H3C MSR 系列路由器

MPLS 配置指导(V7)

杭州华三通信技术有限公司
http://www.h3c.com.cn

资料版本：6W103-20140512
产品版本：MSR-CMW710-R0105

Copyright © 2013-2014 杭州华三通信技术有限公司及其许可者版权所有，保留一切权利。

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

H3C、 、H3CS、H3CIE、H3CNE、Aolynk、 、H^{3}Care、 、IRF、NetPilot、Netflow、SecEngine、SecPath、SecCenter、SecBlade、Comware、ITCMM、HUASAN、华三均为杭州华三通信技术有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。H3C 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，H3C 尽全力在本手册中提供准确的信息，但是 H3C 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前 言

H3C MSR 系列路由器 配置指导(V7)共分为十五本手册，介绍了 MSR 系列路由器各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。《《MPLS 配置指导》主要介绍 MPLS 相关协议的原理和配置，包括 MPLS TE、MPLS L3VPN 和 MPLS L2VPN 等。

前言部分包含如下内容：

- 适用款型
- 读者对象
- 本书约定
- 产品配套资料
- 资料获取方式
- 技术支持
- 资料意见反馈

适用款型

本手册所描述的内容适用于 MSR 系列路由器中的如下款型：

款型	
MSR 2600	MSR 26-30
MSR 3600	MSR 36-10
	MSR 36-20
	MSR 36-40
	MSR 36-60
	MSR3600-28
	MSR3600-51
MSR 5600	MSR 56-60
	MSR 56-80

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
说明	对操作内容的描述进行必要的补充和说明。
窍门	配置、操作、或使用设备的技巧、小窍门。

3. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。

4. 端口编号示例约定

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

产品配套资料

H3C MSR 系列路由器的配套资料包括如下部分：

大类	资料名称	内容介绍
产品知识介绍	路由器产品彩页	帮助您了解产品的主要规格参数及亮点
硬件描述与安装	路由器安装指导	帮助您详细了解设备硬件规格和安装方法，指导您对设备进行安装
	MSR 系列路由器接口模块手册	帮助您详细了解单板的硬件规格
业务配置	MSR 系列路由器配置指导(V7)	帮助您掌握设备软件功能的配置方法及配置步骤
	MSR 系列路由器命令参考(V7)	详细介绍设备的命令，相当于命令字典，方便您查阅各个命令的功能
运行维护	路由器版本说明书	帮助您了解产品版本的相关信息（包括：版本配套说明、兼容性说明、特性变更说明、技术支持信息）及软件升级方法

资料获取方式

您可以通过H3C网站（www.h3c.com.cn）获取最新的产品资料：

H3C 网站与产品资料相关的主要栏目介绍如下：

- [服务支持/文档中心]：可以获取硬件安装类、软件升级类、配置类或维护类等产品资料。
- [产品技术]：可以获取产品介绍和技术介绍的文档，包括产品相关介绍、技术介绍、技术白皮书等。
- [解决方案]：可以获取解决方案类资料。
- [服务支持/软件下载]：可以获取与软件版本配套的资料。

技术支持

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

网址：http://www.h3c.com.cn

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 MPLS基础……1-1
1.1 MPLS简介……1-1
1.1.1 MPLS基本概念……1-1
1.1.2 MPLS网络结构……1-3
1.1.3 LSP建立……1-3
1.1.4 MPLS转发过程……1-4
1.1.5 倒数第二跳弹出……1-5
1.1.6 协议规范……1-5
1.2 MPLS配置任务简介……1-5
1.3 使能MPLS功能……1-6
1.3.1 配置准备……1-6
1.3.2 使能MPLS功能……1-6
1.4 配置MPLS MTU……1-7
1.5 配置Egress分配的标签类型……1-7
1.6 配置TTL复制……1-8
1.7 使能MPLS的TTL超时消息发送功能……1-10
1.8 配置MPLS转发统计功能……1-10
1.8.1 配置FTN转发统计功能……1-10
1.8.2 配置MPLS标签转发统计功能……1-10
1.9 开启告警功能……1-11
1.10 MPLS显示和维护……1-11

1 MPLS基础

1.1 MPLS简介

MPLS（Multiprotocol Label Switching，多协议标签交换）是目前应用比较广泛的一种骨干网技术。MPLS 在无连接的 IP 网络上引入面向连接的标签交换概念，将第三层路由技术和第二层交换技术相结合，充分发挥了 IP 路由的灵活性和二层交换的简洁性。

MPLS 广泛应用于大规模网络中，它具有以下优点：

- 在 MPLS 网络中，设备根据短而定长的标签转发报文，省去了查找 IP 路由表的繁琐过程，为数据在骨干网络中的传送提供了一种高速高效的方式。
- MPLS 位于链路层和网络层之间，它可以建立在各种链路层协议（如 PPP、ATM、帧中继、以太网等）之上，为各种网络层（IPv4、IPv6、IPX 等）提供面向连接的服务。
- 支持多层标签和面向连接的特点，使得 MPLS 具有良好的扩展性，在 MPLS 网络基础上可以为客户提供各种服务。目前，MPLS 在 VPN、流量工程、QoS 等方面得到广泛应用。

1.1.1 MPLS基本概念

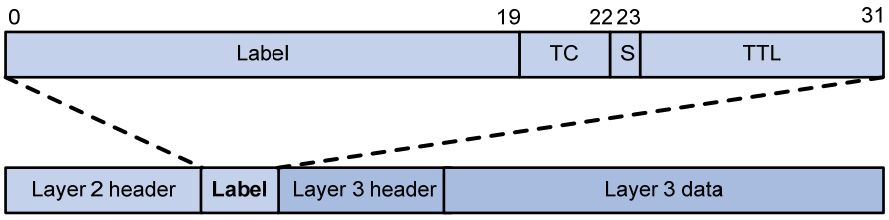
1. 转发等价类

FEC（Forwarding Equivalence Class，转发等价类）是 MPLS 中的一个重要概念。MPLS 将具有相同特征（目的地相同或具有相同服务等级等）的报文归为一类，称为 FEC。属于相同 FEC 的报文在 MPLS 网络中将获得完全相同的处理。

2. 标签

标签是一个长度固定、只具有本地意义的标识符，用于唯一标识一个报文所属的 FEC。一个标签只能代表一个 FEC。

图1-1 标签的封装结构



如 图 1-1 所示，标签封装在链路层帧头和网络层报文头之间，长度为 4 个字节，由以下四个字段组成：

- Label：标签值，长度为 20bits，用来标识一个 FEC。
- TC（Traffic Class，流量等级）：3bits，用于 QoS。该字段又称为 Exp 字段。
- S：标签栈底标识位，长度为 1bit。MPLS 支持多重标签，即在链路层帧头和网络层报文头之间可以封装多个标签，形成标签栈。靠近链路层帧头的最外层标签为栈顶标签；靠近网络层报文头的最内层标签为栈底标签。S 位为 1 时表示为栈底标签；S 位为 0 时表示为非栈底标签。

- TTL：8bits，和 IP 报文中的 TTL 意义相同，可以用来防止环路。

3. 标签交换路由器

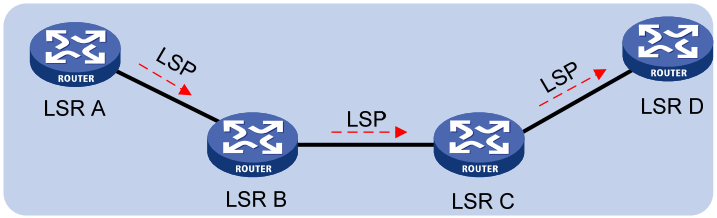
LSR（Label Switching Router，标签交换路由器）是具有标签分发能力和标签交换能力的设备，是 MPLS 网络中的基本元素。

4. 标签交换路径

属于同一个 FEC 的报文在 MPLS 网络中经过的路径称为 LSP（Label Switched Path，标签交换路径）。

LSP是一条单向报文转发路径。在一条LSP上，沿数据传送的方向，相邻的LSR分别称为上游LSR和下游LSR。如 图 1-2 所示，LSR B为LSR A的下游LSR，相应的，LSR A为LSR B的上游LSR。

图1-2 标签交换路径



5. 标签转发表

与 IP 网络中的 FIB（Forwarding Information Base，转发信息库）类似，在 MPLS 网络中，LSR 接收到带标签的报文后，通过查找 LFIB（Label Forwarding Information Base，标签转发信息库）获取对应的标签操作类型、出标签值、下一跳等，以确定如何转发该报文。

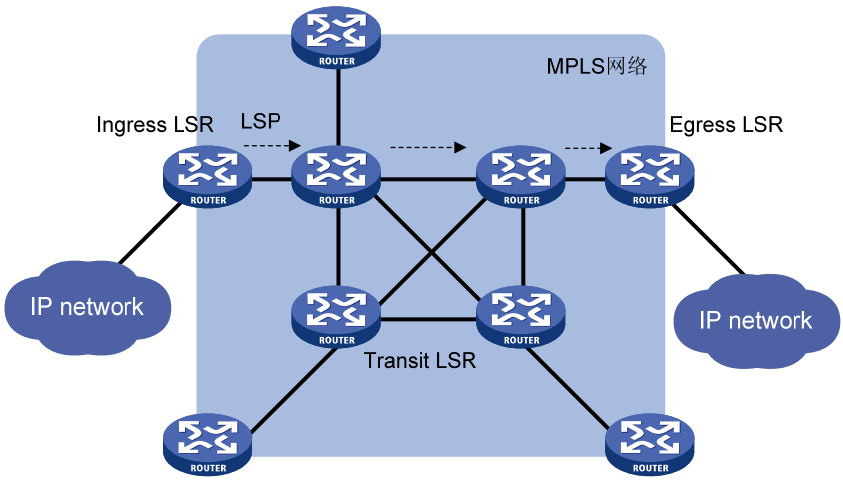
6. 控制平面和转发平面

MPLS 节点由两部分组成：

- 控制平面（Control Plane）：负责标签的分配、FEC—标签映射的交换、标签转发表的建立、标签交换路径的建立、拆除等工作；
- 转发平面（Forwarding Plane）：依据标签转发表对收到的报文进行转发。

1.1.2 MPLS网络结构

图1-3 MPLS 网络结构



如 图 1-3 所示，MPLS网络的基本构成单元是LSR。MPLS网络包括以下几个组成部分：

- 入节点 Ingress：报文的入口 LSR，负责为进入 MPLS 网络的报文添加标签。
- 中间节点 Transit：MPLS 网络内部的 LSR，根据标签沿着由一系列 LSR 构成的 LSP 将报文传送给出口 LSR。
- 出节点 Egress：报文的出口 LSR，负责剥离报文中的标签，并转发给目的网络。

1.1.3 LSP建立

LSP 的建立过程实际就是将 FEC 和标签进行绑定，在 LSR 上建立标签转发表的过程。LSP 既可以通过手工配置的方式静态建立，也可以利用标签分发协议动态建立。

(1) 手工配置的方式建立静态 LSP

建立静态 LSP 需要用户在报文转发路径中的各个 LSR 上手工配置为 FEC 分配的标签。建立静态 LSP 消耗的资源比较少，但静态建立的 LSP 不能根据网络拓扑变化动态调整。因此，静态 LSP 适用于拓扑结构简单并且稳定的小型网络。

(2) 利用标签分发协议动态建立 LSP

标签分发协议是 MPLS 的信令协议，负责划分 FEC、通告 FEC—标签绑定、建立维护 LSP 等。标签分发协议的种类较多，有专为标签分发而制定的协议，如 LDP（Label Distribution Protocol，标签分发协议），也有扩展后支持标签分发的协议，如 MP-BGP、RSVP-TE。

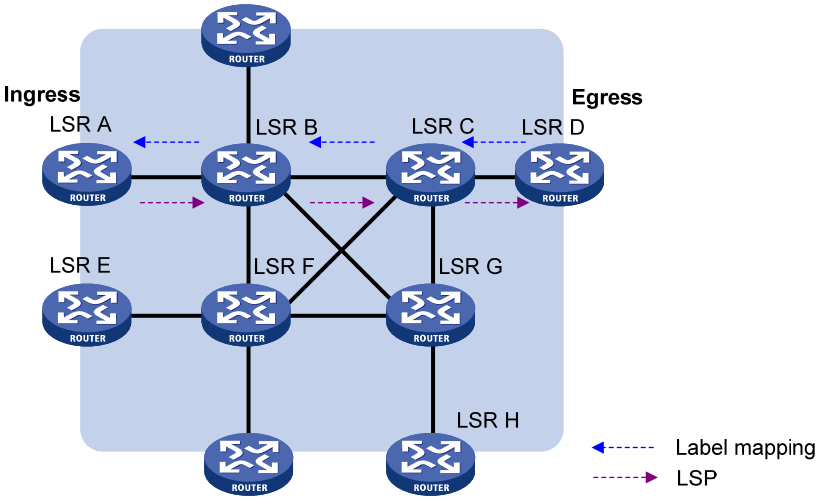
说明

为了区分，本文中“标签分发协议”表示广义上所有用于标签分发的协议的总称；“LDP”表示 RFC 5036 规定的标签分发协议。

利用标签分发协议动态建立LSP的过程如 图 1-4 所示。下游LSR根据目的地址划分FEC，为特定FEC分配标签，并将FEC—标签绑定关系通告给上游LSR；上游LSR根据该绑定关系建立标签转发表项。

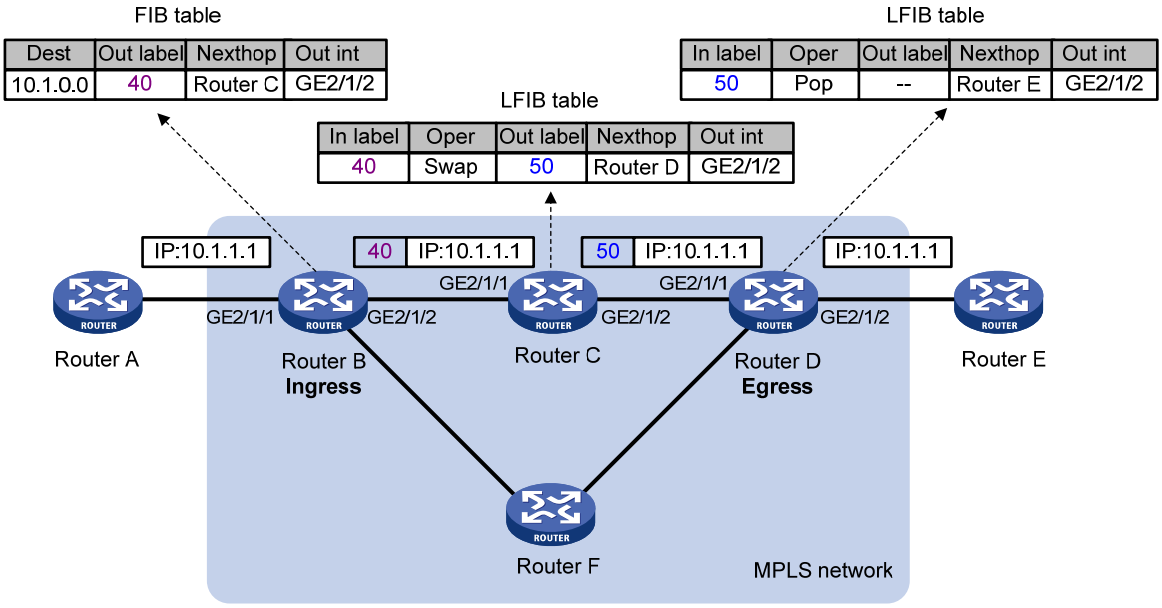
报文转发路径上的所有LSR都为该FEC建立对应的标签转发表项后，就成功地建立了用于转发属于该FEC报文的LSP。

图1-4 动态 LSP 建立过程



1.1.4 MPLS转发过程

图1-5 MPLS 转发过程示意图



如 图 1-5 所示，MPLS网络中报文的基本转发过程为：

(1) Ingress（Router B）接收到不带标签的报文，根据报文的目的 IP 地址查找 FIB 表获取报文的出标签（40）、下一跳 LSR（Router C）和出接口（GigabitEthernet2/1/2），为报文添加标签，并从相应的出接口将带有标签的报文转发给下一跳 LSR。

(2) Router C 根据报文上的标签(40)查找 LFIB 表获取报文的标签操作(交换标签)、出标签(50)、下一跳 LSR（Router D）和出接口（GigabitEthernet2/1/2），用新的标签（50）替换原有标签后，从相应的出接口将带有标签的报文转发给下一跳 LSR。

(3) Egress（Router D）接收到标签报文，根据报文上的标签（50）查找 LFIB 表获取报文的标签操作（删除标签）、下一跳 LSR（Router E）和出接口（GigabitEthernet2/1/2），删除报文中的标签，从相应的出接口将不带标签的报文转发给下一跳 LSR。如果 LFIB 表项中没有记录下一跳和出接口，则根据 IP 报文头查 FIB 表转发该报文。

1.1.5 倒数第二跳弹出

MPLS 网络中，Egress 节点接收到带有标签的报文后，查找标签转发表，弹出报文中的标签后，再进行下一层的标签转发或 IP 转发。Egress 节点转发报文之前要查找两次转发表：两次标签转发表，或一次标签转发表一次路由转发表。

为了减轻 Egress 节点的负担，提高 MPLS 网络对报文的处理能力，可以利用 PHP(Penultimate Hop Popping，倒数第二跳弹出）功能，在倒数第二跳节点处将标签弹出，Egress 节点只需查找一次转发表。

可以通过分配隐式空标签实现倒数第二跳弹出。隐式空标签的标签值为 3，这个值不会出现在标签栈中。当一个 LSR 发现下游 LSR 通告的标签为隐式空标签时，它并不用这个值替代栈顶原来的标签，而是直接弹出标签，并将报文转发给下游 LSR（即 Egress)。Egress 接收到报文后，直接进行下一层的转发处理。

使用隐式空标签时，倒数第二跳 LSR 弹出了标签栈，而在某些情况下，Egress 需要根据标签栈中的 TC 等信息决定 QoS 策略，此时利用显式空标签就可以在保留标签栈信息的同时，简化 Egress 节点的转发处理。IPv4 显式空标签的值为 0。Egress 为 FEC 分配 IPv4 显式空标签，并通告给上游 LSR 后，上游 LSR 用这个值替代栈顶原来的标签，并将报文转发给 Egress。Egress 收到标签值为 0 的报文时，不会查找标签转发表，从标签中获取 TC 等信息后，直接弹出标签栈，进行下一层的转发处理。

1.1.6 协议规范

与 MPLS 相关的协议规范有：

- RFC 3031：Multiprotocol Label Switching Architecture
- RFC 3032：MPLS Label Stack Encoding
- RFC 5462：Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field

1.2 MPLS配置任务简介

表1-1 MPLS 配置任务简介

配置任务	说明	详细配置
使能MPLS功能	必选	1.3
配置MPLS MTU	可选	1.4
配置Egress分配的标签类型	可选	1.5

配置任务	说明	详细配置
配置TTL复制	可选	1.6
使能MPLS的TTL超时消息发送功能	可选	1.7
配置MPLS转发统计功能	可选	1.8
开启告警功能	可选	1.9

1.3 使能MPLS功能

MPLS 网络中参与 MPLS 转发的设备接口上，必须先使能 MPLS 功能，才能进行 MPLS 转发。

1.3.1 配置准备

在使能 MPLS 功能之前，需要完成以下任务：

- 配置链路层协议，保证链路层通信正常。
- 配置接口的网络层地址，使各相邻节点网络层可达。
- 配置单播静态路由或 IGP 协议，保证各 LSR 在网络层互通。

1.3.2 使能MPLS功能

表1-2 使能 MPLS 功能

操作	命令	说明
进入系统视图	**system-view**	-
配置本节点的LSR ID	**mpls lsr-id** *lsr-id*	缺省情况下，未配置LSR ID LSR ID在MPLS网络内必须唯一 LSR ID采用点分十进制格式，与IP地址格式相同。推荐使用Loopback接口的IP地址作为LSR ID
进入需要转发MPLS报文的接口视图	**interface** *interface-type interface-number*	-
使能接口的MPLS能力	**mpls enable**	缺省情况下，未使能接口的MPLS能力

1.4 配置MPLS MTU

提示

- 配置的 MPLS MTU 值大于接口 MTU 时，有可能导致数据转发失败。
- 如果 MPLS 报文内封装的是 L2VPN 报文或 IPv6 报文，则即使报文长度大于 MPLS MTU，也会发送该报文，报文能否发送成功由接口的实际情况决定。

MPLS 标签栈位于链路层帧头和网络层报文头之间。在 MPLS 转发过程中，虽然网络层报文长度小于接口的 MTU，但是增加 MPLS 标签后，报文长度可能超过链路层允许发送的范围，从而导致报文无法正常转发。

为此，设备上定义了 MPLS MTU，MPLS 转发时将增加标签后的报文长度与 MPLS MTU 比较。报文长度大于 MPLS MTU 时：

- 如果允许分片，则 LSR 移除报文的标签栈，对 IP 报文进行分片（分片大小为 MPLS MTU 值减去标签栈的长度），分片后将被移除的标签栈添加到每个分片上，再进行转发；
- 如果不允许分片，则直接丢弃报文。

表1-3 配置 MPLS MTU

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口的MPLS MTU	**mpls mtu** *value*	缺省情况下，未配置接口的MPLS MTU值 如果未配置接口的MPLS MTU值，则根据接口的MTU值进行分片，分片的长度不包含MPLS标签栈长度，为分片添加MPLS标签栈后MPLS报文的长度可能会大于接口MTU的值，导致MPLS报文发送失败

1.5 配置Egress分配的标签类型

提示

- 对于 LDP LSP，执行 **mpls label advertise** 命令修改 Egress 分配的标签类型后，已经建立的 LDP LSP 会被拆除，并根据新的标签类型重新建立。
- 对于 BGP LSP，**mpls label advertise** 命令只对新建立的 BGP LSP 生效，执行本命令前已经建立的 BGP LSP 不受影响。若要使本命令对已经建立的 BGP LSP 生效，则需要从 BGP 路由表中删除 BGP LSP 对应的路由，并重新引入该路由。

MPLS 网络中，Egress 分配的标签类型分为以下几种：

- 隐式空标签：标签值为 3。
- 显式空标签：标签值为 0。
- 非空标签。

对于采用标签分发协议动态建立的 LSP，Egress 分配的标签类型决定了倒数第二跳转发带标签报文的方式：

- 如果分配的是隐式空标签，则倒数第二跳根据标签找到下一跳转发信息后，直接弹出标签。
- 如果分配的是显式空标签，则倒数第二跳将标签值替换为显式空标签。
- 如果分配的是非空标签，则倒数第二跳将标签值替换为 Egress 分配的标签值。

请根据实际情况选择 Egress 节点分配的标签类型：如果倒数第二跳节点支持 PHP（Penultimate Hop Popping，倒数第二跳弹出）功能，则建议采用隐式空标签；如果在简化 Egress 节点转发处理的同时，希望 Egress 节点能够根据标签中的 TC 等信息决定 QoS 策略，则建议采用显式空标签；非空标签只使用在一些比较特殊的场景，比如 Egress 节点上部署了 OAM，只有根据标签才能对应到 OAM 功能实体的情况，通常情况下不建议使用非空标签。

设备作为倒数第二跳节点时，允许 Egress 节点向其通告显式空标签、隐式空标签和非空标签。

表1-4 配置 Egress 分配的标签类型

操作	命令	说明
进入系统视图	**system-view**	-
配置设备作为Egress节点时分配的标签类型，即向倒数第二跳通告的标签类型	**mpls label advertise** { **explicit-null** | **implicit-null** | **non-null** }	缺省情况下，Egress节点向倒数第二跳通告隐式空标签（**implicit-null**）

1.6 配置TTL复制

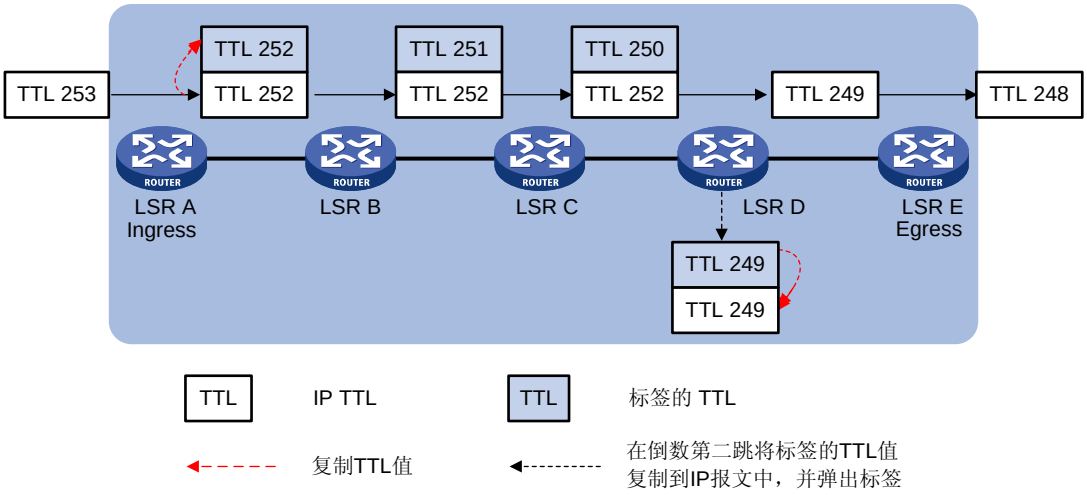
提示

- 建议在 LSP 经过的 LSR 上配置相同的 TTL 域处理方式。
- 如果配置 **mpls ttl propagate vpn** 命令使能对 VPN 报文的 TTL 复制功能，则建议在同一个 VPN 的所有 PE 上都使能此功能，以保证不同的 PE 上执行 Tracert 得到的结果一致。

IP 报文进入 MPLS 网络和 IP 报文离开 MPLS 网络时，TTL 的处理方式分为以下几种：

- 使能 TTL 复制功能：Ingress 节点为 IP 报文压入标签时，将原 IP 报文中的 TTL 值复制到新增加的标签的 TTL 域。LSR 转发标签报文时，对标签的 TTL 值做减一操作。LSR 弹出报文的标签时，将标签的 TTL 值复制回 IP 报文。使用这种方式时，MPLS 骨干网中的节点对用户网络的报文可见。报文沿着 LSP 传输的过程中，TTL 逐跳递减，Tracert 的结果将反映报文实际经过的路径。

图1-6 使能 TTL 复制功能时的处理过程



- 未使能 TTL 复制功能：Ingress 节点为 IP 报文压入标签时，不会将原 IP 报文中的 TTL 值复制到新增加的标签的 TTL 域，标签的 TTL 取值为 255。LSR 转发标签报文时，对标签的 TTL 值做减一操作。LSR 弹出标签时，不修改 IP TTL 的值。使用这种方式时，MPLS 骨干网中的节点对用户网络的报文不可见。Tracert 的结果不包括 MPLS 骨干网络中的每一跳，从而隐藏 MPLS 骨干网络的结构。

图1-7 未使能 TTL 复制功能时的处理过程

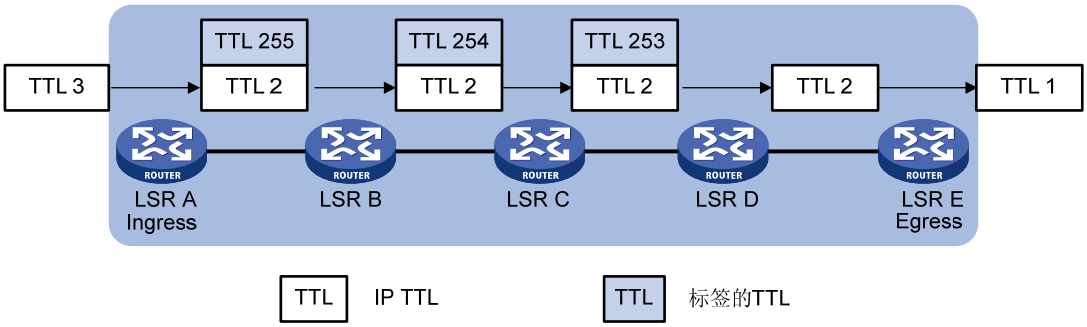


表1-5 配置 TTL 复制功能

操作	命令	说明
进入系统视图	**system-view**	-
使能TTL复制功能	**mpls ttl propagate { public | vpn }**	缺省情况下，只对公网报文使能TTL复制功能 在MPLS网络内部，MPLS报文多层标签之间的TTL值总是互相复制。本命令只决定是否将IP TTL复制到标签的TTL域、是否将标签的TTL复制到IP的TTL域

1.7 使能MPLS的TTL超时消息发送功能

使能 MPLS 的 TTL 超时消息发送功能后，当 LSR 收到 TTL 为 1 的 MPLS 报文时，LSR 会生成 ICMP 的 TTL 超时消息。对于一层标签的 MPLS 报文，LSR 沿着本地 IP 路由返回 ICMP TTL 超时消息；对于多层标签的 MPLS 报文，LSR 沿着发送 MPLS 报文的 LSP 转发 ICMP TTL 超时消息，由 Egress 节点将该消息返回给发送者。

表1-6 配置 MPLS 的 TTL 超时消息发送功能

操作	命令	说明
进入系统视图	**system-view**	-
使能MPLS的TTL超时消息发送功能	**mpls ttl expiration enable**	缺省情况下，MPLS的TTL超时消息发送功能处于开启状态

1.8 配置MPLS转发统计功能

1.8.1 配置FTN转发统计功能

FTN（FEC to NHLFE map，FEC 到 NHLFE 表项的映射）表项是一类特殊的 FIB 表项，该类 FIB 表项中包含出标签值信息。FTN 转发是指接收到不带标签的报文，该报文的目的 IP 地址匹配 FTN 表项，为报文添加 FTN 表项中的出标签值后转发该报文。本配置用来开启 FTN 转发的统计功能。

表1-7 配置 FTN 转发统计功能

操作	命令	说明
进入系统视图	**system-view**	-
进入RIB视图	**rib**	-
创建RIB IPv4地址族，并进入RIB IPv4地址族视图	**address-family ipv4**	缺省情况下，没有创建RIB IPv4地址族
开启RIB的FTN表项维护功能	**ftn enable**	缺省情况下，RIB的FTN表项维护功能处于关闭状态
使能指定目的网络的FTN转发统计功能	**mpls-forwarding statistics prefix-list** *prefix-list-name*	缺省情况下，所有目的网络的FTN转发统计功能均处于关闭状态

1.8.2 配置MPLS标签转发统计功能

MPLS 标签转发是指接收到带有标签的报文后，根据报文中的入标签转发该报文。

本配置用来开启 MPLS 标签转发统计功能和统计信息收集功能，以便用户通过 **display mpls lsp verbose** 命令查看 MPLS 标签的转发统计信息。

表1-8 配置 MPLS 标签转发统计功能

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
使能指定LSP的MPLS标签转发统计功能	**mpls statistics** { **all** | [**vpn-instance** *vpn-instance-name*] { **ipv4** *ipv4-destination mask-length* | **ipv6** *ipv6-destination prefix-length* } | **static** | **te** *ingress-lsr-id tunnel-id* }	缺省情况下，所有LSP的MPLS标签转发统计功能均处于关闭状态
使能MPLS标签转发统计信息的收集功能，并设置统计信息收集的时间间隔	**mpls statistics interval** *interval*	缺省情况下，MPLS标签转发统计信息收集功能处于关闭状态

1.9 开启告警功能

开启 MPLS 模块的告警功能后，该模块会生成告警信息，用于报告该模块的重要事件。生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。

有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

表1-9 开启告警功能

操作	命令	说明
进入系统视图	**system-view**	-
开启MPLS模块的告警功能	**snmp-agent trap enable mpls**	缺省情况下，MPLS模块的告警功能处于开启状态

1.10 MPLS显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 MPLS 的运行情况，用户可以通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 MPLS 统计信息。

表1-10 MPLS 显示和维护

操作	命令
显示使能了MPLS能力接口的MPLS相关信息	**display mpls interface** [*interface-type interface-number*]
显示MPLS标签的使用状态	**display mpls label** { *label-value1* [**to** *label-value2*] | **all** }
显示LSP信息	**display mpls lsp** [**egress** | **in-label** *label-value* | **ingress** | **outgoing-interface** *interface-type interface-number* | **protocol** { **bgp** | **ldp** | **local** | **rsvp-te** | **static** | **static-cr** } | **transit**] [**vpn-instance** *vpn-instance-name*] [*ipv4-dest mask-length* | **ipv6** [*ipv6-dest prefix-length*]] [**verbose**]
显示MPLS的NIB（Nexthop Information Base，下一跳信息库）信息	**display mpls nib** [*nib-id*]
显示MPLS NHLFE表项索引的使用状态	**display mpls nid** [*nid-value1* [**to** *nid-value2*]]

操作	命令
显示LSP的统计信息	**display mpls lsp statistics**
显示MPLS汇总信息	**display mpls summary**
显示ILM表项信息（MSR 2600/MSR 3600）	**display mpls forwarding ilm** [*label*]
显示ILM表项信息（MSR 5600）	**display mpls forwarding ilm** [*label*] [**slot** *slot-number*]
显示NHLFE表项信息（MSR 2600/MSR 3600）	**display mpls forwarding nhlfe** [*nid*]
显示NHLFE表项信息（MSR 5600）	**display mpls forwarding nhlfe** [*nid*] [**slot** *slot-number*]
清除指定LSP的MPLS转发统计信息	**reset mpls statistics** { **all** | [**vpn-instance** *vpn-instance-name*] { **ipv4** *ipv4-destination mask-length* | **ipv6** *ipv6-destination prefix-length* } | **static** | **te** *ingress-lsr-id tunnel-id* }

目 录

1 静态LSP 1-1
1.1 静态LSP简介 1-1
1.2 建立静态LSP 1-1
1.2.1 配置准备 1-1
1.2.2 建立静态LSP 1-2
1.3 静态LSP显示和维护 1-2
1.4 建立静态LSP配置举例 1-2

1 静态LSP

1.1 静态LSP简介

不依靠标签分发协议，而是在报文经过的每一跳设备上（包括 Ingress、Transit 和 Egress）分别手工指定入标签、出标签等信息，建立标签转发表项，采用这种方式建立的 LSP（Label Switched Path，标签交换路径），称为静态 LSP。

建立静态 LSP 消耗的资源比较少，但静态建立的 LSP 不能根据网络拓扑变化动态调整。因此，静态 LSP 适用于拓扑结构简单并且稳定的小型网络。

建立静态 LSP 时，静态 LSP 经过的不同类型的节点上配置内容有所不同：

- Ingress：Ingress 根据报文的目的 IP 地址划分 FEC（Forwarding Equivalence Class，转发等价类），并为报文添加标签。因此，在 Ingress 上需要指定目的网段对应的出标签、LSP 的下一跳或到达下一跳的出接口。Ingress 查找报文的目的 IP 地址所属的目的网段（即查找报文所属的 FEC），为报文添加该 FEC 对应的出标签，并将报文转发给指定的下一跳，或通过出接口转发该报文。
- Transit：Transit 根据报文中携带的标签值，查找标签转发表项，用新的标签替换原有标签。因此，Transit 上需要指定入标签对应的出标签、LSP 的下一跳或到达下一跳的出接口。Transit 接收到带有标签的报文后，将报文中的标签替换为该标签对应的出标签，并将报文转发给指定的下一跳，或通过出接口转发该报文。
- Egress：如果没有在倒数第二跳弹出标签，则 Egress 负责弹出报文中的标签，并对报文进行下一层转发处理。因此，Egress 上只需指定入标签值。Egress 接收到带有指定入标签值的报文后，弹出该标签。

配置 Ingress、Transit、Egress 时，需要遵循以下原则：相邻两个 LSR（Label Switching Router，标签交换路由器）之间，上游 LSR 的出标签值和下游 LSR 的入标签值必须相同。

1.2 建立静态LSP

1.2.1 配置准备

在配置静态 LSP 之前，需完成以下任务：

- 确定静态 LSP 的 Ingress 节点、Transit 节点和 Egress 节点。
- 在参与 MPLS 转发的设备接口上使能 MPLS 功能，配置方法请参见“MPLS 配置指导”中的“MPLS 基本配置”。
- 在 Ingress 节点上建立静态 LSP 时，需确保该节点上存在 FEC 目的地址对应的路由。Transit 节点和 Egress 节点上不需要存在 FEC 目的地址对应的路由。

1.2.2 建立静态LSP

表1-1 建立静态 LSP

操作	命令	说明
进入系统视图	**system-view**	-
配置静态LSP的Ingress节点	**static-lsp ingress** *lsp-name* **destination** *dest-addr* { *mask* | *mask-length* } { **nexthop** *next-hop-addr* | **outgoing-interface** *interface-type interface-number* } **out-label** *out-label*	配置静态LSP的Ingress节点时，如果指定下一跳，则需要保证节点上存在该下一跳地址对应的激活路由
配置静态LSP的Transit节点	**static-lsp transit** *lsp-name* **in-label** *in-label* { **nexthop** *next-hop-addr* | **outgoing-interface** *interface-type interface-number* } **out-label** *out-label*	配置静态LSP的Transit节点时，如果指定下一跳，则需要保证节点上存在该下一跳地址对应的激活路由
配置静态LSP的Egress节点	**static-lsp egress** *lsp-name* **in-label** *in-label*	如果静态LSP的倒数第二跳节点上配置的出标签为0或3，则不需要在Egress节点上执行本命令

1.3 静态LSP显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后静态 LSP 的运行情况，用户可以通过查看显示信息验证配置的效果。

表1-2 静态 LSP 显示和维护

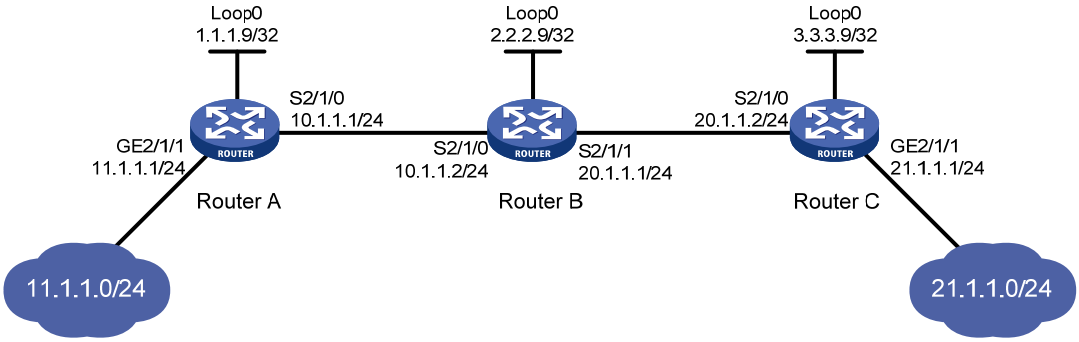
操作	命令
显示静态LSP的信息	**display mpls static-lsp** [**lsp-name** *lsp-name*]

1.4 建立静态LSP配置举例

1. 组网需求

- Router A、Router B 和 Router C 均支持 MPLS。
- 在 Router A 和 Router C 之间建立静态 LSP，使 11.1.1.0/24 和 21.1.1.0/24 这两个网段中互访的报文能够通过 MPLS 进行传输。

图1-1 静态建立 LSP 组网图



2. 配置思路

- 手工指定静态 LSP 的标签时，需要遵循以下原则：一条 LSP 上，上游 LSR 出标签的值与下游 LSR 入标签的值相同。
- LSP 是一条单向路径，因此需要在数据传输的两个方向上分别配置一条静态 LSP。
- 配置静态 LSP 时，只要求在 Ingress 节点上存在到达 FEC 目的地址的路由，Transit 节点和 Egress 节点上不需要存在到达 FEC 目的地址的路由。因此，无需配置路由协议保证路由器之间路由可达，只需在 Ingress 节点上配置到达 FEC 目的地址的静态路由即可。

3. 配置步骤

(1) 配置各接口的 IP 地址

按照 图 1-1 配置各接口的IP地址和掩码，包括Loopback接口，具体配置过程略。

(2) 在 Ingress 上配置到达 FEC 目的地址的静态路由

在 Router A 上配置到达 21.1.1.0/24 网段的静态路由。

```
<RouterA> system-view
[RouterA] ip route-static 21.1.1.0 24 10.1.1.2
```

在 Router C 上配置到达 11.1.1.0/24 网段的静态路由。

```
<RouterC> system-view
[RouterC] ip route-static 11.1.1.0 255.255.255.0 20.1.1.1
```

(3) 使能 MPLS 功能

配置 Router A。

```
[RouterA] mpls lsr-id 1.1.1.9
[RouterA] interface serial 2/1/0
[RouterA-Serial2/1/0] mpls enable
[RouterA-Serial2/1/0] quit
```

配置 Router B。

```
[RouterB] mpls lsr-id 2.2.2.9
[RouterB] interface serial 2/1/0
[RouterB-Serial2/1/0] mpls enable
[RouterB-Serial2/1/0] quit
[RouterB] interface serial 2/1/1
[RouterB-Serial2/1/1] mpls enable
[RouterB-Serial2/1/1] quit
```

配置 Router C。

```
[RouterC] mpls lsr-id 3.3.3.9
[RouterC] interface serial 2/1/0
[RouterC-Serial2/1/0] mpls enable
[RouterC-Serial2/1/0] quit
```

(4)　创建从 Router A 到 Router C 的静态 LSP

配置 Ingress Router A。

```
[RouterA] static-lsp ingress AtoC destination 21.1.1.0 24 nexthop 10.1.1.2 out-label 30
```

配置 Transit Router B

```
[RouterB] static-lsp transit AtoC in-label 30 nexthop 20.1.1.2 out-label 50
```

配置 Egress Router C。

```
[RouterC] static-lsp egress AtoC in-label 50
```

(5)　创建从 Router C 到 Router A 的静态 LSP

配置 Ingress Router C。

```
[RouterC] static-lsp ingress CtoA destination 11.1.1.0 24 nexthop 20.1.1.1 out-label 40
```

配置 Transit Router B。

```
[RouterB] static-lsp transit CtoA in-label 40 nexthop 10.1.1.1 out-label 70
```

配置 Egress Router A。

```
[RouterA] static-lsp egress CtoA in-label 70
```

4. 验证配置

配置完成后，可以在各路由器上通过**display mpls static-lsp**命令查看静态 LSP 的信息。以 Router A 的显示信息为例。

```
[RouterA] display mpls static-lsp
Total: 2
Name            FEC               In/Out Label Nexthop/Out Interface    State
AtoC            21.1.1.0/24       NULL/30      10.1.1.2                 Up
CtoA            -/-               70/NULL      -                        Up
```

在 Router A 上检测 Router A 到 Router C 静态 LSP 的可达性。

```
[RouterA] ping mpls -a 11.1.1.1 ipv4 21.1.1.0 24
MPLS Ping FEC: 21.1.1.0/24 : 100 data bytes
100 bytes from 20.1.1.2: Sequence=1 time=4 ms
100 bytes from 20.1.1.2: Sequence=2 time=1 ms
100 bytes from 20.1.1.2: Sequence=3 time=1 ms
100 bytes from 20.1.1.2: Sequence=4 time=1 ms
100 bytes from 20.1.1.2: Sequence=5 time=1 ms

--- FEC: 21.1.1.0/24 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max = 1/1/4 ms
```

在 Router C 上检测 Router C 到 Router A 静态 LSP 的可达性。

```
[RouterC] ping mpls -a 21.1.1.1 ipv4 11.1.1.0 24
MPLS Ping FEC: 11.1.1.0/24 : 100 data bytes
100 bytes from 10.1.1.1: Sequence=1 time=5 ms
100 bytes from 10.1.1.1: Sequence=2 time=1 ms
```

```
100 bytes from 10.1.1.1: Sequence=3 time=1 ms
100 bytes from 10.1.1.1: Sequence=4 time=1 ms
100 bytes from 10.1.1.1: Sequence=5 time=1 ms

--- FEC: 11.1.1.0/24 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max = 1/1/5 ms
```

目 录

1 LDP ····· 1-1
1.1 LDP简介 ····· 1-1
1.1.1 LDP基本概念 ····· 1-1
1.1.2 LDP消息类型 ····· 1-1
1.1.3 LDP工作过程 ····· 1-2
1.1.4 LDP的标签分发和管理 ····· 1-3
1.1.5 LDP GR ····· 1-5
1.1.6 LDP NSR ····· 1-6
1.1.7 LDP IGP同步 ····· 1-7
1.1.8 LDP快速重路由 ····· 1-8
1.1.9 协议规范 ····· 1-9
1.2 LDP配置任务简介 ····· 1-9
1.3 使能LDP能力 ····· 1-10
1.3.1 全局使能LDP能力 ····· 1-10
1.3.2 在接口上使能LDP能力 ····· 1-10
1.4 配置Hello消息参数 ····· 1-10
1.5 配置LDP会话参数 ····· 1-11
1.6 配置LDP倒退机制的延迟时间 ····· 1-12
1.7 配置LDP MD5 认证 ····· 1-13
1.8 配置LDP引入BGP IPv4 单播路由 ····· 1-13
1.9 配置LSP触发策略 ····· 1-14
1.10 配置LDP标签分发控制方式 ····· 1-14
1.11 配置标签通告控制策略 ····· 1-15
1.12 配置标签接受控制策略 ····· 1-16
1.13 配置LDP环路检测 ····· 1-17
1.14 配置LDP会话保护 ····· 1-18
1.15 配置LDP GR ····· 1-18
1.16 配置LDP NSR ····· 1-19
1.17 配置LDP IGP同步 ····· 1-19
1.17.1 配置LDP OSPF同步 ····· 1-19
1.17.2 配置LDP IS-IS同步 ····· 1-20
1.18 配置LDP快速重路由 ····· 1-21
1.19 配置发送的LDP报文的DSCP优先级 ····· 1-21

1.20 重启LDP会话 ····· 1-21
1.21 开启告警功能 ····· 1-22
1.22 LDP显示和维护 ····· 1-22
1.23 LDP配置举例 ····· 1-23
1.23.1 利用LDP动态建立LSP配置举例 ····· 1-23
1.23.2 标签接受控制策略配置举例 ····· 1-27
1.23.3 标签通告控制策略配置举例 ····· 1-31
1.23.4 LDP快速重路由配置举例 ····· 1-37

1 LDP

1.1 LDP简介

LDP（Label Distribution Protocol，标签分发协议）用来动态建立 LSP。通过 LDP，LSR 可以把网络层的 IP 路由信息映射到 MPLS 的标签交换路径上。

1.1.1 LDP基本概念

1. LDP会话

LDP 会话是指建立在 TCP 连接之上的 LDP 协议连接，用于在 LSR 之间交换 FEC—标签映射（FEC-Label Mapping）。

2. LDP对等体

LDP 对等体是指相互之间存在 LDP 会话，并通过 LDP 会话交换 FEC—标签映射关系的两个 LSR。

3. 标签空间与LDP标识符

标签空间是指标签的取值范围。有以下几种类型的标签空间：

- 每接口标签空间（per-interface label space）：每个接口使用一个独立的标签空间。不同接口使用的标签空间中包括的标签值可以相同。
- 每平台标签空间（per-platform label space）：整个 LSR 统一使用一个标签空间。

目前，设备上只支持每平台标签空间。

LDP ID（LDP Identifier，LDP 标识符）用于标识特定 LSR 的标签空间，为一个六字节的数值，格式如下：

<LSR ID>：<标签空间序号>

其中，LSR ID 占四字节；标签空间序号占两字节，取值为 0 时表示每平台标签空间，取值为非 0 值时表示某个接口使用的标签空间。

4. FEC和FEC—标签映射

FEC（Forwarding Equivalence Class，转发等价类）是 MPLS 中的一个重要概念。MPLS 将具有相同特征（目的地相同或具有相同服务等级等）的报文归为一类，称为 FEC。属于相同 FEC 的报文在 MPLS 网络中将获得完全相同的处理。

LDP 支持根据目的 IP 地址和 PW（Pseudo Wire，伪线）划分 FEC。本文只介绍根据目的 IP 地址划分 FEC。根据 PW 划分 FEC 的详细介绍，请参见“MPLS 配置指导”中的“MPLS L2VPN”。

FEC—标签映射也称为 FEC—标签绑定（FEC-Label Binding），是本地 LSR 设备上标签与 FEC 的对应关系。LDP 通过 Label Mapping 消息将 FEC—标签映射通告给对等体。

1.1.2 LDP消息类型

LDP 协议主要使用四类消息：

- 发现（Discovery）消息：用于通告和维护网络中的 LSR，例如 Hello 消息。

- 会话（Session）消息：用于建立、维护和终止 LDP 对等体之间的会话，例如用来协商会话参数的 Initialization 消息和用于维护会话的 Keepalive 消息。
- 通告（Advertisement）消息：用于创建、改变和删除“FEC—标签”映射关系，例如用来通告标签映射的 Label Mapping 消息。
- 通知（Notification）消息：用于提供建议性信息的消息和差错通知，例如 Notification 消息。

为保证 LDP 消息的可靠发送，除了发现消息使用 UDP 传输外，LDP 的会话消息、通告消息和通知消息都使用 TCP 传输。

1.1.3 LDP工作过程

LDP 工作过程主要包括以下几个阶段：

1. 对等体发现与维护

使能了 LDP 能力的 LSR 周期性地发送 Hello 消息，通告自己的存在。通过 Hello 消息，LSR 可以自动发现它周围的 LSR 邻居，并与其建立 Hello 邻接关系。

LDP 对等体发现机制分为两种：

- 基本发现机制：用于发现本地直连的 LSR 邻居，即通过链路层直接相连的 LSR。这种方式下，LSR 周期性地向“子网内所有路由器”的组播地址 224.0.0.2 发送 LDP 的 Link Hello 消息，以便链路层直接相连的 LSR 发现此 LSR。
- 扩展发现机制：用于发现远端非直连的 LSR 邻居，即不通过链路层直接相连的 LSR。这种方式下，LSR 周期性地向指定的 IP 地址发送 LDP 的 Targeted Hello 消息，以便指定 IP 地址对应的 LSR 发现此 LSR。扩展发现机制主要应用于 MPLS L2VPN 和 LDP over MPLS TE，详细介绍请参见“MPLS 配置指导”中的“MPLS L2VPN”和“MPLS TE”。

LSR 可以与直连的邻居同时建立 Link Hello 和 Targeted Hello 两种邻接关系。

LDP 对等体之间通过周期性地发送 Hello 消息来维护 Hello 邻接关系。如果 Hello 保持定时器超时时仍没有收到新的 Hello 消息，则删除 Hello 邻接关系。

2. 会话建立与维护

通过交互 Hello 消息发现 LSR 邻居后，LSR 开始与其建立会话。这一过程又可分为两步：

(1) 建立传输层连接，即在 LSR 之间建立 TCP 连接；

(2) 对 LSR 之间的会话进行初始化，协商会话中涉及的各种参数，如 LDP 版本、标签通告方式、Keepalive 保持时间等。如果会话参数协商通过，则 LSR 之间成功建立 LDP 会话。

会话建立后，LDP 对等体之间通过发送 LDP PDU（LDP PDU 中携带一个或多个 LDP 消息）来维护这个会话。如果在 Keepalive 报文发送时间间隔内，LDP 对等体之间没有需要交互的信息，则 LSR 发送 Keepalive 消息给 LDP 对等体，以便维持 LDP 会话。如果 Keepalive 保持定时器超时时，没有收到任何 LDP PDU，LSR 将关闭 TCP 连接，结束 LDP 会话。

一个 LDP 会话上可能存在多个 Hello 邻接关系。当 LDP 会话上的最后一个 Hello 邻接关系被删除后，LSR 将发送通知消息，结束该 LDP 会话。

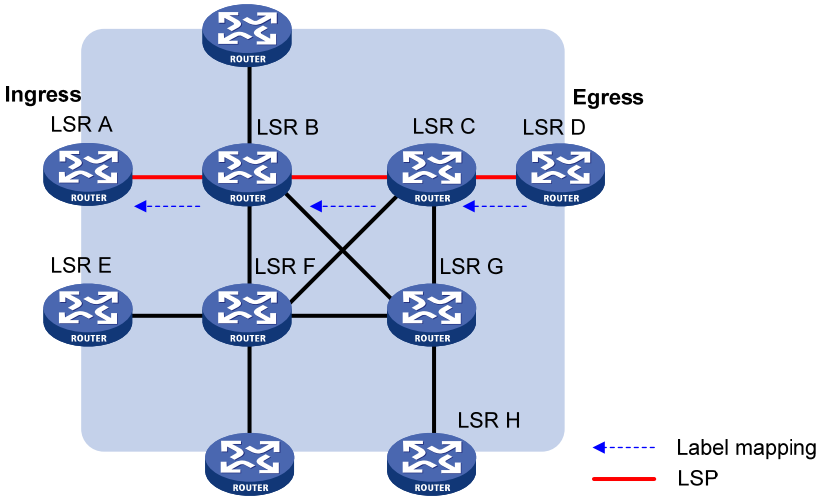
LSR 还可以通过发送 Shutdown 消息，通知它的 LDP 对等体结束 LDP 会话。

3. LSP建立

利用LDP动态建立LSP的过程如 图 1-1 所示。LSR根据IP路由表项中的目的IP地址划分FEC，为不同的FEC分配不同的标签，并将FEC—标签映射通告给对端LSR；对端LSR根据接收到的FEC—标

签映射及本地为该FEC分配的标签建立标签转发表项。从Ingress到Egress的所有LSR都为该FEC建立对应的标签转发表项后，就成功地建立了用于转发属于该FEC报文的LSP。

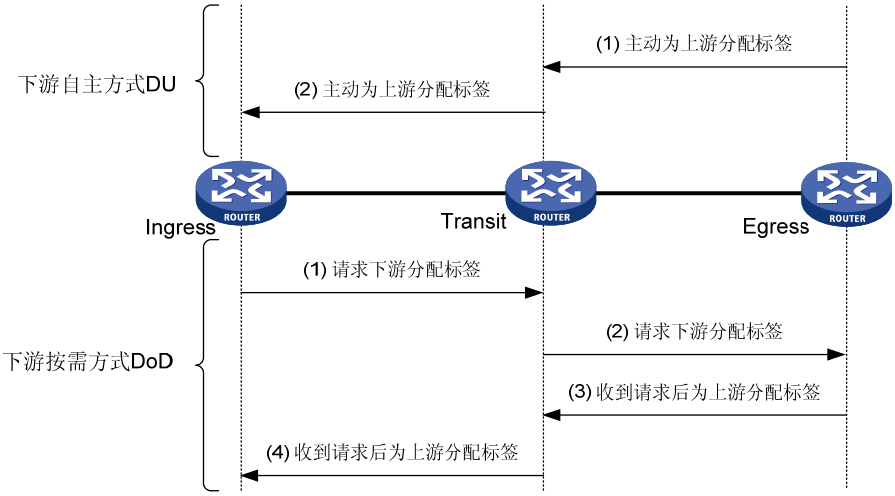
图1-1 动态 LSP 建立过程



1.1.4 LDP的标签分发和管理

1. 标签通告方式（Label Advertisement Mode）

图1-2 标签通告方式



如 图 1-2 所示，根据建立了会话的一对LSR中哪个LSR负责发起标签映射过程，标签通告方式分为：

- DU（Downstream Unsolicited，下游自主方式）：下游 LSR 主动将 FEC—标签映射通告给上游 LSR，无需等待上游 LSR 的标签请求。在 DU 方式中，下游 LSR 负责发起标签映射过程。
- DoD（Downstream On Demand，下游按需方式）：上游 LSR 请求下游 LSR 为 FEC 分配标签，下游 LSR 收到请求后，才会将该 FEC 的 FEC—标签映射通告给请求标签的上游 LSR。在 DoD 方式中，上游 LSR 负责发起标签映射过程。

目前，设备只支持 DU 标签通告方式。

提示

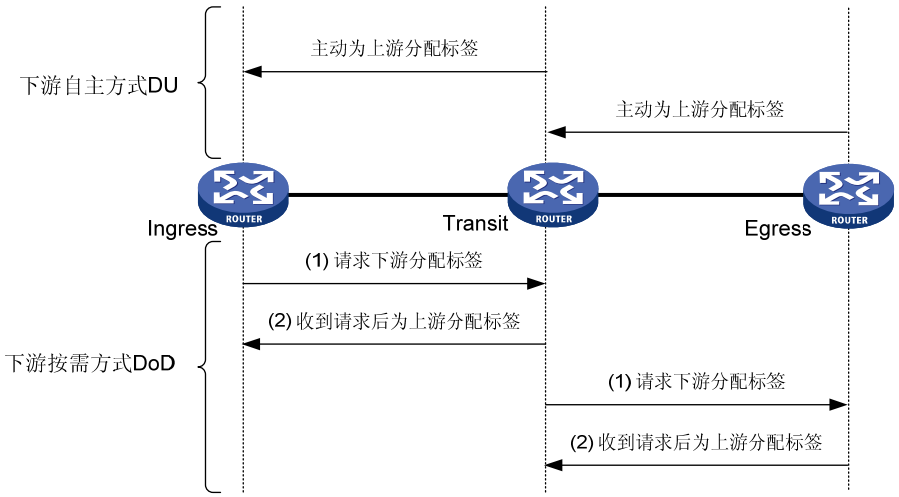
具有标签分发邻接关系的上游 LSR 和下游 LSR 之间必须使用相同的标签通告方式，否则 LSP 无法正常建立。

2. 标签分发控制方式（Label Distribution Control Mode）

根据通告 FEC—标签映射前是否要求收到下游的 FEC—标签映射，标签分发控制方式分为独立标签分发控制方式（Independent）和有序标签分发控制方式（Ordered）。

- 独立标签分发控制方式：LSR可以在任意时间向与它连接的LSR通告FEC—标签映射。使用这种方式时，LSR可能会在收到下游LSR的FEC—标签映射之前就向上游通告了FEC—标签映射。如 图 1-3 所示，如果标签通告方式是DU，则即使没有获得下游的FEC—标签映射，也会直接向上游LSR通告FEC—标签映射；如果标签通告方式是DoD，则接收到标签请求的LSR直接向它的上游LSR通告FEC—标签映射，不必等待来自它的下游的FEC—标签映射。

图1-3 独立标签分发控制方式



- 有序标签分发控制方式：LSR只有收到它的下游LSR为某个FEC通告的FEC—标签映射，或该LSR是此FEC的出口节点时，才会向它的上游LSR通告此FEC的FEC—标签映射。图 1-2 中的标签通告过程采用了有序标签控制方式：如果标签通告方式为DU，则LSR只有收到下游LSR通告的FEC—标签映射，才会向自己的上游LSR通告FEC—标签映射；如果标签通告方式为DoD，则下游LSR（Transit）收到上游LSR（Ingress）的标签请求后，继续向它的下游LSR（Egress）发送标签请求，Transit收到Egress通告的FEC—标签映射后，才会向Ingress通告FEC—标签映射。

3. 标签保持方式（Label Retention Mode）

根据 LSR 是否保持收到的、但暂时未使用的 FEC—标签映射，标签保持方式分为：

- 自由标签保持方式（Liberal）：对于从邻居 LSR 收到的标签映射，无论邻居 LSR 是不是指定 FEC 的下一跳都保留。这种方式的优点是 LSR 能够迅速适应网络拓扑变化，但是由于需要保留所有不能生成 LSP 的标签，浪费了内存等系统资源。

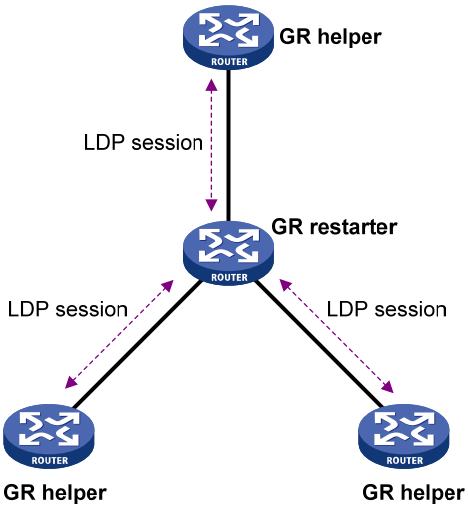
- 保守标签保持方式（Conservative）：对于从邻居 LSR 收到的标签映射，只有当邻居 LSR 是指定 FEC 的下一跳时才保留。这种方式的优点是节省标签，但是对拓扑变化的响应较慢。

目前，设备只支持自由标签保持方式。

1.1.5 LDP GR

LDP GR（Graceful Restart，平滑重启）利用 MPLS 转发平面与控制平面分离的特点，在信令协议或控制平面出现异常时，保持标签转发表项，LSR 依然根据该表项转发报文，从而保证数据转发不中断。

图1-4 LDP GR

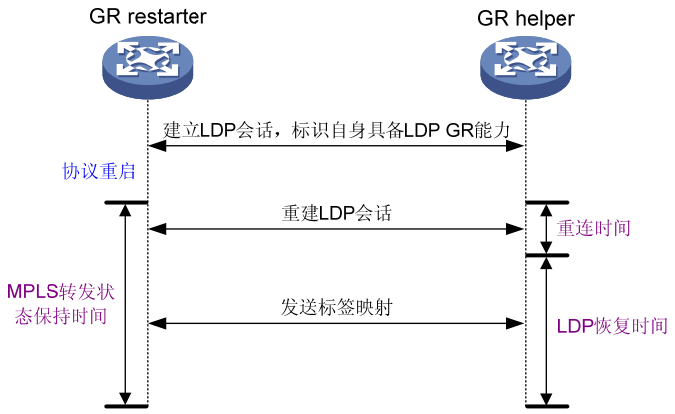


如 图 1-4 所示，参与LDP GR过程的设备分为以下两种：

- GR restarter：GR 重启的 LSR，指由管理员手工触发或控制平面异常而重启协议的设备，它必须具备 GR 能力。
- GR helper：GR restarter 的邻居 LSR，与重启的 GR restarter 保持邻居关系，并协助其恢复重启前的转发状态。

设备既可以作为 GR restarter，又可以作为 GR helper，设备的角色由该设备在 LDP GR 过程中的作用决定。

图1-5 LDP GR 工作过程示意图



如 图 1-5 所示，LDP GR的工作过程为：

(1) LSR 之间建立 LDP 会话时，LSR 在发送的 Initialization 消息中携带 FT（Fault Tolerance，容错）会话 TLV，且 L 标记位置为 1，标识它们支持 LDP GR。

(2) GR restarter 进行协议重启时，启动 MPLS 转发状态定时器，并将标签转发表项置为 Stale 状态。GR helper 发现与 GR restarter 之间的 LDP 会话 down 后，将通过该 LDP 会话接收的 FEC—标签映射置为 Stale 状态，并启动重连定时器。

(3) GR restarter 协议重启后，重新建立与 GR helper 的 LDP 会话。如果在重连定时器超时前，没有建立 LDP 会话，则 GR helper 删除标记为 Stale 的 FEC—标签映射及对应的标签转发表项。如果在重连定时器超时前，重新建立 LDP 会话，GR restarter 将转发状态保持定时器的剩余时间作为恢复定时器时间值通告给 GR helper。

(4) GR restarter 和 GR helper 之间重新建立 LDP 会话后，GR helper 启动 LDP 恢复定时器。

(5) GR restarter 和 GR helper 在新建立的 LDP 会话上交互标签映射，更新标签转发表。GR restarter 接收到标签映射后，与标签转发表进行比较：如果标签转发表中存在与标签映射一致的 Stale 表项，则删除该表项的 Stale 标记；否则，按照正常的 LDP 处理流程，添加新的标签转发表项。GR helper 接收到标签映射后，与本地保存的 FEC—标签映射进行比较：如果存在一致的标签映射，则删除该 FEC—标签映射的 Stale 标记；否则，按照正常的 LDP 处理流程，添加新的 FEC—标签映射及对应的标签转发表项。

(6) MPLS 转发状态保持定时器超时后，GR restarter 删除标记为 Stale 的标签转发表项。

(7) LDP 恢复定时器超时后，GR helper 删除标记为 Stale 的 FEC—标签映射。

说明

GR restarter 在 LDP 会话协商时，将本地配置的 GR 重连超时时间和 GR 转发状态保持定时器的剩余时间发送给 GR helper，GR helper 分别将其作为重连定时器的值和 LDP 恢复定时器的值。

1.1.6 LDP NSR

MSR 系列路由器各款型对于本节所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR 2600	LDP NSR	不支持
MSR 3600		不支持
MSR 5600		支持

LDP NSR（Nonstop Routing，不间断路由）是一种通过在 LDP 协议主备进程之间备份必要的协议状态和数据（如 LDP 会话信息和 LSP 信息），使得 LDP 协议的主进程中断时，备份进程能够无缝地接管主进程的工作，从而确保对等体感知不到 LDP 协议中断，保证 LDP 会话保持 Operational 状态，并保证转发不会中断的技术。

导致 LDP 主进程中断的事件包括以下几种：

- LDP 主进程重启
- LDP 主进程所在的主控板发生故障
- LDP 主进程所在的主控板进行 ISSU（In-Service Software Upgrade，不中断业务升级）
- 进程分布优化为 LDP 进程决策出的位置不同于当前运行的位置而进行进程主备倒换

LDP NSR 与 LDP GR 具有如下区别，请根据实际情况选择合适的方式确保数据转发不中断：

- 对设备要求不同：LDP 协议的主进程和备进程运行在不同的主控板上，因此要运行 LDP NSR 功能，设备上必须有两个或两个以上的主控板。要运行 LDP GR 功能，设备上可以只有一个主控板。
- 对 LDP 对等体的要求不同：使用 LDP NSR 功能时，LDP 对等体不会感知本地设备发生了 LDP 进程的异常重启或主备倒换等故障，不需要 LDP 对等体协助恢复 MPLS 转发信息。LDP GR 要求 LDP 对等体能够识别本地设备的 GR 能力标识（即能处理 Initialization 消息中的 GR 相关扩展），并且在 LDP 会话中断恢复时，LDP 对等体能够作为 GR helper 协助本地设备恢复 MPLS 转发信息。

1.1.7 LDP IGP同步

1. 基本工作机制

LDP 基于 IGP 最优路由建立 LSP，LDP 和 IGP 不同步可能导致 MPLS 流量转发中断。LDP 和 IGP 不同步包括如下情况：

- 某条链路 up 后，IGP 通告并使用了这条链路，而此时这条链路上 LDP LSP 尚未建立；
- 当 LDP 会话 down 时，IGP 继续使用这条链路，而此时这条链路上的 LDP LSP 已经拆除；
- 标签分发控制方式为有序方式时，还没有收到下游设备通告的标签映射，尚未建立 LDP LSP，IGP 就已经使用该链路。

启用 LDP IGP 同步功能后，只有 LDP 在某条链路上收敛，IGP 才会为这条链路通告正常的开销值，否则通告链路开销的最大值，使得这条链路在 IGP 拓扑中可见，但是在其它链路可用的情况下，IGP 不会将该链路选为最优路由，从而确保设备收到 MPLS 报文时，不会因为最优路由上的 LDP LSP 没有建立而丢弃 MPLS 报文。

同时满足如下条件时，设备认为 LDP 在某条链路上已收敛：

- 在该链路上本地设备至少与一个对等体建立了 LDP 会话，且该 LDP 会话已进入 operational 状态。

- 在该链路上本地设备至少向一个对等体发送完标签映射。

2. LDP收敛后的延迟通知机制

缺省情况下，LDP 在某条链路上收敛后立即通知 IGP，以便 IGP 发布该链路的正常开销值。但是，在某些情况下，LDP 收敛后立即通知 IGP，可能会导致 MPLS 流量转发中断，例如：

- 对等体的标签分发控制方式为有序方式时，LDP 会话进入 operational 状态后，设备需要等待下游的标签映射。如果尚未收到下游的标签映射就向 IGP 通知 LDP 收敛，则可能导致 MPLS 流量转发中断。
- 下游的标签映射比较多时，如果 LDP 收敛后立即通知 IGP，则下游的标签映射可能尚未通告完成，导致 MPLS 流量转发中断。

在这些情况下，需要配置恰当的延迟通知时间，即 LDP 在某条链路上收敛后，等待延迟时间再通知 IGP，以最大限度地缩短 MPLS 流量中断的时间。

3. LDP协议重启或倒换后的延迟通知机制

LDP 协议重启或倒换后，需要等待一段时间 LDP 才会收敛。如果在协议重启或倒换后，LDP 立即将当前所有的 LDP IGP 同步状态通知给 IGP，在 LDP 收敛后再更新这些状态，则可能会导致 IGP 频繁地根据不同的同步状态进行处理，增加了 IGP 的处理开销。

LDP 协议重启或倒换后的延迟通知机制可以用来解决上述问题。该机制提供了 LDP 进程级别的延迟通知时间，即在 LDP 协议重启或倒换的情况下，等待 LDP 恢复到重启或倒换前的收敛状态后，再批量通知 LDP IGP 同步状态，以减少 IGP 的处理开销。如果到达指定的最大延迟时间时，仍未恢复之前的收敛状态，则立即向 IGP 批量通告当前的 LDP IGP 同步状态。

