernet1/0/0.1] quit
```

完成上述配置后，在 PE1 上执行 **display vsi name ldp1 verbose** 命令，可以看到名字为 ldp1 的 VSI 建立了到 PE2 和 PE3 的 PW，VSI 状态为 UP。

以 PE1 为例：

```
[PE1] display vsi name bgp1 verbose
***VSI Name          : ldp1
VSI Index            : 0
PW Signaling         : ldp
Member Discovery Style : static
PW MAC Learn Style   : unqualify
Encapsulation Type   : vlan
MTU                  : 1500
VSI State            : up
VSI ID              : 2
*Peer Router ID      : 3.3.3.3
VC Label             : 23552
Peer Type            : dynamic
Session             : up
Tunnel ID            : 0x6002003,
*Peer Router ID      : 2.2.2.2
VC Label             : 23553
Peer Type            : dynamic
Session             : up
Tunnel ID            : 0x6002000,
Interface Name       : GigabitEthernet1/0/0.1
State                : up
**PW Information:
*Peer Ip Address     : 2.2.2.2
PW State            : up
Local VC Label       : 23553
Remote VC Label      : 23552
PW Type             : label
```

```
Tunnel ID          : 0x6002000,  
*Peer Ip Address   : 3.3.3.3  
PW State           : up  
Local VC Label     : 23552  
Remote VC Label    : 23552  
PW Type            : label  
Tunnel ID          : 0x6002003,
```

CE1、CE2 和 CE3 下的主机能够相互 Ping 通。

以 CE1 为例：

```
[CE1] ping 10.1.1.2  
PING 10.1.1.2: 56 data bytes, press CTRL_C to break  
Reply from 10.1.1.2: bytes=56 Sequence=1 ttl=255 time=50 ms  
Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=255 time=1 ms  
Reply from 10.1.1.2: bytes=56 Sequence=3 ttl=255 time=1 ms  
Reply from 10.1.1.2: bytes=56 Sequence=4 ttl=255 time=1 ms  
Reply from 10.1.1.2: bytes=56 Sequence=5 ttl=255 time=1 ms  
--- 10.1.1.2 ping statistics ---  
5 packet(s) transmitted  
5 packet(s) received  
0.00% packet loss  
round-trip min/avg/max = 1/10/50 ms  
[CE1] ping 10.1.1.3  
PING 10.1.1.3: 56 data bytes, press CTRL_C to break  
Reply from 10.1.1.3: bytes=56 Sequence=1 ttl=255 time=1 ms  
Reply from 10.1.1.3: bytes=56 Sequence=2 ttl=255 time=1 ms  
Reply from 10.1.1.3: bytes=56 Sequence=3 ttl=255 time=1 ms  
Reply from 10.1.1.3: bytes=56 Sequence=4 ttl=255 time=1 ms  
Reply from 10.1.1.3: bytes=56 Sequence=5 ttl=255 time=1 ms  
--- 10.1.1.3 ping statistics ---  
5 packet(s) transmitted  
5 packet(s) received  
0.00% packet loss  
round-trip min/avg/max = 1/1/1 ms
```

步骤 7 在 PE 上配置以太网 CFM 功能

配置 PE1。

```
[PE1] cfm enable  
[PE1] cfm md md1  
[PE1-md-md1] ma ma1  
[PE1-md-md1-ma-ma1] ccm-interval 100  
[PE1-md-md1-ma-ma1] map vsi ldpl  
[PE1-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 1/0/0.1 inward  
[PE1-md-md1-ma-ma1] remote-mep mep-id 2  
[PE1-md-md1-ma-ma1] remote-mep mep-id 3  
[PE1-md-md1-ma-ma1] mep ccm-send enable  
[PE1-md-md1-ma-ma1] remote-mep ccm-receive enable  
[PE1-md-md1-ma-ma1] quit
```

配置 PE2。

```
[PE2] cfm enable  
[PE2] cfm md md1  
[PE2-md-md1] ma ma1  
[PE2-md-md1-ma-ma1] ccm-interval 100  
[PE2-md-md1-ma-ma1] map vsi ldpl  
[PE2-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet 1/0/0.1 inward  
[PE2-md-md1-ma-ma1] remote-mep mep-id 1  
[PE2-md-md1-ma-ma1] remote-mep mep-id 3  
[PE2-md-md1-ma-ma1] mep ccm-send enable  
[PE2-md-md1-ma-ma1] remote-mep ccm-receive enable  
[PE2-md-md1-ma-ma1] quit
```

配置 PE3。

```
[PE3] cfm enable
```

```
[PE3] cfm md md1
[PE3-md-md1] ma ma1
[PE3-md-md1-ma-ma1] ccm-interval 100
[PE3-md-md1-ma-ma1] map vsi ldpl
[PE3-md-md1-ma-ma1] mep mep-id 3 interface gigabitethernet 1/0/0.1 inward
[PE3-md-md1-ma-ma1] remote-mep mep-id 1
[PE3-md-md1-ma-ma1] remote-mep mep-id 2
[PE3-md-md1-ma-ma1] mep ccm-send enable
[PE3-md-md1-ma-ma1] remote-mep ccm-receive enable
[PE3-md-md1-ma-ma1] quit
```

步骤 8 检查配置结果

完成上述配置后，在 PE1、PE2 或 PE3 上执行 **display cfm mep** 命令和 **display cfm remote-mep** 命令，可以看到以太网 CFM 已经建立成功。以太网 CFM 能够快速检测到 VSI 的 PE 之间的故障，并通知给网管系统。

以 PE1 为例：

```
[PE1] display cfm mep md md1
The total number of MEPS is 2
MD Name          : md1
MD Name Format    : string
Level            : 0
MA Name          : ma1
MA Name Format    : string
MEP ID           : 2
Vlan ID          : --
VSI Name         : --
Interface Name   : GigabitEthernet1/0/1.1
CCM Send         : enabled
Direction       : inward
MD Name          : md1
MD Name Format    : string
Level            : 0
MA Name          : ma1
MA Name Format    : string
MEP ID           : 3
Vlan ID          : --
VSI Name         : --
Interface Name   : GigabitEthernet1/0/1.1
CCM Send         : enabled
Direction       : inward
[PE1] display cfm remote-mep md md1
The total number of RMEPS is 2
The status of RMEPS : 2 up, 0 down
-----
MD Name          : md1
Level            : 0
MA Name          : ma1
RMEP ID          : 2
Vlan ID          : --
VSI Name         : --
MAC              : --
CCM Receive      : enabled
Trigger-If-Down  : disabled
CFM Status       : up
MD Name          : md1
Level            : 0
MA Name          : ma1
RMEP ID          : 3
Vlan ID          : --
VSI Name         : --
MAC              : --
CCM Receive      : enabled
Trigger-If-Down  : disabled
CFM Status       : up
```

----结束

配置文件

- PE1 的配置文件

```
#
 sysname PE1
#
 cfm enable
#
 mpls lsr-id 1.1.1.1
 mpls
 mpls l2vpn
#
 vsi ldpl static
 pwsignal ldp
 vsi-id 2
 peer 2.2.2.2
 peer 3.3.3.3
#
 mpls ldp
#
 interface GigabitEthernet1/0/0
 undo shutdown
#
 interface GigabitEthernet1/0/0.1
 undo shutdown
 vlan-type dot1q 10
 l2 binding vsi ldpl
#
 interface GigabitEthernet2/0/0
 undo shutdown
 ip address 100.1.1.1 255.255.255.252
 mpls
 mpls ldp
#
 interface GigabitEthernet3/0/0
 undo shutdown
 ip address 100.2.1.1 255.255.255.252
 mpls
 mpls ldp
#
 interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
 cfm md mdl
 ma mal
 ccm-interval 100
 map vsi ldpl
 mep mep-id 1 interface gigabitEthernet 1/0/0.1 inward
 mep ccm-send mep-id 1 enable
 remote-mep mep-id 2
 remote-mep ccm-receive mep-id 2 enable
 remote-mep mep-id 3
 remote-mep ccm-receive mep-id 3 enable
#
 ospf 1
 area 0.0.0.0
 network 1.1.1.1 0.0.0.0
 network 100.1.1.0 0.0.0.3
 network 100.2.1.0 0.0.0.3
#
return
```

- PE2 的配置文件

```
#
 sysname PE2
#
 cfm enable
#
 mpls lsr-id 2.2.2.2
```

```

mpls
mpls l2vpn
#
vsi ldpl static
pwsignal ldp
vsi-id 2
peer 1.1.1.1
peer 3.3.3.3
#
mpls ldp
#
interface GigabitEthernet1/0/0
undo shutdown
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 10
l2 binding vsi ldpl
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 100.1.1.2 255.255.255.252
mpls
mpls ldp
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 100.3.1.1 255.255.255.252
mpls
mpls ldp
#
interface LoopBack1
ip address 2.2.2.2 255.255.255.255
#
cfm md mdl
ma mal
ccm-interval 100
map vsi ldpl
mep mep-id 2 interface gigabitEthernet 1/0/0.1 inward
mep ccm-send mep-id 2 enable
remote-mep mep-id 1
remote-mep ccm-receive mep-id 1 enable
remote-mep mep-id 3
remote-mep ccm-receive mep-id 3 enable
#
ospf 1
area 0.0.0.0
network 2.2.2.2 0.0.0.0
network 100.1.1.0 0.0.0.3
network 100.3.1.0 0.0.0.3
#
return

```

● PE3 的配置文件

```

#
sysname PE3
#
cfm enable
#
mpls lsr-id 3.3.3.3
mpls
mpls l2vpn
#
vsi ldpl static
pwsignal ldp
vsi-id 2
peer 1.1.1.1
peer 2.2.2.2
#
mpls ldp

```

```
#
interface GigabitEthernet1/0/0
 undo shutdown
#
interface GigabitEthernet1/0/0.1
 undo shutdown
 vlan-type dot1q 10
 l2 binding vsi ldp1
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 100.2.1.2 255.255.255.252
 mpls
 mpls ldp
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 100.3.1.2 255.255.255.252
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
cfm md mdl
 ma mal
 ccm-interval 100
 map vsi ldp1
 mep mep-id 3 interface gigabitEthernet 1/0/0.1 inward
 mep ccm-send mep-id 3 enable
 remote-mep mep-id 1
 remote-mep ccm-receive mep-id 1 enable
 remote-mep mep-id 2
 remote-mep ccm-receive mep-id 2 enable
#
ospf 1
 area 0.0.0.0
 network 3.3.3.3 0.0.0.0
 network 100.2.1.0 0.0.0.3
 network 100.3.1.0 0.0.0.3
#
return
```

- CE1 的配置文件

```
#
sysname CE1
#
interface GigabitEthernet1/0/0
 undo shutdown
#
interface GigabitEthernet1/0/0.1
 undo shutdown
 vlan-type dot1q 10
 ip address 10.1.1.1 255.255.255.0
#
return
```

- CE2 的配置文件

```
#
sysname CE2
#
interface GigabitEthernet1/0/0
 undo shutdown
#
interface GigabitEthernet1/0/0.1
 undo shutdown
 vlan-type dot1q 10
 ip address 10.1.1.2 255.255.255.0
#
```

```
return
```

- CE3 的配置文件

```
#
sysname CE3
#
interface GigabitEthernet1/0/0
undo shutdown
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 10
ip address 10.1.1.3 255.255.255.0
#
return
```

8.18.8 配置基于 VPLS 的以太网 CFM 示例（使用 QinQ 终结子接口）

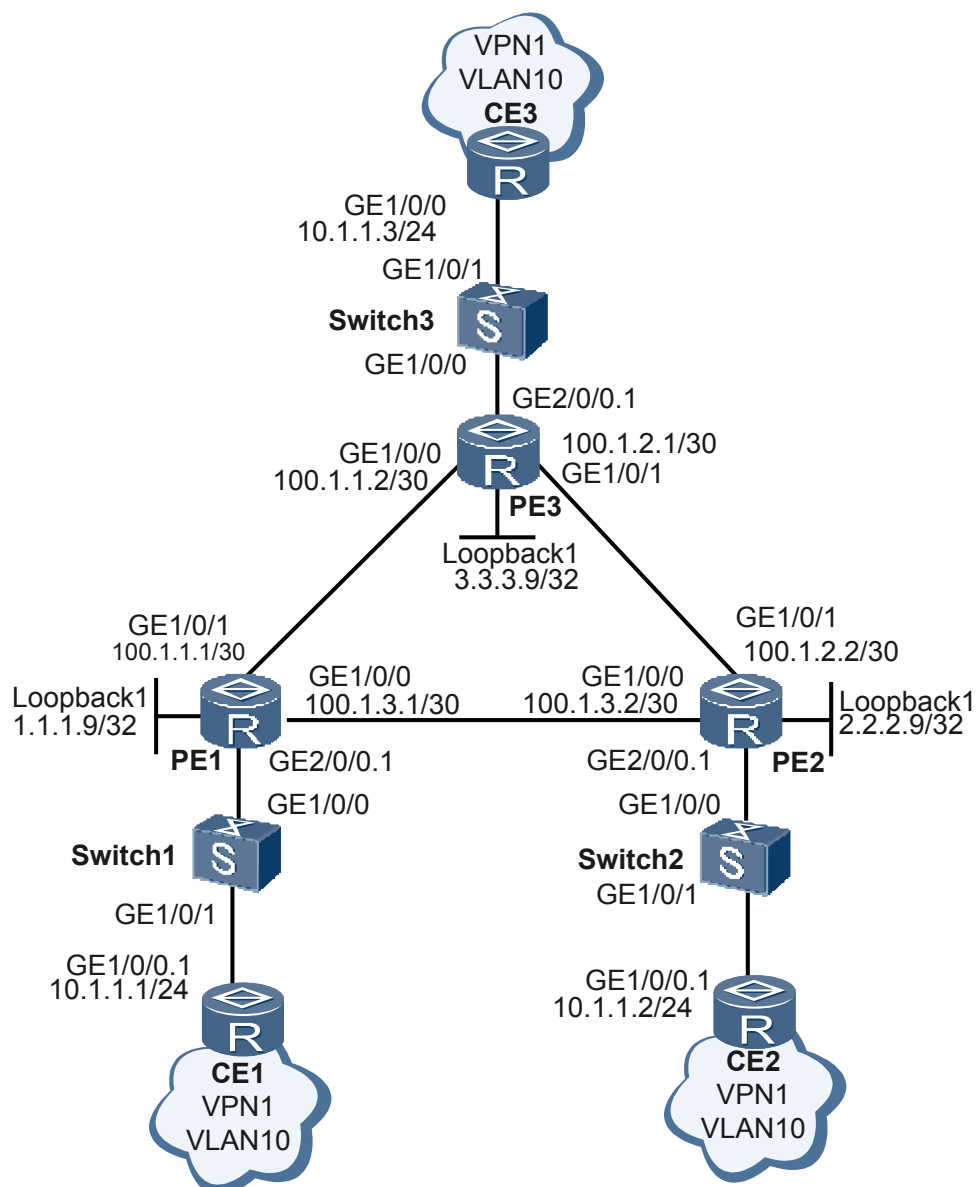
通过组网环境描述 PE 设备收到带有两层 Tag 的报文后接入 VPLS 网络，为了提高网络的可靠性，在 PE 设备 AC 侧配置 QinQ 终结子接口绑定 VSI 接入 VPLS 网络，再部署 CFM 功能。

组网需求

如图 8-23 所示，用户网络 VLAN10 通过 Switch 接入 PE 的网络，Switch 发送到 PE 的报文带有两层 Tag。

骨干网采用 Martini 方式的 VPLS，使用 LDP 作为信令建立 PW。为了提高网络的可靠性，在 PE 的 AC 侧配置 QinQ 终结子接口绑定 VSI，再部署基于 VPLS 的以太网 CFM，用于快速检测 PE 之间的 VPLS 连通性。

图 8-23 基于 VPLS 的以太网 CFM 组网图



配置思路

采用如下的思路配置基于 VPLS 的以太网 CFM 的基本功能：

1. 配置 PE 的接口模式为用户终结模式。
2. 在骨干网上运行 IGP 路由协议，使骨干网各路由器能互通。
3. 在骨干网上配置路由协议实现互通，并使能 MPLS 基本能力。
4. 在 PE 之间建立 LSP 隧道。
5. 在 PE 上使能 MPLS L2VPN。
6. 在 PE 的 AC 侧接口上配置 QinQ 终结子接口。
7. 在 PE 上创建 VSI，并将 VSI 与 QinQ 终结子接口进行绑定。

8. 在 PE 上配置基于 VPLS 的以太网 CFM。
9. 配置 Switch 的二层转发和 QinQ 功能。

数据准备

为完成此配置例，需准备如下的数据：

- 接口的 IP 地址。
- 各个 PE 上的 MPLS LSR-ID。
- PE1、PE2 和 PE3 上的 VSI 名称和 VSI-ID。
- 绑定 VSI 的接口。
- 以太网 CFM 中 MD 的名称和级别、MA 的名称和 MEP 的 ID、MEP 所在接口的名称、MEP 的类型。

操作步骤

步骤 1 配置接口的模式为用户终结模式

配置 PE1

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] interface gigabitethernet 2/0/0
[PE1-GigabitEthernet2/0/0] mode user-termination
[PE1-GigabitEthernet2/0/0] undo shutdown
[PE1-GigabitEthernet2/0/0] quit
```

配置 PE2

```
<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] interface gigabitethernet 2/0/0
[PE2-GigabitEthernet2/0/0] mode user-termination
[PE2-GigabitEthernet2/0/0] undo shutdown
[PE2-GigabitEthernet2/0/0] quit
```

配置 PE3

```
<HUAWEI> system-view
[HUAWEI] sysname PE3
[PE3] interface gigabitethernet 2/0/0
[PE3-GigabitEthernet2/0/0] mode user-termination
[PE3-GigabitEthernet2/0/0] undo shutdown
[PE3-GigabitEthernet2/0/0] quit
```

步骤 2 配置 MPLS 骨干网的 IGP，本示例中使用 OSPF

按图 8-23 配置 PE 的各接口地址。配置 OSPF 时，注意需要发布 PE 的 32 位 Loopback 接口地址。

配置 PE1。

```
[PE1] interface loopback 1
[PE1-LoopBack1] ip address 1.1.1.9 32
[PE1-LoopBack1] quit
[PE1] interface gigabitethernet 1/0/0
[PE1-GigabitEthernet1/0/0] ip address 100.1.3.1 30
[PE1-GigabitEthernet1/0/0] undo shutdown
[PE1-GigabitEthernet1/0/0] quit
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] ip address 100.1.1.1 30
[PE1-GigabitEthernet1/0/1] undo shutdown
```

```
[PE1-GigabitEthernet1/0/1] quit
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.3
[PE1-ospf-1-area-0.0.0.0] network 100.1.3.0 0.0.0.3
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

配置 PE2。

```
[PE2] interface LoopBack 1
[PE2-LoopBack1] ip address 2.2.2.9 32
[PE2-LoopBack1] quit
[PE2] interface gigabitethernet 1/0/0
[PE2-GigabitEthernet1/0/0] ip address 100.1.3.2 30
[PE2-GigabitEthernet1/0/0] undo shutdown
[PE2-GigabitEthernet1/0/0] quit
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] ip address 100.1.2.2 30
[PE2-GigabitEthernet1/0/1] undo shutdown
[PE2-GigabitEthernet1/0/1] quit
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 100.1.3.0 0.0.0.3
[PE2-ospf-1-area-0.0.0.0] network 100.1.2.0 0.0.0.3
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

配置 PE3

```
[PE3] interface loopback 1
[PE3-LoopBack1] ip address 3.3.3.9 32
[PE3-LoopBack1] quit
[PE3] interface gigabitethernet 1/0/0
[PE3-GigabitEthernet1/0/0] ip address 100.1.1.2 30
[PE3-GigabitEthernet1/0/0] undo shutdown
[PE3-GigabitEthernet1/0/0] quit
[PE3] interface gigabitethernet 1/0/1
[PE3-GigabitEthernet1/0/1] ip address 100.1.2.1 30
[PE3-GigabitEthernet1/0/1] undo shutdown
[PE3-GigabitEthernet1/0/1] quit
[PE3] ospf
[PE3-ospf-1] area 0
[PE3-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.3
[PE3-ospf-1-area-0.0.0.0] network 100.1.2.0 0.0.0.3
[PE3-ospf-1-area-0.0.0.0] quit
[PE3-ospf-1] quit
```

完成此步骤后，PE1 和 PE2、PE1 和 PE3 之间通过 OSPF 协议发现的对方 Loopback1 的 IP 路由，并应能互相 Ping 通。

以 PE1 的显示为例。

```
<PE1> display ip routing-table
```

Route Flags: R - relied, D - download to fib

Routing Tables: Public

Destination/Mask	Destinations : 12	Proto	Pre	Cost	Flags	NextHop	Routes : 13	Interface
1.1.1.9/32		Direct	0	0	D	127.0.0.1		InLoopBack0
2.2.2.9/32		OSPF	10	2	D	100.1.3.2		GigabitEthernet1/0/0
3.3.3.9/32		OSPF	10	2	D	100.1.1.2		GigabitEthernet1/0/1
100.1.1.0/30		Direct	0	0	D	100.1.1.1		GigabitEthernet1/0/1
100.1.1.1/32		Direct	0	0	D	127.0.0.1		InLoopBack0
100.1.1.2/32		Direct	0	0	D	100.1.1.2		GigabitEthernet1/0/1
100.1.2.0/30		OSPF	10	2	D	100.1.1.2		GigabitEthernet1/0/1

```
OSPF 10 2 D 100.1.3.2 GigabitEthernet1/0/0
100.1.3.0/30 Direct 0 0 D 100.1.3.1 GigabitEthernet1/0/0
100.1.3.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
100.1.3.2/32 Direct 0 0 D 100.1.3.2 GigabitEthernet1/0/0
127.0.0.0/8 Direct 0 0 D 127.0.0.1 InLoopBack0
127.0.0.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
<PE1> ping 100.1.2.2
PING 100.1.2.2: 56 data bytes, press CTRL_C to break
Reply from 100.1.2.2: bytes=56 Sequence=1 ttl=255 time=250 ms
Reply from 100.1.2.2: bytes=56 Sequence=2 ttl=255 time=30 ms
Reply from 100.1.2.2: bytes=56 Sequence=3 ttl=255 time=60 ms
Reply from 100.1.2.2: bytes=56 Sequence=4 ttl=255 time=60 ms
Reply from 100.1.2.2: bytes=56 Sequence=5 ttl=255 time=60 ms
--- 100.1.2.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 30/92/250 ms
```

步骤 3 在 MPLS 骨干网上使能 MPLS 基本能力和 LDP

配置 PE1。

```
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface gigabitethernet 1/0/0
[PE1-GigabitEthernet1/0/0] mpls
[PE1-GigabitEthernet1/0/0] mpls ldp
[PE1-GigabitEthernet1/0/0] quit
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] mpls
[PE1-GigabitEthernet1/0/1] mpls ldp
[PE1-GigabitEthernet1/0/1] quit
```

配置 PE2

```
[PE2] mpls lsr-id 2.2.2.9
[PE2] mpls
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface gigabitethernet1/0/0
[PE2-GigabitEthernet1/0/0] mpls
[PE2-GigabitEthernet1/0/0] mpls ldp
[PE2-GigabitEthernet1/0/0] quit
[PE2] interface gigabitethernet1/0/1
[PE2-GigabitEthernet1/0/1] mpls
[PE2-GigabitEthernet1/0/1] mpls ldp
[PE2-GigabitEthernet1/0/1] quit
```

配置 PE3

```
[PE3] mpls lsr-id 3.3.3.9
[PE3] mpls
[PE3-mpls] quit
[PE3] mpls ldp
[PE3-mpls-ldp] quit
[PE3] interface gigabitethernet 1/0/0
[PE3-GigabitEthernet1/0/0] mpls
[PE3-GigabitEthernet1/0/0] mpls ldp
[PE3-GigabitEthernet1/0/0] quit
[PE3] interface gigabitethernet 1/0/1
[PE3-GigabitEthernet1/0/1] mpls
[PE3-GigabitEthernet1/0/1] mpls ldp
[PE3-GigabitEthernet1/0/1] quit
```


上述配置完成后，PE 之间应能建立 LDP 会话，执行 **display mpls ldp session** 命令可以看到显示结果中 Status 项为 “Operational”。

以 PE1 的显示为例。

```
<PE1> display mpls ldp session
LDP Session(s) in Public Network
Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
A '*' before a session means the session is being deleted.
```

PeerID	Status	LAM	SsnRole	SsnAge	KASent/Rcv
2.2.2.9:0	Operational	DU	Passive	0000:00:09	37/37
3.3.3.9:0	Operational	DU	Passive	0000:00:03	13/13

TOTAL: 2 session(s) Found.

说明

如果 PE 之间非直连，还需要使用 **mpls ldp remote-peer** 和 **remote-ip** 命令，在 PE 之间建立远端 LDP 会话。

步骤 4 在 PE 上使能 MPLS L2VPN

配置 PE1。

```
[PE1] mpls l2vpn
```

配置 PE2。

```
[PE2] mpls l2vpn
```

配置 PE3。

```
[PE3] mpls l2vpn
```

步骤 5 创建 VSI，指定 VSI 的信令为 LDP

配置 PE1

```
[PE1] vsi ldpl static
[PE1-vsi-ldpl] pwsignal ldp
[PE1-vsi-ldpl-ldp] vsi-id 2
[PE1-vsi-ldpl-ldp] peer 2.2.2.9
[PE1-vsi-ldpl-ldp] peer 3.3.3.9
```

配置 PE2

```
[PE2] vsi ldpl static
[PE2-vsi-ldpl] pwsignal ldp
[PE2-vsi-ldpl-ldp] vsi-id 2
[PE2-vsi-ldpl-ldp] peer 1.1.1.9
[PE2-vsi-ldpl-ldp] peer 3.3.3.9
```

配置 PE3

```
[PE3] vsi ldpl static
[PE3-vsi-ldpl] pwsignal ldp
[PE3-vsi-ldpl-ldp] vsi-id 2
[PE3-vsi-ldpl-ldp] peer 1.1.1.9
[PE3-vsi-ldpl-ldp] peer 2.2.2.9
```

步骤 6 在 PE 上配置 QinQ 终结子接口并将 VSI 与 AC 接口进行绑定

配置 PE1

```
[PE1] interface gigabitethernet 2/0/0.1
[PE1-GigabitEthernet2/0/0.1] control-vid 1 qinq-termination
[PE1-GigabitEthernet2/0/0.1] qinq termination l2 symmetry
```

```
[PE1-GigabitEthernet2/0/0.1] qinq termination pe-vid 100 ce-vid 10
[PE1-GigabitEthernet2/0/0.1] l2 binding vsi ldpl
[PE1-GigabitEthernet2/0/0.1] undo shutdown
[PE1-GigabitEthernet2/0/0.1] quit
```

配置 PE2

```
[PE2] interface gigabitethernet 2/0/0.1
[PE2-GigabitEthernet2/0/0.1] control-vid 1 qinq-termination
[PE2-GigabitEthernet2/0/0.1] qinq termination l2 symmetry
[PE2-GigabitEthernet2/0/0.1] qinq termination pe-vid 100 ce-vid 10
[PE2-GigabitEthernet2/0/0.1] l2 binding vsi ldpl
[PE2-GigabitEthernet2/0/0.1] undo shutdown
[PE2-GigabitEthernet2/0/0.1] quit
```

配置 PE3

```
[PE3] interface gigabitethernet 2/0/0.1
[PE3-GigabitEthernet2/0/0.1] control-vid 1 qinq-termination
[PE3-GigabitEthernet2/0/0.1] qinq termination l2 symmetry
[PE3-GigabitEthernet2/0/0.1] qinq termination pe-vid 100 ce-vid 10
[PE3-GigabitEthernet2/0/0.1] l2 binding vsi ldpl
[PE3-GigabitEthernet2/0/0.1] undo shutdown
[PE3-GigabitEthernet2/0/0.1] quit
```

说明

同一主接口上使用 **qinq termination** 命令时，当两个不同的子接口的 **pe-vid** 取值相同时，**ce-vid** 的取值范围不能有重叠。

步骤 7 在 PE 上配置以太网 CFM 功能

配置 PE1。

```
[PE1] cfm enable
[PE1] cfm version standard
[PE1] cfm md md1
[PE1-md-md1] ma ma1
[PE1-md-md1-ma-ma1] ccm-interval 30
[PE1-md-md1-ma-ma1] map vsi ldpl
[PE1-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 2/0/0.1 pe-vid 100 ce-vid 10 inward
[PE1-md-md1-ma-ma1] remote-mep mep-id 2
[PE1-md-md1-ma-ma1] remote-mep mep-id 3
[PE1-md-md1-ma-ma1] mep ccm-send enable
[PE1-md-md1-ma-ma1] remote-mep ccm-receive enable
[PE1-md-md1-ma-ma1] quit
```

配置 PE2。

```
[PE2] cfm enable
[PE2] cfm version standard
[PE2] cfm md md1
[PE2-md-md1] ma ma1
[PE2-md-md1-ma-ma1] ccm-interval 30
[PE2-md-md1-ma-ma1] map vsi ldpl
[PE2-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet 2/0/0.1 pe-vid 100 ce-vid 10 inward
[PE2-md-md1-ma-ma1] remote-mep mep-id 1
[PE2-md-md1-ma-ma1] remote-mep mep-id 3
[PE2-md-md1-ma-ma1] mep ccm-send enable
[PE2-md-md1-ma-ma1] remote-mep ccm-receive enable
[PE2-md-md1-ma-ma1] quit
```

配置 PE3。

```
[PE3] cfm enable
[PE2] cfm version standard
[PE3] cfm md md1
[PE3-md-md1] ma ma1
[PE3-md-md1-ma-ma1] ccm-interval 30
[PE3-md-md1-ma-ma1] map vsi ldpl
```

```
[PE3-md-md1-ma-ma1] mep mep-id 3 interface gigabitethernet 2/0/0.1 pe-vid 100 ce-vid 10 inward
[PE3-md-md1-ma-ma1] remote-mep mep-id 1
[PE3-md-md1-ma-ma1] remote-mep mep-id 2
[PE3-md-md1-ma-ma1] mep ccm-send enable
[PE3-md-md1-ma-ma1] remote-mep ccm-receive enable
[PE3-md-md1-ma-ma1] quit
```

步骤 8 配置 QinQ 功能，使 Switch 发送到 PE 的报文带有两层 Tag

配置 Switch1

```
<HUAWEI> system-view
[HUAWEI] sysname Switch1
[Switch1] vlan 100
[Switch1-vlan100] quit
[Switch1] interface gigabitethernet 1/0/0
[Switch1-GigabitEthernet1/0/0] undo shutdown
[Switch1-GigabitEthernet1/0/0] port trunk allow-pass vlan 100
[Switch1-GigabitEthernet1/0/0] quit
[Switch1] interface gigabitethernet 1/0/1
[Switch1-GigabitEthernet1/0/1] undo shutdown
[Switch1-GigabitEthernet1/0/1] port vlan-stacking outside-vlan 10 stack-vlan 100
[Switch1-GigabitEthernet1/0/1] quit
```

配置 Switch2

```
<HUAWEI> system-view
[HUAWEI] sysname Switch2
[Switch2] vlan 100
[Switch2-vlan100] quit
[Switch2] interface gigabitethernet 1/0/0
[Switch2-GigabitEthernet1/0/0] portswitch
[Switch2-GigabitEthernet1/0/0] undo shutdown
[Switch2-GigabitEthernet1/0/0] port trunk allow-pass vlan 100
[Switch2-GigabitEthernet1/0/0] quit
[Switch2] interface gigabitethernet 1/0/1
[Switch2-GigabitEthernet1/0/1] portswitch
[Switch2-GigabitEthernet1/0/1] undo shutdown
[Switch2-GigabitEthernet1/0/1] port vlan-stacking outside-vlan 10 stack-vlan 100
[Switch2-GigabitEthernet1/0/1] quit
```

配置 Switch3

```
<HUAWEI> system-view
[HUAWEI] sysname Switch3
[Switch3] vlan 100
[Switch3-vlan100] quit
[Switch3] interface gigabitethernet 1/0/0
[Switch3-GigabitEthernet1/0/0] undo shutdown
[Switch3-GigabitEthernet1/0/0] port trunk allow-pass vlan 100
[Switch3-GigabitEthernet1/0/0] quit
[Switch3] interface gigabitethernet 1/0/1
[Switch3-GigabitEthernet1/0/1] undo shutdown
[Switch3-GigabitEthernet1/0/1] port vlan-stacking outside-vlan 10 stack-vlan 100
[Switch3-GigabitEthernet1/0/1] quit
```

说明

如果设备不支持 **port vlan-stacking** 命令，也可以在接口上使用 **port link-type dot1q-tunnel** 和 **port default vlan** 来配置 QinQ 功能。

按图 8-23 配置各 CE 子接口 IP 的地址，使 CE 发送到 Switch 的报文带有一层 Tag。

配置 CE1

```
<HUAWEI> system-view
[HUAWEI] sysname CE1
[CE1] interface gigabitethernet 1/0/0.1
[CE1-GigabitEthernet1/0/0.1] ip address 10.1.1.1 24
[CE1-GigabitEthernet1/0/0.1] vlan-type dot1q 10
```

```
[CE1-GigabitEthernet1/0/0.1] undo shutdown
[CE1-GigabitEthernet1/0/0.1] quit

# 配置 CE2

<HUAWEI> system-view
[HUAWEI] sysname CE2
[CE2] interface gigabitethernet 1/0/0.1
[CE2-GigabitEthernet1/0/0.1] ip address 10.1.1.2 24
[CE2-GigabitEthernet1/0/0.1] vlan-type dot1q 10
[CE2-GigabitEthernet1/0/0.1] undo shutdown
[CE2-GigabitEthernet1/0/0.1] quit

# 配置 CE3

<HUAWEI> system-view
[HUAWEI] sysname CE3
[CE3] interface gigabitethernet 1/0/0.1
[CE3-GigabitEthernet1/0/0.1] ip address 10.1.1.3 24
[CE3-GigabitEthernet1/0/0.1] vlan-type dot1q 10
[CE3-GigabitEthernet1/0/0.1] undo shutdown
[CE3-GigabitEthernet1/0/0.1] quit
```

步骤 9 检查配置结果

完成上述配置后，在 PE1、PE2 或 PE3 上执行 **display cfm mep** 命令和 **display cfm remote-mep** 命令，可以看到以太网 CFM 已经建立成功。以太网 CFM 能够快速检测到 VSI 的 PE 之间的故障，并通知给网管系统。

以 PE1 为例：

```
<PE1> display cfm mep md md1
The total number of MEPS is : 1
-----
MD Name          : md1
MD Name Format    : string
Level            : 0
MA Name          : mal
MA Name Format    : string
MEP ID           : 1
Vlan ID          : --
VSI Name         : ldp1
L2VC ID          : --
Interface Name   : GigabitEthernet2/0/0.1
CCM Send         : enabled
Direction       : inward
MAC Address      : 00e0-fc6e-bb11
MEP Pe-vid       : 100
MEP Ce-vid       : 10
MEP Vid          : --
<PE1> display cfm remote-mep md md1
The total number of RMEPS is : 2
The status of RMEPS : 2 up, 0 down
-----
MD Name          : md1
Level            : 0
MA Name          : mal
RMEP ID          : 2
Vlan ID          : --
VSI Name         : ldp1
L2VC ID          : --
MAC              : 00e0-0003-0003
CCM Receive      : enabled
Trigger-If-Down  : disabled
CFM Status       : up

MD Name          : md1
Level            : 0
MA Name          : mal
```

```
RMEP ID          : 3
Vlan ID          : --
VSI Name         : ldp1
L2VC ID          : --
MAC              : --
CCM Receive      : enabled
Trigger-If-Down  : disabled
CFM Status       : up
```

----结束

配置文件

● PE1 的配置文件

```
#
sysname PE1
#
cfm version standard
cfm enable
#
mpls lsr-id 1.1.1.9
mpls
#
mpls l2vpn
#
vsi ldp1 static
pwsignal ldp
vsi-id 2
peer 2.2.2.9
peer 3.3.3.9
#
mpls ldp
#
interface GigabitEthernet2/0/0
undo shutdown
mode user-termination
#
interface GigabitEthernet2/0/0.1
undo shutdown
control-vid 1 qinq-termination
qinq termination l2 symmetry
qinq termination pe-vid 100 ce-vid 10
l2 binding vsi ldp1
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 100.1.3.1 255.255.255.252
mpls
mpls ldp
#
interface GigabitEthernet1/0/1
undo shutdown
ip address 100.1.1.1 255.255.255.252
mpls
mpls ldp
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
#
cfm md mdl
ma mal
map vsi ldp1
ccm-interval 30
mep mep-id 1 interface gigabitEthernet 2/0/0.1 pe-vid 100 ce-vid 10 inward
mep ccm-send mep-id 1 enable
remote-mep mep-id 2
remote-mep ccm-receive mep-id 2 enable
remote-mep mep-id 3
```

```

        remote-mep ccm-receive mep-id 3 enable
#
ospf 1
 area 0.0.0.0
   network 1.1.1.9 0.0.0.0
   network 100.1.1.0 0.0.0.3
   network 100.1.3.0 0.0.0.3
#
return

```

● PE2 的配置文件

```

#
sysname PE2
#
cfm version standard
cfm enable
#
mpls lsr-id 2.2.2.9
mpls
#
mpls l2vpn
#
vsi ldpl static
 pwsignal ldp
 vsi-id 2
 peer 1.1.1.9
 peer 3.3.3.9
#
mpls ldp
#
interface GigabitEthernet2/0/0
 undo shutdown
 mode user-termination
#
interface GigabitEthernet2/0/0.1
 undo shutdown
 control-vid 1 qinq-termination
 qinq termination l2 symmetry
 qinq termination pe-vid 100 ce-vid 10
 l2 binding vsi ldpl
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 100.1.3.2 255.255.255.252
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 100.1.2.2 255.255.255.252
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
cfm md mdl
 ma mal
 map vsi ldpl
 ccm-interval 30
 mep mep-id 2 interface gigabitethernet 2/0/0.1 pe-vid 100 ce-vid 10 inward
 mep ccm-send mep-id 2 enable
 remote-mep mep-id 1
 remote-mep ccm-receive mep-id 1 enable
 remote-mep mep-id 3
 remote-mep ccm-receive mep-id 3 enable
#
ospf 1
 area 0.0.0.0
 network 2.2.2.9 0.0.0.0

```

```

        network 100.1.2.0 0.0.0.3
        network 100.1.3.0 0.0.0.3
    #
    return

```

● PE3 的配置文件

```

#
sysname PE3
#
cfm version standard
cfm enable
#
mpls lsr-id 3.3.3.9
mpls
#
mpls l2vpn
#
vsi ldpl static
pwsignal ldp
vsi-id 2
peer 1.1.1.9
peer 2.2.2.9
#
mpls ldp
#
interface GigabitEthernet2/0/0
    undo shutdown
    mode user-termination
#
interface GigabitEthernet2/0/0.1
    undo shutdown
    control-vid 1 qinq-termination
    qinq termination l2 symmetry
    qinq termination pe-vid 100 ce-vid 10
    l2 binding vsi ldpl
#
interface GigabitEthernet1/0/0
    undo shutdown
    ip address 100.1.1.2 255.255.255.252
    mpls
    mpls ldp
#
interface GigabitEthernet1/0/1
    undo shutdown
    ip address 100.1.2.1 255.255.255.252
    mpls
    mpls ldp
#
interface LoopBack1
    ip address 3.3.3.9 255.255.255.255
#
cfm md mdl
    ma mal
        ccm-interval 30
        map vsi ldpl
        mep mep-id 3 interface gigabitEthernet 2/0/0.1 pe-vid 100 ce-vid 10 inward
        mep ccm-send mep-id 3 enable
        remote-mep mep-id 1
        remote-mep ccm-receive mep-id 1 enable
        remote-mep mep-id 2
        remote-mep ccm-receive mep-id 2 enable
#
ospf 1
    area 0.0.0.0
        network 3.3.3.9 0.0.0.0
        network 100.1.2.0 0.0.0.3
        network 100.1.1.0 0.0.0.3
#
return

```

- Switch1 的配置文件

```
#
 sysname Switch1
#
 vlan batch 100
#
 interface GigabitEthernet1/0/0
  undo shutdown
  port trunk allow-pass vlan 100
#
 interface GigabitEthernet1/0/1
  undo shutdown
  port vlan-stacking outside-vlan 10 stack-vlan 100
#
return
```

- Switch2 的配置文件

```
#
 sysname Switch2
#
 vlan batch 100
#
 interface GigabitEthernet1/0/0
  undo shutdown
  port trunk allow-pass vlan 100
#
 interface GigabitEthernet1/0/1
  undo shutdown
  port vlan-stacking outside-vlan 10 stack-vlan 100
#
return
```

- Switch3 的配置文件

```
#
 sysname Switch3
#
 vlan batch 100
#
 interface GigabitEthernet1/0/0
  undo shutdown
  port trunk allow-pass vlan 100
#
 interface GigabitEthernet1/0/1
  undo shutdown
  port vlan-stacking outside-vlan 10 stack-vlan 100
#
return
```

- CE1 的配置文件

```
#
 sysname CE1
#
 interface GigabitEthernet1/0/0.1
  undo shutdown
  vlan-type dot1q 10
  ip address 10.1.1.1 255.255.255.0
#
return
```

- CE2 的配置文件

```
#
 sysname CE2
#
 interface GigabitEthernet1/0/0.1
  undo shutdown
  vlan-type dot1q 10
  ip address 10.1.1.2 255.255.255.0
#
```



```
return
● CE3 的配置文件
#
sysname CE3
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 10
ip address 10.1.1.3 255.255.255.0
#
return
```

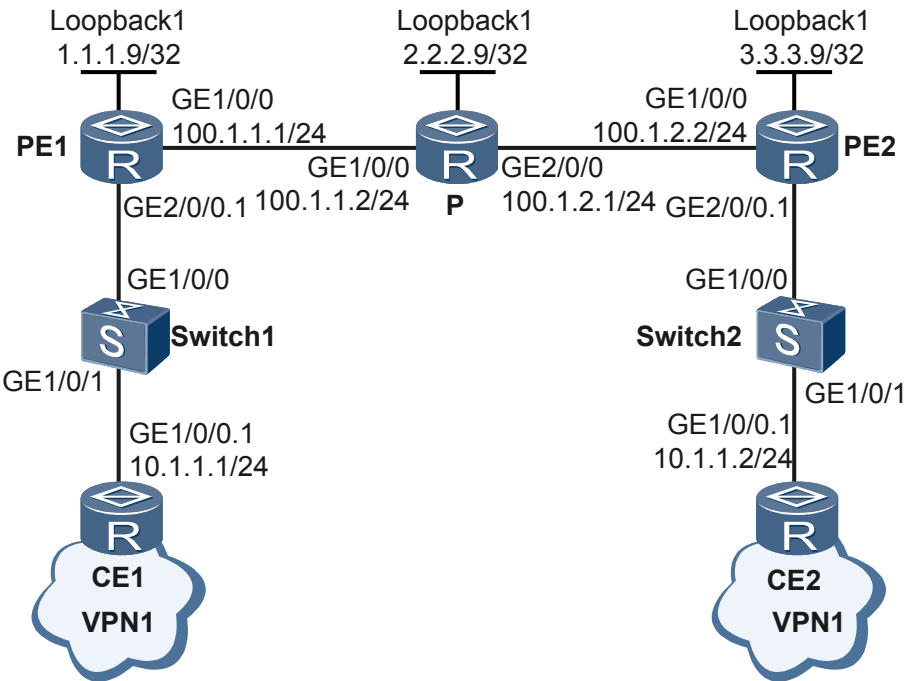
8.18.9 配置基于 VLL 的以太网 CFM 示例（使用 QinQ 终结子接口）

通过组网环境描述 PE 设备收到带有两层 Tag 的报文后接入 VLL 网络，为了提高网络的可靠性，在 PE 设备 AC 侧配置 QinQ 终结子接口绑定 L2VC 接入 VLL 网络，再部署 CFM 功能。

组网需求

如图 8-24 所示，CE 的子接口 GE1/0/0.1 通过 Switch 接入 PE，Switch 配置 QinQ，对从 CE 接收到的用户报文打上外层 Tag 100，以达到节约公网的 VLAN 数量的目的。这样 Switch 发送到 PE 的用户报文就带有两层 Tag。骨干网采用 Martini 方式的 VLL，使用 LDP 作为信令建立 PW。为了提高网络的可靠性，在 PE 的 AC 侧配置 QinQ 终结子接口绑定 L2VC，再部署基于 VLL 的以太网 CFM，用于快速检测 PE 之间的 VLL 连通性。

图 8-24 基于 VLL 的以太网 CFM 组网图



配置思路

采用如下的思路配置基于 QinQ 终结子接口接入 L2VPN 的基本功能：

1. 配置 PE1 和 PE2 的接口模式为用户终结模式。
2. 在骨干网上运行 IGP 路由协议，使骨干网各路由器能互通。
3. 在骨干网上使能 MPLS 基本能力，建立 LSP 隧道。
4. PW 两端的 PE 之间建立 MPLS LDP 远端对等体关系。
5. 在 PE 的 AC 侧接口上配置 QinQ 终结子接口。
6. 在 PE 上创建 MPLS L2VC，并将 L2VC 与 QinQ 终结子接口进行绑定。
7. 在 PE 上配置基于 VLL 的以太网 CFM。
8. 在 Switch 上配置二层转发和 QinQ 功能。

数据准备

为完成此配置例，需准备如下的数据：

- 与 CE 设备相连 PE 的接口名称。
- 接口的 IP 地址。
- PW 两端的 L2VC ID（必需一致）。
- 各个 PE 及 P 上的 MPLS LSR-ID。
- 设置 PE 远端对等体的 IP 地址。
- QinQ 终结子接口终结的 Tag 值。
- 以太网 CFM 中 MD 的名称和级别、MA 的名称和 MEP 的 ID、MEP 所在接口的名称、MEP 的类型。

操作步骤

步骤 1 配置接口的模式为用户终结模式

```
# 配置 PE1

<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] interface gigabitethernet 2/0/0
[PE1-GigabitEthernet2/0/0] mode user-termination
[PE1-GigabitEthernet2/0/0] undo shutdown
[PE1-GigabitEthernet2/0/0] quit

# 配置 PE2

<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] interface gigabitethernet 2/0/0
[PE2-GigabitEthernet2/0/0] mode user-termination
[PE2-GigabitEthernet2/0/0] undo shutdown
[PE2-GigabitEthernet2/0/0] quit
```

步骤 2 配置 MPLS 骨干网的 IGP，本示例中使用 OSPF

按图 8-24 配置 PE 和 P 的各接口地址。配置 OSPF 时，注意需要发布 PE1、P 和 PE2 的 32 位 Loopback 接口地址。

```
# 配置 PE1。

[PE1] interface loopback 1
[PE1-LoopBack1] ip address 1.1.1.9 32
[PE1-LoopBack1] quit
[PE1] interface gigabitethernet 1/0/0
[PE1-GigabitEthernet1/0/0] ip address 100.1.1.1 24
```

```
[PE1-GigabitEthernet1/0/0] undo shutdown
[PE1-GigabitEthernet1/0/0] quit
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

配置 P。

```
<HUAWEI> system-view
[HUAWEI] sysname P
[P] interface LoopBack 1
[P-LoopBack1] ip address 2.2.2.9 32
[P-LoopBack1] quit
[P] interface gigabitethernet 1/0/0
[P-GigabitEthernet1/0/0] ip address 100.1.1.2 24
[P-GigabitEthernet1/0/0] undo shutdown
[P-GigabitEthernet1/0/0] quit
[P] interface gigabitethernet 2/0/0
[P-GigabitEthernet2/0/0] ip address 100.1.2.1 24
[P-GigabitEthernet2/0/0] undo shutdown
[P-GigabitEthernet2/0/0] quit
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 100.1.2.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

配置 PE2

```
[PE2] interface loopback 1
[PE2-LoopBack1] ip address 3.3.3.9 32
[PE2-LoopBack1] quit
[PE2] interface gigabitethernet 1/0/0
[PE2-GigabitEthernet1/0/0] ip address 100.1.2.2 24
[PE2-GigabitEthernet1/0/0] undo shutdown
[PE2-GigabitEthernet1/0/0] quit
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 100.1.2.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

完成此步骤后，PE1 和 PE2 相互之间有 OSPF 协议发现的对方 Loopback1 的 IP 路由，并能互相 Ping 通。

以 PE1 的显示为例。

```
<PE1> display ip routing-table
Route Flags: R - relied, D - download to fib
```

```
-----
Routing Tables: Public
  Destinations : 9          Routes : 9
Destination/Mask    Proto Pre  Cost   Flags NextHop         Interface
 1.1.1.9/32         Direct 0    0       D  127.0.0.1         InLoopBack0
 2.2.2.9/32         OSPF   10    2       D  100.1.1.2         GigabitEthernet1/0/0
 3.3.3.9/32         OSPF   10    3       D  100.1.1.2         GigabitEthernet1/0/0
100.1.1.0/24        Direct 0    0       D  100.1.1.1         GigabitEthernet1/0/0
100.1.1.1/32        Direct 0    0       D  127.0.0.1         InLoopBack0
100.1.1.2/32        Direct 0    0       D  100.1.1.2         GigabitEthernet1/0/0
100.1.2.0/24        OSPF   10    2       D  100.1.1.2         GigabitEthernet1/0/0
127.0.0.0/8         Direct 0    0       D  127.0.0.1         InLoopBack0
127.0.0.1/32        Direct 0    0       D  127.0.0.1         InLoopBack0
<PE1> ping 100.1.2.2
```

```
PING 100.1.2.2: 56 data bytes, press CTRL_C to break
  Reply from 100.1.2.2: bytes=56 Sequence=1 ttl=254 time=200 ms
  Reply from 100.1.2.2: bytes=56 Sequence=2 ttl=254 time=60 ms
  Reply from 100.1.2.2: bytes=56 Sequence=3 ttl=254 time=90 ms
  Reply from 100.1.2.2: bytes=56 Sequence=4 ttl=254 time=90 ms
  Reply from 100.1.2.2: bytes=56 Sequence=5 ttl=254 time=90 ms
--- 100.1.2.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 60/106/200 ms
```

步骤 3 在 MPLS 骨干网上使能 MPLS 基本能力和 LDP

```
# 配置 PE1。

[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface gigabitethernet 1/0/0
[PE1-GigabitEthernet1/0/0] mpls
[PE1-GigabitEthernet1/0/0] mpls ldp
[PE1-GigabitEthernet1/0/0] quit
```

```
# 配置 P。

[P] mpls lsr-id 2.2.2.9
[P] mpls
[P-mpls] quit
[P] mpls ldp
[P-mpls-ldp] quit
[P] interface gigabitethernet1/0/0
[P-GigabitEthernet1/0/0] mpls
[P-GigabitEthernet1/0/0] mpls ldp
[P-GigabitEthernet1/0/0] quit
[P] interface gigabitethernet2/0/0
[P-GigabitEthernet2/0/0] mpls
[P-GigabitEthernet2/0/0] mpls ldp
[P-GigabitEthernet2/0/0] quit
```

```
# 配置 PE2。

[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface gigabitethernet 1/0/0
[PE2-GigabitEthernet1/0/0] mpls
[PE2-GigabitEthernet1/0/0] mpls ldp
[PE2-GigabitEthernet1/0/0] quit
```

上述配置完成后，PE1 与 P、P 与 PE2 之间应能建立 LDP 会话，执行 **display mpls ldp session** 命令可以看到显示结果中 Status 项为“Operational”。

以 PE1 的显示为例。

```
<PE1> display mpls ldp session
LDP Session(s) in Public Network
Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
A '*' before a session means the session is being deleted.

-----
PeerID              Status      LAM  SsnRole  SsnAge      KASent/Rcv
-----
2.2.2.9:0           Operational DU   Active  0000:03:01 726/726
-----

TOTAL: 1 session(s) Found.
```

步骤 4 在 PE 之间建立远端 LDP 会话

配置 PE1。

```
[PE1] mpls ldp remote-peer 3.3.3.9
[PE1-mpls-ldp-remote-3.3.3.9] remote-ip 3.3.3.9
[PE1-mpls-ldp-remote-3.3.3.9] quit
```

配置 PE2。

```
[PE2] mpls ldp remote-peer 1.1.1.9
[PE2-mpls-ldp-remote-1.1.1.9] remote-ip 1.1.1.9
[PE2-mpls-ldp-remote-1.1.1.9] quit
```

上述配置完成后，PE1 与 PE2 之间应能建立 LDP 会话，执行 **display mpls ldp session** 命令可以看到显示结果中 Status 项为“Operational”。

以 PE1 的显示为例。

```
<PE1> display mpls ldp session
LDP Session(s) in Public Network
Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
A '*' before a session means the session is being deleted.
```

PeerID	Status	LAM	SsnRole	SsnAge	KASent/Rcv
2.2.2.9:0	Operational	DU	Passive	0000:00:09	37/37
3.3.3.9:0	Operational	DU	Passive	0000:00:03	13/13

TOTAL: 2 session(s) Found.

步骤 5 使能 MPLS L2VPN 和创建 VC 连接，并配置 QinQ 终结子接口

配置 PE1。

```
[PE1] mpls l2vpn
[PE1-l2vpn] quit
[PE1] interface gigabitethernet 2/0/0.1
[PE1-GigabitEthernet2/0/0.1] control-vid 1 qinq-termination
[PE1-GigabitEthernet2/0/0.1] qinq termination l2 symmetry
[PE1-GigabitEthernet2/0/0.1] qinq termination pe-vid 100 ce-vid 10
[PE1-GigabitEthernet2/0/0.1] mpls l2vc 3.3.3.9 101
[PE1-GigabitEthernet2/0/0.1] quit
```

配置 PE2。

```
[PE2] mpls l2vpn
[PE2-l2vpn] quit
[PE2] interface gigabitethernet 2/0/0.1
[PE2-GigabitEthernet2/0/0.1] control-vid 1 qinq-termination
[PE2-GigabitEthernet2/0/0.1] qinq termination l2 symmetry
[PE2-GigabitEthernet2/0/0.1] qinq termination pe-vid 100 ce-vid 10
[PE2-GigabitEthernet2/0/0.1] mpls l2vc 1.1.1.9 101
[PE2-GigabitEthernet2/0/0.1] quit
```

 说明

同一主接口上使用 **qinq termination** 命令时，当两个不同的子接口的 **pe-vid** 取值相同时，**ce-vid** 的取值范围不能有重叠。

步骤 6 在 PE 上配置以太网 CFM 功能

配置 PE1。

```
[PE1] cfm enable
[PE1] cfm version standard
[PE1] cfm md md1
[PE1-md-md1] ma ma1
[PE1-md-md1-ma-ma1] ccm-interval 30
```

```
[PE1-md-md1-ma-ma1] map mpls l2vc 101 tagged
[PE1-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 2/0/0.1 pe-vid 100 ce-vid 10 inward
[PE1-md-md1-ma-ma1] remote-mep mep-id 2
[PE1-md-md1-ma-ma1] mep ccm-send enable
[PE1-md-md1-ma-ma1] remote-mep ccm-receive enable
[PE1-md-md1-ma-ma1] quit
```

配置 PE2。

```
[PE2] cfm enable
[PE2] cfm version standard
[PE2] cfm md md1
[PE2-md-md1] ma ma1
[PE2-md-md1-ma-ma1] ccm-interval 30
[PE2-md-md1-ma-ma1] map mpls l2vc 101 tagged
[PE2-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet 2/0/0.1 pe-vid 100 ce-vid 10 inward
[PE2-md-md1-ma-ma1] remote-mep mep-id 1
[PE2-md-md1-ma-ma1] mep ccm-send enable
[PE2-md-md1-ma-ma1] remote-mep ccm-receive enable
[PE2-md-md1-ma-ma1] quit
```

步骤 7 配置 QinQ 功能，使 Switch 发送到 PE 的报文带有两层 Tag

配置 Switch1

```
<HUAWEI> system-view
[HUAWEI] sysname Switch1
[Switch1] vlan 100
[Switch1-vlan100] quit
[Switch1] interface gigabitethernet 1/0/0
[Switch1-GigabitEthernet1/0/0] portswitch
[Switch1-GigabitEthernet1/0/0] undo shutdown
[Switch1-GigabitEthernet1/0/0] port trunk allow-pass vlan 100
[Switch1-GigabitEthernet1/0/0] quit
[Switch1] interface gigabitethernet 1/0/1
[Switch1-GigabitEthernet1/0/1] portswitch
[Switch1-GigabitEthernet1/0/1] port vlan-stacking outside-vlan 10 stack-vlan 100
[Switch1-GigabitEthernet1/0/1] undo shutdown
[Switch1-GigabitEthernet1/0/1] quit
```

配置 Switch2

```
<HUAWEI> system-view
[HUAWEI] sysname Switch2
[Switch2] vlan 100
[Switch2-vlan100] quit
[Switch2] interface gigabitethernet 1/0/0
[Switch2-GigabitEthernet1/0/0] portswitch
[Switch2-GigabitEthernet1/0/0] undo shutdown
[Switch2-GigabitEthernet1/0/0] port trunk allow-pass vlan 100
[Switch2-GigabitEthernet1/0/0] quit
[Switch2] interface gigabitethernet 1/0/1
[Switch2-GigabitEthernet1/0/1] portswitch
[Switch2-GigabitEthernet1/0/1] undo shutdown
[Switch2-GigabitEthernet1/0/1] port vlan-stacking outside-vlan 10 stack-vlan 100
[Switch2-GigabitEthernet1/0/1] quit
[Switch2-GigabitEthernet1/0/2] quit
```

 说明

如果设备不支持 **port vlan-stacking** 命令，也可以在接口上使用 **port link-type dot1q-tunnel** 和 **port default vlan** 来配置 QinQ 功能。

按图 8-24 配置各 CE 子接口 IP 的地址，使 CE 发送到 Switch 的报文带有一层 Tag。

配置 CE1

```
<HUAWEI> system-view
[HUAWEI] sysname CE1
[CE1] interface gigabitethernet 1/0/0.1
```

```
[CE1-GigabitEthernet1/0/0.1] ip address 10.1.1.1 24
[CE1-GigabitEthernet1/0/0.1] vlan-type dot1q 10
[CE1-GigabitEthernet1/0/0.1] undo shutdown
[CE1-GigabitEthernet1/0/0.1] quit
```

配置 CE2

```
<HUAWEI> system-view
[HUAWEI] sysname CE2
[CE2] interface gigabitethernet 1/0/0.1
[CE2-GigabitEthernet1/0/0.1] ip address 10.1.1.2 24
[CE2-GigabitEthernet1/0/0.1] vlan-type dot1q 10
[CE2-GigabitEthernet1/0/0.1] undo shutdown
[CE2-GigabitEthernet1/0/0.1] quit
```

步骤 8 检查配置结果

完成上述配置后，在 PE1、PE2 或 PE3 上执行 **display cfm mep** 命令和 **display cfm remote-mep** 命令，可以看到以太网 CFM 已经建立成功。以太网 CFM 能够快速检测到 VSI 的 PE 之间的故障，并通知给网管系统。

以 PE1 为例：

```
<PE1> display cfm mep md md1
The total number of MEPS is : 1
-----
MD Name           : md1
MD Name Format     : string
Level             : 0
MA Name           : mal
MA Name Format     : string
MEP ID            : 2
Vlan ID           : --
VSI Name          : --
L2VC ID           : 101 tagged
Interface Name    : GigabitEthernet2/0/0.1
CCM Send          : enabled
Direction        : inward
MAC Address       : 00e0-fc6e-bb11
MEP Pe-vid        : 100
MEP Ce-vid        : 10
MEP Vid           : --
[PE1] display cfm remote-mep md md1
The total number of RMEPS is : 1
The status of RMEPS : 1 up, 0 down
-----
MD Name           : md1
Level             : 0
MA Name           : mal
RMEP ID           : 1
Vlan ID           : --
VSI Name          : --
L2VC ID           : 101 tagged
MAC               : 00e0-0003-0003
CCM Receive       : enabled
Trigger-If-Down   : disabled
CFM Status        : up
```

----结束

配置文件

● PE1 的配置文件

```
#
sysname PE1
#
cfm version standard
```

```

cfm enable
#
mpls lsr-id 1.1.1.9
mpls
#
mpls l2vpn
#
mpls ldp remote-peer 3.3.3.9
remote-ip 3.3.3.9
#
interface GigabitEthernet2/0/0
undo shutdown
mode user-termination
#
interface GigabitEthernet2/0/0.1
undo shutdown
control-vid 1 qinq-termination
qinq termination l2 symmetry
qinq termination pe-vid 100 ce-vid 10
mpls l2vc 3.3.3.9 101
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 100.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
#
cfm md mdl
ma mal
map mpls l2vc 101 tagged
ccm-interval 30
mep mep-id 1 interface gigabitEthernet 2/0/0.1 pe-vid 100 ce-vid 10 inward
mep ccm-send mep-id 1 enable
remote-mep mep-id 2
remote-mep ccm-receive mep-id 2 enable
#
ospf 1
area 0.0.0.0
network 1.1.1.9 0.0.0.0
network 100.1.1.0 0.0.0.255
#
return

```

● PE2 的配置文件

```

#
sysname PE2
#
cfm version standard
cfm enable
#
mpls lsr-id 3.3.3.9
mpls
#
mpls l2vpn
#
mpls ldp remote-peer 1.1.1.9
remote-ip 1.1.1.9
#
interface GigabitEthernet2/0/0
undo shutdown
mode user-termination
#
interface GigabitEthernet2/0/0.1
undo shutdown
control-vid 1 qinq-termination
qinq termination l2 symmetry
qinq termination pe-vid 100 ce-vid 10

```



```

mpls l2vc 1.1.1.9 101
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 100.1.2.2 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
#
cfm md mdl
ma mal
map mpls l2vc 101 tagged
ccm-interval 30
mep mep-id 1 interface gigabitEthernet 2/0/0.1 pe-vid 100 ce-vid 10 inward
mep ccm-send mep-id 2 enable
remote-mep mep-id 1
remote-mep ccm-receive mep-id 1 enable
#
ospf 1
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 100.1.2.0 0.0.0.255
#
return

```

● P 的配置文件

