



**Huawei AR1200 系列企业路由器
V200R002C01**

配置指南-MPLS

文档版本 01
发布日期 2012-04-20

版权所有 © 华为技术有限公司 2012。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，本档内容会不定期进行更新。除非另有约定，本档仅作为使用指导，本档中的所有陈述、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

读者对象

本文档介绍了 AR1200 中静态 LSP 配置、MPLS LDP 配置的基本概念、在不同应用场景中的配置过程和配置举例。

本文档提供了静态 LSP 配置、MPLS LDP 配置的配置方法。

本文档主要适用于以下工程师：

- 数据配置工程师
- 调测工程师
- 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	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	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	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	表示能帮助您解决某个问题或节省您的时间。
 说明	表示是正文的附加信息，是对正文的强调和补充。

命令行格式约定

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

接口编号约定

本手册中出现的接口编号仅作示例，并不代表设备上实际具有此编号的接口，实际使用中请以设备上存在的接口编号为准。

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 01 (2012-04-20)

第一次正式发布。

目录

前言.....	ii
1 静态 LSP 配置.....	1
1.1 静态 LSP 概述.....	2
1.2 AR1200 支持的静态 LSP 特性.....	2
1.3 配置静态 LSP.....	2
1.3.1 建立配置任务.....	2
1.3.2 配置 LSR ID.....	3
1.3.3 使能 MPLS.....	3
1.3.4 配置静态 LSP 的 Ingress.....	4
1.3.5 配置静态 LSP 的 Transit.....	4
1.3.6 配置静态 LSP 的 Egress.....	5
1.3.7 检查配置结果.....	5
1.4 配置静态 BFD 检测静态 LSP.....	6
1.4.1 建立配置任务.....	6
1.4.2 使能全局 BFD 能力.....	7
1.4.3 配置 Ingress BFD 参数.....	7
1.4.4 配置 Egress BFD 参数.....	8
1.4.5 检查配置结果.....	9
1.5 维护静态 LSP.....	10
1.5.1 检测 LSP 连通性/可达性.....	10
1.5.2 配置 LSP 的 Trap 功能.....	10
1.6 配置举例.....	11
1.6.1 配置静态 LSP 示例.....	11
1.6.2 配置静态 BFD 检测静态 LSP 示例.....	17
2 MPLS LDP 配置.....	25
2.1 MPLS LDP 概述.....	27
2.2 AR1200 支持的 MPLS LDP 特性.....	27
2.3 配置 LDP 本地会话.....	29
2.3.1 建立配置任务.....	29
2.3.2 配置全局 MPLS LDP 能力.....	30
2.3.3 （可选）配置 LDP 动态能力通告功能.....	31
2.3.4 配置 LDP 本地会话.....	31

2.3.5 (可选) 配置 LDP 传输地址.....	32
2.3.6 (可选) 配置 LDP 本地会话的定时器.....	32
2.3.7 检查配置结果.....	35
2.4 配置 LDP 远端会话.....	37
2.4.1 建立配置任务.....	37
2.4.2 配置全局 MPLS LDP 能力.....	38
2.4.3 (可选) 配置 LDP 动态能力通告功能.....	39
2.4.4 配置 LDP 远端会话.....	39
2.4.5 (可选) 配置 LDP 远端会话的定时器.....	40
2.4.6 检查配置结果.....	43
2.5 配置 LDP LSP.....	45
2.5.1 建立配置任务.....	45
2.5.2 建立 LDP LSP.....	46
2.5.3 (可选) 配置 PHP 特性.....	46
2.5.4 (可选) 配置 LDP 标签发布方式.....	47
2.5.5 (可选) 配置 LDP 自动触发 DoD 请求功能.....	47
2.5.6 (可选) 配置接口的 MPLS MTU.....	49
2.5.7 (可选) 配置 LDP MTU 信令功能.....	49
2.5.8 (可选) 配置 LDP 水平分割策略.....	50
2.5.9 (可选) 配置 LDP Inbound 策略和 Outbound 策略.....	50
2.5.10 (可选) 配置 LSP 建立的触发策略.....	52
2.5.11 (可选) 配置 Transit LSP 建立的触发策略.....	53
2.5.12 检查配置结果.....	53
2.6 配置 LDP 跨域扩展.....	54
2.6.1 建立配置任务.....	55
2.6.2 配置 LDP 跨域扩展.....	55
2.6.3 检查配置结果.....	56
2.7 配置静态 BFD 检测 LDP LSP.....	56
2.7.1 建立配置任务.....	56
2.7.2 使能全局 BFD 能力.....	57
2.7.3 配置 Ingress BFD 参数.....	57
2.7.4 配置 Egress BFD 参数.....	59
2.7.5 检查配置结果.....	60
2.8 配置动态 BFD 检测 LDP LSP.....	60
2.8.1 建立配置任务.....	61
2.8.2 使能全局 BFD 能力.....	61
2.8.3 使能 MPLS 动态创建 BFD 会话功能.....	62
2.8.4 配置动态 BFD 检测 LDP LSP 的触发策略.....	62
2.8.5 (可选) 调整 BFD 检测参数.....	63
2.8.6 检查配置结果.....	63
2.9 配置 Manual LDP FRR.....	65
2.9.1 建立配置任务.....	65

2.9.2 使能 Manual LDP FRR 功能.....	66
2.9.3 检查配置结果.....	66
2.10 配置 LDP Auto FRR.....	66
2.10.1 建立配置任务.....	67
2.10.2 使能 LDP Auto FRR 功能.....	67
2.10.3 检查配置结果.....	68
2.11 配置 LDP 和 IGP 同步.....	69
2.11.1 建立配置任务.....	69
2.11.2 使能 LDP 和 IGP 同步功能.....	69
2.11.3 （可选）设置 hold-down 定时器的值.....	70
2.11.4 （可选）设置 hold-max-cost 定时器的值.....	70
2.11.5 （可选）设置 delay 定时器的值.....	71
2.11.6 检查配置结果.....	72
2.12 配置 LDP 和静态路由同步.....	72
2.12.1 建立配置任务.....	72
2.12.2 使能 LDP 和静态路由同步功能.....	74
2.12.3 （可选）设置 hold-down 定时器的值.....	74
2.12.4 检查配置结果.....	75
2.13 配置 LDP GTSM.....	76
2.13.1 建立配置任务.....	76
2.13.2 配置 LDP GTSM.....	76
2.13.3 检查配置结果.....	77
2.14 配置 LDP 安全特性.....	77
2.14.1 建立配置任务.....	77
2.14.2 配置 LDP MD5 认证.....	78
2.14.3 配置 LDP Keychain 认证.....	79
2.14.4 配置 LDP GTSM.....	80
2.14.5 检查配置结果.....	81
2.15 配置 LDP GR.....	82
2.15.1 建立配置任务.....	82
2.15.2 使能 LDP GR 能力.....	82
2.15.3 （可选）配置 GR Helper 的定时器.....	83
2.15.4 检查配置结果.....	84
2.16 维护 MPLS LDP.....	84
2.16.1 重启 LDP.....	84
2.16.2 检测 LSP 连通性/可达性.....	85
2.16.3 配置 LSP 的 Trap 功能.....	85
2.17 配置举例.....	85
2.17.1 配置 LDP 本地会话示例.....	86
2.17.2 配置 LDP 远端会话示例.....	89
2.17.3 配置使用 LDP 建立 LSP 示例.....	93
2.17.4 配置 LDP 自动触发 DoD 请求功能示例.....	97

2.17.5 配置 LDP Inbound 策略示例.....	102
2.17.6 配置 LDP Outbound 策略示例.....	107
2.17.7 配置 Transit LSP 示例（使用前缀列表）.....	111
2.17.8 配置 LDP 跨域扩展示例.....	117
2.17.9 配置静态 BFD 检测 LDP LSP 示例.....	123
2.17.10 配置动态 BFD 检测 LDP LSP 示例.....	129
2.17.11 配置 Manual LDP FRR 示例.....	133
2.17.12 配置 LDP Auto FRR 示例.....	137
2.17.13 配置 LDP 和 IGP 同步示例.....	144
2.17.14 配置 LDP 和静态路由同步示例.....	149
2.17.15 配置 LDP GTSM 示例.....	154
3 MPLS TE 配置.....	158
3.1 MPLS TE 简介.....	160
3.1.1 MPLS TE 概述.....	160
3.1.2 AR1200 支持的 MPLS TE 特性.....	160
3.2 配置静态 CR-LSP.....	162
3.2.1 建立配置任务.....	162
3.2.2 使能 MPLS TE.....	163
3.2.3 （可选）配置链路的带宽.....	164
3.2.4 配置 MPLS TE 隧道接口.....	165
3.2.5 配置静态 CR-LSP 的入节点.....	165
3.2.6 配置静态 CR-LSP 的中间节点.....	166
3.2.7 配置静态 CR-LSP 的出节点.....	167
3.2.8 检查配置结果.....	167
3.3 配置 RSVP-TE 隧道.....	168
3.3.1 建立配置任务.....	168
3.3.2 使能 MPLS TE 和 RSVP-TE.....	169
3.3.3 （可选）配置链路的带宽.....	169
3.3.4 配置 OSPF TE.....	170
3.3.5 配置 IS-IS TE.....	170
3.3.6 （可选）配置 MPLS TE 显式路径.....	171
3.3.7 配置 MPLS TE 隧道接口.....	172
3.3.8 配置 MPLS TE 隧道的约束条件.....	173
3.3.9 （可选）配置 RSVP 资源预留风格.....	174
3.3.10 配置 CSPF.....	174
3.3.11 检查配置结果.....	175
3.4 调整 RSVP 信令参数.....	177
3.4.1 建立配置任务.....	177
3.4.2 配置 RSVP 的 Hello 扩展.....	177
3.4.3 配置 RSVP 的状态定时器.....	178
3.4.4 配置 RSVP-TE 摘要刷新.....	178
3.4.5 配置 RSVP-TE 预留确认.....	179

3.4.6 检查配置结果.....	180
3.5 配置 RSVP 认证.....	180
3.5.1 建立配置任务.....	180
3.5.2 配置 RSVP 密钥验证.....	181
3.5.3 （可选）配置 RSVP 认证生存时间.....	182
3.5.4 （可选）配置 handshake 功能.....	183
3.5.5 （可选）配置 message window 功能.....	184
3.5.6 检查配置结果.....	184
3.6 调整 CR-LSP 的路径选择.....	185
3.6.1 建立配置任务.....	185
3.6.2 配置管理组和亲和属性.....	186
3.6.3 配置 SRLG.....	187
3.6.4 配置 CR-LSP 的跳数限制值.....	188
3.6.5 配置选路使用的度量.....	188
3.6.6 配置 CSPF 的仲裁方法.....	189
3.6.7 配置失效链路定时器.....	189
3.6.8 配置环路检测.....	190
3.6.9 配置路由锁定.....	191
3.6.10 检查配置结果.....	191
3.7 调整 MPLS TE 隧道的建立.....	191
3.7.1 建立配置任务.....	191
3.7.2 配置隧道的优先级.....	192
3.7.3 配置 CR-LSP 重优化.....	193
3.7.4 配置 CR-LSP 和 Overload 联动功能.....	193
3.7.5 配置隧道重建.....	194
3.7.6 配置记录路由和标签.....	195
3.7.7 配置 RSVP 信令延迟触发功能.....	195
3.7.8 检查配置结果.....	195
3.8 调整流量的转发.....	196
3.8.1 建立配置任务.....	196
3.8.2 配置 IGP Shortcut.....	197
3.8.3 配置转发邻接.....	197
3.8.4 配置切换延迟时间和删除延迟时间.....	198
3.8.5 检查配置结果.....	199
3.9 调整带宽的泛洪阈值.....	199
3.9.1 建立配置任务.....	199
3.9.2 配置带宽的泛洪阈值.....	200
3.9.3 检查配置结果.....	201
3.10 配置 TE 隧道流量限速.....	201
3.10.1 建立配置任务.....	201
3.10.2 配置 TE 流量限速.....	202
3.10.3 检查配置结果.....	202

3.11 配置手工 TE FRR.....	203
3.11.1 建立配置任务.....	203
3.11.2 使能 TE FRR.....	204
3.11.3 配置旁路隧道.....	204
3.11.4 （可选）配置 TE FRR 扫描定时器.....	206
3.11.5 （可选）修改 PSB 和 RSB 的超时倍数.....	206
3.11.6 检查配置结果.....	207
3.12 配置 MPLS TE Auto FRR.....	208
3.12.1 建立配置任务.....	208
3.12.2 使能 TE Auto FRR.....	209
3.12.3 使能 TE FRR 并配置自动旁路隧道的属性.....	209
3.12.4 （可选）配置 TE FRR 扫描定时器.....	210
3.12.5 （可选）修改 PSB 和 RSB 的超时倍数.....	210
3.12.6 检查配置结果.....	211
3.13 配置 CR-LSP 备份.....	211
3.13.1 建立配置任务.....	211
3.13.2 配置 CR-LSP 备份.....	213
3.13.3 （可选）配置热备份 CR-LSP 动态带宽功能.....	214
3.13.4 （可选）配置逃生路径.....	214
3.13.5 检查配置结果.....	215
3.14 配置旁路保护隧道与备份 CR-LSP 同步.....	215
3.14.1 建立配置任务.....	215
3.14.2 使能旁路保护隧道与备份 CR-LSP 同步.....	216
3.14.3 检查配置结果.....	217
3.15 配置 RSVP GR.....	217
3.15.1 建立配置任务.....	217
3.15.2 使能 RSVP Hello 扩展.....	218
3.15.3 使能 RSVP Full-GR.....	218
3.15.4 （可选）使能 RSVP GR 支持能力.....	219
3.15.5 （可选）配置 RSVP GR 节点间 hello 会话.....	219
3.15.6 （可选）修改基础时间.....	220
3.15.7 检查配置结果.....	220
3.16 配置静态 BFD for CR-LSP.....	221
3.16.1 建立配置任务.....	221
3.16.2 使能全局 BFD 能力.....	222
3.16.3 配置入节点 BFD 参数.....	222
3.16.4 配置出节点 BFD 参数.....	223
3.16.5 检查配置结果.....	224
3.17 配置静态 BFD for TE.....	225
3.17.1 建立配置任务.....	225
3.17.2 使能全局 BFD 能力.....	226
3.17.3 配置入节点 BFD 参数.....	226

3.17.4 配置出节点 BFD 参数.....	227
3.17.5 检查配置结果.....	228
3.18 配置动态 BFD for CR-LSP.....	229
3.18.1 建立配置任务.....	229
3.18.2 全局使能 BFD.....	230
3.18.3 入节点上使能 TE 动态创建 BFD 会话.....	230
3.18.4 出节点使能被动创建 BFD 会话.....	231
3.18.5 (可选) 调整入节点的 BFD 检测参数.....	231
3.18.6 检查配置结果.....	232
3.19 配置动态 BFD for RSVP.....	233
3.19.1 建立配置任务.....	233
3.19.2 RSVP 两端全局使能 BFD.....	234
3.19.3 RSVP 两端使能 BFD for RSVP.....	234
3.19.4 (可选) 调整 BFD 检测参数.....	235
3.19.5 检查配置结果.....	236
3.20 维护 MPLS TE.....	237
3.20.1 检测 TE 隧道的连通性.....	237
3.20.2 查看隧道错误信息.....	237
3.20.3 清除运行信息.....	238
3.20.4 重启隧道接口.....	238
3.20.5 重启 RSVP 进程.....	239
3.20.6 删除/重建自动生成的旁路隧道.....	239
3.21 配置举例.....	239
3.21.1 配置静态 MPLS TE 隧道示例.....	239
3.21.2 配置 RSVP-TE 隧道示例.....	245
3.21.3 配置 MPLS TE FRR 示例.....	253
3.21.4 配置 MPLS TE Auto FRR 示例.....	263
3.21.5 配置 CR-LSP 热备份示例.....	271
3.21.6 配置静态 BFD for CR-LSP 示例.....	277
3.21.7 配置动态 BFD for CR-LSP 示例.....	283

1 静态 LSP 配置

关于本章

通过手工为 LSR 分配标签，可以配置静态 LSP。静态 LSP 适用于拓扑结构简单并且稳定的小型网络。

1.1 静态 LSP 概述

静态 LSP 不能使用标签发布协议动态建立，需要由管理员手工配置。适用于拓扑结构简单并且稳定的小型网络。

1.2 AR1200 支持的静态 LSP 特性

1.3 配置静态 LSP

只有通过手工为 LSR 均进行相应配置，才可以建立静态 LSP。

1.4 配置静态 BFD 检测静态 LSP

通过配置静态 BFD 检测静态 LSP，可以检测手工创建的静态 LSP 的连通性。

1.5 维护静态 LSP

维护静态 LSP，包括清除 MPLS 的统计信息、检测 LSP 连通性/可达性、配置 LDP LSP 的 Trap 功能。

1.6 配置举例

介绍静态 LSP 配置举例。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、配置思路等。

1.1 静态 LSP 概述

静态 LSP 不能使用标签发布协议动态建立，需要由管理员手工配置。适用于拓扑结构简单并且稳定的小型网络。

配置静态 LSP 时，管理员需要为各 LSR 手工分配标签，需要遵循的原则是：前一节点出标签的值等于下一个节点入标签的值。静态 LSP 上的各 LSR 之间不能相互感知整条 LSP 的情况，因此静态 LSP 是一个本地概念。

静态 LSP 不使用标签发布协议，不需要交互控制报文，因此消耗资源比较小，适用于拓扑结构简单并且稳定的小型网络。但通过静态方式分配标签建立的 LSP 不能根据网络拓扑变化动态调整，需要管理员干预。

1.2 AR1200 支持的静态 LSP 特性

静态 LSP

静态 LSP 需要由管理员手工配置。静态 LSP 上的各 LSR 之间不能相互感知整条 LSP 的情况，因此静态 LSP 是一个本地概念。当路由发生变化时，静态 LSP 不能自动调整，需要由管理员手工干预。

静态 BFD 检测静态 LSP

AR1200 支持静态 BFD 对静态 LSP 的快速检测。BFD 是一种双向检测机制，当使用静态 BFD 检测静态 LSP 这些单向链路时，反向链路可以是 IP 或者静态 LSP。

1.3 配置静态 LSP

只有通过手工为 LSR 均进行相应配置，才可以建立静态 LSP。

1.3.1 建立配置任务

在配置静态 LSP 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，可以快速、准确地完成配置任务。

应用环境

静态 LSP 需要管理员对沿途的 LSR 均进行相应配置后，才能正常工作。

静态 LSP 不使用标签发布协议，不需要交互控制报文，因此消耗资源比较小，适用于拓扑结构简单并且稳定的小型网络。但通过静态方式分配标签建立的 LSP 不能根据网络拓扑变化动态调整，需要管理员干预。

静态 LSP 可以用于 MPLS L2VPN。

关于 MPLS L2VPN 的配置请参考《Huawei AR1200 系列企业路由器 配置指南 VPN》。

前置任务

在配置静态 LSP 之前，需完成以下任务：

- 配置单播静态路由或 IGP 协议，保证各 LSR 在网络层互通

数据准备

在配置静态 LSP 之前，需准备以下数据。

序号	数据
1	静态 LSP 的名称
2	目的地址和掩码
3	各节点入标签和出标签的值
4	Ingress 的下一跳地址或出接口
5	Transit 的入接口、下一跳地址或出接口
6	Egress 的入接口

1.3.2 配置 LSR ID

配置 LSR ID 是使能 MPLS 能力的前提条件。

背景信息

配置 LSR ID 时，请注意以下事项：

- 配置 LSR ID 是配置其它 MPLS 命令的前提。
- LSR 没有缺省的 LSR ID，必须手工配置。
- 推荐使用 LSR 某个 Loopback 接口的地址作为 LSR ID。
- 如果要修改已经配置的 LSR ID，必须在系统视图下执行 **undo mpls** 命令删除所有 MPLS 配置。

请在 MPLS 域的所有节点上进行以下配置。

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 **mpls lsr-id lsr-id**，配置本节点的 LSR ID。

lsr-id:点分十进制格式，用于标识一个 LSR。

---结束

1.3.3 使能 MPLS

使能 MPLS 功能后，才可以进行 MPLS 特性的相关配置。

背景信息

请在 MPLS 域的所有节点上进行以下配置。

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 **mpls**，使能本节点的 MPLS，并进入 MPLS 视图。
 - 步骤 3** 执行命令 **quit**，退回系统视图。
 - 步骤 4** 执行命令 **interface interface-type interface-number**，配置需要转发 MPLS 报文的接口。
 - 步骤 5** 执行命令 **mpls**，使能接口的 MPLS。
- 结束

1.3.4 配置静态 LSP 的 Ingress

配置静态 LSP，需要在静态 LSP 的 Ingress 进行手工配置。

背景信息

请在 Ingress 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 **static-lsp ingress lsp-name destination ip-address { mask-length | mask } { nexthop next-hop-address | outgoing-interface interface-type interface-number } * out-label out-label**，配置本节点为指定 LSP 的 Ingress。
- 如果对参数 **destination destination-address**、**nexthop next-hop-address**、**outgoing-interface interface-type interface-number**、**out-label out-label** 进行了配置后，需要修改这些参数时，可以直接执行 **static-lsp ingress** 命令进行配置，而不需要执行 **undo static-lsp ingress** 命令取消原有配置。即以上参数支持更新。
- 结束

1.3.5 配置静态 LSP 的 Transit

配置静态 LSP，需要在静态 LSP 的 Transit 进行手工配置。

背景信息

请在 Transit 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 **static-lsp transit lsp-name incoming-interface interface-type interface-number in-label in-label { nexthop next-hop-address | outgoing-interface interface-type interface-number } * out-label out-label**，配置本节点为指定 LSP 的 Transit。
- 如果对参数 **incoming-interface interface-type interface-number**、**in-label in-label**、**nexthop next-hop-address**、**outgoing-interface interface-type interface-number**、**out-label**

out-label 进行了配置后，需要修改这些参数时，可以直接执行 **static-lsp transit** 命令进行配置，而不需要执行 **undo static-lsp transit** 命令取消原有配置。即以上参数支持更新。

---结束

1.3.6 配置静态 LSP 的 Egress

配置静态 LSP，需要在静态 LSP 的 Egress 进行手工配置。

背景信息

请在 Egress 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 **static-lsp egress lsp-name incoming-interface interface-type interface-number in-label in-label [lsr-id ingress-lsr-id]**，配置本节点为指定 LSP 的 Egress。

如果对参数 **incoming-interface interface-type interface-number**、**in-label in-label** 进行了配置后，需要修改这些参数时，可以直接执行 **static-lsp egress** 命令进行配置，而不需要执行 **undo static-lsp egress** 命令取消原有配置。即以上参数支持更新。

---结束

1.3.7 检查配置结果

静态 LSP 配置成功后，可以查看到 LSP 状态为 Up，且路由的状态为 Ready。

前提条件

已经完成静态 LSP 功能的所有配置。

操作步骤

- 使用 **display mpls static-lsp [lsp-name] [{ include | exclude } ip-address mask-length] [verbose]** 命令查看静态 LSP 的信息。
- 使用 **display mpls route-state [vpn-instance vpn-instance-name] [{ exclude | include } { idle | ready | settingup } * | destination-address mask-length] [verbose]** 命令查看 LSP 的路由相关信息。

---结束

任务示例

在配置成功时，应能得到如下的结果：

- 执行 **display mpls static-lsp** 命令查看静态 LSP 的信息，包括静态 LSP 的名字、FEC、入/出标签、入/出接口等配置信息，LSP 状态为 Up。

```
<Huawei> display mpls static-lsp
TOTAL          : 1          STATIC LSP(S)
UP              : 1          STATIC LSP(S)
DOWN           : 0          STATIC LSP(S)
Name           FEC          I/O Label  I/O If          Status
```

lsp1 3.3.3.9/32 NULL/100 -/GE1/0/0 Up

1.4 配置静态 BFD 检测静态 LSP

通过配置静态 BFD 检测静态 LSP，可以检测手工创建的静态 LSP 的连通性。

1.4.1 建立配置任务

在配置静态 BFD 检测静态 LSP 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，可以快速、准确地完成配置任务。

应用环境

对于手工创建的静态 LSP，其连通性可以通过 BFD 进行检测。

说明

静态 BFD 检测静态 LSP 时，对非主机路由也可以建立 BFD 会话。

BFD 检测 LSP 时，往返转发方式可以不一致（如报文从源端到目的端走 LSP，从目的端到源端走 IP 转发），但要求往返路径一致，如果不一致，则检测到故障时，不能确定具体是哪条路径的故障。因此部署 BFD 检测时，要确认往返路径是否一致，以便检测到的故障确实是检测路径故障。

前置任务

在配置 BFD 检测静态 LSP 之前，需完成以下任务：

- 配置静态 LSP

说明

与 TE 隧道绑定的静态 CR-LSP 只能通过 BFD 绑定 MPLS TE 的方式进行故障检测。

数据准备

在配置 BFD 检测静态 LSP 之前，需准备以下数据。

序号	数据
1	静态 LSP 的名称
2	BFD 配置名
3	反向通道的参数 <ul style="list-style-type: none">● IP 链路：Egress 的 IP 地址、出接口（可选）、源 IP 地址（可选）● 动态 LSP：Egress 的 IP 地址、LSP 下一跳地址、出接口（可选）● 静态 LSP：LSP 的名称● MPLS TE：TE 隧道编号
4	BFD 会话的本地标识符和远端标识符

1.4.2 使能全局 BFD 能力

通过在待检测链路的两端节点上进行配置，可以全局使能 BFD 能力。

背景信息

在待检测链路的两端节点上进行下列配置。

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**，对本节点使能全局 BFD 能力并进入 BFD 全局视图。

---结束

1.4.3 配置 Ingress BFD 参数

配置静态 BFD 检测静态 LSP，需要在静态 LSP 的 Ingress 上配置 BFD 的参数。

背景信息

在静态 LSP 的 Ingress 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 bind static-lsp lsp-name**，配置绑定静态 LSP 的 BFD 会话。

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。

步骤 4 (可选) 执行下列命令调整本地发送 BFD 报文的最小时间间隔、本地允许接收 BFD 报文的最小时间间隔和本地 BFD 检测倍数。

1. 执行命令 **quit**，退回系统视图。
2. 执行命令 **mpls**，使能本节点的 MPLS 能力，并进入 MPLS 视图。
3. 执行命令 **mpls bfd min-tx-interval interval**，调整本地发送 BFD 报文的最小时间间隔。

缺省值是 1000 毫秒。

当反向通道采用 IP 链路时，不能配置本地参数。

本地 BFD 报文实际发送时间间隔 = MAX { 本地配置的发送时间间隔，对端配置的接收时间间隔 }；本地实际接收时间间隔 = MAX { 对端配置的发送时间间隔，本地配置的接收时间间隔 }；本地检测时间 = 本地接收时间间隔 × 对端配置的 BFD 检测倍数。

例如：

- 本地配置的发送时间间隔为 200ms，接收时间间隔为 300ms，检测倍数为 4。

- 对端配置的发送时间间隔为 100ms，接收时间间隔为 600ms，检测倍数为 5。
则：
 - 本地实际的发送时间间隔为 $\text{MAX} \{ 200\text{ms}, 600\text{ms} \} = 600\text{ms}$ ，接收时间间隔为 $\text{MAX} \{ 100\text{ms}, 300\text{ms} \} = 300\text{ms}$ ，检测时间间隔为 $300\text{ms} \times 5 = 1500\text{ms}$ 。
 - 对端实际的发送时间间隔为 $\text{MAX} \{ 100\text{ms}, 300\text{ms} \} = 300\text{ms}$ ，接收时间间隔为 $\text{MAX} \{ 200\text{ms}, 600\text{ms} \} = 600\text{ms}$ ，检测时间间隔为 $600\text{ms} \times 4 = 2400\text{ms}$ 。
- 4. 执行命令 **mpls bfd min-rx-interval interval**，调整本地允许接收 BFD 报文的最小时间间隔。

缺省值是 1000 毫秒。

当反向通道采用 IP 链路时，不能配置本地参数。
- 5. 执行命令 **mpls bfd detect-multiplier multiplier**，调整本地 BFD 检测倍数。

缺省值是 3。
- 6. 执行命令 **quit**，退回系统视图。
- 7. 执行命令 **bfd cfg-name**，进入 BFD 会话视图。

步骤 5 执行命令 **commit**，提交配置。

配置检测静态 LSP 的 BFD 会话时需要注意：

- 当静态 LSP 的状态变为 Up 时，会重新建立 BFD 会话。
- 当静态 LSP 的状态变为 Down 时，BFD 会话的状态也变为 Down。

---结束

1.4.4 配置 Egress BFD 参数

配置静态 BFD 检测静态 LSP，需要在静态 LSP 的 Egress 上配置 BFD 的参数。

背景信息

用于向入节点通告故障的反向通道可以是 IP 链路、LSP 或者 TE 隧道，为了避免反向 LSP 故障影响 BFD 的检测，一般情况下优先选用 IP 链路。若此反向通道也需要 BFD 检测，可以再配置一对 BFD 会话进行检测。

在 LSP 的 Egress 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 配置 BFD 会话：

- IP 链路：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]**。
- 动态 LSP：执行命令 **bfd cfg-name bind ldp-lsp peer-ip ip-address nexthop ip-address [interface interface-type interface-number]**。
- 静态 LSP：执行命令 **bfd cfg-name bind static-lsp lsp-name**
- MPLS TE：执行命令 **bfd cfg-name bind mpls-te interface tunnel interface-number [te-lsp [backup]]**

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。

步骤 4 (可选) 执行下列命令调整本地发送 BFD 报文的最小时间间隔、本地允许接收 BFD 报文的最小时间间隔和本地 BFD 检测倍数。

1. 执行命令 **quit**, 退回系统视图。
2. 执行命令 **mpls**, 使能本节点的 MPLS 能力, 并进入 MPLS 视图。
3. 执行命令 **mpls bfd min-tx-interval *interval***, 调整本地发送 BFD 报文的最小时间间隔。

缺省值是 1000 毫秒。

当反向通道采用 IP 链路时, 不能配置本地参数。

本地 BFD 报文实际发送时间间隔 = MAX { 本地配置的发送时间间隔, 对端配置的接收时间间隔 }; 本地实际接收时间间隔 = MAX { 对端配置的发送时间间隔, 本地配置的接收时间间隔 }; 本地检测时间 = 本地接收时间间隔 × 对端配置的 BFD 检测倍数。

例如:

- 本地配置的发送时间间隔为 200ms, 接收时间间隔为 300ms, 检测倍数为 4。
- 对端配置的发送时间间隔为 100ms, 接收时间间隔为 600ms, 检测倍数为 5。

则:

- 本地实际的发送时间间隔为 MAX { 200ms, 600ms } = 600ms, 接收时间间隔为 MAX { 100ms, 300ms } = 300ms, 检测时间间隔为 300ms × 5 = 1500ms。
- 对端实际的发送时间间隔为 MAX { 100ms, 300ms } = 300ms, 接收时间间隔为 MAX { 200ms, 600ms } = 600ms, 检测时间间隔为 600ms × 4 = 2400ms。

4. 执行命令 **mpls bfd min-rx-interval *interval***, 调整本地允许接收 BFD 报文的最小时间间隔。

缺省值是 1000 毫秒。

当反向通道采用 IP 链路时, 不能配置本地参数。

5. 执行命令 **mpls bfd detect-multiplier *multiplier***, 调整本地 BFD 检测倍数。

缺省值是 3。

6. 执行命令 **quit**, 退回系统视图。
7. 执行命令 **bfd *cfg-name***, 进入 BFD 会话视图。

步骤 5 执行命令 **commit**, 提交配置。

---结束

1.4.5 检查配置结果

静态 BFD 检测静态 LSP 配置成功后, 可以查看 BFD 配置信息、BFD 会话信息、BFD 统计信息以及静态 LSP 的状态。

前提条件

已经完成静态 BFD 检测静态 LSP 功能的所有配置。

操作步骤

- 使用 **display bfd configuration { all | static } [for-lsp]**命令查看 BFD 配置信息。
- 使用 **display bfd session { all | static } [for-lsp]**命令查看 BFD 会话信息。
- 使用 **display bfd statistics session { all | static } [for-ip | for-lsp]**命令查看 BFD 统计信息。
- 使用 **display mpls static-lsp [lsp-name] [{ include | exclude } ip-address mask-length] [verbose]**命令查看静态 LSP 的状态。

----结束

1.5 维护静态 LSP

维护静态 LSP，包括清除 MPLS 的统计信息、检测 LSP 连通性/可达性、配置 LDP LSP 的 Trap 功能。

1.5.1 检测 LSP 连通性/可达性

通过执行 **ping/tracert** 命令，检测 LSP 连通性/可达性。

背景信息

可以在任意视图下选择执行以下命令，进行 MPLS Ping/Traceroute 测试。

操作步骤

- 执行 **ping lsp [-a source-ip | -c count | -exp exp-value | -h ttl-value | -m interval | -r reply-mode | -s packet-size | -t time-out | -v] * ip destination-address mask-length [ip-address] [nexthop nexthop-address | draft6]**命令，进行 MPLS Ping 测试。

如果指定 **draft6** 参数，**ping lsp** 命令按 draft-ietf-mpls-lsp-ping-06 实现。默认情况下按 RFC4379 实现。

- 执行 **tracert lsp [-a source-ip | -exp exp-value | -h ttl-value | -r reply-mode | -t time-out] * ip destination-address mask-length [ip-address] [nexthop nexthop-address | draft6]**命令，进行 MPLS Traceroute 测试。

如果指定 **draft6** 参数，**tracert** 命令按 draft-ietf-mpls-lsp-ping-06 实现。默认情况下按 RFC4379 实现。

----结束

1.5.2 配置 LSP 的 Trap 功能

通过配置 LSP 的 Trap 功能，可以将 LSP 的状态变化通知给网管系统。

背景信息

如果需要将 LSP 的状态变化通知给网管系统，请在系统视图下进行下列配置。

缺省情况下，LDP LSP 创建过程中不使能 Trap 功能。

操作步骤

步骤 1 在系统视图下，使用 `snmp-agent trap suppress feature-name lsp trap-name { mplsxcup | mplsxcdown } trap-interval trap-interval [max-trap-number max-trap-number]` 命令，使能 LDP LSP 的 Trap 功能，并打开 mplsxcup 或 mplsxcdown 海量告警开关。

----结束

1.6 配置举例

介绍静态 LSP 配置举例。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、配置思路等。

1.6.1 配置静态 LSP 示例

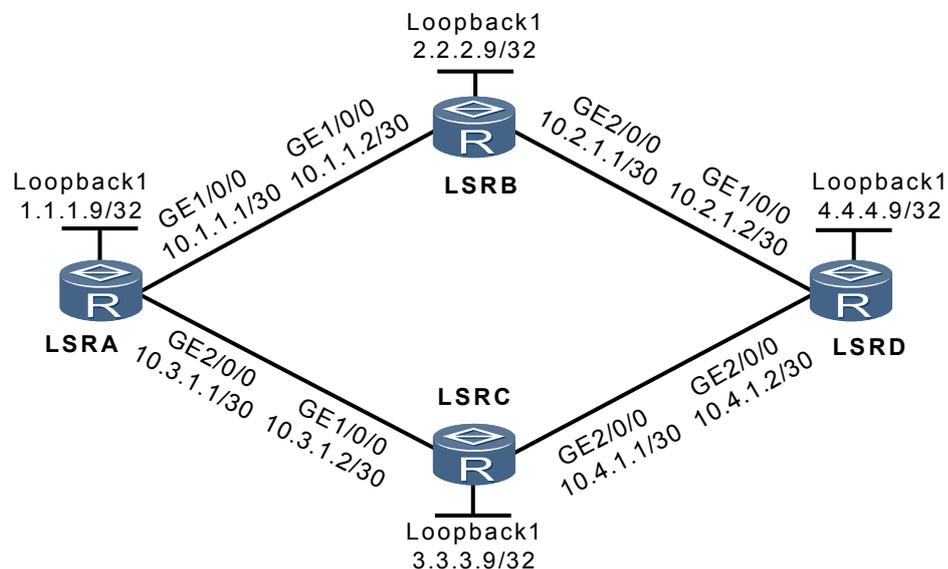
介绍静态 LSP 的配置过程，包括在各设备以及各接口使能 MPLS。

组网需求

如图 1-1 所示，各节点均支持 MPLS，运行 OSPF 作为 MPLS 骨干网上的 IGP。

在 LSRA 和 LSRD 之间建立双向静态 LSP。其中从 LSRA 到 LSRD 的 LSP 路径为 LSRA →LSRB→LSRD；从 LSRD 到 LSRA 的 LSP 路径为 LSRD→LSRC→LSRA。

图 1-1 配置静态 LSP 组网图



配置思路

采用如下的思路配置静态 LSP：

1. 配置各节点接口的 IP 地址及作为 LSR ID 的 Loopback 地址，并用 OSPF 协议通告各接口所连网段和 LSR ID 主机路由。

2. 全局使能各节点的 MPLS。
3. 使能各接口的 MPLS。
4. 在 Ingress 配置此 LSP 的目的地址、下一跳和出标签的值。
5. 在 Transit 配置此 LSP 的入接口、与上一节点出标签相等的入标签的值、对应的下一跳和出标签的值。
6. 在 Egress 配置此 LSP 的入接口及与上一节点出标签相等的入标签的值。

数据准备

为完成此配置例，需准备如下的数据：

- 各节点接口的 IP 地址如 [图 1-1](#)，OSPF 进程号，所在的区域
- 静态 LSP 的名称
- 各接口上出标签的值

操作步骤

步骤 1 配置各接口的 IP 地址

按照 [图 1-1](#) 配置各接口 IP 地址和掩码，包括 Loopback 接口，具体配置过程略。

步骤 2 配置 OSPF 协议发布各节点接口所连网段和 LSR ID 的主机路由

配置 LSRA。

```
[LSRA] ospf 1
[LSRA-ospf-1] area 0
[LSRA-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[LSRA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.3
[LSRA-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.3
[LSRA-ospf-1-area-0.0.0.0] quit
[LSRA-ospf-1] quit
```

配置 LSRB。

```
[LSRB] ospf 1
[LSRB-ospf-1] area 0
[LSRB-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[LSRB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.3
[LSRB-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.3
[LSRB-ospf-1-area-0.0.0.0] quit
[LSRB-ospf-1] quit
```

配置 LSRC。

```
[LSRC] ospf 1
[LSRC-ospf-1] area 0
[LSRC-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[LSRC-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.3
[LSRC-ospf-1-area-0.0.0.0] network 10.4.1.0 0.0.0.3
[LSRC-ospf-1-area-0.0.0.0] quit
[LSRC-ospf-1] quit
```

配置 LSRD。

```
[LSRD] ospf 1
[LSRD-ospf-1] area 0
[LSRD-ospf-1-area-0.0.0.0] network 4.4.4.9 0.0.0.0
[LSRD-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.3
[LSRD-ospf-1-area-0.0.0.0] network 10.4.1.0 0.0.0.3
[LSRD-ospf-1-area-0.0.0.0] quit
[LSRD-ospf-1] quit
```

配置完成后，在各节点上执行 **display ip routing-table** 命令，可以看到相互之间都学到了彼此的路由。

LSRA 上的显示为：

```
[LSRA] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
  Destinations : 14      Routes : 15
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 10.1.1.2          GigabitEthernet1/0/0
3.3.3.9/32         OSPF   10    2           D 10.3.1.2          GigabitEthernet2/0/0
4.4.4.9/32        OSPF  10    3           D 10.1.1.2          GigabitEthernet1/0/0
                   OSPF  10    3           D 10.3.1.2          GigabitEthernet2/0/0
10.1.1.0/30        Direct 0    0           D 10.1.1.1          GigabitEthernet1/0/0
10.1.1.1/32        Direct 0    0           D 127.0.0.1         InLoopBack0
10.1.1.2/32        Direct 0    0           D 10.1.1.2          GigabitEthernet1/0/0
10.2.1.0/30        OSPF   10    2           D 10.1.1.2          GigabitEthernet1/0/0
10.3.1.0/30        Direct 0    0           D 10.3.1.1          GigabitEthernet2/0/0
10.3.1.1/32        Direct 0    0           D 127.0.0.1         InLoopBack0
10.3.1.2/32        Direct 0    0           D 10.3.1.2          GigabitEthernet2/0/0
10.4.1.0/30        OSPF   10    2           D 10.3.1.2          GigabitEthernet2/0/0
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
```

由 LSRA 到 LSRD 上 4.4.4.9/32 的静态 LSP 的下一跳/出接口由路由表决定，已用粗体表示。本例中选用下一跳 IP 地址为 10.1.1.2/30。

LSRD 上的显示为：

```
[LSRD] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
  Destinations : 14      Routes : 15
Destination/Mask    Proto Pre  Cost   Flags NextHop         Interface
1.1.1.9/32        OSPF  10    3           D 10.2.1.1          GigabitEthernet1/0/0
                   OSPF  10    3           D 10.4.1.1          GigabitEthernet2/0/0
2.2.2.9/32         OSPF   10    2           D 10.2.1.1          GigabitEthernet1/0/0
3.3.3.9/32         OSPF   10    2           D 10.4.1.1          GigabitEthernet2/0/0
4.4.4.9/32         Direct 0    0           D 127.0.0.1         InLoopBack0
10.1.1.0/30        OSPF   10    2           D 10.2.1.1          GigabitEthernet1/0/0
10.2.1.0/30        Direct 0    0           D 10.2.1.2          GigabitEthernet1/0/0
10.2.1.1/32        Direct 0    0           D 10.2.1.1          GigabitEthernet1/0/0
10.2.1.2/32        Direct 0    0           D 127.0.0.1         InLoopBack0
10.3.1.0/30        OSPF   10    2           D 10.4.1.1          GigabitEthernet2/0/0
10.4.1.0/30        Direct 0    0           D 10.4.1.2          GigabitEthernet2/0/0
10.4.1.1/32        Direct 0    0           D 10.4.1.1          GigabitEthernet2/0/0
10.4.1.2/32        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
```

由 LSRD 到 LSRA 上 1.1.1.9/32 的静态 LSP 的下一跳/出接口由路由表决定，已用粗体表示。本例中选用下一跳 IP 地址为 10.4.1.1/30。

步骤 3 配置各节点全局的 MPLS 能力

配置 LSRA。

```
[LSRA] mpls lsr-id 1.1.1.9
[LSRA] mpls
[LSRA-mpls] quit
```

配置 LSRB。

```
[LSRB] mpls lsr-id 2.2.2.9
```

```
[LSRB] mpls
[LSRB-mpls] quit

# 配置 LSRC。

[LSRC] mpls lsr-id 3.3.3.9
[LSRC] mpls
[LSRC-mpls] quit

# 配置 LSRD。

[LSRD] mpls lsr-id 4.4.4.9
[LSRD] mpls
[LSRD-mpls] quit
```

步骤 4 配置各接口的 MPLS 能力

```
# 配置 LSRA。

[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] mpls
[LSRA-GigabitEthernet1/0/0] quit
[LSRA] interface gigabitethernet 2/0/0
[LSRA-GigabitEthernet2/0/0] mpls
[LSRA-GigabitEthernet2/0/0] quit

# 配置 LSRB。

[LSRB] interface gigabitethernet 1/0/0
[LSRB-GigabitEthernet1/0/0] mpls
[LSRB-GigabitEthernet1/0/0] quit
[LSRB] interface gigabitethernet 2/0/0
[LSRB-GigabitEthernet2/0/0] mpls
[LSRB-GigabitEthernet2/0/0] quit

# 配置 LSRC。

[LSRC] interface gigabitethernet 1/0/0
[LSRC-GigabitEthernet1/0/0] mpls
[LSRC-GigabitEthernet1/0/0] quit
[LSRC] interface gigabitethernet 2/0/0
[LSRC-GigabitEthernet2/0/0] mpls
[LSRC-GigabitEthernet2/0/0] quit

# 配置 LSRD。

[LSRD] interface gigabitethernet 1/0/0
[LSRD-GigabitEthernet1/0/0] mpls
[LSRD-GigabitEthernet1/0/0] quit
[LSRD] interface gigabitethernet 2/0/0
[LSRD-GigabitEthernet2/0/0] mpls
[LSRD-GigabitEthernet2/0/0] quit
```

步骤 5 创建从 LSRA 到 LSRD 的静态 LSP

```
# 配置 Ingress LSRA。

[LSRA] static-lsp ingress RtoRD destination 4.4.4.9 32 nexthop 10.1.1.2 out-label 20

# 配置 Transit LSRB。

[LSRB] static-lsp transit RtoRD incoming-interface gigabitethernet 1/0/0 in-label 20 nexthop
10.2.1.2 out-label 40

# 配置 Egress LSRD。

[LSRD] static-lsp egress RtoRD incoming-interface gigabitethernet 1/0/0 in-label 40
```

配置完成后,可在各节点上用 **display mpls static-lsp** 命令查看静态 LSP 的状态。以 LSRA 的显示为例:

```
[LSRA] display mpls static-lsp
TOTAL          : 1          STATIC LSP(S)
UP             : 1          STATIC LSP(S)
DOWN          : 0          STATIC LSP(S)
Name          FEC          I/O Label  I/O If          Status
RAtoRD       4.4.4.9/32    NULL/20   -/GE1/0/0      Up
```

LSP 是单向的，需要再配置 LSRD 到 LSRA 的静态 LSP。

步骤 6 创建从 LSRD 到 LSRA 的静态 LSP

用同样的方法可配置 LSRD 到 LSRA 的静态 LSP。

配置 Ingress LSRD。

```
[LSRD] static-lsp ingress RDtoRA destination 1.1.1.9 32 nexthop 10.4.1.1 out-label 30
```

配置 Transit LSRC。

```
[LSRC] static-lsp transit RDtoRA incoming-interface gigabitethernet 2/0/0 in-label 30 nexthop
10.3.1.1 out-label 60
```

配置 Egress LSRA。

```
[LSRA] static-lsp egress RDtoRA incoming-interface gigabitethernet 2/0/0 in-label 60
```

步骤 7 检查配置结果

配置完成后，在 LSRD 上执行命令 **ping lsp ip 1.1.1.9 32**，发现 **ping lsp** 是通的。

然后在各节点上用 **display mpls static-lsp** 或 **display mpls static-lsp verbose** 命令查看静态 LSP 的状态及其详细信息。以 LSRD 的显示为例：

```
[LSRD] display mpls static-lsp
TOTAL          : 2          STATIC LSP(S)
UP             : 2          STATIC LSP(S)
DOWN          : 0          STATIC LSP(S)
Name          FEC          I/O Label  I/O If          Status
RAtoRD       -/-          40/NULL   GE1/0/0/-      Up
RDtoRA       1.1.1.9/32    NULL/30   -/GE2/0/0      Up
[LSRD] display mpls static-lsp verbose
No           : 1
LSP-Name    : RAtoRD
LSR-Type    : Egress
FEC         : -/-
In-Label    : 40
Out-Label   : NULL
In-Interface : GigabitEthernet1/0/0
Out-Interface : -
NextHop     : -
Static-Lsp Type: Normal
Lsp Status  : Up
No           : 2
LSP-Name    : RDtoRA
LSR-Type    : Ingress
FEC         : 1.1.1.9/32
In-Label    : NULL
Out-Label   : 30
In-Interface : -
Out-Interface : GigabitEthernet2/0/0
NextHop     : 10.4.1.1
Static-Lsp Type: Normal
Lsp Status  : Up
```

----结束

配置文件

- #
sysname LSRA

mpls lsr-id 1.1.1.9
mpls

interface GigabitEthernet1/0/0
ip address 10.1.1.1 255.255.255.252
mpls

interface GigabitEthernet2/0/0
ip address 10.3.1.1 255.255.255.252
mpls

interface LoopBack1
ip address 1.1.1.9 255.255.255.255

ospf 1
area 0.0.0.0
network 1.1.1.9 0.0.0.0
network 10.1.1.0 0.0.0.3
network 10.3.1.0 0.0.0.3

static-lsp ingress RAtoRD destination 4.4.4.9 32 nexthop 10.1.1.2 out-label 20
static-lsp egress RDtoRA incoming-interface GigabitEthernet2/0/0 in-label 60

return
- LSRB 的配置文件

sysname LSRB

mpls lsr-id 2.2.2.9
mpls

interface GigabitEthernet1/0/0
ip address 10.1.1.2 255.255.255.252
mpls

interface GigabitEthernet2/0/0
ip address 10.2.1.1 255.255.255.252
mpls

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 10.1.1.0 0.0.0.3
network 10.2.1.0 0.0.0.3

static-lsp transit RAtoRD incoming-interface GigabitEthernet1/0/0 in-label 20 nexthop 10.2.1.2
out-label 40

return
- LSRC 的配置文件

sysname LSRC

mpls lsr-id 3.3.3.9
mpls

interface GigabitEthernet1/0/0
ip address 10.3.1.2 255.255.255.252
mpls

```
#
interface GigabitEthernet2/0/0
 ip address 10.4.1.1 255.255.255.252
 mpls
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 3.3.3.9 0.0.0.0
  network 10.3.1.0 0.0.0.3
  network 10.4.1.0 0.0.0.3
#
static-lsp transit RDtoRA incoming-interface GigabitEthernet2/0/0 in-label 30 nexthop 10.3.1.1
 out-label 60
#
return
```

● LSRD 的配置文件

```
#
 sysname LSRD
#
 mpls lsr-id 4.4.4.9
 mpls
#
interface GigabitEthernet1/0/0
 ip address 10.2.1.2 255.255.255.252
 mpls
#
interface GigabitEthernet2/0/0
 ip address 10.4.1.2 255.255.255.252
 mpls
#
interface LoopBack1
 ip address 4.4.4.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 4.4.4.9 0.0.0.0
  network 10.2.1.0 0.0.0.3
  network 10.4.1.0 0.0.0.3
#
static-lsp egress RtoRD incoming-interface GigabitEthernet1/0/0 in-label 40
static-lsp ingress RDtoRA destination 1.1.1.9 32 nexthop 10.4.1.1 out-label 30
#
return
```

1.6.2 配置静态 BFD 检测静态 LSP 示例

介绍静态 BFD 检测静态 LSP 的配置过程，包括配置静态 LSP 和配置 BFD。

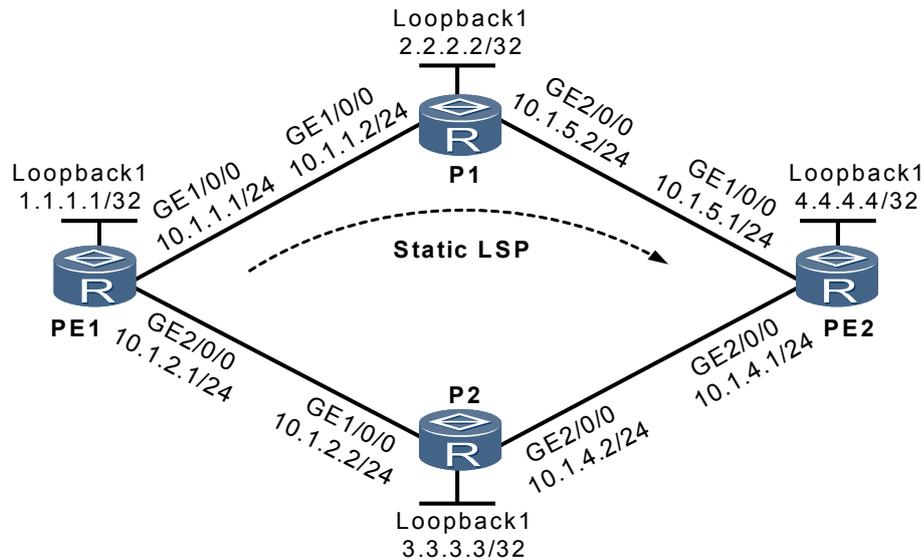
组网需求

如图 1-2 所示：

- PE1、PE2、P1 和 P2 同在一个 MPLS 域内
- PE1-P1-PE2 之间有一条静态 LSP

要求当静态 LSP 出现故障时，PE1 能够在 50ms 之内收到故障通告。

图 1-2 配置静态 BFD 检测静态 LSP 组网图



配置思路

采用如下思路配置：

- 整个 MPLS 域采用 OSPF 协议，各节点之间 IP 可达。
- 在 PE1 上配置 BFD 会话检测静态 LSP。
- 在 PE2 上配置 BFD 会话，将检测到的静态 LSP 的故障通告给 PE1（该方向仅 IP 可达即可）。

数据准备

为完成此配置示例，需要准备如下的数据：

1. 各节点的接口 IP 地址
2. OSPF 进程号
3. BFD 会话参数（配置名、最小发送和接收检测时间间隔）

操作步骤

步骤 1 配置各接口的 IP 地址和 OSPF 协议

按照图 1-2 配置各接口的 IP 地址和掩码，包括各 Loopback 接口。

在所有节点上配置 OSPF 协议，发布各自 Loopback 接口的主机路由，具体配置过程略。

配置完成后，各 LSR 可以互相 Ping 通对方的 LSR-ID，在各 LSR 上执行 **display ip routing-table** 命令可以看到到达各 LSR 的路由表项。

```
<PE1> display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 14          Routes : 15
```

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
1.1.1.1/32	Direct	0	0	D	127.0.0.1	LoopBack1
2.2.2.2/32	OSPF	10	2	D	10.1.1.2	GigabitEthernet1/0/0
3.3.3.3/32	OSPF	10	2	D	10.1.2.2	GigabitEthernet2/0/0
4.4.4.4/32	OSPF	10	3	D	10.1.1.2	GigabitEthernet1/0/0
	OSPF	10	3	D	10.1.2.2	GigabitEthernet2/0/0
10.1.1.0/24	Direct	0	0	D	10.1.1.1	GigabitEthernet1/0/0
10.1.1.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet1/0/0
10.1.1.2/32	Direct	0	0	D	10.1.1.2	GigabitEthernet1/0/0
10.1.2.0/24	Direct	0	0	D	10.1.2.1	GigabitEthernet2/0/0
10.1.2.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet2/0/0
10.1.2.2/32	Direct	0	0	D	10.1.2.2	GigabitEthernet2/0/0
10.1.4.0/24	OSPF	10	2	D	10.1.2.2	GigabitEthernet2/0/0
10.1.5.0/24	OSPF	10	2	D	10.1.1.2	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 2 使能节点的 MPLS 和 BFD 能力

在节点 PE1 上全局使能 MPLS，在各接口使能 MPLS。

```
<PE1> system-view
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls
[PE1-mpls] quit
[PE1] interface gigabitethernet 1/0/0
[PE1-GigabitEthernet1/0/0] mpls
[PE1-GigabitEthernet1/0/0] quit
[PE1] interface gigabitethernet 2/0/0
[PE1-GigabitEthernet2/0/0] mpls
[PE1-GigabitEthernet2/0/0] quit
```

在节点 PE1 上全局使能 BFD。

```
[PE1] bfd
[PE1-bfd] quit
```

PE2、P1、P2 上的操作同 PE1（略）。

步骤 3 建立静态 LSP，Ingress 是 PE1，Egress 是 PE2

在 Ingress PE1 上配置静态 LSP，名称是 lto4。

```
[PE1] static-lsp ingress lto4 destination 4.4.4.4 32 nexthop 10.1.1.2 out-label 20
```

在 Transit P1 上配置静态 LSP

```
[P1] static-lsp transit lto4 incoming-interface gigabitethernet 1/0/0 in-label 20 nexthop 10.1.5.1 out-label 30
```

在 Egress PE2 上配置静态 LSP

```
[PE2] static-lsp egress lto4 incoming-interface gigabitethernet 1/0/0 in-label 30
```

配置完成后，在 PE1 上执行命令 **ping lsp ip 4.4.4.4 32**，发现 **ping lsp** 是通的。

步骤 4 配置 BFD 会话检测静态 LSP

在 Ingress PE1 上配置 BFD 会话，其中本地标识符是 1，远端标识符是 2，发送报文的最小时间间隔是 10 秒，接收报文的最小时间间隔是 10 秒；并且能够修改端口状态表。

```
[PE1] bfd lto4 bind static-lsp lto4
[PE1-bfd-lsp-session-lto4] discriminator local 1
[PE1-bfd-lsp-session-lto4] discriminator remote 2
[PE1-bfd-lsp-session-lto4] min-tx-interval 10
[PE1-bfd-lsp-session-lto4] min-rx-interval 10
[PE1-bfd-lsp-session-lto4] process-pst
[PE1-bfd-lsp-session-lto4] commit
[PE1-bfd-lsp-session-lto4] quit
```

在 Egress PE2 上配置 BFD 会话，通过 IP 链路通告静态 LSP 故障。

```
[PE2] bfd 4to1 bind peer-ip 1.1.1.1
[PE2-bfd-session-4to1] discriminator local 2
[PE2-bfd-session-4to1] discriminator remote 1
[PE2-bfd-session-4to1] min-tx-interval 10
[PE2-bfd-session-4to1] min-rx-interval 10
[PE2-bfd-session-4to1] commit
[PE2-bfd-session-4to1] quit
```

在 PE1 上执行 **display bfd session all verbose** 查看配置结果，可以看到在 PE1 上 BFD 会话已经 Up。

```
[PE1] display bfd session all verbose
```

```
-----
Session MIndex : 256          State : Up          Name : lto4
-----
Local Discriminator      : 1          Remote Discriminator   : 2
Session Detect Mode     : Asynchronous Mode Without Echo Function
BFD Bind Type           : STATIC_LSP
Bind Session Type       : Static
Bind Peer Ip Address    : 4.4.4.4
NextHop Ip Address     : 10.1.1.2
Bind Interface           : -
Static LSP name         : lto4          LSP Token               : 0x2
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                     : 1
Proc Interface Status   : Disable    Process PST              : Enable
WTR Interval (ms)      : -
Active Multi            : 3
Last Local Diagnostic   : Neighbor Signaled Session Down(Receive AdminDown)
Bind Application        : LSPM | L2VPN | OAM_MANAGER
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-2
Session Description     : -
-----
```

Total UP/DOWN Session Number : 1/0

在 PE2 上执行 **display bfd session all verbose** 查看配置结果。

```
[PE2] display bfd session all verbose
```

```
-----
Session MIndex : 256          (Multi Hop) State : Up          Name : 4to1
-----
Local Discriminator      : 2          Remote Discriminator   : 1
Session Detect Mode     : Asynchronous Mode Without Echo Function
BFD Bind Type           : Peer Ip Address
Bind Session Type       : Static
Bind Peer Ip Address    : 1.1.1.1
Bind Interface           : -
Track Interface         : -
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                     : 254
Proc Interface Status   : Disable    Process PST              : Disable
WTR Interval (ms)      : -
Active Multi            : 3
Last Local Diagnostic   : Neighbor Signaled Session Down
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

步骤 5 检测配置结果

对 P1 的 GigabitEthernet2/0/0 接口进行 shutdown 操作，模拟静态 LSP 故障。

```

[P1] interface gigabitethernet 2/0/0
[P1-GigabitEthernet2/0/0] shutdown

```

在 PE2 上执行 **display bfd session all verbose**，查看 BFD 的状态。

```

[PE2] display bfd session all verbose

```

```

Session MIndex : 256      (Multi Hop) State : Down      Name : 4to1
-----
Local Discriminator      : 2           Remote Discriminator   : 1
Session Detect Mode     : Asynchronous Mode Without Echo Function
BFD Bind Type           : Peer Ip Address
Bind Session Type       : Static
Bind Peer Ip Address    : 1.1.1.1
Bind Interface          : -
Track Interface         : -
FSM Board Id           : 0           TOS-EXP                : 7
Min Tx Interval (ms)   : 10          Min Rx Interval (ms)  : 10
Actual Tx Interval (ms): 11500       Actual Rx Interval (ms): 11500
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
Local Demand Mode      : Disable
Last Local Diagnostic  : Control Detection Time Expired
Bind Application       : No Application Bind
Session TX TmrID      : 295          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 : 0/1

在 PE1 上执行 **display bfd session all verbose**，查看 BFD 的状态。

```

[PE1] display bfd session all verbose

```

```

Session MIndex : 256      State : Down      Name : 1to4
-----
Local Discriminator      : 1           Remote Discriminator   : 2
Session Detect Mode     : Asynchronous Mode Without Echo Function
BFD Bind Type           : STATIC_LSP
Bind Session Type       : Static
Bind Peer Ip Address    : 4.4.4.4
NextHop Ip Address     : 10.1.1.2
Bind Interface          : -
Static LSP name         : 1to4        LSP Token              : 0x0
FSM Board Id           : 1           TOS-EXP                : 7
Min Tx Interval (ms)   : 10          Min Rx Interval (ms)  : 10
Actual Tx Interval (ms): 13500       Actual Rx Interval (ms): 13500
Local Detect Multi      : 3           Detect Interval (ms)  : -
Echo Passive           : Disable      Acl Number             : -
Destination Port       : 3784        TTL                    : 1
Proc Interface Status  : Disable      Process PST            : Enable
WTR Interval (ms)     : -
Proc interface status  : Disable

```

```
Active Multi          : 3
Last Local Diagnostic : Control Detection Time Expired
Bind Application      : LSPM | L2VPN | OAM_MANAGER
Session TX TmrID     : 305          Session Detect TmrID   : -
Session Init TmrID   : -           Session WTR TmrID     : -
Session Echo Tx TmrID : -
PDT Index            : FSM-0 | RCV-0 | IF-0 | TOKEN-2
Session Description  : -
```

Total UP/DOWN Session Number : 0/1

---结束

配置文件

- PE1 的配置文件

```
#
sysname PE1
#
mpls lsr-id 1.1.1.1
mpls
#
bfd
#
interface GigabitEthernet1/0/0
ip address 10.1.1.1 255.255.255.0
mpls
#
interface GigabitEthernet2/0/0
ip address 10.1.2.1 255.255.255.0
mpls
#
interface LoopBack1
ip address 1.1.1.1 255.255.255.255
#
ospf 100
area 0.0.0.0
network 1.1.1.1 0.0.0.0
network 10.1.1.0 0.0.0.255
network 10.1.2.0 0.0.0.255
#
static-lsp ingress lto4 destination 4.4.4.4 32 nexthop 10.1.1.2 out-label 20
#
bfd lto4 bind static-lsp lto4
discriminator local 1
discriminator remote 2
min-tx-interval 10
min-rx-interval 10
process-pst
commit
#
Return
```

- PE2 的配置文件

```
#
sysname PE2
#
mpls lsr-id 4.4.4.4
mpls
#
bfd
#
interface GigabitEthernet1/0/0
ip address 10.1.5.1 255.255.255.0
mpls
#
interface GigabitEthernet2/0/0
ip address 10.1.4.1 255.255.255.0
```

```
mpls
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
#
bfd 4to1 bind peer-ip 1.1.1.1
 discriminator local 2
 discriminator remote 1
 min-tx-interval 10
 min-rx-interval 10
 commit
#
ospf 100
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 10.1.4.0 0.0.0.255
  network 10.1.5.0 0.0.0.255
#
static-lsp egress lto4 incoming-interface GigabitEthernet1/0/0 in-label 30
#
Return
```

● P1 的配置文件

```
#
 sysname P1
#
 mpls lsr-id 2.2.2.2
 mpls
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
 mpls
#
interface GigabitEthernet2/0/0
 ip address 10.1.5.2 255.255.255.0
 mpls
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
ospf 100
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.5.0 0.0.0.255
#
static-lsp transit lto4 incoming-interface GigabitEthernet1/0/0 in-label 20 nexthop 10.1.5.1
 out-label 30
#
return
```

● P2 的配置文件

```
#
 sysname P2
#
 mpls lsr-id 3.3.3.3
 mpls
#
interface GigabitEthernet1/0/0
 ip address 10.1.2.2 255.255.255.0
 mpls
#
interface GigabitEthernet2/0/0
 ip address 10.1.4.2 255.255.255.0
 mpls
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
ospf 100
```

```
area 0.0.0.0
 network 3.3.3.3 0.0.0.0
 network 10.1.2.0 0.0.0.255
 network 10.1.4.0 0.0.0.255
#
return
```

2 MPLS LDP 配置

关于本章

MPLS LDP 规定了标签分发过程中的各种消息以及相关的处理进程，主要用于 LSR 之间协商会话参数，进行标签分配，进而建立起标签交换路径（LSP）。

2.1 MPLS LDP 概述

MPLS LDP 是一种标签分发协议，广泛应用于 VPN 网络，具有组网简单、配置简单、可以提供路由拓扑驱动建立 LSP、支持大容量 LSP 等优点。

2.2 AR1200 支持的 MPLS LDP 特性

系统支持的 MPLS LDP 特性有 LDP 会话、LDP LSP、LDP 跨域扩展、可靠性。

2.3 配置 LDP 本地会话

创建 LDP LSP 之前，必须在待创建 LSP 上的所有 LSR 之间配置 LDP 本地会话。

2.4 配置 LDP 远端会话

远端 LDP 会话可以建立在不相邻的 LSR 之间，也可以建立在相邻的 LSR 之间。

2.5 配置 LDP LSP

LDP 是一种标签发布方式，可以作为 MPLS 域的标签发布协议建立 LSP。

2.6 配置 LDP 跨域扩展

通过配置 LDP 跨域扩展，可以使能 LDP 按照最长匹配方式查找路由，建立跨越 IGP 域的 LDP LSP。

2.7 配置静态 BFD 检测 LDP LSP

配置静态 BFD 检测 LDP LSP，可以通过指定的参数检测 LSP 的连通性。

2.8 配置动态 BFD 检测 LDP LSP

配置动态 BFD 检测 LDP LSP，不需要指定 BFD 参数，能够提高链路故障检测速度、减少配置工作量。

2.9 配置 Manual LDP FRR

配置 Manual LDP FRR，可以使 LDP 在链路发生故障时，将流量快速切换到备份 LSP 上，保证流量不中断。

2.10 配置 LDP Auto FRR

配置 LDP Auto FRR 功能，可以在网络故障时实现业务的迅速切换，提高网络的可靠性。

2.11 配置 LDP 和 IGP 同步

通过配置 LDP 和 IGP 同步，可以抑制 IGP 邻居关系建立来推迟路由回切，直至 LDP 完成收敛。

2.12 配置 LDP 和静态路由同步

LDP 和静态路由同步通过抑制静态路由活跃来迫使正切场景下静态路由切换到备份链路，回切场景下推迟流量回切，使静态路由和 LDP 保持同步来保证流量不中断。

2.13 配置 LDP GTSM

通过配置 LDP GTSM，可以检测 TTL 来防止攻击。

2.14 配置 LDP 安全特性

在对安全性要求较高的网络中，可以通过配置 LDP MD5 认证、LDP Keychain 认证、LDP GTSM 来提高网络的安全性。

2.15 配置 LDP GR

通过配置 LDP GR，可以实现主备倒换或协议重启的设备（Restarter）转发不中断，从而达到限制控制层协议震荡的目的。

2.16 维护 MPLS LDP

维护 MPLS LDP，包括清除 MPLS 的统计信息、检测 LSP 连通性/可达性、配置 LDP LSP 的 Trap 功能。

2.17 配置举例

介绍 MPLS LDP 配置举例。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、配置思路等。

2.1 MPLS LDP 概述

MPLS LDP 是一种标签分发协议，广泛应用于 VPN 网络，具有组网简单、配置简单、可以提供路由拓扑驱动建立 LSP、支持大容量 LSP 等优点。

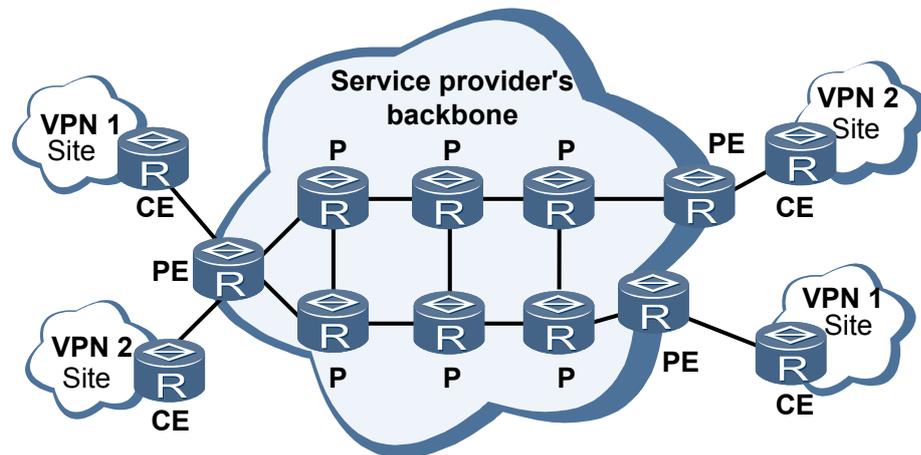
20 世纪 90 年代初，Internet 快速普及。传统的 IP 技术虽然简单，但由于当时硬件技术的限制，采用最长匹配查找的 IP 技术已经成为限制网络转发性能的一大瓶颈。ATM (Asynchronous Transfer Mode) 技术采用定长标签，并且只需要维护比路由表规模小得多的标签表，能够提供比 IP 路由方式高得多的转发性能。虽然 ATM 技术性能高，但其复杂的控制信令和高昂的部署成本使得它很难普及。MPLS (Multiprotocol Label Switching) 技术就是在这种背景下产生的，它把 IP 和 ATM 的优势很好地结合在一起。

MPLS 最初是为了提高设备的转发速度而提出的。随着 ASIC (Application Specific Integrated Circuit) 技术的发展，路由查找速度已经不是阻碍网络发展的瓶颈。这使得 MPLS 在提高转发速度方面不再具备明显的优势。但是 MPLS 支持多层标签、转发平面面向连接和控制平面面向无连接的特性，使其在 VPN (Virtual Private Network)、流量工程、QoS (Quality of Service) 等方面得到广泛应用。

LDP (Label Distribution Protocol, 标签分发协议) 是 MPLS (Multi-Protocol Label Switching, 多协议标签交换) 的一种控制协议。与大多数路由协议类似，LDP 通过组播 Hello 报文自动发现邻居建立邻居关系，或者通过单播 Hello 报文建立目标邻居关系。LDP 通过邻居间 TCP 连接的建立和参数的协商来建立邻居间的会话关系。在 LDP 会话基础上，LDP 协议分发标签映射关系，根据路由来建立标签交换路径 LSP。数据报文通过 LSP 穿越 MPLS 网络。

在实际网络中，LDP 可以运行在骨干网的 P 设备上，进行 LDP 转发；也可以运行在边缘 PE 设备上，以便部署 LDP over TE 等业务。

图 2-1 LDP 适用组网



2.2 AR1200 支持的 MPLS LDP 特性

系统支持的 MPLS LDP 特性有 LDP 会话、LDP LSP、LDP 跨域扩展、可靠性。

LDP 会话

LDP (Label Distribution Protocol) 会话用于在 LSR (Label Switching Router) 之间进行标签交换。LDP 会话分为以下两种：

- 本地 LDP 会话 (Local LDP Session)：本地 LDP 会话只能在相邻的 LSR 之间建立。
- 远端 LDP 会话 (Remote LDP Session)：远端 LDP 会话主要建立在不相邻的 LSR 之间，也可以建立在相邻的 LSR 之间。

LDP LSP

LDP 协议是创建动态 LSP 的一种方法。如果管理员不需要严格控制 LSP 建立的过程，且不需要在 MPLS 网络中部署流量工程，则推荐采用 LDP 协议来创建 LSP。

LDP 跨域扩展

LDP 跨域扩展支持按照最长匹配方式查找路由，建立跨越 IGP 区域的 LDP LSP。

可靠性

AR1200 支持以下 LDP LSP 的可靠性保护措施：

- BFD
BFD 可以用来检测 LDP LSP 转发路径的故障，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 LDP LSP 数据平面的故障具有以下优势：
 - 快速检测
 - 支持大规模 LSP 的故障检测
- LDP FRR
传统的 IP FRR (Fast ReRoute) 无法有效保护 MPLS 网络中的流量，AR1200 提供 LDP 快速重路由 (LDP FRR) 功能，为 MPLS 网络提供端口级的保护方案。
网络运行正常时，使用主用 LSP 转发，如果主用 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。
AR1200 支持 LDP Auto FRR 和 Manual LDP FRR。
- LDP 和 IGP 同步
在存在主备链路的组网中，当主链路故障时，流量从主链路切换到备份链路，这个过程流量的中断时间较短，约几百毫秒。当主链路故障恢复时，流量从备份链路切换到主链路，这个过程流量的中断时间较长，约为 5 秒。
通过配置 LDP 和 IGP 同步功能，能够缩短流量从备份链路切换到主链路时的中断时间，并控制在毫秒级。
- LDP 和静态路由同步
在存在主备 LSP 的 MPLS 组网中，LSR 之间依靠静态路由建立 LSP，当主链路故障时，流量从主链路切换到备份链路，这个过程流量的中断时间较短，约几百毫秒。当主链路故障恢复时，流量从备份链路切换到主链路，这个过程流量的中断时间较长，约为几秒。
通过配置 LDP 和静态路由同步功能，能够缩短流量从备份链路切换到主链路时的中断时间，并控制在毫秒级。

LDP 和静态路由同步通过抑制静态路由活跃来迫使正切场景下流量切换到备份链路，回切场景下推迟流量回切，使静态路由的转发路径和 LSP 保持同步。

- LDP 安全特性

LDP 安全特性包括 LDP MD5 认证、LDP Keychain 认证、LDP GTSM。

- LDP MD5 认证：MD5 的典型应用是针对一段信息计算出对应的信息摘要，从而防止信息被篡改。MD5 信息摘要是通过不可逆的字符串变换算法产生的，结果唯一。因此，不管信息内容在传输过程中发生任何形式的改变，只要重新计算就会产生不同的信息摘要，接收端就可以由此判定收到的是一个不正确的报文。
- LDP Keychain 认证：Keychain 是一种增强型加密算法，类似于 MD5，Keychain 也是针对同一段信息计算出对应的信息摘要，实现 LDP 报文防篡改校验。
- LDP GTSM：GTSM 机制通过 TTL 的检测来达到防止攻击的目的。通过检测 IP 报文头中的 TTL 值是否在一个预先定义好的特定范围内来对节点进行保护，增强系统的安全性。

- LDP GR

GR (Graceful Restart) 是实现 HA (High Availability) 的关键技术。GR 目前已经被广泛的应用在主备倒换和系统升级方面。LDP GR 可以保证当系统进行主备倒换时不复位接口板，数据层面上的 LDP LSP 信息被保留，使 LSP 转发不中断，减少对 MPLS 报文转发的影响。



说明

AR1200 只能作为 Helper 路由器，不能作为 Restarter 路由器。

2.3 配置 LDP 本地会话

创建 LDP LSP 之前，必须在待创建 LSP 上的所有 LSR 之间配置 LDP 本地会话。

2.3.1 建立配置任务

在配置 LDP 本地会话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，可以快速、准确地完成配置任务。

应用环境

LDP 协议通过标签转发路径 LSP 实现标签的分发和交换。创建 LSP 之前，需要首先建立 LDP 本地会话。因此，需要部署 LDP 业务时，必须在待创建 LSP 上的所有 LSR 之间建立 LDP 本地会话。

前置任务

在配置 LDP 本地会话之前，需完成以下任务：

- 配置静态路由或 IGP 协议，使各节点间的 IP 路由可达。

数据准备

在配置 LDP 本地会话之前，需要准备以下数据。

序号	数据
1	各节点的 LSR ID
2	建立 LDP 本地会话的接口名称和编号
3	(可选) LDP 传输地址
4	(可选) LDP 定时器 <ul style="list-style-type: none">● 链路 Hello 保持定时器的值● 链路 Hello 发送定时器的值● KeepAlive 保持定时器的值● KeepAlive 发送定时器的值● 指数回退 (Backoff) 定时器的值

2.3.2 配置全局 MPLS LDP 能力

配置 LDP 会话前，需要首先在 MPLS 域的所有节点配置全局 MPLS LDP 能力。

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 lsr-id lsr-id`，配置本节点的 LSR ID。

配置 LSR ID 时，请注意以下事项：

- 配置 LSR ID 是进行所有 MPLS 配置的前提。
- LSR 没有缺省的 LSR ID，必须手工配置。
- 推荐使用 LSR 某个 Loopback 接口的地址做为 LSR ID。
- 如果要修改已经配置的 LSR ID，必须在系统视图下执行 `undo mpls` 命令删除所有 MPLS 配置。



执行 `undo mpls` 命令会导致所有 MPLS 的相关配置都被删除，包括建立成功的 LDP 会话及 LSP，造成业务中断。因此，请配置前对网络中每个 LSR 的 LSR ID 进行统一规划，避免出现修改 LSR ID 的情况。

步骤 3 执行命令 `mpls`，使能全局 MPLS 功能，并进入 MPLS 视图。

缺省情况下，没有使能全局的 MPLS 功能。

步骤 4 执行命令 `quit`，退回系统视图。

步骤 5 执行命令 `mpls ldp`，使能全局的 LDP 功能，并进入 MPLS-LDP 视图。

缺省情况下，没有使能全局的 LDP 功能。

步骤 6（可选）执行命令 **lsp-id lsp-id**，配置 LDP 实例的 LSR ID。

缺省情况下，LDP 实例的 LSR ID 等于节点的 LSR ID。推荐采用缺省值。

---结束

2.3.3（可选）配置 LDP 动态能力通告功能

在配置全局的 MPLS LDP 能力后，如果配置 LDP 动态能力通告功能，可以确保在不中断会话的情况下，动态的使能或者去使能 LDP 新的扩展能力，保证 LSP 的稳定性。

背景信息

对于未使能 LDP 动态能力通告功能的情况下建立的 LDP 会话，在使能 LDP 某特性时，LDP 会话都会中断，进行该特性的协商，造成 LSP 的不稳定。使能 LDP 动态能力通告功能，可以确保在不中断会话的情况下，动态的使能或者去使能支持 LDP 动态能力通告功能的 LDP 特性，保证 LSP 的稳定性。

 说明

建议在使能 LDP 能力后就使能 LDP 动态能力通告功能，因为该功能不会对以往的功能造成影响，而且便于新的扩展功能的动态能力通告。

配置 LDP 动态能力通告功能前，需要先全局使能 MPLS 和 MPLS LDP 能力。

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 ldp**，进入 MPLS-LDP 视图。

步骤 3 执行命令 **capability-announcement**，使能 LDP 动态能力通告功能。

缺省情况下，没有使能 LDP 动态能力通告功能。

 说明

如果在 LDP 会话建立后使能 LDP 动态能力通告功能，则会导致 LDP 会话重建。

---结束

2.3.4 配置 LDP 本地会话

配置 LDP 本地会话之后，LSR 之间才可以建立 LDP LSP，从而进行标签交换。

背景信息

LDP 本地会话的建立基于 TCP。TCP 连接建立成功后，LSR 之间会协商 LDP 会话的相关参数。对于会话相关参数的协商结果，如果建立会话的 LSR 都可以接受，那么 LDP 本地会话就可以成功建立了。