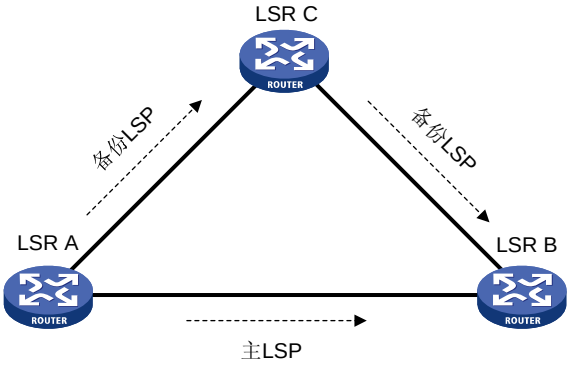
1.1.8 LDP快速重路由

当 MPLS 网络中的链路或某台路由器发生故障时，需要通过故障链路或故障路由器传送才能到达目的地的 MPLS 报文将会丢弃，MPLS 流量转发将会中断，直到 LDP 沿着新的路径建立新的 LDP LSP，被中断的 MPLS 流量才能恢复正常的传送。

LDP 快速重路由功能可用来缩短网络故障导致的 MPLS 流量中断时间。LDP 快速重路由完全基于 IP 快速重路由实现，在 IP 快速重路由使能后，LDP 快速重路由即自动使能。使能 IP 快速重路由有两种实现方式：

- 配置 IGP 协议自动计算备份下一跳
- 配置 IGP 协议通过路由策略指定备份下一跳

图1-6 LDP 快速重路由功能示意图



如 图 1-6 所示，LSR A上使能IP快速重路由功能后，IGP将为路由自动计算或通过路由策略指定备份下一跳，建立主备两条路由，LDP基于主备路由建立主备两条LSP。主LSP正常工作时，MPLS流量通过主LSP转发；当主LSP出现故障时，MPLS流量快速切换到备份LSP，从而缩短网络故障导致的流量中断时间。

通过备份 LSP 转发流量的同时，IGP 会根据变化后的网络拓扑重新计算最优路由，LDP 也会基于该路由建立新的 LSP。LDP LSP 的建立在 IGP 路由收敛之后，如果 LDP 收敛之前 IGP 就采用新的路由，则将导致 MPLS 流量中断。因此在使用 LDP 快速重路由的情况下，建议同时使能 LDP IGP 同步功能，以减少故障发生后 IGP 重新收敛导致的流量中断的时间。

1.1.9 协议规范

与 MPLS 相关的协议规范有：

- RFC 5036：LDP Specification

1.2 LDP配置任务简介

表1-1 LDP 配置任务简介

配置任务		说明	详细配置
使能LDP能力	全局使能LDP能力	必选	1.3.1
	在接口上使能LDP能力	必选	1.3.2
配置Hello消息参数		可选	1.4
配置LDP会话参数		可选	1.5
配置LDP倒退机制的延迟时间		可选	1.6
配置LDP MD5认证		可选	1.7
配置LDP引入BGP IPv4单播路由		可选	1.8
配置LSP触发策略		可选	1.9
配置LDP标签分发控制方式		可选	1.10
配置标签通告控制策略		可选	1.11
配置标签接受控制策略		可选	1.12
配置LDP环路检测		可选	1.13
配置LDP会话保护		可选	1.14
配置LDP GR		可选	1.15
配置LDP NSR		可选	1.16
配置LDP IGP同步		可选	1.17
配置LDP快速重路由		可选	1.18
配置发送的LDP报文的DSCP优先级		可选	1.19
重启LDP会话		可选	1.20

配置任务	说明	详细配置
开启告警功能	可选	1.21

1.3 使能LDP能力

1.3.1 全局使能LDP能力

表1-2 全局使能 LDP 能力

操作		命令	说明
进入系统视图		**system-view**	-
使能本节点的LDP能力，或使能指定VPN实例的LDP能力	使能本节点的LDP能力，并进入LDP视图	**mpls ldp**	缺省情况下，未使能LDP能力
	使能指定VPN实例的LDP能力，为该VPN创建LDP实例，并进入LDP-VPN实例视图	**mpls ldp**	
		vpn-instance *vpn-instance-name*	
配置LDP的LSR ID		**lsr-id** *lsr-id*	缺省情况下，LDP的LSR ID与MPLS LSR ID相同

1.3.2 在接口上使能LDP能力

表1-3 在接口上使能 LDP 能力

操作	命令	说明
进入系统视图	**system-view**	-
进入需要建立LDP会话的接口视图	**interface** *interface-type interface-number*	如果该接口绑定了VPN实例，则需要在LDP视图下通过**vpn-instance**命令使能指定VPN实例的LDP能力
使能接口的LDP能力	**mpls ldp enable**	缺省情况下，在接口上未使能LDP能力

1.4 配置Hello消息参数

LDP 的 Hello 消息分为以下几种：

- 用于发现直连邻居的 Link hello 消息
- 用于发现非直连邻居的 Targeted hello 消息

Hello 消息参数包括：

- Link hello 保持时间和报文发送时间间隔
- Targeted hello 保持时间和报文发送时间间隔

表1-4 配置 Link hello 消息参数

操作	命令	说明
进入系统视图	**system-view**	-
进入建立LDP会话的接口视图	**interface** *interface-type interface-number*	-
配置Link hello保持时间	**mpls ldp timer hello-hold** *timeout*	缺省情况下，Link hello保持时间为15秒
配置Link hello报文发送时间间隔	**mpls ldp timer hello-interval** *interval*	缺省情况下，Link hello报文发送时间间隔为5秒

表1-5 配置 Targeted hello 消息参数

操作	命令	说明
进入系统视图	**system-view**	-
进入LDP视图	**mpls ldp**	-
配置主动向指定对等体发送Targeted hello消息来建立LDP会话，允许应答指定对等体的Targeted hello消息，并进入LDP对等体视图	**targeted-peer** *peer-lsr-id*	缺省情况下，设备不会主动向对等体发送Targeted hello消息，也不会应答对等体的Targeted hello消息
配置Targeted hello保持时间	**mpls ldp timer hello-hold** *timeout*	缺省情况下，Targeted hello保持时间为45秒
配置Targeted hello报文发送时间间隔	**mpls ldp timer hello-interval** *interval*	缺省情况下，Targeted hello报文发送时间间隔为15秒

1.5 配置LDP会话参数

可以通过配置修改如下 LDP 会话参数：

- Keepalive 保持时间和报文发送时间间隔。
- LDP 传输地址，即用来建立 TCP 连接的 IP 地址。

LDP可以通过基本发现和扩展发现两种机制来发现LSR邻居。LSR与通过基本发现机制发现的LSR邻居建立LDP会话时，采用的LDP会话参数配置方法如 表 1-6 所示；LSR与通过扩展发现机制发现的LSR邻居建立LDP会话时，采用的LDP会话参数配置方法如 表 1-7 所示。

配置 LDP 会话参数时，需要注意：

- 配置的 LDP 传输地址应为设备上处于 up 状态的接口的 IP 地址，否则 LDP 会话将无法建立。
- 两端 LSR 的 LDP 传输地址必须路由可达。否则，无法建立 TCP 连接。

表1-6 配置基本发现机制的 LDP 会话参数

操作	命令	说明
进入系统视图	**system-view**	-
进入建立LDP会话的接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
配置Keepalive保持时间	**mpls ldp timer keepalive-hold** *timeout*	缺省情况下，Keepalive保持时间为45秒
配置Keepalive报文发送时间间隔	**mpls ldp timer keepalive-interval** *interval*	缺省情况下，Keepalive报文发送时间间隔为15秒
配置LDP传输地址	**mpls ldp transport-address** { *ip-address* | **interface** }	缺省情况下，如果建立LDP会话的接口属于公网，则传输地址是本LSR的LSR ID；如果该接口属于某个VPN，则传输地址是本接口的主IP地址 如果建立LDP会话的接口与某个VPN实例绑定，则本命令指定的接口或指定的传输地址所在的接口需要与同一个VPN实例绑定

表1-7 配置扩展发现机制的 LDP 会话参数

操作	命令	说明
进入系统视图	**system-view**	-
进入LDP视图	**mpls ldp**	-
配置主动向指定对等体发送Targeted hello消息来建立LDP会话，允许应答指定对等体的Targeted hello消息，并进入LDP对等体视图	**targeted-peer** *peer-lsr-id*	缺省情况下，设备不会主动向对等体发送Targeted hello消息，也不会应答对等体的Targeted hello消息
配置Keepalive保持时间	**mpls ldp timer keepalive-hold** *timeout*	缺省情况下，Keepalive保持时间为45秒
配置Keepalive报文发送时间间隔	**mpls ldp timer keepalive-interval** *interval*	缺省情况下，Keepalive报文发送时间间隔为15秒
配置LDP传输地址	**mpls ldp transport-address** *ip-address*	缺省情况下，传输地址是本LSR的LSR ID

1.6 配置LDP倒退机制的延迟时间

如果 LDP 对等体上配置的 LDP 会话参数不兼容（如 LDP 对等体使用的标签通告方式不同），则会导致会话参数协商失败、LDP 对等体无休止地反复尝试建立会话。

LDP 倒退机制用来抑制尝试建立会话的频率。如果会话因为参数不兼容而建立失败，LSR 将等待初始延迟时间再尝试建立会话；如果会话再次因为参数不兼容而建立失败，则再次尝试建立会话的延迟时间为上一次延迟时间× 2；延迟时间达到配置的最大值后，尝试建立会话的等待时间将保持为配置的最大延迟。

表1-8 配置 LDP 倒退机制的延迟时间

操作	命令	说明
进入系统视图	**system-view**	-

操作		命令	说明
进入LDP视图或LDP-VPN实例视图	进入LDP视图	**mpls ldp**	-
	进入LDP-VPN实例视图	**mpls ldp**	
		vpn-instance *vpn-instance-name*	
配置LDP倒退机制的初始延迟和最大延迟		**backoff initial** *initial-time* **maximum** *maximum-time*	缺省情况下，LDP倒退机制的初始延迟为15秒，最大延迟为120秒

1.7 配置LDP MD5认证

为了提高 LDP 会话的安全性，可以配置在 LDP 会话使用的 TCP 连接上采用 MD5 认证，来验证 LDP 消息的完整性。

要想在 LDP 对等体之间成功建立 LDP 会话，必须保证 LDP 对等体上的 LDP MD5 认证配置一致。

表1-9 配置 LDP MD5 认证

操作		命令	说明
进入系统视图		**system-view**	-
进入LDP视图或LDP-VPN实例视图	进入LDP视图	**mpls ldp**	-
	进入LDP-VPN实例视图	**mpls ldp**	
		vpn-instance *vpn-instance-name*	
使能LDP的MD5认证功能		**md5-authentication** *peer-lsr-id* { **cipher** | **plain** } *password*	缺省情况下，未使能LDP的MD5认证功能

1.8 配置LDP引入BGP IPv4单播路由

在设备上使能 LDP 协议后，LDP 可将设备上的路由表项引入至 LDP 中，为其分配标签，建立 LSP。缺省情况下，LDP 自动引入 IGP 路由和已引入至 IGP 中的 BGP 路由。在某些应用场景下，如果未配置 OSPF、ISIS 等 IGP 协议，则 BGP 路由无法自动引入 LDP，即无法为其分配标签。

通过配置 LDP 引入 BGP IPv4 单播路由，可使 LDP 引入 BGP IPv4 单播路由，以便为其分配标签。如在运营商的运营商组网中，如果一级运营商的 PE 与二级运营商 CE 之间未配置 OSPF、IS-IS 等 IGP 协议，则需在该 PE 和 CE 上配置 LDP 引入 BGP IPv4 单播路由功能，使 LDP 引入 BGP IPv4 单播路由，以便为其分配标签并建立 LSP。有关运营商的运营商组网的详细信息，请参见“MPLS 配置指导”中的“MPLS L3VPN”。

表1-10 配置 LDP 引入 BGP IPv4 单播路由

操作		命令	说明
进入系统视图		**system-view**	-
进入LDP视图或LDP-VPN实例	进入LDP视图	**mpls ldp**	-
	进入LDP-VPN	**mpls ldp**	

操作		命令	说明
视图	实例视图	**vpn-instance** *vpn-instance-name*	
使能LDP引入BGP IPv4单播路由功能		**import bgp**	缺省情况下，未使能LDP引入BGP IPv4单播路由功能

1.9 配置LSP触发策略

使能 LDP 后，LDP 可将路由表项中的路由引入至 LDP，并根据其目的网络地址划分 FEC。在 LSR 上配置 LSP 触发策略，可以限制哪些引入到 LDP 的路由表项能够触发 LDP 为其目的网络地址分配标签并建立 LSP，从而控制 LSP 的数量，避免 LSP 数量过多导致设备运行不稳定。

对于引入到 LDP 的路由表项，LSP 触发策略包括：

- 所有路由表项都会触发 LDP 建立 LSP。
- 利用 IP 地址前缀列表对路由表项进行过滤，被 IP 地址前缀列表拒绝的路由表项不能触发建立 LSP。采用这种 LSP 触发策略时，需要创建 IP 地址前缀列表，创建方法请参见“三层技术-IP 路由配置指导”中的“路由策略”。
- 只有 32 位掩码的主机路由能够触发 LDP 建立 LSP。

缺省情况下，只有 32 位掩码的主机路由能够触发 LDP 建立 LSP。在非必要的情况下，建议用户不要随意修改 LSP 触发策略，以免建立过多的 LSP，占用系统和网络资源。

表1-11 配置 LSP 触发策略

操作		命令	说明
进入系统视图		**system-view**	-
进入LDP视图或LDP-VPN实例视图	进入LDP视图	**mpls ldp**	-
	进入LDP-VPN实例视图	**mpls ldp**	
		vpn-instance *vpn-instance-name*	
配置LSP的触发策略		**lsp-trigger** { **all** | **prefix-list** *prefix-list-name* }	缺省情况下，只有引入到LDP的32位掩码的主机路由能够触发LDP建立LSP

1.10 配置LDP标签分发控制方式

表1-12 配置 LDP 标签分配控制方式

操作		命令	说明
进入系统视图		**system-view**	-
进入LDP视图或LDP-VPN实例视图	进入LDP视图	**mpls ldp**	-
	进入LDP-VPN实例视图	**mpls ldp**	
		vpn-instance *vpn-instance-name*	

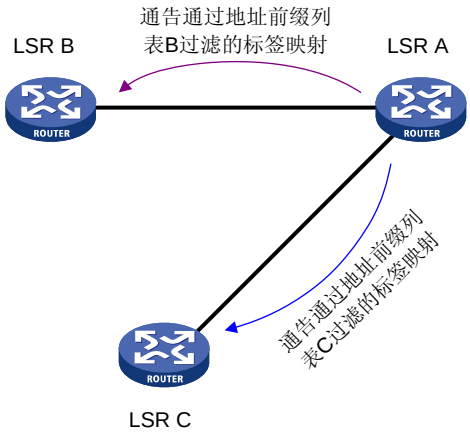
操作	命令	说明
配置标签分发控制方式	**label-distribution { independent | ordered }**	缺省情况下，标签分发控制方式为有序方式（**ordered**） 会话建立后，需重启LDP会话，本命令的配置才能生效

1.11 配置标签通告控制策略

标签通告控制用来控制向哪些对等体通告哪些 FEC—标签映射，即 LSR 只将指定地址前缀的标签映射通告给指定的对等体。在复杂的 MPLS 网络环境中，通过标签通告控制可以规划动态建立的 LSP，并避免设备通告大量的标签映射。

如 图 1-7，LSR A将FEC目的地址通过地址前缀列表B过滤的FEC—标签映射通告给LSR B；将FEC目的地址通过地址前缀列表C过滤的FEC—标签映射通告给LSR C。

图1-7 标签通告控制示意图



在下游 LSR 上配置标签通告控制策略与在上游 LSR 上配置标签接受控制策略具有相同的效果。如果下游 LSR 支持配置标签通告控制策略，则推荐使用标签通告控制策略，以减轻网络负担。

在配置 LDP 标签通告控制策略时，需要创建 IP 地址前缀列表，创建方法请参见“三层技术-IP 路由配置指导”中的“路由策略”。

表1-13 配置 LDP 标签通告控制策略

操作		命令	说明
进入系统视图		**system-view**	-
进入LDP视图或LDP-VPN实例视图	进入LDP视图	**mpls ldp**	-
	进入LDP-VPN实例视图	**mpls ldp**	
		vpn-instance *vpn-instance-name*	

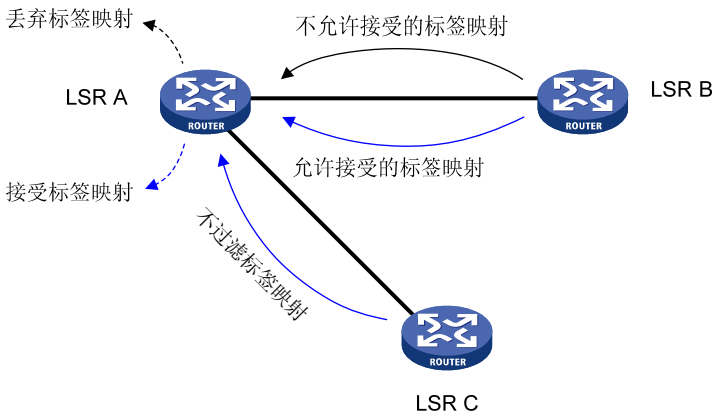
操作	命令	说明
配置标签通告控制策略	**advertise-label prefix-list** *prefix-list-name* [**peer** *peer-prefix-list-name*]	缺省情况下，未配置标签通告控制策略，即向所有对等体通告满足LSP触发策略的所有IP地址前缀的标签映射

1.12 配置标签接受控制策略

标签接受控制用来实现对从指定对等体接收的 FEC—标签映射进行过滤，只接受指定地址前缀的FEC—标签映射。在复杂的 MPLS 网络环境中，通过标签接受控制可以规划动态建立的 LSP，并避免设备保存大量的标签映射。

如 图 1-8，LSR A对LSR B通告的FEC—标签映射进行过滤，只有FEC的目的地址通过指定地址前缀列表过滤后，才会接受该FEC—标签映射；对LSR C通告的标签不进行过滤。

图1-8 标签接受控制示意图



在下游 LSR 上配置标签通告控制策略与在上游 LSR 上配置标签接受控制策略具有相同的效果。如果下游 LSR 支持配置标签通告控制策略，则推荐使用标签通告控制策略，以减轻网络负担。

在配置 LDP 标签接受控制策略时，需要创建 IP 地址前缀列表，创建方法请参见“三层技术-IP 路由配置指导”中的“路由策略”。

表1-14 配置 LDP 标签接受控制策略

操作		命令	说明
进入系统视图		**system-view**	-
进入LDP视图或LDP-VPN实例视图	进入LDP视图	**mpls ldp**	-
	进入LDP-VPN实例视图	**mpls ldp**	
		vpn-instance *vpn-instance-name*	
配置标签接受控制策略		**accept-label peer** *peer-lsr-id* **prefix-list** *prefix-list-name*	缺省情况下，未配置标签接受控制策略，接受来自所有对等体的所有IP地址前缀的标签映射

1.13 配置LDP环路检测

提示

环路检测机制用于非 TTL 递减设备（如标签控制的 ATM 交换机）组成的网络。支持 TTL 递减的设备上启动 LDP 环路检测功能没有实际用途,还会因为频繁发送标签请求或标签映射消息来更新环路检测的路径向量或跳数，而产生额外处理开销。因此，不推荐用户使用环路检测功能。

LDP 环路检测机制可以检测 LSP 环路，并避免在 MPLS 网络中发生环路。

LDP 环路检测有两种方式：

(1) 最大跳数

在传递标签映射（或者标签请求）的消息中包含跳数信息，每经过一跳该值就加一。当该值达到规定的最大值时即认为出现环路，终止 LSP 的建立过程。

(2) 路径向量

在传递标签映射（或者标签请求）的消息中记录路径信息，每经过一跳，相应的设备就检查自己的 LSR ID 是否在此记录中。如果记录中没有自身的 LSR ID，就会将自身的 LSR ID 添加到该记录中；如果记录中已有本 LSR 的记录，则认为出现环路，终止 LSP 的建立过程。

采用路径向量方式进行环路检测时，也需要规定 LSP 路径的最大跳数，当路径的跳数达到配置的最大值时，也会认为出现环路，终止 LSP 的建立过程。

表1-15 配置 LDP 环路检测

操作		命令	说明
进入系统视图		**system-view**	-
进入LDP视图或LDP-VPN实例视图	进入LDP视图	**mpls ldp**	-
	进入LDP-VPN实例视图	**mpls ldp**	
		vpn-instance *vpn-instance-name*	
开启环路检测功能		**loop-detect**	缺省情况下，环路检测功能处于关闭状态 开启环路检测功能后，将同时使用最大跳数和路径向量两种方法检测环路
配置最大跳数环路检测方式下LSP的最大跳数		**maxhops** *hop-number*	缺省情况下，最大跳数环路检测方式下LSP的最大跳数为32
配置路径向量环路检测方式下LSP的最大跳数		**pv-limit** *pv-number*	缺省情况下，路径向量环路检测方式下LSP的最大跳数为32

1.14 配置LDP会话保护

会话保护功能实现了基本发现机制失效时，利用扩展发现机制来保持与对等体的会话，确保基本发现机制恢复时，LDP 协议能够快速收敛。会话保护功能主要应用在 LDP 对等体之间存在直连和非直连多条路径的组网环境中。

使能与指定对等体的会话保护功能后，如果通过 Link hello 消息发现了该直连的 LDP 对等体，则本地 LSR 不仅与其建立 Link hello 邻接关系，还会向该对等体发送 Targeted hello 消息，与其建立 Targeted hello 邻接关系。当直连链路出现故障时，Link hello 邻接关系将被删除。如果此时非直连链路正常工作，则 Targeted hello 邻接关系依然存在，因此，LDP 会话不会被删除，基于该会话的 FEC—标签映射等信息也不会删除。直连链路恢复后，不需要重新建立 LDP 会话、重新学习 FEC—标签映射等信息，从而加快了 LDP 收敛速度。

使能会话保护功能时，还可以指定会话保护持续时间，即 Link hello 邻接关系被删除后，用 Targeted hello 邻接关系继续保持会话的时间。如果在会话保护持续时间内，Link hello 邻接关系没有恢复，则删除 Targeted hello 邻接关系，对应的 LDP 会话也将被删除。如果未指定会话保护持续时间，则用 Targeted hello 邻接关系永久保持会话。

表1-16 配置 LDP 会话保护

操作	命令	说明
进入系统视图	**system-view**	-
进入LDP视图	**mpls ldp**	-
使能会话保护功能	**session protection** [**duration** *time*] [**peer** *peer-prefix-list-name*]	缺省情况下，未使能会话保护功能

1.15 配置LDP GR

配置 LDP GR 之前，需要在作为 GR restarter 和作为 GR helper 的设备上均配置 LDP 能力。

表1-17 配置 LDP GR

操作	命令	说明
进入系统视图	**system-view**	-
进入LDP视图	**mpls ldp**	-
使能LDP协议的GR能力	**graceful-restart**	缺省情况下，LDP协议的GR能力处于关闭状态
配置GR重连超时时间	**graceful-restart timer reconnect** *reconnect-time*	缺省情况下，GR重连超时时间为120秒
配置GR转发状态保持定时器的值	**graceful-restart timer forwarding-hold** *hold-time*	缺省情况下，GR转发状态保持定时器的值为180秒

1.16 配置LDP NSR

MSR 系列路由器各款型对于本节所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR 2600	LDP NSR	不支持
MSR 3600		不支持
MSR 5600		支持

表1-18 配置 LDP NSR

操作	命令	说明
进入系统视图	**system-view**	-
进入LDP视图	**mpls ldp**	-
使能LDP NSR功能	**non-stop-routing**	缺省情况下，LDP NSR功能处于关闭状态

1.17 配置LDP IGP同步

在 OSPF 进程、OSPF 区域或 IS-IS 进程下使能 LDP IGP 同步功能后，所有属于该 OSPF 进程、OSPF 区域或 IS-IS 进程的接口上都会自动使能 LDP IGP 同步功能。用户可以根据实际需要，在某个接口上禁止 LDP IGP 同步功能。

1.17.1 配置LDP OSPF同步

执行 **ospf** 命令时，如果通过 **vpn-instance** *vpn-instance-name* 参数指定了 OSPF 进程所属的 VPN 实例，则该 OSPF 进程下、该进程的 OSPF 区域下不能配置 LDP IGP 同步功能。

表1-19 在 OSPF 进程下配置 LDP OSPF 同步

操作	命令	说明
进入系统视图	**system-view**	-
进入OSPF视图	**ospf** [*process-id* | **router-id** *router-id*] *	-
使能LDP OSPF同步	**mpls ldp sync**	缺省情况下，LDP OSPF同步功能处于关闭状态
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
（可选）在接口上禁止LDP IGP同步功能	**mpls ldp igp sync disable**	缺省情况下，接口允许LDP IGP同步功能，是否具有LDP IGP同步功能由IGP协议的配置决定

操作	命令	说明
退回系统视图	**quit**	-
进入LDP视图	**mpls ldp**	-
（可选）配置向IGP通知LDP已收敛的延迟时间	**igp sync delay** *time*	缺省情况下，LDP收敛后立即通知IGP
（可选）配置在LDP协议重启或倒换后，向IGP通告LDP IGP同步状态的最大延迟时间	**igp sync delay on-restart** *time*	缺省情况下，在LDP协议重启或倒换后，向IGP通告LDP IGP同步状态的最大延迟时间为90秒

表1-20 在 OSPF 区域下配置 LDP OSPF 同步

操作	命令	说明
进入系统视图	**system-view**	-
进入OSPF视图	**ospf** [*process-id* | **router-id** *router-id*] *	-
进入OSPF区域视图	**area** *area-id*	
使能LDP OSPF同步	**mpls ldp sync**	缺省情况下，LDP OSPF同步功能处于关闭状态
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
（可选）在接口上禁止LDP IGP同步功能	**mpls ldp igp sync disable**	缺省情况下，接口允许LDP IGP同步功能，是否具有LDP IGP同步功能由IGP协议的配置决定
退回系统视图	**quit**	-
进入LDP视图	**mpls ldp**	-
（可选）配置向IGP通知LDP已收敛的延迟时间	**igp sync delay** *time*	缺省情况下，LDP收敛后立即通知IGP
（可选）配置在LDP协议重启或倒换后，向IGP通告LDP IGP同步状态的最大延迟时间	**igp sync delay on-restart** *time*	缺省情况下，在LDP协议重启或倒换后，向IGP通告LDP IGP同步状态的最大延迟时间为90秒

1.17.2 配置LDP IS-IS同步

执行 **isis** 命令时，如果通过 **vpn-instance** *vpn-instance-name* 参数指定了 IS-IS 进程所属的 VPN 实例，则该 IS-IS 进程下不能配置 LDP IGP 同步功能。

表1-21 配置 LDP IS-IS 同步

操作	命令	说明
进入系统视图	**system-view**	-
进入IS-IS视图	**isis** [*process-id*]	-

操作	命令	说明
使能LDP IS-IS同步	**mpls ldp sync** [**level-1** | **level-2**]	缺省情况下，LDP IS-IS同步功能处于关闭状态
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
（可选）在接口上禁止LDP IGP同步功能	**mpls ldp igp sync disable**	缺省情况下，接口允许LDP IGP同步功能，是否具有LDP IGP同步功能由IGP协议的配置决定
退回系统视图	**quit**	-
进入LDP视图	**mpls ldp**	-
（可选）配置向IGP通知LDP已收敛的延迟时间	**igp sync delay** *time*	缺省情况下，LDP收敛后立即通知IGP
（可选）配置在LDP协议重启或倒换后，向IGP通告LDP IGP同步状态的最大延迟时间	**igp sync delay on-restart** *time*	缺省情况下，在LDP协议重启或倒换后，向IGP通告LDP IGP同步状态的最大延迟时间为90秒

1.18 配置LDP快速重路由

LDP 快速重路由完全基于 IP 快速重路由实现，在 IP 快速重路由使能后，LDP 快速重路由即自动使能。有关 IP 快速重路由的配置内容请参见“三层技术-IP 路由配置指导”。

1.19 配置发送的LDP报文的DSCP优先级

DSCP（Differentiated Services Code point，差分服务编码点）携带在 IP 报文中的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。通过本配置可以指定发送的 LDP 报文中携带的 DSCP 优先级的取值。

表1-22 配置发送的 LDP 报文的 DSCP 优先级

操作	命令	说明
进入系统视图	**system-view**	-
进入LDP视图	**mpls ldp**	-
配置发送的LDP报文的DSCP优先级	**dscp** *dscp-value*	缺省情况下，发送的LDP报文的DSCP优先级为48

1.20 重启LDP会话

LDP 会话状态为 up 后，修改 LDP 会话参数不会立即生效。此时，需要重启 LDP 会话，重新协商各种参数，建立 LDP 会话，使得修改后的 LDP 会话参数生效。

在用户视图下执行 **reset mpls ldp** 命令可以重启 LDP 会话。

表1-23 重启 LDP 会话

操作	命令
重启LDP会话	**reset mpls ldp** [**vpn-instance** *vpn-instance-name*] [**peer** *peer-id*]

1.21 开启告警功能

开启 LDP 模块的告警功能后，当 LDP 会话状态发生变化时会产生 RFC 3815 中规定的告警信息。生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。

有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

表1-24 开启告警功能

操作	命令	说明
进入系统视图	**system-view**	-
开启LDP模块的告警功能	**snmp-agent trap enable ldp**	缺省情况下，LDP模块的告警功能处于开启状态

1.22 LDP显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 LDP 的运行情况，用户可以通过查看显示信息验证配置的效果。

表1-25 显示 LDP 运行状态

操作	命令
显示LDP发现过程相关信息（MSR 2600/MSR 3600）	**display mpls ldp discovery** [**vpn-instance** *vpn-instance-name*] [**interface** *interface-type interface-number* | **peer** *peer-lsr-id* | **targeted-peer** *peer-lsr-id*] [**verbose**]
显示LDP发现过程相关信息（MSR 5600）	**display mpls ldp discovery** [**vpn-instance** *vpn-instance-name*] [**interface** *interface-type interface-number* | **peer** *peer-lsr-id* | **targeted-peer** *peer-lsr-id*] [**verbose**] [**standby slot** *slot-number*]
显示通过LDP学习到的FEC—标签映射信息（MSR 2600/MSR 3600）	**display mpls ldp fec** [**vpn-instance** *vpn-instance-name*] [*destination-address mask-length* | **summary**]
显示通过LDP学习到的FEC—标签映射信息（MSR 5600）	**display mpls ldp fec** [**vpn-instance** *vpn-instance-name*] [*destination-address mask-length* | **summary**] [**standby slot** *slot-number*]
显示使能了LDP能力的接口的LDP相关信息	**display mpls ldp interface** [**vpn-instance** *vpn-instance-name*] [*interface-type interface-number*]
显示接口的LDP IGP同步信息	**display mpls ldp igp sync** [**interface** *interface-type interface-number*]
显示LDP协议生成的LSP信息，即LDP LSP信息	**display mpls ldp lsp** [**vpn-instance** *vpn-instance-name*] [*destination-address mask-length*]

操作	命令
显示LDP的运行参数	**display mpls ldp parameter** [**vpn-instance** *vpn-instance-name*]
显示LDP对等体和LDP会话信息（MSR 2600/MSR 3600）	**display mpls ldp peer** [**vpn-instance** *vpn-instance-name*] [*peer-lsr-id*] [**verbose**]
显示LDP对等体和LDP会话信息（MSR 5600）	**display mpls ldp peer** [**vpn-instance** *vpn-instance-name*] [*peer-lsr-id*] [**verbose**] [**standby slot** *slot-number*]
显示LDP运行数据汇总信息（MSR 2600/MSR 3600）	**display mpls ldp summary** [**all** | **vpn-instance** *vpn-instance-name*]
显示LDP运行数据汇总信息（MSR 5600）	**display mpls ldp summary** [**all** | **vpn-instance** *vpn-instance-name*] [**standby slot** *slot-number*]

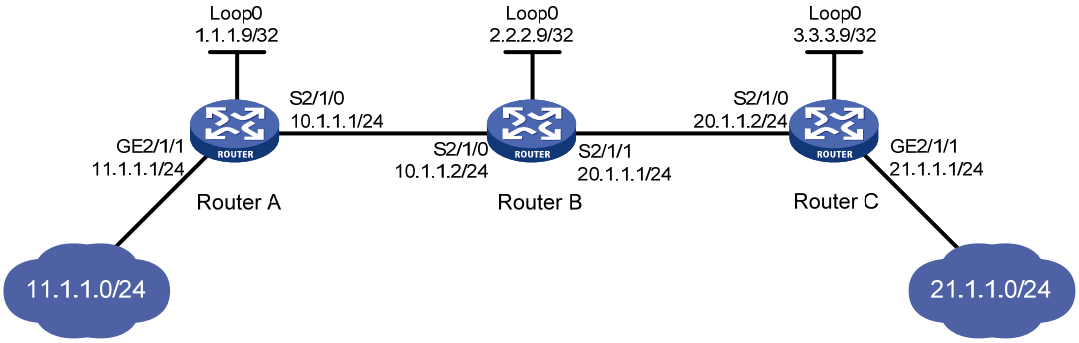
1.23 LDP配置举例

1.23.1 利用LDP动态建立LSP配置举例

1. 组网需求

- Router A、Router B 和 Router C 均支持 MPLS。
- 在 Router A 和 Router C 之间使用 LDP 动态建立 LSP，使 11.1.1.0/24 和 21.1.1.0/24 这两个网段中互访的报文能够通过 MPLS 进行传输。
- Router A、Router B 和 Router C 上只允许目的地址为 1.1.1.9/32、2.2.2.9/32、3.3.3.9/32、11.1.1.0/24 和 21.1.1.0/24 的路由表项触发 LDP 建立 LSP，其他路由表项不能触发 LDP 建立 LSP，以避免建立的 LSP 数量过多，影响设备性能。

图1-9 利用 LDP 动态建立 LSP 配置组网图



2. 配置思路

- LDP 根据路由信息动态分配标签，因此，利用 LDP 动态建立 LSP 时，需要配置路由协议，使得各路由器之间路由可达。本例中，采用的路由协议为 OSPF。
- 在各台路由器上启动 LDP 协议。
- 为了控制建立的 LSP 数量，在 Router A、Router B 和 Router C 上需要配置 LSP 触发策略。

3. 配置步骤

(1) 配置各接口的 IP 地址

按照 图 1-9 配置各接口IP地址和掩码，包括Loopback接口，具体配置过程略。

(2) 配置 OSPF，以保证各路由器之间路由可达

配置 Router A。

```
<RouterA> system-view
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[RouterA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

配置 Router B。

```
<RouterB> system-view
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

配置 Router C。

```
<RouterC> system-view
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[RouterC-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 21.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

配置完成后，在各路由器上执行 **display ip routing-table** 命令，可以看到相互之间都学到了到对方的主机路由。以 Router A 为例：

```
[RouterA] display ip routing-table

Destinations : 21        Routes : 21

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
1.1.1.9/32          Direct 0    0            127.0.0.1       InLoop0
2.2.2.9/32          OSPF   10   1            10.1.1.2        S2/1/0
3.3.3.9/32          OSPF   10   2            10.1.1.2        S2/1/0
10.1.1.0/24         Direct 0    0            10.1.1.1        S2/1/0
10.1.1.0/32         Direct 0    0            10.1.1.1        S2/1/0
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.1.1.255/32       Direct 0    0            10.1.1.1        S2/1/0
```

```
11.1.1.0/24         Direct 0    0           11.1.1.1        GE2/1/1
11.1.1.0/32         Direct 0    0           11.1.1.1        GE2/1/1
11.1.1.1/32         Direct 0    0           127.0.0.1       InLoop0
11.1.1.255/32       Direct 0    0           11.1.1.1        GE2/1/1
20.1.1.0/24         OSPF   10   2           10.1.1.2        S2/1/0
21.1.1.0/24         OSPF   10   3           10.1.1.2        S2/1/0
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
224.0.0.0/4         Direct 0    0           0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0           0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
```

(3) 使能 MPLS 和 LDP 功能

配置 Router A。

```
[RouterA] mpls lsr-id 1.1.1.9
[RouterA] mpls ldp
[RouterA-ldp] quit
[RouterA] interface serial 2/1/0
[RouterA-Serial2/1/0] mpls enable
[RouterA-Serial2/1/0] mpls ldp enable
[RouterA-Serial2/1/0] quit
```

配置 Router B。

```
[RouterB] mpls lsr-id 2.2.2.9
[RouterB] mpls ldp
[RouterB-ldp] quit
[RouterB] interface serial 2/1/0
[RouterB-Serial2/1/0] mpls enable
[RouterB-Serial2/1/0] mpls ldp enable
[RouterB-Serial2/1/0] quit
[RouterB] interface serial 2/1/1
[RouterB-Serial2/1/1] mpls enable
[RouterB-Serial2/1/1] mpls ldp enable
[RouterB-Serial2/1/1] quit
```

配置 Router C。

```
[RouterC] mpls lsr-id 3.3.3.9
[RouterC] mpls ldp
[RouterC-ldp] quit
[RouterC] interface serial 2/1/0
[RouterC-Serial2/1/0] mpls enable
[RouterC-Serial2/1/0] mpls ldp enable
[RouterC-Serial2/1/0] quit
```

(4) 配置 LSP 触发策略

在 Router A 上创建 IP 地址前缀列表 routera，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[RouterA] ip prefix-list routera index 10 permit 1.1.1.9 32
[RouterA] ip prefix-list routera index 20 permit 2.2.2.9 32
```

```
[RouterA] ip prefix-list routera index 30 permit 3.3.3.9 32
[RouterA] ip prefix-list routera index 40 permit 11.1.1.0 24
[RouterA] ip prefix-list routera index 50 permit 21.1.1.0 24
[RouterA] mpls ldp
[RouterA-ldp] lsp-trigger prefix-list routera
[RouterA-ldp] quit
```

在 Router B 上创建 IP 地址前缀列表 routerb，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[RouterB] ip prefix-list routerb index 10 permit 1.1.1.9 32
[RouterB] ip prefix-list routerb index 20 permit 2.2.2.9 32
[RouterB] ip prefix-list routerb index 30 permit 3.3.3.9 32
[RouterB] ip prefix-list routerb index 40 permit 11.1.1.0 24
[RouterB] ip prefix-list routerb index 50 permit 21.1.1.0 24
[RouterB] mpls ldp
[RouterB-ldp] lsp-trigger prefix-list routerb
[RouterB-ldp] quit
```

在 Router C 上创建 IP 地址前缀列表 routerc，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[RouterC] ip prefix-list routerc index 10 permit 1.1.1.9 32
[RouterC] ip prefix-list routerc index 20 permit 2.2.2.9 32
[RouterC] ip prefix-list routerc index 30 permit 3.3.3.9 32
[RouterC] ip prefix-list routerc index 40 permit 11.1.1.0 24
[RouterC] ip prefix-list routerc index 50 permit 21.1.1.0 24
[RouterC] mpls ldp
[RouterC-ldp] lsp-trigger prefix-list routerc
[RouterC-ldp] quit
```

4. 验证配置

配置完成后，在各设备上执行 **display mpls ldp lsp** 命令，可以看到 LDP LSP 的建立情况。以 Router A 为例：

```
[RouterA] display mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup
FECs: 5            Ingress: 3          Transit: 3      Egress: 2

FEC                In/Out Label        Nexthop         OutInterface
1.1.1.9/32         3/-
                   -/1279(L)
2.2.2.9/32         -/3                 10.1.1.2        S2/1/0
                   1279/3              10.1.1.2        S2/1/0
3.3.3.9/32         -/1278              10.1.1.2        S2/1/0
                   1278/1278           10.1.1.2        S2/1/0
11.1.1.0/24        1277/-
                   -/1277(L)
21.1.1.0/24        -/1276              10.1.1.2        S2/1/0
                   1276/1276           10.1.1.2        S2/1/0
```

在 Router A 上检测 Router A 到 Router C 的 LDP LSP 的可达性。

```
[RouterA] ping mpls -a 11.1.1.1 ipv4 21.1.1.0 24
```

```
MPLS Ping FEC: 21.1.1.0/24 : 100 data bytes
100 bytes from 20.1.1.2: Sequence=1 time=1 ms
100 bytes from 20.1.1.2: Sequence=2 time=1 ms
100 bytes from 20.1.1.2: Sequence=3 time=8 ms
100 bytes from 20.1.1.2: Sequence=4 time=2 ms
100 bytes from 20.1.1.2: Sequence=5 time=1 ms

--- FEC: 21.1.1.0/24 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max = 1/2/8 ms
```

在 Router C 上检测 Router C 到 Router A 的 LDP LSP 的可达性。

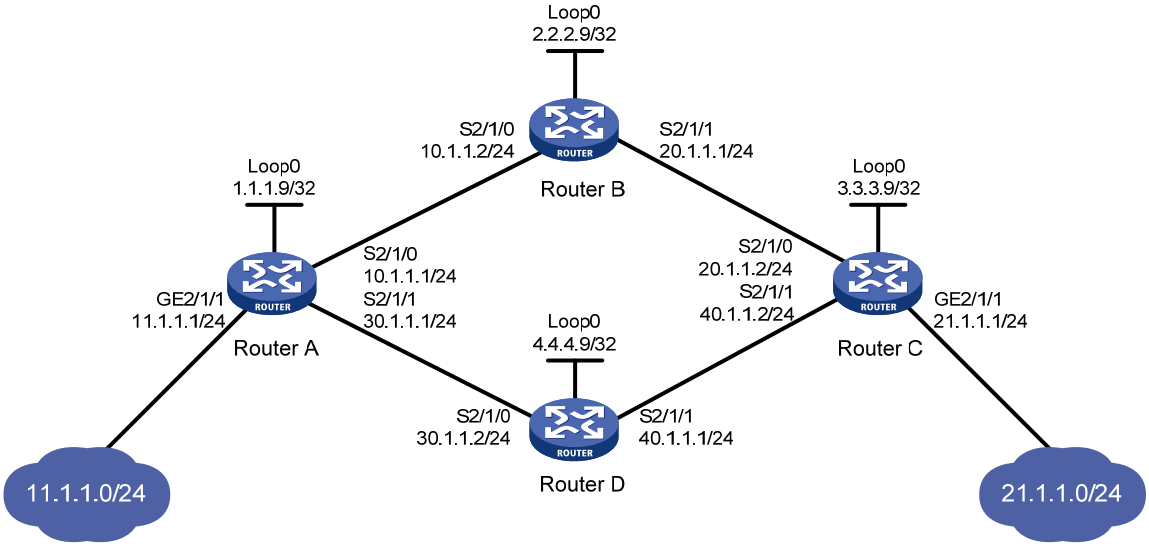
```
[RouterC] ping mpls -a 21.1.1.1 ipv4 11.1.1.0 24
MPLS Ping FEC: 11.1.1.0/24 : 100 data bytes
100 bytes from 10.1.1.1: Sequence=1 time=1 ms
100 bytes from 10.1.1.1: Sequence=2 time=1 ms
100 bytes from 10.1.1.1: Sequence=3 time=1 ms
100 bytes from 10.1.1.1: Sequence=4 time=1 ms
100 bytes from 10.1.1.1: Sequence=5 time=1 ms

--- FEC: 11.1.1.0/24 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max = 1/1/1 ms
```

1.23.2 标签接受控制策略配置举例

1. 组网需求

11.1.1.0/24 和 21.1.1.0/24 网段之间存在两条路径：Router A—Router B—Router C 和 Router A—Router D—Router C。通过配置标签接受控制策略，实现只沿着路径 Router A—Router B—Router C 建立 LSP，11.1.1.0/24 和 21.1.1.0/24 网段之间互访的报文通过该 LSP 进行 MPLS 转发。

图1-10 标签接受控制策略配置组网图



2. 配置思路

(1) 在各台路由器上配置路由协议，使得各路由器之间路由可达。本例中，采用的路由协议为 OSPF。

(2) 在各台路由器上启动 LDP 协议。

(3) 在各台路由器上配置 LSP 触发策略，使得目的地址为 11.1.1.0/24 和 21.1.1.0/24 的路由表项能够触发 LDP 建立 LSP。

(4) 配置标签接受控制策略，使得 LDP 仅沿着路径 Router A—Router B—Router C 建立 LSP。具体配置方法为：

- Router A 只接受 Router B 通告的 FEC 目的地址为 21.1.1.0/24 的 FEC—标签映射；Router A 拒绝 Router D 通告的 FEC 目的地址为 21.1.1.0/24 的 FEC—标签映射。
- Router C 只接受 Router B 通告的 FEC 目的地址为 11.1.1.0/24 的 FEC—标签映射；Router C 拒绝 Router D 通告的 FEC 目的地址为 11.1.1.0/24 的 FEC—标签映射。

3. 配置步骤

(1) 配置各接口的 IP 地址

按照 图 1-10 配置各接口IP地址和掩码，包括Loopback接口，具体配置过程略。

(2) 配置 OSPF

在各台路由器上配置 OSPF，以保证各路由器之间路由可达，具体配置过程略。

(3) 使能 MPLS 和 LDP 功能

配置 Router A。

```
<RouterA> system-view
[RouterA] mpls lsr-id 1.1.1.9
[RouterA] mpls ldp
[RouterA-ldp] quit
[RouterA] interface serial 2/1/0
[RouterA-Serial2/1/0] mpls enable
[RouterA-Serial2/1/0] mpls ldp enable
[RouterA-Serial2/1/0] quit
[RouterA] interface serial 2/1/1
[RouterA-Serial2/1/1] mpls enable
[RouterA-Serial2/1/1] mpls ldp enable
[RouterA-Serial2/1/1] quit
```

配置 Router B。

```
<RouterB> system-view
[RouterB] mpls lsr-id 2.2.2.9
[RouterB] mpls ldp
[RouterB-ldp] quit
[RouterB] interface serial 2/1/0
[RouterB-Serial2/1/0] mpls enable
[RouterB-Serial2/1/0] mpls ldp enable
[RouterB-Serial2/1/0] quit
[RouterB] interface serial 2/1/1
[RouterB-Serial2/1/1] mpls enable
[RouterB-Serial2/1/1] mpls ldp enable
[RouterB-Serial2/1/1] quit
```

配置 Router C。

```
<RouterC> system-view
[RouterC] mpls lsr-id 3.3.3.9
[RouterC] mpls ldp
[RouterC-ldp] quit
[RouterC] interface serial 2/1/0
[RouterC-Serial2/1/0] mpls enable
[RouterC-Serial2/1/0] mpls ldp enable
[RouterC-Serial2/1/0] quit
[RouterC] interface serial 2/1/1
[RouterC-Serial2/1/1] mpls enable
[RouterC-Serial2/1/1] mpls ldp enable
[RouterC-Serial2/1/1] quit
```

配置 Router D。

```
<RouterD> system-view
[RouterD] mpls lsr-id 4.4.4.9
[RouterD] mpls ldp
[RouterD-ldp] quit
[RouterD] interface serial 2/1/0
[RouterD-Serial2/1/0] mpls enable
[RouterD-Serial2/1/0] mpls ldp enable
[RouterD-Serial2/1/0] quit
[RouterD] interface serial 2/1/1
[RouterD-Serial2/1/1] mpls enable
[RouterD-Serial2/1/1] mpls ldp enable
[RouterD-Serial2/1/1] quit
```

(4) 配置 LSP 触发策略

在 Router A 上创建 IP 地址前缀列表 routera，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[RouterA] ip prefix-list routera index 10 permit 11.1.1.0 24
[RouterA] ip prefix-list routera index 20 permit 21.1.1.0 24
[RouterA] mpls ldp
[RouterA-ldp] lsp-trigger prefix-list routera
[RouterA-ldp] quit
```

在 Router B 上创建 IP 地址前缀列表 routerb，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[RouterB] ip prefix-list routerb index 10 permit 11.1.1.0 24
[RouterB] ip prefix-list routerb index 20 permit 21.1.1.0 24
[RouterB] mpls ldp
[RouterB-ldp] lsp-trigger prefix-list routerb
[RouterB-ldp] quit
```

在 Router C 上创建 IP 地址前缀列表 routerc，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[RouterC] ip prefix-list routerc index 10 permit 11.1.1.0 24
[RouterC] ip prefix-list routerc index 20 permit 21.1.1.0 24
[RouterC] mpls ldp
```

```
[RouterC-ldp] lsp-trigger prefix-list routerc
[RouterC-ldp] quit
```

在 Router D 上创建 IP 地址前缀列表 routerd，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[RouterD] ip prefix-list routerd index 10 permit 11.1.1.0 24
[RouterD] ip prefix-list routerd index 20 permit 21.1.1.0 24
[RouterD] mpls ldp
[RouterD-ldp] lsp-trigger prefix-list routerd
[RouterD-ldp] quit
```

(5) 配置标签接受控制策略

在 Router A 上创建允许 21.1.1.0/24 通过的 IP 地址前缀列表 prefix-from-b，该列表用来过滤 Router B 通告给 Router A 的 FEC—标签映射。

```
[RouterA] ip prefix-list prefix-from-b index 10 permit 21.1.1.0 24
```

在 Router A 上创建拒绝 21.1.1.0/24 通过的 IP 地址前缀列表 prefix-from-d，该列表用来过滤 Router D 通告给 Router A 的 FEC—标签映射。

```
[RouterA] ip prefix-list prefix-from-d index 10 deny 21.1.1.0 24
```

在 Router A 上配置过滤 Router B 和 Router D 通告的 FEC—标签映射的标签接受控制策略。

```
[RouterA] mpls ldp
[RouterA-ldp] accept-label peer 2.2.2.9 prefix-list prefix-from-b
[RouterA-ldp] accept-label peer 4.4.4.9 prefix-list prefix-from-d
[RouterA-ldp] quit
```

在 Router C 上创建允许 11.1.1.0/24 通过的 IP 地址前缀列表 prefix-from-b，该列表用来过滤 Router B 通告给 Router C 的 FEC—标签映射。

```
[RouterC] ip prefix-list prefix-from-b index 10 permit 11.1.1.0 24
```

在 Router C 上创建拒绝 11.1.1.0/24 通过的 IP 地址前缀列表 prefix-from-d，该列表用来过滤 Router D 通告给 Router C 的 FEC—标签映射。

```
[RouterC] ip prefix-list prefix-from-d index 10 deny 11.1.1.0 24
```

在 Router C 上配置过滤 Router B 和 Router D 通告的 FEC—标签映射的标签接受控制策略。

```
[RouterC] mpls ldp
[RouterC-ldp] accept-label peer 2.2.2.9 prefix-list prefix-from-b
[RouterC-ldp] accept-label peer 4.4.4.9 prefix-list prefix-from-d
[RouterC-ldp] quit
```

4. 验证配置

配置完成后，在各设备上执行 **display mpls ldp lsp** 命令，可以看到 LDP LSP 的建立情况。以 Router A 为例，在 Router A 上 FEC 目的地址为 21.1.1.0/24 的 LSP 的下一跳为 Router B（地址为 10.1.1.2），即只沿着路径 Router A—Router B—Router C 建立了 LSP，路径 Router A—Router D—Router C 上未建立 LSP。

```
[RouterA] display mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup
FECs: 2           Ingress: 1          Transit 1       Egress: 1

FEC               In/Out Label        Nexthop         OutInterface
11.1.1.0/24       1277/-
                  -/1148(L)
```

```
21.1.1.0/24        -/1149(L)
                   -/1276              10.1.1.2        S2/1/0
                   1276/1276           10.1.1.2        S2/1/0
```

在 Router A 上检测 Router A 到 Router C 的 LDP LSP 的可达性。

```
[RouterA] ping mpls -a 11.1.1.1 ipv4 21.1.1.0 24
MPLS Ping FEC: 21.1.1.0/24 : 100 data bytes
100 bytes from 20.1.1.2: Sequence=1 time=1 ms
100 bytes from 20.1.1.2: Sequence=2 time=1 ms
100 bytes from 20.1.1.2: Sequence=3 time=8 ms
100 bytes from 20.1.1.2: Sequence=4 time=2 ms
100 bytes from 20.1.1.2: Sequence=5 time=1 ms

--- FEC: 21.1.1.0/24 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max = 1/2/8 ms
```

在 Router C 上检测 Router C 到 Router A 的 LDP LSP 的可达性。

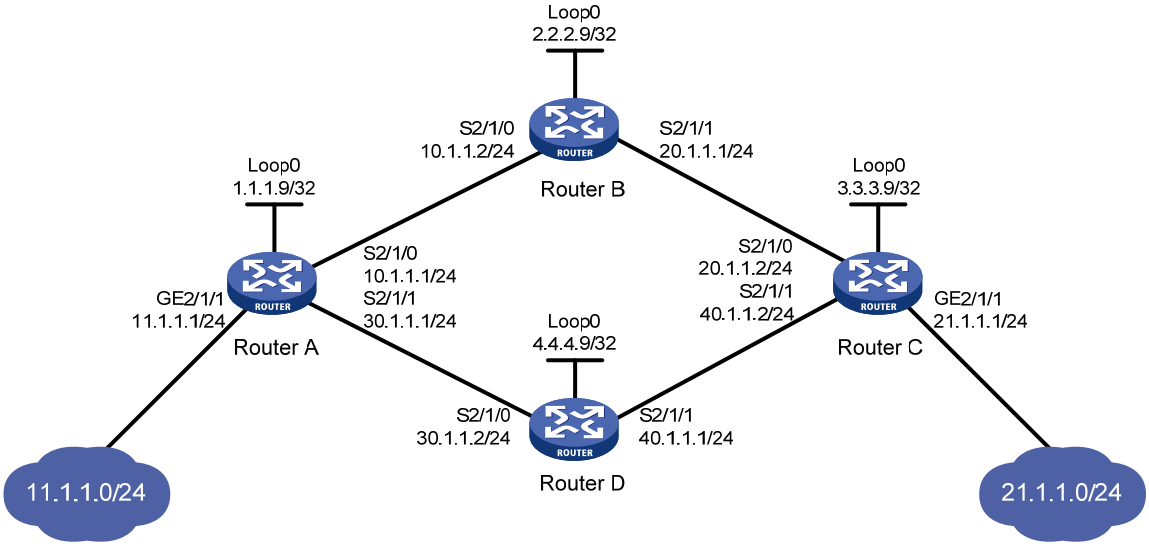
```
[RouterC] ping mpls -a 21.1.1.1 ipv4 11.1.1.0 24
MPLS Ping FEC: 11.1.1.0/24 : 100 data bytes
100 bytes from 10.1.1.1: Sequence=1 time=1 ms
100 bytes from 10.1.1.1: Sequence=2 time=1 ms
100 bytes from 10.1.1.1: Sequence=3 time=1 ms
100 bytes from 10.1.1.1: Sequence=4 time=1 ms
100 bytes from 10.1.1.1: Sequence=5 time=1 ms

--- FEC: 11.1.1.0/24 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max = 1/1/1 ms
```

1.23.3 标签通告控制策略配置举例

1. 组网需求

11.1.1.0/24 和 21.1.1.0/24 网段之间存在两条路径：Router A—Router B—Router C 和 Router A—Router D—Router C。通过配置标签通告控制策略，实现只沿着路径 Router A—Router B—Router C 建立 LSP，11.1.1.0/24 和 21.1.1.0/24 网段之间互访的报文通过该 LSP 进行 MPLS 转发。

图1-11 标签通告控制策略配置组网图



2. 配置思路

(1) 在各台路由器上配置路由协议，使得各路由器之间路由可达。本例中，采用的路由协议为 OSPF。

(2) 在各台路由器上启动 LDP 协议。

(3) 在各台路由器上配置 LSP 触发策略，使得目的地址为 11.1.1.0/24 和 21.1.1.0/24 的路由表项能够触发 LDP 建立 LSP。

(4) 配置标签通告控制策略，使得 LDP 仅沿着路径 Router A—Router B—Router C 建立 LSP。具体配置方法为：

- Router A 只将 FEC 目的地址为 11.1.1.0/24 的 FEC—标签映射通告给 Router B；Router A 不通告任何其他的 FEC—标签映射。
- Router C 只将 FEC 目的地址为 21.1.1.0/24 的 FEC—标签映射通告给 Router B；Router C 不通告任何其他的 FEC—标签映射。
- Router D 不将 FEC 目的地址为 21.1.1.0/24 的 FEC—标签映射通告给 Router A；Router D 不将 FEC 目的地址为 11.1.1.0/24 的 FEC—标签映射通告给 Router C。

3. 配置步骤

(1) 配置各接口的 IP 地址

按照 图 1-11 配置各接口IP地址和掩码，包括Loopback接口，具体配置过程略。

(2) 配置 OSPF

在各台路由器上配置 OSPF，以保证各路由器之间路由可达，具体配置过程略。

(3) 使能 MPLS 和 LDP 功能

配置 Router A。

```
<RouterA> system-view
[RouterA] mpls lsr-id 1.1.1.9
[RouterA] mpls ldp
[RouterA-ldp] quit
[RouterA] interface serial 2/1/0
[RouterA-Serial2/1/0] mpls enable
```

```
[RouterA-Serial2/1/0] mpls ldp enable
[RouterA-Serial2/1/0] quit
[RouterA] interface serial 2/1/1
[RouterA-Serial2/1/1] mpls enable
[RouterA-Serial2/1/1] mpls ldp enable
[RouterA-Serial2/1/1] quit
```

配置 Router B。

```
<RouterB> system-view
[RouterB] mpls lsr-id 2.2.2.9
[RouterB] mpls ldp
[RouterB-ldp] quit
[RouterB] interface serial 2/1/0
[RouterB-Serial2/1/0] mpls enable
[RouterB-Serial2/1/0] mpls ldp enable
[RouterB-Serial2/1/0] quit
[RouterB] interface serial 2/1/1
[RouterB-Serial2/1/1] mpls enable
[RouterB-Serial2/1/1] mpls ldp enable
[RouterB-Serial2/1/1] quit
```

配置 Router C。

```
<RouterC> system-view
[RouterC] mpls lsr-id 3.3.3.9
[RouterC] mpls ldp
[RouterC-ldp] quit
[RouterC] interface serial 2/1/0
[RouterC-Serial2/1/0] mpls enable
[RouterC-Serial2/1/0] mpls ldp enable
[RouterC-Serial2/1/0] quit
[RouterC] interface serial 2/1/1
[RouterC-Serial2/1/1] mpls enable
[RouterC-Serial2/1/1] mpls ldp enable
[RouterC-Serial2/1/1] quit
```

配置 Router D。

```
<RouterD> system-view
[RouterD] mpls lsr-id 4.4.4.9
[RouterD] mpls ldp
[RouterD-ldp] quit
[RouterD] interface serial 2/1/0
[RouterD-Serial2/1/0] mpls enable
[RouterD-Serial2/1/0] mpls ldp enable
[RouterD-Serial2/1/0] quit
[RouterD] interface serial 2/1/1
[RouterD-Serial2/1/1] mpls enable
[RouterD-Serial2/1/1] mpls ldp enable
[RouterD-Serial2/1/1] quit
```

(4) 配置 LSP 触发策略

在 Router A 上创建 IP 地址前缀列表 routera，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[RouterA] ip prefix-list routera index 10 permit 11.1.1.0 24
[RouterA] ip prefix-list routera index 20 permit 21.1.1.0 24
[RouterA] mpls ldp
[RouterA-ldp] lsp-trigger prefix-list routera
[RouterA-ldp] quit
```

在 Router B 上创建 IP 地址前缀列表 routerb，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[RouterB] ip prefix-list routerb index 10 permit 11.1.1.0 24
[RouterB] ip prefix-list routerb index 20 permit 21.1.1.0 24
[RouterB] mpls ldp
[RouterB-ldp] lsp-trigger prefix-list routerb
[RouterB-ldp] quit
```

在 Router C 上创建 IP 地址前缀列表 routerc，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[RouterC] ip prefix-list routerc index 10 permit 11.1.1.0 24
[RouterC] ip prefix-list routerc index 20 permit 21.1.1.0 24
[RouterC] mpls ldp
[RouterC-ldp] lsp-trigger prefix-list routerc
[RouterC-ldp] quit
```

在 Router D 上创建 IP 地址前缀列表 routerd，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[RouterD] ip prefix-list routerd index 10 permit 11.1.1.0 24
[RouterD] ip prefix-list routerd index 20 permit 21.1.1.0 24
[RouterD] mpls ldp
[RouterD-ldp] lsp-trigger prefix-list routerd
[RouterD-ldp] quit
```

(5) 配置标签通告控制策略

在 Router A 上创建允许 11.1.1.0/24 通过的 IP 地址前缀列表 prefix-to-b，该列表用来过滤通告给 Router B 的 FEC—标签映射。

```
[RouterA] ip prefix-list prefix-to-b index 10 permit 11.1.1.0 24
```

在 Router A 上创建允许 2.2.2.9/32 通过的 IP 地址前缀列表 peer-b，该列表用来过滤 LDP 对等体。

```
[RouterA] ip prefix-list peer-b index 10 permit 2.2.2.9 32
```

在 Router A 上配置标签通告控制策略：只将 FEC 目的地址为 11.1.1.0/24 的 FEC—标签映射通告给 Router B。

```
[RouterA] mpls ldp
[RouterA-ldp] advertise-label prefix-list prefix-to-b peer peer-b
[RouterA-ldp] quit
```

在 Router C 上创建允许 21.1.1.0/24 通过的 IP 地址前缀列表 prefix-to-b，该列表用来过滤通告给 Router B 的 FEC—标签映射。

```
[RouterC] ip prefix-list prefix-to-b index 10 permit 21.1.1.0 24
```

在 Router C 上创建允许 2.2.2.9/32 通过的 IP 地址前缀列表 peer-b，该列表用来过滤 LDP 对等体。

```
[RouterC] ip prefix-list peer-b index 10 permit 2.2.2.9 32
```

在 Router C 上配置标签通告控制策略：只将 FEC 目的地址为 21.1.1.0/24 的 FEC—标签映射通告给 Router B。

```
[RouterC] mpls ldp
[RouterC-ldp] advertise-label prefix-list prefix-to-b peer peer-b
[RouterC-ldp] quit
```

在 Router D 上创建拒绝 21.1.1.0/24 通过的 IP 地址前缀列表 prefix-to-a，该列表用来过滤通告给 Router A 的 FEC—标签映射。

```
[RouterD] ip prefix-list prefix-to-a index 10 deny 21.1.1.0 24
[RouterD] ip prefix-list prefix-to-a index 20 permit 0.0.0.0 0 less-equal 32
```

在 Router D 上创建允许 1.1.1.9/32 通过的 IP 地址前缀列表 peer-a，该列表用来过滤 LDP 对等体。

```
[RouterD] ip prefix-list peer-a index 10 permit 1.1.1.9 32
```

在 Router D 上创建拒绝 11.1.1.0/24 通过的 IP 地址前缀列表 prefix-to-c，该列表用来过滤通告给 Router C 的 FEC—标签映射。

```
[RouterD] ip prefix-list prefix-to-c index 10 deny 11.1.1.0 24
[RouterD] ip prefix-list prefix-to-c index 20 permit 0.0.0.0 0 less-equal 32
```

在 Router D 上创建允许 3.3.3.9/32 通过的 IP 地址前缀列表 peer-c，该列表用来过滤 LDP 对等体。

```
[RouterD] ip prefix-list peer-c index 10 permit 3.3.3.9 32
```

在 Router D 上配置标签通告控制策略：不将 FEC 目的地址为 21.1.1.0/24 的 FEC—标签映射通告给 Router A；不将 FEC 目的地址为 11.1.1.0/24 的 FEC—标签映射通告给 Router C。

```
[RouterD] mpls ldp
[RouterD-ldp] advertise-label prefix-list prefix-to-a peer peer-a
[RouterD-ldp] advertise-label prefix-list prefix-to-c peer peer-c
[RouterD-ldp] quit
```

4. 验证配置

配置完成后，在各设备上执行 **display mpls ldp lsp** 命令，可以看到 LDP LSP 的建立情况。Router A 和 Router C 只接收到 Router B 通告的 FEC—标签映射；Router B 接收到了 Router A 和 Router C 通告的 FEC—标签映射； Router D 没有接收到 Router A 和 Router C 通告的 FEC—标签映射；即只沿着路径 Router A—Router B—Router C 建立了 LSP。

```
[RouterA] display mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup
FECs: 2            Ingress: 1          Transit: 1      Egress: 1

FEC                In/Out Label        Nexthop         OutInterface
11.1.1.0/24        1277/-
                   -/1151(L)
                   -/1277(L)
21.1.1.0/24        -/1276              10.1.1.2        S2/1/0
                   1276/1276           10.1.1.2        S2/1/0
[RouterB] display mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup
FECs: 2            Ingress: 2          Transit: 2      Egress: 0

FEC                In/Out Label        Nexthop         OutInterface
11.1.1.0/24        -/1277              10.1.1.1        S2/1/0
                   1277/1277           10.1.1.1        S2/1/0
```

```
21.1.1.0/24        -/1149              20.1.1.2        S2/1/1
                   1276/1149           20.1.1.2        S2/1/1
[RouterC] display mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup
FECs: 2            Ingress: 1          Transit: 1      Egress: 1

FEC                In/Out Label        Nexthop         OutInterface
11.1.1.0/24        -/1277              20.1.1.1        S2/1/0
                   1148/1277           20.1.1.1        S2/1/0
21.1.1.0/24        1149/-
                   -/1276(L)
                   -/1150(L)
[RouterD] display mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup
FECs: 2            Ingress: 0          Transit: 0      Egress: 2

FEC                In/Out Label        Nexthop         OutInterface
11.1.1.0/24        1151/-
                   -/1277(L)
21.1.1.0/24        1150/-
```

在 Router A 上检测 Router A 到 Router C 的 LDP LSP 的可达性。

```
[RouterA] ping mpls -a 11.1.1.1 ipv4 21.1.1.0 24
MPLS Ping FEC: 21.1.1.0/24 : 100 data bytes
100 bytes from 20.1.1.2: Sequence=1 time=1 ms
100 bytes from 20.1.1.2: Sequence=2 time=1 ms
100 bytes from 20.1.1.2: Sequence=3 time=8 ms
100 bytes from 20.1.1.2: Sequence=4 time=2 ms
100 bytes from 20.1.1.2: Sequence=5 time=1 ms

--- FEC: 21.1.1.0/24 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max = 1/2/8 ms
```

在 Router C 上检测 Router C 到 Router A 的 LDP LSP 的可达性。

```
[RouterC] ping mpls -a 21.1.1.1 ipv4 11.1.1.0 24
MPLS Ping FEC: 11.1.1.0/24 : 100 data bytes
100 bytes from 10.1.1.1: Sequence=1 time=1 ms
100 bytes from 10.1.1.1: Sequence=2 time=1 ms
100 bytes from 10.1.1.1: Sequence=3 time=1 ms
100 bytes from 10.1.1.1: Sequence=4 time=1 ms
100 bytes from 10.1.1.1: Sequence=5 time=1 ms

--- FEC: 11.1.1.0/24 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max = 1/1/1 ms
```

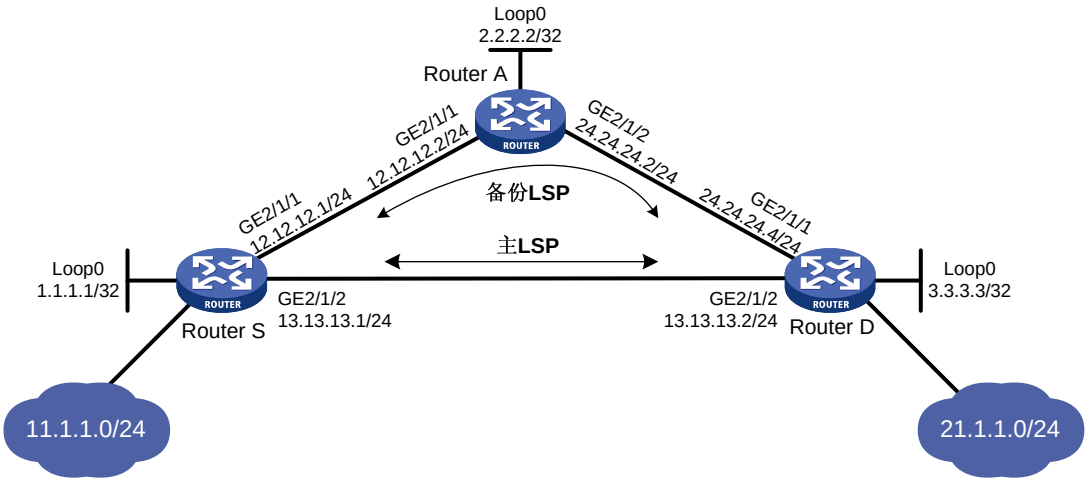
1.23.4 LDP快速重路由配置举例

1. 组网需求

Router S、Router A 和 Router D 属于同一 OSPF 区域，通过 OSPF 协议实现网络互连。在 Router S—Router D、Router S—Router A—Router D 两条路径上利用 LDP 分别建立主 LSP 和备份 LSP，实现：