```

#
sysname P
#
mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 100.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 100.1.2.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 2.2.2.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 2.2.2.9 0.0.0.0
network 100.1.2.0 0.0.0.255
network 100.1.1.0 0.0.0.255
#
return

```

● CE1 的配置文件

```

#
sysname CE1
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 10
ip address 10.1.1.1 255.255.255.0
#
return

```

● CE2 的配置文件

```
#
 sysname CE2
#
interface GigabitEthernet1/0/0.1
 undo shutdown
 vlan-type dot1q 10
 ip address 10.1.1.2 255.255.255.0
#
return
```

● Switch1 的配置文件

```
#
 sysname Switch1
#
 vlan batch 100
#
interface GigabitEthernet1/0/0
 undo shutdown
 port trunk allow-pass vlan 100
#
interface GigabitEthernet1/0/1
 undo shutdown
 port vlan-stacking outside-vlan 10 stack-vlan 100
#
return
```

● Switch2 的配置文件

```
#
 sysname Switch2
#
 vlan batch 100
#
interface GigabitEthernet1/0/0
 undo shutdown
 port trunk allow-pass vlan 100
#
interface GigabitEthernet1/0/1
 undo shutdown
 port vlan-stacking outside-vlan 10 stack-vlan 100
#
return
```

8.18.10 配置 EFM OAM 与 MPLS OAM 联动功能示例

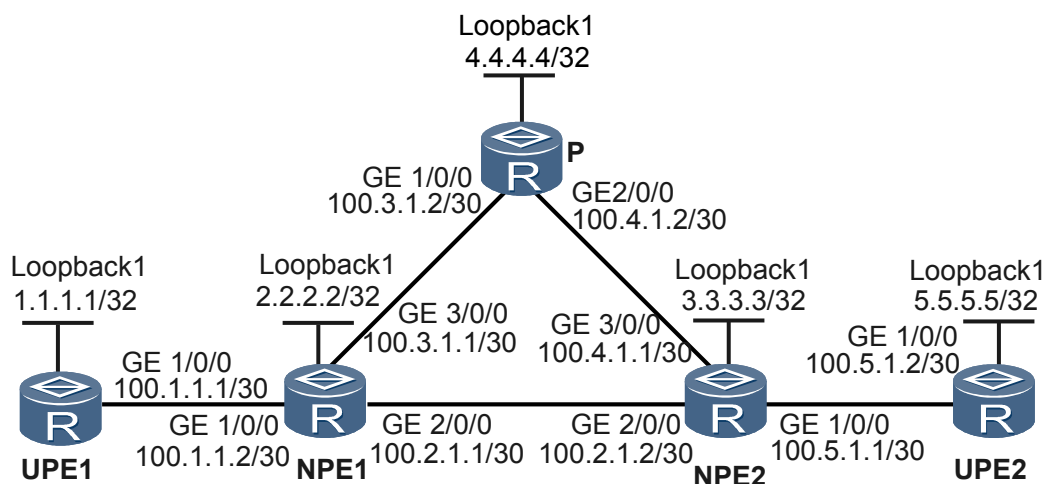
本示例中，通过 EFM OAM 与 MPLS OAM 联动功能，实现 EFM OAM 之间通过以太网 CFM 进行故障信息传递。

组网需求

在图 8-25 所示的运营商网络中，NPE 和 P 之间采用以太网链路，UPE 和 NPE 之间采用以太网链路。

要求在 NPE 之间配置 MPLS OAM，在 UPE 和 NPE 之间配置 EFM OAM，并且配置 EFM OAM 和 MPLS OAM 之间的联动，使 UPE1 和 NPE1 之间 EFM OAM 发现的故障，能够通过 MPLS OAM 传递给 NPE2 与 UPE2 的 EFM OAM。

图 8-25 配置 EFM OAM 与 MPLS OAM 联动功能组网图



配置思路

采用如下思路配置 EFM OAM 与 MPLS OAM 联动的基本功能：

1. 在运营商网络中运行 IGP，实现各设备之间的互通。
2. 在 NPE 之间配置 MPLS OAM。
3. 在 NPE 和 UPE 之间配置 EFM OAM。
4. 配置 UPE1 与 NPE1 之间的 EFM OAM 向 MPLS OAM 传递故障，MPLS OAM 向 NPE2 与 UPE2 之间的 EFM OAM 传递故障。

数据准备

为完成此配置例，需准备如下的数据：

- 各路由器的接口 IP 地址、各隧道接口名、隧道 ID。
- 发送的检测报文类型。
- 反向通道的占用方式等参数。

操作步骤

步骤 1 配置各接口 IP 地址（略）

按照图 8-25 配置各接口的 IP 地址和掩码，包括各 Loopback 接口地址，具体配置请参见配置文件。

步骤 2 配置 IGP 协议，本例中使用 IS-IS

配置 UPE1。

```
[UPE1] isis 1
[UPE1-isis-1] network-entity 00.0005.0000.0000.0001.00
[UPE1-isis-1] is-level level-2
[UPE1-isis-1] quit
[UPE1] interface gigabitethernet 1/0/0
[UPE1-GigabitEthernet1/0/0] isis enable 1
```

```
[UPE1-GigabitEthernet1/0/0] undo shutdown
[UPE1-GigabitEthernet1/0/0] quit
[UPE1] interface loopback 1
[UPE1-LoopBack1] isis enable 1
[UPE1-LoopBack1] quit

# 配置 NPE1。

[NPE1] isis 1
[NPE1-isis-1] network-entity 00.0005.0000.0000.0002.00
[NPE1-isis-1] is-level level-2
[NPE1-isis-1] quit
[NPE1] interface gigabitethernet 1/0/0
[NPE1-GigabitEthernet1/0/0] isis enable 1
[NPE1-GigabitEthernet1/0/0] undo shutdown
[NPE1-GigabitEthernet1/0/0] quit
[NPE1] interface gigabitethernet 2/0/0
[NPE1-GigabitEthernet2/0/0] isis enable 1
[NPE1-GigabitEthernet2/0/0] undo shutdown
[NPE1-GigabitEthernet2/0/0] quit
[NPE1] interface gigabitethernet 3/0/0
[NPE1-GigabitEthernet3/0/0] isis enable 1
[NPE1-GigabitEthernet3/0/0] undo shutdown
[NPE1-GigabitEthernet3/0/0] quit
[NPE1] interface loopback 1
[NPE1-LoopBack1] isis enable 1
[NPE1-LoopBack1] quit

# 配置 P。

[P] isis 1
[P-isis-1] network-entity 00.0005.0000.0000.0004.00
[P-isis-1] is-level level-2
[P-isis-1] quit
[P] interface gigabitethernet 1/0/0
[P-GigabitEthernet1/0/0] isis enable 1
[P-GigabitEthernet1/0/0] undo shutdown
[P-GigabitEthernet1/0/0] quit
[P] interface gigabitethernet 2/0/0
[P-GigabitEthernet2/0/0] isis enable 1
[P-GigabitEthernet2/0/0] undo shutdown
[P-GigabitEthernet2/0/0] quit
[P] interface loopback 1
[P-LoopBack1] isis enable 1
[P-LoopBack1] quit

# 配置 NPE2。

[NPE2] isis 1
[NPE2-isis-1] network-entity 00.0005.0000.0000.0003.00
[NPE2-isis-1] is-level level-2
[NPE2-isis-1] quit
[NPE2] interface gigabitethernet 1/0/0
[NPE2-GigabitEthernet1/0/0] isis enable 1
[NPE2-GigabitEthernet1/0/0] undo shutdown
[NPE2-GigabitEthernet1/0/0] quit
[NPE2] interface gigabitethernet 2/0/0
[NPE2-GigabitEthernet2/0/0] isis enable 1
[NPE2-GigabitEthernet2/0/0] undo shutdown
[NPE2-GigabitEthernet2/0/0] quit
[NPE2] interface gigabitethernet 3/0/0
[NPE2-GigabitEthernet3/0/0] isis enable 1
[NPE2-GigabitEthernet3/0/0] undo shutdown
[NPE2-GigabitEthernet3/0/0] quit
[NPE2] interface loopback 1
[NPE2-LoopBack1] isis enable 1
[NPE2-LoopBack1] quit

# 配置 UPE2。
```

```
[UPE2] isis 1
[UPE2-isis-1] network-entity 00.0005.0000.0000.0005.00
[UPE2-isis-1] is-level level-2
[UPE2-isis-1] quit
[UPE2] interface gigabitethernet 1/0/0
[UPE2-GigabitEthernet1/0/0] isis enable 1
[UPE2-GigabitEthernet1/0/0] undo shutdown
[UPE2-GigabitEthernet1/0/0] quit
[UPE2] interface loopback 1
[UPE2-LoopBack1] isis enable 1
[UPE2-LoopBack1] quit
```

配置完成后，在各路由器上执行 **display ip routing-table** 命令，可以看到相互之间都学到了对方的路由。以 UPE1 的显示为例：

```
[UPE1] display ip routing-table
Route Flags: R - relied, D - download to fib
-----
Routing Tables: Public
      Destinations : 10          Routes : 10
Destination/Mask    Proto    Pre  Cost   Flags  NextHop    Interface
1.1.1.9/32         Direct   0     0       D    127.0.0.1   InLoopBack0
2.2.2.9/32         ISIS     15    10       D    100.1.1.2   GigabitEthernet1/0/0
3.3.3.9/32         ISIS     15    20       D    100.1.1.2   GigabitEthernet1/0/0
4.4.4.9/32         ISIS     15    20       D    100.1.1.2   GigabitEthernet1/0/0
5.5.5.9/32         ISIS     15    30       D    100.1.1.2   GigabitEthernet1/0/0
100.1.1.0/24        Direct   0     0       D    100.1.1.1   GigabitEthernet1/0/0
100.1.1.1/32        Direct   0     0       D    127.0.0.1   InLoopBack0
100.2.1.0/24        ISIS     15    20       D    100.1.1.2   GigabitEthernet1/0/0
100.3.1.0/24        ISIS     15    20       D    100.1.1.2   GigabitEthernet1/0/0
100.4.1.0/24        ISIS     15    30       D    100.1.1.2   GigabitEthernet1/0/0
100.5.1.0/24        ISIS     15    30       D    100.1.1.2   GigabitEthernet1/0/0
127.0.0.0/8         Direct   0     0       D    127.0.0.1   InLoopBack0
127.0.0.1/32        Direct   0     0       D    127.0.0.1   InLoopBack0
```

步骤 3 在 NPE 和 P 上配置 MPLS 基本能力，使能 MPLS TE、RSVP-TE 和 CSPF

配置 NPE1。

```
[NPE1] mpls lsr-id 2.2.2.2
[NPE1] mpls
[NPE1-mpls] mpls te
[NPE1-mpls] mpls rsdp-te
[NPE1-mpls] mpls te cspf
[NPE1-mpls] quit
[NPE1] interface gigabitethernet 2/0/0
[NPE1-GigabitEthernet2/0/0] mpls
[NPE1-GigabitEthernet2/0/0] mpls te
[NPE1-GigabitEthernet2/0/0] mpls rsdp-te
[NPE1-GigabitEthernet2/0/0] quit
[NPE1] interface gigabitethernet 3/0/0
[NPE1-GigabitEthernet3/0/0] mpls
[NPE1-GigabitEthernet3/0/0] mpls te
[NPE1-GigabitEthernet3/0/0] mpls rsdp-te
[NPE1-GigabitEthernet3/0/0] quit
```

配置 P。

```
[P] mpls lsr-id 4.4.4.4
[P] mpls
[P-mpls] mpls te
[P-mpls] mpls rsdp-te
[P-mpls] quit
[P] interface gigabitethernet 1/0/0
[P-GigabitEthernet1/0/0] mpls
[P-GigabitEthernet1/0/0] mpls te
[P-GigabitEthernet1/0/0] mpls rsdp-te
[P-GigabitEthernet1/0/0] quit
[P] interface gigabitethernet 2/0/0
```

```
[P-GigabitEthernet2/0/0] mpls
[P-GigabitEthernet2/0/0] mpls te
[P-GigabitEthernet2/0/0] mpls rsvp-te
[P-GigabitEthernet2/0/0] quit

# 配置 NPE2。

[NPE2] mpls lsr-id 3.3.3.3
[NPE2] mpls
[NPE2-mpls] mpls te
[NPE2-mpls] mpls rsvp-te
[NPE2-mpls] mpls te cspf
[NPE2-mpls] quit
[NPE2] interface gigabitEthernet 2/0/0
[NPE2-GigabitEthernet2/0/0] mpls
[NPE2-GigabitEthernet2/0/0] mpls te
[NPE2-GigabitEthernet2/0/0] mpls rsvp-te
[NPE2-GigabitEthernet2/0/0] quit
[NPE2] interface gigabitEthernet 3/0/0
[NPE2-GigabitEthernet3/0/0] mpls
[NPE2-GigabitEthernet3/0/0] mpls te
[NPE2-GigabitEthernet3/0/0] mpls rsvp-te
[NPE2-GigabitEthernet3/0/0] quit
```

步骤 4 在 NPE 和 P 上配置 IS-IS TE

```
# 配置 NPE1。

[NPE1] isis 1
[NPE1-isis-1] cost-style wide
[NPE1-isis-1] traffic-eng level-2
[NPE1-isis-1] quit

# 配置 P。

[P] isis 1
[P-isis-1] cost-style wide
[P-isis-1] traffic-eng level-2
[P-isis-1] quit

# 配置 NPE2。

[NPE2] isis 1
[NPE2-isis-1] cost-style wide
[NPE2-isis-1] traffic-eng level-2
[NPE2-isis-1] quit
```

步骤 5 在 NPE 上采用显式路径配置 TE 隧道

```
# 配置 NPE1。

[NPE1] explicit-path npe1-to-npe2
[NPE1-explicit-path-npe1-to-npe2] next hop 100.2.1.2
[NPE1-explicit-path-npe1-to-npe2] quit
[NPE1] interface tunnel 2/0/0
[NPE1-Tunnel2/0/0] ip address unnumbered interface loopback 1
[NPE1-Tunnel2/0/0] tunnel-protocol mpls te
[NPE1-Tunnel2/0/0] destination 3.3.3.3
[NPE1-Tunnel2/0/0] mpls te tunnel-id 100
[NPE1-Tunnel2/0/0] mpls te signal-protocol rsvp-te
[NPE1-Tunnel2/0/0] mpls te path explicit-path work
[NPE1-Tunnel2/0/0] mpls te commit
[NPE1-Tunnel2/0/0] quit

# 配置 NPE2。

[NPE2] explicit-path npe2-to-npe1
[NPE2-explicit-path-npe2-to-npe1] next hop 100.4.1.2
[NPE2-explicit-path-npe2-to-npe1] quit
[NPE2] interface tunnel 3/0/0
```

```
[NPE2-Tunnel3/0/0] ip address unnumbered interface loopback 1
[NPE2-Tunnel3/0/0] tunnel-protocol mpls te
[NPE2-Tunnel3/0/0] destination 2.2.2.2
[NPE2-Tunnel3/0/0] mpls te tunnel-id 200
[NPE2-Tunnel3/0/0] mpls te signal-protocol rsvp-te
[NPE2-Tunnel3/0/0] mpls te path explicit-path work
[NPE2-Tunnel3/0/0] mpls te commit
[NPE2-Tunnel3/0/0] quit
```

完成上述配置后，在 NPE 上执行 **display interface tunnel** 命令可以看到隧道接口状态为 Up。以 NPE1 为例：

```
[NPE1] display interface tunnel
Tunnel2/0/0 current state : UP
Line protocol current state : UP
Description : Tunnel2/0/0 Interface
The Maximum Transmit Unit is 1500 bytes
Internet Address is unnumbered, using address of LoopBack1 (2.2.2.2/32)
Encapsulation is TUNNEL, loopback not set
Tunnel destination 3.3.3.3
Tunnel protocol/transport MPLS/MPLS, ILM is available,
primary tunnel id is 0x1002001, secondary tunnel id is 0x0
The tunnelIfIndex is 0xc000505
    5 minutes output rate 0 bits/s, 0 packets/s
    0 packets output, 0 bytes
    0 packets output dropped
```

步骤 6 在 NPE 上配置 MPLS OAM 功能，NPE1 为入节点，NPE2 为出节点

配置 NPE1。

```
[NPE1] mpls
[NPE1-mpls] mpls oam
[NPE1-mpls] quit
[NPE1] mpls oam ingress tunnel2/0/0 type ffd frequency 100
[NPE1] mpls oam ingress enable all
```

配置 NPE2。

```
[NPE2] mpls
[NPE2-mpls] mpls oam
[NPE2-mpls] quit
[NPE2] mpls oam egress lsr-id 2.2.2.2 tunnel-id 100 auto-protocol backward-lsp tunnel 3/0/0 private
```

配置完成后，在入节点 NPE1 和出节点 NPE2 上查看 LSP 的 MPLS OAM 参数及状态信息。可以看到入节点和出节点都处于正常检测状态，没有故障。

以 NPE2 的显示为例。

```
[NPE2] display mpls oam egress all verbose
```

```
Verbose information about the NO.1 oam at the egress
```

lsp basic information:		oam basic information:	
Lsp name	: --	Oam-Index	: 256
Lsp signal status	: Up	Oam select board	: 1
Lsp establish type	: Rsvp lsp	Enable-state	: --
Lsp incoming Label	: 3	Auto-protocol	: Enable
Lsp ingress lsr-id	: 2.2.2.2	Auto-overtime (s)	: 300
Lsp tnl-id/lsp-id	: 100/1	Ttsi/lsr-id	: 2.2.2.2
Lsp Incoming-int	: Gigabitethernet2/0/0	Ttsi/tunnel-id	: 100
oam detect information:		oam backward information:	
Type	: FFD	Tunnel name	: Tunnel2/0/0
Frequency	: 100 ms	Share attribute	: Private
Detect-state	: Start	Lsp signal status	: Up
Defect-state	: Non-defect	Bdi-frequency	: Detect-freq
Available state	: Available		

```
Unavailable time (s): 0
```

```
-----  
Total Oam Num:                1  
Total Start Oam Num:          1  
Total Defect Oam Num:         0  
Total Unavailable Oam Num:    0
```

步骤 7 在 UPE 和 NPE 上配置 EFM OAM

配置 UPE1。

```
[UPE1] efm enable  
[UPE1] interface gigabitethernet 1/0/0  
[UPE1-GigabitEthernet1/0/0] efm enable  
[UPE1-GigabitEthernet1/0/0] quit
```

配置 NPE1。

```
[NPE1] efm enable  
[NPE1] interface gigabitethernet 1/0/0  
[NPE1-GigabitEthernet1/0/0] efm enable  
[NPE1-GigabitEthernet1/0/0] quit
```

配置 UPE2。

```
[UPE2] efm enable  
[UPE2] interface gigabitethernet 1/0/0  
[UPE2-GigabitEthernet1/0/0] efm enable  
[UPE2-GigabitEthernet1/0/0] quit
```

配置 NPE2。

```
[NPE2] efm enable  
[NPE2] interface gigabitethernet 1/0/0  
[NPE2-GigabitEthernet1/0/0] efm enable  
[NPE2-GigabitEthernet1/0/0] quit
```

配置完成后，在 UPE 或 NPE 上执行 **display efm session** 命令，可看到接口 GE1/0/0 的 EFM OAM 协议状态为“detect”。以 UPE2 为例：

```
[UPE2] display efm session interface gigabitethernet 1/0/0  
Interface                EFM State                Loopback Timeout  
-----  
GigabitEthernet1/0/0    detect                    --
```

步骤 8 在 NPE 上配置 EFM OAM 和 MPLS OAM 的联动

配置 NPE1。

```
[NPE1] oam-mgr  
[NPE1-oam-mgr] oam-bind ingress efm interface gigabitethernet 1/0/0 egress mpls oam tunnel 2/0/0
```

配置 NPE2。

```
[NPE2] oam-mgr  
[NPE2-oam-mgr] oam-bind ingress mpls oam lsr-id 2.2.2.2 tunnel-id 200 egress efm interface  
gigabitethernet 1/0/0
```

 说明

在创建静态 LSP 时，如果指定了 lsr-id 和 tunnel-id，那么据此创建的 MPLS OAM 检测实例只记录 lsr-id 和 tunnel-id 信息，此时配置 ETH OAM 和 MPLS OAM 联动时，必须采用指定 lsr-id 和 tunnel-id 的方式。

步骤 9 检查配置结果

完成上述配置后，UPE1 和 NPE1 之间 EFM OAM 检测到的故障，可以通过 MPLS OAM 通告给 UPE2 和 NPE2 之间的 EFM OAM。

----结束

配置文件

● UPE1 的配置文件

```
#
 sysname UPE1
#
 efm enable
#
 isis 1
  is-level level-2
  network-entity 00.0005.0000.0000.0001.00
#
 interface GigabitEthernet1/0/0
  undo shutdown
  ip address 100.1.1.1 255.255.255.252
  isis enable 1
  efm enable
#
 interface LoopBack1
  ip address 1.1.1.1 255.255.255.255
  isis enable 1
#
return
```

● NPE1 的配置文件

```
#
 sysname NPE1
#
 efm enable
#
 mpls lsr-id 2.2.2.2
 mpls
  mpls te
  mpls rsvp-te
  mpls oam
  mpls te cspf
#
 explicit-path npe1-to-npe2
  next hop 100.2.1.2
#
 isis 1
  is-level level-2
  cost-style wide
  network-entity 00.0005.0000.0000.0002.00
  traffic-eng level-2
#
 interface GigabitEthernet1/0/0
  undo shutdown
  ip address 100.1.1.2 255.255.255.252
  isis enable 1
  efm enable
#
 interface GigabitEthernet2/0/0
  undo shutdown
  ip address 100.2.1.2 255.255.255.252
  isis enable 1
  mpls
  mpls te
  mpls rsvp-te
#
 interface GigabitEthernet3/0/0
  undo shutdown
  ip address 100.3.1.1 255.255.255.252
```

```
isis enable 1
mpls
mpls te
mpls rsvp-te
#
interface LoopBack1
ip address 2.2.2.2 255.255.255.255
isis enable 1
#
interface Tunnel2/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 3.3.3.3
mpls te tunnel-id 100
mpls te path explicit-path npel-to-npe2
mpls te commit
#
mpls oam ingress Tunnel2/0/0 type ffd frequency 100
mpls oam ingress enable Tunnel2/0/0
#
oam-mgr
oam-bind ingress efm interface GigabitEthernet 1/0/0 egress mpls oam Tunnel 2/0/0
#
return
```

● P 的配置文件

```
#
sysname P
#
mpls lsr-id 4.4.4.4
mpls
mpls te
mpls rsvp-te
#
isis 1
is-level level-2
cost-style wide
network-entity 00.0005.0000.0000.0004.00
traffic-eng level-2
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 100.3.1.2 255.255.255.252
isis enable 1
mpls
mpls te
mpls rsvp-te
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 100.4.1.2 255.255.255.252
isis enable 1
mpls
mpls te
mpls rsvp-te
#
interface LoopBack1
ip address 4.4.4.4 255.255.255.255
isis enable 1
#
return
```

● NPE2 的配置文件

```
#
sysname NPE2
#
efm enable
#
mpls lsr-id 3.3.3.3
mpls
```

```

mpls te
mpls rsvp-te
mpls oam
mpls te cspf
#
explicit-path npe2-to-npe1
next hop 100.4.1.2
#
isis 1
is-level level-2
cost-style wide
network-entity 00.0005.0000.0000.0003.00
traffic-eng level-2
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 100.5.1.1 255.255.255.252
isis enable 1
efm enable
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 100.2.1.2 255.255.255.252
isis enable 1
mpls
mpls te
mpls rsvp-te
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 100.4.1.1 255.255.255.252
isis enable 1
mpls
mpls te
mpls rsvp-te
#
interface LoopBack1
ip address 3.3.3.3 255.255.255.255
isis enable 1
#
interface Tunnel3/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 2.2.2.2
mpls te tunnel-id 200
mpls te path explicit-path npe2-to-npe1
mpls te commit
#
mpls oam egress lsr-id 1.1.1.1 tunnel-id 100 backward-lsp Tunnel3/0/0 private
#
oam-mgr
oam-bind ingress mpls oam lsr-id 2.2.2.2 tunnel-id 200 egress efm interface GigabitEthernet
1/0/0
#
return

```

● UPE1 的配置文件

```

#
sysname UPE1
#
efm enable
#
isis 1
is-level level-2
network-entity 00.0005.0000.0000.0005.00
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 100.5.1.2 255.255.255.252
isis enable 1

```

```
efm enable
#
interface LoopBack1
ip address 5.5.5.5 255.255.255.255
isis enable 1
#
return
```

8.18.11 配置 EFM OAM 扩展 FOR VRRP 示例

本示例中，在 CE 和 PE 之间配置 EFM OAM，在 PE 之间配置 VRRP 备份组，实现主用设备承担网络流量。

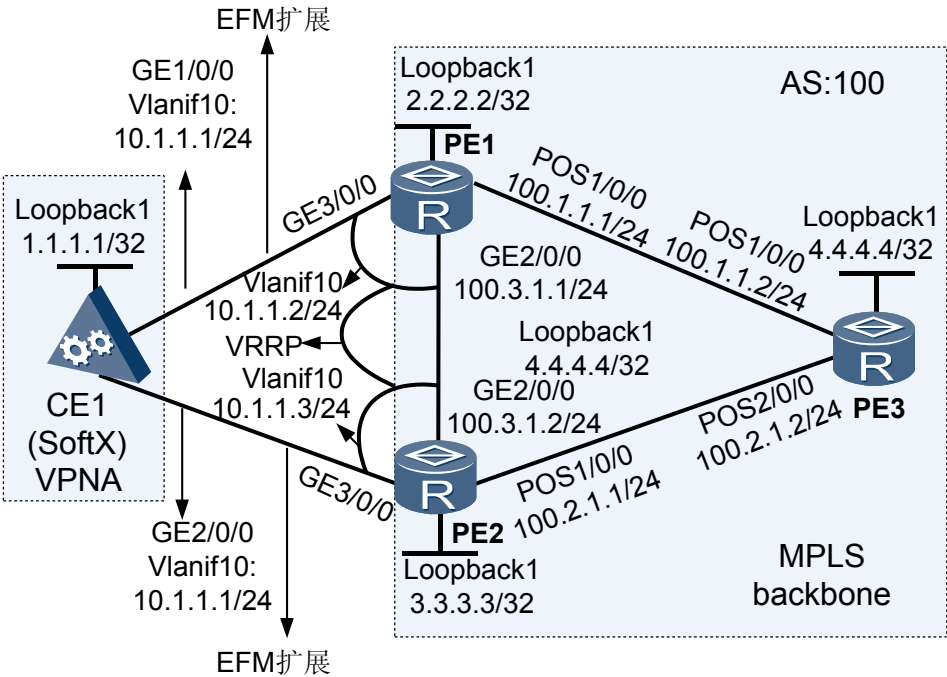
组网需求

说明

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

如图 8-26 所示。

图 8-26 配置 EFM OAM 扩展 FOR VRRP 组网图



CE1（SoftX 设备）上使用一对接口板做主备，主备接口板上配置同一个 IP 地址，通常情况下主接口板上 IP 有效。SoftX 业务双归接入网关 PE1 和 PE2。

PE1 和 PE2 之间配置 VLANIF，使两台路由器处于同一个广播域，路由器下行口为二层口，加入到该 VLAN。SoftX 通过使能 EFM OAM 扩展功能对连接 PE1 和 PE2 的链路分别运行 EFM 进行故障检测。

配置思路

采用如下的思路配置 EFM OAM 扩展 FOR VRRP 示例：

1. PE 之间配置 ISIS，实现 PE 之间的互通。
2. 在 PE 之间建立 MPLS LSP。
3. PE 上配置 VPN 实例，并把与 CE 相连的接口和相应的 VPN 实例绑定。
4. PE 之间配置 MP-IBGP 交换 VPN 路由信息。
5. 在 PE1 和 CE1、PE2 和 CE1 之间使能 EFM OAM 扩展功能，同时配置 EFM OAM 扩展会话与接口联动。
6. 创建 VRRP 备份组并配置跟踪接口状态。

数据准备

为完成此配置例，需准备如下的数据。

- 物理接口和 VLANIF 接口的 IP 地址。
- PE 上的 MPLS LSR ID。
- PE 上的 VPN 实例的名称、RD 及 VPN-Target。
- VRRP 备份组的虚拟 IP 地址、优先级。

操作步骤

步骤 1 配置路由器 PE1、PE2 的接口 IP 地址以及 CE1 的接口 IP 地址

配置 PE1。创建 VLAN10，将 GE2/0/0 和 GE3/0/0 加入 VLAN10。

```
<PE1> system-view
[PE1] interface gigabitethernet 2/0/0
[PE1-GigabitEthernet2/0/0] portswitch
[PE1-GigabitEthernet2/0/0] quit
[PE1] interface gigabitethernet 3/0/0
[PE1-GigabitEthernet3/0/0] portswitch
[PE1-GigabitEthernet3/0/0] quit
[PE1] vlan 10
[PE1-vlan10] port gigabitethernet 2/0/0
[PE1-vlan10] port gigabitethernet 3/0/0
[PE1-vlan10] interface vlanif10
[PE1-vlanif10] ip address 10.1.1.2 255.255.255.0
[PE1-vlanif10] quit
```

配置 PE2。创建 VLAN10，将 GE2/0/0 和 GE3/0/0 加入 VLAN10。

```
<PE2> system-view
[PE2] interface gigabitethernet 2/0/0
[PE2-GigabitEthernet2/0/0] portswitch
[PE2-GigabitEthernet2/0/0] quit
[PE2] interface gigabitethernet 3/0/0
[PE2-GigabitEthernet3/0/0] portswitch
[PE2-GigabitEthernet3/0/0] quit
[PE2] vlan 10
[PE2-vlan10] port gigabitethernet 2/0/0
[PE2-vlan10] port gigabitethernet 3/0/0
[PE2-vlan10] interface vlanif10
[PE2-vlanif10] ip address 10.1.1.3 255.255.255.0
[PE2-vlanif10] quit
```

配置 CE1。创建 VLAN10，将 GE1/0/0 和 GE2/0/0 加入 VLAN10。

```
<CE1> system-view
[CE1] interface gigabitethernet 1/0/0
[CE1-GigabitEthernet1/0/0] portswitch
[CE1-GigabitEthernet1/0/0] quit
[CE1] interface gigabitethernet 2/0/0
```

```
[CE1-GigabitEthernet2/0/0] portswitch
[CE1-GigabitEthernet2/0/0] quit
[CE1-vlan10] port gigabitethernet 1/0/0
[CE1-vlan10] port gigabitethernet 2/0/0
[CE1-vlan10] interface vlanif10
[CE1-vlanif10] ip address 10.1.1.1 255.255.255.0
[CE1-vlanif10] quit
```

步骤 2 在 MPLS 骨干网上配置 IGP 协议，实现骨干网的互通

配置 PE1。

```
[PE1] interface loopback 1
[PE1-LoopBack1] ip address 2.2.2.2 32
[PE1-LoopBack1] quit
[PE1] interface pos 1/0/0
[PE1-Pos1/0/0] ip address 100.1.1.1 24
[PE1-Pos1/0/0] isis enable
[PE1-Pos1/0/0] quit
[PE1] isis 1
[PE1-isis-1] is-level level-1-2
[PE1-isis-1] network-entity 10.0000.0000.0001.00
[PE1-isis-1] quit
```

配置 PE2。

```
[PE2] interface loopback 1
[PE2-LoopBack1] ip address 3.3.3.3 32
[PE2-LoopBack1] quit
[PE2] interface pos 1/0/0
[PE2-Pos1/0/0] ip address 100.2.1.1 24
[PE2-Pos1/0/0] isis enable
[PE2-Pos1/0/0] quit
[PE2] isis 1
[PE2-isis-1] is-level level-1-2
[PE2-isis-1] network-entity 10.0000.0000.0002.00
[PE2-isis-1] quit
```

配置 PE3。

```
[PE3] interface loopback 1
[PE3-LoopBack1] ip address 4.4.4.4 32
[PE3-LoopBack1] quit
[PE3] interface pos 1/0/0
[PE3-Pos1/0/0] ip address 100.1.1.2 24
[PE3-Pos1/0/0] isis enable
[PE3-Pos1/0/0] quit
[PE3] interface pos 2/0/0
[PE3-Pos2/0/0] ip address 100.2.1.2 24
[PE3-Pos2/0/0] isis enable
[PE3-Pos2/0/0] quit
[PE3] isis 1
[PE3-isis-1] is-level level-1-2
[PE3-isis-1] network-entity 10.0000.0000.0003.00
[PE3-isis-1] quit
```

步骤 3 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP。

配置 PE1。

```
[PE1] mpls lsr-id 2.2.2.2
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] interface pos 1/0/0
[PE1-Pos1/0/0] mpls
[PE1-Pos1/0/0] mpls ldp
[PE1-Pos1/0/0] quit
```

PE2 的配置如下：

```
[PE2] mpls lsr-id 3.3.3.3
[PE2] mpls
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-ldp] quit
[PE2] interface pos 1/0/0
[PE2-Pos1/0/0] mpls
[PE2-Pos1/0/0] mpls ldp
[PE2-Pos1/0/0] quit
```

PE3 的配置如下：

```
[PE3] mpls lsr-id 4.4.4.4
[PE3] mpls
[PE3-mpls] quit
[PE3] mpls ldp
[PE3-ldp] quit
[PE3] interface pos 1/0/0
[PE3-Pos1/0/0] mpls
[PE3-Pos1/0/0] mpls ldp
[PE3-Pos1/0/0] quit
[PE3] interface pos 2/0/0
[PE3-Pos2/0/0] mpls
[PE3-Pos2/0/0] mpls ldp
[PE3-Pos2/0/0] quit
```

上述配置完成后，PE 之间应能建立 LDP 会话，执行 **display mpls ldp session** 命令可以看到显示结果中 Status 项为“Operational”。

步骤 4 在 PE 上配置 VPN 实例，将 CE 接入 PE。

配置 PE1。

```
[PE1] ip vpn-instance vpna
[PE1-vpn-instance-vpna] route-distinguisher 100:1
[PE1-vpn-instance-vpna] vpn-target 111:1 both
[PE1-vpn-instance-vpna] quit
[PE1] interface vlanif 10
[PE1-vlanif10] ip binding vpn-instance vpna
[PE1-vlanif10] ip address 10.1.1.2 24
[PE1-vlanif10] quit
```

配置 PE2。

```
[PE2] ip vpn-instance vpna
[PE2-vpn-instance-vpna] route-distinguisher 100:2
[PE2-vpn-instance-vpna] vpn-target 111:1 both
[PE2-vpn-instance-vpna] quit
[PE2] interface vlanif 10
[PE2-vlanif10] ip binding vpn-instance vpna
[PE2-vlanif10] ip address 10.1.1.3 24
[PE2-vlanif10] quit
```

步骤 5 在 PE1 和 CE1、PE2 和 CE1 之间使能 EFM OAM 扩展功能。

配置 PE1。

```
[PE1] efm enable
[PE1] interface gigabitethernet 3/0/0
[PE1-GigabitEthernet3/0/0] efm enable
[PE1-GigabitEthernet3/0/0] efm trigger if-down
[PE1-GigabitEthernet3/0/0] quit
```

配置 PE2。

```
[PE2] efm enable
[PE2] interface gigabitethernet 3/0/0
```

```
[PE2-GigabitEthernet3/0/0] efm enable
[PE2-GigabitEthernet3/0/0] efm trigger if-down
[PE2-GigabitEthernet3/0/0] quit
```

步骤 6 在 PE1 和 PE2 配置指向 CE1 的静态路由，将静态路由引入 BGP。

配置 PE1。

```
[PE1] ip route-static vpn-instance vpna 1.1.1.1 32 10.1.1.1
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-vpna] import-route direct
[PE1-bgp-vpna] import-route static
[PE1-bgp-vpna] quit
```

配置 PE2。

```
[PE2] ip route-static vpn-instance vpna 1.1.1.1 32 10.1.1.1
[PE2] bgp 100
[PE2-bgp] ipv4-family vpn-instance vpna
[PE2-bgp-vpna] import-route direct
[PE2-bgp-vpna] import-route static
[PE2-bgp-vpna] quit
```

配置 CE1。将 VRRP 备份组的虚拟 IP 地址作为网关。

```
[CE1] ip route-static 0.0.0.0 0.0.0.0 10.1.1.111
```

步骤 7 在 PE 之间建立 MP-IBGP 对等体关系。

配置 PE1。

```
[PE1] bgp 100
[PE1-bgp] peer 3.3.3.3 as-number 100
[PE1-bgp] peer 3.3.3.3 connect-interface loopback 1
[PE1-bgp] peer 4.4.4.4 as-number 100
[PE1-bgp] peer 4.4.4.4 connect-interface loopback 1
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp] peer 3.3.3.3 enable
[PE1-bgp] peer 4.4.4.4 enable
[PE1-bgp] quit
```

配置 PE2。

```
[PE2] bgp 100
[PE2-bgp] peer 2.2.2.2 as-number 100
[PE2-bgp] peer 2.2.2.2 connect-interface loopback 1
[PE2-bgp] peer 4.4.4.4 as-number 100
[PE2-bgp] peer 4.4.4.4 connect-interface loopback 1
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp] peer 2.2.2.2 enable
[PE2-bgp] peer 4.4.4.4 enable
[PE2-bgp] quit
```

配置 PE3。

```
[PE3] bgp 100
[PE3-bgp] peer 2.2.2.2 as-number 100
[PE3-bgp] peer 2.2.2.2 connect-interface loopback 1
[PE3-bgp] peer 3.3.3.3 as-number 100
[PE3-bgp] peer 3.3.3.3 connect-interface loopback 1
[PE3-bgp] ipv4-family vpnv4
[PE3-bgp] peer 2.2.2.2 enable
[PE3-bgp] peer 3.3.3.3 enable
[PE3-bgp] quit
```

步骤 8 在 PE1 和 PE2 的 VLANIF 接口上配置 VRRP 备份组 track 接口。

配置 PE1。


```
[PE1] interface vlanif 10
[PE1-vlanif10] vrrp vrid 1 virtual-ip 10.1.1.111
[PE1-vlanif10] vrrp vrid 1 track interface gigabitethernet 3/0/0 reduced 60
[PE1-vlanif10] quit
```

配置 PE2。

```
[PE1] interface vlanif 10
[PE2-vlanif10] vrrp vrid 1 virtual-ip 10.1.1.111
[PE2-vlanif10] vrrp vrid 1 track interface gigabitethernet 3/0/0 reduced 60
[PE2-vlanif10] quit
```

步骤 9 检查配置结果

完成以上配置后，在 PE2 使用 **display interface** 命令查看备用接口状态，可以看到接口的协议状态为“DOWN (EFM down)”。此时接口处于阻塞状态，不转发流量。

```
[PE2] display interface GigabitEthernet 3/0/0
GigabitEthernet3/0/0 current state : UP
Line protocol current state : DOWN (EFM down)

Description: GigabitEthernet3/0/0 Interface
Switch Port,PVID : 10,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-0003-0003
The Vendor Name is AGILENT , The Vendor PN is HFCT-5710L
Transceiver BW: 1G, Transceiver Mode: Single Mode
WaveLength: 1310nm, Transmission Distance: 10km
Loopback:none, full-duplex mode, negotiation: disable, Pause Flowcontrol:Receive
Enable and Send Enable

Last physical up time : 2008-12-27 19:40:57
Last physical down time : 2008-12-27 19:40:56Statistics last cleared:2008-12-27
17:13:58
Last 300 seconds input rate: 520 bits/sec, 1 packets/sec
Last 300 seconds output rate: 592 bits/sec, 1 packets/sec
Input: 2041312 bytes, 15821 packets
Output: 591032 bytes, 9228 packets
Input:
  Unicast: 6176 packets, Multicast: 9627 packets
  Broadcast: 18 packets, JumboOctets: 0 packets
  CRC: 0 packets, Symbol: 0 packets
  Overrun: 0 packets, InRangeLength: 0 packets
  LongPacket: 0 packets, Jabber: 0 packets, Alignment: 0 packets
  Fragment: 0 packets, Undersized Frame: 0 packets
  RxPause: 0 packets
Output:
  Unicast: 21 packets, Multicast: 9144 packets
  Broadcast: 63 packets, JumboOctets: 0 packets
  Lost: 0 packets, Overflow: 0 packets, Underrun: 0 packets
  System: 0 packets, Overruns: 0 packets
  TxPause: 0 packets
  Unknown Vlan: 0 packets
```

在 PE1 和 PE2 上分别使用 **display vrrp** 命令查看 VRRP 备份组状态，可以看到 PE1 状态为“Master”，PE2 状态为“Backup”。即，PE1 为主用设备，承担流量转发任务。PE2 为备用设备，不转发流量。

```
[PE1] display vrrp
Vlanif10 | Virtual Router 1
  State : Master
  Virtual IP : 10.1.1.111
  Master IP : 10.1.1.2
  PriorityRun : 40
  PriorityConfig : 100
  MasterPriority : 100
  Preempt : YES Delay Time : 0
  TimerRun : 1
  TimerConfig : 1
```

```

Auth Type : NONE
Virtual Mac : 0000-5e00-0101
Check TTL : YES
Config type : normal-vrrp
Track IF : GigabitEthernet3/0/0    priority reduced : 60
IF State : Up
[PE2] display vrrp
Vlanif10 | Virtual Router 1
  State : Backup
  Virtual IP : 10.1.1.111
  Master IP  : 10.1.1.3
  PriorityRun : 40
  PriorityConfig : 100
  MasterPriority : 100
  Preempt : YES    Delay Time : 0
  TimerRun : 1
  TimerConfig : 1
  Auth Type : NONE
  Virtual Mac : 0000-5e00-0101
  Check TTL : YES
  Config type : normal-vrrp
  Track IF : GigabitEthernet3/0/0    priority reduced : 60
  IF State : DOWN

```

----结束

配置文件

- PE1 的配置文件

```

#
sysname PE1
#
vlan 10
#
ip vpn-instance vpna
 route-distinguisher 100:1
 vpn-target 111:1 export-extcommunity
 vpn-target 111:1 import-extcommunity
#
mpls lsr-id 2.2.2.2
mpls
#
mpls ldp
#
isis 1
 network-entity 10.0000.0000.0001.00
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 1 track interface GigabitEthernet3/0/0 reduced 60
 ip binding vpn-instance vpna
#
interface Pos1/0/0
 link-protocol ppp
 ip address 100.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 undo shutdown
 portswitch
 port default vlan 10
#
interface GigabitEthernet3/0/0
 undo shutdown
 portswitch
 port default vlan 10

```

```
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
bgp 100
 peer 4.4.4.4 as-number 100
 peer 4.4.4.4 connect-interface LoopBack1
 peer 3.3.3.3 as-number 100
 peer 3.3.3.3 connect-interface LoopBack1
#
ipv4-family unicast
 undo synchronization
 peer 4.4.4.4 enable
 peer 3.3.3.3 enable
#
ipv4-family vpnv4
 policy vpn-target
 peer 3.3.3.3 enable
 peer 4.4.4.4 enable
#
ipv4-family vpn-instance vpna
 import-route direct
import-route static
#
 ip route-static vpn-instance vpna 1.1.1.1 255.255.255.255 10.1.1.1
#
return
```

● PE2 的配置文件

```
#
 sysname PE2
#
 vlan 10
#
ip vpn-instance vpna
 route-distinguisher 100:1
 vpn-target 111:1 export-extcommunity
 vpn-target 111:1 import-extcommunity
#
 mpls lsr-id 3.3.3.3
 mpls
#
 mpls ldp
#
 isis 1
 network-entity 10.0000.0000.0002.00
#
interface Vlanif10
 ip address 10.1.1.3 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 1 track interface GigabitEthernet3/0/0 reduced 60
 ip binding vpn-instance vpna
#
interface Pos1/0/0
 link-protocol ppp
 ip address 100.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 undo shutdown
 portswitch
 port default vlan 10
#
interface GigabitEthernet3/0/0
 undo shutdown
 portswitch
 port default vlan 10
#
interface LoopBack1
```

```

    ip address 3.3.3.3 255.255.255.255
#
bgp 100
peer 4.4.4.4 as-number 100
peer 4.4.4.4 connect-interface LoopBack1
peer 2.2.2.2 as-number 100
peer 2.2.2.2 connect-interface LoopBack1
#
ipv4-family unicast
undo synchronization
peer 4.4.4.4 enable
peer 2.2.2.2 enable
#
ipv4-family vpnv4
policy vpn-target
peer 2.2.2.2 enable
peer 4.4.4.4 enable
#
ipv4-family vpn-instance vpna
import-route direct
import-route static
#
ip route-static vpn-instance vpna 1.1.1.1 255.255.255.255 10.1.1.1
#
return

```

● PE3 的配置文件

```

#
sysname PE3
#
mpls lsr-id 4.4.4.4
mpls
#
mpls ldp
#
isis 1
network-entity 10.0000.0000.0003.00
#
interface Pos1/0/0
link-protocol ppp
ip address 100.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
ip address 100.2.1.2 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 4.4.4.4 255.255.255.255
#
bgp 100
peer 2.2.2.2 as-number 100
peer 2.2.2.2 connect-interface LoopBack1
peer 3.3.3.3 as-number 100
peer 3.3.3.3 connect-interface LoopBack1
#
ipv4-family unicast
peer 2.2.2.2 enable
peer 3.3.3.3 enable
#
ipv4-family vpnv4
policy vpn-target
peer 2.2.2.2 enable
peer 3.3.3.3 enable
#
return

```

● CE1 的配置文件

```
#
 sysname CE1
#
 efm enable
#
 interface GigabitEthernet1/0/0
  undo shutdown
  portswitch
  port default vlan 10
#
 interface GigabitEthernet2/0/0
  undo shutdown
  portswitch
  port default vlan 10
#
 interface LoopBack1
  ip address 1.1.1.1 255.255.255.255
#
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.111
#
return
```

8.18.12 配置 EFM OAM 扩展 FOR 静态路由示例

本示例中，通过在 CE 和 PE 之间配置 EFM OAM 功能，在 PE 上配置到 CE 的静态路由，实现链路保护和切换。

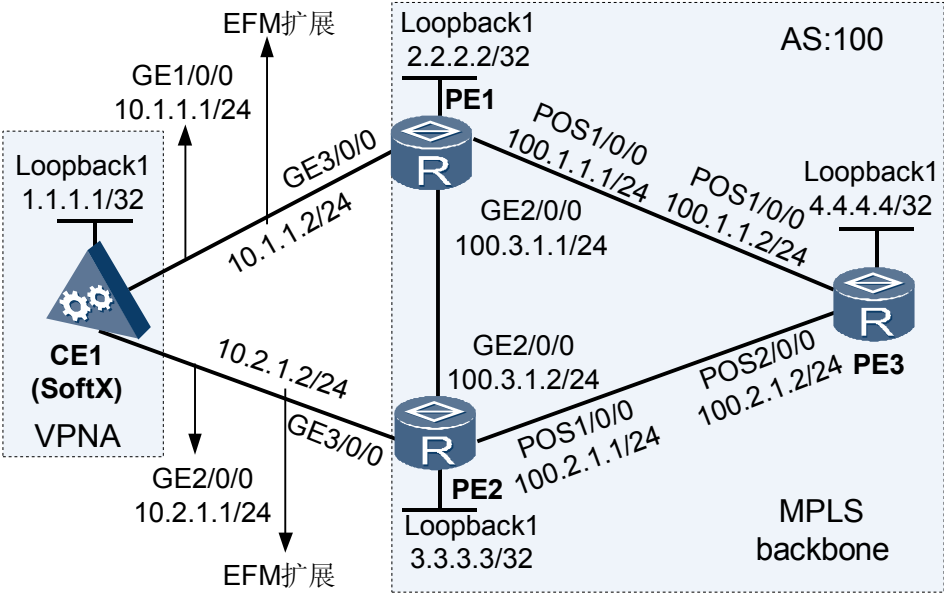
组网需求

说明

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

如图 8-27 所示。

图 8-27 配置 EFM OAM 扩展 FOR 静态路由组网图



CE1（SoftX）上使用一对接口板做主备，主备接口板上配置同一个 IP 地址，通常情况下主接口板上 IP 有效。SoftX 业务双归接入网关 PE1 和 PE2。

PE1、PE2 上配置到 CE1 的静态路由，并配置静态路由跟踪 EFM OAM 扩展会话的状态进行链路保护和切换。

配置思路

采用如下的思路配置 EFM OAM 扩展 FOR 静态路由示例：

1. PE 之间配置 ISIS，实现 PE 之间的互通。
2. 在 PE 之间建立 MPLS LSP。
3. PE 上配置 VPN 实例，并把与 CE 相连的接口和相应的 VPN 实例绑定。
4. PE 之间配置 MP-IBGP 交换 VPN 路由信息。
5. 在 PE1 和 CE1、PE2 和 CE1 之间使能 EFM OAM 扩展。
6. 在 PE1、PE2 上分别配置到 CE1 的静态路由。配置静态路由跟踪 EFM OAM 扩展会话。将静态路由引入 BGP。

数据准备

为完成此配置例，需准备如下的数据。

- 物理接口的 IP 地址。
- PE 上的 MPLS LSR ID。
- PE 上的 VPN 实例的名称、RD 及 VPN-Target。

操作步骤

步骤 1 在 MPLS 骨干网上配置 IGP 协议，实现骨干网的互通

配置 PE1。

```
[PE1] interface loopback 1
[PE1-LoopBack1] ip address 2.2.2.2 32
[PE1-LoopBack1] quit
[PE1] interface pos 1/0/0
[PE1-Pos1/0/0] ip address 100.1.1.1 24
[PE1-Pos1/0/0] isis enable
[PE1-Pos1/0/0] quit
[PE1] interface pos 20/0
[PE1-Pos2//0] ip address 100.3.1.1 24
[PE1-Pos2/0/0] isis enable
[PE1-Pos20/0] quit
[PE1] isis 1
[PE1-isis-1] is-level level-1-2
[PE1-isis-1] network-entity 10.0000.0000.0001.00
[PE1-isis-1] quit
```

配置 PE2。

```
[PE2] interface loopback 1
[PE2-LoopBack1] ip address 3.3.3.3 32
[PE2-LoopBack1] quit
[PE2] interface pos 1/0/0
[PE2-Pos1/0/0] ip address 100.2.1.1 24
[PE2-Pos1/0/0] isis enable
[PE2-Pos1/0/0] quit
[PE2] interface pos 20/0
[PE2-Pos2/0/0] ip address 100.3.1.1 24
```

```
[PE2-Pos2/0/0] isis enable
[PE2-Pos2/0/0] quit
[PE2] isis 1
[PE2-isis-1] is-level level-1-2
[PE2-isis-1] network-entity 10.0000.0000.0002.00
[PE2-isis-1] quit
```

配置 PE3。

```
[PE3] interface loopback 1
[PE3-LoopBack1] ip address 4.4.4.4 32
[PE3-LoopBack1] quit
[PE3] interface pos 1/0/0
[PE3-Pos1/0/0] ip address 100.1.1.2 24
[PE3-Pos1/0/0] isis enable
[PE3-Pos1/0/0] quit
[PE3] interface pos 2/0/0
[PE3-Pos2/0/0] ip address 100.2.1.2 24
[PE3-Pos2/0/0] isis enable
[PE3-Pos2/0/0] quit
[PE3] isis 1
[PE3-isis-1] is-level level-1-2
[PE3-isis-1] network-entity 10.0000.0000.0003.00
[PE3-isis-1] quit
```

配置完成后，PE1、PE2、PE3 之间应能建立 IS-IS 邻居关系，执行 **display ip routing-table** 命令可以看到 PE 之间学习到对方的 Loopback1 路由。

以 PE1 的显示为例：

```
[PE1] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 29          Routes : 30
Destination/Mask    Proto Pre  Cost   Flags NextHop         Interface
-----
      1.1.1.1/32     Direct 0    0       D    127.0.0.1       InLoopBack0
      3.3.3.3/32     ISIS   15   10       D    100.3.1.2       GigabitEthernet2/0/0
      4.4.4.4/32     ISIS   15   10       D    100.1.1.2       POS1/0/0
      10.1.1.0/24    Direct 0    0       D    10.1.1.2       GigabitEthernet3/0/0
      10.1.1.2/32    Direct 0    0       D    127.0.0.1       InLoopBack0
      10.1.1.255/32  Direct 0    0       D    127.0.0.1       InLoopBack0

      127.0.0.0/8    Direct 0    0       D    127.0.0.1       InLoopBack0
      127.0.0.1/32   Direct 0    0       D    127.0.0.1       InLoopBack0
255.255.255.255/32  Direct 0    0       D    127.0.0.1       InLoopBack0
      100.1.1.0/24   Direct 0    0       D    100.1.1.1       POS1/0/0
      100.1.1.1/32   Direct 0    0       D    127.0.0.1       InLoopBack0
      100.1.1.255/32 Direct 0    0       D    127.0.0.1       InLoopBack0
      100.2.1.0/24   ISIS   15   20       D    100.3.1.2       GigabitEthernet2/0/0
                        ISIS   15   20       D    100.1.1.2       POS1/0/0
      100.3.1.0/24   Direct 0    0       D    100.3.1.1       GigabitEthernet2/0/0
      100.3.1.1/32   Direct 0    0       D    127.0.0.1       InLoopBack0
      100.3.1.255/32 Direct 0    0       D    127.0.0.1       InLoopBack0
255.255.255.255/32  Direct 0    0       D    127.0.0.1       InLoopBack0
```

步骤 2 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP。

配置 PE1。

```
[PE1] mpls lsr-id 2.2.2.2
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] interface pos 1/0/0
[PE1-Pos1/0/0] mpls
[PE1-Pos1/0/0] mpls ldp
```

```
[PE1-Pos1/0/0] quit
[PE1] interface pos 2/0/0
[PE1-Pos2/0/0] mpls
[PE1-Pos2/0/0] mpls ldp
[PE1-Pos2/0/0] quit
```

PE2 的配置如下:

```
[PE2] mpls lsr-id 3.3.3.3
[PE2] mpls
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-ldp] quit
[PE2] interface pos 1/0/0
[PE2-Pos1/0/0] mpls
[PE2-Pos1/0/0] mpls ldp
[PE2-Pos1/0/0] quit
[PE2] interface pos 2/0/0
[PE2-Pos2/0/0] mpls
[PE2-Pos2/0/0] mpls ldp
[PE2-Pos2/0/0] quit
```

PE3 的配置如下:

```
[PE3] mpls lsr-id 4.4.4.4
[PE3] mpls
[PE3-mpls] quit
[PE3] mpls ldp
[PE3-ldp] quit
[PE3] interface pos 1/0/0
[PE3-Pos1/0/0] mpls
[PE3-Pos1/0/0] mpls ldp
[PE3-Pos1/0/0] quit
[PE3] interface pos 2/0/0
[PE3-Pos2/0/0] mpls
[PE3-Pos2/0/0] mpls ldp
[PE3-Pos2/0/0] quit
```

上述配置完成后, PE 之间应能建立 LDP 会话, 执行 **display mpls ldp session** 命令可以看到显示结果中 Status 项为 “Operational”。

以 PE1 的显示为例:

```
[PE1] display mpls ldp session
```

LDP Session(s) in Public Network					
Peer-ID	Status	LAM	SsnRole	SsnAge	KA-Sent/Rcv
3.3.3.3:0	Operational	DU	Passive	000:02:22	572/572
4.4.4.4:0	Operational	DU	Passive	000:02:21	566/566
TOTAL: 2 session(s) Found.					
LAM : Label Advertisement Mode SsnAge Unit : DDD:HH:MM					

步骤 3 在 PE 上配置 VPN 实例, 将 CE 接入 PE。

配置 PE1。

```
[PE1] ip vpn-instance vpna
[PE1-vpn-instance-vpna] route-distinguisher 100:1
[PE1-vpn-instance-vpna] vpn-target 111:1 both
[PE1-vpn-instance-vpna] quit
[PE1] interface gigabitethernet 3/0/0
[PE1-GigabitEthernet3/0/0] ip binding vpn-instance vpna
[PE1-GigabitEthernet3/0/0] ip address 10.1.1.2 24
[PE1-GigabitEthernet3/0/0] quit
```

配置 PE2。


```
[PE2] ip vpn-instance vpna
[PE2-vpn-instance-vpna] route-distinguisher 100:2
[PE2-vpn-instance-vpna] vpn-target 111:1 both
[PE2-vpn-instance-vpna] quit
[PE2] interface gigabitethernet 3/0/0
[PE2-GigabitEthernet3/0/0] ip binding vpn-instance vpna
[PE2-GigabitEthernet3/0/0] ip address 10.1.1.2 24
[PE2-GigabitEthernet3/0/0] quit
```

配置 CE1。SoftX 设备的主板接口 IP 地址相同。

```
[CE1] interface gigabitethernet 1/0/0
[CE1-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[CE1-GigabitEthernet1/0/0] quit
[CE1] interface gigabitethernet 2/0/0
[CE1-GigabitEthernet2/0/0] ip address 10.1.1.1 24
[CE1-GigabitEthernet2/0/0] quit
```

配置完成后，在 PE 上执行 **display ip vpn-instance verbose** 命令可以看到 VPN 实例的配置情况。各 PE 能 ping 通自己接入的 CE。

以 PE1 和 CE1 为例：

```
[PE1] display ip vpn-instance verbose
Total VPN-Instances configured : 1

VPN-Instance Name and ID : vpna, 1
Create date : 2008/12/27 15:42:43
Up time : 0 days, 00 hours, 04 minutes and 15 seconds
Route Distinguisher : 100:1
Export VPN Targets : 111:1
Import VPN Targets : 111:1
Label policy : label per route
The diffserv-mode Information is : uniform
The ttl-mode Information is : pipe
Interfaces : GigabitEthernet3/0/0
[PE1] ping -vpn-instance vpna 10.1.1.1
PING 10.1.1.1: 56 data bytes, press CTRL_C to break
  Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=255 time=5 ms
  Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=255 time=2 ms
  Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=255 time=2 ms
  Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=255 time=2 ms
  Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=255 time=2 ms

--- 10.1.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 2/2/5 ms
```

步骤 4 在 PE1 和 CE1、PE2 和 CE1 之间使能 EFM OAM 扩展功能。

配置 PE1。

```
[PE1] efm enable
[PE1] interface gigabitethernet 3/0/0
[PE1-GigabitEthernet3/0/0] efm enable
[PE1-GigabitEthernet3/0/0] quit
```

配置 PE2。

```
[PE2] efm enable
[PE2] interface gigabitethernet 3/0/0
[PE2-GigabitEthernet3/0/0] efm enable
[PE2-GigabitEthernet3/0/0] quit
```

配置 CE1。

```
[CE1] efm enable
[CE1] interface gigabitethernet 1/0/0
```

```
[PE2-GigabitEthernet1/0/0] efm enable
[PE2-GigabitEthernet1/0/0] quit
interface gigabitethernet 2/0/0
[PE2-GigabitEthernet2/0/0] efm enable
[PE2-GigabitEthernet2/0/0] quit
```

步骤 5 在 PE1 和 PE2 配置指向 CE1 的静态路由，配置静态路由跟踪 EFM OAM 扩展会话状态。将静态路由引入 BGP。

配置 PE1。

```
[PE1] ip route-static vpn-instance vpna 1.1.1.1 32 10.1.1.1 track efm-state gigabitethernet 3/0/0
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-vpna] import-route direct
[PE1-bgp-vpna] import-route static
[PE1-bgp-vpna] quit
[PE1] interface gigabitethernet 1/0/3
[PE1-GigabitEthernet1/0/3] efm enable
[PE1-GigabitEthernet1/0/3] quit
```

配置 PE2。

```
[PE2] ip route-static vpn-instance vpna 1.1.1.1 32 10.2.1.1 track efm-state gigabitethernet 3/0/0
[PE2] bgp 100
[PE2-bgp] ipv4-family vpn-instance vpna
[PE2-bgp-vpna] import-route direct
[PE2-bgp-vpna] import-route static
[PE2-bgp-vpna] quit
```

步骤 6 在 PE 之间建立 MP-IBGP 对等体关系。

配置 PE1。

```
[PE1] bgp 100
[PE1-bgp] peer 3.3.3.3 as-number 100
[PE1-bgp] peer 3.3.3.3 connect-interface loopback 1
[PE1-bgp] peer 4.4.4.4 as-number 100
[PE1-bgp] peer 4.4.4.4 connect-interface loopback 1
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp] peer 3.3.3.3 enable
[PE1-bgp] peer 4.4.4.4 enable
[PE1-bgp] quit
```

配置 PE2。

```
[PE2] bgp 100
[PE2-bgp] peer 2.2.2.2 as-number 100
[PE2-bgp] peer 2.2.2.2 connect-interface loopback 1
[PE2-bgp] peer 4.4.4.4 as-number 100
[PE2-bgp] peer 4.4.4.4 connect-interface loopback 1
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp] peer 2.2.2.2 enable
[PE2-bgp] peer 4.4.4.4 enable
[PE2-bgp] quit
```

配置 PE3。

```
[PE3] bgp 100
[PE3-bgp] peer 2.2.2.2 as-number 100
[PE3-bgp] peer 2.2.2.2 connect-interface loopback 1
[PE3-bgp] peer 3.3.3.3 as-number 100
[PE3-bgp] peer 3.3.3.3 connect-interface loopback 1
[PE3-bgp] ipv4-family vpnv4
[PE3-bgp] peer 2.2.2.2 enable
[PE3-bgp] peer 3.3.3.3 enable
[PE3-bgp] quit
```

配置完成后，在 PE 上执行 **display bgp peer** 命令，可以看到 PE 之间的 BGP 对等体关系已建立，并达到“Established”状态。

```
[PE1] display bgp peer

BGP local router ID : 2.2.2.2
Local AS number : 100
Total number of peers : 2                Peers in established state : 2

Peer          V    AS  MsgRcvd  MsgSent   OutQ  Up/Down   State PrefRcv
4.4.4.4        4   100    205     202      0 03:05:25 Established    0
3.3.3.3        4   100    197     254      0 03:06:54 Established    0
```

步骤 7 检查配置结果

在 PE 上查看 VPN 路由表，静态路由存在于路由表中