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**，进入需要建立 LDP 会话的接口视图。

步骤 3 执行命令 **mpls**，使能接口的 MPLS 能力。

步骤 4 执行命令 `mpls ldp`，使能接口的 MPLS LDP 能力。

缺省情况下，没有使能接口的 MPLS LDP 能力。

 说明

如果去使能接口的 MPLS LDP 能力，将会导致接口下的所有 LDP 会话中断，基于这些会话的所有 LSP 也将被删除。

---结束

2.3.5 （可选）配置 LDP 传输地址

LDP 会话基于 TCP 连接，当两台 LSR 之间要建立 LDP 会话前，它们需要先确认对端的 LDP 传输地址，然后才能建立 TCP 连接。

背景信息

传输地址是用来与对等体建立 TCP 连接的，因此建立 LDP 本地会话的对等体都需要有到达对端传输地址的路由。通常使用 LSR ID（Loopback 接口地址）作为传输地址。

 说明

- 两个 LSR 之间存在多条链路时，若要在多条链路上建立 LDP 会话，会话同一端的接口都应采用默认的传输地址，或者配置相同的传输地址。如果会话的一端接口配置了不同的传输地址，将导致 LDP 会话只能建立在一条链路上。
- 修改 LDP 传输地址的配置时，会导致 LDP 会话中断，请谨慎配置。

一般情况下，建议用户不要修改 LDP 传输地址。

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`，进入建立 LDP 会话的接口视图。

步骤 3 执行命令 `mpls ldp transport-address { interface-type interface-number | interface }`，配置 LDP 传输地址为指定接口的 IP 地址。

- `interface-type interface-number`：指定接口类型和编号。LDP 使用指定的接口主 IP 地址做为 TCP 传输地址。
- `interface`：LDP 使用当前接口的主 IP 地址做为 TCP 传输地址。

缺省情况下，公网的 LDP 传输地址等于节点的 LSR ID，私网的传输地址等于接口的主 IP 地址。

---结束

2.3.6 （可选）配置 LDP 本地会话的定时器

LDP 本地会话的定时器分为链路 Hello 发送定时器、链路 Hello 保持定时器、KeepAlive 发送定时器、KeepAlive 保持定时器以及指数回退定时器。

背景信息

LDP 本地会话使用以下定时器：

表 2-1 LDP 本地会话的定时器

定时器	描述	使用建议
链路 Hello 发送定时器	LSR 使用 Hello 定时器周期性地发送 Hello 消息，向邻居 LSR 通告它在网络中的存在，并建立 Hello 邻接关系。LDP 本地会话中的 Hello 发送定时器叫作链路 Hello 发送定时器。	在网络状况不是很好的网络中，可以适当调小 Hello 发送定时器的时间，以便尽早发现网络故障。
链路 Hello 保持定时器	建立了 Hello 邻接关系的 LDP 对等体之间，通过周期性发送 Hello 报文表明自己希望继续维持这种邻接关系。如果 Hello 保持定时器超时，没有收到新的 Hello 报文，则拆除 Hello 邻接关系。LDP 本地会话中的 Hello 保持定时器叫作链路 Hello 保持定时器。	在链路状态不稳定，或者发送报文数量较大的网络中，可以适当调大 Hello 保持定时器的时间，以避免会话被频繁拆除和建立。
KeepAlive 发送定时器	LDP 会话建立以后，LSR 启动 KeepAlive 发送定时器周期性地发送 KeepAlive 消息，用于保持 LDP 会话。	在网络状况不是很好的网络中，可以适当调小 KeepAlive 发送定时器的时间，以便尽早发现网络故障。
KeepAlive 保持定时器	LDP 对等体之间通过 LDP 协议报文（PDU）维持 LDP 会话，如果会话保持定时器超时，没有收到任何 LDP PDU，则关闭连接，结束 LDP 会话。	在链路状态不稳定的网络中，可以适当调大 KeepAlive 保持定时器的时间，以尽量避免 LDP 会话振荡。
指数回退定时器	LDP 会话初始化消息处理失败或者收到对端 LSR 会话初始化消息的拒绝通知后，会话发起的主动端会启动指数回退定时器，定期尝试重新建立会话。	<ul style="list-style-type: none"> ● 当设备升级时，需要延长会话发起端尝试建立会话的周期，可以配置较大的指数回退定时器的初始值和最大值。 ● 当设备承载业务容易发生闪断时，需要缩短会话发起端尝试建立会话的周期，可以配置较小的指数回退定时器的初始值和最大值。

通常情况下，建议使用各定时器的缺省配置。

操作步骤

- 配置链路 Hello 发送定时器
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **interface interface-type interface-number**，进入建立 LDP 会话的接口视图。
 3. 执行命令 **mpls ldp timer hello-send interval**，配置链路 Hello 发送定时器。

缺省情况下，链路 Hello 发送定时器的值是实际生效的链路 Hello 保持定时器值的 1/3。

链路 Hello 发送定时器的实际生效值=Min { 链路 Hello 发送定时器的配置值，实际生效的链路 Hello 保持定时器值的 1/3 }

- 配置链路 Hello 保持定时器

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface interface-type interface-number**，进入建立 LDP 会话的接口视图。
3. 执行命令 **mpls ldp timer hello-hold interval**，配置链路 Hello 保持定时器。

缺省情况下，链路 Hello 保持定时器的值是 15 秒。

本端 LSR 所配置的 Hello 保持定时器的值并不一定等于实际生效的定时器的值。实际生效的定时器值等于 LDP 本地会话两端 LSR 所配置的定时器的较小值。

- 配置本地 LDP 会话的 KeepAlive 发送定时器

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface interface-type interface-number**，进入建立 LDP 会话的接口视图。
3. 执行命令 **mpls ldp timer keepalive-send interval**，配置本地 LDP 会话的 KeepAlive 发送定时器。

缺省情况下，本地 LDP 会话的 KeepAlive 发送定时器的值是实际生效的本地 LDP 会话的 KeepAlive 保持定时器值的 1/3。

本地 LDP 会话 KeepAlive 发送定时器的实际生效值=Min { 本地 LDP 会话 KeepAlive 发送定时器的配置值，实际生效的本地 LDP 会话 KeepAlive 保持定时器值的 1/3 }

如果两个 LSR 之间使能 LDP 的链路条数超过 1 条，所有链路的 KeepAlive 发送定时器时间必须相同，否则 LDP 会话可能不稳定。



注意

修改 KeepAlive 发送定时器的值会导致相关 LDP 实例的会话重建。

- 配置本地 LDP 会话的 KeepAlive 保持定时器

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface interface-type interface-number**，进入建立 LDP 会话的接口视图。
3. 执行命令 **mpls ldp timer keepalive-hold interval**，配置本地 LDP 会话的 KeepAlive 保持定时器。

缺省情况下，本地 LDP 会话的 KeepAlive 保持定时器的值是 45 秒。

本端 LSR 所配置的 KeepAlive 保持定时器的值并不一定等于实际生效的定时器的值。实际生效的定时器值等于 LDP 本地会话两端 LSR 所配置的定时器的较小值。

如果两个 LSR 之间使能 LDP 的链路条数超过 1 条，所有链路的 KeepAlive 保持定时器时间必须相同，否则 LDP 会话可能不稳定。



注意

修改 KeepAlive 保持定时器的值会导致相关 LDP 实例的会话重建。

- 配置指数回退定时器
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **mpls**，进入 MPLS 视图。
 3. 执行命令 **quit**，退回系统视图。
 4. 执行命令 **mpls ldp**，进入 MPLS-LDP 视图。
 5. 执行命令 **backoff timer init max**，配置指数回退定时器。
 - **init**: 指数回退定时器的初始值。整数形式，取值范围是 5 ~ 2147483，单位是秒。缺省值是 15 秒。
 - **max**: 配置指数回退定时器的最大值。整数形式，取值范围是 5 ~ 2147483，单位是秒。缺省值是 120 秒。

说明

建议配置指数回退定时器初始值 **init** 不小于 15 秒，最大值 **max** 不小于 120 秒。

需要调整会话发起端尝试建立会话的周期时，可以配置 **backoff timer** 命令。

- 当设备升级时，需要延长会话发起端尝试建立会话的周期，此时可以执行 **backoff timer** 命令，配置较大的指数回退定时器的初始值和最大值。
- 当设备承载业务容易发生闪断时，需要缩短会话发起端尝试建立会话的周期，此时可以执行 **backoff timer** 命令，配置较小的指数回退定时器的初始值和最大值。

---结束

2.3.7 检查配置结果

LDP 本地会话配置成功后，可以查看使能了 MPLS 和 MPLS LDP 的接口信息、LDP 信息、LDP 会话状态信息、LDP 会话的对等体信息以及 LDP 会话的远端对等体信息。

前提条件

已完成 LDP 本地会话功能的所有配置。

操作步骤

- 使用 **display mpls interface [interface-type interface-number] [verbose]** 命令查看使能了 MPLS 的接口信息。
- 使用 **display mpls ldp [all] [verbose]** 命令查看 LDP 信息。
- 使用以下命令查看使能了 LDP 的接口信息：
 - **display mpls ldp interface [interface-type interface-number | verbose]**
 - **display mpls ldp interface [all] [verbose]**
- 使用以下命令查看 LDP 会话状态信息：
 - **display mpls ldp session [verbose | peer-id]**
 - **display mpls ldp session [all] [verbose]**
- 使用以下命令查看 LDP 会话的对等体信息：

- **display mpls ldp peer** [**verbose** | *peer-id*]
- **display mpls ldp peer** [**all**] [**verbose**]

----结束

任务示例

执行命令 **display mpls interface** 命令，可以看到所有使能了 MPLS 的接口信息。

```
<Huawei> display mpls interface
Interface          Status   TE Attr  LSP Count  CRLSP Count Effective MTU
GE1/0/0            Up       Dis      0           0           1500
```

执行 **display mpls ldp** 命令查看 LDP 全局信息，包括各种定时器信息等。

```
<Huawei> display mpls ldp
LDP Global Information
-----
Protocol Version      : V1           Neighbor Liveness      : 600 Sec
Graceful Restart      : Off          FT Reconnect Timer     : 300 Sec
MTU Signaling         : On           Recovery Timer         : 300 Sec
Capability-Announcement : On           Longest-match          : On
LDP Instance Information
-----
Instance ID           : 0            VPN-Instance           :
Instance Status       : Active       LSR ID                 : 4.4.4.4
Loop Detection        : Off          Path Vector Limit      : 32
Label Distribution Mode : Ordered      Label Retention Mode   : Liberal
Instance Deleting State : No           Instance Reseting State : No
Graceful-Delete       : Off          Graceful-Delete Timer  : 5 Sec
```

执行 **display mpls ldp interface [verbose]** 命令查看 LDP 接口信息，包括传输地址、各种定时器信息等。

```
<Huawei> display mpls ldp interface
LDP Interface Information in Public Network
Codes:LAM(Label Advertisement Mode), IFName(Interface name)
A '*' before an interface means the entity is being deleted.
-----
IFName          Status      LAM   TransportAddress  HelloSent/Rcv
-----
GigabitEthernet1/0/0  Active     DU    172.17.1.1        2495/2514
```

```
<Huawei> display mpls ldp interface verbose
LDP Interface Information in Public Network
-----
Interface Name : GigabitEthernet1/0/0
LDP ID         : 1.1.1.1:0           Transport Address : 1.1.1.1
Entity Status  : Active             Effective MTU    : 1500

Configured Hello Hold Timer      : 15 Sec
Negotiated Hello Hold Timer      : 15 Sec
Configured Hello Send Timer      : 2 Sec
Configured Keepalive Hold Timer  : 45 Sec
Configured Keepalive Send Timer  : 3 Sec
Configured Delay Timer           : 0 Sec
Label Advertisement Mode         : Downstream Unsolicited
Hello Message Sent/Rcvd         : 29913/29878 (Message Count)
Entity Deletion Status           : No
```

执行 **display mpls ldp session [verbose]** 命令查看 LDP 会话状态为 Operational。

```
<Huawei> display mpls ldp session
```

```
LDP Session(s) in Public Network
Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
A '*' before a session means the session is being deleted.
-----
PeerID           Status      LAM  SsnRole  SsnAge      KASent/Rcv
-----
2.2.2.2:0       Operational DU   Passive 0000:01:36 387/386
3.3.3.3:0       Operational DU   Passive 0000:01:30 361/361
-----
TOTAL: 2 session(s) Found.
<Huawei> display mpls ldp session verbose

LDP Session(s) in Public Network
-----
Peer LDP ID      : 2.2.2.2:0          Local LDP ID    : 1.1.1.1:0
TCP Connection   : 1.1.1.1 <- 2.2.2.2
Session State    : Operational      Session Role    : Passive
Session FT Flag  : Off                MD5 Flag        : Off
Reconnect Timer  : ---                Recovery Timer   : ---
Keychain Name    : kcl

Negotiated Keepalive Hold Timer : 45 Sec
Configured Keepalive Send Timer : 3 Sec
Keepalive Message Sent/Rcvd     : 438/438 (Message Count)
Label Advertisement Mode        : Downstream Unsolicited
Label Resource Status(Peer/Local) : Available/Available
Session Age                      : 0000:01:49 (DDDD:HH:MM)
Session Deletion Status          : No

Capability:
  Capability-Announcement         : On

Outbound&Inbound Policies Applied :
outbound peer 2.2.2.2 fec none
outbound peer all split-horizon
inbound peer 2.2.2.2 fec none

Addresses received from peer: (Count: 3)
10.1.1.2          2.2.2.2          10.1.2.1
-----
```

执行 **display mpls ldp peer** 命令查看 LDP 会话对等体信息。

```
<Huawei> display mpls ldp peer
LDP Peer Information in Public network
A '*' before a peer means the peer is being deleted.
-----
PeerID           TransportAddress  DiscoverySource
-----
2.2.2.2:0       2.2.2.2          GigabitEthernet1/0/0
3.3.3.3:0       3.3.3.3          GigabitEthernet2/0/0
-----
TOTAL: 2 Peer(s) Found.
```

2.4 配置 LDP 远端会话

远端 LDP 会话可以建立在不相邻的 LSR 之间，也可以建立在相邻的 LSR 之间。

2.4.1 建立配置任务

在配置 LDP 远端会话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，可以快速、准确地完成配置任务。

前置任务

在配置 LDP 远端会话之前，需完成以下任务：

- 配置静态路由或 IGP 协议，使各节点间的 IP 路由可达。

数据准备

在配置 LDP 远端会话之前，需要准备以下数据。

序号	数据
1	各节点的 LSR ID
2	(可选) LDP 定时器 <ul style="list-style-type: none">● Hello 保持定时器的值● Hello 发送定时器的值● KeepAlive 发送定时器的值● KeepAlive 保持定时器的值● 指数回退 (Backoff) 定时器的值

2.4.2 配置全局 MPLS LDP 能力

配置 LDP 会话前，需要首先在 MPLS 域的所有节点配置全局 MPLS LDP 能力。

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 lsr-id lsr-id`，配置本节点的 LSR ID。

配置 LSR ID 时，请注意以下事项：

- 配置 LSR ID 是进行所有 MPLS 配置的前提。
- LSR 没有缺省的 LSR ID，必须手工配置。
- 推荐使用 LSR 某个 Loopback 接口的地址做为 LSR ID。
- 如果要修改已经配置的 LSR ID，必须在系统视图下执行 `undo mpls` 命令删除所有 MPLS 配置。



执行 `undo mpls` 命令会导致所有 MPLS 的相关配置都被删除，包括建立成功的 LDP 会话及 LSP，造成业务中断。因此，请配置前对网络中每个 LSR 的 LSR ID 进行统一规划，避免出现修改 LSR ID 的情况。

步骤 3 执行命令 `mpls`，使能全局 MPLS 功能，并进入 MPLS 视图。

缺省情况下，没有使能全局的 MPLS 功能。

步骤 4 执行命令 **quit**，退回系统视图。

步骤 5 执行命令 **mpls ldp**，使能全局的 LDP 功能，并进入 MPLS-LDP 视图。

缺省情况下，没有使能全局的 LDP 功能。

步骤 6（可选）执行命令 **lsr-id lsr-id**，配置 LDP 实例的 LSR ID。

缺省情况下，LDP 实例的 LSR ID 等于节点的 LSR ID。推荐采用缺省值。

---结束

2.4.3（可选）配置 LDP 动态能力通告功能

在配置全局的 MPLS LDP 能力后，如果配置 LDP 动态能力通告功能，可以确保在不中断会话的情况下，动态的使能或者去使能 LDP 新的扩展能力，保证 LSP 的稳定性。

背景信息

对于未使能 LDP 动态能力通告功能的情况下建立的 LDP 会话，在使能 LDP 某特性时，LDP 会话都会中断，进行该特性的协商，造成 LSP 的不稳定。使能 LDP 动态能力通告功能，可以确保在不中断会话的情况下，动态的使能或者去使能支持 LDP 动态能力通告功能的 LDP 特性，保证 LSP 的稳定性。

 说明

建议在使能 LDP 能力后就使能 LDP 动态能力通告功能，因为该功能不会对以往的功能造成影响，而且便于新的扩展功能的动态能力通告。

配置 LDP 动态能力通告功能前，需要先全局使能 MPLS 和 MPLS LDP 能力。

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 ldp**，进入 MPLS-LDP 视图。

步骤 3 执行命令 **capability-announcement**，使能 LDP 动态能力通告功能。

缺省情况下，没有使能 LDP 动态能力通告功能。

 说明

如果在 LDP 会话建立后使能 LDP 动态能力通告功能，则会导致 LDP 会话重建。

---结束

2.4.4 配置 LDP 远端会话

配置 LDP 远端会话，需要全局使能 MPLS 和 MPLS LDP 能力。

背景信息

远端 LDP 会话可以建立在不相邻的 LSR 之间，也可以建立在相邻的 LSR 之间。

LDP 本地会话和远端会话可以共存，即两个 LSR 之间既可以建立本地会话，又可以建立远端会话。

在本地会话和远端会话共存的情况下，对本地会话和远端会话进行两者都支持的相关配置时，两者的配置需要保持一致。

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 ldp remote-peer remote-peer-name**，创建 MPLS LDP 远端对等体，并进入 MPLS LDP 远端对等体视图。

步骤 3 执行命令 **remote-ip ip-address**，配置 MPLS LDP 远端对等体的 IP 地址。

 说明

- 配置的远端对等体的 IP 地址必须是远端对等体的 LSR ID。LDP LSR ID 和 MPLS LSR ID 不一致时，要使用 LDP LSR ID。
- 修改或删除已经配置的远端对等体地址会导致相应的远端 LDP 会话被删除。

---结束

2.4.5（可选）配置 LDP 远端会话的定时器

LDP 远端会话的定时器分为目标 Hello 发送定时器、目标 Hello 保持定时器、KeepAlive 发送定时器、KeepAlive 保持定时器以及指数回退定时器。

背景信息

LDP 远端会话使用以下定时器：

表 2-2 LDP 远端会话的定时器

定时器	描述	使用建议
目标 Hello 发送定时器	LSR 使用 Hello 定时器周期性地发送 Hello 消息，向邻居 LSR 通告它在网络中的存在，并建立 Hello 邻接关系。LDP 远端会话中的 Hello 发送定时器叫作目标 Hello 发送定时器。	在网络状况不是很好的网络中，可以适当调小 Hello 发送定时器的时间，以便尽早发现网络故障。
目标 Hello 保持定时器	建立了 Hello 邻接关系的 LDP 对等体之间，通过周期性发送 Hello 报文表明自己希望继续维持这种邻接关系。如果 Hello 保持定时器超时，没有收到新的 Hello 报文，则拆除 Hello 邻接关系。LDP 远端会话中的 Hello 保持定时器叫作目标 Hello 保持定时器。	在链路状态不稳定，或者发送报文数量较大的网络中，可以适当调大 Hello 保持定时器的时间，以避免会话被频繁拆除和建立。
KeepAlive 发送定时器	LDP 会话建立以后，LSR 启动 KeepAlive 发送定时器周期性地发送 KeepAlive 消息，用于保持 LDP 会话。	在网络状况不是很好的网络中，可以适当调小 KeepAlive 发送定时器的时间，以便尽早发现网络故障。

定时器	描述	使用建议
KeepAlive 保持定时器	LDP 对等体之间通过 LDP 协议报文（PDU）维持 LDP 会话，如果会话保持定时器超时，没有收到任何 LDP PDU，则关闭连接，结束 LDP 会话。	在链路状态不稳定的网络中，可以适当调大 KeepAlive 保持定时器的时间，以尽量避免 LDP 会话振荡。
指数回退定时器	LDP 会话初始化消息处理失败或者收到对端 LSR 会话初始化消息的拒绝通知后，会话发起的主动端会启动指数回退定时器，定期尝试重新建立会话。	<ul style="list-style-type: none">● 当设备升级时，需要延长会话发起端尝试建立会话的周期，可以配置较大的指数回退定时器的初始值和最大值。● 当设备承载业务容易发生闪断时，需要缩短会话发起端尝试建立会话的周期，可以配置较小的指数回退定时器的初始值和最大值。

通常情况下，建议使用各定时器的缺省配置。

操作步骤

- 配置目标 Hello 发送定时器
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **mpls ldp remote-peer remote-peer-name**，进入 MPLS-LDP 远端对等体视图。
 3. 执行命令 **mpls ldp timer hello-send interval**，配置目标 Hello 发送定时器。

缺省情况下，目标 Hello 发送定时器的值是实际生效的目标 Hello 保持定时器值的 1/3。

目标 Hello 发送定时器的实际生效值=Min{目标 Hello 发送定时器的配置值，实际生效的目标 Hello 保持定时器值的 1/3}
- 配置目标 Hello 保持定时器
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **mpls ldp remote-peer remote-peer-name**，进入 MPLS-LDP 远端对等体视图。
 3. 执行命令 **mpls ldp timer hello-hold interval**，配置目标 Hello 保持定时器。

缺省情况下，目标 Hello 保持定时器的值是 45 秒。

本端 LSR 所配置的 Hello 保持定时器的值并不一定等于实际生效的定时器的值。实际生效的定时器值等于 LDP 远端会话两端所配置的定时器的较小值。
- 配置远端 LDP 会话的 KeepAlive 发送定时器
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **mpls ldp remote-peer remote-peer-name**，进入 MPLS-LDP 远端对等体视图。
 3. 执行命令 **mpls ldp timer keepalive-send interval**，配置远端 LDP 会话的 KeepAlive 发送定时器。

缺省情况下，远端 LDP 会话的 KeepAlive 发送定时器的值是实际生效的远端 LDP 会话的 KeepAlive 保持定时器值的 1/3。

远端 LDP 会话 KeepAlive 发送定时器的实际生效值= $\text{Min}\{\text{远端 LDP 会话 KeepAlive 发送定时器的配置值, 实际生效的远端 LDP 会话 KeepAlive 保持定时器值的 } 1/3\}$

如果两个 LSR 之间使能 LDP 的链路条数超过 1 条，所有链路的 KeepAlive 发送定时器时间必须相同，否则 LDP 会话可能不稳定。



注意

修改 KeepAlive 发送定时器的值会导致相关 LDP 实例的会话重建。

- 配置远端 LDP 会话的 KeepAlive 保持定时器

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **mpls ldp remote-peer remote-peer-name**，进入 MPLS-LDP 远端对等体视图。
3. 执行命令 **mpls ldp timer keepalive-hold interval**，配置远端 LDP 会话的 KeepAlive 保持定时器。

缺省情况下，远端 LDP 会话的 KeepAlive 保持定时器的值是 45 秒。

本端 LSR 所配置的 KeepAlive 保持定时器的值并不一定等于实际生效的定时器的值。实际生效的定时器值等于 LDP 远端会话两端所配置的定时器的较小值。

如果两个 LSR 之间使能 LDP 的链路条数超过 1 条，所有链路的 KeepAlive 保持定时器时间必须相同，否则 LDP 会话可能不稳定。



注意

修改 KeepAlive 保持定时器的值会导致相关 LDP 实例的会话重建。

- 配置指数回退定时器

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **mpls**，进入 MPLS 视图。
3. 执行命令 **quit**，退回系统视图。
4. 执行命令 **mpls ldp**，进入 MPLS-LDP 视图。
5. 执行命令 **backoff timer init max**，配置指数回退定时器。
 - **init**: 指数回退定时器的初始值。整数形式，取值范围是 5 ~ 2147483，单位是秒。缺省值是 15 秒。
 - **max**: 配置指数回退定时器的最大值。整数形式，取值范围是 5 ~ 2147483，单位是秒。缺省值是 120 秒。



说明

建议配置指数回退定时器初始值 **init** 不小于 15 秒，最大值 **max** 不小于 120 秒。

需要调整会话发起端尝试建立会话的周期时，可以配置 **backoff timer** 命令。

- 当设备升级时，需要延长会话发起端尝试建立会话的周期，此时可以执行 **backoff timer** 命令，配置较大的指数回退定时器的初始值和最大值。
- 当设备承载业务容易发生闪断时，需要缩短会话发起端尝试建立会话的周期，此时可以执行 **backoff timer** 命令，配置较小的指数回退定时器的初始值和最大值。

----结束

2.4.6 检查配置结果

LDP 远端会话配置成功后，可以查看使能了 MPLS 和 MPLS LDP 的接口信息、LDP 信息、LDP 会话状态信息、LDP 会话的对等体信息以及 LDP 会话的远端对等体信息。

前提条件

已完成 LDP 远端会话功能的所有配置。

操作步骤

- 使用 **display mpls ldp [all] [verbose]** 命令查看 LDP 信息。
- 使用以下命令查看 LDP 会话状态信息：
 - **display mpls ldp session [verbose | peer-id]**
 - **display mpls ldp session [all] [verbose]**
- 使用以下命令查看 LDP 会话的对等体信息：
 - **display mpls ldp peer [verbose | peer-id]**
 - **display mpls ldp peer [all] [verbose]**
- 使用 **display mpls ldp remote-peer [remote-peer-name]** 命令查看 LDP 会话的远端对等体信息。

----结束

任务示例

执行 **display mpls ldp** 命令查看 LDP 全局信息，包括各种定时器信息等。

```
<Huawei> display mpls ldp
LDP Global Information
-----
Protocol Version      : V1           Neighbor Liveness    : 600 Sec
Graceful Restart     : Off           FT Reconnect Timer  : 300 Sec
MTU Signaling        : On            Recovery Timer       : 300 Sec
Capability-Announcement : On         Longest-match       : On
-----
LDP Instance Information
-----
Instance ID          : 0           VPN-Instance        :
Instance Status      : Active       LSR ID              : 4.4.4.4
Loop Detection       : Off          Path Vector Limit    : 32
Label Distribution Mode : Ordered   Label Retention Mode : Liberal
Instance Deleting State : No       Instance Reseting State : No
Graceful-Delete     : Off          Graceful-Delete Timer : 5 Sec
-----
```

执行 **display mpls ldp interface [verbose]** 命令查看 LDP 接口信息，包括传输地址、各种定时器信息等。

```
<Huawei> display mpls ldp interface

LDP Interface Information in Public Network
```

```
Codes:LAM(Label Advertisement Mode), IFName(Interface name)
A '*' before an interface means the entity is being deleted.
-----
IFName           Status      LAM   TransportAddress  HelloSent/Rcv
-----
GigabitEthernet1/0/0  Active      DU    172.17.1.1       2495/2514
-----
<Huawei> display mpls ldp interface verbose

LDP Interface Information in Public Network
-----
Interface Name : GigabitEthernet1/0/0
LDP ID         : 1.1.1.1:0           Transport Address : 1.1.1.1
Entity Status  : Active              Effective MTU    : 1500

Configured Hello Hold Timer      : 15 Sec
Negotiated Hello Hold Timer      : 15 Sec
Configured Hello Send Timer      : 2 Sec
Configured Keepalive Hold Timer  : 45 Sec
Configured Keepalive Send Timer  : 3 Sec
Configured Delay Timer           : 0 Sec
Label Advertisement Mode         : Downstream Unsolicited
Hello Message Sent/Rcvd         : 29913/29878 (Message Count)
Entity Deletion Status           : No
-----
```

执行 **display mpls ldp session [verbose]** 命令查看 LDP 会话状态为 Operational。

```
<Huawei> display mpls ldp session
LDP Session(s) in Public Network
Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
A '*' before a session means the session is being deleted.
-----
PeerID           Status      LAM   SsnRole  SsnAge      KASent/Rcv
-----
2.2.2.2:0        Operational DU    Passive  0000:01:36  387/386
3.3.3.3:0        Operational DU    Passive  0000:01:30  361/361
-----
TOTAL: 2 session(s) Found.
<Huawei> display mpls ldp session verbose

LDP Session(s) in Public Network
-----
Peer LDP ID      : 2.2.2.2:0           Local LDP ID   : 1.1.1.1:0
TCP Connection   : 1.1.1.1 <- 2.2.2.2
Session State    : Operational      Session Role    : Passive
Session FT Flag  : Off              MD5 Flag        : Off
Reconnect Timer  : ---                    Recovery Timer  : ---
Keychain Name    : kcl

Negotiated Keepalive Hold Timer : 45 Sec
Configured Keepalive Send Timer : 3 Sec
Keepalive Message Sent/Rcvd     : 438/438 (Message Count)
Label Advertisement Mode        : Downstream Unsolicited
Label Resource Status(Peer/Local) : Available/Available
Session Age                      : 0000:01:49 (DDDD:HH:MM)
Session Deletion Status          : No

Capability:
  Capability-Announcement         : On

Outbound&Inbound Policies Applied :
outbound peer 2.2.2.2 fec none
outbound peer all split-horizon
inbound peer 2.2.2.2 fec none

Addresses received from peer: (Count: 3)
10.1.1.2          2.2.2.2          10.1.2.1
```

执行 **display mpls ldp peer** 命令查看 LDP 会话对等体信息。

```
<Huawei> display mpls ldp peer
LDP Peer Information in Public network
A '*' before a peer means the peer is being deleted.
-----
PeerID                TransportAddress  DiscoverySource
-----
2.2.2.2:0             2.2.2.2          GigabitEthernet1/0/0
3.3.3.3:0             3.3.3.3          GigabitEthernet2/0/0
-----
TOTAL: 2 Peer(s) Found.
```

执行 **display mpls ldp remote-peer** 命令查看 LDP 会话的远端对等体信息。

```
<Huawei> display mpls ldp remote-peer
-----
LDP Remote Entity Information
-----
Remote Peer Name   : lsrc
Remote Peer IP    : 3.3.3.9          LDP ID       : 1.1.1.9:0
Transport Address : 1.1.1.9          Entity Status : Active

Configured Keepalive Hold Timer : 45 Sec
Configured Keepalive Send Timer : ---
Configured Hello Hold Timer     : 45 Sec
Negotiated Hello Hold Timer     : 45 Sec
Configured Hello Send Timer     : ---
Configured Delay Timer          : 10 Sec
Hello Packet sent/received      : 61/59
Remote Peer Deletion Status     : No
Auto-config                     : ---
-----
TOTAL: 1 Peer(s) Found.
```

2.5 配置 LDP LSP

LDP 是一种标签发布方式，可以作为 MPLS 域的标签发布协议建立 LSP。

2.5.1 建立配置任务

在配置 LDP LSP 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，可以快速、准确地完成配置任务。

应用环境

如果管理员不需要严格控制 LSP 建立的过程，且不需要在 MPLS 网络中部署流量工程，则可以使用 LDP 作为 MPLS 域的标签发布协议建立 LSP。

设备能够支持的 LSP 数量取决于设备的容量和性能，如果 LSP 数量过多，可能导致设备运行不稳定。

LSP 的建立要求 LSR 上存在符合条件的路由信息，并且 LSR 上有相应的触发策略。只有通过策略过滤的路由信息，才能触发 LSP 的建立，从而控制 LSP 的数量。

建立 Ingress 或 Egress LSP 和建立 Transit LSP 时，可以采用不同的策略控制 LSP 的建立：

- 建立 Ingress 或 Egress LSP 可以采用的策略包括：
 - 所有静态路由和 IGP 路由触发建立 LSP。
 - 为带标签的公网 32 位 BGP 路由触发建立 LSP，相关配置请参见《Huawei AR1200 系列企业路由器 配置指南 VPN》的“BGP/MPLS IP VPN 配置”。
 - 主机路由触发建立 LSP。
 - 根据 IP 前缀列表触发建立 LSP。
 - 所有路由都不触发 LDP 建立 LSP。
- 当设备作为 Transit LSR 时，为防止生成过多的 Transit LSP，可以使用 IP 前缀列表对路由进行过滤，只有满足过滤策略的路由才会用于建立 Transit LSP。

前置任务

在配置 LDP LSP 之前，需完成以下任务：

- [配置 LDP 本地会话](#)

数据准备

在配置 LDP LSP 之前，需要准备以下数据。

序号	数据
1	各节点的 LSR ID

2.5.2 建立 LDP LSP

只有建立了 LDP 会话，LDP LSP 才会自动建立。

前提条件

- [配置 LDP 本地会话](#)

背景信息

在 LSP 沿途的相邻 LSR 之间配置 MPLS LDP 会话。MPLS LDP 会话建立以后，LDP LSP 就开始自动建立。

2.5.3 （可选）配置 PHP 特性

配置 PHP 特性，需要在 Egress 节点上配置向倒数第二跳分配的标签，减轻最后一跳的负担。

背景信息

在 LSP 的最后一跳节点，已不需要再进行标签交换。此时，可以配置倒数第二跳弹出特性 PHP（Penultimate Hop Popping），在倒数第二跳节点处将标签弹出，最后一跳节点直接进行 IP 转发或者下一层标签转发，减少最后一跳标签交换的负担。

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**，进入 MPLS 视图。

步骤 3 执行命令 **label advertise { explicit-null | implicit-null | non-null }**，配置向倒数第二跳分配的标签。

- 缺省情况下，使用的是 **implicit-null**，表示支持 PHP。Egress 向倒数第二跳节点分配隐式空标签，值为 3。
- 如果配置的是 **explicit-null**，表示不支持 PHP。Egress 节点向倒数第二跳分配显式空标签，值为 0。当需要支持 MPLS QOS 属性时，可以选用 **explicit-null**。
- 如果配置的是 **non-null**，表示不支持 PHP。Egress 向倒数第二跳正常分配标签，即分配的标签值不小于 16。

explicit-null 和 **non-null** 两种方式对出节点的资源消耗较大，不推荐使用。

 说明

PHP 特性的修改只对修改后建立的 LSP 生效。

---结束

2.5.4（可选）配置 LDP 标签发布方式

通过配置 LDP 标签发布方式，可以控制 LSP 的建立。

背景信息

缺省情况下，下游设备会向上游设备主动发送标签映射消息，这样网络发生故障时，业务可以迅速切换到备份路径上，提高网络的可靠性。而 MPLS 网络中部署的接入设备 DSLAM，性能较低。在网络规模较大的情况下，为了尽可能的减少 DSLAM 设备上不必要的 MPLS 转发表项，可以配置 LDP 标签发布方式为上游向下游请求标签时，下游才能向上游发送标签映射消息，减少 MPLS 转发表项。

操作步骤

- 配置本地会话标签发布方式。
 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 **mpls ldp advertisement { dod | du }**，配置标签发布方式。

 说明

- 邻居之间存在多链路的时候，所有接口的标签发布方式必须相同。
- 修改标签发布方式会导致 LDP 会话重建。

---结束

2.5.5（可选）配置 LDP 自动触发 DoD 请求功能

配置 LDP 自动触发 DoD 请求功能之前，需要配置 LDP 远端会话。

背景信息

网络规模比较大，且存在数量较多的 LDP 远端对等体时，由于网络边缘 DSLAM 设备属于低端设备，为了保证网络的稳定，需要尽可能的减少不必要的资源浪费。此时可以执行 **remote-ip auto-dod-request** 命令或者 **remote-peer auto-dod-request** 命令，配置自动触发采用 DoD 的标签发布方式向下游请求指定的或者所有的远端对等体的 LSR ID 的标签映射消息，以节省系统资源。

如果需要屏蔽自动触发采用 DoD 的标签发布方式向下游请求指定的远端对等体的 LSR ID 的标签映射消息，可以执行 **remote-ip auto-dod-request block** 命令，屏蔽自动触发采用 DoD 的标签发布方式向下游请求指定的远端对等体的 LSR ID 的标签映射消息。

说明

- 配置 **remote-peer auto-dod-request** 命令或 **remote-ip auto-dod-request** 命令前，需要配置 LDP 远端会话。
- 配置 **remote-peer auto-dod-request** 命令或 **remote-ip auto-dod-request** 命令前，需要执行 **longest-match** 命令，配置 LDP 跨域扩展功能。
- 配置 **remote-peer auto-dod-request** 命令或 **remote-ip auto-dod-request** 命令前，需要首先执行命令 **mpls ldp advertisement dod** 建立和下游的 DoD 会话。

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 ldp**，进入 MPLS LDP 视图。

步骤 3 执行下面两种方式中的一种或两种，配置自动触发采用 DoD 的标签发布方式向下游请求所有的或者指定的远端对等体的 LSR ID 的标签映射消息。

- 执行命令 **remote-peer auto-dod-request**，配置自动触发采用 DoD 的标签发布方式向下游请求所有的远端对等体的 LSR ID 的标签映射消息。
- 执行下列命令，配置自动触发采用 DoD 的标签发布方式向下游请求指定的远端对等体的 LSR ID 的标签映射消息，以及屏蔽自动触发采用 DoD 的标签发布方式向下游请求指定的远端对等体的 LSR ID 的标签映射消息。

1. 执行命令 **quit**，进入系统视图。
2. 执行命令 **mpls ldp remote-peer remote-peer-name**，创建 MPLS LDP 远端对等体，并进入 MPLS LDP 远端对等体视图。
3. 执行命令 **remote-ip ip-address**，配置 MPLS LDP 远端对等体的 IP 地址。

说明

- 配置的远端对等体的 IP 地址必须是远端对等体的 LSR ID。LDPLSR-ID 和 MPLSLSR-ID 不一致时，要使用 LDP LSR-ID。
 - 修改或删除已经配置的远端对等体地址会导致相应的远端 LDP 会话被删除。
4. 执行命令 **remote-ip auto-dod-request**，配置自动触发采用 DoD 的标签发布方式向下游请求指定的远端对等体的 LSR ID 的标签映射消息。

说明

当全局已经配置了 **remote-peer auto-dod-request** 命令时，如果需要屏蔽自动触发采用 DoD 的标签发布方式向下游请求指定的远端对等体的 LSR ID 的标签映射消息，可以执行 **remote-ip auto-dod-request block** 命令。

---结束

2.5.6 （可选）配置接口的 MPLS MTU

通过配置接口的 MPLS MTU，可以决定发送 MPLS 转发报文的大小。

背景信息

MTU 称为最大传输单元（Maximum Transmission Unit）。MTU 的大小决定了发送端一次能够发送报文的最大字节数，如果 MTU 超过了接收端所能够承受的最大值，或者是超过了发送路径上途经的某台设备所能够承受的最大值，这样就会造成报文分片甚至丢弃，加重网络传输的负担。所以设备在进行通信之前必须要把 MTU 计算明确，才能保证每次发送的报文都能够畅通无阻的到达接收端，确保报文发送一次成功。

LDP MTU=Min { 所有下游设备通告的 MTU，本机出接口 MTU }。通告方式为，把计算出来的 MTU 值放在 Label Mapping 消息的 MTU TLV 里面，然后把 Label Mapping 消息发送给上游。

如果 MTU 发生变动，如本机出接口改变或者配置变更，那么 LSR 就应该再次通过 Label Mapping 消息，把重新计算过的 MTU 通告给它的所有上游。

接口的 MPLS MTU 与接口本身的 MTU 之间存在下述关系：

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

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`，进入使能了 MPLS 的接口视图。

步骤 3 执行命令 `mpls mtu mtu`，配置接口的 MPLS MTU 值。

 说明

配置接口的 MPLS MTU 后会直接生效，不需要重启接口。

---结束

2.5.7 （可选）配置 LDP MTU 信令功能

通过配置 LDP MTU 信令功能，可以控制 LSR 发送的 MTU TLV。

背景信息

缺省情况下，使能 MPLS LDP 功能后，LSR 会发送私有的 MTU TLV，与 RFC 3988 中定义的标准 MTU TLV 不同。

- 通常情况下，推荐用户使用缺省值。
- 如果需要与其他厂商设备互连，为了实现互通则需要配置 `mtu-signalling apply-tlv` 命令，使 LSR 发送 RFC 3988 中定义的标准 MTU TLV，否则可能导致用户配置的 LDP MTU 值不生效。

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 `mpls ldp`，进入 MPLS LDP 视图。

步骤 3 执行命令 `mtu-signalling [apply-tlv]`，使能 MTU TLV 的发送功能。

缺省情况下，系统发送私有的 MTU TLV。

 说明

使能或去使能 MTU TLV 发送功能的操作将导致原始 LDP 会话重建。

---结束

2.5.8（可选）配置 LDP 水平分割策略

通过配置 LDP 水平分割策略，可以控制 LSR 不给指定的下游 LDP 对等体分配标签。

背景信息

一般情况下，LSR 会向其上游和下游 LDP 对等体都分配标签，从而提高了 LDP LSP 的收敛速度。而对于 MPLS 网络中部署的接入设备 DSLAM，性能较低。LDP 向所有对等体分配标签会导致大量 LSP 的建立，DSLAM 设备无法承受。因此，为了减少 LSP 的数量，从而节省内存，推荐为 LDP 对等体配置水平分割策略。

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 ldp`，进入 MPLS LDP 视图。

步骤 3 执行命令 `outbound peer { peer-id | all } split-horizon`，为 LDP 对等体配置水平分割策略，即控制 LSR 只向其上游 LDP 对等体分配标签。

缺省情况下，没有为 LDP 对等体配置水平分割策略，即 LSR 会向其上游和下游 LDP 对等体都分配标签。

可以通过配置不同的参数，不给指定的下游对等体分配标签。

- `peer-id`：不给指定的下游 LDP 对等体分配标签。
- `all`：不给所有下游 LDP 对等体分配标签。

 说明

针对所有 peer 的 LDP 水平分割策略比针对某个 peer 的 LDP 水平分割策略优先级高。例如先配置 `outbound peer all split-horizon`，然后再配置 `outbound peer 2.2.2.2 split-horizon`，则单个 peer 的 LDP 水平分割策略不生成配置文件。

---结束

2.5.9（可选）配置 LDP Inbound 策略和 Outbound 策略

通过配置 LDP Inbound 策略和 Outbound 策略，可以限制不必要的 LSP 的建立，从而节省内存。

背景信息

一般情况下，LSR 会接收邻居发送的所有标签映射消息，或者向其上游和下游 LDP 对等体都发送标签映射消息，以提高 LDP LSP 的收敛速度。但是接收所有的标签映射消息，或者向所有对等体发送标签映射消息会导致大量 LSP 的建立，造成资源的浪费。此时可以配置 LDP Inbound 策略或者 Outbound 策略，限制标签映射消息的接收和发送，减少 LSP 的数量，节省内存。

操作步骤

- 配置 LDP Inbound 策略。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **mpls ldp**，进入 MPLS LDP 视图。
3. 执行命令 **inbound peer { peer-id | peer-group peer-group-name | all } fec { none | host | ip-prefix prefix-name }**，配置给指定的对等体针对指定的 IGP 路由应用 Inbound 策略。

如果一组对等体或者全部对等体接收标签映射消息时，对 FEC 的限制范围是相同的，则可以配置关键字 **peer-group peer-group-name** 或者 **all**，为这些对等体配置相同的 FEC 范围。

说明

多个 Inbound 策略共存的情况下，针对某一个对等体，实际生效的 Inbound 策略以第一次的配置为准。例如先后进行了如下配置：

```
inbound peer 2.2.2.2 fec host
```

```
inbound peer peer-group group1 fec none
```

group1 中包含 peer-id 是 2.2.2.2 的对等体，则对于该对等体，实际生效的 Inbound 策略是：

```
inbound peer 2.2.2.2 fec host
```

如果先后配置的两条 Inbound 策略，对于关键字 **peer** 部分的配置完全一样，则新的配置会覆盖旧的配置，即新的配置生效。例如先后进行了如下配置：

```
inbound peer 2.2.2.2 fec host
```

```
inbound peer 2.2.2.2 fec none
```

则第二次的配置覆盖第一次的配置，即对于 peer-id 是 2.2.2.2 的对等体，实际生效的 Inbound 策略是：

```
inbound peer 2.2.2.2 fec none
```

配置 Inbound 策略前，需要先全局使能 MPLS 和 MPLS LDP 能力。

需要删除所有的 Inbound 策略时，如果针对每一个 Inbound 策略执行 **undo** 命令，比较繁琐，并且花费时间较多，此时可以执行 **undo inbound peer all** 命令，一次性删除所有的 Inbound 策略。

- 配置 LDP Outbound 策略。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **mpls ldp**，进入 MPLS LDP 视图。
3. 执行下列命令，配置给指定的对等体针对指定的 IGP 路由或者 BGP 标签路由应用 LDP Outbound 策略。
 - 执行命令 **outbound peer { peer-id | peer-group peer-group-name | all } fec { none | host | ip-prefix prefix-name }**，配置给指定的对等体针对指定的 IGP 路由应用 Outbound 策略。
 - 执行命令 **outbound peer { peer-id | peer-group peer-group-name | all } bgp-label-route { none | ip-prefix prefix-name }**，配置给指定的对等体针对指定的 BGP 标签路由应用 Outbound 策略。

如果一组对等体或者全部对等体发送标签映射消息时，对 FEC 的限制范围是相同的，则可以配置关键字 **peer-group peer-group-name** 或者 **all**，为这些对等体配置相同的 FEC 范围。

说明

多个 Outbound 策略共存的情况下，针对某一个对等体，实际生效的 Outbound 策略以第一次的配置为准。例如先后进行了如下配置：

```
outbound peer 2.2.2.2 fec host
outbound peer peer-group group1 fec none
```

group1 中包含 peer-id 是 2.2.2.2 的对等体，则对于该对等体，实际生效的 Outbound 策略是：

```
outbound peer 2.2.2.2 fec host
```

如果先后配置的两条 Outbound 策略，对于关键字 **peer** 部分的配置完全一样，则新的配置会覆盖旧的配置，即新的配置生效。例如先后进行了如下配置：

```
outbound peer 2.2.2.2 fec host
outbound peer 2.2.2.2 fec none
```

则第二次的配置覆盖第一次的配置，即对于 peer-id 是 2.2.2.2 的对等体，实际生效的 Outbound 策略是：

```
outbound peer 2.2.2.2 fec none
```

配置 Outbound 策略前，需要先全局使能 MPLS 和 MPLS LDP 能力。

需要删除所有的 Outbound 策略时，如果针对每一个 Outbound 策略执行 **undo** 命令，比较繁琐，并且花费时间较多，此时可以执行 **undo outbound peer all** 命令，一次性删除所有的 Outbound 策略。

---结束

2.5.10（可选）配置 LSP 建立的触发策略

通过配置 LSP 建立的触发策略，可以使符合条件的路由触发 LDP 建立 LSP。

背景信息

使能 MPLS LDP 后，LSP 将自动建立，如果不通过策略控制，将有大量的 LSP 建立导致资源浪费。

对于公网的 Ingress LSP 和 Egress LSP，可以配置 LSP 的建立策略，使符合条件的路由触发 LSP 的建立。仅由关注的路由触发 LDP 建立 LSP，从而控制 LSP 的数量，减少系统资源的浪费。

说明

不推荐配置 **lsp-trigger all** 命令。因为配置该命令后，所有 IGP 路由会触发 LDP 建立 LSP，导致 LSP 数量庞大，占用过多的系统资源。如果需要配置该命令，可以先配置路由过滤策略，减少路由数量，从而减少路由触发 LDP 建立的 LSP 的数量，节约系统资源。

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**，进入 MPLS 视图。

步骤 3 执行下面命令，配置 LSP 触发建立策略。

- 执行命令 **lsp-trigger { all | host | ip-prefix ip-prefix-name | none }**，配置触发静态路由和 IGP 路由建立 LSP 的策略。
- 执行命令 **lsp-trigger bgp-label-route [ip-prefix ip-prefix-name]**，配置触发带标签的公网 BGP 路由建立 LSP 的策略。

缺省情况下，触发策略为 **host**，即 32 位地址的主机 IP 路由触发建立 LSP。

- 如果触发策略为 **all**，则所有静态路由和 IGP 路由触发建立 LSP。BGP 公网路由不能触发建立 LSP。
- 如果触发策略为 **ip-prefix**，则只有通过 IP 地址前缀列表过滤的 FEC 项能够触发建立 LSP。
- 如果触发策略为 **none**，则不触发建立 LSP。
- 如果触发策略为 **bgp-label-route**，则触发带标签的公网 BGP 路由建立 LSP。

 说明

LSP 的建立需要 LSR 上有精确匹配的路由，如果使用 32 位掩码的 Loopback 接口，则必须有精确匹配的主机路由才能触发 LSP 的建立。

LDP GR 期间修改 LSP 触发策略的操作无效。

---结束

2.5.11 （可选）配置 Transit LSP 建立的触发策略

通过配置 Transit LSP 建立的触发策略，可以使满足特定要求的路由触发 LDP 建立 Transit LSP。

背景信息

使能 MPLS LDP 后，LDP LSP 将自动建立，因此可能会建立大量的 Transit LSP 导致资源的浪费。通过配置 Transit LSP 建立策略，只允许通过过滤条件的路由触发 Transit LSP 的建立，而对于没有通过过滤条件的路由，本地将不往上游发送标签映射消息，这样可以有效减少 LSP 的数量，节约网络资源。

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 ldp**，进入 MPLS LDP 视图。

步骤 3 执行命令 **propagate mapping for ip-prefix ip-prefix-name**，配置 Transit LSP 建立策略。

缺省情况下，LDP 在建立 Transit LSP 时，不对收到的路由进行过滤。

 说明

LDP GR 期间修改 Transit LSP 建立策略的操作无效。

---结束

2.5.12 检查配置结果

LDP LSP 配置成功后，可以查看 LDP 的信息、LDP LSP 的建立信息以及 LSP 的建立信息。

前提条件

已经完成 LDP LSP 功能的所有配置。

操作步骤

- 使用 **display mpls ldp [all] [verbose]** 命令查看 LDP 的信息。

- 使用 **display mpls ldp lsp [all]**命令查看 LDP LSP 的建立信息。
- 使用 **display mpls ldp [verbose]**命令查看 LSP 的建立信息。

---结束

任务示例

在配置成功时，执行上面的命令，应能得到如下的结果：

执行 **display mpls ldp** 命令查看 LDP 的相关信息。

```
<Huawei> display mpls ldp

                                LDP Global Information
-----
Protocol Version      : V1           Neighbor Liveness    : 600 Sec
Graceful Restart      : Off          FT Reconnect Timer   : 300 Sec
MTU Signaling         : On           Recovery Timer       : 300 Sec
Capability-Announcement : Off       Longest-match        : Off
                                LDP Instance Information
-----
Instance ID           : 0           VPN-Instance         :
Instance Status       : Active        LSR ID               : 4.4.4.4
Loop Detection         : Off          Path Vector Limit    : 32
Label Distribution Mode : Ordered   Label Retention Mode : Liberal
Instance Deleting State : No       Instance Reseting State : No
Graceful-Delete       : Off          Graceful-Delete Timer : 5 Sec
-----
```

执行命令 **display mpls ldp lsp**，可以看到 LDP LSP 的建立信息。

```
<Huawei> display mpls ldp lsp

LDP LSP Information
-----
DestAddress/Mask  In/OutLabel  UpstreamPeer  NextHop      OutInterface
-----
3.3.3.9/32        NULL/1025    -              10.1.1.2     GigabitEthernet1/0/0
-----

TOTAL: 1 Normal LSP(s) Found.
TOTAL: 0 Liberal LSP(s) Found.
TOTAL: 0 Frr LSP(s) Found.
A '*' before an LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
A '*' before a UpstreamPeer means the session is stale
A '*' before a DS means the session is stale
A '*' before a NextHop means the LSP is FRR LSP
```

执行命令 **display mpls lsp**，可以看到 LSP 的建立信息。

```
<Huawei> display mpls lsp

                                LSP Information: LDP LSP
-----
FEC                In/Out Label  In/Out IF      Vrf Name
-----
1.1.1.1/32         NULL/3        -/GigabitEthernet1/0/0
```

2.6 配置 LDP 跨域扩展

通过配置 LDP 跨域扩展，可以使能 LDP 按照最长匹配方式查找路由，建立跨越 IGP 域的 LDP LSP。

2.6.1 建立配置任务

在配置 LDP 跨域扩展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，可以快速、准确地完成配置任务。

应用环境

当网络规模比较大时，通常需要配置多个 IGP 区域来达到灵活部署和快速收敛的目的。在这种情况下，IGP 区域间进行路由通告时，为了避免路由数量多而引起的对资源的过多占用，区域边界路由器（ABR）需要将区域内路由聚合，再通告给相邻的 IGP 区域。然而，缺省情况下，LDP 在建立 LSP 的时候，会在路由表中查找与收到的标签映射消息中携带的 FEC 精确匹配的路由，对于聚合路由，LDP 只能建立 Liberal LSP，无法建立跨越 IGP 区域的 LDP LSP。

此时，可以执行 **longest-match** 命令，使能 LDP 按照最长匹配方式查找路由，建立跨域 LDP LSP。

前置任务

在配置 LDP 跨域扩展之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。
- 配置 IGP 协议发布各节点接口所连网段和 LSR ID 的主机路由。
- 配置聚合路由的策略。
- 配置 MPLS 及 MPLS LDP 功能。

数据准备

在配置 LDP 跨域扩展之前，需准备以下数据。

序号	数据
1	各节点的 IS-IS 区域地址及各节点和接口的 Level 级别

2.6.2 配置 LDP 跨域扩展

配置 LDP 跨域扩展，需要在 Ingress 或 Transit 节点进行配置。

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 ldp**，进入 MPLS LDP 视图。

步骤 3 执行命令 **longest-match**，使能 LDP 按照最长匹配方式查找路由建立 LSP。

 说明

LDP GR 期间不允许配置此命令。

---结束

2.6.3 检查配置结果

LDP 跨域扩展配置成功后，可以查看跨域 LSP 的建立情况。

前提条件

已经完成 LDP 跨域扩展功能的所有配置。

操作步骤

- 使用 **display mpls lsp** 命令查看使能 LDP 按照最长匹配方式查找路由建立 LSP 功能之后的跨域 LSP 的建立信息。

----结束

任务示例

使能 LDP 按照最长匹配方式查找路由建立 LSP，1.3.0.1/32、1.3.0.2/32 是到其他 IGP 域的路由，可以看到跨域 LSP 已经建立。检查配置结果如下：

```
[Huawei] display mpls lsp
```

```
-----  
LSP Information: LDP LSP  
-----  
FEC                In/Out Label  In/Out IF                Vrf Name  
1.2.0.1/32         NULL/3        -/GE1/0/0  
1.2.0.1/32         1024/3       -/GE1/0/0  
1.3.0.1/32         NULL/1025    -/GE1/0/0  
1.3.0.1/32         1025/1025   -/GE1/0/0  
1.3.0.2/32         NULL/1026    -/GE1/0/0  
1.3.0.2/32         1026/1026   -/GE1/0/0
```

2.7 配置静态 BFD 检测 LDP LSP

配置静态 BFD 检测 LDP LSP，可以通过指定的参数检测 LSP 的连通性。

2.7.1 建立配置任务

在配置静态 BFD 检测 LDP LSP 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，可以快速、准确地完成配置任务。

应用环境

静态 BFD 检测 LDP LSP 时，有以下注意事项：

- 只能在 LDP LSP 的 Ingress 进行 BFD 绑定。
- 一条 LSP 只能与一个 BFD 会话绑定。
- 只支持主机路由触发建立的 LDP LSP。

 说明

BFD 检测 LSP 时，往返转发方式可以不一致（如报文从源端到目的端走 LSP，从目的端到源端走 IP 转发），但要求往返路径一致，如果不一致，则检测到故障时，不能确定具体是哪条路径的故障。因此部署 BFD 检测时，要确认往返路径是否一致，以便检测到的故障确实是检测路径故障。

前置任务

在配置静态 BFD 检测 LDP LSP 之前，需完成以下任务：

- 配置网络层参数，使网络可达
- 使能各节点的 MPLS LDP，建立 LDP 会话
- 配置 LDP LSP

数据准备

在配置静态 BFD 检测 LDP LSP 之前，需准备以下数据。

序号	数据
1	BFD 配置名
2	LDP LSP 的参数： <ul style="list-style-type: none">● LSP 的下一跳地址● （可选）出接口类型和编号
3	BFD 会话的本地标识符和远端标识符

2.7.2 使能全局 BFD 能力

只需要在被检测链路的两端节点上使能 BFD 能力。

背景信息

在需要检测的链路两端节点上进行下列配置。

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`，对本节点使能全局 BFD 能力并进入 BFD 全局视图。

---结束

2.7.3 配置 Ingress BFD 参数

配置静态 BFD 检测 LDP LSP，需要在 Ingress 上进行相关 BFD 参数的配置。

背景信息

在 LSP 的 Ingress 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 bind ldp-lsp peer-ip ip-address nexthop ip-address [interface interface-type interface-number]`，配置绑定动态 LSP 的 BFD 会话。

当待检测 LSP 的出接口的 IP 地址是借用其它接口的，或者被其它接口借用时，必须指定出接口。

 说明

在 LDP over TE 场景下配置静态 BFD 检测 LDP LSP 时，需要配置 **interface interface-type interface-number** 为 TE 隧道的接口。

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 (可选) 执行下列命令调整本地发送 BFD 报文的最小时间间隔、本地允许接收 BFD 报文的最小时间间隔和本地 BFD 检测倍数。

1. 执行命令 **quit**，退回系统视图。
2. 执行命令 **mpls**，使能本节点的 MPLS 能力，并进入 MPLS 视图。
3. 执行命令 **mpls bfd min-tx-interval *interval***，调整本地发送 BFD 报文的最小时间间隔。

缺省值是 1000 毫秒。

当反向通道采用 IP 链路时，不能配置本地参数。

本地 BFD 报文实际发送时间间隔 = MAX { 本地配置的发送时间间隔，对端配置的接收时间间隔 }；本地实际接收时间间隔 = MAX { 对端配置的发送时间间隔，本地配置的接收时间间隔 }；本地检测时间 = 本地接收时间间隔 × 对端配置的 BFD 检测倍数。

例如：

- 本地配置的发送时间间隔为 200ms，接收时间间隔为 300ms，检测倍数为 4。
- 对端配置的发送时间间隔为 100ms，接收时间间隔为 600ms，检测倍数为 5。

则：

- 本地实际的发送时间间隔为 MAX { 200ms, 600ms } = 600ms，接收时间间隔为 MAX { 100ms, 300ms } = 300ms，检测时间间隔为 300ms × 5 = 1500ms。
- 对端实际的发送时间间隔为 MAX { 100ms, 300ms } = 300ms，接收时间间隔为 MAX { 200ms, 600ms } = 600ms，检测时间间隔为 600ms × 4 = 2400ms。

4. 执行命令 **mpls bfd min-rx-interval *interval***，调整本地允许接收 BFD 报文的最小时间间隔。

缺省值是 1000 毫秒。

当反向通道采用 IP 链路时，不能配置本地参数。

5. 执行命令 **mpls bfd detect-multiplier *multiplier***，调整本地 BFD 检测倍数。

缺省值是 3。

6. 执行命令 **quit**，退回系统视图。
7. 执行命令 **bfd *cfg-name***，进入 BFD 会话视图。

步骤 5 执行命令 **commit**，提交配置。

---结束

后续处理

BFD 会话创建成功并且状态为 Up 以后，开始对 LDP LSP 进行故障检测。

当 LDP LSP 被删除时，BFD 的状态变为 Down。

2.7.4 配置 Egress BFD 参数

配置静态 BFD 检测 LDP LSP，需要在 Egress 上进行相关 BFD 参数的配置。

背景信息

用于向入节点通告故障的反向通道可以是 IP 链路、LSP 或者 TE 隧道，为了避免反向 LSP 故障影响 BFD 的检测，一般情况下优先选用 IP 链路。若此反向通道也需要 BFD 检测，可以再配置一对 BFD 会话进行检测。

在 LSP 的 Egress 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 配置 BFD 会话：

- IP 链路：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]**。
- 动态 LSP：执行命令 **bfd cfg-name bind ldp-lsp peer-ip ip-address nexthop ip-address [interface interface-type interface-number]**。
- 静态 LSP：执行命令 **bfd cfg-name bind static-lsp lsp-name**

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（可选）执行下列命令调整本地发送 BFD 报文的最小时间间隔、本地允许接收 BFD 报文的最小时间间隔和本地 BFD 检测倍数。

1. 执行命令 **quit**，退回系统视图。
2. 执行命令 **mpls**，使能本节点的 MPLS 能力，并进入 MPLS 视图。
3. 执行命令 **mpls bfd min-tx-interval interval**，调整本地发送 BFD 报文的最小时间间隔。

缺省值是 1000 毫秒。

当反向通道采用 IP 链路时，不能配置本地参数。

本地 BFD 报文实际发送时间间隔 = MAX { 本地配置的发送时间间隔，对端配置接收时间间隔 }；本地实际接收时间间隔 = MAX { 对端配置的发送时间间隔，本

地配置的接收时间间隔}; 本地检测时间=本地接收时间间隔×对端配置的 BFD 检测倍数。

例如:

- 本地配置的发送时间间隔为 200ms, 接收时间间隔为 300ms, 检测倍数为 4。
- 对端配置的发送时间间隔为 100ms, 接收时间间隔为 600ms, 检测倍数为 5。

则:

- 本地实际的发送时间间隔为 $\text{MAX}\{200\text{ms}, 600\text{ms}\} = 600\text{ms}$, 接收时间间隔为 $\text{MAX}\{100\text{ms}, 300\text{ms}\} = 300\text{ms}$, 检测时间间隔为 $300\text{ms} \times 5 = 1500\text{ms}$ 。
- 对端实际的发送时间间隔为 $\text{MAX}\{100\text{ms}, 300\text{ms}\} = 300\text{ms}$, 接收时间间隔为 $\text{MAX}\{200\text{ms}, 600\text{ms}\} = 600\text{ms}$, 检测时间间隔为 $600\text{ms} \times 4 = 2400\text{ms}$ 。

4. 执行命令 **mpls bfd min-rx-interval interval**, 调整本地允许接收 BFD 报文的最小时间间隔。

缺省值是 1000 毫秒。

当反向通道采用 IP 链路时, 不能配置本地参数。

5. 执行命令 **mpls bfd detect-multiplier multiplier**, 调整本地 BFD 检测倍数。

缺省值是 3。

6. 执行命令 **quit**, 退回系统视图。
7. 执行命令 **bfd cfg-name**, 进入 BFD 会话视图。

步骤 5 执行命令 **commit**, 提交配置。

---结束

2.7.5 检查配置结果

静态 BFD 检测 LDP LSP 配置成功后, 可以指定查看 BFD 配置信息、BFD 会话信息以及 BFD 统计信息。

前提条件

已经完成静态 BFD 检测 LDP LSP 功能的所有配置。

操作步骤

- 使用 **display bfd configuration { all | static }** 命令查看 BFD 配置信息。
- 使用 **display bfd session { all | static }** 命令查看 BFD 会话信息。
- 使用 **display bfd statistics session { all | static }** 命令查看 BFD 统计信息。

---结束

2.8 配置动态 BFD 检测 LDP LSP

配置动态 BFD 检测 LDP LSP, 不需要指定 BFD 参数, 能够提高链路故障检测速度、减少配置工作量。

2.8.1 建立配置任务

在配置动态 BFD 检测 LDP LSP 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，可以快速、准确地完成配置任务。

应用环境

使用动态 BFD 检测 LDP LSP，能够提高链路故障检测速度、减少配置工作量，以支持 LDP FRR 等其他特性，减低链路故障对承载业务的影响。

说明

动态 BFD 检测 LDP LSP 时，只支持主机路由触发建立的 LDP LSP。

BFD 检测 LSP 时，往返转发方式可以不一致（如报文从源端到目的端走 LSP，从目的端到源端走 IP 转发），但要求往返路径一致，如果不一致，则检测到故障时，不能确定具体是哪条路径的故障。因此部署 BFD 检测时，要确认往返路径是否一致，以便检测到的故障确实是检测路径故障。

前置任务

在配置动态 BFD 检测 LDP LSP 之前，需完成以下任务：

- 配置 MPLS 基本能力
- 配置 MPLS LDP
- （可选）创建要使能 BFD 检测的 FEC 列表

数据准备

在配置动态 BFD 检测 LDP LSP 之前，需要准备以下数据。

序号	数据
1	各节点的 LSR ID
2	BFD 的触发方式
3	（可选）FEC 列表
4	（可选）BFD 检测参数

2.8.2 使能全局 BFD 能力

只需要在源端和宿端上全局使能 BFD 能力。

背景信息

在源端和宿端上进行下列配置。

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**，使能全局的 BFD 能力。

---结束

2.8.3 使能 MPLS 动态创建 BFD 会话功能

在源端和宿端上使能 BFD 能力，就可以使能 MPLS 动态创建 BFD 会话功能。

操作步骤

- 在源端上进行如下配置。
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **mpls**，进入 MPLS 视图。
 3. 执行命令 **mpls bfd enable**，使能 LDP LSP 动态创建 BFD 会话的能力。

执行完该命令并不创建 BFD 会话。

- 在宿端上进行如下配置。
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **bfd**，进入 BFD 视图。
 3. 执行命令 **mpls-passive**，使能被动创建 BFD 会话功能。

执行完该命令不创建 BFD 会话，而是等接收到源端发送的携带 BFD TLV 的 LSP Ping 请求报文后才建立 BFD 会话。

---结束

2.8.4 配置动态 BFD 检测 LDP LSP 的触发策略

配置动态 BFD 检测 LDP LSP 的触发策略有两种：主机触发和 FEC 列表触发，可以根据需要进行配置。

背景信息

在被检测 LSP 的源端上进行下列配置。

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 **mpls**，进入 MPLS 视图。

步骤 3 执行命令 **mpls bfd-trigger [host [nexthop next-hop-address | outgoing-interface interface-type interface-number] * | fec-list list-name]**，配置动态 BFD 检测 LDP LSP 的触发策略。

执行完该命令才真正开始创建 BFD 会话。

动态 BFD 检测 LDP LSP 的触发策略有两种：

- **主机触发**：如果需要所有的主机地址均能触发 BFD 会话的建立，则采用主机触发方式。还可以通过指定 **nexthop** 和 **outgoing-interface** 来约束哪些 LSP 可以建立 BFD 会话。

- FEC 列表触发：如果只需要其中的一部分主机触发 BFD 会话的建立，可以采用 **fec-list** 触发方式，来指定相应的主机地址。

---结束

2.8.5（可选）调整 BFD 检测参数

调整 BFD 检测参数，可以改变 BFD 检测时间和检测倍数。

背景信息

请在源端进行以下配置。

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**，进入 BFD 视图。
- 步骤 3** 执行命令 **mpls ping interval interval**，调节发送 LSP Ping 报文的时间间隔。
- 步骤 4** 执行命令 **quit**，退出 BFD 视图。
- 步骤 5** 执行命令 **mpls**，进入 MPLS 视图。
- 步骤 6** 执行命令 **mpls bfd { min-tx-interval interval | min-rx-interval interval | detect-multiplier multiplier }***，设置 BFD 检测的时间参数。

BFD 报文的最小发送时间间隔和最小接收时间间隔的缺省值都是 1000 毫秒，检测倍数的缺省值是 3。

本地 BFD 报文实际发送时间间隔 = MAX { 本地配置的发送时间间隔，对端配置的接收时间间隔 }；本地实际接收时间间隔 = MAX { 对端配置的发送时间间隔，本地配置的接收时间间隔 }；本地检测时间 = 本地接收时间间隔 × 对端配置的 BFD 检测倍数。

例如：

- 本地配置的发送时间间隔为 200ms，接收时间间隔为 300ms，检测倍数为 4。
- 对端配置的发送时间间隔为 100ms，接收时间间隔为 600ms，检测倍数为 5。

则：

- 本地实际的发送时间间隔为 MAX { 200ms, 600ms } = 600ms，接收时间间隔为 MAX { 100ms, 300ms } = 300ms，检测时间间隔为 300ms × 5 = 1500ms。
- 对端实际的发送时间间隔为 MAX { 100ms, 300ms } = 300ms，接收时间间隔为 MAX { 200ms, 600ms } = 600ms，检测时间间隔为 600ms × 4 = 2400ms。

---结束

2.8.6 检查配置结果

动态 BFD 检测 LDP LSP 配置成功后，可以指定查看源端和宿端的 BFD 配置信息、BFD 会话信息。

前提条件

已经完成动态 BFD 检测 LDP LSP 功能的所有配置。

操作步骤

- 使用 **display bfd configuration all [verbose]** 命令查看 BFD 配置信息（源端）。
- 使用 **display bfd configuration passive-dynamic [peer-ip peer-ip remote-discriminator discriminator] [verbose]** 命令查看 BFD 配置信息（宿端）。
- 使用 **display bfd session all [verbose]** 命令查看 BFD 会话信息（源端）。
- 使用 **display mpls bfd session [statistics [protocol { ldp | cr-static | rsvp-te }] [outgoing-interface interface-type interface-number] [nexthop ip-address] [fec fec-address] | verbose | monitor]** 命令查看 BFD 会话信息（源端）。

---结束

任务示例

在源端执行命令 **display bfd session all** 查看动态创建的 BFD 会话状态，可以看到 BFD 会话状态为 Up，会话绑定的链路类型是 LDP_LSP。

```
<Huawei> display bfd session all verbose
-----
Session MIndex : 256      State : Up      Name : dyn_8192
-----
Local Discriminator      : 8192      Remote Discriminator   : 8192
Session Detect Mode     : Asynchronous Mode Without Echo Function
BFD Bind Type           : LDP_LSP
Bind Session Type       : Dynamic
Bind Peer Ip Address    : 3.3.3.3
NextHop Ip Address     : 192.168.1.2
Bind Interface          : GE1/0/0
LSP Token               : 0x3002001
FSM Board Id           : 3
Min Tx Interval (ms)   : 100      Min Rx Interval (ms)  : 100
Actual Tx Interval (ms): 100      Actual Rx Interval (ms): 100
Local Detect Multi      : 4
Echo Passive           : Disable
Destination Port       : 3784
Proc interface status   : Disable
WTR Interval (ms)     : -
Active Multi           : 3
Last Local Diagnostic   : No Diagnostic
Bind Application        : VRRP | LSPM | LSPM | L2VPN | OAM_MANAGER
Session TX TmrID       : -
Session Init TmrID     : -
Session Echo Tx TmrID  : -
PDT Index              : FSM-0 | RCV-0 | IF-0 | TOKEN-0
Session Description     : -
-----
Total UP/DOWN Session Number : 1/0
```

在宿端上执行 **display bfd session passive-dynamic verbose** 命令查看被动创建 BFD 会话状态。其中 BFD Bind Type 字段的值为“Peer IP Address”，说明该宿端发送的 BFD 报文是通过 IP 路由传输的；由于不能在宿端调整 BFD 检测参数，所以 min-tx-interval 和 min-rx-interval 的缺省值取最小值 10，实际采用的发送和接收时间间隔是两端协商的结果。

```
<Huawei> display bfd session passive-dynamic verbose
-----
Session MIndex : 256      (Multi Hop) State : Up      Name : dyn_8192
-----
Local Discriminator      : 8192      Remote Discriminator   : 8192
Session Detect Mode     : Asynchronous Mode Without Echo Function
BFD Bind Type           : Peer Ip Address
Bind Session Type       : Entire_Dynamic
Bind Peer Ip Address    : 192.168.1.1
```

```
Bind Interface      : --
FSM Board Id       : 3
Min Tx Interval (ms) : 10
Actual Tx Interval (ms) : 100
Local Detect Multi  : 3
Echo Passive       : Disable
Destination Port    : 3784
Proc Interface Status : Disable
WTR Interval (ms)  : -
Active Multi       : 3
Last Local Diagnostic : No Diagnostic
Bind Application
Session TX TmrID   : -
Session Init TmrID : -
Session Echo Tx TmrID : -
PDT Index          : FSM-0 | RCV-0 | IF-0 | TOKEN-0
Session Description : -
TOS-EXP            : 6
Min Rx Interval (ms) : 10
Actual Rx Interval (ms) : 100
Detect Interval (ms) : 300
Acl Number         : -
TTL                : 253
Process PST        : Disable
Session Detect TmrID : -
Session WTR TmrID  : -
```

Total UP/DOWN Session Number : 1/0

2.9 配置 Manual LDP FRR

配置 Manual LDP FRR，可以使 LDP 在链路发生故障时，将流量快速切换到备份 LSP 上，保证流量不中断。

2.9.1 建立配置任务

在配置 Manual LDP FRR 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，可以快速、准确地完成配置任务。

应用环境

LDP 快速重路由（LDP FRR）为 MPLS 网络提供快速重路由功能，实现本地的端口级备份，从而减少了流量丢失。

前置任务

在配置 LDP FRR 之前，需完成以下任务：

- 使能 MPLS
- 配置 MPLS LDP

数据准备

在配置 LDP FRR 之前，需准备以下数据。

序号	数据
1	建立备份 LSP 的接口类型和接口编号
2	备份 LSP 的下一跳 IP 地址
3	可以触发生成备份 LSP 的 IP 前缀列表的名称
4	备份 LSP 的优先级
5	（可选）BFD 单跳检测的配置名

2.9.2 使能 Manual LDP FRR 功能

配置 Manual LDP FRR 功能，需要在 Ingress 或 Transit 节点进行配置。

背景信息

请在 Ingress 或 Transit 节点进行以下配置。

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 **mpls ldp frr nexthop nexthop-address [ip-prefix ip-prefix-name] [priority priority]**，在接口上使能 LDP FRR。

在同一个接口下，最多可以有 10 项不同优先级的 LDP FRR 配置，但最终根据优先级只会生成一条备份 LSP。优先级的值越小，其优先级越高。优先级的缺省值为 50。

 说明

- LDP GR 期间禁止使能或去使能 LDP FRR 功能。
- 混合应用 LDP FRR 和 IP FRR 情况下，优先选择 IP FRR。
- 在系统视图下执行 **undo mpls ldp** 命令或在接口视图下执行 **undo mpls ldp** 命令去使能 LDP 功能时，接口视图下的 LDP FRR 配置不会被自动删除，但 LDP FRR 功能已经失效。
- 在 LDP FRR 的配置中，备份 LSP 必须是 Liberal 状态的 LSP，即备份 LSP 的 ingress 到 egress 的路由状态必须是 “Inactive Adv”。

----结束

2.9.3 检查配置结果

Manual LDP FRR 配置成功后，可以指定查看使能了 Manual LDP FRR 的 LSP 信息。

前提条件

已经完成 LDP FRR 功能的所有配置。

操作步骤

- 使用 **display mpls lsp** 命令查看使能了 LDP FRR 的 LSP 信息。

----结束

2.10 配置 LDP Auto FRR

配置 LDP Auto FRR 功能，可以在网络故障时实现业务的迅速切换，提高网络的可靠性。

2.10.1 建立配置任务

在配置 LDP Auto FRR 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，可以快速、准确地完成配置任务。

应用环境

在通常的 MPLS 网络中，存在备份链路的情况下，当出现链路故障时，IGP 路由会首先收敛到备份路径上。待 IGP 路由收敛成功后，LDP LSP 才可以切换到备份路径上，造成流量的中断。此时可以配置 LDP 快速重路由功能。

LDP FRR 原理是通过 LDP 信令的 Liberal 标签保持方式，先获取 Liberal 标签，为该标签申请转发表项资源，并将转发信息下发到转发平面作为主 LSP 的备用转发表项。在配置了 LDP 快速重路由功能的网络中，当接口故障（接口自己感知或者结合 BFD 检测）或者主 LSP 不通（结合 BFD 检测）时，LDP 快速重路由功能会将流量快速切换到备份 LDP LSP 上，实现对主 LSP 的保护，保证流量中断时间小于 50ms，实现 50ms 以内切换。

LDP 快速重路由功能的配置方法有两种：手工配置的 LDP FRR、LDP Auto FRR。

- 手工配置的 LDP FRR 需要通过手工指定出接口或下一跳，配置备份 LSP。配置过程比较复杂，但是可以人为指定备份 LSP，因此比较灵活，适用于结构比较简单的网络。
- LDP Auto FRR 不需要手工指定，会依据触发策略，自动生成备份 LSP，配置过程比较简单，并且避免了手工配置可能出现的环路问题，适用于结构比较复杂的大型网络。

前置任务

在配置 LDP Auto FRR 之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。
- 配置 IGP 协议发布各节点接口所连网段和 LSR ID 的主机路由。
- 配置 MPLS LDP 功能。
- 配置 IS-IS Auto FRR 功能。

数据准备

在配置 LDP Auto FRR 之前，需准备以下数据。

序号	数据
1	建立备份 LSP 的接口类型和接口编号
2	可以触发 LDP 建立备份 LSP 的策略

2.10.2 使能 LDP Auto FRR 功能

配置 LDP Auto FRR，需要在 Ingress 或 Transit 节点进行配置。

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 ldp**，进入 MPLS LDP 视图。

步骤 3 执行命令 **auto-frr lsp-trigger { all | host | ip-prefix ip-prefix-name | none }**，配置触发 LDP 建立备份 LSP 的策略。

缺省情况下，32 位地址的备份路由触发 LDP 建立备份 LSP。

 说明

LDP Auto FRR 依赖 IS-IS 的自动重路由功能。执行 **frr (IS-IS)** 命令使能 IS-IS 自动重路由功能后，LDP Auto FRR 功能自动使能。如果需要调整备份 LDP LSP 的建立策略，可以执行 **auto-frr lsp-trigger** 命令。

auto-frr lsp-trigger 命令受 **lsp-trigger** 命令的限制。如果同时配置了 **auto-frr lsp-trigger** 命令和 **lsp-trigger** 命令，那么建立的备份 LSP 会同时满足 LDP 建立 LSP 的触发策略以及 LDP 建立备份 LSP 的触发策略。

LDP GR 期间不允许修改备份 LSP 的触发策略。

---结束

2.10.3 检查配置结果

LDP Auto FRR 配置成功后，可以指定查看使能了 LDP Auto FRR 的 LSP 信息。

前提条件

已经完成 LDP Auto FRR 功能的所有配置。

操作步骤

- 使用 **display mpls lsp** 命令查看使能了 LDP Auto FRR 之后的 LSP 的建立信息。

---结束

任务示例

使能 LDP Auto FRR 功能，可以看到目的地址为 2.2.2.9/32 的 LSP 的备份 LSP 已经建立。检查配置结果如下：

```
<Huawei> display mpls lsp
```

```
-----  
LSP Information: LDP LSP  
-----  
FEC                In/Out Label  In/Out IF                Vrf Name  
2.2.2.9/32         NULL/3        -/GE1/0/0  
**LDP FRR**       /1025        /GE1/0/1  
2.2.2.9/32         1024/3       -/GE1/0/0  
**LDP FRR**       /1025        /GE1/0/1  
3.3.3.9/32         NULL/3        -/GE1/0/1  
**LDP FRR**       /1025        /GE1/0/0  
3.3.3.9/32         1025/3       -/GE1/0/1  
**LDP FRR**       /1025        /GE1/0/0  
4.4.4.9/32         NULL/1026    -/GE1/0/1  
**LDP FRR**       /1026        /GE1/0/0  
4.4.4.9/32         1026/1026   -/GE1/0/1  
**LDP FRR**       /1026        /GE1/0/0  
10.1.3.0/24       1027/3       -/GE1/0/1
```

```
10.1.4.0/24      1028/3      -/GE1/0/1
**LDP FRR**     /1027       /GE1/0/0
```