- 当 Router S—Router D 这条 LSP 正常工作时，11.1.1.0/24 和 21.1.1.0/24 两个网段之间的流量通过该 LSP 传输。
- 当 Router S—Router D 这条 LSP 出现故障时，11.1.1.0/24 和 21.1.1.0/24 两个网段之间的流量快速切换到 Router S—Router A—Router D 这条备份 LSP 上传输。

图1-12 LDP 快速重路由配置组网图



2. 配置思路

- 在各台路由器上配置路由协议，使得各路由器之间路由可达。本例中，采用的路由协议为 OSPF。
- 在各台路由器上启动 LDP 协议。
- 在各台路由器上配置 LSP 触发策略，使得目的地址为 11.1.1.0/24 和 21.1.1.0/24 的路由表项能够触发 LDP 建立 LSP。
- 为了建立备份 LSP，在 Router S 和 Router D 上需要配置 OSPF 快速重路由。

3. 配置步骤

(1) 配置各接口的 IP 地址

按照 图 1-12 配置各接口IP地址和掩码，包括Loopback接口，具体配置过程略。

(2) 配置 OSPF

在各台路由器上配置 OSPF，以保证各路由器之间路由可达，具体配置过程略。

(3) 配置 OSPF 快速重路由

OSPF 快速重路由有两种配置方法，可以任选一种。

方法一：使能 Router S 和 Router D 的 OSPF 快速重路由功能（通过 LFA 算法选取备份下一跳信息）

配置 Router S。

```
<RouterS> system-view
```

```
[RouterS] bfd echo-source-ip 10.10.10.10
[RouterS] ospf 1
[RouterS-ospf-1] fast-reroute lfa
[RouterS-ospf-1] quit
```

配置 Router D。

```
<RouterD> system-view
[RouterD] bfd echo-source-ip 11.11.11.11
[RouterD] ospf 1
[RouterD-ospf-1] fast-reroute lfa
[RouterD-ospf-1] quit
```

方法二：使能 Router S 和 Router D 的 OSPF 快速重路由功能（通过路由策略指定备份下一跳）

配置 Router S。

```
<RouterS> system-view
[RouterS] bfd echo-source-ip 10.10.10.10
[RouterS] ip prefix-list abc index 10 permit 21.1.1.0 24
[RouterS] route-policy frr permit node 10
[RouterS-route-policy] if-match ip address prefix-list abc
[RouterS-route-policy] apply fast-reroute backup-interface gigabitethernet 2/1/1
backup-nexthop 12.12.12.2
[RouterS-route-policy] quit
[RouterS] ospf 1
[RouterS-ospf-1] fast-reroute route-policy frr
[RouterS-ospf-1] quit
```

配置 Router D。

```
<RouterD> system-view
[RouterD] bfd echo-source-ip 10.10.10.10
[RouterD] ip prefix-list abc index 10 permit 11.1.1.0 24
[RouterD] route-policy frr permit node 10
[RouterD-route-policy] if-match ip address prefix-list abc
[RouterD-route-policy] apply fast-reroute backup-interface gigabitethernet 2/1/1
backup-nexthop 24.24.24.2
[RouterD-route-policy] quit
[RouterD] ospf 1
[RouterD-ospf-1] fast-reroute route-policy frr
[RouterD-ospf-1] quit
```

(4) 使能 MPLS 和 MPLS LDP 功能

配置 Router S。

```
[RouterS] mpls lsr-id 1.1.1.1
[RouterS] mpls ldp
[RouterS-mpls-ldp] quit
[RouterS] interface gigabitethernet 2/1/1
[RouterS-GigabitEthernet2/1/1] mpls enable
[RouterS-GigabitEthernet2/1/1] mpls ldp enable
[RouterS-GigabitEthernet2/1/1] quit
[RouterS] interface gigabitethernet 2/1/2
[RouterS-GigabitEthernet2/1/2] mpls enable
[RouterS-GigabitEthernet2/1/2] mpls ldp enable
```

```
[RouterS-GigabitEthernet2/1/2] quit
```

配置 Router D。

```
[RouterD] mpls lsr-id 3.3.3.3
[RouterD] mpls ldp
[RouterD-mpls-ldp] quit
[RouterD] interface gigabitethernet 2/1/1
[RouterD-GigabitEthernet2/1/1] mpls enable
[RouterD-GigabitEthernet2/1/1] mpls ldp enable
[RouterD-GigabitEthernet2/1/1] quit
[RouterD] interface gigabitethernet 2/1/2
[RouterD-GigabitEthernet2/1/2] mpls enable
[RouterD-GigabitEthernet2/1/2] mpls ldp enable
[RouterD-GigabitEthernet2/1/2] quit
```

配置 Router A。

```
[RouterA] mpls lsr-id 2.2.2.2
[RouterA] mpls ldp
[RouterA-mpls-ldp] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mpls enable
[RouterA-GigabitEthernet2/1/1] mpls ldp enable
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] mpls enable
[RouterA-GigabitEthernet2/1/2] mpls ldp enable
[RouterA-GigabitEthernet2/1/2] quit
```

(5) 配置 LSP 的触发建立策略为所有静态路由和 IGP 路由项都能触发 LDP 建立 LSP

配置 Router S。

```
[RouterS] mpls ldp
[RouterS-ldp] lsp-trigger all
[RouterS-ldp] quit
```

配置 Router D。

```
[RouterD] mpls ldp
[RouterD-ldp] lsp-trigger all
[RouterD-ldp] quit
```

配置 Router A。

```
[RouterA] mpls ldp
[RouterA-ldp] lsp-trigger all
[RouterA-ldp] quit
```

4. 验证配置

在 Router S 和 Router D 上执行 **display mpls ldp lsp** 命令，可以看到 Router S 和 Router D 之间建立了主备 LSP（在 Out Label 后存在“B”，表示该 LSP 为备份 LSP）。以 Router S 为例：

```
[RouterS] display mpls ldp lsp 21.1.1.0 24
Status Flags: * - stale, L - liberal, B - backup
FECs: 1           Ingress: 2          Transit: 2      Egress: 0

FEC               In/Out Label        Nexthop         OutInterface
```

21.1.1.0/24	-/3	13.13.13.2	GE2/1/2
	2174/3	13.13.13.2	GE2/1/2
	-/3(B)	12.12.12.2	GE2/1/1
	2174/3(B)	12.12.12.2	GE2/1/1

目 录

1 MPLS TE ····· 1-1

1.1 MPLS TE简介 ····· 1-1

1.1.1 流量工程与MPLS TE ····· 1-1

1.1.2 MPLS TE的基本概念 ····· 1-1

1.1.3 静态建立CRLSP ····· 1-1

1.1.4 动态建立CRLSP ····· 1-2

1.1.5 流量转发 ····· 1-3

1.1.6 make-before-break ····· 1-5

1.1.7 路由固定 ····· 1-5

1.1.8 隧道重优化 ····· 1-6

1.1.9 自动带宽调整 ····· 1-6

1.1.10 CRLSP备份 ····· 1-6

1.1.11 快速重路由 ····· 1-6

1.1.12 DiffServ-Aware TE ····· 1-8

1.1.13 MPLS TE双向隧道 ····· 1-10

1.1.14 协议规范 ····· 1-11

1.2 MPLS TE配置任务简介 ····· 1-11

1.3 开启MPLS TE能力 ····· 1-12

1.4 配置Tunnel接口 ····· 1-13

1.5 配置DiffServ-Aware TE ····· 1-13

1.6 配置MPLS TE隧道采用静态CRLSP ····· 1-14

1.7 配置MPLS TE隧道采用RSVP-TE动态建立的CRLSP ····· 1-15

1.7.1 配置任务简介 ····· 1-15

1.7.2 配置链路的MPLS TE属性 ····· 1-15

1.7.3 配置通过IGP的TE扩展发布链路的MPLS TE属性 ····· 1-16

1.7.4 配置MPLS TE隧道的约束条件 ····· 1-17

1.7.5 使用RSVP-TE建立MPLS TE隧道 ····· 1-19

1.7.6 调整CRLSP的路径选择 ····· 1-19

1.7.7 调整MPLS TE隧道的建立 ····· 1-22

1.8 配置MPLS TE隧道非均衡负载分担 ····· 1-24

1.9 配置流量转发 ····· 1-25

1.9.1 配置静态路由使流量沿MPLS TE隧道/捆绑隧道转发 ····· 1-25

1.9.2 配置策略路由使流量沿MPLS TE隧道/捆绑隧道转发 ····· 1-25

1.9.3 配置自动路由发布使流量沿MPLS TE隧道/捆绑隧道转发 ····· 1-26
1.10 配置MPLS TE双向隧道 ····· 1-27
1.11 配置CRLSP备份 ····· 1-28
1.12 配置MPLS TE快速重路由 ····· 1-29
1.12.1 开启快速重路由功能 ····· 1-29
1.12.2 在PLR上配置Bypass隧道 ····· 1-29
1.12.3 配置节点故障检测 ····· 1-32
1.12.4 配置快速重路由的Bypass隧道优选时间间隔 ····· 1-33
1.13 开启告警功能 ····· 1-33
1.14 MPLS TE显示和维护 ····· 1-34
1.15 MPLS TE典型配置举例 ····· 1-34
1.15.1 使用静态CRLSP配置MPLS TE隧道示例 ····· 1-34
1.15.2 使用RSVP-TE配置MPLS TE隧道示例 ····· 1-39
1.15.3 使用RSVP-TE配置跨域的MPLS TE隧道示例 ····· 1-45
1.15.4 配置MPLS TE双向隧道 ····· 1-52
1.15.5 配置CRLSP备份示例 ····· 1-59
1.15.6 配置快速重路由示例（手工配置Bypass隧道） ····· 1-62
1.15.7 配置自动快速重路由示例 ····· 1-68
1.15.8 配置IETF DS-TE模式MPLS TE隧道示例 ····· 1-74
1.16 MPLS TE常见配置错误举例 ····· 1-81
1.16.1 不能产生TE LSA ····· 1-81

1 MPLS TE

1.1 MPLS TE简介

1.1.1 流量工程与MPLS TE

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导致的局部拥塞。TE（Traffic Engineering，流量工程）可以用来解决负载不均衡导致的拥塞问题。

流量工程通过实时监控网络的流量和网络单元的负载，动态调整流量管理参数、路由参数和资源约束参数等，使网络运行状态迁移到理想状态，优化网络资源的使用，避免负载不均衡导致的拥塞。

MPLS TE 结合了 MPLS 技术与流量工程，通过建立沿着指定路径的 LSP 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。

MPLS TE 是一种可扩展性好、简单的流量工程解决方案，受到了服务提供商的青睐。通过 MPLS TE 技术，服务提供商能够在已有的 MPLS 骨干网上简单地部署流量工程，充分利用现有的网络资源提供多样化的服务，同时可以优化网络资源，并进行科学的网络管理。

1.1.2 MPLS TE的基本概念

1. CRLSP

CRLSP（Constraint-based Routed Label Switched Paths，基于约束路由的 LSP）是基于一定约束条件建立的 LSP。与普通 LSP 不同，CRLSP 的建立不仅依赖路由信息，还需要满足其他一些条件，比如带宽需求、显式路径等。

MPLS TE 可以通过静态和动态两种方式建立 CRLSP。

2. MPLS TE隧道

MPLS TE 隧道是从头节点到目的节点的一条虚拟点到点连接。通常情况下，MPLS TE 隧道由一条 CRLSP 构成。在部署 CRLSP 备份或需要将流量通过多条路径传输等情况下，需要为同一种流量建立多条 CRLSP，在这种情况下，MPLS TE 隧道由一组 CRLSP 构成。

头节点上 MPLS TE 隧道由 MPLS TE 模式的 Tunnel 接口标识。当流量的出接口为 Tunnel 接口时，该流量将通过构成 MPLS TE 隧道的 CRLSP 来转发。

1.1.3 静态建立CRLSP

静态建立 CRLSP 是指在流量经过的每一跳设备上（包括 Ingress、Transit 和 Egress）分别手工指定入标签、出标签、流量所需的带宽等信息，从而建立满足约束条件的 CRLSP。该方式的优点是配置简单，缺点是不能根据网络的变化动态调整建立的 CRLSP。

静态 CRLSP 的详细介绍，请参见“MPLS 配置指导”中的“静态 CRLSP”。

1.1.4 动态建立CRLSP

动态建立 CRLSP 是指根据链路状态信息计算出路径后，通过标签分发协议（如 RSVP-TE）通告标签，并在经过的节点上为流量预留所需的带宽资源，从而建立满足约束条件的 CRLSP。该方式的优点是能根据网络的变化动态调整建立的 CRLSP，且支持 CRLSP 备份、快速重路由等功能，缺点是配置复杂。

采用动态方式建立 CRLSP 时，MPLS TE 需要实现如下功能：

- 发布包含链路 TE 属性的信息，以便根据这些信息选择满足约束条件的路径。
- 计算出到达某个节点的满足 TE 属性要求的最短路径。
- 通过标签分发协议沿着计算出的路径建立 CRLSP，并预留资源。

1. 发布TE属性

MPLS TE 通过对现有的使用链路状态算法的 IGP 协议（如 OSPF 和 IS-IS）进行扩展来发布每条链路的 TE 相关属性，如链路的最大带宽、链路的最大可预留带宽、每个优先级的未被预留带宽、链路属性等。这些信息通过 IGP 协议在网络上泛洪。每台设备收集本区域或本级别所有设备上每条链路的 TE 相关信息，生成 TEDB（TE DataBase，流量工程数据库）。

2. 计算路径

MPLS TE 使用 CSPF（Constraint-based Shortest Path First，基于约束的最短路径优先）算法，根据通过 IS-IS 或 OSPF 扩展产生的 TEDB，计算出到达某个节点的符合带宽、亲和属性、建立/保持优先级、显式路径等约束条件的最短路径。

CSPF 是一种改进的 SPF（Shortest Path First，最短路径优先）算法。CSPF 的计算过程就是针对 MPLS TE 隧道的要求，先对 TEDB 中的链路进行剪切，把不满足 TE 属性要求的链路剪掉；再采用 SPF 算法，寻找一条到 Egress 节点的满足 TE 属性要求的最短路径（即一组 LSR 地址）。

CSPF 计算的结果是一条满足约束条件的完全明确的路径，通常只在 MPLS TE 隧道的 Ingress 节点进行 CSPF 计算。

MPLS TE 隧道的约束条件需要在 Ingress 节点上配置，约束条件包括：

(1) 带宽

带宽要求是指经过 MPLS TE 隧道的流量所属的服务类型及其所需的带宽。只有链路上针对流量所属服务类型的可预留带宽大于等于流量所需带宽时，该链路才满足带宽约束条件。

(2) 亲和属性

MPLS TE 隧道的亲和属性和链路的属性配合，决定了该隧道可以使用哪些链路。

链路属性、亲和属性、亲和属性的掩码都是 32 位的二进制数。如果希望某条链路能够被隧道所用，则需要满足如下要求：

- 对于掩码为 1 的位，亲和属性为 1 的位中链路属性至少有 1 位也为 1，亲和属性为 0 的位对应的链路属性位不能为 1。
- 对于掩码为 0 的位，不对链路属性的相应位进行检查。

例如，亲和属性为 0xFFFFFFF0，掩码为 0x0000FFFF，则可用链路的链路属性高 16 位可以任意取 0 或 1，17～28 位中至少有 1 位为 1，且低 4 位不能为 1。

(3) 建立和保持优先级

如果在建立 MPLS TE 隧道时，无法找到满足所需带宽要求的路径，可以拆除另外一条已经建立的 MPLS TE 隧道，占用为它分配的带宽资源，这种处理方式称为抢占。

MPLS TE 隧道使用两个优先级属性来决定是否可以进行抢占：建立优先级（Setup Priority）和保持优先级（Holding Priority）。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。只有当一条 MPLS TE 隧道的建立优先级数值小于另一条 MPLS TE 隧道的保持优先级时，该隧道才可以抢占另一条隧道的资源。

MPLS TE 隧道的建立优先级不能高于该隧道的保持优先级，即其在数值上应大于或等于保持优先级，否则可能会导致 MPLS TE 隧道间无穷尽地互相抢占，造成振荡。

(4) 显式路径

通过显式路径可以指定到达某个目的地所必须经过的节点、不允许经过的节点等。将显式路径作为约束条件，可以动态计算出符合规划要求的路径。

显式路径分为：

- 严格显式路径：指定必须经过哪些节点，并且指定的下一跳与前一跳必须直接相连。通过严格显式路径，可以最精确地控制 MPLS TE 隧道所经过的路径。
- 松散显式路径：指定必须经过哪些节点，并且指定的下一跳和前一跳之间可以存在其他节点。通过松散显式路径，可以模糊地限制 MPLS TE 隧道所经过的路径。

严格显式路径和松散显式路径还可以配合使用，即在显式路径中部分节点之间必须直接相连，部分节点之间可以存在其他节点。

3. 通过RSVP-TE建立CRLSP

使用 CSPF 算法计算出满足约束条件的路径后，MPLS TE 通过标签分发协议沿着计算出的路径建立 CRLSP，并在路径经过的节点上预留资源。

目前，设备上支持的 MPLS TE 标签分发协议为 RSVP-TE。RSVP（Resource Reservation Protocol，资源预留协议）是一种用来在网络上请求预留资源的信令协议。RSVP 经扩展后可以支持 MPLS 标签的分发，并在传送标签绑定消息的同时携带资源预留信息，这种扩展后的 RSVP 称为 RSVP-TE。

RSVP 的详细介绍，请参见“MPLS 配置指导”中的“RSVP”。

1.1.5 流量转发

当 MPLS TE 隧道建立之后，流量不会自动通过 MPLS TE 隧道转发，需要通过如下方法配置流量沿 MPLS TE 隧道转发。

1. 静态路由

使用静态路由转发流量，是指定义一条通过 Tunnel 接口到达目的网络地址的静态路由，把流量引入到 MPLS TE 隧道上进行转发。

静态路由是将流量引入 MPLS TE 隧道的最简便、直观的方法。该方法的缺点是：如果多个目的网络的流量都需要引入到 MPLS TE 隧道上，则需要配置多条静态路由，配置和维护难度比较大。

有关静态路由的介绍请参见“三层技术-IP 路由配置指导”中的“静态路由”。

2. 策略路由

使用 PBR（Policy-based routing，基于策略的路由）转发流量，是指定义策略路由，在策略路由中将匹配 ACL 规则的流量的出接口指定为 Tunnel 接口，并在流量的入接口上应用该策略路由，从而实现将流量引入到 MPLS TE 隧道上进行转发。

策略路由方式不仅可以根据目的 IP 地址来匹配需要通过 Tunnel 接口转发的流量，还可以根据源 IP 地址、协议类型等来匹配流量。与静态路由方式相比，策略路由方式更加灵活，但是配置比较复杂。

有关策略路由的介绍请参见“三层技术-IP 路由配置指导”中的“策略路由”。

3. 自动路由发布

自动路由发布是指将 MPLS TE 隧道发布到 IGP（OSPF 或 IS-IS）路由中，让 MPLS TE 隧道参与 IGP 路由的计算，使得流量可以通过 MPLS TE 隧道转发。自动路由发布方式的配置和维护都比较简单。

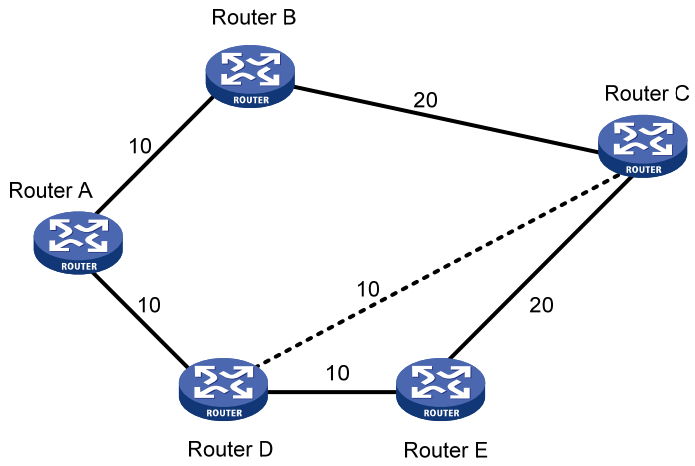
自动路由发布包括以下两种方式：

- IGP Shortcut：也称为自动路由宣告（AutoRoute Announce），该功能将 MPLS TE 隧道当作一条直接连接隧道 Ingress 节点（头节点）和 Egress 节点（尾节点）的链路，在隧道的 Ingress 节点上进行 IGP 路由计算时考虑该 MPLS TE 隧道。
- 转发邻接：该功能将 MPLS TE 隧道当作一条直接连接隧道 Ingress 节点和 Egress 节点的链路，通过 IGP 路由协议将该链路发布到网络中，以便网络中的节点在路由计算时使用 MPLS TE 隧道。

IGP Shortcut 和转发邻接功能的区别在于：

- 在隧道的 Ingress 节点上开启 IGP Shortcut 功能后，只有 Ingress 节点计算 IGP 路由时会考虑 MPLS TE 隧道。IGP Shortcut 功能不会通过 IGP 路由协议将 MPLS TE 隧道作为一条链路发布出去。因此，其他设备在路由计算时不会考虑 MPLS TE 隧道。
- 在隧道的 Ingress 节点上开启转发邻接功能后，Ingress 节点会通过 IGP 路由协议将 MPLS TE 隧道作为一条链路发布出去。因此，IGP 网络中的所有设备在路由计算时都会考虑 MPLS TE 隧道。

图1-1 IGP Shortcut 与转发邻接示意图



在 图 1-1 中，Router D到Router C之间存在一条MPLS TE隧道，IGP Shortcut只能使Ingress节点Router D在计算IGP路由时利用这条隧道，Router A并不能利用这条隧道到达Router C。如果配置了转发邻接功能，则Router A也能够知道这条MPLS TE隧道的存在，从而可以利用该隧道将到Router C的流量转发到Router D上。

1.1.6 make-before-break

make-before-break 是一种在尽可能不丢失数据，也不占用额外带宽的前提下改变 MPLS TE 隧道的机制。

在隧道重优化、自动带宽调整等情况下，如果在新的 CRLSP 建立之前拆除旧的 CRLSP，则会导致流量转发中断。通过 make-before-break 机制可以确保新 CRLSP 建立、并将流量切换到新的 CRLSP 后，再拆除旧 CRLSP，从而有效地避免流量转发中断。此时，存在的问题是：如果新的 CRLSP 和旧 CRLSP 部分路径相同，则在这些路径上需要重复为新旧 CRLSP 预留带宽，造成带宽资源的浪费。make-before-break 机制采用 SE 资源预留风格解决这个问题。

资源预留风格是 RSVP-TE 协议在建立 CRLSP 时预留带宽资源的方式。MPLS TE 隧道使用的资源预留风格由隧道的 Ingress 节点决定，并通过 RSVP 协议通知给各个节点。

目前，设备支持以下两种资源预留风格：

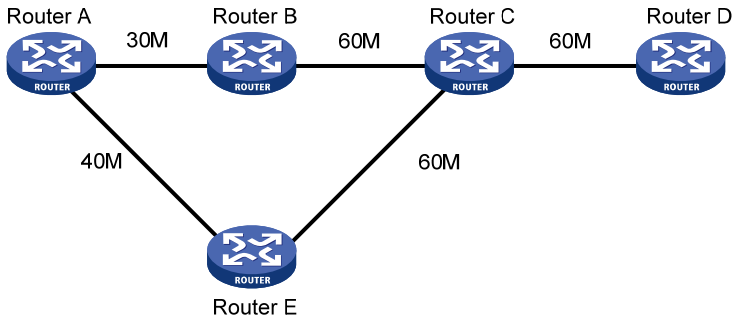
- FF（Fixed-Filter，固定过滤器）：为每个发送者单独预留资源，同一会话中的不同发送者不能共享资源。
- SE（Shared-Explicit，共享显式）：为同一个会话中的不同发送者预留同一个资源，不同发送者之间可以共享资源。该方式主要用于 make-before-break。

在 图 1-2 中，假设需要建立一条Router A到Router D的CRLSP，保留 30M带宽，起初建立的路径是Router A→Router B→Router C→Router D。

现在希望将带宽增大为 40M，Router A→Router B→Router C→Router D 路径不能满足要求。而如果选择 Router A→Router E→Router C→Router D，则 Router C→Router D 需要同时预留 30M 和 40M 带宽，也存在带宽不够的问题。

采用 make-before-break 机制，新建立的 CRLSP 在 Router C→Router D 可以共享原 CRLSP 的带宽，不需要为新 CRLSP 和旧 CRLSP 重复预留带宽。新 CRLSP 建立成功后，流量切换到新 CRLSP 上，之后拆除原 CRLSP，从而有效地避免了流量中断。

图1-2 make-before-break 示意图



1.1.7 路由固定

路由固定是指 CRLSP 创建成功后，即使路由发生变化，也不重新选择最优路径，而是沿用已创建的 CRLSP。

在路由变化频繁的网络中，如果不希望 CRLSP 随着路由频繁变化，则可以通过本功能确保只要已建立的 CRLSP 可用就不重新创建 CRLSP。

1.1.8 隧道重优化

隧道重优化功能是指周期性地或通过命令行手工触发隧道的 Ingress 节点重新计算路径。如果计算出的路径优于当前路径，则创建一条新的 CRLSP。将流量从旧的 CRLSP 切换至新的 CRLSP 后，删除旧的 CRLSP。

MPLS TE 利用隧道重优化功能实现 CRLSP 的动态优化，以便及时地将 MPLS TE 隧道切换到当前的最优路径。例如，如果在 MPLS TE 隧道建立时，最优路径上的链路没有足够的可预留带宽，则会导致 MPLS TE 隧道未使用最优路径建立。通过隧道重优化功能，可以实现链路上具有足够的带宽时将 MPLS TE 隧道自动切换到最优路径。

1.1.9 自动带宽调整

通常情况下，用户最初不能确定有多少业务需要通过服务提供商的网络传输。因此，服务提供商需要具备这样一种功能：能在最初时为用户请求的带宽建立 MPLS TE 隧道；当用户业务增多时，能够根据用户的业务量自动调整分配给 MPLS TE 隧道的带宽。

MPLS TE 通过自动带宽调整实现上述功能。自动带宽调整功能是指对隧道的平均出口速率进行测量，并周期性地根据测量结果调整隧道的带宽。

自动带宽调整功能的工作机制为：设备定时地对隧道的出口速率进行采样，计算采样时间间隔内的平均出口速率；自动带宽调整时间间隔到达后，将隧道的带宽设置为该时间间隔内多次采样中的最大平均出口速率；根据调整后的隧道带宽建立新的 CRLSP；CRLSP 建立成功后，将流量从旧的 CRLSP 切换到新的 CRLSP，并拆除旧的 CRLSP。

用户可以通过命令行指定允许调整到的最大带宽值和最小带宽值。如果自动带宽调整计算出的隧道带宽大于最大值，则采用最大带宽值建立新的 CRLSP；如果小于最小带宽值，则采用最小带宽值建立新的 CRLSP。

1.1.10 CRLSP备份

CRLSP 备份是指通过备份 CRLSP 对主 CRLSP 进行保护。当 Ingress 感知到主 CRLSP 不可用时，将流量切换到备份 CRLSP 上，当主 CRLSP 路径恢复后再将流量切换回来，以实现对主 CRLSP 的备份保护。

CRLSP 备份有两种备份方法：

- 热备份：创建主 CRLSP 后随即创建备份 CRLSP。主 CRLSP 失效时，直接将流量切换至备份 CRLSP。
- 普通备份：指主 CRLSP 失效后创建备份 CRLSP。

1.1.11 快速重路由

1. 快速重路由概述

FRR（Fast Reroute，快速重路由）是 MPLS TE 中实现网络局部保护的技术。FRR 的切换速度可以达到 50ms，能够最大程度减少网络故障时数据的丢失。

开启隧道的 FRR 功能后，当主 CRLSP 上的某条链路或某个节点失效时，流量会被切换到 Bypass 隧道上。同时，隧道的 Ingress 节点尝试建立新的 CRLSP。新的 CRLSP 建立成功后，流量将切换到新的 CRLSP。

说明

CRLSP 备份是一种端到端的路径保护，对整条 CRLSP 提供保护，而 FRR 则是一种局部保护措施，只能保护 CRLSP 中的某条链路或某个节点。并且，FRR 是一种快速响应的临时性保护措施，对于切换时间有严格要求，CRLSP 备份则没有时间要求。

2. 基本概念

下面介绍 FRR 中的几个概念：

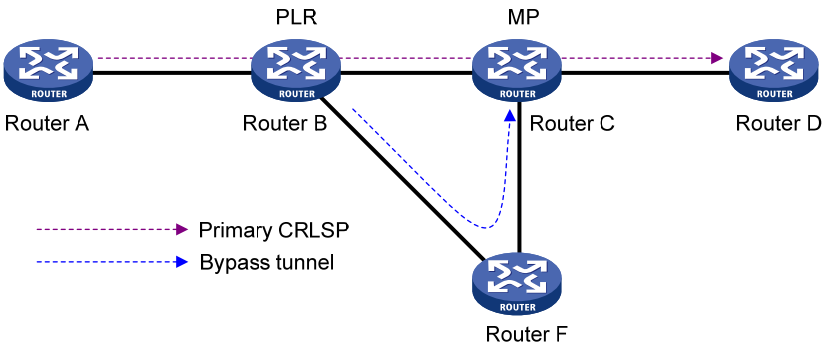
- 主 CRLSP：被保护的 CRLSP。
- Bypass 隧道：旁路隧道，保护主 CRLSP 中的某条链路或某个节点的 MPLS TE 隧道。
- PLR（Point of Local Repair，本地修复节点）：Bypass 隧道的 Ingress 节点，必须在主 CRLSP 的路径上，并且不能是主 CRLSP 的 Egress 节点。
- MP（Merge Point，汇聚点）：Bypass 隧道的 Egress 节点，必须在主 CRLSP 的路径上，并且不能是主 CRLSP 的 Ingress 节点。

3. 保护方式

根据保护的对象不同，FRR 分为两类：

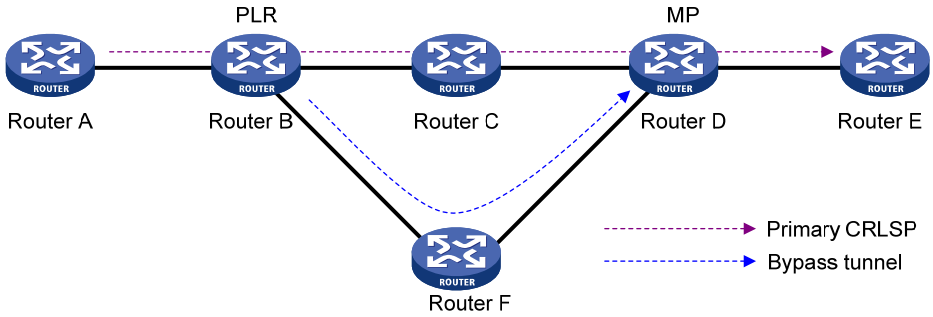
- 链路保护：又称为Next-hop（NHOP）保护。PLR和MP之间有直接链路连接，主CRLSP经过这条链路。当这条链路失效时，流量可以切换到Bypass隧道上。如 图 1-3 所示，主CRLSP是Router A→Router B→Router C→Router D，Bypass隧道是Router B→Router F→Router C。

图1-3 FRR 链路保护示意图



- 节点保护：又称为Next-next-hop（NNHOP）保护。PLR和MP之间通过一台设备连接，主CRLSP经过这台设备。当这台设备失效时，流量可以切换到Bypass隧道上。如 图 1-4 所示，主CRLSP是Router A→Router B→Router C→Router D→Router E，Bypass隧道是Router B→Router F→Router D，Router C是被保护的设备。

图1-4 FRR 节点保护示意图



1.1.12 DiffServ-Aware TE

1. DiffServ-Aware TE简介

DiffServ 作为一种 QoS 解决方案，其主要实现机制是对流量按照服务类型（class of service）进行划分，基于服务类型提供不同的 QoS 保证。而 MPLS TE 作为流量工程解决方案，主要用于对网络资源的使用进行优化。

DiffServ-Aware TE，简称 DS-TE，结合上述两者的优势，能够基于按服务类型划分的流量进行网络资源优化，即对不同的服务类型进行不同的带宽约束。概括来说，DS-TE 将不同服务类型的流量与 CRLSP 进行映射，使流量经过的路径符合对其服务类型的流量工程约束条件。

目前，设备支持两种 DS-TE 模式：

- 自定义的 Prestandard 模式
- 根据 RFC 4124、RFC 4125、RFC 4127 实现的 IETF 模式

2. DS-TE基本概念

- CT（Class Type，服务类型）：流量所属的业务类别，用来实现对不同的流量进行分类。DS-TE 根据业务流所属的 CT 为其分配链路带宽、实施约束路由及进行准入控制。对于一个给定的业务流，在其经过的所有链路上，该业务流都属于相同的 CT。
- BC（Bandwidth Constraint，带宽约束）：用来对各种服务类型流量所能使用的带宽进行限制。
- 带宽约束模型（Bandwidth Constraint Model）：用来实现对不同 CT 的业务流进行带宽约束的算法。带宽约束模型由两部分内容决定：最大 BC 数目、BC 与 CT 的对应关系。DS-TE 支持两种带宽约束模型 RDM（Russian Dolls Model，俄罗斯套娃模型）和 MAM（Maximum Allocation Model，最大分配模型）。
- TE class：CT 及优先级的组合。如果流量属于某个 CT，则传输该流量的 MPLS TE 隧道的建立优先级或保持优先级必须是该 CT 对应的优先级。

说明

Prestandard 模式和 IETF 模式具有如下区别，请根据服务类型的数量、所需带宽约束模型等选择合适的 DS-TE 模式。

- Prestandard 模式支持 2 个 CT（CT 0 和 CT 1），8 种优先级，最大支持 16 个 TE class；IETF 模式支持 4 个 CT（CT 0、CT 1、CT 2 和 CT 3），8 种优先级，最大支持 8 个 TE class。
- Prestandard 模式下不可以通过配置改变 TE class；IETF 模式下可以通过配置改变 TE class。
- Prestandard 模式只支持 RDM 模型；IETF 模式支持 RDM 模型和 MAM 模型。
- Prestandard 模式为自定义模式，无法与所有厂商设备互通；IETF 模式为根据 RFC 标准实现的模式，可以与其他厂商设备互通。

3. DS-TE工作原理

根据流量的服务类型建立 MPLS TE 隧道的过程如下：

(1) 判断流量所属的 CT

设备上根据配置实现不同业务流量的分类：

- 对于动态建立的 MPLS TE 隧道，在隧道接口下执行 **mpls te bandwidth** 命令，可以配置通过该隧道接口的流量所属的 CT。
- 对于静态建立的 MPLS TE 隧道，配置静态隧道时，可以通过 **bandwidth** 参数指定通过该静态隧道转发的流量所属的 CT。

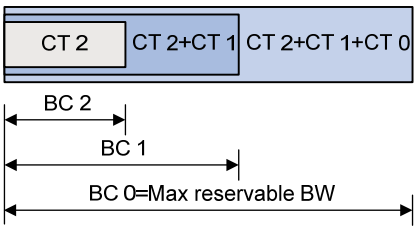
(2) 检查 CT 对应的 BC 中是否存在足够的带宽

用户可以在接口下通过 **mpls te max-reservable-bandwidth** 命令，配置该接口的带宽限制。设备根据流量所属的 CT 及接口的带宽限制，判断是否存在足够的带宽为该流量建立 MPLS TE 隧道。

不同带宽约束模型下，BC 与 CT 的关系不同：

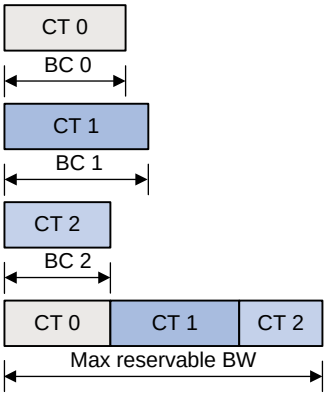
- RDM：限制多种服务类型流量（CT）的共用带宽，允许多种CT间共享使用带宽，而不是限制某一种CT的带宽。如 图 1-5 所示，以三个CT（CT 0、CT 1 和CT 2）为例，BC 2 为CT 2 的带宽限制，即属于CT 2 流量的带宽总和不能超过BC 2；BC 1 为CT 2 和CT 1 两种业务的带宽限制，即属于CT 2 和CT 1 流量的带宽总和不能超过BC 1；BC 0 为CT 2、CT 1 和CT 0 三种业务的带宽限制，即属于CT 2、CT 1 和CT 0 流量的带宽总和不能超过BC 0。在RDM中，BC 0 即为链路的最大可预留带宽。RDM与建立优先级/保持优先级配合，可以实现CT间的带宽隔离。RDM比较适用于属于CT的流量不平稳、可能存在突发流量的情况。

图1-5 RDM 带宽约束模型示意图



- MAM：限制某一CT在接口上占用的带宽总和，即隔离CT之间的带宽使用。如 图 1-6 所示，以三个CT（CT 0、CT 1 和CT 2）为例，BC 0 为CT 0 的带宽限制，即属于CT 0 流量的带宽总和不能超过BC 0；BC 1 为CT 1 的带宽限制，即属于CT 1 流量的带宽总和不能超过BC 1；以此类推。并且，属于CT 0、CT 1 和CT 2 流量的带宽总和不能超过最大可预留带宽。MAM不需要与建立优先级/保持优先级配合，就可以实现CT间的带宽隔离。MAM的特点是比较直观，配置较为容易。MAM比较适用于属于CT的流量较为平稳、不存在突发流量的情况。

图1-6 MAM 带宽约束模型示意图



(3) 检查流量是否与已经存在的 TE class 匹配

根据服务类型建立 MPLS TE 隧道时，还需要检查流量所属的 CT 及 LSP 的建立优先级/保持优先级是否与已经存在的 TE class 匹配。要想为该流量建立隧道，必须同时满足下面两个条件：

- 隧道经过的节点上都存在与流量所属 CT、LSP 建立优先级匹配的 TE class；
- 隧道经过的节点上都存在与流量所属 CT、LSP 保持优先级匹配的 TE class。

1.1.13 MPLS TE双向隧道

MPLS TE 隧道作为 MPLS-TP（MPLS Transport Profile，MPLS 传送技术架构）的分组传送隧道，需要实现双向隧道功能，以支持 1:1 和 1+1 保护倒换，承载 MPLS 传送所需要的 OAM（Operations, Administration, and Maintenance，操作、管理和维护）和 PSC（Protection State Coordination，保护状态协调）等带内检测工具和信令。

一条 MPLS TE 双向隧道由方向相反的一对单向 CRLSP 组成。MPLS TE 双向隧道的建立有如下几种方式：

- Co-routed 方式：对 RSVP-TE 协议进行扩展，通过 RSVP-TE 信令协议建立 MPLS TE 双向隧道，即通过 Path 消息将上游 LSR 分配的标签通告给下游 LSR，在 Path 消息传递的过程中建立一个方向的 CRLSP，再通过 Resv 消息将下游 LSR 分配的标签通告给上游 LSR，在 Resv 消息传递的过程中建立另一个方向的 CRLSP。Co-routed 方式建立的 MPLS TE 双向隧道的正、反两个方向 CRLSP 使用的是相同的路径。
- Associated 方式：通过配置手工将两条方向相反的单向 CRLSP 绑定，从而形成 MPLS TE 双向隧道。绑定在一起的两条单向 CRLSP 可以通过不同的方式建立，例如一个方向上的 CRLSP 使用静态方式建立，而另一个方向上的 CRLSP 使用 RSVP-TE 信令建立。绑定在一起的两条单向 CRLSP 使用的路径可以不同。

通过 RSVP-TE 信令协议建立 MPLS TE 隧道、Path 消息、Resv 消息的详细介绍，请参见“MPLS 配置指导”中的“RSVP”。

1.1.14 协议规范

与 MPLS TE 相关的协议规范有：

- RFC 2702：Requirements for Traffic Engineering Over MPLS
- RFC 3564：Requirements for Support of Differentiated Service-aware MPLS Traffic Engineering
- RFC 3812：Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)
- RFC 4124：Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering
- RFC 4125：Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering
- RFC 4127：Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering
- ITU-T Recommendation Y.1720：Protection switching for MPLS networks

1.2 MPLS TE配置任务简介

MPLS TE 隧道采用静态 CRLSP 时，MPLS TE 的配置主要包括以下几步：

(1) 在 MPLS TE 隧道经过的各个节点和接口上开启 MPLS TE 能力。

(2) 在 MPLS TE 隧道的 Ingress 节点上创建 Tunnel 接口，指定隧道的目的端地址（即 Egress 的地址）。

(3) 在 MPLS TE 隧道经过的各个节点上创建静态 CRLSP，配置方法请参见“MPLS 配置指导”中的“静态 CRLSP”。

(4) 在 MPLS TE 隧道的 Ingress 节点上配置 Tunnel 接口引用已经创建的静态 CRLSP。

(5) 在 MPLS TE 隧道的 Ingress 节点上配置静态路由、策略路由或自动路由发布，将流量引入 MPLS TE 隧道。

MPLS TE 隧道采用 RSVP-TE 动态建立的 CRLSP 时，MPLS TE 的配置主要包括以下几步：

(1) 在 MPLS TE 隧道经过的各个节点和接口上开启 MPLS TE 能力和 RSVP 能力。开启 RSVP 能力的方法，请参见“MPLS 配置指导”中的“RSVP”。

(2) 在 MPLS TE 隧道的 Ingress 节点上创建 Tunnel 接口，指定隧道的目的端地址（即 Egress 的地址），并在 Tunnel 接口下配置 MPLS TE 隧道的约束条件（如隧道的带宽要求、亲和属性等）。

(3) 在 MPLS TE 隧道经过的各个接口上配置链路的 MPLS TE 属性，如链路的最大带宽、链路的属性等。

(4) 在 MPLS TE 隧道经过的各个节点上配置 IGP 路由协议，并配置 IGP 支持 MPLS TE，以便各个节点通过 IGP 路由协议发布链路的 TE 相关属性。

(5) 在 MPLS TE 隧道的 Ingress 节点上配置通过 RSVP-TE，沿着根据隧道约束条件、链路 MPLS TE 属性等计算出的路径建立 CRLSP。

(6) 在 MPLS TE 隧道的 Ingress 节点上配置静态路由、策略路由或自动路由发布，将流量引入 MPLS TE 隧道。

除了上述配置外，用户还可以根据实际需要配置 DiffServ-Aware TE、自动带宽调整、快速重路由等功能。

表1-1 MPLS TE 配置任务简介

配置任务		说明	详细配置
开启MPLS TE能力		必选	1.3
配置Tunnel接口		必选	1.4
配置DiffServ-Aware TE		可选	1.5
配置MPLS TE隧道	配置MPLS TE隧道采用静态CRLSP	二者必选其一	1.6
	配置MPLS TE隧道采用RSVP-TE动态建立的CRLSP		1.7
配置MPLS TE隧道非均衡负载分担		可选	1.8
配置流量转发	配置静态路由使流量沿MPLS TE隧道/捆绑隧道转发	三者必选其一	1.9
	配置策略路由使流量沿MPLS TE隧道/捆绑隧道转发		
	配置自动路由发布使流量沿MPLS TE隧道/捆绑隧道转发		
配置MPLS TE双向隧道		可选	1.10
配置CRLSP备份		可选 只有使用RSVP-TE信令协议建立的MPLS TE隧道支持本配置	1.11
配置MPLS TE快速重路由		可选 只有使用RSVP-TE信令协议建立的MPLS TE隧道支持本配置	1.12
开启告警功能		可选	1.13

1.3 开启MPLS TE能力

MPLS TE 隧道经过的各个节点和接口上都需要开启 MPLS TE 能力。

在开启 MPLS TE 能力之前，需要完成以下任务：

- 配置静态路由或 IGP 协议保证各 LSR 之间路由可达。
- 使能 MPLS 功能，详细配置请参见“MPLS 配置指导”中的“MPLS 基础”。

表1-2 开启 MPLS TE 能力

操作	命令	说明
进入系统视图	**system-view**	-
开启本节点的MPLS TE能力，并进入MPLS TE视图	**mpls te**	缺省情况下，MPLS TE能力处于禁止状态
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
开启接口的MPLS TE能力	**mpls te enable**	缺省情况下，接口上的MPLS TE能力处于禁止状态

1.4 配置Tunnel接口

MPLS TE 隧道的属性都是在 Tunnel 接口视图下配置的。因此，在配置 MPLS TE 隧道之前，需要先创建 MPLS TE 隧道模式的 Tunnel 接口。有关 Tunnel 接口的介绍和更多配置请参见“三层技术-IP 业务配置指导”中的“隧道”。

请在 MPLS TE 隧道的 Ingress 节点上执行本配置。

表1-3 配置 Tunnel 接口

操作	命令	说明
进入系统视图	**system-view**	-
创建模式为MPLS TE隧道的Tunnel接口，并进入Tunnel接口视图	**interface tunnel** *tunnel-number* **mode mpls-te**	缺省情况下，设备上不存在任何Tunnel接口
配置Tunnel接口的IP地址	**ip address** *ip-address* { *mask-length* | *mask* }	缺省情况下，未指定Tunnel接口的IP地址
配置隧道的目的端地址	**destination** *ip-address*	缺省情况下，未指定隧道的目的端地址

1.5 配置DiffServ-Aware TE

在 MPLS TE 隧道经过的所有节点上均可执行本配置。

表1-4 配置 DiffServ-Aware TE

操作	命令	说明
进入系统视图	**system-view**	-
进入MPLS TE视图	**mpls te**	-
（可选）配置DS-TE模式为IETF模式	**ds-te mode ietf**	缺省情况下，DS-TE模式为Prestandard模式

操作	命令	说明
（可选）配置IETF DS-TE模式下的带宽约束模型为MAM	**ds-te bc-model mam**	缺省情况下，IETF DS-TE模式的带宽约束模型为RDM
配置IETF DS-TE模式下TE class与服务类型、优先级的对应关系	**ds-te te-class** *te-class-index* **class-type** *class-type-number* **priority** *pri-number*	缺省情况下，IETF模式的TE class如表1-5所示

表1-5 IETF 模式的缺省 TE class

TE Class	CT	Priority
0	0	7
1	1	7
2	2	7
3	3	7
4	0	0
5	1	0
6	2	0
7	3	0

1.6 配置MPLS TE隧道采用静态CRLSP

MPLS TE 隧道采用静态 CRLSP 的配置过程非常简单，不需要配置隧道的约束条件，也不涉及 IGP 扩展，只需要建立一条静态 CRLSP、指定 MPLS TE 隧道采用静态方式建立、并配置 MPLS TE 隧道引用已建立的静态 CRLSP 即可。

表1-6 配置 MPLS TE 隧道采用静态 CRLSP

操作	命令	说明
进入系统视图	**system-view**	-
建立静态CRLSP	配置方法请参见“MPLS配置指导”中的“静态CRLSP”	-
进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	在Ingress节点上执行本命令
配置使用静态CRLSP建立MPLS TE隧道	**mpls te signaling static**	缺省情况下，MPLS TE使用RSVP-TE信令协议建立隧道
指定隧道引用的静态CRLSP	**mpls te static-cr-lsp** *lsp-name*	缺省情况下，隧道没有引用任何静态CRLSP

1.7 配置MPLS TE隧道采用RSVP-TE动态建立的CRLSP

MPLS TE 隧道采用 RSVP-TE 动态建立的 CRLSP 的配置过程可以简要描述为以下几个部分：

- 配置链路的 MPLS TE 属性；
- 通过 IGP 的 TE 扩展发布链路的 MPLS TE 属性，以便在各个节点上生成 TEDB；
- 配置隧道的约束条件；
- 利用动态信令协议 RSVP-TE 建立 CRLSP。

说明

如果不配置 IGP 的 TE 扩展，就不能形成 TEDB。这种情况下计算出的路径是由 IGP 路由得到的，而不是 CSPF 计算出来的。

1.7.1 配置任务简介

表1-7 配置任务简介

配置任务	说明	详细配置
配置链路的MPLS TE属性	必选	1.7.2
配置通过IGP的TE扩展发布链路的MPLS TE属性	必选	1.7.3
配置MPLS TE隧道的约束条件	必选	1.7.4
使用RSVP-TE建立MPLS TE隧道	必选	1.7.5
调整CRLSP的路径选择	可选	1.7.6
调整MPLS TE隧道的建立	可选	1.7.7

1.7.2 配置链路的MPLS TE属性

链路的 MPLS TE 属性包括链路的最大带宽、最大可预留带宽、链路属性等。

请在 MPLS TE 隧道经过的各个接口上执行本配置。

表1-8 配置链路的 MPLS TE 属性

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置用于转发MPLS TE流量的链路最大带宽	**mpls te max-link-bandwidth** *bandwidth-value*	缺省情况下，用于转发MPLS TE流量的链路最大带宽为0

操作	命令	说明
配置Prestandard DS-TE模式下RDM带宽约束模型BC 0和BC 1的最大可预留带宽	**mpls te max-reservable-bandwidth** *bandwidth-value* [**bc1** *bc1-bandwidth*]	请根据“1.5 配置DiffServ-Aware TE”中配置的DS-TE模式和带宽约束模型从三者中选择其一 缺省情况下，最大可预留带宽均为0 在RDM模型中，BC 0即为链路的最大可预留带宽
配置IETF DS-TE模式下MAM带宽约束模型的MPLS TE链路最大可预留带宽及各BC的最大可预留带宽	**mpls te max-reservable-bandwidth mam** *bandwidth-value* { **bc0** *bc0-bandwidth* | **bc1** *bc1-bandwidth* | **bc2** *bc2-bandwidth* | **bc3** *bc3-bandwidth* } *	
配置IETF DS-TE模式RDM带宽约束模型各BC的最大可预留带宽	**mpls te max-reservable-bandwidth rdm** *bandwidth-value* [**bc1** *bc1-bandwidth*] [**bc2** *bc2-bandwidth*] [**bc3** *bc3-bandwidth*]	
配置链路的属性	**mpls te link-attribute** *attribute-value*	缺省情况下，链路的属性值为0x00000000

1.7.3 配置通过IGP的TE扩展发布链路的MPLS TE属性

OSPF、IS-IS 扩展后可以用来发布链路的 MPLS TE 相关属性。OSPF、IS-IS 的这种扩展分别称为 OSPF TE 和 IS-IS TE。如果同时配置了 OSPF TE 和 IS-IS TE，则 MPLS TE 优先根据 OSPF TE 学习到的 MPLS TE 属性信息进行 CSPF 计算。

1. 配置OSPF TE

OSPF TE 使用 Opaque Type 10 LSA 携带链路的 TE 属性信息，因此，配置 OSPF TE 时必须先使能 OSPF 的 Opaque 能力。有关 OSPF Opaque 能力的介绍请参见“三层技术-IP 路由配置指导”中的“OSPF”。

由于 MPLS TE 无法在 OSPF 虚连接上预留资源和分配标签，即 MPLS TE 无法通过 OSPF 虚连接建立 CRLSP 隧道。因此，配置 OSPF TE 时，OSPF 路由域内不能存在虚连接。

表1-9 配置 OSPF TE

操作	命令	说明
进入系统视图	**system-view**	-
进入OSPF协议视图	**ospf** [*process-id*]	-
使能OSPF的Opaque LSA发布接收能力	**opaque-capability enable**	缺省情况下，OSPF的Opaque LSA发布接收能力处于开启状态 本命令的详细介绍，请参见“三层技术-IP路由命令参考”中的“OSPF”
进入OSPF的区域视图	**area** *area-id*	-
在当前OSPF区域下使能MPLS TE能力	**mpls te enable**	缺省情况下，OSPF区域不支持MPLS TE能力

2. 配置IS-IS TE

IS-IS TE 使用扩展 IS 可达性 TLV（类型为 22）的子 TLV 携带 TE 属性信息，扩展 IS 可达性 TLV 携带 wide 类型的开销值。因此，配置 IS-IS TE 时，必须配置 IS-IS 的开销值类型为 **wide**、**compatible** 或 **wide-compatible**。有关 IS-IS 的介绍请参见“三层技术-IP 路由配置指导”中的“IS-IS”。

在某些情况下 IS 可达性 TLV 的长度可能会达到其最大长度 255 个字节。为了使 IS-IS LSP 能顺利携带此类 TLV 并且在使能 IS-IS 的所有接口上进行正确泛洪，要求使能 IS-IS 的所有接口的 MTU 不小于 284 字节（其中包含 LSP 头长度 27 字节以及 TLV 头长度 2 字节）。如果 LSP 同时需要携带认证信息，则最小 MTU 需要根据报文结构另行推算。综合考虑以上因素，使能 IS-IS TE 的所有接口的 MTU 不要小于 512 字节，以确保 IS-IS LSP 能在网络上正确泛洪。

表1-10 配置 ISIS TE

操作	命令	说明
进入系统视图	**system-view**	-
创建一个IS-IS进程，并进入IS-IS视图	**isis** [*process-id*]	缺省情况下，系统没有运行任何IS-IS进程
配置IS-IS开销值的类型	**cost-style** { **wide** | **wide-compatible** | **compatible** [**relax-spf-limit**] }	缺省情况下，IS-IS只接收和发送采用**narrow**方式表示路径开销值的报文 本命令的详细介绍，请参见“三层技术-IP路由命令参考”中的“IS-IS”
在当前IS-IS进程下使能MPLS TE能力	**mpls te enable** [**level-1** | **level-2**]	缺省情况下，IS-IS进程不支持MPLS TE能力
配置携带DS-TE参数的子TLV的类型值	**te-subtlv** { **bw-constraint** *value* | **unreserved-bw-sub-pool** *value* } *	缺省情况下，带宽约束**bw-constraint**的子TLV类型值为252；子池未预订带宽**unreserved-bw-sub-pool**的子TLV类型值为251

1.7.4 配置MPLS TE隧道的约束条件

请在 MPLS TE 隧道的 Ingress 节点上执行本节中的配置。

1. 配置MPLS TE隧道的带宽要求

表1-11 配置 MPLS TE 隧道的带宽要求

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
配置隧道所需的带宽，并指定隧道流量所属的服务类型	**mpls te bandwidth** [**ct0** | **ct1** | **ct2** | **ct3**] *bandwidth*	缺省情况下，未配置MPLS TE隧道所需的带宽，即带宽为0，隧道流量属于CT0

2. 配置MPLS TE隧道的亲和属性

提示

不同厂商实现的链路属性和亲和属性的关系可能有所不同，当在同一网络中使用不同厂商的设备时，需要事先了解各自的实现方式，正确配置链路的属性和隧道的亲和属性，以便准确建立隧道。

表1-12 配置 MPLS TE 隧道的亲和属性

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
配置隧道的亲和属性	**mpls te affinity-attribute** *attribute-value* [**mask** *mask-value*]	缺省情况下，隧道的亲和属性为0x00000000，掩码为0x00000000，即隧道可以使用任意属性的链路

3. 配置MPLS TE隧道的建立优先级和保持优先级

表1-13 配置 MPLS TE 隧道的建立优先级和保持优先级

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
配置MPLS TE隧道的建立优先级和保持优先级	**mpls te priority** *setup-priority* [*hold-priority*]	缺省情况下，建立优先级和保持优先级都为7

4. 配置显式路径

提示

在不同的区域或自治系统之间建立 MPLS TE 隧道时必须使用松散显式路径，指定显式路径的下一跳为 ABR（Area Border Router，区域边界路由器）或 ASBR（Autonomous System Boundary Router，自治系统边界路由器），并保证隧道 Ingress 节点与 ABR 或 ASBR 之间路由可达。

显式路径由一系列节点构成，一条显式路径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设备。

在向显式路径中增加或修改节点时，参数 **include** 表示建立的 CRLSP 必须经过指定节点；参数 **exclude** 表示建立的 CRLSP 不能经过指定节点。

表1-14 配置 MPLS TE 显式路径

操作	命令	说明
进入系统视图	**system-view**	-
创建隧道的显式路径，并进入显式路径视图	**explicit-path** *path-name*	缺省情况下，设备上不存在任何显式路径
启用当前显式路径	**undo disable**	缺省情况下，显式路径可用
在显式路径中添加或修改节点及其属性	**nexthop** [**index** *index-number*] *ip-address* [**exclude** | **include** [**loose** | **strict**]]	缺省情况下，显式路径中不存在任何节点
退回系统视图	**quit**	-
进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
配置CRLSP应用显式路径，并指定显式路径的优先级	**mpls te path preference** *value* **explicit-path** *path-name* [**no-cspf**]	缺省情况下，使用自动计算的路径建立CRLSP

1.7.5 使用RSVP-TE建立MPLS TE隧道

执行本配置前，需要通过 **rsvp**、**rsvp enable** 命令在 MPLS TE 隧道经过的所有节点和接口上都开启 RSVP 能力，详细介绍请参见“MPLS 配置指导”中的“RSVP”。

请在 MPLS TE 隧道的 Ingress 节点上执行本配置。

表1-15 配置使用 RSVP-TE 建立 MPLS TE 隧道

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
配置使用RSVP-TE信令协议建立隧道	**mpls te signaling rsvp-te**	缺省情况下，MPLS TE使用RSVP-TE信令协议建立隧道
配置CRLSP应用的路径及路径的优先级	**mpls te path preference** *value* { **dynamic** | **explicit-path** *path-name* } [**no-cspf**]	缺省情况下，使用自动计算的路径建立CRLSP

1.7.6 调整CRLSP的路径选择

提示

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，以免影响 CRLSP 的建立。

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 CRLSP。MPLS TE 提供多种方式影响 CSPF 的计算，从而调整 CRLSP 的路径选择。

1. 配置选路使用的度量

在MPLS TE中每条链路都具有两种度量值：IGP度量值和TE度量值。通过合理地规划两种度量值，可以实现为不同种类的业务选择不同的隧道。例如，使用 IGP 度量值来表示链路延迟的大小（IGP 度量值越小，链路的延迟越小），使用 TE 度量值来表示链路带宽的大小（TE 度量值越小，链路的带宽越大）。建立两条 MPLS TE 隧道（Tunnel1 和 Tunnel2），分别用来承载语音业务和视频业务。Tunnel1 选择路径时使用 IGP 度量值，可以实现为延迟要求较高的语音业务选择延迟小的路径；Tunnel2 选择路径时使用 TE 度量值，可以实现为数据量较大的视频业务选择带宽大的路径。

表1-16 配置选路使用的度量

操作	命令	说明
进入系统视图	**system-view**	-
进入MPLS TE视图	**mpls te**	-
配置未配置度量类型的隧道选路时使用的链路度量值类型	**path-metric-type** { **igp** | **te** }	缺省情况下，未配置度量类型的隧道选路时使用TE度量值 请在MPLS TE隧道的Ingress节点上执行本命令
退回系统视图	**quit**	-
进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
配置为当前隧道选路时使用的链路度量值类型	**mpls te path-metric-type** { **igp** | **te** }	缺省情况下，没有指定当前隧道选路时使用的链路度量值类型，采用MPLS TE视图下配置的链路度量值类型 请在MPLS TE隧道的Ingress节点上执行本命令
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置链路的TE度量值	**mpls te metric** *value*	缺省情况下，链路使用其IGP度量作为TE的度量值 本命令可以在MPLS TE隧道经过的所有接口上执行

2. 配置路由固定

如果使用路由固定功能，则不能同时使用 MPLS TE 隧道重优化和自动带宽调整功能。

请在 MPLS TE 隧道的 Ingress 节点上执行本配置。

表1-17 配置路由固定

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
开启路由固定功能	**mpls te route-pinning**	缺省情况下，路由固定功能处于关闭状态

3. 配置隧道重优化

隧道重优化功能是指周期性地或通过命令行手工触发隧道的 Ingress 节点重新计算路径。如果重计算的路径优于当前路径，则沿着计算出的路径创建一条新的 CRLSP，将流量从旧的 CRLSP 切换至新的 CRLSP 后，删除旧的 CRLSP。

请在 MPLS TE 隧道的 Ingress 节点上执行本配置。

表1-18 配置隧道重优化

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
开启隧道重优化功能	**mpls te reoptimization** [**frequency** *seconds*]	缺省情况下，隧道重优化功能处于关闭状态
退到用户视图	**return**	-
（可选）立即对所有开启了重优化功能的MPLS TE隧道进行重优化	**mpls te reoptimization**	-

4. 配置TE信息泛洪阈值及泛洪时间间隔

当 MPLS TE 相关链路的带宽发生变化时，需要通过 IGP 泛洪该信息，以便 Ingress 节点利用 CSPF 算法重新计算路径。

为防止链路带宽变化导致的 CSPF 计算占用过多资源，可以规定当带宽变化到达一定限度时才通过 IGP 泛洪链路的 TE 相关信息。用户可以进行两种配置：

- 当链路可预留带宽的增加值达到阈值时进行泛洪；
- 当链路可预留带宽的减少值达到阈值时进行泛洪。

如果配置了泛洪阈值，则没有及时泛洪的链路带宽变化，可以按照配置的时间间隔周期性地通告给网络中的设备。

本配置可以在 MPLS TE 隧道经过的所有节点上执行。

表1-19 配置 TE 信息泛洪阈值及泛洪时间间隔

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
配置通过IGP泛洪TE信息的带宽变化阈值	**mpls te bandwidth change thresholds** { **down** | **up** } *percent*	缺省情况下，通过IGP泛洪TE信息的带宽变化阈值为10%，即可预留带宽增加或减少10%时进行IGP泛洪
退回系统视图	**quit**	-
进入MPLS TE视图	**mpls te**	-
设置通过IGP周期性泛洪TE信息的时间间隔	**link-management periodic-flooding timer** *interval*	缺省情况下，通过IGP周期性泛洪TE信息的时间间隔为180秒

1.7.7 调整MPLS TE隧道的建立

提示

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，以免影响 MPLS TE 隧道的建立。

请在 MPLS TE 隧道的 Ingress 节点上执行本节中的配置。

1. 配置环路检测

配置隧道建立时进行环路检测后，将自动启动该隧道的路由记录功能，而不管用户是否配置了 **mpls te record-route** 命令。隧道经过的节点根据记录的路由信息，判断是否出现环路。

表1-20 配置环路检测

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
配置隧道建立时进行环路检测	**mpls te loop-detection**	缺省情况下，隧道建立时不进行环路检测

2. 配置记录路由和标签

路由记录和标签记录功能用来记录 MPLS TE 隧道经过的各个节点及各个节点分配的标签值，以便用户根据记录的信息了解 MPLS TE 隧道经过的路径和标签分配情况。在 MPLS TE 隧道出现故障时，用户也可以根据记录的信息对故障进行定位。

表1-21 配置记录路由和标签

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-

操作		命令	说明
开启隧道的路由记录或标签记录功能	仅开启路由记录功能	**mpls te record-route**	缺省情况下，隧道的路由记录和标签记录功能处于关闭状态
	同时开启路由记录和标签记录功能	**mpls te record-route label**	

3. 配置隧道重建

MPLS TE 隧道建立失败后，隧道的 Ingress 节点等待隧道重建时间间隔后，将尝试重新建立隧道，直到隧道建立成功或尝试建立隧道的次数达到配置的最大值。如果尝试建立隧道的次数达到配置的最大值时仍未成功建立隧道，则等待较长的一段时间后，重复上述过程。

表1-22 配置隧道重建

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
配置尝试建立隧道的最大次数	**mpls te retry** *times*	缺省情况下，尝试建立隧道的最大次数为3次
配置隧道重建的时间间隔	**mpls te timer retry** *seconds*	缺省情况下，隧道重建的时间间隔为2秒

4. 配置自动带宽调整功能

表1-23 配置自动带宽调整

操作	命令	说明
进入系统视图	**system-view**	-
进入MPLS TE视图	**mpls te**	-
全局开启自动带宽调整功能，并配置出口速率采样的时间间隔	**auto-bandwidth enable** [**sample-interval** *seconds*]	缺省情况下，全局自动带宽调整功能处于关闭状态 MPLS TE视图下配置的采样时间间隔对所有MPLS TE隧道有效。所有MPLS TE隧道的出口速率每经过一个采样周期就会被记录下来，这样可以获得一条MPLS TE隧道在一个采样周期内的实际平均带宽
进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
开启隧道的自动带宽调整功能	**mpls te auto-bandwidth adjustment** [**frequency** *seconds*] [**max-bw** *max-bandwidth* | **min-bw** *min-bandwidth*] *	二者选其一 缺省情况下，隧道的自动带宽调整和出口速率收集功能处于关闭状态
开启隧道的出口速率收集功能	**mpls te auto-bandwidth collect-bw** [**frequency** *seconds*]	
退到用户视图	**return**	-

操作	命令	说明
（可选）重启自动带宽调整功能	**reset mpls te auto-bandwidth-adjustment timers**	执行本命令后，会清除出口速率采样信息，并清除距下一次带宽调整的剩余时间，以便重新进行出口速率采样和带宽调整

5. 配置RSVP资源预留风格

表1-24 配置 RSVP 资源预留风格

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
配置隧道的资源预留风格	**mpls te resv-style** { **ff** | **se** }	缺省情况下，隧道的资源预留风格为SE 在目前的MPLS TE应用中，隧道的建立通常采用make-before-break方式。因此，推荐使用SE资源预留风格

1.8 配置MPLS TE隧道非均衡负载分担

MPLS TE隧道非均衡负载分担功能通过为一个负载分担模式的隧道捆绑接口（Tunnel-Bundle接口）指定多个成员接口——MPLS TE 隧道接口，形成一个捆绑隧道，实现流量的出接口为隧道捆绑接口时，该流量能够在多条 MPLS TE 隧道间进行负载分担。

通过 **member interface** 命令为 Tunnel-Bundle 接口指定成员接口时，还可以利用 **load-share** 参数指定该成员接口的负载分担权重，根据权重确定成员接口转发流量的比例。例如，隧道捆绑接口下存在三个成员接口：Tunnel1、Tunnel2 和 Tunnel3，负载分担权重分别为 1、1 和 2，则成员接口承担的流量比重分别为 1/4、1/4 和 1/2。

请在 MPLS TE 隧道的 Ingress 节点上执行本配置。

表1-25 配置 MPLS TE 隧道非均衡负载分担

操作	命令	说明
进入系统视图	**system-view**	-
创建负载分担模式的Tunnel-Bundle接口，并进入Tunnel-Bundle接口视图	**interface tunnel-bundle** *number*	缺省情况下，设备上不存在任何Tunnel-Bundle接口
配置Tunnel-Bundle接口的IP地址	**ip address** *ip-address* { *mask-length* | *mask* }	缺省情况下，未指定Tunnel-Bundle接口的IP地址
配置Tunnel-Bundle接口的隧道目的端地址	**destination** *ip-address*	缺省情况下，未指定Tunnel-Bundle接口的隧道目的端地址

操作	命令	说明
为Tunnel-Bundle接口指定成员接口	**member interface tunnel** *tunnel-number* [**load-share** *value*]	缺省情况下，Tunnel-Bundle接口下不存在任何成员接口 重复执行本命令，可以为Tunnel-Bundle接口指定多个成员接口 建议为成员接口和Tunnel-Bundle接口配置相同的目的端地址。如果不同，则需要确保通过成员接口能够到达Tunnel-Bundle接口的目的端地址；否则，会导致流量转发不通

1.9 配置流量转发

请在 MPLS TE 隧道的 Ingress 节点上执行本节中的配置。

1.9.1 配置静态路由使流量沿MPLS TE隧道/捆绑隧道转发

表1-26 配置静态路由使流量沿 MPLS TE 隧道/捆绑隧道转发

操作	命令	说明
进入系统视图	**system-view**	-
配置静态路由使流量沿MPLS TE隧道/捆绑隧道转发	静态路由命令的详细介绍请参见“三层技术-IP路由命令参考”中的“静态路由”	缺省情况下，设备上不存在任何静态路由 本命令中指定的接口应为MPLS TE隧道模式的Tunnel接口或负载分担模式的Tunnel-Bundle接口

1.9.2 配置策略路由使流量沿MPLS TE隧道/捆绑隧道转发

本配置中各命令的详细介绍，请参见“三层技术-IP 路由命令参考”中的“策略路由”。

表1-27 配置策略路由使流量沿 MPLS TE 隧道/捆绑隧道转发

操作	命令	说明
进入系统视图	**system-view**	-
创建策略节点，并进入策略节点视图	**policy-based-route** *policy-name* [**deny** | **permit**] **node** *node-number*	缺省情况下，没有创建策略节点
设置ACL匹配规则	**if-match acl** { *acl-number* | **name** *acl-name* }	缺省情况下，未设置ACL匹配规则
设置报文的发送接口为Tunnel接口或Tunnel-Bundle接口	**apply output-interface** { { **tunnel** *tunnel-number* | **tunnel-bundle** *number* } [**track** *track-entry-number*] }&<1-2>	-
退回系统视图	**quit**	-