```
[PE2] display ip routing-table vpn-instance vpna
Route Flags: R - relay, D - download to fib

-----
Routing Tables: vpna
      Destinations : 8          Routes : 8

Destination/Mask    Proto Pre  Cost   Flags NextHop         Interface
-----
      1.1.1.1/32 Static 60   0      RD    10.1.1.1      GigabitEthernet3/0/0
      10.1.1.0/24 Direct 0    0      D     10.1.1.2      GigabitEthernet3/0/0
      10.1.1.2/32 Direct 0    0      D     127.0.0.1     InLoopBack0
      10.1.1.255/32 Direct 0    0      D     127.0.0.1     InLoopBack0
      10.2.1.0/24 BGP   255  0      RD    3.3.3.9       GigabitEthernet2/0/0
      10.3.1.0/24 BGP   255  0      RD    4.4.4.4       POS1/0/0
      10.3.1.2/32 BGP   255  0      RD    4.4.4.4       POS1/0/0
      255.255.255.255/32 Direct 0    0      D     127.0.0.1     InLoopBack0
```

```
[PE2] display ip routing-table vpn-instance vpna
Route Flags: R - relay, D - download to fib

-----
Routing Tables: vpna
      Destinations : 8          Routes : 8

Destination/Mask    Proto Pre  Cost   Flags NextHop         Interface
-----
      1.1.1.1/32 BGP   255  0      RD    1.1.1.1       GigabitEthernet3/0/0
      10.1.1.0/24 BGP   255  0      RD    1.1.1.1       GigabitEthernet2/0/0
      10.2.1.0/24 Direct 0    0      D     10.2.1.2      GigabitEthernet3/0/0
      10.2.1.2/32 Direct 0    0      D     127.0.0.1     InLoopBack0
      10.2.1.255/32 Direct 0    0      D     127.0.0.1     InLoopBack0
      10.3.1.0/24 BGP   255  0      RD    4.4.4.4       POS1/0/0
      10.3.1.2/32 BGP   255  0      RD    4.4.4.4       POS1/0/0
      255.255.255.255/32 Direct 0    0      D     127.0.0.1     InLoopBack0
```

当 IP 业务设备主备接口切换后，其网关由 PE1 切换到 PE2。路由显示如下：

```
[PE1] display ip routing-table vpn-instance vpna
Route Flags: R - relay, D - download to fib

-----
Routing Tables: vpna
      Destinations : 8          Routes : 8

Destination/Mask    Proto Pre  Cost   Flags NextHop         Interface
-----
      1.1.1.1/32 BGP   255  0      RD    3.3.3.9       GigabitEthernet3/0/0
      10.1.1.0/24 Direct 0    0      D     10.1.1.2      GigabitEthernet3/0/0
      10.1.1.2/32 Direct 0    0      D     127.0.0.1     InLoopBack0
      10.1.1.255/32 Direct 0    0      D     127.0.0.1     InLoopBack0
      10.2.1.0/24 BGP   255  0      RD    3.3.3.9       GigabitEthernet2/0/0
      10.3.1.0/24 BGP   255  0      RD    4.4.4.4       POS1/0/0
      10.3.1.2/32 BGP   255  0      RD    4.4.4.4       POS1/0/0
      255.255.255.255/32 Direct 0    0      D     127.0.0.1     InLoopBack0
[PE2] display ip routing-table vpn-instance vpna
Route Flags: R - relay, D - download to fib
```

Routing Tables: vpna						
Destinations : 8			Routes : 8			
Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
1.1.1.1/32	Static	60	0	RD	10.2.1.1	GigabitEthernet3/0/0
10.1.1.0/24	BGP	255	0	RD	1.1.1.1	GigabitEthernet2/0/0
10.2.1.0/24	Direct	0	0	D	10.2.1.2	GigabitEthernet3/0/0
10.2.1.2/32	Direct	0	0	D	127.0.0.1	InLoopBack0
10.2.1.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
10.3.1.0/24	BGP	255	0	RD	4.4.4.4	POS1/0/0
10.3.1.2/32	BGP	255	0	RD	4.4.4.4	POS1/0/0
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

----结束

配置文件

```
● PE1 的配置文件
#
 sysname PE1
#
 efm enable
#
 ip vpn-instance vpna
  route-distinguisher 100:1
  vpn-target 111:1 export-extcommunity
  vpn-target 111:1 import-extcommunity
#
 mpls lsr-id 2.2.2.2
 mpls
#
 mpls ldp
#
 isis 1
  network-entity 10.0000.0000.0001.00
#
 interface GigabitEthernet3/0/0
  ip binding vpn-instance vpna
  ip address 10.1.1.2 255.255.255.0
  efm enable
#
 interface Pos1/0/0
  link-protocol ppp
  ip address 100.1.1.1 255.255.255.0
  mpls
  mpls ldp
#
 interface Pos2/0/0
  link-protocol ppp
  ip address 100.3.1.1 255.255.255.0
  mpls
  mpls ldp
#
 interface LoopBack1
  ip address 2.2.2.2 255.255.255.255
#
 bgp 100
  peer 4.4.4.4 as-number 100
  peer 4.4.4.4 connect-interface LoopBack1
  peer 3.3.3.3 as-number 100
  peer 3.3.3.3 connect-interface LoopBack1
#
 ipv4-family unicast
  undo synchronization
  peer 4.4.4.4 enable
  peer 3.3.3.3 enable
```

```
#
ipv4-family vpnv4
 policy vpn-target
 peer 3.3.3.3 enable
 peer 4.4.4.4 enable
#
ipv4-family vpn-instance vpna
 import-route direct
 import-route static
#
ip route-static vpn-instance vpna 1.1.1.1 255.255.255.255 10.1.1.1 track efm-state
gigabitethernet 3/0/0
#
return
```

● PE2 的配置文件

```
#
sysname PE2
#
efm enable
#
ip vpn-instance vpna
 route-distinguisher 100:2
 vpn-target 111:1 export-extcommunity
 vpn-target 111:1 import-extcommunity
#
mpls lsr-id 3.3.3.3
mpls
#
mpls ldp
#
isis 1
 network-entity 10.0000.0000.0002.00
#
interface GigabitEthernet3/0/0
 ip binding vpn-instance vpna
 ip address 10.2.1.2 255.255.255.0
 efm enable
#
interface Pos1/0/0
 link-protocol ppp
 ip address 100.2.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface Pos2/0/0
 link-protocol ppp
 ip address 100.3.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
bgp 100
 peer 4.4.4.4 as-number 100
 peer 4.4.4.4 connect-interface LoopBack1
 peer 2.2.2.2 as-number 100
 peer 2.2.2.2 connect-interface LoopBack1
#
ipv4-family unicast
 undo synchronization
 peer 4.4.4.4 enable
 peer 2.2.2.2 enable
#
ipv4-family vpnv4
 policy vpn-target
 peer 2.2.2.2 enable
 peer 4.4.4.4 enable
#
```

```

    ipv4-family vpn-instance vpna
        import-route direct
        import-route static
    #
    ip route-static vpn-instance vpna 1.1.1.1 255.255.255.255 10.2.1.1 track efm-state
    gigabitethernet 3/0/0
    #
    return

```

● PE3 的配置文件

```

#
sysname PE3
#
mpls lsr-id 4.4.4.4
mpls
#
mpls ldp
#
isis 1
    network-entity 10.0000.0000.0003.00
#
interface Pos1/0/0
    link-protocol ppp
    ip address 100.1.1.2 255.255.255.0
    mpls
    mpls ldp
#
interface Pos2/0/0
    link-protocol ppp
    ip address 100.2.1.2 255.255.255.0
    mpls
    mpls ldp
#
interface LoopBack1
    ip address 4.4.4.4 255.255.255.255
#
bgp 100
    peer 2.2.2.2 as-number 100
    peer 2.2.2.2 connect-interface LoopBack1
    peer 3.3.3.3 as-number 100
    peer 3.3.3.3 connect-interface LoopBack1
#
ipv4-family unicast
    peer 2.2.2.2 enable
    peer 3.3.3.3 enable
#
ipv4-family vpnv4
    policy vpn-target
    peer 2.2.2.2 enable
    peer 3.3.3.3 enable
#
return

```

● CE1 的配置文件

```

#
sysname CE1
#
efm enable
#
interface GigabitEthernet1/0/0
    ip address 10.1.1.1 255.255.255.0
    efm enable
#
interface GigabitEthernet2/0/0
    ip address 10.2.1.1 255.255.255.0
    efm enable
#
interface LoopBack1
    ip address 1.1.1.1 255.255.255.255
#

```

```
ip route-static 0.0.0.0 0.0.0.0 10.1.1.2
ip route-static 0.0.0.0 0.0.0.0 10.2.1.2
#
return
```

9 Y.1731 配置

关于本章

Y.1731 为网络层的 OAM 协议，不仅包含 IEEE802.1ag 的故障检测功能，同时还提供了如时延统计、丢包统计及 AIS 等性能检测和统计功能。

9.1 Y.1731 简介

9.2 配置 VLL 的单端丢包统计功能

组网环境为 VLL 场景，需要对链路的丢包性能进行统计且对等 MEP 不支持或一方不支持 CC 功能时，可以配置 VLL 的单端丢包统计功能。

9.3 配置 VLL 的双端丢包统计功能

组网环境为 VLL，需要同时检测链路连通性和丢包情况且对等 MEP 间均支持 CC（连通性检测）功能时，可以配置 VLL 的双端丢包统计功能。

9.4 配置 VLL 的单向时延统计功能

VLL 组网环境下，需要测量链路单方向的网络时延时，可以配置 VLL 的单向时延统计功能。

9.5 配置 VLL 的双向时延统计功能

VLL 组网环境下，需要统计链路时延功能且对等体 MEP 时钟不同步、对链路时延统计要求不高的情况下，可以采用双向时延统计功能。

9.6 配置 VPLS 的单端丢包统计功能

VPLS 组网下，需要对链路丢包性能进行统计且对等 MEP 不支持或一方不支持 CC 功能时，可以配置 VPLS 的单端丢包统计功能。

9.7 配置 VPLS 的双端丢包统计功能

VPLS 组网环境下，需要同时检测链路连通性和丢包情况并且对等 MEP 间均支持 CC（连通性检测）功能时，可以配置 VPLS 的双端丢包统计功能。

9.8 配置 VPLS 的单向时延统计功能

VPLS 组网环境下，需要测量链路单方向的网络时延时，可以配置 VPLS 的单向时延统计功能。

9.9 配置 VPLS 的双向时延统计功能

VPLS 组网环境下，需要测量链路网络时延且对等体 MEP 时钟不同步、对链路时延统计要求不高的情况下，可以采用双向时延统计功能。

9.10 配置举例

配置举例结合组网需求、配置思路和数据准备例举了 Y.1731 的基本功能及其应用。

9.1 Y.1731 简介

9.1.1 Y.1731 概述

Y.1731 作为 ITU-T 标准组织提出的 OAM 协议，除了能够实现城域以太网的端到端连通性检测、环回和链路跟踪外，还提供了诊断测试、性能管理（包括丢包率统计、帧时延统计、帧时延抖动统计、吞吐量统计）功能。

Y.1731 概述

以太网原来主要用于 LAN 技术中，OAM 能力较弱，且只有网元级的管理系统，其管理工具不足以支持公用电信网所必须的网络管理。当以太网技术用于城域网后，其 OAM 功能需求越来越受到重视。

根据网络的分层/分级架构，需要提供分层/分级的以太 OAM 功能。

- 802.3ah（Ethernet in the First Mile，简称 EFM）主要用于用户接入部分的以太网物理层规范以及接入部分的以太网 OAM，是链路级的 OAM。
- 802.1ag（Connectivity Fault Management，简称 CFM）定义了基于以太网承载网络的连接检测的 OAM 功能，包括 CC/LB/LT，适用于大规模组网的端到端场景，是网络级的 OAM。
- Y.1731 是由 ITU-T 标准组织提出的 OAM 协议，它不仅包含 IEEE802.1ag 所规定的内容，而且还增加了更多的 OAM 消息组合，包括 RDI（Remote Defect Indication），锁信号 LCK(Locked Signal)，测试信号，自动保护切换 APS（Automatic Protection Switching），维护通信通道 MCC（Maintenance Communication Channel），试验 EXP（Experimental OAM），供应商特定的 VSP（Vendor Specific OAM）故障管理以及用于性能监视的丢包管理 LM（Loss Measurement）和延迟评估 DM（Delay Measurement）等。

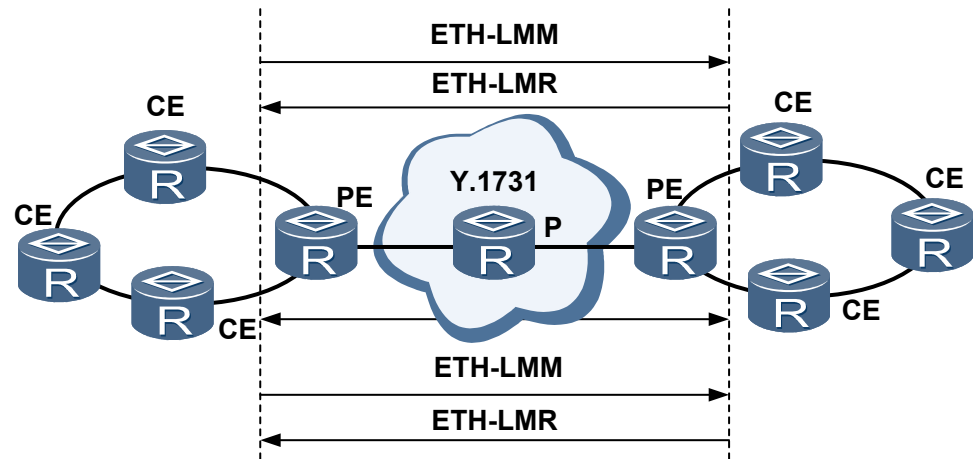
Y.1731 相关术语及基本原理

- 单端丢包统计

丢包统计功能是通过向其对等 MEP 发送带有 ETH-LM（Loss Measurement）信息的帧，并类似地从对等 MEP 接收带有 ETH-LM 信息的帧实现的。如图 9-1 所示，单端丢包统计时：

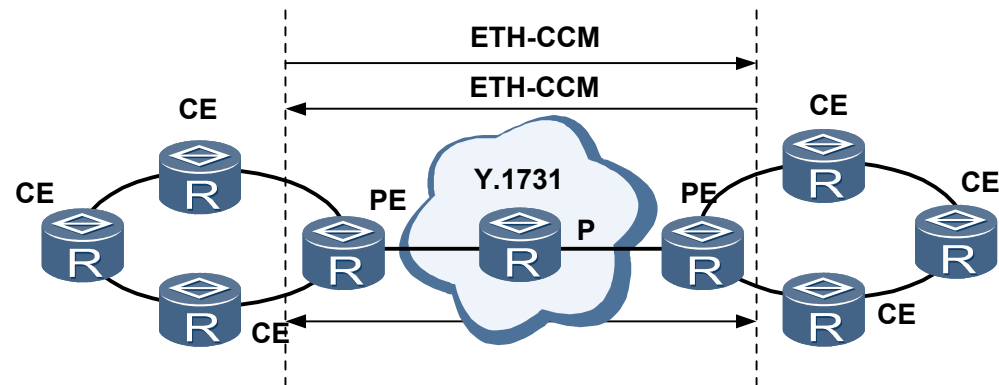
1. 本端设备的 MEP 向对端设备的 MEP 发送带有 ETH-LM 请求信息的帧(ETH-LMM)，ETH-LMM 报文包含了报文发送时本地发送计数器的值。
2. 对端设备的 MEP 收到 ETH-LMM 报文后，回复带有 ETH-LM 应答信息的帧(ETH-LMR)。
3. 本端设备的 MEP 收到 ETH-LMR 报文后，根据报文中的内容得到对应的统计信息，并计算出相应的丢包率。

图 9-1 单端丢包率统计组网图



- 双端丢包统计
丢包统计功能是通过向其对等 MEP 发送带有 ETH-LM (Loss Measurement) 信息的帧，并类似地从对等 MEP 接收带有 ETH-LM 信息的帧实现的。如图 9-2 所示，双端丢包统计时：
 1. 每个设备的 MEP 都向对端设备的 MEP 发送带有 ETH-LM 请求信息的帧。ETH-LM 信息的帧在这里就是 CCM 报文。
 2. 每个设备的 MEP 都处理对端设备发送来的带有 ETH-LM 信息的帧，进行近端和远端丢失帧的测量。
 3. 每个设备根据 CCM 报文中的内容得到对应的统计信息，并计算出相应的丢包率。

图 9-2 双端丢包率统计组网图



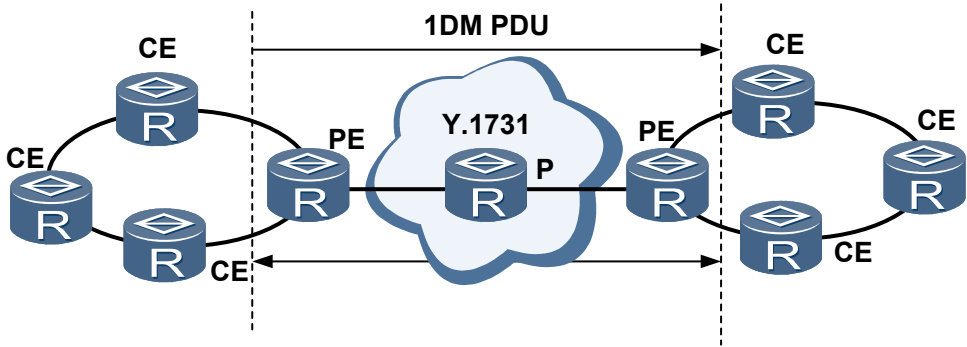
- 单向时延统计
单向时延统计是在端到端 MEP 之间，通过发送/接收 DM 报文进行计算。如图 9-3 所示，单向时延统计时：
 1. MEP 将周期地发送带有 TxTimeStampf (DM 传输时的时间戳) 数值的 DM 帧。
 2. RMEP 接收到 DM 报文后，解析出 DM 报文中 TxTimeStampf 值，与自身接收 DM 报文的时间 RxTimef 进行比较，得出单向时延值。计算公式如下：

$$\text{帧时延} = \text{RxTimef} - \text{TxTimeStampf}$$

通过上面公式中的帧时延还可以计算出帧时延变化，即帧时延抖动。

时延抖动：是对一对业务帧之间帧时延变化的度量，本次时延与上次时延之间的绝对差值。

图 9-3 单向时延统计组网图



● 双向时延统计

双向时延统计是在端到端 MEP 之间进行，通过接收 DMM 报文和发送 DMR 报文进行计算。如图 9-4 所示，双向时延统计时：

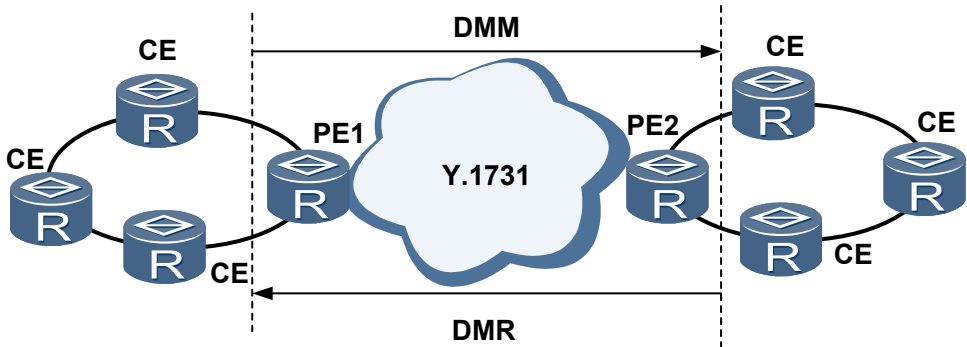
1. MEP 将周期性地发送带有 TxTimeStampf (DM 传输时的时间戳) 数值的 DMM 帧。
2. RMEP 接收到 DMM 报文后，填充 DMM 报文接收的时间戳值 RxTimeStampf, 然后修改报文的类型为 DMR 报文，并交换报文的目的 MAC 和源 MAC 发送出去，同时带上发送时间戳 TxTimeStampb。
3. 当 DMM 发送端收到 DMR 时与接收到 DMR 报文的时间 RxTimeb 进行比较，得出双向时延值。计算公式如下：

$$\text{帧时延} = (\text{RxTimeb} - \text{TxTimeStampf}) - (\text{TxTimeStampb} - \text{RxTimeStampf})$$

通过上面公式中的帧时延还可以计算出帧时延变化，即帧时延抖动。

时延抖动：是对一对业务帧之间帧时延变化的度量，本次时延与上次时延之间的绝对差值。

图 9-4 双向时延统计图



9.1.2 NE80E/40E 支持的 Y.1731 特性

本章节从 Y.1731 支持的应用场景及其功能角度介绍 NE80E/40E 支持的 Y.1731 特性。

NE80E/40E 支持的 Y.1731 特性包括 VLL/VPLS 组网环境下的单端丢包统计功能、双端丢包统计功能、单向时延统计功能、双向时延统计功能。其功能描述及其选择原则如表 9-1 所示。请根据实际的组网环境和需要实现的功能进行选择。

 说明

- 丢包统计和时延统计功能只支持 PE 之间公网隧道类型为 LDP LSP 和 TE LSP 的场景。
- 丢包统计功能不支持 PE 之间 PW 侧链路接口为 Eth-Trunk。

表 9-1 Y.1731 支持的功能

功能	单端丢包统计	双端丢包统计	单向时延统计	双向时延统计
功能描述	单端丢包统计通过对等 MEP 一方设备上进行网络丢包情况的测量,以确定链路的质量。	双端丢包统计通过对等 MEP 的两台设备上进行网络丢包情况的测量，以确定链路的质量。	单向时延统计通过测量对等 MEP 之间链路单方向的网络时延，以确定链路的质量。	双向时延统计通过测量对等 MEP 之间网络的往返时延，以确定链路的质量。
选择原则	当用户需要对链路的丢包性能进行检测时，可以选择单端丢包统计或者双端丢包统计，选择原则： ● 当用户需要同时检测链路连通性和丢包情况时，并且对等 MEP 间均支持 CC（连通性检测）功能时，可以选择双端丢包统计功能。 ● 当对等 MEP 间不支持或者一方不支持 CC 功能时，可以选择单端丢包统计功能。		当用户需要对链路的时延性能进行检测或者监控时，可以选择单向时延统计或者双向时延统计，选择原则： ● 当对等体 MEP 时钟同步且对链路时延统计要求较高的情况下，可以采用单向时延统计功能。 ● 当对等体 MEP 时钟不同步且对链路时延统计要求不高的情况下，可以采用双向时延统计功能。	

9.2 配置 VLL 的单端丢包统计功能

组网环境为 VLL 场景，需要对链路的丢包性能进行统计且对等 MEP 不支持或一方不支持 CC 功能时，可以配置 VLL 的单端丢包统计功能。

9.2.1 建立配置任务

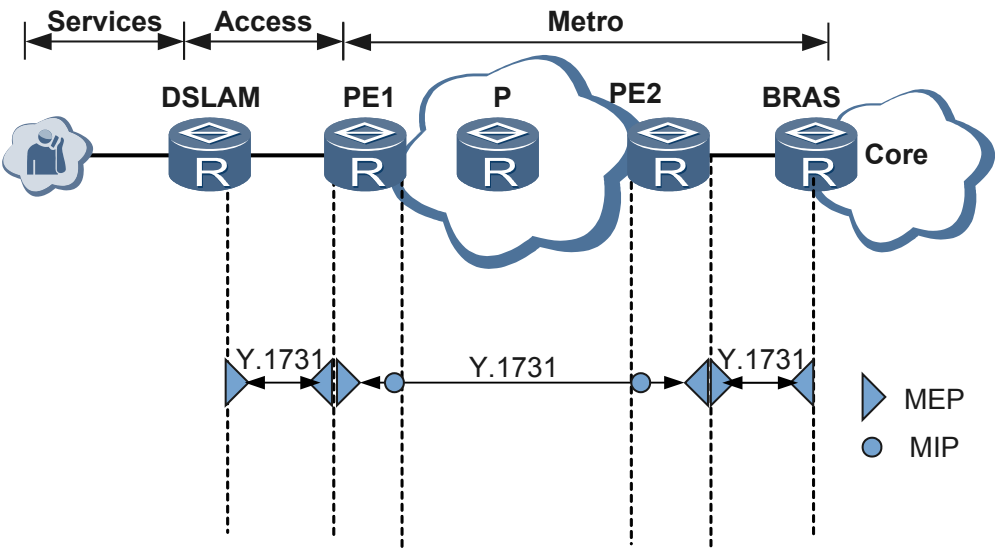
在配置 VLL 的单端丢包统计功能前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 9-5 所示，当用户认为购买的以太网隧道业务出现了服务质量问题，或者运营商对自己的网络进行例行的 SLA（Service level agreement）监测时，可以使用 Y.1731 所定义的性能测试工具对链路进行检测：

- 单端丢包统计
- 双端丢包统计
- 单向时延统计
- 双向时延统计

图 9-5 性能检测组网图



本章仅介绍运营商网络 PE 间通过 VLL 互联时 VLL 的 AC 侧和 PW 侧的单端丢包统计功能。

前置任务

在配置 VLL 的单端丢包统计之前，需完成以下任务：

- PW 侧单端丢包统计功能
 - 在 PE 两端设备上完成 VLL 相关配置
具体配置可参见《NE80E/40E 配置指南-VPN》中的 VLL 配置。
 - 完成 CFM 相关配置，并配置 MEP 类型为 inward 型。

数据准备

在配置 VLL 的单端丢包统计之前，需要准备以下数据。

序号	数据
1	MD、MA 的名称
2	MEP 的 ID、MEP 所在接口的名称、MEP 的类型
3	与 MA 绑定的 VLL 的 VC ID
4	报文的发送间隔和个数

9.2.2 配置 MA 与 VLL 绑定

配置 MA 与 VLL 绑定是配置 VLL 的单端丢包统计、双端丢包统计、单向时延统计、双向时延统计功能的首要步骤。

背景信息

基于 VLL 的性能统计功能是针对指定的 L2VC 的性能统计，因此在部署 Y.1731 的性能统计功能时，应当首先将 MA 与指定的 L2VC 进行绑定，然后再对 MA 进行性能统计，从而得出指定 PW 或者 AC 上的性能统计信息。

- 如果进行 PW 侧检测，请在 VLL 网络两端的 PE 上进行如下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **cfm md md-name**，进入 MD 视图。
- 步骤 3** 执行命令 **ma ma-name**，进入 MA 视图。
- 步骤 4** 执行命令 **map mpls l2vc vc-id { raw | tagged }**，配置 MA 与一条指定的 L2VC 进行绑定。



802.1ag 不支持 MA 关联备份 VC。

将接口设置为 **raw** 或 **tagged** 的类型，接口对报文的处理方式也不同。如表 9-2 和表 9-3 所示。

表 9-2 报文入接口处理

入接口类型	raw 封装方式（以太封装方式）	tagged 封装方式（VLAN 封装方式）
Dot1q 子接口	剥掉一层 Tag	不做处理，保留 Tag
Dot1q 终结子接口	剥掉一层 Tag	不做处理，保留 Tag
QinQ 终结子接口（对称方式）	剥掉外层 Tag	不处理，两层 Tag 都保留
QinQ 终结子接口（非对称方式）	两层 Tag 都剥掉	剥掉两层 Tag，再添加一层 Tag

表 9-3 报文出接口处理

出接口类型	raw 封装方式（以太封装方式）	tagged 封装方式（VLAN 封装方式）
Dot1q 子接口	添加一层 Tag	替换为出接口封装的 Tag
Dot1q 终结子接口	添加一层 Tag	替换为出接口封装的 Tag

出接口类型	raw 封装方式（以太封装方式）	tagged 封装方式（VLAN 封装方式）
QinQ 终结子接口（对称方式）	添加外层 Tag	替换外层 Tag 为出接口封装的 Tag
QinQ 终结子接口（非对称方式）	添加两层 Tag	剥掉外层 Tag，再添加出接口封装的两层 Tag

----结束

9.2.3 配置对端设备接收 LMM 报文功能

对链路进行单端丢包性能统计时，需要配置远端设备接收 LMM（Loss measurement message）报文功能。

背景信息

丢包统计功能是通过向其对等 MEP 发送带有 ETH-LM（Loss Measurement）信息的帧，并类似地从对等 MEP 接收带有 ETH-LM 信息的帧实现的。当对链路进行性能统计时，需要配置远端 MEP 设备接收 LMM 报文功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md md-name**，进入 MD 视图。

步骤 3 执行命令 **ma ma-name**，进入 MA 视图。

步骤 4 执行命令 **loss-measure single-ended receive [8021p { 8021p-value } &<1 - 3>]**，配置对端设备接收 LMM 报文功能。

 说明

如果指定参数 **8021p 8021p-value**，则接收端基于指定的优先级统计链路的丢包。如果不指定该参数，则接收端基于所有优先级统计链路的丢包。

----结束

9.2.4 使能 VLL 的单端丢包统计功能

VLL 的单端丢包统计包含按需单端丢包统计和连续单端丢包统计功能。

背景信息

按需的 OAM 是指有限的时间内为了诊断而由人工干预发起的 OAM 动作，可导致在诊断期间单次的或周期的 OAM 动作。连续的 OAM 是指连续、不间断发生的 OAM 动作。VLL 的单端丢包统计包含按需的单端丢包统计功能和连续的单端丢包统计功能。

- 当用户需要单次或者周期性的统计 PW 侧链路的丢包性能，可以通过 VLL 按需单端丢包统计功能实现。
- 当用户需要连续不间断统计 PW 侧链路的丢包性能，可以通过 VLL 连续单端丢包统计功能实现。

网络中的报文通常携带 802.1p 优先级以区分不同的业务，部署不同策略。如图 9-6 所示，经过 VLL 网络中 P 设备的流量携带的 802.1p 优先级分别为 1 和 2。

当对 PE1 和 PE2 之间的链路进行丢包率统计时，如果不参与丢包统计计算的流量（优先级为 2）在丢包使能后发出。但由于优先级较高，该流量会被优先转发，从而阻塞正常参与丢包统计计算的流量（优先级为 1）按时到达 PE2 设备，导致链路的丢包率统计不正确。

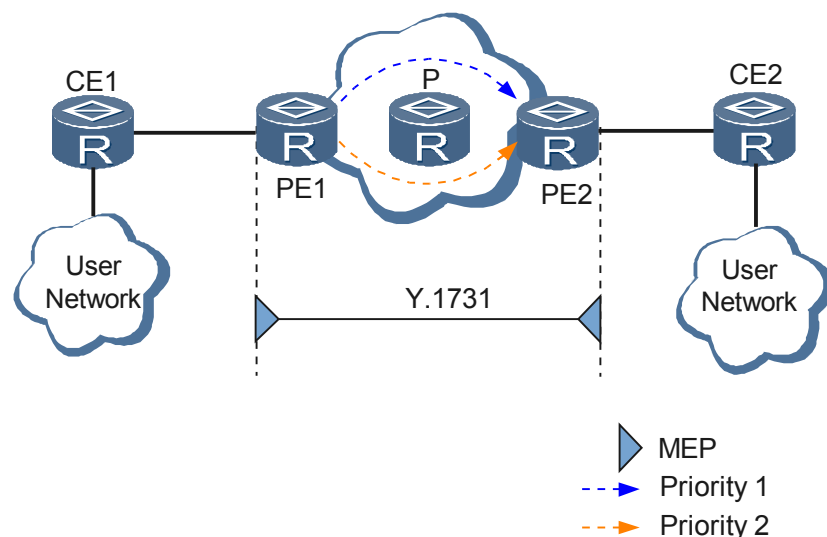
此时，可以配置基于 802.1p 优先级的 VLL 的单端丢包统计功能，实现更为精确的链路连续性丢包测试。

说明

当在对 PW 侧链路的丢包性能进行统计时，通过对 AC 侧报文携带的 802.1p 优先级进行映射，还可以实现更加灵活的链路连续性丢包测试。

- 在 PE 上通过配置 QoS 简单流分类优先级映射，可以将一种网络流量中的优先级映射到另外一种网络流量中，使流量在另外一种网络中按照原来的或用户配置的优先级传送。所有进入 PE 的报文，其原先的外部优先级标记将被映射为内部优先级（以 Diff-Serv 的服务等级和颜色表示）；PE 发出报文时，将内部优先级映射为某种外部业务优先级。
- 此时，可以配置基于 QoS 简单流分类优先级映射的 VLL 的单端丢包统计功能，通过在 PE 上设置不同的优先级映射关系，将报文的业务优先级进行更改或者重新分类，从而实现更加灵活的链路连续性丢包测试。

图 9-6 VLL 的基于优先级统计 Y.1731 功能组网图



操作步骤

- 按需求的单端丢包统计

说明

请在 PW 侧链路单端丢包统计的发起设备上进行如下配置。

– PW 侧按需单端丢包统计

- 执行命令 **system-view**，进入系统视图。
- 执行命令 **cfm md md-name**，进入 MD 视图。
- 执行命令 **ma ma-name**，进入 MA 视图。
- 执行命令 **loss-measure single-ended mep mep-id mep-id [mac mac-address | remote-mep mep-id mep-id] interval { 1000 | 10000 } count count-value**，使能 PW 侧的按需单端丢包统计功能。



说明

- 如果本端 MEP 没有学到远端 MEP 的 MAC 地址, 则必须使用指定目的 MAC 的方式进行丢包统计。
- 如果本端 MEP 已经学到远端 MEP 的 MAC 地址或 RMEP 已经绑定了对端 MAC, 则可以使用指定目的远端 MEP 号的方式进行丢包统计。

- 连续的单端丢包统计



说明

连续的单端丢包统计功能仅针对 PW 侧链路进行统计, 请在 PW 侧单端丢包发起设备上进行如下配置。

1. 执行命令 **system-view**, 进入系统视图。
2. 执行命令 **cfm md md-name**, 进入 MD 视图。
3. 执行命令 **ma ma-name**, 进入 MA 视图。
4. 执行命令 **loss-measure single-ended continual mep mep-id mep-id [mac mac-address | remote-mep mep-id mep-id] interval 30000 [8021p { 8021p-value } &<1 - 3>]**, 使能 PW 侧的连续单端丢包统计功能。

如果指定参数 **8021p 8021p-value**, 则基于指定 **8021p-value** 优先级的报文进行 PW 链路的丢包统计。如果不指定该参数, 则基于所有优先级的报文进行 PW 链路的丢包统计。



说明

- 如果本端 MEP 没有学到远端 MEP 的 MAC 地址, 则必须使用指定目的 MAC 的方式进行丢包统计。
- 如果本端 MEP 已经学到远端 MEP 的 MAC 地址或 RMEP 已经绑定了对端 MAC, 则可以使用指定目的远端 MEP 号的方式进行丢包统计。

----结束

9.2.5 检查配置结果

VLL 的单端丢包统计功能配置成功后, 可以查看到 VLL 的单端丢包统计信息。

前提条件

已经完成 VLL 的单端丢包统计功能的所有配置。

操作步骤

- 使用 **display y1731 statistic-type single-loss md md-name ma ma-name [8021p { 8021p-value } &<1 - 3>] [count count-value]** 命令查看 Y.1731 的性能统计数据。



说明

目前, VLL 的单端丢包统计功能支持通过与当前设备版本配套的网管系统来查看配置结果。

----结束

任务示例

执行 **display y1731 statistic-type** 命令, 可以看到单端丢包率的统计信息。

```
<HUAWEI> display Y.1731 statistic-type single-loss md md1 ma ma1
Latest single-ended loss statistics:
Index Local-loss ratio Remote-loss ratio
1      20          50.0000% 30          75.0000%
2      20          50.0000% 30          75.0000%
```

3	20	50.0000%	30	75.0000%
4	20	50.0000%	30	75.0000%
5	20	50.0000%	30	75.0000%
6	20	50.0000%	30	75.0000%
7	20	50.0000%	30	75.0000%
8	20	50.0000%	30	75.0000%
9	20	50.0000%	30	75.0000%
10	20	50.0000%	30	75.0000%
11	20	50.0000%	30	75.0000%
12	20	50.0000%	30	75.0000%
13	20	50.0000%	30	75.0000%
14	20	50.0000%	30	75.0000%
<HUAWEI> display y1731 statistic-type single-loss md md1 ma mal 8021p 1 2				
Latest single-ended loss statistics of 802.1p 1:				
Index	Local-loss	ratio	Remote-loss	ratio
1	20	50.0000%	30	75.0000%
2	20	50.0000%	30	75.0000%
3	20	50.0000%	30	75.0000%
4	20	50.0000%	30	75.0000%
5	20	50.0000%	30	75.0000%
6	20	50.0000%	30	75.0000%
7	20	50.0000%	30	75.0000%
8	20	50.0000%	30	75.0000%
9	20	50.0000%	30	75.0000%
10	20	50.0000%	30	75.0000%
11	20	50.0000%	30	75.0000%
12	20	50.0000%	30	75.0000%
13	20	50.0000%	30	75.0000%
14	20	50.0000%	30	75.0000%
15	20	50.0000%	30	75.0000%
16	20	50.0000%	30	75.0000%
17	20	50.0000%	30	75.0000%
18	20	50.0000%	30	75.0000%
19	20	50.0000%	30	75.0000%
20	20	50.0000%	30	75.0000%
21	20	50.0000%	30	75.0000%
22	20	50.0000%	30	75.0000%
23	20	50.0000%	30	75.0000%
24	20	50.0000%	30	75.0000%
25	20	50.0000%	30	75.0000%
26	20	50.0000%	30	75.0000%
27	20	50.0000%	30	75.0000%
28	20	50.0000%	30	75.0000%
29	20	50.0000%	30	75.0000%
30	20	50.0000%	30	75.0000%
Latest single-ended loss statistics of 8021p 2:				
Index	Local-loss	ratio	Remote-loss	ratio
1	20	50.0000%	30	75.0000%
2	20	50.0000%	30	75.0000%
3	20	50.0000%	30	75.0000%
4	20	50.0000%	30	75.0000%
5	20	50.0000%	30	75.0000%
6	20	50.0000%	30	75.0000%
7	20	50.0000%	30	75.0000%
8	20	50.0000%	30	75.0000%
9	20	50.0000%	30	75.0000%
10	20	50.0000%	30	75.0000%
11	20	50.0000%	30	75.0000%
12	20	50.0000%	30	75.0000%
13	20	50.0000%	30	75.0000%
14	20	50.0000%	30	75.0000%
15	20	50.0000%	30	75.0000%
16	20	50.0000%	30	75.0000%
17	20	50.0000%	30	75.0000%
18	20	50.0000%	30	75.0000%
19	20	50.0000%	30	75.0000%
20	20	50.0000%	30	75.0000%
21	20	50.0000%	30	75.0000%
22	20	50.0000%	30	75.0000%

23	20	50.0000%	30	75.0000%
24	20	50.0000%	30	75.0000%
25	20	50.0000%	30	75.0000%
26	20	50.0000%	30	75.0000%
27	20	50.0000%	30	75.0000%
28	20	50.0000%	30	75.0000%
29	20	50.0000%	30	75.0000%
30	20	50.0000%	30	75.0000%

9.3 配置 VLL 的双端丢包统计功能

组网环境为 VLL，需要同时检测链路连通性和丢包情况且对等 MEP 间均支持 CC（连通性检测）功能时，可以配置 VLL 的双端丢包统计功能。

9.3.1 建立配置任务

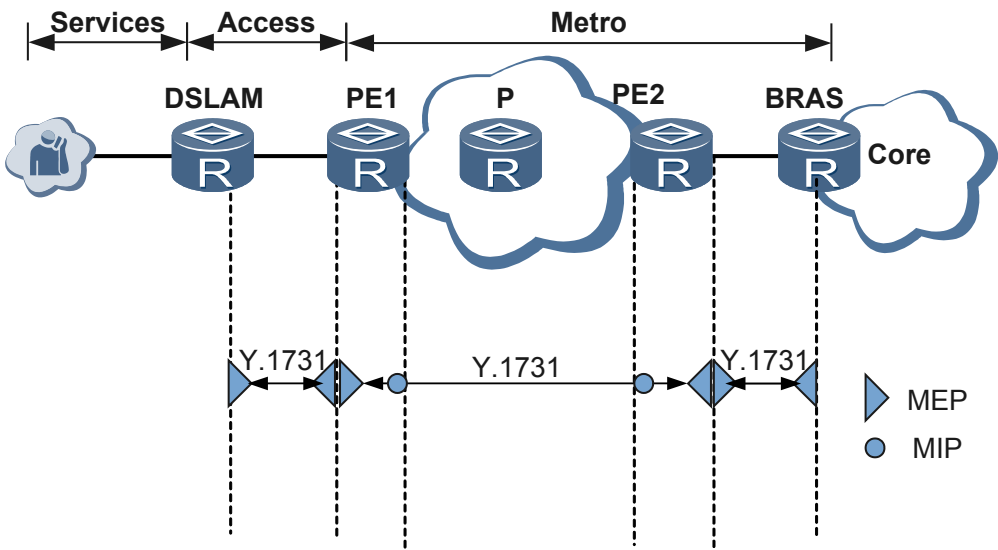
在配置 VLL 的双端丢包统计功能前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 9-7 所示，当用户认为购买的以太网隧道业务出现了服务质量问题，或者运营商对自己的网络进行例行的 SLA（Service level agreement）监测时，可以使用 Y.1731 所定义的性能测试工具对链路进行检测：

- 单端丢包统计
- 双端丢包统计
- 单向时延统计
- 双向时延统计

图 9-7 性能检测组网图



本章仅介绍运营商网络 PE 之间通过 VLL 互联时 VLL 的 PW 侧双端丢包统计功能。

前置任务

在配置 VLL 的双丢包统计之前，需完成以下任务：

- PW 侧双端丢包统计功能
 - 完成 VLL 相关配置。
具体配置可参见《NE80E/40E 配置指南-VPN》中的 VLL 配置。
 - 完成 CFM 相关配置，并配置 MEP 类型为 inward 型。

数据准备

在配置 VLL 的双端丢包统计之前，需要准备以下数据。

序号	数据
1	MD、MA 的名称
2	MEP 的 ID、MEP 所在接口的名称、MEP 的类型
3	RMEP 的 ID、RMEP 所在接口的 MAC 地址
4	MA 内 MEP 发送 CCM 消息的时间间隔
5	与 MA 绑定的 VLL 的 VC ID

9.3.2 配置 MA 与 VLL 绑定

配置 MA 与 VLL 绑定是配置 VLL 的单端丢包统计、双端丢包统计、单向时延统计、双向时延统计功能的首要步骤。

背景信息

基于 VLL 的性能统计功能是针对指定的 L2VC 的性能统计，因此在部署 Y.1731 的性能统计功能时，应当首先将 MA 与指定的 L2VC 进行绑定，然后再对 MA 进行性能统计，从而得出指定 PW 或者 AC 上的性能统计信息。

- 如果进行 PW 侧检测，请在 VLL 网络两端的 PE 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md md-name**，进入 MD 视图。

步骤 3 执行命令 **ma ma-name**，进入 MA 视图。

步骤 4 执行命令 **map mpls l2vc vc-id { raw | tagged }**，配置 MA 与一条指定的 L2VC 进行绑定。

 说明

802.1ag 不支持 MA 关联备份 VC。

将接口设置为 **raw** 或 **tagged** 的类型，接口对报文的处理方式也不同。如表 9-4 和表 9-5 所示。

表 9-4 报文入接口处理

入接口类型	raw 封装方式（以太封装方式）	tagged 封装方式（VLAN 封装方式）
Dot1q 子接口	剥掉一层 Tag	不做处理，保留 Tag
Dot1q 终结子接口	剥掉一层 Tag	不做处理，保留 Tag
QinQ 终结子接口（对称方式）	剥掉外层 Tag	不处理，两层 Tag 都保留
QinQ 终结子接口（非对称方式）	两层 Tag 都剥掉	剥掉两层 Tag，再添加一层 Tag

表 9-5 报文出接口处理

出接口类型	raw 封装方式（以太封装方式）	tagged 封装方式（VLAN 封装方式）
Dot1q 子接口	添加一层 Tag	替换为出接口封装的 Tag
Dot1q 终结子接口	添加一层 Tag	替换为出接口封装的 Tag
QinQ 终结子接口（对称方式）	添加外层 Tag	替换外层 Tag 为出接口封装的 Tag
QinQ 终结子接口（非对称方式）	添加两层 Tag	剥掉外层 Tag，再添加出接口封装的两层 Tag

----结束

9.3.3 使能 VLL 的双端丢包统计功能

VLL 的双端丢包统计功能在对等 MEP 的两台设备上网络丢包的测量，同时提供链路连通性检测。

背景信息

连续的 OAM 为连续、不间断的 OAM 动作。VLL 的双端丢包功能为连续的 OAM。

请根据检测需要（PW 检测）对如下配置进行选取：

- 进行 PW 侧检测时，请在对等 MEP 的两端 PE 上进行如下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **cfm md md-name**，进入 MD 视图。
- 步骤 3** 执行命令 **ma ma-name**，进入 MA 视图。
- 步骤 4** 执行命令 **loss-measure dual-ended continual mep mep-id mep-id remote-mep mep-id mep-id**，使能 VLL 的双端丢包统计功能。

VLL 的双端丢包统计是在端到端 MEP 之间进行，设备通过发送、接收 CCM 报文中携带的计数字段来进行计算。进行双端丢包统计时，需要确保 RMEP 的状态处于 Up，VLL 的双端丢包统计功能才能执行成功。

----结束

9.3.4 检查配置结果

VLL 的双端丢包统计功能配置成功后，可以查看到 VLL 的双端丢包统计信息。

前提条件

已经完成 VLL 的双端丢包统计功能的所有配置。

操作步骤

- 使用 **display y1731 statistic-type dual-loss md md-name ma ma-name [count count-value]** 命令查看 Y.1731 的性能统计数据。



目前，VLL 的双端丢包统计功能支持通过与当前设备版本配套的网管系统来查看配置结果。

----结束

任务示例

执行 **display y1731 statistic-type** 命令，可以看到双端丢包率的统计信息。

```
<HUAWEI> display y1731 statistic-type dual-loss md md1 ma ma1
Latest dual-ended loss statistics:
Index  Local-loss  ratio  Remote-loss  ratio
1      4294967295  100.0000%  4294967295  100.0000%
2      4294967295  100.0000%  4294967295  100.0000%
3      4294967295  100.0000%  4294967295  100.0000%
4      4294967295  100.0000%  4294967295  100.0000%
5      4294967295  100.0000%  4294967295  100.0000%
6      4294967295  100.0000%  4294967295  100.0000%
7      4294967295  100.0000%  4294967295  100.0000%
8      4294967295  100.0000%  4294967295  100.0000%
9      4294967295  100.0000%  4294967295  100.0000%
10     4294967295  100.0000%  4294967295  100.0000%
11     4294967295  100.0000%  4294967295  100.0000%
```

9.4 配置 VLL 的单向时延统计功能

VLL 组网环境下，需要测量链路单方向的网络时延时，可以配置 VLL 的单向时延统计功能。

9.4.1 建立配置任务

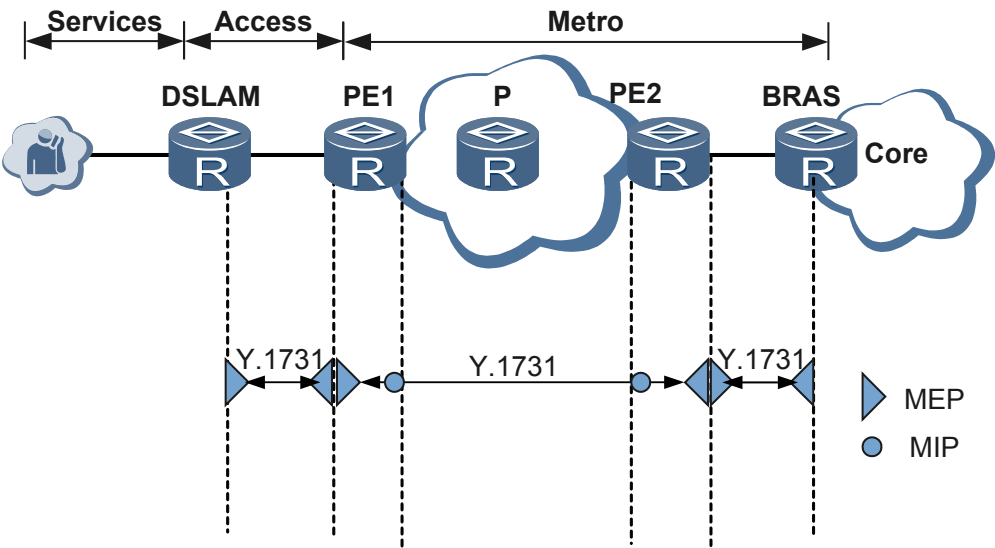
在配置 VLL 的单向时延统计功能前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 9-8 所示，当用户认为购买的以太网隧道业务出现了服务质量问题，或者运营商对自己的网络进行例行的 SLA（Service level agreement）监测时，可以使用 Y.1731 所定义的性能测试工具对链路进行检测：

- 单端丢包统计
- 双端丢包统计
- 单向时延统计
- 双向时延统计

图 9-8 性能检测组网图



本章仅介绍 PE 之间通过 VLL 互联时 VLL 的 PW 侧单向时延统计功能。

前置任务

在配置 VLL 的单向时延统计功能之前，需完成以下任务：

- PW 侧单向时延统计功能
 - 完成 VLL 相关配置。
具体配置可参见《NE80E/40E 配置指南-VPN》中的 VLL 配置。
 - 完成 CFM 相关配置，并配置 MEP 类型为 inward 型。

数据准备

在配置 VLL 的单向时延统计功能之前，需要准备以下数据。

序号	数据
1	MD、MA 的名称
2	MEP 的 ID、MEP 所在接口的名称、MEP 的类型
3	与 MA 绑定的 VLL 的 VC ID
4	RMEP 的 ID、RMEP 所在接口的 MAC 地址
5	MA 内 MEP 发送 CCM 消息的时间间隔

9.4.2 配置 MA 与 VLL 绑定

配置 MA 与 VLL 绑定是配置 VLL 的单端丢包统计、双端丢包统计、单向时延统计、双向时延统计功能的首要步骤。

背景信息

基于 VLL 的性能统计功能是针对指定的 L2VC 的性能统计，因此在部署 Y.1731 的性能统计功能时，应当首先将 MA 与指定的 L2VC 进行绑定，然后再对 MA 进行性能统计，从而得出指定 PW 或者 AC 上的性能统计信息。

- 如果进行 PW 侧检测，请在 VLL 网络两端的 PE 上进行如下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **cfm md md-name**，进入 MD 视图。
- 步骤 3** 执行命令 **ma ma-name**，进入 MA 视图。
- 步骤 4** 执行命令 **map mpls l2vc vc-id { raw | tagged }**，配置 MA 与一条指定的 L2VC 进行绑定。



说明

802.1ag 不支持 MA 关联备份 VC。

将接口设置为 **raw** 或 **tagged** 的类型，接口对报文的处理方式也不同。如表 9-6 和表 9-7 所示。

表 9-6 报文入接口处理

入接口类型	raw 封装方式（以太封装方式）	tagged 封装方式（VLAN 封装方式）
Dot1q 子接口	剥掉一层 Tag	不做处理，保留 Tag
Dot1q 终结子接口	剥掉一层 Tag	不做处理，保留 Tag
QinQ 终结子接口（对称方式）	剥掉外层 Tag	不处理，两层 Tag 都保留
QinQ 终结子接口（非对称方式）	两层 Tag 都剥掉	剥掉两层 Tag，再添加一层 Tag

表 9-7 报文出接口处理

出接口类型	raw 封装方式（以太封装方式）	tagged 封装方式（VLAN 封装方式）
Dot1q 子接口	添加一层 Tag	替换为出接口封装的 Tag
Dot1q 终结子接口	添加一层 Tag	替换为出接口封装的 Tag

出接口类型	raw 封装方式（以太封装方式）	tagged 封装方式（VLAN 封装方式）
QinQ 终结子接口（对称方式）	添加外层 Tag	替换外层 Tag 为出接口封装的 Tag
QinQ 终结子接口（非对称方式）	添加两层 Tag	剥掉外层 Tag，再添加出接口封装的两层 Tag

----结束

9.4.3 配置对端设备接收 DM 报文功能

单向时延统计时，需要在对端设备上配置接收 DM 报文功能。

背景信息

- PW 侧检测时，请在远端 MEP 的 PE 设备上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cfm md md-name**，进入 MD 视图。

步骤 3 执行命令 **ma ma-name**，进入 MA 视图。

步骤 4 根据统计方式进行如下配置：

- 如果进行 PW 侧连续统计时，执行命令 **delay-measure one-way continual receive [8021p { 8021p-value } &<1 - 3>]**，配置对端设备接收 DM 报文功能。

 说明

如果指定参数 **8021p 8021p-value**，则接收端基于指定的优先级统计链路的时延。如果不指定该参数，则接收端基于所有优先级统计链路的时延。

- 如果进行 PW 侧按需统计时，执行命令 **delay-measure one-way receive**，配置对端设备接收 DM 报文功能。

----结束

9.4.4 使能 VLL 的单向时延统计功能

VLL 可以实现点到点的 VPN 组网。为了精确的统计一条 VLL PW 链路的单向时延，可以配置 VLL 的单向时延统计功能。

背景信息

按需的 OAM 是指有限的时间内为了诊断而由人工干预发起的 OAM 动作，可导致在诊断期间单次的或周期的 OAM 动作。连续的 OAM 是指连续、不间断发生的 OAM 动作。VLL 的单向时延统计包含按需的单向时延统计功能和连续的单向时延统计功能。

- 当用户需要单次或者周期性的统计 PW 侧链路的时延性能，可以通过 VLL 按需单向时延统计功能实现。
- 当用户需要连续不间断统计 PW 侧链路的时延性能，可以通过 VLL 连续单向时延统计功能实现。

网络中的报文通常携带 802.1p 优先级以区分不同的业务，部署不同策略。如图 9-9 所示，经过 VLL 网络中 P 设备的流量携带的 802.1p 优先级分别为 1 和 2。

当对 PE1 和 PE2 之间的链路进行单向时延统计时，如果不参与时延统计计算（优先级为 2）的流量在单向时延使能后发出。由于优先级较高，该流量会被优先转发，从而阻塞正常参与时延统计计算（优先级为 1）的流量按时到达 PE2 设备，导致链路的时延统计不正确。

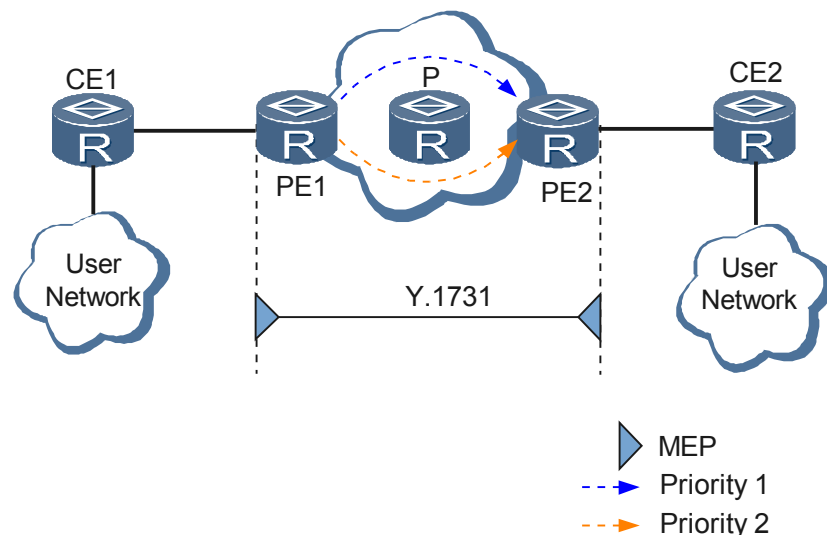
此时，可以配置基于 802.1p 优先级的 VLL 的连续单向时延统计功能，实现更为精确的链路连续性时延测试。

说明

当在对 PW 侧链路的时延性能进行统计时，通过对 AC 侧报文携带的 802.1p 优先级进行映射，还可以实现更加灵活的链路连续性时延测试。

- 在 PE 上通过配置 QoS 简单流分类优先级映射，可以将一种网络流量中的优先级映射到另外一种网络流量中，使流量在另外一种网络中按照原来的或用户配置的优先级传送。所有进入 PE 的报文，其原先的外部优先级标记将被映射为内部优先级（以 Diff-Serv 的服务等级和颜色表示）；PE 发出报文时，将内部优先级映射为某种外部业务优先级。
- 此时，可以配置基于 QoS 简单流分类优先级映射的 VLL 的单端时延统计功能，通过在 PE 上设置不同的优先级映射关系，将报文的业务优先级进行更改或者重新分类，从而实现更加灵活的链路连续性时延测试。

图 9-9 VLL 的基于优先级统计 Y.1731 功能组网图



操作步骤

- 按需求的单向时延统计

说明

请在 PW 侧链路时延统计的发起设备上进行如下配置。

– PW 侧按需单向时延统计

- 执行命令 **system-view**，进入系统视图。
- 执行命令 **cfm md md-name**，进入 MD 视图。
- 执行命令 **ma ma-name**，进入 MA 视图。
- 执行命令 **delay-measure one-way mep mep-id mep-id { mac mac-address | remote-mep mep-id mep-id } interval { 1000 | 10000 } count count-value**，使能 PW 侧的按需单向时延统计功能。

如果本端 MEP 没有学到远端 MEP 的 MAC 地址, 则必须使用指定目的 MAC 的方式进行时延统计。

如果本端 MEP 已经学到远端 MEP 的 MAC 地址或 RMEP 已经绑定了对端 MAC, 则可以使用指定目的远端 MEP 号的方式进行时延统计。

- 连续的单向时延统计

 说明

连续的单向时延统计功能仅针对 PW 侧链路进行统计, 请在 PW 侧单向时延发起设备上进行如下配置。

1. 执行命令 **system-view**, 进入系统视图。
2. 执行命令 **cfm md md-name**, 进入 MD 视图。
3. 执行命令 **ma ma-name**, 进入 MA 视图。
4. 执行命令 **delay-measure one-way continual mep-id mep-id { mac mac-address | remote-mep mep-id mep-id } interval 1000 [8021p { 8021p-value } &<1 - 3>]**, 使能 PW 侧的连续单向时延统计功能。

如果指定参数 **8021p 8021p-value**, 则基于指定 **8021p-value** 优先级的报文进行 PW 链路的时延统计。如果不指定该参数, 则基于所有优先级的报文进行 PW 链路的时延统计。

如果本端 MEP 没有学到远端 MEP 的 MAC 地址, 则必须使用指定目的 MAC 的方式进行时延统计。

如果本端 MEP 已经学到远端 MEP 的 MAC 地址或 RMEP 已经绑定了对端 MAC, 则可以使用指定目的远端 MEP 号的方式进行时延统计。

----结束

9.4.5 检查配置结果

VLL 的单向时延统计功能配置成功后, 可以查看到单向时延统计信息。

前提条件

已经完成 VLL 的单向时延统计功能的所有配置。

操作步骤

- 使用 **display y1731 statistic-type oneway-delay md md-name ma ma-name [8021p { 8021p-value } &<1 - 3>] [count value]** 命令查看 Y.1731 的性能统计信息。

 说明

目前, VLL 的单端丢包统计功能支持通过与当前设备版本配套的网管系统来查看配置结果。

----结束

任务示例

配置成功后, 在 MEP 所在的设备上执行 **display y1731 statistic-type** 命令, 可以看到时延值和时延抖动值。

```
<HUAWEI> display y1731 statistic-type oneway-delay md mdl ma ma1
Latest one-way delay statistics:
Index  One-way delay(usec) Delay variation(usec)
1      20000              0
2      20000              0
3      20000              0
```