2.11 配置 LDP 和 IGP 同步

通过配置 LDP 和 IGP 同步，可以抑制 IGP 邻居关系建立来推迟路由回切，直至 LDP 完成收敛。

2.11.1 建立配置任务

在配置 LDP 和 IGP 同步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，可以快速、准确地完成配置任务。

应用环境

LDP 和 IGP 同步功能主要用来解决在 LSP 存在主备链路的组网中，主 LSP 发生故障，导致的流量丢失问题。具体情况如下：

- 当主链路发生故障时，IGP 流量和 LSP 流量均切换到备份链路上。但当主链路从故障中恢复时，由于 IGP 比 LDP 收敛速度快，IGP 会先于 LDP 切换回主链路，因此造成 LSP 流量丢失。
- 当主链路正常，但主链路节点间的 LDP 会话发生故障时，LSP 流量从主链路切换到备份链路，而 IGP 流量继续从主链路转发，导致 LSP 流量丢失。

前置任务

在配置 LDP 和 IGP 同步之前，需完成以下任务：

- 使能 MPLS 能力
- 配置全局和各接口的 MPLS LDP 能力

数据准备

在配置 LDP 和 IGP 同步之前，需准备以下数据。

序号	数据
1	配置 LDP 和 IGP 同步的接口类型和接口编号
2	配置定时器的接口类型和接口编号
3	定时器的设定值（可选）

2.11.2 使能 LDP 和 IGP 同步功能

使能 LDP 和 IGP 同步功能，需要在主备链路的分叉节点和主链路上的 LDP 邻居节点之间的链路两端接口上进行相关配置。

操作步骤

- 如果 IGP 使用的是 OSPF 协议，则在主备链路的分叉节点和主链路上的 LDP 邻居节点之间的链路两端接口上进行如下配置。
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **interface interface-type interface-number**，进入接口视图。
 3. 执行命令 **ospf ldp-sync**，使能被保护接口的 LDP 和 OSPF 同步功能。
- 如果 IGP 使用的是 IS-IS 协议，则在主备链路的分叉节点和主链路上的 LDP 邻居节点之间的链路两端接口上进行如下配置。
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **interface interface-type interface-number**，进入接口视图。
 3. 执行命令 **isis enable process-id**，使能 IS-IS 协议。
 4. 执行命令 **isis ldp-sync**，使能被保护接口的 LDP 和 IS-IS 同步功能。

----结束

2.11.3（可选）设置 hold-down 定时器的值

设置 hold-down 定时器的值，也就是设置接口不建立 OSPF 邻居而等待 LDP 会话建立的时间间隔。

背景信息

请在接口上进行以下配置。

操作步骤

- 如果 IGP 使用的是 OSPF 协议，则在主备链路的分叉节点和主链路上的 LDP 邻居节点之间的链路两端接口上进行如下配置。
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **interface interface-type interface-number**，进入接口视图。
 3. 执行命令 **ospf timer ldp-sync hold-down value**，设置接口不建立 OSPF 邻居而等待 LDP 会话建立的时间间隔。

缺省情况下，hold-down 定时器的值是 10 秒。

- 如果 IGP 使用的是 IS-IS 协议，则在主备链路的分叉节点和主链路上的 LDP 邻居节点之间的链路两端接口上进行如下配置。
 1. 执行命令 **system-view**，进入系统视图。
 2. 执行命令 **interface interface-type interface-number**，进入接口视图。
 3. 执行命令 **isis timer ldp-sync hold-down value**，设置接口不建立 IS-IS 邻居而等待 LDP 会话建立的时间间隔。

缺省情况下，hold-down 定时器的值是 10 秒。

----结束

2.11.4（可选）设置 hold-max-cost 定时器的值

设置 hold-max-cost 定时器的值，也就是设置在本地节点的 LSA 中通告最大 cost 值的时间间隔。

背景信息

请在接口上进行以下配置。

操作步骤

- 如果 IGP 使用的是 OSPF 协议，则在主备链路的分叉节点，以及主链路 LDP 邻居节点之间链路的两端接口上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface interface-type interface-number**，进入接口视图。
3. 执行命令 **ospf timer ldp-sync hold-max-cost { value | infinite }**，设置 OSPF 在本地节点的 LSA 中保持通告最大开销值的时间。

缺省情况下，hold-max-cost 定时器的值是 10 秒。

根据不同组网需要，可选择参数进行配置：

- 如果组网中 OSPF 仅承载 LDP 业务，要使 OSPF 的选路和 LDP LSP 始终保持一致，需配置 **infinite** 参数。
- 如果组网中 OSPF 承载了包括 LDP 在内的多种业务时，要使 LDP 会话的中断不影响 OSPF 的正常选路和其他业务，可配置 **value** 参数。

多次配置此命令时，最后一次的配置生效。

- 如果 IGP 使用的是 IS-IS 协议，则在主备链路的分叉节点和主链路上的 LDP 邻居节点之间的链路两端接口上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface interface-type interface-number**，进入接口视图。
3. 执行命令 **isis timer ldp-sync hold-max-cost { value | infinite }**，设置 IS-IS 在本地节点的 LSP（Link State PDU）中保持通告最大开销值的时间。

缺省情况下，hold-max-cost 定时器的值是 10 秒。

根据不同组网需要，可选择参数进行配置：

- 如果组网中 IS-IS 仅承载 LDP 业务，要使 IS-IS 的选路和 LDP LSP 始终保持一致，需配置 **infinite** 参数。
- 如果组网中 IS-IS 承载了包括 LDP 在内的多种业务时，要使 LDP 会话的中断不影响 IS-IS 的正常选路和其他业务，可配置 **value** 参数。

多次配置此命令时，最后一次的配置生效。

---结束

2.11.5（可选）设置 delay 定时器的值

设置 delay 定时器的值，也就是设置等待 LSP 建立的时间间隔。

背景信息

在主备链路的分叉节点和主链路上的 LDP 邻居节点之间的链路两端接口上进行如下配置。

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 **mpls ldp timer igp-sync-delay value**，设置 LDP 会话建立以后，等待 LSP 建立的时间间隔。

缺省情况下，delay 定时器的值是 10 秒。

---结束

2.11.6 检查配置结果

LDP 和 IGP 同步配置成功后，可以指定查看配置了 LDP 和 IGP 同步功能的接口的同步信息以及接口的路由管理信息。

前提条件

已经完成 LDP 和 IGP 同步功能的所有配置。

操作步骤

- 使用 **display ospf ldp-sync interface { all | interface-type interface-number }** 命令查看配置了 LDP 和 OSPF 同步功能的接口的同步信息。
- 使用 **display isis [process-id | vpn-instance vpn-instance-name] ldp-sync interface** 命令查看配置了 LDP 和 ISIS 同步功能的接口的同步信息。
- 使用 **display rm interface [interface-type interface-number | vpn-instance vpn-instance-name]** 命令查看接口的路由管理信息。

---结束

任务示例

在配置成功时，执行上面的命令，可得到如下的结果：

- 执行 **display ospf ldp-sync** 或者 **display isis ldp-sync** 命令后，可以看到配置了 LDP 和 IGP 同步功能的接口状态为“Sync-Achieved”。
- 执行 **display rm interface** 命令，可以看到 LDP-ISIS 或 LDP-OSPF 的使能情况为“enabled”。

2.12 配置 LDP 和静态路由同步

LDP 和静态路由同步通过抑制静态路由活跃来迫使正切场景下静态路由切换到备份链路，回切场景下推迟流量回切，使静态路由和 LDP 保持同步来保证流量不中断。

2.12.1 建立配置任务

在配置 LDP 和静态路由同步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，有助于快速、准确地完成配置任务。

应用环境

LDP 和静态路由同步主要用在存在主备 LSP 的 MPLS 组网中，LSR 之间依靠静态路由建立 LSP，当主链路的 LDP 会话故障（非链路故障导致）时，或者主链路故障后再恢复时，用来解决 LSP 正切和回切导致的流量丢失问题。如图 2-2 所示，LSRA 和 LSRD 之间通过静态路由连通，LDP 在两端基于静态路由建立 LSP，正常情况下优选路径 LSRA → LSRB → LSRD。

- 正切场景：主链路的 LDP 会话发生故障（非链路故障导致）时，静态路由的流量并不会切换到备份路径，从而导致主链路上的 MPLS 流量中断。

LDP Session 正常建立的情况下，MPLS 流量走主链路（LSRA → LSRB → LSRD）。如果 LSRA 和 LSRB 之间的 LDP 会话中断时，LSP 立即切换到备份链路（LSRA → LSRC → LSRD），但由于 LSRA 和 LSRB 之间的链路正常，静态路由的流量并不切换到备份路径，造成 LDP 和静态路由不同步而导致 MPLS 流量中断。

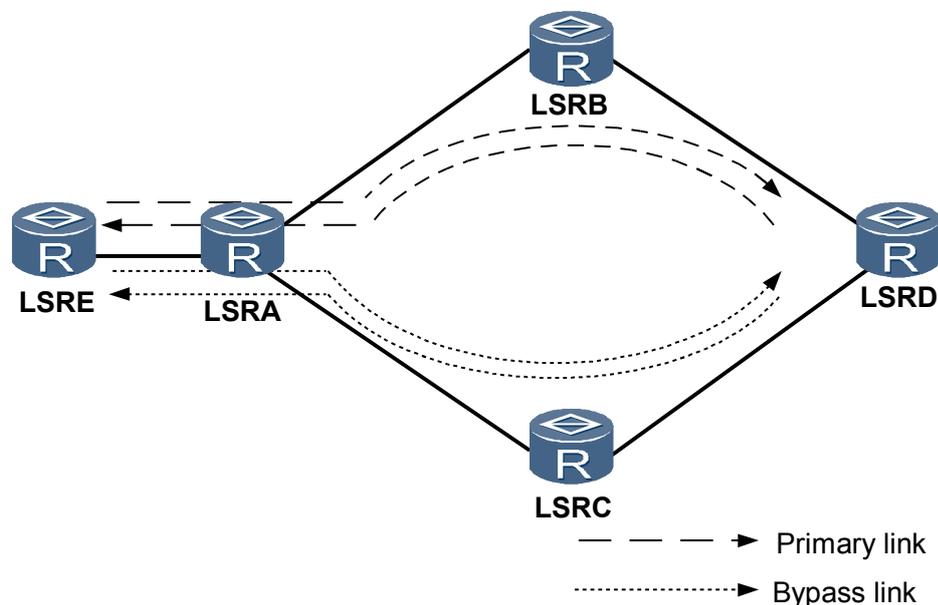
如果使能 LDP 和静态路由同步后，当 LDP 会话状态为 Down 时，流量自动切换到备份链路，保证流量不中断。

- 回切场景：主链路故障恢复，由于静态路由比 LDP 收敛速度快，静态路由的流量会先于 LDP 切换回主链路，则备份 LSP 路径无法使用，而主 LSP 尚未建立，导致 MPLS 流量中断。

LSRA 和 LSRB 之间的链路发生故障时，流量立即切换到备份链路（LSRA → LSRC → LSRD）。待 LSRA 和 LSRB 之间的链路恢复后，静态路由的流量会立即切换到主链路（LSRA → LSRB → LSRD），备份 LSP 无法使用，而主 LSP 尚未恢复，流量在此时间差内发生中断。

如果使能 LDP 和静态路由同步功能后，当主 LSP 建立时，流量再回切到主链路，保证流量不中断。

图 2-2 LDP 和静态路由同步组网图



前置任务

在配置 LDP 和静态路由同步之前，需完成以下任务：

- 使能 MPLS 能力
- 使能全局和接口下的 MPLS LDP 能力
- 各设备之间建立 LDP 会话

数据准备

在配置 LDP 和静态路由同步之前，需准备以下数据。

序号	数据
1	配置静态路由出接口的接口类型和接口编号
2	静态路由等待 LDP 会话建立的时间间隔（hold-down 定时器的设定值，可选）

2.12.2 使能 LDP 和静态路由同步功能

在存在主备 LSP 的 MPLS 组网中，LSR 之间依靠静态路由建立 LSP，通过在主备链路的两端使能 LDP 和静态路由同步功能，可以避免 MPLS 流量的中断。

背景信息

LDP 和静态路由同步是一种通过抑制静态路由活跃来迫使正切场景下流量切换到备份链路，回切场景下推迟流量切换到主用链路，使静态路由和 LDP 保持同步状态的技术。

说明

只有配置了出接口的静态路由才能配置 LDP 和静态路由同步。

在主备链路的两端分别进行如下配置。

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 `ip route-static ip-address { mask | mask-length } interface-type interface-number [nexthop-address] [preference preference | tag tag] * ldp-sync [description text]`，配置 LDP 和静态路由同步。

缺省情况下，不使能 LDP 和静态路由同步功能。

----结束

2.12.3 （可选）设置 hold-down 定时器的值

主链路故障恢复，静态路由不立即活跃，而是在 hold-down 定时器的设定值内等待 LDP 会话建立之后，静态路由才活跃，流量才回切到主链路。

背景信息

设置接口上 hold-down 定时器的值后，使能 LDP 和静态路由同步功能的静态路由暂时不活跃，而是在 hold-down 定时器的设定值内等待 LDP 会话建立，从而达到 LDP 和静态路由的同步。如果定时器超时，无论 LDP 会话是否建立，静态路由都开始活跃。



说明

系统不支持在 Loopback 和 NULL 接口下配置 hold-down 定时器。

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**，进入静态路由主链路的出接口视图。

步骤 3 执行命令 **static-route timer ldp-sync hold-down { timer | infinite }**，设置静态路由不活跃等待 LDP 会话建立的时间间隔。

缺省情况下，hold-down 定时器的值是 10 秒。

- 当 hold-down 定时器为 0 秒时，关闭该接口下的 LDP 和静态路由联动功能。
- 当 hold-down 定时器为 **infinite** 时，定时器将永不超时，只有等待 LDP 会话建立后静态路由才活跃，MPLS 流量才进行切换。

----结束

2.12.4 检查配置结果

LDP 和静态路由同步配置成功后，可以查看所有使能了 LDP 和静态路由同步功能的接口状态信息。

前提条件

已经完成 LDP 和静态路由同步的所有配置。

操作步骤

- 使用命令 **display static-route ldp-sync [interface interface-type interface-number]**查看使能了 LDP 和静态路由同步功能的接口状态信息。

配置参数 **interface interface-type interface-number** 时，将只显示指定接口的状态信息。

----结束

任务示例

配置 LDP 和静态路由同步成功后，执行 **display static-route ldp-sync** 命令，可得到如下的结果：

```
<Huawei> display static-route ldp-sync
Total number of routes enable LDP-sync: 1
-----
interface GigabitEthernet1/0/0
Enable ldp-sync static routes number: 1
Static-route ldp-sync holddown timer
Sync State: Normal
Dest = 1.1.1.1, Mask = 32, NextHop = 2.2.2.2
-----
```

2.13 配置 LDP GTSM

通过配置 LDP GTSM，可以检测 TTL 来防止攻击。

2.13.1 建立配置任务

在配置 LDP GTSM 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，可以快速、准确地完成配置任务。

应用环境

GTSM 机制通过 TTL 的检测来达到防止攻击的目的。攻击者模拟真实的 LDP 协议单播报文，对节点发送报文。当设备的接口板接收到这些报文后，发现是本机报文，则直接上送控制层面的 LDP 协议处理，而不加辨别其“合法性”。控制层面因为处理这些“合法”报文，导致系统异常繁忙，CPU 占用率高。

配置 GTSM 功能，通过检测 IP 报文头中的 TTL 值是否在一个预先定义好的特定范围内来对节点进行保护，增强系统的安全性。

前置任务

在配置 LDP GTSM 的基本功能之前，需完成以下任务：

- 使能 MPLS 和 MPLS LDP 能力。

数据准备

在配置 LDP GTSM 的基本功能之前，需要准备以下数据。

序号	数据
1	LDP 对等体的传输地址
2	GTSM 功能允许的最大有效跳数

2.13.2 配置 LDP GTSM

配置 LDP GTSM，需要在 LDP 对等体两节点上进行相关配置。

背景信息

请在需要配置 GTSM 功能的 LDP 对等体两端节点上进行以下配置。

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 `mpls ldp`，进入 MPLS LDP 视图。

步骤 3 执行命令 `gtsm peer ip-address valid-ttl-hops hops`，配置 LDP GTSM 功能。

如果将 `hops` 设置为 GTSM 功能允许的最大有效跳数，当 LDP 对等体发来报文的 TTL 值在 $255 - hops + 1 \sim 255$ 范围内，则接收该报文，否则丢弃该报文。

----结束

2.13.3 检查配置结果

LDP GTSM 配置成功后，可以指定查看 GTSM 的统计信息。

前提条件

已经完成 LDP GTSM 功能的所有配置。

操作步骤

- 使用 `display gtsm statistics { slot-id | all }` 命令查看 GTSM 的统计信息。

----结束

任务示例

执行 `display gtsm statistics` 可以看到各单板上的 GTSM 的统计信息，包括 LDP、BGP、BGP4+和 OSPF 的报文总数、通过的报文数量、丢弃的报文数量。

```
<Huawei> display gtsm statistics all
GTSM Statistics Table
```

SlotId	Protocol	Total Counters	Drop Counters	Pass Counters
0	BGP	0	0	0
0	OSPF	0	0	0
0	LDP	11	0	11

2.14 配置 LDP 安全特性

在对安全性要求较高的网络中，可以通过配置 LDP MD5 认证、LDP Keychain 认证、LDP GTSM 来提高网络的安全性。

2.14.1 建立配置任务

在配置 LDP 安全特性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，可以快速、准确地完成配置任务。

应用环境

为提供网络安全性，可以在 MPLS 网络中配置 LDP MD5 认证、LDP Keychain 认证或 LDP GTSM 功能。

- 配置 LDP MD5 认证

MD5 的典型应用是针对一段信息计算出对应的信息摘要，从而防止信息被篡改。MD5 信息摘要是通过不可逆的字符串变换算法产生的，结果唯一。因此，不管信息内容在传输过程中发生任何形式的改变，只要重新计算就会产生不同的信息摘要，接收端就可以由此判定收到的是一个不正确的报文。

配置 MD5 认证时，LDP 会话的两个对等体可以配置不同的认证方式：明文方式或者密文方式，但是密码必须相同。

- 配置 LDP Keychain 认证

Keychain 是一种增强型加密算法，类似于 MD5，Keychain 也是针对同一段信息计算出对应的信息摘要，实现 LDP 报文防篡改校验。

Keychain 允许用户定义一组密码，形成一个密码串，并且分别为每个密码指定加解密算法（包括 MD5，SHA-1 等）及密码使用的有效时间。在收发报文时，系统会按照用户的配置选出一个当前有效的密码，并按照与此密码相匹配的加密解密算法以及密码的有效时间，进行发送时加密和接收时解密报文。此外，系统可以依据密码使用的有效时间，自动完成有效密码的切换，避免了长时间不更改密码导致的密码易破解问题。

在配置 LDP Keychain 认证之前，首先需要配置全局的 Keychain 认证，才能配置成功。否则 LDP 会话将会断开。

- 配置 LDP GTSM 功能

GTSM 机制通过 TTL 的检测来达到防止攻击的目的。攻击者模拟真实的 LDP 协议单播报文，对节点发送报文。当设备的接口板接收到这些报文后，发现是本机报文，则直接上送控制层面的 LDP 协议处理，而不加辨别其“合法性”。控制层面因为处理这些“合法”报文，导致系统异常繁忙，CPU 占用率高。

配置 GTSM 功能，通过检测 IP 报文头中的 TTL 值是否在一个预先定义好的特定范围内来对节点进行保护，增强系统的安全性。

前置任务

在配置 LDP 安全特性之前，需完成以下任务：

- 使能 MPLS 和 MPLS LDP 能力。

数据准备

在配置 LDP 安全特性之前，需准备以下数据。

序号	数据
1	LDP 对等体的传输地址
2	(可选) MD5 认证密码 (可选) 全局 Keychain 认证的名称 (可选) GTSM 功能允许的最大有效跳数

2.14.2 配置 LDP MD5 认证

配置 LDP 认证，可以提高 LDP 会话连接的安全性。需要在会话两端的 LSR 上进行配置。

背景信息

为了提高 LDP 会话连接的安全性，可以对 LDP 使用的 TCP 连接配置 MD5 认证。LDP 会话的两个对等体可以配置不同的认证方式，但是密码必须相同。

LDP MD5 就是应用其对同一信息段产生唯一摘要信息的特点来实现 LDP 报文防篡改校验，比一般意义上 TCP 校验更为严格。

可以根据需求的不同选择配置 LDP MD5 认证或者 LDP Keychain 认证。

- MD5 算法配置简单，配置后生成单一密码，需要人为干预才可以切换密码，适用于需要短时间加密的网络。
- Keychain 具有一组密码，可以根据配置自动切换，但是配置过程较为复杂，适用于对安全性能要求比较高的网络。

 说明

对于同一邻居，在配置 Keychain 认证后，不能再配置 MD5 认证；同样，在配置 MD5 认证后，不能再配置 Keychain 认证。

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 ldp`，进入 MPLS-LDP 视图。

步骤 3 执行命令 `md5-password { plain | cipher } peer-lsr-id password`，使能 MD5 认证，并配置认证密码。

在用户配置认证密码时有明文和密文两种形式选择，这里的明文密文是对用户设置的认证密码在配置文件中的记录形式而言的。明文就是直接记录用户设置的字符串，密文就是记录经过特殊算法加密后的字符串。

缺省情况下，LDP 对等体之间不进行 MD5 认证。

 说明

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 `"^#^#"` 同时作为密文密码的起始和结束字符。



注意

配置 LDP MD5 认证会导致 LDP 会话重建，与原来会话相关的 LSP 将被删除。

----结束

2.14.3 配置 LDP Keychain 认证

配置 LDP Keychain 认证，可以提高 LDP 会话连接的安全性。需要在会话两端的 LSR 上进行配置。

背景信息

为了提高 LDP 会话连接的安全性，可以对 LDP 使用的 TCP 连接配置 Keychain 认证。

Keychain 允许用户定义一组密码，形成一个密码串，并且分别为每个密码指定加解密算法（包括 MD5，SHA-1 等）及密码使用的有效时间。在收发报文时，系统会按照用户的配置选出一个当前有效的密码，并按照与此密码相匹配的加密解密算法以及密码的有效时间，进行发送时加密和接收时解密报文。此外，系统可以依据密码使用的有效时间，自动完成有效密码的切换，避免了长时间不更改密码导致的密码易破解问题。

可以根据需求的不同选择配置 LDP MD5 认证或者 LDP Keychain 认证。

- MD5 算法配置简单，配置后生成单一密码，需要人为干预才可以切换密码，适用于需要短时间加密的网络。
- Keychain 具有一组密码，可以根据配置自动切换，但是配置过程较为复杂，适用于对安全性能要求比较高的网络。

 说明

对于同一邻居，在配置 Keychain 认证后，不能再配置 MD5 认证；同样，在配置 MD5 认证后，不能再配置 Keychain 认证。

配置 LDP Keychain 认证之前，首先要配置全局 Keychain。具体配置过程参见《AR1200 配置指南-安全》。

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 ldp`，进入 MPLS-LDP 视图。

步骤 3 执行命令 `authentication key-chain peer peer-id name keychain-name`，使能 LDP Keychain 认证，并引用配置的 Keychain 名称。

缺省情况下，LDP 对等体之间不进行 LDP Keychain 认证。



注意

配置 LDP Keychain 认证会导致 LDP 会话重建，与原来会话相关的 LSP 将被删除。

---结束

2.14.4 配置 LDP GTSM

配置 LDP GTSM，需要在 LDP 对等体两节点上进行相关配置。

背景信息

通用 TTL 安全保护机制 GTSM (Generalized TTL Security Mechanism) 通过判定报文的 TTL 值，确定报文是否有效，从而保护设备免受攻击。在 LDP 对等体上配置 GTSM 功能，通过配置的 TTL 有效范围，对 LDP 对等体间的 LDP 消息报文进行 TTL 检测。如果 LDP 消息报文的 TTL 不符合配置的范围要求，就认为此报文为非法攻击报文予以丢弃，以免 LDP 协议在收到大量伪装报文时，因处理报文导致 CPU 利用率过高等情况的攻击，进而实现对上层协议的保护。

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 ldp`，进入 MPLS LDP 视图。

步骤 3 执行命令 `gtsm peer ip-address valid-ttl-hops hops`，配置 LDP GTSM 功能。

如果将 hops 设置为 GTSM 功能允许的最大有效跳数，当 LDP 对等体发来报文的 TTL 值在[255 - hops+1, 255]范围内，则接收该报文，否则丢弃该报文。

---结束

2.14.5 检查配置结果

LDP 安全特性配置成功后，可以指定查看 LDP MD5 认证、LDP Keychain 认证、LDP GTSM 的配置情况。

前提条件

已经完成 LDP 安全特性的所有配置。

操作步骤

- 使用 **display mpls ldp session verbose** 命令查看 LDP MD5 认证、LDP Keychain 认证的配置情况。
- 使用 **display gtsm statistics all** 命令查看 GTSM 的统计信息。

---结束

任务示例

执行 **display mpls ldp session verbose** 命令可以看到是否配置了 LDP MD5 认证，以及 LDP Keychain 认证引用的全局 Keychain 认证的名称。

```
<Huawei> display mpls ldp session verbose

LDP Session(s) in Public Network
-----
Peer LDP ID      : 2.2.2.2:0          Local LDP ID      : 1.1.1.1:0
TCP Connection   : 1.1.1.1 <- 2.2.2.2
Session State    : Operational      Session Role      : Passive
Session FT Flag  : Off              MD5 Flag          : Off
Reconnect Timer  : ---              Recovery Timer    : ---
Keychain Name    : kcl

Negotiated Keepalive Hold Timer : 45 Sec
Configured Keepalive Send Timer : 3 Sec
Keepalive Message Sent/Rcvd     : 438/438 (Message Count)
Label Advertisement Mode        : Downstream Unsolicited
Label Resource Status(Peer/Local) : Available/Available
Session Age                      : 0000:01:49 (DDDD:HH:MM)
Session Deletion Status          : No

Capability:
Capability-Announcement          : On

Outbound&Inbound Policies Applied :
outbound peer all split-horizon

Addresses received from peer: (Count: 3)
10.1.1.2          2.2.2.2          10.1.2.1
-----
```

执行 **display gtsm statistics** 命令可以看到各单板上的 GTSM 的统计信息，包括 LDP、BGP、BGPv6 和 OSPF 的报文总数、通过的报文数量、丢弃的报文数量。

```
<Huawei> display gtsm statistics all
GTSM Statistics Table
-----
```

SlotId	Protocol	Total Counters	Drop Counters	Pass Counters
6	BGP	0	0	0
6	BGPv6	0	0	0
6	OSPF	0	0	0
6	LDP	11	0	11

2.15 配置 LDP GR

通过配置 LDP GR，可以实现主备倒换或协议重启的设备（Restarter）转发不中断，从而达到限制控制层协议震荡的目的。

2.15.1 建立配置任务

在配置 LDP GR 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，可以快速、准确地完成配置任务。

应用环境

在主备倒换或系统升级过程中，为了保证 MPLS 继续正常转发，并在主备倒换或系统升级完成后恢复 LDP 会话和 LSP 的建立，需要配置 LDP GR。

说明

在实际应用中，为了实现业务转发不受主板故障的影响，通常在双主板的硬件环境下配置系统级 GR 才有意义。

AR1200 只能作为 Helper 路由器，不能作为 Restarter 路由器。

前置任务

在配置 LDP GR 之前，需完成以下任务：

- 配置 IGP GR 功能。
- 配置 MPLS LDP 本地会话。

数据准备

在配置 LDP GR 之前，需准备以下数据。

序号	数据
1	MPLS 本节点的 LSR ID
2	LDP 会话重连接定时器的值（可选）
3	邻居存活定时器的值（可选）
4	LSP 恢复定时器的值（可选）

2.15.2 使能 LDP GR 能力

使能 LDP GR 能力，需要在 GR Restarter 及其邻居节点分别使能。

背景信息

请在 GR Restarter 及其邻居节点上进行以下配置。

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 `mpls lsr-id lsr-id`，配置本节点的 LSR ID。
- 步骤 3** 执行命令 `mpls`，使能本节点的 MPLS 能力，并进入 MPLS 视图。
- 步骤 4** 执行命令 `quit`，退回系统视图。
- 步骤 5** 执行命令 `mpls ldp`，使能本节点的 LDP 能力，并进入 LDP 视图。
- 步骤 6** 执行命令 `graceful-restart`，使能 LDP GR 能力。

缺省情况下，LDP GR 能力被禁止。

 说明

- 使能和去使能 LDP GR 能力都会导致 LDP 会话重建。
- LDP GR 期间禁止执行 `undo mpls ldp` 和 `reset mpls ldp` 命令。
- LDP GR 期间执行 `lsp-trigger`、`propagate mapping` 和 `lsp-trigger bgp-label-route` 命令修改 LSP 触发策略的操作无效。

----结束

2.15.3 （可选）配置 GR Helper 的定时器

配置 GR Helper 的定时器，也就是 LSP 恢复定时器的值。

背景信息

请在 GR Helper 上进行以下配置。

 说明

修改 LDP GR 相关定时器的值会导致 LDP 会话重建。

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 ldp`，进入 MPLS LDP 视图。
- 步骤 3** 执行命令 `graceful-restart timer recovery time`，配置 LSP 恢复定时器的值。
缺省情况下，LSP 恢复定时器的值为 300 秒。
- 步骤 4** 执行命令 `graceful-restart timer neighbor-liveness time`，配置邻居存活定时器的值。
缺省情况下，邻居存活定时器的值为 600 秒。

----结束

2.15.4 检查配置结果

LDP GR 配置成功后，可以指定查看 MPLS 相关的所有协议的 GR 信息、LDP 协议的相关信息以及 LDP 会话的相关信息。

前提条件

已经完成 LDP GR 功能的所有配置。

操作步骤

- 使用 **display mpls graceful-restart** 命令查看 MPLS 相关的所有协议的 GR 信息。
- 使用 **display mpls ldp [all] [verbose]**命令查看 LDP 协议的相关信息。
- 使用 **display mpls ldp session [all] [verbose]**命令查看 LDP 会话的相关信息。

----结束

任务示例

在配置成功时，执行上面的命令，应能得到如下的结果：

- 执行 **display mpls ldp** 命令，可以看到 Graceful Restart 的状态为“On”，即使能了 LDP GR。
- 执行 **display mpls ldp** 或 **display mpls ldp session verbose** 命令，可以查看 LSP 恢复定时器的值。

2.16 维护 MPLS LDP

维护 MPLS LDP，包括清除 MPLS 的统计信息、检测 LSP 连通性/可达性、配置 LDP LSP 的 Trap 功能。

2.16.1 重启 LDP

重启 LDP 将导致 LSP 的建立受到影响，请在操作前仔细确认。

背景信息



注意

重启 LDP 将导致 LSP 的建立受到影响，务必仔细确认是否必须执行复位 LDP 的操作。
LDP GR 期间禁止重启 LDP。

操作步骤

- 在需要重启全局 LDP 实例的情况下，可以在用户视图下，执行 **reset mpls ldp** 命令来复位全局 LDP 实例，使新的配置生效。

- 在需要重启所有 LDP 实例的情况下，可以在用户视图下，执行 **reset mpls ldp all** 命令来复位所有 LDP 实例，使新的配置生效。
- 在需要重启指定 LDP 对等体的情况下，可以在用户视图下，执行 **reset mpls ldp peer peer-id** 命令来复位指定 LDP 对等体，使新的配置生效。

----结束

2.16.2 检测 LSP 连通性/可达性

通过执行 **ping/tracert** 命令，检测 LSP 连通性/可达性。

背景信息

可以在任意视图下选择执行以下命令，进行 MPLS Ping/Traceroute 测试。

操作步骤

- 执行 **ping lsp [-a source-ip | -c count | -exp exp-value | -h ttl-value | -m interval | -r reply-mode | -s packet-size | -t time-out | -v] * ip destination-address mask-length [ip-address] [nexthop nexthop-address | draft6]**命令，进行 MPLS Ping 测试。

如果指定 **draft6** 参数，**ping lsp** 命令按 draft-ietf-mpls-lsp-ping-06 实现。默认情况下按 RFC4379 实现。

- 执行 **tracert lsp [-a source-ip | -exp exp-value | -h ttl-value | -r reply-mode | -t time-out] * ip destination-address mask-length [ip-address] [nexthop nexthop-address | draft6]**命令，进行 MPLS Traceroute 测试。

如果指定 **draft6** 参数，**tracert** 命令按 draft-ietf-mpls-lsp-ping-06 实现。默认情况下按 RFC4379 实现。

----结束

2.16.3 配置 LSP 的 Trap 功能

通过配置 LSP 的 Trap 功能，可以将 LSP 的状态变化通知给网管系统。

背景信息

如果需要将 LSP 的状态变化通知给网管系统，请在系统视图下进行下列配置。

缺省情况下，LDP LSP 创建过程中不使能 Trap 功能。

操作步骤

- 步骤 1** 在系统视图下，使用 **snmp-agent trap suppress feature-name lsp trap-name { mplsxcup | mplsxcdown } trap-interval trap-interval [max-trap-number max-trap-number]**命令，使能 LDP LSP 的 Trap 功能，并打开 mplsxcup 或 mplsxcdown 海量告警开关。

----结束

2.17 配置举例

介绍 MPLS LDP 配置举例。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、配置思路等。

2.17.1 配置 LDP 本地会话示例

介绍 LDP 本地会话的配置过程，包括在各设备以及各接口使能 MPLS 以及 MPLS LDP。

组网需求

如图 2-3 所示，LSRA、LSRB、LSRC 是 MPLS 网络的核心设备。数据流量从 PE 设备进入 MPLS 网络。要实现数据流在 MPLS 域内的转发，则需要 LSRA、LSRB、LSRC 之间配置 LDP 本地会话，从而进行标签交换，建立 LDP LSP。

按照图 2-4 所示，对 LSRA、LSRB、LSRC 进行地址规划。

图 2-3 配置 LDP 本地会话组网图（1）

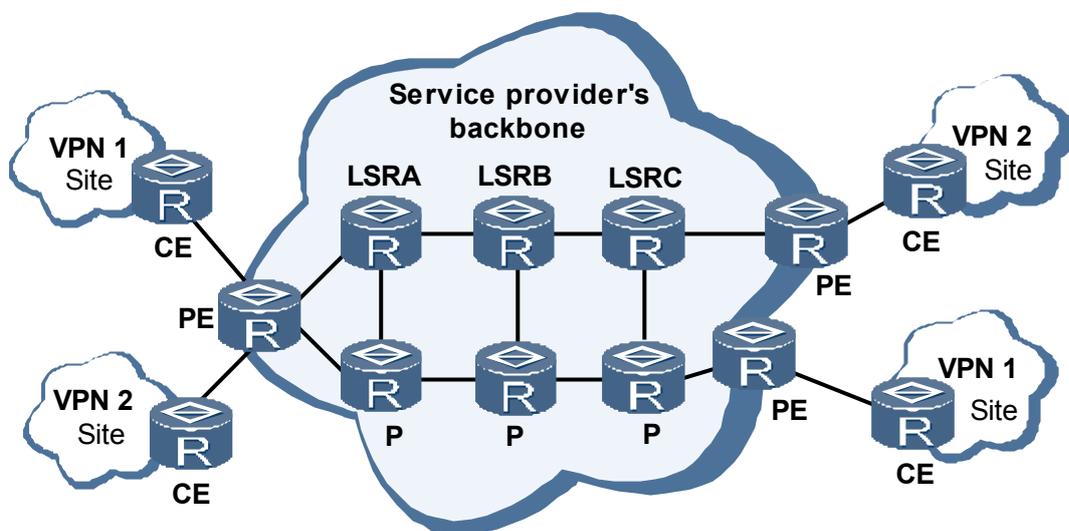
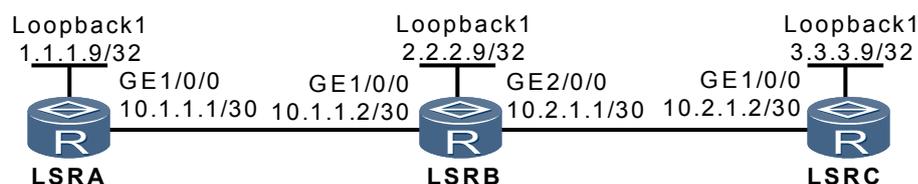


图 2-4 配置 LDP 本地会话组网图（2）



配置思路

采用如下的思路配置 LDP 本地会话：

1. 在各 LSR 上使能全局的 MPLS 和 MPLS LDP 能力。
2. 在各 LSR 的接口上使能 MPLS 能力。
3. 在 LDP 本地会话两端 LSR 的接口上使能 MPLS LDP 能力。

数据准备

为完成此配置例，需准备如下的数据：

- 各 LSR 接口的 IP 地址如 [图 2-4](#)，OSPF 进程号，所在的区域
- 各节点的 LSR ID

操作步骤

步骤 1 配置各接口的 IP 地址

按照 [图 2-4](#) 配置各接口 IP 地址和掩码，包括 Loopback 接口，并使用 OSPF 协议通告各接口所连网段和 LSR ID 主机路由，具体配置过程略。

步骤 2 在各 LSR 上使能全局的 MPLS 和 MPLS LDP 能力

配置 LSRA。

```
<LSRA> system-view
[LSRA] mpls lsr-id 1.1.1.9
[LSRA] mpls
[LSRA-mpls] quit
[LSRA] mpls ldp
[LSRA-mpls-ldp] quit
```

配置 LSRB。

```
<LSRB> system-view
[LSRB] mpls lsr-id 2.2.2.9
[LSRB] mpls
[LSRB-mpls] quit
[LSRB] mpls ldp
[LSRB-mpls-ldp] quit
```

配置 LSRC。

```
<LSRC> system-view
[LSRC] mpls lsr-id 3.3.3.9
[LSRC] mpls
[LSRC-mpls] quit
[LSRC] mpls ldp
[LSRC-mpls-ldp] quit
```

步骤 3 在各 LSR 的接口上使能 MPLS 能力

配置 LSRA。

```
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] mpls
[LSRA-GigabitEthernet1/0/0] quit
```

配置 LSRB。

```
[LSRB] interface gigabitethernet 1/0/0
[LSRB-GigabitEthernet1/0/0] mpls
[LSRB-GigabitEthernet1/0/0] quit
[LSRB] interface gigabitethernet 2/0/0
[LSRB-GigabitEthernet2/0/0] mpls
[LSRB-GigabitEthernet2/0/0] quit
```

配置 LSRC。

```
[LSRC] interface gigabitethernet 1/0/0
[LSRC-GigabitEthernet1/0/0] mpls
[LSRC-GigabitEthernet1/0/0] quit
```

步骤 4 在 LDP 本地会话两端 LSR 的接口上使能 MPLS LDP 能力

配置 LSRA。

```
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] mpls ldp
[LSRA-GigabitEthernet1/0/0] quit
```

配置 LSRB。

```
[LSRB] interface gigabitethernet 1/0/0
[LSRB-GigabitEthernet1/0/0] mpls ldp
[LSRB-GigabitEthernet1/0/0] quit
[LSRB] interface gigabitethernet 2/0/0
[LSRB-GigabitEthernet2/0/0] mpls ldp
[LSRB-GigabitEthernet2/0/0] quit
```

配置 LSRC。

```
[LSRC] interface gigabitethernet 1/0/0
[LSRC-GigabitEthernet1/0/0] mpls ldp
[LSRC-GigabitEthernet1/0/0] quit
```

步骤 5 检查配置结果

配置完成后，在节点上执行 **display mpls ldp session** 命令，可以看到 LSRA 和 LSRB、LSRB 和 LSRC 之间的 LDP 本地会话状态为“Operational”。

以 LSRA 的显示为例：

```
<LSRA> 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 0000:00:22 91/91
-----
TOTAL: 1 session(s) Found.
```

----结束

配置文件

- LSRA 的配置文件

```
#
sysname LSRA
#
mpls lsr-id 1.1.1.9
mpls
#
mpls ldp
#
interface GigabitEthernet1/0/0
ip address 10.1.1.1 255.255.255.252
mpls
mpls ldp
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 1.1.1.9 0.0.0.0
network 10.1.1.0 0.0.0.3
#
```

```
return
```

- LSRB 的配置文件

```
#
sysname LSRB
#
mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
#
interface GigabitEthernet1/0/0
ip address 10.1.1.2 255.255.255.252
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
ip address 10.2.1.1 255.255.255.252
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 10.1.1.0 0.0.0.3
network 10.2.1.0 0.0.0.3
#
return
```
- LSRC 的配置文件

```
#
sysname LSRC
#
mpls lsr-id 3.3.3.9
mpls
#
mpls ldp
#
interface GigabitEthernet1/0/0
ip address 10.2.1.2 255.255.255.252
mpls
mpls ldp
#
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 10.2.1.0 0.0.0.3
#
return
```

2.17.2 配置 LDP 远端会话示例

介绍 LDP 远端会话的配置过程，包括在各设备以及各接口使能 MPLS。

组网需求

如图 2-5 所示的网络中，LSRA、LSRC 是骨干网的边缘设备。在该网络中部署 VPN 业务，建立跨越 VPN 区域的 LDP LSP，则需要 LSRA 和 LSRC 之间建立远端 LDP 会话，从而为 VPN 业务提供服务。

按照图 2-6 所示，对 LSRA、LSRB、LSRC 进行地址规划。

图 2-5 配置 LDP 远端会话组网图 (1)

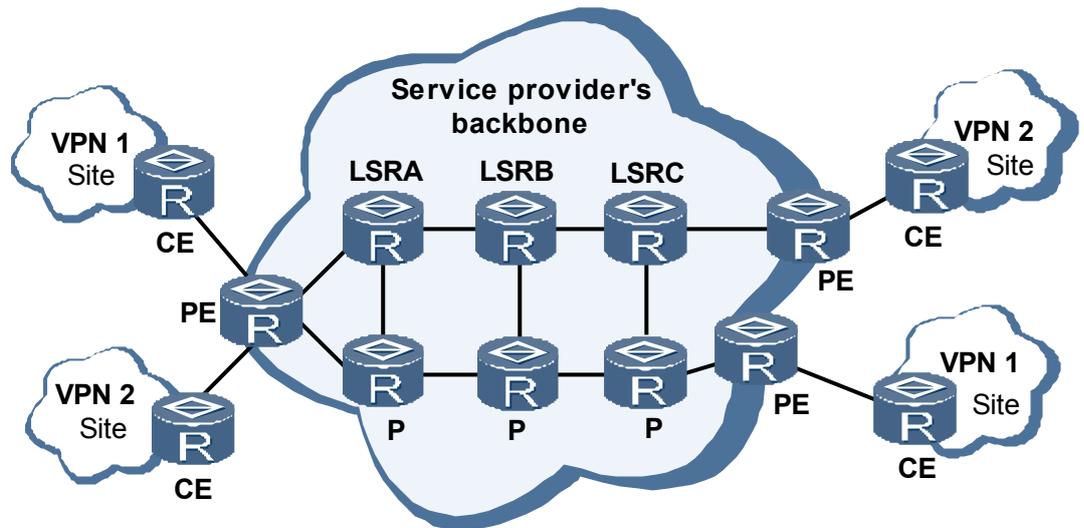
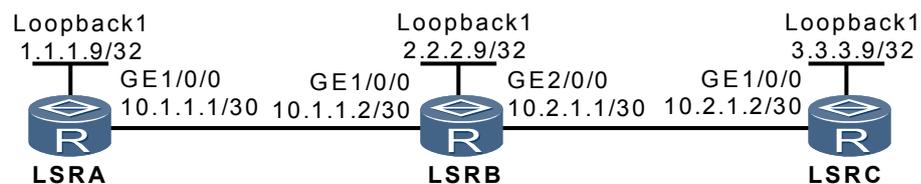


图 2-6 配置 LDP 远端会话组网图 (2)



配置思路

采用如下的思路配置 LDP 远端会话：

1. 在各 LSR 上使能全局的 MPLS 和 MPLS LDP 能力。
2. 在 LDP 远端会话两端 LSR 上指定远端对等体及 IP 地址。

数据准备

为完成此配置例，需准备如下的数据：

- 各节点接口的 IP 地址如图 2-6，OSPF 进程号，所在的区域
- 各节点的 LSR ID
- LDP 远端会话的远端对等体名称及 IP 地址

操作步骤

步骤 1 配置各接口的 IP 地址

按照图 2-6 配置各接口 IP 地址和掩码，包括 Loopback 接口，并使用 OSPF 协议通告各接口所连网段和 LSR ID 主机路由，具体配置过程略。

步骤 2 在各 LSR 上配置全局的 MPLS 和 MPLS LDP 能力

```
# 配置 LSRA。

<LSRA> system-view
[LSRA] mpls lsr-id 1.1.1.9
[LSRA] mpls
[LSRA-mpls] quit
[LSRA] mpls ldp
[LSRA-mpls-ldp] quit

# 配置 LSRB。

<LSRB> system-view
[LSRB] mpls lsr-id 2.2.2.9
[LSRB] mpls
[LSRB-mpls] quit
[LSRB] mpls ldp
[LSRB-mpls-ldp] quit

# 配置 LSRC。

<LSRC> system-view
[LSRC] mpls lsr-id 3.3.3.9
[LSRC] mpls
[LSRC-mpls] quit
[LSRC] mpls ldp
[LSRC-mpls-ldp] quit
```

步骤 3 在 LDP 远端会话两端 LSR 上指定远端对等体及 IP 地址

```
# 配置 LSRA。

[LSRA] mpls ldp remote-peer LSRC
[LSRA-mpls-ldp-remote-lsrc] remote-ip 3.3.3.9
[LSRA-mpls-ldp-remote-lsrc] quit

# 配置 LSRC。

[LSRC] mpls ldp remote-peer LSRA
[LSRC-mpls-ldp-remote-lsra] remote-ip 1.1.1.9
[LSRC-mpls-ldp-remote-lsra] quit
```

步骤 4 检查配置结果

配置完成后，在节点上执行 **display mpls ldp session** 命令，可以看到 LSRA 和 LSRC 之间的 LDP 远端会话状态为“Operational”。

以 LSRA 的显示为例：

```
[LSRA] 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
-----
3.3.3.9:0              Operational DU   Passive  0000:00:01  6/6
-----
TOTAL: 1 session(s) Found.
```

在 LDP 远端会话两端 LSR 上执行 **display mpls ldp remote-peer** 命令，可以看到 LSR 的远端对等体信息。

以 LSRA 的显示为例：

```
[LSRA] display mpls ldp remote-peer

LDP Remote Entity Information
```

```
-----  
Remote Peer Name : LSRC  
Remote Peer IP   : 3.3.3.9           LDP ID       : 1.1.1.9:0  
Transport Address : 1.1.1.9         Entity Status : Active  
  
Configured Keepalive Hold Timer : 45 Sec  
Configured Keepalive Send Timer : ---  
Configured Hello Hold Timer     : 45 Sec  
Negotiated Hello Hold Timer    : 45 Sec  
Configured Hello Send Timer     : ---  
Configured Delay Timer          : 0 Sec  
Hello Packet sent/received      : 10/7  
Remote Peer Deletion Status     : No  
Auto-config                     : ---  
-----  
TOTAL: 1 Peer(s) Found.
```

----结束

配置文件

- LSRA 的配置文件

```
#  
sysname LSRA  
#  
mpls lsr-id 1.1.1.9  
mpls  
#  
mpls ldp  
#  
mpls ldp remote-peer LSRC  
remote-ip 3.3.3.9  
#  
interface GigabitEthernet1/0/0  
ip address 10.1.1.1 255.255.255.252  
#  
interface LoopBack1  
ip address 1.1.1.9 255.255.255.255  
#  
ospf 1  
area 0.0.0.0  
network 1.1.1.9 0.0.0.0  
network 10.1.1.0 0.0.0.3  
#  
return
```

- LSRB 的配置文件

```
#  
sysname LSRB  
#  
mpls lsr-id 2.2.2.9  
mpls  
#  
mpls ldp  
#  
interface GigabitEthernet1/0/0  
ip address 10.1.1.2 255.255.255.252  
#  
interface GigabitEthernet2/0/0  
ip address 10.2.1.1 255.255.255.252  
#  
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 10.1.1.0 0.0.0.3
```

```

network 10.2.1.0 0.0.0.3
#
return

```

- LSRC 的配置文件

```

#
sysname LSRC
#
mpls lsr-id 3.3.3.9
mpls
#
mpls ldp
#
mpls ldp remote-peer LSRA
remote-ip 1.1.1.9
#
interface GigabitEthernet1/0/0
ip address 10.2.1.2 255.255.255.252
#
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 10.2.1.0 0.0.0.3
#
return

```

2.17.3 配置使用 LDP 建立 LSP 示例

介绍使用 LDP 建立 LSP 的配置过程，包括配置本地 LDP 会话以及在各 LSR 上修改 LDP LSP 的触发策略。

组网需求

如图 2-7 所示，LSRA、LSRB、LSRC 是 MPLS 网络的核心设备。在该网络中，LSR 之间成功建立 LDP 本地会话后，就建立 LDP LSP，进行标签交换，从而在该网络中部署 MPLS 业务。如图 2-8 所示，在 LSRA 到 LSRC 之间使用 LDP 建立 LSP。

图 2-7 配置 LDP LSP 组网图(1)

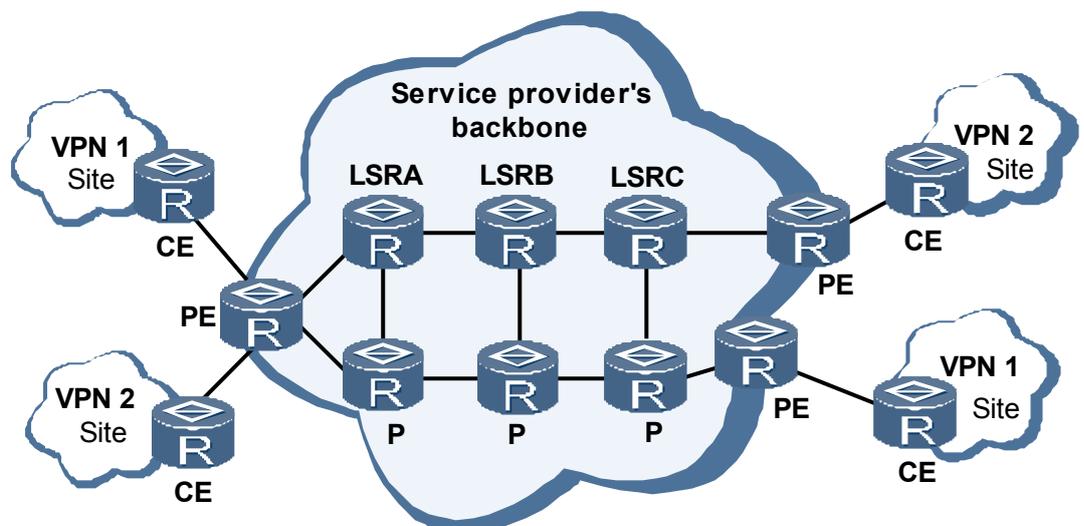
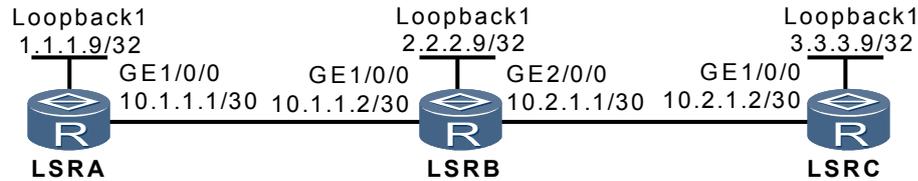


图 2-8 配置 LDP LSP 组网图(2)



配置思路

采用如下的思路实现使用 LDP 建立 LSP:

1. 配置本地 LDP 会话。
2. (可选) 在各 LSR 上修改 LDP LSP 的触发策略。

数据准备

为完成此配置例, 需准备如下的数据:

- 各 LSR 接口的 IP 地址如图 2-8, OSPF 进程号, 所在的区域
- (可选) 修改 LDP LSP 的触发策略

操作步骤

步骤 1 配置 LDP LSP

在完成[配置 LDP 本地会话示例](#)后, 各 LSR 已根据默认的 LDP LSP 触发策略, 即所有主机路由触发建立 LDP LSP。

在各 LSR 上执行 **display mpls ldp lsp** 命令, 可以看到所有主机路由都触发建立了 LDP LSP。

以 LSRA 的显示为例:

```
[LSRA] display mpls ldp lsp
LDP LSP Information
-----
```

DestAddress/Mask	In/OutLabel	UpstreamPeer	NextHop	OutInterface
1.1.1.9/32	3/NULL	2.2.2.9	127.0.0.1	InLoop0
*1.1.1.9/32	Liberal			
2.2.2.9/32	NULL/3	-	10.1.1.2	GE1/0/0
2.2.2.9/32	1024/3	2.2.2.9	10.1.1.2	GE1/0/0
3.3.3.9/32	NULL/1025	-	10.1.1.2	GE1/0/0
3.3.3.9/32	1025/1025	2.2.2.9	10.1.1.2	GE1/0/0

```
-----
TOTAL: 5 Normal LSP(s) Found.
TOTAL: 1 Liberal LSP(s) Found.
TOTAL: 0 Frr LSP(s) Found.
A '*' before an LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
A '*' before a UpstreamPeer means the session is in GR state
A '*' before a NextHop means the LSP is FRR LSP
```

 说明

通常情况下，使用缺省的触发策略，即“host”方式触发建立 LDP LSP 即可。也可以根据实际需要，执行以下步骤修改 LDP LSP 的触发策略。

步骤 2（可选）修改 LDP LSP 的触发策略

在各 LSR 上将 LDP LSP 的触发策略修改为 **all**，使路由表中的所有静态路由和 IGP 表项都可以触发建立 LDP LSP。

配置 LSRA。

```
[LSRA] mpls
[LSRA-mpls] lsp-trigger all
[LSRA-mpls] quit
```

配置 LSRB。

```
[LSRB] mpls
[LSRB-mpls] lsp-trigger all
[LSRB-mpls] quit
```

配置 LSRC。

```
[LSRC] mpls
[LSRC-mpls] lsp-trigger all
[LSRC-mpls] quit
```

步骤 3 检查配置结果

配置完成后，在各节点上执行 **display mpls ldp lsp** 命令，可以看到 LDP LSP 的建立情况。以 LSRA 的显示为例。

```
[LSRA] display mpls ldp lsp
LDP LSP Information
-----
DestAddress/Mask  In/OutLabel  UpstreamPeer  NextHop  OutInterface
-----
1.1.1.9/32        3/NULL       2.2.2.9       127.0.0.1  InLoop0
*1.1.1.9/32       Liberal
2.2.2.9/32        NULL/3        -              10.1.1.2   GE1/0/0
2.2.2.9/32        1024/3        2.2.2.9       10.1.1.2   GE1/0/0
3.3.3.9/32        NULL/1025     -              10.1.1.2   GE1/0/0
3.3.3.9/32        1025/1025    2.2.2.9       10.1.1.2   GE1/0/0
10.1.1.0/30       3/NULL       2.2.2.9       10.1.1.1   GE1/0/0
*10.1.1.0/30      Liberal
10.1.2.0/30       NULL/3        -              10.1.1.2   GE1/0/0
10.1.2.0/30       1026/3        2.2.2.9       10.1.1.2   GE1/0/0
-----
TOTAL: 8 Normal LSP(s) Found.
TOTAL: 2 Liberal LSP(s) Found.
TOTAL: 0 Frr LSP(s) Found.
A '*' before an LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
A '*' before a UpstreamPeer means the session is in GR state
A '*' before a NextHop means the LSP is FRR LSP
```

----结束

配置文件

- LSRA 的配置文件

```
#
sysname LSRA
#
mpls lsr-id 1.1.1.9
mpls
```

```
    lsp-trigger all
#
mpls ldp
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.252
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.3
#
return
```

● LSRB 的配置文件

```
#
sysname LSRB
#
mpls lsr-id 2.2.2.9
mpls
  lsp-trigger all
#
mpls ldp
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.252
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 ip address 10.2.1.1 255.255.255.252
 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 10.1.1.0 0.0.0.3
  network 10.2.1.0 0.0.0.3
#
return
```

● LSRC 的配置文件

```
#
sysname LSRC
#
mpls lsr-id 3.3.3.9
mpls
  lsp-trigger all
#
mpls ldp
#
interface GigabitEthernet1/0/0
 ip address 10.2.1.2 255.255.255.252
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
```

```
network 3.3.3.9 0.0.0.0
network 10.2.1.0 0.0.0.3
#
return
```

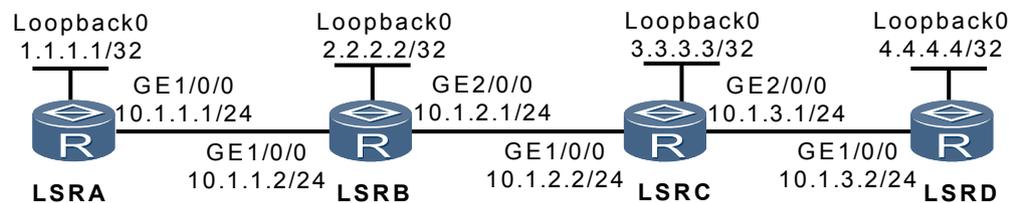
2.17.4 配置 LDP 自动触发 DoD 请求功能示例

介绍 LDP 自动触发 DoD 请求功能的配置过程，包括全局使能 MPLS 和 MPLS LDP 以及配置 DoD 的标签发布方式。

组网需求

如图 2-9 所示，LSRA、LSRD 是两台网络边缘设备。为了建立 PW，必须在 LSRA 和 LSRD 之间建立 LDP 远端会话，从而建立公网隧道。由于网络规模宏大，为了尽可能的节省网络资源，需要配置自动触发采用 DoD 的标签发布方式向下游请求远端对等体的 LSR ID 的标签映射消息，以减少不必要的 IP 和 MPLS 表项。

图 2-9 配置 LDP 跨域扩展组网图



配置思路

采用如下的思路实现 LDP 自动触发 DoD 请求功能：

1. 配置各节点接口的 IP 地址及作为 LSR ID 的 Loopback 地址。
2. 配置骨干网设备的 IS-IS 协议的基本功能，以及边缘设备和邻居的静态路由。
3. 使能各节点全局和接口的 MPLS 和 MPLS LDP 能力。
4. 配置 DoD 的标签发布方式。
5. 配置 LDP 跨域扩展。
6. 配置 LDP 远端会话，并使能 LDP 自动触发 DoD 请求功能。

数据准备

为完成此配置例，需准备如下的数据：

- 各节点接口的 IP 地址如图 2-9
- 各节点的 IS-IS 级别

操作步骤

步骤 1 配置各节点接口的 IP 地址及作为 LSR ID 的 Loopback 地址

按照图 2-9 配置各接口 IP 地址和掩码，包括 Loopback 接口，具体配置过程略。

步骤 2 配置骨干网设备的 IS-IS 协议的基本功能，以及边缘设备和邻居的静态路由

配置 LSRB 的 IS-IS 基本功能。

```
<LSRB> system-view
[LSRB] isis 1
[LSRB-isis-1] network-entity 10.0000.0000.0001.00
[LSRB-isis-1] quit
[LSRB] interface gigabitethernet 2/0/0
[LSRB-GigabitEthernet2/0/0] isis enable 1
[LSRB-GigabitEthernet2/0/0] quit
[LSRB] interface loopback 0
[LSRB-LoopBack0] isis enable 1
[LSRB-LoopBack0] quit
```

配置 LSRC 的 IS-IS 基本功能，并引入静态路由。

```
<LSRC> system-view
[LSRC] isis 1
[LSRC-isis-1] network-entity 10.0000.0000.0002.00
[LSRC-isis-1] import-route static
[LSRC-isis-1] quit
[LSRC] interface gigabitethernet 1/0/0
[LSRC-GigabitEthernet1/0/0] isis enable 1
[LSRC-GigabitEthernet1/0/0] quit
[LSRC] interface loopback 0
[LSRC-LoopBack0] isis enable 1
[LSRC-LoopBack0] quit
```

在 LSRA 上配置下一跳为 10.1.1.2 的缺省路由。

```
<LSRA> system-view
[LSRA] ip route-static 0.0.0.0 0.0.0.0 10.1.1.2
```

在 LSRB 上配置到 LSRA 的静态路由。

```
<LSRB> system-view
[LSRB] ip route-static 1.1.1.1 255.255.255.0 10.1.1.1
```

在 LSRC 上配置到 LSRD 的静态路由。

```
<LSRC> system-view
[LSRC] ip route-static 4.4.4.4 255.255.255.0 10.1.3.2
```

在 LSRD 上配置下一跳为 10.1.3.1 的缺省路由。

```
<LSRB> system-view
[LSRB] ip route-static 0.0.0.0 0.0.0.0 10.1.3.1
```

在 LSRA 上执行 **display ip routing-table** 命令查看路由信息。

```
[LSRA] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 7          Routes : 7

Destination/Mask    Proto Pre  Cost    Flags NextHop         Interface
-----
0.0.0.0/0          Static 60   0       RD  10.1.1.2           GigabitEthernet1/0/0
1.1.1.1/32         Direct 0     0       D   127.0.0.1          InLoopBack0
10.1.1.0/24         Direct 0     0       D   10.1.1.1           GigabitEthernet1/0/0
10.1.1.1/32         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
```

可以看到 LSRA 上已存在配置的缺省路由。

在 LSRB 上执行 **display ip routing-table** 命令查看路由信息。

```
[LSRB] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 12          Routes : 12

Destination/Mask    Proto    Pre  Cost           Flags NextHop         Interface
-----
 1.1.1.1/24        Static   60   0              RD  10.1.1.1           GigabitEthernet1/0/0
 2.2.2.2/32        Direct   0     0              D   127.0.0.1          InLoopBack0
 3.3.3.3/32        ISIS-L1  15   10             D   10.1.2.2           GigabitEthernet2/0/0
 4.4.4.4/32        ISIS-L1  15   74             D   10.1.2.2           GigabitEthernet2/0/0
10.1.1.0/24        Direct   0     0              D   10.1.1.2           GigabitEthernet1/0/0
10.1.1.2/32        Direct   0     0              D   127.0.0.1          InLoopBack0
10.1.2.0/24        Direct   0     0              D   10.1.2.1           GigabitEthernet2/0/0
10.1.2.1/32        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
```

可以看到 LSRB 上已存在配置的到 LSRA 的静态路由。

步骤 3 使能各节点全局和接口的 MPLS 和 MPLS LDP 能力

配置 LSRA。

```
<LSRA> system-view
[LSRA] mpls lsr-id 1.1.1.1
[LSRA] mpls
[LSRA-mpls] quit
[LSRA] mpls ldp
[LSRA-mpls-ldp] quit
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] mpls
[LSRA-GigabitEthernet1/0/0] mpls ldp
[LSRA-GigabitEthernet1/0/0] quit
```

LSRB、LSRC、LSRD 的配置同 LSRA，此处不做赘述。

步骤 4 配置 DoD 的标签发布方式

配置 LSRA。

```
<LSRA> system-view
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] mpls ldp advertisement dod
[LSRA-GigabitEthernet1/0/0] quit
```

配置 LSRB。

```
<LSRB> system-view
[LSRB] interface gigabitethernet 1/0/0
[LSRB-GigabitEthernet1/0/0] mpls ldp advertisement dod
[LSRB-GigabitEthernet1/0/0] quit
```

配置 LSRC。

```
<LSRC> system-view
[LSRC] interface gigabitethernet 2/0/0
[LSRC-GigabitEthernet2/0/0] mpls ldp advertisement dod
[LSRC-GigabitEthernet2/0/0] quit
```

配置 LSRD。

```
<LSRD> system-view
[LSRD] interface gigabitethernet 1/0/0
[LSRD-GigabitEthernet1/0/0] mpls ldp advertisement dod
[LSRD-GigabitEthernet1/0/0] quit
```

步骤 5 配置 LDP 跨域扩展

在 LSRA 上执行 **longest-match** 命令，使能 LDP 按照最长匹配方式查找路由建立 LSP。

```
<LSRA> system-view
[LSRA] mpls ldp
[LSRA-mpls-ldp] longest-match
[LSRA-mpls-ldp] quit
```

在 LSRD 上执行 **longest-match** 命令，使能 LDP 按照最长匹配方式查找路由建立 LSP。

```
<LSRD> system-view
[LSRD] mpls ldp
[LSRD-mpls-ldp] longest-match
[LSRD-mpls-ldp] quit
```

步骤 6 配置 LDP 远端会话，并使能 LDP 自动触发 DoD 请求功能

配置 LSRA。

```
<LSRA> system-view
[LSRA] mpls ldp remote-peer lsr
[LSRA-mpls-ldp-remote-lsr] remote-ip 4.4.4.4
[LSRA-mpls-ldp-remote-lsr] remote-ip auto-dod-request
[LSRA-mpls-ldp-remote-lsr] quit
```

配置 LSRD。

```
<LSRD> system-view
[LSRD] mpls ldp remote-peer lsra
[LSRD-mpls-ldp-remote-lsra] remote-ip 1.1.1.1
[LSRD-mpls-ldp-remote-lsra] remote-ip auto-dod-request
[LSRD-mpls-ldp-remote-lsra] quit
```

步骤 7 检查配置结果

上述配置完成后，在 LSRA 上执行 **display ip routing-table 4.4.4.4** 命令，查看路由。

```
<LSRA> display ip routing-table 4.4.4.4
Route Flags: R - relay, D - download to fib
-----
Routing Table : Public
Summary Count : 1
Destination/Mask    Proto Pre  Cost           Flags NextHop         Interface
-----
0.0.0.0/0           Static 60   0              RD   10.1.1.2           GigabitEthernet1/0/0
```

从显示信息可以看到，路由表中没有到 4.4.4.4 的精确路由，只有一条缺省路由。

在 LSRA 上执行 **display mpls ldp lsp** 命令，查看已经建立的 LSP。

```
<LSRA> display mpls ldp lsp

LDP LSP Information
-----
DestAddress/Mask    In/OutLabel    UpstreamPeer    NextHop         OutInterface
-----
4.4.4.4/32         NULL/1026      -               10.1.1.2        GigabitEthernet1/0/0
-----

TOTAL: 1 Normal LSP(s) Found.
TOTAL: 0 Liberal LSP(s) Found.
TOTAL: 0 Frr LSP(s) Found.
A '*' before an LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
A '*' before a UpstreamPeer means the session is in GR state
A '*' before a NextHop means the LSP is FRR LSP
```

从显示信息可以看到，已经建立了到 4.4.4.4 的 LSP。可见 LSRA 已经自动向 LSRB 请求了到 4.4.4.4 的标签映射消息，从而建立了 LSP。

在 LSRA 上执行 **display tunnel-info all** 命令，查看已经建立的隧道。

```
<LSRA> display tunnel-info all
* -> Allocated VC Token
Tunnel ID          Type          Destination      Token
-----
0x1000             lsp           4.4.4.4          0
```

从显示信息可以看到，LSRA 到 LSRD 的隧道已经建立。

---结束

配置文件

- LSRA 的配置文件

```
#
 sysname LSRA
#
 mpls lsr-id 1.1.1.1
 mpls
#
 mpls ldp
 longest-match
#
 mpls ldp remote-peer lsrD
 remote-ip 4.4.4.4
 undo remote-ip pwe3
 remote-ip auto-dod-request
#
 interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
 mpls ldp advertisement dod
#
 interface LoopBack0
 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
#
 return
```

- LSRB 的配置文件

```
#
 sysname LSRB
#
 mpls lsr-id 2.2.2.2
 mpls
#
 mpls ldp
#
 isis 1
 network-entity 10.0000.0000.0001.00
#
 interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
 mpls ldp advertisement dod
#
 interface GigabitEthernet2/0/0
 ip address 10.1.2.1 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
 interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
```

```
#
ip route-static 1.1.1.1 255.255.255.0 10.1.1.1
#
return
```

- LSRC 的配置文件

```
#
sysname LSRC
#
mpls lsr-id 3.3.3.3
mpls
#
mpls ldp
#
isis 1
network-entity 10.0000.0000.0002.00
import-route static
#
interface GigabitEthernet1/0/0
ip address 10.1.2.2 255.255.255.0
isis enable 1
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
ip address 10.1.3.1 255.255.255.0
mpls
mpls ldp
mpls ldp advertisement dod
#
interface LoopBack0
ip address 3.3.3.3 255.255.255.255
isis enable 1
#
ip route-static 4.4.4.0 255.255.255.0 10.1.3.2
#
return
```

- LSRD 的配置文件

```
#
sysname LSRD
#
mpls lsr-id 4.4.4.4
mpls
#
mpls ldp
longest-match
#
mpls ldp remote-peer lsra
remote-ip 1.1.1.1
undo remote-ip pwe3
remote-ip auto-dod-request
#
interface GigabitEthernet1/0/0
ip address 10.1.3.2 255.255.255.0
mpls
mpls ldp
mpls ldp advertisement dod
#
interface LoopBack0
ip address 4.4.4.4 255.255.255.255
#
ip route-static 0.0.0.0 0.0.0.0 10.1.3.1
#
return
```

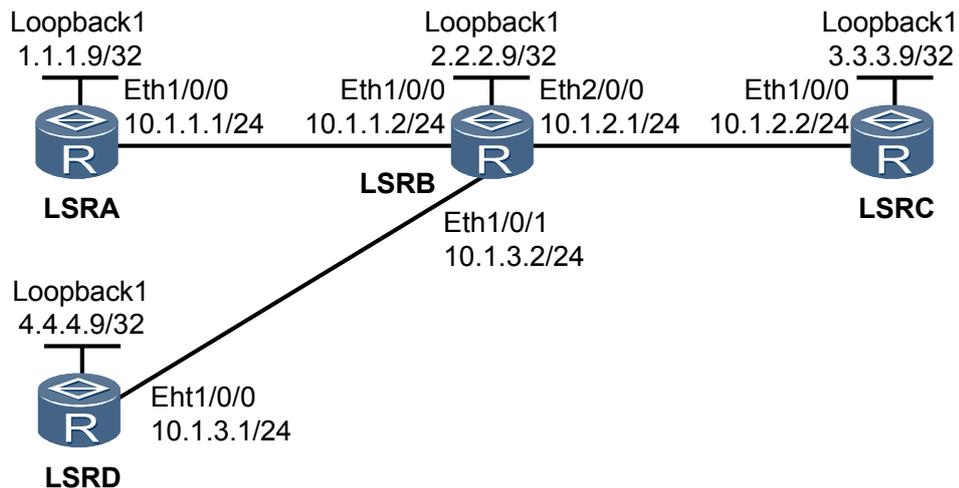
2.17.5 配置 LDP Inbound 策略示例

介绍 LDP Inbound 策略的配置过程，包括配置全局使能 MPLS 和 MPLS LDP。

组网需求

如图 2-10 所示网络中，部署了 MPLS LDP 业务。LSRD 是接入设备 DSLAM，性能较低。如果不对 LSRD 收到的标签进行控制，则会建立大量的 LSP，消耗大量内存，LSRD 无法承受。配置 LDP Inbound 策略，LSRD 只接收到达 LSRC 的标签映射消息，使 LSRD 只建立到 LSRC 的 LSP，从而减少资源的浪费。

图 2-10 配置 LDP Inbound 策略组网图



配置思路

采用如下的思路配置 LDP Inbound 策略：

1. 配置各节点接口的 IP 地址和 Loopback 地址。
2. 配置 OSPF 协议发布各节点接口所连网段和 LSR ID 的主机路由。
3. 使能各节点全局和接口的 MPLS 和 MPLS LDP。
4. 配置 LDP Inbound 策略。

数据准备

为完成此配置例，需准备如下的数据：

- 各 LSR 接口的 IP 地址如图 2-10，OSPF 进程号，所在的区域
- 各节点的 LSR ID

操作步骤

步骤 1 配置各接口的 IP 地址和 IGP 路由协议

按照图 2-10 配置各接口 IP 地址和掩码，包括 Loopback 接口，并使用 OSPF 协议通告各接口所连网段和 LSR ID 主机路由，具体配置过程略。

步骤 2 使能各节点全局和接口的 MPLS 和 MPLS LDP 能力

配置 LSRA。

```
<LSRA> system-view
[LSRA] mpls lsr-id 1.1.1.9
[LSRA] mpls
[LSRA-mpls] quit
[LSRA] mpls ldp
[LSRA-mpls-ldp] quit
[LSRA] interface ethernet 1/0/0
[LSRA-Ethernet1/0/0] mpls
[LSRA-Ethernet1/0/0] mpls ldp
[LSRA-Ethernet1/0/0] quit
```

配置 LSRB。

```
<LSRB> system-view
[LSRB] mpls lsr-id 2.2.2.9
[LSRB] mpls
[LSRB-mpls] quit
[LSRB] mpls ldp
[LSRB-mpls-ldp] quit
[LSRB] interface ethernet 1/0/0
[LSRB-Ethernet1/0/0] mpls
[LSRB-Ethernet1/0/0] mpls ldp
[LSRB-Ethernet1/0/0] quit
[LSRB] interface ethernet 1/0/1
[LSRB-Ethernet1/0/1] mpls
[LSRB-Ethernet1/0/1] mpls ldp
[LSRB-Ethernet1/0/1] quit
[LSRB] interface ethernet 2/0/0
[LSRB-Ethernet2/0/0] mpls
[LSRB-Ethernet2/0/0] mpls ldp
[LSRB-Ethernet2/0/0] quit
```

配置 LSRC。

```
<LSRC> system-view
[LSRC] mpls lsr-id 3.3.3.9
[LSRC] mpls
[LSRC-mpls] quit
[LSRC] mpls ldp
[LSRC-mpls-ldp] quit
[LSRC] interface ethernet 1/0/0
[LSRC-Ethernet1/0/0] mpls
[LSRC-Ethernet1/0/0] mpls ldp
[LSRC-Ethernet1/0/0] quit
```

配置 LSRD。

```
<LSRD> system-view
[LSRD] mpls lsr-id 4.4.4.9
[LSRD] mpls
[LSRD-mpls] quit
[LSRD] mpls ldp
[LSRD-mpls-ldp] quit
[LSRD] interface ethernet 1/0/0
[LSRD-Ethernet1/0/0] mpls
[LSRD-Ethernet1/0/0] mpls ldp
[LSRD-Ethernet1/0/0] quit
```

配置完成后，在 LSRD 上执行 **display mpls lsp** 命令，查看已经建立的 LSP。

```
<LSRD> display mpls lsp
```

```
-----
LSP Information: LDP LSP
-----
```

FEC	In/Out Label	In/Out IF	Vrf Name
1.1.1.9/32	NULL/1024	-/Eth1/0/0	
1.1.1.9/32	1024/1024	-/Eth1/0/0	
2.2.2.9/32	NULL/3	-/Eth1/0/0	
2.2.2.9/32	1025/3	-/Eth1/0/0	

```
3.3.3.9/32      NULL/1025      -/Eth1/0/0
3.3.3.9/32      1026/1025     -/Eth1/0/0
```

从显示信息可以看到，LSRD 上建立了到 LSRA、LSRB、LSRC 的 LSP。

步骤 3 配置 LDP Inbound 策略

在 LSRD 上配置 IP 地址前缀列表，只允许到 LSRC 的路由通过。

```
<LSRD> system-view
[LSRD] ip ip-prefix prefix1 permit 3.3.3.9 32
```

在 LSRD 上配置 Inbound 策略，只接收由 LSRD 发送的到 LSRC 的标签映射消息。

```
<LSRD> system-view
[LSRD] mpls ldp
[LSRD-mpls-ldp] inbound peer 2.2.2.9 fec ip-prefix prefix1
[LSRB-mpls-ldp] quit
```

步骤 4 检查配置结果

配置完成后，在 LSRD 上执行 **display mpls lsp** 命令，可以看到只建立了到 LSRC 的 LSP。

```
<LSRD> display mpls lsp
```

```
-----
                        LSP Information: LDP LSP
-----
FEC                In/Out Label  In/Out IF                Vrf Name
3.3.3.9/32         NULL/1025     -/Eth1/0/0
3.3.3.9/32         1026/1025    -/Eth1/0/0
```

----结束

配置文件

● LSRA 的配置文件

```
#
 sysname LSRA
#
 mpls lsr-id 1.1.1.9
 mpls
#
 mpls ldp
#
 interface Ethernet1/0/0
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
 interface NULL0
#
 interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
 ospf 1
 area 0.0.0.0
 network 1.1.1.9 0.0.0.0
 network 10.1.1.0 0.0.0.255
#
 return
```

● LSRB 的配置文件

```
#
```

```
    sysname LSRB
#
    mpls lsr-id 2.2.2.9
    mpls
#
    mpls ldp
#
    interface Ethernet1/0/0
        ip address 10.1.1.2 255.255.255.0
        mpls
        mpls ldp
#
    interface Ethernet1/0/1
        ip address 10.1.3.2 255.255.255.0
        mpls
        mpls ldp
#
    interface Ethernet2/0/0
        ip address 10.1.2.1 255.255.255.0
        mpls
        mpls ldp
#
    interface NULL0
#
    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 10.1.1.0 0.0.0.255
            network 10.1.2.0 0.0.0.255
            network 10.1.3.0 0.0.0.255
#
    return
```

● LSRC 的配置文件

```
#
    sysname LSRC
#
    mpls lsr-id 3.3.3.9
    mpls
#
    mpls ldp
#
    interface Ethernet1/0/0
        ip address 10.1.2.2 255.255.255.0
        mpls
        mpls ldp
#
    interface NULL0
#
    interface LoopBack1
        ip address 3.3.3.9 255.255.255.255
#
    ospf 1
        area 0.0.0.0
            network 3.3.3.9 0.0.0.0
            network 10.1.2.0 0.0.0.255
#
    return
```

● LSRD 的配置文件

```
#
    sysname LSRD
#
    mpls lsr-id 4.4.4.9
    mpls
```

```
#
mpls ldp
inbound peer 2.2.2.9 fec ip-prefix prefix1
#
interface Ethernet1/0/0
ip address 10.1.3.1 255.255.255.0
mpls
mpls ldp
#
interface NULL0
#
interface LoopBack1
ip address 4.4.4.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 4.4.4.9 0.0.0.0
network 10.1.3.0 0.0.0.255
#
ip ip-prefix prefix1 index 10 permit 3.3.3.9 32
#
return
```