操作		命令	说明
应用策略路由	开启本地策略路由	**ip local policy-based-route** *policy-name*	二者选其一 缺省情况下，没有应用策略路由
	对接口转发的报文应用策略	**interface** *interface-type interface-number* **ip policy-based-route** *policy-name*	

1.9.3 配置自动路由发布使流量沿MPLS TE隧道/捆绑隧道转发

自动路由发布包括 IGP Shortcut 和转发邻接两种方式。使用 IGP Shortcut 功能时，可以指定 MPLS TE 隧道/捆绑隧道的度量值。如果使用绝对度量（**absolute**），则 MPLS TE 隧道/捆绑隧道的度量值就是配置的值；如果使用相对度量（**relative**），则 MPLS TE 隧道/捆绑隧道的度量值是相应 IGP 路径度量值加上相对度量值。

配置自动路由发布前，需要完成以下操作：

- 在 Tunnel 接口/Tunnel-bundle 接口上开启 OSPF 或 IS-IS 路由协议，以便将 Tunnel 接口/Tunnel-bundle 接口地址发布到 IGP 协议（OSPF 或 ISIS）中。
- 在 OSPF 区域视图或 IS-IS 视图下，执行 **mpls te enable** 命令使能 OSPF 区域或 IS-IS 进程的 MPLS TE 能力。

使用自动路由发布功能时，需要注意以下事项：

- MPLS TE 隧道/捆绑隧道的目的地址可以配置为 Egress 节点的 LSR ID 或 Egress 节点上接口的主 IP 地址。配置为接口主 IP 地址时，要求该接口上必须使能 MPLS TE 能力，并配置 OSPF 或 IS-IS 路由协议，确保在该接口建立 OSPF 或 IS-IS 邻居关系，接口的主地址能够通过 OSPF 或 IS-IS 发布给邻居。推荐用户将 MPLS TE 隧道/捆绑隧道的目的地址配置为 Egress 节点的 LSR ID。
- Tunnel 接口/Tunnel-bundle 接口地址和隧道目的地址对应的路由必须在同一个 OSPF 区域内或属于同一个 IS-IS Level。

1. 配置IGP Shortcut

表1-28 配置 IGP Shortcut

操作		命令	说明
进入系统视图		**system-view**	-
进入接口视图	进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
	进入负载分担模式的Tunnel-Bundle接口视图	**interface tunnel-bundle** *number*	

操作	命令	说明
开启IGP Shortcut功能	**mpls te igp shortcut** [**isis** | **ospf**]	缺省情况下，IGP Shortcut功能处于关闭状态 如果开启IGP Shortcut功能时不指定IGP类型，则OSPF和IS-IS协议的路由计算中都考虑MPLS TE隧道/捆绑隧道
配置MPLS TE隧道/捆绑隧道的度量值	**mpls te igp metric** { **absolute** *value* | **relative** *value* }	缺省情况下，MPLS TE隧道/捆绑隧道的度量值等于其IGP度量值

2. 配置转发邻接

要想使转发邻接功能生效，需要创建方向相反的两条 MPLS TE 隧道/捆绑隧道，并在隧道的两端同时配置转发邻接功能。

表1-29 配置转发邻接（Tunnel 接口视图）

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
开启转发邻接功能	**mpls te igp advertise** [**hold-time** *value*]	缺省情况下，转发邻接功能处于关闭状态

表1-30 配置转发邻接（Tunnel-Bundle 接口视图）

操作	命令	说明
进入系统视图	**system-view**	-
进入负载分担模式的Tunnel-Bundle接口视图	**interface tunnel-bundle** *number*	-
开启转发邻接功能	**mpls te igp advertise**	缺省情况下，转发邻接功能处于关闭状态

1.10 配置MPLS TE双向隧道

在配置 MPLS TE 双向隧道之前，需完成以下任务：

- 在隧道两端都关闭 PHP 功能。
- 建立 Co-routed 方式 MPLS TE 双向隧道前，必须配置建立隧道使用的信令协议为 RSVP-TE，且必须通过 **mpls te resv-style** 命令配置资源预留方式为 FF 方式。
- 如果 Associated 方式 MPLS TE 双向隧道中的某条单向 CRLSP 采用 RSVP-TE 信令建立，则必须通过 **mpls te resv-style** 命令配置该 CRLSP 的资源预留方式为 FF 方式。

配置 MPLS TE 双向隧道时，需要在隧道的两端都建立 MPLS TE 隧道接口，并在隧道接口下启用双向隧道功能。

- 对于 Co-routed 方式双向隧道，隧道的两端需要分别配置为主动方（Active）和被动方（Passive），在被动方需要指定关联的反向 CRLSP。
- 对于 Associated 方式双向隧道，隧道的两端都需要指定关联的反向 CRLSP。

表1-31 配置 Co-routed 方式 MPLS TE 双向隧道的主动方

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
在MPLS TE隧道接口上启用双向隧道功能，并指定本端为Co-routed方式MPLS TE双向隧道的主动方	**mpls te bidirectional co-routed active**	缺省情况下，未启用MPLS TE隧道接口的双向隧道功能，MPLS TE隧道接口上建立的隧道为MPLS TE单向隧道

表1-32 配置 Co-routed 方式 MPLS TE 双向隧道的被动方

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
在MPLS TE隧道接口上启用双向隧道功能，并指定本端为Co-routed方式MPLS TE双向隧道的被动方	**mpls te bidirectional co-routed passive reverse-lsp lsr-id** *ingress-lsr-id* **tunnel-id** *tunnel-id*	缺省情况下，未启用MPLS TE隧道接口的双向隧道功能，MPLS TE隧道接口上建立的隧道为MPLS TE单向隧道

表1-33 配置 Associated 方式 MPLS TE 双向隧道

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
在MPLS TE隧道接口上启用双向隧道功能，并指定双向隧道建立方式为Associated方式	**mpls te bidirectional associated reverse-lsp** { **lsp-name** *lsp-name* | **lsr-id** *ingress-lsr-id* **tunnel-id** *tunnel-id* } }	缺省情况下，未启用MPLS TE隧道接口的双向隧道功能，MPLS TE隧道接口上建立的隧道为MPLS TE单向隧道

1.11 配置CRLSP备份

CRLSP 备份用于端到端的路径保护，对整条 CRLSP 提供保护。只有使用 RSVP-TE 信令协议建立的 MPLS TE 隧道支持 CRLSP 备份。

请在 MPLS TE 隧道的 Ingress 节点上执行本配置。

表1-34 配置 CRLSP 备份

操作	命令	说明
进入系统视图	**system-view**	-
进入模式为MPLS TE隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
开启当前隧道的备份功能，并配置使用的备份模式	**mpls te backup** { **hot-standby** | **ordinary** }	缺省情况下，隧道不进行备份
配置主CRLSP应用的路径及路径的优先级	**mpls te path preference** *value* { **dynamic** | **explicit-path** *path-name* } [**no-cspf**]	缺省情况下，使用自动计算的路径建立主CRLSP
配置备份CRLSP应用的路径及路径的优先级	**mpls te backup-path preference** *value* { **dynamic** | **explicit-path** *path-name* } [**no-cspf**]	缺省情况下，使用自动计算的路径建立备份CRLSP

1.12 配置MPLS TE快速重路由

FRR 是 MPLS TE 中的临时性局部保护技术。配置 FRR 时需要注意：

- 建议不要在同一个接口同时配置快速重路由功能和 RSVP 认证功能。
- 只有使用 RSVP-TE 信令协议建立的 MPLS TE 隧道支持 FRR 功能。

1.12.1 开启快速重路由功能

请在主 CRLSP 的 Ingress 节点上开启快速重路由功能。

表1-35 开启快速重路由功能

操作	命令	说明
进入系统视图	**system-view**	-
进入主CRLSP对应的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
开启快速重路由功能	**mpls te fast-reroute** [**bandwidth**]	缺省情况下，快速重路由功能处于关闭状态 执行本命令时，如果指定了**bandwidth**参数，则表示主CRLSP需要进行带宽保护；否则，表示主CRLSP不需要进行带宽保护

1.12.2 在PLR上配置Bypass隧道

1. 功能简介

配置快速重路由时，需要在 PLR 上配置 Bypass 隧道。Bypass 隧道的配置方式有如下两种：

- 手工配置 Bypass 隧道：在 PLR 上创建一条 MPLS TE 隧道，该 MPLS TE 隧道作为主 CRLSP 的 Bypass 隧道。指定该 Bypass 隧道可以保护的带宽和 CT 类型，并在主 CRLSP 的出接口

上将该 Bypass 隧道与出接口绑定。当出接口连接的链路或节点出现故障时，可将流量切换到 Bypass 隧道转发，以避免流量中断。

- 自动创建 Bypass 隧道：在 PLR 上开启自动隧道备份功能后，PLR 为经过它的所有主 CRLSP 都自动建立一条链路保护的 Bypass 隧道和一条节点保护的 Bypass 隧道。自动创建的 Bypass 隧道可以保护所有 CT 类型，且不限制保护带宽，即不能够提供带宽保护。自动创建 Bypass 隧道可以简化配置，该功能又称为自动快速重路由（auto FRR）功能。

手工为主 CRLSP 配置 Bypass 隧道或为主 CRLSP 自动建立 Bypass 隧道后，该 Bypass 隧道将与主 CRLSP 关联。一条主 CRLSP 同时最多可以与 3 条手工创建的 Bypass 隧道和 2 条自动创建的 Bypass 隧道关联，PLR 从中选择一条 Bypass 隧道保护主 CRLSP，即为主 CRLSP 绑定该 Bypass 隧道。

PLR 为主 CRLSP 选择 Bypass 隧道时，优先选择手工创建的 Bypass 隧道。如果不存在手工创建的 Bypass 隧道，则选择自动创建的 Bypass 隧道，且自动创建的节点保护类型的 Bypass 隧道优于链路保护类型的 Bypass 隧道。

如果 PLR 上同时存在多条手工配置的 Bypass 隧道，则选择原则为：

(1) 根据主CRLSP所需带宽、主CRLSP是否需要进行带宽保护和Bypass隧道能否提供带宽保护，按照 表 1-36 所示的原则选择Bypass隧道。

表1-36 FRR 保护规则

主 CRLSP 所需带宽	主 CRLSP 是否需要进行带宽保护	Bypass 隧道能够提供带宽保护，即配置保护带宽为具体的带宽值	Bypass 隧道不能提供带宽保护，即配置保护带宽为 un-limited
0	是	不能绑定	没有指定Bypass隧道保护流量的CT类型或指定该CT类型为CT0时，可以绑定；否则，无法绑定 绑定后RRO无带宽保护标记，即Bypass隧道不会为主CRLSP提供带宽保护，Bypass隧道尽力转发主CRLSP的流量
	否		
非0	是	Bypass隧道的保护带宽大于等于主CRLSP所需带宽，且没有指定Bypass隧道保护流量的CT类型或Bypass隧道保护流量与主CRLSP流量的CT类型相同时，可以绑定；否则，无法绑定 主CRLSP优选此Bypass隧道 绑定后RRO设置带宽保护标记，即Bypass隧道为主CRLSP提供带宽保证	没有指定Bypass隧道保护流量的CT类型或Bypass隧道保护流量与主CRLSP流量的CT类型相同时，可以绑定；否则，无法绑定 不存在能够提供带宽保护、且满足条件的Bypass隧道时，才会绑定此Bypass隧道 绑定后RRO无带宽保护标记
非0	否	Bypass隧道的保护带宽大于等于主CRLSP所需带宽，且没有指定Bypass隧道保护流量的CT类型或Bypass隧道保护流量与主CRLSP流量的CT类型相同时，可以绑定；否则，无法绑定 不存在不能够提供带宽保护的Bypass隧道时，才会绑定此Bypass隧道 绑定后RRO设置带宽保护标记	没有指定Bypass隧道保护流量的CT类型或Bypass隧道保护流量与主CRLSP流量的CT类型相同时，可以绑定；否则，无法绑定 主CRLSP优选此Bypass隧道 绑定后RRO无带宽保护标记

(2) 节点保护的 Bypass 隧道优于链路保护的 Bypass 隧道

(3) 编号小的 Bypass 隧道优于编号大的 Bypass 隧道。

2. 配置限制和指导

在 PLR 上配置 Bypass 隧道时，需要注意：

- 由于 FRR 使用的 Bypass 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快速重路由保护。
- 用户在配置时应保证 Bypass 隧道的带宽不小于被保护的所有主 CRLSP 所需带宽之和，否则可能导致部分主 CRLSP 不能被 Bypass 隧道保护。
- Bypass 隧道一般不转发数据。如果 Bypass 隧道在保护主 CRLSP 的同时转发流量，需要为 Bypass 隧道提供足够的带宽。
- Bypass 隧道不能作为 VPN 等业务的承载隧道。
- 不能为 Bypass 隧道配置快速重路由功能。也就是说，Bypass 隧道不能同时作为主 CRLSP 被其他 Bypass 隧道保护，隧道不能被嵌套保护。
- Bypass 隧道不能经过被保护的接口或节点。
- 不要求带宽保护的主 CRLSP 和提供保护带宽的 Bypass 隧道绑定成功后，主 CRLSP 占用 Bypass 隧道的保护带宽。提供带宽保护的 Bypass 隧道的保护带宽先到先得，需要带宽保护的主 CRLSP 并不能抢占不需要带宽保护的主 CRLSP。
- 发生 FRR 切换后，如果修改 Bypass 隧道的保护带宽，使得保护带宽类型不同、保护带宽不够或者引起 FRR 保护类型（是否为主 CRLSP 提供带宽保护）变化，都将导致主 CRLSP Down。

3. 手工配置Bypass隧道

Bypass 隧道的建立方法与普通 MPLS TE 隧道相同，此处不再赘述，只介绍快速重路由功能相关的配置。

表1-37 在 PLR 上配置 Bypass 隧道

操作	命令	说明
进入系统视图	**system-view**	-
进入Bypass隧道的Tunnel接口视图	**interface tunnel** *tunnel-number* [**mode mpls-te**]	-
配置Bypass隧道的目的地址	**destination** *ip-address*	隧道的目的地址应配置为MP设备的LSR ID
配置Bypass隧道可以保护的带宽和CT类型	**mpls te backup bandwidth** [**ct0** | **ct1** | **ct2** | **ct3**] { *bandwidth* | **un-limited** }	缺省情况下，未指定Bypass隧道可以保护的带宽和CT类型 对于Bypass隧道，必须使用本命令配置可保护的带宽。否则，将导致主CRLSP不能绑定到Bypass隧道
退回系统视图	**quit**	-
进入主CRLSP出接口的接口视图	**interface** *interface-type interface-number*	-
为被保护的接口（当前接口）指定一条Bypass隧道	**mpls te fast-reroute bypass-tunnel tunnel** *tunnel-number*	缺省情况下，接口上不存在任何Bypass隧道

4. 自动创建Bypass隧道

自动创建 Bypass 隧道时需要注意：倒数第二跳节点作为 PLR 时，不会自动创建节点保护类型的 Bypass 隧道。

表1-38 在 PLR 上自动创建 Bypass 隧道

操作	命令	说明
进入系统视图	**system-view**	-
进入MPLS TE视图	**mpls te**	-
全局开启自动隧道备份功能，并进入MPLS TE自动隧道备份视图	**auto-tunnel backup**	缺省情况下，自动隧道备份功能处于全局关闭状态
配置自动创建的Bypass隧道的接口编号范围	**tunnel-number min** *min-number* **max** *max-number*	缺省情况下，未指定自动创建Bypass隧道的接口编号范围，不能自动创建Bypass隧道 全局开启自动隧道备份功能后，必须配置本命令，才能自动建立Bypass隧道
（可选）配置仅自动创建链路保护类型的Bypass隧道	**nhop-only**	缺省情况下，链路保护和节点保护的Bypass隧道都会自动创建 配置本命令后，已自动创建的节点保护类型的Bypass隧道会被删除
（可选）配置空闲Bypass隧道的自动清除时间	**timers removal unused** *seconds*	缺省情况下，空闲Bypass隧道的自动清除时间为3600秒
（可选）退回系统视图	**quit**	-
（可选）进入接口视图	**interface** *interface-type interface-number*	-
（可选）关闭接口的自动隧道备份功能	**mpls te auto-tunnel backup disable**	缺省情况下，全局开启了自动隧道备份功能后，所有使能RSVP能力的接口都会开启自动隧道备份功能，允许自动创建Bypass隧道 配置本命令后，已自动创建的保护该接口的Bypass隧道会被删除

1.12.3 配置节点故障检测

如果使用 FRR 进行节点保护，则在 PLR 和被保护节点上可以进行本配置，以便通过 Hello 机制或 BFD 检测到节点故障；如果只是进行链路保护，则不必进行本配置。

对于 PLR 和被保护节点之间链路故障引发的节点失效，不需要使用 RSVP 的 Hello 机制或 BFD 来进行节点故障检测。本配置主要用于在链路正常但信令协议故障的特殊情况下检测节点故障。

表1-39 配置节点故障检测

操作	命令	说明
进入系统视图	**system-view**	-
进入PLR与被保护节点直连接口的接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
开启RSVP的Hello扩展功能	**rsvp hello enable**	二者选其一 缺省情况下，RSVP的Hello扩展功能处于关闭状态；不会通过BFD检测本地设备和RSVP邻居之间链路的状态 **rsvp hello enable**和**rsvp bfd enable**命令的详细介绍，请参见“MPLS配置指导”中的“RSVP”
配置通过BFD检测本地设备和RSVP邻居之间链路的状态	**rsvp bfd enable**	

1.12.4 配置快速重路由的Bypass隧道优选时间间隔

如果为一条主 CRLSP 指定了多条 Bypass 隧道，MPLS TE 会从中选择一条最优的 Bypass 隧道，当主 CRLSP 出现故障时，将流量切换到该 Bypass 隧道转发。在某些情况下（如 Bypass 隧道的可预留带宽发生变化），当前的最优隧道可能不是之前选中的 Bypass 隧道。因此，MPLS TE 需要周期性地选择最优的 Bypass 隧道。通过本配置可以调整 Bypass 隧道优选的周期。

请在 PLR 节点上进行本配置。

表1-40 配置快速重路由的 Bypass 隧道优选时间间隔

操作	命令	说明
进入系统视图	**system-view**	-
进入MPLS TE视图	**mpls te**	-
配置在多条Bypass隧道中进行优选的时间间隔	**fast-reroute timer** *interval*	缺省情况下，在多条Bypass隧道中进行优选的时间间隔为300秒

1.13 开启告警功能

开启 MPLS TE 模块的告警功能后，当 MPLS TE 状态发生变化时会产生 RFC 3812 中规定的告警信息。生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。

有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

表1-41 开启告警功能

操作	命令	说明
进入系统视图	**system-view**	-
开启MPLS TE模块的告警功能	**snmp-agent trap enable te**	缺省情况下，MPLS TE模块的告警功能处于开启状态

1.14 MPLS TE显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 MPLS TE 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 MPLS TE 统计信息。

表1-42 MPLS TE 的显示和维护

操作	命令
显示显式路径的信息	**display explicit-path** [*path-name*]
显示DS-TE相关信息	**display mpls te ds-te**
显示开启了MPLS TE的接口上的带宽相关信息	**display mpls te link-management bandwidth-allocation** [**interface** *interface-type interface-number*]
显示MPLS TE隧道接口的信息	**display mpls te tunnel-interface** [**tunnel** *number*]
显示OSPF TEDB中的链路和节点信息	**display ospf** [*process-id*] [**area** *area-id*] **mpls te advertisement** [**originate-router** *advertising-router-id* | **self-originate**]
显示OSPF TEDB中的Network信息	**display ospf** [*process-id*] [**area** *area-id*] **mpls te network** [**originate-router** *advertising-router-id* | **self-originate**]
显示OSPF的Tunnel接口信息	**display ospf** [*process-id*] [**area** *area-id*] **mpls te tunnel**
显示IS-IS TEDB中的链路和节点信息	**display isis mpls te advertisement** [[**level-1** | **level-2**] | [**originate-system** *system-id* | **local**] | **verbose**] * [*process-id*]
显示IS-IS TEDB中的网络信息	**display isis mpls te network** [[**level-1** | **level-2**] | **local** | **lsp-id** *lsp-id*]* [*process-id*]
显示IS-IS 的Tunnel接口信息	**display isis mpls te tunnel** [**level-1** | **level-2**] [*process-id*]
显示IS-IS TE配置的子TLV类型值信息	**display isis mpls te configured-sub-tlvs** [*process-id*]
显示隧道捆绑接口及其成员接口的信息	**display tunnel-bundle** [*number*]
显示MPLS TEDB信息	**display mpls te tedb** { { **isis** { **level-1** | **level-2** } | **ospf area** *area-id* } | **link** *ip-address* | **network** | **node** [**local** | *mpls-lsr-id*] | **summary** }
重启自动带宽调整功能	**reset mpls te auto-bandwidth-adjustment timers**

1.15 MPLS TE典型配置举例

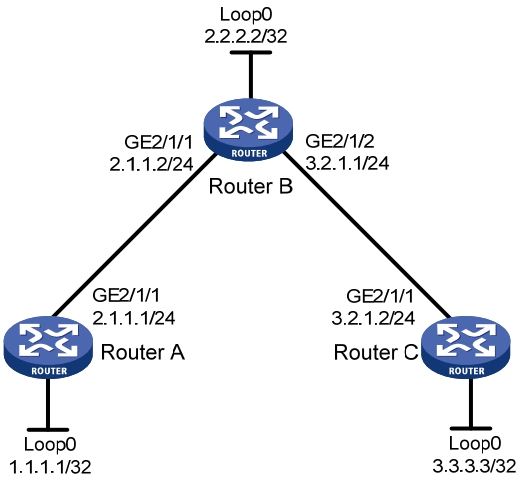
1.15.1 使用静态CRLSP配置MPLS TE隧道示例

1. 组网需求

- 设备 Router A、Router B 和 Router C 运行 IS-IS；
- 使用静态 CRLSP 建立一条 Router A 到 Router C 的 MPLS TE 隧道，隧道需要的带宽为 2000kbps；
- 隧道沿途的链路最大带宽为 10000kbps，最大可预留带宽为 5000kbps。

2. 组网图

图1-7 静态 CRLSP 配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址

按照 图 1-7 配置各接口的IP地址和掩码，具体配置过程略。

(2) 配置 IS-IS 协议发布接口所在网段的路由，包括 Loopback 接口

配置 Router A。

```
<RouterA> system-view
[RouterA] isis 1
[RouterA-isis-1] network-entity 00.0005.0000.0000.0001.00
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] isis enable 1
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface loopback 0
[RouterA-LoopBack0] isis enable 1
[RouterA-LoopBack0] quit
```

配置 Router B。

```
<RouterB> system-view
[RouterB] isis 1
[RouterB-isis-1] network-entity 00.0005.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] isis enable 1
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] isis enable 1
[RouterB-GigabitEthernet2/1/2] quit
[RouterB] interface loopback 0
[RouterB-LoopBack0] isis enable 1
[RouterB-LoopBack0] quit
```

配置 Router C。

```
<RouterC> system-view
[RouterC] isis 1
[RouterC-isis-1] network-entity 00.0005.0000.0000.0003.00
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] isis enable 1
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface loopback 0
[RouterC-LoopBack0] isis enable 1
[RouterC-LoopBack0] quit
```

配置完成后，在各设备上执行 **display ip routing-table** 命令，可以看到相互之间都学到了到对方的路由，包括 Loopback 接口对应的主机路由。

(3) 配置 LSR ID、开启 MPLS 能力和 MPLS TE 能力

配置 Router A。

```
[RouterA] mpls lsr-id 1.1.1.1
[RouterA] mpls te
[RouterA-te] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mpls enable
[RouterA-GigabitEthernet2/1/1] mpls te enable
[RouterA-GigabitEthernet2/1/1] quit
```

配置 Router B。

```
[RouterB] mpls lsr-id 2.2.2.2
[RouterB] mpls te
[RouterB-te] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mpls enable
[RouterB-GigabitEthernet2/1/1] mpls te enable
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] mpls enable
[RouterB-GigabitEthernet2/1/2] mpls te enable
[RouterB-GigabitEthernet2/1/2] quit
```

配置 Router C。

```
[RouterC] mpls lsr-id 3.3.3.3
[RouterC] mpls te
[RouterC-te] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] mpls enable
[RouterC-GigabitEthernet2/1/1] mpls te enable
[RouterC-GigabitEthernet2/1/1] quit
```

(4) 配置链路的 MPLS TE 属性

在 Router A 上配置链路的最大带宽和最大可预留带宽。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
```

```
[RouterA-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth 5000
[RouterA-GigabitEthernet2/1/1] quit
```

在 Router B 上配置链路的最大带宽和最大可预留带宽。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterB-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth 5000
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] mpls te max-link-bandwidth 10000
[RouterB-GigabitEthernet2/1/2] mpls te max-reservable-bandwidth 5000
[RouterB-GigabitEthernet2/1/2] quit
```

在 Router C 上配置链路的最大带宽和最大可预留带宽。

```
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterC-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth 5000
[RouterC-GigabitEthernet2/1/1] quit
```

(5) 配置 MPLS TE 隧道

在 Router A 上配置 MPLS TE 隧道 Tunnel0：目的地址为 Router C 的 LSR ID（3.3.3.3）；采用静态 CRLSP 建立 MPLS TE 隧道。

```
[RouterA] interface tunnel 0 mode mpls-te
[RouterA-Tunnel0] ip address 6.1.1.1 255.255.255.0
[RouterA-Tunnel0] destination 3.3.3.3
[RouterA-Tunnel0] mpls te signaling static
[RouterA-Tunnel0] quit
```

(6) 创建静态 CRLSP

配置 Router A 为静态 CRLSP 的 Ingress 节点，下一跳地址为 2.1.1.2，出标签为 20，隧道所需的带宽为 2000kbps。

```
[RouterA] static-cr-lsp ingress static-cr-lsp-1 nexthop 2.1.1.2 out-label 20 bandwidth 2000
```

在 Router A 上配置隧道 Tunnel0 引用名称为 static-cr-lsp-1 的静态 CRLSP。

```
[RouterA] interface tunnel 0
[RouterA-Tunnel0] mpls te static-cr-lsp static-cr-lsp-1
[RouterA-Tunnel0] quit
```

配置 Router B 为静态 CRLSP 的 Transit 节点，入标签为 20，下一跳地址为 3.2.1.2，出标签为 30，隧道所需的带宽为 2000kbps。

```
[RouterB] static-cr-lsp transit static-cr-lsp-1 in-label 20 nexthop 3.2.1.2 out-label 30
bandwidth 2000
```

配置 Router C 为静态 CRLSP 的 Egress 节点，入标签为 30。

```
[RouterC] static-cr-lsp egress static-cr-lsp-1 in-label 30
```

(7) 配置静态路由使流量沿 MPLS TE 隧道转发

在 Router A 上配置静态路由，使得到达网络 3.2.1.0/24 的流量通过 MPLS TE 隧道接口 Tunnel0 转发。

```
[RouterA] ip route-static 3.2.1.2 24 tunnel 0 preference 1
```

4. 验证配置

配置完成后，在 Router A 上执行 **display interface tunnel** 命令，可以看到 Tunnel 接口的状态为 up。

```
[RouterA] display interface tunnel
Tunnel0
Current state: UP
Line protocol state: UP
Description: Tunnel0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1496
Internet Address is 6.1.1.1/24 Primary
Tunnel source unknown, destination 3.3.3.3
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

在 Router A 上执行 **display mpls te tunnel-interface** 命令，可以看到 MPLS TE 隧道的建立情况。

```
[RouterA] display mpls te tunnel-interface
Tunnel Name            : Tunnel 0
Tunnel State           : Up (Main CRLSP up)
Tunnel Attributes      :
  LSP ID               : 1              Tunnel ID            : 0
  Admin State          : Normal
  Ingress LSR ID       : 1.1.1.1        Egress LSR ID        : 3.3.3.3
  Signaling            : Static         Static CRLSP Name    : static-cr-lsp-1
  Resv Style           : -
  Tunnel mode          : -
  Reverse-LSP name     : -
  Reverse-LSP LSR ID   : -              Reverse-LSP Tunnel ID: -
  Class Type           : -              Tunnel Bandwidth     : -
  Reserved Bandwidth   : -
  Setup Priority       : 0              Holding Priority     : 0
  Affinity Attr/Mask   : -/-
  Explicit Path        : -
  Backup Explicit Path : -
  Metric Type          : TE
  Record Route         : -              Record Label         : -
  FRR Flag             : -              Bandwidth Protection : -
  Backup Bandwidth Flag: -              Backup Bandwidth Type: -
  Backup Bandwidth     : -
  Bypass Tunnel        : -              Auto Created         : -
```

```
  Route Pinning        : -
  Retry Limit          : 3              Retry Interval       : 2 sec
  Reoptimization       : -              Reoptimization Freq  : -
  Backup Type          : -              Backup LSP ID        : -
  Auto Bandwidth       : -              Auto Bandwidth Freq  : -
  Min Bandwidth        : -              Max Bandwidth        : -
  Collected Bandwidth  : -
```

在各设备上执行 **display mpls lsp** 或 **display mpls static-cr-lsp** 命令，可以看到静态 CRLSP 的建立情况。

```
[RouterA] display mpls lsp
FEC                       Proto    In/Out Label    Interface/Out NHLFE
1.1.1.1/0/1               StaticCR -/20            GE2/1/1
2.1.1.2                   Local    -/-             GE2/1/1
[RouterB] display mpls lsp
FEC                       Proto    In/Out Label    Interface/Out NHLFE
-                         StaticCR 20/30           GE2/1/2
3.2.1.2                   Local    -/-             GE2/1/2
[RouterC] display mpls lsp
FEC                       Proto    In/Out Label    Interface/Out NHLFE
-                         StaticCR 30/-            -
[RouterA] display mpls static-cr-lsp
Name            LSR Type    In/Out Label   Out Interface        State
static-cr-lsp-1 Ingress     Null/20        GE2/1/1               Up
[RouterB] display mpls static-cr-lsp
Name            LSR Type    In/Out Label   Out Interface        State
static-cr-lsp-1 Transit     20/30          GE2/1/2               Up
[RouterC] display mpls static-cr-lsp
Name            LSR Type    In/Out Label   Out Interface        State
static-cr-lsp-1 Egress      30/Null        -                    Up
```

在 RouterA 上执行 **display ip routing-table** 命令，可以看到路由表中有以 Tunnel0 为出接口的静态路由信息。

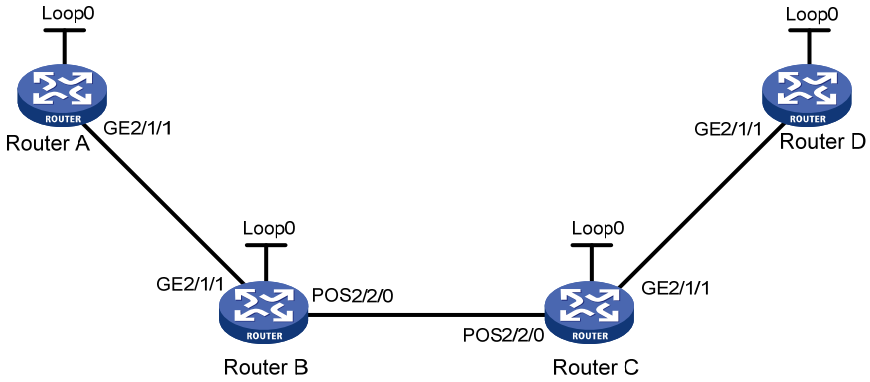
1.15.2 使用RSVP-TE配置MPLS TE隧道示例

1. 组网需求

- 设备 Router A、Router B、Router C 和 Router D 运行 IS-IS，都是 Level-2 设备；
- 使用 RSVP-TE 建立一条从 Router A 到 Router D 的 MPLS TE 隧道，隧道需要的带宽为 2000kbps；
- 隧道沿途的链路最大带宽为 10000kbps，最大可预留带宽为 5000kbps。

2. 组网图

图1-8 使用 RSVP-TE 配置 MPLS TE 隧道组网图



设备	接口	IP地址	设备	接口	IP地址
Router A	Loop0	1.1.1.9/32	Router C	Loop0	3.3.3.9/32
	GE2/1/1	10.1.1.1/24		GE2/1/1	30.1.1.1/24
Router B	Loop0	2.2.2.9/32		POS2/2/0	20.1.1.2/24
	GE2/1/1	10.1.1.2/24	Router D	Loop0	4.4.4.9/32
	POS2/2/0	20.1.1.1/24		GE2/1/1	30.1.1.2/24

3. 配置步骤

(1) 配置各接口的 IP 地址

按照 图 1-8 配置各接口的IP地址和掩码，具体配置过程略。

(2) 配置 IS-IS 协议发布接口所在网段的路由，包括 Loopback 接口

配置 Router A。

```
<RouterA> system-view
[RouterA] isis 1
[RouterA-isis-1] network-entity 00.0005.0000.0000.0001.00
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] isis enable 1
[RouterA-GigabitEthernet2/1/1] isis circuit-level level-2
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface loopback 0
[RouterA-LoopBack0] isis enable 1
[RouterA-LoopBack0] isis circuit-level level-2
[RouterA-LoopBack0] quit
```

配置 Router B。

```
<RouterB> system-view
[RouterB] isis 1
[RouterB-isis-1] network-entity 00.0005.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] isis enable 1
[RouterB-GigabitEthernet2/1/1] isis circuit-level level-2
[RouterB-GigabitEthernet2/1/1] quit
```

```
[RouterB] interface pos 2/2/0
[RouterB-POS2/2/0] isis enable 1
[RouterB-POS2/2/0] isis circuit-level level-2
[RouterB-POS2/2/0] quit
[RouterB] interface loopback 0
[RouterB-LoopBack0] isis enable 1
[RouterB-LoopBack0] isis circuit-level level-2
[RouterB-LoopBack0] quit
```

配置 Router C。

```
<RouterC> system-view
[RouterC] isis 1
[RouterC-isis-1] network-entity 00.0005.0000.0000.0003.00
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] isis enable 1
[RouterC-GigabitEthernet2/1/1] isis circuit-level level-2
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface pos 2/2/0
[RouterC-POS2/2/0] isis enable 1
[RouterC-POS2/2/0] isis circuit-level level-2
[RouterC-POS2/2/0] quit
[RouterC] interface loopback 0
[RouterC-LoopBack0] isis enable 1
[RouterC-LoopBack0] isis circuit-level level-2
[RouterC-LoopBack0] quit
```

配置 Router D。

```
<RouterD> system-view
[RouterD] isis 1
[RouterD-isis-1] network-entity 00.0005.0000.0000.0004.00
[RouterD-isis-1] quit
[RouterD] interface gigabitethernet 2/1/1
[RouterD-GigabitEthernet2/1/1] isis enable 1
[RouterD-GigabitEthernet2/1/1] isis circuit-level level-2
[RouterD-GigabitEthernet2/1/1] quit
[RouterD] interface loopback 0
[RouterD-LoopBack0] isis enable 1
[RouterD-LoopBack0] isis circuit-level level-2
[RouterD-LoopBack0] quit
```

配置完成后，在各设备上执行 **display ip routing-table** 命令，可以看到相互之间都学到了到对方的路由，包括 Loopback 接口对应的主机路由。

(3) 配置 LSR ID，开启 MPLS、MPLS TE 和 RSVP-TE 能力

配置 Router A。

```
[RouterA] mpls lsr-id 1.1.1.9
[RouterA] mpls te
[RouterA-te] quit
[RouterA] rsvp
[RouterA-rsvp] quit
```

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mpls enable
[RouterA-GigabitEthernet2/1/1] mpls te enable
[RouterA-GigabitEthernet2/1/1] rsvp enable
[RouterA-GigabitEthernet2/1/1] quit
```

配置 Router B。

```
[RouterB] mpls lsr-id 2.2.2.9
[RouterB] mpls te
[RouterB-te] quit
[RouterB] rsvp
[RouterB-rsvp] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mpls enable
[RouterB-GigabitEthernet2/1/1] mpls te enable
[RouterB-GigabitEthernet2/1/1] rsvp enable
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface pos 2/1/0
[RouterB-POS2/2/0] mpls enable
[RouterB-POS2/2/0] mpls te enable
[RouterB-POS2/2/0] rsvp enable
[RouterB-POS2/2/0] quit
```

配置 Router C。

```
[RouterC] mpls lsr-id 3.3.3.9
[RouterC] mpls te
[RouterC-te] quit
[RouterC] rsvp
[RouterC-rsvp] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] mpls enable
[RouterC-GigabitEthernet2/1/1] mpls te enable
[RouterC-GigabitEthernet2/1/1] rsvp enable
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface pos 2/2/0
[RouterC-POS2/2/0] mpls enable
[RouterC-POS2/2/0] mpls te enable
[RouterC-POS2/2/0] rsvp enable
[RouterC-POS2/2/0] quit
```

配置 Router D。

```
[RouterD] mpls lsr-id 4.4.4.9
[RouterD] mpls te
[RouterD-te] quit
[RouterD] rsvp
[RouterD-rsvp] quit
[RouterD] interface gigabitethernet 2/1/1
[RouterD-GigabitEthernet2/1/1] mpls enable
[RouterD-GigabitEthernet2/1/1] mpls te enable
[RouterD-GigabitEthernet2/1/1] rsvp enable
[RouterD-GigabitEthernet2/1/1] quit
```

(4) 配置 IS-IS TE

配置 Router A。

```
[RouterA] isis 1
[RouterA-isis-1] cost-style wide
[RouterA-isis-1] mpls te enable level-2
[RouterA-isis-1] quit
```

配置 Router B。

```
[RouterB] isis 1
[RouterB-isis-1] cost-style wide
[RouterB-isis-1] mpls te enable level-2
[RouterB-isis-1] quit
```

配置 Router C。

```
[RouterC] isis 1
[RouterC-isis-1] cost-style wide
[RouterC-isis-1] mpls te enable level-2
[RouterC-isis-1] quit
```

配置 Router D。

```
[RouterD] isis 1
[RouterD-isis-1] cost-style wide
[RouterD-isis-1] mpls te enable level-2
[RouterD-isis-1] quit
```

(5) 配置链路的 MPLS TE 属性

在 Router A 上配置链路的最大带宽和最大可预留带宽。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterA-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth 5000
[RouterA-GigabitEthernet2/1/1] quit
```

在 Router B 上配置链路的最大带宽和最大可预留带宽。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterB-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth 5000
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface pos 2/2/0
[RouterB-POS2/2/0] mpls te max-link-bandwidth 10000
[RouterB-POS2/2/0] mpls te max-reservable-bandwidth 5000
[RouterB-POS2/2/0] quit
```

在 Router C 上配置链路的最大带宽和最大可预留带宽。

```
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterC-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth 5000
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface pos 2/2/0
[RouterC-POS2/2/0] mpls te max-link-bandwidth 10000
[RouterC-POS2/2/0] mpls te max-reservable-bandwidth 5000
[RouterC-POS2/2/0] quit
```

在 Router D 上配置链路的最大带宽和最大可预留带宽。

```
[RouterD] interface gigabitethernet 2/1/1
[RouterD-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterD-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth 5000
[RouterD-GigabitEthernet2/1/1] quit
```

(6) 配置 MPLS TE 隧道

在 Router A 上配置 MPLS TE 隧道 Tunnel1：目的地址为 Router D 的 LSR ID（4.4.4.9）；采用 RSVP-TE 信令协议建立 MPLS TE 隧道；隧道所需的带宽为 2000kbps。

```
[RouterA] interface tunnel 1 mode mpls-te
[RouterA-Tunnel1] ip address 7.1.1.1 255.255.255.0
[RouterA-Tunnel1] destination 4.4.4.9
[RouterA-Tunnel1] mpls te signaling rsvp-te
[RouterA-Tunnel1] mpls te bandwidth 2000
[RouterA-Tunnel1] quit
```

(7) 配置静态路由使流量沿 MPLS TE 隧道转发

在 Router A 上配置静态路由，使得到达网络 30.1.1.0/24 的流量通过 MPLS TE 隧道接口 Tunnel1 转发。

```
[RouterA] ip route-static 30.1.1.2 24 tunnel 1 preference 1
```

4. 验证配置

配置完成后，在 Router A 上执行 **display interface tunnel** 命令可以看到隧道接口状态为 up。

```
[RouterA] display interface tunnel
Tunnel1 current state: UP
Line protocol current state: UP
Description: Tunnel1 Interface
The Maximum Transmit Unit is 64000
Internet Address is 7.1.1.1/24 Primary
Tunnel source unknown, destination 4.4.4.9
Tunnel bandwidth 64 (kbps)
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Last clearing of counters: Never
    Last 300 seconds input:  0 bytes/sec, 0 packets/sec
    Last 300 seconds output:  0 bytes/sec, 0 packets/sec
    0 packets input,  0 bytes
    0 input error
    0 packets output,  0 bytes
    0 output error
```

在 Router A 上执行 **display mpls te tunnel-interface** 命令可以看到隧道的详细信息。

```
[RouterA] display mpls te tunnel-interface
Tunnel Name            : Tunnel 1
Tunnel State           : Up (Main CRLSP up, Shared-resource CRLSP down)
Tunnel Attributes      :
  LSP ID               : 23331           Tunnel ID            : 1
  Admin State          : Normal
  Ingress LSR ID       : 1.1.1.9         Egress LSR ID        : 4.4.4.9
  Signaling            : RSVP-TE         Static CRLSP Name    : -
  Resv Style           : SE
```

```
Tunnel mode          : -
Reverse-LSP name     : -
Reverse-LSP LSR ID   : -                Reverse-LSP Tunnel ID: -
Class Type           : CT0              Tunnel Bandwidth     : 2000 kbps
Reserved Bandwidth   : 2000 kbps
Setup Priority       : 7                Holding Priority     : 7
Affinity Attr/Mask   : 0/0
Explicit Path        : -
Backup Explicit Path : -
Metric Type          : TE
Record Route         : Disabled         Record Label         : Disabled
FRR Flag             : Disabled         Bandwidth Protection : Disabled
Backup Bandwidth Flag: Disabled         Backup Bandwidth Type: -
Backup Bandwidth     : -
Bypass Tunnel        : No               Auto Created         : No
Route Pinning        : Disabled
Retry Limit          : 10               Retry Interval       : 2 sec
Reoptimization       : Disabled         Reoptimization Freq  : -
Backup Type          : None             Backup LSP ID        : -
Auto Bandwidth       : Disabled         Auto Bandwidth Freq  : -
Min Bandwidth        : -                Max Bandwidth        : -
Collected Bandwidth  : -
```

在 Router A 上执行 **display ip routing-table** 命令，可以看到路由表中有以 Tunnel1 为出接口的静态路由信息。

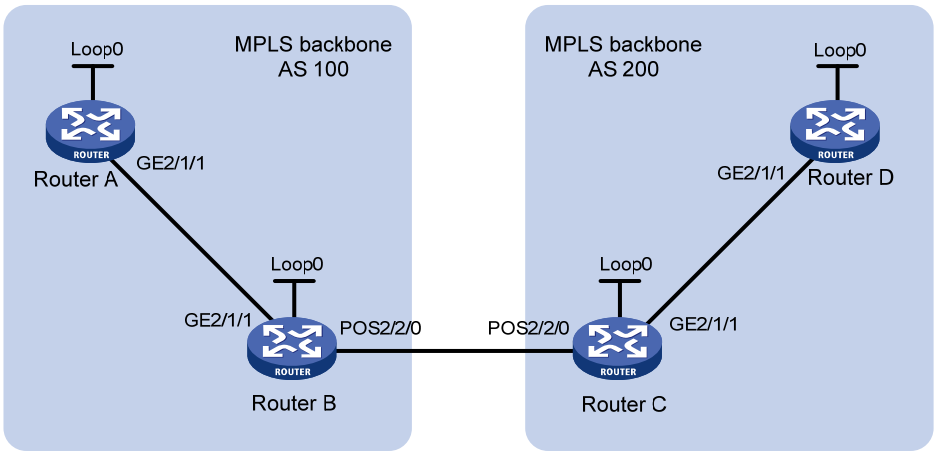
1.15.3 使用RSVP-TE配置跨域的MPLS TE隧道示例

1. 组网需求

- Router A 和 Router B 位于 AS 100 内，AS 100 内使用 OSPF 作为 IGP 协议。
- Router C 和 Router D 位于 AS 200 内，AS 200 内使用 OSPF 作为 IGP 协议。
- 在作为 ASBR 的 Router B 和 Router C 之间建立 EBGP 连接，配置 BGP 引入 OSPF 路由，OSPF 进程引入 BGP 路由，使得 AS 100 和 AS 200 之间路由可达。
- 使用 RSVP-TE 从 Router A 到 Router D 建立一条跨域的 MPLS TE 隧道，隧道所需带宽为 2000kbps。
- 隧道沿途的链路最大带宽为 10000kbps，最大可预留带宽为 5000kbps。

2. 组网图

图1-9 使用 RSVP-TE 配置跨域的 MPLS TE 隧道组网图



设备	接口	IP地址	设备	接口	IP地址
Router A	Loop0	1.1.1.9/32	Router C	Loop0	3.3.3.9/32
	GE2/1/1	10.1.1.1/24		GE2/1/1	30.1.1.1/24
Router B	Loop0	2.2.2.9/32		POS2/2/0	20.1.1.2/24
	GE2/1/1	10.1.1.2/24	Router D	Loop0	4.4.4.9/32
	POS2/2/0	20.1.1.1/24		GE2/1/1	30.1.1.2/24

3. 配置步骤

(1) 配置各接口的 IP 地址

按照 图 1-9 配置各接口的IP地址和掩码，具体配置过程略。

(2) 配置使用 OSPF 在 AS 内发布路由信息，并在 Router B 和 Router C 上配置 OSPF 引入直连路由和 BGP 路由

配置 Router A。

```
<RouterA> system-view
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

配置 Router B。

```
<RouterB> system-view
[RouterB] ospf
[RouterB-ospf-1] import-route direct
[RouterB-ospf-1] import-route bgp
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

配置 Router C。

```
<RouterC> system-view
[RouterC] ospf
[RouterC-ospf-1] import-route direct
[RouterC-ospf-1] import-route bgp
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

配置 Router D。

```
<RouterD> system-view
[RouterD] ospf
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] network 4.4.4.9 0.0.0.0
[RouterD-ospf-1-area-0.0.0.0] quit
[RouterD-ospf-1] quit
```

配置完成后，在各设备上执行 **display ip routing-table** 命令，可以看到 AS 内的设备之间都学到了到对方的路由，包括 Loopback 接口对应的主机路由。以 Router A 为例：

```
[RouterA] display ip routing-table

Destinations : 6        Routes : 6

Destination/Mask    Proto  Pre  Cost         NextHop         Interfac
1.1.1.9/32          Direct 0    0            127.0.0.1       InLoop0
2.2.2.9/32          OSPF   10   1            10.1.1.2        GE2/1/1
10.1.1.0/24         Direct 0    0            10.1.1.1        GE2/1/1
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

(3) 在 Router B 和 Router C 之间配置 BGP，使得 AS 之间路由可达

配置 Router B。

```
[RouterB] bgp 100
[RouterB-bgp] peer 20.1.1.2 as-number 200
[RouterB-bgp] address-family ipv4 unicast
[RouterB-bgp-ipv4] peer 20.1.1.2 enable
[RouterB-bgp-ipv4] import-route ospf
[RouterB-bgp-ipv4] import-route direct
[RouterB-bgp-ipv4] quit
[RouterB-bgp] quit
```

配置 Router C。

```
[RouterC] bgp 200
[RouterC-bgp] peer 20.1.1.1 as-number 100
[RouterC-bgp] address-family ipv4 unicast
[RouterC-bgp-ipv4] peer 20.1.1.1 enable
[RouterC-bgp-ipv4] import-route ospf
[RouterC-bgp-ipv4] import-route direct
```

```
[RouterC-bgp-ipv4] quit
[RouterC-bgp] quit
```

配置完成后，在各设备上执行 **display ip routing-table** 命令，可以看到设备学习到了 AS 外部的路由。以 Router A 为例：

```
[RouterA] display ip routing-table

Destinations : 10       Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
1.1.1.9/32          Direct 0    0            127.0.0.1       InLoop0
2.2.2.9/32          OSPF   10   1            10.1.1.2        GE2/1/1
3.3.3.9/32          O_ASE  150  1            10.1.1.2        GE2/1/1
4.4.4.9/32          O_ASE  150  1            10.1.1.2        GE2/1/1
10.1.1.0/24         Direct 0    0            10.1.1.1        GE2/1/1
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         O_ASE  150  1            10.1.1.2        GE2/1/1
30.1.1.0/24         O_ASE  150  1            10.1.1.2        GE2/1/1
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

(4) 配置 LSR ID，开启 MPLS、MPLS TE 和 RSVP-TE 能力

配置 Router A。

```
[RouterA] mpls lsr-id 1.1.1.9
[RouterA] mpls te
[RouterA-te] quit
[RouterA] rsvp
[RouterA-rsvp] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mpls enable
[RouterA-GigabitEthernet2/1/1] mpls te enable
[RouterA-GigabitEthernet2/1/1] rsvp enable
[RouterA-GigabitEthernet2/1/1] quit
```

配置 Router B。

```
[RouterB] mpls lsr-id 2.2.2.9
[RouterB] mpls te
[RouterB-te] quit
[RouterB] rsvp
[RouterB-rsvp] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mpls enable
[RouterB-GigabitEthernet2/1/1] mpls te enable
[RouterB-GigabitEthernet2/1/1] rsvp enable
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface pos 2/2/0
[RouterB-POS2/2/0] mpls enable
[RouterB-POS2/2/0] mpls te enable
[RouterB-POS2/2/0] rsvp enable
[RouterB-POS2/2/0] quit
```

配置 Router C。

```
[RouterC] mpls lsr-id 3.3.3.9
[RouterC] mpls te
[RouterC-te] quit
[RouterC] rsvp
[RouterC-rsvp] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] mpls enable
[RouterC-GigabitEthernet2/1/1] mpls te enable
[RouterC-GigabitEthernet2/1/1] rsvp enable
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface pos 2/2/0
[RouterC-POS2/2/0] mpls enable
[RouterC-POS2/2/0] mpls te enable
[RouterC-POS2/2/0] rsvp enable
[RouterC-POS2/2/0] quit
```

配置 Router D。

```
[RouterD] mpls lsr-id 4.4.4.9
[RouterD] mpls te
[RouterD-te] quit
[RouterD] rsvp
[RouterD-rsvp] quit
[RouterD] interface gigabitethernet 2/1/1
[RouterD-GigabitEthernet2/1/1] mpls enable
[RouterD-GigabitEthernet2/1/1] mpls te enable
[RouterD-GigabitEthernet2/1/1] rsvp enable
[RouterD-GigabitEthernet2/1/1] quit
```

(5) 配置 OSPF TE

配置 Router A。

```
[RouterA] ospf
[RouterA-ospf-1] opaque-capability enable
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] mpls te enable
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

配置 Router B。

```
[RouterB] ospf
[RouterB-ospf-1] opaque-capability enable
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] mpls te enable
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

配置 Router C。

```
[RouterC] ospf
[RouterC-ospf-1] opaque-capability enable
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] mpls te enable
```

```
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

配置 Router D。

```
[RouterD] ospf
[RouterD-ospf-1] opaque-capability enable
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] mpls te enable
[RouterD-ospf-1-area-0.0.0.0] quit
[RouterD-ospf-1] quit
```

(6) 配置松散显式路径

在 Router A 上配置松散显式路径。

```
[RouterA] explicit-path atod
[RouterA-explicit-path-atod] nexthop 10.1.1.2 include loose
[RouterA-explicit-path-atod] nexthop 20.1.1.2 include strict
[RouterA-explicit-path-atod] nexthop 30.1.1.2 include loose
[RouterA-explicit-path-atod] quit
```

(7) 配置链路的 MPLS TE 属性

在 Router A 上配置链路的最大带宽和最大可预留带宽。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterA-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth 5000
[RouterA-GigabitEthernet2/1/1] quit
```

在 Router B 上配置链路的最大带宽和最大可预留带宽。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterB-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth 5000
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface pos 2/2/0
[RouterB-POS2/2/0] mpls te max-link-bandwidth 10000
[RouterB-POS2/2/0] mpls te max-reservable-bandwidth 5000
[RouterB-POS2/2/0] quit
```

在 Router C 上配置链路的最大带宽和最大可预留带宽。

```
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterC-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth 5000
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface pos 2/2/0
[RouterC-POS2/2/0] mpls te max-link-bandwidth 10000
[RouterC-POS2/2/0] mpls te max-reservable-bandwidth 5000
[RouterC-POS2/2/0] quit
```

在 Router D 上配置链路的最大带宽和最大可预留带宽。

```
[RouterD] interface gigabitethernet 2/1/1
[RouterD-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterD-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth 5000
[RouterD-GigabitEthernet2/1/1] quit
```

(8) 配置 MPLS TE 隧道

在 Router A 上配置 MPLS TE 隧道 Tunnel1：目的地址为 Router D 的 LSR ID（4.4.4.9）；采用 RSVP-TE 信令协议建立 MPLS TE 隧道；隧道所需的带宽为 2000kbps；为隧道指定显式路径 atod。

```
[RouterA] interface tunnel 1 mode mpls-te
[RouterA-Tunnel1] ip address 7.1.1.1 255.255.255.0
[RouterA-Tunnel1] destination 4.4.4.9
[RouterA-Tunnel1] mpls te signaling rsvp-te
[RouterA-Tunnel1] mpls te bandwidth 2000
[RouterA-Tunnel1] mpls te path preference 5 explicit-path atod
[RouterA-Tunnel1] quit
```

(9) 配置静态路由使流量沿 MPLS TE 隧道转发

在 Router A 上配置静态路由，使得到达网络 30.1.1.0/24 的流量通过 MPLS TE 隧道接口 Tunnel1 转发。

```
[RouterA] ip route-static 30.1.1.2 24 tunnel 1 preference 1
```

4. 验证配置

配置完成后，在 Router A 上执行 **display interface tunnel** 命令可以看到隧道接口状态为 up。

```
[RouterA] display interface tunnel 1
Tunnel1 current state: UP
Line protocol current state: UP
Description: Tunnel1 Interface
The Maximum Transmit Unit is 64000
Internet Address is 7.1.1.1/24 Primary
Tunnel source unknown, destination 4.4.4.9
Tunnel bandwidth 64 (kbps)
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Last clearing of counters: Never
    Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    3077 packets output, 197028 bytes, 0 drops
```

在 Router A 上执行 **display mpls te tunnel-interface** 命令可以看到隧道的详细信息。

```
[RouterA] display mpls te tunnel-interface
Tunnel Name            : Tunnel 1
Tunnel State           : Up (Main CRLSP up, Shared-resource CRLSP down)
Tunnel Attributes      :
  LSP ID               : 23549           Tunnel ID            : 1
  Admin State          : Normal
  Ingress LSR ID       : 1.1.1.9         Egress LSR ID        : 4.4.4.9
  Signaling            : RSVP-TE         Static CRLSP Name    : -
  Resv Style           : SE
  Tunnel mode          : -
  Reverse-LSP name     : -
  Reverse-LSP LSR ID   : -               Reverse-LSP Tunnel ID: -
  Class Type           : CT0             Tunnel Bandwidth     : 2000 kbps
  Reserved Bandwidth   : 2000 kbps
  Setup Priority       : 7               Holding Priority     : 7
```

```
  Affinity Attr/Mask   : 0/0
  Explicit Path        : atod
  Backup Explicit Path : -
  Metric Type          : TE
  Record Route         : Disabled        Record Label         : Disabled
  FRR Flag             : Disabled        Bandwidth Protection : Disabled
  Backup Bandwidth Flag: Disabled        Backup Bandwidth Type: -
  Backup Bandwidth     : -
  Bypass Tunnel        : No              Auto Created         : No
  Route Pinning        : Disabled
  Retry Limit          : 10              Retry Interval       : 2 sec
  Reoptimization       : Disabled        Reoptimization Freq  : -
  Backup Type          : None            Backup LSP ID        : -
  Auto Bandwidth       : Disabled        Auto Bandwidth Freq  : -
  Min Bandwidth        : -               Max Bandwidth        : -
  Collected Bandwidth  : -
```

在 Router A 上执行 **display ip routing-table** 命令，可以看到路由表中有以 Tunnel1 为出接口的静态路由信息。

```
[RouterA] display ip routing-table

Destinations : 14       Routes : 14

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

1.1.1.9/32          Direct 0    0            127.0.0.1       InLoop0
2.2.2.9/32          OSPF   10   1            10.1.1.2        GE2/1/1
3.3.3.9/32          O_ASE  150  1            10.1.1.2        GE2/1/1
4.4.4.9/32          O_ASE  150  1            10.1.1.2        GE2/1/1
7.1.1.0/24          Direct 0    0            7.1.1.1         Tun1
7.1.1.1/32          Direct 0    0            127.0.0.1       InLoop0
10.1.1.0/24         Direct 0    0            10.1.1.1        GE2/1/1
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         O_ASE  150  1            10.1.1.2        GE2/1/1
30.1.1.0/24         Static 1    0            7.1.1.1         Tun1
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

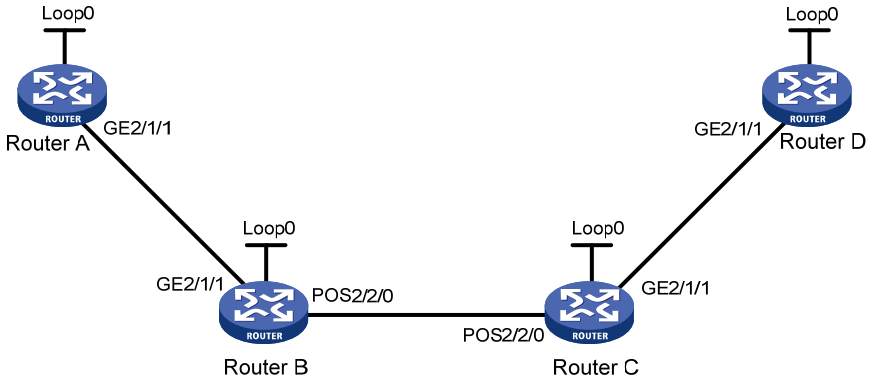
1.15.4 配置MPLS TE双向隧道

1. 组网需求

- 设备 Router A、Router B、Router C 和 Router D 运行 IS-IS，都是 Level-2 设备；
- 使用 RSVP-TE 建立从 Router A 到 Router D 的 MPLS TE 双向隧道。

2. 组网图

图1-10 配置 MPLS TE 双向隧道组网图



设备	接口	IP地址	设备	接口	IP地址
Router A	Loop0	1.1.1.9/32	Router C	Loop0	3.3.3.9/32
	GE2/1/1	10.1.1.1/24		GE2/1/1	30.1.1.1/24
Router B	Loop0	2.2.2.9/32		POS2/2/0	20.1.1.2/24
	GE2/1/1	10.1.1.2/24	Router D	Loop0	4.4.4.9/32
	POS2/2/0	20.1.1.1/24		GE2/1/1	30.1.1.2/24

3. 配置步骤

(1) 配置各接口的 IP 地址

按照 图 1-10 配置各接口的IP地址和掩码，具体配置过程略。

(2) 配置 IS-IS 协议发布接口所在网段的路由，包括 Loopback 接口

具体过程请参见“1.15.2 使用RSVP-TE配置MPLS TE隧道示例”。

(3) 配置 LSR ID，开启 MPLS、MPLS TE 和 RSVP-TE 能力，并在 Router A 和 Router D 上配置为倒数第二跳分配非空标签

配置 Router A。

```
<RouterA> system-view
[RouterA] mpls lsr-id 1.1.1.9
[RouterA] mpls label advertise non-null
[RouterA] mpls te
[RouterA-te] quit
[RouterA] rsvp
[RouterA-rsvp] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mpls enable
[RouterA-GigabitEthernet2/1/1] mpls te enable
[RouterA-GigabitEthernet2/1/1] rsvp enable
[RouterA-GigabitEthernet2/1/1] quit
```

配置 Router B。

```
<RouterB> system-view
[RouterB] mpls lsr-id 2.2.2.9
[RouterB] mpls te
[RouterB-te] quit
```

```
[RouterB] rsvp
[RouterB-rsvp] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mpls enable
[RouterB-GigabitEthernet2/1/1] mpls te enable
[RouterB-GigabitEthernet2/1/1] rsvp enable
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface pos 2/2/0
[RouterB-POS2/2/0] mpls enable
[RouterB-POS2/2/0] mpls te enable
[RouterB-POS2/2/0] rsvp enable
[RouterB-POS2/2/0] quit
```

配置 Router C。

```
<RouterC> system-view
[RouterC] mpls lsr-id 3.3.3.9
[RouterC] mpls te
[RouterC-te] quit
[RouterC-] rsvp
[RouterC-rsvp] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] mpls enable
[RouterC-GigabitEthernet2/1/1] mpls te enable
[RouterC-GigabitEthernet2/1/1] rsvp enable
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface pos 2/2/0
[RouterC-POS2/2/0] mpls enable
[RouterC-POS2/2/0] mpls te enable
[RouterC-POS2/2/0] rsvp enable
[RouterC-POS2/2/0] quit
```

配置 Router D。

```
<RouterD> system-view
[RouterD] mpls lsr-id 4.4.4.9
[RouterD] mpls label advertise non-null
[RouterD] mpls te
[RouterD-te] quit
[RouterD] rsvp
[RouterD-rsvp] quit
[RouterD] interface gigabitethernet 2/1/1
[RouterD-GigabitEthernet2/1/1] mpls enable
[RouterD-GigabitEthernet2/1/1] mpls te enable
[RouterD-GigabitEthernet2/1/1] rsvp enable
[RouterD-GigabitEthernet2/1/1] quit
```

(4) 配置 IS-IS TE

配置 Router A。

```
[RouterA] isis 1
[RouterA-isis-1] cost-style wide
[RouterA-isis-1] mpls te enable level-2
```

```
[RouterA-isis-1] quit
```

配置 Router B。

```
[RouterB] isis 1
[RouterB-isis-1] cost-style wide
[RouterB-isis-1] mpls te enable level-2
[RouterB-isis-1] quit
```

配置 Router C。

```
[RouterC] isis 1
[RouterC-isis-1] cost-style wide
[RouterC-isis-1] mpls te enable level-2
[RouterC-isis-1] quit
```

配置 Router D。

```
[RouterD] isis 1
[RouterD-isis-1] cost-style wide
[RouterD-isis-1] mpls te enable level-2
[RouterD-isis-1] quit
```

(5) 配置 MPLS TE 双向隧道

配置 Router A 作为 Co-routed 方式双向隧道的 active 端。

```
[RouterA] interface tunnel 1 mode mpls-te
[RouterA-Tunnel1] ip address 7.1.1.1 255.255.255.0
[RouterA-Tunnel1] destination 4.4.4.9
[RouterA-Tunnel1] mpls te signaling rsvp-te
[RouterA-Tunnel1] mpls te resv-style ff
[RouterA-Tunnel1] mpls te bidirectional co-routed active
[RouterA-Tunnel1] quit
```

配置 Router D 作为 Co-routed 方式双向隧道的 passive 端。

```
[RouterD] interface tunnel 4 mode mpls-te
[RouterD-Tunnel4] ip address 8.1.1.1 255.255.255.0
[RouterD-Tunnel4] destination 1.1.1.9
[RouterD-Tunnel4] mpls te signaling rsvp-te
[RouterD-Tunnel4] mpls te resv-style ff
[RouterD-Tunnel4] mpls te bidirectional co-routed passive reverse-lsp lsr-id 1.1.1.9
tunnel-id 1
[RouterD-Tunnel4] quit
```

4. 验证配置

配置完成后，在 Router A 上执行 **display interface tunnel** 命令可以看到隧道接口状态为 up。

```
[RouterA] display interface tunnel
Tunnel1 current state: UP
Line protocol current state: UP
Description: Tunnel1 Interface
The Maximum Transmit Unit is 64000
Internet Address is 7.1.1.1/24 Primary
Tunnel source unknown, destination 4.4.4.9
Tunnel bandwidth 64 (kbps)
Tunnel protocol/transport CR_LSP
Last clearing of counters: Never
```

```
    Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    0 packets output, 0 bytes, 0 drops
```

在 Router A 上执行 **display mpls te tunnel-interface** 命令可以看到隧道的详细信息。

```
[RouterA] display mpls te tunnel-interface
Tunnel Name            : Tunnel 1
Tunnel State           : Up (Main CRLSP up, Reverse CRLSP up)
Tunnel Attributes      :
  LSP ID               : 30478           Tunnel ID            : 1
  Admin State          : Normal
  Ingress LSR ID       : 1.1.1.9         Egress LSR ID        : 4.4.4.9
  Signaling            : RSVP-TE         Static CRLSP Name    : -
  Resv Style           : FF
  Tunnel mode          : Co-routed, active
  Reverse-LSP name     : -
  Reverse-LSP LSR ID   : -               Reverse-LSP Tunnel ID: -
  Class Type           : CT0             Tunnel Bandwidth     : 0 kbps
  Reserved Bandwidth   : 0 kbps
  Setup Priority       : 7               Holding Priority     : 7
  Affinity Attr/Mask   : 0/0
  Explicit Path        : -
  Backup Explicit Path : -
  Metric Type          : TE
  Record Route         : Disabled        Record Label         : Disabled
  FRR Flag             : Disabled        Bandwidth Protection : Disabled
  Backup Bandwidth Flag: Disabled        Backup Bandwidth Type: -
  Backup Bandwidth     : -
  Bypass Tunnel        : No              Auto Created         : No
  Route Pinning        : Disabled
  Retry Limit          : 10              Retry Interval       : 2 sec
  Reoptimization       : Disabled        Reoptimization Freq  : -
  Backup Type          : None            Backup LSP ID        : -
  Auto Bandwidth       : Disabled        Auto Bandwidth Freq  : -
  Min Bandwidth        : -               Max Bandwidth        : -
  Collected Bandwidth  : -
```

在 Router A 上执行 **display mpls lsp verbose** 命令可以看到双向隧道的详细信息。

```
[RouterA] display mpls lsp verbose
Destination  : 4.4.4.9
FEC          : 1.1.1.9/1/30478
Protocol     : RSVP
LSR Type     : Ingress
Service      : -
NHLFE ID     : 1027
State        : Active
Out-Label    : 1149
Nexthop      : 10.1.1.2
Out-Interface: GE2/1/1
```

```
Destination  : 4.4.4.9
FEC          : 1.1.1.9/1/30478
Protocol     : RSVP
LSR Type     : Egress
Service      : -
In-Label     : 1151
State        : Active
Nexthop      : 127.0.0.1
Out-Interface: -

Destination  : 10.1.1.2
FEC          : 10.1.1.2
Protocol     : Local
LSR Type     : Ingress
Service      : -
NHLFE ID     : 1026
State        : Active
Nexthop      : 10.1.1.2
Out-Interface: GE2/1/1
```

在 Router D 上执行 **display interface tunnel** 命令可以看到隧道接口状态为 up。

```
[RouterD] display interface tunnel
Tunnel4 current state: UP
Line protocol current state: UP
Description: Tunnel8 Interface
The Maximum Transmit Unit is 64000
Internet Address is 8.1.1.1/24 Primary
Tunnel source unknown, destination 1.1.1.9
Tunnel bandwidth 64 (kbps)
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Last clearing of counters: Never
    Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    0 packets output, 0 bytes, 0 drops
```

在 Router D 上执行 **display mpls te tunnel-interface** 命令可以看到隧道的详细信息。

```
[RouterD] display mpls te tunnel-interface
Tunnel Name            : Tunnel 4
Tunnel State           : Up (Main CRLSP up, Reverse CRLSP up)
Tunnel Attributes      :
  LSP ID               : -               Tunnel ID            : 8
  Admin State          : Normal
  Ingress LSR ID       : -               Egress LSR ID        : -
  Signaling            : RSVP-TE         Static CRLSP Name    : -
  Resv Style           : FF
  Tunnel mode          : Co-routed, passive
  Reverse-LSP name     : -
```