```
4      30000      10000
5      10000      20000
6      10000      0
7      10000      0
8      10000      0
9      20000      10000
10     20000      0
<HUAWEI>display y1731 statistic-type oneway-delay md md1 ma ma1 8021p 1 2
Latest one-way delay statistics of 802.1p 1:
Index  One-way delay(usec) Delay variation(usec)
1      0                  0
2      0                  0
3      20000             20000
4      10000             10000
5      20000             10000
6      10000             10000
7      20000             10000
8      10000             10000
9      20000             10000
10     10000             10000
11     20000             10000
-----
Latest one-way delay statistics of 8021p 2:
Index  One-way delay(usec) Delay variation(usec)
1      20000             0
2      10000             10000
3      10000             0
4      20000             10000
5      10000             10000
6      20000             10000
7      10000             10000
8      20000             10000
9      10000             10000
10     20000             10000
11     10000             10000
```

9.5 配置 VLL 的双向时延统计功能

VLL 组网环境下，需要统计链路时延功能且对等体 MEP 时钟不同步、对链路时延统计要求不高的情况下，可以采用双向时延统计功能。

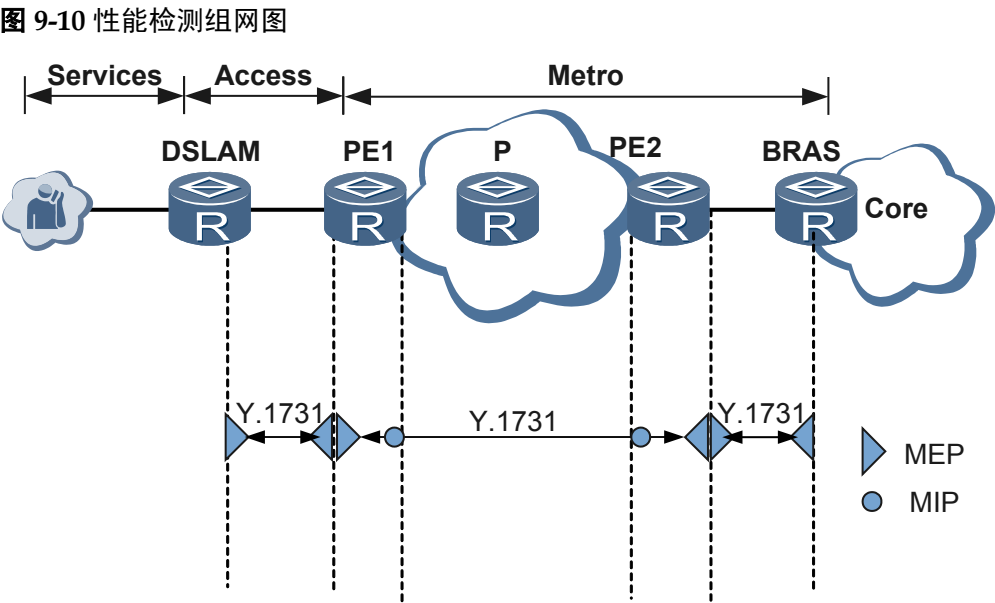
9.5.1 建立配置任务

在配置 VLL 的双向时延统计功能前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 9-10 所示，当用户认为购买的以太网隧道业务出现了服务质量问题，或者运营商对自己的网络进行例行的 SLA（Service level agreement）监测时，可以使用 Y.1731 所定义的性能测试工具对链路进行检测：

- 单端丢包统计
- 双端丢包统计
- 单向时延统计
- 双向时延统计



本章仅介绍 PE 之间通过 VLL 互联时 VLL 的 PW 侧双向时延统计功能。

前置任务

在配置 VLL 的双向时延统计功能之前，需完成以下任务：

- PW 侧双向时延统计功能
 - 完成 VLL 相关配置。
具体配置可参见《NE80E/40E 配置指南-VPN》中的 VLL 配置。
 - 完成 CFM 相关配置，并配置 MEP 类型为 inward 型。

数据准备

在配置 VLL 的双向时延统计功能之前，需要准备以下数据。

序号	数据
1	MD、MA 的名称
2	MEP 的 ID、MEP 所在接口的名称、MEP 的类型
3	与 MA 绑定的 VLL 的 VC ID
4	RMEP 的 ID、RMEP 所在接口的 MAC 地址
5	MA 内 MEP 发送 CCM 消息的时间间隔

9.5.2 配置 MA 与 VLL 绑定

配置 MA 与 VLL 绑定是配置 VLL 的单端丢包统计、双端丢包统计、单向时延统计、双向时延统计功能的首要步骤。

背景信息

基于 VLL 的性能统计功能是针对指定的 L2VC 的性能统计，因此在部署 Y.1731 的性能统计功能时，应当首先将 MA 与指定的 L2VC 进行绑定，然后再对 MA 进行性能统计，从而得出指定 PW 或者 AC 上的性能统计信息。

- 如果进行 PW 侧检测，请在 VLL 网络两端的 PE 上进行如下配置。

操作步骤

- 步骤 1 执行命令 **system-view**，进入系统视图。
- 步骤 2 执行命令 **cfm md md-name**，进入 MD 视图。
- 步骤 3 执行命令 **ma ma-name**，进入 MA 视图。
- 步骤 4 执行命令 **map mpls l2vc vc-id { raw | tagged }**，配置 MA 与一条指定的 L2VC 进行绑定。

 说明

802.1ag 不支持 MA 关联备份 VC。

将接口设置为 **raw** 或 **tagged** 的类型，接口对报文的处理方式也不同。如表 9-8 和表 9-9 所示。

表 9-8 报文入接口处理

入接口类型	raw 封装方式（以太封装方式）	tagged 封装方式（VLAN 封装方式）
Dot1q 子接口	剥掉一层 Tag	不做处理，保留 Tag
Dot1q 终结子接口	剥掉一层 Tag	不做处理，保留 Tag
QinQ 终结子接口（对称方式）	剥掉外层 Tag	不处理，两层 Tag 都保留
QinQ 终结子接口（非对称方式）	两层 Tag 都剥掉	剥掉两层 Tag，再添加一层 Tag

表 9-9 报文出接口处理

出接口类型	raw 封装方式（以太封装方式）	tagged 封装方式（VLAN 封装方式）
Dot1q 子接口	添加一层 Tag	替换为出接口封装的 Tag
Dot1q 终结子接口	添加一层 Tag	替换为出接口封装的 Tag
QinQ 终结子接口（对称方式）	添加外层 Tag	替换外层 Tag 为出接口封装的 Tag
QinQ 终结子接口（非对称方式）	添加两层 Tag	剥掉外层 Tag，再添加出接口封装的两层 Tag

----结束

9.5.3 配置对端设备接收 DMM 报文功能

只有使能对端设备接收 DMM 报文，双向时延统计才有可能正常工作。

背景信息

请在 RMEP 所在的设备上进行以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **cfm md md-name**，进入 MD 视图。
- 步骤 3** 执行命令 **ma ma-name**，进入 MA 视图。
- 步骤 4** 执行命令 **delay-measure two-way receive [8021p { 8021p-value } &<1 - 3>]**，配置对端设备接收 DMM 报文功能。

 说明

如果指定参数 8021p 8021p-value，则接收端基于指定的优先级统计链路的时延。如果不指定该参数，则接收端基于所有优先级统计链路的时延。

----结束

9.5.4 使能 VLL 的双向时延统计功能

VLL 可以实现点到点的 VPN 组网。为了精确的统计一条 VLL PW 或者 AC 链路的双向时延，可以配置 VLL 的双向时延统计功能。

背景信息

按需的 OAM 是指有限的时间内为了诊断而由人工干预发起的 OAM 动作，可导致在诊断期间单次的或周期的 OAM 动作。连续的 OAM 是指连续、不间断发生的 OAM 动作。VLL 的双向时延统计包含按需的双向时延统计功能和连续的双向时延统计功能。

- 当用户需要单次或者周期性的统计 PW 侧或者 AC 侧链路的时延性能，可以通过 VLL 按需双向时延统计功能实现。
- 当用户需要连续不间断统计 PW 侧链路的时延性能，可以通过 VLL 连续双向时延统计功能实现。

网络中的报文通常携带 802.1p 优先级以区分不同的业务，部署不同策略。如图 9-11 所示，经过 P 设备的流量携带的 802.1p 优先级分别为 1 和 2。

当对 PE1 和 PE2 之间的链路进行双向时延率统计时，如果不参与时延统计计算（优先级为 2）的流量在时延使能后发出。由于优先级较高，该流量会被优先转发，从而阻塞正常参与时延统计计算（优先级为 1）的流量按时到达 PE2 设备，导致链路的时延率统计不正确。

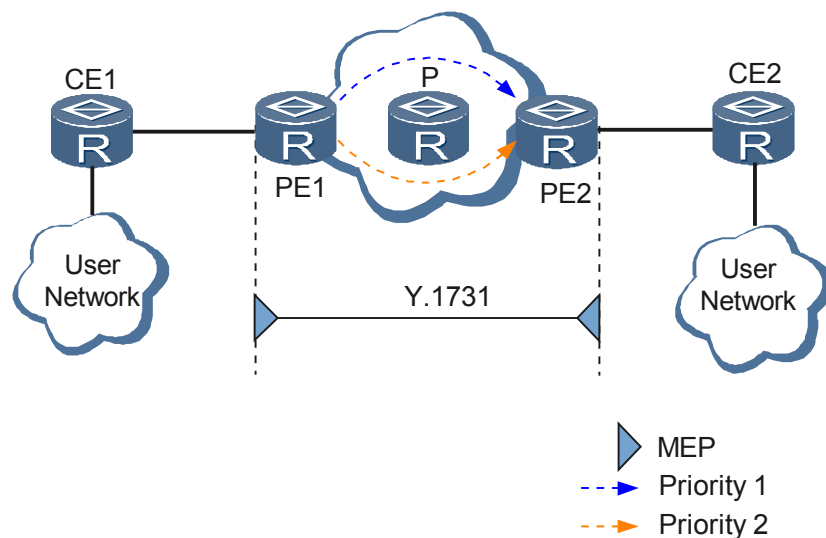
此时，可以配置基于 802.1p 优先级的 VLL 的双向时延统计功能，实现更为精确的链路连续性时延测试。

说明

当在对 PW 侧链路的时延性能进行统计时，通过对 AC 侧报文携带的 802.1p 优先级进行映射，还可以实现更加灵活的链路连续性时延测试。

- 在 PE 上通过配置 QoS 简单流分类优先级映射，可以将一种网络流量中的优先级映射到另外一种网络流量中，使流量在另外一种网络中按照原来的或用户配置的优先级传送。所有进入 PE 的报文，其原先的外部优先级标记将被映射为内部优先级（以 Diff-Serv 的服务等级和颜色表示）；PE 发出报文时，将内部优先级映射为某种外部业务优先级。
- 此时，可以配置基于 QoS 简单流分类优先级映射的 VLL 的单端时延统计功能，通过在 PE 上设置不同的优先级映射关系，将报文的业务优先级进行更改或者重新分类，从而实现更加灵活的链路连续性时延测试。

图 9-11 VLL 的基于优先级统计 Y.1731 功能组网图



操作步骤

- 按需的双向时延统计

说明

请在 PW 侧链路时延统计的发起设备上进行如下配置。

- PW 侧按需双向时延统计

- 执行命令 **system-view**，进入系统视图。
- 执行命令 **cfm md md-name**，进入 MD 视图。
- 执行命令 **ma ma-name**，进入 MA 视图。
- 执行命令 **delay-measure two-way mep mep-id mep-id { mac mac-address | remote-mep mep-id mep-id } interval { 1000 | 10000 } count count-value**，使能 PW 侧的按需双向时延统计功能。

如果本端 MEP 没有学到远端 MEP 的 MAC 地址，则必须使用指定目的 MAC 的方式进行时延统计。

如果本端 MEP 已经学到远端 MEP 的 MAC 地址或 RMEP 已经绑定了对端 MAC，则可以使用指定目的远端 MEP 号的方式进行时延统计。

- 连续的双向时延统计

说明

连续的双向时延统计功能仅针对 PW 侧链路进行统计，请在 PW 侧双向时延发起设备上如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cfm md md-name**，进入 MD 视图。
3. 执行命令 **ma ma-name**，进入 MA 视图。
4. 执行命令 **delay-measure two-way continual mep mep-id mep-id { mac mac-address | remote-mep mep-id mep-id } interval 30000 [8021p { 8021p-value } &<1 - 3>]**，使能 PW 侧的连续双向时延统计功能。

如果指定参数 **8021p 8021p-value**，则基于指定 **8021p-value** 优先级的报文进行 PW 链路的时延统计。如果不指定该参数，则基于所有优先级的报文进行 PW 链路的时延统计。

如果本端 MEP 没有学到远端 MEP 的 MAC 地址，则必须使用指定目的 MAC 的方式进行时延统计。

如果本端 MEP 已经学到远端 MEP 的 MAC 地址或 RMEP 已经绑定了对端 MAC，则可以使用指定目的远端 MEP 号的方式进行时延统计。

----结束

9.5.5 检查配置结果

VLL 的双向时延统计功能配置成功后，可以查看到双向时延统计信息。

前提条件

已经完成 VLL 的双向时延统计功能的所有配置。

操作步骤

- 使用 **display y1731 statistic-type twoway-delay md md-name ma ma-name [8021p { 8021p-value } &<1 - 3>] [count value]** 命令查看 Y.1731 的性能统计信息。



说明

目前，VLL 的双向时延统计功能支持通过与当前设备版本配套的网管系统来查看配置结果。

----结束

任务示例

配置成功后，在双向时延发起设备上执行 **display y1731 statistic-type** 命令，可以看到时延值和时延抖动值。

```
<HUAWEI>display y1731 statistic-type twoway-delay md md1 ma ma1 8021p 2 3
Latest one-way delay statistics of 8021p 2:
Index  Two-way delay(usec)  Delay variation(usec)
1      0                   0
2      0                   0
3      0                   0
4      0                   0
-----
Latest one-way delay statistics of 8021p 3:
Index  Two-way delay(usec)  Delay variation(usec)
1      0                   0
2      0                   0
3      0                   0
4      0                   0
<HUAWEI> display y1731 statistic-type twoway-delay md md1 ma ma1
Two-way delay measurement statistics:
Index  Two-way delay(usec)  Delay variation(usec)
1      20000              0
2      20000              0
```

3	10000	10000
4	20000	10000
5	10000	10000
6	20000	10000
7	10000	10000
8	10000	10000
9	20000	10000
10	10000	10000
11	20000	10000
12	20000	0
13	20000	0
14	30000	10000
15	20000	10000
16	20000	0

9.6 配置 VPLS 的单端丢包统计功能

VPLS 组网下，需要对链路丢包性能进行统计且对等 MEP 不支持或一方不支持 CC 功能时，可以配置 VPLS 的单端丢包统计功能。

9.6.1 建立配置任务

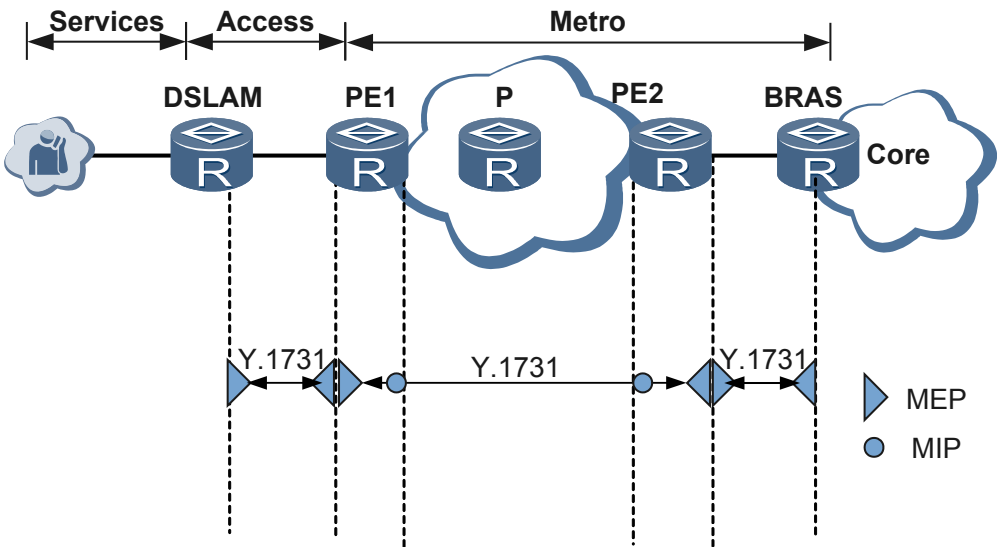
在配置 VPLS 的单端丢包统计功能前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 9-12 所示，当用户认为购买的以太网隧道业务出现了服务质量问题，或者运营商对自己的网络进行例行的 SLA（Service level agreement）监测时，可以使用 Y.1731 所定义的性能测试工具对链路进行检测：

- 单端丢包统计
- 双端丢包统计
- 单向时延统计
- 双向时延统计

图 9-12 性能检测组网图



本章仅介绍 PE 之间通过 VPLS 互联时 VPLS 的 PW 侧单端丢包统计功能。

前置任务

在配置 VPLS 的单端丢包统计之前，需完成以下任务：

- PW 侧单端丢包统计功能
 - 完成 VPLS 相关配置。
具体配置可参见《NE80E/40E 配置指南-VPN》中的 VPLS 配置。
 - 完成 CFM 相关配置，并配置 MEP 类型为 inward 型。

数据准备

在配置 VPLS 的单端丢包统计功能之前，需要准备以下数据。

序号	数据
1	MD、MA 的名称
2	MEP 的 ID、MEP 所在接口的名称、MEP 的类型
3	与 MA 绑定的 VSI name
4	报文的发送间隔和次数

9.6.2 配置 MA 与 VPLS 绑定

配置 MA 与 VPLS 绑定是配置 VPLS 的单端统计功能、双端丢包统计功能、单向时延统计功能、双向时延统计功能的首要步骤。

背景信息

基于 VPLS 的性能统计功能是针对指定的 VSI 的性能统计，因此在部署 Y.1731 的性能统计功能时，应当首先将 MA 与指定的 VSI 进行绑定，然后再对 MA 进行性能统计，从而得出指定 PW 或者 AC 上的性能统计信息。

- 如果进行 PW 侧检测，请在 VPLS 网络两端的 PE 上进行如下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **cfm md md-name**，进入 MD 视图。
- 步骤 3** 执行命令 **ma ma-name**，进入 MA 视图。
- 步骤 4** 执行命令 **map vsi vsi-name**，配置 MA 与 VSI 进行绑定。
- 结束

9.6.3 配置对端设备接收 LMM 报文功能

对链路进行单端丢包性能统计时，需要配置远端设备接收 LMM（Loss measurement message）报文功能。

背景信息

丢包统计功能是通过向其对等 MEP 发送带有 ETH-LM (Loss Measurement) 信息的帧, 并类似地从对等 MEP 接收带有 ETH-LM 信息的帧实现的。当对链路进行性能统计时, 需要配置远端 MEP 设备接收 LMM 报文功能。

操作步骤

步骤 1 执行命令 **system-view**, 进入系统视图。

步骤 2 执行命令 **cfm md md-name**, 进入 MD 视图。

步骤 3 执行命令 **ma ma-name**, 进入 MA 视图。

步骤 4 执行命令 **loss-measure single-ended receive [8021p { 8021p-value } &<1 - 3>]**, 配置对端设备接收 LMM 报文功能。

 说明

如果指定参数 **8021p 8021p-value**, 则接收端基于指定的优先级统计链路的丢包。如果不指定该参数, 则接收端基于所有优先级统计链路的丢包。

----结束

9.6.4 使能 VPLS 的单端丢包统计功能

VPLS 的单端丢包统计功能为按需的单端丢包统计。

背景信息

按需的 OAM 是指有限的时间内为了诊断而由人工干预发起的 OAM 动作, 可导致在诊断期间单次的或周期的 OAM 动作。当用户需要单次或者周期性的统计 PW 侧链路的丢包性能, 可以通过 VPLS 按需单端丢包统计功能实现。

- 如果进行 PW 侧检测, 请在链路丢包发起端 PE 上进行如下配置。

操作步骤

- PW 侧按需单端丢包统计

1. 执行命令 **system-view**, 进入系统视图。
2. 执行命令 **cfm md md-name**, 进入 MD 视图。
3. 执行命令 **ma ma-name**, 进入 MA 视图。
4. 执行命令 **loss-measure single-ended mep mep-id mep-id [mac mac-address | remote-mep mep-id mep-id] interval { 1000 | 10000 } count count-value [peer-ip peer-ip [vc-id vc-id]]**, 使能 PW 侧的按需单端丢包统计功能。

 说明

- 如果本端 MEP 没有学到远端 MEP 的 MAC 地址, 则必须使用指定目的 MAC 的方式进行丢包统计。
- 如果本端 MEP 已经学到远端 MEP 的 MAC 地址或 RMEP 已经绑定了对端 MAC, 则可以使用指定目的远端 MEP 号的方式进行丢包统计。

----结束

9.6.5 检查配置结果

VPLS 的单端丢包统计功能配置成功后，可以查看到 VPLS 的单端丢包统计信息。

前提条件

已经完成 VPLS 的单端丢包统计功能的所有配置。

操作步骤

- 使用 **display y1731 statistic-type single-loss md md-name ma ma-name [count count-value]** 命令查看 Y.1731 的性能统计数据。



说明
目前，VPLS 的单端丢包统计功能支持通过与当前设备版本配套的网管系统来查看配置结果。

----结束

任务示例

执行 **display y1731 statistic-type** 命令，可以看到单端丢包率的统计信息。

```
<HUAWEI> display Y.1731 statistic-type single-loss md md1 ma ma1
```

Latest single-ended loss statistics:

Index	Local-loss	ratio	Remote-loss	ratio
1	20	50.0000%	30	75.0000%
2	20	50.0000%	30	75.0000%
3	20	50.0000%	30	75.0000%
4	20	50.0000%	30	75.0000%
5	20	50.0000%	30	75.0000%
6	20	50.0000%	30	75.0000%
7	20	50.0000%	30	75.0000%
8	20	50.0000%	30	75.0000%
9	20	50.0000%	30	75.0000%
10	20	50.0000%	30	75.0000%
11	20	50.0000%	30	75.0000%
12	20	50.0000%	30	75.0000%
13	20	50.0000%	30	75.0000%
14	20	50.0000%	30	75.0000%

9.7 配置 VPLS 的双端丢包统计功能

VPLS 组网环境下，需要同时检测链路连通性和丢包情况并且对等 MEP 间均支持 CC（连通性检测）功能时，可以配置 VPLS 的双端丢包统计功能。

9.7.1 建立配置任务

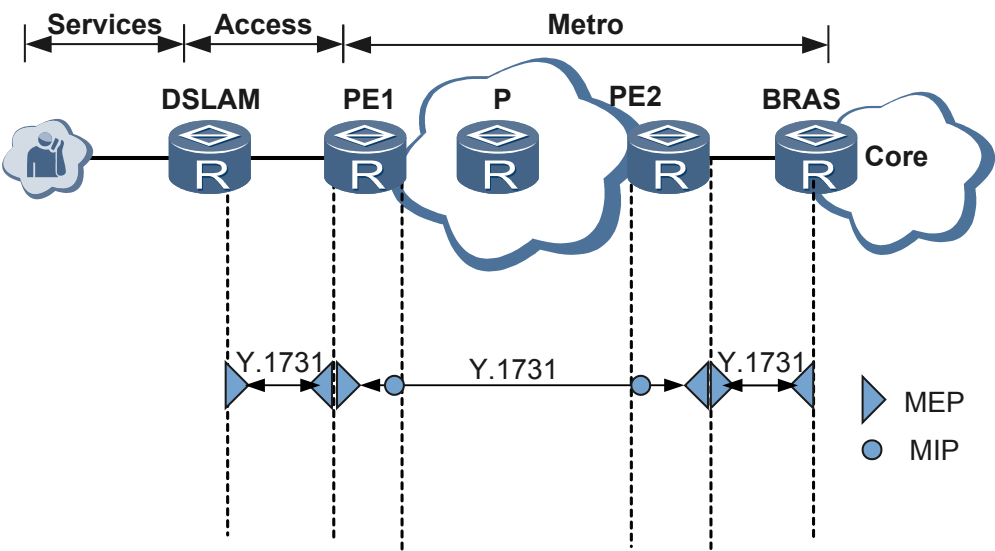
在配置 VPLS 的双端丢包统计功能前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 9-13 所示，当用户认为购买的以太网隧道业务出现了服务质量问题，或者运营商对自己的网络进行例行的 SLA（Service level agreement）监测时，可以使用 Y.1731 所定义的性能测试工具对链路进行检测：

- 单端丢包统计
- 双端丢包统计
- 单向时延统计
- 双向时延统计

图 9-13 性能检测组网图



本章仅介绍运营商网络 PE 之间通过 VPLS 互联时 VPLS 的 PW 侧双端丢包统计功能。

前置任务

在配置 VPLS 的双端丢包统计之前，需完成以下任务：

- PW 侧双端丢包统计功能
 - 完成 VPLS 相关配置。
具体配置可参见《NE80E/40E 配置指南-VPN》中的 VPLS 配置。
 - 完成 CFM 相关配置，并配置 MEP 类型为 inward 型。

数据准备

在配置 VPLS 的双端丢包统计功能之前，需要准备以下数据。

序号	数据
1	MD、MA 的名称
2	MEP 的 ID、MEP 所在接口的名称、MEP 的类型
3	RMEP 的 ID、RMEP 所在设备的桥 MAC 地址
4	MA 内 MEP 发送 CCM 消息的时间间隔
5	与 MA 绑定的 VSI name

9.7.2 配置 MA 与 VPLS 绑定

配置 MA 与 VPLS 绑定是配置 VPLS 的单端统计功能、双端丢包统计功能、单向时延统计功能、双向时延统计功能的首要步骤。

背景信息

基于 VPLS 的性能统计功能是针对指定的 VSI 的性能统计，因此在部署 Y.1731 的性能统计功能时，应当首先将 MA 与指定的 VSI 进行绑定，然后再对 MA 进行性能统计，从而得出指定 PW 或者 AC 上的性能统计信息。

- 如果进行 PW 侧检测，请在 VPLS 网络两端的 PE 上进行如下配置。

操作步骤

- 步骤 1 执行命令 **system-view**，进入系统视图。
- 步骤 2 执行命令 **cfm md md-name**，进入 MD 视图。
- 步骤 3 执行命令 **ma ma-name**，进入 MA 视图。
- 步骤 4 执行命令 **map vsi vsi-name**，配置 MA 与 VSI 进行绑定。

----结束

9.7.3 使能 VPLS 的双端丢包统计功能

VPLS 的双端丢包统计功能在对等 MEP 的两台设备上网络丢包的测量，同时提供链路连通性检测。

背景信息

连续的 OAM 是指连续、不间断的 OAM 动作。VPLS 的双端丢包统计功能为连续的 OAM。

请根据检测需要（PW 检测）对如下配置进行选取：

- 如果要进行 PW 侧检测，请在 VPLS 两端 PE 上进行如下配置。

操作步骤

- 步骤 1 执行命令 **system-view**，进入系统视图。
- 步骤 2 执行命令 **cfm md md-name**，进入 MD 视图。
- 步骤 3 执行命令 **ma ma-name**，进入 MA 视图。
- 步骤 4 配置 VPLS 的双端丢包统计功能。
 - 对于 PW 侧检测，在两端 PE 上执行命令 **loss-measure dual-ended continual mep mep-id mep-id remote-mep mep-id mep-id peer-ip peer-ip [vc-id vc-id]**，使能 VPLS PW 侧的双端丢包统计功能。

----结束

9.7.4 检查配置结果

VPLS 的双端丢包统计功能配置成功后，可以查看到双端丢包统计信息。

前提条件

已经完成 VPLS 的双端丢包统计功能的所有配置。

操作步骤

- 使用 **display y1731 statistic-type dual-loss md md-name ma ma-name [count count-value]** 命令查看 Y.1731 的性能统计数据。



说明

目前，VPLS 的双端丢包统计功能支持通过与当前设备版本配套的网管系统来查看配置结果。

----结束

任务示例

执行 **display y1731 statistic-type** 命令，可以看到双端丢包率的统计信息。

```
<HUAWEI> display y1731 statistic-type dual-loss md mdl ma mal peer-ip 1.1.1.1 vc-id 2
```

Latest dual-ended loss statistics:

Index	Local-loss	ratio	Remote-loss	ratio
1	4294967295	100.0000%	4294967295	100.0000%
2	4294967295	100.0000%	4294967295	100.0000%
3	4294967295	100.0000%	4294967295	100.0000%
4	4294967295	100.0000%	4294967295	100.0000%
5	4294967295	100.0000%	4294967295	100.0000%
6	4294967295	100.0000%	4294967295	100.0000%
7	4294967295	100.0000%	4294967295	100.0000%
8	4294967295	100.0000%	4294967295	100.0000%
9	4294967295	100.0000%	4294967295	100.0000%
10	4294967295	100.0000%	4294967295	100.0000%
11	4294967295	100.0000%	4294967295	100.0000%

9.8 配置 VPLS 的单向时延统计功能

VPLS 组网环境下，需要测量链路单方向的网络时延时，可以配置 VPLS 的单向时延统计功能。

9.8.1 建立配置任务

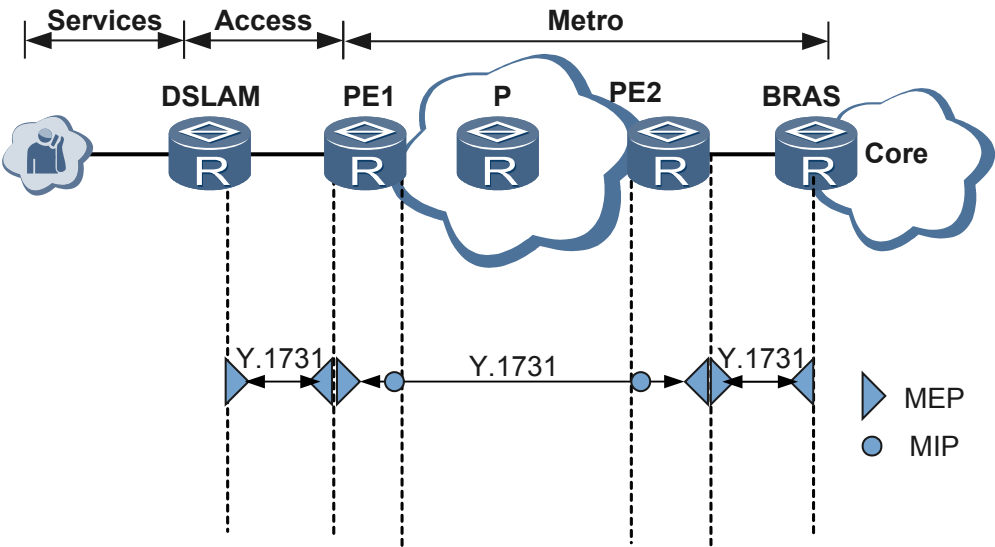
在配置 VPLS 的单向时延统计功能前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 9-14 所示，当用户认为购买的以太网隧道业务出现了服务质量问题，或者运营商对自己的网络进行例行的 SLA（Service level agreement）监测时，可以使用 Y.1731 所定义的性能测试工具对链路进行检测：

- 单端丢包统计
- 双端丢包统计
- 单向时延统计
- 双向时延统计

图 9-14 性能检测组网图



本章仅介绍运营商网络 PE 之间通过 VPLS 互联时 VPLS 的 PW 侧单向时延功能。

前置任务

在配置 VPLS 的单向时延统计功能之前，需完成以下任务：

- PW 侧单向时延统计功能
 - 完成 VPLS 相关配置。
具体配置可参见《NE80E/40E 配置指南-VPN》中的 VPLS 配置。
 - 完成 CFM 相关配置，并配置 MEP 类型为 inward 型。

数据准备

在配置 VPLS 的单向时延统计功能之前，需要准备以下数据。

序号	数据
1	MD、MA 的名称
2	MEP 的 ID、MEP 所在接口的名称、MEP 的类型
3	与 MA 绑定的 VSI name
4	RMEP 的 ID、RMEP 所在接口的 MAC 地址

9.8.2 配置 MA 与 VPLS 绑定

配置 MA 与 VPLS 绑定是配置 VPLS 的单端统计功能、双端丢包统计功能、单向时延统计功能、双向时延统计功能的首要步骤。

背景信息

基于 VPLS 的性能统计功能是针对指定的 VSI 的性能统计，因此在部署 Y.1731 的性能统计功能时，应当首先将 MA 与指定的 VSI 进行绑定，然后再对 MA 进行性能统计，从而得出指定 PW 或者 AC 上的性能统计信息。

- 如果进行 PW 侧检测，请在 VPLS 网络两端的 PE 上进行如下配置。

操作步骤

- 步骤 1 执行命令 **system-view**，进入系统视图。
- 步骤 2 执行命令 **cfm md md-name**，进入 MD 视图。
- 步骤 3 执行命令 **ma ma-name**，进入 MA 视图。
- 步骤 4 执行命令 **map vsi vsi-name**，配置 MA 与 VSI 进行绑定。

----结束

9.8.3 配置对端设备接收 DM 报文功能

单向时延统计时，需要在对端设备上配置接收 DM 报文功能。

背景信息

- 如果进行 PW 侧检测时，请在远端 MEP 的 PE 设备上进行以下配置。

操作步骤

- 步骤 1 执行命令 **system-view**，进入系统视图。
- 步骤 2 执行命令 **cfm md md-name**，进入 MD 视图。
- 步骤 3 执行命令 **ma ma-name**，进入 MA 视图。
- 步骤 4 请根据统计方式进行如下配置。
 - 进行 PW 侧检测时，执行命令 **delay-measure one-way receive peer-ip peer-ip vc-id vc-id**，配置接收 DM 报文功能。

----结束

9.8.4 使能 VPLS 的单向时延统计功能

VPLS 可以实现多点到多点的 VPN 组网，同一个 VSI 之间可能存在多条 PW 连接。为了精确统计一条 PW 的时延，需要配置 VPLS 的单向时延统计功能。

背景信息

按需的 OAM 是指有限的时间内为了诊断而由人工干预发起的 OAM 动作，可导致在诊断期间单次的或周期的 OAM 动作。VPLS 的单向时延统计为按需的 OAM。。当用户需要单次或者周期性的统计 PW 侧链路的时延性能，可以通过 VPLS 按需单向时延统计功能实现。

- 如果进行 PW 侧检测，请在链路时延发起端 PE 上进行如下配置。

操作步骤

- PW 侧按需单向时延统计
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **cfm md md-name**，进入 MD 视图。
 3. 执行命令 **ma ma-name**，进入 MA 视图。
 4. 执行命令 **delay-measure one-way mep mep-id mep-id { mac mac-address | remote-mep mep-id mep-id } interval { 1000 | 10000 } count count-value [peer-ip peer-ip [vc-id vc-id]]**，使能 PW 侧的按需单向时延统计功能。

 说明

- 如果本端 MEP 没有学到远端 MEP 的 MAC 地址，则必须使用指定目的 MAC 的方式进行时延统计。
- 如果本端 MEP 已经学到远端 MEP 的 MAC 地址或 RMEP 已经绑定了对端 MAC，则可以使用指定目的远端 MEP 号的方式进行时延统计。

----结束

9.8.5 检查配置结果

VPLS 的单向时延统计功能配置成功后，可以查看到单向时延统计信息。

前提条件

已经完成 VPLS 的单向时延统计功能的所有配置。

操作步骤

- 使用 **display y1731 statistic-type oneway-delay md md-name ma ma-name peer-ip ip-address [count count-value]** 命令查看 Y.1731 的性能统计信息。

----结束

任务示例

配置成功后，在 MEP 所在的设备上执行 **display y1731 statistic-type** 命令，可以看到时延值和时延抖动值。

```
<HUAWEI> display y1731 statistic-type oneway-delay md md1 ma ma1 peer-ip 1.1.1.1
Latest one-way delay statistics:
Index  One-way delay(usec)  Delay variation(usec)
1      10000                0
2      10000                0
3      10000                0
4      20000               10000
5      10000               10000
6      20000               10000
7      20000                0
```

9.9 配置 VPLS 的双向时延统计功能

VPLS 组网环境下，需要测量链路网络时延且对等体 MEP 时钟不同步、对链路时延统计要求不高的情况下，可以采用双向时延统计功能。

9.9.1 建立配置任务

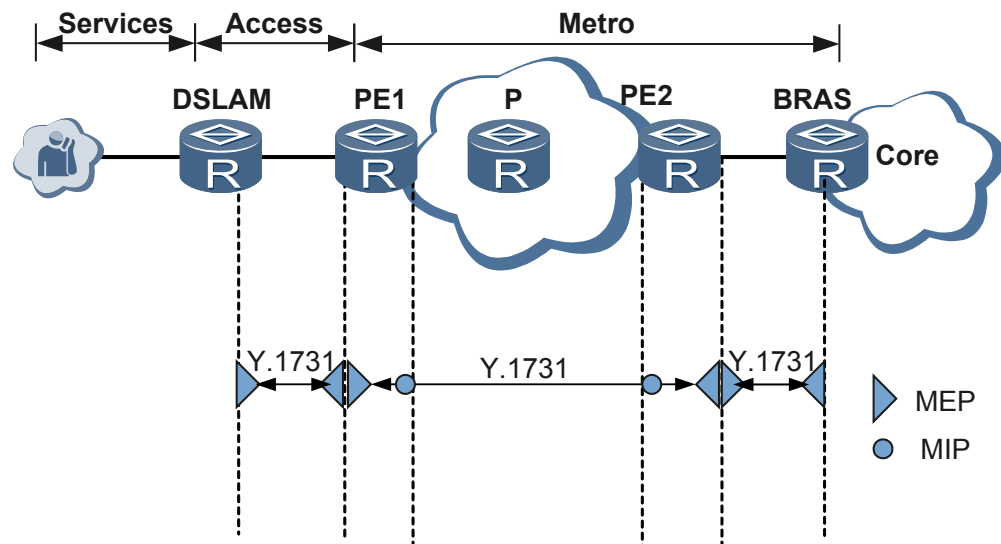
在配置 VPLS 的双向时延统计功能前了解此特性的应用环境、配置此特性的前置任务和
数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如图 9-15 所示，当用户认为购买的以太网隧道业务出现了服务质量问题，或者运营商
对自己的网络进行例行的 SLA（Service level agreement）监测时，可以使用 Y.1731 所定
义的性能测试工具对链路进行检测：

- 单端丢包统计
- 双端丢包统计
- 单向时延统计
- 双向时延统计

图 9-15 性能检测组网图



本章仅介绍运营商网络 PE 之间通过 VPLS 互联时 VPLS 的 PW 侧双向时延功能。

前置任务

在配置 VPLS 的双向时延统计功能之前，需完成以下任务：

- PW 侧双向时延统计功能
 - 配置 Martini 方式 VPLS
具体配置可参见《NE80E/40E 配置指南-VPN》中的 VPLS 配置。
 - 完成 CFM 相关配置，并配置 MEP 类型为 inward 型。

数据准备

在配置 VPLS 的双向时延统计功能之前，需要准备以下数据。

序号	数据
1	MD、MA 的名称
2	MEP 的 ID、MEP 所在接口的名称、MEP 的类型
3	与 MA 绑定的 VSI name
4	RMEP 的 ID、RMEP 所在接口的 MAC 地址

9.9.2 配置 MA 与 VPLS 绑定

配置 MA 与 VPLS 绑定是配置 VPLS 的单端统计功能、双端丢包统计功能、单向时延统计功能、双向时延统计功能的首要步骤。

背景信息

基于 VPLS 的性能统计功能是针对指定的 VSI 的性能统计，因此在部署 Y.1731 的性能统计功能时，应当首先将 MA 与指定的 VSI 进行绑定，然后再对 MA 进行性能统计，从而得出指定 PW 或者 AC 上的性能统计信息。

- 如果进行 PW 侧检测，请在 VPLS 网络两端的 PE 上进行如下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **cfm md md-name**，进入 MD 视图。
- 步骤 3** 执行命令 **ma ma-name**，进入 MA 视图。
- 步骤 4** 执行命令 **map vsi vsi-name**，配置 MA 与 VSI 进行绑定。

----结束

9.9.3 配置对端设备接收 DMM 报文功能

只有使能对端设备接收 DMM 报文，双向时延统计才有可能正常工作。

背景信息

请在 RMEP 所在的设备上以下配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **cfm md md-name**，进入 MD 视图。
- 步骤 3** 执行命令 **ma ma-name**，进入 MA 视图。
- 步骤 4** 请根据统计方式进行如下配置

- 进行 PW 侧检测时，请在远端 MEP 设备上执行命令 **delay-measure two-way receive peer-ip peer-ip vc-id vc-id**，配置对端设备接收 DMM 报文功能。

----结束

9.9.4 使能 VPLS 的双向时延统计功能

VPLS 可以实现多点到多点的 VPN 组网，同一个 VSI 之间可能存在多条 PW 连接。为了精确统计一条 PW 链路的时延，需要配置 VPLS 的双向时延统计功能。

背景信息

按需的 OAM 是指有限的时间内为了诊断而由人工干预发起的 OAM 动作，可导致在诊断期间单次的或周期的 OAM 动作。VPLS 的单向时延统计为按需的 OAM。当用户需要单次或者周期性的统计 PW 侧链路的时延性能，可以通过 VPLS 按需双向时延统计功能实现。

- 如果要进行 PW 侧检测，请在对等 MEP 发起 PE 设备上进行如下配置。

操作步骤

- PW 侧按需双向时延统计

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **cfm md md-name**，进入 MD 视图。
3. 执行命令 **ma ma-name**，进入 MA 视图。
4. 执行命令 **delay-measure two-way mep mep-id mep-id { mac mac-address | remote-mep mep-id mep-id } interval { 1000 | 10000 } count count-value [peer-ip peer-ip [vc-id vc-id]]**，使能 PW 侧的按需双向时延统计功能。

 说明

- 如果本端 MEP 没有学到远端 MEP 的 MAC 地址，则必须使用指定目的 MAC 的方式进行时延统计。
- 如果本端 MEP 已经学到远端 MEP 的 MAC 地址或 RMEP 已经绑定了对端 MAC，则可以使用指定目的远端 MEP 号的方式进行时延统计。

----结束

9.9.5 检查配置结果

VPLS 的双向时延统计功能配置成功后，可以查看到双向时延统计信息。

前提条件

已经完成 VPLS 的双向时延统计功能的所有配置。

操作步骤

- 使用 **display y1731 statistic-type twoway-delay md md-name ma ma-name peer-ip ip-address [count count-value]** 命令查看 Y.1731 的性能统计信息。

----结束

任务示例

配置成功后，在 MEP 所在的设备上执行 `display y1731 statistic-type` 命令，可以看到时延值和时延抖动值。

```
<HUAWEI> display y1731 statistic-type twoway-delay md mdl ma mal peer-ip 2.2.2.2
Latest two-way delay statistics:
Index  Two-way delay(usec)  Delay variation
1      30000                0
2      40000                10000
3      10000                30000
4      40000                30000
5      30000                10000
6      40000                10000
7      10000                30000
8      10000                0
9      0                  10000
10     30000                30000
11     0                  30000
12     10000               10000
13     0                  10000
14     40000               40000
```

9.10 配置举例

配置举例结合组网需求、配置思路和数据准备例举了 Y.1731 的基本功能及其应用。

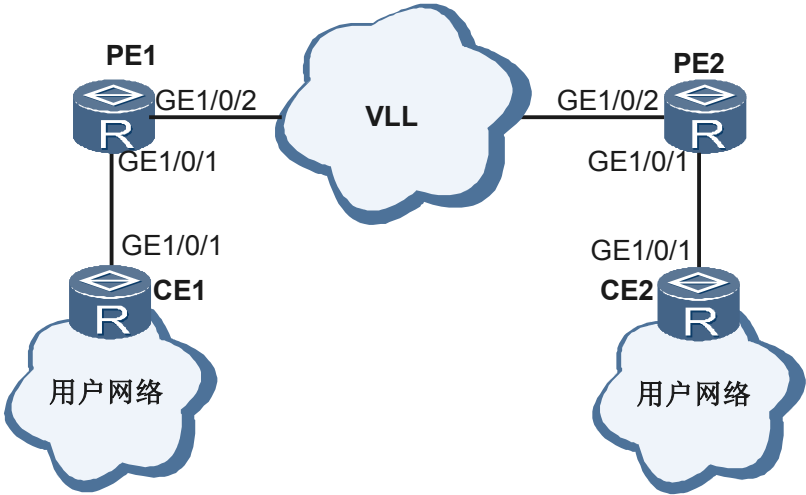
9.10.1 配置 VLL 的单端丢包统计功能示例（按需统计）

以典型组网为例，介绍了 VLL 组网环境下 PW 侧按需单端丢包统计应用。

组网需求

为了保证用户网络和运营商网络之间链路的可靠性和稳定性，提高运营商对连接链路的监控，可以在用户网络或者运营商网络上配置 Y.1731 功能。

图 9-16 VLL 的 Y.1731 组网图



本举例中介绍 VLL 的 PW 侧按需单端丢包统计功能。

配置思路

采用如下的思路配置 VLL 的按需单端丢包统计功能：

- 配置 PE 之间 PW 侧链路按需单端丢包统计功能。

数据准备

为完成此配置例，需准备如下的数据：

- VC ID。
- PE1 与 PE2 的 MD、MA 名称。

操作步骤

步骤 1 配置 PE 之间 PW 侧链路按需单端丢包统计功能

1. 配置 VLL 连接

在 PE1 与 PE2 之间配置 VLL 连接，具体配置过程略。请参考《*HUAWEI NetEngine80E/40E 路由器配置指南 VPN*》中的“VLL 配置”或者本配置举例中的配置文件。

上述配置完成后，在 PE 设备上执行命令 **display mpls l2vc**，可以查看到 VC 和 AC 链路信息。

```
<PE1>display mpls l2vc
total LDP VC : 1      1 up      0 down

*client interface      : GigabitEthernet1/0/1.1
Administrator PW      : no
session state         : up
AC status             : up
VC state              : up
Label state           : 0
Token state           : 0
VC ID                 : 2
VC type               : VLAN
destination            : 2.2.2.2
local VC label        : 1027      remote VC label      : 1025
control word          : disable
forwarding entry       : exist
local group ID        : 0
manual fault          : not set
active state          : active
link state             : up
local VC MTU          : 1500      remote VC MTU      : 1500
tunnel policy name    : --
traffic behavior name : --
PW template name      : --
primary or secondary  : primary
create time           : 0 days, 0 hours, 1 minutes, 12 seconds
up time               : 0 days, 0 hours, 0 minutes, 42 seconds
last change time      : 0 days, 0 hours, 0 minutes, 42 seconds
VC last up time       : 2010/10/13 15:02:23
VC total up time      : 0 days, 0 hours, 0 minutes, 42 seconds
CKey                  : 4
NKey                  : 3
AdminPw interface     : --
AdminPw link state    : --
```

2. 配置以太网 CFM 的基本功能，指定 MEP 类型为 Inward 型

在 PE 上配置以太网 CFM 的基本功能。指定以太网 CFM 协议为 Standard2007 标准版本，MD 的名称是 md1，MA 的名称是 ma1，并且配置 MA 与 VLL 绑定。

配置 PE1

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] cfm enable
[PE1] cfm version standard
[PE1] cfm md md1
[PE1-md-md1] ma ma1
[PE1-md-md1-ma-ma1] map mpls l2vc 2 tagged
[PE1-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet1/0/1.1 inward
[PE1-md-md1-ma-ma1] remote-mep mep-id 2
[PE1-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[PE1-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit
```

配置 PE2

```
<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] cfm enable
[PE2] cfm version standard
[PE2] cfm md md1
[PE2-md-md1] ma ma1
[PE2-md-md1-ma-ma1] map mpls l2vc 2 tagged
[PE2-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet1/0/1.1 inward
[PE2-md-md1-ma-ma1] remote-mep mep-id 1
[PE2-md-md1-ma-ma1] mep ccm-send mep-id 2 enable
[PE2-md-md1-ma-ma1] remote-mep ccm-receive mep-id 1 enable
[PE2-md-md1-ma-ma1] quit
[PE2-md-md1] quit
```

3. 在远端 PE2 设备上配置接收 LMM 报文功能

配置 PE2

```
[PE2-md-md1-ma-ma1] loss-measure single-ended receive
```

4. 使能 VLL 的 PW 侧按需单端丢包统计功能

配置 PE1

```
[PE1-md-md1-ma-ma1] loss-measure single-ended mep mep-id 1 mac 01-22-33
interval 1000 count 20
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit
```

5. 验证配置结果

在 PE1 执行 **display y1731 statistic-type** 命令，可以看到单端丢包率的统计信息。

```
<PE1>display y1731 statistic-type single-loss md md1 ma ma1
```

Index	Local-loss	ratio	Remote-loss	ratio
1	20	50.0000%	30	75.0000%
2	20	50.0000%	30	75.0000%
3	20	50.0000%	30	75.0000%
4	20	50.0000%	30	75.0000%
5	20	50.0000%	30	75.0000%
6	20	50.0000%	30	75.0000%
7	20	50.0000%	30	75.0000%
8	20	50.0000%	30	75.0000%
9	20	50.0000%	30	75.0000%
10	20	50.0000%	30	75.0000%
11	20	50.0000%	30	75.0000%
12	20	50.0000%	30	75.0000%
13	20	50.0000%	30	75.0000%
14	20	50.0000%	30	75.0000%

----结束

配置文件

- PE1 的配置文件

```
#
sysname PE1
#
cfm version standard
cfm enable
#
mpls lsr-id 1.1.1.1
mpls
#
mpls l2vpn
#
mpls ldp
#
interface GigabitEthernet1/0/1.1
vlan-type dot1q 2
mpls l2vc 2.2.2.2 2
#
interface GigabitEthernet1/0/2
undo shutdown
ip address 100.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 1.1.1.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 1.1.1.1 0.0.0.0
network 100.1.1.0 0.0.0.255
#
cfm md md1
ma mal
map mpls l2vc 2 tagged
mep mep-id 1 interface GigabitEthernet1/0/1.1 inward
mep ccm-send mep-id 1 enable
remote-mep mep-id 2
remote-mep ccm-receive mep-id 2 enable

#
return
```

- PE2 的配置文件

```
#
sysname PE2
#
cfm version standard
cfm enable
#
mpls lsr-id 2.2.2.2
mpls
#
mpls l2vpn
#
mpls ldp
#
#
interface GigabitEthernet1/0/1.1
vlan-type dot1q 2
mpls l2vc 1.1.1.1 2
#
interface GigabitEthernet1/0/2
undo shutdown
ip address 100.1.1.2 255.255.255.0
mpls
```

```
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 100.1.1.0 0.0.0.255
#
cfm md mdl
 ma mal
  map mpls l2vc 2 tagged
  mep mep-id 2 interface GigabitEthernet1/0/1.1 inward
  mep ccm-send mep-id 2 enable
  remote-mep mep-id 1
  remote-mep ccm-receive mep-id 1 enable
  loss-measure single-ended receive
#
return
```

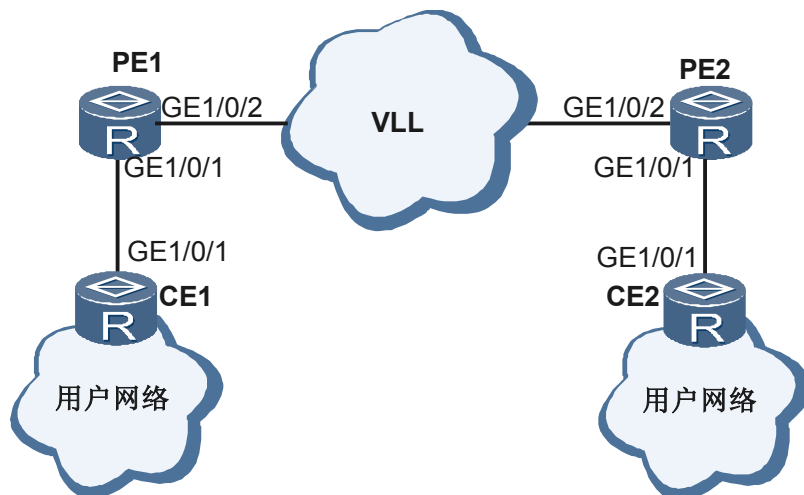
9.10.2 配置 VLL 的单端丢包统计功能示例（连续统计）

以典型组网为例，介绍了 VLL 组网环境下 PW 侧连续性单端丢包统计应用。

组网需求

为了保证用户网络和运营商网络之间链路的可靠性和稳定性，提高运营商对连接链路的监控，可以在用户网络或者运营商网络上配置 Y.1731 功能。

图 9-17 VLL 的 Y.1731 组网图



本举例中介绍 VLL 下 PW 侧连续丢包统计功能。

配置思路

采用如下的思路配置 VLL 的连续单端丢包统计功能：

- 配置 PE 间 VLL 功能。
- 配置 PW 链路 CFM 基本功能。
- 配置 PW 链路连续单端丢包统计功能。

数据准备

为完成此配置例，需准备如下的数据：

- VC ID。
- PE1 与 PE2 的 MD、MA 名称，CE1 和 PE1 的 MA 名称。

操作步骤

步骤 1 配置 VLL 连接

在 PE1 与 PE2 之间配置 VLL 连接，具体配置过程略。请参考《HUAWEI NetEngine80E/40E 路由器配置指南 VPN》中的“VLL 配置”或者本配置举例中的配置文件。

上述配置完成后，在 PE 设备上执行命令 **display mpls l2vc**，可以查看到 VC 和 AC 链路信息。

```
<PE1>display mpls l2vc
total LDP VC : 1      1 up      0 down

*client interface      : GigabitEthernet1/0/1.1
Administrator PW      : no
session state         : up
AC status              : up
VC state               : up
Label state            : 0
Token state            : 0
VC ID                  : 2
VC type                : VLAN
destination            : 2.2.2.2
local VC label         : 1027      remote VC label      : 1025
control word           : disable
forwarding entry       : exist
local group ID         : 0
manual fault           : not set
active state           : active
link state              : up
local VC MTU           : 1500      remote VC MTU      : 1500
tunnel policy name     : --
traffic behavior name  : --
PW template name       : --
primary or secondary   : primary
create time            : 0 days, 0 hours, 1 minutes, 12 seconds
up time                : 0 days, 0 hours, 0 minutes, 42 seconds
last change time       : 0 days, 0 hours, 0 minutes, 42 seconds
VC last up time        : 2010/10/13 15:02:23
VC total up time       : 0 days, 0 hours, 0 minutes, 42 seconds
CKey                   : 4
NKey                   : 3
AdminPw interface      : --
AdminPw link state     : --
```

步骤 2 配置以太网 CFM 的基本功能，指定 MEP 类型为 Inward 型

在 PE 上配置以太网 CFM 的基本功能。指定以太网 CFM 协议为 Standard2007 标准版本，MD 的名称是 md1，MA 的名称是 ma1，并且配置 MA 与 VLL 绑定。

配置 PE1

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] cfm enable
[PE1] cfm version standard
[PE1] cfm md md1
```

```
[PE1-md-md1] ma ma1
[PE1-md-md1-ma-ma1] map mpls l2vc 2 tagged
[PE1-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet1/0/1.1 inward
[PE1-md-md1-ma-ma1] remote-mep mep-id 2
[PE1-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[PE1-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit
```

配置 PE2

```
<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] cfm enable
[PE2] cfm version standard
[PE2] cfm md md1
[PE2-md-md1] ma ma1
[PE2-md-md1-ma-ma1] map mpls l2vc 2 tagged
[PE2-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet1/0/1.1 inward
[PE2-md-md1-ma-ma1] remote-mep mep-id 1
[PE2-md-md1-ma-ma1] mep ccm-send mep-id 2 enable
[PE2-md-md1-ma-ma1] remote-mep ccm-receive mep-id 1 enable
[PE2-md-md1-ma-ma1] quit
[PE2-md-md1] quit
```

步骤 3 在远端 PE2 设备上配置接收 LMM 报文功能

配置 PE2

```
[PE2-md-md1-ma-ma1] loss-measure single-ended receive
```

步骤 4 使能 VLL 的连续单端丢包统计功能

配置 PE1

```
[PE1-md-md1-ma-ma1] loss-measure single-ended continual mep mep-id 1 mac 0001-0001-0001 interval
30000
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit
```

步骤 5 验证配置结果

在 PE1 执行 **display y1731 statistic-type** 命令，可以看到单端丢包率的统计信息。

```
<PE1> display y1731 statistic-type single-loss md md1 ma ma1
```

Index	Local-loss	ratio	Remote-loss	ratio
1	20	50.0000%	30	75.0000%
2	20	50.0000%	30	75.0000%
3	20	50.0000%	30	75.0000%
4	20	50.0000%	30	75.0000%
5	20	50.0000%	30	75.0000%
6	20	50.0000%	30	75.0000%
7	20	50.0000%	30	75.0000%
8	20	50.0000%	30	75.0000%
9	20	50.0000%	30	75.0000%
10	20	50.0000%	30	75.0000%
11	20	50.0000%	30	75.0000%
12	20	50.0000%	30	75.0000%
13	20	50.0000%	30	75.0000%
14	20	50.0000%	30	75.0000%
15	20	50.0000%	30	75.0000%
16	20	50.0000%	30	75.0000%
17	20	50.0000%	30	75.0000%
18	20	50.0000%	30	75.0000%
19	20	50.0000%	30	75.0000%
20	20	50.0000%	30	75.0000%

----结束

配置文件

- PE1 的配置文件

```
#
sysname PE1
#
cfm version standard
cfm enable
#
mpls lsr-id 1.1.1.1
mpls
#
mpls l2vpn
#
mpls ldp
#
interface GigabitEthernet1/0/1.1
vlan-type dot1q 2
mpls l2vc 2.2.2.2 2
#
interface GigabitEthernet1/0/2
undo shutdown
ip address 100.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 1.1.1.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 1.1.1.1 0.0.0.0
network 100.1.1.0 0.0.0.255
#
cfm md md1
ma mal
map mpls l2vc 2 tagged
mep mep-id 1 interface GigabitEthernet1/0/1.1 inward
mep ccm-send mep-id 1 enable
remote-mep mep-id 2
remote-mep ccm-receive mep-id 2 enable
loss-measure single-ended continual mep mep-id 1 mac 0001-0001-0001 interval 30000
#
return
```

- PE2 的配置文件

```
#
sysname PE2
#
cfm version standard
cfm enable
#
mpls lsr-id 2.2.2.2
mpls
#
mpls l2vpn
#
mpls ldp
#
#
interface GigabitEthernet1/0/1.1
vlan-type dot1q 2
mpls l2vc 1.1.1.1 2
#
interface GigabitEthernet1/0/2
undo shutdown
ip address 100.1.1.2 255.255.255.0
mpls
```

```
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 100.1.1.0 0.0.0.255
#
cfm md mdl
 ma mal
  map mpls l2vc 2 tagged
  mep mep-id 2 interface GigabitEthernet1/0/1.1 inward
  mep ccm-send mep-id 4 enable
  remote-mep mep-id 3
  remote-mep ccm-receive mep-id 3 enable
  loss-measure single-ended receive
#
return
```

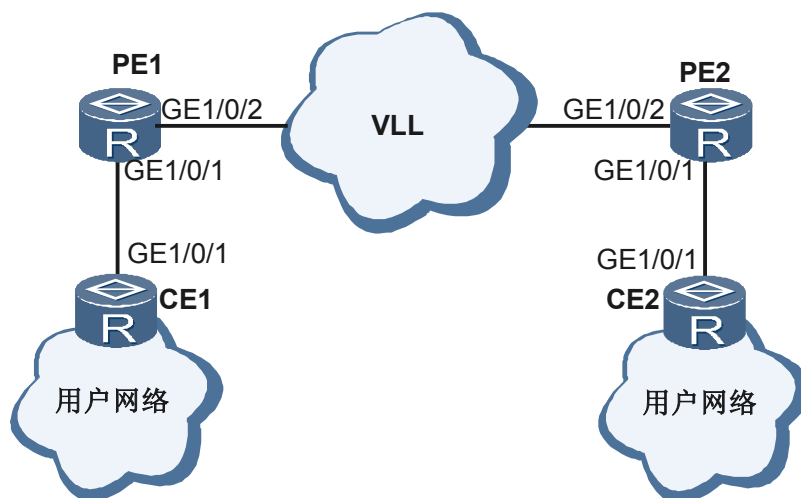
9.10.3 配置 VLL 的双端丢包统计功能示例（连续统计）

以典型组网为例，介绍了 VLL 组网环境下 PW 侧双端丢包统计应用。

组网需求

为了保证用户网络和运营商网络之间链路的可靠性和稳定性，提高运营商对连接链路的监控，可以在用户网络或者运营商网络上配置 Y.1731 功能。

图 9-18 VLL 的 Y.1731 组网图



本举例中介绍 VLL 的 PW 侧双端丢包统计功能。

配置思路

采用如下的思路配置 VLL 的双端丢包统计功能：

- 配置 PE 间 PW 侧双端丢包统计功能。

数据准备

为完成此配置例，需准备如下的数据：

- VC ID。
- PE1 与 PE2 的 MD、MA 名称。

操作步骤

步骤 1 配置 PE 间 PW 侧双端丢包统计功能。

1. 配置 VLL 连接

在 PE1 与 PE2 之间配置 VLL 连接，具体配置过程略。请参考《HUAWEI NetEngine80E/40E 路由器 配置指南 VPN》中的“VLL 配置”或者本配置举例中的配置文件。

上述配置完成后，在 PE 设备上执行命令 **display mpls l2vc**，可以查看到 VC 和 AC 信息。

```
<PE1>display mpls l2vc
total LDP VC : 1      1 up      0 down

*client interface      : GigabitEthernet1/0/1.1
Administrator PW      : no
session state         : up
AC status             : up
VC state              : up
Label state           : 0
Token state           : 0
VC ID                 : 2
VC type               : VLAN
destination            : 2.2.2.2
local VC label        : 1027      remote VC label      : 1025
control word          : disable
forwarding entry       : exist
local group ID        : 0
manual fault          : not set
active state          : active
link state             : up
local VC MTU          : 1500      remote VC MTU      : 1500
tunnel policy name    : --
traffic behavior name : --
PW template name      : --
primary or secondary  : primary
create time           : 0 days, 0 hours, 30 minutes, 6 seconds
up time               : 0 days, 0 hours, 29 minutes, 36 seconds
last change time      : 0 days, 0 hours, 29 minutes, 36 seconds
VC last up time       : 2010/10/13 15:02:23
VC total up time      : 0 days, 0 hours, 29 minutes, 36 seconds
CKey                  : 4
NKey                  : 3
AdminPw interface     : --
AdminPw link state    : --
```

2. 配置以太网 CFM 的基本功能，指定 MEP 类型为 Inward 型

在 PE 上配置以太网 CFM 的基本功能。指定以太网 CFM 协议为 Standard2007 标准版本，MD 的名称是 md1，MA 的名称是 ma1，并且配置 MA 与 VLL 绑定。

配置 PE1

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] cfm enable
[PE1] cfm version standard
[PE1] cfm md md1
[PE1-md-md1] ma ma1
[PE1-md-md1-ma-ma1] map mpls l2vc 2 tagged
[PE1-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet1/0/1.1 inward
[PE1-md-md1-ma-ma1] remote-mep mep-id 2
[PE1-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
```

```
[PE1-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit

# 配置 PE2

<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] cfm enable
[PE2] cfm version standard
[PE2] cfm md md1
[PE2-md-md1] ma ma1
[PE2-md-md1-ma-ma1] map mpls l2vc 2 tagged
[PE2-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet1/0/1.1 inward
[PE2-md-md1-ma-ma1] remote-mep mep-id 1
[PE2-md-md1-ma-ma1] mep ccm-send mep-id 2 enable
[PE2-md-md1-ma-ma1] remote-mep ccm-receive mep-id 1 enable
[PE2-md-md1-ma-ma1] quit
[PE2-md-md1] quit
```

3. 使能 VLL 的双端丢包统计功能

配置 PE1

```
[PE1-md-md1-ma-ma1] loss-measure dual-ended continual mep mep-id 1 remote-mep mep-id 2
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit
```

配置 PE2

```
[PE2-md-md1-ma-ma1] loss-measure dual-ended continual mep mep-id 2 remote-mep mep-id 1
[PE2-md-md1-ma-ma1] quit
[PE2-md-md1] quit
```