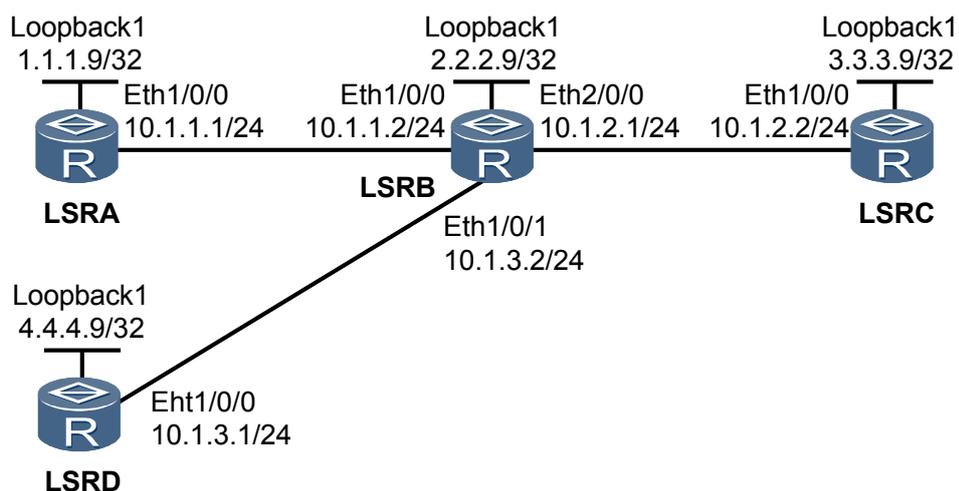
2.17.6 配置 LDP Outbound 策略示例

介绍 LDP Outbound 策略的配置过程，包括配置全局使能 MPLS 和 MPLS LDP。

组网需求

如图 2-11 所示网络中，部署了 MPLS LDP 业务。LSRD 是接入设备 DSLAM，性能较低。如果不对 LSRD 收到的标签进行控制，则会建立大量的 LSP，消耗大量内存，LSRD 无法承受。配置 LDP Outbound 策略，只给 LSRD 发送到 LSRC 的标签映射消息，使 LSRD 只建立到 LSRC 的 LSP，从而减少资源的浪费。

图 2-11 配置 LDP Outbound 策略组网图



配置思路

采用如下的思路配置 LDP Outbound 策略：

1. 配置各节点接口的 IP 地址和 Loopback 地址。
2. 配置 OSPF 协议发布各节点接口所连网段和 LSR ID 的主机路由。
3. 使能各节点全局和接口的 MPLS 和 MPLS LDP。
4. 配置 LDP Outbound 策略。

数据准备

为完成此配置例，需准备如下的数据：

- 各 LSR 接口的 IP 地址如图 2-11，OSPF 进程号，所在的区域
- 各节点的 LSR ID

操作步骤

步骤 1 配置各接口的 IP 地址和 IGP 路由协议

按照图 2-11 配置各接口 IP 地址和掩码，包括 Loopback 接口，并使用 OSPF 协议通告各接口所连网段和 LSR ID 主机路由，具体配置过程略。

步骤 2 使能各节点全局和接口的 MPLS 和 MPLS LDP 能力

配置 LSRA。

```
<LSRA> system-view
[LSRA] mpls lsr-id 1.1.1.9
[LSRA] mpls
[LSRA-mppls] quit
[LSRA] mpls ldp
[LSRA-mppls-ldp] quit
[LSRA] interface ethernet 1/0/0
[LSRA-Ethernet1/0/0] mpls
[LSRA-Ethernet1/0/0] mpls ldp
[LSRA-Ethernet1/0/0] quit
```

配置 LSRB。

```
<LSRB> system-view
[LSRB] mpls lsr-id 2.2.2.9
[LSRB] mpls
[LSRB-mppls] quit
[LSRB] mpls ldp
[LSRB-mppls-ldp] quit
[LSRB] interface ethernet 1/0/0
[LSRB-Ethernet1/0/0] mpls
[LSRB-Ethernet1/0/0] mpls ldp
[LSRB-Ethernet1/0/0] quit
[LSRB] interface ethernet 1/0/1
[LSRB-Ethernet1/0/1] mpls
[LSRB-Ethernet1/0/1] mpls ldp
[LSRB-Ethernet1/0/1] quit
[LSRB] interface ethernet 2/0/0
[LSRB-Ethernet2/0/0] mpls
[LSRB-Ethernet2/0/0] mpls ldp
[LSRB-Ethernet2/0/0] quit
```

配置 LSRC。

```
<LSRC> system-view
[LSRC] mpls lsr-id 3.3.3.9
[LSRC] mpls
[LSRC-mppls] quit
[LSRC] mpls ldp
[LSRC-mppls-ldp] quit
```

```
[LSRC] interface ethernet 1/0/0
[LSRC-Ethernet1/0/0] mpls
[LSRC-Ethernet1/0/0] mpls ldp
[LSRC-Ethernet1/0/0] quit
```

配置 LSRD。

```
<LSRD> system-view
[LSRD] mpls lsr-id 4.4.4.9
[LSRD] mpls
[LSRD-mpls] quit
[LSRD] mpls ldp
[LSRD-mpls-ldp] quit
[LSRD] interface ethernet 1/0/0
[LSRD-Ethernet1/0/0] mpls
[LSRD-Ethernet1/0/0] mpls ldp
[LSRD-Ethernet1/0/0] quit
```

配置完成后，在 LSRD 上执行 **display mpls lsp** 命令，查看已经建立的 LSP。

```
<LSRD> display mpls lsp
```

```
-----
LSP Information: LDP LSP
-----
FEC                In/Out Label  In/Out IF                Vrf Name
1.1.1.9/32         NULL/1024    -/Eth1/0/0
1.1.1.9/32         1024/1024   -/Eth1/0/0
2.2.2.9/32         NULL/3       -/Eth1/0/0
2.2.2.9/32         1025/3      -/Eth1/0/0
3.3.3.9/32         NULL/1025   -/Eth1/0/0
3.3.3.9/32         1026/1025   -/Eth1/0/0
```

从显示信息可以看到，LSRD 上建立了到 LSRA、LSRB、LSRC 的 LSP。

步骤 3 配置 LDP Outbound 策略

在 LSRB 上配置 IP 地址前缀列表，只允许到 LSRC 的路由通过。

```
<LSRB> system-view
[LSRB] ip ip-prefix prefix1 permit 3.3.3.9 32
```

在 LSRB 上配置 Outbound 策略，只给 LSRD 发送到 LSRC 的标签映射消息。

```
<LSRB> system-view
[LSRB] mpls ldp
[LSRB-mpls-ldp] outbound peer 4.4.4.9 fec ip-prefix prefix1
[LSRB-mpls-ldp] quit
```

步骤 4 检查配置结果

配置完成后，在 LSRD 上执行 **display mpls lsp** 命令，可以看到只建立了到 LSRC 的 LSP。

```
<LSRD> display mpls lsp
```

```
-----
LSP Information: LDP LSP
-----
FEC                In/Out Label  In/Out IF                Vrf Name
3.3.3.9/32         NULL/1025    -/Eth1/0/0
3.3.3.9/32         1026/1025   -/Eth1/0/0
```

----结束

配置文件

- LSRA 的配置文件

```
#
sysname LSRA
#
mpls lsr-id 1.1.1.9
mpls
#
mpls ldp
#
interface Ethernet1/0/0
ip address 10.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface NULL0
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 1.1.1.9 0.0.0.0
network 10.1.1.0 0.0.0.255
#
return
```

- LSRB 的配置文件

```
#
sysname LSRB
#
mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
outbound peer 4.4.4.9 fec ip-prefix prefix1
#
interface Ethernet1/0/0
ip address 10.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Ethernet1/0/1
ip address 10.1.3.2 255.255.255.0
mpls
mpls ldp
#
interface Ethernet2/0/0
ip address 10.1.2.1 255.255.255.0
mpls
mpls ldp
#
interface NULL0
#
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 10.1.1.0 0.0.0.255
network 10.1.2.0 0.0.0.255
network 10.1.3.0 0.0.0.255
#
ip ip-prefix prefix1 index 10 permit 3.3.3.9 32
```

```
#
return
```

- LSRC 的配置文件

```
#
sysname LSRC
#
mpls lsr-id 3.3.3.9
mpls
#
mpls ldp
#
interface Ethernet1/0/0
ip address 10.1.2.2 255.255.255.0
mpls
mpls ldp
#
interface NULL0
#
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 10.1.2.0 0.0.0.255
#
return
```

- LSRD 的配置文件

```
#
sysname LSRD
#
mpls lsr-id 4.4.4.9
mpls
#
mpls ldp
#
interface Ethernet1/0/0
ip address 10.1.3.1 255.255.255.0
mpls
mpls ldp
#
interface NULL0
#
interface LoopBack1
ip address 4.4.4.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 4.4.4.9 0.0.0.0
network 10.1.3.0 0.0.0.255
#
return
```

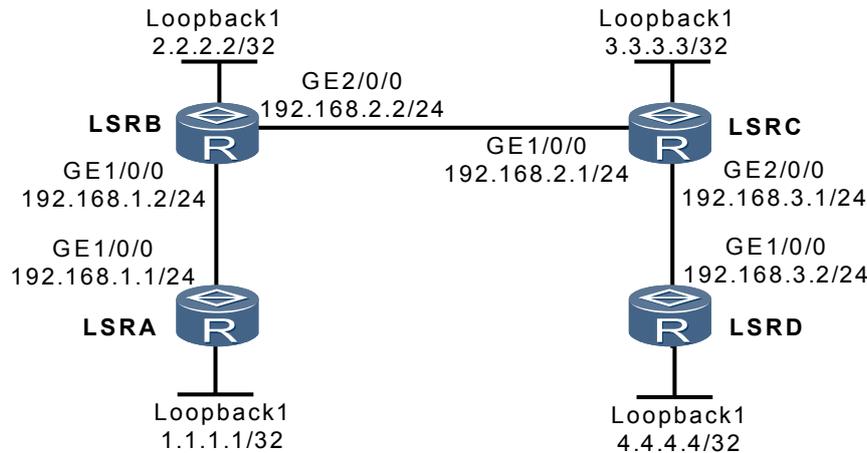
2.17.7 配置 Transit LSP 示例（使用前缀列表）

介绍配置 Transit LSP 的配置过程，包括配置本地 LDP 会话以及在 Transit LSR 上配置 IP 前缀列表对路由进行过滤。

组网需求

如图 2-12 所示，在各节点之间建立 LDP LSP，但在 LSRB 上只允许 4.4.4.4/32 的 FEC 建立 Transit LSP。

图 2-12 配置 Transit LSP 组网图



配置思路

采用如下的思路使用前缀列表配置 LDP LSP：

1. 配置各节点接口的 IP 地址及作为 LSR ID 的 Loopback 地址，并用 OSPF 协议通告各接口所连网段和 LSR ID 主机路由。
2. 全局使能各节点的 MPLS 和 MPLS LDP，并配置 LSP 的触发建立策略。
3. 根据 LSP 控制需求来配置 IP 前缀列表。
4. 在 Transit LSRB 使用此 IP 前缀列表对用于 Transit LSP 的路由进行过滤。
5. 使能各接口的 MPLS 和 MPLS LDP。

数据准备

为完成此配置例，需准备如下的数据：

- 各节点接口的 IP 地址如图 2-12，OSPF 进程号，所在的区域
- LSP 的触发建立策略
- 前缀列表名，以及 Transit 上需要过滤的路由

操作步骤

步骤 1 配置各节点接口的 IP 地址，并用 OSPF 协议通告各接口所连网段和 LSR ID 主机路由。

按照图 2-12 配置各接口 IP 地址和掩码，包括 Loopback 接口，并使用 OSPF 协议通告各接口所连网段和 LSR ID 主机路由，具体配置过程略。

步骤 2 在 Transit LSRB 上配置 IP 前缀列表

在 Transit LSRB 配置 IP 前缀列表，只允许 LSRD 上的 4.4.4.4/32 来建立 Transit LSP。

```
[LSRB]ip ip-prefix FilterOnTransit permit 4.4.4.4 32
```

步骤 3 配置节点和接口的 MPLS 基本能力，并使能 LDP

配置 LSRA。

```
[LSRA] mpls lsr-id 1.1.1.1
[LSRA] mpls
[LSRA-mpls] lsp-trigger all
[LSRA-mpls] quit
[LSRA] mpls ldp
[LSRA-mpls-ldp] quit
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] mpls
[LSRA-GigabitEthernet1/0/0] mpls ldp
[LSRA-GigabitEthernet1/0/0] quit
```

配置 LSRB。

```
[LSRB] mpls lsr-id 2.2.2.2
[LSRB] mpls
[LSRB-mpls] lsp-trigger all
[LSRB-mpls] quit
[LSRB] mpls ldp
[LSRB-mpls-ldp] propagate mapping for ip-prefix FilterOnTransit
[LSRB-mpls-ldp] quit
[LSRB] interface gigabitethernet 1/0/0
[LSRB-GigabitEthernet1/0/0] mpls
[LSRB-GigabitEthernet1/0/0] mpls ldp
[LSRB-GigabitEthernet1/0/0] quit
[LSRB] interface gigabitethernet 2/0/0
[LSRB-GigabitEthernet2/0/0] mpls
[LSRB-GigabitEthernet2/0/0] mpls ldp
[LSRB-GigabitEthernet2/0/0] quit
```

LSRC、LSRD 的配置与 LSRA、LSRB 类似，不再赘述。

步骤 4 检查配置结果

可以用 **display mpls ldp lsp** 命令来查看 LSP 的建立情况。

查看 LSRA 上的 LDP LSP。

```
[LSRA] display mpls ldp lsp
```

```
LDP LSP Information
-----
DestAddress/Mask  In/OutLabel  UpstreamPeer  NextHop      OutInterface
-----
1.1.1.1/32       3/NULL       2.2.2.2       127.0.0.1    InLoop0
2.2.2.2/32       NULL/3       -             192.168.1.2  GE1/0/0
2.2.2.2/32       1024/3       2.2.2.2       192.168.1.2  GE1/0/0
4.4.4.4/32       NULL/1026    -             192.168.1.2  GE1/0/0
4.4.4.4/32       1026/1026    2.2.2.2       192.168.1.2  GE1/0/0
192.168.1.0/24   3/NULL       2.2.2.2       192.168.1.1  GE1/0/0
*192.168.1.0/24  Liberal
192.168.2.0/24   NULL/3       -             192.168.1.2  GE1/0/0
192.168.2.0/24   1027/3       2.2.2.2       192.168.1.2  GE1/0/0
-----
TOTAL: 8 Normal LSP(s) Found.
TOTAL: 1 Liberal LSP(s) Found.
TOTAL: 0 Frr LSP(s) Found.
A '*' before an LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
A '*' before a UpstreamPeer means the session is in GR state
A '*' before a NextHop means the LSP is FRR LSP
```

查看 LSRB 上的 LDP LSP。

```
[LSRB] display mpls ldp lsp
```

```
LDP LSP Information
-----
DestAddress/Mask  In/OutLabel  UpstreamPeer  NextHop      OutInterface
-----
```

```

1.1.1.1/32      NULL/3      -           192.168.1.1    GE1/0/0
2.2.2.2/32      3/NULL      1.1.1.1    127.0.0.1     InLoop0
2.2.2.2/32      3/NULL      3.3.3.3    127.0.0.1     InLoop0
*2.2.2.2/32     Liberal
*2.2.2.2/32     Liberal
3.3.3.3/32      NULL/3      -           192.168.2.1    GE2/0/0
4.4.4.4/32      NULL/1026   -           192.168.2.1    GE2/0/0
4.4.4.4/32      1026/1026   1.1.1.1    192.168.2.1    GE2/0/0
4.4.4.4/32      1026/1026   3.3.3.3    192.168.2.1    GE2/0/0
*4.4.4.4/32     Liberal
192.168.1.0/24  3/NULL      1.1.1.1    192.168.1.2    GE1/0/0
192.168.1.0/24  3/NULL      3.3.3.3    192.168.1.2    GE1/0/0
*192.168.1.0/24 Liberal
*192.168.1.0/24 Liberal
192.168.2.0/24  3/NULL      1.1.1.1    192.168.2.2    GE2/0/0
192.168.2.0/24  3/NULL      3.3.3.3    192.168.2.2    GE2/0/0
*192.168.2.0/24 Liberal
*192.168.2.0/24 Liberal
192.168.3.0/24  NULL/3      -           192.168.2.1    GE2/0/0

```

TOTAL: 12 Normal LSP(s) Found.

TOTAL: 7 Liberal LSP(s) Found.

TOTAL: 0 Frr LSP(s) Found.

A '*' before an LSP means the LSP is not established

A '*' before a Label means the USCB or DSCB is stale

A '*' before a UpstreamPeer means the session is in GR state

A '*' before a NextHop means the LSP is FRR LSP

查看 LSRC 上的 LDP LSP。

[LSRC] **display mpls ldp lsp**

LDP LSP Information

DestAddress/Mask	In/OutLabel	UpstreamPeer	NextHop	OutInterface
2.2.2.2/32	NULL/3	-	192.168.2.2	GE1/0/0
2.2.2.2/32	1025/3	2.2.2.2	192.168.2.2	GE1/0/0
2.2.2.2/32	1025/3	4.4.4.4	192.168.2.2	GE1/0/0
*2.2.2.2/32	Liberal			
3.3.3.3/32	3/NULL	2.2.2.2	127.0.0.1	InLoop0
3.3.3.3/32	3/NULL	4.4.4.4	127.0.0.1	InLoop0
*3.3.3.3/32	Liberal			
4.4.4.4/32	NULL/3	-	192.168.3.2	GE2/0/0
4.4.4.4/32	1026/3	2.2.2.2	192.168.3.2	GE2/0/0
4.4.4.4/32	1026/3	4.4.4.4	192.168.3.2	GE2/0/0
*4.4.4.4/32	Liberal			
192.168.1.0/24	NULL/3	-	192.168.2.2	GE1/0/0
192.168.1.0/24	1027/3	2.2.2.2	192.168.2.2	GE1/0/0
192.168.1.0/24	1027/3	4.4.4.4	192.168.2.2	GE1/0/0
*192.168.1.0/24	Liberal			
192.168.2.0/24	3/NULL	2.2.2.2	192.168.2.1	GE1/0/0
192.168.2.0/24	3/NULL	4.4.4.4	192.168.2.1	GE1/0/0
*192.168.2.0/24	Liberal			
*192.168.2.0/24	Liberal			
192.168.3.0/24	3/NULL	2.2.2.2	192.168.3.1	GE2/0/0
192.168.3.0/24	3/NULL	4.4.4.4	192.168.3.1	GE2/0/0
*192.168.3.0/24	Liberal			

TOTAL: 15 Normal LSP(s) Found.

TOTAL: 7 Liberal LSP(s) Found.

TOTAL: 0 Frr LSP(s) Found.

A '*' before an LSP means the LSP is not established

A '*' before a Label means the USCB or DSCB is stale

A '*' before a UpstreamPeer means the session is in GR state

A '*' before a NextHop means the LSP is FRR LSP

查看 LSRD 上的 LDP LSP。

[LSRD] **display mpls ldp lsp**

```
LDP LSP Information
-----
DestAddress/Mask  In/OutLabel  UpstreamPeer  NextHop      OutInterface
-----
2.2.2.2/32        NULL/1025    -              192.168.3.1  GE1/0/0
2.2.2.2/32        1025/1025    3.3.3.3        192.168.3.1  GE1/0/0
3.3.3.3/32        NULL/3       -              192.168.3.1  GE1/0/0
3.3.3.3/32        1026/3       3.3.3.3        192.168.3.1  GE1/0/0
4.4.4.4/32        3/NULL       3.3.3.3        127.0.0.1    InLoop0
*4.4.4.4/32       Liberal
192.168.1.0/24    NULL/1027    -              192.168.3.1  GE1/0/0
192.168.1.0/24    1027/1027    3.3.3.3        192.168.3.1  GE1/0/0
192.168.2.0/24    NULL/3       -              192.168.3.1  GE1/0/0
192.168.2.0/24    1028/3       3.3.3.3        192.168.3.1  GE1/0/0
192.168.3.0/24    3/NULL       3.3.3.3        192.168.3.2  GE1/0/0
*192.168.3.0/24   Liberal
-----
TOTAL: 10 Normal LSP(s) Found.
TOTAL: 2 Liberal LSP(s) Found.
TOTAL: 0 Frr LSP(s) Found.
A '*' before an LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
A '*' before a UpstreamPeer means the session is in GR state
A '*' before a NextHop means the LSP is FRR LSP
```

从以上显示信息可以看到，由于配置了 LSP 的控制策略，各节点上只存在以 LSRB 为 Transit 的关于 4.4.4.4/32 的 LDP LSP，以及其他不是以 LSRB 为 Transit 的 LDP LSP。

---结束

配置文件

● LSRA 的配置文件

```
#
 sysname LSRA
#
 mpls lsr-id 1.1.1.1
 mpls
  lsp-trigger all
#
 mpls ldp
#
 interface GigabitEthernet1/0/0
  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
#
 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
#
 return
```

● LSRB 的配置文件

```
#
 sysname LSRB
#
 mpls lsr-id 2.2.2.2
 mpls
  lsp-trigger all
#
 mpls ldp
  propagate mapping for ip-prefix FilterOnTransit
```

```
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 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
#
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 2.2.2.2 0.0.0.0
#
ip ip-prefix FilterOnTransit index 10 permit 4.4.4.4 32
#
return
```

● LSRC 的配置文件

```
#
 sysname LSRC
#
 mpls lsr-id 3.3.3.3
 mpls
 lsp-trigger all
#
 mpls ldp
#
interface GigabitEthernet1/0/0
 ip address 192.168.2.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
ospf 1
 area 0.0.0.0
 network 192.168.2.0 0.0.0.255
 network 192.168.3.0 0.0.0.255
 network 3.3.3.3 0.0.0.0
#
return
```

● LSRD 的配置文件

```
#
 sysname LSRD
#
 mpls lsr-id 4.4.4.4
 mpls
 lsp-trigger all
#
 mpls ldp
#
interface GigabitEthernet1/0/0
 ip address 192.168.3.2 255.255.255.0
 mpls
 mpls ldp
#
```

```

interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 192.168.3.0 0.0.0.255
  network 4.4.4.4 0.0.0.0
#
return
    
```

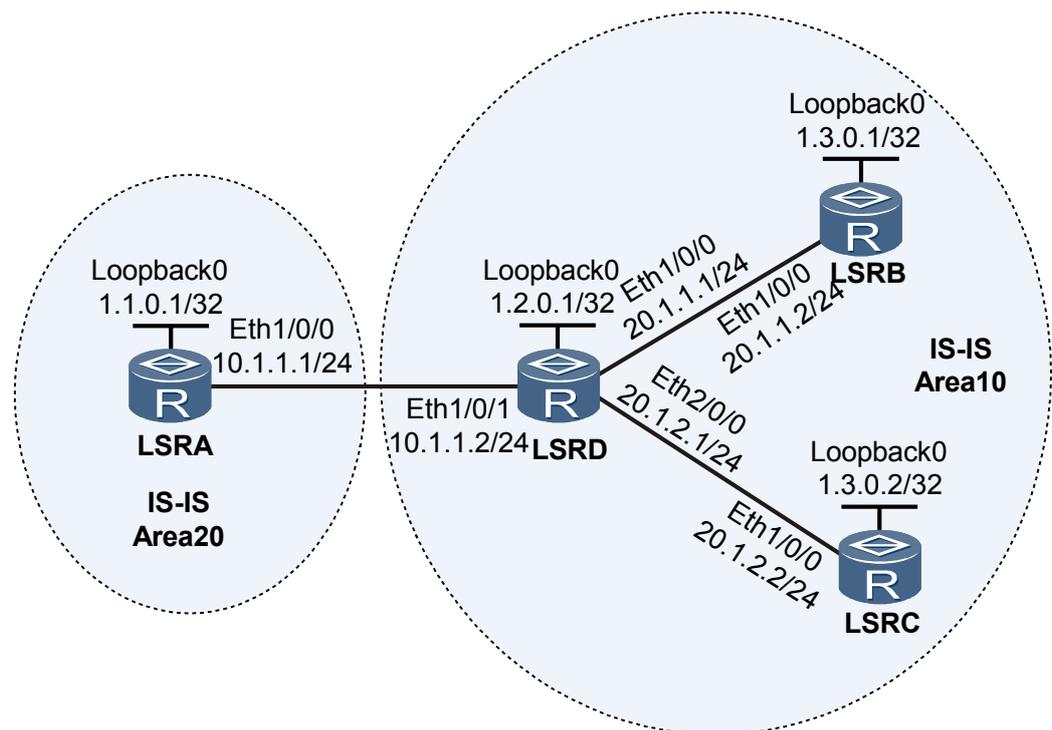
2.17.8 配置 LDP 跨域扩展示例

介绍 LDP 跨域扩展的配置过程，包括配置全局使能 MPLS 和 MPLS LDP 以及配置聚合路由的策略。

组网需求

如图 2-13 所示，存在 Area 10 和 Area 20 两个 IGP 域。需要建立 LSRA 到 LSRB 以及 LSRA 到 LSRC 的跨越两个 IGP 域的 LSP。要求在 LSRA 上配置 LDP 跨域扩展功能，使 LSRA 查找最长匹配路由建立 LSP。

图 2-13 配置 LDP 跨域扩展组网图



配置思路

采用如下的思路实现 LDP 跨域扩展：

1. 配置各节点接口的 IP 地址及作为 LSR ID 的 Loopback 地址。
2. 配置 IS-IS 协议的基本功能。

3. 配置聚合路由的策略。
4. 使能各节点全局和接口的 MPLS 和 MPLS LDP。
5. 配置 LDP 跨域扩展。

数据准备

为完成此配置例，需准备如下的数据：

- 各节点接口的 IP 地址如 [图 2-13](#)
- 各节点的 IS-IS 区域地址及各节点和接口的 Level 级别

操作步骤

步骤 1 配置各节点接口的 IP 地址及作为 LSR ID 的 Loopback 地址

按照 [图 2-13](#) 配置各接口 IP 地址和掩码，包括 Loopback 接口，具体配置过程略。

步骤 2 配置 IS-IS 协议的基本功能

配置 LSRA。

```
<LSRA> system-view
[LSRA] isis 1
[LSRA-isis-1] is-level level-2
[LSRA-isis-1] network-entity 20.0010.0100.0001.00
[LSRA-isis-1] quit
[LSRA] interface ethernet 1/0/0
[LSRA-Ethernet1/0/0] isis enable 1
[LSRA-Ethernet1/0/0] quit
[LSRA] interface loopback 0
[LSRA-LoopBack0] isis enable 1
[LSRA-LoopBack0] quit
```

配置 LSRD。

```
<LSRD> system-view
[LSRD] isis 1
[LSRD-isis-1] network-entity 10.0010.0200.0001.00
[LSRD-isis-1] quit
[LSRD] interface ethernet 1/0/0
[LSRD-Ethernet1/0/0] isis enable 1
[LSRD-Ethernet1/0/0] isis circuit-level level-1
[LSRD-Ethernet1/0/0] quit
[LSRD] interface ethernet 1/0/1
[LSRD-Ethernet1/0/1] isis enable 1
[LSRD-Ethernet1/0/1] isis circuit-level level-2
[LSRD-Ethernet1/0/1] quit
[LSRD] interface ethernet 2/0/0
[LSRD-Ethernet2/0/0] isis enable 1
[LSRD-Ethernet2/0/0] isis circuit-level level-1
[LSRD-Ethernet2/0/0] quit
[LSRD] interface loopback 0
[LSRD-LoopBack0] isis enable 1
[LSRD-LoopBack0] quit
```

配置 LSRB。

```
<LSRB> system-view
[LSRB] isis 1
[LSRB-isis-1] is-level level-1
[LSRB-isis-1] network-entity 10.0010.0300.0001.00
[LSRB-isis-1] quit
[LSRB] interface ethernet 1/0/0
[LSRB-Ethernet1/0/0] isis enable 1
```

```
[LSRB-Ethernet1/0/0] quit
[LSRB] interface loopback 0
[LSRB-LoopBack0] isis enable 1
[LSRB-LoopBack0] quit
```

配置 LSRC。

```
<LSRC> system-view
[LSRC] isis 1
[LSRC-isis-1] is-level level-1
[LSRC-isis-1] network-entity 10.0010.0300.0002.00
[LSRC-isis-1] quit
[LSRC] interface ethernet 1/0/0
[LSRC-Ethernet1/0/0] isis enable 1
[LSRC-Ethernet1/0/0] quit
[LSRC] interface loopback 0
[LSRC-LoopBack0] isis enable 1
[LSRC-LoopBack0] quit
```

在 LSRA 上执行 **display ip routing-table** 命令查看路由信息。

```
[LSRA] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 11          Routes : 11

Destination/Mask    Proto    Pre  Cost           Flags NextHop         Interface
-----
 1.1.0.1/32        Direct   0    0              D  127.0.0.1          InLoopBack0
 1.2.0.1/32        ISIS-L1  15   10             D  10.1.1.2           Ethernet1/0/0
 1.3.0.1/32        ISIS-L1  15   20             D  10.1.1.2           Ethernet1/0/0
 1.3.0.2/32        ISIS-L1  15   20             D  10.1.1.2           Ethernet1/0/0
 10.1.1.0/24       Direct   0    0              D  10.1.1.1           Ethernet1/0/0
 10.1.1.1/32       Direct   0    0              D  127.0.0.1          InLoopBack0
 20.1.1.0/24       ISIS-L1  15   20             D  10.1.1.2           Ethernet1/0/0
 20.1.2.0/24       ISIS-L1  15   20             D  10.1.1.2           Ethernet1/0/0
 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 配置聚合路由的策略

在 LSRD 上执行 **summary** 命令将到 LSRB 和 LSRC 的主机路由聚合。

```
[LSRD] isis 1
[LSRD-isis-1] summary 1.3.0.0 255.255.255.0 avoid-feedback
```

在 LSRA 上执行 **display ip routing-table** 命令查看路由信息。

```
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 10          Routes : 10

Destination/Mask    Proto    Pre  Cost           Flags NextHop         Interface
-----
 1.1.0.1/32        Direct   0    0              D  127.0.0.1          InLoopBack0
 1.2.0.1/32        ISIS-L1  15   10             D  10.1.1.2           Ethernet1/0/0
 1.3.0.0/24       ISIS-L1  15  20          D  10.1.1.2       Ethernet1/0/0
 10.1.1.0/24       Direct   0    0              D  10.1.1.1           Ethernet1/0/0
 10.1.1.1/32       Direct   0    0              D  127.0.0.1          InLoopBack0
 20.1.1.0/24       ISIS-L1  15   20             D  10.1.1.2           Ethernet1/0/0
 20.1.2.0/24       ISIS-L1  15   20             D  10.1.1.2           Ethernet1/0/0
 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
```

从显示信息可以看到，到 LSRB 和 LSRC 的主机路由已经聚合。

步骤 4 配置各节点全局和接口的 MPLS 和 MPLS LDP 能力，使网络能够转发 MPLS 流量，并查看 LSP 建立情况

配置 LSRA。

```
[LSRA] mpls lsr-id 1.1.0.1
[LSRA] mpls
[LSRA-mpls] quit
[LSRA] mpls ldp
[LSRA-mpls-ldp] quit
[LSRA] interface ethernet 1/0/0
[LSRA-Ethernet1/0/0] mpls
[LSRA-Ethernet1/0/0] mpls ldp
[LSRA-Ethernet1/0/0] quit
```

配置 LSRD。

```
[LSRD] mpls lsr-id 1.2.0.1
[LSRD] mpls
[LSRD-mpls] quit
[LSRD] mpls ldp
[LSRD-mpls-ldp] quit
[LSRD] interface ethernet 1/0/0
[LSRD-Ethernet1/0/0] mpls
[LSRD-Ethernet1/0/0] mpls ldp
[LSRD-Ethernet1/0/0] quit
[LSRD] interface ethernet 1/0/1
[LSRD-Ethernet1/0/1] mpls
[LSRD-Ethernet1/0/1] mpls ldp
[LSRD-Ethernet1/0/1] quit
[LSRD] interface ethernet 2/0/0
[LSRD-Ethernet2/0/0] mpls
[LSRD-Ethernet2/0/0] mpls ldp
[LSRD-Ethernet2/0/0] quit
```

配置 LSRB。

```
[LSRB] mpls lsr-id 1.3.0.1
[LSRB] mpls
[LSRB-mpls] quit
[LSRB] mpls ldp
[LSRB-mpls-ldp] quit
[LSRB] interface ethernet 1/0/0
[LSRB-Ethernet1/0/0] mpls
[LSRB-Ethernet1/0/0] mpls ldp
[LSRB-Ethernet1/0/0] quit
```

配置 LSRC。

```
[LSRC] mpls lsr-id 1.3.0.2
[LSRC] mpls
[LSRC-mpls] quit
[LSRC] mpls ldp
[LSRC-mpls-ldp] quit
[LSRC] interface ethernet 1/0/0
[LSRC-Ethernet1/0/0] mpls
[LSRC-Ethernet1/0/0] mpls ldp
[LSRC-Ethernet1/0/0] quit
```

配置完成后，在 LSRA 上执行 **display mpls lsp** 命令，查看已经建立的 LSP。

```
[LSRA] display mpls lsp
```

```
-----
LSP Information: LDP LSP
-----
```

FE	In/Out Label	In/Out IF	Vrf Name
1.2.0.1/32	NULL/3	~/Eth1/0/0	
1.2.0.1/32	1024/3	~/Eth1/0/0	

从显示信息可以看到，缺省情况下，LDP 没有建立从 LSRA 到 LSRB 和 LSRC 的跨域 LSP。

步骤 5 配置 LDP 跨域扩展

在 LSRA 上执行 **longest-match** 命令，使能 LDP 按照最长匹配方式查找路由建立 LSP。

```
[LSRA] mpls ldp
[LSRA-mpls-ldp] longest-match
[LSRA-mpls-ldp] quit
```

步骤 6 检查配置结果

上述配置完成后，在 LSRA 上执行 **display mpls lsp** 命令，查看已经建立的 LSP。

```
[LSRA] display mpls lsp
```

```
-----
LSP Information: LDP LSP
-----
FEC                In/Out Label  In/Out IF                Vrf Name
1.2.0.1/32         NULL/3        -/Eth1/0/0
1.2.0.1/32         1024/3        -/Eth1/0/0
1.3.0.1/32         NULL/1025     -/Eth1/0/0
1.3.0.1/32         1025/1025    -/Eth1/0/0
1.3.0.2/32         NULL/1026     -/Eth1/0/0
1.3.0.2/32         1026/1026    -/Eth1/0/0
```

从显示信息可以看到，LDP 建立了从 LSRA 到 LSRB 和 LSRC 的跨越两个 IGP 域的 LSP。

----结束

配置文件

● LSRA 的配置文件

```
#
sysname LSRA
#
mpls lsr-id 1.1.0.1
mpls
#
mpls ldp
longest-match
#
isis 1
is-level level-2
network-entity 20.0010.0100.0001.00
#
interface Ethernet1/0/0
ip address 10.1.1.1 255.255.255.0
isis enable 1
mpls
mpls ldp
#
interface LoopBack0
ip address 1.1.0.1 255.255.255.255
isis enable 1
#
return
```

● LSRB 的配置文件

```
#
sysname LSRB
#
mpls lsr-id 1.3.0.1
mpls
```

```
#
mpls ldp
#
isis 1
 is-level level-1
 network-entity 10.0010.0300.0001.00
#
interface Ethernet1/0/0
 ip address 20.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 1.3.0.1 255.255.255.255
 isis enable 1
#
return
```

● LSRC 的配置文件

```
#
 sysname LSRC
#
 mpls lsr-id 1.3.0.2
 mpls
#
 mpls ldp
#
 isis 1
 is-level level-1
 network-entity 10.0010.0300.0002.00
#
interface Ethernet1/0/0
 ip address 20.1.2.2 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 1.3.0.2 255.255.255.255
 isis enable 1
#
return
```

● LSRD 的配置文件

```
#
 sysname LSRD
#
 mpls lsr-id 1.2.0.1
 mpls
#
 mpls ldp
#
 isis 1
 network-entity 10.0010.0200.0001.00
 summary 1.3.0.0 255.255.255.0 avoid-feedback
#
interface Ethernet1/0/0
 ip address 20.1.1.1 255.255.255.0
 isis enable 1
 isis circuit-level level-1
 mpls
 mpls ldp
#
interface Ethernet1/0/1
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
 isis circuit-level level-2
 mpls
 mpls ldp
```

```
#
interface Ethernet2/0/0
 ip address 20.1.2.1 255.255.255.0
 isis enable 1
 isis circuit-level level-1
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 1.2.0.1 255.255.255.255
 isis enable 1
#
return
```

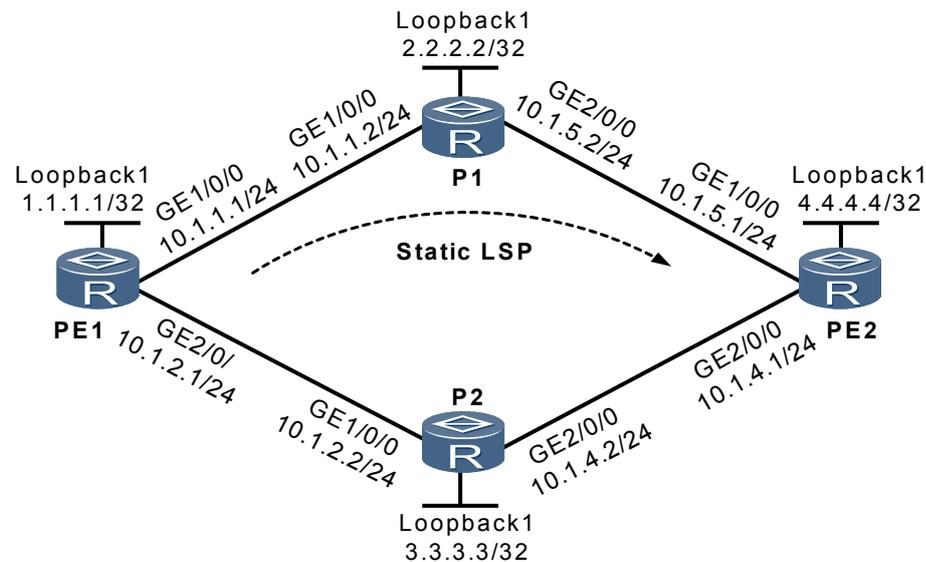
2.17.9 配置静态 BFD 检测 LDP LSP 示例

介绍配置静态 BFD 检测 LDP LSP 的配置过程，包括在各设备以及各接口使能 MPLS、MPLS LDP，以及在被检测链路的两端节点上使能 BFD 能力。

组网需求

如图 2-14 所示，在 PE1→P1→PE2 上建立 LDP LSP，PE2→P2→PE1 为 IP 链路，要求使用静态 BFD 检测 LDP LSP 的连通性。

图 2-14 配置静态 BFD 检测 LDP LSP 组网图



配置思路

采用如下思路配置本示例：

1. 整个 MPLS 域采用 OSPF 协议，各节点之间 IP 可达。
2. 在 PE1→P1→PE2 上建立 LDP LSP。
3. 在 PE1 上配置绑定 LDP LSP 的 BFD 会话。
4. 在 PE2 上配置绑定 IP 链路的 BFD 会话，将检测到的 LDP LSP 的故障通告给 PE1。

数据准备

要完成此配置示例，需准备以下数据：

- 各接口的 IP 地址
- OSPF 进程号
- BFD 配置名、本地标识符、远端标识符

操作步骤

步骤 1 配置各接口的 IP 地址和 OSPF 协议

按照图 2-14 配置各接口的 IP 地址和掩码，包括各 Loopback 接口。

在所有节点上配置 OSPF 协议，发布各自 Loopback 接口的主机路由，具体配置过程略。

配置完成后，各 LSR 可以互相 Ping 通对方的 LSR-ID，在各 LSR 上执行 **display ip routing-table** 命令可以看到到达各 LSR 的路由表项。

```
<PE1> display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 14          Routes : 15

Destination/Mask    Proto Pre  Cost   Flags NextHop         Interface
-----
 1.1.1.1/32        Direct 0    0       D 127.0.0.1         LoopBack1
 2.2.2.2/32        OSPF  10    2       D 10.1.1.2         GigabitEthernet1/0/0
 3.3.3.3/32        OSPF  10    2       D 10.1.2.2         GigabitEthernet2/0/0
 4.4.4.4/32        OSPF  10    3       D 10.1.2.2         GigabitEthernet2/0/0
                   OSPF  10    3       D 10.1.1.2         GigabitEthernet1/0/0
10.1.1.0/24        Direct 0    0       D 10.1.1.1         GigabitEthernet1/0/0
10.1.1.1/32        Direct 0    0       D 127.0.0.1         GigabitEthernet1/0/0
10.1.1.2/32        Direct 0    0       D 10.1.1.2         GigabitEthernet1/0/0
10.1.2.0/24        Direct 0    0       D 10.1.2.1         GigabitEthernet2/0/0
10.1.2.1/32        Direct 0    0       D 127.0.0.1         GigabitEthernet2/0/0
10.1.2.2/32        Direct 0    0       D 10.1.2.2         GigabitEthernet2/0/0
10.1.4.0/24        OSPF  10    2       D 10.1.2.2         GigabitEthernet2/0/0
10.1.5.0/24        OSPF  10    2       D 10.1.1.2         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 2 在 PE1—>P1—>PE2 上建立 LDP LSP。

配置 PE1。

```
<PE1> system-view
[PE1] mpls lsr-id 1.1.1.1
[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 P1。

```
<P1> system-view
[P1] mpls lsr-id 2.2.2.2
[P1] mpls
[P1-mpls] quit
[P1] mpls ldp
```

```
[P1-mpls-ldp] quit
[P1]interface gigabitethernet 1/0/0
[P1-GigabitEthernet1/0/0] mpls
[P1-GigabitEthernet1/0/0] mpls ldp
[P1-GigabitEthernet1/0/0] quit
[P1]interface gigabitethernet 2/0/0
[P1-GigabitEthernet2/0/0] mpls
[P1-GigabitEthernet2/0/0] mpls ldp
[P1-GigabitEthernet2/0/0] quit
```

配置 PE2。

```
<PE2> system-view
[PE2] mpls lsr-id 4.4.4.4
[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
```

执行命令 **display mpls ldp lsp**，可以看到在 PE1 上建立了到目的地址为 4.4.4.4/32 的 LDP LSP。

```
<PE1> display mpls ldp lsp
```

```
LDP LSP Information
-----
DestAddress/Mask  In/OutLabel      UpstreamPeer      NextHop           OutInterface
-----
1.1.1.1/32        3/NULL           2.2.2.2           127.0.0.1        InLoop0
*1.1.1.1/32       Liberal
2.2.2.2/32        NULL/3           -                 10.1.1.2         GE1/0/0
2.2.2.2/32        1024/3           2.2.2.2           10.1.1.2         GE1/0/00
4.4.4.4/32        NULL/1025        -                 10.1.1.2         GE1/0/0
4.4.4.4/32        1025/1025        2.2.2.2           10.1.1.2         GE1/0/0
-----
TOTAL: 5 Normal LSP(s) Found.
TOTAL: 1 Liberal LSP(s) Found.
TOTAL: 0 Frr LSP(s) Found.
A '*' before an LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
A '*' before a UpstreamPeer means the session is in GR state
A '*' before a NextHop means the LSP is FRR LSP
```

步骤 3 在被检测链路两端节点上使能全局 BFD 能力

配置 PE1。

```
<PE1> system-view
[PE1] bfd
[PE1-bfd] quit
```

配置 PE2。

```
<PE2> system-view
[PE2] bfd
[PE2-bfd] quit
```

步骤 4 在 Ingress 上配置绑定到 LDP LSP 的 BFD 会话。

配置 PE1。

```
<PE1> system-view
[PE1] bfd lto4 bind ldp-lsp peer-ip 4.4.4.4 nexthop 10.1.1.2 interface gigabitethernet 1/0/0
[PE1-bfd-lsp-session-lto4] discriminator local 1
[PE1-bfd-lsp-session-lto4] discriminator remote 2
```

```
[PE1-bfd-lsp-session-1to4] process-pst
[PE1-bfd-lsp-session-1to4] commit
[PE1-bfd-lsp-session-1to4] quit
```

步骤 5 在 Egress 上配置绑定到 IP 链路的 BFD 会话，用来将 LDP LSP 的故障通告给 Ingress。

配置 PE2。

```
<PE2> system-view
[PE2] bfd 4tol bind peer-ip 1.1.1.1
[PE2-bfd-session-4ot1] discriminator local 2
[PE2-bfd-session-4ot1] discriminator remote 1
[PE2-bfd-session-4ot1] commit
[PE2-bfd-session-4ot1] quit
```

步骤 6 检测配置结果

配置完成后，在 Ingress 上执行命令 **display bfd session all verbose**，可以看到“State”字段的值为“Up”，且“BFD Bind Type”字段的值为“LDP_LSP”。

```
<PE1> display bfd session all verbose
```

```
-----
Session MIndex : 256          State : Up          Name : 1to4
-----
Local Discriminator      : 1          Remote Discriminator   : 2
Session Detect Mode     : Asynchronous Mode Without Echo Function
BFD Bind Type          : LDP_LSP
Bind Session Type      : Static
Bind Peer IP Address   : 4.4.4.4
NextHop Ip Address     : 10.1.1.2
Bind Interface         : GigabitEthernet1/0/0
FSM Board Id           : 0          TOS-EXP                : 7
Min Tx Interval (ms)   : 1000       Min Rx Interval (ms)  : 1000
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                    : 1
Proc Interface Status  : Disable     Process PST            : Enable
WTR Interval (ms)     : -
Active Multi           : 3
Last Local Diagnostic  : No Diagnostic
Bind Application       : LSPM | L2VPN | OAM_MANAGER
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-5
Session Description    : -
-----
```

```
Total UP/DOWN Session Number : 1/0
```

在 Egress 上执行命令 **display bfd session all verbose**，可以看到“(Multi Hop) State”字段的值为“Up”，且“BFD Bind Type”字段的值为“Peer IP Address”。

```
<PE2> display bfd session all verbose
```

```
-----
Session MIndex : 64          (Multi Hop) State : Up          Name : 4tol
-----
Local Discriminator      : 2          Remote Discriminator   : 1
Session Detect Mode     : Asynchronous Mode Without Echo Function
BFD Bind Type          : Peer IP Address
Bind Session Type      : Static
Bind Peer IP Address   : 1.1.1.1
Bind Interface         : -
Track Interface        : -
FSM Board Id           : 0          TOS-EXP                : 7
Min Tx Interval (ms)   : 10          Min Rx Interval (ms)  : 10
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                   : 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-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
#
 bfd
#
 mpls lsr-id 1.1.1.1
 mpls
#
 mpls ldp
#
 interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
 interface GigabitEthernet2/0/0
 ip address 10.1.2.1 255.255.255.0
#
 interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
 ospf 1
 area 0.0.0.0
 network 1.1.1.1 0.0.0.0
 network 10.1.1.0 0.0.0.255
 network 10.1.2.0 0.0.0.255
#
 bfd lto4 bind ldp-lsp peer-ip 4.4.4.4 nexthop 10.1.1.2 interface GigabitEthernet1/0/0
 discriminator local 1
 discriminator remote 2
 process-pst
 commit
#
 return
    
```

- PE2 的配置文件

```

#
 sysname PE2
#
 bfd
#
 mpls lsr-id 4.4.4.4
 mpls
#
 mpls ldp
#
    
```

```
interface GigabitEthernet1/0/0
 ip address 10.1.5.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 ip address 10.1.4.1 255.255.255.0
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
#
bfd 4to1 bind peer-ip 1.1.1.1
 discriminator local 2
 discriminator remote 1
 commit
#
ospf 1
 area 0.0.0.0
 network 10.1.5.0 0.0.0.255
 network 10.1.4.0 0.0.0.255
 network 4.4.4.4 0.0.0.0
#
return
```

● P1 的配置文件

```
#
 sysname P1
#
 mpls lsr-id 2.2.2.2
 mpls
#
 mpls ldp
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 ip address 10.1.5.2 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
ospf 1
 area 0.0.0.0
 network 2.2.2.2 0.0.0.0
 network 10.1.1.0 0.0.0.255
 network 10.1.5.0 0.0.0.255
#
return
```

● P2 的配置文件

```
#
 sysname P2
#
interface GigabitEthernet1/0/0
 ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.4.2 255.255.255.0
#
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 10.1.4.0 0.0.0.255
network 10.1.2.0 0.0.0.255
#
return
```

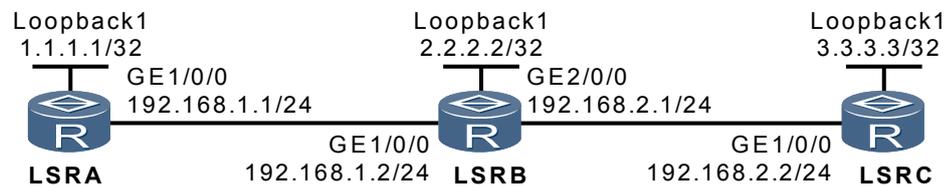
2.17.10 配置动态 BFD 检测 LDP LSP 示例

介绍配置动态 BFD 检测 LDP LSP 的配置过程，包括在各设备以及各接口使能 MPLS、MPLS LDP，以及在源端和对端上使能 BFD 能力。

组网需求

如图 2-15 所示，节点 LSRA、LSRB 和 LSRC 属于同一 MPLS 域，LSRA 和 LSRC 之间创建 LDP LSP 链路，要求使用动态 BFD 检测 LDP LSP 的连通性。

图 2-15 配置动态 BFD 检测 LDP LSP 示例组网图



配置思路

采用如下的思路配置动态 BFD 检测 LDP LSP 示例。

1. 在 LSRA 和 LSRC 之间创建 LDP LSP 链路；
2. 配置 BFD 基本能力；
3. 调整 BFD 检测参数。

数据准备

为完成此配置例，需准备如下的数据。

- 各节点的 LSR ID 和接口 IP 地址
- BFD 检测参数

操作步骤

步骤 1 配置各接口的 IP 地址（略）

步骤 2 配置 OSPF（略）

步骤 3 创建 LSRA 和 LSRC 之间的 LDP LSP

配置 LSRA。

```
<LSRA> system-view
[LSRA] mpls lsr-id 1.1.1.1
[LSRA] mpls
[LSRA-mpls] quit
[LSRA] mpls ldp
```

```
[LSRA-mpls-ldp] quit
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] mpls
[LSRA-GigabitEthernet1/0/0] mpls ldp
[LSRA-GigabitEthernet1/0/0] quit
```

LSRB 和 LSRC 的配置和 LSRA 相似（略）。

配置完成后，在 LSRA 上执行 **display mpls ldp lsp** 命令，可以看到 LSRA 到 LSRC 之间的 LDP LSP 已经建立，以 LSRA 的显示为例。

```
<LSRA> display mpls ldp lsp
```

```
LDP LSP Information
-----
DestAddress/Mask  In/OutLabel  UpstreamPeer  NextHop      OutInterface
-----
1.1.1.1/32       3/NULL       2.2.2.2       127.0.0.1    InLoop0
*1.1.1.1/32      Liberal      -              DS/2.2.2.2
2.2.2.2/32       NULL/3       -              192.168.1.2  GE1/0/0
2.2.2.2/32       1024/3       2.2.2.2       192.168.1.2  GE1/0/0
3.3.3.3/32       NULL/1025    -              192.168.1.2  GE1/0/0
3.3.3.3/32       1025/1025    2.2.2.2       192.168.1.2  GE1/0/0
-----
TOTAL: 5 Normal LSP(s) Found.
TOTAL: 1 Liberal LSP(s) Found.
TOTAL: 0 Frr LSP(s) Found.
A '*' before an LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
A '*' before a UpstreamPeer means the session is in GR state
A '*' before a NextHop means the LSP is FRR LSP
```

步骤 4 配置动态 BFD 会话检测 LSRA 到 LSRC 之间的 LDP LSP

在 LSRA 上配置 FEC 列表，这样就可以保障只触发 BFD 检测 LSRA 到 LSRC 之间的 LDP LSP。

```
[LSRA] fec-list tortc
[LSRA-fec-list-tortc] fec-node 3.3.3.3
```

在 LSRA 上使能 BFD，指定动态触发 BFD 会话的 FEC 列表，并调整 BFD 检测参数。

```
[LSRA] bfd
[LSRA-bfd] quit
[LSRA] mpls
[LSRA-mpls] mpls bfd-trigger fec-list tortc
[LSRA-mpls] mpls bfd enable
[LSRA-mpls] mpls bfd min-tx-interval 100 min-rx-interval 600 detect-multiplier 4
```

在 LSRC 上配置被动使能 BFD for LSP 能力。

```
[LSRC] bfd
[LSRC-bfd] mpls-passive
```

步骤 5 验证配置结果

执行 **display bfd session all verbose** 命令查看动态创建的 BFD 会话状态。

```
<LSRA> display bfd session all verbose
```

```
-----
Session MIndex : 68          State : Up          Name : dyn_8194
-----
Local Discriminator   : 8194          Remote Discriminator : 8192
Session Detect Mode   : Asynchronous Mode Without Echo Function
BFD Bind Type        : LDP_LSP
Bind Session Type     : Dynamic
Bind Peer IP Address  : 4.4.4.4
NextHop Ip Address    : 10.1.1.2
Bind Interface        : GigabitEthernet0/0/2
```

```

LSP Token           : 0x5
FSM Board Id       : 0
Min Tx Interval (ms) : 100
Actual Tx Interval (ms) : 100
Local Detect Multi  : 4
Echo Passive       : Disable
Destination Port    : 3784
Proc Interface Status : Disable
WTR Interval (ms)  : -
Active Multi        : 3
Last Local Diagnostic : No Diagnostic
Bind Application    : LSPM | LDP | L2VPN | OAM_MANAGER
Session TX TmrID   : -
Session Init TmrID : -
Session Echo Tx TmrID : -
PDT Index          : FSM-0 | RCV-0 | IF-0 | TOKEN-5
Session Description : -
TOS-EXP            : 7
Min Rx Interval (ms) : 600
Actual Rx Interval (ms) : 600
Detect Interval (ms) : 1800
Acl Number         : -
TTL                : 1
Process PST        : Enable
    
```

Total UP/DOWN Session Number : 1/0

查看 LSRC 上的被动创建的 BFD 会话状态，其中 BFD Bind Type 字段的值为“Peer IP Address”，说明 LSRC 发送的 BFD 报文是通过 IP 路由传输的。

<LSRC> **display bfd session passive-dynamic verbose**

```

Session MIndex : 65          (Multi Hop) State : Up          Name : dyn_8192
-----
Local Discriminator      : 8192          Remote Discriminator : 8194
Session Detect Mode     : Asynchronous Mode Without Echo Function
BFD Bind Type           : Peer IP Address
Bind Session Type       : Entire_Dynamic
Bind Peer IP Address    : 1.1.1.1
Bind Interface          : -
FSM Board Id           : 0
Min Tx Interval (ms)   : 10
Actual Tx Interval (ms) : 600
Local Detect Multi      : 3
Echo Passive           : Disable
Destination Port        : 3784
Proc Interface Status   : Disable
WTR Interval (ms)      : -
Active Multi            : 4
Last Local Diagnostic   : No Diagnostic
Bind Application        : LSPV
Session TX TmrID       : -
Session Init TmrID     : -
Session Echo Tx TmrID  : -
PDT Index              : FSM-0 | RCV-0 | IF-0 | TOKEN-0
Session Description     : -
TOS-EXP                 : 7
Min Rx Interval (ms)   : 10
Actual Rx Interval (ms) : 100
Detect Interval (ms)   : 400
Acl Number              : -
TTL                     : 253
Process PST             : Disable
    
```

Total UP/DOWN Session Number : 1/0

---结束

配置文件

- LSRA 的配置文件

```

#
sysname LSRA
#
bfd
#
mpls lsr-id 1.1.1.1
mpls
mpls bfd enable
mpls bfd-trigger fec-list tortc
    
```

```
mpls bfd min-tx-interval 100 min-rx-interval 600 detect-multiplier 4
#
fec-list tortc
fec-node 3.3.3.3
#
mpls ldp
#
interface GigabitEthernet1/0/0
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
#
ospf 100
area 0.0.0.0
network 1.1.1.1 0.0.0.0
network 192.168.1.0 0.0.0.255
#
return
```

● LSRB 的配置文件

```
#
sysname LSRB
#
mpls lsr-id 2.2.2.2
mpls
#
mpls ldp
#
interface GigabitEthernet1/0/0
ip address 192.168.1.2 255.255.255.0
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
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
#
ospf 100
area 0.0.0.0
network 2.2.2.2 0.0.0.0
network 192.168.1.0 0.0.0.255
network 192.168.2.0 0.0.0.255
#
return
```

● LSRC 的配置文件

```
#
sysname LSRC
#
bfd
mpls-passive
#
mpls lsr-id 3.3.3.3
mpls
#
mpls ldp
#
interface GigabitEthernet1/0/0
ip address 192.168.2.2 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
```

```

ip address 3.3.3.3 255.255.255.255
#
ospf 100
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 192.168.2.0 0.0.0.255
#
return
    
```

2.17.11 配置 Manual LDP FRR 示例

介绍配置 Manual LDP FRR 的配置过程，包括在各设备以及各接口使能 MPLS、MPLS LDP，以及指定备份 LSP 的出接口和下一跳。

组网需求

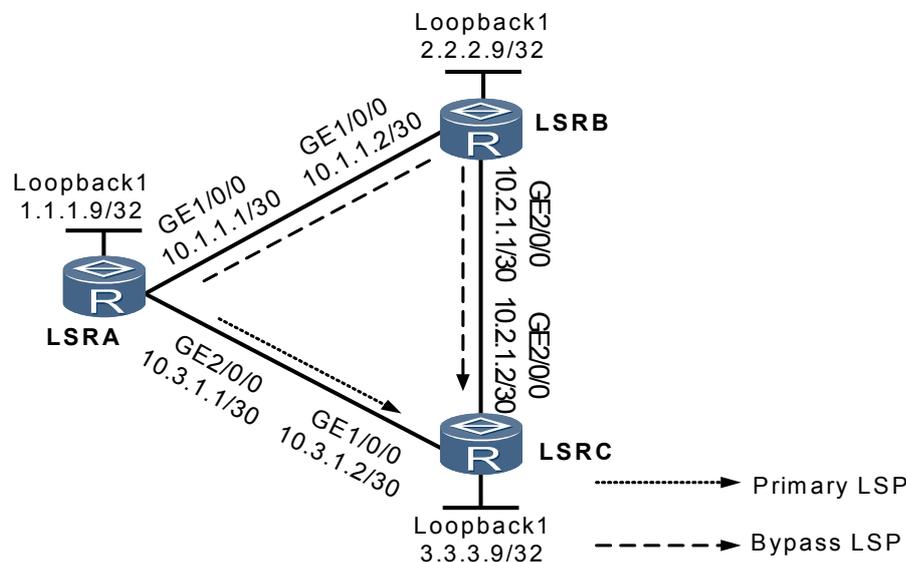
如图 2-16 所示，要求 LSRA 到 LSRC 之间存在两条主备 LSP，其中 LSRA → LSRC 为主用 LSP，LSRA → LSRB → LSRC 为备份 LSP。要求在 LSRA 上配置 Manual LDP FRR 功能，实现 LSRA 本地的端口级备份，从而减少流量丢失。

这里只需 LSRA 支持 Manual LDP FRR。

说明

在 Manual LDP FRR 的组网中，备份 LSP 必须是 Liberal 状态的 LSP，即在使能 FRR 的节点上执行 **display ip routing-table ip-address verbose** 命令可以发现备份 LSP 的路由状态是 “Inactive Adv”。

图 2-16 配置 Manual LDP FRR 组网图



配置思路

采用如下的思路实现 Manual LDP FRR：

1. 配置各节点接口的 IP 地址及作为 LSR ID 的 Loopback 地址，并用 OSPF 协议通告各接口所连网段和 LSR ID 主机路由。

2. 全局使能各节点的 MPLS 和 MPLS LDP。
3. 使能各接口的 MPLS 和 MPLS LDP。
4. 在被保护的接口上指定 Manual LDP FRR 用于生成备用 LSP 的下一跳地址。

数据准备

为完成此配置例，需准备如下的数据：

- 各节点接口的 IP 地址如图 2-16，OSPF 进程号，所在的区域
- LSP 的触发建立策略
- Manual LDP FRR 用于生成备用 LSP 的下一跳地址

操作步骤

步骤 1 配置各接口的 IP 地址

按照图 2-16 配置各接口 IP 地址和掩码，包括 Loopback 接口，具体配置过程略。

步骤 2 配置 OSPF 协议发布各节点接口所连网段和 LSR ID 的主机路由

配置 LSRA。

```
<LSRA> system-view
[LSRA] ospf 1
[LSRA-ospf-1] area 0
[LSRA-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[LSRA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.3
[LSRA-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.3
[LSRA-ospf-1-area-0.0.0.0] quit
[LSRA-ospf-1] quit
```

配置 LSRB。

```
<LSRB> system-view
[LSRB] ospf 1
[LSRB-ospf-1] area 0
[LSRB-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[LSRB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.3
[LSRB-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.3
[LSRB-ospf-1-area-0.0.0.0] quit
[LSRB-ospf-1] quit
```

配置 LSRC。

```
<LSRC> system-view
[LSRC] ospf 1
[LSRC-ospf-1] area 0
[LSRC-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[LSRC-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.3
[LSRC-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.3
[LSRC-ospf-1-area-0.0.0.0] quit
[LSRC-ospf-1] quit
```

配置完成后，在各节点上执行 **display ip routing-table** 命令，可以看到相互之间都学到了彼此的路由。以 LSRA 的显示为例：

```
<LSRA> display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
  Destinations : 12          Routes : 13
Destination/Mask  Proto Pre  Cost   Flags NextHop         Interface
 1.1.1.9/32      Direct 0     0           D 127.0.0.1         LoopBack1
```

```
2.2.2.9/32 OSPF 10 2 D 10.1.1.2 GigabitEthernet1/0/0
3.3.3.9/32 OSPF 10 2 D 10.3.1.2 GigabitEthernet2/0/0
10.1.1.0/30 Direct 0 0 D 10.1.1.1 GigabitEthernet1/0/0
10.1.1.1/32 Direct 0 0 D 127.0.0.1 GigabitEthernet1/0/0
10.1.1.2/32 Direct 0 0 D 10.1.1.2 GigabitEthernet1/0/0
10.2.1.0/30 OSPF 10 2 D 10.3.1.2 GigabitEthernet2/0/0
OSPF 10 2 D 10.1.1.2 GigabitEthernet1/0/0
10.3.1.0/30 Direct 0 0 D 10.3.1.1 GigabitEthernet2/0/0
10.3.1.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
10.3.1.2/32 Direct 0 0 D 10.3.1.2 GigabitEthernet2/0/0
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 配置各节点全局和接口的 MPLS 和 MPLS LDP 能力，使网络能够转发 MPLS 流量

配置 LSRA。

```
[LSRA] mpls lsr-id 1.1.1.9
[LSRA] mpls
[LSRA-mppls] quit
[LSRA] mpls ldp
[LSRA-mppls-ldp] quit
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] mpls
[LSRA-GigabitEthernet1/0/0] mpls ldp
[LSRA-GigabitEthernet1/0/0] quit
[LSRA] interface gigabitethernet 2/0/0
[LSRA-GigabitEthernet2/0/0] mpls
[LSRA-GigabitEthernet2/0/0] mpls ldp
[LSRA-GigabitEthernet2/0/0] quit
```

配置 LSRB。

```
[LSRB] mpls lsr-id 2.2.2.9
[LSRB] mpls
[LSRB-mppls] quit
[LSRB] mpls ldp
[LSRB-mppls-ldp] quit
[LSRB] interface gigabitethernet 1/0/0
[LSRB-GigabitEthernet1/0/0] mpls
[LSRB-GigabitEthernet1/0/0] mpls ldp
[LSRB-GigabitEthernet1/0/0] quit
[LSRB] interface gigabitethernet 2/0/0
[LSRB-GigabitEthernet2/0/0] mpls
[LSRB-GigabitEthernet2/0/0] mpls ldp
[LSRB-GigabitEthernet2/0/0] quit
```

配置 LSRC。

```
[LSRC] mpls lsr-id 3.3.3.9
[LSRC] mpls
[LSRC-mppls] quit
[LSRC] mpls ldp
[LSRC-mppls-ldp] quit
[LSRC] interface gigabitethernet 1/0/0
[LSRC-GigabitEthernet1/0/0] mpls
[LSRC-GigabitEthernet1/0/0] mpls ldp
[LSRC-GigabitEthernet1/0/0] quit
[LSRC] interface gigabitethernet 2/0/0
[LSRC-GigabitEthernet2/0/0] mpls
[LSRC-GigabitEthernet2/0/0] mpls ldp
[LSRC-GigabitEthernet2/0/0] quit
```

上述配置完成后，相邻节点之间应该建立起 LDP 会话。在各节点上执行 **display mpls ldp session** 命令可以看到显示结果中 Status 项为“Operational”。以 LSRA 的显示为例：

```
<LSRA> 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	0000:00:01	8/8
3.3.3.9:0	Operational	DU	Passive	0000:00:01	6/6

TOTAL: 2 session(s) Found.

步骤 4 在 LSRA 的接口 GigabitEthernet2/0/0 下使能 Manual LDP FRR，指定用于生成备用 LSP 的下一跳地址

配置 LSRA。

```
[LSRA] interface gigabitethernet 2/0/0
[LSRA-GigabitEthernet2/0/0] mpls ldp frr nexthop 10.1.1.2
[LSRA-GigabitEthernet2/0/0] quit
```

步骤 5 检查配置结果

上述配置完成后，在 LSRA 节点上执行 **display mpls lsp** 命令，可以看到到达 LSRC 的 LSP 上存在 Manual LDP FRR。

<LSRA> **display mpls lsp**

```
-----
LSP Information: LDP LSP
-----
```

FEC	In/Out Label	In/Out IF	Vrf Name
3.3.3.9/32	NULL/3	-/GE2/0/0	
LDP FRR	/1025	/GE1/0/0	
3.3.3.9/32	1025/3	-/GE2/0/0	
LDP FRR	/1025	/GE1/0/0	
2.2.2.9/32	NULL/3	-/GE1/0/0	
2.2.2.9/32	1024/3	-/GE1/0/0	

---结束

配置文件

- LSRA 的配置文件

```
#
sysname LSRA
#
mpls lsr-id 1.1.1.9
mpls
#
mpls ldp
#
interface GigabitEthernet1/0/0
ip address 10.1.1.1 255.255.255.252
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
ip address 10.3.1.1 255.255.255.252
mpls
mpls ldp
mpls ldp frr nexthop 10.1.1.2
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 1.1.1.9 0.0.0.0
network 10.1.1.0 0.0.0.3
network 10.3.1.0 0.0.0.3
```

```
#
return

● LSRB 的配置文件

#
sysname LSRB
#
mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
#
interface GigabitEthernet1/0/0
ip address 10.1.1.2 255.255.255.252
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
ip address 10.2.1.1 255.255.255.252
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 10.1.1.0 0.0.0.3
network 10.2.1.0 0.0.0.3
#
return

● LSRC 的配置文件

#
sysname LSRC
#
mpls lsr-id 3.3.3.9
mpls
#
mpls ldp
#
interface GigabitEthernet1/0/0
ip address 10.3.1.2 255.255.255.252
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
ip address 10.2.1.2 255.255.255.252
mpls
mpls ldp
#
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 10.3.1.0 0.0.0.3
network 10.2.1.0 0.0.0.3
#
return
```

2.17.12 配置 LDP Auto FRR 示例

介绍 LDP Auto FRR 的配置过程，包括配置全局使能 MPLS 和 MPLS LDP 以及 IS-IS Auto FRR。

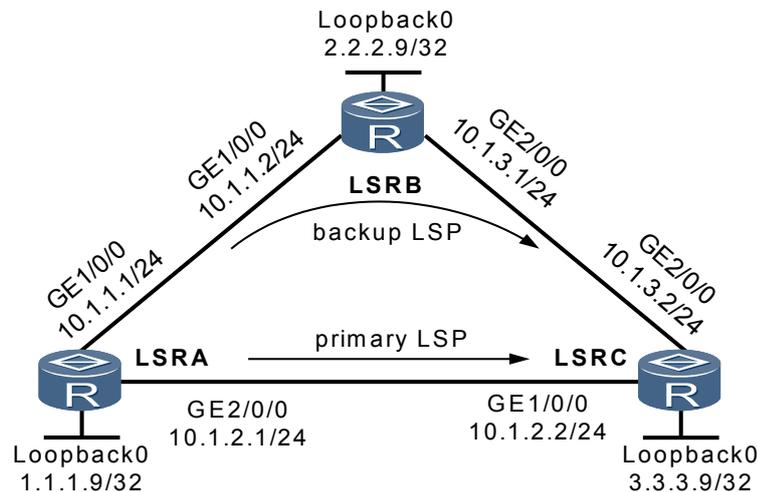
组网需求

现代网络业务对实时性的要求越来越高，例如 VoIP，在线游戏，在线视频业务等，很多业务都基于 VPN，而 VPN 业务目前通常使用 LDP 隧道。链路发生故障导致的数据丢失对这些业务造成比较严重的影响。

使用手工配置的 LDP FRR 技术，在故障发生时，可以使得公网业务流量在路由重新收敛、新的主 LSP 重新生成之前，沿着备份 LSP 转发。整个流量中断时间仅限于故障检测和切换到备份 LSP 的时间，从而使得丢包时间低于 50ms。但是路由重新收敛结束后，VPN 切换到新的主 LSP 的时间依赖于 VPN 的实现。因此 VPN 业务的流量中断时间要达到 50ms 以内，还需提高 VPN 切换到新的主 LSP 的速度。配置 LDP Auto FRR 可以解决这一问题。

如图 2-17 所示，LSRA 到 LSRC 之间存在主备 LSP，其中 LSRA→LSRC 为主用 LSP，LSRA→LSRB→LSRC 为备份 LSP。要求在主用 LSP 发生故障的时候，流量能够快速切换到备份 LSP。在 LSRA 上配置 LDP Auto FRR 功能，使能 LSRA 自动建立备份 LSP，从而实现故障时流量的快速切换，减少流量丢失。

图 2-17 配置 LDP Auto FRR 组网图



配置思路

采用如下的思路实现 LDP Auto FRR：

1. 配置各节点接口的 IP 地址以及作为 LSR ID 的 Loopback 地址。
2. 配置 IS-IS 协议发布各节点接口所连网段和 LSR ID 的主机路由。
3. 使能各节点全局和接口的 MPLS 和 MPLS LDP。
4. 在被保护流量的始发 LSR 上使能 IS-IS Auto FRR。
5. 改变 LSP 的触发策略，所有路由触发 LDP 建立 LSP。
6. 在被保护流量的始发 LSR 上配置备份 LSP 的触发策略。

数据准备

为完成此配置例，需准备如下的数据：

- 各节点接口的 IP 地址如图 2-17，IS-IS 进程号，所在的区域
- 备份 LSP 的触发建立策略

操作步骤

步骤 1 配置各接口的 IP 地址

按照图 2-17 配置各接口 IP 地址和掩码，包括 Loopback 接口，具体配置过程略。

步骤 2 配置 IS-IS 协议发布各节点接口所连网段和 LSR ID 的主机路由

配置 LSRA。

```
<LSRA> system-view
[LSRA] isis 1
[LSRA-isis-1] network-entity 10.0000.0000.0001.00
[LSRA-isis-1] quit
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] isis enable 1
[LSRA-GigabitEthernet1/0/0] quit
[LSRA] interface gigabitethernet 2/0/0
[LSRA-GigabitEthernet2/0/0] isis enable 1
[LSRA-GigabitEthernet2/0/0] quit
[LSRA] interface loopback 0
[LSRA-LoopBack0] isis enable 1
[LSRA-LoopBack0] quit
```

配置 LSRB。

```
<LSRB> system-view
[LSRB] isis 1
[LSRB-isis-1] network-entity 10.0000.0000.0002.00
[LSRB-isis-1] quit
[LSRB] interface gigabitethernet 1/0/0
[LSRB-GigabitEthernet1/0/0] isis enable 1
[LSRB-GigabitEthernet1/0/0] quit
[LSRB] interface gigabitethernet 2/0/0
[LSRB-GigabitEthernet2/0/0] isis enable 1
[LSRB-GigabitEthernet2/0/0] quit
[LSRB] interface loopback 0
[LSRB-LoopBack0] isis enable 1
[LSRB-LoopBack0] quit
```

配置 LSRC。

```
<LSRC> system-view
[LSRC] isis 1
[LSRC-isis-1] network-entity 10.0000.0000.0003.00
[LSRC-isis-1] quit
[LSRC] interface gigabitethernet 1/0/0
[LSRC-GigabitEthernet1/0/0] isis enable 1
[LSRC-GigabitEthernet1/0/0] quit
[LSRC] interface gigabitethernet 2/0/0
[LSRC-GigabitEthernet2/0/0] isis enable 1
[LSRC-GigabitEthernet2/0/0] quit
[LSRC] interface loopback 0
[LSRC-LoopBack0] isis enable 1
[LSRC-LoopBack0] quit
```

步骤 3 配置各节点全局和接口的 MPLS 和 MPLS LDP 能力，使网络能够转发 MPLS 流量，并查看 LSP 建立情况

配置 LSRA。

```
[LSRA] mpls lsr-id 1.1.1.9
[LSRA] mpls
[LSRA-mpls] quit
```

```
[LSRA] mpls ldp
[LSRA-mpls-ldp] quit
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] mpls
[LSRA-GigabitEthernet1/0/0] mpls ldp
[LSRA-GigabitEthernet1/0/0] quit
[LSRA] interface gigabitethernet 2/0/0
[LSRA-GigabitEthernet2/0/0] mpls
[LSRA-GigabitEthernet2/0/0] mpls ldp
[LSRA-GigabitEthernet2/0/0] quit
```

配置 LSRB。

```
[LSRB] mpls lsr-id 2.2.2.9
[LSRB] mpls
[LSRB-mpls] quit
[LSRB] mpls ldp
[LSRB-mpls-ldp] quit
[LSRB] interface gigabitethernet 1/0/0
[LSRB-GigabitEthernet1/0/0] mpls
[LSRB-GigabitEthernet1/0/0] mpls ldp
[LSRB-GigabitEthernet1/0/0] quit
[LSRB] interface gigabitethernet 2/0/0
[LSRB-GigabitEthernet2/0/0] mpls
[LSRB-GigabitEthernet2/0/0] mpls ldp
[LSRB-GigabitEthernet2/0/0] quit
```

配置 LSRC。

```
[LSRC] mpls lsr-id 3.3.3.9
[LSRC] mpls
[LSRC-mpls] quit
[LSRC] mpls ldp
[LSRC-mpls-ldp] quit
[LSRC] interface gigabitethernet 1/0/0
[LSRC-GigabitEthernet1/0/0] mpls
[LSRC-GigabitEthernet1/0/0] mpls ldp
[LSRC-GigabitEthernet1/0/0] quit
[LSRC] interface gigabitethernet 2/0/0
[LSRC-GigabitEthernet2/0/0] mpls
[LSRC-GigabitEthernet2/0/0] mpls ldp
[LSRC-GigabitEthernet2/0/0] quit
```

配置完成后，在 LSRA 上执行 **display mpls lsp** 命令，查看已经建立的 LSP。

```
[LSRA] display mpls lsp
```

```
-----
LSP Information: LDP LSP
-----
FEC                In/Out Label  In/Out IF                Vrf Name
2.2.2.9/32         NULL/3        -/GE1/0/0
2.2.2.9/32         1024/3        -/GE1/0/0
3.3.3.9/32         NULL/3        -/GE2/0/0
3.3.3.9/32         1025/3        -/GE2/0/0
```

从显示信息可以看到，缺省情况下，32 位的主机路由触发 LDP 建立了 LSP。

步骤 4 在 LSRA 上使能 IS-IS Auto FRR，并查看路由信息，以及备份 LSP 的建立情况。

在 LSRA 上使能 IS-IS Auto FRR。

```
[LSRA] isis
[LSRA-isis-1] frr
[LSRA-isis-1-frr] loop-free-alternate
[LSRA-isis-1-frr] quit
[LSRA-isis-1] quit
```

查看 LSRA 到 LSRC 之间直连链路的路由信息。

```
[LSRA] display ip routing-table 10.1.2.0 verbose

Route Flags: R - relay, D - download to fib
-----
Routing Table : Public
Summary Count : 1

Destination: 10.1.2.0/24
  Protocol: ISIS                Process ID: 1
  Preference: 15                Cost: 0
  NextHop: 10.1.2.2            Neighbour: 0.0.0.0
  State: Active Adv            Age: 00h05m38s
  Tag: 0                        Priority: high
  Label: NULL                   QoSInfo: 0x0
  IndirectID: 0x0
  RelayNextHop: 0.0.0.0        Interface: GigabitEthernet2/0/0
  TunnelID: 0x0                Flags: D
  BkNextHop: 10.1.1.2          BkInterface: GigabitEthernet1/0/0
  BkLabel: NULL                SecTunnelID: 0x0
  BkPETunnelID: 0x0           BkPESecTunnelID: 0x0
  BkIndirectID: 0x0
```

从显示信息可以看到，由于使能了 IS-IS Auto FRR，IS-IS 生成了一条备份路由。

在 LSRA 上执行 **display mpls lsp** 命令，查看 LSP 的建立情况。

```
[LSRA] display mpls lsp
-----
LSP Information: LDP LSP
-----
FEC                In/Out Label  In/Out IF          Vrf Name
2.2.2.9/32         NULL/3        -/GE1/0/0
  **LDP FRR**      /1025         /GE2/0/0
2.2.2.9/32         1024/3        -/GE1/0/0
  **LDP FRR**      /1025         /GE2/0/0
3.3.3.9/32         NULL/3        -/GE2/0/0
  **LDP FRR**      /1025         /GE1/0/0
3.3.3.9/32         1025/3        -/GE2/0/0
  **LDP FRR**      /1025         /GE1/0/0
```

从显示信息可以看到，缺省情况下，32 位的备份路由触发 LDP 建立了备份 LSP。

步骤 5 配置 LSP 触发策略，所有路由触发 LDP 建立 LSP，并查看 LSP 建立情况

在 LSRC 上执行 **lsp-trigger** 命令，改变 LSP 触发策略，所有路由触发 LDP 建立 LSP。

```
[LSRC] mpls
[LSRC-mpls] lsp-trigger all
[LSRC-mpls] quit
```

在 LSRA 上执行 **display mpls lsp** 命令，查看已经建立的 LSP。