```
  Reverse-LSP LSR ID   : 1.1.1.9         Reverse-LSP Tunnel ID: 1
  Class Type           : -               Tunnel Bandwidth     : -
  Reserved Bandwidth   : -
  Setup Priority       : -               Holding Priority     : -
  Affinity Attr/Mask   : -/-
  Explicit Path        : -
  Backup Explicit Path : -
  Metric Type          : -
  Record Route         : -               Record Label         : -
  FRR Flag             : -               Bandwidth Protection : -
  Backup Bandwidth Flag: -               Backup Bandwidth Type: -
  Backup Bandwidth     : -
  Bypass Tunnel        : -               Auto Created         : -
  Route Pinning        : -
  Retry Limit          : -               Retry Interval       : -
  Reoptimization       : -               Reoptimization Freq  : -
  Backup Type          : -               Backup LSP ID        : -
  Auto Bandwidth       : -               Auto Bandwidth Freq  : -
  Min Bandwidth        : -               Max Bandwidth        : -
  Collected Bandwidth  : -
```

在 Router D 上执行 **display mpls lsp verbose** 命令可以看到双向隧道的详细信息。

```
[RouterD] display mpls lsp verbose
Destination  : 4.4.4.9
FEC          : 1.1.1.9/1/30478
Protocol     : RSVP
LSR Type     : Egress
Service      : -
In-Label     : 3
State        : Active
Nexthop      : 127.0.0.1
Out-Interface: -

Destination  : 4.4.4.9
FEC          : 1.1.1.9/1/30478
Protocol     : RSVP
LSR Type     : Ingress
Service      : -
NHLFE ID     : 1025
State        : Active
Out-Label    : 1150
Nexthop      : 30.1.1.1
Out-Interface: GE2/1/1

Destination  : 30.1.1.1
FEC          : 30.1.1.1
Protocol     : Local
LSR Type     : Ingress
Service      : -
```

```
NHLFE ID     : 1024
State        : Active
Nexthop      : 30.1.1.1
Out-Interface: GE2/1/1
```

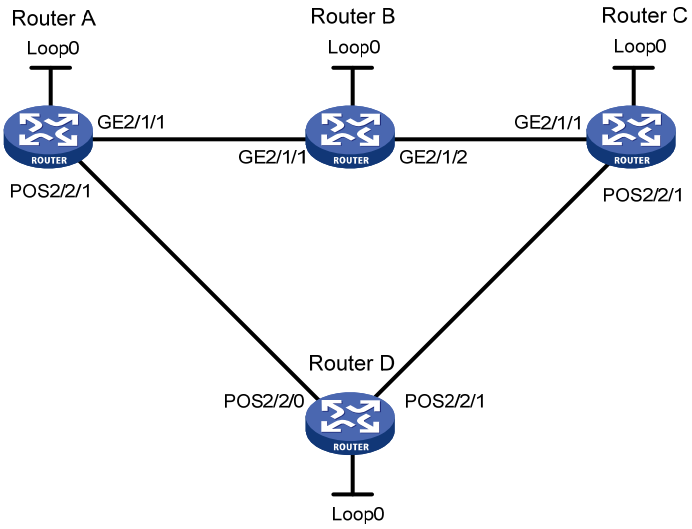
1.15.5 配置CRLSP备份示例

1. 组网需求

- 设备 Router A、Router B、Router C 和 Router D 运行 IS-IS；
- 使用 RSVP-TE 从 Router A 到 Router C 建立一条 MPLS TE 隧道；
- MPLS TE 隧道支持 CRLSP 热备份，即同时建立主备两条 CRLSP，实现主 CRLSP 故障时将流量切换到备份 CRLSP。

2. 组网图

图1-11 CRLSP 备份组网图



设备	接口	IP地址	设备	接口	IP地址
Router A	Loop0	1.1.1.9/32	Router D	Loop0	4.4.4.9/32
	GE2/1/1	10.1.1.1/24		POS2/2/0	30.1.1.2/24
	POS2/2/1	30.1.1.1/24		POS2/2/1	40.1.1.1/24
Router B	Loop0	2.2.2.9/32	Router C	Loop0	3.3.3.9/32
	GE2/1/1	10.1.1.2/24		GE2/1/1	20.1.1.2/24
	GE2/1/2	20.1.1.1/24		POS2/2/1	40.1.1.2/24

3. 配置步骤

(1) 配置各接口的 IP 地址

按照 图 1-11 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。

(2) 配置 IS-IS 协议发布接口所在网段的路由，包括 Loopback 接口（具体配置过程略）

(3) 配置 LSR ID，开启 MPLS、MPLS TE 和 RSVP-TE 能力

配置 Router A。

```
<RouterA> system-view
[RouterA] mpls lsr-id 1.1.1.9
[RouterA] mpls te
```

```
[RouterA-te] quit
[RouterA] rsvp
[RouterA-rsvp] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mpls enable
[RouterA-GigabitEthernet2/1/1] mpls te enable
[RouterA-GigabitEthernet2/1/1] rsvp enable
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface pos 2/2/1
[RouterA-POS2/2/1] mpls enable
[RouterA-POS2/2/1] mpls te enable
[RouterA-POS2/2/1] rsvp enable
[RouterA-POS2/2/1] quit
```

Router B、Router C 和 Router D 的配置与 Router A 相似，此处不再赘述。

(4) 配置 MPLS TE 隧道

在 Router A 上配置 MPLS TE 隧道 Tunnel3：目的地址为 Router C 的 LSR ID（3.3.3.9）；采用 RSVP-TE 信令协议建立 MPLS TE 隧道；隧道支持 CRLSP 热备份功能。

```
[RouterA] interface tunnel 3 mode mpls-te
[RouterA-Tunnel3] ip address 9.1.1.1 255.255.255.0
[RouterA-Tunnel3] destination 3.3.3.9
[RouterA-Tunnel3] mpls te signaling rsvp-te
[RouterA-Tunnel3] mpls te backup hot-standby
[RouterA-Tunnel3] quit
```

(5) 配置静态路由使流量沿 MPLS TE 隧道转发

在 Router A 上配置静态路由，使得到达网络 20.1.1.0/24 的流量通过 MPLS TE 隧道接口 Tunnel3 转发。

```
[RouterA] ip route-static 20.1.1.2 24 tunnel 3 preference 1
```

4. 验证配置

配置完成后，在 Router A 上执行 **display interface tunnel** 命令，可以看到 Tunnel3 的状态为 up。

```
[RouterA] display interface tunnel
Tunnel3 current state: UP
Line protocol current state: UP
Description: Tunnel3 Interface
The Maximum Transmit Unit is 64000
Internet Address is 9.1.1.1/24 Primary
Tunnel source unknown, destination 3.3.3.9
Tunnel bandwidth 64 (kbps)
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Last clearing of counters: Never
    Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    0 packets output, 0 bytes, 0 drops
```

在 Router A 上执行 **display mpls lsp** 命令，可以看到存在两条 CRLSP，出接口分别是 GigabitEthernet2/1/1 和 POS2/2/1，即主 CRLSP 创建后，备份 CRLSP 也建立了。

```
[RouterA] display mpls lsp
FEC                        Proto    In/Out Label    Interface/Out NHLFE
1.1.1.9/3/30106            RSVP     -/1137          GE2/1/1
1.1.1.9/3/30107            RSVP     -/1150          POS2/2/1
10.1.1.2                   Local    -/-             GE2/1/1
30.1.1.2                   Local    -/-             POS2/2/1
```

在 Router A 上执行 **display rsvp lsp verbose** 命令，可以看到这两条 CRLSP 使用的路径。

```
[RouterA] display rsvp lsp verbose
Tunnel name: RouterA_t3
Destination: 3.3.3.9                    Source: 1.1.1.9
Tunnel ID: 3                            LSP ID: 30106
LSR type: Ingress                       Direction: Unidirectional
Setup priority: 7                       Holding priority: 7
In-Label: -                             Out-Label: 1137
In-Interface: -                         Out-Interface: GE2/1/1
Nexthop: 10.1.1.2                       Exclude-any: 0
Include-Any: 0                          Include-all: 0
Mean rate (CIR): 0 kbps                 Mean burst size (CBS): 1000.00 bytes
Path MTU: 1500                          Class type: CT0
RRO number: 6
  10.1.1.1/32        Flag: 0x00 (No FRR)
  10.1.1.2/32        Flag: 0x00 (No FRR)
  2.2.2.9/32         Flag: 0x20 (No FRR/Node-ID)
  20.1.1.1/32        Flag: 0x00 (No FRR)
  20.1.1.2/32        Flag: 0x00 (No FRR)
  3.3.3.9/32         Flag: 0x20 (No FRR/Node-ID)
Fast Reroute protection: None

Tunnel name: Tunnel3
Destination: 3.3.3.9                    Source: 1.1.1.9
Tunnel ID: 3                            LSP ID: 30107
LSR type: Ingress                       Direction: Unidirectional
Setup priority: 7                       Holding priority: 7
In-Label: -                             Out-Label: 1150
In-Interface: -                         Out-Interface: GE2/1/4
Nexthop: 30.1.1.2                       Exclude-any: 0
Include-Any: 0                          Include-all: 0
Mean rate (CIR): 0 kbps                 Mean burst size (CBS): 1000.00 bytes
Path MTU: 1500                          Class type: CT0
RRO number: 6
  30.1.1.1/32        Flag: 0x00 (No FRR)
  30.1.1.2/32        Flag: 0x00 (No FRR)
  4.4.4.9/32         Flag: 0x20 (No FRR/Node-ID)
  40.1.1.1/32        Flag: 0x00 (No FRR)
  40.1.1.2/32        Flag: 0x00 (No FRR)
  3.3.3.9/32         Flag: 0x20 (No FRR/Node-ID)
Fast Reroute protection: None
```

对隧道目的地址 3.3.3.9 进行 Tracert 操作，可以看出目前使用的是经过 Router B 的 CRLSP，不是经过 Router D 的 CRLSP。

```
[RouterA] tracert –a 1.1.1.9 3.3.3.9
traceroute to 3.3.3.9 (3.3.3.9) from 1.1.1.9, 30 hops at most, 40 bytes each pac
ket, press CTRL_C to break
 1 10.1.1.2 (10.1.1.2)  1.000 ms  1.000 ms  1.000 ms
 2 * * *
```

在 Router B 的接口 GigabitEthernet2/1/2 上执行 **shutdown** 命令，然后再对隧道目的地址进行 Tracert 操作，可以看到报文使用经过 Router D 的 CRLSP 转发。

```
[RouterA] tracert –a 1.1.1.9 3.3.3.9
traceroute to 3.3.3.9 (3.3.3.9) from 9.1.1.1, 30 hops at most, 40 bytes each pac
ket, press CTRL_C to break
 1  30.1.1.2 (30.1.1.2)  3.000 ms  7.000 ms  3.000 ms
 2  * * *
```

在 Router A 上执行 **display mpls lsp** 命令，可以看到只剩下一条经过 RouterD 的 CRLSP。

```
[RouterA] display mpls lsp
FEC                       Proto    In/Out Label    Interface/Out NHLFE
1.1.1.9/3/30107           RSVP     -/1150          POS2/2/1
30.1.1.2                  Local    -/-             POS2/2/1
```

在 Router A 上执行 **display ip routing-table** 命令，可以看到路由表中有以 Tunnel3 为出接口的静态路由信息。

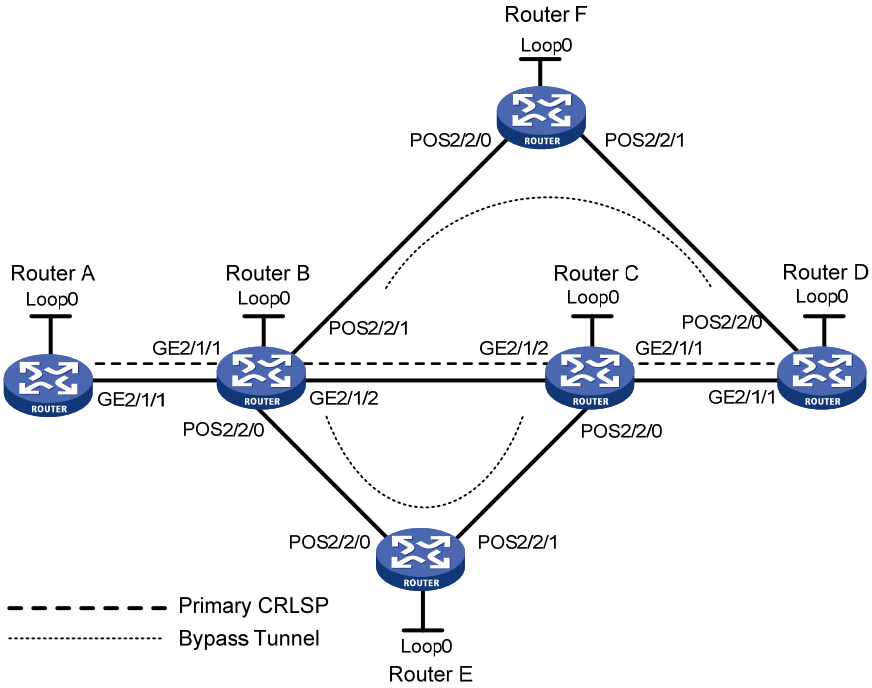
1.15.6 配置快速重路由示例（手工配置Bypass隧道）

1. 组网需求

- 主 CRLSP 使用路径 Router A→Router B→Router C→Router D，要求对 Router B→Router C 这段链路通过 FRR 进行链路保护。
- 使用 RSVP-TE 信令协议、基于显式路径约束条件建立 MPLS TE 隧道的主 CRLSP 和 Bypass 隧道。Bypass 隧道使用路径 Router B→Router E→Router C（Router B 是本地修复节点 PLR，Router C 是汇聚点 MP）。
- 在 Router B 和 Router C 之间配置 RSVP-TE 与 BFD 联动，当 Router B 和 Router C 之间的链路出现故障后，BFD 能够快速检测并通告 RSVP-TE 协议，以便快速将流量切换到 Bypass 隧道。

2. 组网图

图1-12 MPLS TE 快速重路由配置组网图



设备	接口	IP地址	设备	接口	IP地址
Router A	Loop0	1.1.1.1/32	Router E	Loop0	5.5.5.5/32
	GE2/1/1	2.1.1.1/24		POS2/2/0	3.2.1.2/24
Router B	Loop0	2.2.2.2/32		POS2/2/1	3.3.1.1/24
	GE2/1/1	2.1.1.2/24	Router C	Loop0	3.3.3.3/32
	GE2/1/2	3.1.1.1/24		GE2/1/1	4.1.1.1/24
	POS2/2/0	3.2.1.1/24		GE2/1/2	3.1.1.2/24
Router D	Loop0	4.4.4.4/32		POS2/2/0	3.3.1.2/24
	GE2/1/1	4.1.1.2/24			

3. 配置步骤

(1) 配置各接口的 IP 地址

按照 图 1-12 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。

(2) 配置 IS-IS 协议发布接口所在网段的路由，包括 Loopback 接口（具体配置过程略）

(3) 配置 LSR ID，开启 MPLS、MPLS TE 和 RSVP-TE 能力，并在 Router B 和 Router C 上配置 RSVP-TE 与 BFD 联动，以检测 Router B 与 Router C 之间链路的状态

配置 Router A。

```
<RouterA> system-view
[RouterA] mpls lsr-id 1.1.1.1
[RouterA] mpls te
[RouterA-te] quit
[RouterA] rsvp
[RouterA-rsvp] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mpls enable
[RouterA-GigabitEthernet2/1/1] mpls te enable
```

```
[RouterA-GigabitEthernet2/1/1] rsvp enable
[RouterA-GigabitEthernet2/1/1] quit
```

配置 Router B。

```
<RouterB> system-view
[RouterB] mpls lsr-id 2.2.2.2
[RouterB] mpls te
[RouterB-te] quit
[RouterB] rsvp
[RouterB-rsvp] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mpls enable
[RouterB-GigabitEthernet2/1/1] mpls te enable
[RouterB-GigabitEthernet2/1/1] rsvp enable
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] mpls enable
[RouterB-GigabitEthernet2/1/2] mpls te enable
[RouterB-GigabitEthernet2/1/2] rsvp enable
[RouterB-GigabitEthernet2/1/2] rsvp bfd enable
[RouterB-GigabitEthernet2/1/2] quit
[RouterB] interface pos 2/2/0
[RouterB-POS2/2/0] mpls enable
[RouterB-POS2/2/0] mpls te enable
[RouterB-POS2/2/0] rsvp enable
[RouterB-POS2/2/0] quit
```

Router C 的配置与 Router B 的配置相似，Router D、Router E 的配置与 Router A 的配置相似，此处不再赘述。

(4) 在主 CRLSP 的 Ingress 节点 Router A 上建立 MPLS TE 隧道

配置主 CRLSP 的显式路径。

```
[RouterA] explicit-path pri-path
[RouterA-explicit-path-pri-path] nexthop 2.1.1.2
[RouterA-explicit-path-pri-path] nexthop 3.1.1.2
[RouterA-explicit-path-pri-path] nexthop 4.1.1.2
[RouterA-explicit-path-pri-path] nexthop 4.4.4.4
[RouterA-explicit-path-pri-path] quit
```

配置主 CRLSP 的 MPLS TE 隧道 Tunnel4：目的地址为 Router D 的 LSR ID（4.4.4.4）；采用 RSVP-TE 信令协议建立 MPLS TE 隧道；隧道引用显式路径 pri-path。

```
[RouterA] interface tunnel 4 mode mpls-te
[RouterA-Tunnel4] ip address 10.1.1.1 255.255.255.0
[RouterA-Tunnel4] destination 4.4.4.4
[RouterA-Tunnel4] mpls te signaling rsvp-te
[RouterA-Tunnel4] mpls te path preference 1 explicit-path pri-path
```

开启 MPLS TE 隧道的 FRR 功能。

```
[RouterA-Tunnel4] mpls te fast-reroute
[RouterA-Tunnel4] quit
```

配置完成后，在 Router A 上执行 **display interface tunnel** 命令，可以看到 Tunnel4 的状态为 up。

```
[RouterA] display interface tunnel
Tunnel4 current state: UP
Line protocol current state: UP
Description: Tunnel3 Interface
The Maximum Transmit Unit is 64000
Internet Address is 9.1.1.1/24 Primary
Tunnel source unknown, destination 3.3.3.9
Tunnel bandwidth 64 (kbps)
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Last clearing of counters: Never
    Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate: 1911 bytes/sec, 15288 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    1526 packets output, 22356852 bytes, 0 drops
```

在 Router A 上执行 **display mpls te tunnel-interface** 命令，可以看到隧道接口的详细信息。

```
[RouterA] display mpls te tunnel-interface
Tunnel Name            : Tunnel 4
Tunnel State           : Up (Main CRLSP up, Shared-resource CRLSP down)
Tunnel Attributes      :
  LSP ID               : 48960           Tunnel ID            : 4
  Admin State          : Normal
  Ingress LSR ID       : 1.1.1.1         Egress LSR ID        : 3.3.3.3
  Signaling            : RSVP-TE         Static CRLSP Name    : -
  Resv Style           : SE
  Tunnel mode          : -
  Reverse-LSP name     : -
  Reverse-LSP LSR ID   : -               Reverse-LSP Tunnel ID: -
  Class Type           : CT0             Tunnel Bandwidth     : 0 kbps
  Reserved Bandwidth   : 0 kbps
  Setup Priority       : 7               Holding Priority     : 7
  Affinity Attr/Mask   : 0/0
  Explicit Path        : pri-path
  Backup Explicit Path : -
  Metric Type          : TE
  Record Route         : Enabled         Record Label         : Enabled
  FRR Flag             : Enabled         Bandwidth Protection : Disabled
  Backup Bandwidth Flag: Disabled        Backup Bandwidth Type: -
  Backup Bandwidth     : -
  Bypass Tunnel        : No              Auto Created         : No
  Route Pinning        : Disabled
  Retry Limit          : 10              Retry Interval       : 2 sec
  Reoptimization       : Disabled        Reoptimization Freq  : -
  Backup Type          : None            Backup LSP ID        : -
  Auto Bandwidth       : Disabled        Auto Bandwidth Freq  : -
  Min Bandwidth        : -               Max Bandwidth        : -
  Collected Bandwidth  : -
```

(5) 在作为 PLR 的 Router B 上配置 Bypass 隧道

配置 Bypass 隧道的显式路径。

```
[RouterB] explicit-path by-path
[RouterB-explicit-path-by-path] nexthop 3.2.1.2
[RouterB-explicit-path-by-path] nexthop 3.3.1.2
[RouterB-explicit-path-by-path] nexthop 3.3.3.3
[RouterB-explicit-path-by-path] quit
```

配置 Bypass 隧道 Tunnel5：目的地址为 Router C 的 LSR ID（3.3.3.3）；采用 RSVP-TE 信令协议建立 MPLS TE 隧道；隧道引用显式路径 by-path。

```
[RouterB] interface tunnel 5 mode mpls-te
[RouterB-Tunnel5] ip address 11.1.1.1 255.255.255.0
[RouterB-Tunnel5] destination 3.3.3.3
[RouterB-Tunnel5] mpls te signaling rsvp-te
[RouterB-Tunnel5] mpls te path preference 1 explicit-path by-path
```

配置 Bypass 隧道可保护的带宽。

```
[RouterB-Tunnel5] mpls te backup bandwidth un-limited
[RouterB-Tunnel5] quit
```

将 Bypass 隧道绑定到被保护的接口。

```
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] mpls te fast-reroute bypass-tunnel tunnel 5
[RouterB-GigabitEthernet2/1/2] quit
```

配置完成后，在 Router B 上执行 **display interface tunnel** 命令可以看到接口 Tunnel5 的状态为 up。

(6)　配置静态路由使流量沿 MPLS TE 隧道转发

在 Router A 上配置静态路由，使得到达网络 4.1.1.0/24 的流量通过 MPLS TE 隧道接口 Tunnel4 转发。

```
[RouterA] ip route-static 4.1.1.2 24 tunnel 4 preference 1
```

4. 验证配置

在所有设备上执行 **display mpls lsp** 命令，可以看到 LSP 表项。在 Router B 和 Router C 上存在两条 LSP，通过 Bypass 隧道保护主 CRLSP。

```
[RouterA] display mpls lsp
FEC                         Proto    In/Out Label    Interface/Out NHLFE
1.1.1.1/4/48960             RSVP     -/1245          GE2/1/1
2.1.1.2                     Local    -/-             GE2/1/1
[RouterB] display mpls lsp
FEC                         Proto    In/Out Label    Interface/Out NHLFE
1.1.1.1/4/48960             RSVP     1245/3          GE2/1/2
Backup                               1245/3          Tun5
2.2.2.2/5/31857             RSVP     -/3             GE2/1/2
3.2.1.2                     Local    -/-             POS2/2/0
3.1.1.2                     Local    -/-             GE2/1/2
```

在 PLR 上 **shutdown** 被保护的出接口 GigabitEthernet2/1/2。

```
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] shutdown
[RouterB-GigabitEthernet2/1/2] quit
```

在 Router A 上执行 **display interface tunnel** 4 命令查看主 CRLSP 的状态，可以看到 Tunnel 接口仍然处于 up 状态。

在 Router A 上执行 **display mpls te tunnel-interface** 命令，可以看到隧道接口的详细信息。

```
[RouterA] display mpls te tunnel-interface
Tunnel Name            : Tunnel 4
Tunnel State           : Up (Main CRLSP up, Shared-resource CRLSP being set up)
Tunnel Attributes      :
  LSP ID               : 18753          Tunnel ID            : 4
  Admin State          : Normal
  Ingress LSR ID       : 1.1.1.1        Egress LSR ID        : 3.3.3.3
  Signaling            : RSVP-TE        Static CRLSP Name    : -
  Resv Style           : SE
  Tunnel mode          : -
  Reverse-LSP name     : -
  Reverse-LSP LSR ID   : -              Reverse-LSP Tunnel ID: -
  Class Type           : CT0            Tunnel Bandwidth     : 0 kbps
  Reserved Bandwidth   : 0 kbps
  Setup Priority       : 7              Holding Priority     : 7
  Affinity Attr/Mask   : 0/0
  Explicit Path        : pri-path
  Backup Explicit Path : -
  Metric Type          : TE
  Record Route         : Enabled        Record Label         : Enabled
  FRR Flag             : Enabled        Bandwidth Protection : Disabled
  Backup Bandwidth Flag: Disabled       Backup Bandwidth Type: -
  Backup Bandwidth     : -
  Bypass Tunnel        : No             Auto Created         : No
  Route Pinning        : Disabled
  Retry Limit          : 10             Retry Interval       : 2 sec
  Reoptimization       : Disabled       Reoptimization Freq  : -
  Backup Type          : None           Backup LSP ID        : -
  Auto Bandwidth       : Disabled       Auto Bandwidth Freq  : -
  Min Bandwidth        : -              Max Bandwidth        : -
  Collected Bandwidth  : -
```

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 CRLSP。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 Router B 上执行 **display mpls lsp** 命令，可以看到 Bypass 隧道被使用。

```
[RouterB] display mpls lsp
FEC                       Proto    In/Out Label    Interface/Out NHLFE
1.1.1.1/4/18753           RSVP     1122/3          Tun5
2.2.2.2/5/40312           RSVP     -/1150          GE2/1/4
3.2.1.2                   Local    -/-             GE2/1/4
```

在 PLR 上配置在多条旁路隧道中进行优选的时间间隔为 5 秒。

```
[RouterB] mpls te
[RouterB-te] fast-reroute timer 5
[RouterB-te] quit
```

在 PLR 上 **undo shutdown** 被保护的出接口 GigabitEthernet2/1/2。

```
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] undo shutdown
[RouterB-GigabitEthernet2/1/2] quit
```

在 Router A 上执行 **display interface tunnel** 4 命令查看主 CRLSP 的状态，可以看到 Tunnel 接口处于 up 状态。

等待约 5 秒钟后，在 Router B 上执行 **display mpls lsp verbose** 命令，可以看到 Tunnel5 仍绑定到出接口 GigabitEthernet2/1/2，但未被使用。

在 Router A 上执行 **display ip routing-table** 命令，可以看到路由表中有以 Tunnel4 为出接口的静态路由信息。

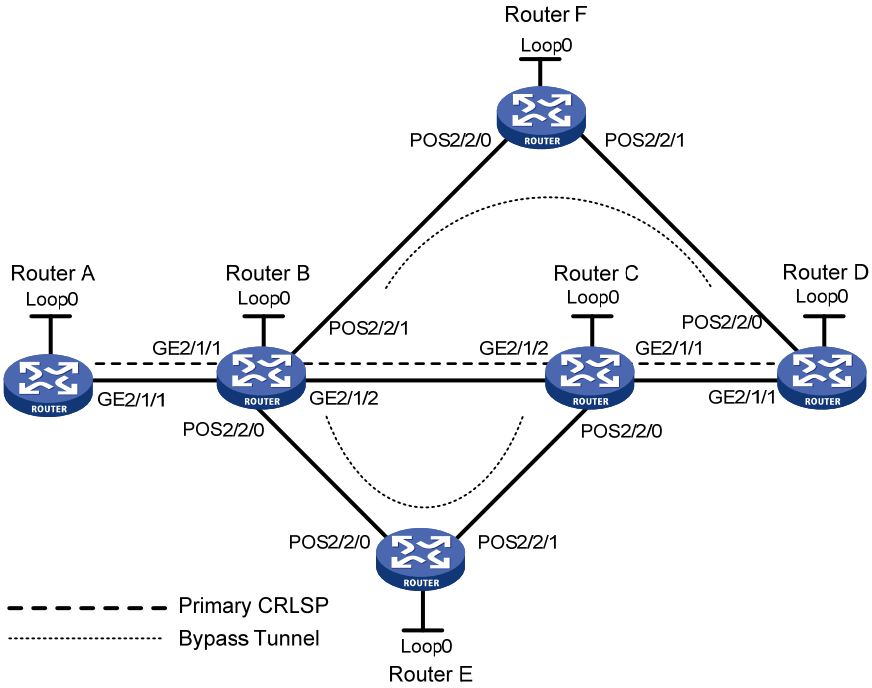
1.15.7 配置自动快速重路由示例

1. 组网需求

- 使用 RSVP-TE 信令协议、基于显式路径约束条件建立主 CRLSP。主 CRLSP 使用的路径为 Router A→Router B→Router C→Router D。
- 在 Router B 上配置自动隧道备份功能，自动为主 CRLSP 建立 Bypass 隧道。
- 在 Router B 和 Router C 之间配置 RSVP-TE 与 BFD 联动，当 Router B 和 Router C 之间的链路出现故障后，BFD 能够快速检测并通告 RSVP-TE 协议，以便快速将流量切换到 Bypass 隧道。

2. 组网图

图1-13 MPLS TE 自动快速重路由配置组网图



设备	接口	IP地址	设备	接口	IP地址
Router A	Loop0	1.1.1.1/32	Router E	Loop0	5.5.5.5/32
	GE2/1/1	2.1.1.1/24		POS2/2/0	3.2.1.2/24
Router B	Loop0	2.2.2.2/32		POS2/2/1	3.4.1.1/24
	GE2/1/1	2.1.1.2/24	Router C	Loop0	3.3.3.3/32
	GE2/1/2	3.1.1.1/24		GE2/1/1	4.1.1.1/24
	POS2/2/0	3.2.1.1/24		GE2/1/2	3.1.1.2/24
	POS2/2/1	3.3.1.1/24		POS2/2/0	3.4.1.2/24
Router D	Loop0	4.4.4.4/32	Router F	Loop0	5.5.5.5/32
	GE2/1/1	4.1.1.2/24		POS2/2/0	3.3.1.2/24
	POS2/2/0	4.2.1.2/24		POS2/2/1	4.2.1.1/24

3. 配置步骤

(1) 配置各接口的 IP 地址

按照 图 1-13 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。

(2) 配置 IS-IS 协议发布接口所在网段的路由，包括 Loopback 接口（具体配置过程略）

(3) 配置 LSR ID，开启 MPLS、MPLS TE 和 RSVP-TE 能力，并在 Router B 和 Router C 之间配置 RSVP-TE 与 BFD 联动，以检测 Router B 与 Router C 之间链路的状态

配置 Router A。

```
<RouterA> system-view
[RouterA] mpls lsr-id 1.1.1.1
[RouterA] mpls te
[RouterA-te] quit
[RouterA] rsvp
[RouterA-rsvp] quit
[RouterA] interface gigabitethernet 2/1/1
```

```
[RouterA-GigabitEthernet2/1/1] mpls enable
[RouterA-GigabitEthernet2/1/1] mpls te enable
[RouterA-GigabitEthernet2/1/1] rsvp enable
[RouterA-GigabitEthernet2/1/1] quit
```

配置 Router B。

```
<RouterB> system-view
[RouterB] mpls lsr-id 2.2.2.2
[RouterB] mpls te
[RouterB-te] quit
[RouterB] rsvp
[RouterB-rsvp] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mpls enable
[RouterB-GigabitEthernet2/1/1] mpls te enable
[RouterB-GigabitEthernet2/1/1] rsvp enable
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] mpls enable
[RouterB-GigabitEthernet2/1/2] mpls te enable
[RouterB-GigabitEthernet2/1/2] rsvp enable
[RouterB-GigabitEthernet2/1/2] rsvp bfd enable
[RouterB-GigabitEthernet2/1/2] quit
[RouterB] interface pos 2/2/0
[RouterB-POS2/2/0] mpls enable
[RouterB-POS2/2/0] mpls te enable
[RouterB-POS2/2/0] rsvp enable
[RouterB-POS2/2/0] quit
[RouterB] interface pos 2/2/1
[RouterB-POS2/2/1] mpls enable
[RouterB-POS2/2/1] mpls te enable
[RouterB-POS2/2/1] rsvp enable
[RouterB-POS2/2/1] quit
```

Router C 的配置与 Router B 的配置相似，Router D、Router E、Router F 的配置与 Router A 的配置相似，此处不再赘述。

(4) 在主 CRLSP 的 Ingress 节点 Router A 上建立 MPLS TE 隧道

配置主 CRLSP 的显式路径。

```
[RouterA] explicit-path pri-path
[RouterA-explicit-path-pri-path] nexthop 2.1.1.2
[RouterA-explicit-path-pri-path] nexthop 3.1.1.2
[RouterA-explicit-path-pri-path] nexthop 4.1.1.2
[RouterA-explicit-path-pri-path] nexthop 4.4.4.4
[RouterA-explicit-path-pri-path] quit
```

配置主 CRLSP 的 MPLS TE 隧道 Tunnel1：目的地址为 Router D 的 LSR ID（4.4.4.4）；采用 RSVP-TE 信令协议建立 MPLS TE 隧道；隧道引用显式路径 pri-path。

```
[RouterA] interface tunnel 1 mode mpls-te
[RouterA-Tunnel1] ip address 10.1.1.1 255.255.255.0
[RouterA-Tunnel1] destination 4.4.4.4
```

```
[RouterA-Tunnel1] mpls te signaling rsvp-te
[RouterA-Tunnel1] mpls te path preference 1 explicit-path pri-path
```
开启 MPLS TE 隧道的 FRR 功能。
```
[RouterA-Tunnel1] mpls te fast-reroute
[RouterA-Tunnel1] quit
```
配置完成后，在 Router A 上执行 **display interface tunnel** 命令，可以看到 Tunnel1 的状态为 up。
```
[RouterA] display interface tunnel
Tunnel1 current state: UP
Line protocol current state: UP
Description: Tunnel1 Interface
The Maximum Transmit Unit is 64000
Internet Address is 10.1.1.1/24 Primary
Tunnel source unknown, destination 4.4.4.4
Tunnel bandwidth 64 (kbps)
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Last clearing of counters: Never
    Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate: 1911 bytes/sec, 15288 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    1526 packets output, 22356852 bytes, 0 drops
```
在 Router A 上执行 **display mpls te tunnel-interface** 命令，可以看到隧道接口的详细信息。
```
[RouterA] display mpls te tunnel-interface
Tunnel Name            : Tunnel 1
Tunnel State           : Up (Main CRLSP up, Shared-resource CRLSP down)
Tunnel Attributes      :
  LSP ID               : 16802           Tunnel ID            : 1
  Admin State          : Normal
  Ingress LSR ID       : 2.2.2.2         Egress LSR ID        : 4.4.4.4
  Signaling            : RSVP-TE         Static CRLSP Name    : -
  Resv Style           : SE
  Tunnel mode          : -
  Reverse-LSP name     : -
  Reverse-LSP LSR ID   : -               Reverse-LSP Tunnel ID: -
  Class Type           : CT0             Tunnel Bandwidth     : 0 kbps
  Reserved Bandwidth   : 0 kbps
  Setup Priority       : 7               Holding Priority     : 7
  Affinity Attr/Mask   : 0/0
  Explicit Path        : exp1
  Backup Explicit Path : -
  Metric Type          : TE
  Record Route         : Enabled         Record Label         : Enabled
  FRR Flag             : Enabled         Bandwidth Protection : Disabled
  Backup Bandwidth Flag: Disabled        Backup Bandwidth Type: -
  Backup Bandwidth     : -
  Bypass Tunnel        : No              Auto Created         : No
  Route Pinning        : Disabled
  Retry Limit          : 3               Retry Interval       : 2 sec
```

```
  Reoptimization       : Disabled        Reoptimization Freq  : -
  Backup Type          : None            Backup LSP ID        : -
  Auto Bandwidth       : Disabled        Auto Bandwidth Freq  : -
  Min Bandwidth        : -               Max Bandwidth        : -
  Collected Bandwidth  : -
```

(5) 在作为 PLR 的 Router B 上配置自动隧道备份功能

全局开启自动隧道备份功能，并配置自动创建的 Bypass 隧道接口编号范围为 50～100。

```
[RouterB] mpls te
[RouterB-te] auto-tunnel backup
[RouterB-te-auto-bk] tunnel-number min 50 max 100
[RouterB-te-auto-bk] quit
```

4. 验证配置

在 Router B 上执行 **display interface tunnel brief** 命令，可以看到自动创建了两条隧道。

```
[RouterB] display interface tunnel brief
Brief information on interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Main IP         Description
Tun50                 UP    UP        --
Tun51                 UP    UP        --
```

在 Router B 上执行 **display mpls te tunnel-interface** 命令，查看 Tunnel50 和 Tunnel51 的信息，可以看到该隧道为自动创建的 Bypass 隧道，且 Tunnel50 为节点保护类型的 Bypass 隧道（Egress LSR ID 为 4.4.4.4，Router D 的 LSR ID），Tunnel51 为链路保护类型的 Bypass 隧道（Egress LSR ID 为 3.3.3.3，Router C 的 LSR ID）

```
[RouterB] display mpls te tunnel-interface tunnel 50
Tunnel Name            : Tunnel 50
Tunnel State           : Up (Main CRLSP up, Shared-resource CRLSP down)
Tunnel Attributes      :
  LSP ID               : 16802           Tunnel ID            : 50
  Admin State          : Normal
  Ingress LSR ID       : 2.2.2.2         Egress LSR ID        : 4.4.4.4
  Signaling            : RSVP-TE         Static CRLSP Name    : -
  Resv Style           : SE
  Tunnel mode          : -
  Reverse-LSP name     : -
  Reverse-LSP LSR ID   : -               Reverse-LSP Tunnel ID: -
  Class Type           : CT0             Tunnel Bandwidth     : 0 kbps
  Reserved Bandwidth   : 0 kbps
  Setup Priority       : 7               Holding Priority     : 7
  Affinity Attr/Mask   : 0/0
  Explicit Path        : -
  Backup Explicit Path : -
  Metric Type          : TE
  Record Route         : Enabled         Record Label         : Disabled
  FRR Flag             : Disabled        Bandwidth Protection : Disabled
  Backup Bandwidth Flag: Disabled        Backup Bandwidth Type: -
```

```
  Backup Bandwidth     : -
  Bypass Tunnel        : Yes              Auto Created         : Yes
  Route Pinning        : Disabled
  Retry Limit          : 3                Retry Interval       : 2 sec
  Reoptimization       : Disabled         Reoptimization Freq  : -
  Backup Type          : None             Backup LSP ID        : -
  Auto Bandwidth       : Disabled         Auto Bandwidth Freq  : -
  Min Bandwidth        : -                Max Bandwidth        : -
  Collected Bandwidth  : -
[RouterB] display mpls te tunnel-interface tunnel 51
Tunnel Name            : Tunnel 51
Tunnel State           : Up (Main CRLSP up, Shared-resource CRLSP down)
Tunnel Attributes      :
  LSP ID               : 16802            Tunnel ID            : 51
  Admin State          : Normal
  Ingress LSR ID       : 2.2.2.2          Egress LSR ID        : 3.3.3.3
  Signaling            : RSVP-TE          Static CRLSP Name    : -
  Resv Style           : SE
  Tunnel mode          : -
  Reverse-LSP name     : -
  Reverse-LSP LSR ID   : -                Reverse-LSP Tunnel ID: -
  Class Type           : CT0              Tunnel Bandwidth     : 0 kbps
  Reserved Bandwidth   : 0 kbps
  Setup Priority       : 7                Holding Priority     : 7
  Affinity Attr/Mask   : 0/0
  Explicit Path        : -
  Backup Explicit Path : -
  Metric Type          : TE
  Record Route         : Enabled          Record Label         : Disabled
  FRR Flag             : Disabled         Bandwidth Protection : Disabled
  Backup Bandwidth Flag: Disabled         Backup Bandwidth Type: -
  Backup Bandwidth     : -
  Bypass Tunnel        : Yes              Auto Created         : Yes
  Route Pinning        : Disabled
  Retry Limit          : 3                Retry Interval       : 2 sec
  Reoptimization       : Disabled         Reoptimization Freq  : -
  Backup Type          : None             Backup LSP ID        : -
  Auto Bandwidth       : Disabled         Auto Bandwidth Freq  : -
  Min Bandwidth        : -                Max Bandwidth        : -
  Collected Bandwidth  : -
```

在 Router B 上执行 **display mpls lsp** 命令，可以看到当前用来保护主 CRLSP 的 Bypass 隧道是 Tunnel50。

```
[RouterB] display mpls lsp
FEC                       Proto    In/Out Label    Interface/Out NHLFE
2.2.2.2/51/16802          RSVP     -/3             POS2/2/0
2.2.2.2/1/16802           RSVP     -/1151          GE2/1/2
Backup                             -/3             Tun50
2.2.2.2/50/16802          RSVP     -/3             POS2/2/1
```

```
3.2.1.2                    Local    -/-            POS2/2/1
3.3.1.2                    Local    -/-            POS2/2/0
```

在 Router A 上执行 **display rsvp lsp verbose** 命令，查看 Tunnel ID 为 1 的 MPLS TE 隧道的详细信息，可以看到主 CRLSP Tunnel1 被节点保护类型的自动隧道 Tunnel50 保护。

```
[RouterA] dispaly rsvp lsp tunnel-id 1 verbose
Tunnel name: Tunnel1
Destination: 4.4.4.4                      Source: 1.1.1.1
Tunnel ID: 1                              LSP ID: 16802
LSR type: Ingress                         Direction: Unidirectional
Setup priority: 7                         Holding priority: 7
In-Label: -                               Out-Label: 1150
In-Interface: -                           Out-Interface: GE2/1/1
Nexthop: 2.1.1.2                          Exclude-any: 0
Include-Any: 0                            Include-all: 0
Average bitrate: 0 kbps                   Maximum burst: 1000.00 bytes
Path MTU: 1500                            Class type: CT0
RRO number: 12
  2.1.1.1/32         Flag: 0x00 (No FRR)
  2.1.1.2/32         Flag: 0x00 (No FRR)
  1150               Flag: 0x01 (Global label)
  2.2.2.2/32         Flag: 0x20 (No FRR/Node-ID)
  3.1.1.1/32         Flag: 0x09 (FRR Avail/Node-Prot)
  3.1.1.2/32         Flag: 0x00 (No FRR)
  1151               Flag: 0x01 (Global label)
  3.3.3.3/32         Flag: 0x20 (No FRR/Node-ID)
  4.1.1.1/32         Flag: 0x00 (No FRR)
  4.1.1.2/32         Flag: 0x00 (No FRR)
  3                  Flag: 0x01 (Global label)
  4.4.4.4/32         Flag: 0x20 (No FRR/Node-ID)
Fast Reroute protection: Ready
  FRR inner label: 3          Bypass tunnel: Tunnel50
```

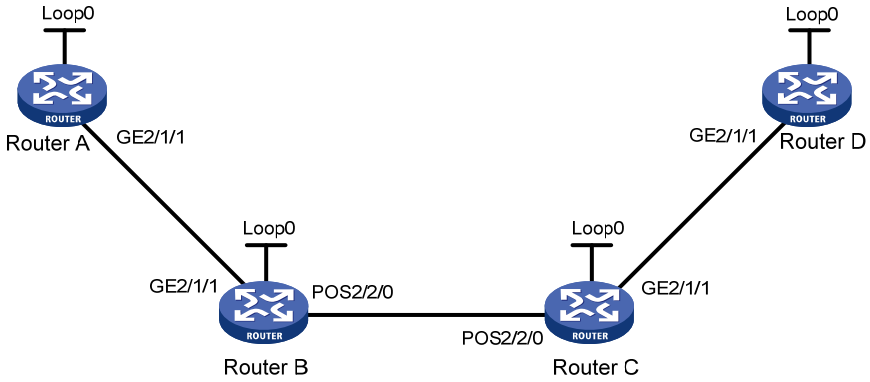
1.15.8 配置IETF DS-TE模式MPLS TE隧道示例

1. 组网需求

- 设备 Router A、Router B、Router C 和 Router D 运行 IS-IS，且都是 Level-2 设备；
- 使用 RSVP-TE 建立一条从 Router A 到 Router D 的 MPLS TE 隧道，该隧道的流量属于 CT 2，所需带宽为 4000kbps；
- 隧道沿途的链路最大带宽为 10000kbps，链路最大可预留带宽为 10000kbps，BC 1 的最大可预留带宽为 8000kbps，BC 2 的最大可预留带宽为 5000kbps，BC 3 的最大可预留带宽为 2000kbps。

2. 组网图

图1-14 IETF DS-TE 配置组网图



设备	接口	IP地址	设备	接口	IP地址
Router A	Loop0	1.1.1.9/32	Router C	Loop0	3.3.3.9/32
	GE2/1/1	10.1.1.1/24		GE2/1/1	30.1.1.1/24
Router B	Loop0	2.2.2.9/32		POS2/2/0	20.1.1.2/24
	GE2/1/1	10.1.1.2/24	Router D	Loop0	4.4.4.9/32
	POS2/2/0	20.1.1.1/24		GE2/1/1	30.1.1.2/24

3. 配置步骤

(1) 配置各接口的 IP 地址

按照 图 1-14 配置各接口的IP地址和掩码，具体配置过程略。

(2) 配置 IS-IS 协议发布接口所在网段的路由，包括 Loopback 接口

配置 Router A。

```
<RouterA> system-view
[RouterA] isis 1
[RouterA-isis-1] network-entity 00.0005.0000.0000.0001.00
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] isis enable 1
[RouterA-GigabitEthernet2/1/1] isis circuit-level level-2
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface loopback 0
[RouterA-LoopBack0] isis enable 1
[RouterA-LoopBack0] isis circuit-level level-2
[RouterA-LoopBack0] quit
```

配置 Router B。

```
<RouterB> system-view
[RouterB] isis 1
[RouterB-isis-1] network-entity 00.0005.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] isis enable 1
[RouterB-GigabitEthernet2/1/1] isis circuit-level level-2
[RouterB-GigabitEthernet2/1/1] quit
```

```
[RouterB] interface pos 2/2/0
[RouterB-POS2/2/0] isis enable 1
[RouterB-POS2/2/0] isis circuit-level level-2
[RouterB-POS2/2/0] quit
[RouterB] interface loopback 0
[RouterB-LoopBack0] isis enable 1
[RouterB-LoopBack0] isis circuit-level level-2
[RouterB-LoopBack0] quit
```

配置 Router C。

```
<RouterC> system-view
[RouterC] isis 1
[RouterC-isis-1] network-entity 00.0005.0000.0000.0003.00
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] isis enable 1
[RouterC-GigabitEthernet2/1/1] isis circuit-level level-2
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface pos 2/2/0
[RouterC-POS2/2/0] isis enable 1
[RouterC-POS2/2/0] isis circuit-level level-2
[RouterC-POS2/2/0] quit
[RouterC] interface loopback 0
[RouterC-LoopBack0] isis enable 1
[RouterC-LoopBack0] isis circuit-level level-2
[RouterC-LoopBack0] quit
```

配置 Router D。

```
<RouterD> system-view
[RouterD] isis 1
[RouterD-isis-1] network-entity 00.0005.0000.0000.0004.00
[RouterD-isis-1] quit
[RouterD] interface gigabitethernet 2/1/1
[RouterD-GigabitEthernet2/1/1] isis enable 1
[RouterD-GigabitEthernet2/1/1] isis circuit-level level-2
[RouterD-GigabitEthernet2/1/1] quit
[RouterD] interface loopback 0
[RouterD-LoopBack0] isis enable 1
[RouterD-LoopBack0] isis circuit-level level-2
[RouterD-LoopBack0] quit
```

配置完成后，在各设备上执行 **display ip routing-table** 命令，可以看到相互之间都学到了到对方的路由，包括 Loopback 接口对应的主机路由。以 Router A 为例：

```
[RouterA] display ip routing-table
Destinations : 10       Routes : 10
Destination/Mask  Proto  Pre  Cost     NextHop         Interface
1.1.1.9/32   Direct 0    0        127.0.0.1       InLoop0
2.2.2.9/32    ISIS   15   10        10.1.1.2        GE2/1/1
3.3.3.9/32    ISIS   15   20        10.1.1.2        GE2/1/1
4.4.4.9/32    ISIS   15   30        10.1.1.2        GE2/1/1
```

```
10.1.1.0/24   Direct 0    0        10.1.1.1        GE2/1/1
10.1.1.1/32   Direct 0    0        127.0.0.1       InLoop0
20.1.1.0/24   ISIS   15   20       10.1.1.2        GE2/1/1
30.1.1.0/24   ISIS   15   30       10.1.1.2        GE2/1/1
127.0.0.0/8   Direct 0    0        127.0.0.1       InLoop0
127.0.0.1/32  Direct 0    0        127.0.0.1       InLoop0
```

(3) 配置 LSR ID，开启 MPLS、MPLS TE 和 RSVP-TE 能力，并将 DS-TE 模式配置为 IETF 模式

配置 Router A。

```
[RouterA] mpls lsr-id 1.1.1.9
[RouterA] mpls te
[RouterA-te] ds-te mode ietf
[RouterA-te] quit
[RouterA] rsvp
[RouterA-rsvp] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mpls enable
[RouterA-GigabitEthernet2/1/1] mpls te enable
[RouterA-GigabitEthernet2/1/1] rsvp enable
[RouterA-GigabitEthernet2/1/1] quit
```

配置 Router B。

```
[RouterB] mpls lsr-id 2.2.2.9
[RouterB] mpls te
[RouterB-te] ds-te mode ietf
[RouterB-te] quit
[RouterB] rsvp
[RouterB-rsvp] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mpls enable
[RouterB-GigabitEthernet2/1/1] mpls te enable
[RouterB-GigabitEthernet2/1/1] rsvp enable
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface pos 2/2/0
[RouterB-POS2/2/0] mpls enable
[RouterB-POS2/2/0] mpls te enable
[RouterB-POS2/2/0] rsvp enable
[RouterB-POS2/2/0] quit
```

配置 Router C。

```
[RouterC] mpls lsr-id 3.3.3.9
[RouterC] mpls te
[RouterC-te] ds-te mode ietf
[RouterC-te] quit
[RouterC] rsvp
[RouterC-rsvp] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] mpls enable
[RouterC-GigabitEthernet2/1/1] mpls te enable
[RouterC-GigabitEthernet2/1/1] rsvp enable
```

```
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface pos 2/2/0
[RouterC-POS2/2/0] mpls enable
[RouterC-POS2/2/0] mpls te enable
[RouterC-POS2/2/0] rsvp enable
[RouterC-POS2/2/0] quit
```

配置 Router D。

```
[RouterD] mpls lsr-id 4.4.4.9
[RouterD] mpls te
[RouterD-te] ds-te mode ietf
[RouterD-te] quit
[RouterD] rsvp
[RouterC-rsvp] quit
[RouterD] interface gigabitethernet 2/1/1
[RouterD-GigabitEthernet2/1/1] mpls enable
[RouterD-GigabitEthernet2/1/1] mpls te enable
[RouterD-GigabitEthernet2/1/1] rsvp enable
[RouterD-GigabitEthernet2/1/1] quit
```

(4) 开启 IS-IS TE 功能，并配置 IS-IS 只可以接收和发送采用 wide 方式表示路径开销的消息

配置 Router A。

```
[RouterA] isis 1
[RouterA-isis-1] cost-style wide
[RouterA-isis-1] mpls te enable level-2
[RouterA-isis-1] quit
```

配置 Router B。

```
[RouterB] isis 1
[RouterB-isis-1] cost-style wide
[RouterB-isis-1] mpls te enable level-2
[RouterB-isis-1] quit
```

配置 Router C。

```
[RouterC] isis 1
[RouterC-isis-1] cost-style wide
[RouterC-isis-1] mpls te enable level-2
[RouterC-isis-1] quit
```

配置 Router D。

```
[RouterD] isis 1
[RouterD-isis-1] cost-style wide
[RouterD-isis-1] mpls te enable level-2
[RouterD-isis-1] quit
```

(5) 配置链路的 MPLS TE 属性

在 Router A 上配置链路的最大带宽和最大可预留带宽。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterA-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth rdm 10000 bc1 8000 bc2 5000
bc3 2000
[RouterA-GigabitEthernet2/1/1] quit
```

在 Router B 上配置链路的最大带宽和最大可预留带宽。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterB-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth rdm 10000 bc1 8000 bc2 5000 bc3 2000
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface pos 2/2/0
[RouterB-POS2/2/0] mpls te max-link-bandwidth 10000
[RouterB-POS2/2/0] mpls te max-reservable-bandwidth rdm 10000 bc1 8000 bc2 5000 bc3 2000
[RouterB-POS2/2/0] quit
```

在 Router C 上配置链路的最大带宽和最大可预留带宽。

```
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterC-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth rdm 10000 bc1 8000 bc2 5000 bc3 2000
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface pos 2/2/0
[RouterC-POS2/2/0] mpls te max-link-bandwidth 10000
[RouterC-POS2/2/0] mpls te max-reservable-bandwidth rdm 10000 bc1 8000 bc2 5000 bc3 2000
[RouterC-POS2/2/0] quit
```

在 Router D 上配置链路的最大带宽和最大可预留带宽。

```
[RouterD] interface gigabitethernet 2/1/1
[RouterD-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterD-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth rdm 10000 bc1 8000 bc2 5000 bc3 2000
[RouterD-GigabitEthernet2/1/1] quit
```

(6) 配置 MPLS TE 隧道

在 Router A 上配置 MPLS TE 隧道 Tunnel1：目的地址为 Router D 的 LSR ID（4.4.4.9）；采用 RSVP-TE 信令协议建立 MPLS TE 隧道；隧道的流量属于 CT 2，所需带宽为 4000kbps；隧道的建立和保持优先级均为 0。

```
[RouterA] interface Tunnel 1 mode mpls-te
[RouterA-Tunnel1] ip address 7.1.1.1 255.255.255.0
[RouterA-Tunnel1] destination 4.4.4.9
[RouterA-Tunnel1] mpls te signaling rsvp-te
[RouterA-Tunnel1] mpls te bandwidth ct2 4000
[RouterA-Tunnel1] mpls te priority 0
[RouterA-Tunnel1] quit
```

(7) 配置静态路由使流量沿 MPLS TE 隧道转发

在 Router A 上配置静态路由，使得到达网络 30.1.1.0/24 的流量通过 MPLS TE 隧道接口 Tunnel1 转发。

```
[RouterA] ip route-static 30.1.1.2 24 tunnel 1 preference 1
```

4. 验证配置

配置完成后，在 Router A 上执行 **display interface tunnel** 命令可以看到隧道接口状态为 up。

```
[RouterA] display interface tunnel
Tunnel1 current state: UP
Line protocol current state: UP
```

```
Description: Tunnel1 Interface
The Maximum Transmit Unit is 64000
Internet Address is 7.1.1.1/24 Primary
Tunnel source unknown, destination 4.4.4.9
Tunnel bandwidth 64 (kbps)
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Last clearing of counters: Never
    Last 300 seconds input rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes 0 drops
    0 packets output, 0 bytes 0 drops
```

在 Router A 上执行 **display mpls te tunnel-interface** 命令可以看到隧道的详细信息。

```
[RouterA] display mpls te tunnel-interface
Tunnel Name            : Tunnel 1
Tunnel State           : Up (Main CRLSP up, Shared-resource CRLSP down)
Tunnel Attributes      :
  LSP ID               : 36882           Tunnel ID            : 1
  Admin State          : Normal
  Ingress LSR ID       : 1.1.1.9         Egress LSR ID        : 4.4.4.9
  Signaling            : RSVP-TE         Static CRLSP Name    : -
  Resv Style           : SE
  Tunnel mode          : -
  Reverse-LSP name     : -
  Reverse-LSP LSR ID   : -               Reverse-LSP Tunnel ID: -
  Class Type           : CT2             Tunnel Bandwidth     : 4000 kbps
  Reserved Bandwidth   : 4000 kbps
  Setup Priority       : 0               Holding Priority     : 0
  Affinity Attr/Mask   : 0/0
  Explicit Path        : -
  Backup Explicit Path : -
  Metric Type          : TE
  Record Route         : Disabled        Record Label         : Disabled
  FRR Flag             : Disabled        Bandwidth Protection : Disabled
  Backup Bandwidth Flag: Disabled        Backup Bandwidth Type: -
  Backup Bandwidth     : -
  Bypass Tunnel        : No              Auto Created         : No
  Route Pinning        : Disabled
  Retry Limit          : 10              Retry Interval       : 2 sec
  Reoptimization       : Disabled        Reoptimization Freq  : -
  Backup Type          : None            Backup LSP ID        : -
  Auto Bandwidth       : Disabled        Auto Bandwidth Freq  : -
  Min Bandwidth        : -               Max Bandwidth        : -
  Collected Bandwidth  : -
```

在 Router A 上执行 **display mpls te link-management bandwidth-allocation** 命令查看接口带宽信息。

```
[RouterA] display mpls te link-management bandwidth-allocation interface
gigabitethernet2/11/1
Interface:  GigabitEthernet2/1/1
  Max Link Bandwidth                          : 10000 kbps
  Max Reservable Bandwidth of Prestandard RDM : 0 kbps
  Max Reservable Bandwidth of IETF RDM        : 10000 kbps
  Max Reservable Bandwidth of IETF MAM        : 0 kbps
  Allocated Bandwidth-Item Count  : 1
  Allocated Bandwidth             : 4000 kbps
  Physical Link Status            : Up
  BC  Prestandard RDM(kbps)  IETF RDM(kbps)       IETF MAM(kbps)
  0   0                      10000                0
  1   0                      8000                 0
  2   -                      5000                 0
  3   -                      2000                 0
  TE Class    Class Type    Priority   BW Reserved(kbps)  BW Available(kbps)
  0           0             7          0                  6000
  1           1             7          0                  4000
  2           2             7          0                  1000
  3           3             7          0                  1000
  4           0             0          0                  6000
  5           1             0          0                  4000
  6           2             0          4000               1000
  7           3             0          0                  1000
```

在 Router A 上执行 **display ip routing-table** 命令，可以看到路由表中有以 Tunnel1 为出接口的静态路由信息。

1.16 MPLS TE常见配置错误举例

1.16.1 不能产生TE LSA

1. 故障现象

配置 OSPF TE，无法产生描述 MPLS TE 信息的 TE LSA。

2. 分析

至少有一个 OSPF 邻居达到 FULL 状态时，才可能产生 TE LSA。

3. 处理过程

- 执行 **display current-configuration** 命令，检查是否在相关接口上配置了 MPLS TE；
- 执行 **debugging ospf mpls-te** 命令打开 OSPF TE 的调试开关，检查 OSPF 是否收到建立 TE LINK 的消息；
- 执行 **display ospf peer** 命令，检查 OSPF 邻居是否正常建立。

目 录

1 静态CRLSP ····· 1-1
1.1 静态CRLSP简介 ····· 1-1
1.2 建立静态CRLSP ····· 1-1
1.3 静态CRLSP显示和维护 ····· 1-2
1.4 静态CRLSP配置举例 ····· 1-2

1 静态CRLSP

1.1 静态CRLSP简介

静态 CRLSP（Constraint-based Routed Label Switched Paths，基于约束路由的 LSP）是指在报文经过的每一跳设备上（包括 Ingress、Transit 和 Egress）分别手工指定入标签、出标签、流量所需的带宽等信息，建立标签转发表项和资源预留，从而建立的 CRLSP。静态 CRLSP 与静态 LSP 的区别是：静态 CRLSP 需要在每一跳设备上为流量预留一定的带宽资源，如果设备上的带宽资源不满足流量需求，则无法建立静态 CRLSP。

建立静态 CRLSP 消耗的资源比较少，但静态建立的 CRLSP 不能根据网络拓扑变化动态调整。因此，静态 CRLSP 适用于拓扑结构简单并且稳定的小型网络。

建立静态 CRLSP 时，静态 CRLSP 经过的不同类型的节点上配置内容有所不同：

- Ingress：在 Ingress 上需要指定 CRLSP 的出标签、下一跳或到达下一跳的出接口、流量所需的带宽。在 Ingress 上创建 MPLS TE 隧道模式的 Tunnel 接口，并在该接口下引用指定的静态 CRLSP 后，如果需要通过 Tunnel 接口转发报文，则为该报文添加指定静态 CRLSP 的出标签，并将报文转发给指定的下一跳，或通过出接口转发该报文。
- Transit：Transit 根据报文中携带的标签值，查找标签转发表项，用新的标签替换原有标签。因此，Transit 上需要指定入标签对应的出标签、CRLSP 的下一跳或到达下一跳的出接口、流量所需的带宽。Transit 接收到带有标签的报文后，将报文中的标签替换为该标签对应的出标签，并将报文转发给指定的下一跳，或通过出接口转发该报文。
- Egress：如果没有在倒数第二跳弹出标签，则 Egress 负责弹出报文中的标签，并对报文进行下一层转发处理。因此，Egress 上只需指定入标签值。Egress 接收到带有指定入标签值的报文后，弹出该标签。

配置 Ingress、Transit、Egress 时，需要遵循以下原则：相邻两个 LSR（Label Switching Router，标签交换路由器）之间，上游 LSR 的出标签值和下游 LSR 的入标签值必须相同。

1.2 建立静态CRLSP

静态 CRLSP 作为一种特殊的静态 LSP，与静态 LSP 使用相同的标签空间，在同一台设备上静态 CRLSP 和静态 LSP 的入标签不能相同。

只有在 Ingress 节点创建 MPLS TE 隧道模式的 Tunnel 接口，并在该接口下引用静态 CRLSP 后，该静态 CRLSP 才能用来转发 MPLS TE 流量。MPLS TE 的详细介绍，请参见“MPLS 配置指导”中的“MPLS TE”。

在配置静态 CRLSP 之前，需完成以下任务：

- 确定静态 CRLSP 的 Ingress 节点、Transit 节点和 Egress 节点。
- 在参与 MPLS 转发的设备接口上使能 MPLS 功能，配置方法请参见“MPLS 配置指导”中的“MPLS 基本配置”。
- 在 Ingress、Transit 和 Egress 节点上开启本节点的 MPLS TE 能力，并在 CRLSP 经过的接口上开启接口的 MPLS TE 能力，配置方法请参见“MPLS 配置指导”中的“MPLS TE”。

表1-1 建立静态 CRLSP

操作	命令	说明
进入系统视图	**system-view**	-
配置静态CRLSP的Ingress节点	**static-cr-lsp ingress** *lsp-name* { **nexthop** *next-hop-addr* | **outgoing-interface** *interface-type interface-number* } **out-label** *out-label-value* [**bandwidth** [**ct0** | **ct1** | **ct2** | **ct3**] *bandwidth-value*]	请根据节点在静态CRLSP上的位置从三者中选择其一 缺省情况下，设备上不存在任何静态CRLSP 配置静态CRLSP的Ingress节点和Transit节点时，指定的下一跳地址不能是本地设备上的公网IP地址 如果静态CRLSP的倒数第二跳节点上配置的出标签为0或3，则不需要在Egress节点上执行本命令
配置静态CRLSP的Transit节点	**static-cr-lsp transit** *lsp-name* **in-label** *in-label-value* { **nexthop** *next-hop-addr* | **outgoing-interface** *interface-type interface-number* } **out-label** *out-label-value* [**bandwidth** [**ct0** | **ct1** | **ct2** | **ct3**] *bandwidth-value*]	
配置静态CRLSP的Egress节点	**static-cr-lsp egress** *lsp-name* **in-label** *in-label-value*	

1.3 静态CRLSP显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后静态 CRLSP 的运行情况，用户可以通过查看显示信息验证配置的效果。

表1-2 静态 CRLSP 显示和维护

操作	命令
显示静态CRLSP信息	**display mpls static-cr-lsp** [**lsp-name** *lsp-name*] [**verbose**]

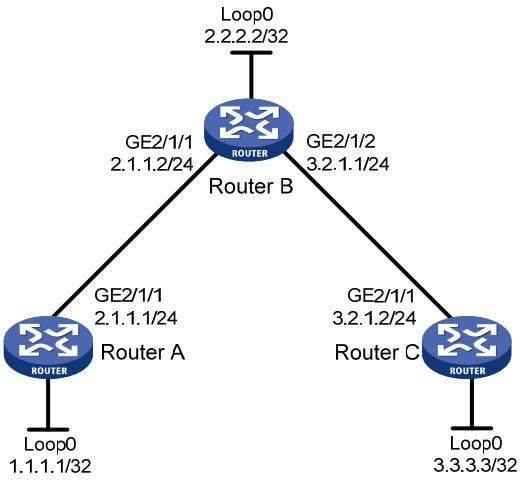
1.4 静态CRLSP配置举例

1. 组网需求

- 设备 Router A、Router B 和 Router C 运行 IS-IS；
- 使用静态 CRLSP 建立一条 Router A 到 Router C 的 MPLS TE 隧道，隧道需要的带宽为 2000kbps；
- 隧道沿途的链路最大带宽为 10000kbps，最大可预留带宽为 5000kbps。

2. 组网图

图1-1 静态 CRLSP 配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址

按照 图 1-1 配置各接口的IP地址和掩码，具体配置过程略。

(2) 配置 IS-IS 协议发布接口所在网段的路由，包括 Loopback 接口

配置 Router A。

```
<RouterA> system-view
[RouterA] isis 1
[RouterA-isis-1] network-entity 00.0005.0000.0000.0001.00
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] isis enable 1
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface loopback 0
[RouterA-LoopBack0] isis enable 1
[RouterA-LoopBack0] quit
```

配置 Router B。

```
<RouterB> system-view
[RouterB] isis 1
[RouterB-isis-1] network-entity 00.0005.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] isis enable 1
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] isis enable 1
[RouterB-GigabitEthernet2/1/2] quit
[RouterB] interface loopback 0
[RouterB-LoopBack0] isis enable 1
[RouterB-LoopBack0] quit
```

配置 Router C。

```
<RouterC> system-view
[RouterC] isis 1
[RouterC-isis-1] network-entity 00.0005.0000.0000.0003.00
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] isis enable 1
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface loopback 0
[RouterC-LoopBack0] isis enable 1
[RouterC-LoopBack0] quit
```

配置完成后，在各设备上执行 **display ip routing-table** 命令，可以看到相互之间都学到了到对方的路由，包括 Loopback 接口对应的主机路由。

(3) 配置 LSR ID、开启 MPLS 能力和 MPLS TE 能力

配置 Router A。

```
[RouterA] mpls lsr-id 1.1.1.1
[RouterA] mpls te
[RouterA-te] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mpls enable
[RouterA-GigabitEthernet2/1/1] mpls te enable
[RouterA-GigabitEthernet2/1/1] quit
```

配置 Router B。

```
[RouterB] mpls lsr-id 2.2.2.2
[RouterB] mpls te
[RouterB-te] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mpls enable
[RouterB-GigabitEthernet2/1/1] mpls te enable
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] mpls enable
[RouterB-GigabitEthernet2/1/2] mpls te enable
[RouterB-GigabitEthernet2/1/2] quit
```

配置 Router C。

```
[RouterC] mpls lsr-id 3.3.3.3
[RouterC] mpls te
[RouterC-te] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] mpls enable
[RouterC-GigabitEthernet2/1/1] mpls te enable
[RouterC-GigabitEthernet2/1/1] quit
```

(4) 配置链路的 MPLS TE 属性

在 Router A 上配置链路的最大带宽和最大可预留带宽。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
```

```
[RouterA-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth 5000
[RouterA-GigabitEthernet2/1/1] quit
```

在 Router B 上配置链路的最大带宽和最大可预留带宽。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterB-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth 5000
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] mpls te max-link-bandwidth 10000
[RouterB-GigabitEthernet2/1/2] mpls te max-reservable-bandwidth 5000
[RouterB-GigabitEthernet2/1/2] quit
```

在 Router C 上配置链路的最大带宽和最大可预留带宽。

```
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterC-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth 5000
[RouterC-GigabitEthernet2/1/1] quit
```

(5) 配置 MPLS TE 隧道

在 Router A 上配置 MPLS TE 隧道 Tunnel0：目的地址为 Router C 的 LSR ID（3.3.3.3）；采用静态 CRLSP 建立 MPLS TE 隧道。

```
[RouterA] interface tunnel 0 mode mpls-te
[RouterA-Tunnel0] ip address 6.1.1.1 255.255.255.0
[RouterA-Tunnel0] destination 3.3.3.3
[RouterA-Tunnel0] mpls te signaling static
[RouterA-Tunnel0] quit
```

(6) 创建静态 CRLSP

配置 Router A 为静态 CRLSP 的 Ingress 节点，下一跳地址为 2.1.1.2，出标签为 20，隧道所需的带宽为 2000kbps。

```
[RouterA] static-cr-lsp ingress static-cr-lsp-1 nexthop 2.1.1.2 out-label 20 bandwidth 2000
```

在 Router A 上配置隧道 Tunnel0 引用名称为 static-cr-lsp-1 的静态 CRLSP。

```
[RouterA] interface Tunnel0
[RouterA-Tunnel0] mpls te static-cr-lsp static-cr-lsp-1
[RouterA-Tunnel0] quit
```

配置 Router B 为静态 CRLSP 的 Transit 节点，入标签为 20，下一跳地址为 3.2.1.2，出标签为 30，隧道所需的带宽为 2000kbps。

```
[RouterB] static-cr-lsp transit static-cr-lsp-1 in-label 20 nexthop 3.2.1.2 out-label 30
bandwidth 2000
```

配置 Router C 为静态 CRLSP 的 Egress 节点，入标签为 30。

```
[RouterC] static-cr-lsp egress static-cr-lsp-1 in-label 30
```

(7) 配置静态路由使流量沿 MPLS TE 隧道转发

在 Router A 上配置静态路由，使得到达网络 3.2.1.0/24 的流量通过 MPLS TE 隧道接口 Tunnel0 转发。