4. 验证配置结果

在 PE1 执行 **display y1731 statistic-type** 命令，可以看到双端丢包率的统计信息。

```
<PE1>display y1731 statistic-type dual-loss md md1 ma ma1
Latest dual-ended loss statistics:
Index  Local-loss  ratio  Remote-loss  ratio
1      4294967295  100.0000%  4294967295  100.0000%
2      4294967295  100.0000%  4294967295  100.0000%
3      4294967295  100.0000%  4294967295  100.0000%
4      4294967295  100.0000%  4294967295  100.0000%
5      4294967295  100.0000%  4294967295  100.0000%
6      4294967295  100.0000%  4294967295  100.0000%
7      4294967295  100.0000%  4294967295  100.0000%
8      4294967295  100.0000%  4294967295  100.0000%
9      4294967295  100.0000%  4294967295  100.0000%
10     4294967295  100.0000%  4294967295  100.0000%
11     4294967295  100.0000%  4294967295  100.0000%
```

----结束

配置文件

● PE1 的配置文件

```
#
sysname PE1
#
cfm version standard
cfm enable
#
mpls lsr-id 1.1.1.1
mpls
#
mpls l2vpn
#
mpls ldp
#
```

```
interface GigabitEthernet1/0/1.1
  vlan-type dot1q 2
  mpls l2vc 2.2.2.2 2
#
interface GigabitEthernet1/0/2
  undo shutdown
  ip address 100.1.1.1 255.255.255.0
  mpls
  mpls ldp
#
interface LoopBack0
  ip address 1.1.1.1 255.255.255.0
#
ospf 1
  area 0.0.0.0
    network 1.1.1.1 0.0.0.0
    network 100.1.1.0 0.0.0.255
#
cfm md md1
  ma ma1
  map mpls l2vc 2 tagged
  mep mep-id 1 interface GigabitEthernet1/0/1.1 inward
  mep ccm-send mep-id 1 enable
  remote-mep mep-id 2
  remote-mep ccm-receive mep-id 2 enable
  loss-measure dual-ended continual mep mep-id 1 remote-mep mep-id 2
#
return
```

● PE2 的配置文件

```
#
sysname PE2
#
cfm version standard
cfm enable
#
mpls lsr-id 2.2.2.2
mpls
#
mpls l2vpn
#
mpls ldp
#
interface GigabitEthernet1/0/1.1
  vlan-type dot1q 2
  mpls l2vc 1.1.1.1 2
#
interface GigabitEthernet1/0/2
  undo shutdown
  ip address 100.1.1.2 255.255.255.0
  mpls
  mpls ldp
#
interface LoopBack0
  ip address 2.2.2.2 255.255.255.0
#
ospf 1
  area 0.0.0.0
    network 2.2.2.2 0.0.0.0
    network 100.1.1.0 0.0.0.255
#
cfm md md1
  ma ma1
  map mpls l2vc 2 tagged
  mep mep-id 2 interface GigabitEthernet1/0/1.1 inward
  mep ccm-send mep-id 2 enable
  remote-mep mep-id 1
  remote-mep ccm-receive mep-id 1 enable
  loss-measure dual-ended enable mep mep-id 2 remote-mep mep-id 1
```

```
#
return
```

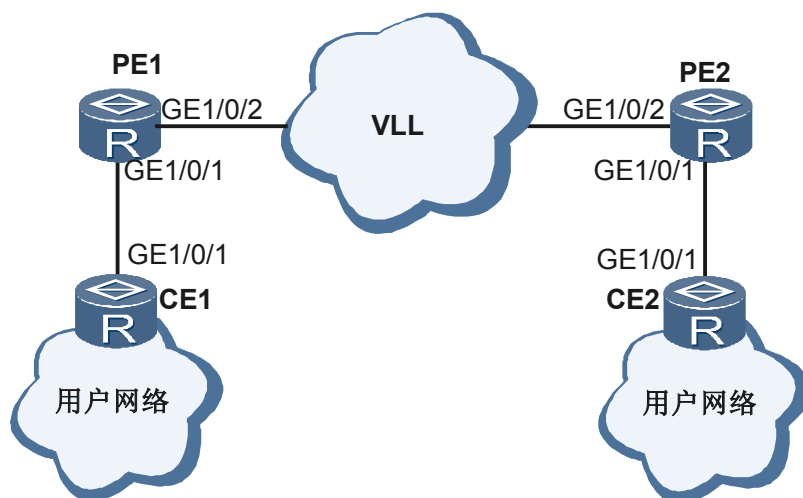
9.10.4 配置 VLL 的单向时延统计功能示例（按需统计）

以典型组网为例，介绍了 VLL 组网环境下 PW 侧按需单向时延统计应用。

组网需求

为了保证用户网络和运营商网络之间链路的可靠性和稳定性，提高运营商对连接链路的监控，可以在用户网络或者运营商网络上配置 Y.1731 功能。

图 9-19 VLL 的 Y.1731 组网图



本举例中介绍 VLL 的 PW 侧按需单向时延统计功能。

配置思路

采用如下的思路配置 VLL 的按需单向时延统计功能：

- 配置 PE 之间 PW 侧链路按需单向时延统计功能。

数据准备

为完成此配置例，需准备如下的数据：

- VC ID。
- PE1 与 PE2 的 MD、MA 名称。

操作步骤

步骤 1 配置 PE 之间 PW 侧链路按需单向时延统计功能

1. 配置 VLL 连接

在 PE1 与 PE2 之间配置 VLL 连接，具体配置过程略。请参考《HUAWEI NetEngine80E/40E 路由器配置指南 VPN》中的“VLL 配置”或者本配置举例中的配置文件。

上述配置完成后，在 PE 设备上执行命令 **display mpls l2vc**，可以查看到 VC 和 AC 链路信息。

```
<PE1>display mpls l2vc
total LDP VC : 1      1 up      0 down

*client interface      : GigabitEthernet1/0/1.1
Administrator PW      : no
session state          : up
AC status              : up
VC state               : up
Label state            : 0
Token state            : 0
VC ID                  : 2
VC type                : VLAN
destination            : 2.2.2.2
local VC label         : 1027      remote VC label      : 1025
control word           : disable
forwarding entry       : exist
local group ID         : 0
manual fault           : not set
active state           : active
link state              : up
local VC MTU           : 1500      remote VC MTU      : 1500
tunnel policy name     : --
traffic behavior name  : --
PW template name       : --
primary or secondary   : primary
create time            : 0 days, 0 hours, 1 minutes, 12 seconds
up time                : 0 days, 0 hours, 0 minutes, 42 seconds
last change time       : 0 days, 0 hours, 0 minutes, 42 seconds
VC last up time        : 2010/10/13 15:02:23
VC total up time       : 0 days, 0 hours, 0 minutes, 42 seconds
CKey                   : 4
NKey                   : 3
AdminPw interface     : --
AdminPw link state     : --
```

2. 配置以太网 CFM 的基本功能，指定 MEP 类型为 Inward 型

在 PE 上配置以太网 CFM 的基本功能。指定以太网 CFM 协议为 Standard2007 标准版本，MD 的名称是 md1，MA 的名称是 ma1，并且配置 MA 与 VLL 绑定。

配置 PE1

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] cfm enable
[PE1] cfm version standard
[PE1] cfm md md1
[PE1-md-md1] ma ma1
[PE1-md-md1-ma-ma1] map mpls l2vc 2 tagged
[PE1-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet1/0/1.1 inward
[PE1-md-md1-ma-ma1] remote-mep mep-id 2
[PE1-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[PE1-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit
```

配置 PE2

```
<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] cfm enable
[PE2] cfm version standard
[PE2] cfm md md1
[PE2-md-md1] ma ma1
[PE2-md-md1-ma-ma1] map mpls l2vc 2 tagged
[PE2-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet1/0/1.1 inward
[PE2-md-md1-ma-ma1] remote-mep mep-id 1
[PE2-md-md1-ma-ma1] mep ccm-send mep-id 2 enable
```

```
[PE2-md-md1-ma-ma1] remote-mep ccm-receive mep-id 1 enable
[PE2-md-md1-ma-ma1] quit
[PE2-md-md1] quit
```

3. 在远端 PE2 设备上配置接收 DMM 报文功能

配置 PE2

```
[PE2-md-md1-ma-ma1] delay-measure one-way receive
```

4. 使能 VLL 的 PW 侧按需单向时延统计功能

配置 PE1

```
[PE1-md-md1-ma-ma1] delay-measure one-way mep mep-id 1 mac 1-1-1 interval 1000 count 20
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit
```

5. 验证配置结果

在 PE2 执行 **display y1731 statistic-type** 命令，可以看到单向时延的统计信息。

```
<PE2>display y1731 statistic-type oneway-delay md md1 ma ma1
One-way delay measurement statistics:
Index  One-way delay(usec) Delay variation(usec)
1      30000                0
2      10000               20000
3      30000               20000
4      20000               10000
5      10000               10000
6      20000               10000
7      10000               10000
8      20000               10000
9      20000                0
10     10000               10000
11     10000                0
12     10000                0
13     30000               20000
14     10000               20000
15     30000               20000
```

----结束

配置文件

● PE1 的配置文件

```
#
sysname PE1
#
cfm version standard
cfm enable
#
mpls lsr-id 1.1.1.1
mpls
#
mpls l2vpn
#
mpls ldp
#
interface GigabitEthernet1/0/1.1
vlan-type dot1q 2
mpls l2vc 2.2.2.2 2
#
interface GigabitEthernet1/0/2
undo shutdown
ip address 100.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 1.1.1.1 255.255.255.0
```

```
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 100.1.1.0 0.0.0.255
#
cfm md md1
 ma ma1
 map mpls l2vc 2 tagged
 mep mep-id 1 interface GigabitEthernet1/0/1.1 inward
 mep ccm-send mep-id 1 enable
 remote-mep mep-id 2
 remote-mep ccm-receive mep-id 2 enable
#
return
```

● PE2 的配置文件

```
#
sysname PE2
#
cfm version standard
cfm enable
#
mpls lsr-id 2.2.2.2
mpls
#
mpls l2vpn
#
vsi ldpl static
 pwsignal ldp
 vsi-id 1
 peer 1.1.1.1
#
mpls ldp
#
#
interface GigabitEthernet1/0/1.1
 vlan-type dot1q 2
 mpls l2vc 1.1.1.1 2
#
interface GigabitEthernet1/0/2
 undo shutdown
 ip address 100.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 100.1.1.0 0.0.0.255
#
cfm md md1
 ma ma1
 map mpls l2vc 2 tagged
 mep mep-id 2 interface GigabitEthernet1/0/1.1 inward
 mep ccm-send mep-id 2 enable
 remote-mep mep-id 1
 remote-mep ccm-receive mep-id 1 enable
 delay-measure one-way receive
#
return
```

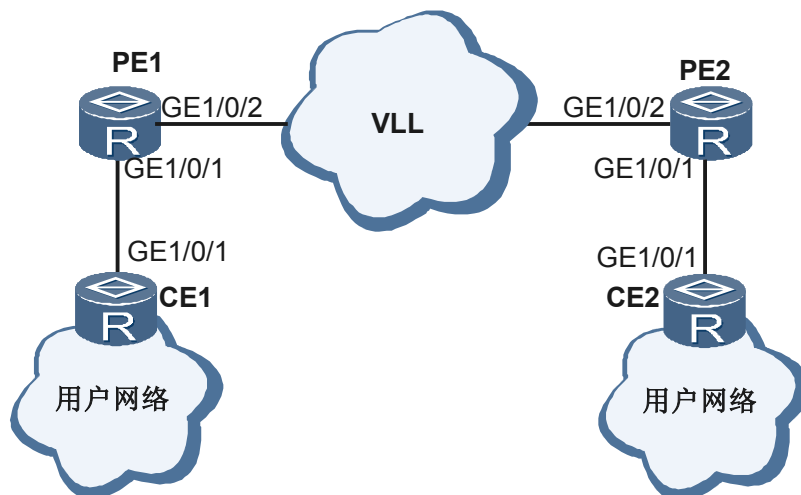
9.10.5 配置 VLL 的单向时延统计功能示例（连续统计）

以典型组网为例，介绍了 VLL 组网环境下 PW 侧连续单向时延统计应用。

组网需求

为了保证用户网络和运营商网络之间链路的可靠性和稳定性，提高运营商对连接链路的监控，可以在用户网络或者运营商网络上配置 Y.1731 功能。

图 9-20 VLL 的 Y.1731 组网图



本举例中介绍 VLL 的 PW 侧连续单向时延统计功能。

配置思路

采用如下的思路配置 VLL 的连续单向时延统计功能：

- 配置 PE 之间链路为 VLL。
- 完成 CFM 基本配置。
- 使能 VLL 的连续单向时延统计功能。

数据准备

为完成此配置例，需准备如下的数据：

- VC ID。
- PE1 与 PE2 的 MD、MA 名称，CE1 和 PE1 的 MA 名称。

操作步骤

步骤 1 配置 VLL 连接

在 PE1 与 PE2 之间配置 VLL 连接，具体配置过程略。请参考《HUAWEI NetEngine80E/40E 路由器配置指南 VPN》中的“VLL 配置”或者本配置举例中的配置文件。

上述配置完成后，在 PE 设备上执行命令 **display mpls l2vc**，可以查看到 VC 和 AC 链路信息。

```
<PE1>display mpls l2vc
total LDP VC : 1      1 up      0 down

*client interface      : GigabitEthernet1/0/1.1
```



```
Administrator PW      : no
session state         : up
AC status              : up
VC state              : up
Label state           : 0
Token state           : 0
VC ID                  : 2
VC type                : VLAN
destination            : 2.2.2.2
local VC label         : 1027      remote VC label      : 1025
control word           : disable
forwarding entry       : exist
local group ID         : 0
manual fault           : not set
active state           : active
link state             : up
local VC MTU           : 1500      remote VC MTU       : 1500
tunnel policy name     : --
traffic behavior name  : --
PW template name       : --
primary or secondary   : primary
create time            : 0 days, 0 hours, 1 minutes, 12 seconds
up time                : 0 days, 0 hours, 0 minutes, 42 seconds
last change time       : 0 days, 0 hours, 0 minutes, 42 seconds
VC last up time        : 2010/10/13 15:02:23
VC total up time       : 0 days, 0 hours, 0 minutes, 42 seconds
CKey                   : 4
NKey                   : 3
AdminPw interface      : --
AdminPw link state     : --
```

步骤 2 配置以太网 CFM 的基本功能，指定 MEP 类型为 Inward 型

在 PE 上配置以太网 CFM 的基本功能。指定以太网 CFM 协议为 Standard2007 标准版本，MD 的名称是 md1，MA 的名称是 ma1，并且配置 MA 与 VLL 绑定。

配置 PE1

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] cfm enable
[PE1] cfm version standard
[PE1] cfm md md1
[PE1-md-md1] ma ma1
[PE1-md-md1-ma-ma1] map mpls l2vc 2 tagged
[PE1-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet1/0/1.1 inward
[PE1-md-md1-ma-ma1] remote-mep mep-id 2
[PE1-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[PE1-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit
```

配置 PE2

```
<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] cfm enable
[PE2] cfm version standard
[PE2] cfm md md1
[PE2-md-md1] ma ma1
[PE2-md-md1-ma-ma1] map mpls l2vc 2 tagged
[PE2-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet1/0/1.1 inward
[PE2-md-md1-ma-ma1] remote-mep mep-id 1
[PE2-md-md1-ma-ma1] mep ccm-send mep-id 2 enable
[PE2-md-md1-ma-ma1] remote-mep ccm-receive mep-id 1 enable
[PE2-md-md1-ma-ma1] quit
[PE2-md-md1] quit
```

步骤 3 在远端 PE2 设备上配置接收 DMM 报文能力

配置 PE2

```
[PE2-md-md1-ma-ma1] delay-measure one-way continual receive
```

步骤 4 使能 VLL 的连续单向时延统计功能

```
[PE1-md-md1-ma-ma1] delay-measure one-way continual mep mep-id 1 mac 0001-0001-0001 interval 1000
```

```
[PE1-md-md1-ma-ma1] quit
```

```
[PE1-md-md1] quit
```

步骤 5 验证配置结果

在 PE2 执行 **display y1731 statistic-type** 命令，可以看到单向时延的统计信息。

```
<PE2>display y1731 statistic-type oneway-delay md md1 ma ma1
```

Index	One-way delay(usec)	Delay variation(usec)
1	20000	0
2	20000	0
3	20000	0
4	30000	10000
5	10000	20000
6	10000	0
7	10000	0
8	10000	0
9	20000	10000
10	20000	0
11	10000	10000
12	10000	0
13	20000	10000
14	20000	0
15	20000	0
16	10000	10000
17	20000	10000
18	20000	0
19	20000	0
20	10000	10000
21	10000	0
22	20000	10000
23	20000	0

----结束

配置文件

● PE1 的配置文件

```
#
 sysname PE1
#
 cfm version standard
 cfm enable
#
 mpls lsr-id 1.1.1.1
 mpls
#
 mpls l2vpn
#
 mpls ldp
#
 interface GigabitEthernet1/0/1.1
  vlan-type dot1q 2
  mpls l2vc 2.2.2.2 2
#
 interface GigabitEthernet1/0/2
  undo shutdown
  ip address 100.1.1.1 255.255.255.0
  mpls
  mpls ldp
```

```
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 100.1.1.0 0.0.0.255
#
cfm md md1
 ma mal
 map mpls l2vc 2 tagged
 mep mep-id 1 interface GigabitEthernet1/0/1.1 inward
 mep ccm-send mep-id 1 enable
 remote-mep mep-id 2
 remote-mep ccm-receive mep-id 2 enable
 delay-measure one-way continual mep mep-id 1 mac 0001-0001-0001 interval 1000
#
return
```

● PE2 的配置文件

```
#
sysname PE2
#
cfm version standard
cfm enable
#
mpls lsr-id 2.2.2.2
mpls
#
mpls l2vpn
#
vsi ldpl static
 pwsignal ldp
 vsi-id 1
 peer 1.1.1.1
#
mpls ldp
#
#
interface GigabitEthernet1/0/1.1
 vlan-type dot1q 2
 mpls l2vc 1.1.1.1 2
#
interface GigabitEthernet1/0/2
 undo shutdown
 ip address 100.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 100.1.1.0 0.0.0.255
#
cfm md md1
 ma mal
 map mpls l2vc 2 tagged
 mep mep-id 2 interface GigabitEthernet1/0/1.1 inward
 mep ccm-send mep-id 2 enable
 remote-mep mep-id 1
 remote-mep ccm-receive mep-id 1 enable
 delay-measure one-way continual receive
#
return
```

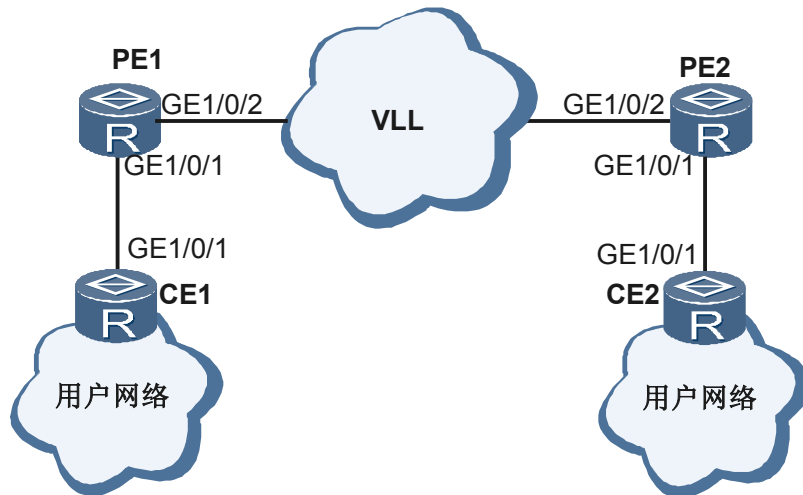
9.10.6 配置 VLL 的双向时延统计功能示例（按需统计）

以典型组网为例，介绍了 VLL 组网环境下 PW 侧双向时延统计应用。

组网需求

为了保证用户网络和运营商网络之间链路的可靠性和稳定性，提高运营商对连接链路的监控，可以在用户网络或者运营商网络上配置 Y.1731 功能。

图 9-21 VLL 的 Y.1731 组网图



本举例中介绍 VLL 下 PW 侧双向时延统计功能。

配置思路

采用如下的思路配置 VLL 的按需双向时延统计功能：

1. 配置 PE 间 PW 侧双向时延统计功能。

数据准备

为完成此配置例，需准备如下的数据：

- VC ID。
- PE1 与 PE2 的 MD、MA 名称。

操作步骤

步骤 1 配置 PE 间 PW 侧按需双向时延统计功能

1. 配置 VLL 连接

在 PE1 与 PE2 之间配置 VLL 连接，具体配置过程略。请参考《HUAWEI NetEngine80E/40E 路由器配置指南 VPN》中的“VLL 配置”或者本配置举例中的配置文件。

上述配置完成后，在 PE 设备上执行命令 **display mpls l2vc**，可以查看到 VC 和 AC 链路信息。

```
<PE1>display mpls l2vc
total LDP VC : 1      1 up      0 down
*client interface : GigabitEthernet1/0/1.1
  Administrator PW : no
  session state    : up
  AC status        : up
  VC state         : up
  Label state      : 0
  Token state      : 0
  VC ID           : 2
  VC type          : VLAN
  destination      : 2.2.2.2
  local VC label   : 1027      remote VC label : 1025
  control word     : disable
  forwarding entry : exist
  local group ID   : 0
  manual fault     : not set
  active state     : active
  link state       : up
  local VC MTU     : 1500      remote VC MTU : 1500
  tunnel policy name : --
  traffic behavior name: --
  PW template name : --
  primary or secondary : primary
  create time      : 0 days, 0 hours, 1 minutes, 12 seconds
  up time          : 0 days, 0 hours, 0 minutes, 42 seconds
  last change time : 0 days, 0 hours, 0 minutes, 42 seconds
  VC last up time  : 2010/10/13 15:02:23
  VC total up time : 0 days, 0 hours, 0 minutes, 42 seconds
  CKey            : 4
  NKey            : 3
  AdminPw interface : --
  AdminPw link state : --
```

2. 配置以太网 CFM 的基本功能，指定 MEP 类型为 Inward 型

在 PE 上配置以太网 CFM 的基本功能。指定以太网 CFM 协议为 Standard2007 标准版本，MD 的名称是 md1，MA 的名称是 ma1，并且配置 MA 与 VLL 绑定。

配置 PE1

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] cfm enable
[PE1] cfm version standard
[PE1] cfm md md1
[PE1-md-md1] ma ma1
[PE1-md-md1-ma-ma1] map mpls l2vc 2 tagged
[PE1-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet1/0/1.1 inward
[PE1-md-md1-ma-ma1] remote-mep mep-id 2
[PE1-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[PE1-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit
```

配置 PE2

```
<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] cfm enable
[PE2] cfm version standard
[PE2] cfm md md1
[PE2-md-md1] ma ma1
[PE2-md-md1-ma-ma1] map mpls l2vc 2 tagged
[PE2-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet1/0/1.1 inward
[PE2-md-md1-ma-ma1] remote-mep mep-id 1
[PE2-md-md1-ma-ma1] mep ccm-send mep-id 2 enable
[PE2-md-md1-ma-ma1] remote-mep ccm-receive mep-id 1 enable
[PE2-md-md1-ma-ma1] quit
[PE2-md-md1] quit
```

3. 配置远端 PE2 设备接收 DMM 报文功能

配置 PE2

```
[PE2-md-md1-ma-ma1] delay-measure two-way receive
[PE2-md-md1-ma-ma1] quit
[PE2-md-md1] quit
```

4. 使能 VLL 的 PW 侧双向时延统计功能

配置 PE1

```
[PE1-md-md1-ma-ma1] delay-measure two-way mep mep-id 1 mac 1-1-1 interval 1000 count 60
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit
```

5. 检查配置结果

在 PE1 执行 **display y1731 statistic-type** 命令，可以看到双向时延的统计信息。

```
<PE1> display y1731 statistic-type twoway-delay md md1 ma ma1
```

Two-way delay measurement statistics:

Index	Two-way delay(usec)	Delay variation(usec)
1	10000	0
2	10000	10000
3	20000	10000
4	10000	10000
5	10000	0
6	20000	10000
7	10000	10000
8	10000	0
9	10000	0
10	20000	10000
11	20000	0
12	10000	10000
13	20000	10000
14	10000	10000
15	20000	10000

----结束

配置文件

● PE1 的配置文件

```
#
sysname PE1
#
cfm version standard
cfm enable
#
mpls lsr-id 1.1.1.1
mpls
#
mpls l2vpn
#
mpls ldp
#
interface GigabitEthernet1/0/1
undo shutdown
#
interface GigabitEthernet1/0/1.1
vlan-type dot1q 2
mpls l2vc 2.2.2.2 2
#
interface GigabitEthernet1/0/2
undo shutdown
ip address 100.1.1.1 255.255.255.0
mpls
mpls ldp
#
```

```
interface NULL0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 100.1.1.0 0.0.0.255
#
cfm md md1
 ma mal
  map mpls l2vc 2 tagged
  mep mep-id 1 interface GigabitEthernet1/0/1.1 inward
  mep ccm-send mep-id 1 enable
  remote-mep mep-id 2
  remote-mep ccm-receive mep-id 2
enable
#
return
```

● PE2 的配置文件

```
#
sysname PE2
#
cfm version standard
cfm enable
#
mpls lsr-id 2.2.2.2
mpls
#
mpls l2vpn
#
mpls ldp
#
interface GigabitEthernet1/0/1.1
 vlan-type dot1q 2
 mpls l2vc 1.1.1.1 2
#
interface GigabitEthernet1/0/2
 undo shutdown
 ip address 100.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 100.1.1.0 0.0.0.255
#
cfm md md1
 ma mal
  map mpls l2vc 2 tagged
  mep mep-id 2 interface GigabitEthernet1/0/1.1 inward
  mep ccm-send mep-id 2 enable
  remote-mep mep-id 1
  remote-mep ccm-receive mep-id 1
enable
 delay-measure two-way receive
#
return
```

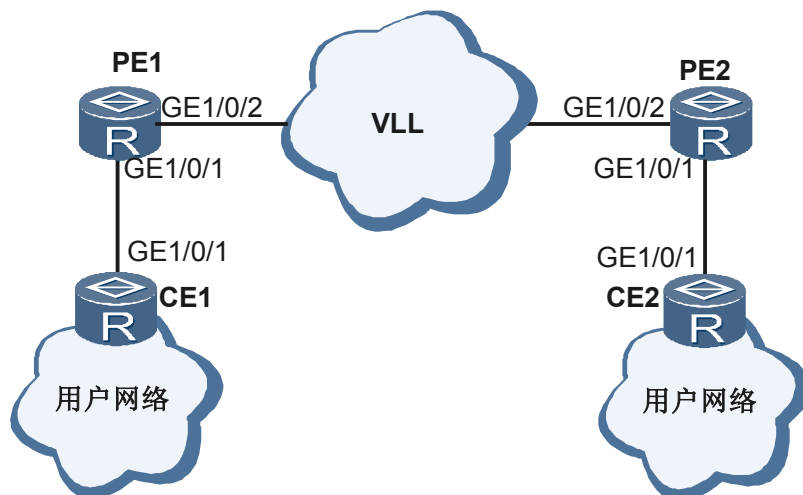
9.10.7 配置 VLL 的双向时延统计功能示例（连续统计）

以典型组网为例，介绍了 VLL 组网环境下 PW 侧连续双向时延统计应用。

组网需求

为了保证用户网络和运营商网络之间链路的可靠性和稳定性，提高运营商对连接链路的监控，可以在用户网络或者运营商网络上配置 Y.1731 功能。

图 9-22 VLL 的 Y.1731 组网图



本举例中介绍 VLL 的 PW 侧连续双向时延统计功能。

配置思路

采用如下的思路配置 VLL 的连续双向时延统计功能：

- 配置 PE 之间链路为 VLL。
- 完成 CFM 基本配置。
- 使能 VLL 的连续双向时延统计功能。

数据准备

为完成此配置例，需准备如下的数据：

- VC ID。
- PE1 与 PE2 的 MD、MA 名称，CE1 和 PE1 的 MA 名称。

操作步骤

步骤 1 配置 VLL 连接

在 PE1 与 PE2 之间配置 VLL 连接，具体配置过程略。请参考《HUAWEI NetEngine80E/40E 路由器配置指南 VPN》中的“VLL 配置”或者本配置举例中的配置文件。

上述配置完成后，在 PE 设备上执行命令 **display mpls l2vc**，可以查看到 VC 和 AC 链路信息。

```
<PE1>display mpls l2vc
total LDP VC : 1      1 up      0 down

*client interface      : GigabitEthernet1/0/1.1
```



```
Administrator PW      : no
session state         : up
AC status             : up
VC state              : up
Label state           : 0
Token state           : 0
VC ID                 : 2
VC type               : VLAN
destination           : 2.2.2.2
local VC label        : 1027      remote VC label      : 1025
control word          : disable
forwarding entry      : exist
local group ID        : 0
manual fault          : not set
active state          : active
link state            : up
local VC MTU          : 1500      remote VC MTU       : 1500
tunnel policy name    : --
traffic behavior name : --
PW template name      : --
primary or secondary  : primary
create time           : 0 days, 0 hours, 1 minutes, 12 seconds
up time               : 0 days, 0 hours, 0 minutes, 42 seconds
last change time      : 0 days, 0 hours, 0 minutes, 42 seconds
VC last up time       : 2010/10/13 15:02:23
VC total up time      : 0 days, 0 hours, 0 minutes, 42 seconds
CKey                  : 4
NKey                  : 3
AdminPw interface     : --
AdminPw link state    : --
```

步骤 2 配置以太网 CFM 的基本功能，指定 MEP 类型为 Inward 型

在 PE 上配置以太网 CFM 的基本功能。指定以太网 CFM 协议为 Standard2007 标准版本，MD 的名称是 md1，MA 的名称是 ma1，并且配置 MA 与 VLL 绑定。

配置 PE1

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] cfm enable
[PE1] cfm version standard
[PE1] cfm md md1
[PE1-md-md1] ma ma1
[PE1-md-md1-ma-ma1] map mpls l2vc 2 tagged
[PE1-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet1/0/1.1 inward
[PE1-md-md1-ma-ma1] remote-mep mep-id 2
[PE1-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[PE1-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit
```

配置 PE2

```
<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] cfm enable
[PE2] cfm version standard
[PE2] cfm md md1
[PE2-md-md1] ma ma1
[PE2-md-md1-ma-ma1] map mpls l2vc 2 tagged
[PE2-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet1/0/1.1 inward
[PE2-md-md1-ma-ma1] remote-mep mep-id 1
[PE2-md-md1-ma-ma1] mep ccm-send mep-id 2 enable
[PE2-md-md1-ma-ma1] remote-mep ccm-receive mep-id 1 enable
[PE2-md-md1-ma-ma1] quit
[PE2-md-md1] quit
```

步骤 3 在远端 PE2 设备上配置接收 DMM 报文能力

配置 PE2

```
[PE2-md-md1-ma-mal] delay-measure two-way receive
```

步骤 4 使能 VLL 的连续双向时延统计功能

```
[PE1-md-md1-ma-mal] delay-measure two-way continual mep mep-id 1 mac 0001-0001-0001 interval 30000  
[PE1-md-md1-ma-mal] quit  
[PE1-md-md1] quit
```

步骤 5 验证配置结果

在 PE2 执行 **display y1731 statistic-type** 命令，可以看到双向时延的统计信息。

```
<PE2>display y1731 statistic-type oneway-delay md md1 ma mal  
Two-way delay measurement statistics:  
Index Two-way delay(usec) Delay variation(usec)  
1      10000                0  
2      30000                20000  
3      10000                20000  
4      20000                10000
```

----结束

配置文件

● PE1 的配置文件

```
#  
sysname PE1  
#  
cfm version standard  
cfm enable  
#  
mpls lsr-id 1.1.1.1  
mpls  
#  
mpls l2vpn  
#  
mpls ldp  
#  
interface GigabitEthernet1/0/1.1  
vlan-type dot1q 2  
mpls l2vc 2.2.2.2 2  
#  
interface GigabitEthernet1/0/2  
undo shutdown  
ip address 100.1.1.1 255.255.255.0  
mpls  
mpls ldp  
#  
interface LoopBack0  
ip address 1.1.1.1 255.255.255.0  
#  
ospf 1  
area 0.0.0.0  
network 1.1.1.1 0.0.0.0  
network 100.1.1.0 0.0.0.255  
#  
cfm md md1  
ma mal  
map mpls l2vc 2 tagged  
mep mep-id 1 interface GigabitEthernet1/0/1.1 inward  
mep ccm-send mep-id 1 enable  
remote-mep mep-id 2  
remote-mep ccm-receive mep-id 2 enable  
delay-measure two-way continual mep mep-id 1 mac 0001-0001-0001 interval 30000
```

```
#
return
● PE2 的配置文件
#
sysname PE2
#
cfm version standard
cfm enable
#
mpls lsr-id 2.2.2.2
mpls
#
mpls l2vpn
#
mpls ldp
#
#
interface GigabitEthernet1/0/1.1
vlan-type dot1q 2
mpls l2vc 1.1.1.1 2
#
interface GigabitEthernet1/0/2
undo shutdown
ip address 100.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 2.2.2.2 255.255.255.0
#
ospf 1
area 0.0.0.0
network 2.2.2.2 0.0.0.0
network 100.1.1.0 0.0.0.255
#
cfm md md1
ma ma1
map mpls l2vc 2 tagged
mep mep-id 2 interface GigabitEthernet1/0/1.1 inward
mep ccm-send mep-id 2 enable
remote-mep mep-id 1
remote-mep ccm-receive mep-id 1 enable
delay-measure two-way receive
#
return
```

9.10.8 配置 VPLS 的单端丢包统计功能示例（按需统计）

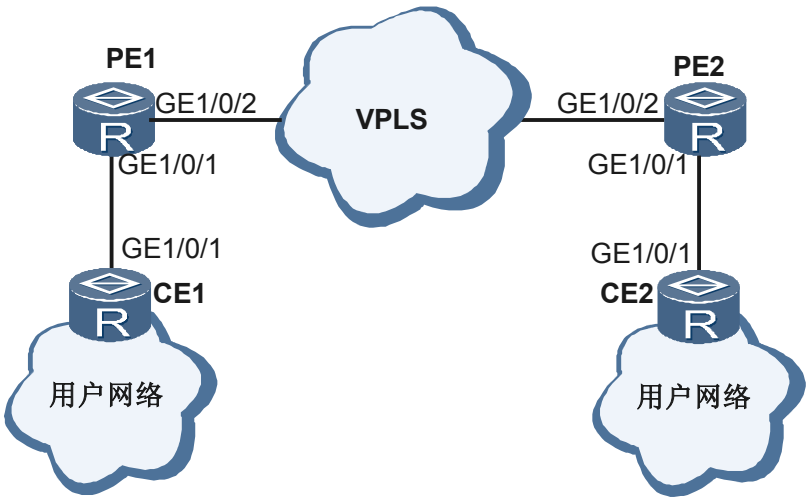
以典型组网为例，介绍了 VPLS 组网环境下 PW 侧按需单端丢包统计应用。

组网需求

为了保证用户网络和运营商网络之间链路的可靠性和稳定性，提高运营商对连接链路的监控，可以在用户网络或者运营商网络上配置 Y.1731 功能。

本举例中介绍 PW 侧按需单端丢包统计功能。

图 9-23 VPLS 的单端丢包统计功能组网图



配置思路

采用如下的思路配置 VPLS 的按需单端丢包统计功能：

- 配置 PE 之间 PW 侧链路丢包统计功能。

数据准备

为完成此配置例，需准备如下的数据：

- VSI name。
- PE1 与 PE2 的 MD、MA 名称，CE1 和 PE1 的 MA 名称。

操作步骤

步骤 1 配置 PE 之间 PW 侧链路按需单端丢包统计功能

1. 配置 VPLS 连接

在 PE1 与 PE2 之间配置 VPLS 连接，具体配置过程略。请参考《HUAWEI NetEngine80E/40E 路由器配置指南 VPN》中的“VPLS 配置”或者本配置举例中的配置文件。

上述配置完成后，在 PE 设备上执行命令 **display vsi name vsi-name verbose**，可以查考到 VSI 和 PW 信息。

```
<PE1>display vsi name ldpl verbose

***VSI Name           : ldpl
Administrator VSI     : no
Isolate Spoken        : disable
VSI Index             : 0
PW Signaling          : ldp
Member Discovery Style : static
PW MAC Learn Style    : unqualify
Encapsulation Type    : vlan
MTU                   : 1500
Diffserv Mode         : uniform
Service Class         : --
Color                 : --
DomainId              : 255
```

```
Domain Name           :
Ignore AcState        : disable
Create Time           : 0 days, 3 hours, 29 minutes, 53 seconds
VSI State              : up

VSI ID                 : 1
*Peer Router ID        : 2.2.2.2
primary or secondary   : primary
ignore-standby-state   : no
VC Label               : 1025
Peer Type              : dynamic
Session                : up
Tunnel ID              : 0x800003
Broadcast Tunnel ID    : 0x800003
Broad BackupTunnel ID  : 0x0
CKey                   : 2
NKey                   : 1
StpEnable              : 0
PwIndex                : 0

Interface Name         : GigabitEthernet1/0/1.1
State                  : up
Last Up Time           : 2010/10/12 14:18:39
Total Up Time          : 0 days, 1 hours, 2 minutes, 44 seconds

**PW Information:

*Peer Ip Address       : 2.2.2.2
PW State               : up
Local VC Label         : 1025
Remote VC Label        : 1025
PW Type                : label
Tunnel ID              : 0x800003
Broadcast Tunnel ID    : 0x800003
Broad BackupTunnel ID  : 0x0
Ckey                   : 0x2
Nkey                   : 0x1
Main PW Token          : 0x800003
Slave PW Token         : 0x0
Tnl Type               : LSP
OutInterface           : GigabitEthernet1/0/2
Backup OutInterface    :
Stp Enable             : 0
PW Last Up Time        : 2010/10/12 14:19:55
PW Total Up Time       : 0 days, 1 hours, 1 minutes, 28 seconds
```

2. 配置以太网 CFM 的基本功能，指定 MEP 类型为 Inward 型

在 PE 上配置以太网 CFM 的基本功能。指定以太网 CFM 协议为 Standard2007 标准版本，MD 的名称是 md1，MA 的名称是 ma1，并且配置 MA 与 VSI 绑定。

配置 PE1

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] cfm enable
[PE1] cfm version standard
[PE1] cfm md md1
[PE1-md-md1] ma ma1
[PE1-md-md1-ma-ma1] map vsi ldp1
[PE1-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet1/0/1.1 inward
[PE1-md-md1-ma-ma1] remote-mep mep-id 2
[PE1-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[PE1-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit
```

配置 PE2

```
<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] cfm enable
```

```
[PE2] cfm version standard
[PE2] cfm md md1
[PE2-md-md1] ma ma1
[PE2-md-md1-ma-ma1] map vsi ldp1
[PE2-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet1/0/1.1 inward
[PE2-md-md1-ma-ma1] remote-mep mep-id 1
[PE2-md-md1-ma-ma1] mep ccm-send mep-id 2 enable
[PE2-md-md1-ma-ma1] remote-mep ccm-receive mep-id 1 enable
[PE2-md-md1-ma-ma1] quit
[PE2-md-md1] quit
```

3. 在远端 PE2 设备上配置接收 LMM 报文功能

配置 PE2

```
[PE2-md-md1-ma-ma1] loss-measure single-ended receive peer-ip 1.1.1.1
```

4. 使能 VPLS 的按需单端丢包统计功能

配置 PE1

```
[PE1-md-md1-ma-ma1] loss-measure single-ended mep mep-id 1 mac 01-22-33
interval 1000 count 10 peer-ip 2.2.2.2
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit
```



在 PE1 上使能 VPLS 的单端丢包统计功能，配置文件中不显示相关配置命令。

5. 验证配置结果

在 PE1 执行 **display y1731 statistic-type single-loss md test ma ma1 peer-ip 2.2.2.2** 命令，可以看到单端丢包率的统计信息。

```
<PE1>display y1731 statistic-type single-loss md test ma ma1 peer-ip 2.2.2.2
Latest single-ended loss statistics:
Index  Local-loss  ratio    Remote-loss  ratio
1      20           50.0000%  30           75.0000%
2      20           50.0000%  30           75.0000%
3      20           50.0000%  30           75.0000%
4      20           50.0000%  30           75.0000%
5      20           50.0000%  30           75.0000%
6      20           50.0000%  30           75.0000%
7      20           50.0000%  30           75.0000%
8      20           50.0000%  30           75.0000%
9      20           50.0000%  30           75.0000%
10     20           50.0000%  30           75.0000%
11     20           50.0000%  30           75.0000%
12     20           50.0000%  30           75.0000%
13     20           50.0000%  30           75.0000%
14     20           50.0000%  30           75.0000%
```

----结束

配置文件

● PE1 的配置文件

```
#
sysname PE1
#
cfm version standard
cfm enable
#
mpls lsr-id 1.1.1.1
mpls
#
mpls l2vpn
#
vsi ldp1 static
pwsignal ldp
vsi-id 1
```

```

    peer 2.2.2.2
#
mpls ldp
#
interface GigabitEthernet1/0/1.1
    vlan-type dot1q 1
    l2 binding vsi ldp1
#
interface GigabitEthernet1/0/2
    undo shutdown
    ip address 100.1.1.1 255.255.255.0
    mpls
    mpls ldp
#
interface LoopBack0
    ip address 1.1.1.1 255.255.255.0
#
ospf 1
    area 0.0.0.0
        network 1.1.1.1 0.0.0.0
        network 100.1.1.0 0.0.0.255
#
cfm md md
    ma mal
        map vsi ldp1
        mep mep-id 1 interface GigabitEthernet1/0/1.1 inward
        mep ccm-send mep-id 1 enable
        remote-mep mep-id 2
        remote-mep ccm-receive mep-id 2 enable
#
return

```

● PE2 的配置文件

```

#
sysname PE2
#
cfm version standard
cfm enable
#
mpls lsr-id 2.2.2.2
mpls
#
mpls l2vpn
#
vsi ldp1 static
    pwsignal ldp
    vsi-id 1
    peer 1.1.1.1
#
mpls ldp
#
#
interface GigabitEthernet1/0/1.1
    vlan-type dot1q 2
    l2 binding vsi ldp1
#
interface GigabitEthernet1/0/2
    undo shutdown
    ip address 100.1.1.2 255.255.255.0
    mpls
    mpls ldp
#
interface LoopBack0
    ip address 2.2.2.2 255.255.255.0
#
ospf 1
    area 0.0.0.0
        network 2.2.2.2 0.0.0.0
        network 100.1.1.0 0.0.0.255
#

```

```
cfm md mdl
ma mal
map vsi ldp1
mep mep-id 2 interface GigabitEthernet1/0/1.1 inward
mep ccm-send mep-id 2 enable
remote-mep mep-id 1
remote-mep ccm-receive mep-id 1 enable
loss-measure single-ended receive peer-ip 1.1.1.1
#
return
```

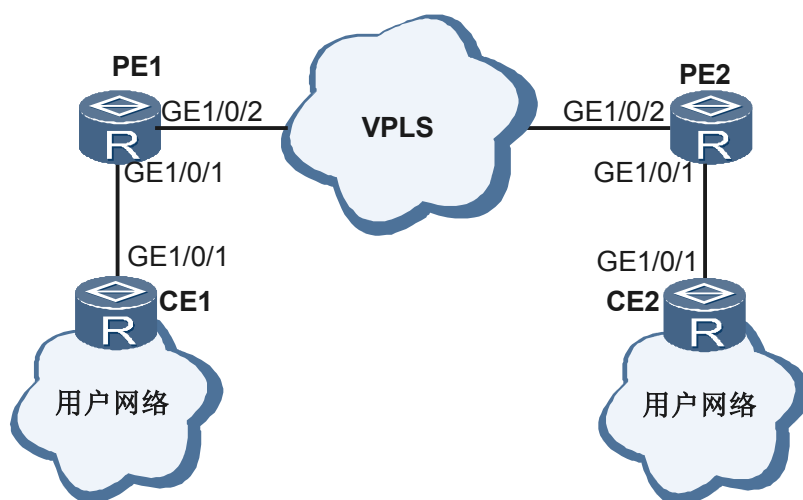
9.10.9 配置 VPLS 的双端丢包统计功能示例（连续统计）

以典型组网为例，介绍了 VPLS 组网环境下 PW 侧双端丢包统计应用。

组网需求

为了保证用户网络和运营商网络之间链路的可靠性和稳定性，提高运营商对连接链路的监控，可以在用户网络或者运营商网络上配置 Y.1731 功能。

图 9-24 VPLS 的单端丢包统计功能组网图



本举例中介绍 PW 侧双端丢包统计功能。

配置思路

采用如下的思路配置 VPLS 的双端丢包统计功能：

- 配置 PE 间 PW 侧双端丢包统计功能。

数据准备

为完成此配置例，需准备如下的数据：

- VSI name。
- PE1 与 PE2 的 MD、MA 名称。

操作步骤

步骤 1 配置 PE 间 PW 侧双端丢包统计功能。

1. 配置 VPLS 连接

在 PE1 与 PE2 之间配置 VPLS 连接，具体配置过程略。请参考《*HUAWEI NetEngine80E/40E 路由器配置指南 VPN*》中的“VPLS 配置”或者本配置举例中的配置文件。

上述配置完成后，在 PE 设备上执行命令 **display vsi name vsi-name verbose**，可以查考到 VSI 和 PW 信息。

```
<PE1>display vsi name ldp1 verbose

***VSI Name          : ldp1
  Administrator VSI   : no
  Isolate Spoken      : disable
  VSI Index           : 0
  PW Signaling        : ldp
  Member Discovery Style : static
  PW MAC Learn Style  : unqualify
  Encapsulation Type  : vlan
  MTU                  : 1500
  Diffserv Mode       : uniform
  Service Class       : --
  Color               : --
  DomainId            : 255
  Domain Name         :
  Ignore AcState      : disable
  Create Time         : 0 days, 3 hours, 29 minutes, 53 seconds
  VSI State           : up

  VSI ID              : 1
  *Peer Router ID     : 2.2.2.2
    primary or secondary : primary
    ignore-standby-state : no
  VC Label            : 1025
  Peer Type           : dynamic
  Session             : up
  Tunnel ID           : 0x800003
  Broadcast Tunnel ID : 0x800003
  Broad BackupTunnel ID : 0x0
  CKey                : 2
  NKey                : 1
  StpEnable           : 0
  PwIndex             : 0

  Interface Name      : GigabitEthernet1/0/1.1
  State               : up
  Last Up Time        : 2010/10/12 14:18:39
  Total Up Time       : 0 days, 1 hours, 2 minutes, 44 seconds

**PW Information:

  *Peer Ip Address    : 2.2.2.2
  PW State            : up
  Local VC Label      : 1025
  Remote VC Label     : 1025
  PW Type             : label
  Tunnel ID           : 0x800003
  Broadcast Tunnel ID : 0x800003
  Broad BackupTunnel ID : 0x0
  Ckey                : 0x2
  Nkey                : 0x1
  Main PW Token       : 0x800003
  Slave PW Token      : 0x0
  Tnl Type            : LSP
```

```
OutInterface      : GigabitEthernet1/0/2
Backup OutInterface :
Stp Enable        : 0
PW Last Up Time   : 2010/10/12 14:19:55
PW Total Up Time   : 0 days, 1 hours, 1 minutes, 28 seconds
```

2. 配置以太网 CFM 的基本功能，指定 MEP 类型为 Inward 型

在 PE 上配置以太网 CFM 的基本功能。指定以太网 CFM 协议为 Standard2007 标准版本，MD 的名称是 md1，MA 的名称是 ma1，并且配置 MA 与 VSI 绑定。

配置 PE1

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] cfm enable
[PE1] cfm version standard
[PE1] cfm md md1
[PE1-md-md1] ma ma1
[PE1-md-md1-ma-ma1] map vsi ldp1
[PE1-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet1/0/1.1 inward
[PE1-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[PE1-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit
```

配置 PE2

```
<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] cfm enable
[PE2] cfm version standard
[PE2] cfm md md1
[PE2-md-md1] ma ma1
[PE2-md-md1-ma-ma1] map vsi ldp1
[PE2-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet1/0/1.1 inward
[PE2-md-md1-ma-ma1] mep ccm-send mep-id 2 enable
[PE2-md-md1-ma-ma1] remote-mep ccm-receive mep-id 1 enable
[PE2-md-md1-ma-ma1] quit
[PE2-md-md1] quit
```

3. 使能 VPLS 的 PW 侧双端丢包统计功能

配置 PE1

```
[PE1-md-md1-ma-ma1] loss-measure dual-ended continual mep mep-id 1 remote-mep mep-id 2 peer-ip
2.2.2.2
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit
```

配置 PE2

```
[PE2-md-md1-ma-ma1] loss-measure dual-ended continual mep mep-id 2 remote-mep mep-id 1 peer-ip
1.1.1.1
[PE2-md-md1-ma-ma1] quit
[PE2-md-md1] quit
```

说明

在 PE 上使能 VPLS 的双丢包统计功能，配置文件中不显示相关配置命令。

4. 验证配置结果

在 PE1 执行 **display y1731 statistic-type** 命令，可以看到双端丢包率的统计信息。

```
<PE1>display y1731 statistic-type dual-loss md md1 ma ma1 peer-ip 2.2.2.2
Latest dual-ended loss statistics:
Index  Local-loss  ratio  Remote-loss  ratio
1      4294967295  100.0000%  4294967295  100.0000%
2      4294967295  100.0000%  4294967295  100.0000%
3      4294967295  100.0000%  4294967295  100.0000%
4      4294967295  100.0000%  4294967295  100.0000%
5      4294967295  100.0000%  4294967295  100.0000%
6      4294967295  100.0000%  4294967295  100.0000%
7      4294967295  100.0000%  4294967295  100.0000%
```

8	4294967295	100.0000%	4294967295	100.0000%
9	4294967295	100.0000%	4294967295	100.0000%
10	4294967295	100.0000%	4294967295	100.0000%
11	4294967295	100.0000%	4294967295	100.0000%

----结束

配置文件

- PE1 的配置文件

```
#
sysname PE1
#
cfm version standard
cfm enable
#
mpls lsr-id 1.1.1.1
mpls
#
mpls l2vpn
#
vsi ldpl static
pwsignal ldpl
vsi-id 1
peer 2.2.2.2
#
mpls ldp
#
interface GigabitEthernet1/0/1.1
vlan-type dot1q 1
l2 binding vsi ldpl
#
interface GigabitEthernet1/0/2
undo shutdown
ip address 100.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 1.1.1.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 1.1.1.1 0.0.0.0
network 100.1.1.0 0.0.0.255
#
cfm md md1
ma mal
map vsi ldpl
mep mep-id 1 interface GigabitEthernet1/0/1.1 inward
mep ccm-send mep-id 1 enable
remote-mep mep-id 2
remote-mep ccm-receive mep-id 2 enable
loss-measure dual-ended continual mep mep-id 1 remote-mep mep-id 2 peer-ip 2.2.2.2
#
return
```

- PE2 的配置文件

```
#
sysname PE2
#
cfm version standard
cfm enable
#
mpls lsr-id 2.2.2.2
mpls
```

```
#
mpls l2vpn
#
vsi ldpl static
pwsignal ldp
vsi-id 1
peer 1.1.1.1
#
mpls ldp
#
interface GigabitEthernet1/0/1.1
vlan-type dot1q 2
l2 binding vsi ldpl
#
interface GigabitEthernet1/0/2
undo shutdown
ip address 100.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 2.2.2.2 255.255.255.0
#
ospf 1
area 0.0.0.0
network 2.2.2.2 0.0.0.0
network 100.1.1.0 0.0.0.255
#
cfm md md1
ma ma1
map vsi ldpl
mep mep-id 2 interface GigabitEthernet1/0/1.1 inward
mep ccm-send mep-id 2 enable
remote-mep mep-id 1
remote-mep ccm-receive mep-id 1 enable
loss-measure dual-ended continual mep mep-id 2 remote-mep mep-id 1 peer-ip 1
.1.1.1
#
return
```

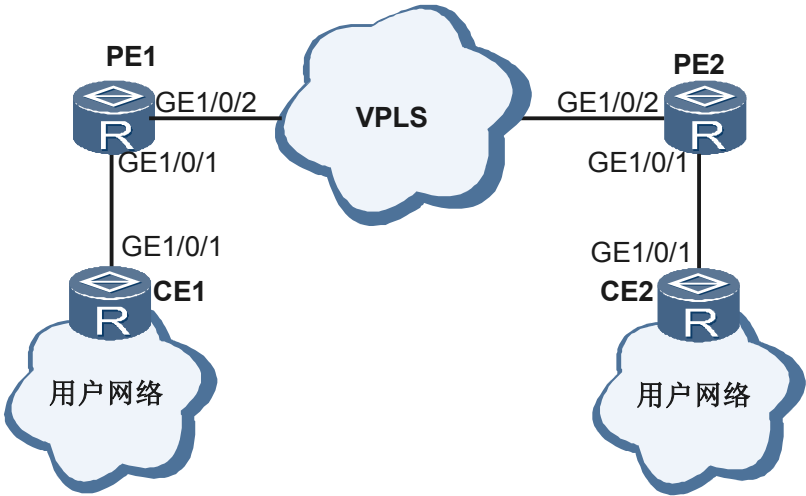
9.10.10 配置 VPLS 的单向时延计功能示例（按需统计）

以典型组网为例，介绍了 VPLS 组网环境下 PW 侧按需单向时延统计应用。

组网需求

为了保证用户网络和运营商网络之间链路的可靠性和稳定性，提高运营商对连接链路的监控，可以在用户网络或者运营商网络上配置 Y.1731 功能。

图 9-25 VPLS 的单端丢包统计功能组网图



本举例中介绍 PW 侧按需单向时延统计功能。

配置思路

采用如下的思路配置 VPLS 的按需单向时延计功能：

- 1. 配置 PE 间 PW 侧按需单向时延统计功能。

数据准备

为完成此配置例，需准备如下的数据：

- VSI name。
- 单向时延告警门限值。
- PE1 与 PE2 的 MD、MA 名称。

操作步骤

步骤 1 配置 PE 间 PW 侧单向时延统计功能。

- 1. 配置 VPLS 连接
在 PE1 与 PE2 之间配置 VPLS 连接，具体配置过程略。请参考《HUAWEI NetEngine80E/40E 路由器配置指南 VPN》中的“VPLS 配置”或者本配置举例中的配置文件。
上述配置完成后，在 PE 设备上执行命令 **display vsi name vsi-name verbose**，可以查考到 VSI 和 PW 信息。

```
<PE1>display vsi name ldpl verbose

***VSI Name           : ldpl
Administrator VSI     : no
Isolate Spoken        : disable
VSI Index             : 0
PW Signaling          : ldp
Member Discovery Style : static
PW MAC Learn Style    : unqualify
Encapsulation Type    : vlan
```

```
MTU : 1500
Diffserv Mode : uniform
Service Class : --
Color : --
DomainId : 255
Domain Name :
Ignore AcState : disable
Create Time : 0 days, 3 hours, 29 minutes, 53 seconds
VSI State : up

VSI ID : 1
*Peer Router ID : 2.2.2.2
primary or secondary : primary
ignore-standby-state : no
VC Label : 1025
Peer Type : dynamic
Session : up
Tunnel ID : 0x800003
Broadcast Tunnel ID : 0x800003
Broad BackupTunnel ID : 0x0
CKey : 2
NKey : 1
StpEnable : 0
PwIndex : 0

Interface Name : GigabitEthernet1/0/1.1
State : up
Last Up Time : 2010/10/12 14:18:39
Total Up Time : 0 days, 1 hours, 2 minutes, 44 seconds

**PW Information:

*Peer Ip Address : 2.2.2.2
PW State : up
Local VC Label : 1025
Remote VC Label : 1025
PW Type : label
Tunnel ID : 0x800003
Broadcast Tunnel ID : 0x800003
Broad BackupTunnel ID : 0x0
Ckey : 0x2
Nkey : 0x1
Main PW Token : 0x800003
Slave PW Token : 0x0
Tnl Type : LSP
OutInterface : GigabitEthernet1/0/2
Backup OutInterface :
Stp Enable : 0
PW Last Up Time : 2010/10/12 14:19:55
PW Total Up Time : 0 days, 1 hours, 1 minutes, 28 seconds
```

2. 配置以太网 CFM 的基本功能，指定 MEP 类型为 Inward 型

在 PE 上配置以太网 CFM 的基本功能。指定以太网 CFM 协议为 Standard2007 标准版本，MD 的名称是 md1，MA 的名称是 mal，并且配置 MA 与 VSI 绑定。

配置 PE1

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] cfm enable
[PE1] cfm version standard
[PE1] cfm md md1
[PE1-md-md1] ma mal
[PE1-md-md1-ma-mal] map vsi ldp1
[PE1-md-md1-ma-mal] mep mep-id 1 interface gigabitethernet1/0/1.1 inward
[PE1-md-md1-ma-mal] remote-mep mep-id 2
[PE1-md-md1-ma-mal] mep ccm-send mep-id 1 enable
[PE1-md-md1-ma-mal] remote-mep ccm-receive mep-id 2 enable
[PE1-md-md1-ma-mal] quit
[PE1-md-md1] quit
```

配置 PE2

```
<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] cfm enable
[PE2] cfm version standard
[PE2] cfm md md1
[PE2-md-md1] ma ma1
[PE2-md-md1-ma-ma1] map vsi ldp1
[PE2-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet1/0/1.1 inward
[PE2-md-md1-ma-ma1] remote-mep mep-id 1
[PE2-md-md1-ma-ma1] mep ccm-send mep-id 2 enable
[PE2-md-md1-ma-ma1] remote-mep ccm-receive mep-id 1 enable
[PE2-md-md1-ma-ma1] quit
[PE2-md-md1] quit
```

3. 在远端 PE2 设备上配置接收 DMM 报文功能

配置 PE2

```
[PE2-md-md1-ma-ma1]delay-measure one-way receive peer-ip 1.1.1.1
```

4. 使能 VPLS 的单向时延统计功能

在 PE1 上使能 VPLS 的单向时延统计功能，发包间隔为 1 秒。

配置 PE1

```
[PE1-md-md1-ma-ma1]delay-measure one-way mep mep-id 1 mac 1-1-1 interval 1000 count 20 peer-
ip 2.2.2.2
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit
```

5. 验证配置结果

在 PE2 上执行 **display y1731 statistic-type** 命令，可以看到时延值。

```
<PE2> display Y.1731 statistic-type oneway-delay md md1 ma ma1 peer-ip 1.1.1.1
Latest one-way delay statistics:
Index  One-way delay(usec) Delay variation(usec)
1      10000                0
2      10000                0
3      20000               10000
4      20000                0
5      10000               10000
6      10000                0
7      20000               10000
8      20000                0
9      30000               10000
10     10000               20000
11     20000               10000
12     20000                0
13     10000               10000
14     20000               10000
15     20000                0
16     20000                0
17     20000                0
18     30000               10000
19     10000               20000
20     10000                0
21     10000                0
22     20000               10000
23     20000                0
24     20000                0
25     30000               10000
26     10000               20000
27     10000                0
28     10000                0
29     10000                0
30     50000               40000
31     10000               40000
32     10000                0
33     20000               10000
34     20000                0
```

35	20000	0
36	20000	0
37	10000	10000
38	20000	10000
39	20000	0
40	20000	0

----结束

配置文件

● PE1 的配置文件

```
#
sysname PE1
#
cfm version standard
cfm enable
#
mpls lsr-id 1.1.1.1
mpls
#
mpls l2vpn
#
vsi ldpl static
pwsignal ldp
vsi-id 1
peer 2.2.2.2
#
mpls ldp
#
interface GigabitEthernet1/0/1.1
vlan-type dot1q 1
l2 binding vsi ldpl
#
interface GigabitEthernet1/0/2
undo shutdown
ip address 100.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 1.1.1.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 1.1.1.1 0.0.0.0
network 100.1.1.0 0.0.0.255
#
cfm md md1
ma mal
map vsi ldpl
ccm-interval 10
mep mep-id 1 interface GigabitEthernet1/0/1.1 inward
mep ccm-send mep-id 1 enable
remote-mep mep-id 2
remote-mep ccm-receive mep-id 2 enable
delay-measure one-way receive
#
return
```

● PE2 的配置文件