```
[LSRA] display mpls lsp
-----
LSP Information: LDP LSP
-----
FEC                In/Out Label  In/Out IF          Vrf Name
2.2.2.9/32         NULL/3        -/GE1/0/0
  **LDP FRR**      /1025         /GE2/0/0
2.2.2.9/32         1024/3        -/GE1/0/0
  **LDP FRR**      /1025         /GE2/0/0
3.3.3.9/32         NULL/3        -/GE2/0/0
  **LDP FRR**      /1025         /GE1/0/0
3.3.3.9/32         1025/3        -/GE2/0/0
  **LDP FRR**      /1025         /GE1/0/0
10.1.3.0/24      1027/3      -/GE2/0/0
```

从显示信息可以看到，24 位的路由也触发建立了 LSP。

步骤 6 配置备份 LSP 的触发策略，所有备份路由触发 LDP 建立备份 LSP

在 LSRA 上执行 **auto-frr lsp-trigger** 命令，为所有备份路由生成备份 LSP。

```
[LSRA] mpls ldp
[LSRA-mpls-ldp] auto-frr lsp-trigger all
[LSRA-mpls-ldp] quit
```

步骤 7 检查配置结果

上述配置完成后，在 LSRA 节点上执行 **display mpls lsp** 命令，查看备份 LSP 的建立情况。

```
[LSRA] display mpls lsp
```

```
-----
LSP Information: LDP LSP
-----
```

FEC	In/Out Label	In/Out IF	Vrf Name
2.2.2.9/32	NULL/3	-/GE1/0/0	
LDP FRR	/1025	/GE2/0/0	
2.2.2.9/32	1024/3	-/GE1/0/0	
LDP FRR	/1025	/GE2/0/0	
3.3.3.9/32	NULL/3	-/GE2/0/0	
LDP FRR	/1025	/GE1/0/0	
3.3.3.9/32	1025/3	-/GE2/0/0	
LDP FRR	/1025	/GE1/0/0	
10.1.3.0/24	1027/3	-/GE2/0/0	
LDP FRR	/1027	/GE1/0/0	

从显示信息可以看到，已经建立了从 LSRA 到达 LSRC 之间直连链路的主 LSP 的备份 LSP。

----结束

配置文件

● LSRA 的配置文件

```
#
 sysname LSRA
#
 mpls lsr-id 1.1.1.9
 mpls
#
 mpls ldp
 auto-frr lsp-trigger all
#
 isis 1
 frr
  loop-free-alternate level-1
  loop-free-alternate level-2
 network-entity 10.0000.0000.0001.00
#
 interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
 interface GigabitEthernet2/0/0
 ip address 10.1.2.1 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
```

```
interface NULL0
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
 isis enable 1
#
return
```

● LSRB 的配置文件

```
#
 sysname LSRB
#
 mpls lsr-id 2.2.2.9
 mpls
#
 mpls ldp
#
 isis 1
  network-entity 10.0000.0000.0002.00
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 ip address 10.1.3.1 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
interface NULL0
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
 isis enable 1
#
return
```

● LSRC 的配置文件

```
#
 sysname LSRC
#
 mpls lsr-id 3.3.3.9
 mpls
  lsp-trigger all
#
 mpls ldp
#
 isis 1
  network-entity 10.0000.0000.0003.00
#
interface GigabitEthernet1/0/0
 ip address 10.1.2.2 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 ip address 10.1.3.2 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
interface NULL0
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
 isis enable 1
```

```
#
return
```

2.17.13 配置 LDP 和 IGP 同步示例

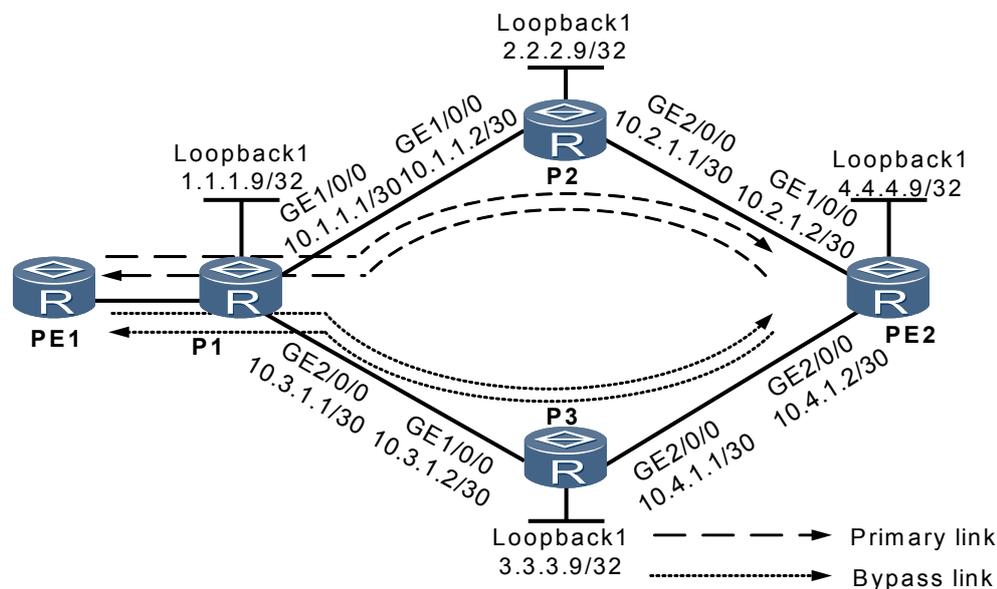
介绍配置 LDP 和 IGP 同步的配置过程，包括在各设备以及各接口使能 MPLS、MPLS LDP，以及在主备链路的分叉节点和主链路上的 LDP 邻居节点之间的链路两端接口上进行相关配置。

组网需求

如图 2-18 所示，在 PE1 到 PE2 之间建立两条链路，PE1→P1→P2→PE2 为主链路，PE1→P1→P3→PE2 为备份链路。

在主备链路的分叉节点 P1 和主链路上的 LDP 邻居节点 P2 之间的链路两端接口上配置 LDP 和 IGP 同步功能。当主链路故障后恢复时，能够缩短流量从备份链路切换到主链路的时间间隔，将该中断时间控制在毫秒级。

图 2-18 配置 LDP 和 IGP 同步组网图



配置思路

采用如下的思路实现 LDP 和 IGP 同步：

1. 在相邻节点之间及 P1 到 PE2 之间建立 LDP 会话。
2. 在主备链路的分叉节点 P1 和主链路上的 LDP 邻居节点 P2 之间的链路两端接口上使能 LDP 和 IGP 同步功能。
3. 在主备链路的分叉节点 P1 和主链路上的 LDP 邻居节点 P2 之间的链路两端接口上设置定时器 hold-down、hold-max-cost 和 delay 的值。

数据准备

为完成此配置例，需准备如下的数据：

- 各节点接口的 IP 地址如图 2-18，OSPF 进程号，所在的区域
- 定时器 hold-down、hold-max-cost 和 delay 的值

操作步骤

步骤 1 配置各接口的 IP 地址

按照图 2-18 配置各接口 IP 地址和掩码，包括 Loopback 接口，并使用 OSPF 协议通告各接口所连网段和 LSR ID 主机路由，具体配置过程略。

其中 PE1→P1→P2→PE2 为主链路，PE1→P1→P3→PE2 为备份链路，P1 的接口 GigabitEthernet2/0/0 的 cost 值为 1000。

上述配置完成后，在各节点上执行 **display ip routing-table** 命令，可以看到相互之间都学到了到达彼此的路由，且 P1 的路由的出接口为 GigabitEthernet1/0/0。以 P1 的显示为例：

```
<P1> display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
  Destinations : 14      Routes : 14
Destination/Mask    Proto Pre  Cost   Flags NextHop         Interface
1.1.1.9/32         Direct 0     0      D    127.0.0.1         LoopBack1
2.2.2.9/32         OSPF   10    2      D    10.1.1.2          GigabitEthernet1/0/0
3.3.3.9/32         OSPF   10    4      D    10.1.1.2          GigabitEthernet1/0/0
4.4.4.9/32         OSPF   10    3      D    10.1.1.2          GigabitEthernet1/0/0
10.1.1.0/30        Direct 0     0      D    10.1.1.1          GigabitEthernet1/0/0
10.1.1.1/32        Direct 0     0      D    127.0.0.1         Pos1/0/0
10.1.1.2/32        Direct 0     0      D    10.1.1.2          GigabitEthernet1/0/0
10.2.1.0/30        OSPF   10    2      D    10.1.1.2          GigabitEthernet1/0/0
10.3.1.0/30        Direct 0     0      D    10.3.1.1          GigabitEthernet2/0/0
10.3.1.1/32        Direct 0     0      D    127.0.0.1         Pos2/0/0
10.3.1.2/32        Direct 0     0      D    10.3.1.2          GigabitEthernet2/0/0
10.4.1.0/30        OSPF   10    3      D    10.1.1.2          GigabitEthernet1/0/0
127.0.0.0/20       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 2 使能各节点全局和各接口的 MPLS 和 MPLS LDP

配置 P1。

```
<P1> system-view
[P1] mpls lsr-id 1.1.1.9
[P1] mpls
[P1-mpls] quit
[P1] mpls ldp
[P1-mpls-ldp] quit
[P1] interface gigabitethernet 1/0/0
[P1-GigabitEthernet1/0/0] mpls
[P1-GigabitEthernet1/0/0] mpls ldp
[P1-GigabitEthernet1/0/0] quit
[P1] interface gigabitethernet 2/0/0
[P1-GigabitEthernet2/0/0] mpls
[P1-GigabitEthernet2/0/0] mpls ldp
[P1-GigabitEthernet2/0/0] quit
```

配置 P2。

```
<P2> system-view
[P2] mpls lsr-id 2.2.2.9
[P2] mpls
[P2-mpls] quit
[P2] mpls ldp
[P2-mpls-ldp] quit
[P2] interface gigabitethernet 1/0/0
```

```
[P2-GigabitEthernet1/0/0] mpls
[P2-GigabitEthernet1/0/0] mpls ldp
[P2-GigabitEthernet1/0/0] quit
[P2] interface gigabitethernet 2/0/0
[P2-GigabitEthernet2/0/0] mpls
[P2-GigabitEthernet2/0/0] mpls ldp
[P2-GigabitEthernet2/0/0] quit
```

配置 P3。

```
<P3> system-view
[P3] mpls lsr-id 3.3.3.9
[P3] mpls
[P3-mpls] quit
[P3] mpls ldp
[P3-mpls-ldp] quit
[P3] interface gigabitethernet 1/0/0
[P3-GigabitEthernet1/0/0] mpls
[P3-GigabitEthernet1/0/0] mpls ldp
[P3-GigabitEthernet1/0/0] quit
[P3] interface gigabitethernet 2/0/0
[P3-GigabitEthernet2/0/0] mpls
[P3-GigabitEthernet2/0/0] mpls ldp
[P3-GigabitEthernet2/0/0] quit
```

配置 PE2。

```
<PE2> system-view
[PE2] mpls lsr-id 4.4.4.9
[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
[PE2] interface gigabitethernet 2/0/0
[PE2-GigabitEthernet2/0/0] mpls
[PE2-GigabitEthernet2/0/0] mpls ldp
[PE2-GigabitEthernet2/0/0] quit
```

上述配置完成后，相邻节点之间应该建立起 LDP 会话。在各节点上执行 **display mpls ldp session** 命令可以看到显示结果中 Status 项为“Operational”。以 P1 的显示为例：

```
<P1> 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	0000:00:56	227/227
3.3.3.9:0	Operational	DU	Passive	0000:00:56	227/227

TOTAL: 2 session(s) Found.

步骤 3 在主备链路的分叉节点 P1 和主链路上的 LDP 邻居节点 P2 之间的链路两端接口上使能 LDP 和 IGP 同步功能

配置 P1。

```
<P1> system-view
[P1] interface gigabitethernet 1/0/0
[P1-GigabitEthernet1/0/0] ospf ldp-sync
[P1-GigabitEthernet1/0/0] quit
```

配置 P2。

```
<P2> system-view
```

```
[P2] interface gigabitethernet 1/0/0
[P2-GigabitEthernet1/0/0] ospf ldp-sync
[P2-GigabitEthernet1/0/0] quit
```

步骤 4 在主备链路的分叉节点 P1 和主链路上的 LDP 邻居节点 P2 之间的链路两端接口上配置定时器 hold-down 的值

配置 P1。

```
<P1> system-view
[P1] interface gigabitethernet 1/0/0
[P1-GigabitEthernet1/0/0] ospf timer ldp-sync hold-down 8
[P1-GigabitEthernet1/0/0] quit
```

配置 P2。

```
<P2> system-view
[P2] interface gigabitethernet 1/0/0
[P2-GigabitEthernet1/0/0] ospf timer ldp-sync hold-down 8
[P2-GigabitEthernet1/0/0] quit
```

步骤 5 在主备链路的分叉节点 P1 和主链路上的 LDP 邻居节点 P2 之间的链路两端接口上配置定时器 hold-max-cost 的值

配置 P1。

```
<P1> system-view
[P1] interface gigabitethernet 1/0/0
[P1-GigabitEthernet1/0/0] ospf timer ldp-sync hold-max-cost 9
[P1-GigabitEthernet1/0/0] quit
```

配置 P2。

```
<P2> system-view
[P2] interface gigabitethernet 1/0/0
[P2-GigabitEthernet1/0/0] ospf timer ldp-sync hold-max-cost 9
[P2-GigabitEthernet1/0/0] quit
```

步骤 6 在主备链路的分叉节点 P1 和主链路上的 LDP 邻居节点 P2 之间的链路两端接口上配置定时器 delay 的值

配置 P1。

```
<P1> system-view
[P1] interface gigabitethernet 1/0/0
[P1-GigabitEthernet1/0/0] mpls ldp timer igp-sync-delay 6
[P1-GigabitEthernet1/0/0] quit
```

配置 P2。

```
<P2> system-view
[P2] interface gigabitethernet 1/0/0
[P2-GigabitEthernet1/0/0] mpls ldp timer igp-sync-delay 6
[P2-GigabitEthernet1/0/0] quit
```

步骤 7 检查配置结果

上述配置完成后，在 P1 节点上执行 **display ospf ldp-sync** 命令，可以看到接口状态为“Sync-Achieved”。

```
<P1> display ospf ldp-sync interface gigabitethernet 1/0/0
Interface GigabitEthernet1/0/0
HoldDown Timer: 8          HoldMaxCost Timer: 9
LDP State: Up              OSPF Sync State: Sync-Achieved
```

----结束

配置文件

- P1 的配置文件

```
#
 sysname P1
#
 mpls lsr-id 1.1.1.9
 mpls
#
 mpls ldp
#
 interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.252
 ospf ldp-sync
 ospf timer ldp-sync hold-down 8
 ospf timer ldp-sync hold-max-cost 9
 mpls
 mpls ldp
 mpls ldp timer igp-sync-delay 6
#
 interface GigabitEthernet2/0/0
 ip address 10.3.1.1 255.255.255.252
 ospf cost 1000
 mpls
 mpls ldp
#
 interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
 ospf 1
 area 0.0.0.0
 network 1.1.1.9 0.0.0.0
 network 10.1.1.0 0.0.0.3
 network 10.3.1.0 0.0.0.3
#
 return
```

- P2 的配置文件

```
#
 sysname P2
#
 mpls lsr-id 2.2.2.9
 mpls
#
 mpls ldp
#
 interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.252
 ospf ldp-sync
 ospf timer ldp-sync hold-down 8
 ospf timer ldp-sync hold-max-cost 9
 mpls
 mpls ldp
 mpls ldp timer igp-sync-delay 6
#
 interface GigabitEthernet2/0/0
 ip address 10.2.1.1 255.255.255.252
 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 10.1.1.0 0.0.0.3
 network 10.2.1.0 0.0.0.3
#
```

```
return
```

- P3 的配置文件

```
#
sysname P3
#
mpls lsr-id 3.3.3.9
mpls
#
mpls ldp
#
interface GigabitEthernet1/0/0
ip address 10.3.1.2 255.255.255.252
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
ip address 10.4.1.1 255.255.255.252
mpls
mpls ldp
#
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 10.3.1.0 0.0.0.3
network 10.4.1.0 0.0.0.3
#
return
```

- PE2 的配置文件

```
#
sysname PE2
#
mpls lsr-id 4.4.4.9
mpls
#
mpls ldp
#
interface GigabitEthernet1/0/0
ip address 10.2.1.2 255.255.255.252
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
ip address 10.4.1.2 255.255.255.252
mpls
mpls ldp
#
interface LoopBack1
ip address 4.4.4.9 255.255.255.255
#
#
ospf 1
area 0.0.0.0
network 4.4.4.9 0.0.0.0
network 10.2.1.0 0.0.0.3
network 10.4.1.0 0.0.0.3
#
return
```

2.17.14 配置 LDP 和静态路由同步示例

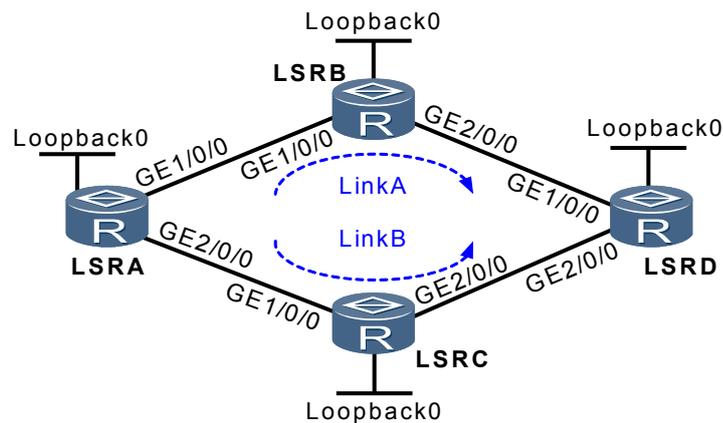
LDP 和静态路由同步功能主要用来解决依赖静态路由建立的 LSP 存在主备链路的组网中，主链路正切和回切过程中导致的 MPLS 流量丢失问题。

组网需求

在存在主备 LSP 的 MPLS 组网中，LSR 之间依靠静态路由建立 LSP，当主链路的 LDP 会话故障（非链路故障导致）时，或者主链路故障后再恢复时，由于静态路由和 LDP 的不同步，都会导致 MPLS 流量的中断（短时中断）。

如图 2-19 所示，LSRA 有分别经过 LSRB 和 LSRC 到 LSRD 的静态路由，并基于静态路由建立了 LDP 会话，其中 LinkA 为主用链路，LinkB 为备用链路。现通过配置 LDP 和静态路由同步功能，使得 LinkA 上的 LDP 会话中断或者 LinkA 发生故障再恢复的情况下，保证 MPLS 流量不中断。

图 2-19 配置 LDP 和静态路由同步组网图



路由器	接口	IP 地址	路由器	接口	IP 地址
LSRA	GE 1/0/0	10.1.1.1/30	LSRC	GE 1/0/0	20.1.1.2/30
	GE 2/0/0	20.1.1.1/30		GE 2/0/0	40.1.1.2/30
	Loopback0	1.1.1.1/32		Loopback0	3.3.3.3/32
LSRB	GE 1/0/0	10.1.1.2/30	LSRD	GE 1/0/0	30.1.1.2/30
	GE 2/0/0	30.1.1.1/30		GE 2/0/0	40.1.1.2/30
	Loopback0	2.2.2.2/32		Loopback0	4.4.4.4/32

配置思路

采用如下的思路配置 LDP 和静态路由同步：

1. 各 LSR 上配置到其他 LSR 的静态路由，使网络互通。
2. LSR 的全局及接口下使能 MPLS、MPLS LDP 能力。
3. 使能 LDP 和静态路由同步能力，并检查配置结果。

数据准备

为完成此配置例，需准备如下的数据：

- LSR 各接口的 IP 地址。

- LSR 的 MPLS LSR-ID。
- hold-down 定时器的值。

操作步骤

步骤 1 配置各接口的 IP 地址

根据图 2-19 配置各接口的 IP 地址，具体配置过程略。

步骤 2 在各节点上配置静态路由，使网络互通

LSRA 上配置到 LSRD 的两条优先级不同的静态路由，同时 LSRD 上也相应配置到 LSRA 的两条优先级不同的静态路由。

配置 LSRA。

```
[LSRA] ip route-static 2.2.2.2 32 10.1.1.2
[LSRA] ip route-static 3.3.3.3 32 20.1.1.2
[LSRA] ip route-static 30.1.1.1 30 10.1.1.2
[LSRA] ip route-static 40.1.1.1 30 20.1.1.2
[LSRA] ip route-static 4.4.4.4 32 10.1.1.2 preference 40
[LSRA] ip route-static 4.4.4.4 32 20.1.1.2 preference 60
```

配置 LSRB。

```
[LSRB] ip route-static 1.1.1.1 32 10.1.1.1
[LSRB] ip route-static 4.4.4.4 32 30.1.1.1
```

配置 LSRC。

```
[LSRC] ip route-static 1.1.1.1 32 20.1.1.1
[LSRC] ip route-static 4.4.4.4 32 40.1.1.1
```

配置 LSRD。

```
[LSRD] ip route-static 2.2.2.2 32 30.1.1.2
[LSRD] ip route-static 3.3.3.3 32 40.1.1.2
[LSRD] ip route-static 10.1.1.2 30 30.1.1.2
[LSRD] ip route-static 20.1.1.2 30 40.1.1.2
[LSRD] ip route-static 1.1.1.1 32 30.1.1.2 preference 40
[LSRD] ip route-static 1.1.1.1 32 40.1.1.2 preference 60
```

配置完成后，在各节点上执行 **display ip routing-table protocol static** 命令可以查看到配置的静态路由。以 LSRA 为例：

```
[LSRA] display ip routing-table protocol static
Route Flags: R - relay, D - download to fib
```

```
-----
Public routing table : Static
  Destinations : 5      Routes : 6      Configured Routes : 6
```

```
Static routing table status : <Active>
  Destinations : 5      Routes : 5
```

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
2.2.2.2/32	Static	60	0	D	10.1.1.1	GigabitEthernet1/0/0
3.3.3.3/32	Static	60	0	D	20.1.1.1	GigabitEthernet2/0/0
4.4.4.4/32	Static	40	0	D	10.1.1.1	GigabitEthernet1/0/0
30.1.1.0/30	Static	60	0	D	10.1.1.1	GigabitEthernet1/0/0
40.1.1.0/30	Static	60	0	D	20.1.1.1	GigabitEthernet2/0/0

```
Static routing table status : <Inactive>
  Destinations : 1      Routes : 1
```

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

4.4.4.4/32 Static 60 0 20.1.1.1 GigabitEthernet2/0/0

步骤 3 在各 LSR 上使能 MPLS LDP 能力，建立 LDP LSP

配置 LSRA。

```
[LSRA] mpls lsr-id 1.1.1.1
[LSRA] mpls
[LSRA-mpls] quit
[LSRA] mpls ldp
[LSRA-mpls-ldp] quit
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] mpls
[LSRA-GigabitEthernet1/0/0] mpls ldp
[LSRA-GigabitEthernet1/0/0] quit
[LSRA] interface gigabitethernet 2/0/0
[LSRA-GigabitEthernet2/0/0] mpls
[LSRA-GigabitEthernet2/0/0] mpls ldp
[LSRA-GigabitEthernet2/0/0] quit
```

LSRB、LSRC 和 LSRD 的配置与 LSRA 类似，具体配置过程请参见配置文件。

在各节点上执行 **display mpls ldp session** 命令可以看到 LDP Session 已经建立（状态为 **Operational**）。以 LSRA 为例：

```
[LSRA] display mpls ldp session
LDP Session(s) in Public Network
Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
A '*' before a session means the session is being deleted.
-----
PeerID                Status      LAM  SsnRole  SsnAge      KASent/Rcv
-----
2.2.2.2:0             Operational DU   Passive  0000:00:00  1/1
3.3.3.3:0             Operational DU   Passive  0000:00:02  12/12
-----
TOTAL: 2 session(s) Found.
```

步骤 4 在 LSRA 和 LSRD 上分别配置 LDP 和静态路由同步功能

配置 LSRA。

```
[LSRA] ip route-static 4.4.4.4 32 10.1.1.2 ldp-sync
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] static-route timer ldp-sync hold-down 20
[LSRA-GigabitEthernet1/0/0] quit
```

配置 LSRD。

```
[LSRD] ip route-static 1.1.1.1 32 30.1.1.2 ldp-sync
[LSRD] interface gigabitethernet 1/0/0
[LSRD-GigabitEthernet1/0/0] static-route timer ldp-sync hold-down 20
[LSRD-GigabitEthernet1/0/0] quit
```

步骤 5 检查配置结果

在 LSRA 上查看使能了 LDP 和静态路由同步功能的静态路由出接口的状态信息。

```
[LSRA] display static-route ldp-sync
Total number of routes enable Ldp-Sync: 1
-----
Interface GigabitEthernet1/0/0
Enable ldp-sync static routes number: 1
Static-route ldp-sync holddown timer: 20s
Sync state: Normal
Dest = 4.4.4.4, Mask = 32, NextHop = 10.1.1.1.
-----
```

可以看到，LDP 和静态路由同步功能已经配置（状态为 **Normal**）。

- 当主链路的 LDP 会话中断时，为了保证静态路由与 LSP 的同步，流量立即切换到备份链路(LinkB)来保证流量不中断。
- 当主链路(LinkA)发生故障再恢复时，下一跳为 10.1.1.1 的静态路由并不会马上被优选。只有等到 hold-down 定时器超时（20 秒），主链路的 LDP 会话建立后，才会看到下一跳为 10.1.1.1 的静态路由活跃，达到静态路由和 LDP 的同步，从而保证 MPLS 流量不中断。

---结束

配置文件

- LSRA 的配置文件

```
#
sysname LSRA
#
mpls lsr-id 1.1.1.1
mpls
#
mpls ldp
#
interface GigabitEthernet1/0/0
ip address 10.1.1.1 255.255.255.252
static-route timer ldp-sync hold-down 20
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
ip address 20.1.1.1 255.255.255.252
mpls
mpls ldp
#
interface loopback0
ip address 1.1.1.1 255.255.255.255
#
ip route-static 2.2.2.2 255.255.255.255 10.1.1.2
ip route-static 3.3.3.3 255.255.255.255 20.1.1.2
ip route-static 4.4.4.4 255.255.255.255 10.1.1.2 preference 40 ldp-sync
ip route-static 4.4.4.4 255.255.255.255 20.1.1.2 preference 60
ip route-static 30.1.1.0 255.255.255.252 10.1.1.2
ip route-static 40.1.1.0 255.255.255.252 20.1.1.2
#
return
```

- LSRB 的配置文件

```
#
sysname LSRB
#
mpls lsr-id 2.2.2.2
mpls
#
mpls ldp
#
interface GigabitEthernet1/0/0
ip address 10.1.1.2 255.255.255.252
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
ip address 30.1.1.1 255.255.255.252
mpls
mpls ldp
#
interface loopback0
ip address 2.2.2.2 255.255.255.255
#
ip route-static 1.1.1.1 255.255.255.255 10.1.1.1
ip route-static 4.4.4.4 255.255.255.255 30.1.1.1
```

```
#
return
● LSRC 的配置文件
#
sysname LSRC
#
mpls lsr-id 3.3.3.3
mpls
#
mpls ldp
#
interface GigabitEthernet1/0/0
ip address 20.1.1.2 255.255.255.252
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
ip address 40.1.1.1 255.255.255.252
mpls
mpls ldp
#
interface loopback0
ip address 3.3.3.3 255.255.255.255
#
ip route-static 1.1.1.1 255.255.255.255 20.1.1.1
ip route-static 4.4.4.4 255.255.255.255 40.1.1.1
#
return
● LSRD 的配置文件
#
sysname LSRD
#
mpls lsr-id 4.4.4.4
mpls
#
mpls ldp
#
interface GigabitEthernet1/0/0
ip address 30.1.1.2 255.255.255.252
static-route timer ldp-sync hold-down 20
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
ip address 40.1.1.2 255.255.255.252
mpls
mpls ldp
#
interface loopback0
ip address 4.4.4.4 255.255.255.255
#
ip route-static 1.1.1.1 255.255.255.255 30.1.1.2 preference 40 ldp-sync
ip route-static 1.1.1.1 255.255.255.255 40.1.1.2 preference 60
ip route-static 2.2.2.2 255.255.255.255 30.1.1.2
ip route-static 3.3.3.3 255.255.255.255 40.1.1.2
ip route-static 10.1.1.0 255.255.255.252 30.1.1.2
ip route-static 20.1.1.0 255.255.255.252 40.1.1.2
#
return
```

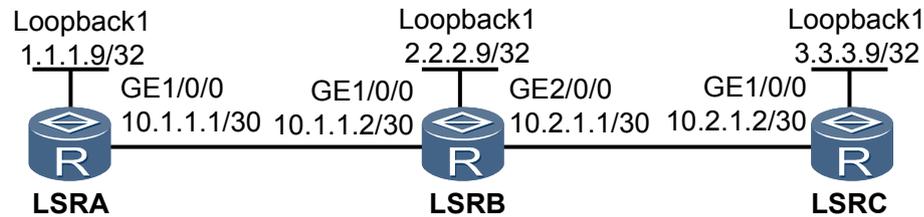
2.17.15 配置 LDP GTSM 示例

介绍配置 LDP GTSM 的配置过程，包括在各设备以及各接口使能 MPLS、MPLS LDP，以及在 LDP 对等体两节点上进行 LDP GTSM 配置。

组网需求

如图 2-20 所示。各节点间运行 MPLS 和 MPLS LDP 协议，在 LSRB 上启用 GTSM 保护功能。

图 2-20 配置 LDP GTSM 组网图



配置思路

采用如下思路配置 LDP GTSM 功能：

1. 配置 MPLS 和 MPLS LDP 基本功能
2. 在 LDP 对等体两端节点上配置 GTSM 功能

数据准备

为完成此配置示例，需要准备如下数据：

- LDP 对等体的 LSR ID
- GTSM 功能允许的最大有效跳数

操作步骤

步骤 1 配置各接口的 IP 地址（略）

步骤 2 配置 OSPF 协议发布各节点接口所连网段和 LSR ID 的主机路由（略）

步骤 3 配置各节点和接口的 MPLS 和 MPLS LDP 能力（略）

完成上述配置后，在各节点上执行 `display mpls ldp session` 命令，可以看到 LDP 会话的建立情况。以 LSRA 的显示为例：

```
<LSRA> 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 0000:00:02 9/9
-----
TOTAL: 1 session(s) Found.
```

步骤 4 配置 LDP GTSM

在 LSRA 上配置：LSRB 发送给 LSRA 的 LDP 报文的有效 TTL 范围是 253 到 255。

```
<LSRA> system-view
```

```
[LSRA] mpls ldp
[LSRA-mpls-ldp] gtsm peer 2.2.2.9 valid-ttl-hops 3
```

在 LSRB 上配置：LSRA 发送给 LSRB 的 LDP 报文的有效 TTL 范围是 252 到 255；LSRC 发送给 LSRB 的 LDP 报文的有效 TTL 范围是 251 到 255。

```
<LSRB> system-view
[LSRB] mpls ldp
[LSRB-mpls-ldp] gtsm peer 1.1.1.9 valid-ttl-hops 4
[LSRB-mpls-ldp] gtsm peer 3.3.3.9 valid-ttl-hops 5
```

在 LSRC 上配置：LSRB 发送给 LSRC 的 LDP 报文的有效 TTL 范围是 250 到 255。

```
<LSRC> system-view
[LSRC] mpls ldp
[LSRC-mpls-ldp] gtsm peer 2.2.2.9 valid-ttl-hops 6
```

此时如果主机 PC 模拟 LSRA 的 LDP 协议报文对 LSRB 进行攻击，由于该报文到达 LSRB 时，TTL 值不在 252 ~ 255 范围内，所以被丢弃。在 LSRB 的 GTSM 统计信息中丢弃的报文数也会相应的增加。

----结束

配置文件

- LSRA 的配置文件

```
#
sysname LSRA
#
mpls lsr-id 1.1.1.9
mpls
#
mpls ldp
gtsm peer 2.2.2.9 valid-ttl-hops 3
#
interface GigabitEthernet1/0/0
ip address 10.1.1.1 255.255.255.252
mpls
mpls ldp
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 1.1.1.9 0.0.0.0
network 10.1.1.0 0.0.0.3
#
return
```

- LSRB 的配置文件

```
#
sysname LSRB
#
mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
gtsm peer 1.1.1.9 valid-ttl-hops 4
gtsm peer 3.3.3.9 valid-ttl-hops 5
#
interface GigabitEthernet1/0/0
ip address 10.1.1.2 255.255.255.252
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
```

```
ip address 10.2.1.1 255.255.255.252
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 10.1.1.0 0.0.0.3
network 10.2.1.0 0.0.0.3
#
return
```

● LSRC 的配置文件