```
[RouterA] ip route-static 3.2.1.2 24 tunnel 0 preference 1
```

4. 验证配置

配置完成后，在 Router A 上执行 **display interface tunnel** 命令，可以看到 Tunnel 接口的状态为 up。

```
[RouterA] display interface tunnel
Tunnel0
Current state: UP
Line protocol state: UP
Description: Tunnel0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1496
Internet Address is 6.1.1.1/24 Primary
Tunnel source unknown, destination 3.3.3.3
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

在 Router A 上执行 **display mpls te tunnel-interface** 命令，可以看到 MPLS TE 隧道的建立情况。

```
[RouterA] display mpls te tunnel-interface
Tunnel Name            : Tunnel 0
Tunnel State           : Up (Main CRLSP up)
Tunnel Attributes      :
  LSP ID               : 1              Tunnel ID            : 0
  Admin State          : Normal
  Ingress LSR ID       : 1.1.1.1        Egress LSR ID        : 3.3.3.3
  Signaling            : Static         Static CRLSP Name    : static-cr-lsp-1
  Resv Style           : -
  Tunnel mode          : -
  Reverse-LSP name     : -
  Reverse-LSP LSR ID   : -              Reverse-LSP Tunnel ID: -
  Class Type           : -              Tunnel Bandwidth     : -
  Reserved Bandwidth   : -
  Setup Priority       : 0              Holding Priority     : 0
  Affinity Attr/Mask   : -/-
  Explicit Path        : -
  Backup Explicit Path : -
  Metric Type          : TE
  Record Route         : -              Record Label         : -
  FRR Flag             : -              Backup Bandwidth Flag: -
  Backup Bandwidth Type: -              Backup Bandwidth     : -
  Route Pinning        : -
  Retry Limit          : 3              Retry Interval       : 2 sec
```

```
  Reoptimization       : -              Reoptimization Freq  : -
  Backup Type          : -              Backup LSP ID        : -
  Auto Bandwidth       : -              Auto Bandwidth Freq  : -
  Min Bandwidth        : -              Max Bandwidth        : -
  Collected Bandwidth  : -
```

在各设备上执行 **display mpls lsp** 或 **display mpls static-cr-lsp** 命令，可以看到静态 CRLSP 的建立情况。

```
[RouterA] display mpls lsp
FEC                        Proto    In/Out Label    Interface/Out NHLFE
1.1.1.1/0/1                StaticCR -/20            GE2/1/1
2.1.1.2                    Local    -/-             GE2/1/1
[RouterB] display mpls lsp
FEC                        Proto    In/Out Label    Interface/Out NHLFE
-                          StaticCR 20/30           GE2/1/2
3.2.1.2                    Local    -/-             GE2/1/2
[RouterC] display mpls lsp
FEC                        Proto    In/Out Label    Interface/Out NHLFE
-                          StaticCR 30/-            -
[RouterA] display mpls static-cr-lsp
Name            LSR Type    In/Out Label   Out Interface        State
static-cr-lsp-1 Ingress     Null/20        GE2/1/1               Up
[RouterB] display mpls static-cr-lsp
Name            LSR Type    In/Out Label   Out Interface        State
static-cr-lsp-1 Transit     20/30          GE2/1/2               Up
[RouterC] display mpls static-cr-lsp
Name            LSR Type    In/Out Label   Out Interface        State
static-cr-lsp-1 Egress      30/Null        -                    Up
```

在 RouterA 上执行 **display ip routing-table** 命令，可以看到路由表中有以 Tunnel0 为出接口的静态路由信息。

目 录

1 RSVP ····· 1-1
1.1 RSVP简介 ····· 1-1
1.1.1 RSVP消息 ····· 1-1
1.1.2 CRLSP建立过程 ····· 1-2
1.1.3 RSVP刷新机制 ····· 1-2
1.1.4 RSVP认证功能 ····· 1-3
1.1.5 RSVP GR ····· 1-3
1.1.6 协议规范 ····· 1-4
1.2 RSVP配置任务简介 ····· 1-4
1.3 开启RSVP能力 ····· 1-4
1.4 配置RSVP的Refresh消息刷新功能 ····· 1-5
1.5 配置RSVP摘要刷新和RSVP消息的可靠传递功能 ····· 1-5
1.6 配置RSVP的Hello扩展功能 ····· 1-6
1.7 配置RSVP认证功能 ····· 1-6
1.8 配置发送的RSVP报文的DSCP优先级 ····· 1-8
1.9 配置RSVP GR ····· 1-8
1.10 配置RSVP与BFD联动 ····· 1-9
1.11 RSVP显示和维护 ····· 1-9
1.12 RSVP配置举例 ····· 1-10
1.12.1 使用RSVP-TE配置MPLS TE隧道示例 ····· 1-10
1.12.2 配置RSVP GR示例 ····· 1-16

1 RSVP

1.1 RSVP简介

RSVP（Resource Reservation Protocol，资源预留协议）是一种用来在网络上请求预留资源的信令协议。RSVP 经扩展后支持 MPLS 标签的分发，在传送标签绑定消息的同时携带资源预留信息。这种扩展后的 RSVP 可以作为 MPLS TE 的标签分发协议，沿着指定路径分发 MPLS 标签并预留资源，以建立 CRLSP（Constraint-based Routed Label Switched Paths，基于约束路由的 LSP）。扩展后的 RSVP 称为 RSVP-TE。

1.1.1 RSVP消息

RSVP 消息分为以下几种：

- Path 消息：由发送者沿数据报文传输的方向向下游发送，在沿途所有节点上保存路径状态。
- Resv 消息：由接收者沿与数据报文传输相反的方向发送，在沿途所有节点上进行资源预留，并创建和维护预留状态。
- PathTear 消息：由发送者或中间节点向下游发送，用来删除沿途节点的路径状态和相关的预留状态。
- ResvTear 消息：由接收者或中间节点向上游发送，用来删除沿途节点的预留状态。
- PathErr 消息：如果接收者或中间节点在处理 Path 消息的过程中发生了错误，就会向上游发送 PathErr 消息，PathErr 消息不影响沿途节点的状态，只是把错误报告给发送者。
- ResvErr 消息：如果发送者或中间节点在处理 Resv 消息的过程中发生了错误，或者由于抢占导致预留被破坏，就会向下游节点发送 ResvErr 消息。
- ResvConf 消息：该消息发往接收者，用于对预留消息进行确认。
- Hello 消息：用来在两个直连的 RSVP 邻居之间建立和维持邻居关系，以检测邻居的状态。只有开启 RSVP 的 Hello 扩展功能后，才会发送该消息。

RSVP-TE 对 RSVP 消息的扩展主要是在 Path 消息和 Resv 消息中增加了新的对象。新增对象除了可以携带标签信息外，还可以携带在沿途寻找路径时的限制信息，从而实现对约束条件和快速重路由的支持。

Path 消息新增的对象包括：

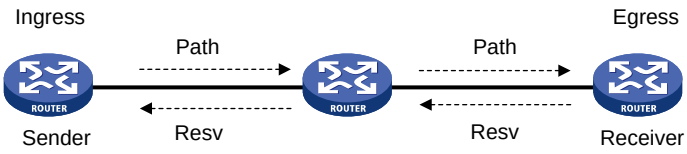
- LABEL_REQUEST：用来请求下游节点分配标签。
- EXPLICIT_ROUTE：用来携带 Ingress 节点计算出的路径信息，确保沿着该路径建立 CRLSP。
- RECORD_ROUTE：用来记录 CRLSP 实际经过的路径及各个节点分配的标签。
- SESSION_ATTRIBUTE：用来携带 MPLS TE 隧道的属性信息，如建立优先级、保持优先级、亲和属性等。

Resv 消息新增的对象包括：

- LABEL：用来将下游节点分配的标签通告给上游节点。
- RECORD_ROUTE：用来记录 CRLSP 实际经过的路径及各个节点分配的标签。

1.1.2 CRLSP建立过程

图1-1 CRLSP 建立过程



如 图 1-1 所示，使用RSVP-TE建立CRLSP的过程为：

(1) Ingress LSR 产生携带 LABEL_REQUEST 对象的 Path 消息，沿着通过 CSPF 计算出的路径逐跳发送给 Egress LSR。Path 消息经过的 LSR，都依据 Path 消息生成路径状态。

(2) Egress LSR 收到 Path 消息后，产生携带预留信息和 LABEL 对象的 Resv 消息，沿着 Path 消息的相反路径逐跳发送给 Ingress LSR。Resv 消息通告标签的同时，在沿途的 LSR 上预留一定的资源，并生成预留状态。

(3) 当 Ingress LSR 收到 Resv 消息时，CRLSP 建立成功。

1.1.3 RSVP刷新机制

1. Refresh消息

由于 RSVP 是软状态协议，因此需要定时发送消息来维护节点上的资源预留状态。

资源预留状态包括路径状态和预留状态，分别保存在如下状态块中：

- PSB（Path State Block，路径状态块）：由 Path 消息创建，用来保存 LABEL_REQUEST 对象。
- RSB（Reservation State Block，预留状态块）：由 Resv 消息创建，用来保存 LABEL 对象。

路径状态和预留状态分别由周期性发送的 Path 消息和 Resv 消息来刷新。对于某个状态，如果在一定时间内没有收到刷新消息，则 PSB 或 RSB 中相应的状态将被删除，根据该状态建立的 CRLSP 也将被删除。

用来刷新资源预留状态的 Path 和 Resv 消息，统称为 Refresh 消息。Refresh 消息除了刷新资源预留状态外，还可以用于恢复丢失的 RSVP 消息。

由于 Refresh 消息是周期性发送的，当网络中的 RSVP 会话比较多时，Refresh 消息会加重网络负担，此时 Path 和 Resv 消息的刷新时间间隔不易过小；而对于时延敏感的应用，当 RSVP 消息丢失时，希望能够尽快通过 Refresh 消息恢复丢失的消息，此时 Path 和 Resv 消息的刷新时间间隔不易过大。简单地调整刷新间隔并不能同时解决这两类问题。

Srefresh（Summary Refresh，摘要刷新）和 RSVP 消息的可靠传递功能可以很好地解决上述问题。

2. 摘要刷新功能

摘要刷新功能的工作机制为：发送 Path 和 Resv 消息时，在消息中携带 Message ID，用来唯一标识一个消息；RSVP 通过发送携带待刷新消息 Message ID 的 Srefresh 消息，来刷新对应的 Path 和 Resv 消息。

采用摘要刷新功能后，不必传送标准的 Path 和 Resv 消息，只需传递携带 Path 和 Resv 消息摘要的 Srefresh 消息，即可实现对 RSVP 路径和预留状态进行刷新，减少了网络上的 Refresh 消息流量，并加快了节点对刷新消息的处理速度。

3. RSVP消息的可靠传递功能

RSVP 消息没有重传机制，消息丢失后发送端无法获悉，无法重传丢失的消息。通过 RSVP 消息的可靠性传递功能可以提高消息传递的可靠性。

RSVP 消息的可靠传递功能是指对端设备需要应答本端发送的 RSVP 消息，否则将会重传此消息。其工作机制为：节点发送了携带 Message_ID 对象的消息，且 Message_ID 对象的 ACK_Desired 标识（是否需要应答标识）置位后，如果在重传时间 Rf 内没有收到携带对应 Message_ID_ACK 对象的消息，则重传时间 Rf 超时后重传此消息，并将重传时间置为（1＋Delta）×Rf。节点持续按照上述方法重传此消息，直到节点在重传时间超时前接收到对应的应答消息，或消息传送次数达到 3 次。

1.1.4 RSVP认证功能

RSVP 认证功能可以用来确保 RSVP 消息不会被篡改，以防止伪造的资源预留请求非法占用网络资源。

RSVP 认证功能是指：发送 RSVP 消息时使用 MD5 算法对认证密钥和消息内容计算出消息摘要，并将消息摘要添加到发送的 RSVP 消息中。对端接收到 RSVP 消息后，进行同样地计算，并将计算结果和消息中的摘要进行比较。如果一致，则认证通过，接收该消息；否则认证失败，丢弃该消息。

通过在消息中携带序列号，RSVP 认证功能还可以用来防止报文重放攻击。设备记录接收到的 RSVP 消息的序列号，并根据记录的序列号判断后续消息是否符合要求。只有收到的消息的序列号在允许的范围内时，才接收该消息；否则，丢弃该消息。

1.1.5 RSVP GR

RSVP GR（Graceful Restart，平滑重启）功能是指在信令协议或控制平面出现异常时，保持转发表项信息，以保证数据转发不中断。

参与 RSVP GR 过程的设备分为以下两种角色：

- GR Restarter：GR 重启路由器，指由管理员手工或设备故障触发而重启协议的设备，它必须具备 GR 能力。
- GR Helper：GR Restarter 的邻居，与重启的 GR Restarter 保持邻居关系，并协助其恢复重启前的转发状态，它也必须具备 GR 能力。

目前，设备只能作为 RSVP GR 的 GR Helper。

RSVP GR 依赖于 RSVP 的 Hello 扩展能力，通过 Hello 消息向邻居通告自己的 GR 能力和相关时间参数。设备和邻居如果都具备 RSVP GR 能力，那么在完成 GR 参数的交互后，就可以在检测到对方发生 GR 重启时，充当对方的 GR Helper，保证在 GR Restarter 重启的过程中，数据转发不会中断。

当 GR Restarter 发生重启时，GR Helper 连续丢失的 Hello 消息次数达到了配置的值，GR Helper 由此判定 GR Restarter 发生了重启。此时 GR Helper 会保留与该邻居相关的软状态信息，并保持向对方周期性发送 Hello 消息，直到重启定时器（Restart Timer）超时。

在重启定时器超时前，如果 GR Helper 接收到了 GR Restarter 发送的 Hello 消息，那么启动恢复定时器，并触发信令消息交互以恢复原有的软状态；否则，将删除与该邻居相关的所有 RSVP 软状态信息和转发表项。恢复定时器超时后，删除仍然没有恢复的软状态和转发表项。

1.1.6 协议规范

与 RSVP 相关的协议规范有：

- RFC 2205：Resource ReSerVation Protocol
- RFC 3209：RSVP-TE: Extensions to RSVP for LSP Tunnels
- RFC 2961：RSVP Refresh Overhead Reduction Extensions

1.2 RSVP配置任务简介

表1-1 RSVP 配置任务简介

配置任务	说明	详细配置
开启RSVP能力	必选	1.3
配置RSVP的Refresh消息刷新功能	可选 请根据实际组网需求，在MPLS TE隧道经过的节点上选择配置各功能	1.4
配置RSVP摘要刷新和RSVP消息的可靠传递功能		1.5
配置RSVP的Hello扩展功能		1.6
配置RSVP认证功能		1.7
配置发送的RSVP报文的DSCP优先级		1.8
配置RSVP GR		1.9
配置RSVP与BFD联动		1.10

1.3 开启RSVP能力

为了建立 MPLS TE 隧道，在 MPLS TE 隧道经过的所有节点和接口上都需要开启 RSVP 能力。

表1-2 开启 RSVP 能力

操作	命令	说明
进入系统视图	**system-view**	-
全局开启RSVP能力，并进入RSVP视图	**rsvp**	缺省情况下，全局RSVP能力处于关闭状态
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
开启接口的RSVP能力	**rsvp enable**	缺省情况下，接口的RSVP能力处于关闭状态

1.4 配置RSVP的Refresh消息刷新功能

表1-3 配置 RSVP 的 Refresh 消息刷新功能

操作	命令	说明
进入系统视图	**system-view**	-
进入RSVP视图	**rsvp**	-
配置路径消息和预留消息的刷新时间间隔	**refresh interval** *interval*	缺省情况下，路径消息和预留消息的刷新时间间隔为30秒
配置PSB和RSB的老化超时倍数	**keep-multiplier** *number*	缺省情况下，PSB和RSB的老化超时倍数为3

1.5 配置RSVP摘要刷新和RSVP消息的可靠传递功能

提示

开启摘要刷新功能后，将不会周期性发送 Refresh 消息维护路径和预留状态。

表1-4 配置 RSVP 摘要刷新和 RSVP 消息的可靠传递功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
开启摘要刷新功能和RSVP消息的可靠传递功能	**rsvp reduction srefresh** [**reliability**]	缺省情况下，摘要刷新功能和RSVP消息的可靠传递功能处于关闭状态
配置RSVP消息可靠传递功能的重传增量	**rsvp reduction retransmit increment** *increment-value*	缺省情况下，RSVP消息可靠传递功能的重传增量为1 通过**rsvp reduction srefresh reliability**命令开启RSVP消息的可靠传递功能后，本命令才会生效
配置RSVP消息可靠传递功能的重传时间间隔	**rsvp reduction retransmit interval** *retrans-timer-value*	缺省情况下，RSVP消息可靠传递功能的重传时间间隔为500毫秒 通过**rsvp reduction srefresh reliability**命令开启RSVP消息的可靠传递功能后，本命令才会生效

1.6 配置RSVP的Hello扩展功能

在接口视图下开启 RSVP 的 Hello 扩展功能后，设备会通过该接口发送和接收 Hello 消息，通过 Hello 消息检测邻居的状态。

在 **hello interval** 命令指定的时间内，如果没有收到邻居发送的 Hello Request 消息，则主动向邻居发送 Hello Request 消息；如果收到了邻居发送的 Hello Request 消息，则立即向邻居回应 Hello Ack 消息。

当连续未收到 Hello 消息或收到错误的 Hello 消息的次数达到 **hello lost** 命令配置的次数时，认为邻居设备发生故障。如果配置了 GR 功能，则本地设备作为 GR Helper 协助邻居进行 GR 重启；如果没有配置 GR 功能，但配置了 FRR（Fast Reroute，快速重路由）功能，则进行 FRR 切换。

FRR 的详细介绍，请参见“MPLS 配置指导”中的“MPLS TE”。

表1-5 配置 RSVP 的 Hello 扩展功能

操作	命令	说明
进入系统视图	**system-view**	-
进入RSVP视图	**rsvp**	-
配置Hello消息连续丢失或错误的最大次数	**hello lost** *times*	缺省情况下，Hello消息连续丢失或错误的最大次数为4次
配置Hello Request消息的发送时间间隔	**hello interval** *interval*	缺省情况下，Hello Request消息的发送时间间隔为5秒
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
开启RSVP的Hello扩展功能	**rsvp hello enable**	缺省情况下，RSVP的Hello扩展功能处于关闭状态

1.7 配置RSVP认证功能

提示

建议不要在同一个接口上同时配置快速重路由功能和 RSVP 认证功能。

为防止伪造的资源预留请求非法占用网络资源，RSVP 采用逐跳认证机制来验证 RSVP 消息的合法性。一条链路两端的接口上需要配置相同的认证密钥，只有这样，接口之间才可以正确地交互 RSVP 消息。

RSVP 认证功能可以在如下视图配置：

- RSVP 视图：该视图下的配置对所有 RSVP SA 生效。
- RSVP 邻居视图：该视图下的配置只对与指定 RSVP 邻居之间的 RSVP SA 生效。
- 接口视图：该视图下的配置只对根据指定接口下的配置生成的 RSVP SA 生效。

三个视图下配置的优先级从高到低依次为：RSVP 邻居视图、接口视图、RSVP 视图。

表1-6 配置 RSVP 认证功能（RSVP 邻居视图）

操作	命令	说明
进入系统视图	**system-view**	-
进入RSVP视图	**rsvp**	-
创建RSVP认证邻居，并进入RSVP邻居视图	**peer** *ip-address*	缺省情况下，设备上不存在任何RSVP认证邻居
为指定RSVP邻居开启RSVP认证功能，并配置认证密钥	**authentication key** { **cipher** | **plain** } *auth-key*	缺省情况下，RSVP认证功能处于关闭状态，即不进行RSVP认证
为指定RSVP邻居开启RSVP认证的challenge-response握手功能	**authentication challenge**	缺省情况下，认证的challenge-response握手功能处于关闭状态
为指定RSVP邻居配置RSVP SA（Security Association，安全联盟）的空闲老化时间	**authentication lifetime** *life-time*	缺省情况下，RSVP SA的空闲老化时间为1800秒（30分钟）
为指定RSVP邻居配置对于带有认证信息的RSVP消息，最大可允许的乱序消息数量	**authentication window-size** *number*	缺省情况下，对于带有认证信息的RSVP消息，最大可允许的乱序消息数量为1

表1-7 配置 RSVP 认证功能（接口视图）

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
在接口下开启RSVP认证功能，并配置认证密钥	**rsvp authentication key** { **cipher** | **plain** } *auth-key*	缺省情况下，RSVP认证功能处于关闭状态，即不进行RSVP认证
在接口下开启RSVP认证的challenge-response握手功能	**rsvp authentication challenge**	缺省情况下，RSVP认证的challenge-response握手功能处于关闭状态
在接口下配置RSVP SA的空闲老化时间	**rsvp authentication lifetime** *life-time*	缺省情况下，RSVP SA的空闲老化时间为1800秒（30分钟）
在接口下配置对于带有认证信息的RSVP消息，最大可允许的乱序消息数量	**rsvp authentication window-size** *number*	缺省情况下，对于带有认证信息的RSVP消息，最大可允许的乱序消息数量为1

表1-8 配置 RSVP 认证功能（RSVP 视图）

操作	命令	说明
进入系统视图	**system-view**	-
进入RSVP视图	**rsvp**	-

操作	命令	说明
全局开启RSVP认证功能，并配置认证密钥	**authentication key** { **cipher** | **plain** } *auth-key*	缺省情况下，RSVP认证功能处于关闭状态，即不进行RSVP认证
全局开启RSVP认证的challenge-response握手功能	**authentication challenge**	缺省情况下，认证的challenge-response握手功能处于关闭状态
全局配置RSVP SA的空闲老化时间	**authentication lifetime** *life-time*	缺省情况下，RSVP SA的空闲老化时间为1800秒（30分钟）
全局配置对于带有认证信息的RSVP消息，最大可允许的乱序消息数量	**authentication window-size** *number*	缺省情况下，对于带有认证信息的RSVP消息，最大可允许的乱序消息数量为1

1.8 配置发送的RSVP报文的DSCP优先级

DSCP（Differentiated Services Code point，差分服务编码点）携带在 IP 报文中的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。通过本配置可以指定发送的 RSVP 报文中携带的 DSCP 优先级的取值。

表1-9 配置发送的 RSVP 报文的 DSCP 优先级

操作	命令	说明
进入系统视图	**system-view**	-
进入RSVP视图	**rsvp**	-
配置发送的RSVP报文的DSCP优先级	**dscp** *dscp-value*	缺省情况下，RSVP报文的DSCP优先级为48

1.9 配置RSVP GR

RSVP GR 功能依赖于 RSVP 的 Hello 扩展能力，因此在配置 RSVP GR 功能时必须开启 RSVP 的 Hello 扩展能力。

在 GR 设备上进行以下配置。

表1-10 配置 RSVP GR

操作	命令	说明
进入系统视图	**system-view**	-
进入RSVP视图	**rsvp**	-
开启RSVP的GR功能	**graceful-restart enable**	缺省情况下，RSVP的GR功能处于关闭状态
退回系统视图	**quit**	-

操作	命令	说明
进入接口视图	**interface** *interface-type interface-number*	-
开启RSVP的Hello扩展功能	**rsvp hello enable**	缺省情况下，RSVP的Hello扩展功能处于关闭状态

1.10 配置RSVP与BFD联动

在 MPLS TE 网络中，LSR 邻居之间的链路发生故障将导致 MPLS TE 转发报文失败，而 MPLS TE 本身无法快速检测到链路故障。通过在 MPLS TE 隧道内的两个 RSVP 邻居上分别配置 RSVP 与 BFD（Bidirectional Forwarding Detection，双向转发检测）联动，可以快速地感知邻居之间链路的故障，确保链路出现故障时将业务从主路径切换到备份路径上。

表1-11 配置 RSVP 与 BFD 联动

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	该接口上需要开启RSVP能力
配置通过BFD检测本地设备和RSVP邻居之间链路的状态	**rsvp bfd enable**	缺省情况下，不会通过BFD检测本地设备和RSVP邻居之间链路的状态

1.11 RSVP显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 RSVP 的运行情况，用户可以通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 RSVP 统计信息。

表1-12 RSVP 的显示和维护

操作	命令
显示RSVP的信息	**display rsvp** [**interface** [*interface-type interface-number*]]
显示本地设备与RSVP邻居建立的RSVP SA信息	**display rsvp authentication** [**from** *ip-address*] [**to** *ip-address*] [**verbose**]
显示RSVP建立的CR-LSP信息	**display rsvp lsp** [**destination** *ip-address*] [**source** *ip-address*] [**tunnel-id** *tunnel-id*] [**lsp-id** *lsp-id*] [**verbose**]
显示RSVP邻居的信息	**display rsvp peer** [**interface** *interface-type interface-number*] [**ip** *ip-address*] [**verbose**]
显示向上游设备发送的RSVP资源预留请求的信息	**display rsvp request** [**destination** *ip-address*] [**source** *ip-address*] [**tunnel-id** *tunnel-id*] [**prevhop** *ip-address*] [**verbose**]

操作	命令
显示RSVP资源预留状态信息	**display rsvp reservation** [**destination** *ip-address*] [**source** *ip-address*] [**tunnel-id** *tunnel-id*] [**nexthop** *ip-address*] [**verbose**]
显示RSVP路径状态信息	**display rsvp sender** [**destination** *ip-address*] [**source** *ip-address*] [**tunnel-id** *tunnel-id*] [**lsp-id** *lsp-id*] [**verbose**]
显示RSVP统计信息	**display rsvp statistics** [**interface** [*interface-type interface-number*]]
手工清除RSVP SA	**reset rsvp authentication** [**from** *ip-address* **to** *ip-address*]
清除RSVP的统计信息	**reset rsvp statistics** [**interface** [*interface-type interface-number*]

1.12 RSVP配置举例

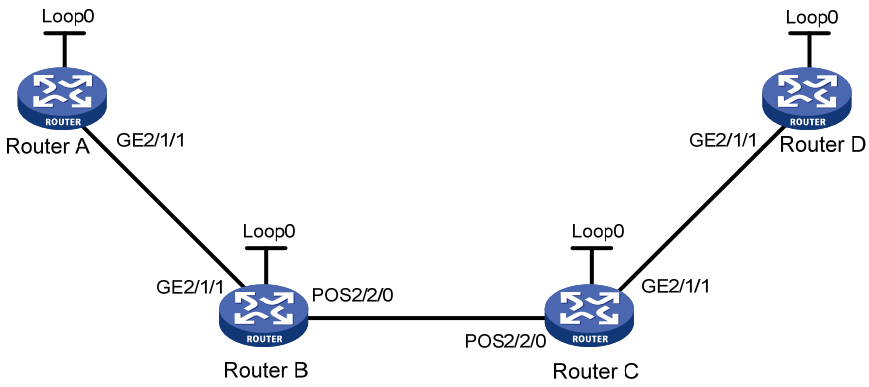
1.12.1 使用RSVP-TE配置MPLS TE隧道示例

1. 组网需求

- 设备 Router A、Router B、Router C 和 Router D 运行 IS-IS，都是 Level-2 设备；
- 使用 RSVP-TE 建立一条从 Router A 到 Router D 的 MPLS TE 隧道，隧道需要的带宽为 2000kbps；
- 隧道沿途的链路最大带宽为 10000kbps，最大可预留带宽为 5000kbps。

2. 组网图

图1-2 使用 RSVP-TE 配置 MPLS TE 隧道组网图



设备	接口	IP地址	设备	接口	IP地址
Router A	Loop0	1.1.1.9/32	Router C	Loop0	3.3.3.9/32
	GE2/1/1	10.1.1.1/24		GE2/1/1	30.1.1.1/24
Router B	Loop0	2.2.2.9/32		POS2/2/0	20.1.1.2/24
	GE2/1/1	10.1.1.2/24	Router D	Loop0	4.4.4.9/32
	POS2/2/0	20.1.1.1/24		GE2/1/1	30.1.1.2/24

3. 配置步骤

(1) 配置各接口的 IP 地址

按照 图 1-2 配置各接口的IP地址和掩码，具体配置过程略。

(2)　配置 IS-IS 协议发布接口所在网段的路由，包括 Loopback 接口

配置 Router A。

```
<RouterA> system-view
[RouterA] isis 1
[RouterA-isis-1] network-entity 00.0005.0000.0000.0001.00
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] isis enable 1
[RouterA-GigabitEthernet2/1/1] isis circuit-level level-2
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface loopback 0
[RouterA-LoopBack0] isis enable 1
[RouterA-LoopBack0] isis circuit-level level-2
[RouterA-LoopBack0] quit
```

配置 Router B。

```
<RouterB> system-view
[RouterB] isis 1
[RouterB-isis-1] network-entity 00.0005.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] isis enable 1
[RouterB-GigabitEthernet2/1/1] isis circuit-level level-2
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface pos 2/2/0
[RouterB-POS2/2/0] isis enable 1
[RouterB-POS2/2/0] isis circuit-level level-2
[RouterB-POS2/2/0] quit
[RouterB] interface loopback 0
[RouterB-LoopBack0] isis enable 1
[RouterB-LoopBack0] isis circuit-level level-2
[RouterB-LoopBack0] quit
```

配置 Router C。

```
<RouterC> system-view
[RouterC] isis 1
[RouterC-isis-1] network-entity 00.0005.0000.0000.0003.00
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] isis enable 1
[RouterC-GigabitEthernet2/1/1] isis circuit-level level-2
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface pos 2/2/0
[RouterC-POS2/2/0] isis enable 1
[RouterC-POS2/2/0] isis circuit-level level-2
[RouterC-POS2/2/0] quit
[RouterC] interface loopback 0
[RouterC-LoopBack0] isis enable 1
```

```
[RouterC-LoopBack0] isis circuit-level level-2
[RouterC-LoopBack0] quit
```

配置 Router D。

```
<RouterD> system-view
[RouterD] isis 1
[RouterD-isis-1] network-entity 00.0005.0000.0000.0004.00
[RouterD-isis-1] quit
[RouterD] interface gigabitethernet 2/1/1
[RouterD-GigabitEthernet2/1/1] isis enable 1
[RouterD-GigabitEthernet2/1/1] isis circuit-level level-2
[RouterD-GigabitEthernet2/1/1] quit
[RouterD] interface loopback 0
[RouterD-LoopBack0] isis enable 1
[RouterD-LoopBack0] isis circuit-level level-2
[RouterD-LoopBack0] quit
```

配置完成后，在各设备上执行 **display ip routing-table** 命令，可以看到相互之间都学到了到对方的路由，包括 Loopback 接口对应的主机路由。

(3) 配置 LSR ID，开启 MPLS、MPLS TE 和 RSVP 能力

配置 Router A。

```
[RouterA] mpls lsr-id 1.1.1.9
[RouterA] mpls te
[RouterA-te] quit
[RouterA] rsvp
[RouterA-rsvp] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mpls enable
[RouterA-GigabitEthernet2/1/1] mpls te enable
[RouterA-GigabitEthernet2/1/1] rsvp enable
[RouterA-GigabitEthernet2/1/1] quit
```

配置 Router B。

```
[RouterB] mpls lsr-id 2.2.2.9
[RouterB] mpls te
[RouterB-te] quit
[RouterB] rsvp
[RouterB-rsvp] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mpls enable
[RouterB-GigabitEthernet2/1/1] mpls te enable
[RouterB-GigabitEthernet2/1/1] rsvp enable
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface pos 2/2/0
[RouterB-POS2/2/0] mpls enable
[RouterB-POS2/2/0] mpls te enable
[RouterB-POS2/2/0] rsvp enable
[RouterB-POS2/2/0] quit
```

配置 Router C。

```
[RouterC] mpls lsr-id 3.3.3.9
```

```
[RouterC] mpls te
[RouterC-te] quit
[RouterC] rsvp
[RouterC-rsvp] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] mpls enable
[RouterC-GigabitEthernet2/1/1] mpls te enable
[RouterC-GigabitEthernet2/1/1] rsvp enable
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface pos 2/2/0
[RouterC-POS2/2/0] mpls enable
[RouterC-POS2/2/0] mpls te enable
[RouterC-POS2/2/0] rsvp enable
[RouterC-POS2/2/0] quit
```

配置 Router D。

```
[RouterD] mpls lsr-id 4.4.4.9
[RouterD] mpls te
[RouterD-te] quit
[RouterD] rsvp
[RouterD-rsvp] quit
[RouterD] interface gigabitethernet 2/1/1
[RouterD-GigabitEthernet2/1/1] mpls enable
[RouterD-GigabitEthernet2/1/1] mpls te enable
[RouterD-GigabitEthernet2/1/1] rsvp eanble
[RouterD-GigabitEthernet2/1/1] quit
```

(4) 配置 IS-IS TE

配置 Router A。

```
[RouterA] isis 1
[RouterA-isis-1] cost-style wide
[RouterA-isis-1] mpls te enable level-2
[RouterA-isis-1] quit
```

配置 Router B。

```
[RouterB] isis 1
[RouterB-isis-1] cost-style wide
[RouterB-isis-1] mpls te enable level-2
[RouterB-isis-1] quit
```

配置 Router C。

```
[RouterC] isis 1
[RouterC-isis-1] cost-style wide
[RouterC-isis-1] mpls te enable level-2
[RouterC-isis-1] quit
```

配置 Router D。

```
[RouterD] isis 1
[RouterD-isis-1] cost-style wide
[RouterD-isis-1] mpls te enable level-2
[RouterD-isis-1] quit
```

(5) 配置链路的 MPLS TE 属性

在 Router A 上配置链路的最大带宽和最大可预留带宽。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterA-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth 5000
[RouterA-GigabitEthernet2/1/1] quit
```

在 Router B 上配置链路的最大带宽和最大可预留带宽。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterB-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth 5000
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface pos 2/2/0
[RouterB-POS2/2/0] mpls te max-link-bandwidth 10000
[RouterB-POS2/2/0] mpls te max-reservable-bandwidth 5000
[RouterB-POS2/2/0] quit
```

在 Router C 上配置链路的最大带宽和最大可预留带宽。

```
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterC-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth 5000
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface pos 2/2/0
[RouterC-POS2/2/0] mpls te max-link-bandwidth 10000
[RouterC-POS2/2/0] mpls te max-reservable-bandwidth 5000
[RouterC-POS2/2/0] quit
```

在 Router D 上配置链路的最大带宽和最大可预留带宽。

```
[RouterD] interface gigabitethernet 2/1/1
[RouterD-GigabitEthernet2/1/1] mpls te max-link-bandwidth 10000
[RouterD-GigabitEthernet2/1/1] mpls te max-reservable-bandwidth 5000
[RouterD-GigabitEthernet2/1/1] quit
```

(6) 配置 MPLS TE 隧道

在 Router A 上配置 MPLS TE 隧道 Tunnel1：目的地址为 Router D 的 LSR ID（4.4.4.9）；采用 RSVP-TE 信令协议建立 MPLS TE 隧道；隧道所需的带宽为 2000kbps。

```
[RouterA] interface tunnel 1 mode mpls-te
[RouterA-Tunnel1] ip address 7.1.1.1 255.255.255.0
[RouterA-Tunnel1] destination 4.4.4.9
[RouterA-Tunnel1] mpls te signaling rsvp-te
[RouterA-Tunnel1] mpls te bandwidth 2000
[RouterA-Tunnel1] quit
```

(7) 配置静态路由使流量沿 MPLS TE 隧道转发

在 Router A 上配置静态路由，使得到达网络 30.1.1.0/24 的流量通过 MPLS TE 隧道接口 Tunnel1 转发。

```
[RouterA] ip route-static 30.1.1.2 24 tunnel 1 preference 1
```

4. 验证配置

配置完成后，在 Router A 上执行 **display interface tunnel** 命令可以看到隧道接口状态为 up。

```
[RouterA] display interface tunnel
Tunnel1
```

```
Current state: UP
Line protocol state: UP
Description: Tunnel1 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 64000
Internet Address is 7.1.1.1/24 Primary
Tunnel source unknown, destination 4.4.4.9
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

在 Router A 上执行 **display mpls te tunnel-interface** 命令可以看到隧道的详细信息。

```
[RouterA] display mpls te tunnel-interface
Tunnel Name            : Tunnel 1
Tunnel State            : Up (Main CRLSP up, Shared-resource CRLSP down)
Tunnel Attributes      :
  LSP ID               : 23331          Tunnel ID            : 1
  Admin State          : Normal
  Ingress LSR ID       : 1.1.1.9        Egress LSR ID        : 4.4.4.9
  Signaling            : RSVP-TE        Static CRLSP Name    : -
  Resv Style           : SE
  Tunnel mode          : -
  Reverse-LSP name     : -
  Reverse-LSP LSR ID   : -              Reverse-LSP Tunnel ID: -
  Class Type           : CT0            Tunnel Bandwidth     : 2000 kbps
  Reserved Bandwidth   : 2000 kbps
  Setup Priority       : 7              Holding Priority     : 7
  Affinity Attr/Mask   : 0/0
  Explicit Path        : -
  Backup Explicit Path : -
  Metric Type          : TE
  Record Route         : Disabled       Record Label         : Disabled
  FRR Flag             : Disabled       Backup Bandwidth Flag: Disabled
  Backup Bandwidth Type: -              Backup Bandwidth     : -
  Route Pinning        : Disabled
  Retry Limit          : 10             Retry Interval       : 2 sec
  Reoptimization       : Disabled       Reoptimization Freq  : -
  Backup Type          : None           Backup LSP ID        : -
  Auto Bandwidth       : Disabled       Auto Bandwidth Freq  : -
  Min Bandwidth        : -              Max Bandwidth        : -
  Collected Bandwidth  : -
```

在 Router A 上执行 **display ip routing-table** 命令，可以看到路由表中有以 Tunnel1 为出接口的静态路由信息。

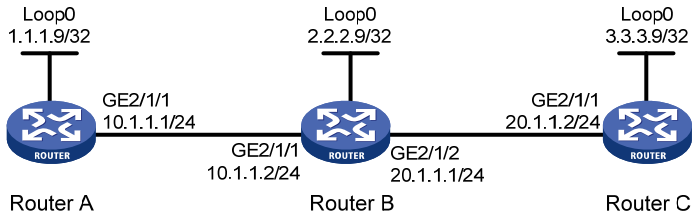
1.12.2 配置RSVP GR示例

1. 组网需求

- 设备 Router A、Router B 和 Router C 运行 IS-IS，都是 Level-2 设备；
- 使用 RSVP-TE 建立从 Router A 到 Router C 的 MPLS TE 隧道；
- 设备 Router A、Router B 和 Router C 支持 RSVP 的 Hello 扩展能力；
- Router A、Router B 和 Router C 为 RSVP 邻居，通过开启 GR 能力，邻居之间可以在对方发生 GR Restart 的时候提供 GR Helper 支持。

2. 组网图

图1-3 RSVP GR 配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址

按照 图 1-3 配置各接口的IP地址和掩码，具体配置过程略。

(2) 配置 IS-IS 协议发布接口所在网段的路由，包括 Loopback 接口（具体配置过程略）

(3) 配置 LSR ID，开启 MPLS、MPLS TE、RSVP 和 RSVP 的 Hello 扩展能力

配置 Router A

```
<RouterA> system-view
[RouterA] mpls lsr-id 1.1.1.9
[RouterA] mpls te
[RouterA-te] quit
[RouterA] rsvp
[RouterA-rsvp] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mpls enable
[RouterA-GigabitEthernet2/1/1] mpls te enable
[RouterA-GigabitEthernet2/1/1] rsvp enable
[RouterA-GigabitEthernet2/1/1] rsvp hello enable
[RouterA-GigabitEthernet2/1/1] quit
```

配置 Router B

```
<RouterB> system-view
[RouterB] mpls lsr-id 2.2.2.9
[RouterB] mpls te
```

```
[RouterBte] quit
[RouterB] rsvp
[RouterB] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mpls enable
[RouterB-GigabitEthernet2/1/1] mpls te enable
[RouterB-GigabitEthernet2/1/1] rsvp enable
[RouterB-GigabitEthernet2/1/1] rsvp hello enable
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] mpls enable
[RouterB-GigabitEthernet2/1/2] mpls te enable
[RouterB-GigabitEthernet2/1/2] rsvp enable
[RouterB-GigabitEthernet2/1/2] rsvp hello enable
[RouterB-GigabitEthernet2/1/2] quit
```

配置 Router C

```
<RouterC> system-view
[RouterC] mpls lsr-id 3.3.3.9
[RouterC] mpls te
[RouterC-te] quit
[RouterC] rsvp
[RouterC-rsvp] rsvp
[RouterC-mpls] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] mpls enable
[RouterC-GigabitEthernet2/1/1] mpls te enable
[RouterC-GigabitEthernet2/1/1] rsvp enable
[RouterC-GigabitEthernet2/1/1] rsvp hello enable
[RouterC-GigabitEthernet2/1/1] quit
```

(4) 配置 IS-IS TE（具体配置过程略）

(5) 配置 MPLS TE 隧道（具体配置过程略）

(6) 配置 RSVP GR

配置 Router A

```
[RouterA] rsvp
[RouterA-rsvp] graceful-restart enable
```

配置 Router B

```
[RouterB] rsvp
[RouterB-rsvp] graceful-restart enable
```

配置 Router C

```
[RouterC] rsvp
[RouterC-rsvp] graceful-restart enable
```

4. 验证配置

在 Router A 和 Router C 之间创建隧道且运行稳定后，通过命令可以看到邻居的 GR 状态已经为 Ready 状态。

```
<RouterA> display rsvp peer verbose
Peer: 10.1.1.2                          Interface: GE2/1/1
Hello state: Up                         Hello type: Active
```

```
PSB count: 0                              RSB count: 1
Src instance: 0x1f08                      Dst instance: 0x22
Refresh reduction: Disabled               Graceful Restart state: Ready
Peer GR restart time: 120000 ms           Peer GR recovery time: 0 ms
```

目 录

1 隧道策略 ····· 1-1
1.1 隧道策略简介 ····· 1-1
1.2 配置隧道策略 ····· 1-1
1.3 隧道策略显示和维护 ····· 1-3
1.4 隧道策略配置举例 ····· 1-3
1.4.1 配置首选隧道 ····· 1-3
1.4.2 配置独占隧道 ····· 1-4
1.4.3 配置按顺序选择隧道 ····· 1-4
1.4.4 配置首选隧道和按顺序选择隧道 ····· 1-5

1 隧道策略

1.1 隧道策略简介

MPLS LSP、MPLS TE（Traffic Engineering，流量工程）隧道、GRE（Generic Routing Encapsulation，通用路由封装）隧道等多种类型的隧道都可以作为 MPLS VPN（Virtual Private Network，虚拟专用网络）的承载隧道。当 MPLS VPN 的两个 PE（Provider Edge，服务提供商网络边缘）设备之间存在多种隧道、每种隧道都有多条时，如何选择隧道，是网络部署必须考虑的重要问题。合理的选择隧道，不仅有利于服务提供商网络的管理和规划，还可以降低 PE 设备的处理开销。

隧道策略提供了灵活的隧道选择方法，可以满足 MPLS VPN 对隧道的多种选择要求，例如指定首选隧道、流量在隧道间负载分担等。

为了提高承载隧道的可靠性，还可以将多条 MPLS TE 隧道关联，形成一条捆绑隧道，指定该捆绑隧道为首选隧道。

MPLS TE 的详细介绍请参见“MPLS 配置指导”中的“MPLS TE”。GRE 的详细介绍请参见“三层技术-IP 业务配置指导”中的“GRE”。MPLS VPN 的详细介绍请参见“MPLS 配置指导”中的“MPLS L3VPN”、“MPLS L2VPN”。捆绑隧道的详细介绍请参见“MPLS 配置指导”中的“MPLS TE”。

1.2 配置隧道策略

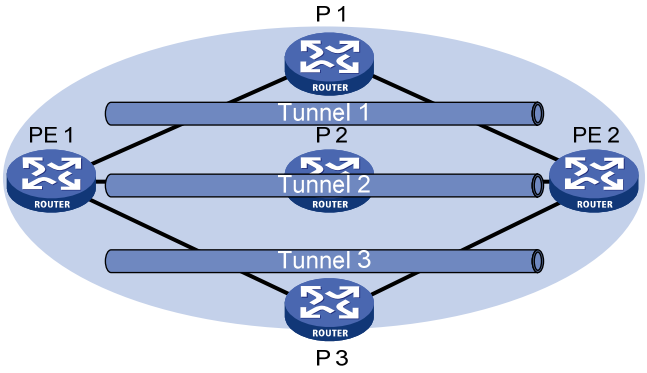
隧道策略分为以下两种：

- 只使用一条隧道/捆绑隧道转发流量：通过 **preferred-path** 命令配置首选隧道，每条首选隧道对应一个隧道接口或隧道捆绑接口。如果对端 PE 地址与隧道接口/隧道捆绑接口的目的地址相同，则通过该隧道/捆绑隧道转发到达该 PE 的流量。如果存在多条目的地址相同的首选隧道，则选择配置的第一条首选隧道；如果第一条首选隧道不可用，则选择下一条首选隧道；以此类推。也就是说到达同一个目的地址只能存在一条首选隧道，不会在多条隧道间进行负载分担。该方式为 MPLS VPN 显式指定了一条 MPLS TE 隧道、GRE 隧道或捆绑隧道，选择的隧道是明确的、可以预期的，便于网络流量规划。推荐使用该方式配置隧道策略。
- 选择多条隧道，流量在隧道之间进行负载分担：通过 **select-seq load-balance-number** 命令配置隧道的选择顺序和负载分担的隧道数目。该命令配置的隧道类型越靠前，其优先级越高。例如：配置了 **select-seq lsp gre load-balance-number 3** 命令，则优先选择 LSP；在没有 LSP 或 LSP 不足 3 条的情况下，选用 GRE 隧道。采用该方式时，选择的隧道具有随机性，不便于网络流量规划。不推荐使用该方式配置隧道策略。

如果隧道策略中同时配置了上述两种方式，则优先选择 **preferred-path** 命令指定的首选隧道，即：

- 如果对端 PE 地址与某条首选隧道的目的地址相同，则采用该隧道/捆绑隧道转发流量，不会再根据 **select-seq load-balance-number** 命令指定的隧道选择顺序和负载分担数目选择隧道。
- 如果不存在隧道目的地址与对端 PE 地址相同的首选隧道，则根据 **select-seq load-balance-number** 命令指定的隧道选择顺序和负载分担数目选择隧道。

图1-1 MPLS VPN 隧道选择示例图



如 图 1-1 所示，当PE 1 和PE 2 之间存在多条隧道，且PE 1 和PE 2 连接多个MPLS VPN时，可以采用如下方式部署MPLS VPN的流量：

- 配置多个隧道策略，每个隧道策略中分别通过 **preferred-path** 命令指定一条首选隧道，不同的 MPLS VPN 引用不同的隧道策略，从而实现不同 VPN 的流量通过不同的隧道转发。
- 在隧道策略中通过 **select-seq load-balance-number** 命令指定隧道的选择顺序和负载分担的隧道数目，配置 MPLS VPN 引用该隧道策略，从而实现每个 VPN 的流量都在多条隧道之间进行负载分担。

采用第二种方式时，单个 VPN 的流量分担到多条隧道上，不同隧道的延时差别可能很大，设备或上层应用对报文进行排序处理可能会导致比较大的延迟。因此，不推荐使用第二种方式。

表1-1 配置隧道策略

操作	命令	说明
进入系统视图	**system-view**	-
创建隧道策略，并进入隧道策略视图	**tunnel-policy** *tunnel-policy-name*	缺省情况下，设备上不存在任何隧道策略
配置到固定目的地址的首选隧道	**preferred-path** { **tunnel** *number* | **tunnel-bundle** *number* }	缺省情况下，未指定到固定目的地址的首选隧道
配置隧道的选择顺序和负载分担的隧道数目	**select-seq** { **cr-lsp** | **gre** | **lsp** } * **load-balance-number** *number*	缺省情况下，选择的隧道类型优先级依次是LSP、GRE、CR-LSP，负载分担的隧道数目为1

说明

独用隧道是指隧道只能被一个 VPN 使用，即隧道只能转发一个 VPN 的流量。通过在隧道策略中使用 **preferred-path** 命令配置首选隧道，并保证该隧道策略只能被一个 VPN 实例引用，可以实现独用隧道。

1.3 隧道策略显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后隧道策略的运行情况，用户可以通过查看显示信息验证配置的效果。

表1-2 隧道策略显示和维护

操作	命令
显示隧道信息	**display mpls tunnel** { **all** | **statistics** | [**vpn-instance** *vpn-instance-name*] **destination** { *tunnel-ipv4-dest* | *tunnel-ipv6-dest* } }

1.4 隧道策略配置举例

1.4.1 配置首选隧道

1. 组网需求

PE 1 上存在到达 PE 2 的多条隧道：

- 1 条 MPLS TE 隧道，对应的隧道接口为 Tunnel1。
- 1 条 GRE 隧道，对应的隧道接口为 Tunnel2。
- 1 条 LDP LSP 隧道。

在 PE 1 上存在两个 MPLS VPN 实例 vpna 和 vpnb，这两个 VPN 实例都要求使用 MPLS TE 隧道转发流量。

2. 配置步骤

(1) 在 PE 1 上配置隧道策略

创建隧道策略 preferredte1，并指定首选隧道为 Tunnel 1。

```
<PE1> system-view
[PE1] tunnel-policy preferredte1
[PE1-tunnel-policy-preferredte1] preferred-path tunnel 1
[PE1-tunnel-policy-preferredte1] quit
```

(2) 配置 MPLS VPN 实例，并在实例下引用隧道策略

创建 MPLS VPN 实例 vpna，并配置 vpna 实例引用隧道策略 preferredte1。

```
[PE1] ip vpn-instance vpna
[PE1-vpn-instance-vpna] route-distinguisher 100:1
[PE1-vpn-instance-vpna] vpn-target 100:1
[PE1-vpn-instance-vpna] tnl-policy preferredte1
[PE1-vpn-instance-vpna] quit
```

创建 MPLS VPN 实例 vpnb，并配置 vpnb 实例引用隧道策略 preferredte1。

```
[PE1] ip vpn-instance vpnb
[PE1-vpn-instance-vpnb] route-distinguisher 100:2
[PE1-vpn-instance-vpnb] vpn-target 100:2
[PE1-vpn-instance-vpnb] tnl-policy preferredte1
```

1.4.2 配置独占隧道

1. 组网需求

PE 1 上存在到达 PE 2 的多条隧道：

- 1 条 MPLS TE 隧道，对应的隧道接口为 Tunnel1。
- 1 条 GRE 隧道，对应的隧道接口为 Tunnel2。
- 1 条 LDP LSP 隧道。

在 PE 1 上存在两个 MPLS VPN 实例 vpna 和 vpnb，vpna 独占 MPLS TE 隧道（即 MPLS TE 隧道只转发 vpna 的流量），vpnb 独占 GRE 隧道（即 GRE 隧道只转发 vpnb 的流量）。

2. 配置步骤

(1) 在 PE 1 上配置隧道策略

创建隧道策略 preferredte1，并指定首选隧道为 Tunnel 1。

```
<PE1> system-view
[PE1] tunnel-policy preferredte1
[PE1-tunnel-policy-preferredte1] preferred-path tunnel 1
[PE1-tunnel-policy-preferredte1] quit
```

创建隧道策略 preferredgre2，并指定首选隧道为 Tunnel 2。

```
[PE1] tunnel-policy preferredgre2
[PE1-tunnel-policy-preferredgre2] preferred-path tunnel 2
[PE1-tunnel-policy-preferredgre2] quit
```

(2) 配置 MPLS VPN 实例，并在实例下引用隧道策略

创建 MPLS VPN 实例 vpna，并配置 vpna 实例引用隧道策略 preferredte1。

```
[PE1] ip vpn-instance vpna
[PE1-vpn-instance-vpna] route-distinguisher 100:1
[PE1-vpn-instance-vpna] vpn-target 100:1
[PE1-vpn-instance-vpna] tnl-policy preferredte1
[PE1-vpn-instance-vpna] quit
```

创建 MPLS VPN 实例 vpnb，并配置 vpnb 实例引用隧道策略 preferredgre2。

```
[PE1] ip vpn-instance vpnb
[PE1-vpn-instance-vpnb] route-distinguisher 100:2
[PE1-vpn-instance-vpnb] vpn-target 100:2
[PE1-vpn-instance-vpnb] tnl-policy preferredgre2
```

1.4.3 配置按顺序选择隧道

1. 组网需求

PE 1 上存在到达 PE 2 的多条隧道：

- 1 条 MPLS TE 隧道，对应的隧道接口为 Tunnel1。
- 1 条 GRE 隧道，对应的隧道接口为 Tunnel2。
- 1 条 LDP LSP 隧道。

在 PE 1 上存在一个 MPLS VPN 实例 vpna，要求 vpna 按 LDP LSP、MPLS TE、GRE 的顺序选择隧道（即只要 LDP LSP 可用，就优先选择 LDP LSP；如果 LDP LSP 不可用，则选择 MPLS TE 隧道；如果 MPLS TE 隧道也不可用，才选择 GRE 隧道），并且同时只能使用一条隧道转发流量。

2. 配置步骤

(1) 在 PE 1 上配置隧道策略

创建隧道策略 seq-lsp-te-gre，并指定隧道选择顺序为 LSP、MPLS TE 隧道、GRE 隧道，负载分担数目为 1。

```
<PE1> system-view
[PE1] tunnel-policy seq-lsp-te-gre
[PE1-tunnel-policy-seq-lsp-te-gre] select-seq lsp cr-lsp gre load-balance-number 1
[PE1-tunnel-policy-seq-lsp-te-gre] quit
```

(2) 配置 MPLS VPN 实例，并在实例下引用隧道策略

创建 MPLS VPN 实例 vpna，并配置 vpna 实例引用隧道策略 seq-lsp-te-gre。

```
[PE1] ip vpn-instance vpna
[PE1-vpn-instance-vpna] route-distinguisher 100:1
[PE1-vpn-instance-vpna] vpn-target 100:1
[PE1-vpn-instance-vpna] tnl-policy seq-lsp-te-gre
```

1.4.4 配置首选隧道和按顺序选择隧道

1. 组网需求

PE 1 上存在到达 PE 2 的多条隧道：

- 2 条 MPLS TE 隧道，对应的隧道接口为 Tunnel1 和 Tunnel3。
- 1 条 GRE 隧道，对应的隧道接口为 Tunnel2。
- 1 条 LDP LSP 隧道。

在PE 1 上存在多个MPLS VPN实例：vpna、vpnb、vpnc、vpnd、vpne、vpnf和vpng。每个VPN实例使用的隧道策略如 表 1-3 所示。

表1-3 VPN 实例使用的隧道策略列表

VPN 实例	隧道策略
vpna、vpnb	首选MPLS TE隧道Tunnel 1
vpnc、vpnd	首选MPLS TE隧道Tunnel 3
vpne、vpnf	首选GRE隧道Tunnel 2
vpng	按照LDP LSP、GRE隧道、MPLS TE隧道的顺序选择隧道，负载分担数目为1

2. 配置步骤

(1) 在 PE 1 上配置隧道策略

创建隧道策略 preferredte1，并指定首选隧道为 Tunnel 1。

```
<PE1> system-view
[PE1] tunnel-policy preferredte1
[PE1-tunnel-policy-preferredte1] preferred-path tunnel 1
[PE1-tunnel-policy-preferredte1] quit
```

创建隧道策略 preferredte3，并指定首选隧道为 Tunnel 3。

```
[PE1] tunnel-policy preferredte3
[PE1-tunnel-policy-preferredte3] preferred-path tunnel 3
```

```
[PE1-tunnel-policy-preferredte3] quit
```

创建隧道策略 preferredgre2，并指定首选隧道为 Tunnel 2。

```
[PE1] tunnel-policy preferredgre2
[PE1-tunnel-policy-preferredgre2] preferred-path tunnel 2
[PE1-tunnel-policy-preferredgre2] quit
```

创建隧道策略 select-lsp，按照 LDP LSP、GRE 隧道、MPLS TE 隧道的顺序选择隧道，负载分担数目为 1。

```
[PE1] tunnel-policy select-lsp
[PE1-tunnel-policy-select-lsp] select-seq lsp gre cr-lsp load-balance-number 1
[PE1-tunnel-policy-select-lsp] quit
```

(2) 配置 MPLS VPN 实例，并在实例下引用隧道策略

创建 MPLS VPN 实例 vpna 和 vpnb，并配置 vpna 和 vpnb 引用隧道策略 preferredte1。

```
[PE1] ip vpn-instance vpna
[PE1-vpn-instance-vpna] route-distinguisher 100:1
[PE1-vpn-instance-vpna] vpn-target 100:1
[PE1-vpn-instance-vpna] tnl-policy preferredte1
[PE1-vpn-instance-vpna] quit
[PE1] ip vpn-instance vpnb
[PE1-vpn-instance-vpnb] route-distinguisher 100:2
[PE1-vpn-instance-vpnb] vpn-target 100:2
[PE1-vpn-instance-vpnb] tnl-policy preferredte1
[PE1-vpn-instance-vpnb] quit
```

创建 MPLS VPN 实例 vpnc 和 vpnd，并配置 vpnc 和 vpnd 引用隧道策略 preferredte3。

```
[PE1] ip vpn-instance vpnc
[PE1-vpn-instance-vpnc] route-distinguisher 100:3
[PE1-vpn-instance-vpnc] vpn-target 100:3
[PE1-vpn-instance-vpnc] tnl-policy preferredte3
[PE1-vpn-instance-vpnc] quit
[PE1] ip vpn-instance vpnd
[PE1-vpn-instance-vpnd] route-distinguisher 100:4
[PE1-vpn-instance-vpnd] vpn-target 100:4
[PE1-vpn-instance-vpnd] tnl-policy preferredte3
[PE1-vpn-instance-vpnd] quit
```

创建 MPLS VPN 实例 vpne 和 vpnf，并配置 vpne 和 vpnf 引用隧道策略 preferredgre2。

```
[PE1] ip vpn-instance vpne
[PE1-vpn-instance-vpne] route-distinguisher 100:5
[PE1-vpn-instance-vpne] vpn-target 100:5
[PE1-vpn-instance-vpne] tnl-policy preferredgre2
[PE1-vpn-instance-vpne] quit
[PE1] ip vpn-instance vpnf
[PE1-vpn-instance-vpnf] route-distinguisher 100:6
[PE1-vpn-instance-vpnf] vpn-target 100:6
[PE1-vpn-instance-vpnf] tnl-policy preferredgre2
[PE1-vpn-instance-vpnf] quit
```

创建 MPLS VPN 实例 vpng，并配置 vpng 引用隧道策略 select-lsp。