```
#
sysname PE2
#
cfm version standard
cfm enable
#
```



```
mpls lsr-id 2.2.2.2
mpls
#
mpls l2vpn
#
vsi ldpl static
pwsignal ldpl
vsi-id 1
peer 1.1.1.1
#
mpls ldp
#
interface GigabitEthernet1/0/1.1
vlan-type dot1q 2
l2 binding vsi ldpl
#
interface GigabitEthernet1/0/2
undo shutdown
ip address 100.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 2.2.2.2 255.255.255.0
#
ospf 1
area 0.0.0.0
network 2.2.2.2 0.0.0.0
network 100.1.1.0 0.0.0.255
#
cfm md md1
ma mal
map vsi ldpl
ccm-interval 10
mep mep-id 2 interface GigabitEthernet1/0/1.1 inward
mep ccm-send mep-id 2 enable
remote-mep mep-id 1
remote-mep ccm-receive mep-id 1
enable
#
return
```

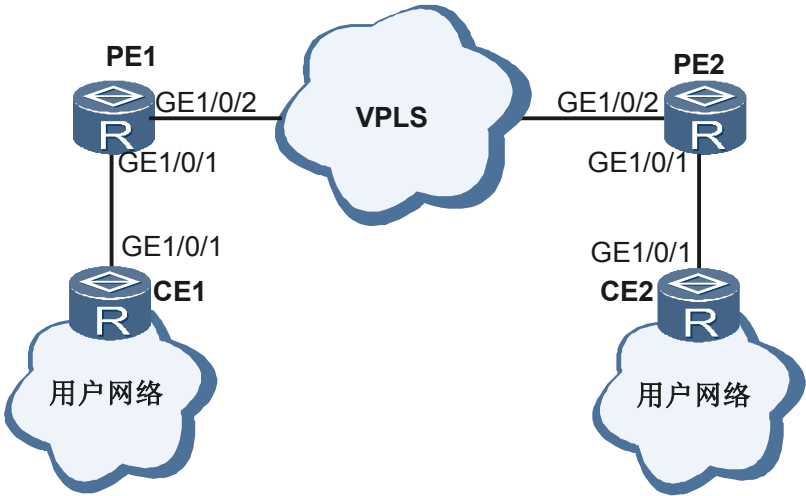
9.10.11 配置 VPLS 的双向时延计功能示例（按需统计）

以典型组网为例，介绍 VPLS 组网环境下 PW 侧按需双向时延统计应用。

组网需求

为了保证用户网络和运营商网络之间链路的可靠性和稳定性，提高运营商对连接链路的监控，可以在用户网络或者运营商网络上配置 Y.1731 功能。

图 9-26 VPLS 的单端丢包统计功能组网图



本举例中介绍 VPLS 组网环境下 PW 侧按需双向时延统计功能。

配置思路

采用如下的思路配置 VPLS 的按需双向时延统计功能：

- 1. 配置 PE 间 PW 侧按需双向时延统计功能。

数据准备

为完成此配置例，需准备如下的数据：

- VSI name。
- 单向时延告警门限值。
- PE1 与 PE2 的 MD、MA 名称。

操作步骤

步骤 1 配置 PE 间 PW 侧双向时延统计功能

- 1. 配置 VPLS 连接
在 PE1 与 PE2 之间配置 VPLS 连接，具体配置过程略。请参考《HUAWEI NetEngine80E/40E 路由器配置指南 VPN》中的“VPLS 配置”或者本配置举例中的配置文件。
上述配置完成后，在 PE 设备上执行命令 **display vsi name vsi-name verbose**，可以查考到 VSI 和 PW 信息。

```
<PE1>display vsi name ldpl verbose

***VSI Name           : ldpl
Administrator VSI     : no
Isolate Spoken        : disable
VSI Index             : 0
PW Signaling          : ldp
Member Discovery Style : static
PW MAC Learn Style    : unqualify
Encapsulation Type    : vlan
```

```
MTU : 1500
Diffserv Mode : uniform
Service Class : --
Color : --
DomainId : 255
Domain Name :
Ignore AcState : disable
Create Time : 0 days, 3 hours, 29 minutes, 53 seconds
VSI State : up

VSI ID : 1
*Peer Router ID : 2.2.2.2
primary or secondary : primary
ignore-standby-state : no
VC Label : 1025
Peer Type : dynamic
Session : up
Tunnel ID : 0x800003
Broadcast Tunnel ID : 0x800003
Broad BackupTunnel ID : 0x0
CKey : 2
NKey : 1
StpEnable : 0
PwIndex : 0

Interface Name : GigabitEthernet1/0/1.1
State : up
Last Up Time : 2010/10/12 14:18:39
Total Up Time : 0 days, 1 hours, 2 minutes, 44 seconds

**PW Information:

*Peer Ip Address : 2.2.2.2
PW State : up
Local VC Label : 1025
Remote VC Label : 1025
PW Type : label
Tunnel ID : 0x800003
Broadcast Tunnel ID : 0x800003
Broad BackupTunnel ID : 0x0
Ckey : 0x2
Nkey : 0x1
Main PW Token : 0x800003
Slave PW Token : 0x0
Tnl Type : LSP
OutInterface : GigabitEthernet1/0/2
Backup OutInterface :
Stp Enable : 0
PW Last Up Time : 2010/10/12 14:19:55
PW Total Up Time : 0 days, 1 hours, 1 minutes, 28 seconds
```

2. 配置以太网 CFM 的基本功能，指定 MEP 类型为 Inward 型

在 PE 上配置以太网 CFM 的基本功能。指定以太网 CFM 协议为 Standard2007 标准版本，MD 的名称是 md1，MA 的名称是 ma1，并且配置 MA 与 VSI 绑定。

配置 PE1

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] cfm enable
[PE1] cfm version standard
[PE1] cfm md md1
[PE1-md-md1] ma ma1
[PE1-md-md1-ma-ma1] map vsi ldp1
[PE1-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet1/0/1.1 inward
[PE1-md-md1-ma-ma1] remote-mep mep-id 2
[PE1-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[PE1-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
```

配置 PE2

```
<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] cfm enable
[PE2] cfm version standard
[PE2] cfm md md1
[PE2-md-md1] ma ma1
[PE2-md-md1-ma-ma1] map vsi ldp1
[PE2-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet1/0/1.1 inward
[PE2-md-md1-ma-ma1] remote-mep mep-id 1
[PE2-md-md1-ma-ma1] mep ccm-send mep-id 2 enable
[PE2-md-md1-ma-ma1] remote-mep ccm-receive mep-id 1 enable
```

3. 配置远端 PE2 设备接收 DMM 报文功能

配置 PE2

```
[PE2-md-md1-ma-ma1] delay-measure two-way receive peer-ip 1.1.1.1
[PE2-md-md1-ma-ma1] quit
[PE2-md-md1] quit
```

4. 使能 VPLS 的双向时延统计功能

配置 PE1

```
[PE1-md-md1-ma-ma1] delay-measure two-way mep mep-id 101 mac 1-1-1 interval
1 1000 count 20 peer-ip 2.2.2.2
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit
```

5. 检查配置结果

在 PE1 执行 **display y1731 statistic-type** 命令，可以看到双向时延的统计信息。

```
<PE1> display y1731 statistic-type twoway-delay md md ma ma1 peer-ip 2.2.2.2
Latest two-way delay statistics:
Index  Two-way delay(usec) Delay variation(usec)
1      30000                0
2      40000                10000
3      10000                30000
4      40000                30000
5      30000                10000
6      40000                10000
7      10000                30000
8      10000                0
9      0                   10000
10     30000                30000
11     0                   30000
12     10000                10000
13     0                   10000
14     40000                40000
15     20000                20000
16     10000                10000
17     40000                30000
18     10000                30000
```

----结束

配置文件

● PE1 的配置文件

```
#
sysname PE1
#
cfm version standard
cfm enable
#
mpls lsr-id 1.1.1.1
mpls
#
mpls l2vpn
#
```

```
vsi ldp1 static
 pwsignal ldp
  vsi-id 1
  peer 2.2.2.2
#
mpls ldp
#
interface GigabitEthernet1/0/1.1
 vlan-type dot1q 1
 l2 binding vsi ldp1
#
interface GigabitEthernet1/0/2
 undo shutdown
 ip address 100.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 100.1.1.0 0.0.0.255
#
cfm md md1
 ma mal
 map vsi ldp1
 ccm-interval 10
 mep mep-id 1 interface GigabitEthernet1/0/1.1 inward
 mep ccm-send mep-id 1 enable
 remote-mep mep-id 2
 remote-mep ccm-receive mep-id 2
enable
#
return
```

● PE2 的配置文件

```
#
 sysname PE2
#
 cfm version standard
 cfm enable
#
 mpls lsr-id 2.2.2.2
 mpls
#
 mpls l2vpn
#
vsi ldp1 static
 pwsignal ldp1
  vsi-id 1
  peer 1.1.1.1
#
mpls ldp
#
interface GigabitEthernet1/0/1.1
 vlan-type dot1q 2
 l2 binding vsi ldp1
#
interface GigabitEthernet1/0/2
 undo shutdown
 ip address 100.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.0
#
ospf 1
```

```
area 0.0.0.0
 network 2.2.2.2 0.0.0.0
 network 100.1.1.0 0.0.0.255
#
 cfm md md1
  ma mal
  map vsi ldp1
  mep mep-id 2 interface GigabitEthernet1/0/1.1 inward
  mep ccm-send mep-id 2 enable
  remote-mep mep-id 1
  remote-mep ccm-receive mep-id 1
enable
 delay-measure two-way receive peer-ip 1.1.1.1
#
return
```

9.10.12 配置基于 QoS 简单流分类的 Y.1731 统计功能示例

通过在 PE 上设置不同的优先级映射关系，将报文的业务优先级进行更改或者重新分类，从而更加灵活的统计 PW 侧的丢包或者时延。本示例对基于 QoS 简单流分类的 Y.1731 统计功能进行详细介绍，配置示例包括组网需求、思路准备、操作步骤和配置文件。

组网需求

说明

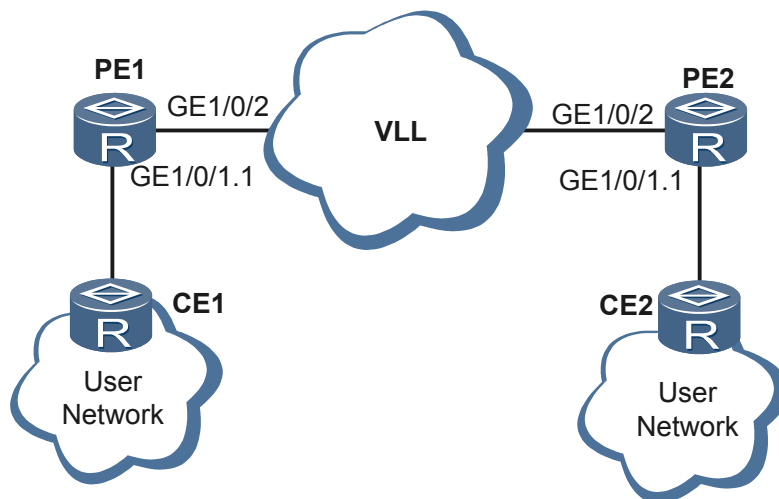
仅 VLL 的单端丢包统计、单向时延统计和双向时延统计功能支持配置基于 QoS 简单流分类的 Y.1731 统计功能。

此示例以配置 VLL 的单端丢包统计功能（连续统计）为例进行介绍，VLL 的单向时延、双向时延功能的配置方式类似。

如图 9-27 所示，在 PE 上通过配置 QoS 简单流分类，可以将一种网络流量中的优先级映射到另外一种网络流量中，使流量在另外一种网络中按照原来的或用户配置的优先级传送。所有进入 PE 的报文，其原先的外部优先级标记将被映射为内部优先级（以 QoS 服务等级和颜色表示）；PE 发出报文时，将内部优先级映射为某种外部业务优先级。

路由器可以基于指定的优先级对链路进行丢包或者时延统计。当需要在 PW 侧进行基于指定优先级的丢包或者时延统计，就能通过在 PE 上设置不同的优先级映射关系，将报文的业务优先级进行更改或者重新分类，从而更加灵活的统计 PW 侧的丢包或者时延。

图 9-27 VLL 的 Y.1731 组网图



配置思路

- 采用如下的思路配置：
- 配置 QoS 简单流分类。
 - 配置 PE 间的 VLL 功能。
 - 配置 PW 链路 CFM 基本功能。
 - 配置 PW 链路连续单端丢包统计功能。

数据准备

- 为完成此配置例，需准备如下的数据：
- DS 域下的优先级映射关系。
 - VC ID。
 - PE1 与 PE2 的 MD、MA 名称。

操作步骤

步骤 1 配置 VLAN 报文 802.1p 优先级和 QoS 服务等级、颜色之间的映射关系

配置步骤详见《HUAWEI NetEngine80E/40E 路由器配置指南 QoS》中的[配置 VLAN 报文的优先级映射](#)，此处不赘述，具体配置结果请参见配置文件。

 说明

在 PE1 和 PE2 的 AC 侧子接口上应用流量策略。
主接口上只能绑定 DS 域，并不能使能根据 802.1p 的简单流分类，802.1p 优先级的映射关系将继承 IP 报文的 DSCP 值和 QoS 服务等级、颜色之间的映射关系。

本例使用的 DS 域 AC 的上行 VLAN 报文的 802.1p 的值与路由器内部的服务等级的对应关系如下：

表 9-10 DS 域 AC 的上行 VLAN 报文的 802.1p 的值与路由器内部的服务等级的对应关系

802.1p	Service	Color
0	be	green
1	be	green
2	be	green
3	af2	green
4	af3	green
5	af4	green
6	ef	green
7	be	green

本例使用的 DS 域 AC 的下行 VLAN 报文在路由器内部的服务等级和报文颜色对应路由器外部的 802.1p 的值如下：

表 9-11 DS 域 AC 的下行 VLAN 报文在路由器内部的服务等级和报文颜色对应路由器外部的 802.1p 的值

QoS 服务等级	Color	802.1p 优先级
BE	green	0
AF1	green、yellow、red	1
AF2	green	3
AF2	yellow、red	2
AF3	green	4
AF3	yellow、red	3
AF4	green	5
AF4	yellow、red	4
EF	green	6
CS6	green	6
CS7	green	7

步骤 2 配置 MPLS 报文的 EXP 值和 QoS 服务等级、颜色之间的映射关系

配置步骤详见《HUAWEI NetEngine80E/40E 路由器配置指南 QoS》中的[配置 MPLS 报文的优先级映射](#)，此处不赘述，具体配置结果请参见配置文件。

说明

在 PE1 和 PE2 的 PW 侧接口上绑定 DS 域，使能简单流分类。

本例使用的 DS 域 PW 的上行 MPLS 报文 EXP 域值和路由器内部服务等级的对应关系如下：

表 9-12 DS 域 PW 的上行 MPLS 报文 EXP 域值和路由器内部服务等级的对应关系

EXP	Service	Color
0	be	green
1	af1	green
2	af2	green
3	af3	green
4	af4	green
5	ef	green
6	cs7	green

EXP	Service	Color
7	cs7	green

本例使用的 DS 域 PW 的下行报文的服务等级和颜色标记对应的 EXP 域值如下：

表 9-13 DS 域 PW 的下行报文的服务等级和颜色标记对应的 EXP 域值

Service	Color	MPLS EXP
BE	green	0
AF1	green、yellow、red	1
AF2	green、yellow、red	2
AF3	green、yellow、red	3
AF4	green、yellow、red	4
EF	green	5
CS6	green	6
CS7	green	6

步骤 3 配置 VLL 连接

在 PE1 与 PE2 之间配置 VLL 连接，具体配置过程略。请参考《HUAWEI NetEngine80E/40E 路由器 配置指南 VPN》中的“VLL 配置”或者本配置举例中的配置文件。

上述配置完成后，在 PE 设备上执行命令 **display mpls l2vc**，可以查看到 VC 和 AC 链路信息。

```
<PE1>display mpls l2vc
total LDP VC : 1      1 up      0 down

*client interface      : GigabitEthernet1/0/1.1
Administrator PW      : no
session state         : up
AC status             : up
VC state              : up
Label state           : 0
Token state           : 0
VC ID                 : 2
VC type               : VLAN
destination            : 2.2.2.2
local VC label        : 1027      remote VC label      : 1025
control word          : disable
forwarding entry       : exist
local group ID        : 0
manual fault          : not set
active state          : active
link state             : up
local VC MTU          : 1500      remote VC MTU       : 1500
tunnel policy name    : --
traffic behavior name : --
PW template name      : --
```

```
primary or secondary : primary
create time          : 0 days, 0 hours, 1 minutes, 12 seconds
up time              : 0 days, 0 hours, 0 minutes, 42 seconds
last change time     : 0 days, 0 hours, 0 minutes, 42 seconds
VC last up time      : 2010/10/13 15:02:23
VC total up time     : 0 days, 0 hours, 0 minutes, 42 seconds
CKey                 : 4
NKey                 : 3
AdminPw interface    : --
AdminPw link state   : --
```

步骤 4 配置以太网 CFM 的基本功能，指定 MEP 类型为 Inward 型

在 PE 上配置以太网 CFM 的基本功能。指定以太网 CFM 协议为 Standard2007 标准版本，MD 的名称是 md1，MA 的名称是 ma1，并且配置 MA 与 VLL 绑定。

配置 PE1

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] cfm enable
[PE1] cfm version standard
[PE1] cfm md md1
[PE1-md-md1] ma ma1
[PE1-md-md1-ma-ma1] map mpls l2vc 2 tagged
[PE1-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet1/0/1.1 inward
[PE1-md-md1-ma-ma1] remote-mep mep-id 2
[PE1-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[PE1-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit
```

配置 PE2

```
<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] cfm enable
[PE2] cfm version standard
[PE2] cfm md md1
[PE2-md-md1] ma ma1
[PE2-md-md1-ma-ma1] map mpls l2vc 2 tagged
[PE2-md-md1-ma-ma1] mep mep-id 2 interface gigabitethernet1/0/1.1 inward
[PE2-md-md1-ma-ma1] remote-mep mep-id 1
[PE2-md-md1-ma-ma1] mep ccm-send mep-id 2 enable
[PE2-md-md1-ma-ma1] remote-mep ccm-receive mep-id 1 enable
[PE2-md-md1-ma-ma1] quit
[PE2-md-md1] quit
```

步骤 5 在远端 PE2 设备上配置接收 LMM 报文功能

配置 PE2

```
[PE2-md-md1-ma-ma1] loss-measure single-ended receive 8021p 0
```

步骤 6 使能 VLL 的连续单端丢包统计功能

配置 PE1

```
[PE1-md-md1-ma-ma1] loss-measure single-ended continual mep mep-id 1 mac 0001-0001-0001 interval
30000 8021p 0
[PE1-md-md1-ma-ma1] quit
[PE1-md-md1] quit
```

步骤 7 验证配置结果

在 PE1 执行 **display y1731 statistic-type** 命令，可以看到单端丢包率的统计信息。

```
<PE1> display y1731 statistic-type single-loss md md1 ma ma1
Latest single-ended loss statistics of 802.1p 0:
```

Index	Local-loss	ratio	Remote-loss	ratio
1	20	50.0000%	30	75.0000%
2	20	50.0000%	30	75.0000%
3	20	50.0000%	30	75.0000%
4	20	50.0000%	30	75.0000%
5	20	50.0000%	30	75.0000%
6	20	50.0000%	30	75.0000%
7	20	50.0000%	30	75.0000%
8	20	50.0000%	30	75.0000%
9	20	50.0000%	30	75.0000%
10	20	50.0000%	30	75.0000%
11	20	50.0000%	30	75.0000%
12	20	50.0000%	30	75.0000%
13	20	50.0000%	30	75.0000%
14	20	50.0000%	30	75.0000%
15	20	50.0000%	30	75.0000%
16	20	50.0000%	30	75.0000%
17	20	50.0000%	30	75.0000%
18	20	50.0000%	30	75.0000%
19	20	50.0000%	30	75.0000%
20	20	50.0000%	30	75.0000%

----结束

配置文件

- PE1 的配置文件

```
#
sysname PE1
#
diffserv domain AC
8021p-inbound 1 phb be green
8021p-inbound 2 phb be green
8021p-inbound 3 phb af2 green
8021p-inbound 4 phb af3 green
8021p-inbound 5 phb af4 green
8021p-inbound 6 phb ef green
8021p-inbound 7 phb be green
8021p-outbound af2 green map 3
8021p-outbound af3 green map 4
8021p-outbound af4 green map 5
8021p-outbound ef green map 6
#
diffserv domain PW
8021p-inbound 1 phb be green
8021p-inbound 2 phb be green
8021p-inbound 3 phb af1 green
8021p-inbound 4 phb af1 green
8021p-inbound 6 phb be green
8021p-inbound 7 phb be green
8021p-outbound be green map 7
8021p-outbound af1 green map 3
8021p-outbound af2 green map 3
8021p-outbound af4 green map 3
8021p-outbound cs7 green map 5
mpls-exp-inbound 6 phb cs7 green
mpls-exp-outbound cs7 green map 6
#
cfm version standard
#
cfm enable
#
mpls lsr-id 1.1.1.1
mpls
#
mpls l2vpn
#
```

```
mpls ldp
#
interface GigabitEthernet1/0/1.1
vlan-type dot1q 2
mpls l2vc 2.2.2.2 2
trust upstream AC
trust 8021p
#
interface GigabitEthernet1/0/2
undo shutdown
ip address 100.1.1.1 255.255.255.0
mpls
mpls ldp
trust upstream PW
#
interface LoopBack0
ip address 1.1.1.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 1.1.1.1 0.0.0.0
network 100.1.1.0 0.0.0.255
#
cfm md md1
ma ma1
map mpls l2vc 2 tagged
mep mep-id 1 interface GigabitEthernet1/0/1.1 inward
mep ccm-send mep-id 1 enable
remote-mep mep-id 2
remote-mep ccm-receive mep-id 2 enable
loss-measure single-ended continual mep mep-id 1 mac 0001-0001-0001 interval 30000 8021p 0
#
return
```

● PE2 的配置文件

```
#
sysname PE2
#
diffserv domain AC
8021p-inbound 1 phb be green
8021p-inbound 2 phb be green
8021p-inbound 3 phb af2 green
8021p-inbound 4 phb af3 green
8021p-inbound 5 phb af4 green
8021p-inbound 6 phb ef green
8021p-inbound 7 phb be green
8021p-outbound af2 green map 3
8021p-outbound af3 green map 4
8021p-outbound af4 green map 5
8021p-outbound ef green map 6
#
diffserv domain PW
8021p-inbound 1 phb be green
8021p-inbound 2 phb be green
8021p-inbound 3 phb af1 green
8021p-inbound 4 phb af1 green
8021p-inbound 6 phb be green
8021p-inbound 7 phb be green
8021p-outbound be green map 7
8021p-outbound af1 green map 3
8021p-outbound af2 green map 3
8021p-outbound af4 green map 3
8021p-outbound cs7 green map 5
mpls-exp-inbound 6 phb cs7 green
mpls-exp-outbound cs7 green map 6
#
cfm version standard
cfm enable
#
mpls lsr-id 2.2.2.2
```

```
mpls
#
mpls l2vpn
#
mpls ldp
#
#
interface GigabitEthernet1/0/1.1
vlan-type dot1q 2
mpls l2vc 1.1.1.1 2
trust upstream AC
trust 8021p
#
interface GigabitEthernet1/0/2
undo shutdown
ip address 100.1.1.2 255.255.255.0
mpls
mpls ldp
trust upstream PW
#
interface LoopBack0
ip address 2.2.2.2 255.255.255.0
#
ospf 1
area 0.0.0.0
network 2.2.2.2 0.0.0.0
network 100.1.1.0 0.0.0.255
#
cfm md md1
ma mal
map mpls l2vc 2 tagged
mep mep-id 2 interface GigabitEthernet1/0/1.1 inward
mep ccm-send mep-id 2 enable
remote-mep mep-id 1
remote-mep ccm-receive mep-id 1 enable
loss-measure single-ended receive 8021p 0
#
return
```

10 MPLS-TP OAM 配置

关于本章

介绍了 MPLS-TP OAM（Multiprotocol Label Switching Transport Profile Operation Administration & Maintenance）的基本原理，CC/CV，LB/LT，AIS，RDI 和 LM/DM 功能的配置过程和典型配置举例。

10.1 MPLS-TP OAM 简介

MPLS-TP OAM（Operation Administration & Maintenance）机制用于 MPLS-TP 的运维管理。

10.2 配置 LSP 的 MPLS-TP OAM 功能

NE80E/40E 提供的 MPLS-TP OAM 支持对双向 LSP 链路进行检测。

10.3 配置 PW 的 MPLS-TP OAM 功能

NE80E/40E 提供的 MPLS-TP OAM 支持对基于双向 LSP 的 PW 链路进行检测。

10.4 配置举例

配置举例结合组网需求、配置思路和数据准备例举了 MPLS-TP OAM 的典型应用场景，并提供配置文件。

10.1 MPLS-TP OAM 简介

MPLS-TP OAM（Operation Administration & Maintenance）机制用于 MPLS-TP 的运维管理。

10.1.1 MPLS-TP OAM 概述

MPLS-TP OAM 可以有效检测、识别和定位 MPLS-TP 用户层面故障；在链路或节点出现缺陷或故障时迅速进行保护倒换。运维管理 OAM（Operation Administration & Maintenance）是降低网络维护成本的有效手段，MPLS-TP OAM 机制用于 MPLS-TP 层的运维管理。

MPLS-TP OAM 产生

随着网络和业务的转型和融合，各种新兴的业务，例如三重播放、NGN、电信级以太网（Carrier Ethernet）、FTTx 等，都对传送网络的投资成本、运维成本、QoS 保证、全业务接入、网络扩展性、网络可靠性和网络可管理性等提出了更高的要求。然而传统的传送网（MSTP，SDH，WDM）等技术缺乏控制平面，不能适应这些新的需求。MPLS-TP 具有传送网特性、又支持分组业务处理能力的下一代分组传送网来满足这些需求。

由于传统的传送网络（如 SDH/OTN）在可靠性和运维这两个方面树立了一个很高的基准，因此 MPLS-TP 需要提供完善的 OAM 能力。简单来说，MPLS-TP OAM 主要包括三个方面：

- 故障管理（Fault Management）
- 性能监控（Performance Monitoring）
- 保护倒换（Protection Switching）

MPLS-TP OAM 功能组件

MPLS-TP OAM 的功能操作均基于维护实体 ME（Maintenance Entity）进行。一个 ME 可以简单地理解为一条传送路径的两个端点，即一对 MEP（Maintenance Entity Group End Points），以及传送路径在这两个端点之间经过的中间节点，即一组 MIP（Maintenance Entity Group Intermediate Points）。

下面对 MPLS-TP OAM 的功能组件进行详细介绍：

- 维护实体（ME）

ME 代表需要管理的一个实体，它是两个维护实体组端点之间的一种关系。在双向 LSP 网络中的两个 ME 可以同时进行 MPLS-TP OAM 检测，互不干扰。ME 可以相互嵌套，但不能重叠。

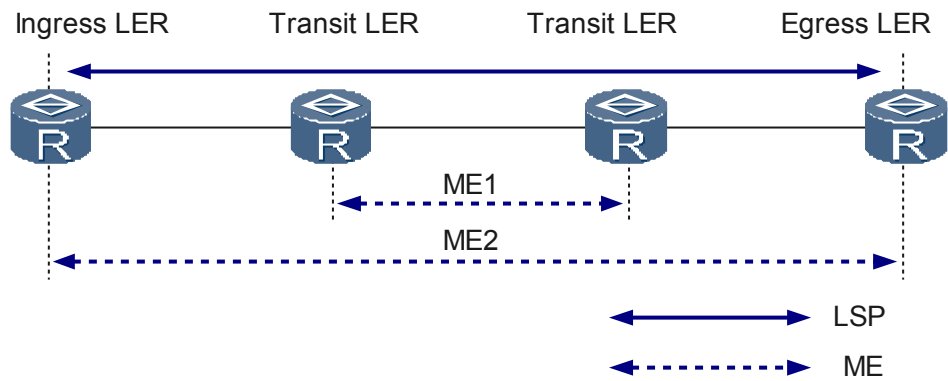
如图 10-1 所示，以 ME1 和 ME2 为例：

- ME1 由两个 MEP 节点组成，不包含 MIP 节点
- ME2 由两个 MEP 节点和两个 MIP 节点组成

 说明

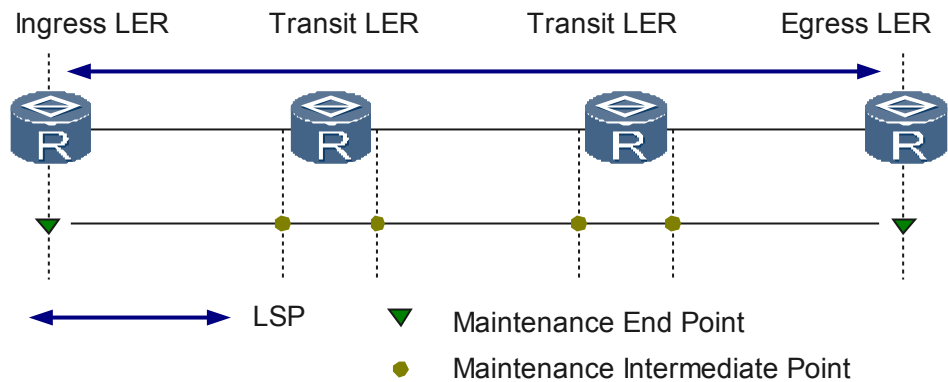
NE80E/40E 暂未实现 Transit 节点之间的 ME 部署，即不支持 ME1。

图 10-1 点到点双向 LSP 的 ME 部署示意图



- ME 组（MEG）
一个或者多个属于同一条传送路径的 ME 构成一个维护实体组 MEG（Maintenance Entity Group）。对于双向共路 LSP/PW 的点到点双向路径时，MEG 只包含一个 ME。
- MEG 端点（MEP）
如图 10-2 所示，MEP 是 MEG 的源、宿点。

图 10-2 ME 的节点部署示意图



- 对于一条双向 LSP 来说，只有 LER 才能作为 MEP，如图 10-1 所示，只有 Ingress LER 和 Egress LER 可以作为 MEP。
 - 对于 MPLS-TP PW，只有 UPE 可以作为 MEP。
- MEP 用来触发和控制 MPLS-TP OAM 的操作，它可以产生和终结 OAM 报文。

10.1.2 NE80E/40E 支持的 MPLS-TP OAM 特性

MPLS-TP OAM 支持性能检测和故障检测功能。

NE80E/40E 支持的 MPLS-TP OAM 故障管理功能

如表 10-1 所示，MPLS-TP OAM 支持连通性故障检测和告警抑制功能。

表 10-1 MPLS-TP OAM 故障管理功能表

功能类型	功能说明
CC（Continuity Check）	连通性持续检测
CV（Connectivity Verification）	转发故障持续检测
LB（Loopback Function）	环回检测
RDI（Remote Defect Indication）	远端缺陷通告
AIS（Alarm Indication Signal）	服务层告警指示

NE80E/40E 支持的 MPLS-TP OAM 性能管理功能

如表 10-2 所示，MPLS-TP OAM 支持丢包和时延统计功能。

表 10-2 MPLS-TP OAM 性能管理功能

功能类型	功能说明
LM（Loss Measurement）	丢包率统计： ● 单端丢包统计 ● 双端丢包统计
DM（Delay Measurement）	时延和时延抖动统计： ● 单向时延和时延抖动统计 ● 双向时延和时延抖动统计

10.2 配置 LSP 的 MPLS-TP OAM 功能

NE80E/40E 提供的 MPLS-TP OAM 支持对双向 LSP 链路进行检测。

10.2.1 建立配置任务

MPLS-TP OAM 可用于检测 LSP。配置 MPLS-TP OAM 前，需要先创建 LSP。以下说明配置 OAM 的基本检测功能的应用环境、前置任务、数据准备、配置过程。

应用环境

MPLS-TP 已经开始广泛应用于传送网络，但由于传统的传送网络（如 SDH/OTN）在可靠性和运维这两个方面树立了一个很高的基准，因此 MPLS-TP 需要提供完善的 OAM 能力。

对于双向 LSP 网络，MPLS-TP OAM 可以对其故障进行管理，同时对各项性能指标进行统计。如图 10-3 所示，以 Ingress LER 作为本端 MEP，Egress LER 作为对端 MEP，Transit LER 作为MIP 端点进行 MPLS-TP OAM 配置，可以实现如表 10-3 所示的各项 MPLS-TP OAM 功能。

图 10-3 双向 LSP 组网图

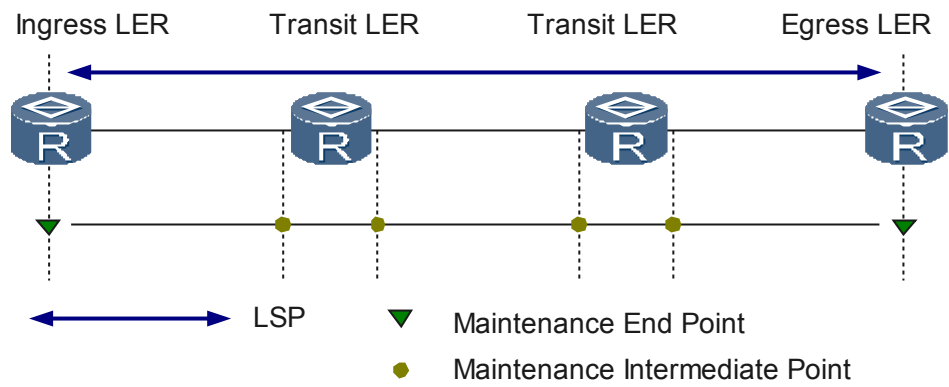


表 10-3 NE80E/40E 支持 MPLS-TP OAM 功能表

MPLS-TP OAM 功能类型	检测场景	配置过程
故障管理	连通性检测	CC（Continuity Check）功能： 检测 Ingress LER 和 Egress LER 之间双向 LSP 的持续连通性，如果链路故障即上报告警，同时使链路进入故障状态。
		LB（Loopback Function）功能： 以按需方式检测 Ingress LER 和 Egress LER 之间双向 LSP 的持续连通性，检测结果直接打印在终端上。
		CV（Connectivity Verification）功能： 检测 Ingress LER 和 Egress LER 两端 CC 配置一致性，并且上报相应告警。
	告警抑制功能	AIS（Alarm Indication Signal）功能： 如果被检测 LSP 出现故障则会向上一层发送 AIS 报文。
	丢包率统计	LM（Loss Measurement）功能： 检测 Ingress LER 和 Egress LER 之间双向 LSP 的丢包率统计信息。
	时延和时延抖动统计	DM（Delay Measurement）功能： 检测 Ingress LER 和 Egress LER 之间双向 LSP 的时延和时延抖动统计信息。

前置任务

在 LSP 的 MPLS-TP OAM 功能之前，需要完成以下任务：

- 已经完成双向 LSP 的配置。
- 已经使能 Tunnel 接口报文统计功能。

数据准备

在配置 LSP 的 MPLS-TP OAM 功能之前，需要准备以下数据。

序号	数据
1	MEG 名称
2	ME 绑定接口名称
3	（可选）CC 报文发送间隔、CC 报文优先级
4	（可选）单端丢包统计检测报文发送间隔、发送次数、报文优先级
4	（可选）时延统计检测报文发送间隔、发送次数、报文优先级
5	（可选）AIS 检测报文发送间隔和报文优先级

10.2.2 配置 ME 实例和接口绑定

创建 ME 实例并绑定到一条双向 LSP。

背景信息

由于承载 TE 主要业务的 RSVP 隧道是单向的，业务流只能从隧道的入节点到出节点方向发送，如果希望业务或者数据从出节点发送到入节点，只能通过路由转发，不能避免拥塞的问题；并且，如果将出节点到入节点的路径也配置为 RSVP 隧道，则当一条隧道故障倒换时，不能及时通知另一条隧道也倒换，造成业务中断。通过部署静态双向 LSP 可以解决上述问题，目前支持的静态双向 LSP 有如下两种类型：

- **双向共路静态 LSP：**双向共路静态 LSP 和两条独立的方向相反的方向 LSP 类似，区别在于双向共路静态 LSP 是一个整体，整条 LSP 对应两个转发表，必须两个方向的转发条件都满足整条 LSP 才会 Up。如果一个方向满足另一个方向不满足则双向均处于 Down 状态。而且两个转发表项之间互相感知对方的存在，在没有 IP 转发能力的情况下，任意中间节点可以沿原路径返回回应报文。
双向共路静态 LSP 作为 MPLS-TP 场景支持的一个重要特性，可以通过配置 TPOAM 进行检测。此时 MEG 对应该整条双向 LSP，其中只包含一个 ME，MEP 位于 LSP 的 Ingress 和 Egress 节点。
- **双向关联静态 LSP：**在互为源端和宿端的两台设备上，部署两条 RSVP-TE 协议的隧道，将两条隧道的 LSP 首尾绑定，即可形成动态双向关联 LSP（Dynamic Bidirectional Associated Label Switch Path）。这样，在网络中配置双向 LSP 承载双向流量后，不但可以解决拥塞的问题，而且当一端出现故障时会通过 LSP 将消息及时通知另一端，实现两端同时倒换，保证双向业务不出现中断。

双向关联静态 LSP 同样是 MPLS-TP 场景支持的一个重要特性，可以通过配置 TP OAM 进行检测。此时 MEG 对应该双向 LSP，其中包含二个 ME，MEP 位于 LSP 的 Ingress 和 Egress 节点。

传送路径为双向 P2P LSP 的场景下，MEG 对应该双向 P2P LSP，其中只包含一个 ME，正反两个方向对外表现为一条 LSP。

请在本端设备和目的端设备进行如下配置：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mpls-tp meg meg-name**，创建一个维护组，并进入到 MEG 视图。

步骤 3 执行命令 **me te interface interface-type interface-number mep-id mep-id remote-mep-id remote-mep-id**，配置 ME 实例并绑定到一条双向共路的 TE Tunnel。

----结束

10.2.3 （可选）配置 LSP 持续连通性和转发故障检测（CC/CV）功能

使用 MPLS-TP OAM 对 LSP 持续连通性和转发正确性进行检测。

背景信息

CC（Continuity Check）和 CV（Connectivity Verification）实际上是两种不同的 MPLS-TP OAM 功能。CC 用于同一 MEG 的两个 MEP 之间的连续性缺陷检测 dLOC（loss of continuity）。而 CV 用于检测两个 MEG 或者同一 MEG 的 MEP 之间 MEG 配置的一致性。CC 和 CV 在检测目的上存在很大区别，详见如下对比：

- 双向 LSP 持续连通性检测（CC）作为一种主动性的 OAM，用于检测一个 MEG 中任何一对 MEP 间连续性的报文丢失。本端周期性的向目的端发送 CCM 报文，如果目的端在 3.5 个报文发送周期内没有收到 CCM 报文，则认为本端到目的端连通性有问题，上报告警，同时进入故障状态并触发 APS 倒换。当目的端重新收到本端发送的 CCM 报文，则恢复告警并且退出故障状态。
- 双向 LSP 转发故障检测（CV）同样是一种主动性的 OAM，MEP 端点在接收到非预期的报文时会上报告警。比如使能 CV 检测功能的设备从某条 LSP 收到报文，却发现该报文不是这条 LSP 应该承载的，此时会上报转发错误告警。

传送网对于数据转发正确性要求很高，而 MPLS-TP 要求数据平面可在不具有 IP 能力的情况下工作，即只依赖于标签进行转发操作，所以必须保证标签转发的正确性。

但是在实际应用中这两者通常是联系在一起，共同执行，所以 NE80E/40E 把这两种检测功能放在一起。请在本端设备和目的端设备进行如下配置：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mpls-tp meg meg-name**，并进入到 MEG 视图。

步骤 3 （可选）针对不同的场景，对检测方式进行配置：

 说明

如果进行可选配置，必须保证本端和目的端取值一致。否则会上报相应告警。

- 执行命令 **cc interval interval-value**，配置检测报文发送周期。

CCM 报文的发送周期取值与应用场景如下：

- 3.3 毫秒：每秒 300 帧的传输速率，建议保护转换应用使用该发送周期。
- 10 毫秒：每秒 100 帧的传输速率。
- 100 毫秒：每秒 10 帧的传输速率，建议性能监测应用使用该发送周期。
- 1000 毫秒：每秒 1 帧的传输速率，建议故障管理应用使用该发送周期。
- 10000 毫秒：每分钟 6 帧的传输速率。
- 60000 毫秒：每分钟 1 帧的传输速率。
- 600000 毫秒：每小时 6 帧的传输速率。

请根据 CC 检测的应用领域，选取合适的 CCM 报文发送周期。

- 执行命令 **cc exp exp-value**，配置检测报文的优先级。

如果当前 MPLS-TP 网络拥塞严重，而且检测报文优先级较低，将会导致检测报文不能正常发送。所以，请根据网络状况选取合适的检测报文优先级。

步骤 4 使能 CC/CV 功能。为了避免使能过程中产生误报，请按照如下顺序依次使能本端和对端：

1. 在本端执行命令 **cc send enable**，使能本端发送 CC/CV 检测报文功能。
2. 在对端执行命令 **cc send enable**，使能对端发送 CC/CV 检测报文功能。
3. 在本端执行命令 **cc receive enable**，使能本端接收 CC/CV 检测报文功能。
4. 在对端执行命令 **cc receive enable**，使能对端接收 CC/CV 检测报文功能。

----结束

10.2.4 （可选）配置 LSP 按需连通性检测（LB）功能

LB 检测是最常见的用于检测 MPLS-TP 网络连通性的调试工具。

背景信息

环回检测 LB（LoopBack）功能用于检测本端 MEP 与对端 MEP 间的连通性。相对于主动方式的 CC/CV 检测，LB 主要用做按需方式连通性故障检测。

LB 的连通性检测是通过命令实现，它使用 LB 报文信息可以来检测如下信息：

- 远程设备是否可用
- 与远程主机通信的来回旅程(round-trip)的延迟(delay)
- 探测报文的丢失情况

操作步骤

步骤 1 执行命令 **ping meg meg-name [-c count-value | -t timeout-value]***，对 MPLS-TP 链路进行连通性检测。

 说明

如果网络速度较慢，执行 **ping meg** 测试时可适当加大 **timeout-value** 参数指定的等待响应报文超时时间。

----结束

10.2.5 （可选）配置 LSP 丢包率统计（LM）功能

通过配置单端丢包率或双端丢包率对双向 LSP 可靠性性能进行统计。

背景信息

丢包率度量 LM（Packet Loss Measurement）是 MPLS-TP 性能监控 PM（Performance Monitoring）的一项功能。双端丢包率度量在 LSP 的两个端点 MEP 进行。度量的数据实际上包含两个方面：

- 近端丢包率（near-end packet loss）：近端丢包率表示本端 MEP 收方向（本端 MEP 接收从远端 MEP 发过来）的丢包统计。
- 远端丢包率（far-end packet loss）：远端丢包率表示本端 MEP 发方向（远端 MEP 接收从本端 MEP 发过去）的丢包统计。

NE80E/40E 支持两种 LM 功能，第一种称为单端（Single-end）LM，第二种称为双端（Dual-end）LM。两者主要区别如下：

表 10-4 单端丢包统计与双端丢包统计的区别

比较项目	单端丢包统计	双端丢包统计
统计结果显示	在本端设备通过如下两种方式都可以查看到统计信息： ● 执行 loss-measure single-ended 命令会在设备上直接打印显示单端丢包的统计信息。 ● 执行 display mpls-tp oam statistic-type lost-measure single-ended 命令，查询显示单端丢包的统计信息。	在本端或者对端设备执行 display mpls-tp oam statistic-type lost-measure dual-ended 命令，查询显示双端丢包的统计信息。
检测场景	On-demand Monitoring：按照用户需求的被动性检测。	Proactive Monitoring：无需用户反复操作的主动性检测。

单端丢包统计与双端丢包统计的配置过程如下：



说明

如果没有说明，操作步骤需要同时在本端和对端配置。

操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **mpls-tp meg meg-name**，并进入到 MEG 视图。
- 步骤 3** 根据单端丢包统计和双端丢包统计可以划分为如下两种场景，在检测的时候请参考背景信息选择一种进行配置：
- 配置单端丢包统计功能：

1. 执行命令 **lost-measure single-ended receive enable**，使能对端的单端丢包统计接收功能。
 2. 执行命令 **loss-measure single-ended [interval interval-value | count count-value | exp exp-value]***，启动本端的单端丢包统计功能。
- 配置双端丢包统计功能：
 1. （可选）执行命令 **cc interval interval-value**，配置检测报文发送周期。
典型的检测报文发送周期取值与应用场景如下：
 - 3.3：每秒 300 帧的传输速率，建议保护转换应用使用该发送周期。
 - 100：每秒 10 帧的传输速率，建议性能监测应用使用该发送周期。
 - 1000：每秒 1 帧的传输速率，建议故障管理应用使用该发送周期。
 2. （可选）执行命令 **cc exp exp-value**，配置检测报文的优先级。

 说明

如果当前 MPLS-TP 网络拥塞严重，而且检测报文优先级较低，将会导致检测报文不能正常发送。所以，请根据网络状况选取合适的检测报文优先级。
 3. 在本端执行命令 **cc send enable**，使能本端发送 CC/CV 检测报文功能。
 4. 在对端执行命令 **cc send enable**，使能对端发送 CC/CV 检测报文功能。
 5. 在本端执行命令 **cc receive enable**，使能本端接收 CC/CV 检测报文功能。
 6. 在对端执行命令 **cc receive enable**，使能对端接收 CC/CV 检测报文功能。
 7. （可选）执行命令 **lost-measure dual-ended loss-ratio { threshold1 threshold1-value | threshold2 threshold2-value }**，配置丢包统计的告警门限阈值。
 8. 执行命令 **lost-measure dual-ended enable**，命令使能双端丢包统计功能。

----结束

10.2.6 （可选）配置 LSP 时延和抖动统计（DM）功能

通过配置单向/双向时延和抖动功能对双向 LSP 可靠性性能进行统计。

背景信息

报文时延度量 DM（Packet Delay Measurement）同样也是 MPLS-TP 性能监控 PM（Performance Monitoring）中的一项功能。根据统计的时延信息，可监控出传送路径的报文时延抖动（packet delay variation）情况。目前支持两种方式的时延和时延抖动统计：

- 单向时延和时延抖动：通过本端 MEP 在点到点 ME 中向对端 MEP 发送单向探测报文，实现对单向报文时延和单向报文时延变化的测量。

 说明

如果两个 MEP 之间时钟是同步的，单向报文时延测量可以进行；否则将只能进行双向时延变化的测量。

- 双向时延和时延抖动：通过本端 MEP 在点到点 ME 中向对端 MEP 发送带有请求信息的单向探测报文，并从对端 MEP 接收带有回复信息的探测报文，实现对双向报文时延和双向报文时延变化的测量。

单向/双向时延和时延抖动在使用场景上的区别如下：

表 10-5 单向时延和时延抖动统计与双向时延和时延抖动统计的区别

比较项目	单向时延和时延抖动统计	双向时延和时延抖动统计
统计结果显示	在对端设备执行 display mpls-tp oam meg meg-name statistic-type delay-measure one-way 命令，查看本端单向时延和时延抖动统计信息。	在本端设备通过如下两种方式都可以查看到统计信息： ● 执行 delay-measure two-way [interval interval-value count count-value exp exp-value two-time-stamp]*，查看双向时延和时延抖动统计信息。 ● 执行 display mpls-tp oam meg-name statistic-type delay-measure two-way 命令，查看双向时延和时延抖动统计信息。
检测场景	On-demand Monitoring: 按照用户需求的被动性检测。	On-demand Monitoring: 按照用户需求的被动性检测。

单向/双向时延和时延抖动统计的配置过程如下：



说明

如果没有说明，操作步骤需要同时在本端和对端配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mpls-tp meg meg-name**，并进入到 MEG 视图。

步骤 3 请根据使用场景参考背景信息，选择单向或者双向时延和时延抖动统计功能：

- 配置单向时延和时延抖动统计功能。

执行命令 **delay-measure one-way [interval interval-value | count count-value | exp exp-value]***，使能单向时延和时延抖动统计功能。

请按照如下方式对单向时延和时延抖动统计信息结果进行查询：

- 如果在本端 MEP 执行 **delay-measure one-way** 命令，表示统计从源端到目的端链路的时延值，此时的统计结果需要在对端 MEP 执行 **display mpls-tp oam meg meg-name statistic-type delay-measure one-way** 命令进行查询。
- 如果在对端 MEP 执行 **delay-measure one-way** 命令，表示统计从目的端到源端链路的时延值，此时的统计结果需要在本端 MEP 执行 **display mpls-tp oam meg meg-name statistic-type delay-measure one-way** 命令进行查询。

- 配置双向时延和时延抖动统计功能。

执行命令 **delay-measure two-way [interval interval-value | count count-value | exp exp-value | two-time-stamp]***，使能双向时延和时延抖动统计功能。

----结束

10.2.7 （可选）配置 LSP 告警抑制（AIS）功能

如果 LSR 间下层链路出现故障，使能告警抑制的设备将向与故障产生相反的方向延 LSP 周期性地发送 AIS 报文，抑制上层 PW 触发告警。

背景信息

传统的传送网络中，一条电路（比如 T1 线路）通常会跨越多个交换设备，当这条电路中的任一节点设备或链路故障，故障点会立即产生告警抑制消息，同时触发保护倒换。对于承载传送网业务的 MPLS-TP 网络，NE80E/40E 是通过告警抑制功能 AIS（Alarm Indication Signal）实现告警抑制功能。

在 MPLS-TP AIS 已经使能的场景下：

- 如果当前 MEG 所在的下层网络（server layer）感知到故障发生，则会向网管设备发送告警，然后通知上层网络（client layer），从而抑致高级别网络设备向网管设备发送同样的故障告警。
- 在检测到 AIS 故障情况之后，如果对端 MEP 在 AIS 传输周期 3.5 倍的时间间隔内未收到 AIS 报文，该 MEP 将从告警抑制状态恢复。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 根据需要使能 AIS 功能的视图选择如下配置：

- 如果在 MEG 视图下使能 AIS 功能，请执行命令 **mpls-tp meg meg-name**，并进入到 MEG 视图。
- 如果在接口视图下使能 AIS 功能，请执行命令 **interface interface-type interface-number**，并进入到接口视图。

步骤 3 （可选）执行命令 **ais exp exp-value**，配置 AIS 报文优先级。

步骤 4 （可选）执行命令 **ais interval interval-value**，配置 AIS 报文发送的间隔。

步骤 5 执行命令 **ais enable**，使能 AIS 功能。

----结束

10.2.8 检查配置结果

在完成 LSP 的 MPLS-TP OAM 功能配置后，可以查看性能统计信息和故障检测信息。

前提条件

已经完成 LSP 的 MPLS-TP OAM 功能的所有配置。

操作步骤

- 执行 **display mpls-tp oam ais** 命令查看设备上的 AIS 配置信息。
- 执行 **display mpls-tp oam current-alarm** 命令查看 MEG 下的告警信息。
- 执行 **display mpls-tp oam me { meg meg-name [mep-id mep-id | remote-mep-id remote-mep-id] | brief }** 命令查看 MEG 下的 ME 信息。
- 执行 **display mpls-tp oam meg** 命令查看当前设备上的 MEG 信息。

- 执行 **display mpls-tp oam statistic-type** 命令查看 MPLS-TP OAM 性能统计结果。

----结束

任务示例

执行 **display mpls-tp oam ais** 命令查看设备上的 AIS 配置信息。

```
<HUAWEI> display mpls-tp oam ais meg test
```

```
-----
Meg test
-----
Ais Interval      : 60000
Ais Exp           : 0
Ais Timer         : 0xFFFFFFFF
Ais Enable        : YES
```

执行 **display mpls-tp oam current-alarm** 命令查看 MEG 下的告警信息。

```
<HUAWEI> display mpls-tp oam current-alarm meg test
```

Alarm Name	ab.	Start Time	Meg Name	Sended
SD1 near-end	SD1-NEAR	2011-01-24 10:24:41.410	test	YES
SD1 far-end	SD1-FAR	2011-01-24 17:31:15.320	test	YES
SD2 near-end	SD2-NEAR	2011-01-24 10:24:41.410	test	YES
SD2 far-end	SD2-FAR	2011-01-24 17:31:15.320	test	YES

执行 **display mpls-tp oam me** 命令查看 MEG 下的 ME 信息。

```
<HUAWEI> display mpls-tp oam me brief
```

```
-----
MEG test
-----
[ME 1]
index           : 0
direction       : dual
mep id          : 8191
remote mep id   : 8191
status board    : 1
service type    : te (cr-static-lsp)
tunnel-name     : Tunnel1/0/0

lsp name        :
state           : UP
alarm indicate  : SD1-NEAR, SD1-FAR, SD2-NEAR, SD2-FAR
```

执行 **display mpls-tp oam meg** 命令查看当前设备上的 MEG 信息。

```
<HUAWEI> display mpls-tp oam meg test
```

```
-----
MEG abc
-----
meg name        : test
me count        : 1
cc send         : enable
cc receive      : enable
cc interval     : 1000
cc exp          : 7
ais             : enable
ais interval    : 60000
ais exp         : 0
lm single-end receive : disable
lm dual-end     : enable
lm dual-end SD1 threshold: 1
lm dual-end SD2 threshold: 10

[ME 1]
index           : 0
direction       : dual
mep id          : 8191
remote mep id   : 8191
status board    : 1
service type    : te (cr-static-lsp)
```

```
tunnel-name          : Tunnel1/0/0

lsp name              :
state                 : UP
alarm indicate        : SD1-NEAR, SD1-FAR, SD2-NEAR, SD2-FAR
```

执行 **display mpls-tp oam statistic-type** 命令查看 MPLS-TP OAM 单向时延统计结果。

<HUAWEI> **display mpls-tp oam meg test statistic-type delay-measure one-way**

```
One-way delay measure statistics
Index    delay(us)      delay variation(us)
-----
1         4294827296    --
2         4294847296    20000
3         4294847296    0
4         4294827296    20000
5         4294847296    20000
6         4294847296    0
7         4294847296    0
8         4294847296    0
9         4294827296    20000
10        4294847296    20000
11        4294847296    0
12        4294847296    0
13        4294847296    0
14        4294827296    20000
15        4294827296    0
16        4294847296    20000
17        4294847296    0
18        4294847296    0
19        4294847296    0
20        4294847296    0
The Max delay:4294847296   The Max delay variation:20000
The Min delay:4294827296   The Min delay variation:0
The delay average:4294842296 The delay variation average:7368
The total number of the record is: 20
```

执行 **display mpls-tp oam statistic-type** 命令查看 MPLS-TP OAM 双向丢包统计结果。

<HUAWEI> **display mpls-tp oam meg test statistic-type lost-measure dual-ended**