```
#
sysname LSRC
#
mpls lsr-id 3.3.3.9
mpls
#
mpls ldp
gtsm peer 2.2.2.9 valid-ttl-hops 6
#
interface GigabitEthernet1/0/0
ip address 10.2.1.2 255.255.255.252
mpls
mpls ldp
#
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 10.2.1.0 0.0.0.3
#
return
```

3 MPLS TE 配置

关于本章

MPLS TE 隧道主要用于承载 MPLS L2VPN（VLL 和 VPLS）和 MPLS L3VPN 业务，使得 VPN 业务不仅有良好的安全性，而且有可靠的 QoS 保证。

3.1 MPLS TE 简介

MPLS TE 结合了 MPLS 技术与流量工程，从而解决由于负载不均衡导致的拥塞。

3.2 配置静态 CR-LSP

配置静态 CR-LSP 的过程比较简单，手工分配标签，不使用信令协议，不需要交互控制报文，因此消耗资源比较小。

3.3 配置 RSVP-TE 隧道

RSVP-TE 隧道是 MPLS TE 隧道的一种，是配置 MPLS TE 的所有高级特性和应用的基础。

3.4 调整 RSVP 信令参数

RSVP-TE 提供了丰富的信令参数，能够满足用户对于可靠性、网络资源、以及一些 MPLS TE 高级特性的应用。

3.5 配置 RSVP 认证

RSVP 认证用来防止非授权的节点与本节点进行 RSVP 邻居的建立和防止通过构造报文来达到欺骗的目的。

3.6 调整 CR-LSP 的路径选择

介绍调整 CR-LSP 路径计算和选择的几种方式。

3.7 调整 MPLS TE 隧道的建立

MPLS TE 提供多种属性，用于灵活调整 TE 隧道的建立。

3.8 调整流量的转发

调整 MPLS TE 流量的转发，可能导致 IP 流量或 MPLS 流量经过的路径变化、或限制 TE 隧道流量类型的配置。

3.9 调整带宽的泛洪阈值

通过调整带宽的泛洪阈值，可以抑制更新 TEDB 和泛洪的频率，避免对网络资源造成浪费。

3.10 配置 TE 隧道流量限速

如果要使 TE 流量被限定在实际配置的隧道带宽范围内，则需要对该 TE 隧道配置 TE 流量限速。

3.11 配置手工 TE FRR

手工 TE FRR 是 MPLS TE 中的一种局部性保护机制，用于保护主隧道的链路和节点故障，需要用户手工配置旁路隧道。

3.12 配置 MPLS TE Auto FRR

MPLS TE Auto FRR 是 MPLS TE 中的一种局部性保护机制，用于保护 CR-LSP 的链路和节点故障，用户无需手工配置。

3.13 配置 CR-LSP 备份

通过配置 CR-LSP 备份，可以实现对 CR-LSP 端到端的保护。

3.14 配置旁路保护隧道与备份 CR-LSP 同步

介绍当主 CR-LSP 故障后，系统启用 TE FRR 旁路保护隧道并尝试恢复主 CR-LSP 的同时，也尝试创建备份 CR-LSP 的配置方法。

3.15 配置 RSVP GR

介绍 RSVP TE GR 的配置方法，即介绍使 TE 隧道节点在主备倒换时维持 RSVP 邻居会话的配置方法。

3.16 配置静态 BFD for CR-LSP

介绍静态 BFD 检测静态 CR-LSP 或 RSVP CR-LSP 链路故障的配置方法。

3.17 配置静态 BFD for TE

介绍了静态 BFD 检测 TE 隧道故障的配置方法。

3.18 配置动态 BFD for CR-LSP

介绍动态 BFD 检测静态 CR_LSP 或 RSVP CR-LSP 链路故障的配置方法。

3.19 配置动态 BFD for RSVP

介绍动态 BFD 检测 RSVP 邻居之间的链路故障的配置方法。

3.20 维护 MPLS TE

介绍如何清除 MPLS TE 运行信息。

3.21 配置举例

介绍 MPLS TE 的各种组网举例。配置示例中包括组网需求、配置注意事项、配置思路等。

3.1 MPLS TE 简介

MPLS TE 结合了 MPLS 技术与流量工程，从而解决由于负载不均衡导致的拥塞。

3.1.1 MPLS TE 概述

MPLS TE 通过在建立隧道时进行资源预留，使网络流量绕开拥塞节点，达到平衡网络流量的目的。

流量工程

网络拥塞是影响骨干网络性能的主要问题。拥塞的原因可能是网络资源不足，也可能是网络资源负载不均衡。流量工程用于防止网络拥塞与优化网络资源。

流量工程通过动态监控网络的流量和网络单元的负载，实时调整流量管理参数、路由参数和资源约束参数等，优化网络资源的使用，避免负载不均衡导致的拥塞。

MPLS TE

MPLS TE (Multiprotocol Label Switching Traffic Engineering) 结合了 MPLS (Multiprotocol Label Switching) 技术与流量工程，通过建立到达指定路径的 LSP (Label Switched Path) 隧道进行资源预留，使网络流量绕开拥塞节点，达到平衡网络流量的目的。

在资源紧张的情况下，高优先级 LSP 可以抢占低优先级 LSP 的带宽等资源，优先满足高优先级业务的需求。

同时，当 LSP 隧道故障或网络的某一节点发生拥塞时，MPLS TE 可以通过快速重路由 FRR (Fast ReRoute) 和备份路径，提供保护。

使用 MPLS TE，网络管理员只需要建立一些 LSP 就可以消除网络拥塞。随着 LSP 数量的增长，还可以使用特定的离线工具进行流量分析。

3.1.2 AR1200 支持的 MPLS TE 特性

系统中支持的 MPLS TE 特性包括：静态 MPLS TE 隧道、RSVP-TE 隧道和 MPLS TE 可靠性。

说明

本文简单介绍 AR1200 支持的 MPLS TE 特性。MPLS TE 特性详细介绍请参见《Huawei AR1200 系列企业路由器 特性描述-MPLS》中的“MPLS TE”一章。

静态 MPLS TE 隧道

静态 TE 隧道中的标签是由手工分配，不使用信令协议，不需要交互控制报文。如果设备性能较低，网络相对稳定，可考虑部署静态 MPLS TE 隧道。

静态 MPLS TE 隧道的 CR-LSP 优先级最高，因此带宽不会被抢占。同时静态 TE 隧道的 CR-LSP 也不会抢占其他任何类型的 LSP。

RSVP-TE 隧道

RSVP-TE 隧道使用 RSVP-TE 信令协议建立，可以根据网络变化动态改变。

下面分类介绍 AR1200 实现的 RSVP-TE 特性：

- 链路信息收集和发布
RSVP-TE 使用扩展的 IGP（OSPF-TE 和 ISIS-TE）来收集和发布 TE 链路信息，建立 TEDB 数据库。扩展的 IGP 除了周期性对链路进行泛洪，在链路生效或失效时、链路属性发生变化时，以及链路可预留带宽变化达到一定程度时都会进行泛洪。用户可通过命令调整泛洪阈值。
- 路径计算
AR1200 支持使用 CSPF 计算 TE 隧道的路径。当遇到多条权值相同的路径时，会根据跳数和用户配置的仲裁策略，选择其中的一条。
用户可以配置链路的可预留带宽、管理组属性等，并可以指定隧道的如下属性：
 - 隧道带宽
 - 亲和属性
 - 显式路径
 - 最大跳数限制值
 - SRLG（Shared Risk Link Group）
- 隧道的建立
用户可以通过配置决定 RSVP-TE 隧道在建立过程中是否记录路由和标签，是否进行环路检测；如果资源不足，根据建立优先级（Setup Priority）和保持优先级（Holding Priority）决定是否抢占。
如果隧道建立不成功，系统会每隔一定时间尝试重建。
- 信令机制
AR1200 支持使用 RSVP-TE 进行资源预留，支持 FF（Fixed Filter）和 SE（Shared-Explicit）两种预留风格。AR1200 支持 RSVP 扩展机制，例如，RSVP 消息的确认和重传机制、摘要刷新、Hello 机制，用于减轻网络负载、提供网络可靠性。此外，AR1200 支持 RSVP 认证，用于提高网络安全性。
- 流量转发
用户可通过配置策略路由将 VPN 流量引入 TE 隧道，通过配置静态路由、策略路由、IGP Shortcut 或转发邻接，将非 VPN 流量引入 TE 隧道。

可靠性

CR-LSP 备份提供的是一种端到端的保护机制，通常需要与其他快速检测或保护机制配合使用，以确保流量能够快速切换，避免流量丢失。

- CR-LSP 备份与 TE FRR 配合使用
TE FRR 是一种局部保护措施，只能保护 CR-LSP 中的某条链路和某个节点，而且切换速度快。而 CR-LSP 备份是一种端到端的路径保护，提供整条 LSP 的保护。CR-LSP 备份可以分为 CR-LSP 热备份与 CR-LSP 普通备份，每种备份形式都可以与 TE FRR 配合使用：
 - CR-LSP 热备份与 TE FRR 配合使用：快速重路由可以及时响应链路故障，将流量在最短的时间内切换到旁路隧道上。链路故障信息通过信令带到入口节点，然后将流量切换到备份 CR-LSP 上。
 - CR-LSP 普通备份与 TE FRR 配合使用：快速重路由可以及时响应链路故障，将流量在最短的时间内切换到旁路隧道上。当 TE FRR 的主隧道和旁路隧道同时出现故障时，将流量切换到备份 CR-LSP 上。
- CR-LSP 备份与 BFD 配合使用

TE FRR 只能检测某条直连链路或者某个节点的故障，而 BFD 能够实现对整条 CR-LSP 的快速检测。BFD 只能用于检测热备份模式 CR-LSP。当 BFD 检测到当前隧道故障时，能够快速将流量切换到热备份 CR-LSP，或者快速将流量回切到主隧道。

AR1200 支持以下 TE 隧道的可靠性保护措施：

- TE FRR

TE FRR 为网络提供了一种快速的局部保护功能。它一般部署在对可靠性要求比较高的网络中，当网络中出现链路或节点故障时，流量能够快速切换到保护隧道，从而对业务的影响较小。TE FRR 分为手工重路由和自动重路由两种方式。

 说明

由于 FRR 使用的旁路隧道需要预先建立，占用额外的带宽，因此，在网络带宽余量不多的情况下，应该只对关键的接口或链路进行 TE FRR 保护。

- CR-LSP 备份

在对业务可靠性要求较高的网络中，通常会配置备份 CR-LSP 来提供端到端的保护，提高网络的可靠性。当主 CR-LSP 故障时，流量能够及时切换到备份 CR-LSP 上，确保用户业务不中断。

CR-LSP 支持热备份模式和普通备份模式。为了增强可靠性，当备份模式失效后，还提供了逃生路径模式。CR-LSP 备份和逃生路径模式建立方式不同：

- 热备份模式：系统在建立主 CR-LSP 的同时，会创建一条与主 CR-LSP 路径分离的备份 CR-LSP。
- 普通备份模式：当主 CR-LSP 失效后，系统将使用其他显式路径建立备份 CR-LSP。
- 逃生路径模式：当主 CR-LSP 和备份 CR-LSP 都失效后，系统将使用剩余的路径建立逃生路径。

- BFD

BFD 能对 CR-LSP 链路实现毫秒级别的缺陷检测。在没有硬件检测机制而需要提供快速故障检测的情况下，可考虑使用 BFD 检测，减少故障感知时间。

AR1200 支持 BFD 检测热备份模式 CR-LSP 和隧道保护组。

- RSVP GR

RSVP GR 是 RSVP TE 的一种状态恢复机制。当控制平面因故障和人为的操作进行主备倒换时，RSVP GR 可以保证转发平面上的数据传输不会中断，并恢复控制平面的 RSVP-TE LSP 的正常状态。AR1200 支持 GR 期间进行快速重路由。

 说明

AR1200 只能作为 Helper 路由器，不能作为 Restarter 路由器。

3.2 配置静态 CR-LSP

配置静态 CR-LSP 的过程比较简单，手工分配标签，不使用信令协议，不需要交互控制报文，因此消耗资源比较小。

3.2.1 建立配置任务

在配置静态 CR-LSP 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

配置静态 CR-LSP 的过程比较简单，手工分配标签，不使用信令协议，不需要交互控制报文，因此消耗资源比较小，且不涉及 IGP TE 扩展或 CSPF。但静态 CR-LSP 不能根据网络的变化动态调整，因此实际应用有限。

静态 CR-LSP 作为一种特殊的静态 LSP，其配置限制条件与静态 LSP 类似。

前置任务

在配置静态 CR-LSP 之前，需完成以下任务：

- 配置单播静态路由或 IGP 协议，保证各 LSR 在网络层互通
- 配置各 LSR 的 LSR-ID
- 在各 LSR 节点上全局和接口下使能 MPLS

数据准备

在配置静态 CR-LSP 之前，需要准备以下数据。

序号	数据
1	静态 CR-LSP 经过的节点
2	静态 CR-LSP 沿途各 LSR 上的出标签的值
3	隧道接口的接口编号、Tunnel ID、目的地址
4	静态 CR-LSP 的目的地址
5	静态 CR-LSP 入节点的下一跳地址或出接口
6	静态 CR-LSP 中间节点的入接口、下一跳地址或出接口
7	静态 CR-LSP 出节点的入接口
8	静态 CR-LSP 入节点和中间节点链路上的带宽

说明

- 每个节点出标签的值就是其下一个节点入标签的值。
- 静态 CR-LSP 的目的地址取 Tunnel 接口的目的地址。

3.2.2 使能 MPLS TE

使能 MPLS TE 是配置静态 CR-LSP 的首要步骤。

背景信息

在静态 CR-LSP 的各节点上进行如下配置。

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 **mpls**，进入 MPLS 视图。

步骤 3 执行命令 **mpls te**，全局使能本节点的 MPLS TE。

需先在 MPLS 视图下全局使能 MPLS TE，然后才能在各个相应接口下使能 MPLS TE。

步骤 4 执行命令 **quit**，退回系统视图。

步骤 5 执行命令 **interface interface-type interface-number**，进入接口视图。

步骤 6 执行命令 **mpls**，在接口上使能 MPLS。

步骤 7 执行命令 **mpls te**，在接口上使能 MPLS TE。

 说明

接口视图下，去使能 MPLS TE，当前接口上的所有 CR-LSP 将变为 Down。

MPLS 视图下，去使能 MPLS TE，接口的 MPLS TE 也同时被去使能，所有的 CR-LSP 将被删除。

---结束

3.2.3（可选）配置链路的带宽

通过配置链路的带宽可以限定 CR-LSP 的带宽。

背景信息

 说明

如果要限定 CR-LSP 的带宽，必须配置此步骤。

缺省情况下，链路的最大可预留带宽为 0bit/s。如果不配置链路的最大可预留带宽，则限定 CR-LSP 的带宽时，CR-LSP 的带宽大于链路最大可预留带宽，因此 CR-LSP 无法建立。

在隧道的各节点上进行如下配置。

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**，进入使能了 MPLS TE 的接口的视图。

步骤 3 执行命令 **mpls te bandwidth max-reservable-bandwidth bw-value**，配置链路最大可预留带宽。

步骤 4 执行命令 **mpls te bandwidth { bc0 bc0-bw-value | bc1 bc1-bw-value }***，配置链路的 BC 带宽。

 说明

- 链路的最大可预留带宽不能大于链路的实际带宽，建议配置链路的可预留最大带宽不超过链路实际带宽的 80%。
- 链路的 BC0 带宽和 BC1 带宽都不能大于链路最大可预留带宽。
- 当配置 MPLS TE 隧道所需的带宽值大于 67105kbps 时，建议配置隧道时多预留出配置带宽千分之一的带宽值。

---结束

3.2.4 配置 MPLS TE 隧道接口

要创建 MPLS TE 隧道，必须先创建一个 tunnel 接口。

背景信息

在 TE 隧道入节点上进行如下配置。

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 tunnel interface-number**，创建 Tunnel 接口，并进入 Tunnel 接口视图。

步骤 3 配置隧道接口的 IP 地址，选择如下方式之一：

- 执行命令 **ip address ip-address { mask | mask-length } [sub]**，配置 Tunnel 接口的 IP 地址。
必须先配置主 IP 地址，才能为 Tunnel 接口配置从 IP 地址。
- 执行命令 **ip address unnumbered interface interface-type interface-number**，配置隧道接口借用其他接口的 IP 地址。

为实现流量转发，Tunnel 接口必须具有 IP 地址，但 MPLS TE 隧道是单向的，不存在对端地址的问题，没有必要为 Tunnel 接口单独配置 IP 地址，通常的做法是 Tunnel 接口借用入节点的 LSR ID 作为地址。

说明

由于 MPLS TE 隧道转发的是 MPLS 报文，因此，在隧道接口下配置 IP 报文转发相关的命令是无效的。

步骤 4 执行命令 **tunnel-protocol mpls te**，配置隧道协议为 MPLS TE。

步骤 5 执行命令 **destination ip-address**，配置隧道的目的地址，一般配置为出节点的 LSR ID。

由于不同类型的隧道对于目的地址要求不同，当隧道协议从其他类型改变为 MPLS TE 时，原先配置的 **destination** 将被自动删除，需要重新配置。

步骤 6 执行命令 **mpls te tunnel-id tunnel-id**，配置隧道 ID。

步骤 7 执行命令 **mpls te signal-protocol cr-static**，配置隧道使用静态 CR-LSP。

步骤 8 执行命令 **mpls te commit**，提交隧道当前配置。

说明

每次更改 Tunnel 接口上的 MPLS TE 参数后，都需要使用 **mpls te commit** 命令提交配置。

----结束

3.2.5 配置静态 CR-LSP 的入节点

配置静态 CR-LSP 时，需要手工指定 CR-LSP 的入节点。

背景信息

在静态 CR-LSP 的入节点进行如下配置。

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 **static-cr-lsp ingress { tunnel-interface tunnel interface-number | tunnel-name } destination destination-address { nexthop next-hop-address | outgoing-interface interface-type interface-number } * out-label out-label [bandwidth [ct0 | ct1] bandwidth]**，配置静态 CR-LSP 的入节点。

如果对参数 **destination destination-address**、**nexthop next-hop-address**、**outgoing-interface interface-type interface-number**、**out-label out-label** 进行了配置后，需要修改这些参数时，可以直接执行 **static-cr-lsp ingress** 命令进行配置，而不需要执行 **undo static-cr-lsp ingress** 命令取消原有配置。即以上参数支持更新。

参数 **tunnel interface-number** 的取值是使用此静态 CR-LSP 的 MPLS TE 隧道的接口编号。带宽约束类型的缺省值为 **ct0**，带宽的缺省值为 0。隧道使用的带宽不能超过链路最大可预留带宽。

参数 **tunnel-name** 不支持空格和缩写。假设使用命令 **interface tunnel0/0/0** 为静态 CR-LSP 创建了一个 Tunnel 接口，则静态 CR-LSP 入节点中的 **tunnel-name** 应该写作“Tunnel0/0/0”，否则隧道将不能正确建立。中间节点和出节点无此限制。

下一跳或出接口由入节点到出节点的路由决定。关于下一跳地址及出接口的区别，请参见《Huawei AR1200 系列企业路由器 配置指南-IP 路由》中“静态路由配置”。

---结束

3.2.6 配置静态 CR-LSP 的中间节点

配置静态 CR-LSP 时，需要手工指定 CR-LSP 的中间节点。此步骤不是必配的，因为 CR-LSP 可以没有中间节点。

背景信息

如果静态 CR-LSP 只有入节点和出节点，则无需进行此配置。如果静态 CR-LSP 有中间节点，则在中间节点上进行如下配置。

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 **static-cr-lsp transit lsp-name incoming-interface interface-type interface-number in-label in-label-value { nexthop next-hop-address | outgoing-interface interface-type interface-number } * out-label out-label-value [bandwidth [ct0 | ct1] bandwidth]**，配置静态 CR-LSP 的中间节点。

如果对参数 **incoming-interface interface-type interface-number**、**in-label in-label-value**、**nexthop next-hop-address**、**outgoing-interface interface-type interface-number**、**out-label out-label-value** 进行了配置后，需要修改这些参数时，可以直接执行 **static-cr-lsp transit** 命令进行配置，而不需要执行 **undo static-cr-lsp transit** 命令取消原有配置。即以上参数支持更新。

---结束

3.2.7 配置静态 CR-LSP 的出节点

配置静态 CR-LSP 时，需要手工指定 CR-LSP 的出节点。

背景信息

在静态 CR-LSP 的出节点进行如下配置。

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 **static-cr-lsp egress lsp-name incoming-interface interface-type interface-number in-label in-label [lsr-id ingress-lsr-id tunnel-id tunnel-id]**，配置静态 CR-LSP 的出节点。

如果对参数 **incoming-interface interface-type interface-number**、**in-label in-label-value** 进行了配置后，需要修改这些参数时，可以直接执行 **static-cr-lsp egress** 命令进行配置，而不需要执行 **undo static-cr-lsp egress** 命令取消原有配置。即以上参数支持更新。

---结束

3.2.8 检查配置结果

静态 CR-LSP 配置成功后，您可以查看静态 CR-LSP 的状态信息。

前提条件

已经完成静态 CR-LSP 的所有配置。

操作步骤

- 使用 **display mpls static-cr-lsp [lsp-name] [{ include | exclude } ip-address mask-length] [verbose]** 命令查看静态 CR-LSP 信息。
- 使用 **display mpls te tunnel [destination ip-address] [lsp-id ingress-lsr-id session-id local-lsp-id | lsr-role { all | egress | ingress | remote | transit }] [name tunnel-name] [{ incoming-interface | interface | outgoing-interface } interface-type interface-number] [verbose]** 命令查看隧道信息。
- 使用命令 **display mpls te tunnel statistics** 或者 **display mpls lsp statistics** 查看隧道统计信息。
- 使用 **display mpls te tunnel-interface [tunnel interface-number]** 命令在静态 CR-LSP 入节点查看隧道接口信息。

---结束

任务示例

在配置成功时，执行上面的命令，应能得到如下的结果：

- 静态隧道名称、入/出标签、入/出接口等相关信息，并且其状态应为 Up。
- 节点上各隧道的状态统计信息。
- 隧道接口的详细信息，包括隧道名、隧道状态描述和隧道属性等相关信息，其中隧道属性包括 LSP ID、隧道入节点、出节点、信令协议等。

3.3 配置 RSVP-TE 隧道

RSVP-TE 隧道是 MPLS TE 隧道的一种，是配置 MPLS TE 的所有高级特性和应用的基础。

3.3.1 建立配置任务

在配置 RSVP-TE 隧道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，可以快速、准确地完成配置任务。

应用环境

RSVP-TE 动态信令协议在继承 RSVP 协议的资源预留能力的基础上，扩展了 MPLS 标签分发、管理能力，丰富了链路的带宽管理属性，支持显示路径，可以根据网络的变化动态调整 TE 隧道的属性。同时支持 TE FRR、CR-LSP 备份等高级特性，具备良好的故障恢复、快速反应能力。推荐配置 MPLS TE 业务时采用 RSVP-TE 类型的 TE 隧道。

前置任务

在配置 RSVP-TE 隧道之前，需完成以下任务：

- 配置 IGP 路由协议，使各节点间的 IP 路由可达。
- 配置各 LSR 节点的 LSR-ID。
- 配置各 LSR 节点的全局 MPLS 能力。
- 配置各 LSR 节点的接口 MPLS 能力。

数据准备

在配置 RSVP-TE 隧道之前，需准备以下数据。

序号	数据
1	CR-LSP 经过的节点 LSR ID
2	参与 MPLS TE 流量转发的物理链路，即确定 MPLS TE 使用的链路
3	链路的最大带宽和最大可预留带宽
4	使能 TE 的 OSPF 区域或 IS-IS 级别
5	Tunnel ID
6	隧道目的地址
7	建立隧道的约束条件，如显式路径、隧道带宽值
8	(可选) RSVP 的资源预留风格 (默认风格是共享显式类型 SE (Shared-Explicit))

3.3.2 使能 MPLS TE 和 RSVP-TE

在配置 RSVP-TE 隧道前必须先在各节点的全局和接口上分别使能 MPLS TE 和 RSVP-TE。

背景信息

配置 RSVP-TE 隧道前，需要首先全局使能本节点的 MPLS TE 和 RSVP-TE 能力，然后再使能接口下的 MPLS TE 和 RSVP-TE 能力，之后才能进行其它相关配置：如链路带宽属性、CSPF 等。

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`，进入 MPLS 视图。
- 步骤 3** 执行命令 `mpls te`，全局使能本节点的 MPLS TE。
- 步骤 4** 执行命令 `mpls rsvp-te`，使能本节点 RSVP-TE。
- 步骤 5** 执行命令 `quit`，退回系统视图。
- 步骤 6** 执行命令 `interface interface-type interface-number`，进入 MPLS TE 链路的接口视图。
- 步骤 7** 执行命令 `mpls te`，使能接口的 MPLS TE。
- 步骤 8** 执行命令 `mpls rsvp-te`，使能接口的 RSVP-TE。

说明

- MPLS 视图下，去使能 MPLS TE，接口的 MPLS TE 也同时被去使能，所有的 CR-LSP 变为 Down。
- 接口视图下，去使能 MPLS TE，当前接口上所有的 CR-LSP 变为 Down。
- 如果禁止节点的 RSVP-TE 功能，将会同时禁止该节点所有接口的 RSVP-TE。

---结束

3.3.3 （可选）配置链路的带宽

在隧道的各节点上配置链路的带宽可以限定 CR-LSP 的带宽，合理利用网络资源。

背景信息

MPLS TE 在现存网络基础上，综合考虑网络的带宽、优先级、亲和属性、显式路径等因素来实施流量工程，优化网络资源。因此需要先配置链路的带宽，以保证 IGP-TE 根据链路带宽等属性计算出 TEDB（Traffic Engineering DataBase），提供后续 CSPF 计算路径。

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`，进入使能了 MPLS TE 的接口的视图。
- 步骤 3** 执行命令 `mpls te bandwidth max-reservable-bandwidth bw-value`，配置链路最大可预留带宽。



说明

如果要限定 CR-LSP 的带宽，必须配置此步骤。并且需要保证对应的 Tunnel 接口配置了 **mpls te lsp-tp outbound** 命令。

缺省情况下，链路的最大可预留带宽为 0kbps。如果不配置链路的带宽，则限定 CR-LSP 的带宽时，CR-LSP 的带宽大于链路的最大可预留带宽，会导致 CR-LSP 无法建立。

步骤 4 执行命令 **mpls te bandwidth { bc0 bc0-bw-value | bc1 bc1-bw-value }***，配置链路的 BC 带宽。



说明

- 链路的最大可预留带宽不能大于链路的实际带宽，建议配置链路的可预留最大带宽不超过链路实际带宽的 80%。
- 链路的 BC0 带宽和 BC1 带宽都不能大于链路最大可预留带宽。
- 当配置 MPLS TE 隧道所需的带宽值大于 67105kbps 时，建议配置隧道时多预留出配置带宽千分之一的带宽值。

---结束

3.3.4 配置 OSPF TE

OSPF TE 通过 Opaque Type 10 LSA 组成流量工程数据库 TEDB 提供给 CSPF 计算。

背景信息

MPLS TE 的路径计算是由 CSPF 完成的，CSPF 计算会考虑链路的带宽、颜色等 TE 链路属性，这些 TE 链路属性需要在 MPLS 区域中的各 LSR 间扩散并同步，最终形成一支的 TEDB，供给 CSPF 算路。OSPF TE 在 OSPF 原有协议基础上扩展使用 Opaque Type 10 LSA 携带链路的 TE 属性信息，能在 MPLS 区域中的各 LSR 间扩散 TE 信息，形成 TEDB，解决上述问题。

缺省情况下，OSPF 区域不支持 TE。因此，必须使能 OSPF 的 Opaque。并且，只有当至少有一个邻居处于 FULL 状态时，才会产生 Opaque Type 10 LSA。



说明

如果不配置 OSPF TE，网络中就不会有 Opaque Type 10 LSA，不能形成 TEDB。这种情况下生成的 CR-LSP 是由 IGP 路由得到的，而不是 CSPF 计算出来的。

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 **ospf [process-id]**，进入 OSPF 视图。

步骤 3 执行命令 **opaque-capability enable**，使能 OSPF 的 Opaque 能力。

步骤 4 执行命令 **area area-id**，进入 OSPF 的区域视图。

步骤 5 执行命令 **mpls-te enable [standard-complying]**，在当前 OSPF 区域使能 TE。

---结束

3.3.5 配置 IS-IS TE

IS-IS TE 通过扩展 TLV 方式组成流量工程数据库 TEDB 提供给 CSPF 计算。

背景信息

IS-IS TE 是 IS-IS 为了支持 MPLS TE 而做的扩展，它通过在 IS-IS LSP 报文中定义新的 TLV 的方式，携带该设备 MPLS TE 的配置信息，通过 LSP 的泛洪同步，实现各 LSR 间 MPLS TE 信息的泛洪和同步。IS-IS TE 把所有 LSP 中携带的 TE 信息提取出来，传递给 MPLS 的 CSPF 模块，用来计算隧道路径。简而言之，IS-IS TE 的主要功能就是：收集 IS-IS 网络中的 TE 信息，传递给 CSPF 模块。

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 `isis [process-id]`，进入 IS-IS 协议视图。

步骤 3 执行命令 `cost-style { compatible [relax-spf-limit] | wide | wide-compatible }`，配置 IS-IS 的 Wide Metric 属性。

IS-IS TE 扩展使用 IS 可达性 TLV (22) 的子 TLV 携带 TE 属性信息。因此，必须使能 IS-IS 的 WideMetric 特性，可以设置 `wide`、`compatible` 或 `wide-compatible`。缺省情况下，IS-IS 只收发 `narrow` 方式表示路由权值的报文。

步骤 4 执行命令 `traffic-eng [level-1 | level-2 | level-1-2]`，使能 IS-IS TE。

缺省情况下，IS-IS 进程不支持 TE。

如果在使能 IS-IS TE 时不指定 Level，则同时对 Level-1 和 Level-2 生效。

步骤 5 (可选) 执行命令 `te-set-subtlv { bw-constraint value | lo-multiplier value | unreserve-bw-sub-pool value }`，设置携带 DS-TE 参数的子 TLV 的类型。

缺省情况下，带宽约束 (BW-Constraint) 的子 TLV 为 252；本地过预订倍数 LOM (Local Overbooking Multipliers) 的子 TLV 为 253；子池未预订带宽 (Unreserve-BW-Sub-Pool) 的子 TLV 为 251。

---结束

3.3.6 (可选) 配置 MPLS TE 显式路径

在隧道入节点上配置显式路径，能够使 CR-LSP 按照指定的路径建立，灵活利用网络资源。

背景信息

显式路由由一系列节点构成，按配置的先后顺序组成一条向量路径。显式路由中的 IP 地址是指节点上接口的 IP 地址，通常采用 Egress 节点上 Loopback 接口的地址作为显式路由的目的地址。通过配置显示路由，可以指定 CR-LSP 必须经过某些路由或节点，更好的进行资源的合理分配，增加隧道路径的可控性。

显式路由上的两个相邻节点之间存在两种关系：

- 严格下一跳 (strict)：两个节点必须直接相连。
- 松散下一跳 (loose)：两个节点之间可以存在其他节点。

严格方式与松散方式可以单独使用，也可以混合使用。



说明

TE 隧道分为区域内隧道和区域间隧道。

- 区域内隧道是指 TE 隧道起止于一个区域内，区域包括 OSPF 区域和 IS-IS 区域，不包括 BGP 的 AS。建立区域内 TE 隧道，对显式路径类型没有限制。
- 区域间隧道是指 TE 隧道跨越多个区域。区域包括 OSPF 区域和 IS-IS 区域，不包括 BGP 的 AS。建立区域间 TE 隧道必须使用松散显式路径，并且指定显式路径的下一个节点为 ABR 或 ASBR。使用中的显式路径支持更新。

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 **explicit-path path-name**，创建显式路径，进入显式路径视图。

步骤 3 执行命令 **next hop ip-address [include [strict | loose] | exclude]**，指定显式路径的下一个节点。

步骤 4 执行命令 **add hop ip-address1 [include [strict | loose] | exclude] { after | before } ip-address2**，向显式路径中插入一个节点。

步骤 5 执行命令 **modify hop ip-address1 ip-address2 [include [strict | loose] | exclude]**，修改显式路径中的节点地址。



说明

缺省情况下，采用 **include strict** 模式，即加入的下一跳与上一节点必须是直连的。作为一种约束条件，显式路径也可以指定必须经过的节点或者不能经过的节点。

参数 **include** 表示建立的 LSP 必须经过指定节点；参数 **exclude** 表示建立的 LSP 不能经过指定节点。

步骤 6 执行命令 **delete hop ip-address**，从显式路径中删除一个节点。

步骤 7 执行命令 **list hop [ip-address]**，查看显式路径节点信息。

---结束

3.3.7 配置 MPLS TE 隧道接口

需要在隧道入节点创建一个 Tunnel 接口，确保完成隧道的建立及指导隧道的数据报文转发。

背景信息

隧道的接口主要负责隧道的建立、管理和指导报文转发，其中：

- 隧道建立：配置好隧道接口后，可以在隧道接口下配置隧道的路径约束、带宽属性等，以及其他高级属性，如 TE FRR，隧道自动重优化等。
- 隧道管理：可以在基本 TE 隧道建立完成后，在隧道接口上配置隧道相关属性，调整隧道的建立。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface tunnel tunnel-number**，创建 Tunnel 接口，并进入 Tunnel 接口视图。



说明

如果在 Tunnel 接口下执行 **shutdown** 命令，则该 Tunnel 对应的 LSP 都将被删除。

步骤 3 配置隧道接口的 IP 地址，选择如下方式之一：

- 执行命令 **ip address ip-address { mask | mask-length } [sub]**，配置 Tunnel 接口的 IP 地址。
必须先配置主 IP 地址，才能为 Tunnel 接口配置从 IP 地址。
- 执行命令 **ip address unnumbered interface interface-type interface-number**，配置隧道接口借用其他接口的 IP 地址。

为实现流量转发，Tunnel 接口必须具有 IP 地址，但 MPLS TE 隧道是单向的，不存在对端地址的问题，没有必要为 Tunnel 接口单独配置 IP 地址，通常的做法是 Tunnel 接口借用 Ingress 节点的 LSR ID 作为地址。



说明

由于 MPLS TE 隧道转发的是 MPLS 报文，因此，在隧道接口下配置 IP 报文转发相关的命令是无效的。

步骤 4 执行命令 **tunnel-protocol mpls te**，配置隧道协议为 MPLS TE。

步骤 5 执行命令 **destination ip-address**，配置隧道的目的地址，一般配置为出节点的 LSR ID。

由于不同类型的隧道对于目的地址要求不同，当隧道协议从其他类型改变为 MPLS TE 时，原先配置的 **destination** 将被自动删除，需要重新配置。

步骤 6 执行命令 **mpls te tunnel-id tunnel-id**，配置隧道 ID。

步骤 7 执行命令 **mpls te signal-protocol rsvp-te**，配置隧道使用 RSVP-TE 作为信令协议。

步骤 8（可选）执行命令 **mpls te signalled tunnel-name**，配置 TE 隧道的名称。

步骤 9（可选）执行命令 **mpls te cspf disable**，使能在建立 TE 隧道的时候，将屏蔽 CSPF 计算。



说明

在 OptionC 方式跨域 VPN 场景下，才需要执行此命令。其他场景不建议执行此命令。

步骤 10 执行命令 **mpls te commit**，提交隧道当前配置。



说明

每次更改 Tunnel 接口上的 MPLS TE 参数后，都需要使用 **mpls te commit** 命令提交配置。

---结束

3.3.8 配置 MPLS TE 隧道的约束条件

在入节点上配置隧道的带宽及显式路径等约束条件，可以精确、灵活地控制 RSVP-TE 隧道的建立。

背景信息

CSPF 会根据隧道的约束条件进行路径计算。因此需要指定隧道的约束条件，保证 CSPF 正确算路，保证 CR-LSP 的正确建立。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 `interface tunnel tunnel-number`，进入 MPLS TE 隧道的 Tunnel 接口视图。

步骤 3 执行命令 `mpls te bandwidth [ct0 ct0-bw-value | ct1 ct1-bw-value]`，配置隧道使用的带宽。

隧道使用的带宽不能超过链路最大可预留带宽。

缺省情况下，隧道带宽类型为 ct0。

如果 TE 隧道只用于改变数据的传输路径，则可以不配置隧道使用的带宽。

步骤 4 执行命令 `mpls te path explicit-path path-name`，配置隧道应用的显式路径。

如果只想限制隧道使用的带宽，不限制传输路径，则可以不配置隧道应用的显式路径。

步骤 5 执行命令 `mpls te commit`，提交隧道当前配置。

当配置 MPLS TE 隧道带宽值大于 28630kbit/s 时，可能导致实际分配的隧道带宽不够精确。但是 MPLS TE 隧道仍然能够建立成功。

---结束

3.3.9（可选）配置 RSVP 资源预留风格

当多条 LSP 有重合节点时，需要在入节点上配置资源预留风格，使得重合节点上的不同 LSP 享有相同的或者不同的资源预留方式。

背景信息

资源预留风格是指 RSVP 节点处理上游入节点的资源预留请求时的资源预留方式。当前，Huawei AR1200 系列支持的资源预留风格包括：

- FF（Fixed Filter）：固定过滤风格，为每个入节点单独预留，即本节点的预留资源的总和等于为每一个入节点预留的资源总和。
- SE（Shared Explicit）：共享显式风格，为本节点显式地指定一个或多个入节点预留资源，这些入节点共享同一个预留资源。

在目前的 TE 应用中，SE 方式主要用于 make-before-break，固定过滤类型 FF（Fixed-Filter）方式则很少使用。

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 tunnel tunnel-number`，进入 MPLS TE 隧道的 Tunnel 接口视图。

步骤 3 执行命令 `mpls te resv-style { ff | se }`，配置隧道的资源预留风格。

 说明

缺省情况下，资源预留风格为共享显式类型 SE（Shared-Explicit）。

步骤 4 执行命令 `mpls te commit`，提交隧道当前配置。

---结束

3.3.10 配置 CSPF

在隧道入节点上配置 CSPF，根据 TEDB 和显式路径计算出符合约束条件的路径。

背景信息

CSPF 对传统 SPF 算法进行了扩展，能够根据 MPLS TE 的要求算出相应的最短路径。它在计算路径时将考虑以下条件：

- 从 IGP-TE 获得并在 TEDB 中维护的链路状态信息。
- 从 IGP-TE 承载并存储在 TEDB 中的与网络资源状态相关的属性（链路最大带宽、最大可预留带宽、亲和属性等）。
- 由用户指定的路径约束条件（显式路径）。



说明

推荐在所有的 Transit 节点都配置 CSPF，防止 Ingress 节点没法算完整条路径。

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**，进入 MPLS 视图。

步骤 3 执行命令 **mpls te cspf**，使能本节点的 CSPF。

缺省情况下，未启动 CSPF。

步骤 4（可选）执行命令 **mpls te cspf preferred-igp { isis | ospf }**，配置优先 IGP 协议。

---结束

3.3.11 检查配置结果

RSVP-TE 隧道配置成功后，可以查看 RSVP-TE 隧道的信息和隧道的状态统计信息。

前提条件

已经完成 RSVP-TE 隧道功能的所有配置。

操作步骤

- 执行命令 **display mpls te link-administration bandwidth-allocation [interface interface-type interface-number]** 命令查看链路带宽分配信息。
- 执行命令 **display ospf [process-id] mpls-te [area area-id] [self-originated]** 命令查看 OSPF TE 信息。
- 执行命令查看 IS-IS TE 状态：
 - **display isis traffic-eng advertisements**
 - **display isis traffic-eng link**
 - **display isis traffic-eng network**
 - **display isis traffic-eng statistics**
 - **display isis traffic-eng sub-tlvs**
- 执行命令 **display explicit-path [path-name] [verbose]** 查看已经配置的显式路径。
- 执行命令 **display mpls te cspf destination ip-address [affinity properties [mask mask-value] | bandwidth { ct0 ct0-bandwidth | ct1 ct1-bandwidth | ct2 ct2-bandwidth | ct3 ct3-bandwidth | ct4 ct4-bandwidth | ct5 ct5-bandwidth | ct6 ct6-bandwidth | ct7 ct7-bandwidth }* | explicit-path path-name | hop-limit hop-limit-number | metric-type**

- { **igp** | **te** } | **priority** *setup-priority* | **srlg-strict** *exclude-path-name* | **tie-breaking** { **random** | **most-fill** | **least-fill** }]*查看满足指定条件的 CSPF 计算的路径。
- 执行命令 **display mpls te cspf tedb** { **all** | **area** *area-id* | **interface** *ip-address* | **network-lsa** | **node** [*router-id*] } 查看满足指定条件的用于 CSPF 计算的 TEDB 信息。
 - 执行命令 **display mpls rsvp-te** 查看 RSVP 的相关信息。
 - 执行命令 **display mpls rsvp-te established** [**interface** *interface-type interface-number peer-ip-address*] 查看已建立的 RSVP LSP 信息。
 - 执行命令 **display mpls rsvp-te peer** [**interface** *interface-type interface-number*] 命令查看 RSVP 邻居参数。
 - 执行命令 **display mpls rsvp-te reservation** [**interface** *interface-type interface-number peer-ip-address*] 查看 RSVP 资源预留信息。
 - 执行命令 **display mpls rsvp-te request** [**interface** *interface-type interface-number peer-ip-address*] 查看 RSVP LSP 发送方请求的资源预留信息。
 - 执行命令 **display mpls rsvp-te sender** [**interface** *interface-type interface-number peer-ip-address*] 查看 RSVP 发送方信息。
 - 执行命令 **display mpls rsvp-te statistics** { **global** | **interface** [*interface-type interface-number*] } 查看 RSVP-TE 运行统计信息。
 - 执行命令 **display mpls te link-administration admission-control** [**interface** *interface-type interface-number* | **stale-interface** *interface-index*] 查看本地接纳的隧道。
 - 执行命令 **display mpls te tunnel** [**destination** *ip-address*] [**lsp-id** *ingress-lsr-id session-id local-lsp-id*] [**lsr-role** { **all** | **egress** | **ingress** | **remote** | **transit** }] [**name** *tunnel-name*] [{ **incoming-interface** | **interface** | **outgoing-interface** } *interface-type interface-number*] 查看隧道信息。
 - 执行命令 **display mpls te tunnel statistics** 或者 **display mpls lsp statistics** 查看隧道统计信息。
 - 执行命令 **display mpls te tunnel-interface** [**tunnel** *tunnel-number*] 在隧道入节点查看隧道接口信息。

---结束

任务示例

在配置成功时，执行上面的命令，应能得到如下的结果：

- 物理带宽、可用带宽等链路信息。
- 各节点生成的 OSPF Opaque Type 10 LSA 相关信息。
- 各节点的 IS-IS TE 相关信息。
- MPLS RSVP-TE 的各种计时器信息以及使能了 RSVP-TE 的接口状态、带宽信息；RSVP 邻居参数、发送方以及各种统计信息。
- 隧道名称、入/出标签、入/出接口等相关信息。
- 节点上各隧道的状态统计信息。
- 隧道入节点接口的详细信息，包括隧道名、隧道状态描述和隧道属性等相关信息，其中隧道属性包括 LSP ID、隧道入节点 LSR ID、出节点 LSR ID。

3.4 调整 RSVP 信令参数

RSVP-TE 提供了丰富的信令参数，能够满足用户对于可靠性、网络资源、以及一些 MPLS TE 高级特性的应用。

3.4.1 建立配置任务

在调整 RSVP 信令参数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

RSVP-TE 提供了丰富的信令参数，能够满足用户对于可靠性、网络资源、以及一些 MPLS TE 高级特性的应用。

在实施本节介绍的配置任务之前，需要仔细了解各配置任务的目的和可能对网络造成的影响。

前置任务

在优化 RSVP-TE 隧道之前，需完成以下任务：

- [配置 RSVP-TE 隧道](#)

数据准备

在优化 RSVP-TE 隧道之前，需准备以下数据。

序号	数据
1	RSVP 的刷新周期
2	RSVP 的 PSB、RSB、BSB 超时倍数
3	RSVP 的重传定时器和增量值
4	Hello 消息的发送间隔和允许丢失的最大数目

3.4.2 配置 RSVP 的 Hello 扩展

RSVP 的 Hello 扩展机制用于快速检测 RSVP 邻居节点的可达性。

背景信息

在隧道各节点上进行如下配置。

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 **mpls**，进入 MPLS 视图。

步骤 3 执行命令 **mpls rsvp-te hello**，使能本节点的 RSVP Hello 扩展。

缺省情况下，不启用 Hello 扩展机制。

步骤 4 执行命令 **mpls rsvp-te hello-lost times**，配置允许 Hello 消息丢失的最大次数。

启用 Hello 扩展机制后，缺省情况下，连续未收到 3 次 Hello 应答消息认为节点发生故障，相关的 TE 隧道将被拆除。

步骤 5 执行命令 **mpls rsvp-te timer hello interval**，配置 Hello 消息刷新时间间隔。

启用 Hello 扩展机制后，缺省的 Hello 消息刷新时间间隔为 3 秒。

如果修改刷新周期，该刷新周期的修改结果需要等到上次定时器超时以后才生效。

步骤 6 执行命令 **quit**，退回系统视图。

步骤 7 执行命令 **interface interface-type interface-number**，进入 MPLS TE 链路的接口视图。

步骤 8 执行命令 **mpls rsvp-te hello**，使能接口的 RSVP Hello 扩展。

RSVP 的 Hello 扩展机制用于快速检测 RSVP 邻居节点的可达性，在 RFC3209 中有详细的介绍。

----结束

3.4.3 配置 RSVP 的状态定时器

通过配置 RSVP 的状态定时器，可以设置 Path 消息和 Resv 消息的刷新周期。

背景信息

在隧道各节点上进行如下配置。

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 **mpls**，进入 MPLS 视图。

步骤 3 执行命令 **mpls rsvp-te timer refresh interval**，设置节点 Path、Resv 的刷新周期。

缺省情况下，节点的 Path、Resv 刷新周期为 30 秒。

如果修改刷新周期，该刷新周期的修改需要等到上次定时器超时以后才生效。建议不要设置超长刷新周期或反复修改刷新周期。

步骤 4 执行命令 **mpls rsvp-te keep-multiplier number**，设置 PSB 和 RSB 的超时倍数。

缺省情况下，PSB 和 RSB 的超时倍数为 3。

----结束

3.4.4 配置 RSVP-TE 摘要刷新

在连接两个邻居节点的接口上使能摘要刷新（Srefresh）可以减少开销，提高性能。使能摘要刷新后，接口上同时启动对 Srefresh 的可靠性重传。

背景信息

在两个邻居节点的接口视图下或 MPLS 视图下使能摘要刷新（Srefresh）可以减少开销，提高性能。在接口视图下只能使能该接口的摘要刷新功能；在 MPLS 视图下，将使整台设备所有接口使能摘要刷新。使能摘要刷新后，将同时在单一或全部接口上启动对 Srefresh 的可靠性重传。

如果在重传时间间隔内（假设为 R_f 秒），没有收到应答 ACK，经过 $(1 + \Delta) \times R_f$ 秒后，将重传此消息。 Δ 决定发送方增加重传间隔的速率。重传将一直持续到收到一个 ACK 消息或重传次数达到增量值 RI。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令进入接口视图或者 MPLS 视图。

- 执行命令 **interface interface-type interface-number**，进入 MPLS TE 链路的接口视图。在接口视图下配置摘要刷新功能，仅在当前接口生效。
- 执行命令 **mpls**，进入 MPLS 视图。

在 MPLS 视图下配置摘要刷新功能对全局生效。在 MPLS 视图下配置摘要刷新的方式主要应用于 TE FRR 场景。在 FRR 的 PLR 和 MP 上配置全局的摘要刷新功能，不仅可以提高网络资源的使用率，还可以提高摘要刷新功能的可靠性。

步骤 3 执行命令 **mpls RSVP-te srefresh**，使能摘要刷新功能。

缺省情况下，关闭接口与全局的摘要刷新功能。

步骤 4（可选）在接口视图下执行命令 **mpls RSVP-te timer retransmission { increment-value increment | retransmit-value interval } ***，配置重传参数。

缺省情况下，重传定时器值（*interval*）和增量值（*increment*）分别为 500 毫秒和 1。

---结束

3.4.5 配置 RSVP-TE 预留确认

收到 ResvConf 消息并不表示成功建立了资源预留，只能说明在此 Resv 消息到达的最远上游节点处成功保留了资源，这些资源接下来仍可能被其它应用抢占。

背景信息

在隧道出节点上进行如下配置。

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 **mpls**，进入 MPLS 视图。

步骤 3 执行命令 **mpls RSVP-te resvconfirm**，启动预留确认机制。

预留确认机制由 Path 消息的接收者发起，接收者在发送 Resv 消息时，携带一个要求对预留进行确认的对象。

---结束

3.4.6 检查配置结果

RSVP 信令参数调整完成后，您可以查看接口的刷新信息参数、RSVP 的预留确认和 Hello 扩展的使能状态、状态定时器配置信息。

操作步骤

- 使用 **display mpls rsvp-te** 命令查看 RSVP-TE 的相关信息。
- 使用 **display mpls rsvp-te psb-content [ingress-lsr-id tunnel-id lsp-id]** 命令查看 RSVP-TE PSB 信息。
- 使用 **display mpls rsvp-te rsb-content [ingress-lsr-id tunnel-id lsp-id]** 命令查看 RSVP-TE RSB 信息。
- 使用 **display mpls rsvp-te statistics { global | interface [interface-type interface-number] }** 命令查看 RSVP-TE 运行统计信息。

----结束

任务示例

在配置成功时，执行上面的命令，应能得到如下的结果：

- 接口的刷新信息参数。
- RSVP 的预留确认和 Hello 扩展的使能状态，以及状态定时器配置信息。

3.5 配置 RSVP 认证

RSVP 认证用来防止非授权的节点与本节点进行 RSVP 邻居的建立和防止通过构造报文来达到欺骗的目的。

3.5.1 建立配置任务

在配置 RSVP 认证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

RSVP 认证通过使用密钥验证的方法来防止非授权的节点与本节点进行 RSVP 邻居的建立和防止通过构造报文来达到欺骗的目的。

RSVP 密钥验证可防止以下两种不合法的 RSVP 邻居的建立，避免对本地节点的攻击（如恶意的预留大量带宽）：

- 防止对端在没有授权的情况下和本节点建立邻居关系；
- 防止通过伪造 RSVP 报文的方式和本节点建立 RSVP 邻居。

但只用 RSVP 密钥验证不能防止回放攻击，也不能解决因网络拥塞导致 RSVP 报文失序从而引发 RSVP 邻居之间认证关系终止的问题。这两个问题可以通过配置 **handshake** 功能和 **message window** 功能来解决。

为了防止 RSVP 认证无法终止，可配置 RSVP 认证生存时间。配置 RSVP 认证生存后，当 RSVP 邻居之间不存在 CR-LSP 时可保持 RSVP 邻居关系，直到 RSVP 认证生存时间超时。

前置任务

在配置 RSVP 认证之前，需完成以下任务：

- [配置 RSVP-TE 隧道](#)

数据准备

在配置 RSVP 认证之前，需准备以下数据。

序号	数据
1	RSVP 的验证密钥
2	(可选) RSVP 认证生存时间
3	(可选) Handshake 验证使用的本地密码
4	(可选) RSVP 消息窗口大小 (默认值为 1)

3.5.2 配置 RSVP 密钥验证

RSVP 密钥验证是在两个 RSVP 邻居之间的接口进行的。邻居之间的接口的密钥必须相同，否则验证不能通过，该接口收到的 RSVP 报文都会被丢弃。

背景信息

RSVP 消息通过增加认证对象，并验证对象的正确性，来防止消息被篡改或伪造的恶意攻击，增强网络的可靠性和安全性。

RSVP 密钥验证可以在接口视图或者 MPLS RSVP-TE 邻居视图下进行配置。

- 接口视图下的密钥验证功能应用于两个直连节点。
- MPLS RSVP-TE 邻居视图下配置的 RSVP 密钥验证可以应用于任意两个互相配置为邻居的节点。推荐使用这种配置方式。

可以根据选用的参数，配置 HMAC-MD5 认证或者 Keychain 认证。

- **cipher**：配置 HMAC-MD5 认证，并使用密文方式显示认证密钥。
- **plain**：配置 HMAC-MD5 认证，并使用明文方式显示认证密钥。
- **keychain**：配置 Keychain 认证，引用全局配置的 Keychain。

 说明

RSVP Keychain 认证只支持 HMAC-MD5 算法。

 说明

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。

操作步骤

- 在接口视图下配置 RSVP 密钥验证功能

在两个直连节点间的接口上进行如下配置。



说明

要求在三个刷新周期内，在直连的两个接口都完成配置。如果在三个刷新周期内没有在两个接口都完成配置，则会导致会话 Down。

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 MPLS TE 链路的接口视图。
3. 执行命令 **mpls rsvp-te authentication { { cipher | plain } auth-key } | keychain keychain-name**，配置验证密钥。

在接口视图下配置的 RSVP 密钥验证功能，仅在当前接口下生效且优先级最低。

- 在 MPLS RSVP-TE 邻居视图下配置 RSVP 密钥验证功能

在两个邻居节点上进行如下配置。



说明

要求在三个刷新周期内，在两个邻居节点都完成配置。如果在三个刷新周期内没有在两个邻居节点都完成配置，则会导致会话 Down。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **mpls rsvp-te peer ip-address**，进入 MPLS RSVP-TE 邻居视图。
 - 当 *ip-address* 为邻居的接口地址，且与其 LSR-ID 不相同，则该密钥认证是基于邻居接口地址的配置。这种配置方式只对该邻居的该接口生效，具有较高安全性，所以优先级最高。
 - 当 *ip-address* 与邻居 LSR-ID 相同时，则该密钥认证是基于邻居 LSR-ID 的配置。这种配置方式将使密钥验证功能在该邻居上生效，而不限定邻居的接口，其优先级低于基于邻居接口地址配置的密钥验证的优先级，但高于接口视图下配制的验证功能的优先级。
3. 执行命令 **mpls rsvp-te authentication { { cipher | plain } auth-key } | keychain keychain-name**，配置验证密钥。

---结束

3.5.3 （可选）配置 RSVP 认证生存时间

通过配置认证生存时间，可以设置 RSVP 邻居之间不存在 CR-LSP 时可以保持 RSVP 邻居关系的时间间隔。

背景信息

RSVP 认证时间的功能是：当 RSVP 邻居之间不存在 CR-LSP 时可以保持 RSVP 邻居关系，直到 RSVP 认证生存时间超时。RSVP 认证时间不影响已存在的 CR-LSP 的状态。

在隧道各节点上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 进入接口视图或者 MPLS RSVP-TE 邻居视图。

- 执行命令 **interface interface-type interface-number**，进入 MPLS TE 链路的接口视图。

在接口视图下进行配置，则配置的 RSVP 认证生存时间仅在当前接口下生效。

- 执行命令 **mpls rsvp-te peer ip-address**，进入 MPLS RSVP-TE 邻居视图。
 - 当 *ip-address* 为邻居的接口地址，且与其 LSR-ID 不相同时，则配置的 RSVP 认证生存时间是基于邻居接口地址的配置。这种配置方式只对该接口生效。
 - 当 *ip-address* 与邻居 LSR-ID 相同时，则配置的 RSVP 认证生存时间是基于邻居 LSR-ID 的配置。这种配置方式将使这个配置在整台设备上生效。

步骤 3 执行命令 **mpls rsvp-te authentication lifetime lifetime**，设置 RSVP 认证生存时间。

lifetime 表示认证生存时间，HH: MM: SS 格式，取值范围是 00: 00: 01 ~ 23: 59: 59，缺省值为 00: 30: 00，即 30 分钟。

----结束

3.5.4（可选）配置 handshake 功能

必须先配置 RSVP 密钥验证，才能配置 handshake 功能。

背景信息

在隧道各节点上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 进入接口视图或者 MPLS RSVP-TE 邻居视图。

- 执行命令 **interface interface-type interface-number**，进入 MPLS TE 链路的接口视图。
在接口视图下进行配置，则配置 handshake 功能仅在当前接口下生效。
- 执行命令 **mpls rsvp-te peer ip-address**，进入 MPLS RSVP-TE 邻居视图。
 - 当 *ip-address* 为邻居的接口地址，且与其 LSR-ID 不相同时，则配置的 handshake 功能是基于邻居接口地址的配置。这种配置方式只对该接口生效。
 - 当 *ip-address* 与邻居 LSR-ID 相同时，则配置的 handshake 功能是基于邻居 LSR-ID 的配置。这种配置方式将使 handshake 功能在整台设备上生效。

步骤 3 执行命令 **mpls rsvp-te authentication handshake local-secret**，配置 handshake 功能。

local-secret 只是本地有效，不需要与邻居配置的 *local-secret* 一致。

在本端配置 handshake 功能后，如果本端收到一个没有与自己建立 RSVP 认证关系的邻居所发送的 RSVP 消息，则本端会发送携带 *local-secret* 参数的 Challenge 消息给该邻居，邻居收到 Challenge 消息后回应一个 Response 消息。Response 消息中携带了收到的 Challenge 消息的 *local-secret*。本端收到邻居发来的 Response 消息，如果其中携带的 *local-secret* 与本端配置的一致，就确定可以与该邻居建立 RSVP 认证关系。

说明

如果在邻居之间配置了 Handshake 功能，并且需要执行 **mpls rsvp-te authentication lifetime** 命令配置认证生存时间，那么认证生存时间的时长需要大于 RSVP 刷新消息的发送时间间隔。

如果认证生存时间小于 RSVP 刷新消息的发送时间间隔，就可能造成在认证生存时间内收不到 RSVP 刷新消息而删除认证关系。这样，当下一个刷新消息到来的时候就需要重新进行 Handshake 机制的检测，如此反复可能会造成 TE 隧道无法建立或者被删除。

----结束

3.5.5 （可选）配置 message window 功能

Message window 功能主要是用来解决报文失序问题。

背景信息

缺省情况下，RSVP 消息窗口大小是 1，即本地设备只能保存邻居 RSVP 消息的一个最近的最大的序列号。

当配置的 window-size 大于 1 时，本地就可以保存邻居 RSVP 消息的最近多个有效序列号。

在隧道各节点上进行如下配置。

操作步骤

步骤 1 执行命令 `system-view`，进入系统视图。

步骤 2 进入接口视图或者 MPLS RSVP-TE 邻居视图。

- 执行命令 `interface interface-type interface-number`，进入 MPLS TE 链路的接口视图。在接口视图下进行配置，则配置的 Message window 功能仅在当前接口下生效。
- 执行命令 `mpls rsvp-te peer ip-address`，进入 MPLS RSVP-TE 邻居视图。
 - 当 `ip-address` 为邻居的接口地址，且与其 LSR-ID 不相同，则配置的 Message window 功能是基于邻居接口地址的配置。这种配置方式只对该接口生效。
 - 当 `ip-address` 与邻居 LSR-ID 相同时，则配置的 Message window 功能是基于邻居 LSR-ID 的配置。这种配置方式将使该配置在整台设备上生效。

步骤 3 执行命令 `mpls rsvp-te authentication window-size window-size`，配置 message window 功能，即指定本地设备可保存的邻居 RSVP 消息有效序列号的个数。

必须先[配置 RSVP 密钥验证](#)，才能配置 message window 功能。

说明

当 RSVP 接口类型为 Eth-Trunk 或 IP-Trunk 时，RSVP 邻居之间只在 Trunk 链路上建立一个邻居关系。RSVP 消息可以从 Trunk 的任意一个成员接口接收，且各个成员口不是按顺序接收报文的，这样可能造成 RSVP 消息失序，因此必须配置 RSVP 消息滑动窗口。建议将滑动窗口大小配置为大于 32。如果滑动窗口设置过小，收到的失序的 RSVP 消息有些可能不在窗口范围内而被丢弃，这样会导致 RSVP 邻居关系终止。

----结束

3.5.6 检查配置结果

RSVP 认证配置成功后，您可以查看隧道物理出接口的 RSVP-TE 信息。

前提条件

已经完成 RSVP 认证功能的所有配置。

操作步骤

步骤 1 使用 `display mpls rsvp-te peer [interface interface-type interface-number]` 命令查看使能 RSVP-TE 的接口的 RSVP-TE 邻居信息。

---结束

任务示例

在配置成功时，执行上面的命令，可发现 RSVP-TE 邻居信息中 RSB 数量不为 0。

3.6 调整 CR-LSP 的路径选择

介绍调整 CR-LSP 路径计算和选择的几种方式。

3.6.1 建立配置任务

在进行调整 CR-LSP 的路径选择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

CSPF 使用 TEDB 和约束条件计算出符合要求的路径，并通过信令协议建立 CR-LSP。MPLS TE 提供多种方式影响 CSPF 的计算，从而调整 CR-LSP 的建立，包括：

- 仲裁

CSPF 只计算到达隧道终点的最短路径，当在计算路径的过程中遇到多条权值相同的路径时，只需要选择其中一条即可。

可供选择的仲裁方法包括：

- **Most-fill**：选择已用带宽和最大可预留带宽的比值最大的链路，使链路带宽资源高效使用；
- **Least-fill**：选择已用带宽和最大可预留带宽的比值最小的链路，使各条链路的带宽资源均匀使用；
- **Random**：随机选取，使每条链路上的 LSP 数量均匀分布，不考虑带宽因素。

 说明

由于仲裁依据比率来选择链路，那么在比率相同的情况下，比如没有利用保留带宽，或者利用的份额都是一样，此时不管配置的是 **least-fill** 还是 **most-fill**，选择的的就是首先发现的链路。

- 路由锁定

CR-LSP 创建成功后不随路由变化而变化的特性叫做路由锁定。

- 管理组和亲和属性

MPLS TE 隧道的亲和属性决定隧道使用的链路属性，亲和属性与链路管理组配合，确定隧道可以使用哪些链路。

- SRLG

共享风险链路组 SRLG（Shared Risk Link Group）是一组共享一个公共的物理资源（或是共享一根光纤）的链路。同一个 SRLG 的链路具有相同的风险等级，即如果 SRLG 中的一条链路失效，组内的其他链路也失效。

SRLG 主要用在 CR-LSP 热备份和 TE FRR 组网中增强 TE 隧道的可靠性。共享相同物理资源的多个链路具有相同的风险。例如，当主接口 Down 时，其子接口也通

常变为 Down，所以子接口和主接口通常具有相同的风险。如果主隧道所在的链路和其备份隧道所在链路具有相同的风险，则主隧道变为 Down 时，备份隧道也很可能变为 Down。

- 跳数限制值

跳数限制值作为 CR-LSP 建立时的选路条件之一，可以限制一条 CR-LSP 允许选择的路径跳数不超过某个值。

- 重优化

动态优化 CR-LSP 即定期重计算 CR-LSP 穿越的路由。如果重计算的路由优于当前路由，则创建一条新的 CR-LSP，为之分配新路由，并将业务从旧的 CR-LSP 切换至新的 CR-LSP，删除旧 CR-LSP。

前置任务

本节介绍的配置任务是 MPLS TE 中 CSPF 的一些专门配置，在实施本节的配置任务之前，您需要明确理解这些配置对系统可能造成的影响。

在调整 CR-LSP 的建立之前，需进行以下配置：

- **配置 RSVP-TE 隧道**

数据准备

在调整 CR-LSP 的建立之前，需准备以下数据。

序号	数据
1	节点和隧道的仲裁方法
2	链路的管理组属性和隧道的亲和属性
3	CR-LSP 的重优化周期
4	SLRG 组号、SRLG 路径计算模式(preferred 或 strict)
5	CSPF 失效链路定时器的值

3.6.2 配置管理组和亲和属性

进行管理组属性配置，可以影响新创建的 LSP；而进行亲和属性配置，可以影响该隧道已建立的 LSP，系统将为该隧道重新计算路径。

背景信息

在 CR-LSP 隧道的入节点上进行如下配置。

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 MPLS TE 链路的接口视图。

- 步骤 3** 执行命令 `mpls te link administrative group value`，配置链路的管理组。
- 步骤 4** 执行命令 `quit`，退回系统视图。
- 步骤 5** 执行命令 `interface tunnel interface-number`，进入 MPLS TE 隧道的 Tunnel 接口视图。
- 步骤 6** 执行命令 `mpls te affinity property properties [mask mask-value] [best-effort | secondary]`，配置隧道的亲和属性。缺省情况下，链路管理组的值为 0x0；隧道的亲和属性为 0x0，掩码 0x0。
- 步骤 7** 执行命令 `mpls te commit`，提交隧道当前配置。

----结束

后续处理

更改链路的管理组属性配置，仅对新创建的 LSP 生效，不影响已建立的 LSP。

更改隧道的亲和属性配置，提交后会影响到该隧道已建立的 LSP，系统将为该隧道重新计算路径。

3.6.3 配置 SRLG

在热备份或 TE FRR 的应用场景中，需要为入节点的隧道出接口以及该接口所属的 SRLG 的其它成员链路配置 SRLG 属性。

背景信息

SRLG 配置包括：

- [配置链路 SRLG 属性](#)
- [配置全局 SRLG 路径计算模式](#)

操作步骤

- 配置链路 SRLG 属性

在 SRLG 成员链路的接口下进行如下配置：

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 `mpls te srlg srlg-number`，将该接口加入 SRLG。

在热备份或 TE FRR 的应用场景中，需要为入节点的隧道出接口以及该接口所属的 SRLG 的其它成员链路配置 SRLG 属性。将链路加入 SRLG 时，只需要在这条链路的任意一个出接口上配置 SRLG 属性即可。

- 配置全局 SRLG 路径计算模式

在热备份或 TE FRR 隧道的入节点上进行如下配置：

1. 执行命令 `system-view`，进入系统视图。
2. 执行命令 `mpls`，进入 MPLS 视图。
3. 执行命令 `mpls te srlg path-calculation [preferred | strict]`，配置 SRLG 路径计算模式。



说明

- 如果指定参数 **strict**，则 CSPF 在计算旁路 CR-LSP 或备份 CR-LSP 的路径时，总会将 SRLG 作为约束条件之一。
- 如果指定参数 **preferred**，则 CSPF 在首次计算旁路 CR-LSP 或备份 CR-LSP 的路径时，将 SRLG 作为约束条件之一；如果计算不成功，则不再将 SRLG 作为约束条件。

---结束

3.6.4 配置 CR-LSP 的跳数限制值

跳数限制值作为 CR-LSP 建立时的选路条件之一，就像管理组和亲和属性一样，可以限制一条 CR-LSP 允许选择的路径跳数不超过某个值。

背景信息

在 CR-LSP 隧道的入节点上进行如下配置。

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 tunnel interface-number**，进入 MPLS TE 隧道的 Tunnel 接口视图。

步骤 3 执行命令 **mpls te hop-limit hop-limit-value [best-effort | secondary]**，限制该 Tunnel 的 CR-LSP 的路径跳数。

步骤 4 执行命令 **mpls te commit**，提交隧道当前配置。

---结束

3.6.5 配置选路使用的度量

通过配置选路使用的度量，可以指定隧道使用的度量类型。

操作步骤

- 指定隧道使用的度量类型

在 CR-LSP 隧道入节点进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface tunnel interface-number**，进入 TE 隧道的 Tunnel 接口视图。
3. 执行命令 **mpls te path metric-type { igp | te }**，配置当前隧道选路时使用的度量类型。
4. 执行命令 **mpls te commit**，提交隧道当前配置。
5. 执行命令 **quit**，退回系统视图。
6. （可选）执行命令 **mpls**，进入 MPLS 视图。
7. （可选）执行命令 **mpls te path metric-type { igp | te }**，配置选路时使用的度量类型。

如果在隧道接口视图下没有配置 **mpls te path metric-type**，则使用 MPLS 视图下的度量类型；否则使用隧道接口视图下的度量类型。

缺省情况下，TE 隧道选路时使用的度量类型为 TE。

- （可选）配置链路的 TE 度量值

如果指定隧道的度量类型为 TE 时，则可在 Ingress 节点和 Transmit 节点的数据流出接口上通过以下配置修改链路的 TE 度量值。

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 MPLS TE 链路的接口视图。
3. 执行命令 **mpls te metric value**，配置链路的 TE 度量值。

缺省情况下，链路使用其 IGP 度量作为 TE 的度量。

---结束

3.6.6 配置 CSPF 的仲裁方法

当 CSPF 在计算路径的过程中遇到多条权值相同的路径时，通过配置 CSPF 仲裁可以从中选择出一条路径。

背景信息

在 CR-LSP 隧道的入节点上进行如下配置。

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 **mpls**，进入 MPLS 视图。

步骤 3 执行命令 **mpls te tie-breaking { least-fill | most-fill | random }**，配置本节点的 CR-LSP 仲裁方法。

缺省情况下，本节点的仲裁方法为随机选择方式 **random**。

步骤 4 执行命令 **quit**，退回系统视图。

步骤 5 执行命令 **interface tunnel interface-number**，进入 MPLS TE 隧道的 Tunnel 接口视图。

步骤 6 执行命令 **mpls te tie-breaking { least-fill | most-fill | random }**，配置当前隧道的 CR-LSP 仲裁方法。

步骤 7 执行命令 **mpls te commit**，提交隧道当前配置。

隧道优先使用本隧道视图下配置的仲裁方法；如果隧道视图下没有配置，将使用 MPLS 视图下的配置。

---结束

3.6.7 配置失效链路定时器

通过配置失效链路定时器，可以避免反复对包含故障链路的路径进行 CSPF 计算。

背景信息

CSPF 计算到目的地址的最短路径时，是根据本地维护的 TE 数据库。信令协议将根据 CSPF 计算的路径请求和预留资源。如果网络某链路发生故障，路由协议有时可能没有

及时通知 CSPF 更新 TE 数据库，信令协议从 CSPF 得到的路径可能包含故障的链路。因链路故障，信令协议的控制报文（如 RSVP 的 Path 消息）将在故障的链路丢失。因此信令协议将返回错误消息通知上游节点。上游节点收到链路错误消息时，触发 CSPF 重新计算路径。又因为 TE 数据库没有更新，CSPF 返回给信令协议的路径仍然包含了故障的链路。因此，信令协议的控制报文又将被丢弃，信令协议又返回错误消息，触发 CSPF 重新计算路径。如此反复，直到 TE 数据库得到更新。

为了避免上述情况的发生，当收到信令协议返回错误消息通知链路故障时，CSPF 将故障链路的状态置为 INACTIVE，并启动失效链路定时器。这样，故障链路将不再参与 CSPF 的路径计算，直到 CSPF 收到数据库更新事件或者链路失效定时器超时。

在链路失效定时器超时前，如果收到数据库更新事件，CSPF 将删除链路失效定时器。

在 CR-LSP 隧道入节点进行如下配置。

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**，进入 MPLS 视图。

步骤 3 执行命令 **mpls te cspf timer failed-link interval**，配置 CSPF 失效链路定时器。

缺省情况下，失效链路定时器的值为 10 秒。

失效链路定时器的值只具有本地意义，如果各个节点上配置的定时器值不同，则可能存在于同一条链路在某些节点上的状态是 ACTIVE，而另一些节点上是 INACTIVE 的情况。

---结束

3.6.8 配置环路检测

通过配置环路检测，可以防止产生环路。

背景信息

TE 中的环路检测机制最大跳数为 32。路径信息记录表中已有本 LSR 的记录，或路径的跳数超过此最大跳数时，均认为出现环路，LSP 建立失败。

在 CR-LSP 隧道入节点进行如下配置。

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 tunnel interface-number**，进入 MPLS TE 隧道的 Tunnel 接口视图。

步骤 3 执行命令 **mpls te loop-detection**，配置隧道建立时进行环路检测。

缺省情况下，不进行环路检测。

步骤 4 执行命令 **mpls te commit**，提交隧道当前配置。

---结束

3.6.9 配置路由锁定

通过配置路由锁定，CR-LSP 能够保持初始选定的路径，而不会按照新的可能的路径重新建立。

背景信息

缺省情况下，关闭路由锁定功能。

 说明

如果使用路由锁定特性，则不能同时使用 CR-LSP 重优化。

在 CR-LSP 隧道的入节点上进行如下配置。

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 tunnel interface-number`，进入 MPLS TE 隧道的 Tunnel 接口视图。
- 步骤 3** 执行命令 `mpls te record-route [label]`，建立隧道时记录路由和标签。
- 步骤 4** 执行命令 `mpls te route-pinning`，配置路由锁定。
- 步骤 5** 执行命令 `mpls te commit`，提交隧道当前配置。

----结束

3.6.10 检查配置结果

调整 CR-LSP 的路径选择配置成功后，您可以看到 CSPF 的仲裁方法、路由锁定的状态、重优化的频率间隔及亲和属性及其掩码。

前提条件

已经完成调整 CR-LSP 路径选择功能的所有配置。

操作步骤

- 步骤 1** 使用 `display mpls te tunnel verbose` 命令查看 MPLS TE 隧道信息。

----结束

任务示例

在配置成功时，执行上面的命令，应能看到亲和属性信息。

3.7 调整 MPLS TE 隧道的建立

MPLS TE 提供多种属性，用于灵活调整 TE 隧道的建立。

3.7.1 建立配置任务

在调整 MPLS TE 隧道的建立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

在建立 MPLS TE 隧道的过程中，根据实际应用，可能还需要进行一些专门的配置来调整隧道的建立。本节介绍这些特殊的配置。

前置任务

需要理解的是，本节介绍的任务是 MPLS TE 中的一些专门配置，在实施本节的配置任务之前，需要明确理解这些配置对系统可能造成的影响。

在调整 MPLS TE 隧道的建立之前，需完成以下任务：

- **配置 RSVP-TE 隧道**

数据准备

在调整 MPLS TE 隧道前，需准备以下数据：

序号	数据
1	隧道重建的次数和重建间隔
2	隧道的建立优先级和保持优先级

3.7.2 配置隧道的优先级

如果在建立 CR-LSP 的过程中，无法找到满足所需带宽要求的路径，可以根据建立优先级和保持优先级进行抢占。

背景信息

在 CR-LSP 隧道入节点进行如下配置。

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 tunnel interface-number`，进入 MPLS TE 隧道的 Tunnel 接口视图。

步骤 3 执行命令 `mpls te priority setup-priority [hold-priority]`，配置隧道的优先级。

建立优先级和保持优先级的取值范围都是 0 ~ 7，数值越小则优先级越高。

缺省情况下，建立优先级和保持优先级的值都为 7。当只配置建立优先级时，保持优先级与建立优先级相同。

 说明

由于建立优先级不能高于保持优先级，故配置的建立优先级的值不应该小于保持优先级的值。

步骤 4 执行命令 `mpls te commit`，提交隧道当前配置。

----结束

3.7.3 配置 CR-LSP 重优化

通过配置隧道重优化，可以定期重计算 CR-LSP 穿越的路由。如果重计算的路由优于当前路由，则创建一条新的 CR-LSP，为之分配新路由，并将业务从旧的 CR-LSP 切换至新的 CR-LSP，删除旧 CR-LSP。

背景信息

 说明

- 如果使用 CR-LSP 重优化，则不能同时使用路由锁定特性。
- 如果隧道的资源预留为固定过滤器类型 FF，则不能配置 CR-LSP 重优化。

在 CR-LSP 隧道的入节点上进行如下配置。

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 tunnel interface-number**，进入 MPLS TE 隧道的 Tunnel 接口视图。

步骤 3 执行命令 **mpls te reoptimization [frequency interval]**，配置定时重优化。

缺省情况下，不进行重优化。定时重优化的缺省间隔是 3600 秒。

步骤 4 执行命令 **mpls te commit**，提交隧道当前配置。

步骤 5 执行命令 **return**，退回用户视图。

步骤 6（可选）执行命令 **mpls te reoptimization**，对 TE 隧道进行立即重优化。

在隧道视图下配置定时重优化后，可以退回用户视图执行 **mpls te reoptimization** 命令，对所有配置了重优化的隧道立即进行重优化。并且，执行了立即重优化后，定时重优化的定时器将被清零，重新计时。

---结束

3.7.4 配置 CR-LSP 和 Overload 联动功能

通过 CR-LSP 和 Overload 联动功能，可以使建立的 CR-LSP 避开 Overload 节点。

背景信息

网络中的节点有两种方式可以成为 Overload 节点：

- 当某节点在网络中由于承载业务较多，出现了超负荷工作状态，导致系统资源耗尽时，该节点会标志自己为 Overload 节点。
- 当网络管理员发现网络中某节点承载业务较多，出现 CPU 比较繁忙的状态时，可以通过执行 **set-overload** 命令，标志该节点为 Overload 节点。

在部署 MPLS TE 业务时，如果希望 TE 流量避开 Overload 节点，即建立的 CR-LSP 都不经过 Overload 节点，可以配置 CR-LSP 和 Overload 联动功能，这样可以减轻 Overload 节点的压力，同时也提高 CR-LSP 的可靠性。

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**，进入 MPLS 视图。

步骤 3 执行命令 **mpls te path-selection overload**，配置 CR-LSP 和 IS-IS Overload 联动功能，使能 CSPF 在算路的时候排除 IS-IS Overload（过载）节点，从而使流量避开 Overload 节点。

说明

配置 CR-LSP 和 IS-IS Overload 联动功能之前，需要首先执行 **mpls te cspf** 命令使能 CSPF 功能，并执行 **mpls te record-route** 命令配置隧道支持路由和标签记录。

在新的 CR-LSP 的建立过程中，流量依然在原来的 CR-LSP 上进行转发。当新的 CR-LSP 建立成功后，流量才会切换到新的 CR-LSP 上，原来的 CR-LSP 才会被删除。也就是流量的切换过程是 Make-before-break 的过程，期间流量不会丢失。

执行 **mpls te path-selection overload** 命令后：

- 已经建立好的 CR-LSP 会进行重优化，CSPF 会重新算路，使流量避开 Overload 节点。
- 对于新建的 LSP，则 CSPF 在进行路径计算时就会排除网络中的 Overload 节点，使流量避开 Overload 节点。

说明

该配置对旁路隧道不生效。

对于某一条 CR-LSP 来说，如果 Ingress 节点或者 Egress 节点被设置为 Overload 节点，那么执行 **mpls te path-selection overload** 命令对已经建立的 CR-LSP 不生效，即该 CR-LSP 不会进行重优化，新的 CR-LSP 无法建立。

----结束

3.7.5 配置隧道重建

通过配置隧道重建，可以定期重计算 CR-LSP 穿越的路由。如果重计算的路由优于当前路由，则创建一条新的 CR-LSP，为之分配新路由，并将业务从旧的 CR-LSP 切换至新的 CR-LSP，删除旧 CR-LSP。

背景信息

在 CR-LSP 隧道入节点进行如下配置。

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 tunnel interface-number**，进入 MPLS TE 隧道的 Tunnel 接口视图。

步骤 3 执行命令 **mpls te retry times**，配置隧道尝试重建的次数。

缺省情况下，尝试重建次数为 5。

步骤 4 执行命令 **mpls te timer retry interval**，配置重建隧道的间隔时间。

缺省情况下，重建隧道的时间间隔为 30 秒。

步骤 5 执行命令 **mpls te commit**，提交隧道当前配置。

如果隧道建立不成功，系统会每隔一定时间（即配置的重建隧道的间隔）开始新一轮重建，每轮的最大重建次数为配置的重建次数。

---结束

3.7.6 配置记录路由和标签

通过配置记录路由和标签功能，用户可以决定 RSVP-TE 隧道在建立过程中是否记录路由和标签。

背景信息

缺省情况下，不记录路由和标签。

在 CR-LSP 隧道入节点进行如下配置。

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 tunnel interface-number**，进入 MPLS TE 隧道的 Tunnel 接口视图。

步骤 3 执行命令 **mpls te record-route [label]**，建立隧道时记录路由和标签。

步骤 4 执行命令 **mpls te commit**，提交隧道当前配置。

---结束

3.7.7 配置 RSVP 信令延迟触发功能

当 MPLS 网络出现故障，需要重新创建大量 RSVP CR-LSP 时，重建大量 RSVP CR-LSP 需要占用不少系统资源。如果配置信令延时触发，则可以降低创建 RSVP CR-LSP 所占用的系统资源。

背景信息

在有大量 CR-LSP 经过的节点上进行如下配置。

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 **mpls**，进入 MPLS 视图。

步骤 3 执行命令 **mpls te signaling-delay-trigger enable**，使能 RSVP 信令延迟触发。

缺省情况下，不使能 RSVP 信令延迟触发。

---结束

3.7.8 检查配置结果

调整完成 MPLS TE 隧道的建立后，您可以查看 TE 隧道的属性。

前提条件

已经完成调整 MPLS TE 隧道建立功能的所有配置。

操作步骤

步骤 1 使用 `display mpls te tunnel-interface [tunnel interface-number]` 命令查看隧道接口信息。

----结束

任务示例

在配置成功时，执行上面的命令，应能得到如下的结果：

- 隧道的记录路由和标签分别为 Enabled
- 隧道重建次数和重建时间间隔
- 隧道的建立和保持优先级

3.8 调整流量的转发

调整 MPLS TE 流量的转发，可能导致 IP 流量或 MPLS 流量经过的路径变化、或限制 TE 隧道流量类型的配置。

3.8.1 建立配置任务

在调整流量的转发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 MPLS TE 中，影响流量转发是指可能导致 IP 流量或 MPLS 流量经过的路径变化、或限制 TE 隧道流量类型的配置。

本节介绍 MPLS TE 中影响流量转发的几种主要措施。

前置任务

本节介绍的配置需要与 CSPF、动态信令协议（如 RSVP-TE）配合使用。

在配置影响流量的转发之前，需完成以下任务：

- [配置 RSVP-TE 隧道](#)

数据准备

在调整 MPLS 流量转发前，需准备以下数据。

序号	数据
1	TE 隧道接口的编号
2	MPLS TE 链路的 TE 度量值
3	TE 隧道的 IGP 度量值
4	切换延迟时间和删除延迟时间

3.8.2 配置 IGP Shortcut

通过配置 IGP Shortcut，则不将这条 LSP 链路发布给邻居节点，因此其他节点不能使用此 LSP。

背景信息

 说明

如果配置了 IGP Shortcut，则不能同时配置转发邻接。

在 CR-LSP 隧道入节点进行如下配置。

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 tunnel interface-number`，进入 MPLS TE 隧道的 Tunnel 接口视图。

步骤 3 执行命令 `mpls te igp shortcut [isis | ospf]`，配置 IGP Shortcut。

 说明

缺省情况下，不使能 IGP Shortcut。

如果配置 IGP Shortcut 时不指定 IGP 类型，则缺省为 OSPF 和 IS-IS 都支持。

步骤 4 执行命令 `mpls te igp metric { absolute | relative } value`，配置 TE 隧道的 IGP 度量值。

缺省情况下，TE 隧道使用的度量值与 IGP 路径相同。

IS-IS 不支持相对度量。

用户可以指定在 IGP Shortcut 特性中计算路径时 TE 隧道使用的度量值：

- 如果使用绝对度量 **absolute**，则 TE 隧道的度量值就是配置的值；
- 如果使用相对度量 **relative**，则 TE 隧道的度量值是相应 IGP 路径度量值加上相对度量值。

步骤 5 执行命令 `mpls te commit`，提交隧道当前配置。

步骤 6 执行下面两种方式中的一种，配置 IGP Shortcut。

- 对于 IS-IS，执行命令 `isis enable [process-id]`，使能隧道接口的 IS-IS 进程。
- 对于 OSPF，执行以下三个命令：
 1. 执行命令 `quit`，退回系统视图。
 2. 执行命令 `ospf [process-id]`，进入 OSPF 协议视图。
 3. 执行命令 `enable traffic-adjustment`，使能 IGP Shortcut。

---结束

3.8.3 配置转发邻接

通过配置转发邻接，则将这条 LSP 发布给邻居节点，因此其他节点能够使用此 LSP。

背景信息

路由协议需要对链路进行双向检查。转发邻接将 LSP 链路发布给其他节点，所以在使用时，需要再配置一条返回的 Tunnel，构成双向 Tunnel，并分别使能这两条隧道的转发邻接。

说明

缺省情况下，关闭转发邻接特性。

如果配置了转发邻接，则不能同时配置 IGP Shortcut。

在 CR-LSP 隧道入节点进行如下配置。

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 tunnel interface-number**，进入 MPLS TE 隧道的 Tunnel 接口视图。

步骤 3 执行命令 **mpls te igp advertise [hold-time interval]**，配置转发邻接。

步骤 4 执行命令 **mpls te igp metric { absolute | relative } value**，配置 TE 隧道的 IGP 度量。

说明

IS-IS 不支持相对度量。

仔细选择 TE 隧道的 IGP 度量值，以保证 LSP 链路可以被正确发布和使用。例如，TE 隧道的度量值应该小于不希望流量使用的 IGP 路由的度量值。

步骤 5 执行命令 **mpls te commit**，提交隧道当前配置。

步骤 6 执行下面两种方式中的一种，配置转发邻接。

- 对于 IS-IS，执行命令 **isis enable [process-id]**，使能隧道接口的 IS-IS 进程。
- 对于 OSPF，执行以下三个命令：
 1. 执行命令 **quit**，退回系统视图。
 2. 执行命令 **ospf [process-id]**，进入 OSPF 协议视图。
 3. 执行命令 **enable traffic-adjustment advertise**，使能转发邻接。

---结束

3.8.4 配置切换延迟时间和删除延迟时间

为了避免在新 CR-LSP 建立前删除原 CR-LSP，需要配置切换延迟时间和删除延迟时间，从而避免流量中断。

背景信息

MPLS TE 采用 Make-before-break 机制。当 MPLS TE 隧道属性（例如，带宽和路径）改变时，需要建立符合新属性的 CR-LSP（也称为 Modified LSP）。为了在流量切换时尽可能不丢失数据，需要在原 CR-LSP（也称为 Primary LSP）被拆除前先建立新 CR-LSP。通过 Make-before-break 机制，预留新 CR-LSP 的带宽不被重复计算，即新 CR-LSP 与原 CR-LSP 共用带宽。

在实际应用中，当上游和下游节点的繁忙程度相差比较大时，有可能出现原 CR-LSP 被提前删除，导致流量短暂中断的现象。

为了避免这一问题，可以在隧道入节点上配置切换延迟时间和删除延迟时间。

请在隧道入节点上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入隧道入节点的系统视图。

步骤 2 执行命令 **mpls**，进入 MPLS 视图。

步骤 3 执行命令 **mpls te switch-delay switch-time delete-delay delete-time**，配置切换延迟时间和删除延迟时间。

缺省情况下，切换延迟时间是 5 秒，删除延迟时间是 7 秒。

---结束

3.8.5 检查配置结果

调整流量的转发后，您可以查看流量转发的相关信息。

前提条件

已经完成调整流量转发的所有配置。

操作步骤

步骤 1 使用 **display current-configuration** 命令查看调整流量转发的相关信息。

---结束

任务示例

在配置成功时，执行上面的命令，应能得到如下的结果：

- IGP 度量值
- 切换延迟时间和删除延迟时间

3.9 调整带宽的泛洪阈值

通过调整带宽的泛洪阈值，可以抑制更新 TEDB 和泛洪的频率，避免对网络资源造成浪费。

3.9.1 建立配置任务

在调整带宽的泛洪阈值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

为了形成本 IGP 区域内统一的流量工程数据库，当 MPLS 接口的剩余带宽发生变化时，OSPF TE 和 IS-IS TE 需要更新 TEDB 并进行泛洪。

当节点上创建大量需要预留带宽的隧道时，系统会频繁更新 TEDB（Traffic Engineering DataBase）并泛洪。例如某条链路带宽为 100Mbit/s，在此链路上建立 100 条 1Mbit/s 的 TE 隧道时，则需要进行 100 次泛洪。

为了抑制更新 TEDB 和泛洪的频率，系统提供以下机制：

- 当一条链路上为 MPLS TE 隧道保留的带宽与 TEDB 中的链路剩余带宽的比值等于或大于设定的阈值（称为带宽的泛洪阈值）时，OSPF TE 和 IS-IS TE 将该链路信息泛洪到域内的所有节点，并更新 TEDB。
- MPLS TE 隧道释放的带宽与 TEDB 中剩余带宽的比值等于或大于设定的阈值时，OSPF TE 和 IS-IS TE 将该链路信息泛洪到域内的所有节点，并更新 TEDB。

该阈值缺省值为 10%，用户可以通过命令行进行手工调整。

前置任务

在调整带宽的泛洪阈值之前，需完成以下任务：

- [配置 RSVP-TE 隧道](#)

数据准备

在调整带宽的泛洪阈值之前，需准备以下数据。

序号	数据
1	带宽的泛洪阈值

3.9.2 配置带宽的泛洪阈值

带宽的泛洪值是指 TE 隧道占用或释放的链路带宽与 TEDB 中剩余的链路带宽的比值。

背景信息

带宽的泛洪值是指 TE 隧道占用或释放的链路带宽与 TEDB 中剩余的链路带宽的比值。

链路带宽变化很小时对带宽进行泛洪会浪费网络资源。例如某条链路带宽为 100M，在此链路上建立 100 条 1M 的 TE 隧道时，则需要进行 100 次泛洪。

如果设置泛洪阈值为 10%，则建立第 1～9 条时不进行泛洪；当建立第 10 条时才对第 1～10 条所占用的 10M 带宽进行泛洪。当建立第 11～18 条隧道时不进行泛洪，当建立第 19 条时才泛洪。依此类推。因此配置带宽泛洪阈值可减少泛洪次数，节约网络资源。

缺省情况下，当一条链路上为 MPLS TE 隧道保留的带宽与 TEDB 中的链路剩余带宽的比值等于或大于 10%，或 MPLS TE 隧道释放的带宽与 TEDB 中剩余带宽的比值等于或大于 10% 时，IGP 将对该链路信息进行泛洪，OSPF 更新 TEDB。

在 CR-LSP 隧道 Ingress 或 Transit 节点进行如下配置。

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`，进入使能了 MPLS TE 的链路接口的视图。

步骤 3 执行命令 `mpls te bandwidth change thresholds { down | up } percent`，配置带宽的泛洪阈值。

泛洪阈值只能在物理接口下配置。

---结束

3.9.3 检查配置结果

调整带宽的泛洪阈值后，您可以查看泛洪阈值的信息。

前提条件

已经完成调整带宽的泛洪阈值的所有配置。

操作步骤

步骤 1 使用 `display current-configuration` 命令查看带宽的泛洪阈值信息。

---结束

任务示例

在配置成功时，执行上面的命令，应能得到如下的结果：

- 带宽的泛洪阈值

3.10 配置 TE 隧道流量限速

如果要使 TE 流量被限定在实际配置的隧道带宽范围内，则需要对该 TE 隧道配置 TE 流量限速。

3.10.1 建立配置任务

在配置 TE 隧道流量限速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

某条 TE 隧道的实际物理链路中，除了承载该 TE 隧道的流量，可能还同时承载了其他 TE 隧道的流量、其他非 CR-LSP 的 MPLS 流量，甚至 IP 流量。如果要使 TE 流量被限定在实际配置的隧道带宽范围内，则需要对该 TE 隧道配置 TE 流量限速。

配置 TE 流量限速后，TE 流量被限定在实际配置的隧道带宽范围内；超出隧道带宽的 TE 流量被丢弃。

前置任务

在配置 TE 流量限速之前，需完成以下任务：

- [配置静态 CR-LSP](#) 或者 [配置 RSVP-TE 隧道](#)

数据准备

在配置 TE 流量限速之前，需准备以下数据。

序号	数据
1	需要进行流量限速的 TE 隧道接口编号

3.10.2 配置 TE 流量限速

配置 TE 流量限速之前，需要保证对应的隧道接口配置了带宽。

背景信息

 说明

配置 TE 流量限速之前，需要保证对应的 Tunnel 接口配置了 **mpls te bandwidth** 命令。如果 Tunnel 接口没有配置 **mpls te bandwidth** 命令，则不进行 TE 流量限速。

在隧道入节点上进行如下配置。

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 tunnel interface-number**，进入 Tunnel 接口视图。
- 步骤 3** 执行命令 **mpls te lsp-tp outbound**，配置 TE 流量监管。
- 步骤 4** 执行命令 **mpls te commit**，使配置生效。

----结束

3.10.3 检查配置结果

TE 隧道流量限速配置成功后，您可以查看 TE 流量监管信息。

前提条件

已经完成 TE 流量限速功能的所有配置。

操作步骤

- 使用 **display mpls te tunnel-interface [tunnel interface-number]** 命令查看隧道接口信息。

----结束

任务示例

执行命令 **display mpls te tunnel-interface**，可看到显示结果中，“Car Policy”字段对应的值为“Enable”。

3.11 配置手工 TE FRR

手工 TE FRR 是 MPLS TE 中的一种局部性保护机制，用于保护主隧道的链路和节点故障，需要用户手工配置旁路隧道。

3.11.1 建立配置任务

在配置 TE FRR 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

MPLS TE 快速重路由特性为网络提供了一种快速的局部保护。它一般部署在对可靠性要求比较高的网络中，当网络中出现局部失效的时候，快速重路由可以很快地切换到保护隧道，从而对业务的影响较小。

骨干网不但容量大，而且对可靠性也有较高的要求。在出现局部失效的情况下，需要有自动保护和快速恢复机制。而 MPLS TE 的 LSP 一般是通过 RSVP 协议按照 DOD 的方式建立的。在失效引起的路由改变扩散到头节点之前，CSPF 无法算出有效路径；另外，局部失效可能会引起网络中多条 LSP 重建，重建过程中很可能出现带宽不够的问题。这些都导致 MPLS TE 网络从局部失效中恢复的时间可能会较长。

通过在接口上配置 TE FRR 快速重路由保护，就可以在链路或节点失效时，自动地将流量快速切换到保护链路上；然后当被保护的主隧道恢复正常或建立了新的主隧道，流量又会快速回切到原来的主隧道或切换到新建立的主隧道上。从而满足了 MPLS TE 网络的可靠性要求。

说明

- 由于 FRR 使用的旁路隧道需要预先建立，占用额外的带宽，因此，在网络带宽余量不多的情况下，应该只对关键的接口或链路进行 TE FRR 保护。
- SE 风格的 RSVP-TE 隧道支持 FRR；静态 TE 隧道不支持 FRR。

TE FRR 能够与以下特性配合使用：

- 拔板保护

设备支持当 PLR 上的主隧道出接口所在接口板被拔出时，将 MPLS TE 流量快速切换到旁路隧道上。当被拔出的接口板再次插入时，如果主隧道的出接口仍处于可用状态，可进行 MPLS TE 流量的回切。拔板保护主要是保护 PLR 节点上的主隧道出接口。

如果使用 TE FRR 拔板保护功能，PLR 的主隧道 Tunnel 接口、旁路隧道的 Tunnel 接口及旁路隧道的出接口都不能在被拔出的接口板上。建议将 PLR 上的 TE Tunnel 接口配置在主控板上。

说明

LSP 或 CR-LSP 所在接口被删除或接口所在单板被拔出，该接口变为 stale 状态，这类接口称为废弃接口。如果一个节点上废弃接口数目已达到 License 规定的最大数，如果再将主隧道物理出接口所在接口板拔出或故障，则该节点不能对这条主隧道进行 FRR 保护功能。

- RSVP GR

AR1200 支持 RSVP GR 期间进行 TE FRR。即，当 PLR、PLR 上游节点、MP、MP 下游节点中的任意一个节点因故障重启或者进行主备倒换，同时 PLR 的主隧道出接口故障时，进行隧道保护，减短故障时间。

RSVP GR 期间，由隧道出接口的 Down 事件触发 FRR 切换。

前置任务

在配置 MPLS TE FRR 之前，需完成以下任务：

- 配置 RSVP-TE 主隧道
- 在旁路隧道节点的 MPLS 视图和物理接口视图下使能 MPLS TE 和 RSVP-TE，请参见 [3.3.2 使能 MPLS TE 和 RSVP-TE](#)
- （可选）配置旁路隧道的物理链路带宽，请参见 [（可选）配置链路的带宽](#)
- 在 PLR 上使能 CSPF
- （可选）配置旁路隧道的显式路径

数据准备

在配置 MPLS TE FRR 之前，需准备以下数据。

序号	数据
1	FRR 的保护策略，即，确定保护的對象是链路还是节点
2	旁路隧道要保护的接口名称
3	（可选）旁路隧道的显式路径和带宽等信息
4	（可选）TE FRR 扫描间隔
5	（可选）PSB 和 RSB 的超时倍数

3.11.2 使能 TE FRR

在主隧道使能 TE FRR 后，才能够创建旁路隧道。

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 tunnel tunnel-number`，进入主隧道的 Tunnel 接口视图。
- 步骤 3** 执行命令 `mpls te fast-reroute [bandwidth]`，使能 TE FRR。
- 步骤 4** 执行命令 `mpls te commit`，提交隧道配置。

----结束

3.11.3 配置旁路隧道

旁路隧道用于为主隧道的链路或者节点提供局部保护，配置手工 TE FRR 时需要手工指定旁路隧道的路径和属性。

背景信息

在配置旁路隧道时，需要先规划好它所保护的链路或节点，并确保该旁路隧道不会经过它所保护的链路或节点，否则不能真正起到保护作用。

说明

- TE FRR 不支持多点故障。即，如果发生了 FRR 切换，数据从主隧道切换到旁路隧道，在数据通过旁路隧道转发期间，旁路隧道的状态必须始终保持 Up。一旦旁路隧道在此期间状态变为 Down，被保护的数据将不能通过 MPLS 转发，从而可能出现流量中断，FRR 功能失效。以后即使旁路隧道状态重新变为 Up，流量也无法再通过旁路隧道转发，只能等待主隧道恢复或重新创建后，流量才能恢复从主隧道转发。
- 缺省情况下，系统每隔 1 秒会为每条主隧道从当前所有手工配置的旁路隧道中查找最优的旁路隧道，并将该旁路隧道与主隧道绑定。

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 tunnel tunnel-number**，进入旁路隧道的 Tunnel 接口视图。

步骤 3 配置旁路隧道接口的 IP 地址，选择如下方式之一：

- 执行命令 **ip address ip-address { mask | mask-length } [sub]**，配置 Tunnel 接口的 IP 地址。
- 执行命令 **ip address unnumbered interface interface-type interface-number**，配置隧道接口借用其他接口的 IP 地址。

说明

为实现流量转发，Tunnel 接口必须具有 IP 地址。但 MPLS TE 隧道是单向的，不存在对端地址的问题，所以没有必要为 Tunnel 接口单独配置 IP 地址。通常的做法是 Tunnel 接口借用本节点作为 LSR ID 的 Loopback 接口的地址。

步骤 4 执行命令 **tunnel-protocol mpls te**，指定隧道协议为 MPLS TE。

步骤 5 执行命令 **destination ip-address**，配置旁路隧道的目的地址为 MP 节点的 LSR ID。

步骤 6 执行命令 **mpls te tunnel-id tunnel-id**，配置旁路隧道的 Tunnel-ID。

步骤 7（可选）执行命令 **mpls te path explicit-path path-name**，配置旁路隧道使用的显式路径。

说明

旁路隧道经过的路径和主隧道经过的路径不能有重叠的物理链路。

步骤 8 执行命令 **mpls te bypass-tunnel**，使能旁路隧道。

配置旁路隧道后，系统会自动使能记录路由功能，即记录隧道的详细路径信息。

说明

- 同一个 Tunnel 接口不能同时作为旁路隧道和备份隧道，即不能同时配置 **mpls te bypass-tunnel** 命令和 **mpls te backup** 命令。
- 同一个 Tunnel 接口不能同时作为旁路隧道和主隧道，即不能同时配置 **mpls te bypass-tunnel** 命令和 **mpls te fast-reroute** 命令。

否则无法达到保护的目。

步骤 9 执行命令 **mpls te protected-interface interface-type interface-number**，指定旁路隧道要保护的接口。

 说明

- 一条隧道最多能同时保护 6 个物理接口。
- 同一个 Tunnel 接口不能同时作为旁路隧道和备份隧道，即不能同时配置 `mpls te protected-interface` 命令和 `mpls te backup` 命令。

步骤 10 执行命令 `mpls te commit`，提交隧道配置。

---结束

3.11.4 （可选）配置 TE FRR 扫描定时器

配置 TE FRR 后，系统会定时为每条主隧道从当前所有手工配置的旁路隧道中查找最优的旁路隧道，并将该旁路隧道与主隧道绑定。TE FRR 扫描定时器用于设置对 LSP 进行扫描的时间间隔。

操作步骤

步骤 1 执行命令 `system-view`，进入 PLR 节点的系统视图。

步骤 2 执行命令 `mpls`，进入 MPLS 视图。

步骤 3 执行命令 `mpls te timer fast-reroute [weight]`，配置 TE FRR 扫描间隔。

缺省情况下，PLR 对节点上所有 LSP 的扫描间隔为 1000 毫秒（1 秒）。

设置了扫描时间间隔权值后，系统使用以下公式计算出扫描时间间隔 $t1$ 。

$$t1 = (\text{weight} \times 200 \div \text{产品能创建的 RSVP LSP 最大数量}) \times 1000$$

 说明

如果计算出的 $t1$ 大于 1000 毫秒，则以 $t1$ 的值作为实际扫描间隔；否则扫描间隔为 1000 毫秒（1 秒）。

---结束

3.11.5 （可选）修改 PSB 和 RSB 的超时倍数

为了支持在 RSVP GR 期间进行 TE FRR，需要修改 PSB 和 RSB 的超时倍数。防止由于 LSP 数量过多导致 GR 时间过长，而致使 PSB 和 RSB 因超时而被丢弃。

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`，进入 MPLS 视图。

步骤 3 执行命令 `mpls rsdp-te keep-multiplier number`，设置 PSB 和 RSB 的超时倍数。

缺省情况下，PSB 和 RSB 的超时倍数为 3。

 说明

当网络中 CR-LSP 数量过多，并且配置了 RSVP GR 功能时，建议将 PSB 和 RSB 的超时倍数设置为大于或等于 5。

---结束

3.11.6 检查配置结果

手工 TE FRR 配置成功后，可以查看到被保护的主隧道和旁路隧道信息。

前提条件

已经完成手工 TE FRR 功能的所有配置。

操作步骤

- 使用 **display mpls lsp [lsp-id ingress-lsr-id session-id lsp-id] [verbose]** 命令查看主 LSP 的信息。
- 使用 **display mpls lsp attribute bypass-inuse { inuse | not-exists | exists-not-used }** 命令查看 Bypass LSP 的信息。
- 使用 **display mpls lsp attribute bypass-tunnel tunnel-name** 命令查看 Bypass Tunnel 所绑定的主隧道的信息。
- 使用 **display mpls te tunnel-interface [tunnel tunnel-number | auto-bypass-tunnel tunnel-name]** 命令查看主隧道或旁路隧道接口的详细信息。
- 使用 **display mpls te tunnel path [[tunnel-name] tunnel-name] [lsp-id ingress-lsr-id session-id] | fast-reroute { local-protection-available | local-protection-inuse } | lsr-role { ingress | transit | egress }** 命令查看主隧道和旁路隧道的路径信息。

----结束

任务示例

执行命令 **display mpls te tunnel-interface**，应能查看到主隧道或旁路隧道接口的详细信息。

```
<Huawei> display mpls te tunnel-interface tunnel 1/0/0
-----
                        Tunnel/0/0
-----
Tunnel State Desc   : GRACEFUL SWITCH
Active LSP          : Best-Effort LSP
Traffic Switch      : Best-Effort LSP -> Ordinary LSP
Session ID          : 50
Ingress LSR ID     : 1.1.1.1           Egress LSR ID: 2.2.2.2
Admin State         : UP                Oper State    : UP
Primary LSP State   : DOWN
  Main LSP State    : SETTING UP
Hot-Standby LSP State : UP
  Main LSP State    : READY             LSP ID       : 32799
  Modify LSP State  : SETTING UP
Ordinary LSP State  : UP
  Main LSP State    : READY             LSP ID       : 32782
Best-Effort LSP State : UP
  Main LSP State    : READY             LSP ID       : 32780
```

执行命令 **display mpls te tunnel path**，应能查看到主隧道和旁路隧道的路径信息。

```
<Huawei> display mpls te tunnel path
Tunnel Interface Name : Tunnel/0/0
Lsp ID : 1.1.1.9 :100 :1024
Hop Information
Hop 0  10.1.1.1
Hop 1  10.1.1.2
Hop 2  2.2.2.9
Hop 3  20.1.1.1
Hop 4  20.1.1.2
```