```
[PE1] ip vpn-instance vpng
```

```
[PE1-vpn-instance-vpng] route-distinguisher 100:7
[PE1-vpn-instance-vpng] vpn-target 100:7
[PE1-vpn-instance-vpng] tnl-policy select-lsp
```

目 录

1 MPLS L3VPN ····· 1-1
1.1 MPLS L3VPN简介 ····· 1-1
1.1.1 MPLS L3VPN基本网络架构 ····· 1-1
1.1.2 MPLS L3VPN基本概念 ····· 1-1
1.1.3 MPLS L3VPN路由信息发布 ····· 1-3
1.1.4 MPLS L3VPN报文转发 ····· 1-4
1.1.5 MPLS L3VPN常见组网方案 ····· 1-5
1.1.6 跨域VPN ····· 1-7
1.1.7 运营商的运营商 ····· 1-11
1.1.8 嵌套VPN ····· 1-13
1.1.9 HoVPN ····· 1-15
1.1.10 OSPF VPN扩展 ····· 1-16
1.1.11 BGP的AS号替换和SoO属性 ····· 1-19
1.1.12 MPLS L3VPN快速重路由 ····· 1-19
1.1.13 Multi-VPN-Instance CE ····· 1-21
1.1.14 协议规范 ····· 1-22
1.2 MPLS L3VPN配置任务简介 ····· 1-23
1.3 配置基本MPLS L3VPN ····· 1-23
1.3.1 基本MPLS L3VPN配置任务简介 ····· 1-23
1.3.2 配置准备 ····· 1-24
1.3.3 配置VPN实例 ····· 1-24
1.3.4 配置PE-CE间路由交换 ····· 1-26
1.3.5 配置PE-PE间的路由交换 ····· 1-31
1.3.6 配置BGP VPNv4 路由 ····· 1-31
1.4 配置跨域VPN ····· 1-33
1.4.1 配置跨域VPN-OptionA ····· 1-33
1.4.2 配置跨域VPN-OptionB ····· 1-33
1.4.3 配置跨域VPN-OptionC ····· 1-34
1.5 配置嵌套VPN ····· 1-37
1.6 配置HoVPN ····· 1-38
1.7 配置OSPF伪连接 ····· 1-39
1.7.1 配置准备 ····· 1-39
1.7.2 配置Loopback接口 ····· 1-39

1.7.3 发布Loopback接口的路由 1-40
1.7.4 创建伪连接 1-40
1.8 配置Multi-VPN-Instance CE 1-41
1.8.1 配置MCE与站点之间的路由交换 1-41
1.8.2 配置MCE与PE之间的路由交换 1-46
1.9 配置Egress PE上私网路由标签操作方式 1-49
1.10 配置BGP的AS号替换和SoO属性 1-50
1.11 开启告警功能 1-50
1.12 配置MPLS L3VPN快速重路由 1-51
1.13 MPLS L3VPN显示和维护 1-53
1.13.1 复位BGP会话 1-53
1.13.2 显示MPLS L3VPN的运行状态 1-53
1.14 MPLS L3VPN典型配置举例 1-54
1.14.1 配置MPLS L3VPN示例 1-54
1.14.2 配置MPLS L3VPN采用GRE隧道示例 1-61
1.14.3 配置Hub&Spoke组网示例 1-66
1.14.4 配置跨域VPN-OptionA方式示例 1-72
1.14.5 配置跨域VPN-OptionB方式示例 1-77
1.14.6 配置跨域VPN-OptionC方式示例 1-82
1.14.7 配置运营商的运营商示例 1-89
1.14.8 配置嵌套VPN示例 1-96
1.14.9 配置HoVPN示例 1-105
1.14.10 配置OSPF伪连接 1-113
1.14.11 配置MCE示例 1-117
1.14.12 配置BGP的AS号替换 1-122
1.14.13 配置BGP的AS号替换和SoO属性 1-125
1.14.14 配置MPLS L3VPN快速重路由示例一 1-128
1.14.15 配置MPLS L3VPN快速重路由示例二 1-130
1.14.16 配置MPLS L3VPN快速重路由示例三 1-132
2 IPv6 MPLS L3VPN 2-1
2.1 IPv6 MPLS L3VPN简介 2-1
2.1.1 IPv6 MPLS L3VPN概述 2-1
2.1.2 IPv6 MPLS L3VPN的报文转发 2-2
2.1.3 IPv6 MPLS L3VPN的路由发布 2-2
2.1.4 IPv6 MPLS L3VPN支持的组网方案及功能 2-3
2.1.5 协议规范 2-3

2.2 IPv6 MPLS L3VPN配置任务简介 ····· 2-3
2.3 配置基本IPv6 MPLS L3VPN ····· 2-3
2.3.1 基本IPv6 MPLS L3VPN配置任务简介 ····· 2-3
2.3.2 配置准备 ····· 2-4
2.3.3 配置VPN实例 ····· 2-4
2.3.4 配置PE-CE间的路由交换 ····· 2-6
2.3.5 配置PE-PE间的路由交换 ····· 2-11
2.3.6 配置BGP VPNv6 路由 ····· 2-11
2.4 配置IPv6 跨域VPN ····· 2-13
2.4.1 配置准备 ····· 2-13
2.4.2 配置IPv6 跨域VPN-OptionA ····· 2-13
2.4.3 配置IPv6 跨域VPN-OptionC ····· 2-13
2.5 配置Multi-VPN-Instance CE ····· 2-14
2.5.1 配置准备 ····· 2-14
2.5.2 配置MCE与站点之间的路由交换 ····· 2-15
2.5.3 配置MCE与PE之间的路由交换 ····· 2-19
2.6 配置BGP的AS号替换和SoO属性 ····· 2-23
2.7 IPv6 MPLS L3VPN显示和维护 ····· 2-23
2.7.1 复位BGP会话 ····· 2-23
2.7.2 显示IPv6 MPLS L3VPN的运行状态 ····· 2-24
2.8 IPv6 MPLS L3VPN典型配置举例 ····· 2-25
2.8.1 配置IPv6 MPLS L3VPN示例 ····· 2-25
2.8.2 配置IPv6 MPLS L3VPN采用GRE隧道示例 ····· 2-33
2.8.3 配置IPv6 跨域VPN-OptionA方式示例 ····· 2-36
2.8.4 配置IPv6 跨域VPN-OptionC方式示例 ····· 2-41
2.8.5 配置运营商的运营商示例 ····· 2-48
2.8.6 配置IPv6 MCE示例 ····· 2-55
2.8.7 配置BGP的AS号替换 ····· 2-61
2.8.8 配置BGP的AS号替换和SoO属性 ····· 2-66

1 MPLS L3VPN

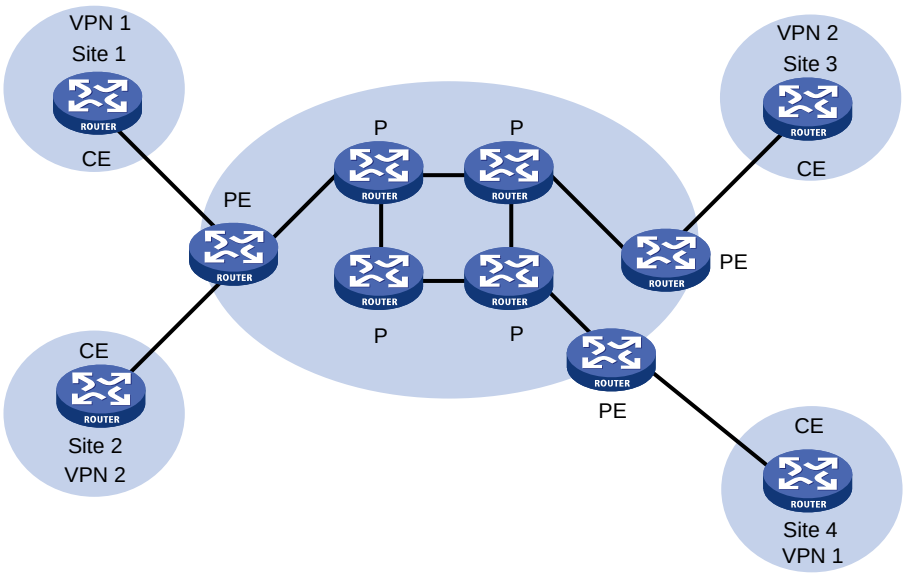
1.1 MPLS L3VPN简介

MPLS L3VPN 是一种三层 VPN 技术，它使用 BGP 在服务提供商骨干网上发布用户站点的私网路由，使用 MPLS 在服务提供商骨干网上转发用户站点之间的私网报文，从而实现通过服务提供商的骨干网连接属于同一个 VPN、位于不同地理位置的用户站点。

MPLS L3VPN 组网方式灵活，可扩展性好，并能够方便地支持 MPLS QoS 和 MPLS TE，因此得到了广泛的应用。

1.1.1 MPLS L3VPN基本网络架构

图1-1 MPLS L3VPN 基本网络架构



MPLS L3VPN的基本网络架构如 图 1-1 所示。MPLS L3VPN网络中设备的角色分为以下几种：

- CE（Customer Edge，用户网络边缘）设备：直接与服务提供商网络相连的用户网络侧设备。CE“感知”不到 VPN 的存在，也不需要支持 MPLS。
- PE（Provider Edge，服务提供商网络边缘）设备：与 CE 相连的服务提供商网络侧设备。在 MPLS L3VPN 网络中，对 VPN 的所有处理都发生在 PE 上。
- P（Provider，服务提供商网络）设备：服务提供商网络中的骨干设备，不与 CE 直接相连。P 只需要在骨干网中将用户网络报文转发给正确的远端 PE，不需要维护和处理 VPN 信息。

1.1.2 MPLS L3VPN基本概念

1. Site

Site（站点）的含义可以从下述几个方面理解：

- Site 是指相互之间具备 IP 连通性的一组 IP 系统，并且这组 IP 系统的 IP 连通性不需通过服务提供商网络实现；
- Site 的划分是根据设备的拓扑关系，而不是地理位置，尽管在大多数情况下一个 Site 中的设备地理位置相邻；
- 一个 Site 中的设备可以属于多个 VPN，换言之，一个 Site 可以属于多个 VPN；
- Site 通过 CE 连接到服务提供商网络，一个 Site 可以包含多个 CE，但一个 CE 只属于一个 Site。

对于多个连接到同一服务提供商网络的 Site，通过制定策略，可以将它们划分为不同的集合（set），只有属于相同集合的 Sites 之间才能通过服务提供商网络互访，这种集合就是 VPN。

2. VPN实例

在 MPLS L3VPN 中，不同 VPN 之间的路由隔离通过 VPN 实例（VPN-instance）实现，VPN 实例又称为 VRF（Virtual Routing and Forwarding，虚拟路由和转发）实例。PE 上每个 VPN 实例都有相对独立的路由表和 LFIB（Label Forwarding Information Base，标签转发信息库），确保 VPN 数据的独立性和安全性。

PE 通过将与 Site 连接的接口与 VPN 实例关联，实现该 Site 与 VPN 实例的关联。一个 Site 只能与一个 VPN 实例关联；不同的 Site 可以关联同一个 VPN 实例。VPN 实例中包含了与其关联的 Site 所属的所有 VPN 的成员关系和路由规则等信息。

VPN 实例中的信息包括：LFIB、IP 路由表、与 VPN 实例关联的接口以及 VPN 实例的管理信息。VPN 实例的管理信息包括 RD（Route Distinguisher，路由标识符）、VPN Target 属性、路由过滤策略等。

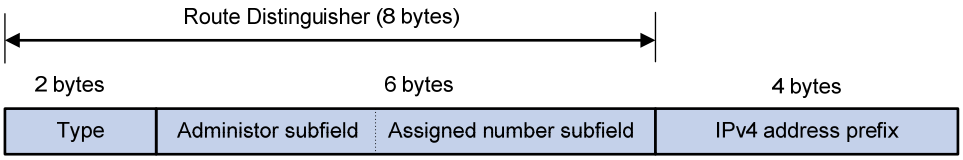
3. VPN-IPv4 地址

VPN 是一种私有网络，不同的 VPN 独立管理自己使用的地址范围，也称为地址空间（Address Space）。不同 VPN 的地址空间可能会在一定范围内重合，比如，VPN 1 和 VPN 2 都使用了 10.110.10.0/24 网段的地址，这就发生了地址空间重叠（Overlapping Address Spaces）。

传统 BGP 无法正确处理地址空间重叠的 VPN 的路由。假设 VPN 1 和 VPN 2 都使用了 10.110.10.0/24 网段的地址，并各自发布了一条去往此网段的路由，BGP 只会选择其中一条路由，从而导致去往另一个 VPN 的路由丢失。

MPLS L3VPN 使用 VPN-IPv4 地址（又称为 VPNv4 地址）来解决上述问题。

图1-2 VPN-IPv4 地址结构



如 图 1-2 所示，VPN-IPv4 地址共有 12 个字节，包括 8 字节的RD和 4 字节的IPv4 地址前缀。其中，RD的作用是将其添加到一个IPv4 地址前缀前，使之成为全局唯一的VPN-IPv4 地址前缀。PE从CE接收到普通IPv4 路由后，为IPv4 地址前缀添加RD，将其转变为VPN-IPv4 路由，并使用MP-BGP（Multiprotocol Border Gateway Protocol，多协议边界网关协议）将VPN-IPv4 路由发布给对端PE，从而实现通过RD区分不同VPN的相同IPv4 地址前缀。

RD 有三种格式，通过 2 字节的 Type 字段区分：

- Type 为 0 时，Administrator 子字段占 2 字节，Assigned number 子字段占 4 字节，格式为：16 位自治系统号:32 位用户自定义数字，例如：100:1。
- Type 为 1 时，Administrator 子字段占 4 字节，Assigned number 子字段占 2 字节，格式为：32 位 IPv4 地址:16 位用户自定义数字，例如：172.1.1.1:1。
- Type 为 2 时，Administrator 子字段占 4 字节，Assigned number 子字段占 2 字节，格式为：32 位自治系统号:16 位用户自定义数字，其中的自治系统号最小值为 65536，例如：65536:1。

为了保证 VPN-IPv4 地址全球唯一，建议不要将 Administrator 子字段的值设置为私有 AS 号或私有 IP 地址。

4. VPN Target属性

MPLS L3VPN 使用 BGP 扩展团体属性——VPN Target（也称为 Route Target）来控制 VPN 路由信息的发布。

VPN Target 属性分为如下两类：

- Export Target 属性：本地 PE 从与自己直接相连的 Site 学习到 IPv4 路由后，将其转换为 VPN-IPv4 路由，为 VPN-IPv4 路由设置 Export Target 属性并发布给其它 PE。
- Import Target 属性：PE 在接收到其它 PE 发布的 VPN-IPv4 路由时，检查其 Export Target 属性。只有当此属性与 PE 上某个 VPN 实例的 Import Target 属性匹配时，才把路由加入到该 VPN 实例的路由表中。

VPN Target 属性定义了一条 VPN-IPv4 路由可以为哪些 Site 所接收，PE 可以接收哪些 Site 发送来的路由。

与 RD 类似，VPN Target 也有三种格式：

- 16 位自治系统号:32 位用户自定义数字，例如：100:1。
- 32 位 IPv4 地址:16 位用户自定义数字，例如：172.1.1.1:1。
- 32 位自治系统号:16 位用户自定义数字，其中的自治系统号最小值为 65536，例如：65536:1。

5. MP-BGP

MP-BGP（Multiprotocol Border Gateway Protocol，多协议边界网关协议）是对 BGP 协议的扩展，它可以为多种网络层协议传递路由信息，如 IPv4 组播、IPv6 单播、IPv6 组播、VPN-IPv4 等。

在 MPLS L3VPN 中，PE 之间利用 MP-BGP 来传递 VPN-IPv4 路由，既实现了 VPN 的私网路由在不同站点之间的传递，又确保了私网路由只在 VPN 内发布。

1.1.3 MPLS L3VPN路由信息发布

在 MPLS L3VPN 组网中，VPN 路由信息的发布涉及 CE 和 PE。P 路由器只维护骨干网的路由，不需要了解任何 VPN 路由信息。PE 路由器只维护与它直接相连的 VPN 的路由信息，不维护所有 VPN 路由。

VPN 路由信息的发布过程包括三部分：本地 CE 到入口 PE、入口 PE 到出口 PE、出口 PE 到远端 CE。完成这三部分后，本地 CE 与远端 CE 之间将建立可达路由。

下面分别对这三部分进行介绍。

1. 本地CE到入口PE的路由信息交换

CE 使用静态路由、RIP、OSPF、IS-IS、EBGP 或 IBGP，将本站点的 VPN 路由发布给 PE。CE 发布给 PE 的是标准的 IPv4 路由。

2. 入口PE到出口PE的路由信息交换

PE 从 CE 学到 VPN 路由信息后，将其存放到相应的 VPN 实例的路由表中。PE 为这些标准 IPv4 路由增加 RD 和 Export Target 属性，并为这些路由分配 MPLS 标签，形成 VPN-IPv4 路由。

入口 PE 通过 MP-BGP 把 VPN-IPv4 路由(包括 Export Target 属性和 MPLS 标签)发布给出口 PE。出口 PE 将 VPN-IPv4 路由的 Export Target 属性与自己维护的 VPN 实例的 Import Target 属性进行匹配。如果出口 PE 上某个 VPN 实例的 Import Target 属性与路由的 Export Target 属性中存在相同的属性值，则将该路由加入到该 VPN 实例的路由表中。

3. 出口PE到远端CE的路由信息交换

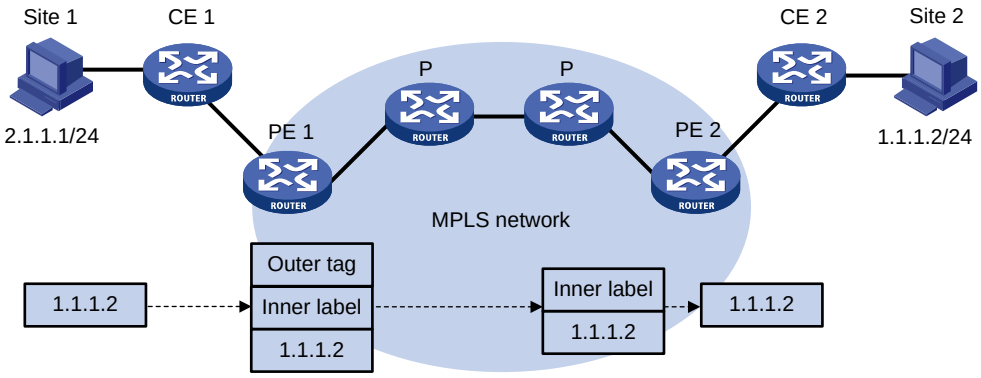
与本地 CE 到入口 PE 的路由信息交换相同，远端 CE 可以通过多种方式从出口 PE 学习 VPN 路由，包括静态路由、RIP、OSPF、IS-IS、EBGP 和 IBGP。

1.1.4 MPLS L3VPN报文转发

在基本 MPLS L3VPN 应用中（不包括跨域的情况），PE 转发 VPN 报文时为报文封装如下内容：

- 外层标记：又称为公网标记。VPN 报文在骨干网上沿着公网隧道从一端 PE 传送到另一端 PE。公网隧道可以是 LSP 隧道、MPLS TE 隧道和 GRE 隧道。当公网隧道为 LSP 隧道或 MPLS TE 隧道时，公网标记为 MPLS 标签，称为公网标签；当公网隧道为 GRE 隧道时，公网标记为 GRE 封装。
- 内层标签：又称为私网标签，用来指示报文应被送到哪个 Site。对端 PE 根据私网标签可以找到转发报文的接口，将报文正确地转发到相应的 Site。PE 之间在通过 MP-BGP 发布 VPN-IPv4 路由时，将为私网路由分配的私网标签通告给对端 PE。

图1-3 VPN 报文转发示意图



如 图 1-3 所示，VPN报文的转发过程为：

(1) Site 1 发出一个目的地址为 1.1.1.2 的 IP 报文，由 CE 1 将报文发送至 PE 1。

(2) PE 1 根据报文到达的接口及目的地址查找对应 VPN 实例的路由表，根据匹配的路由表项为报文添加私网标签，并查找到报文的下一跳为 PE 2。

(3) PE 1 在公网路由表内查找到达 PE 2 的路由，根据查找结果为报文封装公网标签或进行 GRE 封装，并沿着公网隧道转发该报文。

(4) MPLS 网络内，P 根据报文的公网标记转发报文，将报文转发到 PE 2。如果公网标记为 MPLS 标签，则报文在到达 PE 2 的前一跳时剥离公网标签，仅保留私网标签；如果为 GRE 封装，则由 PE 2 剥离报文的 GRE 封装。

(5) PE 2 根据私网标签确定报文的出接口，剥离私网标签后将报文转发至 CE 2。

(6) CE 2 根据正常的 IP 转发过程将报文转发给目的主机。

属于同一个 VPN 的两个 Site 连接到同一个 PE 时，PE 不需要为 VPN 报文封装外层标记和内层标签，只需查找对应 VPN 实例的路由表，找到报文的出接口，将报文转发至相应的 Site。

GRE 的详细介绍，请参见“三层技术-IP 业务配置指导”中的“GRE”。

1.1.5 MPLS L3VPN常见组网方案

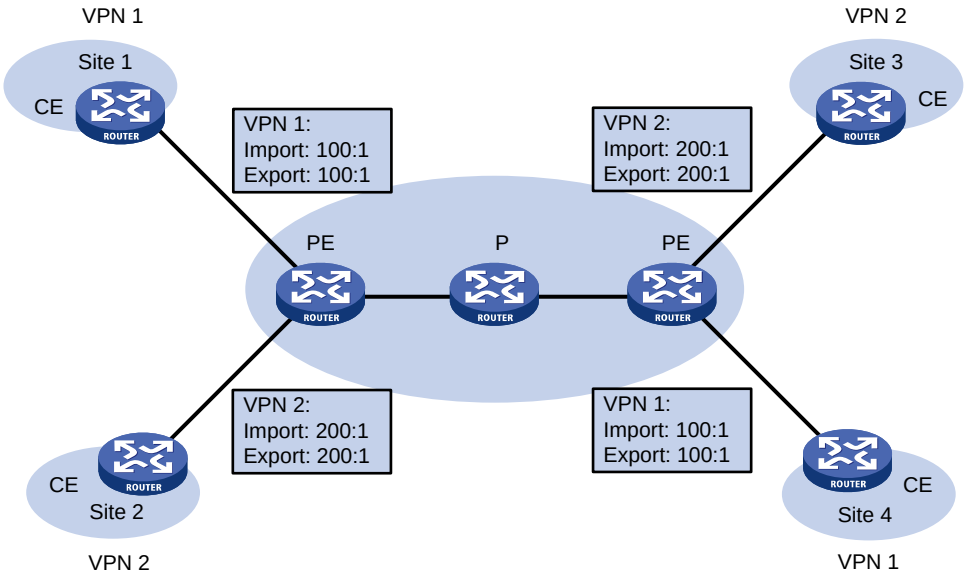
在 MPLS L3VPN 网络中，通过 VPN Target 属性来控制 VPN 路由信息在各 Site 之间的发布和接收。VPN Export Target 和 Import Target 的设置相互独立，并且都可以设置多个值，能够实现灵活的 VPN 访问控制，从而实现多种 VPN 组网方案。

1. 基本的VPN组网方案

最简单的情况下，一个 VPN 中的所有用户形成闭合用户群，相互之间能够进行流量转发，VPN 中的用户不能与任何本 VPN 以外的用户通信。

对于这种组网，需要为每个 VPN 分配一个 VPN Target，作为该 VPN 的 Export Target 和 Import Target，且此 VPN Target 不能被其他 VPN 使用。

图1-4 基本的 VPN 组网方案



如图 1-4所示，PE上为VPN 1分配的VPN Target值为100:1，为VPN 2分配的VPN Target值为200:1。VPN 1 的两个Site之间可以互访，VPN 2 的两个Site之间也可以互访，但VPN 1 和VPN 2 的Site之间不能互访。

2. Hub&Spoke组网方案

使用 Hub&Spoke 组网方案可以实现在 VPN 中设置中心访问控制设备，其它用户的互访都通过中心访问控制设备进行，通过中心设备对其他设备之间的互访进行监控和过滤等。其中：

- 中心访问控制设备所在的站点称为 Hub 站点；该站点的 CE 称为 Hub-CE；与该站点连接的 PE 称为 Hub-PE。

- 其他分支站点称为 Spoke 站点；分支站点的 CE 称为 Spoke-CE；与分支站点连接的 PE 称为 Spoke-PE。

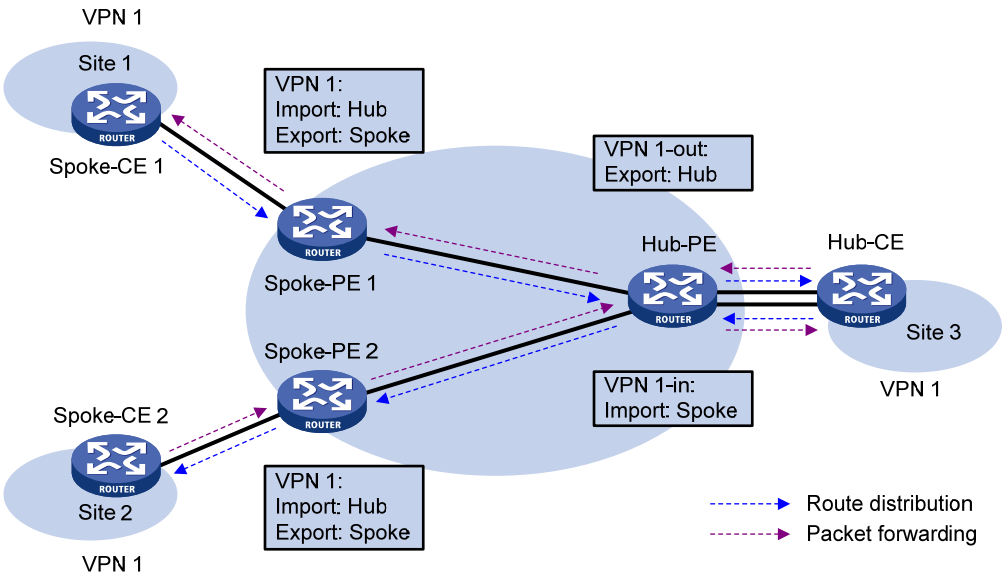
对于这种组网，VPN Target 设置规则为：

- Spoke-PE：Export Target 为“Spoke”，Import Target 为“Hub”；
- Hub-PE：Hub-PE 上需要使用两个接口或子接口连接 Hub-CE，两个接口或子接口分别属于不同的 VPN 实例。一个 VPN 实例用于接收 Spoke-PE 发来的路由，其 Import Target 为“Spoke”；另一个 VPN 实例用于向 Spoke-PE 发布路由，其 Export Target 为“Hub”。

按照上述规则设置 VPN Target，可以实现：

- Hub-PE 能够接收所有 Spoke-PE 发布的 VPN-IPv4 路由。
- Hub-PE 发布的 VPN-IPv4 路由能够为所有 Spoke-PE 接收。
- Hub-PE 将从 Spoke-PE 学到的路由发布给其他 Spoke-PE，因此，Spoke 站点之间可以通过 Hub 站点互访。
- 任意 Spoke-PE 的 Import Target 属性不与其它 Spoke-PE 的 Export Target 属性相同。因此，任意两个 Spoke-PE 之间不直接发布 VPN-IPv4 路由，Spoke 站点之间不能直接互访。

图1-5 Hub&Spoke 组网方案



如 图 1-5 所示，以站点 1 向站点 2 发布路由为例，Spoke站点之间的路由发布过程为：

(1) Spoke-CE 1 将站点 1 内的私网路由发布给 Spoke-PE 1。

(2) Spoke-PE 1 将该路由转变为 VPN-IPv4 路由，通过 MP-BGP 发布给 Hub-PE。

(3) Hub-PE 将该路由学习到 VPN 1-in 的路由表中，并将其转变为标准 IPv4 路由发布给 Hub-CE。

(4) Hub-CE 将该路由再次发布给 Hub-PE，Hub-PE 将其学习到 VPN 1-out 的路由表中。

(5) Hub-PE 将 VPN 1-out 路由表中的私网路由转变为 VPN-IPv4 路由，通过 MP-BGP 发布给 Spoke-PE 2。

(6) Spoke-PE 2 将 VPN-IPv4 路由转变为标准 IPv4 路由发布到站点 2。

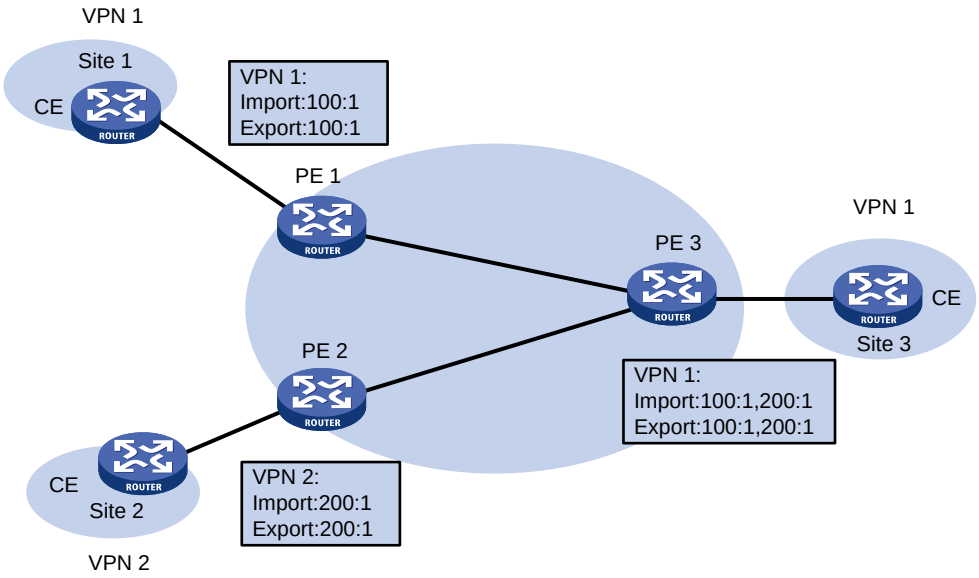
Spoke 站点之间通过 Hub 站点完成路由交互后，Spoke 站点之间的通信将通过 Hub 站点进行。

3. Extranet组网方案

如果一个 VPN 用户希望提供本 VPN 的部分站点资源给非本 VPN 的用户访问，可以使用 Extranet 组网方案。

对于这种组网，需要访问共享站点的 VPN 实例的 Export Target 必须包含在共享站点 VPN 实例的 Import Target 中，而其 Import Target 必须包含在共享站点 VPN 实例的 Export Target 中。

图1-6 Extranet 组网方案



在 图 1-6 中，VPN 1 的Site 3 为共享站点，通过设置VPN Target实现：

- PE 3 能够接受 PE 1 和 PE 2 发布的 VPN-IPv4 路由。
- PE 3 发布的 VPN-IPv4 路由能够为 PE 1 和 PE 2 接受。

基于以上两点，VPN 1 的 Site 1 和 Site 3 之间能够互访，VPN 2 的 Site 2 和 VPN 1 的 Site 3 之间也能够互访。

PE 3 不把从 PE 1 接收的 VPN-IPv4 路由发布给 PE 2，也不把从 PE 2 接收的 VPN-IPv4 路由发布给 PE 1（从 IBGP 邻居学来的路由不会再发送给其他的 IBGP 邻居）。因此，VPN 1 的 Site 1 和 VPN 2 的 Site 2 之间不能互访。

1.1.6 跨域VPN

实际组网应用中，某用户一个 VPN 的多个 Site 可能会连接到使用不同 AS 号的多个服务提供商，或者连接到一个服务提供商的多个 AS。这种 VPN 跨越多个自治系统的应用方式被称为跨域 VPN（Multi-AS VPN）。

跨域 VPN 解决方案分为以下几种：

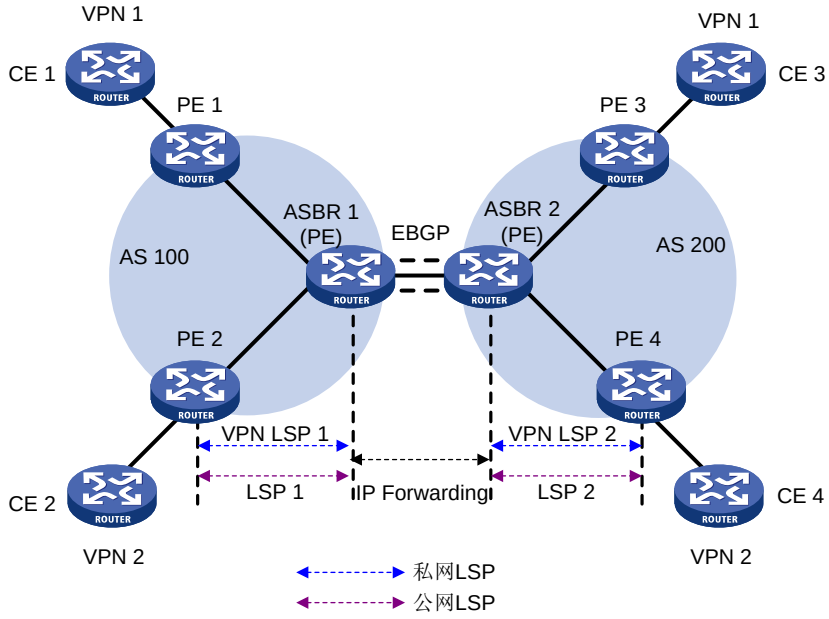
- ASBR 间建立 VRF-to-VRF 连接（VRF-to-VRF connections between ASBRs），也称为 Inter-Provider Option A。
- ASBR 间通过 MP-EBGP 发布 VPN-IPv4 路由（EBGP redistribution of labeled VPN-IPv4 routes between ASBRs），也称为 Inter-Provider Option B；

- PE 间通过 MP-EBGP 发布 VPN-IPv4 路由（Multi-hop EBGP redistribution of labeled VPN-IPv4 routes between PE routers），也称为 Inter-Provider Option C。

1. ASBR间建立VRF-to-VRF连接

这种方式下，两个 AS 的 PE 路由器作为各自所在自治系统的边界路由器 ASBR，通过多个子接口直接相连。两个 PE 都把对方当作自己的 CE 设备，通过 EBGP 会话向对端发布普通的 IPv4 单播路由，并将需要跨域的 VPN 实例与至少一个子接口关联。

图1-7 ASBR 间建立 VRF-to-VRF 连接组网图



如 图 1-7 所示，VPN 1 内路由从CE 1 发布到CE 3 的过程为：

(1) PE 1 从 CE 1 学习到私网路由后，通过 MP-IBGP 发布给 ASBR 1。

(2) ASBR 1 比较 Route Target 属性，将 PE 1 发布的 VPN-IPv4 路由学习到相应的 VPN 实例路由表中，并作为 IPv4 单播路由通过 EBGP 会话发布给它的 CE 设备，即 ASBR 2。

(3) ASBR 2 从它的 CE（ASBR 1）接收到 IPv4 单播路由后，将其加入与接收路由的子接口绑定的 VPN 实例的路由表中，并通过 MP-IBGP 发布给 PE 3。

(4) PE 3 接收到路由后，将其发布给 CE 3。

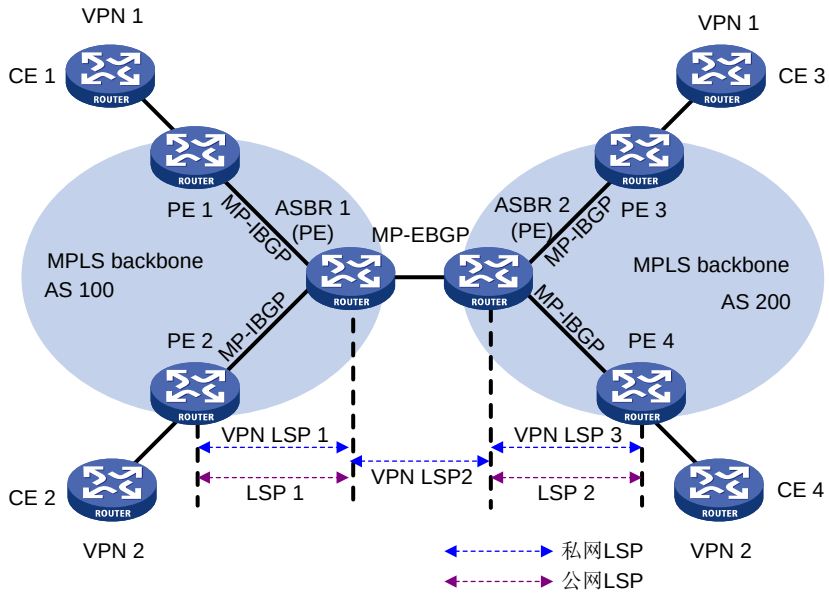
报文转发过程中，在 AS 内部作为 VPN 报文，采用两层标签的方式转发；在 ASBR 之间则采用 IP 转发方式。

这种方式的优点是实现简单，两个作为 ASBR 的 PE 之间不需要为跨域进行特殊配置。缺点是可扩展性差：作为 ASBR 的 PE 需要管理所有 VPN 的路由，为每个 VPN 创建 VPN 实例，导致 PE 上的 VPN-IPv4 路由数量过于庞大；并且，PE 上需要为每个跨域的 VPN 单独创建子接口，提高了对 PE 设备的要求。

2. ASBR间通过MP-EBGP发布VPN-IPv4 路由

这种方式下，两个 ASBR 通过 MP-EBGP 交换它们从各自 AS 的 PE 路由器接收的 VPN-IPv4 路由。

图1-8 ASBR 间通过 MP-EBGP 发布 VPN-IPv4 路由组网图



如 图 1-8 所示，VPN 1 内路由从CE 1 发布到CE 3 的过程为：

(1) PE 1 从 CE 1 学习到私网路由后，通过 MP-IBGP 发布给 ASBR 1。假设 PE 1 为私网路由分配的私网标签为 L1。

(2) ASBR 1 接收 PE 1 发布的 VPN-IPv4 路由，并作为 VPN-IPv4 路由通过 MP-EBGP 将其发布给 ASBR 2。ASBR 1 发布该路由时，将路由的下一跳地址改为自身的地址，为路由分配新的私网标签 L2，并为新的私网标签 L2 和旧的私网标签 L1 建立关联。

(3) ASBR 2 从 ASBR 1 接收到 VPN-IPv4 路由后，通过 MP-IBGP 将路由发布给 PE 3。ASBR 2 在发布路由时，将路由的下一跳地址改为自身的地址，为路由分配新的私网标签 L3，并为新的私网标签 L3 和旧的私网标签 L2 建立关联。

(4) PE 3 接收到路由后，将其发布给 CE 3。

完成路由发布后，报文从 CE 3 到 CE 1 的转发过程为：

(1) PE 3 接收到报文后，为其封装两层标签——私网标签 L3 和从 PE 3 到 ASBR 2 的公网隧道的标签，并将报文转发给 ASBR 2。

(2) ASBR 2 剥离公网标签后，将私网标签 L3 替换为 L2，并将报文发送给 ASBR 1。ASBR 1 和 ASBR 2 之间的报文只带一层私网标签。

(3) ASBR 1 将私网标签 L2 替换为 L1，添加从 ASBR 1 到 PE 1 的公网隧道的标签，并将报文转发给 PE 1。

(4) PE 1 剥离公网标签、私网标签后，将报文转发给 CE 1。

采用这种方式时，ASBR 需要接收所有跨域 VPN 的私网路由，因此，ASBR 上不能根据 Route Target 属性对接收的 VPN-IPv4 路由进行过滤。

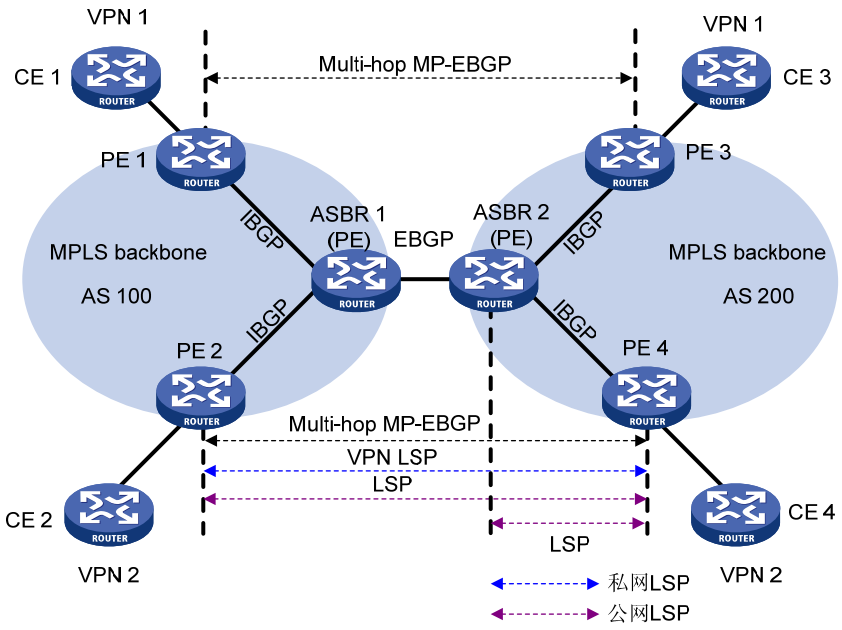
这种方式的扩展性优于 Inter-Provider Option A。缺点是 ASBR 仍然需要参与 VPN 私网路由的维护和发布。

3. PE间通过MP-EBGP发布VPN-IPv4 路由

这种方式下，不同 AS 的 PE 之间建立多跳 MP-EBGP 会话，通过该会话直接在 PE 之间发布 VPN-IPv4 路由。此时，一端 PE 上需要具有到达远端 PE 的路由以及该路由对应的标签，以便在两个 PE 之间建立跨越 AS 的公网隧道。Inter-Provider Option C 通过如下方式建立公网隧道：

- 利用 LDP 等标签分发协议在 AS 内建立公网隧道；
- 通过 ASBR 发布带标签的 IPv4 单播路由，实现跨域 AS 域建立公网隧道。带标签的 IPv4 单播路由是指为 IPv4 单播路由分配 MPLS 标签，并同时发布 IPv4 单播路由和标签，以便将路由和标签关联。

图1-9 PE 间通过 Multi-hop MP-EBGP 发布 VPN-IPv4 路由组网图



如 图 1-9 所示，VPN 1 内路由从CE 1 发布到CE 3 的过程比较简单，为：PE 1 从CE 1 学习到私网路由后，将其作为VPN-IPv4 路由通过多跳MP-EBGP会话发布给PE 3（假设PE 1 为CE 1 分配的私网标签为Lx）；PE 3 将私网路由发布给CE 3。

Inter-Provider Option C 的难点是建立跨越 AS 域的公网隧道。以 PE 3 到 PE 1 为例，公网隧道建立过程为：

(1) 在 AS 100 内，通过 LDP 等标签分发协议建立从 ASBR 1 到 PE 1 的公网隧道。假设 ASBR 1 上该公网隧道的出标签为 L1。

(2) ASBR 1 通过 EBGP 会话向 ASBR 2 发布带标签的 IPv4 单播路由，将 PE 1 地址对应的路由及 ASBR 1 为其分配的标签（假设为 L2）发布给 ASBR 2，路由的下一跳地址为 ASBR 1。这样，就建立了从 ASBR 2 到 ASBR 1 的公网隧道，ASBR 1 上公网隧道的入标签为 L2。

(3) ASBR 2 通过 IBGP 会话向 PE 3 发布带标签的 IPv4 单播路由，将 PE 1 地址对应的路由及 ASBR 2 为其分配的标签（假设为 L3）发布给 PE 3，路由的下一跳地址为 ASBR 2。这样，就建立了从 PE 3 直接到 ASBR 2 的公网隧道，ASBR 2 上公网隧道的入标签为 L3，出标签为 L2。

(4) MPLS 报文不能直接从 PE 3 转发给 ASBR 2，在 AS 200 内，还需要通过 LDP 等标签分发协议逐跳建立另一条从 PE 3 到 ASBR 2 的公网隧道。假设 PE 3 上该公网隧道的出标签为 Lv。

完成路由发布和公网隧道的建立后，报文从 CE 3 转发到 CE 1 的过程为：

(1) PE 3 接收到 CE 3 发送的报文后，查找路由表，发现下一跳地址为 PE 1，私网标签为 Lx，则为报文封装标签 Lx；PE 3 继续查找到达 PE 1 的路由，下一跳为 ASBR 2，标签为 L3，则在标签 Lx 外封装一层标签 L3；PE 3 查找到达 ASBR 2 的路由，出标签为 Lv，则在标签 L3 外再封装标签 Lv。

(2) 在 AS 200 内，路由器根据最外层标签，将报文转发到 ASBR 2。

(3) ASBR 2 剥离最外层标签，将 L3 替换为 L2，并将报文转发给 ASBR 1。

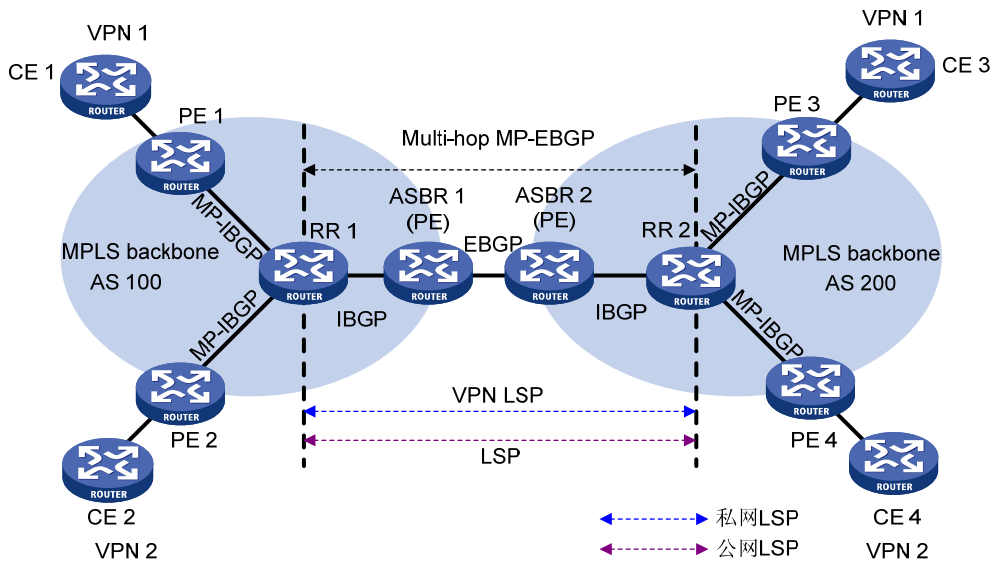
(4) ASBR 1 将 L2 替换为 L1，并转发报文。

(5) 在 AS 100 内，路由器根据最外层标签，将报文转发到 PE 1。

(6) PE 1 剥离最外层标签，根据私网标签 Lx，将报文转发给 CE 1。

如 图 1-10 所示，为提高可扩展性，可以在每个AS中指定一个RR（Route Reflector，路由反射器），与同一AS的PE交换VPN-IPv4 路由信息，由RR保存所有VPN-IPv4 路由。两个AS的RR之间建立多跳MP-EBGP会话，通告VPN-IPv4 路由。

图1-10 采用 RR 的跨域 VPN OptionC 方式组网图



Inter-Provider Option A 和 Inter-Provider Option B 都需要 ASBR 参与 VPN-IPv4 路由的维护和发布。当每个 AS 都有大量的 VPN 路由需要交换时，ASBR 很可能成为阻碍网络进一步扩展的瓶颈。Inter-Provider Option C 中 PE 之间直接交换 VPN-IPv4 路由，具有很好的可扩展性。

1.1.7 运营商的运营商

MPLS L3VPN 服务提供商的用户可能也是一个服务提供商。这种情况下，前者称为提供商运营商（Provider Carrier）或一级运营商（First Carrier），后者称为客户运营商（Customer Carrier）或二级运营商（Second Carrier）。这种组网模型称为运营商的运营商（Carriers' carriers）。

运营商的运营商通过在二级运营商的路由器之间建立 BGP 会话直接交互二级运营商连接的用户网络的路由，实现一级运营商不引入二级运营商的用户网络路由，只引入二级运营商的骨干网路由，从而大大减少一级运营商网络中需要维护的路由数量，提高可扩展性。

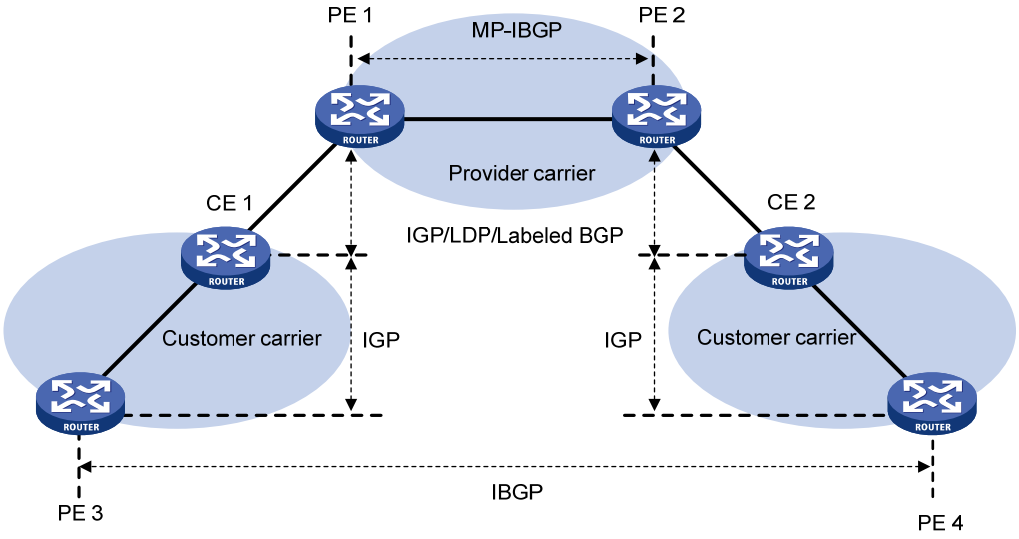
由于一级运营商不引入二级运营商的用户网络路由，为了保证用户网络的报文能够跨越一级运营商传递，在一级运营商 PE 和接入一级运营商的二级运营商 CE（在二级运营商内其为 PE 设备，以下简称为二级运营商 CE）之间需要为二级运营商骨干网的路由分配标签。一级运营商 PE 和二级运营商 CE 之间需要进行如下配置：

- 如果一级运营商 PE 与二级运营商 CE 位于同一个 AS 内，则它们之间配置 IGP 和 LDP；否则，它们之间配置 MP-EBGP，通过 MP-EBGP 为 PE 与 CE 之间交换的 IPv4 单播路由分配标签。
- 无论二者是否位于同一个 AS，二级运营商 CE 上都需要使能 MPLS。并且，二级运营商 CE 上虽然有二级运营商的用户网络路由，但它们并不把这些路由发布给一级运营商 PE，只在二级运营商 PE 之间交换。

二级运营商可能只是普通 ISP，也可能是 MPLS L3VPN 服务提供商。

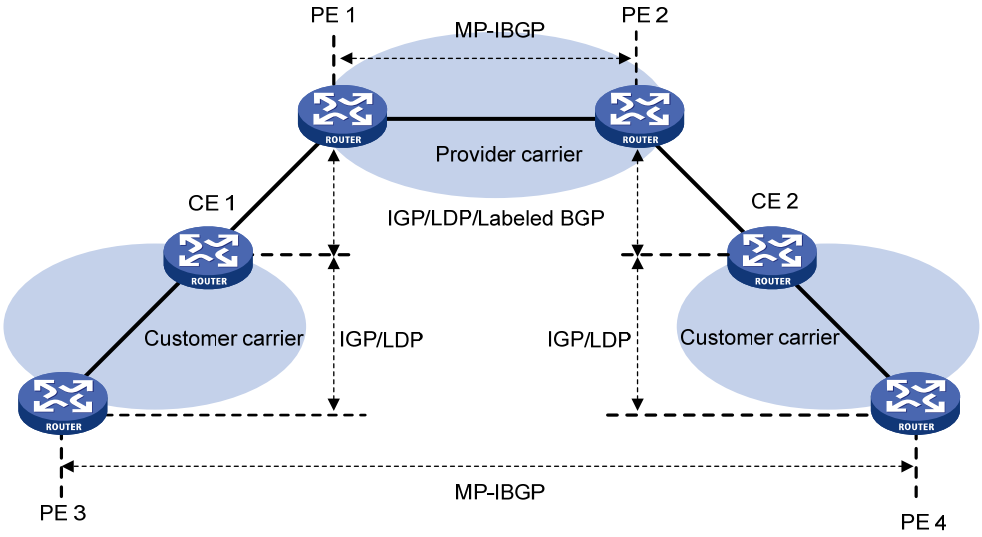
- 如 图 1-11 所示，二级运营商是普通ISP时，其PE不需要运行MPLS，与二级运营商CE之间运行IGP。PE 3 和PE 4 之间通过IBGP会话交换二级运营商的用户网络路由（IPv4 单播路由）。

图1-11 二级运营商是 ISP



- 如 图 1-12 所示，二级运营商是MPLS L3VPN服务提供商时，其PE也需要运行MPLS，与二级运营商CE之间运行IGP和LDP。PE 3 和PE 4 之间通过MP-IBGP会话交换二级运营商的用户网络路由（VPN-IPv4 路由）。

图1-12 二级运营商是 MPLS L3VPN 服务提供商



提示

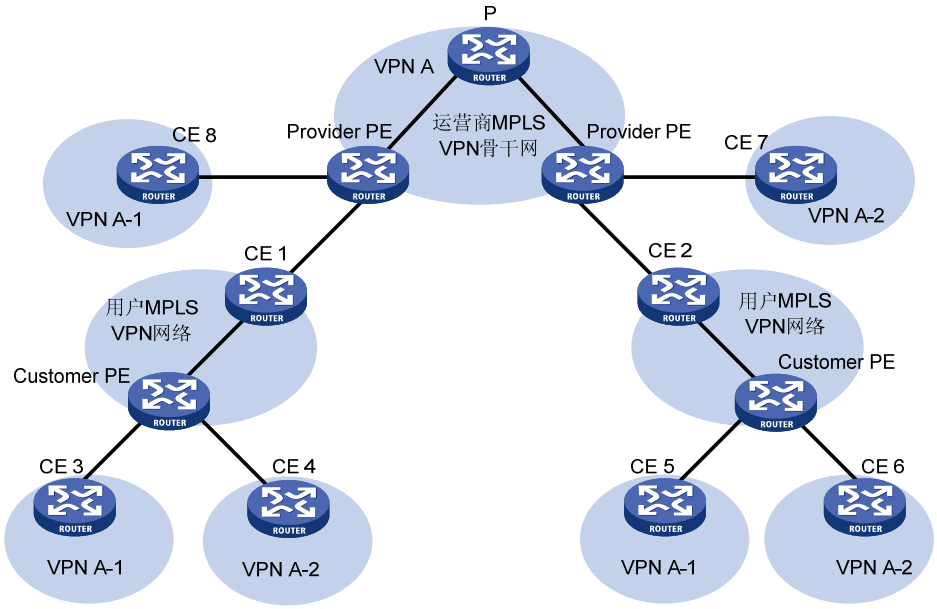
如果一级运营商和二级运营商之间存在等价路由，则建议在一级运营商和二级运营商之间建立对应的等价 LSP。

1.1.8 嵌套VPN

1. 简介

嵌套VPN通过在MPLS L3VPN的PE和CE之间传递VPNv4 路由，使得用户可以管理自己内部的VPN，根据实际需要在用户网络内部进一步划分VPN，运营商不参与用户内部VPN的管理。如 图 1-13 所示，用户网络在运营商MPLS VPN网络上所属的VPN为VPN A，在用户网络内部划分子VPN：VPN A-1 和VPN A-2。运营商PE设备把用户网络当作普通VPN用户对待，不参与子VPN的划分。运营商CE设备（CE 1 和CE 2）和运营商PE设备之间传递包括子VPN路由信息的VPNv4 路由，从而实现用户网络内部子VPN路由信息的传递。

图1-13 嵌套 VPN 组网应用



2. 路由信息的传播过程

嵌套 VPN 中，路由信息的传播过程为：

(1) 用户 PE 从用户 CE 接收到私网路由后，通过 MP-BGP 将 VPN-IPv4 路由发布给运营商 CE 设备。

(2) 运营商 CE 设备通过 MP-BGP 将 VPN-IPv4 路由发布给运营商的 PE 设备。

(3) 运营商的 PE 设备收到 VPN-IPv4 路由后，保留用户网络内部的 VPN 信息，并附加用户在运营商网络上的 MPLS VPN 属性，即将该 VPN-IPv4 路由的 RD 更换为用户所处运营商网络 VPN 的 RD，同时将用户所处运营商网络 VPN 的 Export Target 添加到路由的扩展团体属性列表中。运营商的 PE 设备维护用户网络内部的 VPN 信息。

(4) 运营商的 PE 设备向其他运营商 PE 设备发布这些携带综合 VPN 信息的 VPN-IPv4 路由。

(5) 其他的运营商 PE 设备收到 VPN-IPv4 路由后，与本地 VPN 的 Import Target 进行匹配，每个 VPN 接收属于自己的路由，并将路由发布给运营商 CE 设备。如果运营商 PE 和运营商 CE 设备之间是 IPv4 连接（如 CE 7 和 CE 8），则直接发布 IPv4 路由；如果是 VPN-IPv4 连接（如 CE 1 和 CE 2），则表示通过私网连接的是一个用户 MPLS VPN 网络，运营商 PE 向运营商 CE 发布 VPN-IPv4 路由。

(6) 用户PE通过运营商CE接收到VPN-IPv4 路由后，与本地VPN的Import Target进行匹配，每个VPN接收属于自己的路由，并发布给自己连接的用户CE设备（如 图 1-13 中的CE 3、CE 4、CE 5 和CE 6）。

3. 技术优点

嵌套 VPN 技术的主要优点是：

- 实现了 VPN 聚合功能，可以把用户网络的多个内部 VPN 聚合成一个用户 VPN，接入运营商的 MPLS VPN 网络；

- 支持对称组网方式和非对称组网方式，即属于同一用户网络的不同 Site 包括的用户内部 VPN 数目可以相同，也可以不同；
- 支持用户内部 VPN 的多层嵌套。

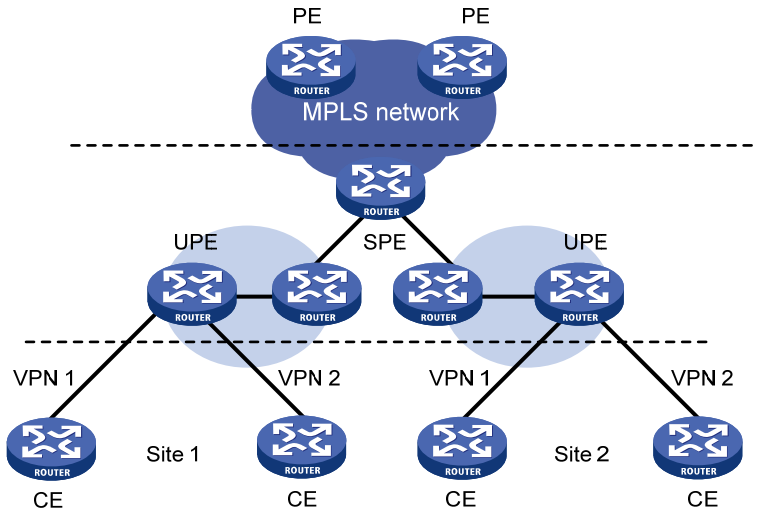
嵌套 VPN 技术降低了用户接入 VPN 网络的复杂度和成本，为用户提供多样化的 VPN 组网方式，实现了用户对内部 VPN 以及多层 VPN 之间的互访权限控制管理。

1.1.9 HoVPN

HoVPN（Hierarchy of VPN，分层 VPN），又称为 HoPE（Hierarchy of PE，分层 PE），用来避免 PE 成为网络的瓶颈，以便于大规模部署 VPN 网络。

HoVPN 将 PE 划分为 UPE（Underlayer PE or User-end PE，下层 PE 或用户侧 PE）和 SPE（Superstratum PE or Service Provider-end PE，上层 PE 或运营商侧 PE）。UPE 和 SPE 分工不同，二者构成分层式 PE，共同完成传统上一个 PE 的功能。分层式 PE 可以同普通 PE 共存于一个 MPLS 网络。

图1-14 HoVPN 的基本结构



如 图 1-14 所示，UPE和SPE的功能分别为：

- UPE 直接连接用户网络，主要完成用户接入功能。UPE 维护其直接相连的 VPN Site 的路由，但不维护 VPN 中其它远程 Site 的路由或仅维护它们的聚合路由；UPE 为其直接相连的 Site 的路由分配内层标签，并通过 MP-BGP 随 VPN 路由发布此标签给 SPE。UPE 的路由容量和转发性能较低，但接入能力强。
- SPE 连接 UPE 并位于运营商网络内部，主要完成 VPN 路由的管理和发布。SPE 维护其通过 UPE 连接的 VPN 所有路由，包括本地和远程 Site 的路由，SPE 将路由信息发布给 UPE，并携带标签。SPE 发布的路由信息可以是 VPN 实例的缺省路由（或聚合路由），也可以是通过路由策略的路由信息。通过后者可以实现对同一 VPN 下不同站点之间互访的控制。SPE 的路由表容量大，转发性能强，但接口资源较少。

SPE 和 UPE 之间运行 MP-IBGP 或 MP-EBGP。采用 MP-IBGP 时，SPE 需要作为多个 UPE 的路由反射器，在 UPE 之间反射路由。

HoVPN 支持分层式 PE 的嵌套：

- 一个分层式 PE 可以作为 UPE，同另一个 SPE 组成新的分层式 PE；
- 一个分层式 PE 可以作为 SPE，同多个 UPE 组成新的分层式 PE；

分层式 PE 的嵌套可以进行多次。在分层式 PE 的嵌套中，SPE 和 UPE 是相对的概念，上层 PE 相对于下层就是 SPE，下层 PE 相对于上层就是 UPE。

图1-15 分层式 PE 的嵌套

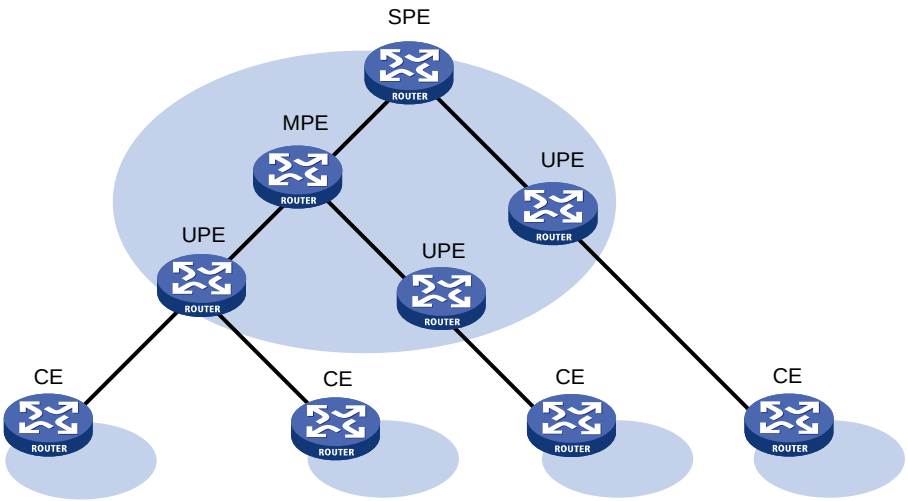


图 1-15 是一个三层的分层式PE，称中间的PE为MPE（Middle-level PE）。SPE和MPE之间，以及MPE和UPE之间，均运行MP-BGP。MP-BGP为上层PE发布下层PE上的所有VPN路由，为下层PE发布上层PE的VPN实例缺省路由或通过路由策略的VPN路由。SPE维护了这个分层式PE接入的所有Site的VPN路由，路由数目最多；UPE只维护它所直接连接的Site的VPN路由，路由数目最少；MPE的路由数目介于SPE和UPE之间。

1.1.10 OSPF VPN扩展

本节重点介绍 OSPF 对 VPN 的扩展，如果需要了解 OSPF 的基本知识，请参见“三层技术-IP 路由配置指导”中的“OSPF”。

1. PE上的OSPF多实例

在 PE-CE 间运行 OSPF 交互私网路由时，PE 必须支持 OSPF 多实例，即每个 OSPF 进程与一个 VPN 实例绑定，通过该 OSPF 进程学习到的路由添加到对应 VPN 实例的路由表中，以实现不同 VPN 实例路由的隔离。

2. PE和CE间的OSPF区域配置

PE 与 CE 之间的 OSPF 区域可以是非骨干区域，也可以是骨干区域。

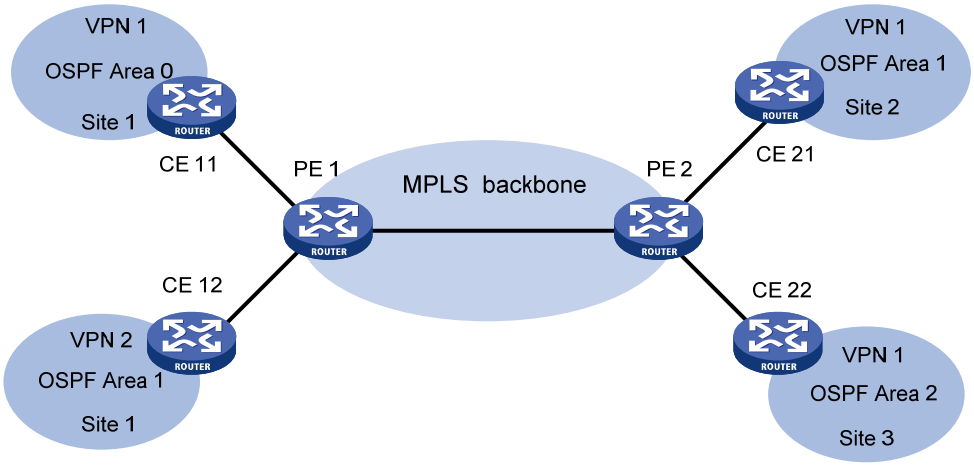
在 OSPF VPN 扩展应用中，MPLS VPN 骨干网被看作是骨干区域 area 0。由于 OSPF 要求骨干区域连续，因此，所有站点的 area 0 必须与 MPLS VPN 骨干网相连（物理连通或通过 Virtual-link 实现逻辑上的连通）。

3. BGP/OSPF交互

如果在 PE 和 CE 间运行 OSPF，则 PE 上需要将 PE 之间传递的 BGP 路由引入到 OSPF 路由中，再将该路由通过 OSPF 发布给 CE。这样就会导致即使不同的站点属于同一个 OSPF 路由域，在一

个站点学到的路由，也将作为外部路由发布给另一站点。通过为属于同一个 OSPF 路由域的站点配置相同的域 ID（Domain ID），可以解决上述问题。

图1-16 BGP/OSPF 交互示意图

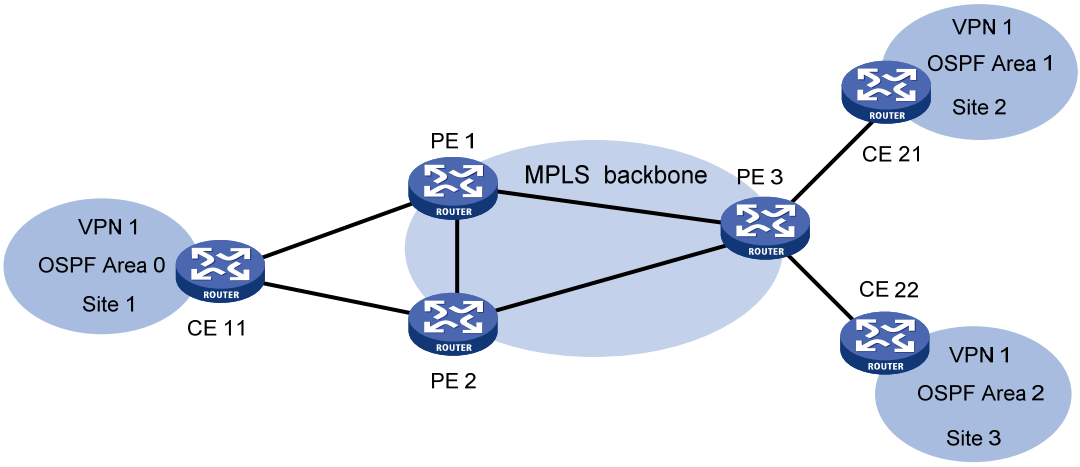


以 图 1-16 为例，CE 11、CE 21 和CE 22 属于同一个VPN，且属于同一个OSPF路由域。配置Domain ID前，VPN 1 内路由从CE 11 发布到CE 21 和CE 22 的过程为：首先在PE 1 上将CE 11 的OSPF路由引入BGP；然后通过BGP将这些VPN路由发布给PE 2；在PE 2 上将BGP路由引入到OSPF，再通过AS External LSA（即Type-5 LSA）或NSSA External LSA（即Type-7 LSA）发布给CE 21 和CE 22。

配置 Domain ID 后，路由传递过程为：在 PE 1 上将 OSPF 路由引入到 BGP 时，将 Domain ID 附加到 BGP VPNv4 路由上，作为 BGP 的扩展团体属性传递给 PE 2。PE 2 接收到 BGP 路由后，将本地配置的 Domain ID 与路由中携带的 Domain ID 进行比较。如果相同，且为区域内或区域间路由，则在 PE 2 将路由重新引入到 OSPF 时，该路由作为 Network Summary LSA（即 Type-3 LSA）发布给 CE 21 和 CE 22；否则，该路由将作为 AS External LSA（即 Type-5 LSA）或 NSSA External LSA（即 Type-7 LSA）发布给 CE 21 和 CE 22。

4. 路由环路的检测与避免

图1-17 路由环路检测与避免示意图



如 图 1-17 所示，同一个站点连接到多个不同PE的情况下，当一个PE通过OSPF向站点发布从MP-BGP学习到的私网路由时，该路由可能被另一个PE接收到，造成路由环路。

OSPF VPN 扩展通过如下方法避免路由环路：

- 对于 Type-3 LSA，通过 DN（Down Bit）标识位避免路由环路：PE 设备上将 BGP 路由引入 OSPF，并生成 Type-3 LSA 时，PE 为生成的 LSA 设置 DN 位。其他 PE 接收到 CE 发布的 Type-3 LSA 后，如果该 LSA 的 DN 位置位，则计算路由时忽略该 LSA，从而避免再次通过 BGP 协议发布该路由造成路由环路。
- 对于 Type-5 LSA 和 Type-7 LSA，通过 Route Tag（VPN 引入路由的外部路由标记）避免路由环路：为连接同一站点的 PE 设备配置相同的 Route Tag。一台 PE 设备将 BGP 路由引入 OSPF，并生成 Type-5 LSA 或 Type-7 LSA 时，为该 Type-5 或 Type-7 LSA 添加本地配置的外部路由标记。其他 PE 接收到 CE 发布的 Type-5 或 Type-7 LSA 后，将其中的外部路由标记值与本地配置的值进行比较。如果相同，则在进行路由计算时忽略该 LSA，从而避免路由环路。

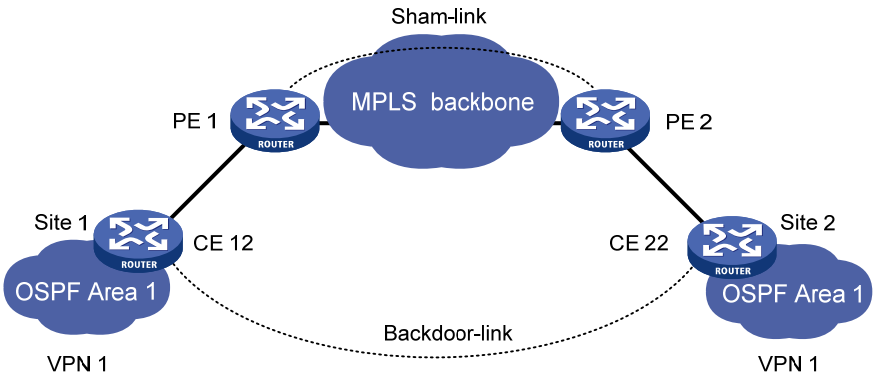
5. OSPF伪连接

如 图 1-18 所示：VPN 1 的两个站点之间存在两条路由：

- 通过 PE 连接的路由：该路由为区域间（域 ID 相同）或外部路由（未配置域 ID 或域 ID 不同）。
- CE 之间直接相连的路由：该路由为区域内路由，称为 backdoor 链路。

前者的优先级低于后者，导致 VPN 流量总是通过 backdoor 链路转发，而不走骨干网。为了避免这种情况发生，可以在 PE 路由器之间建立 OSPF 伪连接（Sham-link），使经过 MPLS VPN 骨干网的路由也成为 OSPF 区域内路由。通过调整度量值，使得 VPN 流量通过骨干网中的 Sham-link 转发。

图1-18 Sham-link 应用示意图



Sham-link 是 VPN 内的一条虚拟点到点链路，该链路在 Type-1 LSA 中发布。Sham-link 通过源 IP 地址和目的 IP 地址来唯一标识。源 IP 地址和目的 IP 地址分别为本端 PE 和远端 PE 上属于该 VPN 的地址，通常情况下采用 32 位掩码的 Loopback 接口地址。

为了保证一端 PE 的 VPN 实例路由表中具有到达 Sham-link 目的 IP 地址的路由，确保路由可达，PE 上需要将 Sham-link 的源 IP 地址作为 VPN-IPv4 地址通过 MP-BGP 发布；为了避免路由环路，Sham-link 路由不会通过 MP-BGP 发布。即，一端 PE 只会通过 MP-BGP 发布 Sham-link 的源 IP 地址，不会发布 Sham-link 的目的 IP 地址。

1.1.11 BGP的AS号替换和SoO属性

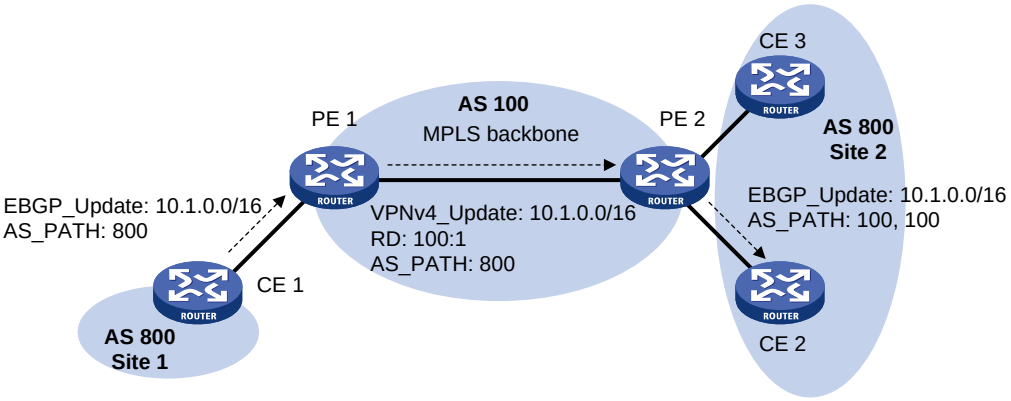
在 MPLS L3VPN 中，如果 PE 和 CE 之间运行 EBGP，由于 BGP 使用 AS 号检测路由环路，为保证路由信息的正确发送，需要为物理位置不同的站点分配不同的 AS 号。

如果物理位置不同的 CE 复用相同的 AS 号，则需要在 PE 上配置 BGP 的 AS 号替换功能，当 PE 向指定对等体（CE）发布路由时，如果路由的 AS_PATH 中存在 CE 所在的 AS 号，则 PE 将该 AS 号替换成 PE 的 AS 号后，再发布该路由，以保证私网路由能够正确发布。

说明

使能 BGP 的 AS 号替换功能后，PE 向对等体组中所有已建立连接的 CE 重新发送所有路由，并对发送路由中的 AS_PATH 属性按上述规则替换。

图1-19 BGP AS 号替换和 SoO 应用示意图



在 图 1-19 中，Site 1 和Site 2 都使用AS号 800，在PE 2 上使能针对CE 2 的AS号替换功能。当CE 1 发来的Update信息从PE 2 发布给CE 2 时，PE 2 发现AS_PATH中存在与CE 2 相同的AS号 800，就把它替换为自己的AS号 100，这样，CE 2 就可以正确接收CE 1 的路由信息。

PE使用不同接口连接同一站点的多个CE时，如 图 1-19 中的CE 2 和CE 3，使用BGP的AS号替换功能，会导致CE 3 发布的路由通过PE 2 和CE 2 再次发布到Site 2，引起路由环路。此时，通过在PE 2 上为对等体CE 2 和CE 3 配置相同的SoO属性，可以避免路由环路。PE 2 从CE 2 或CE 3 接收到路由后为路由添加SoO属性；向CE 2 或CE 3 发布路由时检查路由的SoO属性。由于CE 3 发布路由的SoO属性与CE 2 的SoO属性相同，PE 2 不会将该路由发布给CE 2，从而避免路由环路。

SoO 属性的详细介绍，请参见“三层技术-IP 路由配置指导”中的“BGP”。

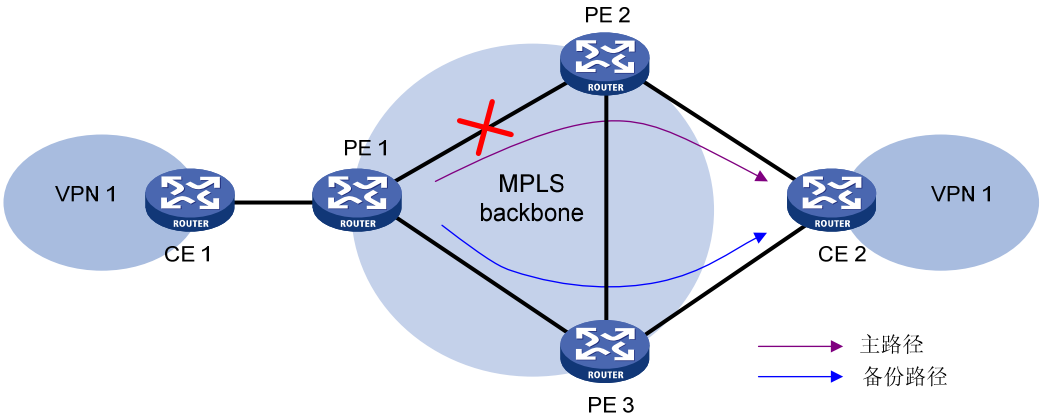
1.1.12 MPLS L3VPN快速重路由

MPLS L3VPN FRR（Fast Reroute，快速重路由）功能用来在 CE 双归属（即一个 CE 同时连接两个 PE）的组网环境下，通过为流量转发的主路径指定一条备份路径，并通过 BFD 检测主路径的状态，实现当主路径出现故障时，将流量迅速切换到备份路径，大大缩短了故障恢复时间。在使用备份路径转发报文的同时，会重新进行路由优选，优选完毕后，使用新的最优路由来转发报文。

MPLS L3VPN 快速重路由的路径备份方式分为如下几种。

(1)　VPNv4 路由备份 VPNv4 路由

图1-20 VPNv4 路由备份 VPNv4 路由示意图



如 图 1-20 所示，在入节点PE 1 上指定VPN 1 的FRR备份下一跳为PE 3，则PE 1 接收到PE 2 和PE 3 发布的到达CE 2 的VPNv4 路由后，PE 1 会记录这两条VPNv4 路由，并将PE 2 发布的VPNv4 路由当作主路径，PE 3 发布的VPNv4 路由当作备份路径。

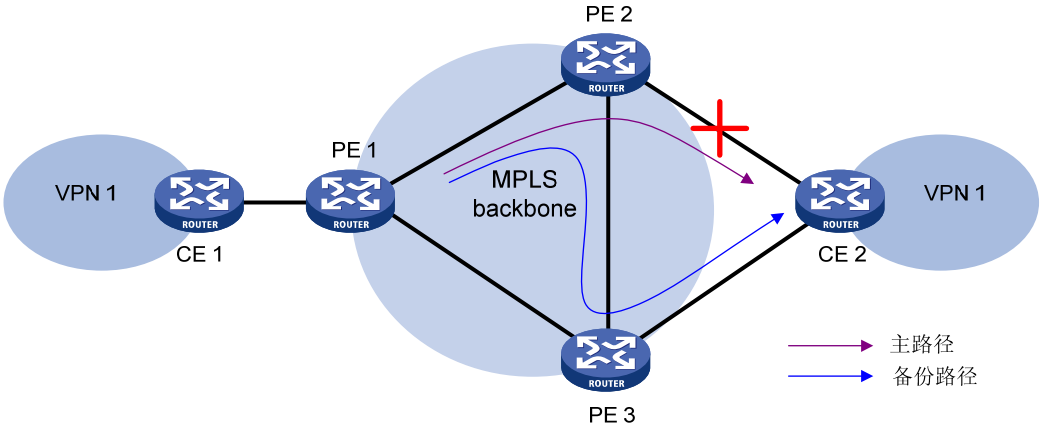
在 PE 1 上配置 BFD 检测 LSP 或 MPLS TE 隧道功能，通过 BFD 检测 PE 1 到 PE 2 之间公网隧道的状态。当公网隧道正常工作时，CE 1 和 CE 2 通过主路径 CE 1—PE 1—PE 2—CE 2 通信。当 PE 1 检测到该公网隧道出现故障时，PE 1 将通过备份路径 CE 1—PE 1—PE 3—CE 2 转发 CE 1 访问 CE 2 的流量。

在这种备份方式中，PE 1 负责主路径检测和流量切换。

BFD 检测 LSP 或 MPLS TE 隧道功能的详细介绍，请参见“MPLS 配置指导”中“MPLS OAM”。

(2)　VPNv4 路由备份 IPv4 路由

图1-21 VPNv4 路由备份 IPv4 路由示意图



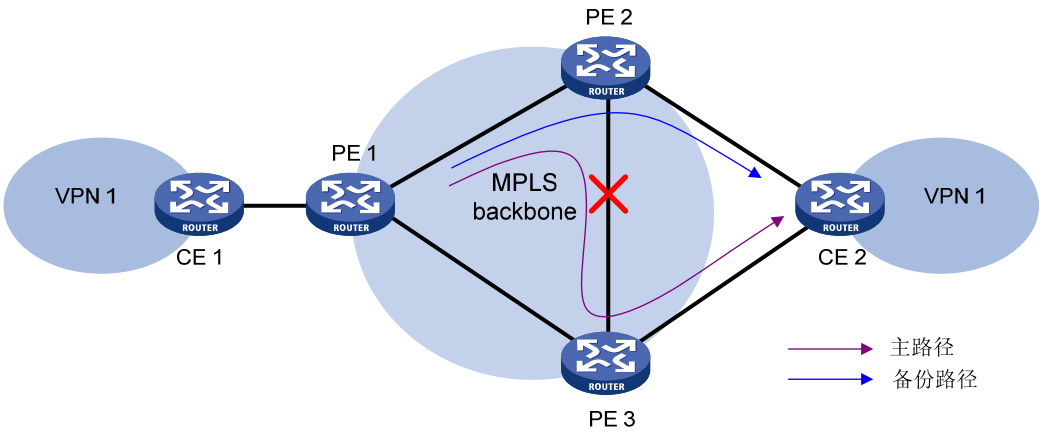
如 图 1-21 所示，在出节点PE 2 上指定VPN 1 的FRR备份下一跳为PE 3，则PE 2 接收到CE 2 发布的IPv4 路由和PE 3 发布的到达CE 2 的VPNv4 路由后，PE 2 会记录这两条路由，并将CE 2 发布的IPv4 路由当作主路径，PE 3 发布的到达CE 2 的VPNv4 路由当作备份路径。同时，PE 2 通过ARP或Echo方式的BFD会话检测PE 2—CE 2 这条路径的状态。当此路径正常工作时，CE 1 和CE 2 通

过主路径CE 1—PE 1—PE 2—CE 2 通信。当PE 2 检测到路径PE 2—CE 2 出现故障时，快速切换到路径PE 2—PE 3—CE 2，CE 1 将通过备份路径CE 1—PE 1—PE 2—PE 3—CE 2 访问CE 2。从而，避免路由收敛（切换到路径CE 1—PE 1—PE 3—CE 2）前，流量转发中断。

在这种备份方式中，PE 2 负责主路径检测和流量切换。

(3) IPv4 路由备份 VPNv4 路由

图1-22 IPv4 路由备份 VPNv4 路由示意图



如 图 1-22 所示，在PE 2 上指定VPN 1 的FRR备份下一跳为CE 2，则PE 2 接收到CE 2 发布的IPv4 路由和PE 3 发布的到达CE 2 的VPNv4 路由后，PE 2 会记录这两条路由，并将PE 3 发布的到达CE 2 的VPNv4 路由当作主路径，CE 2 发布的IPv4 路由当作备份路径。

在 PE 2 上配置 BFD 检测 LSP 或 MPLS TE 隧道功能，通过 BFD 检测 PE 2 到 PE 3 之间公网隧道的状态。当公网隧道正常工作时，CE 1 和 CE 2 通过主路径 CE 1—PE 1—PE 2—PE 3—CE 2 通信。当 PE 2 检测到该公网隧道出现故障时，PE 2 将通过备份路径 CE 1—PE 1—PE 2—CE 2 转发 CE 1 访问 CE 2 的流量。

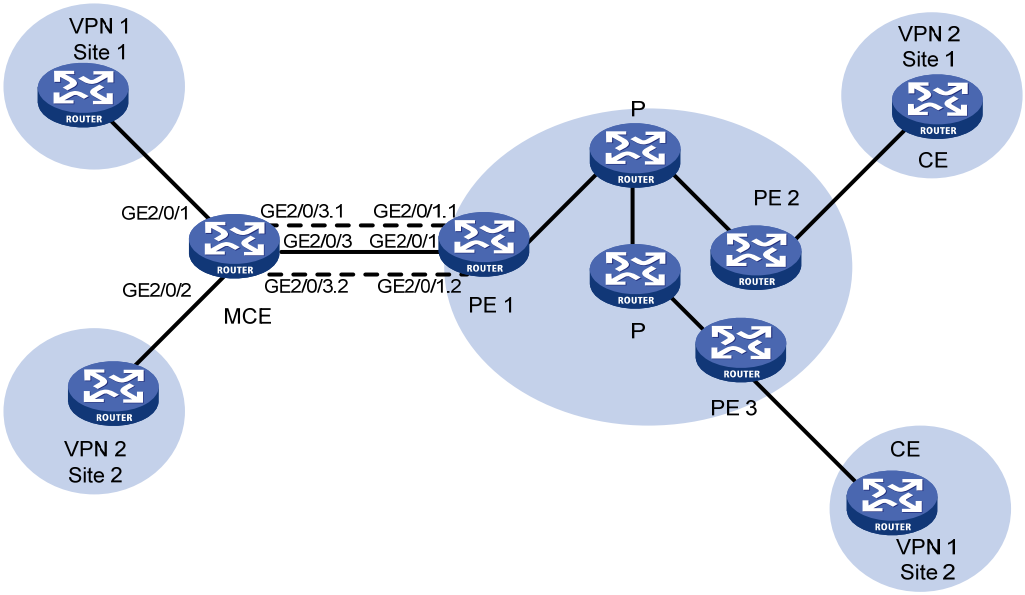
在这种备份方式中，PE 2 负责主路径检测和流量切换。

1.1.13 Multi-VPN-Instance CE

传统的MPLS L3VPN架构要求每个用户站点单独使用一个CE与PE相连，如 图 1-1 所示。随着用户业务的不断细化和安全需求的提高，一个私有网络内的用户可能需要划分成多个VPN，不同VPN用户间的业务需要完全隔离。此时，为每个VPN单独配置一台CE将加大用户的设备开支和维护成本；而多个VPN共用一台CE，使用同一个路由表项，又无法保证数据的安全性。

MCE（Multi-VPN-Instance CE，多 VPN 实例 CE）功能通过在 CE 设备上建立 VPN 实例，为不同的 VPN 提供逻辑独立的路由转发表和地址空间，使多个 VPN 可以共享一个 CE。该 CE 设备称为 MCE 设备。MCE 功能有效地解决了多 VPN 网络带来的用户数据安全与网络成本之间的矛盾。

图1-23 MCE 工作原理示意图



如 图 1-23 所示，MCE组网的关键是在MCE与用户站点之间、MCE与PE之间交互私网路由，并将其正确学习到相应VPN实例的路由表中。其他处理与传统的MPLS L3VPN相同，此处不再赘述。

- MCE 与用户站点之间的私网路由交互：在 MCE 设备上为 VPN 1 和 VPN 2 创建 VPN 实例，并使用 GigabitEthernet2/0/1 接口与 VPN 1 进行绑定、GigabitEthernet2/0/2 接口与 VPN 2 进行绑定。在接收路由信息时，MCE 设备根据路由的接收接口，即可判断该路由信息的来源，并将其维护到对应 VPN 实例的路由表中。
- MCE 与 PE 之间的私网路由交互：MCE 与 PE 1 之间通过以太网子接口连接，在 MCE 上将接口 GigabitEthernet2/0/3.1 与 VPN 1 绑定；将 GigabitEthernet2/0/3.2 与 VPN 2 绑定。在 PE 1 上为 VPN 1 和 VPN 2 创建 VPN 实例，并将连接 MCE 的接口 GigabitEthernet2/0/1.1 和 GigabitEthernet2/0/1.2 与 VPN 实例绑定，绑定的方式与 MCE 设备一致。从而，使得 MCE 与 PE 之间交互的私网路由可以准确地学习到对应 VPN 实例的路由表中。

MCE 与 VPN 站点之间、MCE 与 PE 之间可以使用静态路由、RIP、OSPF、IS-IS、EBGP 或 IBGP 交换路由信息。

说明

MCE 设备上可以配置 DHCP 服务器或 DHCP 中继功能，实现为私网内的 DHCP 客户端动态分配 IP 地址。MCE 作为 DHCP 服务器时，不同私网的 IP 地址空间不能重叠。

1.1.14 协议规范

与 MPLS L3VPN 相关的协议规范有：

- RFC 3107：Carrying Label Information in BGP-4
- RFC 4360：BGP Extended Communities Attribute

- RFC 4364：BGP/MPLS IP Virtual Private Networks (VPNs)
- RFC 4577：OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)

1.2 MPLS L3VPN配置任务简介

表1-1 MPLS L3VPN 配置任务简介

配置任务	说明	详细配置
配置基本MPLS L3VPN	必选	1.3
配置跨域VPN	可选	1.4
配置嵌套VPN	可选	1.5
配置HoVPN	可选	1.6
配置OSPF伪连接	可选	1.7
配置Multi-VPN-Instance CE	可选	1.8
配置Egress PE上私网路由标签操作方式	可选	1.9
配置BGP的AS号替换和SoO属性	可选	1.10
配置MPLS L3VPN快速重路由	可选	1.12
开启告警功能	可选	1.11

1.3 配置基本MPLS L3VPN

1.3.1 基本MPLS L3VPN配置任务简介

配置 MPLS L3VPN 的关键在于管理 VPN 私网路由在 MPLS 骨干网上的发布，包括 PE-CE 间的路由发布管理以及 PE-PE 间的路由发布管理。

表1-2 基本 MPLS L3VPN 配置任务简介

配置任务		说明	详细配置
配置VPN实例	创建VPN实例	必选	1.3.3 1.
	配置VPN实例与接口关联	必选	1.3.3 2.
	配置VPN实例的路由相关属性	可选	1.3.3 3.
配置PE-CE间的路由交换		必选	1.3.4
配置PE-PE间的路由交换		必选	1.3.5
配置BGP VPNv4路由		可选	1.3.6

1.3.2 配置准备

在配置基本 MPLS L3VPN 之前，需完成以下任务：

- 对 MPLS 骨干网（PE、P）配置 IGP，实现骨干网的 IP 连通性
- 对 MPLS 骨干网（PE、P）配置 MPLS 基本能力
- 对 MPLS 骨干网（PE、P）配置 MPLS LDP，建立 LDP LSP

1.3.3 配置VPN实例

VPN 实例不仅可以将 VPN 私网路由与公网路由隔离，还可以隔离不同 VPN 实例的路由，这一特点使得 VPN 实例的使用不限于 MPLS L3VPN。

配置 VPN 实例的操作是在 PE 或 MCE 设备上进行的。

1. 创建VPN实例

VPN 实例在实现中与 Site 关联。VPN 实例不是直接对应于 VPN，一个 VPN 实例综合了和它所对应 Site 的 VPN 成员关系和路由规则。

表1-3 创建 VPN 实例

操作	命令	说明
进入系统视图	**system-view**	-
创建VPN实例，并进入VPN实例视图	**ip vpn-instance** *vpn-instance-name*	缺省情况下，设备上不存在任何VPN实例
配置VPN实例的RD	**route-distinguisher** *route-distinguisher*	缺省情况下，没有指定VPN实例的RD
（可选）配置VPN实例的描述信息	**description** *text*	缺省情况下，未配置VPN实例的描述信息
（可选）配置VPN实例的ID	**vpn-id** *vpn-id*	缺省情况下，没有指定VPN实例的ID
（可选）配置VPN实例的SNMP上下文	**snmp context-name** *context-name*	缺省情况下，没有指定VPN实例的SNMP上下文

MSR 系列路由器各款型对于本节所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR 2600	VPN实例	最多可配置VPN数量为1023
MSR 3600		• MSR3600-28/3600-51 最多可配置 VPN 数量为 1023 • MSR 36-10/MSR 36-20/MSR 36-40/MSR 36-60 最多可配置 VPN 数量为 2047
MSR 5600		最多可配置VPN数量为4095

2. 配置VPN实例与接口关联

提示

执行 **ip binding vpn-instance** 命令将删除接口上已经配置的 IP 地址，因此需要重新配置接口的 IP 地址。

VPN 实例配置完成后，还需要与连接 CE 的接口进行关联。

表1-4 配置 VPN 实例与接口关联

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
将当前接口与VPN实例关联	**ip binding vpn-instance** *vpn-instance-name*	缺省情况下，接口不关联任何VPN实例

3. 配置VPN实例的路由相关属性

表1-5 配置 VPN 实例的路由相关属性

<table>
<tr><th colspan="2">操作</th><th>命令</th><th>说明</th></tr>
<tr><td colspan="2">进入系统视图</td><td>system-view</td><td>-</td></tr>
<tr><td rowspan="3">进入VPN实例视图或IPv4 VPN视图</td><td>进入VPN实例视图</td><td>ip vpn-instance vpn-instance-name</td><td rowspan="3">VPN实例视图下配置的路由相关属性既可以用于IPv4 VPN，也可以用于IPv6 VPN
既可以在VPN实例视图下，也可以在IPv4 VPN视图下，配置IPv4 VPN的路由相关属性。如果同时在两个视图下配置了路由相关属性，则IPv4 VPN采用IPv4 VPN视图下配置的路由相关属性</td></tr>
<tr><td rowspan="2">进入IPv4 VPN视图</td><td>ip vpn-instance vpn-instance-name</td></tr>
<tr><td>address-family ipv4</td></tr>
<tr><td colspan="2">配置VPN实例的VPN Target</td><td>vpn-target vpn-target&<1-8> [both | export-extcommunity | import-extcommunity]</td><td>缺省情况下，没有指定VPN实例的VPN Target</td></tr>
<tr><td colspan="2">配置VPN实例支持的最大激活路由前缀数</td><td>routing-table limit number { warn-threshold | simply-alert }</td><td>缺省情况下，VPN实例可以支持的最大激活路由前缀数与设备型号有关，具体请参见命令手册
配置一个VPN实例可以支持的最大激活路由前缀数，可以防止PE路由器上保存过多的激活路由前缀信息
一个PE路由器最多可以支持的激活路由前缀数与设备的型号有关，具体请参见命令手册</td></tr>
</table>

操作	命令	说明
对当前VPN实例应用入方向路由策略	**import route-policy** *route-policy*	缺省情况下，允许所有VPN Target属性匹配的路由通过 执行本配置时，需要创建路由策略。路由策略的详细介绍，请参见“三层技术-IP路由配置指导”中的“路由策略”
对当前VPN实例应用出方向路由策略	**export route-policy** *route-policy*	缺省情况下，不对发布的路由进行过滤 执行本配置时，需要创建路由策略。路由策略的详细介绍，请参见“三层技术-IP路由配置指导”中的“路由策略”
配置VPN实例的隧道策略	**tnl-policy** *tunnel-policy-name*	缺省情况下，隧道策略为按照LSP隧道－>GRE隧道－>CR-LSP隧道的优先级顺序选择隧道，负载分担条数为1 为VPN实例配置隧道策略之前必须先创建隧道策略，否则将采用缺省策略 隧道策略的创建及配置方法，请参见“MPLS配置指导”中的“隧道策略”

1.3.4 配置PE-CE间路由交换

配置 PE-CE 间路由交换可以使用静态路由、RIP、OSPF、IS-IS、EBGP 和 IBGP 路由协议。具体采用哪种协议请根据配置的实际需要。

1. 配置PE-CE间使用静态路由

表1-6 配置 PE-CE 间使用静态路由

操作	命令	说明
进入系统视图	**system-view**	-
为指定VPN实例配置静态路由	**ip route-static vpn-instance** *s-vpn-instance-name d-vpn-instance-name dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* [**public**] [**track** *track-entry-number*] | **vpn-instance** *d-vpn-instance-name next-hop-address* [**track** *track-entry-number*] } [**permanent**] [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*]	缺省情况下，没有配置静态路由 该配置在PE上进行，CE上的配置方法与普通静态路由相同 静态路由的详细配置请参见“三层技术-IP路由配置指导”中的“静态路由”