```
Dual-end loss measurement statistics:
Index Near-end lost frames Loss ratio Far-end lost frames Loss ratio
1      10                12.50%    10                12.50%
Max near-end lost frames:10,frame loss ratio:12.50%
Min near-end lost frames:10,frame loss ratio:12.50%
Average near-end lost frames:10,frame loss ratio:12.50%
Max far-end lost frames:10,frame loss ratio:12.50%
Min far-end lost frames:10,frame loss ratio:12.50%
Average far-end lost frames:10,frame loss ratio:12.50%
```

10.3 配置 PW 的 MPLS-TP OAM 功能

NE80E/40E 提供的 MPLS-TP OAM 支持对基于双向 LSP 的 PW 链路进行检测。

10.3.1 建立配置任务

MPLS-TP OAM 可用于检测 PW。配置 MPLS-TP OAM 前，需要先创建 PW。以下说明配置 OAM 的基本检测功能的应用环境、前置任务、数据准备、配置过程。

应用环境

MPLS-TP 已经开始广泛应用于传送网络，但由于传统的传送网络（如 SDH/OTN）在可靠性和运维这两个方面树立了一个很高的基准，因此 MPLS-TP 需要提供完善的 OAM 能力。

对于基于双向 LSP 的 PW 网络，MPLS-TP OAM 可以对其故障进行管理，同时对各项性能指标进行统计。如图 10-4 所示，以 T-PE 作为 MEP 端点，S-PE 作为 MIP 端点进行 MPLS-TP OAM 配置，可以实现如表 10-6 所示的各项 MPLS-TP OAM 功能。

图 10-4 基于双向 LSP 的 PW 组网图

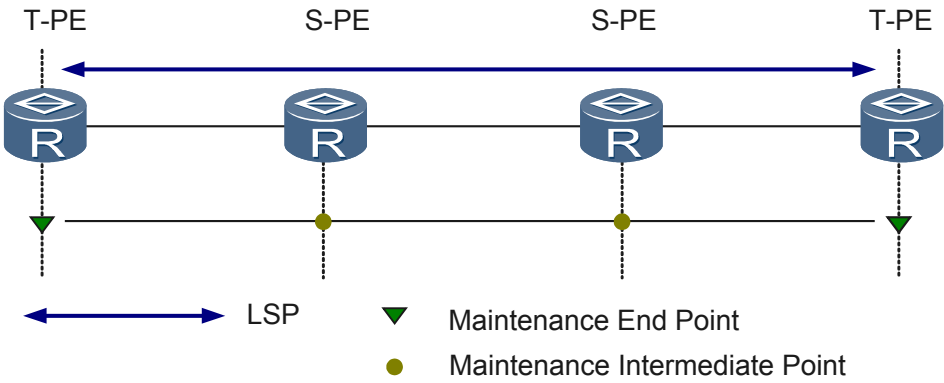


表 10-6 NE80E/40E 支持 MPLS-TP OAM 功能表

MPLS-TP OAM 功能类型	检测场景	配置过程
故障管理	连通性检测	CC（Continuity Check）功能： 检测 T-PE 之间基于双向 LSP 的 PW 的持续连通性，如果链路故障即上报告警，同时使链路进入故障状态。
		LB（Loopback Function）功能： 以按需方式检测 T-PE 之间基于双向 LSP 的 PW 的持续连通性，检测结果直接打印在终端上。
		CV（Connectivity Verification）功能： 检测 T-PE 两端 CC 配置一致性，并且上报相应告警。
性能统计	丢包率统计	LM（Loss Measurement）功能： 检测 T-PE 之间基于双向 LSP 的 PW 的丢包率统计信息。
	时延和时延抖动统计	DM（Delay Measurement）功能： 检测 T-PE 之间基于双向 LSP 的 PW 的时延和时延抖动统计信息。

前置任务

在配置 PW 的 MPLS-TP OAM 功能之前，需要完成以下任务：

- 已经完成基于双向 LSP 的 PW 配置。
- 已经使能 AC 侧接口报文统计功能。

数据准备

在配置 PW 的 MPLS-TP OAM 功能之前，需要准备以下数据。

序号	数据
1	MEG 名称
2	ME 绑定 VC ID
3	(可选) CC 报文发送间隔、CC 报文优先级
4	(可选) 单端丢包统计检测报文发送间隔、发送次数、报文优先级
4	(可选) 时延统计检测报文发送间隔、发送次数、报文优先级
5	(可选) AIS 检测报文发送间隔和报文优先级

10.3.2 配置 ME 实例和 PW 绑定

创建 ME 实例并绑定到单段或多段 PWE3 类型的 PW 链路。

背景信息

传送路径为基于双向 LSP 的 PW 的场景下，必须把创建的 ME 绑定到 PW 才可以进行 MPLS-TP OAM 检测。

请在本端设备和目的端设备进行如下配置：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mpls-tp meg meg-name**，创建一个维护组，并进入到 MEG 视图。

步骤 3 执行命令 **me l2vc peer-ip peer-ip vc-id vc-id vc-type vc-type [remote-peer-ip remote-peer-ip | ttl ttl-number] mep-id mep-id remote-mep-id remote-mep-id**，配置 ME 实例并绑定到单段或多段 PWE3 类型的 PW 链路。

- 对于一条 PW 链路进行 OAM 检测配置如下：
 - 在本端配置 **me l2vc peer-ip peer-ip vc-id vc-id vc-type vc-type mep-id mep-id remote-mep-id remote-mep-id** 命令创建 ME 并绑定到一条单段 PWE3 类型的 PW 链路。
 - 在远端同时配置 **me l2vc peer-ip peer-ip vc-id vc-id vc-type vc-type mep-id mep-id remote-mep-id remote-mep-id** 命令创建 ME 绑定到同一条单段 PWE3 类型的 PW 链路。
- 指定 **remote-peer-ip** 或者 **ttl** 可以检测一条多段 PW 链路：
 - 通过指定 **remote-peer-ip** 来绑定多段
 - 在本端配置 **me l2vc peer-ip peer-ip vc-id vc-id vc-type vc-type remote-peer-ip remote-peer-ip mep-id mep-id remote-mep-id remote-mep-id** 命令创建 ME 并绑定到一条多段 PWE3 类型的 PW 链路, 指定多段 PW 中远端对等体 IP 地址。

- 在远端同时配置 **me l2vc peer-ip peer-ip vc-id vc-id vc-type vc-type remote-peer-ip remote-peer-ip mep-id mep-id remote-mep-id remote-mep-id** 命令创建 ME 绑定到同一条多段 PWE3 类型的 PW 链路, 指定多段 PW 中远端对等体 IP 地址。
- 通过指定 TTL 来绑定多段 PW
 - 在本端配置 **me l2vc peer-ip peer-ip vc-id vc-id vc-type vc-type ttl ttl-number mep-id mep-id remote-mep-id remote-mep-id** 命令创建 ME 并绑定到一条多段 PWE3 类型的 PW 链路。
 - 在远端同时配置 **me l2vc peer-ip peer-ip vc-id vc-id vc-type vc-type ttl ttl-number mep-id mep-id remote-mep-id remote-mep-id** 命令创建 ME 绑定到同一条多段 PWE3 类型的 PW 链路。

----结束

10.3.3 (可选) 配置 PW 持续连通性和转发故障检测 (CC/CV) 功能

使用 MPLS-TP OAM 对 PW 持续连通性和转发正确性进行检测。

背景信息

CC (Continuity Check) 和 CV (Connectivity Verification) 实际上是两种不同的 MPLS-TP OAM 功能。CC 用于同一 MEG 的两个 MEP 之间的连续性缺陷检测 dLOC (loss of continuity defect)。而 CV 用于检测两个 MEG 或者同一 MEG 的 MEP 之间错误的连通性缺陷。但是在实际应用中这两者通常是联系在一起, 共同执行, 所以 NE80E/40E 把这两种检测功能放在一起。但是, CC 和 CV 在检测目的上存在很大区别, 详见如下对比:

- 基于双向 LSP 的 PW 持续连通性检测 (CC) 作为一种主动性的 OAM, 用于检测一个 MEG 中任何一对 MEP 间连续性的报文丢失。本端周期性的向目的端发送 CCM 报文, 如果目的端在 3.5 个报文发送周期内没有收到 CCM 报文, 则认为本端到目的端连通性有问题, 上报告警, 同时进入故障状态并触发 APS 倒换。当目的端重新收到本端发送的 CCM 报文, 则恢复告警并且退出故障状态。
- 基于双向 LSP 的 PW 转发故障检测 (CV) 同样是一种主动性的 OAM, MEP 节点在接收到非预期的报文时会上报告警。比如使能 CV 检测功能的设备从某条 PW 收到报文, 却发现该报文不是这条 PW 应该承载的, 此时会上报转发错误告警。

传送网对于数据转发正确性要求很高, 而 MPLS-TP 要求数据平面可在不具有 IP 能力的情况下工作, 即只依赖于标签进行转发操作, 所以必须保证标签转发的正确性。

请在本端设备和目的端设备进行如下配置:

操作步骤

步骤 1 执行命令 **system-view**, 进入系统视图。

步骤 2 执行命令 **mpls-tp meg meg-name**, 并进入到 MEG 视图。

步骤 3 (可选) 针对不同的场景, 对检测方式进行配置:



说明

如果进行可选配置, 必须保证本端和目的端取值一致。否则会导致 CC/CV 检测失败。

- 执行命令 **cc interval interval-value**, 配置检测报文发送周期。

CCM 报文的发送周期取值与应用场景如下:

- 3.3 毫秒：每秒 300 帧的传输速率，建议保护转换应用使用该发送周期。
- 10 毫秒：每秒 100 帧的传输速率。
- 100 毫秒：每秒 10 帧的传输速率，建议性能监测应用使用该发送周期。
- 1000 毫秒：每秒 1 帧的传输速率，建议故障管理应用使用该发送周期。
- 10000 毫秒：每分钟 6 帧的传输速率。
- 60000 毫秒：每分钟 1 帧的传输速率。
- 600000 毫秒：每小时 6 帧的传输速率。

请根据 CC 检测的应用领域，选取合适的 CCM 报文发送周期。

- 执行命令 **cc exp exp-value**，配置检测报文的优先级。

如果当前 MPLS-TP 网络拥塞严重，而且检测报文优先级较低，将会导致检测报文不能正常发送。所以，请根据网络状况选取合适的检测报文优先级。

步骤 4 使能 CC/CV 功能。为了避免使能过程中产生误报，请按照如下顺序依次使能本端和对端：

1. 在本端执行命令 **cc send enable**，使能本端发送 CC/CV 检测报文功能。
2. 在对端执行命令 **cc send enable**，使能对端发送 CC/CV 检测报文功能。
3. 在本端执行命令 **cc receive enable**，使能本端接收 CC/CV 检测报文功能。
4. 在对端执行命令 **cc receive enable**，使能对端接收 CC/CV 检测报文功能。

----结束

10.3.4 （可选）配置 PW 按需连通性检测（LB）功能

LB 检测是最常见的用于检测 MPLS-TP 网络连通性的调试工具。

背景信息

环回检测 LB（LoopBack）功能用于检测本端 MEP 与对端 MIP 或 MEP 间的连通性。相对于主动方式的 CC/CV 检测，LB 主要用做按需方式连通性故障检测。

LB 的连通性检测是通过 **ping meg** 命令实现，它使用 LB 报文信息可以来检测如下信息：

- 远程设备是否可用
- 与远程主机通信的来回旅程（round-trip）的延迟（delay）
- 探测报文的丢失情况

操作步骤

步骤 1 执行命令 **ping meg meg-name [-c count-value | -t timeout-value]***，对 MPLS-TP 链路进行连通性检测。

 说明

如果网络速度较慢，执行 **ping meg** 测试时可适当加大 **timeout-value** 参数指定的等待响应报文超时时间。

----结束

10.3.5 （可选）配置 PW 丢包率统计（LM）功能

通过配置单端丢包率或双端丢包率对基于双向 LSP 的 PW 可靠性性能进行统计。

背景信息

丢包率度量 LM (Packet Loss Measurement) 是 MPLS-TP 性能监控 PM (Performance Monitoring) 的一项功能。双端丢包率度量在 PW 的两个端点 MEP 进行。度量的数据实际上包含两个方面：

- 近端丢包率 (near-end packet loss)：近端丢包率表示本端 MEP 收方向（本端 MEP 接收从远端 MEP 发过来）的丢包统计。
- 远端丢包率 (far-end packet loss)：远端丢包率表示本端 MEP 发方向（远端 MEP 接收从本端 MEP 发过去）的丢包统计。

NE80E/40E 支持两种 LM 功能，第一种称为单端 (Single-end) LM，第二种称为双端 (Dual-end) LM。两者主要区别如下：

表 10-7 单端丢包统计与双端丢包统计的区别

比较项目	单端丢包统计	双端丢包统计
统计结果显示	在本端设备通过如下两种方式都可以查看到统计信息： ● 执行 loss-measure single-ended 命令会在设备上直接打印显示单端丢包的统计信息。 ● 执行 display mpls-tp oam statistic-type lost-measure single-ended 命令，查询显示单端丢包的统计信息。	在本端或者对端设备执行 display mpls-tp oam statistic-type lost-measure dual-ended 命令，查询显示双端丢包的统计信息。
检测场景	On-demand Monitoring：按照用户需求的被动性检测。	On-demand Monitoring：按照用户需求的被动性检测。

单端丢包统计与双端丢包统计的配置过程如下：



说明

如果没有说明，操作步骤需要同时在本端和对端配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mpls-tp meg meg-name**，并进入到 MEG 视图。

步骤 3 根据单端丢包统计和双端丢包统计可以划分为如下两种场景，在检测的时候请参考背景信息选择一种进行配置：

- 配置单端丢包统计功能：
 1. 执行命令 **lost-measure single-ended receive enable**，使能对端的单端丢包统计接收功能。
 2. 执行命令 **loss-measure single-ended [interval interval-value | count count-value | exp exp-value]***，启动本端的单端丢包统计功能。
- 配置双端丢包统计功能：

1. （可选）执行命令 **cc interval interval-value**，配置检测报文发送周期。
典型的检测报文发送周期取值与应用场景如下：

- 3.3：每秒 300 帧的传输速率，建议保护转换应用使用该发送周期。
- 100：每秒 10 帧的传输速率，建议性能监测应用使用该发送周期。
- 1000：每秒 1 帧的传输速率，建议故障管理应用使用该发送周期。

2. （可选）执行命令 **cc exp exp-value**，配置检测报文的优先级。

 说明

如果当前 MPLS-TP 网络拥塞严重，而且检测报文优先级较低，将会导致检测报文不能正常发送。所以，请根据网络状况选取合适的检测报文优先级。

3. 在本端执行命令 **cc send enable**，使能本端发送 CC/CV 检测报文功能。
4. 在对端执行命令 **cc send enable**，使能对端发送 CC/CV 检测报文功能。
5. 在本端执行命令 **cc receive enable**，使能本端接收 CC/CV 检测报文功能。
6. 在对端执行命令 **cc receive enable**，使能对端接收 CC/CV 检测报文功能。
7. （可选）执行命令 **lost-measure dual-ended loss-ratio { threshold1 threshold1-value | threshold2 threshold2-value }**，配置丢包统计的告警门限阈值。
8. 执行命令 **lost-measure dual-ended enable**，命令使能双端丢包统计功能。

---结束

10.3.6 （可选）配置 PW 时延和抖动统计（DM）功能

通过配置单向/双向时延和抖动功能对基于双向 LSP 的 PW 可靠性性能进行统计。

背景信息

报文时延度量 DM（Packet Delay Measurement）同样也是 MPLS-TP 性能监控 PM（Performance Monitoring）中的一项功能。根据统计的时延信息，可监控出传送路径的报文时延抖动（packet delay variation）情况。目前支持两种方式的时延和时延抖动统计：

- 单向时延和时延抖动：通过本端 MEP 在点到点 ME 中向对端 MEP 发送单向探测报文，实现对单向报文时延和单向报文时延变化的测量。

 说明

如果两个 MEP 之间时钟是同步的，单向报文时延测量可以进行；否则将只能进行双向报文时延变化的测量。

- 双向时延和时延抖动：通过本端 MEP 在点到点 ME 中向对端 MEP 发送带有请求信息的单向探测报文，并从对端 MEP 接收带有回复信息的探测报文，实现对双向报文时延和双向报文时延变化的测量。

单向/双向时延和时延抖动在使用场景上的区别如下：

表 10-8 单向时延和时延抖动统计与双向时延和时延抖动统计的区别

比较项目	单向时延和时延抖动统计	双向时延和时延抖动统计
统计结果显示	在对端设备执行 display mpls-tp oam meg meg-name statistic-type delay-measure one-way 命令，查看本端单向时延和时延抖动统计信息。	在本端设备通过如下两种方式都可以查看到统计信息： ● 执行 delay-measure two-way [interval interval-value count count-value exp exp-value two-time-stamp]*，查看双向时延和时延抖动统计信息。 ● 执行 display mpls-tp oam meg meg-name statistic-type delay-measure two-way 命令，查看双向时延和时延抖动统计信息。
检测场景	On-demand Monitoring: 按照用户需求的被动性检测。	On-demand Monitoring: 按照用户需求的被动性检测。

单向/双向时延和时延抖动统计的配置过程如下：

 说明

如果没有说明，操作步骤需要同时在本端和对端配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mpls-tp meg meg-name**，并进入到 MEG 视图。

步骤 3 请根据使用场景，选择单向或者双向时延和时延抖动统计功能：

- 配置单向时延和时延抖动统计功能。

执行命令 **delay-measure one-way [interval interval-value | count count-value | exp exp-value]***，使能单向时延和时延抖动统计功能。

请按照如下方式对单向时延和时延抖动统计信息结果进行查询：

- 如果在本端 MEP 执行 **delay-measure one-way** 命令，表示统计从源端到目的端链路的时延值，此时的统计结果需要在对端 MEP 执行 **display mpls-tp oam meg meg-name statistic-type delay-measure one-way** 命令进行查询。
- 如果在对端 MEP 执行 **delay-measure one-way** 命令，表示统计从目的端到源端链路的时延值，此时的统计结果需要在本端 MEP 执行 **display mpls-tp oam meg meg-name statistic-type delay-measure one-way** 命令进行查询。

- 配置双向时延和时延抖动统计功能。

执行命令 **delay-measure two-way [interval interval-value | count count-value | exp exp-value | two-time-stamp]***，使能双向时延和时延抖动统计功能。

----结束

10.3.7 检查配置结果

在完成 PW 的 MPLS-TP OAM 功能配置后，可以查看性能统计信息和故障检测信息。

前提条件

已经完成 PW 的 MPLS-TP OAM 功能的所有配置。

操作步骤

- 执行 **display mpls-tp oam ais** 命令查看设备上的 AIS 配置信息。
- 执行 **display mpls-tp oam current-alarm** 命令查看 MEG 下的告警信息。
- 执行 **display mpls-tp oam me { meg meg-name [mep-id mep-id | remote-mep-id remote-mep-id] | brief }** 命令查看 MEG 下的 ME 信息。
- 执行 **display mpls-tp oam meg** 命令查看当前设备上的 MEG 信息。
- 执行 **display mpls-tp oam statistic-type** 命令查看 MPLS-TP OAM 性能统计结果。

----结束

任务示例

执行 **display mpls-tp oam ais** 命令查看设备上的 AIS 配置信息。

```
<HUAWEI> display mpls-tp oam ais meg test
```

```
-----
Meg test
-----
Ais Interval      : 60000
Ais Exp           : 0
Ais Timer         : 0xFFFFFFFF
Ais Enable        : YES
```

执行 **display mpls-tp oam current-alarm** 命令查看 MEG 下的告警信息。

```
<HUAWEI> display mpls-tp oam current-alarm meg test
```

Alarm Name	ab.	Start Time	Meg Name	Sended
SD1 near-end	SD1-NEAR	2011-01-24 10:24:41.410	test	YES
SD1 far-end	SD1-FAR	2011-01-24 17:31:15.320	test	YES
SD2 near-end	SD2-NEAR	2011-01-24 10:24:41.410	test	YES
SD2 far-end	SD2-FAR	2011-01-24 17:31:15.320	test	YES

执行 **display mpls-tp oam me** 命令查看 MEG 下的 ME 信息。

```
<HUAWEI> display mpls-tp oam me brief
```

```
-----
MEG test
-----
[ME 1]
index           : 0
direction       : dual
mep id          : 8191
remote mep id   : 8191
status board    : 1
service type    : te (cr-static-lsp)
tunnel-name     : Tunnel1/0/0

lsp name        :
state           : UP
alarm indicate  : SD1-NEAR, SD1-FAR, SD2-NEAR, SD2-FAR
```

执行 **display mpls-tp oam meg** 命令查看当前设备上的 MEG 信息。

```
<HUAWEI> display mpls-tp oam meg test
```

```
-----
MEG abc
-----
meg name        : test
me count        : 1
cc send         : enable
cc receive      : enable
cc interval     : 1000
```

```
cc exp          : 7
ais             : enable
ais interval    : 60000
ais exp         : 0
lm single-end receive : disable
lm dual-end     : enable
lm dual-end SD1 threshold: 1
lm dual-end SD2 threshold: 10

[ME 1]
index          : 0
direction      : dual
mep id         : 8191
remote mep id  : 8191
status board   : 1
service type   : te (cr-static-lsp)
tunnel-name    : Tunnell/0/0

lsp name       :
state          : UP
alarm indicate : SD1-NEAR, SD1-FAR, SD2-NEAR, SD2-FAR
```

执行 **display mpls-tp oam statistic-type** 命令查看 MPLS-TP OAM 单向时延统计结果。

<HUAWEI> **display mpls-tp oam meg test statistic-type delay-measure one-way**

One-way delay measure statistics

Index	delay(us)	delay variation(us)

1	4294827296	—
2	4294847296	20000
3	4294847296	0
4	4294827296	20000
5	4294847296	20000
6	4294847296	0
7	4294847296	0
8	4294847296	0
9	4294827296	20000
10	4294847296	20000
11	4294847296	0
12	4294847296	0
13	4294847296	0
14	4294827296	20000
15	4294827296	0
16	4294847296	20000
17	4294847296	0
18	4294847296	0
19	4294847296	0
20	4294847296	0

The Max delay:4294847296 The Max delay variation:20000

The Min delay:4294827296 The Min delay variation:0

The delay average:4294842296 The delay variation average:7368

The total number of the record is: 20

执行 **display mpls-tp oam statistic-type** 命令查看 MPLS-TP OAM 双向丢包统计结果。

<HUAWEI> **display mpls-tp oam meg test statistic-type lost-measure dual-ended**

Dual-end loss measurement statistics:

Index	Near-end lost frames	Loss ratio	Far-end lost frames	Loss ratio
1	10	12.50%	10	12.50%

Max near-end lost frames:10,frame loss ratio:12.50%

Min near-end lost frames:10,frame loss ratio:12.50%

Average near-end lost frames:10,frame loss ratio:12.50%

Max far-end lost frames:10,frame loss ratio:12.50%

Min far-end lost frames:10,frame loss ratio:12.50%

Average far-end lost frames:10,frame loss ratio:12.50%

10.4 配置举例

配置举例结合组网需求、配置思路和数据准备例举了 MPLS-TP OAM 的典型应用场景，并提供配置文件。

10.4.1 配置 LSP 持续连通性和转发故障检测（CC/CV）功能示例

该组网的特点是 LSR 之间通过双向 LSP 互连，使用 CC/CV 功能完成对 LSR 之间的持续连通性和故障检测，从而实现对 MPLS-TP 网络的故障进行管理。

组网需求

如图 10-5 所示，LSRA、LSRB 和 LSRC 通过双向 LSP 互连。为了保证 LSRA 和 LSRC 之间的连通性和报文转发正确性做如下部署：

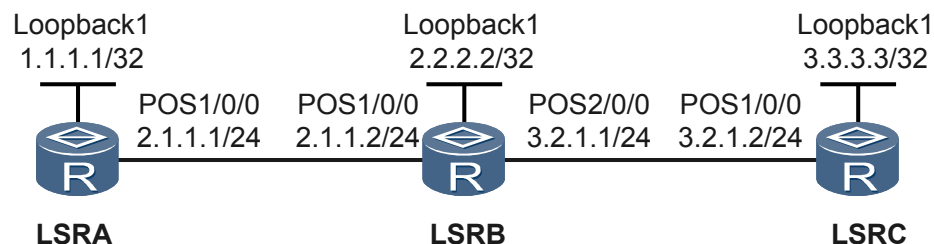
- LSRA 和 LSRC 作为 MEP 端点
- LSRB 作为 MIP 端点

在 MEP 端点上配置 CC/CV 功能。

- 双向 LSP 持续连通性检测（CC）作为一种主动性的 OAM，用于检测一个 MEG 中任何一对 MEP 间连续性的丢失。本端周期性的向目的端发送 CCM 报文，如果目的端在 3.5 个报文发送周期内没有收到 CCM 报文，则认为本端到目的端连通性有问题，上报告警，同时进入故障状态并触发 APS 倒换。当目的端重新收到本端发送的 CCM 报文，则恢复告警并且退出故障状态。
- 双向 LSP 转发故障检测（CV）同样是一种主动性的 OAM，MEP 在接收到非预期的报文时会报告警。比如使能 CV 检测功能的设备从某条 LSP 收到报文，却发现该报文不是这条 LSP 应该承载的，此时会上报转发错误告警。

传送网对于数据转发正确性要求很高，而 MPLS-TP 要求数据平面可在不具有 IP 能力的情况下工作，即只依赖于标签进行转发操作，所以必须保证标签转发的正确性。

图 10-5 双向 LSP 组网图



配置思路

采用如下的思路配置 LSP 持续连通性和转发故障检测功能：

1. 配置 ME 实例并绑定到一条双向的 LSP。
2. 配置检测报文（CC 报文）发送周期和报文优先级。

3. 使能 CC/CV 检测功能。

数据准备

为完成此配置例，需准备如下的数据：

- MEG 名称。
- ME 绑定 TE Tunnel 名称。
- 检测报文（CC 报文）发送周期和报文优先级。

操作步骤

步骤 1 配置双向 LSP

LSR 之间的双向 LSP，具体配置过程略。请参考《HUAWEI NetEngine80E/40E 路由器配置指南 MPLS》中的“配置双向静态 LSP”或者本配置举例中的配置文件。

步骤 2 配置 ME 实例并绑定到一条双向 LSP

在 LSRA 上配置 ME 实例名称为 test，并绑定到 Tunnel 1/0/0 接口。

```
<HUAWEI> system-view
[HUAWEI] sysname LSRA
[LSRA] mpls-tp meg test
[LSRA-mpls-tp-meg-test] me te interface tunnel 1/0/0 mep-id 1 rmep-id 2
```

在 LSRC 上配置 ME 实例名称为 test，并绑定到 Tunnel 2/0/0 接口。

```
<HUAWEI> system-view
[HUAWEI] sysname LSRC
[LSRC] mpls-tp meg test
[LSRC-mpls-tp-meg-test] me te interface tunnel 2/0/0 mep-id 2 rmep-id 1
```

步骤 3 配置检测报文（CC 报文）发送周期和报文优先级

说明

本端和目的端 MEP 的检测报文发送周期和报文优先级配置必须一致，否则会触发错误告警。

在 LSRA 上配置检测报文发送周期为 100 毫秒，报文优先级为 6。

```
[LSRA-mpls-tp-meg-test] cc interval 100
[LSRA-mpls-tp-meg-test] cc exp 6
```

在 LSRC 上配置检测报文发送周期为 100 毫秒，报文优先级为 6。

```
[LSRC-mpls-tp-meg-test] cc interval 100
[LSRC-mpls-tp-meg-test] cc exp 6
```

步骤 4 使能 CC/CV 检测功能

在 LSRA 上使能 CC/CV 检测功能。

```
[LSRA-mpls-tp-meg-test] cc send enable
[LSRA-mpls-tp-meg-test] cc receive enable
[LSRA-mpls-tp-meg-test] return
```

在 LSRC 上使能 CC/CV 检测功能。

```
[LSRC-mpls-tp-meg-test] cc send enable
[LSRC-mpls-tp-meg-test] cc receive enable
[LSRC-mpls-tp-meg-test] return
```

步骤 5 验证配置结果

配置成功后，在 LSRA 设备上使用 **display mpls-tp oam meg** 命令查看当前设备上的 MEG 信息。

```
<LSRA> display mpls-tp oam meg test
-----
```

```
MEG test
-----
meg name          : test
me count          : 1
cc send           : enable
cc receive        : enable
cc interval       : 100
cc exp            : 6
ais               : disable
ais interval      : 1000
ais exp           : 7
lm single-end receive : disable
lm dual-end       : enable
lm dual-end SD1 threshold: 1
lm dual-end SD2 threshold: 10
-----

[ME 1]
index             : 0
direction         : dual
mep id            : 1
remote mep id     : 2
status board      : 1
service type      : te (cr-static-lsp)
tunnel-name       : Tunnel1/0/0

lsp name          :
state             : UP
alarm indicate    : no alarm
-----
```

----结束

配置文件

● LSRA 的配置文件

```
#
 sysname LSRA
#
 mpls lsr-id 1.1.1.1
 mpls
 mpls te
#
 bidirectional static-cr-lsp ingress Tunnel1/0/0
  forward nexthop 2.1.1.2 out-label 20 bandwidth ct0 10000
  backward in-label 20
#
 interface Pos1/0/0
  undo shutdown
  ip address 2.1.1.1 255.255.255.0
  mpls
  mpls te
  mpls te bandwidth max-reservable-bandwidth 100000
  mpls te bandwidth bc0 100000
#
 interface LoopBack1
  ip address 1.1.1.1 255.255.255.255
#
 interface Tunnel1/0/0
  ip address unnumbered interface LoopBack1
  tunnel-protocol mpls te
  destination 3.3.3.3
  mpls te signal-protocol cr-static
  mpls te tunnel-id 100
  mpls te bidirectional
  mpls te commit
#
 ip route-static 2.2.2.2 255.255.255.255 2.1.1.2
```

```

ip route-static 3.3.3.3 255.255.255.255 2.1.1.2
#
mpls-tp meg test
me te interface Tunnel1/0/0 mep-id 1 remote-mep-id 2
cc interval 100
cc exp 6
cc send enable
cc receive enable
#
return

```

● LSRB 的配置文件

```

#
sysname LSRB
#
mpls lsr-id 2.2.2.2
mpls
mpls te
#
bidirectional static-cr-lsp transit lsp1
forward in-label 20 nexthop 3.2.1.2 out-label 40 bandwidth ct0 10000
backward in-label 16 nexthop 2.1.1.1 out-label 20 bandwidth ct0 10000
#
interface Pos1/0/0
undo shutdown
ip address 2.1.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface Pos2/0/0
undo shutdown
ip address 3.2.1.1 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface LoopBack1
ip address 2.2.2.2 255.255.255.255
#
ip route-static 1.1.1.1 255.255.255.255 2.1.1.1
ip route-static 3.3.3.3 255.255.255.255 3.2.1.2
#
return

```

● LSRC 的配置文件

```

#
sysname LSRC
#
mpls lsr-id 3.3.3.3
mpls
mpls te
#
bidirectional static-cr-lsp egress lsp1
forward in-label 40 lsrid 1.1.1.1 tunnel-id 100
backward nexthop 3.2.1.1 out-label 16 bandwidth ct0 10000
#
interface Pos1/0/0
undo shutdown
ip address 3.2.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface LoopBack1
ip address 3.3.3.3 255.255.255.255
#

```



```
interface Tunnel2/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 1.1.1.1
 mpls te signal-protocol cr-static
 mpls te tunnel-id 200
 mpls te passive-tunnel
 mpls te binding bidirectional static-cr-lsp egress lsp1
 mpls te commit
#
 ip route-static 1.1.1.1 255.255.255.255 3.2.1.1
 ip route-static 2.2.2.2 255.255.255.255 3.2.1.1
#
mpls-tp meg test
 me te interface Tunnel2/0/0 mep-id 2 remote-mep-id 1
 cc interval 100
 cc exp 6
 cc send enable
 cc receive enable
#
return
```

10.4.2 配置 LSP 按需连通性检测（LB）功能示例

该组网的特点是 LSR 之间通过双向 LSP 互连，使用 LB 功能完成对 LSR 之间的连通性进行按需检测，从而实现对 MPLS-TP 网络的故障进行管理。

组网需求

如图 10-6 所示，LSRA、LSRB 和 LSRC 通过双向 LSP 互连。为了保证 LSRA 和 LSRC 之间的连通性做如下部署：

- LSRA 和 LSRC 作为 MEP 端点
- LSRB 作为 MIP 端点

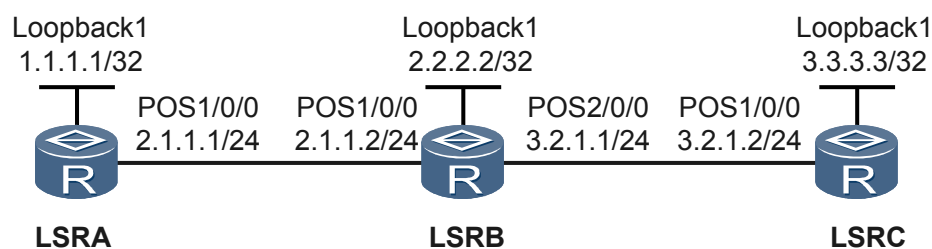
使用 LB 功能可以来检测：

- 远端 MEP 设备是否可达
- 本端 MEP 与远端 MEP 通信的来回旅程（round-trip）的延迟（delay）
- 本端 MEP 与远端 MEP 之间探测报文的丢失情况

📖 说明

LB 只对发送的探测报文的丢失情况进行统计，从而粗略的了解 MEP 之间的丢包率。如果要获得 MEP 之间流量的丢包率可以使用 LM 检测功能。

图 10-6 双向 LSP 组网图



配置思路

采用如下的思路配置 VLL 的单向时延计功能：

1. 配置 ME 实例并绑定到一条双向 LSP。
2. 启动 LB 检测功能。

数据准备

为完成此配置例，需准备如下的数据：

- MEG 名称。
- ME 绑定 TE Tunnel 名称。

操作步骤

步骤 1 配置双向 LSP

LSR 之间的双向 LSP，具体配置过程略。请参考《HUAWEI NetEngine80E/40E 路由器配置指南 MPLS》中的“配置双向静态 LSP”或者本配置举例中的配置文件。

步骤 2 配置 ME 实例并绑定到一条双向 LSP

在 LSRA 上配置 ME 实例名称为 test，并绑定到 Tunnel 1/0/0 接口。

```
<HUAWEI> system-view
[HUAWEI] sysname LSRA
[LSRA] mpls-tp meg test
[LSRA-mpls-tp-meg-test] me te interface tunnel 1/0/0 mep-id 1 rmep-id 2
[LSRA-mpls-tp-meg-test] return
```

在 LSRC 上配置 ME 实例名称为 test，并绑定到 Tunnel 2/0/0 接口。

```
<HUAWEI> system-view
[HUAWEI] sysname LSRC
[LSRC] mpls-tp meg test
[LSRC-mpls-tp-meg-test] me te interface tunnel 2/0/0 mep-id 2 rmep-id 1
```

步骤 3 启动 LB 检测功能

 说明

LB 支持本端 MEP 到远端 MEP 或者 MIP 之间的连通性检测，本示例以 LSRA 到 LSRC 的连通性检测为例。

在 LSRA 上使能 LB 检测功能。

```
<LSRA> ping meg test
PING test: 9 data bytes, press CTRL_C to break
  Reply from vsi: bytes=9, Sequence=1 time=100 ms
  Reply from vsi: bytes=9, Sequence=2 time=90 ms
  Reply from vsi: bytes=9, Sequence=3 time=100 ms
--- ping statistics ---
  3 packet(s) transmitted
  3 packet(s) received
  0.00% packet loss
  round-trip min/avg/max 90/96/100 ms
```

----结束

配置文件

- LSRA 的配置文件
- ```
#
sysname LSRA
```

```
#
mpls lsr-id 1.1.1.1
mpls
mpls te
#
bidirectional static-cr-lsp ingress Tunnel1/0/0
forward nexthop 2.1.1.2 out-label 20 bandwidth ct0 10000
backward in-label 20
#
interface Pos1/0/0
undo shutdown
ip address 2.1.1.1 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface LoopBack1
ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 3.3.3.3
mpls te signal-protocol cr-static
mpls te tunnel-id 100
mpls te bidirectional
mpls te commit
#
ip route-static 2.2.2.2 255.255.255.255 2.1.1.2
ip route-static 3.3.3.3 255.255.255.255 2.1.1.2
#
mpls-tp meg test
me te interface Tunnel1/0/0 mep-id 1 remote-mep-id 2
#
return
```

## ● LSRB 的配置文件

```
#
sysname Quidway
#
mpls lsr-id 2.2.2.2
mpls
mpls te
#
bidirectional static-cr-lsp transit lsp1
forward in-label 20 nexthop 3.2.1.2 out-label 40 bandwidth ct0 10000
backward in-label 16 nexthop 2.1.1.1 out-label 20 bandwidth ct0 10000
#
interface Pos1/0/0
undo shutdown
ip address 2.1.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface Pos2/0/0
undo shutdown
ip address 3.2.1.1 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface LoopBack1
ip address 2.2.2.2 255.255.255.255
#
ip route-static 1.1.1.1 255.255.255.255 2.1.1.1
ip route-static 3.3.3.3 255.255.255.255 3.2.1.2
```

```
#
return
● LSRC 的配置文件
#
sysname LSRC
#
mpls lsr-id 3.3.3.3
mpls
mpls te
#
bidirectional static-cr-lsp egress lspl
forward in-label 40 lsrid 1.1.1.1 tunnel-id 100
backward nexthop 3.2.1.1 out-label 16 bandwidth ct0 10000
#
interface Pos1/0/0
undo shutdown
ip address 3.2.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface LoopBack1
ip address 3.3.3.3 255.255.255.255
#
interface Tunnel2/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 1.1.1.1
mpls te signal-protocol cr-static
mpls te tunnel-id 200
mpls te passive-tunnel
mpls te binding bidirectional static-cr-lsp egress lspl
mpls te commit
#
ip route-static 1.1.1.1 255.255.255.255 3.2.1.1
ip route-static 2.2.2.2 255.255.255.255 3.2.1.1
#
mpls-tp meg test
me te interface Tunnel2/0/0 mep-id 2 remote-mep-id 1
#
return
```

### 10.4.3 配置 LSP 丢包率统计（LM）功能示例

该组网的特点是 LSR 之间通过双向 LSP 互连，使用 LM 功能完成对 LSR 之间的丢包率进行检测，从而实现对 MPLS-TP 网络的性能进行统计。

#### 组网需求

MPLS-TP 作为面向连接的包交换技术，旨在将现有基于电路交换的传送网络，改造成基于包交换的传送网络。其根本目的在于提高传统电路交换网络的尽可能地使用统计复用的包交换网络来尽量提高传输效率。

但是，在应用 MPLS-TP 技术提升带宽利用率同时，必须保证链路的可靠性。例如语音业务，当链路丢包率在 10% 以下时，用户不会有明显的感觉。但是当丢包率大于 20% 时，就会影响语音的质量。

#### 说明

丢包率定义为用百分数表示的未传递的报文数量除以时间间隔内发送报文总数的比率。这里未传递的报文数量，指的是一个点到点 LSP 链路中到达 LSP 入节点的报文数量和传递到 LSP 出结点的报文数量之差。

此时可以使用丢包率度量 LM（Packet Loss Measurement）检测功能对设备间丢包率进行统计，了解链路的真实性能。LM 是 MPLS-TP 性能监控 PM（Performance

Monitoring) 的一项功能, 可以事项两种 LM, 第一种称为单端 (Single-end) LM, 第二种称为双端 (Dual-end) LM。

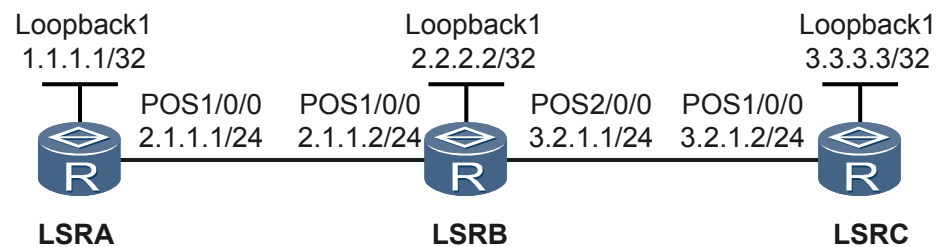
#### 说明

本示例仅以双端丢包统计为例, 单端丢包除了统计结果查询与双端丢包统计不同, 其它配置与双端丢包统计配置相同, 不再赘述。

如图 10-7 所示, LSRA、LSRB 和 LSRC 通过双向 LSP 互连。为了保证 LSRA 和 LSRC 之间的连通可靠性做如下部署, 实现 LSRA 和 LSRC 之间的双端丢包统计:

- LSRA 和 LSRC 作为 MEP 端点
- LSRB 作为 MIP 端点

图 10-7 双向 LSP 组网图



## 配置思路

采用如下的思路配置 LSP 丢包率统计功能:

1. 配置 ME 实例并绑定到一条双向的 LSP。
2. 使能本端和对端 CC 检测功能。
3. 配置丢包率统计阈值告警。
4. 使能双端丢包统计功能。

## 数据准备

为完成此配置例, 需准备如下的数据:

- MEG 名称。
- ME 绑定 TE Tunnel 名称。
- 丢包率统计发送告警的阈值。

## 操作步骤

### 步骤 1 配置双向 LSP

T-PE 之间的双向 LSP, 具体配置过程略。请参考《HUAWEI NetEngine80E/40E 路由器配置指南 MPLS》中的“配置双向静态 LSP”或者本配置举例中的配置文件。

### 步骤 2 配置 ME 实例并绑定到一条双向 LSP

# 在 LSRA 上配置 ME 实例名称为 test, 并绑定到 Tunnel 1/0/0 接口。

```
<HUAWEI> system-view
[HUAWEI] sysname LSRA
```

```
[LSRA] mpls-tp meg test
[LSRA-mpls-tp-meg-test] me te interface tunnel 1/0/0 mep-id 1 rmep-id 2

在 LSRC 上配置 ME 实例名称为 test，并绑定到 Tunnel 2/0/0 接口。
<HUAWEI> system-view
[HUAWEI] sysname LSRC
[LSRC] mpls-tp meg test
[LSRC-mpls-tp-meg-test] me te interface tunnel 2/0/0 mep-id 2 rmep-id 1
```

### 步骤 3 使能本端和对端 CC 检测功能

```
在 LSRA 上使能 CC 检测功能。
[LSRA-mpls-tp-meg-test] cc send enable
[LSRA-mpls-tp-meg-test] cc receive enable

在 LSRC 上使能 CC 检测功能。
[LSRC-mpls-tp-meg-test] cc send enable
[LSRC-mpls-tp-meg-test] cc receive enable
```

### 步骤 4 配置丢包率统计阈值告警

```
在 LSRA 上配置丢包率统计阈值告警。
[LSRA-mpls-tp-meg-test] lost-measure dual-ended loss-ratio threshold1 50

在 LSRC 上配置丢包率统计阈值告警。
[LSRC-mpls-tp-meg-test] lost-measure dual-ended loss-ratio threshold1 50
```

### 步骤 5 使能双端丢包统计功能

```
在 LSRA 上使能双端丢包统计功能。
[LSRA-mpls-tp-meg-test] lost-measure dual-ended enable
[LSRA-mpls-tp-meg-test] return

在 LSRC 上使能双端丢包统计功能。
[LSRC-mpls-tp-meg-test] lost-measure dual-ended enable
[LSRC-mpls-tp-meg-test] return
```

### 步骤 6 验证配置结果

配置成功后，在 LSRA 设备上使用 **display mpls-tp oam** 命令查看当前设备上的丢包率统计信息。

```
<LSRA> display mpls-tp oam meg test statistic-type lost-measure dual-ended
Dual-end loss measurement statistics:
Index Near-end lost frames Loss ratio Far-end lost frames Loss ratio
1 10 12.50% 10 12.50%
Max near-end lost frames:10,frame loss ratio:12.50%
Min near-end lost frames:10,frame loss ratio:12.50%
Average near-end lost frames:10,frame loss ratio:12.50%
Max far-end lost frames:10,frame loss ratio:12.50%
Min far-end lost frames:10,frame loss ratio:12.50%
Average far-end lost frames:10,frame loss ratio:12.50%
```

----结束

## 配置文件

#### ● LSRA 的配置文件

```
#
 sysname LSRA
#
 mpls lsr-id 1.1.1.1
 mpls
 mpls te
#
 bidirectional static-cr-lsp ingress Tunnel1/0/0
```

```

 forward nexthop 2.1.1.2 out-label 20 bandwidth ct0 10000
 backward in-label 20
#
interface Pos1/0/0
undo shutdown
ip address 2.1.1.1 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface LoopBack1
ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 3.3.3.3
mpls te signal-protocol cr-static
mpls te tunnel-id 100
mpls te bidirectional
mpls te commit
#
ip route-static 2.2.2.2 255.255.255.255 2.1.1.2
ip route-static 3.3.3.3 255.255.255.255 2.1.1.2
#
mpls-tp meg test
me te interface Tunnel1/0/0 mep-id 1 remote-mep-id 2
cc send enable
cc receive enable
#
return

```

#### ● LSRB 的配置文件

```

#
sysname Quidway
#
mpls lsr-id 2.2.2.2
mpls
mpls te
#
bidirectional static-cr-lsp transit lsp1
forward in-label 20 nexthop 3.2.1.2 out-label 40 bandwidth ct0 10000
backward in-label 16 nexthop 2.1.1.1 out-label 20 bandwidth ct0 10000
#
interface Pos1/0/0
undo shutdown
ip address 2.1.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface Pos2/0/0
undo shutdown
ip address 3.2.1.1 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface LoopBack1
ip address 2.2.2.2 255.255.255.255
#
ip route-static 1.1.1.1 255.255.255.255 2.1.1.1
ip route-static 3.3.3.3 255.255.255.255 3.2.1.2
#
return

```

#### ● LSRC 的配置文件

```
#
sysname LSRC
#
mpls lsr-id 3.3.3.3
mpls
mpls te
#
bidirectional static-cr-lsp egress lsp1
forward in-label 40 lsrid 1.1.1.1 tunnel-id 100
backward nexthop 3.2.1.1 out-label 16 bandwidth ct0 10000
#
interface Pos1/0/0
undo shutdown
ip address 3.2.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface LoopBack1
ip address 3.3.3.3 255.255.255.255
#
interface Tunnel2/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 1.1.1.1
mpls te signal-protocol cr-static
mpls te tunnel-id 200
mpls te passive-tunnel
mpls te binding bidirectional static-cr-lsp egress lsp1
mpls te commit
#
ip route-static 1.1.1.1 255.255.255.255 3.2.1.1
ip route-static 2.2.2.2 255.255.255.255 3.2.1.1
#
mpls-tp meg test
me te interface Tunnel2/0/0 mep-id 2 remote-mep-id 1
cc send enable
cc receive enable
#
return
```

## 10.4.4 配置 LSP 时延和抖动统计（DM）功能示例

该组网的特点是 LSR 之间通过双向 LSP 互连，使用 DM 功能完成对 LSR 之间的时延和抖动进行检测，从而实现对 MPLS-TP 网络的性能进行统计。

### 组网需求

MPLS-TP 作为面向连接的包交换技术，旨在将现有基于电路交换的传送网络，改造成基于包交换的传送网络。其根本目的在于提高传统电路交换网络的尽可能地使用统计复用的包交换网络来尽量提高传输效率。

但是，在应用 MPLS-TP 技术提升带宽利用率同时，必须保证链路的可靠性。例如语音业务，由于 VoIP 业务需要对语音包进行编码和解码，再加上传输的时延，这就使得 VoIP 业务的时延要比普通基于电路交换的电话时延大得多。如果时延大于 400ms 就可以明显的感觉出来。如果时延大于 2 秒会导致 VoIP 业务基本不可用。同时，当抖动超过一个语音包的时长时，语音质量就会明显下降。

此时可以使用时延和抖动度量 DM（Delay Measurement）检测功能对设备间时延和抖动进行统计，了解链路的真实性能。DM 是 MPLS-TP 性能监控 PM（Performance Monitoring）的一项功能，可以实现两种 DM，第一种称为单向（One-way）DM，第二种称为双向（Two-end）DM。





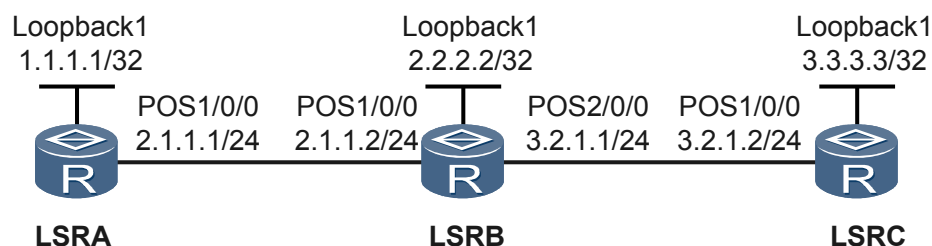
说明

本示例仅以双向时延统计为例，单向时延除了统计结果查询与双向时延统计不同，其它配置与双向时延统计配置相同，不再赘述。

如图 10-8 所示，LSRA、LSRB 和 LSRC 通过双向 LSP 互连。为了保证 LSRA 和 LSRC 之间的连通可靠性做如下部署，实现 LSRA 和 LSRC 之间的双向时延统计：

- LSRA 和 LSRC 作为 MEP 端点
- LSRB 作为 MIP 端点

图 10-8 双向 LSP 组网图



## 配置思路

采用如下的配置 LSP 时延和抖动统计功能：

1. 配置 ME 实例并绑定到一条双向的 LSP。
2. 使能本端和对端 CC 检测功能。
3. 使能双向时延和抖动统计功能。

## 数据准备

为完成此配置例，需准备如下的数据：

- MEG 名称。
- ME 绑定 TE Tunnel 名称。

## 操作步骤

### 步骤 1 配置双向 LSP

T-PE 之间的双向 LSP，具体配置过程略。请参考《HUAWEI NetEngine80E/40E 路由器配置指南 MPLS》中的“配置双向静态 LSP”或者本配置举例中的配置文件。

### 步骤 2 配置 ME 实例并绑定到一条双向 LSP

# 在 LSRA 上配置 ME 实例名称为 test，并绑定到 Tunnel 1/0/0 接口。

```
<HUAWEI> system-view
[HUAWEI] sysname LSRA
[LSRA] mpls-tp meg test
[LSRA-mpls-tp-meg-test] me te interface tunnel 1/0/0 mep-id 1 rmep-id 2
```

# 在 LSRC 上配置 ME 实例名称为 test，并绑定到 Tunnel 2/0/0 接口。

```
<HUAWEI> system-view
[HUAWEI] sysname LSRC
```

```
[LSRC] mpls-tp meg test
[LSRC-mpls-tp-meg-test] me te interface tunnel 2/0/0 mep-id 2 rmep-id 1
```

### 步骤3 使能双向时延和抖动统计功能

```
[LSRA-mpls-tp-meg-test] delay-measure two-way
Two-way delay measure statistics
delay(us): delay variation(us):
182 --
182 0
182 0
183 1
182 1
The Max delay:183, The Max delay variation:1
The Min delay:182, The Min delay variation:0
The delay average:182, The delay variation average:1
Total sent Packets Number:5, Total received Packets Number: 5
```

----结束

## 配置文件

### ● LSRA 的配置文件

```
#
sysname LSRA
#
mpls lsr-id 1.1.1.1
mpls
mpls te
#
bidirectional static-cr-lsp ingress Tunnel1/0/0
 forward nexthop 2.1.1.2 out-label 20 bandwidth ct0 10000
 backward in-label 20
#
interface Pos1/0/0
undo shutdown
ip address 2.1.1.1 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface LoopBack1
ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 3.3.3.3
mpls te signal-protocol cr-static
mpls te tunnel-id 100
mpls te bidirectional
mpls te commit
#
ip route-static 2.2.2.2 255.255.255.255 2.1.1.2
ip route-static 3.3.3.3 255.255.255.255 2.1.1.2
#
mpls-tp meg test
me te interface Tunnel1/0/0 mep-id 1 remote-mep-id 2
#
return
```

### ● LSRB 的配置文件

```
#
sysname LSRB
#
mpls lsr-id 2.2.2.2
mpls
```

```

mpls te
#
bidirectional static-cr-lsp transit lspl
forward in-label 20 nexthop 3.2.1.2 out-label 40 bandwidth ct0 10000
backward in-label 16 nexthop 2.1.1.1 out-label 20 bandwidth ct0 10000
#
interface Pos1/0/0
undo shutdown
ip address 2.1.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface Pos2/0/0
undo shutdown
ip address 3.2.1.1 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface LoopBack1
ip address 2.2.2.2 255.255.255.255
#
ip route-static 1.1.1.1 255.255.255.255 2.1.1.1
ip route-static 3.3.3.3 255.255.255.255 3.2.1.2
#
return

```

## ● LSRC 的配置文件

```

#
sysname LSRC
#
mpls lsr-id 3.3.3.3
mpls
mpls te
#
bidirectional static-cr-lsp egress lspl
forward in-label 40 lsrid 1.1.1.1 tunnel-id 100
backward nexthop 3.2.1.1 out-label 16 bandwidth ct0 10000
#
interface Pos1/0/0
undo shutdown
ip address 3.2.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface LoopBack1
ip address 3.3.3.3 255.255.255.255
#
interface Tunnel2/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 1.1.1.1
mpls te signal-protocol cr-static
mpls te tunnel-id 200
mpls te passive-tunnel
mpls te binding bidirectional static-cr-lsp egress lspl
mpls te commit
#
ip route-static 1.1.1.1 255.255.255.255 3.2.1.1
ip route-static 2.2.2.2 255.255.255.255 3.2.1.1
#
mpls-tp meg test
me te interface Tunnel2/0/0 mep-id 2 remote-mep-id 1

```

```

return
```

## 10.4.5 配置 LSP 告警指示信号（AIS）功能示例

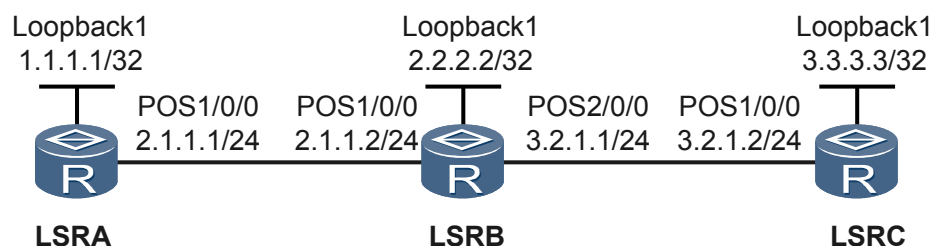
该组网的特点是 LSR 之间通过双向 LSP 互连，使用 AIS 功能抑制远端产生告警。

### 组网需求

在传统的传送网络中，一条电路（比如 T1 线路）通常会跨越多个交换设备，当这条电路中的任一节点设备或链路故障，故障点会立即产生告警抑制消息，同时触发保护倒换。对于承载传送网业务的 MPLS-TP 网络，NE80E/40E 是通过告警抑制功能 AIS（Alarm Indication Signal）实现告警抑制功能。

如图 10-9 所示，LSRA、LSRB 和 LSRC 通过双向 LSP 互连。执行 `ais enable` 命令使能当前 MEG 的 AIS 功能。如果当前 MEG 所在的下层网络（server layer）感知到故障发生，则会向网管设备发送告警，然后通知上层网络（client layer），从而抑致高级别网络设备向网管设备发送同样的故障告警。

图 10-9 双向 LSP 组网图



### 配置思路

采用如下的配置 LSP 时延和抖动统计功能：

1. 配置 ME 实例并绑定到一条双向的 LSP。
2. 使能本端和对端 CC 检测功能。

### 数据准备

为完成此配置例，需准备如下的数据：

- MEG 名称。
- ME 绑定 TE Tunnel 名称。

### 操作步骤

#### 步骤 1 配置双向 LSP

T-PE 之间的双向 LSP，具体配置过程略。请参考《HUAWEI NetEngine80E/40E 路由器配置指南 MPLS》中的“配置双向静态 LSP”或者本配置举例中的配置文件。

#### 步骤 2 配置 ME 实例并绑定到一条双向 LSP

# 在 LSRA 上配置 ME 实例名称为 test，并绑定到 Tunnel 1/0/0 接口。

```
<HUAWEI> system-view
[HUAWEI] sysname LSRA
[LSRA] mpls-tp meg test
[LSRA-mpls-tp-meg-test] me te interface tunnel 1/0/0 mep-id 1 rmep-id 2
[LSRA-mpls-tp-meg-test] cc send enable
[LSRA-mpls-tp-meg-test] cc receive enable
```

# 在 LSRC 上配置 ME 实例名称为 test，并绑定到 Tunnel 2/0/0 接口。

```
<HUAWEI> system-view
[HUAWEI] sysname LSRC
[LSRC] mpls-tp meg test
[LSRC-mpls-tp-meg-test] me te interface tunnel 2/0/0 mep-id 2 rmep-id 1
[LSRC-mpls-tp-meg-test] cc send enable
[LSRC-mpls-tp-meg-test] cc receive enable
```

### 步骤 3 使能 LSRA 设备 MEG 视图下的 AIS 功能

```
<HUAWEI> system-view
[HUAWEI] sysname LSRA
[LSRA-mpls-tp-meg-test] ais enable
```

### 步骤 4 验证配置结果

配置成功后，在 LSRA 设备的接口视图下使用 **display this** 命令查看当前设备上的 AIS 信息。

```
[LSRA-mpls-tp-meg-test] display this
#
mpls-tp meg test
me te interface tunnel 1/0/0 mep-id 1 rmep-id 2
cc send enable
cc receive enable
ais enable
#
```

----结束

## 配置文件

### ● LSRA 的配置文件

```
#
sysname LSRA
#
mpls lsr-id 1.1.1.1
mpls
mpls te
#
bidirectional static-cr-lsp ingress Tunnel1/0/0
forward nexthop 2.1.1.2 out-label 20 bandwidth ct0 10000
backward in-label 20
#
interface Pos1/0/0
undo shutdown
ip address 2.1.1.1 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface LoopBack1
ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 3.3.3.3
mpls te signal-protocol cr-static
```

```
mpls te tunnel-id 100
mpls te bidirectional
mpls te commit
#
ip route-static 2.2.2.2 255.255.255.255 2.1.1.2
ip route-static 3.3.3.3 255.255.255.255 2.1.1.2
#
mpls-tp meg test
me te interface Tunnel1/0/0 mep-id 1 remote-mep-id 2
cc send enable
cc receive enable
ais enable
#
return
```

#### ● LSRB 的配置文件

```
#
sysname Quidway
#
mpls lsr-id 2.2.2.2
mpls
mpls te
#
bidirectional static-cr-lsp transit lsp1
forward in-label 20 nexthop 3.2.1.2 out-label 40 bandwidth ct0 10000
backward in-label 16 nexthop 2.1.1.1 out-label 20 bandwidth ct0 10000
#
interface Pos1/0/0
undo shutdown
ip address 2.1.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
ais enable
#
interface Pos2/0/0
undo shutdown
ip address 3.2.1.1 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
ais enable
#
interface LoopBack1
ip address 2.2.2.2 255.255.255.255
#
ip route-static 1.1.1.1 255.255.255.255 2.1.1.1
ip route-static 3.3.3.3 255.255.255.255 3.2.1.2
#
return
```

#### ● LSRC 的配置文件

```
#
sysname LSRC
#
mpls lsr-id 3.3.3.3
mpls
mpls te
#
bidirectional static-cr-lsp egress lsp1
forward in-label 40 lsrid 1.1.1.1 tunnel-id 100
backward nexthop 3.2.1.1 out-label 16 bandwidth ct0 10000
#
interface Pos1/0/0
undo shutdown
ip address 3.2.1.2 255.255.255.0
mpls
mpls te
```

```
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
interface Tunnel2/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 1.1.1.1
 mpls te signal-protocol cr-static
 mpls te tunnel-id 200
 mpls te passive-tunnel
 mpls te binding bidirectional static-cr-lsp egress lspl
 mpls te commit
#
 ip route-static 1.1.1.1 255.255.255.255 3.2.1.1
 ip route-static 2.2.2.2 255.255.255.255 3.2.1.1
#
mpls-tp meg test
 me te interface Tunnel2/0/0 mep-id 2 remote-mep-id 1
 cc send enable
 cc receive enable
#
return
```

## 10.4.6 配置 PW 持续连通性和转发故障检测（CC/CV）功能示例

该组网的特点是 PE 之间通过基于双向 LSP 的 PW 互连，使用 CC/CV 功能完成对 PE 之间的持续连通性和故障检测，从而实现对 MPLS-TP 网络的故障进行管理。

### 组网需求

如图 10-10 所示，PE1，PE2 和 PE3 通过基于双向 LSP 的 PW 互连。为了保证 PE1 和 PE3 之间的连通性和报文转发正确性做如下部署：

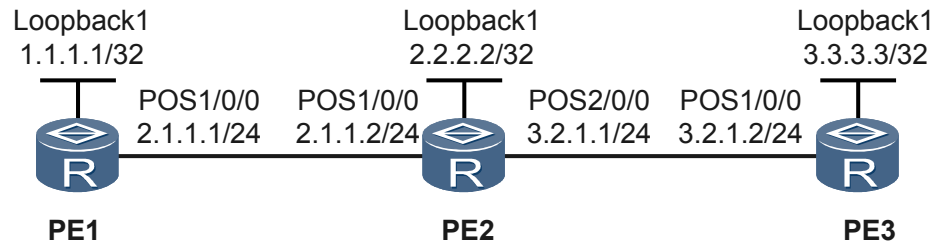
- PE1 和 PE3 作为 MEP 端点
- PE2 作为 MIP 端点

在 MEP 端点上配置 CC/CV 功能。

- 双向 LSP 持续连通性检测（CC）作为一种主动性的 OAM，用于检测一个 MEG 中任何一对 MEP 间连续性的丢失。本端周期性的向目的端发送 CCM 报文，如果目的端在 3.5 个报文发送周期内没有收到 CCM 报文，则认为本端到目的端连通性有问题，上报告警，同时进入故障状态并触发 APS 倒换。当目的端重新收到本端发送的 CCM 报文，则恢复告警并且退出故障状态。
- 双向 LSP 转发故障检测（CV）同样是一种主动性的 OAM，MEP 在接收到非预期的报文时会报告警。比如使能 CV 检测功能的设备从某条 PW 收到报文，却发现该报文不是这条 PW 应该承载的，此时会上报转发错误告警。

传送网对于数据转发正确性要求很高，而 MPLS-TP 要求数据平面可在不具有 IP 能力的情况下工作，即只依赖于标签进行转发操作，所以必须保证标签转发的正确性。

图 10-10 基于双向 LSP 的 PW 组网图



## 配置思路

采用如下的思路配置 PW 持续连通性和转发故障检测功能：

1. 配置 ME 实例并绑定到一条双向 PW。
2. 配置检测报文（CC 报文）发送周期和报文优先级。
3. 使能 CC/CV 检测功能。

## 数据准备

为完成此配置例，需准备如下的数据：

- MEG 名称。
- ME 绑定 VC ID。
- 检测报文（CC 报文）发送周期和报文优先级。

## 操作步骤

### 步骤 1 配置基于双向 LSP 的 PW

LSR 之间的基于双向 LSP 的 PW，具体配置过程略。请参考《HUAWEI NetEngine80E/40E 路由器配置指南 MPLS》中的“配置双向 PW”或者本配置举例中的配置文件。

### 步骤 2 配置 ME 实例并绑定到一条双向 PW

# 在 PE1 上配置 ME 实例名称为 test，并绑定到 PW 链路。

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] mpls-tp meg test
[PE1-mpls-tp-meg-test] me l2vc peer-ip 3.3.3.3 vc-id 30000 vc-type vlan mep-id 1 remote-mep-id 2
```

# 在 PE3 上配置 ME 实例名称为 test，并绑定到 PW 链路。

```
<HUAWEI> system-view
[HUAWEI] sysname PE3
[PE3] mpls-tp meg test
[PE3-mpls-tp-meg-test] me l2vc peer-ip 1.1.1.1 vc-id 30000 vc-type vlan mep-id 2 remote-mep-id 1
```

### 步骤 3 使能 CC/CV 检测功能

# 在 PE1 上使能 CC/CV 检测功能。

```
[PE1-mpls-tp-meg-test] cc send enable
[PE1-mpls-tp-meg-test] cc receive enable
[PE1-mpls-tp-meg-test] return
```

# 在 PE3 上使能 CC/CV 检测功能。



```
[PE3-mpls-tp-meg-test] cc send enable
[PE3-mpls-tp-meg-test] cc receive enable
[PE3-mpls-tp-meg-test] return
```

#### 步骤4 验证配置结果

配置成功后，在 PE1 设备上使用 **display mpls-tp oam meg** 命令查看当前设备上的 MEG 信息。

```
<PE1> display mpls-tp oam meg test

MEG abc

meg name : test
meg level : 7
me count : 1
cc send : enable
cc receive : enable
cc interval : 1000
cc exp : 7
ais : disable
ais interval : 1000
ais exp : 7
lock : disable
lock interval : 1000
lock exp : 7
csf : disable
csf interval : 1000
csf exp : 7
lm single-end receive : disable
lm single-end pro-active : enable
lm single-end SD1 threshold : 1
lm single-end SD2 threshold : 10
lm dual-end : disable

[ME 1]
index : 0
direction : dual
mep id : 1
remote mep id : 2
status board : 3
service type : vll-pw
peer ip : 1.1.1.1
remote peer ip : 2.2.2.2
vc id : 30000
vc type : VLAN
ttl : 2
state : UP
alarm indicate : no alarm

```

----结束

## 配置文件

- PE1 的配置文件

```
#
sysname PE1
#
mpls lsr-id 1.1.1.1
mpls
mpls te
#
mpls l2vpn
#
bidirectional static-cr-lsp ingress Tunnel1/0/0
forward nexthop 2.1.1.2 out-label 20 bandwidth ct0 10000
backward in-label 20
```

```
#
pw-template tpatoc
 peer-address 3.3.3.3
 control-word
 tnl-policy tpatoc
#
interface Pos1/0/0
 undo shutdown
 ip address 2.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
#
interface POS1/0/0.1
 vlan-type dot1q 1
 mpls
 mpls static-l2vc pw-template tpatoc 30000 transmit-vpn-label 101 receive-vpn-label 101
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 2.2.2.2
 mpls te signal-protocol cr-static
 mpls te tunnel-id 100
 mpls te bidirectional
 mpls te reserved-for-binding
 mpls te commit
#
ip route-static 2.2.2.2 255.255.255.255 2.1.1.2
ip route-static 3.3.3.3 255.255.255.255 2.1.1.2
#
tunnel-policy tpatoc
 tunnel binding destination 2.2.2.2 te Tunnel1/0/0
#
mpls-tp meg test
 me l2vc peer-ip 3.3.3.3 vc-id 30000 vc-type vlan mep-id 1 remote-mep-id 2
 cc send enable
 cc receive enable
#
return
```

## ● PE2 的配置文件

```
#
sysname PE2
#
mpls lsr-id 2.2.2.2
mpls
 mpls te
#
bidirectional static-cr-lsp transit lsp1
 forward in-label 20 nexthop 3.2.1.2 out-label 40 bandwidth ct0 10000
 backward in-label 16 nexthop 2.1.1.1 out-label 20 bandwidth ct0 10000
#
interface Pos1/0/0
 undo shutdown
 ip address 2.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 ais enable
#
interface Pos2/0/0
 undo shutdown
 ip address 3.2.1.1 255.255.255.0
 mpls
```

```
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
ais enable
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
 ip route-static 1.1.1.1 255.255.255.255 2.1.1.1
 ip route-static 3.3.3.3 255.255.255.255 3.2.1.2
#
return
```

## ● PE3 的配置文件

```
#
 sysname PE3
#
 mpls lsr-id 3.3.3.3
 mpls
 mpls te
#
 mpls l2vpn
#
 bidirectional static-cr-lsp egress lspl
 forward in-label 40 lsrid 1.1.1.1 tunnel-id 100
 backward nexthop 3.2.1.1 out-label 16 bandwidth ct0 10000
#
 pw-template tpcto
 peer-address 1.1.1.1
 control-word
 tnl-policy tpcto
#
 interface Pos1/0/0
 undo shutdown
 ip address 3.2.1.2 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
#
 interface POS1/0/0.1
 vlan-type dot1q 1
 mpls static-l2vc pw-template tpcto 30000 transmit-vpn-label 101 receive-vpn-label 101
#
 interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
 interface Tunnel2/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 1.1.1.1
 mpls te signal-protocol cr-static
 mpls te tunnel-id 200
 mpls te passive-tunnel
 mpls te binding bidirectional static-cr-lsp egress lspl
 mpls te reserved-for-binding
 mpls te commit
#
 ip route-static 1.1.1.1 255.255.255.255 3.2.1.1
 ip route-static 2.2.2.2 255.255.255.255 3.2.1.1
#
 tunnel-policy tpcto
 tunnel binding destination 1.1.1.1 te Tunnel1/0/0
#
 mpls-tp meg test
 me l2vc peer-ip 1.1.1.1 vc-id 30000 vc-type vlan mep-id 2 remote-mep-id 1
 cc send enable
 cc receive enable
```

```
#
return
```

## 10.4.7 配置 PW 按需连通性检测（LB）功能示例

该组网的特点是 PE 之间通过基于双向 LSP 的 PW 互连，使用 CC/CV 功能完成对 PE 之间的持续连通性和故障检测，从而实现对 MPLS-TP 网络的故障进行管理。

### 组网需求

如图 10-11 所示，PE1、PE2 和 PE3 通过基于双向 LSP 的 PW 互连。为了保证 PE1 和 PE3 之间的连通性和报文转发正确性做如下部署：

- PE1 和 PE3 作为 MEP 端点
- PE2 作为 MIP 端点

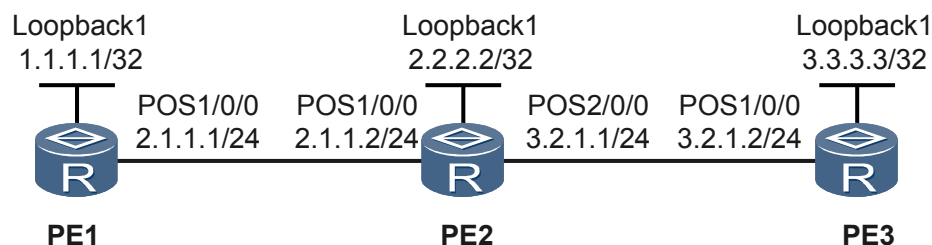
使用 LB 功能可以来检测：

- 远端 MEP 设备是否可达
- 本端 MEP 与远端 MEP 通信的来回旅程（round-trip）的延迟（delay）
- 本端 MEP 与远端 MEP 之间探测报文的丢失情况