```
Hop 5 3.3.3.9
Tunnel Interface Name : Tunnel/0/0
Lsp ID : 1.1.1.9 :100 :2048
Hop Information
Hop 0 30.1.1.1
Hop 1 30.1.1.2
Hop 2 4.4.4.9
Hop 3 40.1.1.1
Hop 4 40.1.1.2
Hop 5 3.3.3.9
```

3.12 配置 MPLS TE Auto FRR

MPLS TE Auto FRR 是 MPLS TE 中的一种局部性保护机制，用于保护 CR-LSP 的链路和节点故障，用户无需手工配置。

3.12.1 建立配置任务

在配置 MPLS TE Auto FRR 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

在对业务可靠性要求较高的网络中，通常会配置 FRR 保护，来提高网络的可靠性。如果网络拓扑比较复杂，需要配置的链路较多，这种配置工作就会非常繁琐。

自动快速重路由（Auto FRR）能够自动创建满足条件的旁路隧道，从而降低了配置工作量。

MPLS TE Auto FRR 和普通的 MPLS TE FRR 一样，支持拔板保护和 RSVP GR 期间进行 FRR。相关介绍请参见[配置手工 TE FRR](#)。

前置任务

在配置 MPLS TE Auto FRR 之前，需要完成以下任务：

- 配置 RSVP-TE 主隧道
- 在旁路隧道各节点上全局和物理接口视图下使能 MPLS、MPLS TE 和 RSVP-TE，请参见 [3.3.2 使能 MPLS TE 和 RSVP-TE](#)
- 在主隧道入节点和中间节点使能 CSPF

数据准备

在配置 MPLS TE Auto FRR 之前，需准备以下数据。

序号	数据
1	Auto FRR 的保护策略，即，确定保护的對象是链路还是节点
2	（可选）Bypass Tunnel 的带宽
3	（可选）TE FRR 扫描间隔

3.12.2 使能 TE Auto FRR

使能 TE Auto FRR 功能是配置自动 TE FRR 的首要步骤。

背景信息

在主隧道的入节点或中间节点上执行如下操作：

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`，进入 MPLS 视图。
- 步骤 3** 执行命令 `mpls te auto-frr`，全局使能 MPLS TE Auto FRR。
- 步骤 4** 执行命令 `quit`，退回系统视图。
- 步骤 5** 执行命令 `interface interface-type interface-number`，进入主隧道出接口的接口视图。
- 步骤 6**（可选）执行命令 `mpls te auto-frr { link | node | default }`，使能 TE Auto FRR。

缺省情况下，全局使能 Auto FRR 后，该设备的所有使能 MPLS TE 的接口都自动配置了 `mpls te auto-frr default`。如果要去使能部分接口的 Auto FRR，需在这些接口下配置命令 `undo mpls te auto-frr`。在接口下配置命令 `undo mpls te auto-frr` 后，不论全局是否已使能或重新使能 Auto FRR，该接口都不具有 Auto FRR 能力。

缺省情况下，未使能 TE Auto FRR。

说明

- 如果在接口下配置 `mpls te auto-frr default` 命令，则接口 Auto FRR 能力与全局 Auto FRR 能力保持一致。
- 使能节点保护后，当拓扑不满足而导致节点保护的旁路隧道创建不成功时，主隧道的倒数第二跳会试图创建链路保护，其他节点则不会降级创建链路保护。

---结束

3.12.3 使能 TE FRR 并配置自动旁路隧道的属性

使能 TE FRR 后系统自动建立旁路保护隧道，无需用户手工干预。

背景信息

请在主隧道的入节点上进行如下配置。

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 tunnel interface-number`，进入主隧道的 tunnel 视图。
- 步骤 3** 执行命令 `tunnel-protocol mpls te` 配置隧道协议为 MPLS TE。
- 步骤 4** 执行命令 `mpls te fast-reroute [bandwidth]`，使能 TE FRR。

如果要求对隧道进行带宽保护，则需要配置参数 `bandwidth`。

步骤 5 (可选) 执行命令 `mpls te bypass-attributes bandwidth bandwidth [priority setup-priority [hold-priority]]`，配置自动旁路隧道的属性。

 说明

- 只有主隧道配置了 `mpls te fast-reroute bandwidth` 后，才能配置旁路隧道的属性。
- 自动旁路隧道的带宽不能大于主隧道的带宽。
- 如果没有配置自动旁路隧道的属性，默认自动旁路隧道的带宽和主隧道的带宽相同。
- 旁路隧道的建立优先级不能高于其保持优先级，并且，二者均不能高于主隧道的相应优先级。
- 当主隧道的带宽值改变或去使能 TE FRR 后，旁路隧道的属性会被自动清除。
- 同一个 TE 隧道接口下，旁路隧道带宽配置与多 CT 配置互斥。

步骤 6 执行命令 `mpls te commit`，提交隧道当前配置。

----结束

3.12.4 (可选) 配置 TE FRR 扫描定时器

通过配置 TE FRR 扫描定时器，可以查找符合成为 Bypass 的那些 LSP，并将其中最优的 LSP 与主 LSP 绑定。

背景信息

请在 PLR 节点上进行如下配置。

操作步骤

步骤 1 执行命令 `system-view`，进入 PLR 节点的系统视图。

步骤 2 执行命令 `mpls`，进入 MPLS 视图。

步骤 3 执行命令 `mpls te timer fast-reroute [weight]`，配置 TE FRR 扫描间隔。

设置了扫描时间间隔权值后，系统使用以下公式计算出扫描时间间隔 t1。

$$t1 = weight \times 1000 \times 200 \div \text{产品能创建的 RSVP LSP 最大数量}$$

如果计算出的 t1 大于 1000 毫秒，则以 t1 的值作为实际扫描间隔；否则扫描间隔为 1000 毫秒。

缺省情况下，PLR 对节点上所有 LSP 的扫描间隔为 1000 毫秒（1 秒）。

配置 FRR 后，PLR 定时扫描，查找符合成为 Bypass 的那些 LSP，并将其中最优的 LSP 与主 LSP 绑定。FRR 切换后，一旦被保护的 LSP 恢复正常或建立了新的 LSP，流量会回切到原 LSP 或切换到新建立的 LSP 上。

----结束

3.12.5 (可选) 修改 PSB 和 RSB 的超时倍数

为了支持在 RSVP GR 期间进行 TE FRR，需要修改 PSB 和 RSB 的超时倍数。

背景信息

为了支持在 RSVP GR 期间进行 FRR，请在隧道各节点上进行如下配置。

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 `mpls`，进入 MPLS 视图。

步骤 3 执行命令 `mpls rsvp-te keep-multiplier number`，设置 PSB 和 RSB 的超时倍数。

建议将 PSB 和 RSB 的超时倍数设置为大于或等于 5，防止 PSB 和 RSB 因 LSP 数量过多而被丢失。

---结束

3.12.6 检查配置结果

MPLS TE Auto FRR 配置成功后，您可以查看旁路隧道的详细信息。

前提条件

已经完成 MPLS TE Auto FRR 功能的所有配置。

操作步骤

- 使用 `display mpls te tunnel verbose` 命令查看主隧道和自动旁路隧道的绑定信息。
- 使用 `display mpls te tunnel-interface [tunnel interface-number | auto-bypass-tunnel tunnel-name]` 命令查看自动旁路隧道的详细信息。
- 使用 `display mpls te tunnel path [[tunnel-name] tunnel-name] [lsp-id ingress-lsr-id session-id] | fast-reroute { local-protection-available | local-protection-inuse } | lsr-role { ingress | transit | egress }` 命令查看主隧道和旁路隧道的路径信息。

---结束

3.13 配置 CR-LSP 备份

通过配置 CR-LSP 备份，可以实现对 CR-LSP 端到端的保护。

3.13.1 建立配置任务

在配置 CR-LSP 备份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

在对业务可靠性要求较高的网络中，通常会配置备份 CR-LSP 来提供端到端的保护，提高网络的可靠性。当主 CR-LSP 故障时，流量能够及时切换到备份 CR-LSP 上，确保用户业务不中断。

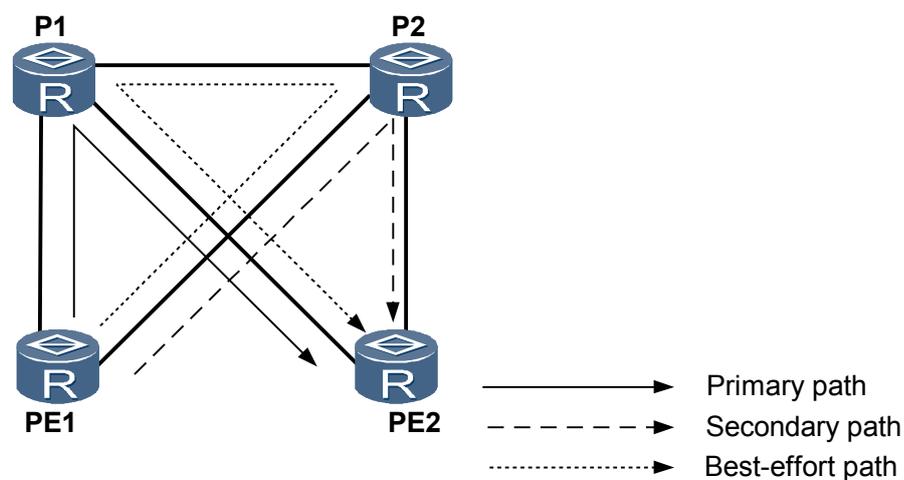
CR-LSP 支持热备份模式和普通备份模式。为了增强可靠性，当备份模式失效后，还提供了逃生路径模式，具体请参见表 3-1。

表 3-1 CR-LSP 备份模式

备份模式	简要描述	优点	缺点
热备份模式	系统在建立主 CR-LSP 的同时，会创建一条与主 CR-LSP 路径分离的备份 CR-LSP	流量切换速度快	如果没有配置热备份 CR-LSP 动态带宽功能，则需要占用额外的带宽
普通备份模式	当主 CR-LSP 失效后，系统将使用其他显式路径建立 CR-LSP	无需占用额外的带宽	流量切换速度不如热备份模式快
逃生路径模式	当主 CR-LSP 和备份 CR-LSP 都失效后，系统将使用剩余的路径建立逃生路径	对路径建立的要求较为宽松，容易建立	可能会降低某些 QoS 保证

如图 3-1，主 CR-LSP 路径为 PE1→P1→PE2；备份 CR-LSP 路径为 PE1→P2→PE2；逃生路径为 PE1→P2→P1→PE2。

图 3-1 逃生路径示意图



前置任务

在配置 CR-LSP 备份之前，需完成以下任务：

- 配置 RSVP-TE 主隧道
- 在备份 CR-LSP 各节点的全局和接口下使能 MPLS、MPLS TE 和 RSVP-TE，请参见 [3.3.2 使能 MPLS TE 和 RSVP-TE](#)

数据准备

在配置 CR-LSP 备份之前，需准备以下数据。

序号	数据
1	确定采用的备份方法
2	(可选) 备份 CR-LSP 使用的显式路径
3	(可选) 备份 CR-LSP 的亲属性
4	(可选) 备份 CR-LSP 的跳数限制值

3.13.2 配置 CR-LSP 备份

主隧道配置 CR-LSP 备份后, 当主 CR-LSP 故障时, 流量会切换到备份 CR-LSP 上, 从而提供了端到端的保护。

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 tunnel tunnel-number**, 进入 MPLS TE 隧道的 Tunnel 接口视图。

步骤 3 执行命令 **mpls te backup { hot-standby [wtr interval] | ordinary }**, 配置备份 CR-LSP 的建立方式。

 说明

同一个 Tunnel 接口不能同时作为备份 CR-LSP 和旁路隧道, 既不能同时配置 **mpls te backup** 命令和 **mpls te bypass-tunnel** 命令, 也不能同时配置 **mpls te backup** 命令和 **mpls te protected-interface** 命令。

配置热备份或普通备份模式后, 系统会自动选择备份 CR-LSP 的路径。如果用户希望流量沿着指定的备份 CR-LSP 通过, 可以执行步骤 4 ~ 6 中的一个或多个步骤进行配置。

步骤 4 (可选) 执行命令 **mpls te path explicit-path path-name secondary**, 指定备份 CR-LSP 使用的显式路径。

 说明

在规划备份 CR-LSP 使用的显式路径时, 注意不要与主 CR-LSP 完全重合, 否则无法达到保护的目。

必须先的系统视图下执行 **explicit-path** 命令配置相应的显式路径并为显式路径指定节点, 否则该命令配置不成功。

步骤 5 (可选) 执行命令 **mpls te affinity property properties [mask mask-value] secondary**, 配置备份 CR-LSP 的亲属性。

缺省情况下, 备份 CR-LSP 的亲属性值为 0x0。

步骤 6 (可选) 执行命令 **mpls te hop-limit hop-limit-value secondary**, 限制该备份 CR-LSP 的路径跳数。

缺省情况下, 备份 CR-LSP 的路径跳数是 32。

步骤 7 执行命令 **mpls te commit**, 提交隧道配置。

---结束

3.13.3 （可选）配置热备份 CR-LSP 动态带宽功能

在主隧道的入节点配置热备份 CR-LSP 动态带宽功能，可以使热备份 CR-LSP 在主 CR-LSP 出现故障之前不占用带宽，节约带宽资源。

背景信息

缺省情况下，创建热备份 CR-LSP 需要占用额外的带宽资源。而使用热备份动态带宽功能则可以在创建主隧道的同时，创建带宽为 0 的热备份 CR-LSP。在主 CR-LSP 出现故障之前，不会占用网络中的带宽资源。当主隧道故障时，系统将采用 Make-before-break 机制，重建一条满足带宽要求的热备份 CR-LSP。此时如果带宽资源不足，则流量会切换到最初创建的带宽为 0 的热备份 CR-LSP，确保切换过程中流量不中断。

操作步骤

步骤 1 执行命令 `system-view`，进入系统视图。

步骤 2 执行命令 `interface tunnel tunnel-number`，进入 MPLS TE 隧道的 Tunnel 接口视图。

步骤 3 执行命令 `tunnel-protocol mpls te`，配置隧道协议为 MPLS TE。

步骤 4 执行命令 `mpls te backup hot-standby dynamic-bandwidth`，配置热备份 CR-LSP 动态带宽功能。

 说明

- 如果已经使用热备份模式创建了一条热备份 CR-LSP，那么配置热备份 CR-LSP 动态带宽功能后，系统将采用 Make-before-break 机制重建一条带宽值为 0 的热备份 CR-LSP，并替代原来的热备份 CR-LSP。
- 用户可以使用命令 `undo mpls te backup hot-standby dynamic-bandwidth` 取消 hot-standby 备份路径动态带宽功能，使热备份 CR-LSP 重新占用带宽。

步骤 5 执行命令 `mpls te commit`，提交隧道配置。

---结束

3.13.4 （可选）配置逃生路径

主隧道的入节点配置逃生路径后，当主 CR-LSP 和备份 CR-LSP 都故障时，流量会切换到逃生路径上。

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 tunnel tunnel-number`，进入 MPLS TE 隧道的 Tunnel 接口视图。

步骤 3 执行命令 `mpls te backup ordinary best-effort`，配置逃生路径。

 说明

逃生路径不能和手工配置的普通备份模式同时配置，即不能同时配置 `mpls te backup ordinary best-effort` 命令和 `mpls te backup ordinary` 命令。

如果用户希望逃生路径沿着指定的路径建立，可以选择步骤 4 和 5 中的一个或多个进行配置。

步骤 4 （可选）执行命令 `mpls te affinity property properties [mask mask-value] best-effort`，配置逃生路径的亲属性和。

缺省情况下，逃生路径的亲属性和属性值为 0x0。

步骤 5 (可选) 执行命令 **mpls te hop-limit hop-limit-value best-effort**，限制该逃生路径的路径跳数。

缺省情况下，逃生路径的路径跳数是 32。

步骤 6 执行命令 **mpls te commit**，提交隧道配置。

---结束

3.13.5 检查配置结果

CR-LSP 备份配置成功后，可以查看到隧道接口和备份状态等信息。

前提条件

已经完成 CR-LSP 备份功能的所有配置。

操作步骤

- 使用 **display mpls te tunnel-interface [tunnel tunnel-number]**命令查看隧道接口信息。
- 使用 **display mpls te hot-standby state { all [verbose] | interface tunnel interface-number }**命令查看热备份状态信息。
- 使用 **display mpls te tunnel [destination ip-address] [lsp-id ingress-lsr-id session-id local-lsp-id] [lsr-role { all | egress | ingress | remote | transit }] [name tunnel-name] [{ incoming-interface | interface | outgoing-interface } interface-type interface-number] [te-class0 | te-class1 | te-class2 | te-class3 | te-class4 | te-class5 | te-class6 | te-class7] [verbose]**命令查看隧道的 CR-LSP 信息。

---结束

3.14 配置旁路保护隧道与备份 CR-LSP 同步

介绍当主 CR-LSP 故障后，系统启用 TE FRR 旁路保护隧道并尝试恢复主 CR-LSP 的同时，也尝试创建备份 CR-LSP 的配置方法。

3.14.1 建立配置任务

在进行旁路保护隧道与备份 CR-LSP 同步的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

对于需要重点保护的链路和节点，可以同时配置 TE FRR 的局部保护和备份 CR-LSP 的端到端保护，且后者的可靠性高于前者。因此为了增加隧道的安全性，建议配置旁路保护隧道与备份 CR-LSP 同步的功能。

- 如果配置的是普通备份：
 - 当被保护链路或节点出现故障时，流量切换到 TE FRR 的旁路保护隧道并尝试恢复主 CR-LSP 的同时，也会尝试创建备份 CR-LSP。

- 当备份 CR-LSP 创建成功，并且主 CR-LSP 未恢复时，流量会切换到备份 CR-LSP。
- 当备份 CR-LSP 创建不成功，且主 CR-LSP 未恢复时，流量仍然从旁路保护隧道通过。
- 如果配置的是热备份：
 - 如果备份 CR-LSP 的状态为 Up，且被保护链路或节点出现故障时，则流量先切换到旁路保护隧道后，立即切换到备份 CR-LSP 上，同时尝试恢复主 CR-LSP。
 - 如果备份 CR-LSP 的状态为 Down，则处理方式与普通备份相同。

当主 CR-LSP 处于 Up 状态的同时，如果热备份 CR-LSP 也处于 Up 状态，则需要占用额外的带宽。而普通备份 CR-LSP 在主 CR-LSP 处于 Frr-in-use 状态时才开始创建，在主 CR-LSP 没有出现故障时，不需要占用额外的带宽资源。因此推荐选择普通备份的方式。

前置任务

在配置旁路保护隧道与备份 CR-LSP 同步之前，需要完成以下任务：

- 配置 RSVP-TE 主隧道
- 配置手工 MPLS TE FRR 或者 MPLS TE Auto FRR，请参见[配置手工 TE FRR](#) 或者 [配置 MPLS Auto TE FRR](#)
- 配置 CR-LSP 备份，可选择热备份或者普通备份方式（逃生路径除外），请参见[配置 CR-LSP 备份](#)

数据准备

在配置旁路保护隧道与备份 CR-LSP 同步之前，需准备以下数据。

序号	数据
1	TE FRR 的保护策略，即，确定保护的對象是链路还是节点
2	确定采用的备份方式

3.14.2 使能旁路保护隧道与备份 CR-LSP 同步

通过使能旁路保护隧道与备份 CR-LSP 同步的配置，可以实现保护整条 LSP 的目的

背景信息

在主隧道的入节点上执行如下操作：

 说明

配置此命令之前，必须先配置热备份或者普通备份方式（逃生路径除外）的端到端保护以及 TE FRR 的局部保护功能。

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 `interface tunnel interface-number`，进入 MPLS TE 隧道的 Tunnel 接口视图。

步骤 3 执行命令 `mpls te backup frr-in-use`，配置当主 CR-LSP 故障后，系统启用 TE FRR 旁路保护隧道（即主 CR-LSP 处于 Frr-in-use 状态）并尝试恢复主 CR-LSP 的同时，也会尝试创建备份 CR-LSP。

步骤 4 执行命令 `mpls te commit`，提交隧道配置。

步骤 5 执行命令 `quit`，退回系统视图。

----结束

3.14.3 检查配置结果

配置旁路保护隧道与备份 CR-LSP 同步成功后，通过执行命令可以查看备份路径信息。

前提条件

已经完成旁路保护隧道与备份 CR-LSP 同步功能的所有配置。

操作步骤

- 使用 `display mpls te tunnel-interface [tunnel interface-number | auto-bypass-tunnel tunnel-name]` 命令查看隧道的状态信息。

----结束

3.15 配置 RSVP GR

介绍 RSVP TE GR 的配置方法，即介绍使 TE 隧道节点在主备倒换时维持 RSVP 邻居会话的配置方法。

3.15.1 建立配置任务

在进行 RSVP GR 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 RSVP 节点进行主备倒换时，该节点与邻居之间的 RSVP 邻接关系会因信令协议超时而删除，从而删除 CR-LSP，引起网络的暂时中断。

RSVP GR 可以解决以上的问题。该特性允许邻居间重新建立邻接关系而不终止 RSVP 会话。

AR1200 支持 RSVP GR 期间进行 FRR 切换。即当 PLR、PLR 上游节点、MP、MP 下游节点中的任意一个节点进行主备倒换，同时 PLR 的主隧道出接口故障时，进行隧道保护，减短故障时间。

说明

在 RSVP GR 期间支持 FRR 场景中，建议将 PSB 和 RSB 的超时倍数设置为大于或等于 5，防止 PSB 和 RSB 因 LSP 数据过大而被丢失。相关配置请参见 [\(可选\) 修改 PSB 和 RSB 的超时倍数](#)。

AR1200 只能作为 Helper 路由器，不能作为 Restarter 路由器。

前置任务

在配置 RSVP GR 之前，需完成以下任务：

- 配置 RSVP-TE 主隧道
- 在各 LSR 上使能 IS-IS GR 或 OSPF GR

数据准备

在配置 RSVP GR 之前，需准备以下数据：

序号	数据
1	网络上使用的 IGP 协议类型： <ul style="list-style-type: none">● 如果使用 IS-IS，则需准备 ISIS 进程号、网络实体名称 NET 及各节点所属的 IS-IS Level● 如果使用 OSPF，则需准备 OSPF 进程号及区域号
2	各节点的 MPLS LSR-ID
3	Tunnel 接口编号、Tunnel ID
4	(可选) RSVP GR 的基础时间

3.15.2 使能 RSVP Hello 扩展

通过配置 RSVP Hello 扩展，可以快速检测 RSVP 节点之间的可达性。

背景信息

在 GR 节点及其邻居节点进行如下配置。

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`，进入 MPLS 视图。
- 步骤 3** 执行命令 `mpls RSVP-te hello`，全局使能节点的 RSVP Hello 扩展。
- 步骤 4** 执行命令 `quit`，退回系统视图。
- 步骤 5** 执行命令 `interface interface-type interface-number`，进入使能了 RSVP-TE 的接口。
- 步骤 6** 执行命令 `mpls RSVP-te hello`，使能接口的 RSVP Hello 扩展。

缺省情况下，即使全局使能 RSVP Hello 扩展，RSVP 接口的 RSVP Hello 扩展功能也是被禁止。

---结束

3.15.3 使能 RSVP Full-GR

通过配置 RSVP Full-GR 使能，以保证转发平面上的数据传输不会中断。

背景信息

在 GR 节点上进行如下配置。

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 `mpls`，进入 MPLS 视图。

步骤 3 执行命令 `mpls rsvp-te hello full-gr`，使能 GR 节点自身 RSVP GR 能力和支持邻居 RSVP GR 能力。

缺省情况下，RSVP GR 能力和 RSVP GR 支持能力都被禁止。

---结束

3.15.4 （可选）使能 RSVP GR 支持能力

通过使能 RSVP GR 支持能力，可以使本地设备具备支持邻居节点 GR 的能力。

背景信息

如果 GR 节点的 RSVP 邻居也是一个 GR 节点，则该邻居节点使能了 RSVP full GR 后，就支持 RSVP GR 支持能力，无需进行此步骤配置。如果该邻居节点不是一个 GR 节点时，需进行此步骤配置。

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`，进入 MPLS 视图。

步骤 3 执行命令 `mpls rsvp-te`，使能 RSVP-TE。

步骤 4 执行命令 `mpls rsvp-te hello`，使能本节点的 RSVP Hello 扩展。

步骤 5 执行命令 `mpls rsvp-te hello support-peer-gr`，使能 RSVP GR 的支持能力。

---结束

3.15.5 （可选）配置 RSVP GR 节点间 hello 会话

如果网络中部署了 TE FRR，则 PLR 节点和 MP 节点间需要建立 hello 会话。

背景信息

如果部署了 TE FRR，则 PLR 节点和 MP 节点间需要建立 hello 会话，即需要在 PLR 节点和 MP 节点上进行如下配置。

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 `mpls`，进入 MPLS 视图。

步骤 3 执行命令 `mpls rsvp-te`，使能 RSVP-TE。

步骤 4 执行命令 `mpls rsvp-te hello`，使能本节点的 RSVP Hello 扩展。

步骤 5 执行命令 `mpls rsvp-te hello nodeid-session ip-address`，配置与 RSVP 邻居节点建立 HELLO 会话。

参数 `ip-address` 表示 RSVP 邻居节点的 LSR-ID。

---结束

3.15.6 （可选）修改基础时间

配置基础时间和 Ingress 类型的 LSP 数量可以影响 Restart Time。

背景信息

RSVP GR 节点在主备板倒换开始之后有一段 RSVP 平滑期，这段期间数据平面可以继续转发数据但控制平面还没有恢复。RSVP 平滑结束后启动 Restart Timer。一般情况下，Restart Timer = 基础时间 + Ingress 类型的 LSP 数量 × 60ms。其中的基础时间缺省值设为 90s，该基础时间可以通过命令行修改。

Restart Timer 结束后系统启动 Recovery Timer。一般情况下，Recovery Timer = Restart Timer + LSP 总数 × 40ms。

如果要修改基础时间，请在 GR 节点上进行如下配置。

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 `mpls`，进入 MPLS 视图。

步骤 3 执行命令 `mpls rsvp-te hello basic-restart-time basic-restart-time`，修改 RSVP GR 的基础时间。

缺省情况下，RSVP GR 的基础时间是 90 秒。

---结束

3.15.7 检查配置结果

配置 RSVP GR 成功后，通过执行命令可以发现 GR 期间，通过该 TE 隧道的数据转发不受影响。

操作步骤

- 使用 `display mpls rsvp-te graceful-restart` 命令查看本地 RSVP GR 的状态。
- 使用 `display mpls rsvp-te graceful-restart peer [{ interface interface-type interface-number | node-id } [ip-address]]` 命令查看邻居 RSVP GR 的状态。

---结束

任务示例

配置完成后，在重启节点上执行 `display mpls rsvp-te graceful-restart` 命令，可以看到“Graceful-Restart Capability”字段对应值为“GR-Self GR-Support”，表示本地设备具备

RSVP GR 能力。在 GR 期间，`display mpls rsvp-te graceful-restart` 命令的显示信息中，“GR Status” 字段对应值为 “Restart time going on” 或 “Recovery time going on”。

在重启节点上执行命令 `display mpls rsvp-te graceful-restart peer`：

- 如果显示信息中，“Neighbor Capability” 字段对应值为 “Can Do Self GR”，表明邻居节点具备 RSVP GR 能力。
- 如果 “Neighbor Capability” 字段对应值为 “Can Support GR”，表明邻居节点具备 RSVP GR 支持能力。
- 如果 “Neighbor Capability” 字段对应值为 “Can Do Self GR” 和 “Can Support GR”，表明邻居节点既具备 RSVP GR 能力又具备 RSVP GR 支持能力。

3.16 配置静态 BFD for CR-LSP

介绍静态 BFD 检测静态 CR-LSP 或 RSVP CR-LSP 链路故障的配置方法。

3.16.1 建立配置任务

在进行静态 BFD for CR-LSP 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

BFD 可以检测的 CR-LSP 包括以下两种类型：

- 静态 CR-LSP
- RSVP CR-LSP

 说明

BFD 检测 LSP 时，往返转发方式可以不一致（如报文从源端到目的端走 LSP，从目的端到源端走 IP 转发），但要求往返路径一致，如果不一致，则检测到故障时，不能确定具体是哪条路径的故障。因此部署 BFD 检测时，要确认往返路径是否一致，以便检测到的故障确实是检测路径故障。

前置任务

在配置静态 BFD for CR-LSP 之前，需完成以下任务。

- [配置静态 CR-LSP](#) 或者 RSVP-TE 隧道或者 [配置 CR-LSP 备份](#) 或者 MPLS TE 隧道保护组

数据准备

在配置静态 BFD for CR-LSP 之前，需准备以下数据。

序号	数据
1	BFD 配置名
2	反向通道（IP 链路、动态 LSP、静态 LSP 或者 MPLS TE）
3	BFD 会话的本地标识符和远端标识符
4	发送 BFD 报文的最小时间间隔

序号	数据
5	允许接收 BFD 报文的最小时间间隔
6	BFD 的本地检测倍数

3.16.2 使能全局 BFD 能力

配置静态 BFD for CR-LSP，需要在隧道入节点和出节点上全局使能 BFD。

背景信息

在隧道入节点和出节点上进行如下配置。

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`，对本节点使能全局 BFD 能力。
- 结束

3.16.3 配置入节点 BFD 参数

可以在入节点上配制的 BFD 参数包括本地标识符、远端标识符、本地发送 BFD 报文的最小时间间隔、本地允许接收 BFD 报文的最小时间间隔和本地 BFD 检测倍数等，这些将会影响会话的建立。

背景信息

在 TE 所在的入节点上进行如下配置。

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 bind mpls-te interface tunnel interface-number te-lsp [backup]`，配置 BFD 会话绑定指定 Tunnel 的主用或备用 CR-LSP。
指定参数 `backup` 则表示 BFD 会话绑定备用 CR-LSP。
- 步骤 3** 执行命令 `discriminator local discr-value`，配置本地标识符。
- 步骤 4** 执行命令 `discriminator remote discr-value`，配置远端标识符。
- 步骤 5**（可选）执行命令 `min-tx-interval interval`，调整本地发送 BFD 报文的最小时间间隔。
缺省值取决于许可证文件。
- 步骤 6**（可选）执行命令 `min-rx-interval interval`，调整本地允许接收 BFD 报文的最小时间间隔。
缺省值取决于许可证文件。

步骤 7 (可选) 执行命令 **detect-multiplier multiplier**, 调整本地 BFD 检测倍数。

缺省情况下, 本地检测倍数为 3。

步骤 8 执行命令 **commit**, 提交配置。

 说明

本地 BFD 报文实际发送时间间隔 = MAX { 本地配置的发送时间间隔, 对端配置的接收时间间隔 }; 本地实际接收时间间隔 = MAX { 对端配置的发送时间间隔, 本地配置的接收时间间隔 }; 本地实际检测时间 = 本地实际接收时间间隔 × 对端配置的 BFD 检测倍数。

例如,

- 本地配置的发送时间间隔为 200ms, 配置的接收时间间隔为 300ms, 检测倍数为 4
- 对端配置的发送时间间隔为 100ms, 配置的接收时间间隔为 600ms, 检测倍数为 5

则:

- 本地实际的发送时间间隔为 MAX { 200ms, 600ms } = 600ms, 实际接收时间间隔为 MAX { 100ms, 300ms } = 300ms, 实际检测时间间隔为 300ms × 5 = 1500ms
- 对端实际的发送时间间隔为 MAX { 100ms, 300ms } = 300ms, 实际接收时间间隔为 MAX { 200ms, 600ms } = 600ms, 实际检测时间间隔为 600ms × 4 = 2400ms

---结束

3.16.4 配置出节点 BFD 参数

可以在出节点上配制的 BFD 参数包括本地标识符、远端标识符、本地发送 BFD 报文的最小时间间隔、本地允许接收 BFD 报文的最小时间间隔和本地 BFD 检测倍数等, 这些将会影响会话的建立。

背景信息

在 TE 隧道的出节点进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**, 进入系统视图。

步骤 2 配置向入节点通告故障的反向通道, 反向通道可以是 IP 链路、LSP 或者 TE 隧道。为了避免反向通道故障影响 BFD 的检测, 一般情况下优先选用 BFD for CR-LSP 且正反 LSP 路径一致。若此反向通道也需要 BFD 检测, 可以再配置一对 BFD 会话进行检测。根据实际需要选择如下配置之一:

- IP 链路: 执行命令 **bfd cfg-name bind peer-ip ip-address [vpn-instance vpn-name] [interface interface-type interface-number] [source-ip ip-address]**
- LDP LSP: 执行命令 **bfd cfg-name bind ldp-lsp peer-ip ip-address nexthop ip-address [interface interface-type interface-number]**
- 静态 LSP: 执行命令 **bfd cfg-name bind static-lsp lsp-name**
- CR-LSP: 执行命令 **bfd cfg-name bind mpls-te interface tunnel interface-number te-lsp [backup]**
- TE 隧道: 执行命令 **bfd cfg-name bind mpls-te interface tunnel interface-number**

步骤 3 执行命令 **discriminator local discr-value**, 配置本地标识符。

步骤 4 执行命令 **discriminator remote discr-value**, 配置远端标识符。

步骤 5 (可选) 执行命令 **min-tx-interval interval**, 调整本地发送 BFD 报文的最小时间间隔。

缺省值取决于许可证文件。

步骤 6 (可选) 执行命令 **min-rx-interval interval**，调整本地允许接收 BFD 报文的最小时间间隔。

缺省值取决于许可证文件。

步骤 7 (可选) 执行命令 **detect-multiplier multiplier**，调整 BFD 检测倍数。

步骤 8 执行命令 **commit**，提交配置。

---结束

3.16.5 检查配置结果

配置静态 BFD for CR-LSP 成功后，通过执行命令查看 BFD 会话状态，可发现 BFD 会话状态为 Up。

操作步骤

- 使用 **display bfd configuration mpls-te interface tunnel interface-number te-lsp [verbose]** 命令查看隧道入节点查看 BFD 配置信息。
- 使用以下命令查看隧道出节点查看 BFD 配置信息：
 - 查看所有 BFD 相关配置信息：**display bfd configuration all [for-ip | for-lsp | for-te] [verbose]**
 - 查看静态 BFD 相关配置信息：**display bfd configuration static [for-ip | for-lsp | for-te | name cfg-name] [verbose]**
 - 查看反向通道为 IP 的 BFD 配置信息：**display bfd configuration peer-ip peer-ip [vpn-instance vpn-instance-name] [verbose]**
 - 查看反向通道为静态 LSP 的 BFD 配置信息：**display bfd configuration static-lsp lsp-name [verbose]**
 - 查看反向通道为 LDP LSP 的 BFD 配置信息：**display bfd configuration ldp-lsp peer-ip peer-ip [interface interface-type interface-number] [verbose]**
 - 查看反向通道为 CR-LSP 的 BFD 配置信息：**display bfd configuration mpls-te interface tunnel interface-number te-lsp [verbose]**
 - 查看反向通道为 TE 隧道的 BFD 配置信息：**display bfd configuration mpls-te interface tunnel interface-number [verbose]**
- 使用 **display bfd session mpls-te interface tunnel interface-number te-lsp [verbose]** 命令查看隧道入节点查看 BFD 会话信息。
- 使用以下命令查看隧道出节点查看 BFD 会话信息：
 - 查看所有 BFD 相关配置信息：**display bfd session all [for-ip | for-lsp | for-te] [verbose]**
 - 查看静态 BFD 相关配置信息：**display bfd session static [for-ip | for-lsp | for-te] [verbose]**
 - 查看反向通道为 IP 的 BFD 配置信息：**display bfd session peer-ip peer-ip [vpn-instance vpn-instance-name] [verbose]**
 - 查看反向通道为静态 LSP 的 BFD 配置信息：**display bfd session static-lsp lsp-name [verbose]**
 - 查看反向通道为 LDP LSP 的 BFD 配置信息：**display bfd session ldp-lsp peer-ip peer-ip [interface interface-type interface-number] [verbose]**

- 查看反向通道为 CR-LSP 的 BFD 配置信息：**display bfd session mpls-te interface tunnel interface-number te-lsp [verbose]**
- 查看反向通道为 TE 隧道的 BFD 配置信息：**display bfd session mpls-te interface tunnel interface-number [verbose]**
- 使用以下命令查看 BFD 统计信息：
 - 查看所有 BFD 会话的统计信息：**display bfd statistics session all [for-ip | for-lsp | for-te]**
 - 查看检测 IP 链路的 BFD 会话统计信息：**display bfd statistics session peer-ip peer-ip [vpn-instance vpn-instance-name]**
 - 查看检测静态 LSP 的 BFD 会话统计信息：**display bfd statistics session static-lsp lsp-name**
 - 查看检测 LDP LSP 的 BFD 会话统计信息：**display bfd statistics session ldp-lsp peer-ip peer-ip [interface interface-type interface-number]**
 - 查看检测 CR-LSP 的 BFD 会话统计信息：**display bfd statistics session mpls-te interface tunnel interface-number te-lsp**

----结束

任务示例

配置成功时，查看 BFD 会话状态，可发现 BFD 会话状态为 Up。

3.17 配置静态 BFD for TE

介绍了静态 BFD 检测 TE 隧道故障的配置方法。

3.17.1 建立配置任务

在进行静态 BFD for TE 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

使用 BFD 检测整条 TE 隧道，可触发 VPN FRR 等应用在主隧道故障时进行快速流量切换，以减少对业务的影响。

说明

BFD 检测 LSP 时，往返转发方式可以不一致（如报文从源端到目的端走 LSP，从目的端到源端走 IP 转发），但要求往返路径一致，如果不一致，则检测到故障时，不能确定具体是哪条路径的故障。因此部署 BFD 检测时，要确认往返路径是否一致，以便检测到的故障确实是检测路径故障。

前置任务

在配置静态 BFD for TE 之前，需完成以下任务。

- **配置静态 CR-LSP** 或者配置 MPLS TE 隧道

数据准备

在配置静态 BFD for TE 之前，需准备以下数据。

序号	数据
1	BFD 配置名
2	反向通道, IP 链路、动态 LSP、静态 LSP 或者 MPLS TE
3	BFD 会话的本地标识符和远端标识符
4	(可选) 发送 BFD 报文的最小时间间隔
5	(可选) 允许接收 BFD 报文的最小时间间隔
6	(可选) BFD 的本地检测倍数

3.17.2 使能全局 BFD 能力

配置静态 BFD for TE, 需要在隧道入节点和出节点上全局使能 BFD。

背景信息

在隧道入节点和出节点上进行如下配置。

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`, 对本节点使能全局 BFD 能力并进入 BFD 视图。
---结束

3.17.3 配置入节点 BFD 参数

可以在入节点上配制的 BFD 参数包括本地标识符、远端标识符、本地发送 BFD 报文的最小时间间隔、本地允许接收 BFD 报文的最小时间间隔和本地 BFD 检测倍数等, 这些将会影响会话的建立。

背景信息

在 TE 所在的入节点上进行如下配置。

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 bind mpls-te interface tunnel interface-number`, 配置 BFD 检测指定的 Tunnel。
- 步骤 3** 执行命令 `discriminator local discr-value`, 配置本地标识符。
- 步骤 4** 执行命令 `discriminator remote discr-value`, 配置远端标识符。
- 步骤 5** (可选) 执行命令 `min-tx-interval interval`, 调整本地发送 BFD 报文的最小时间间隔。

步骤 6 (可选) 执行命令 **min-rx-interval interval**, 调整本地允许接收 BFD 报文的最小时间间隔。

步骤 7 (可选) 执行命令 **detect-multiplier multiplier**, 调整本地 BFD 检测倍数。

步骤 8 执行命令 **commit**, 提交配置。

 说明

当被检测的 Tunnel 的状态为 Down 时, 不能创建 BFD 会话。

本地 BFD 报文实际发送时间间隔 = MAX { 本地配置的发送时间间隔, 对端配置的接收时间间隔 }; 本地实际接收时间间隔 = MAX { 对端配置的发送时间间隔, 本地配置的接收时间间隔 }; 本地实际检测时间 = 本地实际接收时间间隔 × 对端配置的 BFD 检测倍数。

例如,

- 本地配置的发送时间间隔为 200ms, 本地配置的接收时间间隔为 300ms, 本地检测倍数为 4
- 对端配置的发送时间间隔为 100ms, 对端配置的接收时间间隔为 600ms, 对端检测倍数为 5 则:
 - 本地实际的发送时间间隔为 MAX { 200ms, 600ms } = 600ms, 本地实际接收时间间隔为 MAX { 100ms, 300ms } = 300ms, 本地实际检测时间间隔为 300ms × 5 = 1500ms
 - 对端实际的发送时间间隔为 MAX { 100ms, 300ms } = 300ms, 对端实际接收时间间隔为 MAX { 200ms, 600ms } = 600ms, 对端实际检测时间间隔为 600ms × 4 = 2400ms

---结束

3.17.4 配置出节点 BFD 参数

可以在出节点上配制的 BFD 参数包括本地标识符、远端标识符、本地发送 BFD 报文的最小时间间隔、本地允许接收 BFD 报文的最小时间间隔和本地 BFD 检测倍数等, 这些将会影响会话的建立。

背景信息

在 TE 隧道的出节点进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**, 进入系统视图。

步骤 2 配置向入节点通告故障的反向通道, 反向通道可以是 IP 链路、LSP 或者 TE 隧道。为了避免反向通道故障影响 BFD 的检测, 一般情况下优先选用 BFD for CR-LSP 且正反 LSP 路径一致。若此反向通道也需要 BFD 检测, 可以再配置一对 BFD 会话进行检测。根据实际需要选择如下配置之一:

- IP 链路: 执行命令 **bfd cfg-name bind peer-ip ip-address [vpn-instance vpn-name] [interface interface-type interface-number] [source-ip ip-address]**
- LDP LSP: 执行命令 **bfd cfg-name bind ldp-lsp peer-ip ip-address nexthop ip-address [interface interface-type interface-number]**
- 静态 LSP: 执行命令 **bfd cfg-name bind static-lsp lsp-name**
- TE 隧道: 执行命令 **bfd cfg-name bind mpls-te interface tunnel interface-number**

步骤 3 执行命令 **discriminator local discr-value**, 配置本地标识符。

步骤 4 执行命令 **discriminator remote discr-value**, 配置远端标识符。

步骤 5 (可选) 执行命令 **min-tx-interval interval**, 调整本地发送 BFD 报文的最小时间间隔。

缺省情况下，BFD 控制报文发送间隔是 1000 毫秒。

步骤 6（可选）执行命令 **min-rx-interval interval**，调整本地允许接收 BFD 报文的最小时间间隔。

缺省情况下，BFD 控制报文接收间隔是 1000 毫秒。

步骤 7（可选）执行命令 **detect-multiplier multiplier**，调整本地 BFD 检测倍数。

步骤 8 执行命令 **commit**，提交配置。

---结束

3.17.5 检查配置结果

配置静态 BFD for TE 成功后，通过执行命令查看 BFD 会话状态，可发现 BFD 会话状态为 Up。

操作步骤

- 使用 **display bfd configuration mpls-te interface tunnel interface-number [verbose]** 命令在入节点上查看 BFD 配置信息。
- 使用以下命令在出节点上查看 BFD 配置信息：
 - 查看所有 BFD 相关配置信息：**display bfd configuration all [for-ip | for-lsp | for-te] [verbose]**
 - 查看静态 BFD 相关配置信息：**display bfd configuration static [for-ip | for-lsp | for-te | name] [verbose]**
 - 查看反向通道为 IP 的 BFD 配置信息：**display bfd configuration peer-ip peer-ip [vpn-instance vpn-instance-name] [verbose]**
 - 查看反向通道为静态 LSP 的 BFD 配置信息：**display bfd configuration static-lsp lsp-name [verbose]**
 - 查看反向通道为 LDP LSP 的 BFD 配置信息：**display bfd configuration ldp-lsp peer-ip peer-ip [interface interface-type interface-number] [verbose]**
 - 查看反向通道为 CR-LSP 的 BFD 配置信息：**display bfd configuration mpls-te interface tunnel interface-number te-lsp [verbose]**
 - 查看反向通道为 TE 隧道的 BFD 配置信息：**display bfd configuration mpls-te interface tunnel interface-number [verbose]**
- 使用 **display bfd session mpls-te interface tunnel interface-number [verbose]** 命令隧道入节点查看 BFD 会话信息。
- 使用以下命令在隧道出节点查看 BFD 会话信息：
 - 查看所有 BFD 相关配置信息：**display bfd session all [for-ip | for-lsp | for-te] [verbose]**
 - 查看静态 BFD 相关配置信息：**display bfd session static [for-ip | for-lsp | for-te] [verbose]**
 - 查看反向通道为 IP 的 BFD 配置信息：**display bfd session peer-ip peer-ip [vpn-instance vpn-instance-name] [verbose]**
 - 查看反向通道为静态 LSP 的 BFD 配置信息：**display bfd session static-lsp lsp-name [verbose]**
 - 查看反向通道为 LDP LSP 的 BFD 配置信息：**display bfd session ldp-lsp peer-ip peer-ip [interface interface-type interface-number] [verbose]**

- 查看反向通道为 CR-LSP 的 BFD 配置信息：**display bfd session mpls-te interface tunnel interface-number te-lsp [verbose]**
- 查看反向通道为 TE 隧道的 BFD 配置信息：**display bfd session mpls-te interface tunnel interface-number [verbose]**
- 使用以下命令查看 BFD 统计信息：
 - 查看 BFD 所有相关统计信息：**display bfd statistics**
 - 查看所有 BFD 会话的统计信息：**display bfd statistics session all [for-ip | for-lsp | for-te]**
 - 查看检测 IP 链路的 BFD 会话统计信息：**display bfd statistics session peer-ip peer-ip [vpn-instance vpn-instance-name]**
 - 查看检测静态 LSP 的 BFD 会话统计信息：**display bfd statistics session static-lsp lsp-name**
 - 查看检测 LDP LSP 的 BFD 会话统计信息：**display bfd statistics session ldp-lsp peer-ip peer-ip [interface interface-type interface-number]**
 - 查看检测 CR-LSP 的 BFD 会话统计信息：**display bfd statistics session mpls-te interface tunnel interface-number te-lsp**

----结束

任务示例

配置成功时，查看 BFD 会话状态，可发现 BFD 会话状态为 Up。

3.18 配置动态 BFD for CR-LSP

介绍动态 BFD 检测静态 CR_LSP 或 RSVP CR-LSP 链路故障的配置方法。

3.18.1 建立配置任务

在进行动态 BFD for CR-LSP 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

相对静态 BFD 而言，动态创建 BFD 会话可以减少配置的复杂性，减少人为的配置错误。

BFD 可以检测的 CR-LSP 包括以下两种类型：

- 静态 CR-LSP
- RSVP CR-LSP

目前动态 BFD 不能检测整条 TE 隧道。

 说明

BFD 检测 LSP 时，往返转发方式可以不一致（如报文从源端到目的端走 LSP，从目的端到源端走 IP 转发），但要求往返路径一致，如果不一致，则检测到故障时，不能确定具体是哪条路径的故障。因此部署 BFD 检测时，要确认往返路径是否一致，以便检测到的故障确实是检测路径故障。

前置任务

在配置动态 BFD for CR-LSP 之前，需完成以下任务。

- [配置静态 CR-LSP](#) 或者 MPLS TE 隧道

数据准备

在配置动态 BFD for CR-LSP 之前，需准备以下数据。

序号	数据
1	发送 BFD 报文的最小时间间隔
2	允许接收 BFD 报文的最小时间间隔
3	BFD 的本地检测倍数

3.18.2 全局使能 BFD

如果要使能全局 BFD 能力，需要在隧道入节点和出节点上进行相应配置。

背景信息

在 TE 隧道两端节点上进行如下配置。

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`，使能 BFD。

----结束

3.18.3 入节点上使能 TE 动态创建 BFD 会话

在入节点上使能 TE 动态创建 BFD 会话有两种配置方法：全局使能和 Tunnel 接口下使能。

背景信息

使能 TE 动态创建 BFD 会话有两种配置方法：

- 当入节点的大部分 TE 隧道都需要使能自动创建 BFD 会话时，建议选择[全局使能](#)
- 当入节点的小部分 TE 隧道需要使能自动创建 BFD 会话时，建议选择[Tunnel 接口下使能](#)

操作步骤

- 全局使能

在 TE 隧道入节点上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **mpls**，进入 MPLS 视图。
3. 执行命令 **mpls te bfd enable**，触发 MPLS TE 自动创建 BFD 会话。

在 MPLS 视图下配置该命令后，所有 Tunnel 接口都使能了 BFD for TE，除非 Tunnel 接口的 BFD for TE 能力已被阻塞。

4. (可选) 如果有些 TE 隧道不需要使能 BFD for TE，则在这些隧道的 Tunnel 接口下配置阻塞 BFD for TE 能力：
 - 执行命令 **interface tunnel interface-number**，进入 TE 隧道接口。
 - 执行命令 **mpls te bfd block**，阻塞该 TE 隧道自动创建 BFD 会话能力。
 - 执行命令 **mpls te commit**，使配置生效。

- Tunnel 接口下使能

在 TE 隧道入节点上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface tunnel interface-number**，进入 TE 隧道接口。
3. 执行命令 **mpls te bfd enable**，触发该 TE 隧道自动创建 BFD 会话。

在 Tunnel 接口视图下配置该命令只对当前 Tunnel 接口生效。

4. 执行命令 **mpls te commit**，使配置生效。

---结束

3.18.4 出节点使能被动创建 BFD 会话

由于 LSP 路径是单向的，在一条 LSP 路径上，当主动方（源端）创建 BFD 会话后触发 LSP Ping 报文发送，被动方（宿端）收到 Ping 报文后才可能自动创建 BFD 会话。

背景信息

在 TE 隧道出节点上进行如下配置。

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 **mpls-passive**，使能被动创建 BFD 会话功能。

执行完该命令不创建 BFD 会话，而是等接收到源端发送的携带 BFD TLV 的 LSP Ping 请求报文后才建立 BFD 会话。

---结束

3.18.5 (可选) 调整入节点的 BFD 检测参数

隧道入节点的 BFD 检测参数有两种调整方法：调整全局的 BFD 检测参数和调整 Tunnel 接口的 BFD 检测参数。

背景信息

隧道入节点的 BFD 检测参数有两种调整方法：

- **调整全局的 BFD 检测参数**：当入节点的大部分 TE 隧道都使用相同的 BFD 检测参数时使用此方法
- **调整 Tunnel 接口的 BFD 检测参数**：当入节点有些 TE 隧道需要使用与全局不同的 BFD 检测参数时，则在这些隧道的 Tunnel 接口下单独调整 BFD 检测参数，否则 Tunnel 接口使用全局的 BFD 检测参数

说明

本地 BFD 报文实际发送时间间隔 = MAX { 本地配置的发送时间间隔, 对端配置的接收时间间隔 }; 本地实际接收时间间隔 = MAX { 对端配置的发送时间间隔, 本地配置的接收时间间隔 }; 本地实际检测时间 = 本地实际接收时间间隔 × 对端配置的 BFD 检测倍数。

对于被动创建 BFD 会话的 TE 隧道出节点，BFD 报文的接收时间间隔、发送时间间隔和检测倍数都不能调整，缺省值已是 TE 入节点上可设置的最小值。因此，BFD for TE 中，隧道两端节点最终采用的 BFD 检测时间为：

- 入节点实际检测时间间隔 = 入节点配置的接收时间间隔 × 3
- 出节点实际检测时间间隔 = 入节点配置的发送时间间隔 × 入节点配置的检测倍数

操作步骤

- 调整全局的 BFD 检测参数

在隧道入节点上进行以下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **mpls**，进入 MPLS 视图。
3. 执行命令 **mpls te bfd { min-tx-interval tx-interval | min-rx-interval rx-interval | detect-multiplier multiplier }***，设置 BFD 检测的时间参数。

- 调整 Tunnel 接口的 BFD 检测参数

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface tunnel interface-number**，进入 Tunnel 接口视图。
3. 执行命令 **mpls te bfd { min-tx-interval tx-interval | min-rx-interval rx-interval | detect-multiplier multiplier }***，设置 BFD 检测的时间参数。
4. 执行命令 **mpls te commit**，使配置生效。

---结束

3.18.6 检查配置结果

配置动态 BFD for CR-LSP 成功后，执行相关命令可以检查配置结果。

操作步骤

- 使用 **display bfd configuration dynamic [verbose]** 命令在隧道入节点上查看动态 BFD 的配置信息。
- 使用 **display bfd configuration passive-dynamic [peer-ip peer-ip remote-discriminator discriminator] [verbose]** 命令在隧道出节点上查看 BFD 配置信息。
- 使用 **display bfd session dynamic [verbose]** 命令在隧道入节点上查看 BFD 会话信息。

- 使用 **display bfd session [peer-ip peer-ip discriminator] [verbose]** 命令在隧道出节点上查看被动创建的 BFD 会话信息。
- 使用以下命令查看 BFD 统计信息：
 - 查看 BFD 所有相关统计信息：**display bfd statistics**
 - 查看动态 BFD 会话相关统计信息：**display bfd statistics session dynamic**
- 使用 **display mpls bfd session [statistics | [protocol { ldp | cr-static | rsvp-te }] | [outgoing-interface interface-type interface-number] | [nexthop ip-address] | [fec fec-address] | verbose | monitor]** 命令查看与 MPLS 相关的 BFD 会话信息。

----结束

任务示例

完成配置后，可执行上面的命令检查配置结果：

- 在隧道入节点上执行 **display bfd session all verbose** 命令查看 MPLS TE 动态触发的 BFD 会话状态。可以看到 BFD 会话状态为 Up，会话绑定的链路类型是 TE_LSP。

3.19 配置动态 BFD for RSVP

介绍动态 BFD 检测 RSVP 邻居之间的链路故障的配置方法。

3.19.1 建立配置任务

在进行动态 BFD for RSVP 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

BFD for RSVP 一般用在 TE FRR 中 PLR 节点与其下游邻居之间存在二层设备的情况。在 PLR 和 MP 节点使能 GR 的组网中建议配置 BFD for RSVP。

缺省情况下，RSVP 发送 Hello 报文的时间间隔为 3 秒，宣告邻居 down 的时间即相邻 RSVP 节点失效的时间为 Hello 报文间隔的 3 倍。因此，RSVP 节点感知到 RSVP 邻居故障的时间最短是秒级。

在没有 BFD 检测的情况下，如果在 RSVP 邻居之间存在二层设备，在链路发生故障后，邻居节点不能快速检测到链路故障。这将导致数据大量丢失。

BFD 能够提供毫秒级别的故障监测时间，及时检测到被保护的链路或节点出现的故障，并配合 RSVP 协议更快的发现 RSVP 邻接故障，以便使报文切换到旁路隧道上。

说明

BFD 检测 LSP 时，往返转发方式可以不一致（如报文从源端到目的端走 LSP，从目的端到源端走 IP 转发），但要求往返路径一致，如果不一致，则检测到故障时，不能确定具体是哪条路径的故障。因此部署 BFD 检测时，要确认往返路径是否一致，以便检测到的故障确实是检测路径故障。

前置任务

在配置 BFD for RSVP 之前，需完成以下任务：

- [配置 RSVP-TE 隧道](#)

数据准备

在配置 BFD for RSVP 之前，需准备以下数据：

序号	数据
1	发送 BFD 报文的最小时间间隔
2	允许接收 BFD 报文的最小时间间隔
3	BFD 的本地检测倍数

在修改 BFD 会话的参数时，对于不同协议间共享的 BFD 会话，参数选择需要按照下面的规则进行：

- 如果本地节点接口下和全局都配置了发送时间间隔、接收时间间隔、本地检测倍数，则以接口下配置的参数作为本地 RSVP 协议采用的参数。
- 如果本地的 BFD for RSVP 与其他协议共享 BFD 会话时，则本地节点分别选择所有共享 BFD 会话的协议里发送时间间隔、接收时间间隔、本地检测倍数的最小值做为本地的参数。
- 本地 BFD 报文实际发送时间间隔 = MAX { 本地配置的发送时间间隔，对端配置的接收时间间隔 }；本地实际接收时间间隔 = MAX { 对端配置的发送时间间隔，本地配置的接收时间间隔 }；本地实际检测时间 = 本地实际接收时间间隔 × 对端配置的 BFD 检测倍数。

3.19.2 RSVP 两端全局使能 BFD

配置动态 BFD for RSVP，需要在 RSVP 两端上配置全局使能 BFD。

背景信息

在中间存在二层设备的两个 RSVP 邻居节点上进行如下配置。

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`，全局使能 BFD。

---结束

3.19.3 RSVP 两端使能 BFD for RSVP

配置 BFD for RSVP 使能有两种方式，全局使能 BFD for RSVP 和 RSVP 接口下使能 BFD for RSVP。

背景信息

使能 BFD for RSVP 有两种方式：

- 当本节点大部分使能了 RSVP 的接口需要使能 BFD for RSVP 时，建议选择**全局使能 BFD for RSVP**

- 当本节点只有小部分使能了 RSVP 的接口需要使能 BFD for RSVP 时，建议选择 **RSVP 接口下使能 BFD for RSVP**

操作步骤

- 全局使能 BFD for RSVP

在中间存在二层设备的两个 RSVP 邻居节点上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **mpls**，进入 MPLS 视图。
3. 执行命令 **mpls rsvp-te bfd all-interfaces enable**，全局使能 BFD for RSVP。

在 MPLS 视图下配置该命令后，所有使能了 RSVP 的接口都使能了 BFD for RSVP，除非接口的 BFD for RSVP 能力已被阻塞。

4. （可选）如果有些 RSVP 接口不需要使能 BFD for RSVP，则在这些接口下配置阻塞 BFD for RSVP 能力：
 - 执行命令 **interface interface-type interface-number**，进入使能 RSVP 的接口的视图。
 - 执行命令 **mpls rsvp-te bfd block**，阻塞该接口的 BFD for RSVP 能力。

- RSVP 接口下使能 BFD for RSVP

在中间存在二层设备的两个 RSVP 邻居节点上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface interface-type interface-number**，进入使能 RSVP 的接口的视图。
3. 执行命令 **mpls rsvp-te bfd enable**，在接口下使能 BFD for RSVP。

----结束

3.19.4 （可选）调整 BFD 检测参数

通过两种方法可以调整 BFD for RSVP 的检测参数，调整全局的 BFD 检测参数和调整 RSVP 接口的 BFD 检测参数。

背景信息

BFD for RSVP 的检测参数有两种调整方法：

- **调整全局的 BFD 检测参数**：当本节点大部分 BFD for RSVP 都使用相同的 BFD 检测参数时使用此方法
- **调整 RSVP 接口的 BFD 检测参数**：当本节点有些 RSVP 接口的 BFD 参数与全局不一致，则在这些 RSVP 接口下单独调整 BFD 检测参数，否则使用全局的 BFD 检测参数

操作步骤

- 调整全局的 BFD 检测参数

在中间存在二层设备的两个 RSVP 邻居节点上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **mpls**，进入 MPLS 视图。
3. 执行命令 **mpls rsvp-te bfd all-interfaces { min-tx-interval tx-interval | min-rx-interval rx-interval | detect-multiplier multiplier }***，配置全局的 BFD 会话参数。

 说明

参数含义如下：

- 参数 *tx-interval* 表示 DMTI (Desired Min Tx Interval)，即本端期望采用的最短 BFD 控制报文发送时间间隔。
- 参数 *rx-interval* 表示 RMRI (Required Min Rx Interval)，即本端能够支持的最短 BFD 控制报文接收时间间隔。
- 参数 *multiplier* 表示 BFD 检测倍数。

本端实际使用的 BFD 检测参数与配置的参数可能不同：

- 本地 BFD 报文实际发送时间间隔 = MAX { 本地配置的 DMTI，对端配置的 RMRI }；
 - 本地 BFD 报文实际接收时间间隔 = MAX { 对端配置的 DMTI，本地配置的 RMRI }；
 - 本地实际检测周期 = 本地 BFD 报文实际接收时间间隔 × 对端配置的 BFD 检测倍数。
- 调整 RSVP 接口的 BFD 检测参数

在中间存在二层设备的两个 RSVP 邻居节点上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface interface-type interface-number**，进入使能 RSVP 的接口。
3. 执行命令 **mpls rsvp-te bfd { min-tx-interval tx-interval | min-rx-interval rx-interval | detect-multiplier multiplier }***，调整该接口的 BFD 会话参数。

----结束

3.19.5 检查配置结果

配置动态 BFD for CR-LSP 成功后，查看 BFD for RSVP 会话状态，可发现 BFD 会话状态为 Up。

操作步骤

- 使用 **display mpls rsvp-te bfd session { all | interface interface-type interface-number | peer ip-address } [verbose]** 命令查看 BFD for RSVP 会话信息。
- 使用 **display mpls rsvp-te [interface [interface-type interface-number]]** 命令查看 RSVP-TE 配置信息。
- 使用 **display mpls rsvp-te peer [interface interface-type interface-number]** 命令查看 RSVP 邻居信息。
- 使用 **display mpls rsvp-te statistics { global | interface [interface-type interface-number] }** 命令查看 RSVP-TE 的运行统计信息。

----结束

任务示例

配置成功时，查看 BFD for RSVP 会话状态，可发现 BFD 会话状态为 Up。



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。

3.20 维护 MPLS TE

介绍如何清除 MPLS TE 运行信息。

3.20.1 检测 TE 隧道的连通性

检测 TE 隧道的连通性即检查从入节点到出节点是否连通。

前提条件

已经完成检测 TE 隧道功能的所有配置。

操作步骤

- 使用命令 **ping lsp** [-a source-ip | -c count | -exp exp-value | -h ttl-value | -m interval | -r reply-mode | -s packet-size | -t time-out | -v] * te tunnel interface-number [hot-standby] [draft6] 检测 TE tunnel 从入节点到出节点是否连。

如果指定 **draft6** 参数，**ping** 命令按 draft-ietf-mpls-lsp-ping-06 实现。默认情况下按 RFC4379 实现。如果指定 **hot-standby** 参数，则可以实现对 CR-LSP 备份隧道的检测。

- 使用命令 **tracert lsp** [-a source-ip | -exp exp-value | -h ttl-value | -r reply-mode | -t time-out] * te tunnel interface-number [hot-standby] [draft6] 命令查看数据包从 TE tunnel 入节点到出节点所经过的网关。

如果指定 **draft6** 参数，**tracert** 命令按 draft-ietf-mpls-lsp-ping-06 实现。默认情况下按 RFC4379 实现。如果指定 **hot-standby** 参数，则可以实现对 CR-LSP 备份隧道的检测。

----结束

任务示例

配置完 MPLS TE 后，可以在 TE 隧道入节点上执行 **ping lsp** 命令检查 TE tunnel 从入节点到出节点是否连通。如果 ping 不通，使用 **tracert lsp** 命令分析网络什么地方发生了故障。

3.20.2 查看隧道错误信息

如果 RSVP-TE Tunnel 接口的状态为 Down，可执行相关命令查看错误信息。

背景信息

如果 RSVP-TE Tunnel 接口的状态为 Down，可执行如下命令查看错误信息。

操作步骤

步骤 1 使用 **display mpls te tunnel-interface last-error [tunnel-name]**命令查看 Tunnel 接口的错误信息。

----结束

任务示例

display mpls te tunnel-interface last-error 命令可用在 Ingress 节点查看本节点发生的错误或者下游节点发送的 PathErr 消息携带的错误，包括：

- CSPF 计算失败；
- RSVP GR 过程中发生的错误；
- 触发 RSVP 信令出错；
- 从收到的 RSVP PathErr 消息得知的错误。

该命令针对每条 TE 隧道记录最近 20 次错误的信息。

3.20.3 清除运行信息

清除运行信息即通过命令清除运行统计信息。

背景信息

在确认需要清除 RSVP-TE 的运行信息后，请在用户视图下执行下面的 **reset** 命令。

操作步骤

步骤 1 在确认需要清除 RSVP-TE 的运行信息后，请在用户视图下执行 **reset mpls rsvp-te statistics { global | interface [interface-type interface-number] }**命令，清除 RSVP-TE 的运行统计信息。

----结束

3.20.4 重启隧道接口

通过重启隧道接口，可以使隧道的相关配置立即生效。

背景信息

需要使隧道的相关配置立即生效时，可以在 Tunnel 接口视图下配置 **mpls te commit** 命令，并在用户视图下执行下面的 **reset** 命令。

 说明

如果在 TE 隧道的 Tunnel 接口下更改配置但没有执行 **mpls te commit** 命令，则执行 **reset mpls te tunnel-interface tunnel** 命令时，系统提示错误。

操作步骤

步骤 1 使用 **reset mpls te tunnel-interface tunnel interface-number** 命令重启隧道接口。

----结束

3.20.5 重启 RSVP 进程

当需要重建所有的 RSVP 类型的 CR-LSP，或验证 RSVP 工作过程时，可以采取重启 RSVP 进程的方法。

背景信息



注意

重启 RSVP 进程将导致所有 RSVP 类型的 CR-LSP 被拆除重建。

当需要重建所有的 RSVP 类型的 CR-LSP，或验证 RSVP 工作过程时，可在用户视图下执行下面的 **reset** 命令。

操作步骤

步骤 1 使用 **reset mpls rsvp-te** 命令重启 RSVP 进程。

----结束

3.20.6 删除/重建自动生成的旁路隧道

在 MPLS TE Auto FRR 环境中，可执行相关命令删除或重建旁路隧道。

背景信息

在 MPLS TE Auto FRR 环境中，可执行下面的 **reset** 命令删除或重建旁路隧道。

操作步骤

步骤 1 使用 **reset mpls te auto-frr { lsp-id ingress-lsr-id tunnel-id | name bypass-tunnel-name }** 命令删除重建自动生成的旁路隧道。

----结束

3.21 配置举例

介绍 MPLS TE 的各种组网举例。配置示例中包括组网需求、配置注意事项、配置思路等。

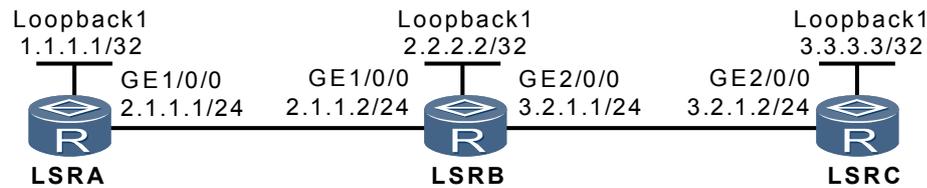
3.21.1 配置静态 MPLS TE 隧道示例

本例描述了静态 MPLS TE 隧道的基本配置过程，包括使能 MPLS TE，配置链路的 MPLS TE 带宽属性，配置 MPLS TE 隧道和创建静态 CR-LSP。

组网需求

如图 3-2 所示，要求建立一条 LSRA 到 LSRC 和一条从 LSRC 到 LSRA 的静态 TE 隧道，带宽为 10M bit/s。

图 3-2 静态 CR-LSP 配置组网图



配置思路

采用如下的思路配置静态 MPLS TE 隧道：

1. 配置各节点接口的 IP 地址及作为 MPLS LSR-ID 的 Loopback 接口的地址，并用 OSPF 协议通告各接口所连网段和 LSR ID 主机路由。
2. 配置 LSR-ID 并全局使能各节点的 MPLS 和 MPLS TE 和各接口的 MPLS 和 MPLS TE。
3. 在隧道沿途的各节点出接口上配置链路的最大可预留带宽和 BC0 带宽（假设该隧道从 BC0 获取带宽）。
4. 在入节点创建隧道接口，指定隧道的 IP 地址、隧道协议、目的地址、隧道 ID 以及建立隧道使用的信令类型。
5. 配置与隧道相关联的静态 LSP，在入节点上配置下一跳地址和出标签，在中间节点配置入接口、下一跳地址和出标签，在出节点上配置入标签和入接口以建立 LSP。

说明

- 每个节点出标签的值就是其下一个节点入标签的值。
- 执行命令 `static-cr-lsp ingress {tunnel-interface tunnel interface-number | tunnel-name } destination destination-address { nexthop next-hop-address | outgoing-interface interface-type interface-number } out-label out-label-value [bandwidth [ct0 | ct1] bandwidth]` 配置 CR-LSP 入节点时需注意，参数 `tunnel-name` 必须与命令 `interface tunnel interface-number` 创建的隧道接口名称一致，且区分大小写，不支持空格。假设使用命令 `interface tunnel 0/0/0` 创建了一个的 Tunnel 接口，则隧道接口名称为 Tunnel0/0/0，其静态 CR-LSP 入节点中的参数应该写作“Tunnel0/0/0”，否则隧道将不能正确建立。中间节点和出节点无此限制。

数据准备

为完成此配置例，需准备如下的数据：

- 各节点的 OSPF 进程号及区域号
- LSRA 和 LSRC 上隧道的接口编号、隧道接口 IP 地址、目的地址、隧道 ID、隧道信令协议（为 cr-static）
- 各链路的最大可预留带宽和 BC 带宽
- 静态 CR-LSP 入节点的下一跳地址和出标签
- 静态 CR-LSP 中间节点的入接口、下一跳和出标签
- 静态 CR-LSP 出节点的入接口

操作步骤

步骤 1 配置各接口的 IP 地址及路由协议

按照图 3-2 配置各接口的 IP 地址和掩码，并配置路由协议，保证各 LSR 之间在网络层互通。

具体配置过程略。

步骤 2 配置 MPLS 基本能力，使能 MPLS TE

配置 LSRA。

```
[LSRA] mpls lsr-id 1.1.1.1
[LSRA] mpls
[LSRA-mpls] mpls te
[LSRA-mpls] quit
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] mpls
[LSRA-GigabitEthernet1/0/0] mpls te
[LSRA-GigabitEthernet1/0/0] quit
```

LSRB、LSRC 与 LSRA 类似，不再赘述。

步骤 3 配置链路的 MPLS TE 带宽属性

在隧道沿途各节点出接口上配置链路的最大可预留带宽和 BC0 带宽。链路的 BC0 带宽必须大于隧道带宽（10M bit/s）。

配置 LSRA。

```
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[LSRA-GigabitEthernet1/0/0] mpls te bandwidth bc0 100000
[LSRA-GigabitEthernet1/0/0] quit
```

配置 LSRB。

```
[LSRB] interface gigabitethernet 1/0/0
[LSRB-GigabitEthernet1/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[LSRB-GigabitEthernet1/0/0] mpls te bandwidth bc0 100000
[LSRB-GigabitEthernet1/0/0] quit
[LSRB] interface gigabitethernet 2/0/0
[LSRB-GigabitEthernet2/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[LSRB-GigabitEthernet2/0/0] mpls te bandwidth bc0 100000
[LSRB-GigabitEthernet2/0/0] quit
```

配置 LSRC。

```
[LSRC] interface gigabitethernet 2/0/0
[LSRC-GigabitEthernet2/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[LSRC-GigabitEthernet2/0/0] mpls te bandwidth bc0 100000
[LSRC-GigabitEthernet2/0/0] quit
```

步骤 4 配置 MPLS TE 隧道

在 LSRA 上配置 LSRA 至 LSRC 的 MPLS TE 隧道。

```
[LSRA] interface tunnel 0/0/0
[LSRA-Tunnel0/0/0] ip address unnumbered interface loopback 1
[LSRA-Tunnel0/0/0] tunnel-protocol mpls te
[LSRA-Tunnel0/0/0] destination 3.3.3.3
[LSRA-Tunnel0/0/0] mpls te tunnel-id 100
[LSRA-Tunnel0/0/0] mpls te signal-protocol cr-static
[LSRA-Tunnel0/0/0] mpls te commit
[LSRA-Tunnel0/0/0] quit
```

在 LSRC 上配置 LSRC 至 LSRA 的 MPLS TE 隧道。

```
[LSRC] interface tunnel 0/0/1
[LSRC-Tunnel0/0/1] ip address unnumbered interface loopback 1
[LSRC-Tunnel0/0/1] tunnel-protocol mpls te
```

```
[LSRC-Tunnel0/0/1] destination 1.1.1.1
[LSRC-Tunnel0/0/1] mpls te tunnel-id 200
[LSRC-Tunnel0/0/1] mpls te signal-protocol cr-static
[LSRC-Tunnel0/0/1] mpls te commit
[LSRC-Tunnel0/0/1] quit
```

步骤 5 创建 LSRA 至 LSRC 的静态 CR-LSP

配置 LSRA 为静态 CR-LSP 的入节点。

```
[LSRA] static-cr-lsp ingress tunnel-interface Tunnel0/0/0 destination 3.3.3.3 nexthop 2.1.1.2 out-label 20 bandwidth ct0 10000
```

配置 LSRB 为静态 CR-LSP 的中间节点。

```
[LSRB] static-cr-lsp transit Tunnel0/0/0 incoming-interface gigabitethernet 1/0/0 in-label 20 nexthop 3.2.1.2 out-label 30 bandwidth ct0 10000
```

配置 LSRC 为静态 CR-LSP 的出节点。

```
[LSRC] static-cr-lsp egress Tunnel0/0/0 incoming-interface gigabitethernet 2/0/0 in-label 30
```

步骤 6 创建 LSRC 至 LSRA 的静态 CR-LSP

配置 LSRC 为静态 CR-LSP 的入节点。

```
[LSRC] static-cr-lsp ingress tunnel-interface Tunnel0/0/1 destination 1.1.1.1 nexthop 3.2.1.1 out-label 120 bandwidth ct0 10000
```

配置 LSRB 为静态 CR-LSP 的中间节点。

```
[LSRB] static-cr-lsp transit Tunnel0/0/1 incoming-interface gigabitethernet 2/0/0 in-label 120 nexthop 2.1.1.1 out-label 130 bandwidth ct0 10000
```

配置 LSRA 为静态 CR-LSP 的出节点。

```
[LSRA] static-cr-lsp egress Tunnel0/0/1 incoming-interface gigabitethernet 1/0/0 in-label 130
```

步骤 7 检查配置结果

配置完成后，在 LSRA 上执行 **display interface tunnel** 命令，可以看到 Tunnel 接口的状态为 Up。

在各节点上执行 **display mpls te tunnel** 命令，可以看到 MPLS TE 隧道的建立情况。

```
[LSRA] display mpls te tunnel
```

```
-----
Ingress LsrId   Destination      LSPID   In/Out Label    R   Tunnel-name
-----
1.1.1.1         3.3.3.3         1       --/20           I   Tunnel0/0/0
-               -               -       130/--         E   Tunnel0/0/1
```

```
[LSRB] display mpls te tunnel
```

```
-----
Ingress LsrId   Destination      LSPID   In/Out Label    R   Tunnel-name
-----
-               -               -       20/30          T   Tunnel0/0/0
-               -               -       120/130        T   Tunnel0/0/1
```

```
[LSRC] display mpls te tunnel
```

```
-----
Ingress LsrId   Destination      LSPID   In/Out Label    R   Tunnel-name
-----
3.3.3.3         1.1.1.1         1       --/120         I   Tunnel0/0/1
-               -               -       30/--         E   Tunnel0/0/0
```

在各节点上执行 **display mpls lsp** 或 **display mpls static-cr-lsp** 命令，可以看到静态 CR-LSP 的建立情况。

在 LSRA 上查看配置结果。

```
[LSRA] display mpls lsp
-----
LSP Information: STATIC CRLSP
-----
FEC                In/Out Label  In/Out IF                Vrf Name
3.3.3.3/32         NULL/20       -/GE1/0/0
-/-                130/NULL     GE1/0/0/-
[LSRA] display mpls static-cr-lsp
TOTAL              : 2          STATIC CRLSP(S)
UP                  : 2          STATIC CRLSP(S)
DOWN                : 0          STATIC CRLSP(S)
Name               FEC                I/O Label  I/O If                Status
Tunnel0/0/0       3.3.3.3/32        NULL/20    -/GE1/0/0            Up
Tunnel0/0/1       -/-              130/NULL   GE1/0/0/-            Up
```

在 LSRB 上查看。

```
[LSRB] display mpls lsp
-----
LSP Information: STATIC CRLSP
-----
FEC                In/Out Label  In/Out IF                Vrf Name
-/-                20/30         GE1/0/0/GE2/0/0
-/-                120/130       GE2/0/0/GE1/0/0
[LSRB] display mpls static-cr-lsp
TOTAL              : 2          STATIC CRLSP(S)
UP                  : 2          STATIC CRLSP(S)
DOWN                : 0          STATIC CRLSP(S)
Name               FEC                I/O Label  I/O If                Status
Tunnel0/0/0       -/-              20/30     GE1/0/0/GE2/0/0     Up
Tunnel0/0/1       -/-              120/130   GE2/0/0/GE1/0/0     Up
```

在 LSRC 上查看。

```
[LSRC] display mpls lsp
-----
LSP Information: STATIC CRLSP
-----
FEC                In/Out Label  In/Out IF                Vrf Name
1.1.1.1/32        NULL/120      -/GE2/0/0
-/-                30/NULL       GE2/0/0/-
[LSRC] display mpls static-cr-lsp
TOTAL              : 2          STATIC CRLSP(S)
UP                  : 2          STATIC CRLSP(S)
DOWN                : 0          STATIC CRLSP(S)
Name               FEC                I/O Label  I/O If                Status
Tunnel0/0/0       1.1.1.1/32      NULL/120   -/GE2/0/0            Up
Tunnel0/0/1       -/-              30/NULL    GE2/0/0/-            Up
```

使用静态 CR-LSP 建立 MPLS TE 隧道时，Transit 节点和 Egress 节点直接根据配置的入标签和出标签进行转发，因此，LSRB 和 LSRC 的相关显示信息中，FEC 等内容为空。

---结束

配置文件

● LSRA 的配置文件

```
#
sysname LSRA
#
mpls lsr-id 1.1.1.1
mpls
mpls te
#
interface GigabitEthernet1/0/0
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 Tunnel0/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te tunnel-id 100
 mpls te signal-protocol cr-static
 mpls te commit
#
ospf 1
 area 0.0.0.0
  network 2.1.1.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
#
static-cr-lsp ingress tunnel-interface Tunnel0/0/0 destination 3.3.3.3 nexthop 2.1.1.2 out-
label 20 bandwidth ct0 10000
static-cr-lsp egress Tunnel0/0/1 incoming-interface GigabitEthernet1/0/0 in-label 130
#
return
```

● LSRB 的配置文件

```
#
sysname LSRB
#
mpls lsr-id 2.2.2.2
mpls
mpls te
#
interface GigabitEthernet1/0/0
 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 GigabitEthernet2/0/0
 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
#
ospf 1
 area 0.0.0.0
  network 2.1.1.0 0.0.0.255
  network 3.2.1.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
#
static-cr-lsp transit Tunnel0/0/0 incoming-interface GigabitEthernet1/0/0 in-label 20 nexthop
3.2.1.2 out-label 30 bandwidth ct0 10000
static-cr-lsp transit Tunnel0/0/1 incoming-interface GigabitEthernet2/0/0 in-label 120 nexthop
2.1.1.1 out-label 130 bandwidth ct0 10000
#
return
```

● LSRC 的配置文件

```
#
sysname LSRC
#
mpls lsr-id 3.3.3.3
```

```
mpls
 mpls te
#
interface GigabitEthernet2/0/0
 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 Tunnel0/0/1
 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 commit
#
ospf 1
 area 0.0.0.0
 network 3.2.1.0 0.0.0.255
 network 3.3.3.3 0.0.0.0
#
static-cr-lsp ingress tunnel-interface Tunnel0/0/1 destination 1.1.1.1 nexthop 3.2.1.1 out-
label 120 bandwidth ct0 10000
static-cr-lsp egress Tunnel0/0/0 incoming-interface GigabitEthernet2/0/0 in-label 30
#
return
```

3.21.2 配置 RSVP-TE 隧道示例

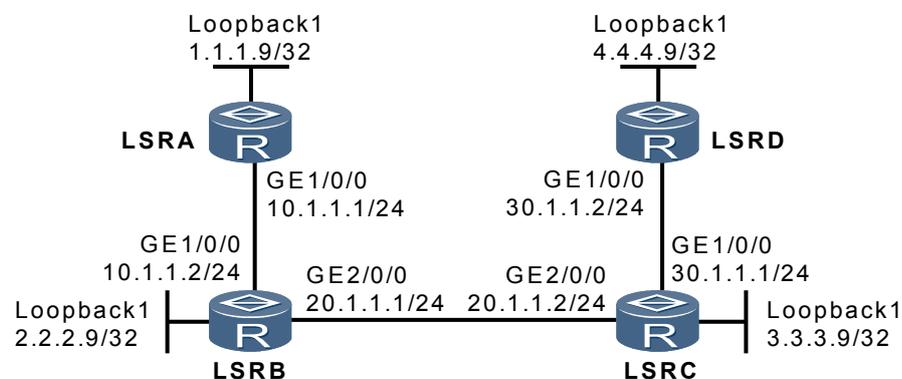
本例描述了配置 RSVP-TE 隧道的过程，包括配置 MPLS 基本能力，使能 MPLS TE、RSVP-TE 和 CSPF。

组网需求

如图 3-3 所示，节点 LSRA、LSRB、LSRC 和 LSRD 运行 IS-IS，都属于 Level-2。

使用 RSVP-TE 从 LSRA 到 LSRD 建立一条 TE 隧道，带宽为 20Mbit/s。隧道沿途的链路最大可预留带宽为 100Mbit/s，采用默认带宽模型 RDM，且 BC0 带宽为 100Mbit/s。

图 3-3 RSVP-TE 隧道组网图



配置思路

采用如下的思路使用 RSVP-TE 配置 MPLS TE 隧道：

1. 配置各接口的 IP 地址及作为 LSR ID 的 Loopback 地址。
2. 全局使能 IS-IS 协议，配置网络实体名称，改变 cost 类型以使能 IS-IS TE。并在各接口（包括 Loopback 接口）上使能 IS-IS。
3. 配置 MPLS LSR-ID 并全局使能 MPLS、MPLS TE、MPLS RSVP-TE、MPLS TE CSPF。
4. 使能各接口的 MPLS、MPLS TE 和 MPLS RSVP-TE。
5. 在隧道沿途的各链路出接口上配置链路的最大可预留带宽和 BC 带宽。
6. 在入节点创建隧道接口，指定隧道的 IP 地址、隧道协议、目的地址、隧道 ID、动态信令协议 RSVP-TE 以及隧道带宽。

数据准备

为完成此配置例，需准备如下的数据：

- 各节点的 IS-IS 区域 ID、起始的系统 ID、IS-IS Level
- 隧道沿途的链路最大带宽和最大可预留带宽
- 隧道接口的接口编号、IP 地址、目的地址、隧道 ID、隧道信令协议（为 **rsvp-te**）、隧道带宽

操作步骤

步骤 1 配置各接口的 IP 地址

按照图 3-3 配置各接口的 IP 地址和掩码，具体配置过程略。

步骤 2 配置 IS-IS 协议发布路由

配置 LSRA。

```
[LSRA] isis 1
[LSRA-isis-1] network-entity 00.0005.0000.0000.0001.00
[LSRA-isis-1] is-level level-2
[LSRA-isis-1] quit
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] isis enable 1
[LSRA-GigabitEthernet1/0/0] quit
[LSRA] interface loopback 1
[LSRA-LoopBack1] isis enable 1
[LSRA-LoopBack1] quit
```

配置 LSRB。

```
[LSRB] isis 1
[LSRB-isis-1] network-entity 00.0005.0000.0000.0002.00
[LSRB-isis-1] is-level level-2
[LSRB-isis-1] quit
[LSRB] interface gigabitethernet 1/0/0
[LSRB-GigabitEthernet1/0/0] isis enable 1
[LSRB-GigabitEthernet1/0/0] quit
[LSRB] interface gigabitethernet 2/0/0
[LSRB-GigabitEthernet2/0/0] isis enable 1
[LSRB-GigabitEthernet2/0/0] quit
[LSRB] interface loopback 1
[LSRB-LoopBack1] isis enable 1
[LSRB-LoopBack1] quit
```

配置 LSRC。

```
[LSRC] isis 1
[LSRC-isis-1] network-entity 00.0005.0000.0000.0003.00
[LSRC-isis-1] is-level level-2
[LSRC-isis-1] quit
[LSRC] interface gigabitethernet 1/0/0
[LSRC-GigabitEthernet1/0/0] isis enable 1
[LSRC-GigabitEthernet1/0/0] quit
[LSRC] interface gigabitethernet 2/0/0
[LSRC-GigabitEthernet2/0/0] isis enable 1
[LSRC-GigabitEthernet2/0/0] quit
[LSRC] interface loopback 1
[LSRC-LoopBack1] isis enable 1
[LSRC-LoopBack1] quit
```

配置 LSRD。

```
[LSRD] isis 1
[LSRD-isis-1] network-entity 00.0005.0000.0000.0004.00
[LSRD-isis-1] is-level level-2
[LSRD-isis-1] quit
[LSRD] interface gigabitethernet 1/0/0
[LSRD-GigabitEthernet1/0/0] isis enable 1
[LSRD-GigabitEthernet1/0/0] quit
[LSRD] interface loopback 1
[LSRD-LoopBack1] isis enable 1
[LSRD-LoopBack1] quit
```

配置完成后，在各节点上执行 **display ip routing-table** 命令，可以看到相互之间都学到了对方的路由。以 LSRA 的显示为例：

```
[LSRA] display ip routing-table
Route Flags: R - relay, 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-L2 15 10 D 10.1.1.2 GigabitEthernet1/0/0
 3.3.3.9/32 ISIS-L2 15 20 D 10.1.1.2 GigabitEthernet1/0/0
 4.4.4.9/32 ISIS-L2 15 30 D 10.1.1.2 GigabitEthernet1/0/0
10.1.1.0/24 Direct 0 0 D 10.1.1.1 GigabitEthernet1/0/0
10.1.1.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
20.1.1.0/24 ISIS-L2 15 20 D 10.1.1.2 GigabitEthernet1/0/0
30.1.1.0/24 ISIS-L2 15 30 D 10.1.1.2 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 配置 MPLS 基本能力，使能 MPLS TE、RSVP-TE 和 CSPF

在各节点全局使能 MPLS、MPLS TE 和 RSVP-TE，在隧道沿途的接口上使能 MPLS、MPLS TE 和 RSVP-TE，并在入节点的系统视图下使能 CSPF。

配置 LSRA。

```
[LSRA] mpls lsr-id 1.1.1.9
[LSRA] mpls
[LSRA-mpls] mpls te
[LSRA-mpls] mpls rsvp-te
[LSRA-mpls] mpls te cspf
[LSRA-mpls] quit
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] mpls
[LSRA-GigabitEthernet1/0/0] mpls te
[LSRA-GigabitEthernet1/0/0] mpls rsvp-te
[LSRA-GigabitEthernet1/0/0] quit
```

配置 LSRB。

```
[LSRB] mpls lsr-id 2.2.2.9
[LSRB] mpls
[LSRB-mpls] mpls te
[LSRB-mpls] mpls rsvp-te
[LSRB-mpls] quit
[LSRB] interface gigabitethernet 1/0/0
[LSRB-GigabitEthernet1/0/0] mpls
[LSRB-GigabitEthernet1/0/0] mpls te
[LSRB-GigabitEthernet1/0/0] mpls rsvp-te
[LSRB-GigabitEthernet1/0/0] quit
[LSRB] interface gigabitethernet 2/0/0
[LSRB-GigabitEthernet2/0/0] mpls
[LSRB-GigabitEthernet2/0/0] mpls te
[LSRB-GigabitEthernet2/0/0] mpls rsvp-te
[LSRB-GigabitEthernet2/0/0] quit
```

配置 LSRC。

```
[LSRC] mpls lsr-id 3.3.3.9
[LSRC] mpls
[LSRC-mpls] mpls te
[LSRC-mpls] mpls rsvp-te
[LSRC-mpls] quit
[LSRC] interface gigabitethernet 1/0/0
[LSRC-GigabitEthernet1/0/0] mpls
[LSRC-GigabitEthernet1/0/0] mpls te
[LSRC-GigabitEthernet1/0/0] mpls rsvp-te
[LSRC-GigabitEthernet1/0/0] quit
[LSRC] interface gigabitethernet 2/0/0
[LSRC-GigabitEthernet2/0/0] mpls
[LSRC-GigabitEthernet2/0/0] mpls te
[LSRC-GigabitEthernet2/0/0] mpls rsvp-te
[LSRC-GigabitEthernet2/0/0] quit
```

配置 LSRD。

```
[LSRD] mpls lsr-id 4.4.4.9
[LSRD] mpls
[LSRD-mpls] mpls te
[LSRD-mpls] mpls rsvp-te
[LSRD-mpls] quit
[LSRD] interface gigabitethernet 1/0/0
[LSRD-GigabitEthernet1/0/0] mpls
[LSRD-GigabitEthernet1/0/0] mpls te
[LSRD-GigabitEthernet1/0/0] mpls rsvp-te
[LSRD-GigabitEthernet1/0/0] quit
```

步骤 4 配置 IS-IS TE

配置 LSRA。

```
[LSRA] isis 1
[LSRA-isis-1] cost-style wide
[LSRA-isis-1] traffic-eng level-2
[LSRA-isis-1] quit
```

配置 LSRB。

```
[LSRB] isis 1
[LSRB-isis-1] cost-style wide
[LSRB-isis-1] traffic-eng level-2
[LSRB-isis-1] quit
```

配置 LSRC。

```
[LSRC] isis 1
[LSRC-isis-1] cost-style wide
[LSRC-isis-1] traffic-eng level-2
[LSRC-isis-1] quit
```

配置 LSRD。

```
[LSRD] isis 1
[LSRD-isis-1] cost-style wide
[LSRD-isis-1] traffic-eng level-2
[LSRD-isis-1] quit
```

步骤 5 配置链路的 MPLS TE 带宽属性

在隧道沿途各接口上配置链路的最大可预留带宽和 BC0 带宽。

配置 LSRA。

```
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[LSRA-GigabitEthernet1/0/0] mpls te bandwidth bc0 100000
[LSRA-GigabitEthernet1/0/0] quit
```

配置 LSRB。

```
[LSRB] interface gigabitethernet 2/0/0
[LSRB-GigabitEthernet2/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[LSRB-GigabitEthernet2/0/0] mpls te bandwidth bc0 100000
[LSRB-GigabitEthernet2/0/0] quit
```

配置 LSRC。

```
[LSRC] interface gigabitethernet 1/0/0
[LSRC-GigabitEthernet1/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[LSRC-GigabitEthernet1/0/0] mpls te bandwidth bc0 100000
[LSRC-GigabitEthernet1/0/0] quit
```

步骤 6 配置 MPLS TE 隧道接口

在隧道入节点上创建 Tunnel 接口，并配置 Tunnel 接口的 IP 地址、隧道协议、目的地地址、Tunnel ID、动态信令协议以及隧道带宽，并执行 **mpls te commit** 命令使配置生效。

配置 LSRA。

```
[LSRA] interface tunnel 0/0/0
[LSRA-Tunnel0/0/0] ip address unnumbered interface loopback 1
[LSRA-Tunnel0/0/0] tunnel-protocol mpls te
[LSRA-Tunnel0/0/0] destination 4.4.4.9
[LSRA-Tunnel0/0/0] mpls te tunnel-id 100
[LSRA-Tunnel0/0/0] mpls te signal-protocol rsvp-te
[LSRA-Tunnel0/0/0] mpls te bandwidth ct0 20000
[LSRA-Tunnel0/0/0] mpls te commit
[LSRA-Tunnel0/0/0] quit
```

步骤 7 检查配置结果

配置完成后，在 LSRA 上执行 **display interface tunnel** 命令可以看到隧道接口状态为 Up。

```
[LSRA] display interface tunnel
Tunnel0/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time: 2012-02-15, 16:35:10
Description : HUAWEL, AR Series, Tunnel0/0/0 Interface
...
```

在 LSRA 上执行 **display mpls te tunnel verbose** 命令可以看到隧道详细信息。

```
<LSRA> display mpls te tunnel verbose
No : 1
Tunnel-Name : Tunnel0/0/0
TunnelIndex : 0 LSP Index : 2048
Session ID : 100 LSP ID : 1
```

```

Lsr Role           : Ingress      Lsp Type           : Primary
Ingress LSR ID    : 1.1.1.9
Egress LSR ID     : 4.4.4.9
In-Interface      : -
Out-Interface     : GE1/0/0
Sign-Protocol     : RSVP TE      Resv Style         : SE
IncludeAnyAff     : 0x0          ExcludeAnyAff      : 0x0
IncludeAllAff     : 0x0
LspConstraint     : -
ER-Hop Table Index : -           AR-Hop Table Index: -
C-Hop Table Index : 0
PrevTunnelIndexInSession: -      NextTunnelIndexInSession: -
PSB Handle        : 1024
Created Time      : 2012/02/16 16:01:18 UTC-08:00
    
```

DS-TE Information

```

Bandwidth Reserved Flag : Reserved
CT0 Bandwidth(Kbit/sec) : 10000      CT1 Bandwidth(Kbit/sec): 0
CT2 Bandwidth(Kbit/sec) : 0          CT3 Bandwidth(Kbit/sec): 0
CT4 Bandwidth(Kbit/sec) : 0          CT5 Bandwidth(Kbit/sec): 0
CT6 Bandwidth(Kbit/sec) : 0          CT7 Bandwidth(Kbit/sec): 0
Setup-Priority          : 0          Hold-Priority       : 0
    
```

FRR Information

```

Primary LSP Info
TE Attribute Flag      : 0x2          Protected Flag      : 0x0
Bypass In Use         : Not Exists
Bypass Tunnel Id      : -
BypassTunnel          : -
Bypass Lsp ID         : -           FrrNextHop         : -
ReferAutoBypassHandle : -
FrrPrevTunnelTableIndex : -       FrrNextTunnelTableIndex: -
Bypass Attribute(Not configured)
Setup Priority         : -           Hold Priority       : -
HopLimit              : -           Bandwidth           : -
IncludeAnyGroup       : -           ExcludeAnyGroup     : -
IncludeAllGroup       : -
Bypass Unbound Bandwidth Info(Kbit/sec)
CT0 Unbound Bandwidth : -           CT1 Unbound Bandwidth: -
CT2 Unbound Bandwidth : -           CT3 Unbound Bandwidth: -
CT4 Unbound Bandwidth : -           CT5 Unbound Bandwidth: -
CT6 Unbound Bandwidth : -           CT7 Unbound Bandwidth: -
    
```

BFD Information

```

NextSessionTunnelIndex : -           PrevSessionTunnelIndex: -
NextLspId              : -           PrevLspId           : -
    
```

在 LSRA 上执行 **display mpls te cspf tedb all** 命令查看 TEDB 中的链路信息。

```

[LSRA] display mpls te cspf tedb all
Maximum Node Supported: 128          Maximum Link Supported: 256
Current Total Node Number: 4        Current Total Link Number: 6
Maximum SRLGs supported: 5120      Current Total SRLG Number: 0
Id   Router-Id   IGP   Process-Id   Area   Link-Count
1    3.3.3.9      ISIS  1            Level-2  2
2    2.2.2.9      ISIS  1            Level-2  2
3    4.4.4.9      ISIS  1            Level-2  1
4    1.1.1.9      ISIS  1            Level-2  1
    
```

----结束

配置文件

- LSRA 的配置文件

#

```
    sysname LSRA
#
mpls lsr-id 1.1.1.9
mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
isis 1
  is-level level-2
  cost-style wide
  network-entity 00.0005.0000.0000.0001.00
  traffic-eng level-2
#
interface GigabitEthernet1/0/0
  ip address 10.1.1.1 255.255.255.0
  isis enable 1
  mpls
  mpls te
  mpls te bandwidth max-reservable-bandwidth 100000
  mpls te bandwidth bc0 100000
  mpls rsvp-te
#
interface LoopBack1
  ip address 1.1.1.9 255.255.255.255
  isis enable 1
#
interface Tunnel0/0/0
  ip address unnumbered interface LoopBack1
  tunnel-protocol mpls te
  destination 4.4.4.9
  mpls te tunnel-id 100
  mpls te bandwidth ct0 20000
  mpls te commit
#
return
```

● LSRB 的配置文件

```
#
  sysname LSRB
#
mpls lsr-id 2.2.2.9
mpls
  mpls te
  mpls rsvp-te
#
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
  ip address 10.1.1.2 255.255.255.0
  isis enable 1
  mpls
  mpls te
  mpls rsvp-te
#
interface GigabitEthernet2/0/0
  ip address 20.1.1.1 255.255.255.0
  isis enable 1
  mpls
  mpls te
  mpls te bandwidth max-reservable-bandwidth 100000
  mpls te bandwidth bc0 100000
  mpls rsvp-te
#
interface LoopBack1
  ip address 2.2.2.9 255.255.255.255
```

```
isis enable 1
#
return
```

- LSRC 的配置文件

```
#
sysname LSRC
#
mpls lsr-id 3.3.3.9
mpls
  mpls te
  mpls rsvp-te
#
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
  ip address 30.1.1.1 255.255.255.0
  isis enable 1
  mpls
  mpls te
  mpls te bandwidth max-reservable-bandwidth 100000
  mpls te bandwidth bc0 100000
  mpls rsvp-te
#
interface GigabitEthernet2/0/0
  ip address 20.1.1.2 255.255.255.0
  isis enable 1
  mpls
  mpls te
  mpls rsvp-te
#
interface LoopBack1
  ip address 3.3.3.9 255.255.255.255
  isis enable 1
#
return
```

- LSRD 的配置文件

```
#
sysname LSRD
#
mpls lsr-id 4.4.4.9
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
  ip address 30.1.1.2 255.255.255.0
  isis enable 1
  mpls
  mpls te
  mpls rsvp-te
#
interface LoopBack1
  ip address 4.4.4.9 255.255.255.255
  isis enable 1
#
return
```

3.21.3 配置 MPLS TE FRR 示例

本例描述了如何利用 TE FRR 实现链路保护。

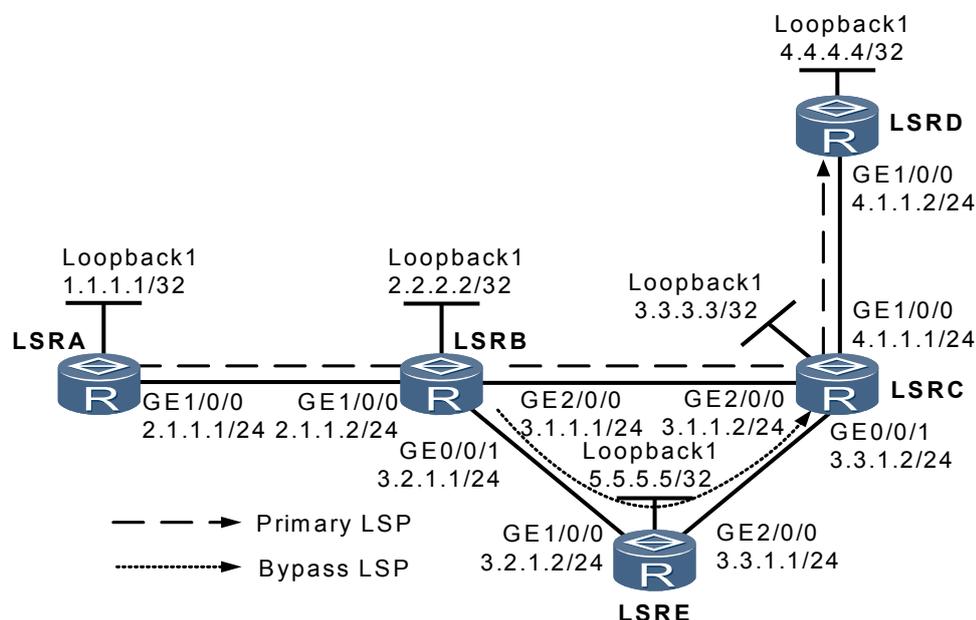
组网需求

如图 3-4 所示，主 LSP 是 LSRA→LSRB→LSRC→LSRD，要求对 LSRB→LSRC 这段链路通过 FRR 进行链路保护。

建立一条 Bypass LSP，使用路径 LSRB→LSRE→LSRC。LSRB 是本地修复节点 PLR，LSRC 是汇聚点 MP。

使用显式路径方式建立 MPLS TE 的主隧道和旁路隧道。使用的信令协议是 RSVP-TE。

图 3-4 MPLS TE FRR 配置组网图



配置思路

采用如下的思路配置 TE FRR：

1. 建立主隧道，在隧道接口下使能 TE FRR。
2. 在被保护链路的入节点即 PLR 配置 Bypass Tunnel，并在隧道接口视图下指定其可保护的带宽以及被保护链路的接口。

数据准备

为完成此配置例，需准备如下的数据：

- 各节点的 IS-IS 区域 ID、起始的系统 ID、IS-IS Level
- 隧道沿途的链路最大可预留带宽和 BC 带宽
- 主 Tunnel 和 Bypass Tunnel 的显式路径

- 主 Tunnel 和 Bypass Tunnel 的接口、IP 地址、目的地址、隧道 ID，隧道信令协议（为 RSVP-TE）
- Bypass Tunnel 可保护的带宽、被保护的链路接口

操作步骤

步骤 1 配置各接口的 IP 地址

按照图 3-4 配置各接口的 IP 地址和掩码，包括各 Loopback 接口，具体配置过程略。

步骤 2 配置 IGP 协议

在所有节点上配置 IS-IS 协议，发布 LSR ID 的主机路由，具体配置过程略。

配置完成后，在各节点上执行 **display ip routing-table** 命令，应可以看到相互之间都学到了对方的路由。

步骤 3 配置 MPLS 基本能力，使能 MPLS TE、CSPF 和 RSVP-TE 及 IS-IS TE

配置 LSRA。

```
[LSRA] mpls lsr-id 1.1.1.1
[LSRA] mpls
[LSRA-mpls] mpls te
[LSRA-mpls] mpls rsvp-te
[LSRA-mpls] mpls te cspf
[LSRA-mpls] quit
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] mpls
[LSRA-GigabitEthernet1/0/0] mpls te
[LSRA-GigabitEthernet1/0/0] mpls rsvp-te
[LSRA-GigabitEthernet1/0/0] quit
[LSRA] isis
[LSRA-isis-1] cost-style wide
[LSRA-isis-1] traffic-eng level-2
```

 说明

LSRB、LSRC、LSRD、LSRE 的配置与 LSRA 的配置类似，此处不再赘述。其中，CSPF 只要在主隧道入节点 LSRA 和旁路隧道入节点 LSRB 上使能即可，LSRC、LSRD 和 LSRE 上无需使能 CSPF。

步骤 4 配置链路的 MPLS TE 带宽属性

在 LSRA、LSRB、LSRC、LSRD 和 LSRE 上配置链路最大可预留带宽为 100Mbit/s，BC0 带宽为 100Mbit/s。

配置 LSRA。

```
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[LSRA-GigabitEthernet1/0/0] mpls te bandwidth bc0 100000
[LSRA-GigabitEthernet1/0/0] quit
```

配置 LSRB。

```
[LSRB] interface gigabitethernet 2/0/0
[LSRB-GigabitEthernet2/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[LSRB-GigabitEthernet2/0/0] mpls te bandwidth bc0 100000
[LSRB-GigabitEthernet2/0/0] quit
[LSRB] interface gigabitethernet 0/0/1
[LSRB-GigabitEthernet0/0/1] mpls te bandwidth max-reservable-bandwidth 100000
[LSRB-GigabitEthernet0/0/1] mpls te bandwidth bc0 100000
[LSRB-GigabitEthernet0/0/1] quit
```

配置 LSRC。

```
[LSRC] interface gigabitethernet 1/0/0
[LSRC-GigabitEthernet1/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[LSRC-GigabitEthernet1/0/0] mpls te bandwidth bc0 100000
[LSRC-GigabitEthernet1/0/0] quit
```

配置 LSRE。

```
[LSRE] interface gigabitethernet 2/0/0
[LSRE-GigabitEthernet2/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[LSRE-GigabitEthernet2/0/0] mpls te bandwidth bc0 100000
[LSRE-GigabitEthernet2/0/0] quit
```

步骤 5 在主 LSP 的入节点 LSRA 上建立 MPLS TE Tunnel

配置主 LSP 的显式路径。

```
[LSRA] explicit-path pri-path
[LSRA-explicit-path-pri-path] next hop 2.1.1.2
[LSRA-explicit-path-pri-path] next hop 3.1.1.2
[LSRA-explicit-path-pri-path] next hop 4.1.1.2
[LSRA-explicit-path-pri-path] next hop 4.4.4.4
[LSRA-explicit-path-pri-path] quit
```

配置主 LSP 的 MPLS TE 隧道。

```
[LSRA] interface tunnel 0/0/0
[LSRA-Tunnel0/0/0] ip address unnumbered interface loopback 1
[LSRA-Tunnel0/0/0] tunnel-protocol mpls te
[LSRA-Tunnel0/0/0] destination 4.4.4.4
[LSRA-Tunnel0/0/0] mpls te tunnel-id 100
[LSRA-Tunnel0/0/0] mpls te signal-protocol rsvp-te
[LSRA-Tunnel0/0/0] mpls te bandwidth ct0 50000
[LSRA-Tunnel0/0/0] mpls te path explicit-path pri-path
```

使能 FRR。

```
[LSRA-Tunnel0/0/0] mpls te fast-reroute
[LSRA-Tunnel0/0/0] mpls te commit
[LSRA-Tunnel0/0/0] quit
```

配置完成后，在 LSRA 上执行 **display interface tunnel** 命令，可以看到 Tunnel0/0/0 的状态为 Up。

```
[LSRA] display interface tunnel 0/0/0
Tunnel0/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time: : 2012-02-12, 09:35:10
Description : HUAWEI, AR Series, Tunnel0/0/0 Interface
...
```

在 LSRA 上执行 **display mpls te tunnel verbose** 命令，可以看到隧道接口的详细信息。

```
[LSRA] display mpls te tunnel verbose
No                : 1
Tunnel-Name       : Tunnel0/0/0
Tunnel Interface Name : Tunnel0/0/0
TunnelIndex      : 0          LSP Index      : 2048
Session ID       : 100       LSP ID       : 1
Lsr Role         : Ingress
Ingress LSR ID   : 1.1.1.1
Egress LSR ID    : 4.4.4.4
In-Interface     : -
Out-Interface    : GE1/0/0
Sign-Protocol    : RSVP TE   Resv Style   : SE
IncludeAnyAff   : 0x0       ExcludeAnyAff : 0x0
IncludeAllAff   : 0x0
LspConstraint    : -
ER-Hop Table Index : 0          AR-Hop Table Index: 0
C-Hop Table Index : 0
```

```
PrevTunnelIndexInSession: -      NextTunnelIndexInSession: -
PSB Handle                : 1081
Created Time               : 2012/02/13 15:02:57 UTC-08:00
-----
DS-TE Information
-----
Bandwidth Reserved Flag : Reserved
CT0 Bandwidth(Kbit/sec) : 50000      CT1 Bandwidth(Kbit/sec): 0
CT2 Bandwidth(Kbit/sec) : 0          CT3 Bandwidth(Kbit/sec): 0
CT4 Bandwidth(Kbit/sec) : 0          CT5 Bandwidth(Kbit/sec): 0
CT6 Bandwidth(Kbit/sec) : 0          CT7 Bandwidth(Kbit/sec): 0
Setup-Priority           : 0          Hold-Priority          : 0
-----
FRR Information
-----
Primary LSP Info
TE Attribute Flag        : 0x2      Protected Flag        : 0x0
Bypass In Use           : Not Exists
Bypass Tunnel Id        : -
BypassTunnel            : -
Bypass Lsp ID           : -          FrrNextHop           : -
ReferAutoBypassHandle  : -
FrrPrevTunnelTableIndex : -          FrrNextTunnelTableIndex: -
Bypass Attribute(Not configured)
Setup Priority           : -          Hold Priority         : -
HopLimit                : -          Bandwidth             : -
IncludeAnyGroup         : -          ExcludeAnyGroup       : -
IncludeAllGroup         : -
Bypass Unbound Bandwidth Info(Kbit/sec)
CT0 Unbound Bandwidth  : -          CT1 Unbound Bandwidth: -
CT2 Unbound Bandwidth  : -          CT3 Unbound Bandwidth: -
CT4 Unbound Bandwidth  : -          CT5 Unbound Bandwidth: -
CT6 Unbound Bandwidth  : -          CT7 Unbound Bandwidth: -
-----
BFD Information
-----
NextSessionTunnelIndex : -          PrevSessionTunnelIndex: -
NextLspId              : -          PrevLspId             : -
```

步骤 6 在作为 PLR 的 LSRB 上配置 Bypass Tunnel

配置 Bypass LSP 的显式路径。

```
[LSRB] explicit-path by-path
[LSRB-explicit-path-by-path] next hop 3.2.1.2
[LSRB-explicit-path-by-path] next hop 3.3.1.2
[LSRB-explicit-path-by-path] next hop 3.3.3.3
[LSRB-explicit-path-by-path] quit
```

配置 Bypass Tunnel。

```
[LSRB] interface tunnel 0/0/1
[LSRB-Tunnel0/0/1] ip address unnumbered interface loopback 1
[LSRB-Tunnel0/0/1] tunnel-protocol mpls te
[LSRB-Tunnel0/0/1] destination 3.3.3.3
[LSRB-Tunnel0/0/1] mpls te tunnel-id 300
[LSRB-Tunnel0/0/1] mpls te signal-protocol rsvp-te
[LSRB-Tunnel0/0/1] mpls te path explicit-path by-path
[LSRB-Tunnel0/0/1] mpls te bandwidth ct0 100000
```

配置 Bypass Tunnel 可保护的带宽。

```
[LSRB-Tunnel0/0/1] mpls te bypass-tunnel
```

将 Bypass Tunnel 绑定到被保护的接口。

```
[LSRB-Tunnel0/0/1] mpls te protected-interface gigabitethernet 2/0/0
[LSRB-Tunnel0/0/1] mpls te commit
[LSRB-Tunnel0/0/1] quit
```

配置完成后，在 LSRB 上执行 **display interface tunnel** 命令可以看到接口 Tunnel0/0/1 的状态为 Up。

在节点上执行 **display mpls lsp** 命令，可以看到 LSP 表项，并且，LSRB 和 LSRC 上有两条 LSP 经过。

```
[LSRA] display mpls lsp
-----
LSP Information: RSVP LSP
-----
FEC                In/Out Label  In/Out IF          Vrf Name
4.4.4.4/32         NULL/13312   -/GE1/0/0
[LSRB] display mpls lsp
-----
LSP Information: RSVP LSP
-----
FEC                In/Out Label  In/Out IF          Vrf Name
4.4.4.4/32         13312/13312  GE1/0/0/GE2/0/0
3.3.3.3/32         NULL/13312   -/GE0/0/1
[LSRC] display mpls lsp
-----
LSP Information: RSVP LSP
-----
FEC                In/Out Label  In/Out IF          Vrf Name
4.4.4.4/32         13312/3      GE2/0/0/GE1/0/0
[LSRE] display mpls lsp
-----
LSP Information: RSVP LSP
-----
FEC                In/Out Label  In/Out IF          Vrf Name
3.3.3.3/32         13312/3      GE1/0/0/GE2/0/0
```

在节点上执行 **display mpls te tunnel** 命令，可以看到隧道的建立情况，LSRB 和 LSRC 上有两条隧道经过。

```
[LSRA] display mpls te tunnel
-----
Ingress LsrId      Destination    LSPID  In/Out Label  R  Tunnel-name
-----
1.1.1.1            4.4.4.4       1      --/3          I  Tunnel0/0/0
[LSRB] display mpls te tunnel
-----
Ingress LsrId      Destination    LSPID  In/Out Label  R  Tunnel-name
-----
1.1.1.1            4.4.4.4       1      1026/3       I  Tunnel0/0/0
2.2.2.2            3.3.3.3       1      --/3          I  Tunnel0/0/1
[LSRC] display mpls te tunnel
-----
Ingress LsrId      Destination    LSPID  In/Out Label  R  Tunnel-name
-----
1.1.1.1            4.4.4.4       1      1024/3       I  Tunnel0/0/0
2.2.2.2            3.3.3.3       1      3/--         I  Tunnel0/0/1
[LSRE] display mpls te tunnel
-----
Ingress LsrId      Destination    LSPID  In/Out Label  R  Tunnel-name
-----
2.2.2.2            3.3.3.3       1      1025/3       I  Tunnel0/0/1
```

在 LSRA 上执行 **display mpls te tunnel name Tunnel0/0/0 verbose** 命令，可以看到旁路隧道绑定到出接口 GE2/0/0，目前未被使用。

```
[LSRA] display mpls te tunnel name Tunnel0/0/0 verbose
No                : 1
Tunnel-Name       : Tunnel0/0/0
```

```
Tunnel Interface Name : Tunnel0/0/0
TunnelIndex          : 1           LSP Index           : 4098
Session ID           : 100         LSP ID              : 1
Lsr Role              : Transit    LSP Type            : Primary
Ingress LSR ID       : 1.1.1.1
Egress LSR ID        : 4.4.4.4
In-Interface         : GE1/0/0
Out-Interface        : GE2/0/0
Sign-Protocol        : RSVP TE     Resv Style           : SE
IncludeAnyAff        : 0x0         ExcludeAnyAff        : 0x0
IncludeAllAff        : 0x0
LspConstraint        : -
ER-Hop Table Index   : -           AR-Hop Table Index  : 2
C-Hop Table Index    : 1
PrevTunnelIndexInSession: -       NextTunnelIndexInSession: -
PSB Handle           : 65546
Created Time         : 2012/02/13 09:42:04
```

DS-TE Information

```
Bandwidth Reserved Flag : Reserved
CT0 Bandwidth(Kbit/sec) : 100000   CT1 Bandwidth(Kbit/sec): 0
CT2 Bandwidth(Kbit/sec) : 0         CT3 Bandwidth(Kbit/sec): 0
CT4 Bandwidth(Kbit/sec) : 0         CT5 Bandwidth(Kbit/sec): 0
CT6 Bandwidth(Kbit/sec) : 0         CT7 Bandwidth(Kbit/sec): 0
Setup-Priority          : 0         Hold-Priority        : 0
```

FRR Information

```
Primary LSP Info
TE Attribute Flag      : 0x63       Protected Flag       : 0x1
Bypass In Use         : Not Used
Bypass Tunnel Id      : 67141670
BypassTunnel        : Tunnel Index[Tunnel0/0/1], InnerLabel[1024]
Bypass Lsp ID         : 9           FrrNextHop         : 3.3.1.2
ReferAutoBypassHandle : -
FrrPrevTunnelTableIndex : -       FrrNextTunnelTableIndex: -
Bypass Attribute(Not configured)
Setup Priority         : -           Hold Priority        : -
HopLimit              : -           Bandwidth            : -
IncludeAnyGroup       : -           ExcludeAnyGroup      : -
IncludeAllGroup       : -
Bypass Unbound Bandwidth Info(Kbit/sec)
CT0 Unbound Bandwidth : -           CT1 Unbound Bandwidth: -
CT2 Unbound Bandwidth : -           CT3 Unbound Bandwidth: -
CT4 Unbound Bandwidth : -           CT5 Unbound Bandwidth: -
CT6 Unbound Bandwidth : -           CT7 Unbound Bandwidth: -
```

BFD Information

```
NextSessionTunnelIndex : -       PrevSessionTunnelIndex: -
NextLspId               : -       PrevLspId             : -
```

步骤 7 检查配置结果

使 PLR 上被保护的出接口失效。

```
[LSRB] interface gigabitethernet 2/0/0
[LSRB-GigabitEthernet2/0/0] shutdown
```

在 LSRA 上执行命令 **display interface tunnel 0/0/0**，查看主 LSP 的状态，可以看到 Tunnel 接口仍然处于 UP 状态。

在 LSRA 上执行 **tracert lsp te tunnel 0/0/0** 命令来查看隧道经过的路径。

```
[LSRA] tracert lsp te tunnel 0/0/0
LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel0/0/0 , press CTRL_C to break.
TTL  Replier          Time  Type      Downstream
0           Ingress  2.1.1.2/[13312 ]
```

1	2.1.1.2	1 ms	Transit
2	3.2.1.2	16 ms	Transit
3	3.3.1.2	1 ms	Transit
4	4.1.1.2	1 ms	Egress

由此可以确认链路已切换到 Bypass Tunnel。

📖 说明

如果在 FRR 切换后马上执行 **display mpls te tunnel-interface** 命令查看隧道接口的详细信息，会看到两条处于 UP 状态的 CR-LSP。这是因为 FRR 采用 Make-before-break 方式建立新的 LSP，旧的 LSP 在新 LSP 建立成功后过一段时间才被删除。

在 LSRA 上执行 **display mpls te tunnel name Tunnel0/0/0 verbose** 命令，可以看到旁路隧道被使用。

```
[LSRA] display mpls te tunnel name Tunnel0/0/0 verbose
No : 1
Tunnel-Name : Tunnel0/0/0
TunnelIndex : 1          LSP Index : 4098
Session ID : 100        LSP ID : 1
Lsr Role : Transit
Ingress LSR ID : 1.1.1.1
Egress LSR ID : 4.4.4.4
In-Interface : GE1/0/0
Out-Interface : GE2/0/0
Sign-Protocol : RSVP TE   Resv Style : SE
IncludeAnyAff : 0x0       ExcludeAnyAff : 0x0
IncludeAllAff : 0x0
ER-Hop Table Index : 3      AR-Hop Table Index: 12
C-Hop Table Index : 50
PrevTunnelIndexInSession: -   NextTunnelIndexInSession: -
PSB Handle : 66000
Created Time : 2012/02/13 10:09:10

-----
DS-TE Information
-----
Bandwidth Reserved Flag : Unreserved
CT0 Bandwidth(Kbit/sec) : 100000   CT1 Bandwidth(Kbit/sec): 0
CT2 Bandwidth(Kbit/sec) : 0         CT3 Bandwidth(Kbit/sec): 0
CT4 Bandwidth(Kbit/sec) : 0         CT5 Bandwidth(Kbit/sec): 0
CT6 Bandwidth(Kbit/sec) : 0         CT7 Bandwidth(Kbit/sec): 0
Setup-Priority : 0                 Hold-Priority : 0

-----
FRR Information
-----
Primary LSP Info
TE Attribute Flag : 0x63           Protected Flag : 0x1
Bypass In Use : In Use
Bypass Tunnel Id : 67141670
BypassTunnel : Tunnel Index[Tunnel0/0/1], InnerLabel[1024]
Bypass Lsp ID : 9                 FrrNextHop : 3.3.1.2
ReferAutoBypassHandle : -
FrrPrevTunnelTableIndex : -       FrrNextTunnelTableIndex: -
Bypass Attribute(Not configured)
Setup Priority : -                 Hold Priority : -
HopLimit : -                       Bandwidth : -
IncludeAnyGroup : -               ExcludeAnyGroup : -
IncludeAllGroup : -
Bypass Unbound Bandwidth Info(Kbit/sec)
CT0 Unbound Bandwidth : -         CT1 Unbound Bandwidth: -
CT2 Unbound Bandwidth : -         CT3 Unbound Bandwidth: -
CT4 Unbound Bandwidth : -         CT5 Unbound Bandwidth: -
CT6 Unbound Bandwidth : -         CT7 Unbound Bandwidth: -

-----
BFD Information
-----
NextSessionTunnelIndex : -         PrevSessionTunnelIndex: -
NextLspId : -                     PrevLspId : -
```

在 PLR 上配置 FRR 的扫描定时器为 5 秒。

```
[LSRB] mpls
[LSRB-mpls] mpls te timer fast-reroute 5
[LSRB-mpls] quit
```

使 PLR 上被保护的出接口重新生效。

```
[LSRB] interface gigabitethernet 2/0/0
[LSRB-GigabitEthernet2/0/0] undo shutdown
```

在 LSRA 上查看主 LSP 的状态，执行命令 **display interface tunnel 0/0/0**，可以看到 Tunnel 接口处于 UP 状态。

等待一段时间后，在 LSRA 上执行 **display mpls te tunnel name Tunnel0/0/0 verbose** 命令，可以看到 Tunnel0/0/0 的 Bypass In Use 的状态为 Not Used，表明数据流已切回到 GE2/0/0 传输。

---结束

配置文件

- LSRA 的配置文件

```
#
sysname LSRA
#
mpls lsr-id 1.1.1.1
mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
explicit-path pri-path
  next hop 2.1.1.2
  next hop 3.1.1.2
  next hop 4.1.1.2
  next hop 4.4.4.4
#
isis 1
  is-level level-2
  cost-style wide
  network-entity 00.0005.0000.0000.0001.00
  traffic-eng level-2
#
interface GigabitEthernet1/0/0
  ip address 2.1.1.1 255.255.255.0
  isis enable 1
  mpls
  mpls te
  mpls te bandwidth max-reservable-bandwidth 100000
  mpls te bandwidth bc0 100000
  mpls rsvp-te
#
interface LoopBack1
  ip address 1.1.1.1 255.255.255.255
  isis enable 1
#
interface Tunnel0/0/0
  ip address unnumbered interface LoopBack1
  tunnel-protocol mpls te
  destination 4.4.4.4
mpls te record-route label
  mpls te path explicit-path pri-path
mpls te tunnel-id 100
mpls te bandwidth ct0 50000
mpls te fast-reroute
mpls te commit
```

```
#
return
● LSRB 的配置文件
#
mpls lsr-id 2.2.2.2
mpls
  mpls te
  mpls te timer fast-reroute 5
  mpls rsvp-te
  mpls te cspf
#
explicit-path by-path
  next hop 3.2.1.2
  next hop 3.3.1.2
  next hop 3.3.3.3
#
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
  ip address 2.1.1.2 255.255.255.0
  isis enable 1
  mpls
  mpls te
  mpls rsvp-te
#
interface GigabitEthernet2/0/0
  ip address 3.1.1.1 255.255.255.0
  isis enable 1
  mpls
  mpls te
  mpls te bandwidth max-reservable-bandwidth 100000
  mpls te bandwidth bc0 100000
  mpls rsvp-te
#
interface GigabitEthernet0/0/1
  ip address 3.2.1.1 255.255.255.0
  isis enable 1
  mpls
  mpls te
  mpls te bandwidth max-reservable-bandwidth 100000
  mpls te bandwidth bc0 100000
  mpls rsvp-te
#
interface LoopBack1
  ip address 2.2.2.2 255.255.255.255
  isis enable 1
#
interface Tunnel0/0/1
  ip address unnumbered interface LoopBack1
  tunnel-protocol mpls te
  destination 3.3.3.3
  mpls te tunnel-id 300
  mpls te record-route
  mpls te path explicit-path by-path
  mpls te bandwidth ct0 100000
  mpls te bypass-tunnel
  mpls te protected-interface GigabitEthernet 2/0/0
  mpls te commit
#
return
● LSRC 的配置文件
#
sysname LSRC
#
```

```
mpls lsr-id 3.3.3.3
mpls
  mpls te
  mpls rsvp-te
#
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
  ip address 4.1.1.1 255.255.255.0
  isis enable 1
  mpls
  mpls te
  mpls te bandwidth max-reservable-bandwidth 100000
  mpls te bandwidth bc0 100000
  mpls rsvp-te
#
interface GigabitEthernet2/0/0
  ip address 3.1.1.2 255.255.255.0
  isis enable 1
  mpls
  mpls te
  mpls rsvp-te
#
interface GigabitEthernet0/0/1
  ip address 3.3.1.2 255.255.255.0
  isis enable 1
  mpls
  mpls te
  mpls rsvp-te
#
interface LoopBack1
  ip address 3.3.3.3 255.255.255.255
  isis enable 1
#
return
```

● LSRD 的配置文件

```
#
sysname LSRD
#
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
  ip address 4.1.1.2 255.255.255.0
  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
```

● LSRE 的配置文件

```
#
```

```
sysname LSRE
#
mpls lsr-id 5.5.5.5
mpls
  mpls te
  mpls rsvp-te
#
isis 1
  is-level level-2
  cost-style wide
  network-entity 00.0005.0000.0000.0005.00
  traffic-eng level-2
#
interface GigabitEthernet1/0/0
  ip address 3.2.1.2 255.255.255.0
  isis enable 1
  mpls
  mpls te
  mpls rsvp-te
#
interface GigabitEthernet2/0/0
  ip address 3.3.1.1 255.255.255.0
  isis enable 1
  mpls
  mpls te
  mpls te bandwidth max-reservable-bandwidth 100000
  mpls te bandwidth bc0 100000
  mpls rsvp-te
#
interface LoopBack1
  ip address 5.5.5.5 255.255.255.255
  isis enable 1
#
return
```

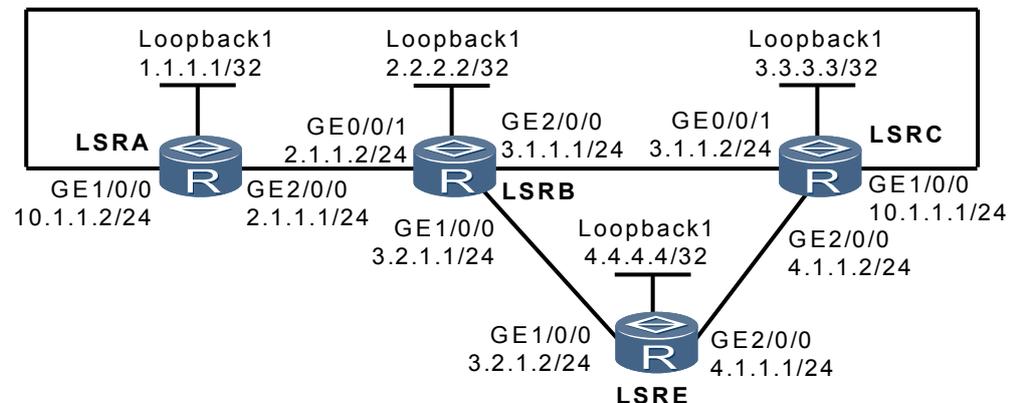
3.21.4 配置 MPLS TE Auto FRR 示例

本例描述了如何在入节点和中间节点上分别创建一条节点保护和一条链路保护的旁路隧道，并且都提供带宽保护的过程。

组网需求

如图 3-5 所示，要求创建一条沿显式路径：LSRA→LSRB→LSRC 的主隧道。在入节点 LSRA 和中间节点 LSRB 上分别创建一条节点保护和一条链路保护的旁路隧道，并且都提供带宽保护。

图 3-5 配置 TE Auto FRR 组网图



配置思路

采用如下的思路配置 TE Auto FRR:

1. 建立主隧道，在隧道接口下使能 TE FRR，并在 MPLS 视图下使能 MPLS Auto FRR。
2. 在隧道接口视图下指定旁路隧道可保护的带宽以及优先级。

数据准备

为完成此配置例，需准备如下的数据:

- 各节点的 OSPF 进程号、所在的区域
- 链路最大可预留带宽和 BC 带宽
- 主隧道经过的路径
- 主隧道接口的接口编号、IP 地址、目的地址、隧道 ID、隧道信令协议（为 RSVP-TE）、隧道带宽

操作步骤

步骤 1 配置各接口的 IP 地址

按照图 3-5 配置各接口的 IP 地址和掩码，包括各 Loopback 接口，具体配置过程略。

步骤 2 配置 OSPF 协议发布各网段路由及 LSR ID 的主机路由

在所有节点上配置 OSPF 协议，发布 LSR ID 的主机路由，具体配置过程略。

配置完成后，在各节点上执行 **display ip routing-table** 命令，应可以看到相互之间都学到了对方 LSR ID 的主机路由。

步骤 3 配置 MPLS 基本能力，使能 MPLS TE、RSVP-TE 和 CSPF

配置 LSRA。

```
[LSRA] mpls lsr-id 1.1.1.1
[LSRA] mpls
[LSRA-mpls] mpls te
[LSRA-mpls] mpls rsvp-te
[LSRA-mpls] mpls te cspf
[LSRA-mpls] quit
[LSRA] interface gigabitethernet 2/0/0
[LSRA-GigabitEthernet2/0/0] mpls
[LSRA-GigabitEthernet2/0/0] mpls te
[LSRA-GigabitEthernet2/0/0] mpls rsvp-te
[LSRA-GigabitEthernet2/0/0] quit
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] mpls
[LSRA-GigabitEthernet1/0/0] mpls te
[LSRA-GigabitEthernet1/0/0] mpls rsvp-te
[LSRA-GigabitEthernet1/0/0] quit
```

 说明

LSRB、LSRC、LSRD 的配置与 LSRA 的配置相似，此处不再赘述。其中，只需在主隧道和旁路隧道的入节点上使能 CSPF。即，只需在 LSRA、LSRB 上使能 CSPF，LSRC 和 LSRD 上无需使能 CSPF。

步骤 4 配置 OSPF TE

配置 LSRA。

```
[LSRA] ospf
[LSRA-ospf-1] opaque-capability enable
[LSRA-ospf-1] area 0
[LSRA-ospf-1-area-0.0.0.0] mpls-te enable
[LSRA-ospf-1-area-0.0.0.0] quit
[LSRA-ospf-1] quit
```

配置 LSRB。

```
[LSRB] ospf
[LSRB-ospf-1] opaque-capability enable
[LSRB-ospf-1] area 0
[LSRB-ospf-1-area-0.0.0.0] mpls-te enable
[LSRB-ospf-1-area-0.0.0.0] quit
[LSRB-ospf-1] quit
```

配置 LSRC。

```
[LSRC] ospf
[LSRC-ospf-1] opaque-capability enable
[LSRC-ospf-1] area 0
[LSRC-ospf-1-area-0.0.0.0] mpls-te enable
[LSRC-ospf-1-area-0.0.0.0] quit
[LSRC-ospf-1] quit
```

配置 LSRD。

```
[LSRD] ospf
[LSRD-ospf-1] opaque-capability enable
[LSRD-ospf-1] area 0
[LSRD-ospf-1-area-0.0.0.0] mpls-te enable
[LSRD-ospf-1-area-0.0.0.0] quit
[LSRD-ospf-1] quit
```

步骤 5 在各链路上配置 MPLS TE 带宽属性

配置链路的最大可预留带宽为 10MBit/s；BC0 带宽为 10MBit/s；BC1 带宽为 3MBit/s。

配置 LSRA。

```
[LSRA] interface gigabitethernet 2/0/0
[LSRA-GigabitEthernet2/0/0] mpls te bandwidth max-reservable-bandwidth 10000
[LSRA-GigabitEthernet2/0/0] mpls te bandwidth bc0 10000 bc1 3000
```

为简便起见，图中的所有主隧道和旁路隧道经过的链路出接口上均使用这些配置，此处不再赘述。

步骤 6 配置显式路径，准备给主隧道使用

```
[LSRA] explicit-path master
[LSRA-explicit-path-master] next hop 2.1.1.2
[LSRA-explicit-path-master] next hop 3.1.1.2
```

步骤 7 使能 TE Auto FRR

配置 LSRA。

```
[LSRA] mpls
[LSRA-mpls] mpls te auto-frr
```

配置 LSRB。

```
[LSRB] mpls
[LSRB-mpls] mpls te auto-frr
```

步骤 8 配置主隧道

```
[LSRA] interface tunnel0/0/0
[LSRA-Tunnel0/0/0] ip address unnumbered interface loopBack1
[LSRA-Tunnel0/0/0] tunnel-protocol mpls te
```

```
[LSRA-Tunnel0/0/0] destination 3.3.3.3
[LSRA-Tunnel0/0/0] mpls te tunnel-id 200
[LSRA-Tunnel0/0/0] mpls te record-route label
[LSRA-Tunnel0/0/0] mpls te path explicit-path master
[LSRA-Tunnel0/0/0] mpls te bandwidth ct0 400
[LSRA-Tunnel0/0/0] mpls te priority 4 3
[LSRA-Tunnel0/0/0] mpls te fast-reroute bandwidth
[LSRA-Tunnel0/0/0] mpls te bypass-attributes bandwidth 200 priority 5 4
[LSRA-Tunnel0/0/0] mpls te commit
[LSRA-Tunnel0/0/0] quit
```

步骤 9 检查配置结果

在入节点 LSRA 上使用命令 **display mpls te tunnel name Tunnel0/0/0 verbose** 查看 LSP 信息时，可以看到主隧道信息及与之绑定的旁路隧道。

```
[LSRA] display mpls te tunnel name Tunnel0/0/0 verbose
No : 1
Tunnel-Name : Tunnel0/0/0
Tunnel Interface Name : Tunnel0/0/0
TunnelIndex : 1 LSP Index : 3072
Session ID : 200 LSP ID : 1
Lsr Role : Ingress LSP Type : Primary
Ingress LSR ID : 1.1.1.1
Egress LSR ID : 3.3.3.3
In-Interface : -
Out-Interface : GE2/0/0
Sign-Protocol : RSVP TE Resv Style : SE
IncludeAnyAff : 0x0 ExcludeAnyAff : 0x0
IncludeAllAff : 0x0
LspConstraint : -
ER-Hop Table Index : - AR-Hop Table Index: 2
C-Hop Table Index : -
PrevTunnelIndexInSession: - NextTunnelIndexInSession: -
PSB Handle : 65546
Created Time : 2012/02/14 09:52:03

-----
DS-TE Information
-----
Bandwidth Reserved Flag : Reserved
CT0 Bandwidth(Kbit/sec) : 400 CT1 Bandwidth(Kbit/sec): 0
CT2 Bandwidth(Kbit/sec) : 0 CT3 Bandwidth(Kbit/sec): 0
CT4 Bandwidth(Kbit/sec) : 0 CT5 Bandwidth(Kbit/sec): 0
CT6 Bandwidth(Kbit/sec) : 0 CT7 Bandwidth(Kbit/sec): 0
Setup-Priority : 4 Hold-Priority : 3

-----
FRR Information
-----
Primary LSP Info
TE Attribute Flag : 0x63 Protected Flag : 0x1
Bypass In Use : Not Used
Bypass Tunnel Id : 67141670
BypassTunnel : Tunnel Index[Tunnel0/0/2048], InnerLabel[3]
Bypass Lsp ID : - FrrNextHop : 10.1.1.1
ReferAutoBypassHandle : 2049
FrrPrevTunnelTableIndex : - FrrNextTunnelTableIndex: -
Bypass Attribute(Not configured)
Setup Priority : 5 Hold Priority : 4
HopLimit : - Bandwidth : -
IncludeAnyGroup : - ExcludeAnyGroup : -
IncludeAllGroup : -
Bypass Unbound Bandwidth Info(Kbit/sec)
CT0 Unbound Bandwidth : - CT1 Unbound Bandwidth: -
CT2 Unbound Bandwidth : - CT3 Unbound Bandwidth: -
CT4 Unbound Bandwidth : - CT5 Unbound Bandwidth: -
CT6 Unbound Bandwidth : - CT7 Unbound Bandwidth: -

-----
BFD Information
-----
```

```

NextSessionTunnelIndex : -          PrevSessionTunnelIndex: -
NextLspId                : -          PrevLspId                : -
    
```

可以看到主隧道和一条自动旁路隧道 Tunnel0/0/2048 绑定。

用命令 **display mpls te tunnel name Tunnel0/0/2048 verbose** 可以看到自动旁路隧道的详细信息。它的带宽和创建、保持优先级和主隧道的 **bypass-attribute** 配置项一致。

```

[LSRA] display mpls te tunnel name Tunnel0/0/2048 verbose
No : 1
Tunnel-Name : Tunnel0/0/2048
Tunnel Interface Name : Tunnel0/0/0
TunnelIndex : 3          LSP Index : 2051
Session ID : 1026       LSP ID : 1
Lsr Role : Ingress     Lsp Type : Primary
Ingress LSR ID : 1.1.1.1
Egress LSR ID : 3.3.3.3
In-Interface : -
Out-Interface : GE1/0/0
Sign-Protocol : RSVP TE  Resv Style : SE
IncludeAnyAff : 0x0      ExcludeAnyAff : 0x0
IncludeAllAff : 0x0
LspConstraint : -
ER-Hop Table Index : -          AR-Hop Table Index: 3
C-Hop Table Index : 3
PrevTunnelIndexInSession: -    NextTunnelIndexInSession: -
PSB Handle : 1027
Created Time : 2010/07/01 13:35:53 UTC-08:00
-----
DS-TE Information
-----
Bandwidth Reserved Flag : Reserved
CT0 Bandwidth(Kbit/sec) : 200    CT1 Bandwidth(Kbit/sec): 0
CT2 Bandwidth(Kbit/sec) : 0      CT3 Bandwidth(Kbit/sec): 0
CT4 Bandwidth(Kbit/sec) : 0      CT5 Bandwidth(Kbit/sec): 0
CT6 Bandwidth(Kbit/sec) : 0      CT7 Bandwidth(Kbit/sec): 0
Setup-Priority : 5              Hold-Priority : 4
-----
FRR Information
-----
Primary LSP Info
TE Attribute Flag : 0x2          Protected Flag : 0x0
Bypass In Use : Not Exists
Bypass Tunnel Id : -
BypassTunnel : -
Bypass Lsp ID : -              FrrNextHop : -
ReferAutoBypassHandle : -
FrrPrevTunnelTableIndex : -     FrrNextTunnelTableIndex: -
Bypass Attribute(Not configured)
Setup Priority : -              Hold Priority : -
HopLimit : -                   Bandwidth : -
IncludeAnyGroup : -            ExcludeAnyGroup : -
IncludeAllGroup : -
Bypass Unbound Bandwidth Info(Kbit/sec)
CT0 Unbound Bandwidth : -       CT1 Unbound Bandwidth: -
CT2 Unbound Bandwidth : -       CT3 Unbound Bandwidth: -
CT4 Unbound Bandwidth : -       CT5 Unbound Bandwidth: -
CT6 Unbound Bandwidth : -       CT7 Unbound Bandwidth: -
-----
BFD Information
-----
NextSessionTunnelIndex : -          PrevSessionTunnelIndex: -
NextLspId                : -          PrevLspId                : -
    
```

可以看到自动旁路隧道保护主隧道的出接口 GigabitEthernet2/0/0，排除了主隧道路径上的三个地址提供节点保护，并且带宽是 200kbps，建立优先级和保持优先级分别是 5 和 4。

在 LSRA 上用命令 **display mpls te tunnel path** 可以看到主隧道和自动旁路隧道的路径信息，在主隧道的出接口这一跳上显示主隧道受节点保护和带宽保护。

```
[LSRA] display mpls te tunnel path
Tunnel Interface Name : Tunnel0/0/0
Lsp ID : 1.1.1.1 :200:1
Hop Information
Hop 0  2.1.1.1 Local-Protection available | bandwidth | node
Hop 1  2.1.1.2 Label 106497
Hop 2  2.2.2.2
Hop 3  3.1.1.1 Local-Protection available | bandwidth
Hop 4  3.1.1.2 Label 3
Hop 5  3.3.3.3
Tunnel Interface Name : Tunnel0/0/2048
Lsp ID : 2.2.2.2 :2049 :2
Hop Information
Hop 0  2.2.2.2
Hop 1  3.2.1.1
Hop 2  3.2.1.2
Hop 3  4.4.4.4
Hop 4  4.1.1.1
Hop 5  4.1.1.2
Hop 6  3.3.3.3
Tunnel Interface Name : Tunnel0/0/2048
Lsp ID : 1.1.1.1 :2049:3
Hop Information
Hop 0  10.1.1.2
Hop 1  10.1.1.1
Hop 2  3.3.3.3
```

----结束

配置文件

- LSRA 的配置文件

```
#
sysname LSRA
#
mpls lsr-id 1.1.1.1
mpls
mpls te
mpls te auto-frr
mpls rsvp-te
mpls te cspf
#
explicit-path master
next hop 2.1.1.2
next hop 3.1.1.2
#
interface GigabitEthernet1/0/0
ip address 10.1.1.2 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 10000
mpls te bandwidth bc0 10000 bc1 3000
mpls rsvp-te
#
interface GigabitEthernet2/0/0
ip address 2.1.1.1 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 10000
mpls te bandwidth bc0 10000 bc1 3000
mpls rsvp-te
#
interface LoopBack1
ip address 1.1.1.1 255.255.255.255
#
```

```
interface Tunnel0/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te tunnel-id 200
 mpls te record-route label
 mpls te bandwidth ct0 400
 mpls te path explicit-path master
 mpls te priority 4 3
 mpls te fast-reroute bandwidth
 mpls te bypass-attributes bandwidth 200 priority 5 4
 mpls te commit
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
 network 2.1.1.0 0.0.0.255
 network 1.1.1.1 0.0.0.0
 mpls-te enable
#
return
```

- LSRB 的配置文件

```
#
 sysname LSRB
#
 mpls lsr-id 2.2.2.2
 mpls
 mpls te
 mpls te auto-frr
 mpls rsvp-te
 mpls te cspf
#
interface GigabitEthernet1/0/0
 ip address 3.2.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000
 mpls te bandwidth bc0 10000 bc1 3000
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 ip address 3.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000
 mpls te bandwidth bc0 10000 bc1 3000
 mpls rsvp-te
#
interface GigabitEthernet0/0/1
 ip address 2.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
 network 3.1.1.0 0.0.0.255
 network 3.2.1.0 0.0.0.255
 network 2.1.1.0 0.0.0.255
 network 2.2.2.2 0.0.0.0
 mpls-te enable
#
return
```

- LSRC 的配置文件

```
#
sysname LSRC
#
mpls lsr-id 3.3.3.3
mpls
mpls te
mpls rsvp-te
#
interface GigabitEthernet1/0/0
ip address 10.1.1.1 255.255.255.0
mpls
mpls te
mpls rsvp-te
#
interface GigabitEthernet2/0/0
ip address 4.1.1.2 255.255.255.0
mpls
mpls te
mpls rsvp-te
#
interface GigabitEthernet0/0/1
ip address 3.1.1.2 255.255.255.0
mpls
mpls te
mpls rsvp-te
#
interface LoopBack1
ip address 3.3.3.3 255.255.255.255
#
ospf 1
opaque-capability enable
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 3.1.1.0 0.0.0.255
network 4.1.1.0 0.0.0.255
network 3.3.3.3 0.0.0.0
mpls-te enable
#
return
```

- LSRD 的配置文件

```
#
sysname LSRD
#
mpls lsr-id 4.4.4.4
mpls
mpls te
mpls rsvp-te
#
interface GigabitEthernet1/0/0
ip address 3.2.1.2 255.255.255.0
mpls
mpls te
mpls rsvp-te
#
interface GigabitEthernet2/0/0
ip address 4.1.1.1 255.255.255.0
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 10000
mpls te bandwidth bc0 10000 bc1 3000
mpls rsvp-te
#
interface LoopBack1
ip address 4.4.4.4 255.255.255.255
#
ospf 1
opaque-capability enable
```

```

area 0.0.0.0
 network 3.2.1.0 0.0.0.255
 network 4.1.1.0 0.0.0.255
 network 4.4.4.0 0.0.0.0
 mpls-te enable
#
Return
    
```

3.21.5 配置 CR-LSP 热备份示例

本例描述了配置 CR-LSP 热备份的过程，主要包括如何配置 CR-LSP 热备份（hot-standby）和逃生路径（best-effort）。

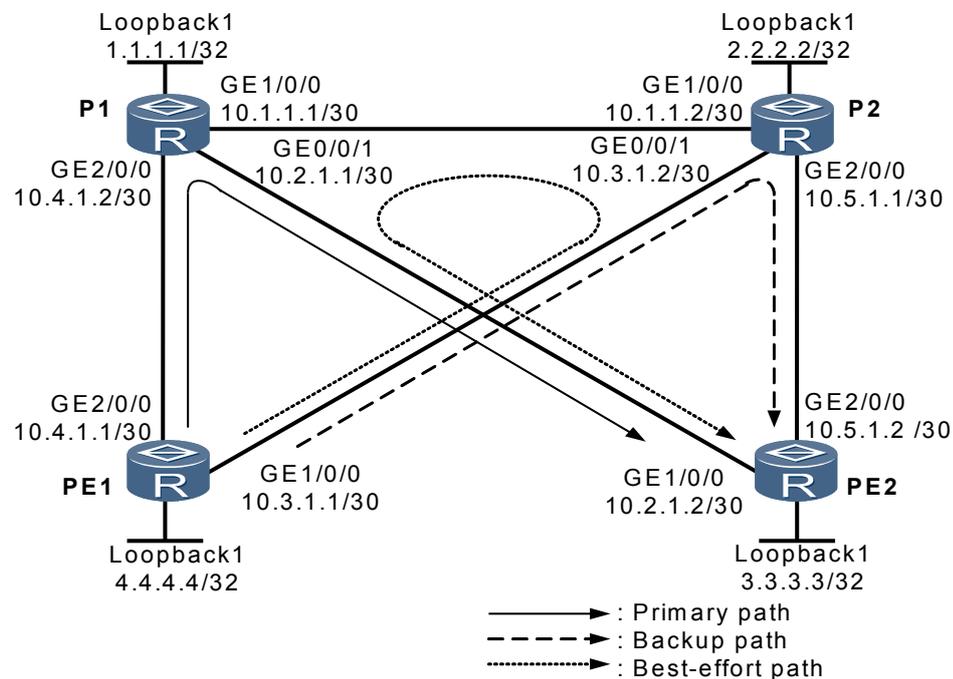
组网需求

图 3-6 为 MPLS VPN 网络。要求从 PE1 上建立一条 TE 隧道，目的地址为 PE2，并配置 CR-LSP 热备份（hot-standby）和逃生路径（best-effort）。其中，

- 主 CR-LSP 的路径为 PE1-->P1-->PE2；
- 备份 CR-LSP 的路径为 PE1-->P2-->PE2；
- 逃生路径为 PE1-->P2-->P1-->PE2。

当主 CR-LSP 故障时，流量切换到备份 CR-LSP；当主 CR-LSP 故障恢复，延时 15 秒后再进行流量回切。如果主、备 CR-LSP 都故障，触发建立逃生路径，使流量切换到逃生路径上。

图 3-6 CR-LSP 热备份组网示意图



配置思路

采用如下思路配置 CR-LSP 热备份：

1. 配置各接口 IP 地址和 IGP 使各节点互通。
2. 配置 MPLS 和 MPLS TE 基本能力。
3. 在 PE1 上配置主、备显式路径。
4. 在 PE1 上创建目的地址为 PE2 的隧道接口，指定显式路径，并使能热备份和逃生路径，配置回切时间为 15 秒。

数据准备

为完成此配置例，需准备如下的数据：

- IGP 协议类型及配置 IGP 所需数据
- MPLS LSR-ID
- 隧道接口编号、隧道占用的带宽
- 主 CR-LSP 的显式路径和备份 CR-LSP 的显式路径

操作步骤

步骤 1 配置各接口的 IP 地址

按照图 3-6 配置 IP 地址，并在节点上创建 Loopback 接口，配置 Loopback 接口的 IP 地址为 MPLS LSR-ID。具体配置内容请参见本例的配置文件。

步骤 2 配置 IGP

在各个节点上配置 OSPF 或 IS-IS，使各节点能互通。本例使用 IS-IS。具体配置内容请参见本例的配置文件。

步骤 3 配置 MPLS 基本能力

在各个节点的系统视图下配置 LSR-ID，使能 MPLS，并在物理接口下使能 MPLS。具体配置内容请参见本例的配置文件。

步骤 4 配置 MPLS TE 基本能力

在各个节点的 MPLS 视图和链路的接口视图下使能 MPLS-TE、MPLS RSVP-TE。配置链路最大可预留带宽为 100Mbps，BC0 带宽为 100Mbps，BC1 带宽为 50Mbps。具体配置内容请参见本例的配置文件。

步骤 5 配置 IS-IS TE，并配置 CSPF

在各个节点上配置 IS-IS TE，并在 PE1 上配置 CSPF。具体配置过程请参见[配置 RSVP-TE 隧道](#)。

步骤 6 配置主、备 CR-LSP 使用的显式路径

在 PE1 上配置主 CR-LSP 使用的显式路径。

```
<PE1> system-view
[PE1] explicit-path main
[PE1-explicit-path-main] next hop 10.4.1.2
[PE1-explicit-path-main] next hop 10.2.1.2
[PE1-explicit-path-main] next hop 3.3.3.3
[PE1-explicit-path-main] quit
```

在 PE1 上配置备份 CR-LSP 使用的显式路径。

```
[PE1] explicit-path backup
[PE1-explicit-path-backup] next hop 10.3.1.2
```

```
[PE1-explicit-path-backup] next hop 10.5.1.2
[PE1-explicit-path-backup] next hop 3.3.3.3
[PE1-explicit-path-backup] quit
```

完成此步骤后，可在 PE1 上执行命令查看显式路径是否配置正确。

```
[PE1] display explicit-path main
Path Name : main          Path Status : Enabled
 1      10.4.1.2          Strict      Include
 2      10.2.1.2          Strict      Include
 3      3.3.3.3           Strict      Include
[PE1] display explicit-path backup
Path Name : backup       Path Status : Enabled
 1      10.3.1.2          Strict      Include
 2      10.5.1.2          Strict      Include
 3      3.3.3.3           Strict      Include
```

步骤 7 配置隧道接口

在 PE1 上创建 Tunnel 接口，指定显式路径，配置隧道带宽为 10Mbps。

```
[PE1] interface tunnel 0/0/0
[PE1-Tunnel0/0/0] ip address unnumbered interface loopback 1
[PE1-Tunnel0/0/0] tunnel-protocol mpls te
[PE1-Tunnel0/0/0] destination 3.3.3.3
[PE1-Tunnel0/0/0] mpls te tunnel-id 100
[PE1-Tunnel0/0/0] mpls te path explicit-path main
[PE1-Tunnel0/0/0] mpls te bandwidth ct0 10000
```

在该 Tunnel 接口配置热备份，回切时间为 15 秒，指定备份显式路径，并配置逃生路径。

```
[PE1-Tunnel0/0/0] mpls te backup hot-standby wtr 15
[PE1-Tunnel0/0/0] mpls te path explicit-path backup secondary
[PE1-Tunnel0/0/0] mpls te backup ordinary best-effort
[PE1-Tunnel0/0/0] mpls te commit
[PE1-Tunnel0/0/0] quit
```

完成步骤后，在 PE1 上执行 **display mpls te tunnel-interface tunnel 0/0/0** 命令，可发现主 CR-LSP、备份 CR-LSP 建立成功。

```
[PE1] display mpls te tunnel-interface tunnel 0/0/0
-----
Tunnel0/0/0
-----
Tunnel State Desc : UP
Active LSP        : Primary LSP
Session ID       : 100
Ingress LSR ID   : 4.4.4.4          Egress LSR ID: 3.3.3.3
Admin State      : UP              Oper State   : UP
Primary LSP State : UP
Main LSP State   : READY          LSP ID     : 1
Hot-Standby LSP State : UP
Main LSP State   : READY          LSP ID     : 32770
```

可使用 **display mpls te hot-standby state interface tunnel 0/0/0** 命令查看热备份信息。

```
[PE1] display mpls te hot-standby state interface tunnel 0/0/0
-----
Verbose information about the Tunnel0/0/0 hot-standby state
-----
session id          : 100
main LSP token      : 0x100201a
hot-standby LSP token : 0x100201b
HSB switch result   : Primary LSP
WTR remain time     : 15s
using same path     : no
```

可使用 **ping lsp te** 命令检测热备份 CR-LSP 连通性。

```
[PE1] ping lsp te tunnel 0/0/0 hot-standby
LSP PING FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel0/0/0 : 100 data bytes, press CTRL_C to break
  Reply from 3.3.3.3: bytes=100 Sequence=1 time = 380 ms
  Reply from 3.3.3.3: bytes=100 Sequence=2 time = 130 ms
  Reply from 3.3.3.3: bytes=100 Sequence=3 time = 70 ms
  Reply from 3.3.3.3: bytes=100 Sequence=4 time = 120 ms
  Reply from 3.3.3.3: bytes=100 Sequence=5 time = 120 ms

--- FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel0/0/0 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 70/164/380 ms
```

可使用 **tracert lsp te** 命令检测热备份 CR-LSP 所经过的路径。

```
[PE1] tracert lsp te tunnel 0/0/0 hot-standby
LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel0/0/0 , press CTRL_C to break.
TTL  Replier          Time   Type      Downstream
0
1    10.3.1.2          90 ms Transit  10.3.1.2/[13313 ]
2    3.3.3.3           130 ms Egress   10.5.1.2/[3 ]
```

步骤 8 检查配置结果

将同一台测试仪的两个接口（Port1 和 Port2）分别接入 PE1 和 PE2，从 Port1 向 Port2 打 MPLS 流（注意标签值的设置）。可发现当拔出 PE1 或 P1 上的 GE2/0/0 接口的线缆时，故障收敛时间为毫秒级。在 PE1 上执行 **display mpls te hot-standby state interface tunnel 0/0/0** 命令，可发现流量被切换到备份 CR-LSP 上。

```
[PE1] display mpls te hot-standby state interface tunnel 0/0/0
```

```
-----
Verbose information about the Tunnel0/0/0 hot-standby state
-----
```

```
session id                : 100
main LSP token             : 0x0
hot-standby LSP token     : 0x100201b
HSB switch result         : Hot-standby LSP
WTR remain time           : 15s
using same path            : no
```

插上刚才拔出的线缆后，等 15 秒后，可发现流量被切换到主 CR-LSP 上。

如果拔出 PE1 或 P1 上的 GE2/0/0 接口后再拔出 PE2 或 P2 上的 GE2/0/0 接口的线缆时，隧道接口变为 Down 后又会变为 Up，逃生路径建立成功，流量被切换到逃生路径上。

```
[PE1] display mpls te tunnel-interface tunnel 0/0/0
```

```
-----
Tunnel0/0/0
-----
Tunnel State Desc      : UP
Active LSP              : Best-Effort LSP
Session ID              : 100
Ingress LSR ID         : 4.4.4.4          Egress LSR ID: 3.3.3.3
Admin State             : UP                Oper State   : UP
Primary LSP State      : DOWN
  Main LSP State        : SETTING UP
Hot-Standby LSP State  : DOWN
  Main LSP State        : SETTING UP
Best-Effort LSP State  : UP
  Main LSP State        : READY             LSP ID      : 32773
[PE1] display mpls te tunnel path
Tunnel Interface Name : Tunnel0/0/0
Lsp ID : 4.4.4.4 :100 :32776
Hop Information
Hop 0  10.3.1.1
Hop 1  10.3.1.2
Hop 2  2.2.2.2
Hop 3  10.1.1.2
```

```
Hop 4 10.1.1.1
Hop 5 1.1.1.1
Hop 6 10.2.1.1
Hop 7 10.2.1.2
Hop 8 3.3.3.3
```

---结束

配置文件

- PE1 的配置文件

```
#
sysname PE1
#
mpls lsr-id 4.4.4.4
mpls
mpls te
mpls rsvp-te
mpls te cspf
#
explicit-path backup
next hop 10.3.1.2
next hop 10.5.1.2
next hop 3.3.3.3
#
explicit-path main
next hop 10.4.1.2
next hop 10.2.1.2
next hop 3.3.3.3
#
isis 1
cost-style wide
network-entity 10.0000.0000.0004.00
traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
ip address 10.3.1.1 255.255.255.252
isis enable 1
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000 bc1 50000
mpls rsvp-te
#
interface GigabitEthernet2/0/0
ip address 10.4.1.1 255.255.255.252
isis enable 1
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000 bc1 50000
mpls rsvp-te
#
interface LoopBack1
ip address 4.4.4.4 255.255.255.255
isis enable 1
#
interface Tunnel0/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 3.3.3.3
mpls te tunnel-id 100
mpls te record-route
mpls te bandwidth ct0 10000
mpls te path explicit-path main
mpls te path explicit-path backup secondary
mpls te backup hot-standby wtr 15
mpls te backup ordinary best-effort
```

```
        mpls te commit
    #
    return
● P1 的配置文件
#
sysname P1
#
mpls lsr-id 1.1.1.1
mpls
    mpls te
    mpls rsvp-te
#
isis 1
    cost-style wide
    network-entity 10.0000.0000.0001.00
    traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
    ip address 10.1.1.1 255.255.255.252
    isis enable 1
    mpls
    mpls te
    mpls rsvp-te
#
interface GigabitEthernet2/0/0
    ip address 10.4.1.2 255.255.255.252
    isis enable 1
    mpls
    mpls te
    mpls rsvp-te
#
interface GigabitEthernet0/0/1
    ip address 10.2.1.1 255.255.255.252
    isis enable 1
    mpls
    mpls te
    mpls te bandwidth max-reservable-bandwidth 100000
    mpls te bandwidth bc0 100000 bc1 50000
    mpls rsvp-te
#
interface LoopBack1
    ip address 1.1.1.1 255.255.255.255
    isis enable 1
#
return
● P2 的配置文件
#
sysname P2
#
mpls lsr-id 2.2.2.2
mpls
    mpls te
    mpls rsvp-te
#
isis 1
    cost-style wide
    network-entity 10.0000.0000.0002.00
    traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
    ip address 10.1.1.2 255.255.255.252
    isis enable 1
    mpls
    mpls te
    mpls te bandwidth max-reservable-bandwidth 100000
    mpls te bandwidth bc0 100000 bc1 50000
    mpls rsvp-te
#
```

```
interface GigabitEthernet2/0/0
 ip address 10.5.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000 bc1 50000
 mpls rsvp-te
#
interface GigabitEthernet0/0/1
 ip address 10.3.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
#
return
```

- PE2 的配置文件

```
#
 sysname PE2
#
 mpls lsr-id 3.3.3.3
 mpls
 mpls te
 mpls rsvp-te
#
 isis 1
 cost-style wide
 network-entity 10.0000.0000.0003.00
 traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
 ip address 10.2.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 ip address 10.5.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 isis enable 1
#
return
```

3.21.6 配置静态 BFD for CR-LSP 示例

本例描述了通过配置静态 BFD for CR-LSP 实现一条隧道上使能热备份且配置有逃生路径。

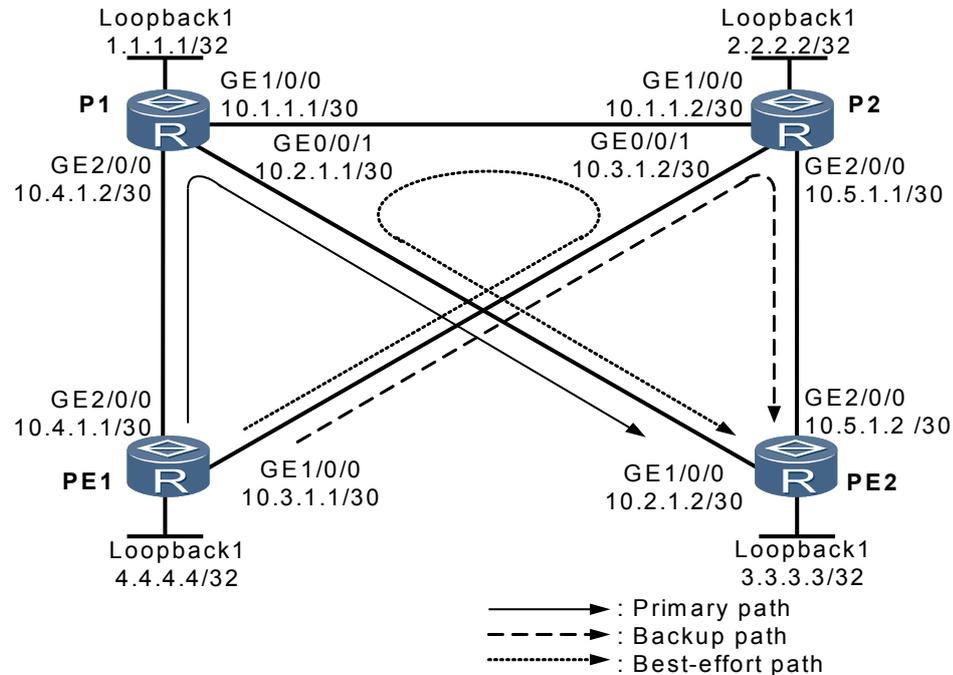
组网需求

图 3-7 为 CR-LSP 热备份组网图。PE1 上建立了一条 TE 隧道，目的地址为 PE2。该隧道使能了热备份且配置了逃生路径。当主 CR-LSP 故障时，流量切换到备份 CR-LSP；当主 CR-LSP 故障恢复，延时 15 秒后再进行流量回切。如果主、备 CR-LSP 都故障，触发建立逃生路径，使流量切换到逃生路径上。

现要求配置两个静态 BFD 会话，分别检测主、备 CR-LSP，使得：

- 主 CR-LSP 故障时，将流量快速切换到备份 CR-LSP；
- 在主 CR-LSP 恢复后的延时回切时间（15 秒）内，如果备份 CR-LSP 故障，可快速感知故障并将流量回切到主 CR-LSP。

图 3-7 CR-LSP 热备份组网示意图



配置思路

采用如下思路配置静态 BFD for CR-LSP：

1. 按照[配置 CR-LSP 热备份示例](#)配置 CR-LSP 热备份。
2. 在 PE1 上建立两个 BFD 会话，绑定 CR-LSP，分别检测主 CR-LSP 和备份 CR-LSP；PE2 上配置两个 BFD 会话，绑定 IP（PE2-->PE1 路由可达即可）。

数据准备

为完成此配置例，需准备如下的数据：

- BFD 配置名、本地标识符和远端标识符
- BFD 报文最大接收时间间隔和最大发送时间间隔
- BFD 本地检测倍数
- 需要准备的其他数据请参见[配置 CR-LSP 热备份示例](#)

操作步骤

步骤 1 配置 CR-LSP 热备份

按照配置 CR-LSP 热备份示例配置主、备 CR-LSP 和逃生路径。

步骤 2 配置 BFD for CR-LSP

在 PE1 和 PE2 之间建立 BFD 会话检测主、备 CR-LSP 故障。PE1 上的 BFD 会话绑定 CR-LSP，PE2 上的 BFD 会话绑定 IP。指定发送 BFD 报文的最小时间间隔和允许接收 BFD 报文的最小时间间隔为 100 毫秒，BFD 本地检测倍数为 3。

配置 PE1。

```
[PE1] bfd
[PE1-bfd] quit
[PE1] bfd mainsptope2 bind mpls-te interface tunnel0/0/0 te-lsp
[PE1-bfd-lsp-session-mainlsptope2] discriminator local 413
[PE1-bfd-lsp-session-mainlsptope2] discriminator remote 314
[PE1-bfd-lsp-session-mainlsptope2] min-tx-interval 100
[PE1-bfd-lsp-session-mainlsptope2] min-rx-interval 100
[PE1-bfd-lsp-session-mainlsptope2] detect-multiplier 3
[PE1-bfd-lsp-session-mainlsptope2] process-pst
[PE1-bfd-lsp-session-mainlsptope2] commit
[PE1-bfd-lsp-session-mainlsptope2] quit
[PE1] bfd backuplsptope2 bind mpls-te interface tunnel0/0/0 te-lsp backup
[PE1-bfd-lsp-session-backuplsptope2] discriminator local 423
[PE1-bfd-lsp-session-backuplsptope2] discriminator remote 324
[PE1-bfd-lsp-session-backuplsptope2] min-tx-interval 100
[PE1-bfd-lsp-session-backuplsptope2] min-rx-interval 100
[PE1-bfd-lsp-session-backuplsptope2] detect-multiplier 3
[PE1-bfd-lsp-session-backuplsptope2] process-pst
[PE1-bfd-lsp-session-backuplsptope2] commit
[PE1-bfd-lsp-session-backuplsptope2] quit
```

配置 PE2。

```
[PE2] bfd
[PE2-bfd] quit
[PE2] bfd mainsptope2 bind peer-ip 4.4.4.4
[PE2-bfd-lsp-session-mainlsptope2] discriminator local 314
[PE2-bfd-lsp-session-mainlsptope2] discriminator remote 413
[PE2-bfd-lsp-session-mainlsptope2] min-tx-interval 100
[PE2-bfd-lsp-session-mainlsptope2] min-rx-interval 100
[PE2-bfd-lsp-session-mainlsptope2] detect-multiplier 3
[PE2-bfd-lsp-session-mainlsptope2] commit
[PE2-bfd-lsp-session-mainlsptope2] quit
[PE2] bfd backuplsptope2 bind peer-ip 4.4.4.4
[PE2-bfd-lsp-session-backuplsptope2] discriminator local 324
[PE2-bfd-lsp-session-backuplsptope2] discriminator remote 423
[PE2-bfd-lsp-session-backuplsptope2] min-tx-interval 100
[PE2-bfd-lsp-session-backuplsptope2] min-rx-interval 100
[PE2-bfd-lsp-session-backuplsptope2] detect-multiplier 3
[PE2-bfd-lsp-session-backuplsptope2] commit
[PE2-bfd-lsp-session-backuplsptope2] quit
```

完成此步骤后，在 PE1 和 PE2 上执行 **display bfd session discriminator local-discriminator-value**，可发现 BFD 会话状态为 Up。

以 PE1 的显示为例：

```
[PE1] display bfd session discriminator 413
-----
Local Remote PeerIpAddr State Type InterfaceName
-----
413 314 3.3.3.3 S_TE_LSP Up Tunnel0/0/0
-----

[PE1] display bfd session discriminator 423
-----
Local Remote PeerIpAddr State Type InterfaceName
-----
423 324 3.3.3.3 S_TE_LSP Up Tunnel0/0/0
-----
```

步骤 3 检查配置结果

将同一台测试仪的两个接口（Port1 和 Port2）分别接入 PE1 和 PE2，从 Port1 向 Port2 打 MPLS 流（注意标签值的设置）。可发现当拔出 PE1 或 P1 上的 GE2/0/0 接口的线缆时，故障收敛时间为毫秒级。

插入拔出的 GE2/0/0 接口的线缆并在 15 秒内拔出 PE1 的 GE1/0/0 接口线缆时，可发现故障收敛时间为毫秒级。

---结束

配置文件

● PE1 的配置文件

```
#
 sysname PE1
#
 bfd
#
 mpls lsr-id 4.4.4.4
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
 explicit-path backup
  next hop 10.3.1.2
  next hop 10.5.1.2
  next hop 3.3.3.3
#
 explicit-path main
  next hop 10.4.1.2
  next hop 10.2.1.2
  next hop 3.3.3.3
#
 isis 1
  cost-style wide
  network-entity 10.0000.0000.0004.00
  traffic-eng level-1-2
#
 interface GigabitEthernet1/0/0
  ip address 10.3.1.1 255.255.255.252
  isis enable 1
  mpls
  mpls te
  mpls te bandwidth max-reservable-bandwidth 100000
  mpls te bandwidth bc0 100000
  mpls rsvp-te
#
 interface GigabitEthernet2/0/0
  ip address 10.4.1.1 255.255.255.252
  isis enable 1
  mpls
  mpls te
  mpls te bandwidth max-reservable-bandwidth 100000
  mpls te bandwidth bc0 100000
  mpls rsvp-te
#
 interface LoopBack1
  ip address 4.4.4.4 255.255.255.255
  isis enable 1
#
 interface Tunnel0/0/0
  ip address unnumbered interface LoopBack1
  tunnel-protocol mpls te
```

```

destination 3.3.3.3
mpls te tunnel-id 100
mpls te record-route
mpls te bandwidth ct0 10000
mpls te path explicit-path main
mpls te path explicit-path backup secondary
mpls te backup hot-standby wtr 15
mpls te backup ordinary best-effort
mpls te commit
#
bfd backuplsptope2 bind mpls-te interface Tunnel0/0/0 te-lsp backup
discriminator local 423
discriminator remote 324
min-tx-interval 100
min-rx-interval 100
process-pst
commit
#
bfd mainsptope2 bind mpls-te interface Tunnel0/0/0 te-lsp
discriminator local 413
discriminator remote 314
min-tx-interval 100
min-rx-interval 100
process-pst
commit
#
return

```

● P1 的配置文件

```

#
sysname P1
#
mpls lsr-id 1.1.1.1
mpls
mpls te
mpls rsvp-te
#
isis 1
cost-style wide
network-entity 10.0000.0000.0001.00
traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
ip address 10.1.1.1 255.255.255.252
isis enable 1
mpls
mpls te
mpls rsvp-te
#
interface GigabitEthernet2/0/0
ip address 10.4.1.2 255.255.255.252
isis enable 1
mpls
mpls te
mpls rsvp-te
#
interface GigabitEthernet0/0/1
ip address 10.2.1.1 255.255.255.252
isis enable 1
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
mpls rsvp-te
#
interface LoopBack1
ip address 1.1.1.1 255.255.255.255
isis enable 1
#

```

- ```
return
```
- P2 的配置文件

```
#
sysname P2
#
mpls lsr-id 2.2.2.2
mpls
mpls te
mpls rsvp-te
#
isis 1
cost-style wide
network-entity 10.0000.0000.0002.00
traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
ip address 10.1.1.2 255.255.255.252
isis enable 1
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
mpls rsvp-te
#
interface GigabitEthernet2/0/0
ip address 10.5.1.1 255.255.255.252
isis enable 1
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 100000
mpls te bandwidth bc0 100000
mpls rsvp-te
#
interface GigabitEthernet0/0/1
ip address 10.3.1.2 255.255.255.252
isis enable 1
mpls
mpls te
mpls rsvp-te
#
interface LoopBack1
ip address 2.2.2.2 255.255.255.255
isis enable 1
#
return
```
  - PE2 的配置文件

```
#
sysname PE2
#
bfd
#
mpls lsr-id 3.3.3.3
mpls
mpls te
mpls rsvp-te
#
isis 1
cost-style wide
network-entity 10.0000.0000.0003.00
traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
ip address 10.2.1.2 255.255.255.252
isis enable 1
mpls
mpls te
mpls rsvp-te
#
```

```
interface GigabitEthernet2/0/0
 ip address 10.5.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 isis enable 1
#
bfd backuplsptope2 bind peer-ip 4.4.4.4
 discriminator local 324
 discriminator remote 423
 min-tx-interval 100
 min-rx-interval 100
 commit
#
bfd mainlsptope2 bind peer-ip 4.4.4.4
 discriminator local 314
 discriminator remote 413
 min-tx-interval 100
 min-rx-interval 100
 commit
#
return
```

### 3.21.7 配置动态 BFD for CR-LSP 示例

本例描述了通过配置动态 BFD for CR-LSP 实现一条隧道上使能热备份且配置有逃生路径。

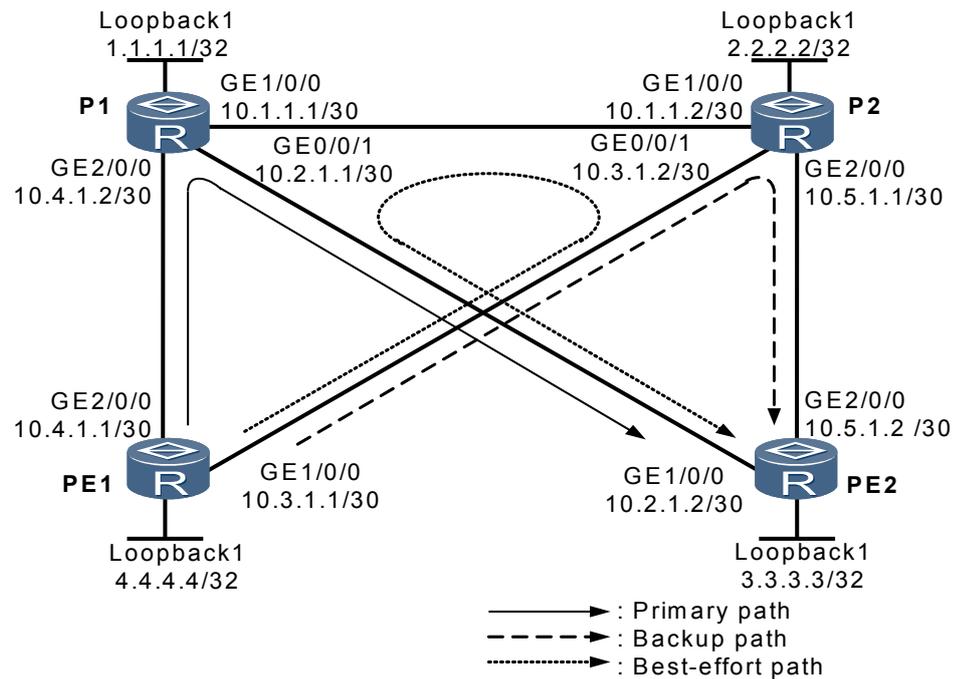
#### 组网需求

图 3-8 为 CR-LSP 热备份组网图。PE1 上建立了一条 TE 隧道，目的地址为 PE2。该隧道使能了热备份且配置了逃生路径。当主 CR-LSP 故障时，流量切换到备份 CR-LSP；当主 CR-LSP 故障恢复，延时 15 秒后再进行流量回切。如果主、备 CR-LSP 都故障，触发建立逃生路径，使流量切换到逃生路径上。

现要求配置动态 BFD for CR-LSP 检测主、备 CR-LSP，使得：

- 主 CR-LSP 故障时，流量快速切换到备份 CR-LSP；
- 在主 CR-LSP 恢复后的延时回切时间（15 秒）内，如果备份 CR-LSP 故障，可快速感知故障并将流量回切到主 CR-LSP。

图 3-8 CR-LSP 热备份组网示意图



说明

相对静态 BFD 而言，动态 BFD 配置简单，且使用动态 BFD 可减少 BFD 会话数目，即可以减少网络上的 BFD 报文数，节约网络资源。因为使用动态 BFD 检测，同一时间内一个 Tunnel 接口只建立了一个 BFD 会话。

## 配置思路

采用如下思路配置动态 BFD for CR-LSP:

1. 按照[配置 CR-LSP 热备份示例](#)配置 CR-LSP 热备份。
2. 在隧道 Ingress 端使能 BFD，配置 MPLS TE BFD，并指定本地发送 BFD 报文的最小时间间隔和允许接收 BFD 报文的最小时间间隔，以及 BFD 本地检测倍数。
3. 在 Egress 端使能被动创建 BFD 会话。

## 数据准备

为完成此配置例，需准备如下的数据：

- Ingress 端发送 BFD 报文的最小时间间隔和允许接收的最小时间间隔（缺省值取决于许可证文件）
- Ingress 端的 BFD 本地检测倍数（缺省值取决于许可证文件）
- 其他需准备的数据请参见[配置 CR-LSP 热备份示例](#)

## 操作步骤

### 步骤 1 配置 CR-LSP 热备份

按照[配置 CR-LSP 热备份示例](#)配置主、备 CR-LSP 和逃生路径。

**步骤 2** 在隧道 Ingress 端使能 BFD 并配置 MPLS TE BFD

# 在 PE1 上的 Tunnel 接口下使能 MPLS TE BFD，并指定本地发送 BFD 报文的最小时间间隔和允许接收的最小时间间隔都为 100 毫秒，BFD 本地检测倍数为 3。

```
<PE1> system-view
[PE1] bfd
[PE1-bfd] quit
[PE1] interface tunnel 0/0/0
[PE1-Tunnel0/0/0] mpls te bfd enable
[PE1-Tunenl0/0/0] mpls te bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 3
[PE1-Tunenl0/0/0] mpls te commit
```

**步骤 3** 在隧道 Egress 端使能被动创建 BFD 会话

```
<PE2> system-view
[PE2] bfd
[PE2-bfd] mpls-passive
[PE2-bfd] quit
```

# 完成此步骤后，在 PE1 和 PE2 上执行 **display bfd session discriminator local-discriminator-value**，可发现 BFD 会话状态为 Up。

```
[PE1] display bfd session mpls-te interface Tunnel 0/0/0 te-lsp
```

| Local | Remote | PeerIpAddr | State    | Type | InterfaceName |
|-------|--------|------------|----------|------|---------------|
| 8208  | 8217   | 3.3.3.3    | D_TE_LSP | Up   | Tunnel0/0/0   |

Total UP/DOWN Session Number : 1/0

**步骤 4** 检查配置结果

将同一台测试仪的两个接口（Port1 和 Port2）分别接入 PE1 和 PE2，从 Port1 向 Port2 打 MPLS 流（注意标签值的设置）。可发现当拔出 PE1 或 P1 上的 GE2/0/0 接口的线缆时，故障收敛时间为毫秒级。

插入拔出的 GE2/0/0 接口的线缆并在 15 秒内拔出 PE1 的 GE1/0/0 接口线缆时，可发现故障收敛时间为毫秒级。

----结束

## 配置文件

## ● PE1 的配置文件

```
#
 sysname PE1
#
 bfd
#
 mpls lsr-id 4.4.4.4
 mpls
 mpls te
 mpls rsvp-te
 mpls te cspf
#
 explicit-path backup
 next hop 10.3.1.2
 next hop 10.5.1.2
 next hop 3.3.3.3
#
 explicit-path main
 next hop 10.4.1.2
 next hop 10.2.1.2
 next hop 3.3.3.3
#
```

```

isis 1
 cost-style wide
 network-entity 10.0000.0000.0004.00
 traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
 ip address 10.3.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 ip address 10.4.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 isis enable 1
#
interface Tunnel0/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te tunnel-id 100
 mpls te bfd enable
 mpls te record-route
 mpls te bandwidth ct0 10000
 mpls te path explicit-path main
 mpls te path explicit-path backup secondary
 mpls te backup hot-standby wtr 15
 mpls te backup ordinary best-effort
 mpls te commit
#
return

```

● P1 的配置文件

```

#
 sysname P1
#
 mpls lsr-id 1.1.1.1
 mpls
 mpls te
 mpls rsvp-te
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0001.00
 traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 ip address 10.4.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te

```

```
#
interface GigabitEthernet0/0/1
 ip address 10.2.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
#
return
```

● P2 的配置文件

```
#
sysname P2
#
mpls lsr-id 2.2.2.2
mpls
 mpls te
 mpls rsvp-te
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0002.00
 traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 ip address 10.5.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
#
interface GigabitEthernet0/0/1
 ip address 10.3.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
#
return
```

● PE2 的配置文件

```
#
sysname PE2
#
bfd
 mpls-passive
#
mpls lsr-id 3.3.3.3
mpls
```

```
mpls te
mpls rsvp-te
#
isis 1
cost-style wide
network-entity 10.0000.0000.0003.00
traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
ip address 10.2.1.2 255.255.255.252
isis enable 1
mpls
mpls te
mpls rsvp-te
#
interface GigabitEthernet2/0/0
ip address 10.5.1.2 255.255.255.252
isis enable 1
mpls
mpls te
mpls rsvp-te
#
interface LoopBack1
ip address 3.3.3.3 255.255.255.255
isis enable 1
#
return
```