 说明

LB 只对发送的探测报文的丢失情况进行统计，从而粗略的了解 MEP 之间的丢包率。如果要获得 MEP 之间流量的丢包率可以使用 LM 检测功能。

图 10-11 基于双向 LSP 的 PW 组网图



### 配置思路

采用如下的思路配置 VLL 的单向时延计功能：

1. 配置 ME 实例并绑定到一条双向 PW。
2. 启动 LB 检测功能。

### 数据准备

为完成此配置例，需准备如下的数据：

- MEG 名称。
- ME 绑定 VC ID。

## 操作步骤

### 步骤 1 配置基于双向 LSP 的 PW

LSR 之间的基于双向 LSP 的 PW，具体配置过程略。请参考《HUAWEI NetEngine80E/40E 路由器配置指南 MPLS》中的“配置双向 PW”或者本配置举例中的配置文件。

### 步骤 2 配置 ME 实例并绑定到一条双向 PW

# 在 PE1 上配置 ME 实例名称为 test，并绑定到 PW 链路。

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] mpls-tp meg test
[PE1-mpls-tp-meg-test] me l2vc peer-ip 3.3.3.3 vc-id 30000 vc-type vlan mep-id 1 remote-mep-id 2
```

# 在 PE3 上配置 ME 实例名称为 test，并绑定到 PW 链路。

```
<HUAWEI> system-view
[HUAWEI] sysname PE3
[PE3] mpls-tp meg test
[PE3-mpls-tp-meg-test] me l2vc peer-ip 1.1.1.1 vc-id 30000 vc-type vlan mep-id 2 remote-mep-id 1
```

### 步骤 3 启动 LB 检测功能

 说明

LB 支持本端 MEP 到远端 MEP 或者 MIP 之间的连通性检测，本示例以 PE1 到 PE2 的连通性检测为例。

在 PE1 上使能 LB 检测功能。

```
<PE1> ping meg test
PING test: 9 data bytes, press CTRL_C to break
 Reply from vsi: bytes=9, Sequence=1 time=100 ms
 Reply from vsi: bytes=9, Sequence=2 time=90 ms
 Reply from vsi: bytes=9, Sequence=3 time=100 ms
--- ping statistics ---
 3 packet(s) transmitted
 3 packet(s) received
 0.00% packet loss
 round-trip min/avg/max 90/96/100 ms
```

----结束

## 配置文件

### ● PE1 的配置文件

```
#
sysname PE1
#
mpls lsr-id 1.1.1.1
mpls
mpls te
#
mpls l2vpn
#
bidirectional static-cr-lsp ingress Tunnel1/0/0
 forward nexthop 2.1.1.2 out-label 20 bandwidth ct0 10000
 backward in-label 20
#
pw-template tpatoc
 peer-address 3.3.3.3
 control-word
 tnl-policy tpatoc
#
interface Pos1/0/0
 undo shutdown
 ip address 2.1.1.1 255.255.255.0
mpls
```

```
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface POS1/0/0.1
vlan-type dot1q 1
mpls
mpls static-l2vc pw-template tpatoc 30000 transmit-vpn-label 101 receive-vpn-label 101
#
interface LoopBack1
ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 2.2.2.2
mpls te signal-protocol cr-static
mpls te tunnel-id 100
mpls te bidirectional
mpls te reserved-for-binding
mpls te commit
#
ip route-static 2.2.2.2 255.255.255.255 2.1.1.2
ip route-static 3.3.3.3 255.255.255.255 2.1.1.2
#
tunnel-policy tpatoc
tunnel binding destination 2.2.2.2 te Tunnel1/0/0
#
mpls-tp meg test
me l2vc peer-ip 3.3.3.3 vc-id 30000 vc-type vlan mep-id 1 remote-mep-id 2
#
return
```

## ● PE2 的配置文件

```
#
sysname PE2
#
mpls lsr-id 2.2.2.2
mpls
mpls te
#
bidirectional static-cr-lsp transit lsp1
forward in-label 20 nexthop 3.2.1.2 out-label 40 bandwidth ct0 10000
backward in-label 16 nexthop 2.1.1.1 out-label 20 bandwidth ct0 10000
#
interface Pos1/0/0
undo shutdown
ip address 2.1.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
ais enable
#
interface Pos2/0/0
undo shutdown
ip address 3.2.1.1 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
ais enable
#
interface LoopBack1
ip address 2.2.2.2 255.255.255.255
#
ip route-static 1.1.1.1 255.255.255.255 2.1.1.1
ip route-static 3.3.3.3 255.255.255.255 3.2.1.2
```

```
#
return
● PE3 的配置文件
#
sysname PE3
#
mpls lsr-id 3.3.3.3
mpls
mpls te
#
mpls l2vpn
#
bidirectional static-cr-lsp egress lspl
forward in-label 40 lsrid 1.1.1.1 tunnel-id 100
backward nexthop 3.2.1.1 out-label 16 bandwidth ct0 10000
#
pw-template tpcto
peer-address 1.1.1.1
control-word
tnl-policy tpcto
#
interface Pos1/0/0
undo shutdown
ip address 3.2.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface POS1/0/0.1
vlan-type dot1q 1
mpls static-l2vc pw-template tpcto 30000 transmit-vpn-label 101 receive-vpn-label 101
#
interface LoopBack1
ip address 3.3.3.3 255.255.255.255
#
interface Tunnel2/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 1.1.1.1
mpls te signal-protocol cr-static
mpls te tunnel-id 200
mpls te passive-tunnel
mpls te binding bidirectional static-cr-lsp egress lspl
mpls te reserved-for-binding
mpls te commit
#
ip route-static 1.1.1.1 255.255.255.255 3.2.1.1
ip route-static 2.2.2.2 255.255.255.255 3.2.1.1
#
tunnel-policy tpcto
tunnel binding destination 1.1.1.1 te Tunnel1/0/0
#
mpls-tp meg test
me l2vc peer-ip 1.1.1.1 vc-id 30000 vc-type vlan mep-id 2 remote-mep-id 1
#
return
```

## 10.4.8 配置 PW 丢包率统计（LM）功能示例

该组网的特点是 PE 之间通过基于双向 LSP 的 PW 互连，使用 LM 功能完成对 LSR 之间的丢包率进行检测，从而实现对 MPLS-TP 网络的性能进行统计。

## 组网需求

MPLS-TP 作为面向连接的包交换技术，旨在将现有基于电路交换的传送网络，改造成基于包交换的传送网络。其根本目的在于提高传统电路交换网络的尽可能地使用统计复用的包交换网络来尽量提高传输效率。

但是，在应用 MPLS-TP 技术提升带宽利用率同时，必须保证链路的可靠性。例如语音业务，当链路丢包率在 10% 以下时，用户不会有明显的感觉。但是当丢包率大于 20% 时，就会影响语音的质量。

此时可以使用丢包率度量 LM（Packet Loss Measurement）检测功能对设备间丢包率进行统计，了解链路的真实性能。LM 是 MPLS-TP 性能监控 PM（Performance Monitoring）的一项功能，可以实现两种 LM，第一种称为单端（Single-end）LM，第二种称为双端（Dual-end）LM。

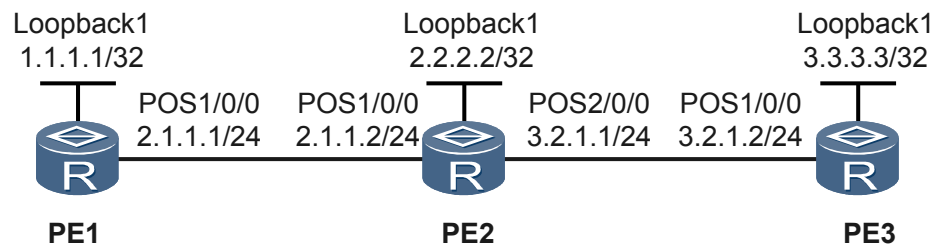
### 说明

本示例仅以双端丢包统计为例，单端丢包除了统计结果查询与双端丢包统计不同，其它配置与双端丢包统计配置相同，不再赘述。

如图 10-12 所示，PE1，PE2 和 PE3 通过基于双向 LSP 的 PW 互连。为了保证 PE1 和 PE3 之间的连通可靠性做如下部署，实现 PE1 和 PE3 之间的双端丢包统计：

- PE1 和 PE3 作为 MEP 端点
- PE2 作为 MIP 端点

图 10-12 基于双向 LSP 的 PW 组网图



## 配置思路

采用如下的思路配置 PW 丢包率统计功能：

1. 配置 ME 实例并绑定到一条双向 PW。
2. 使能本端和对端 CC 检测功能。
3. 配置丢包率统计阈值告警。
4. 使能双端丢包统计功能。

## 数据准备

为完成此配置例，需准备如下的数据：

- MEG 名称。
- ME 绑定 VC ID。
- 丢包率统计发送告警的阈值。



## 操作步骤

### 步骤 1 配置基于双向 LSP 的 PW

LSR 之间的基于双向 LSP 的 PW，具体配置过程略。请参考《HUAWEI NetEngine80E/40E 路由器配置指南 MPLS》中的“配置双向 PW”或者本配置举例中的配置文件。

### 步骤 2 配置 ME 实例并绑定到一条双向的 PW

# 在 PE1 上配置 ME 实例名称为 test，并绑定到 PW 链路。

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] mpls-tp meg test
[PE1-mpls-tp-meg-test] me l2vc peer-ip 3.3.3.3 vc-id 30000 vc-type vlan mep-id 1 remote-mep-id 2
```

# 在 PE3 上配置 ME 实例名称为 test，并绑定到 PW 链路。

```
<HUAWEI> system-view
[HUAWEI] sysname PE3
[PE3] mpls-tp meg test
[PE3-mpls-tp-meg-test] me l2vc peer-ip 1.1.1.1 vc-id 30000 vc-type vlan mep-id 2 remote-mep-id 1
```

### 步骤 3 使能本端和对端 CC 检测功能

# 在 PE1 上使能 CC 检测功能。

```
[PE1-mpls-tp-meg-test] cc send enable
[PE1-mpls-tp-meg-test] cc receive enable
```

# 在 PE3 上使能 CC 检测功能。

```
[PE3-mpls-tp-meg-test] cc send enable
[PE3-mpls-tp-meg-test] cc receive enable
```

### 步骤 4 配置丢包率统计阈值告警

# 在 PE1 上配置丢包率统计阈值告警。

```
[PE1-mpls-tp-meg-test] lost-measure dual-ended loss-ratio threshold1 50
```

# 在 PE3 上配置丢包率统计阈值告警。

```
[PE3-mpls-tp-meg-test] lost-measure dual-ended loss-ratio threshold1 50
```

### 步骤 5 使能双端丢包统计功能

# 在 PE1 上使能双端丢包统计功能。

```
[PE1-mpls-tp-meg-test] lost-measure dual-ended enable
[PE1-mpls-tp-meg-test] return
```

# 在 PE3 上使能双端丢包统计功能。

```
[PE3-mpls-tp-meg-test] lost-measure dual-ended enable
[PE3-mpls-tp-meg-test] return
```

### 步骤 6 验证配置结果

配置成功后，在 PE1 设备上使用 **display mpls-tp oam** 命令查看当前设备上的丢包率统计信息。

```
<PE1> display mpls-tp oam meg test statistic-type lost-measure dual-ended
Dual-end loss measurement statistics:
Index Near-end lost frames Loss ratio Far-end lost frames Loss ratio
1 10 12.50% 10 12.50%
Max near-end lost frames:10,frame loss ratio:12.50%
Min near-end lost frames:10,frame loss ratio:12.50%
Average near-end lost frames:10,frame loss ratio:12.50%
Max far-end lost frames:10,frame loss ratio:12.50%
Min far-end lost frames:10,frame loss ratio:12.50%
Average far-end lost frames:10,frame loss ratio:12.50%
```

----结束

## 配置文件

### ● PE1 的配置文件

```
#
sysname PE1
#
mpls lsr-id 1.1.1.1
mpls
mpls te
#
mpls l2vpn
#
bidirectional static-cr-lsp ingress Tunnel1/0/0
forward nexthop 2.1.1.2 out-label 20 bandwidth ct0 10000
backward in-label 20
#
pw-template tpatoc
peer-address 3.3.3.3
control-word
tnl-policy tpatoc
#
interface Pos1/0/0
undo shutdown
ip address 2.1.1.1 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface POS1/0/0.1
vlan-type dot1q 1
mpls
mpls static-l2vc pw-template tpatoc 30000 transmit-vpn-label 101 receive-vpn-label 101
#
interface LoopBack1
ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 2.2.2.2
mpls te signal-protocol cr-static
mpls te tunnel-id 100
mpls te bidirectional
mpls te reserved-for-binding
mpls te commit
#
ip route-static 2.2.2.2 255.255.255.255 2.1.1.2
ip route-static 3.3.3.3 255.255.255.255 2.1.1.2
#
tunnel-policy tpatoc
tunnel binding destination 2.2.2.2 te Tunnel1/0/0
#
mpls-tp meg test
me l2vc peer-ip 3.3.3.3 vc-id 30000 vc-type vlan mep-id 1 remote-mep-id 2
cc send enable
cc receive enable
#
return
```

### ● PE2 的配置文件

```
#
sysname PE2
#
mpls lsr-id 2.2.2.2
mpls
mpls te
#
bidirectional static-cr-lsp transit lsp1
```

```

 forward in-label 20 nexthop 3.2.1.2 out-label 40 bandwidth ct0 10000
 backward in-label 16 nexthop 2.1.1.1 out-label 20 bandwidth ct0 10000
#
interface Pos1/0/0
undo shutdown
ip address 2.1.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface Pos2/0/0
undo shutdown
ip address 3.2.1.1 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface LoopBack1
ip address 2.2.2.2 255.255.255.255
#
ip route-static 1.1.1.1 255.255.255.255 2.1.1.1
ip route-static 3.3.3.3 255.255.255.255 3.2.1.2
#
return

```

#### ● PE3 的配置文件

```

#
sysname PE3
#
mpls lsr-id 3.3.3.3
mpls
mpls te
#
mpls l2vpn
#
bidirectional static-cr-lsp egress lspl
forward in-label 40 lsrid 1.1.1.1 tunnel-id 100
backward nexthop 3.2.1.1 out-label 16 bandwidth ct0 10000
#
pw-template tpcto
peer-address 1.1.1.1
control-word
tnl-policy tpcto
#
interface Pos1/0/0
undo shutdown
ip address 3.2.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface POS1/0/0.1
vlan-type dot1q 1
mpls static-l2vc pw-template tpcto 30000 transmit-vpn-label 101 receive-vpn-label 101
#
interface LoopBack1
ip address 3.3.3.3 255.255.255.255
#
interface Tunnel2/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 1.1.1.1
mpls te signal-protocol cr-static
mpls te tunnel-id 200
mpls te passive-tunnel
mpls te binding bidirectional static-cr-lsp egress lspl
mpls te reserved-for-binding

```

```
mpls te commit
#
ip route-static 1.1.1.1 255.255.255.255 3.2.1.1
ip route-static 2.2.2.2 255.255.255.255 3.2.1.1
#
tunnel-policy tpcto
tunnel binding destination 1.1.1.1 te Tunnel1/0/0
#
mpls-tp meg test
me l2vc peer-ip 1.1.1.1 vc-id 30000 vc-type vlan mep-id 2 remote-mep-id 1
cc send enable
cc receive enable
#
return
```

## 10.4.9 配置 PW 时延和抖动统计（DM）功能示例

该组网的特点是 PE 之间通过基于双向 LSP 的 PW 互连，使用 DM 功能完成对 PE 之间的时延和抖动进行检测，从而实现对 MPLS-TP 网络的性能进行统计。

### 组网需求

MPLS-TP 作为面向连接的包交换技术，旨在将现有基于电路交换的传送网络，改造成基于包交换的传送网络。其根本目的在于提高传统电路交换网络的尽可能地使用统计复用的包交换网络来尽量提高传输效率。

但是，在应用 MPLS-TP 技术提升带宽利用率同时，必须保证链路的可靠性。例如语音业务，由于 VoIP 业务需要对语音包进行编码和解码，再加上传输的时延，这就使得 VoIP 业务的时延要比普通基于电路交换的电话时延大得多。如果时延大于 400ms 就可以明显的感觉出来。如果时延大于 2 秒会导致 VoIP 业务基本不可用。同时，当抖动超过一个语音包的时长时，语音质量就会明显下降。

此时可以使用时延和抖动度量 DM（Delay Measurement）检测功能对设备间时延和抖动进行统计，了解链路的真实性能。DM 是 MPLS-TP 性能监控 PM（Performance Monitoring）的一项功能，可以实现两种 LM，第一种称为单向（One-way）LM，第二种称为双向（Two-end）DM。

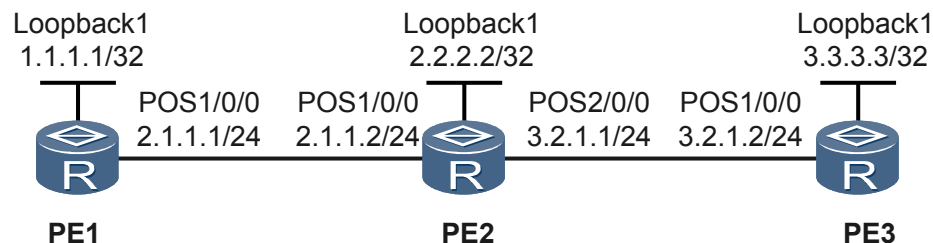
#### 说明

本示例仅以双端时延和抖动统计为例，单端时延和抖动除了统计结果查询与双端时延和抖动统计不同，其它配置与双端时延和抖动统计配置相同，不再赘述。

如图 10-13 所示，PE1、PE2 和 PE3 通过基于双向 LSP 的 PW 互连。为了保证 PE1 和 PE3 之间的连通可靠性做如下部署，实现 PE1 和 PE3 之间的时延和抖动统计：

- PE1 和 PE3 作为 MEP 端点
- PE2 作为 MIP 端点

图 10-13 基于双向 LSP 的 PW 组网图



## 配置思路

采用如下的思路配置 PW 时延和抖动统计功能：

1. 配置 ME 实例并绑定到一条双向的 PW。
2. 使能本端和对端 CC 检测功能。
3. 使能双向时延和抖动统计功能。

## 数据准备

为完成此配置例，需准备如下的数据：

- MEG 名称。
- ME 绑定 VC ID。

## 操作步骤

### 步骤 1 配置基于双向 LSP 的 PW

LSR 之间的基于双向 LSP 的 PW，具体配置过程略。请参考《HUAWEI NetEngine80E/40E 路由器 配置指南 MPLS》中的“配置双向 PW”或者本配置举例中的配置文件。

### 步骤 2 配置 ME 实例并绑定到一条双向 PW

# 在 PE1 上配置 ME 实例名称为 test，并绑定到 PW 链路。

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] mpls-tp meg test
[PE1-mpls-tp-meg-test] me l2vc peer-ip 3.3.3.3 vc-id 30000 vc-type vlan mep-id 1 remote-mep-id 2
```

# 在 PE3 上配置 ME 实例名称为 test，并绑定到 PW 链路。

```
<HUAWEI> system-view
[HUAWEI] sysname PE3
[PE3] mpls-tp meg test
[PE3-mpls-tp-meg-test] me l2vc peer-ip 1.1.1.1 vc-id 30000 vc-type vlan mep-id 2 remote-mep-id 1
```

### 步骤 3 使能双向时延和抖动统计功能

```
<PE1> delay-measure two-way
Two-way delay measure statistics
delay(us): delay variation(us):
100 --
100 0
100 0
99 1
100 1
The Max delay:100, The Max delay variation:1
The Min delay:99, The Min delay variation:0
The delay average:100, The delay variation average:1
Total sent Packets Number:5, Total received Packets Number: 5
```

----结束

## 配置文件

- PE1 的配置文件

```
#
sysname PE1
#
mpls lsr-id 1.1.1.1
mpls
```

```

mpls te
#
mpls l2vpn
#
bidirectional static-cr-lsp ingress Tunnel1/0/0
 forward nexthop 2.1.1.2 out-label 20 bandwidth ct0 10000
 backward in-label 20
#
pw-template tpatoc
 peer-address 3.3.3.3
 control-word
 tnl-policy tpatoc
#
interface Pos1/0/0
 undo shutdown
 ip address 2.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
#
interface POS1/0/0.1
 vlan-type dot1q 1
 mpls
 mpls static-l2vc pw-template tpatoc 30000 transmit-vpn-label 101 receive-vpn-label 101
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 2.2.2.2
 mpls te signal-protocol cr-static
 mpls te tunnel-id 100
 mpls te bidirectional
 mpls te reserved-for-binding
 mpls te commit
#
ip route-static 2.2.2.2 255.255.255.255 2.1.1.2
ip route-static 3.3.3.3 255.255.255.255 2.1.1.2
#
tunnel-policy tpatoc
 tunnel binding destination 2.2.2.2 te Tunnel1/0/0
#
mpls-tp meg test
 me l2vc peer-ip 3.3.3.3 vc-id 30000 vc-type vlan mep-id 1 remote-mep-id 2
#
return

```

## ● PE2 的配置文件

```

#
sysname PE2
#
mpls lsr-id 2.2.2.2
mpls
mpls te
#
bidirectional static-cr-lsp transit lsp1
 forward in-label 20 nexthop 3.2.1.2 out-label 40 bandwidth ct0 10000
 backward in-label 16 nexthop 2.1.1.1 out-label 20 bandwidth ct0 10000
#
interface Pos1/0/0
 undo shutdown
 ip address 2.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 ais enable

```

```
#
interface Pos2/0/0
undo shutdown
ip address 3.2.1.1 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
ais enable
#
interface LoopBack1
ip address 2.2.2.2 255.255.255.255
#
ip route-static 1.1.1.1 255.255.255.255 2.1.1.1
ip route-static 3.3.3.3 255.255.255.255 3.2.1.2
#
return
```

#### ● PE3 的配置文件

```
#
sysname PE3
#
mpls lsr-id 3.3.3.3
mpls
mpls te
#
mpls l2vpn
#
bidirectional static-cr-lsp egress lspl
forward in-label 40 lsrid 1.1.1.1 tunnel-id 100
backward nexthop 3.2.1.1 out-label 16 bandwidth ct0 10000
#
pw-template tpcto
peer-address 1.1.1.1
control-word
tnl-policy tpcto
#
interface Pos1/0/0
undo shutdown
ip address 3.2.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
#
interface POS1/0/0.1
vlan-type dot1q 1
mpls static-l2vc pw-template tpcto 30000 transmit-vpn-label 101 receive-vpn-label 101
#
interface LoopBack1
ip address 3.3.3.3 255.255.255.255
#
interface Tunnel2/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 1.1.1.1
mpls te signal-protocol cr-static
mpls te tunnel-id 200
mpls te passive-tunnel
mpls te binding bidirectional static-cr-lsp egress lspl
mpls te reserved-for-binding
mpls te commit
#
ip route-static 1.1.1.1 255.255.255.255 3.2.1.1
ip route-static 2.2.2.2 255.255.255.255 3.2.1.1
#
tunnel-policy tpcto
tunnel binding destination 1.1.1.1 te Tunnel1/0/0
#
mpls-tp meg test
```

```
me l2vc peer-ip 1.1.1.1 vc-id 30000 vc-type vlan mep-id 2 remote-mep-id 1
#
return
```



# 11 多机备份配置

---

## 关于本章

通过多机备份实现设备间的 ARP 表项等的备份，提高业务运行的可靠性。

### 11.1 简介

互为备份的设备之间通过 TCP 传输协议备份 ARP 表项等。

### 11.2 建立多机备份平台

通过建立多机备份平台实现端口、链路等异常触发业务快速切换。

### 11.3 配置 ARP 双机热备

配置 ARP 双机热备，实现对 VRRP 双机的 ARP 表项备份，以在实现主备切换时保持链路的畅通。

### 11.4 维护

使用监控和清除统计信息命令，查看备份信息，检查配置的效果。

### 11.5 配置举例

介绍多机备份的各种示例。配置示例中包括组网需求、配置注意事项和配置思路等。

## 11.1 简介

互为备份的设备之间通过 TCP 传输协议备份 ARP 表项等。

### 11.1.1 多机备份概述

多机备份通过 VRRP 建立 VRRP 备份组，实现 ARP 双机热备。



说明

NE80E/40E 系列中的 X1 和 X2 设备不支持 RUI 协议，不支持备份 BRAS 用户信息。

- **ARP 双机热备：**

实时保持主备设备上的 ARP 信息同步，包括由 ARP 触发生成的主机路由信息。  
VRRP 主备切换之后，不用做 ARP 学习，下行流量即可接通。

### 11.1.2 NE80E/40E 支持的多机备份特性

NE80E/40E 支持的多机备份包括建立多机备份平台后，实现 ARP 双机热备。

#### 远端备份服务(RBS)

RBS (remote-backup-service) 远端备份服务是从 RUI 中分离出来的模块。将 RUI 公共的部分放在 RBS 中，使 RBS 作为一个通用备份模块，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。

目前 RUI 可以支持 4 个 TCP 连接，多机备份功能启动时，IP 地址较大的设备建立 TCP 监听 SOCKET，而 IP 地址较小的设备则向对端发起建立 TCP 的连接。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。

#### 远端备份策略(RBP)

RBP (remote-backup-profile) 远端备份策略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。

#### 实时备份和批量备份

设备间信息的备份方式分为实时备份和批量备份。当用户上线、下线、用户租期变更、租期结束或管理员使用户下线时，主路由器实时通知各路由器添加、删除或修改备份记录，实现实时备份。对于新加入的备份设备，或备份链路故障恢复后，则采用批量备份方式确保设备间信息一致。

#### 热备份和温备份

对于收到的备份信息，各路由器有两种处理方式：热备份和温备份。

- **热备份**

当各路由器收到主路由器的备份信息后，立即生成用户信息和转发表项，当发生故障时可以实现业务终端快速切换。

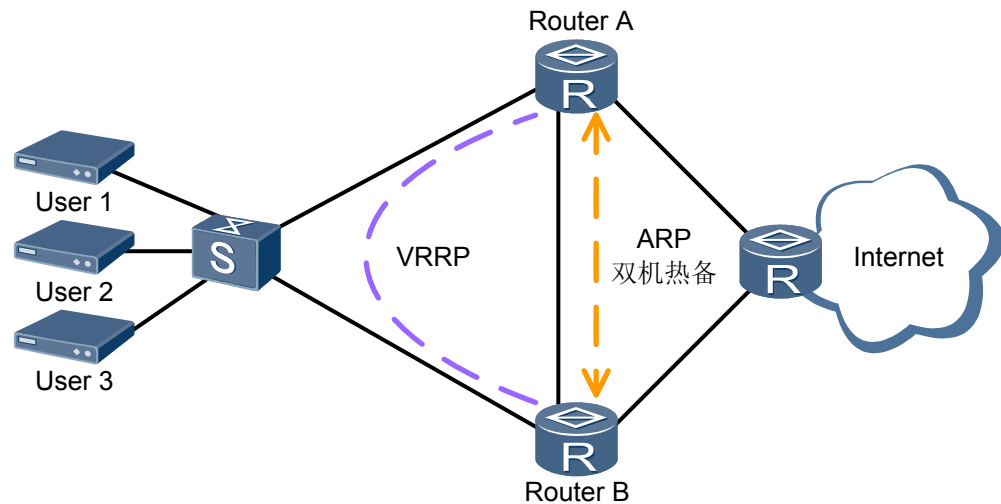
- **温备份**

当各路由器收到主路由器的备份信息后，不立即生成用户信息和转发表项，而是将其保存在主控板内，待发生主备切换后，才开始触发生成用户信息和转发表项，这

种方式适合于 N:1 备份（一备多主）的情况，但业务终端切换时间较长。在实际的部署中，作主的一端要部署为热备份模式，做备的一端部署为温备份模式。

## ARP 双机热备

图 11-1 ARP 双机热备示意图



如图 11-1 所示，ARP 双机热备的主要应用场景是在运行 VRRP 的双机之间备份 ARP 信息，避免因为 VRRP 主用设备与备用设备倒换后，ARP 信息获取不及时而导致的报文丢弃问题。一般情况下，在主用设备和备用设备之间跑 VRRP 协议控制主备角色。正常情况下用户的上行流量和下行流量都经过主用设备转发，一旦主用设备故障，或者主用设备和交换机之间链路故障，备用设备升级为主用设备，用户的上行和下行流量走备用设备转发，这种切换动作用户不感知。VRRP 发生主备切换，备升主之后，新的主用设备需要向上游设备发布网段路由，将下行流量引入新的主用设备。但是此时在新的主用设备上还没有到用户 IP 地址的 ARP 表项，去往用户的下行流量在新的主用设备上触发大量的 ARP MISS，只有当新的主用设备上学到所有下挂的用户 IP 地址的 ARP 之后，下行流量才能通。

这里存在的问题是：备用设备所在的网络位置上，学习用户 IP 地址的 ARP，学习的速度不仅受制于设备自身处理的速度，还受制于用户回应的速度，仅仅优化设备自身 ARP 的处理能力不能从根本上解决下行流量接通慢的问题。

针对上述场景面临的问题，提出 ARP 双机热备的解决方案，基本思路是：在控制层面和转发层面，实时保持主用设备和备用设备上 ARP 信息同步，包括由 ARP 触发生成的主机路由信息。VRRP 主备切换之后，不用做 ARP 学习，下行流量即可接通。

## 11.2 建立多机备份平台

通过建立多机备份平台实现端口、链路等异常触发业务快速切换。

### 11.2.1 建立配置任务

在进行多机备份平台配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

## 应用环境

当 NE80E/40E 作为边缘业务设备时直接与汇聚设备相连，汇聚设备下行与 DSLAM 等设备相连，上行同时与多台 NE80E/40E 相连。当一台或者多台主用 NE80E/40E 设备发生故障时，为了使业务能快速切换到备用设备上，需要多台 NE80E/40E 之间形成 N:1 备份，即多机备份。

多机备份目前采用 VRRP 协议来决策设备的主备关系，VRRP 协议是运行在以太网上的协议。其他的链路检测协议可以与 VRRP 配合，以实现 VRRP 状态变化，这些链路检测协议包括：BFD、802.1ag、802.1ah。

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。

## 前置任务

在建立多机备份平台之前，需完成以下任务：

- 在用户侧配置 Peer BFD、Link BFD 或 ETH OAM。
- 在网络侧配置 Peer BFD。
- 配置一个本地或者远端地址池。互为备份设备上配置的地址池应完全相同。

## 数据准备

在建立多机备份平台之前，需要准备以下数据。

| 序号 | 数据                                                |
|----|---------------------------------------------------|
| 1  | VRRP ID。                                          |
| 2  | 互为备份设备各自的 IP 地址。                                  |
| 3  | Backup ID，可以根据用户的 Backup ID 和远端备份服务确定用户所属的远端备份策略。 |
| 4  | 地址池名称。                                            |

### 11.2.2 配置 VRRP

通过配置 VRRP，实现当主用设备出现故障时，由备用设备承担网路流量。

## 背景信息

 说明

这里只列出了远端信息备份应用中配置 VRRP 的常用步骤，更多信息请参见 VRRP 章节。

在互为备份的设备上进行如下配置。

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

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

**步骤 3** 执行命令 **vrrp vrid virtual-router-ID virtual-ip virtual-address**，建备份组并配置虚拟 IP 地址。

**步骤 4** 执行命令 **admin-vrrp vrid virtual-router-ID**，配置该 VRRP 为管理 VRRP。



说明

VRRP 的类型必须为管理 VRRP。

互为备份的两台设备上配置的 VRID 和虚拟 IP 地址必须一致。

**步骤 5** 执行命令 **vrrp vrid virtual-router-id priority priority-value**，配置路由器在备份组中的优先级。

需要为 VRRP 备份组的两台设备设置不同的优先级，优先级高的为主用设备。

----结束

### 11.2.3 配置远端备份服务

配置远端备份服务包括配置远端服务器的 TCP 连接和监视的接口。

## 背景信息

在互为备份的设备上进行如下配置。

## 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **remote-backup-service service-name**，进入远端备份服务视图。

**步骤 3** 执行命令 **peer peer-ip-address source source-ip-address port port-id**，配置远端服务器 TCP 连接。

*peer-ip-address* 表示互为备份的对端设备 IP 地址，*source-ip-address* 表示互为备份的本端设备 IP 地址。对端设备 IP 地址需要在对端设备某个主接口、子接口或逻辑接口（如 Loopback 接口）上已配置，本端 IP 地址需要在本设备某个主接口、子接口或逻辑接口（如 Loopback 接口）上已配置，并且这两个地址能够互相 ping 通；*port-id* 表示服务器监听的端口号，互为备份的两台设备上对应的 TCP 连接配置的端口号必须相同。



说明

端口号 6000 已经预留给其他协议，不可使用。

**步骤 4** （可选）执行命令 **batch-backup service-type { service-type | all } daily day-time**，配置远端备份服务下所有配置的业务定时同步，保证两端设备上 RUI 表项一致。

**步骤 5** （可选）执行命令 **track interface interface-name**，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。

**步骤 6** （可选）执行命令 **track bfd-session bfd-session**，配置远端备份服务跟踪 bfd 会话状态，快速检测对端状态。



说明

为了达到快速检测的目的，建议用户进行这步配置。使用该命令前，需要在主备设备的网络侧建立 peer bfd 会话。

----结束

## 11.2.4 配置远端备份策略

互为备份的设备上对应远端备份策略下配置的端备份标识符必须相同。

### 背景信息

在互为备份的设备上进行如下配置。

### 操作步骤

- 步骤 1** 执行命令 **system-view**，进入系统视图。
- 步骤 2** 执行命令 **remote-backup-profile profile-name**，进入远端备份策略视图。
- 步骤 3** 执行命令 **peer-backup { hot | warm }**，使能设备间热备份或者温备份。缺省为热备份。
- 步骤 4** 执行命令 **vrrp-id vrid interface interface-type interface-number**，将 vrid 绑定到此远端备份策略视图下。  
  
*vrid* 表示 VRRP 备份组 ID，与相应接口上配置的 VRRP 备份组必须相同。
- 步骤 5** 执行命令 **backup-id backup-id remote-backup-service name**，将此远端备份策略与远端备份服务关联起来。*backup-id* 表示远端备份标识符，可以根据用户的 *backup-id* 和远端备份服务确定用户所属的远端备份策略，互为备份的设备上对应远端备份策略下配置的 *backup-id* 必须相同。

----结束

## 11.2.5 检查配置结果

配置成功后，可以查看到远端服务器连接状态和远端备份策略的配置信息。

### 背景信息

完成上述配置后，请执行下面的命令检查配置结果。

### 操作步骤

- 执行命令 **display remote-backup-profile [ profile-name ]**查看远端备份策略的信息。
- 执行命令 **display remote-backup-service [ service-name [verbose] ]**查看远端备份服务的信息。

----结束

### 任务示例

```
<HUAWEI>display remote-backup-profile test
```

```
Profile-Index : 0x802
Profile-Name : test
Service :
```

```
Remote-backup-service: test
Backup-ID : 10
track protocol : VRRP
VRRP-ID : 1
VRRP-Interface : GigabitEthernet1/0/0.2
Interface :
State : Master
Peer State : Slave
Backup mode : hot
Slot-Number : 1
Card-Number : 0
Port-Number : 0
```

```
<HUAWEI>display remote-backup-service test
```

```

Service-Index : 0
Service-Name : test
TCP-State : Connected
Peer-ip : 88.88.88.88
Source-ip : 22.22.22.22
TCP-Port : 6000
Track-BFD : --
Track-interface0 : GigabitEthernet2/0/0
Track-interface1 : --
Last up time : 2009-11-2 16:15:8
Last down time : 2009-11-2 16:3:36
Last down reason : TCP closed for packet error.
Batch-backup : 03:05:00(Daily)

```

## 11.3 配置 ARP 双机热备

配置 ARP 双机热备，实现对 VRRP 双机的 ARP 表项备份，以在实现主备切换时保持链路的畅通。

### 11.3.1 建立配置任务

在进行 ARP 双机热备配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

#### 应用环境

为了提高网络的可靠性，尽量缩短主备 VRRP 设备切换后用户的断网时间，需要在主备设备之间配置 ARP 双机热备。在控制层面和转发层面，实时保持主用设备和备用设备上 ARP 信息同步，包括由 ARP 触发生成的主机路由信息。VRRP 主备切换之后，不用做 ARP 学习，下行流量即可接通。

#### 前置任务

在配置 ARP 双机热备之前，需完成以下任务：

- 建立多机备份平台。
- [配置接口在备份组中的优先级](#)。

#### 数据准备

无。

## 11.3.2 配置远端备份策略支持备份 ARP 业务

使能 ARP 双机热备，需要指定备份的业务类型。

### 背景信息

在互为备份的设备上进行如下配置。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **remote-backup-profile profile-name**，进入远端备份策略视图。

**步骤 3** 执行命令 **service-type arp**，开启 arp 信息的远端备份服务。

----结束

## 11.3.3 将远端备份策略绑定到接口下

绑定到接口下的远端备份策略必须是系统视图下已经创建的，否则绑定不成功。

### 背景信息

在互为备份的设备上进行如下配置。

### 操作步骤

**步骤 1** 执行命令 **system-view**，进入系统视图。

**步骤 2** 执行命令 **interface interface-type interface-number**，进入接口视图。该接口为 VRRP 备份组用户侧的接口。

 说明

该接口与远端备份模板视图下配置的 **vrrp-id vrid interface interface-type interface-number** 命令指定的接口须为同一接口。

**步骤 3** 执行命令 **remote-backup-profile profile-name**，将 profile 绑定到此接口下。

 说明

主备路由器的 VRRP 接口下的 VLAN 需要保持一致，否则 ARP 不能备份。即：

- 如果主备路由器使用的是普通 VLAN，需要保证 VLAN ID 一致（通过命令 **vlan-type dot1q vlan-id** 设置）。
- 如果主备路由器使用的是 QinQ 终结于接口，需要保证终结范围一致（通过命令 **qinq termination pe-vid pe-vid [ to high-pe-vid ] ce-vid { low-ce-vid [ to high-ce-vid ] | any } [ vlan-group group-id ]** 设置）。

----结束

## 11.3.4 检查配置结果

配置成功后，可以查看到远端服务器连接状态和远端备份策略的配置信息。

### 背景信息

完成上述配置后，请执行下面的命令检查配置结果。



## 操作步骤

- 执行命令 **display remote-backup-profile** [ *profile-name* ]查看远端备份策略的信息。
- 执行命令 **display remote-backup-service** [ *service-name* [ **verbose** ] ]查看远端备份服务的信息。

----结束

## 任务示例

```
<HUAWEI>display remote-backup-profile profile1
```

```

Profile-Index : 0x802
Profile-Name : profile1
Service : arp
Remote-backup-service: servicel
Backup-ID : 10
track protocol : VRRP
VRRP-ID : 1
VRRP-Interface : GigabitEthernet1/0/0.2
Interface :
 : GigabitEthernet1/0/0.1
State : Master
Peer-state : Slave
Backup mode : hot
Slot-Number : 1
Card-Number : 0
Port-Number : 0
Nas logic-port : GigabitEthernet 1/0/0
Nas logic-ip : 1.2.3.4
Nas logic-sysname : huawei
Traffic interval : 10(minutes)
```

```
<HUAWEI>display remote-backup-service servicel
```

```

Service-Index : 0
Service-Name : servicel
TCP-State : Connected
Peer-ip : 88.88.88.88
Source-ip : 22.22.22.22
TCP-Port : 6000
Track-BFD : --
Track-interface0 : GigabitEthernet2/0/0
Track-interface1 : --
Last up time : 2009-11-2 16:15:8
Last down time : 2009-11-2 16:3:36
Last down reason : TCP closed for packet error.
```

## 11.4 维护

使用监控和清除统计信息命令，查看备份信息，检查配置的效果。

### 11.4.1 显示备份信息

使用相关命令查看配置是否生效。

## 背景信息

在完成上述配置后，执行下面的 **display** 命令，查看备份信息，检查配置的效果。运行信息的详细解释请参考《HUAWEI NetEngine80E/40E 路由器 命令参考》。

## 操作步骤

- 步骤 1** 执行命令 **display remote-backup-profile** *[profile-name | {slot slot-id [profile-name]} | {slave [profile-name]}]*，显示远端备份策略的信息。
- 步骤 2** 执行命令 **display remote-backup-service** *[service-name [verbose]]*，显示远端备份服务的信息。
- 结束

## 11.4.2 清除备份信息

清除备份及相关信息可能影响业务，请务必仔细确认执行。

## 背景信息



### 注意

清除备份及相关信息后，以前的信息将无法恢复，请仔细确认。

在确认需要清除的信息后，请在系统视图下执行下面的 **reset** 命令。

## 操作步骤

- 步骤 1** 执行命令 **reset remote-backup-service** *service-name* **statistic**，清除远端备份服务的各类统计信息。
- 结束

## 11.5 配置举例

介绍多机备份的各种示例。配置示例中包括组网需求、配置注意事项和配置思路等。

### 11.5.1 配置 ARP 双机热备示例

本配置举例介绍如何在 VRRP 备份组下配置 ARP 双机热备，结合配置组网图来理解配置 ARP 双机热备的场景及配置过程。配置完成后，当 VRRP 主备切换后，不用做 ARP 学习，下行流量即可接通。

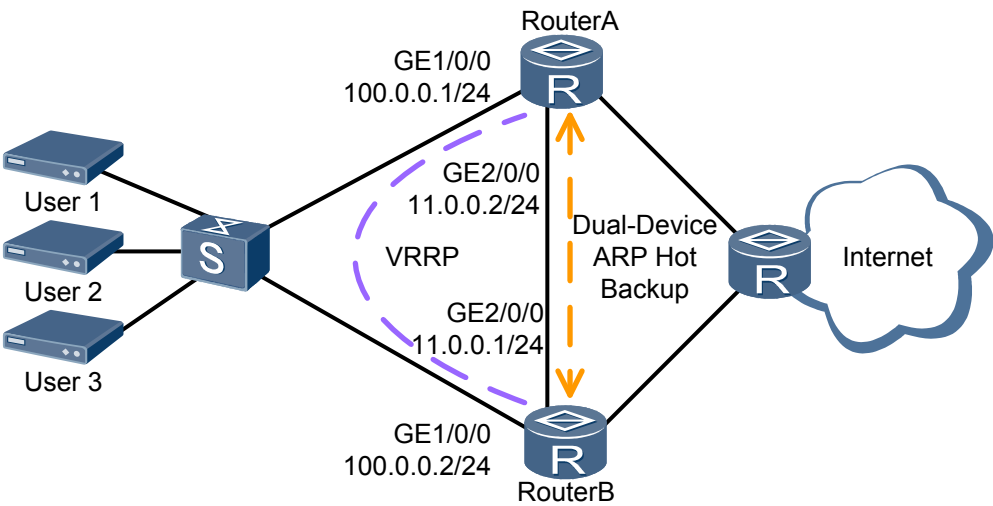
## 组网需求

如图 11-2 所示，用户通过 LSW（Lan Switch）接入 RouterA 和 RouterB。两台设备通过运行 VRRP 成为主备备份，正常情况下，主用设备上学习所有下挂用户 IP 地址的 ARP 表项并进行定期更新，用户上行流量和下行流量都经过主用设备转发。

在 RouterA 和 RouterB 上配置 ARP 双机热备。一旦主用设备故障，或者主用设备和交换机之间链路故障，备用设备升级为主用设备，用户的上行和下行流量将会走备用设备转发。配置 ARP 双机热备后，能够实时保持主用设备和备用设备上 ARP 信息同步，包括由 ARP 触发生成的主机路由信息。VRRP 主备切换之后，不用做 ARP 学习，下行流量

即可接通，避免因备用设备上没有及时学到所有下挂用户 IP 地址的 ARP 表项而造成的丢包现象。

图 11-2 ARP 双机热备配置示例图



| 设备      | 接口        | IP 地址          |
|---------|-----------|----------------|
| RouterA | GE1/0/0   | 100.0.0.1/24   |
|         | GE2/0/0   | 11.0.0.2/24    |
|         | Loopback1 | 22.22.22.22/32 |
| RouterB | GE1/0/0   | 100.0.0.2/24   |
|         | GE2/0/0   | 11.0.0.1/24    |
|         | Loopback1 | 88.88.88.88/32 |

配置思路

采用如下的思路配置 ARP 双机热备功能。

1. 配置 IP 路由保证各设备间路由连通。具体配置请参见《HUAWEI NetEngine80E/40E 路由器 配置指南 — IP 路由》
2. 建立多机备份平台。
3. 配置远端备份策略支持备份 ARP 业务。
4. VRRP 接口下使能备份模板。

数据准备

为完成此配置例，需准备如下的数据。

- VRRP ID
- 互为备份的路由器设备的各自 IP 地址
- Backup ID，可以根据用户的 Backup ID 和远端备份服务确定用户所属的远端备份策略
- 备份组的虚拟 IP 地址

- VRRP 备份组中各路由器的优先级

## 操作步骤

**步骤 1** 建立多机备份平台，以 RouterA 为例，RouterB 的配置与此类似。

 说明

本例只列出组网中用户信息备份的相关配置，其他配置请参考相应手册。

# 在接入侧配置 BFD 会话 bfd，快速感知端口或链路的异常，并触发 VRRP 主备切换。  
其中 100.0.0.2 为 RouterB 设备上接口 GE1/0/0 的 IP 地址。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd bfd bind peer-ip 100.0.0.2
[RouterA-bfd-session-bfd] discriminator local 1
[RouterA-bfd-session-bfd] discriminator remote 2
[RouterA-bfd-session-bfd] commit
[RouterA-bfd-session-bfd] quit
```

# 配置 VRRP 状态的绑定接口（此例中为接口 GE1/0/0），并配置其监视 BFD 会话状态和网络侧接口状态。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] vlan-type dot1q 200
[RouterA-GigabitEthernet1/0/0] ip address 100.0.0.1 255.255.255.0
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 100.0.0.100
[RouterA-GigabitEthernet1/0/0] admin-vrrp vrid 1
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 priority 120
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 preempt-mode timer delay 600
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 track bfd-session 1 peer
[RouterA-GigabitEthernet1/0/0] vrrp vrid 1 track interface gigabitethernet 2/0/0 reduced 50
[RouterA-GigabitEthernet1/0/0] quit
```

 说明

为了区分主备设备，需要在两台设备上配置不同的 vrrp 优先级。其中，优先级高的为主设备。

# 配置远端备份服务。

```
[RouterA] remote-backup-service service1
[RouterA-rm-backup-srv-service1] peer 88.88.88.88 source 22.22.22.22 port 2046
[RouterA-rm-backup-srv-service1] track interface gigabitethernet 2/0/0
```

 说明

本端和远端的 peer 地址能够互通。

在远端备份服务视图下，还可以通过命令 **track bfd-session** 跟踪建立在主备设备网络侧的 peer bfd 会话状态，以达到快速检测对端状态的目的，本举例中不再描述，具体使用方法请参见命令参考。

# 配置远端备份策略。

```
[RouterA] remote-backup-profile profile1
[RouterA-rm-backup-prf-profile1] peer-backup hot
[RouterA-rm-backup-prf-profile1] vrrp-id 1 interface gigabitethernet 1/0/0
[RouterA-rm-backup-prf-profile1] backup-id 10 remote-backup-service service1
[RouterA-rm-backup-prf-profile1] service-type arp
[RouterA-rm-backup-prf-profile1] quit
```

**步骤 2** 将远端备份策略绑定到接口下（此例中为接口 GE1/0/0），以 RouterA 为例，RouterB 的配置与此类似。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] remote-backup-profile profile1
[RouterA-GigabitEthernet1/0/0] quit
```

**步骤 3** 验证配置结果

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 **arp**，此备份策略 **profile1** 绑定在接口 **GigabitEthernet1/0/0** 下，并且 RouterA 状态为 **Master**。

```
<RouterA> display remote-backup-profile profile1
```

```

Profile-Index : 0x802
Profile-Name : profile1
Service : arp
Remote-backup-service: servicel
Backup-ID : 10
track protocol : VRRP
VRRP-ID : 1
VRRP-Interface : GigabitEthernet1/0/0
Interface :
 : GigabitEthernet1/0/0
State : Master
Peer-state : Slave
Backup mode : hot
Slot-Number : 1
Card-Number : 0
Port-Number : 0
Nas logic-port : Gigabitethernet 1/0/0
Nas logic-ip : 1.2.3.4
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**。

```
<RouterA> display remote-backup-service servicel
```

```

Service-Index : 0
Service-Name : servicel
TCP-State : Connected
Peer-ip : 88.88.88.88
Source-ip : 22.22.22.22
TCP-Port : 2046
Track-BFD : --
Track-interface0 : GigabitEthernet2/0/0
Track-interface1 : --
Last up time : 2009-11-2 16:15:8
Last down time : 2009-11-2 16:3:36
Last down reason : TCP closed for packet error.

```

----结束

## 配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
bfd bfd bind peer-ip 100.0.0.2
discriminator local 1
discriminator remote 2
commit
#
interface gigabitethernet 1/0/0
vlan-type dot1q 200
ip address 100.0.0.1 255.255.255.0
vrrp vrid 1 virtual-ip 100.0.0.100
admin-vrrp vrid 1
vrrp vrid 1 priority 120
vrrp vrid 1 preempt-mode timer delay 600
vrrp vrid 1 track bfd-session 1 peer
vrrp vrid 1 track interface gigabitethernet 2/0/0 reduced 50
#
remote-backup-service servicel
```

```

peer 88.88.88.88 source 22.22.22.22 port 2046
track interface gigabitethernet 2/0/0
#
remote-backup-profile profile1
service-type arp
backup-id 10 remote-backup-service service1
peer-backup hot
vrrp-id 1 interface gigabitethernet 1/0/0
#
interface gigabitethernet 1/0/0
user-vlan 50
remote-backup-profile profile1
#
interface LoopBack1
ip address 22.22.22.22 255.255.255.255
#
ospf 1
area 0.0.0.0
network 11.0.0.0 0.0.0.255
network 22.22.22.22 0.0.0.0
#
return

```

## ● RouterB 的配置文件

```

#
sysname RouterB
#
bfd bfd bind peer-ip 100.0.0.1
discriminator local 2
discriminator remote 1
commit
#
interface gigabitethernet 1/0/0
vlan-type dot1q 200
ip address 100.0.0.2 255.255.255.0
vrrp vrid 1 virtual-ip 100.0.0.100
admin-vrrp vrid 1
vrrp vrid 1 track bfd-session 2 peer
vrrp vrid 1 track interface gigabitethernet 2/0/0 reduced 50
#
remote-backup-service service1
peer 22.22.22.22 source 88.88.88.88 port 2046
track interface gigabitethernet 2/0/0
#
remote-backup-profile profile1
service-type arp
backup-id 10 remote-backup-service service1
peer-backup hot
vrrp-id 1 interface gigabitethernet 1/0/0
#
interface gigabitethernet 1/0/0
user-vlan 50
remote-backup-profile profile1
#
interface LoopBack1
ip address 88.88.88.88 255.255.255.255
#
ospf 1
area 0.0.0.0
network 11.0.0.0 0.0.0.255
network 88.88.88.88 0.0.0.0
#
return

```

# A 术语

列出了本手册中使用的术语。

| 术语                 | 含义                                                                                                                                                         |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Numerics</b>    |                                                                                                                                                            |
| 802.1ag MAC Ping   | 802.1ag MAC Ping 与 Ping 类似，通过发送测试报文和接收应答报文来检测从本设备到目的设备是否可达。802.1ag MAC Ping 由 MEP 发起，目的节点可以是同一 MA 内的或不同 MA 内的，与发起节点级别相同的 MEP 或 MIP。                        |
| 802.1 ag MAC Trace | 802.1ag MAC Trace 与 Traceroute（或 Tracert）类似，通过发送测试报文和接收应答报文来检测从本设备到目的设备的路径或定位故障点。802.1ag MAC Trace 由 MEP 发起，目的节点可以是同一 MA 内的或不同 MA 内的，与发起节点级别相同的 MEP 或 MIP。 |
| 1+1 备份             | 两个组件必须互为镜像（mirror）。当主用组件发生故障时，备用组件可以立即接管当前任务，从而保证系统业务不中断                                                                                                   |
| n+1 备份             | 系统通过 n 个相似的组件来提供某项服务，由另外一个组件作为这 n 个组件的备份。当 n 个中的某一个组件发生故障时，备份组件接管故障组件的任务，业务仍然可以继续运行                                                                        |
| <b>B</b>           |                                                                                                                                                            |
| Interface Backup   | 接口备份                                                                                                                                                       |
| 本地 MEP             | 对于运行以太网 CFM 的网络中的任意一台设备，该设备上的 MEP 称为本地 MEP                                                                                                                 |
| 被动模式               | EFM OAM 工作模式的一种，处于被动模式的接口不能发起对端发现和远端环回。                                                                                                                    |
| <b>C</b>           |                                                                                                                                                            |
| CCM 终结             | CCM 由 MEP 产生也由 MEP 终结。当 MEP 接收到大于自身级别的 CCM 时，继续转发该 CCM；当 MEP 接收到小于或等于自身级别的 CCM 时，不再转发该 CCM，以确保低级别 MD 内的 CCM 不会扩散到高级别 MD 中。                                 |

| 术语                | 含义                                                                                                                            |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>E</b>          |                                                                                                                               |
| EFM OAM 工作模式      | EFM OAM 工作模式是具备 EFM OAM 功能的接口的一个属性，共包括两种：主动模式和被动模式。                                                                           |
| <b>G</b>          |                                                                                                                               |
| GR Capable Router | 有 GR 能力的设备                                                                                                                    |
| GR Aware Router   | GR 感知设备                                                                                                                       |
| GR Unaware Router | 无 GR 感知设备                                                                                                                     |
| 骨干 VLAN           | 运营商骨干网的 VLAN ID                                                                                                               |
| 工作隧道              | 在 PBB-TE 保护组中，正常情况下，工作隧道是业务传输的承载者。另参见 PBB-TE 保护组和保护隧道。                                                                        |
| 故障管理              | 以太网 OAM 的故障管理功能包括：网络的连通性检测、故障确认与定位、与自动保护倒换协议配合可以触发保护倒换。                                                                       |
| 故障判定              | 如果某个 MEP 连续 3 个 CCM 发送周期没有接收到另一个远端 MEP 发送的 CCM，则认为和该 MEP 之间发生了连通性故障                                                           |
| 故障通告              | 故障通告是指当本端发生故障事件后，本端设备向对端设备发送 OAMPDU 以通知对端设备，同时将故障事件记入日志并上报给网管系统。                                                              |
| <b>I</b>          |                                                                                                                               |
| IP Address Owner  | IP 地址拥有者                                                                                                                      |
| <b>L</b>          |                                                                                                                               |
| LBM               | 802.1ag MAC Ping 功能的发起节点向目标节点设备发送的 Loopback 消息。LBM 消息中携带本消息的发送时间。                                                             |
| LBR               | 在 802.1ag MAC Ping 功能中，目标节点 MEP 收到 LBM 后，向发起节点 MEP 发送的应答消息，称为 Loopback Reply。该 LBR 中包含 LBM 的发送时间、LBM 的接收时间和 LBR 的发送时间。        |
| LTM               | 在 802.1ag MAC Trace 中，功能的发起节点 MEP 向目的节点 MEP 发送的消息，称为 Linktrace Message。LTM 消息中包含有 TTL (Time to Live) 和目的节点 MEP2 的 MAC 地址。     |
| LTR               | 在 802.1ag MAC Trace 功能中，目标节点 MEP 收到 LTM 后，向发起节点 MEP 发送的应答消息，称为 Linktrace Reply。LTR 中也含有 TTL 字段，该字段的值也等于 LTM 的 TTL 字段的值减 1。    |
| 链路级以太网 OAM        | 链路级以太网 OAM 技术，如遵循 IEEE 802.3ah 协议的 EFM OAM (Ethernet in the First Mile OAM)，针对两台直连设备之间的链路，提供链路连通性检测功能、链路监控功能、远端故障通知功能、远端环回功能。 |



| 术语                 | 含义                                                                                                           |
|--------------------|--------------------------------------------------------------------------------------------------------------|
| 链路监控               | 链路监控是指在设定的观察时长内，如果接口检测到的误帧数量、误码数量或误帧秒数量达到或超过设定的阈值，则该接口通过向对端设备发送 OAMPDU 来通告故障。                                |
| 连通性检测              | 以太网 CFM 通过 MEP 之间定期互发 CCM（Continuity Check Message）来检测各 MEP 之间的连通性，这种检测称为连通性检测或 CC 检测。                       |
| <b>M</b>           |                                                                                                              |
| MEP 数据库            | 每个启动了以太网 CFM 功能的设备上都有一个 MEP 数据库。MEP 数据库中记录着本设备上的 MEP（即本地 MEP）和同一 MA 内的其它设备上的 MEP（即远端 MEP）。                   |
| <b>O</b>           |                                                                                                              |
| OAMPDU             | OAM Protocol Data Unit                                                                                       |
| <b>R</b>           |                                                                                                              |
| RMEP               | 同一 MA 内其它设备上的 MEP 对本设备而言称为远端维护联盟边缘节点 RMEP（Remote Maintenance association End Point）                          |
| <b>S</b>           |                                                                                                              |
| Service VRRP       | 业务 VRRP                                                                                                      |
| <b>V</b>           |                                                                                                              |
| Virtual Router     | 虚拟路由器                                                                                                        |
| Virtual IP Address | 虚拟 IP 地址                                                                                                     |
| <b>W</b>           |                                                                                                              |
| 维护节点               | MEP 和 MIP 统称为维护节点 MP（Maintenance Point）。                                                                     |
| 维护联盟               | 维护联盟 MA（Maintenance Association）是 MD 的一部分。一个 MD 可以划分成一个或多个 MA。                                               |
| 维护联盟边缘节点           | 维护联盟边缘节点 MEP（Maintenance association End Point）是 MA 的边缘节点。                                                   |
| 维护联盟内部节点           | 维护联盟内部节点 MIP（Maintenance association Intermediate Point）是 MA 的内部节点。                                          |
| 维护域                | 维护域 MD（Maintenance Domain）是指对其实施以太网 CFM 管理的一个网络或一个网络的一部分，一个 MD 由一个统一的 ISP（Internet Service Provider）进行管理。    |
| 网络级以太网 OAM         | 网络级以太网 OAM 技术，如 IEEE 802.1ag 协议规定的以太网 CFM（Connectivity Fault Management），针对网络实现端到端的连通性故障检测、故障通知、故障确认和故障定位功能。 |

| 术语       | 含义                                                                                                                                       |
|----------|------------------------------------------------------------------------------------------------------------------------------------------|
| 误帧秒      | 误帧秒是指将设定的观察时长划分为若干个以 1 秒为单位的时间段，如果在某个时间段内检测到了至少一个误帧，则该时间段称为一个误帧秒。                                                                        |
| <b>X</b> |                                                                                                                                          |
| 性能管理     | 性能管理主要是指对网络中的丢包、时延、抖动进行衡量，也包括对网络中各类流量进行统计。性能管理通常在用户接入点实施。有了性能管理工具，运营商可通过网管监测网络运行情况、定位故障，确认网络转发能力是否符合与用户签订的 SLA（Service Level Agreement）。 |
| <b>Y</b> |                                                                                                                                          |
| 远端环回     | 远端环回是指当本端向对端发送除 EFM OAM 协议报文外的所有其它报文时，对端（远端）接收到报文后不按照报文的目的地地址进行转发，而是将报文再发回给本端。远端环回功能可用于定位链路故障和测试链路质量。                                    |
| <b>Z</b> |                                                                                                                                          |
| 主动模式     | EFM OAM 工作模式的一种，对端发现和远端环回都只能由主动模式的接口发起。                                                                                                  |

# B 缩略语

列出了本手册中使用的缩略语。

| 缩略语      | 全称                                 | 含义        |
|----------|------------------------------------|-----------|
| <b>A</b> |                                    |           |
| AMB      | Active Main Board                  | 主用主板      |
| <b>B</b> |                                    |           |
| BFD      | Bidirectional Forwarding Detection | 双向转发检测    |
| BGP      | Border Gateway Protocol            | 边界网关协议    |
| <b>D</b> |                                    |           |
| DMTI     | Desired Min TX Interval            | 期望的最小发送间隔 |
| DM       | Detect Multi                       | 检测倍数      |
| <b>E</b> |                                    |           |
| EFM OAM  | Ethernet in the First Mile OAM     |           |
| <b>F</b> |                                    |           |
| FRR      | Fast ReRoute                       | 快速重路由     |
| <b>G</b> |                                    |           |
| GR       | Graceful Restart                   | 优雅重启      |
| <b>H</b> |                                    |           |
| HA       | High Availability                  | 高可用性      |
| <b>L</b> |                                    |           |
| LSP      | Label Switched Path                | 标签交换路径    |

| 缩略语         | 全称                                                             | 含义             |
|-------------|----------------------------------------------------------------|----------------|
| LACPDU      | Link Aggregation Control Protocol Data Unit                    | LACP 数据单元      |
| <b>M</b>    |                                                                |                |
| MPLS TE FRR | MultiProtocol Label Switching Traffic Engineering Fast Reroute | MPLS 流量工程快速重路由 |
| MTBF        | Mean Time Between Failure                                      | 平均故障间隔时间       |
| MTTR        | Mean Time to Repair                                            | 平均修复时间         |
| <b>O</b>    |                                                                |                |
| OAM         | Operations Administration and Maintenance                      | 运行、管理和维护       |
| <b>R</b>    |                                                                |                |
| RMTI        | Required Min TX Interval                                       | 需要的最小发送间隔      |
| <b>S</b>    |                                                                |                |
| SMB         | Second Main Board                                              | 备用主板           |
| SP          | service provider                                               | 业务提供商          |
| <b>U</b>    |                                                                |                |
| URL         | universal resource locator                                     | 统一资源定位器        |
| UMG         | Universal Media Gateway                                        | 通用媒体网关         |
| <b>V</b>    |                                                                |                |
| VRRP        | Virtual Router Redundancy Protocol                             | 虚拟路由冗余协议       |
| VGMP        | VRRP Group Management Protocol                                 | VRRP 组管理协议     |
| mVRRP       | Management VRRP                                                | 管理 VRRP        |
| <b>W</b>    |                                                                |                |
| WTR         | Wait To Restore                                                | 等待恢复           |