2. 配置PE-CE间使用RIP

一个 RIP 进程只能属于一个 VPN 实例。如果在启动 RIP 进程时不绑定到 VPN 实例，则该进程属于公网进程。有关 RIP 的介绍和详细配置，请参见“三层技术-IP 路由配置指导”中的“RIP”。

表1-7 配置 PE-CE 间使用 RIP

操作	命令	说明
进入系统视图	**system-view**	-
创建PE-CE间的RIP实例，并进入RIP视图	**rip** [*process-id*] **vpn-instance** *vpn-instance-name*	该配置在PE上进行，CE上配置普通RIP即可
在指定网段上使能RIP	**network** *network-address*	缺省情况下，没有网段使能RIP

3. 配置PE-CE间使用OSPF

VPN 实例绑定的 OSPF 进程中不使用系统视图下配置的公网 Router ID，因此用户需要在启动进程时手工配置 Router ID，或者所要绑定的 VPN 实例中至少有一个接口配置了 IP 地址。

一个 OSPF 进程只能属于一个 VPN 实例。如果在启动 OSPF 进程时不绑定到 VPN 实例，则该进程属于公网进程。有关 OSPF 的介绍和详细配置，请参见“三层技术-IP 路由配置指导”中的“OSPF”。

表1-8 配置 PE-CE 间使用 OSPF

操作	命令	说明
进入系统视图	**system-view**	-
创建PE-CE间的OSPF实例，并进入OSPF视图	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	该配置在PE上进行，CE上配置普通OSPF即可 一个VPN实例中最多可以启动的OSPF进程数没有限制，没有最大值，与设备内存有关 删除VPN实例后，相关的所有OSPF进程也将全部被删除
（可选）配置OSPF域标识符	**domain-id** *domain-id* [**secondary**]	缺省情况下，OSPF域标识符为0 该配置在PE上进行，CE上配置普通OSPF即可 OSPF进程的域ID包含在此进程生成的路由中，在将OSPF路由引入BGP时，域ID被附加到BGP路由上，作为BGP的扩展团体属性传递 配置域ID时需要注意： • 每个 OSPF 进程只能配置一个域 ID，不同进程的域 ID 可以相同 • 同一个 VPN 的所有 OSPF 进程应配置相同的域 ID，以保证路由发布的正确性
（可选）配置OSPF扩展团体属性的类型编码	**ext-community-type** { **domain-id** *type-code1* | **router-id** *type-code2* | **route-type** *type-code3* }	缺省情况下，OSPF扩展团体属性Domain ID的类型编码是0x0005，Router ID的类型编码是0x0107，Route Type的类型编码是0x0306 该配置在PE上进行
配置OSPF区域，并进入OSPF区域视图	**area** *area-id*	缺省情况下，没有配置OSPF区域

操作	命令	说明
配置区域所包含的网段并在指定网段的接口上使能OSPF	**network** *ip-address wildcard-mask*	缺省情况下，接口不属于任何区域且OSPF功能处于关闭状态

4. 配置PE-CE间使用IS-IS

一个 IS-IS 进程只能属于一个 VPN 实例。如果在启动 IS-IS 进程时不绑定到 VPN 实例，则该进程属于公网进程。有关 IS-IS 的介绍和详细配置，请参见“三层技术-IP 路由配置指导”中的“IS-IS”。

表1-9 配置 PE-CE 间使用 IS-IS

操作	命令	说明
进入系统视图	**system-view**	-
创建PE-CE间的IS-IS实例，并进入IS-IS视图	**isis** [*process-id*] **vpn-instance** *vpn-instance-name*	该配置在PE上进行，CE上配置普通IS-IS即可
配置网络实体名称	**network-entity** *net*	缺省情况下，没有配置NET
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置指定接口上使能IS-IS路由进程	**isis enable** [*process-id*]	缺省情况下，IS-IS功能在接口上处于关闭状态，且没有任何IS-IS进程与其关联

5. 配置PE-CE间使用EBGP

(1) PE 上的配置

表1-10 PE 上的配置

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
进入BGP-VPN实例视图	**ip vpn-instance** *vpn-instance-name*	BGP-VPN实例视图下的配置任务与BGP视图下的相同，有关介绍和详细配置，请参见“三层技术-IP路由配置指导”中的“BGP”
将CE配置为VPN私网EBGP对等体	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体 BGP的配置中有对等体和对等体组的配置，有关介绍和详细说明请参见“三层技术-IP路由配置指导”中的“BGP”。本章中不将对等体和对等体组加以区分
创建BGP-VPN IPv4单播地址族，并进入BGP-VPN IPv4单播地址族视图	**address-family ipv4** [**unicast**]	缺省情况下，没有创建BGP-VPN IPv4单播地址族

操作	命令	说明
使能本地路由器与指定对等体/对等体组交换IPv4单播路由信息的能力	**peer** { *group-name* | *ip-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv4单播路由信息
引入本端CE路由	**import-route** *protocol* [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]	PE需要将到本端CE的路由引入VPN路由表中，以发布给对端PE
（可选）配置允许本地AS号在所接收的路由的AS_PATH属性中出现，并可同时配置允许重复的次数	**peer** { *group-name* | *ip-address* } **allow-as-loop** [*number*]	缺省情况下，不允许本地AS号在接收路由的AS_PATH属性中出现 通常情况下，BGP通过AS号检测路由环路。但在Hub&Spoke组网方式下，如果在PE和CE之间运行EBGP，当PE将路由信息通告给CE时带上本自治系统的AS号，再从CE接收路由更新时，路由更新消息中会带有本自治系统的AS号，这样PE就不能接收这条路由更新信息，此时需要配置允许路由环路

(2) CE 上的配置

表1-11 CE 上的配置

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
将PE配置为对等体	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体
创建BGP IPv4单播地址族，并进入BGP IPv4单播地址族视图	**address-family ipv4** [**unicast**]	缺省情况下，没有创建BGP IPv4单播地址族
使能本地路由器与指定对等体/对等体组交换IPv4单播路由信息的能力	**peer** { *group-name* | *ip-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv4单播路由信息
（可选）配置路由引入	**import-route** *protocol* [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]	CE需要将自己所能到达的VPN网段地址发布给接入的PE，通过PE发布给对端CE

6. 配置PE-CE间使用IBGP

提示

PE 和 CE 之间使用 IBGP 路由协议只适用于基本的 MPLS L3VPN 组网环境，Hub&Spoke、Extranet、跨域 VPN、运营商的运营商、嵌套 VPN 和 HoVPN 组网中，PE 和 CE 之间不能配置 IBGP。

(1) PE 上的配置

表1-12 PE 上的配置

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
进入BGP-VPN实例视图	**ip vpn-instance** *vpn-instance-name*	BGP-VPN实例视图下的配置任务与BGP视图下的相同，有关介绍和详细配置，请参见“三层技术-IP路由配置指导”中的“BGP”
将CE配置为VPN私网IBGP对等体	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体
创建BGP-VPN IPv4单播地址族，并进入BGP-VPN IPv4单播地址族视图	**address-family ipv4** [**unicast**]	缺省情况下，没有创建BGP-VPN IPv4单播地址族
使能本地路由器与指定对等体/对等体组交换IPv4单播路由信息的能力	**peer** { *group-name* | *ip-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv4单播路由信息
将CE配置为路由反射器的客户端	**peer** { *group-name* | *ip-address* } **reflect-client**	缺省情况下，没有配置路由发射器及其客户端 缺省情况下PE不会向IBGP对等体（包括VPNv4的IBGP对等体）发送从IBGP对等体CE学习的路由，只有将CE配置为路由反射器的客户端后，才能向其它IBGP对等体发送从该CE学习的路由 配置路由反射器后不会修改路由的下一跳。如果需要修改下一跳，则需在路由的接收端通过入策略进行修改
（可选）允许路由反射器在客户机之间反射路由	**reflect between-clients**	缺省情况下，允许路由反射器在客户机之间反射路由
（可选）配置路由反射器的集群ID	**reflector cluster-id** { *cluster-id* | *ip-address* }	缺省情况下，每个路由反射器都使用自己的Router ID作为集群ID 如果一个集群中配置了多个路由反射器，请使用本命令为所有的路由反射器配置相同的集群ID，以避免产生路由环路

(2) CE 上的配置

表1-13 CE 上的配置

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
将PE配置为IBGP对等体	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体

操作	命令	说明
创建BGP IPv4单播地址族，并进入BGP IPv4单播地址族视图	**address-family ipv4** [**unicast**]	缺省情况下，没有创建BGP IPv4单播地址族
使能本地路由器与指定对等体/对等体组交换IPv4单播路由信息的能力	**peer** { *group-name* | *ip-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv4单播路由信息
（可选）配置路由引入	**import-route** *protocol* [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]	CE需要将自己所能到达的VPN网段地址发布给接入的PE，通过PE发布给对端CE

1.3.5 配置PE-PE间的路由交换

表1-14 配置 PE-PE 间的路由交换

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
将对端PE配置为对等体	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体
指定与对等体/对等体组创建BGP会话时建立TCP连接使用的源接口	**peer** { *group-name* | *ip-address* } **connect-interface** *interface-type interface-number*	缺省情况下，BGP使用到达BGP对等体的最佳路由的出接口作为与对等体/对等体组创建BGP会话时建立TCP连接的源接口
创建BGP VPNv4地址族，并进入BGP VPNv4地址族视图	**address-family vpnv4**	缺省情况下，没有创建BGP VPNv4地址族
使能本地路由器与指定对等体交换VPNv4路由信息的能力	**peer** { *group-name* | *ip-address* } **enable**	缺省情况下，本地路由器不能与对等体交换VPNv4路由信息

1.3.6 配置BGP VPNv4 路由

BGP VPNv4 路由的属性需要在 BGP VPNv4 地址族视图下配置。BGP VPNv4 路由的很多配置都与 BGP IPv4 单播路由相同，详细配置请参见“三层技术-IP 路由配置指导”中的“BGP”。

表1-15 配置 BGP VPNv4 路由

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
进入BGP VPNv4地址族视图	**address-family vpnv4**	-

操作	命令	说明
配置对发布的路由信息进行过滤	**filter-policy** { *acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol process-id*]	缺省情况下，不对发布的路由信息进行过滤
配置对接收的路由信息进行过滤	**filter-policy** { *acl-number* | **prefix-list** *prefix-list-name* } **import**	缺省情况下，不对接收的路由信息进行过滤
配置向对等体/对等体组发布团体属性	**peer** { *group-name* | *ip-address* } **advertise-community**	缺省情况下，不向对等体/对等体组发布团体属性
配置对于从对等体/对等体组接收的路由，允许本地AS号在接收路由的AS_PATH属性中出现，并配置允许出现的次数	**peer** { *group-name* | *ip-address* } **allow-as-loop** [*number*]	缺省情况下，不允许本地AS号在接收路由的AS_PATH属性中出现
为对等体/对等体组设置基于AS路径过滤列表的BGP路由过滤策略	**peer** { *group-name* | *ip-address* } **as-path-acl** *as-path-acl-number* { **export** | **import** }	缺省情况下，没有设置基于AS路径过滤列表的BGP路由过滤策略
向对等体/对等体组发送缺省路由	**peer** { *group-name* | *ip-address* } **default-route-advertise vpn-instance** *vpn-instance-name*	缺省情况下，不向对等体/对等体组发送缺省路由
为对等体/对等体组设置基于ACL的BGP路由过滤策略	**peer** { *group-name* | *ip-address* } **filter-policy** *acl-number* { **export** | **import** }	缺省情况下，没有设置基于ACL的BGP路由过滤策略
保存所有来自指定对等体/对等体组的原始路由更新信息，不管这些路由是否通过了路由策略的过滤	**peer** { *group-name* | *ip-address* } **keep-all-routes**	缺省情况下，不保存来自对等体/对等体组的原始路由更新信息
配置向对等体/对等体组发布路由时，将下一跳属性修改为自身的地址	**peer** { *group-name* | *ip-address* } **next-hop-local**	缺省情况下，向对等体/对等体组发布路由时，将下一跳属性修改为自身的地址
配置向EBGP对等体/对等体组发布路由时不改变下一跳	**peer** { *group-name* | *ip-address* } **next-hop-invariable**	缺省情况下，向EBGP对等体/对等体组发布路由时会将下一跳改为自己的地址 如果在跨域VPN OptionC组网中使用路由反射器RR（Route Reflector）通告VPNv4路由，则需要在路由反射器上通过本命令配置向EBGP邻居和反射客户通告VPNv4路由时，不改变路由的下一跳，以保证私网路由下一跳不会被修改
为从指定对等体/对等体组接收的路由分配首选值	**peer** { *group-name* | *ip-address* } **preferred-value** *value*	缺省情况下，从对等体/对等体组接收的路由的首选值为0
为对等体/对等体组设置基于地址前缀列表的BGP路由过滤策略	**peer** { *group-name* | *ip-address* } **prefix-list** *prefix-list-name* { **export** | **import** }	缺省情况下，没有设置基于地址前缀列表的BGP路由过滤策略
配置向指定EBGP对等体/对等体组发送BGP更新消息时只携带公有AS号，不携带私有AS号	**peer** { *group-name* | *ip-address* } **public-as-only**	缺省情况下，向EBGP对等体/对等体组发送BGP更新消息时，既可以携带公有AS号，又可以携带私有AS号

操作	命令	说明
配置将本机作为路由反射器，并将对等体或对等体组作为路由反射器的客户	**peer** { *group-name* | *ip-address* } **reflect-client**	缺省情况下，没有配置路由反射器及其客户
设置允许从指定对等体/对等体组收到的路由数量	**peer** { *group-name* | *ip-address* } **route-limit** *prefix-number* [{ **alert-only** | **discard** | **reconnect** *reconnect-time* } | *percentage-value*] *	缺省情况下，不限制从对等体/对等体组接收的路由数量
对来自对等体/对等体组的路由或发布给对等体/对等体组的路由应用路由策略	**peer** { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** }	缺省情况下，没有为对等体/对等体组指定路由策略
对接收到的VPNv4路由使能VPN-Target过滤功能	**policy vpn-target**	缺省情况下，对接收到的VPNv4路由使能VPN-Target过滤功能
允许路由反射器在客户机之间反射路由	**reflect between-clients**	缺省情况下，允许路由反射器在客户机之间反射路由
配置路由反射器的集群ID	**reflector cluster-id** { *cluster-id* | *ip-address* }	缺省情况下，每个路由反射器都使用自己的Router ID作为集群ID
创建路由反射器的反射策略	**rr-filter** *extended-community-number*	缺省情况下，路由反射器不会对反射的路由进行过滤
为BGP对等体/对等体组配置SoO属性	**peer** { *group-name* | *ip-address* } **soo** *site-of-origin*	缺省情况下，没有为BGP对等体/对等体组配置SoO属性

1.4 配置跨域VPN

如果承载 VPN 路由的 MPLS 骨干网跨越多个 AS，就需要配置跨域 VPN。

跨域VPN有三种解决方案，详细描述请参见“1.1.6 跨域VPN”。请根据实际组网情况，选择合适的跨域VPN方案。

1.4.1 配置跨域VPN-OptionA

跨域VPN-OptionA的实现比较简单，当PE上的VPN数量及VPN路由数量都比较少时可以采用这种方案。跨域VPN-OptionA的配置可以描述为：对各AS分别进行基本MPLS L3VPN配置，对于ASBR，将对端ASBR看作自己的CE配置即可。即：跨域VPN-OptionA方式需要在PE和ASBR上分别配置VPN实例，前者用于接入CE，后者用于接入对端ASBR。配置方法请参见“1.3 配置基本MPLS L3VPN”。

在跨域 VPN-OptionA 方式中，对于同一个 VPN，同一 AS 内的 ASBR 与 PE 的 VPN 实例的 VPN Target 应能匹配；不同 AS 的 PE 之间的 VPN 实例的 VPN Target 则不需要匹配。

1.4.2 配置跨域VPN-OptionB

跨域 VPN-OptionB 的配置主要包括以下内容：

- PE 上的配置：

配置基本MPLS L3VPN，并指定同一AS内的ASBR为MP-IBGP对等体。对于同一个VPN，不同 AS 的 PE 上为该 VPN 实例配置的 VPN Target 需要匹配。

- ASBR 上的配置：
  - 在连接 AS 内部路由器的接口上配置路由协议、使能 MPLS 能力、使能 LDP 能力，以便在 AS 内建立公网隧道。
  - 指定同一 AS 内的 PE 为 MP-IBGP 对等体，不同 AS 的 ASBR 为 MP-EBGP 对等体；
  - 配置不对 VPNv4 路由进行 VPN Target 过滤，使得 ASBR 可以保存所有 VPNv4 路由信息，以通告给对端 ASBR；
  - 在 ASBR 之间使能 MPLS 能力，使其具有转发标签报文的能力，不需要配置 MPLS LDP 等标签分发协议。

配置跨域 VPN-OptionB 时，需要注意：ASBR 在将 VPNv4 路由发布给 MP-IBGP 对等体时，始终会将下一跳修改为自身的地址，不受 **peer next-hop-local** 命令的控制。

PE的配置请参见“1.3 配置基本MPLS L3VPN”，以下配置是在ASBR上进行的。

表1-16 配置跨域 VPN-OptionB 的 ASBR

操作	命令	说明
进入系统视图	**system-view**	-
进入连接对端ASBR接口的接口视图	**interface** *interface-type interface-number*	-
使能接口的MPLS能力	**mpls enable**	缺省情况下，接口的MPLS能力处于关闭状态
退回系统视图	**quit**	-
进入BGP视图	**bgp** *as-number*	-
创建BGP对等体	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体 本配置中，需要将同一AS的PE配置为IBGP对等体，不同AS的ASBR配置为EBGP对等体
进入BGP VPNv4地址族视图	**address-family vpnv4**	-
使能本地路由器与同一AS的PE、不同AS的ASBR交换VPNv4路由信息的能力	**peer** { *group-name* | *ip-address* } **enable**	缺省情况下，本地路由器不能与对等体交换VPNv4路由信息
不对VPNv4路由进行VPN Target过滤	**undo policy vpn-target**	缺省情况下，PE对收到的VPNv4路由进行VPN Target过滤，通过过滤的路由会被加入到路由表中，没有通过过滤的路由将被丢弃

1.4.3 配置跨域VPN-OptionC

跨域 VPN-OptionC 的配置主要包括以下内容：

- PE 上的配置：

- 配置基本 MPLS L3VPN，并指定另一 AS 内的 PE 为 MP-EBGP 对等体。对于同一个 VPN，不同 AS 的 PE 上为该 VPN 实例配置的 VPN Target 需要匹配。
- 由于 PE 之间不是直连，因此需要配置 **peer ebgp-max-hop** 命令，允许本地路由器同非直连网络上的邻居建立 EBGP 会话。
- 指定同一 AS 的 ASBR 为 IBGP 对等体，并使能二者之间交换带标签的 IPv4 单播路由的能力。

- ASBR 上的配置：
  - 在连接 AS 内部路由器的接口上配置路由协议、使能 MPLS 能力、使能 LDP 能力，以便在 AS 内建立公网隧道。
  - 指定同一 AS 内的 PE 为 IBGP 对等体，不同 AS 的 ASBR 为 EBGP 对等体，分别使能二者之间交换带标签的 IPv4 单播路由的能力。
  - 在 ASBR 之间使能 MPLS 能力，使其具有转发标签报文的能力，不需要配置 MPLS LDP 等标签分发协议。
  - ASBR 上还可以配置路由策略，来灵活控制向 IBGP 或 EBGP 对等体发布的哪些 IPv4 单播路由带有 MPLS 标签。

除了上述配置外，还需要在 PE 或 ASBR 上配置通过 BGP 发布 PE 地址对应的路由，配置方法请参见“三层技术-IP 路由配置指导”中的“BGP”。

1. 配置PE

PE上基本MPLS L3VPN的配置方法请参见“1.3 配置基本MPLS L3VPN”，表 1-17 只罗列跨域VPN-OptionC中PE的特殊配置。

表1-17 配置 PE

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
配置本AS的ASBR为IBGP对等体	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体
将另一AS的PE配置为EBGP对等体	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体
创建BGP IPv4单播地址族，并进入BGP IPv4单播地址族视图	**address-family ipv4** [**unicast**]	缺省情况下，没有创建BGP IPv4单播地址族
使能本地路由器与本AS的ASBR交换IPv4单播路由信息的能力	**peer** { *group-name* | *ip-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv4单播路由信息
配置与本AS的ASBR之间能够交换带标签的IPv4路由	**peer** { *group-name* | *ip-address* } **label-route-capability**	缺省情况下，不具有与对等体/对等体组交换带标签IPv4路由的能力
退回BGP视图	**quit**	-
进入BGP VPNv4地址族视图	**address-family vpnv4**	-

操作	命令	说明
使能本地路由器与另一AS的PE交换VPNv4路由信息的能力	**peer** { *group-name* | *ip-address* } **enable**	缺省情况下，本地路由器不能与对等体交换VPNv4路由信息
（可选）配置向EBGP对等体发送路由时不改变下一跳	**peer** { *group-name* | *ip-address* } **next-hop-invariable**	该步骤用于使用RR通告VPNv4路由的情况：在RR上执行本配置，使得RR之间通告VPNv4路由时，路由的下一跳不会被改变

2. 配置ASBR

为了建立跨越 AS 域的公网隧道，ASBR 需要为 PE 地址对应的路由分配 MPLS 标签，并同时发布该路由和标签。通常情况下，ASBR 通过 BGP 发布的路由不仅包括 PE 地址，还包括其他路由。此时，可以通过配置路由策略，实现只对满足某些条件的路由分配标签，其它路由仍作为普通 IPv4 路由发布。

跨域 VPN-OptionC 中，路由策略常用的配置为：

- **if-match mpls-label**：用来匹配带有 MPLS 标签的报文。
- **apply mpls-label**：实现向对等体发布 IPv4 路由时，为其添加 MPLS 标签。本命令可以和 **if-match** 子句配合使用。例如，和 **if-match mpls-label** 配合使用时，表示如果报文中带有 MPLS 标签，则为其分配新的 MPLS 标签，并发布该路由及新分配的标签。

有关路由策略的详细介绍，请参见“三层技术-IP 路由配置指导”中的“路由策略”。

表1-18 配置 ASBR

操作	命令	说明
进入系统视图	**system-view**	-
（可选）创建路由策略，并进入路由策略视图	**route-policy** *route-policy-name* { **deny** | **permit** } **node** *node-number*	缺省情况下，设备上不存在任何路由策略
（可选）匹配带标签的IPv4路由	**if-match mpls-label**	缺省情况下，不匹配路由信息的MPLS标签
（可选）为IPv4路由分配标签	**apply mpls-label**	缺省情况下，没有为IPv4路由分配标签
退回系统视图	**quit**	-
进入BGP视图	**bgp** *as-number*	-
配置本AS的PE为IBGP对等体	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体
将另一AS的ASBR配置为EBGP对等体	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体
创建BGP IPv4单播地址族，并进入BGP IPv4单播地址族视图	**address-family ipv4** [**unicast**]	缺省情况下，没有创建BGP IPv4单播地址族
使能本地路由器与本AS的PE、另一AS的ASBR交换IPv4单播路由信息的能力	**peer** { *group-name* | *ip-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv4单播路由信息

操作	命令	说明
配置与本AS的PE及另一AS的ASBR之间能够交换带标签的IPv4路由	**peer** { *group-name* | *ip-address* } **label-route-capability**	缺省情况下，不具有与对等体/对等体组交换带标签IPv4路由的能力
向本AS的PE发布路由时将下一跳改为自己的地址	**peer** { *group-name* | *ip-address* } **next-hop-local**	缺省情况下，BGP发言者在向IBGP对等体/对等体组发布路由时不会将下一跳改为自己的地址
（可选）对来自对等体/对等体组的路由或发布给对等体/对等体组的路由应用路由策略	**peer** { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** }	缺省情况下，没有为对等体/对等体组指定路由策略

1.5 配置嵌套VPN

如果网络中 VPN 接入数量比较多，管理者想要管理权限层次化（通过 VPN 划分访问权限），且不想让外部知道用户网络内部 VPN 的部署情况，可以使用嵌套 VPN 的组网方式。在嵌套 VPN 组网方式中，用户通过较低的管理复杂度和组网成本，就可以实现内部 VPN 网络的层次化管理。

嵌套 VPN 组网中，需要进行以下配置：

- 用户 PE 和用户 CE 之间的配置：PE 上配置 VPN 实例；配置 PE 和 CE 之间的路由交换。
- 用户 PE 和运营商 CE 之间的配置：配置通过 BGP VPNv4 路由交互用户网络内部子 VPN 的路由；为了确保运营商 CE 能够接收所有的 BGP VPNv4 路由，需要在运营商 CE 上通过 **undo policy vpn-target** 命令配置运营商 CE 不根据 RT 对 VPNv4 路由进行过滤。
- 运营商 CE 和运营商 PE 之间的配置：在 PE 上配置 VPN 实例，并使能嵌套 VPN 功能；配置 PE 和 CE 之间交互 BGP VPNv4 路由。
- 运营商 PE 之间的配置：配置 PE 和 PE 之间交互 BGP VPNv4 路由。

在嵌套 VPN 组网中，用户 PE 也可以直接连接运营商 PE，与运营商 PE 交互 VPNv4 路由，不需要在网络中部署运营商 CE。此时，用户 PE 同时作为运营商 CE 设备，在用户 PE 上要进行运营商 CE 的相关配置。

用户CE、用户PE、运营商CE上的配置与MPLS L3VPN基本配置相似，运营商PE上的配置与MPLS L3VPN基本配置有所不同。运营商PE上的配置如 表 1-19 所示。

配置嵌套 VPN 时，需要注意：

- 同一用户网络的不同子 VPN 之间地址空间不能重叠。
- 建议嵌套 VPN 中对等体 CE 的地址不要与公网中对等体的地址重叠。
- 目前，嵌套 VPN 不支持多跳 EBGP 组网方式，因此运营商 PE 和运营商 CE 之间必须使用直连接口地址建立邻居关系。

表1-19 运营商 PE 上的嵌套 VPN 配置

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-

操作	命令	说明
进入BGP VPNv4地址族视图	**address-family vpnv4**	-
使能嵌套VPN功能	**nesting-vpn**	缺省情况下，嵌套VPN功能处于禁止状态
退回BGP视图	**quit**	-
进入BGP-VPN实例视图	**ip vpn-instance** *vpn-instance-name*	-
配置对等体CE或CE所属对等体组的AS号	**peer** { *group-name* | *peer-address* } **as-number** *as-number*	缺省情况下，没有指定对等体或对等体组的AS号
创建BGP-VPN VPNv4地址族，并进入BGP-VPN VPNv4地址族视图	**address-family vpnv4**	缺省情况下，没有创建BGP-VPN VPNv4地址族
激活对等体CE或CE所属的对等体组，使能与其交换BGP-VPNv4路由信息的能力	**peer** { *group-name* | *peer-address* } **enable**	缺省情况下，未激活对等体和对等体组
（可选）为BGP对等体/对等体组配置SoO属性	**peer** { *group-name* | *ip-address* } **soo** *site-of-origin*	缺省情况下，没有为BGP对等体/对等体组配置SoO属性

1.6 配置HoVPN

在 HoVPN 组网中，UPE 上仅需进行 MPLS L3VPN 基本配置，SPE 上除了 MPLS L3VPN 基本配置外，还需进行以下配置：

- 指定 BGP 对等体或对等体组为 UPE。
- 配置 SPE 向 UPE 发送路由的方式：向 UPE 发送指定 VPN 实例的缺省路由或通过路由策略的路由。
- 创建 BGP-VPN 实例：由于 SPE 上没有接口与用户网络直接相连，因此，SPE 上不需要配置 VPN 实例与接口关联。为了根据 RT 属性将学习到的 VPNv4 路由添加到相应 VPN 实例的 BGP 路由表中，SPE 上需要创建 BGP-VPN 实例。

配置 HoVPN 时，需要注意：

- 建议不要同时配置 **peer default-route-advertise vpn-instance** 命令和 **peer upe route-policy** 命令。
- 建议 SPE 不直接同 CE 连接，如必须连接，则 SPE 上 VPN 实例和 UPE 上 VPN 实例必须配置不同的 RD。

表1-20 配置 HoVPN 的 SPE

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
创建BGP对等体	**peer** { *group-name* | *peer-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体
进入BGP VPNv4地址族视图	**address-family vpnv4**	-

操作	命令	说明
使能本地路由器与指定对等体交换VPNv4路由信息的能力	**peer** { *group-name* | *ip-address* } **enable**	缺省情况下，本地路由器不能与对等体交换VPNv4路由信息
配置BGP对等体或对等体组为UPE	**peer** { *group-name* | *ip-address* } **upe**	缺省情况下，BGP对等体或对等体组不是HoVPN的UPE
向UPE发送指定VPN实例的缺省路由	**peer** { *group-name* | *ip-address* } **default-route-advertise vpn-instance** *vpn-instance-name*	二者必选其一 缺省情况下，不向对等体发布路由 执行**peer default-route-advertise vpn-instance**命令后，不论本地路由表中是否存在缺省路由，SPE都会向UPE发布一条下一跳地址为本地地址的缺省路由 只有BGP对等体或对等体组是UPE时，执行**peer default-route-advertise vpn-instance**命令后，设备才会向BGP对等体或对等体组发布VPN实例缺省路由
向UPE发送通过路由策略的路由	**peer** { *group-name* | *ip-address* } **upe route-policy** *route-policy-name* **export**	
退回BGP视图	**quit**	-
创建BGP-VPN实例，并进入BGP-VPN实例视图	**ip vpn-instance** *vpn-instance-name*	缺省情况下，设备上不存在任何BGP-VPN实例

1.7 配置OSPF伪连接

在 VPN PE 间配置伪连接 Sham-link 后，Sham-link 将被视为 OSPF 区域内路由。这一特性使经过 MPLS VPN 骨干网的路由成为 OSPF 区域内路由，避免 VPN 流量经后门路由转发。

Sham-link 的源地址和目的地址应使用 32 位掩码的 Loopback 接口地址，且该 Loopback 接口需要绑定到 VPN 实例中，并通过 BGP 发布。

1.7.1 配置准备

在配置 OSPF 伪连接之前，需完成以下任务：

- 配置基本 MPLS L3VPN（PE-CE 间使用 OSPF）
- 配置用户 CE 所在局域网的 OSPF

1.7.2 配置Loopback接口

表1-21 配置 Loopback 接口

操作	命令	说明
进入系统视图	**system-view**	-
创建Loopback接口，并进入Loopback接口视图	**interface loopback** *interface-number*	缺省情况下，设备上不存在任何Loopback接口
将Loopback接口与VPN实例关联	**ip binding vpn-instance** *vpn-instance-name*	缺省情况下，接口不关联任何VPN实例，属于公网接口

操作	命令	说明
配置Loopback接口的地址	**ip address** *ip-address* { *mask* | *mask-length* }	缺省情况下，未配置Loopback接口的地址

1.7.3 发布Loopback接口的路由

表1-22 发布 Loopback 接口的路由

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
进入BGP-VPN实例视图	**ip vpn-instance** *vpn-instance-name*	-
进入BGP-VPN IPv4单播地址族视图	**address-family ipv4** [**unicast**]	-
引入直连路由（将Loopback主机路由引入BGP）	**import-route direct**	缺省情况下，不会引入直连路由

1.7.4 创建伪连接

表1-23 创建伪连接

操作	命令	说明
进入系统视图	**system-view**	-
进入OSPF视图	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	建议用户启动OSPF进程时手工配置路由器ID
配置VPN引入路由的外部路由标记值	**route-tag** *tag-value*	缺省情况下，若MPLS骨干网上配置了BGP路由协议，并且BGP的AS号不大于65535，则外部路由标记值的前面两个字节固定为0xD000，后面的两个字节为本端BGP的AS号；否则，外部路由标记值为0
进入OSPF区域视图	**area** *area-id*	-
创建一条OSPF伪连接	**sham-link** *source-ip-address destination-ip-address* [**cost** *cost* | **dead** *dead-interval* | **hello** *hello-interval* | { { **hmac-md5** | **md5** } *key-id* { **cipher** *cipher-string* | **plain** *plain-string* } | **simple** { **cipher** *cipher-string* | **plain** *plain-string* } } | **retransmit** *retrans-interval* | **trans-delay** *delay*] *	缺省情况下，设备上不存在任何OSPF伪连接

1.8 配置Multi-VPN-Instance CE

Multi-VPN-Instance CE 可以看作一种通过路由隔离实现业务隔离的组网方案。配置 MCE 的关键为：

- 配置 MCE 与站点之间的路由交换
- 配置 MCE 与 PE 之间的路由交换

在 MCE 组网方案中，路由计算时需要关闭 PE 上的路由环路检测功能，防止路由丢失；同时禁止各路由协议互操作功能，以节省系统资源。

在配置 Multi-VPN-Instance CE 之前，需要先在 MCE 上创建 VPN 实例，并将 MCE 连接站点和 PE 的接口与 VPN 实例绑定。

1.8.1 配置MCE与站点之间的路由交换

1. 配置MCE与站点之间使用静态路由

MCE 可以通过静态路由与 Site 连接。传统 CE 配置的静态路由对全局生效，无法解决多 VPN 间的地址重叠问题。MCE 功能可以将静态路由与 VPN 实例相绑定，将各 VPN 之间的静态路由进行隔离。

表1-24 配置 MCE 与站点之间使用静态路由

操作	命令	说明
进入系统视图	**system-view**	-
为指定VPN实例配置静态路由	**ip route-static vpn-instance** *s-vpn-instance-name dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* [**public**] [**track** *track-entry-number*] | **vpn-instance** *d-vpn-instance-name next-hop-address* [**track** *track-entry-number*] } [**permanent**] [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*]	缺省情况下，没有配置静态路由 该配置在MCE上进行，站点上的配置方法与普通静态路由相同
（可选）配置静态路由的缺省优先级	**ip route-static default-preference** *default-preference-value*	缺省情况下，静态路由的缺省优先级为60

2. 配置MCE与站点之间使用RIP

一个 RIP 进程只能属于一个 VPN 实例。如果在启动 RIP 进程时不绑定到 VPN 实例，则该进程属于公网进程。通过在 MCE 上将 RIP 进程与 VPN 实例绑定，可以使不同 VPN 内的私网路由通过不同的 RIP 进程在 Site 和 MCE 间进行交互，保证了私网路由的隔离和安全。RIP 的介绍和详细配置，请参见“三层技术-IP 路由配置指导”中的“RIP”。

表1-25 配置 MCE 与站点之间使用 RIP

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
创建MCE与站点间的RIP实例，并进入RIP视图	**rip** [*process-id*] **vpn-instance** *vpn-instance-name*	该配置在MCE上进行，站点上配置普通RIP即可
在指定网段接口上使能RIP	**network** *network-address*	缺省情况下，接口上的RIP功能处于关闭状态
引入由PE发布的远端站点的路由	**import-route** *protocol* [*process-id* | **all-processes** | **allow-ibgp**] [**allow-direct** | **cost** *cost* | **route-policy** *route-policy-name* | **tag** *tag*] *	缺省情况下，RIP未引入其它路由
（可选）配置引入路由的缺省度量值	**default cost** *value*	缺省情况下，引入路由的缺省度量值为0

3. 配置MCE与站点之间使用OSPF

一个 OSPF 进程只能属于一个 VPN 实例。如果在启动 OSPF 进程时不绑定到 VPN 实例，则该进程属于公网进程。

通过在 MCE 上将 OSPF 进程与 VPN 实例绑定，可以使不同 VPN 内的私网路由通过不同的 OSPF 进程在 Site 和 MCE 间进行交互，保证了私网路由的隔离和安全。

OSPF 的介绍和详细配置，请参见“三层技术-IP 路由配置指导”中的“OSPF”。

表1-26 配置 MCE 与站点之间使用 OSPF

操作	命令	说明
进入系统视图	**system-view**	-
创建MCE与站点间的OSPF实例，并进入OSPF视图	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	该配置在MCE上进行，站点上配置普通OSPF即可 VPN实例绑定的OSPF进程中不使用系统视图下配置的公网Router ID，因此用户需要在启动进程时手工配置Router ID 一个OSPF进程只能属于一个VPN实例，但一个VPN实例可以使用多个OSPF进程为其传播私网路由
（可选）配置OSPF域标识符	**domain-id** *domain-id* [**secondary**]	缺省情况下，OSPF域标识符为0 该配置在MCE上进行 同一VPN内的OSPF进程应配置相同的域ID，以保证路由发布的正确性
引入由PE发布的远端站点的路由	**import-route** *protocol* [*process-id* | **all-processes** | **allow-ibgp**] [**allow-direct** | **cost** *cost* | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *	缺省情况下，没有引入其他协议的路由信息
配置OSPF区域，进入OSPF区域视图	**area** *area-id*	缺省情况下，没有配置OSPF区域
配置区域所包含的网段并在指定网段的接口上使能OSPF	**network** *ip-address wildcard-mask*	缺省情况下，接口不属于任何区域且OSPF功能处于关闭状态

4. 配置MCE与站点之间使用IS-IS

一个 IS-IS 进程只能属于一个 VPN 实例。如果在启动 IS-IS 进程时不绑定到 VPN 实例，则该进程属于公网进程。

通过在 MCE 上将 IS-IS 进程与 VPN 实例绑定，可以使不同 VPN 内的私网路由通过不同的 IS-IS 进程在 Site 和 MCE 间进行交互，保证了私网路由的隔离和安全。

IS-IS 协议的介绍和详细配置，请参见“三层技术-IP 路由配置指导”中的“IS-IS”。

表1-27 配置 MCE 与站点之间使用 IS-IS

操作	命令	说明
进入系统视图	**system-view**	-
创建MCE与站点间的IS-IS实例，并进入IS-IS视图	**isis** [*process-id*] **vpn-instance** *vpn-instance-name*	该配置在MCE上进行，站点上配置普通IS-IS即可
配置网络实体名称	**network-entity** *net*	缺省情况下，没有配置网络实体名称
引入由PE发布的远端站点的路由	**import-route** *protocol* [*process-id* | **all-processes** | **allow-ibgp**] [**allow-direct** | **cost** *cost* | **cost-type** { **external** | **internal** } | [**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *	缺省情况下，IS-IS不引入其它协议的路由信息 如果**import-route**命令中不指定引入的级别，则默认为引入路由到Level-2路由表中
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能接口IS-IS并指定要关联的IS-IS进程号	**isis enable** [*process-id*]	缺省情况下，接口上没有使能IS-IS

5. 配置MCE与站点之间使用EBGP

MCE 与站点间使用 EBGP 交换路由信息时，需要在 MCE 上为每个 VPN 实例配置 BGP 对等体，并在站点上引入相应 VPN 内的 IGP 路由信息。

MCE 使用 EBGP 交换路由信息时，还可以通过 Filter-policy 对接收/发布的路由进行过滤。

(1) MCE 上的配置

表1-28 配置 MCE 与站点之间使用 EBGP

操作	命令	说明
进入系统视图	**system-view**	-
启动BGP，并进入BGP视图	**bgp** *as-number*	缺省情况下，系统没有运行BGP
进入BGP-VPN实例视图	**ip vpn-instance** *vpn-instance-name*	BGP-VPN实例视图下的配置任务与BGP视图下的相同，有关介绍和详细配置，请参见“三层技术-IP路由配置指导”中的“BGP”

操作	命令	说明
配置EBGP对等体或对等体组	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体和对等体组
进入BGP-VPN IPv4单播地址族视图	**address-family ipv4** [**unicast**]	-
使能本地路由器与指定对等体交换IPv4单播路由信息的能力	**peer** { *group-name* | *ip-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv4单播路由信息
配置对于从对等体/对等体组接收的路由，允许本地AS号在接收路由的AS_PATH属性中出现，并配置允许出现的次数	**peer** { *group-name* | *ip-address* } **allow-as-loop** [*number*]	缺省情况下，不允许本地AS号在接收路由的AS_PATH属性中出现
引入由PE发布的远端站点的路由	**import-route** *protocol* [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]	缺省情况下，BGP不会引入IGP路由协议的路由信息
（可选）配置对发布的路由信息进行过滤	**filter-policy** { *acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol process-id*]	缺省情况下，不对发布的路由信息进行过滤
（可选）配置对接收的路由信息进行过滤	**filter-policy** { *acl-number* | **prefix-list** *prefix-list-name* } **import**	缺省情况下，不对接收的路由信息进行过滤

(2) 站点上的配置

表1-29 站点上的配置

操作	命令	说明
进入系统视图	**system-view**	-
启动BGP，并进入BGP视图	**bgp** *as-number*	缺省情况下，系统没有运行BGP
将MCE配置为EBGP对等体	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体和对等体组
进入BGP IPv4单播地址族视图	**address-family ipv4** [**unicast**]	-
使能本地路由器与指定对等体交换IPv4单播路由信息的能力	**peer** { *group-name* | *ip-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv4单播路由信息
配置引入VPN内的IGP路由	**import-route** *protocol* [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]	缺省情况下，BGP不会引入IGP路由协议的路由信息 站点需要将自己所能到达的VPN网段地址发布给接入的MCE

6. 配置MCE与站点间使用IBGP

MCE 与站点间使用 IBGP 交换路由信息时，需要在 MCE 上为每个 VPN 实例配置 BGP 对等体，并在站点上引入相应 VPN 内的 IGP 路由信息。

(1) MCE 上的配置

表1-30 配置 MCE 与站点之间使用 IBGP

操作	命令	说明
进入系统视图	**system-view**	-
启动BGP，并进入BGP视图	**bgp** *as-number*	缺省情况下，系统没有运行BGP
进入BGP-VPN实例视图	**ip vpn-instance** *vpn-instance-name*	-
配置IBGP对等体	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体和对等体组
进入BGP-VPN IPv4单播地址族视图	**address-family ipv4** [**unicast**]	-
使能本地路由器与指定对等体交换IPv4单播路由信息的能力	**peer** { *group-name* | *ip-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv4单播路由信息
（可选）配置本地设备作为路由反射器，对端设备作为路由反射器的客户端	**peer** { *group-name* | *ip-address* } **reflect-client**	缺省情况下，没有配置路由反射器及其客户端 将站点配置为IBGP对等体时，从该站点学习的BGP路由不会向其它IBGP对等体（包括VPNv4对等体）发送。只有将站点配置为路由反射器的客户端后，才能向其它IBGP对等体发送从该站点学习的路由
引入由PE发布的远端站点的路由	**import-route** *protocol* [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]	缺省情况下，BGP不引入且不通告其它协议的路由
（可选）配置对发布的路由信息进行过滤	**filter-policy** { *acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol process-id*]	缺省情况下，不对发布的路由信息进行过滤
（可选）配置对接收的路由信息进行过滤	**filter-policy** { *acl-number* | **prefix-list** *prefix-list-name* } **import**	缺省情况下，不对接收的路由信息进行过滤

(2) 站点上的配置

表1-31 站点上的配置

操作	命令	说明
进入系统视图	**system-view**	-
启动BGP，并进入BGP视图	**bgp** *as-number*	缺省情况下，系统没有运行BGP
将MCE配置为IBGP对等体	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体和对等体组
进入BGP IPv4单播地址族视图	**address-family ipv4** [**unicast**]	-

操作	命令	说明
使能本地路由器与指定对等体交换IPv4单播路由信息的能力	**peer** { *group-name* | *ip-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv4单播路由信息
配置引入VPN内的IGP路由	**import-route** *protocol* [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]	缺省情况下，BGP不引入且不通告其它协议的路由 站点需要将自己所能到达的VPN网段地址发布给接入的MCE

1.8.2 配置MCE与PE之间的路由交换

由于在 MCE 设备上已经将站点内的私网路由信息与 VPN 实例进行了绑定，因此，只需要在 MCE 与 PE 之间将接口与 VPN 实例进行绑定、进行简单的路由配置、并将 MCE 上维护的站点内的 VPN 路由引入到 MCE-PE 间的路由协议中，便可以实现私网 VPN 路由信息的传播。

本节中的配置均在MCE上进行，PE上的配置与基本MPLS L3VPN组网中PE上的配置相同，详细介绍请参见“1.3.4 配置PE-CE间路由交换”。

1. 配置MCE与PE之间使用静态路由

表1-32 配置 MCE 与 PE 之间使用静态路由

操作	命令	说明
进入系统视图	**system-view**	-
为指定VPN实例配置静态路由	**ip route-static vpn-instance** *s-vpn-instance-name dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* [**public**] [**track** *track-entry-number*] | **vpn-instance** *d-vpn-instance-name next-hop-address* [**track** *track-entry-number*] } [**permanent**] [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*]	缺省情况下，设备上不存在任何静态路由
（可选）配置静态路由的缺省优先级	**ip route-static default-preference** *default-preference-value*	缺省情况下，静态路由的缺省优先级为60

2. 配置MCE与PE之间使用RIP

表1-33 配置 MCE 与 PE 之间使用 RIP

操作	命令	说明
进入系统视图	**system-view**	-
创建MCE与PE间的RIP实例，并进入RIP视图	**rip** [*process-id*] **vpn-instance** *vpn-instance-name*	-

操作	命令	说明
在指定网段接口上使能RIP	**network** *network-address*	缺省情况下，接口上的RIP功能处于关闭状态
引入站点内的VPN路由	**import-route** *protocol* [*process-id* | **all-processes** | **allow-ibgp**] [**allow-direct** | **cost** *cost* | **route-policy** *route-policy-name* | **tag** *tag*] *	缺省情况下，RIP未引入其它路由
（可选）配置引入路由的缺省度量值	**default cost** *value*	缺省情况下，引入路由的缺省度量值为0

3. 配置MCE与PE之间使用OSPF

表1-34 配置 MCE 与 PE 之间使用 OSPF

操作	命令	说明
进入系统视图	**system-view**	-
创建MCE与PE间的OSPF实例，并进入OSPF视图	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	-
关闭OSPF实例的路由环路检测功能	**vpn-instance-capability simple**	缺省情况下，OSPF实例的路由环路检测功能处于开启状态 需要在MCE上通过本命令关闭OSPF实例的路由环路检测功能。否则，MCE不会接收PE发送过来的OSPF路由，导致路由丢失
（可选）配置OSPF域标识符	**domain-id** *domain-id* [**secondary**]	缺省情况下，OSPF域标识符为0
引入站点内的VPN路由	**import-route** *protocol* [*process-id* | **all-processes** | **allow-ibgp**] [**allow-direct** | **cost** *cost* | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *	缺省情况下，没有引入其他协议的路由信息
（可选）配置对发布的路由进行过滤	**filter-policy** { *acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*]]	缺省情况下，没有对发布的路由信息进行过滤
（可选）配置引入外部路由时的参数缺省值（开销、标记、类型）（该配置仅连接PE端使用）	**default** { **cost** *cost* | **tag** *tag* | **type** *type* } *	缺省情况下，OSPF引入外部路由的度量值为1，外部路由标记值为1，引入的外部路由类型为Type2
配置OSPF区域，进入OSPF区域视图	**area** *area-id*	缺省情况下，没有配置OSPF区域
配置区域所包含的网段并在指定网段的接口上使能OSPF	**network** *ip-address wildcard-mask*	缺省情况下，接口不属于任何区域且OSPF功能处于关闭状态

4. 配置MCE与PE之间使用IS-IS

表1-35 配置 MCE 与 PE 之间使用 IS-IS

操作	命令	说明
进入系统视图	**system-view**	-
创建MCE与PE间的IS-IS实例，并进入IS-IS视图	**isis** [*process-id*] **vpn-instance** *vpn-instance-name*	-
配置网络实体名称	**network-entity** *net*	缺省情况下，没有配置网络实体名称
引入站点内的VPN路由	**import-route** *protocol* [*process-id*	**all-processes**	**allow-ibgp**] [**allow-direct**	**cost** *cost*	**cost-type** { **external**	**internal** }	[**level-1**	**level-1-2**	**level-2**]	**route-policy** *route-policy-name*	**tag** *tag*] *	缺省情况下，IS-IS不引入其它协议的路由信息 如果**import-route**命令中不指定引入的级别，则默认为引入路由到Level-2路由表中
（可选）对发布的路由进行过滤（该配置仅连接PE端使用）	**filter-policy** { *acl-number*	**prefix-list** *prefix-list-name*	**route-policy** *route-policy-name* } **export** [*protocol* [*process-id*]]	缺省情况下，IS-IS不对发布的路由信息进行过滤
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能接口IS-IS并指定要关联的IS-IS进程号	**isis enable** [*process-id*]	缺省情况下，接口上没有使能IS-IS

5. 配置MCE与PE之间使用EBGP

表1-36 配置 MCE 与 PE 之间使用 EBGP

操作	命令	说明
进入系统视图	**system-view**	-
启动BGP，并进入BGP视图	**bgp** *as-number*	缺省情况下，系统没有运行BGP
进入BGP-VPN实例视图	**ip vpn-instance** *vpn-instance-name*	-
将PE配置为EBGP对等体	**peer** { *group-name*	*ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体和对等体组
进入BGP-VPN IPv4单播地址族视图	**address-family ipv4** [**unicast**]	-
使能本地路由器与指定对等体交换IPv4单播路由信息的能力	**peer** { *group-name*	*ip-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv4单播路由信息
引入站点内的VPN路由	**import-route** *protocol* [{ *process-id*	**all-processes** } [**allow-direct**	**med** *med-value*	**route-policy** *route-policy-name*] *]	缺省情况下，BGP不引入且不通告其它协议的路由

操作	命令	说明
（可选）配置对发布的路由信息进行过滤	**filter-policy** { *acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol process-id*]	缺省情况下，不对发布的路由信息进行过滤
（可选）配置对接收的路由信息进行过滤	**filter-policy** { *acl-number* | **prefix-list** *prefix-list-name* } **import**	缺省情况下，不对接收的路由信息进行过滤

6. 配置MCE与PE之间使用IBGP

表1-37 配置 MCE 与 PE 之间使用 IBGP

操作	命令	说明
进入系统视图	**system-view**	-
启动BGP，并进入BGP视图	**bgp** *as-number*	缺省情况下，系统没有运行BGP
进入BGP-VPN实例视图	**ip vpn-instance** *vpn-instance-name*	-
将PE配置为IBGP对等体	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体和对等体组
进入BGP-VPN IPv4单播地址族视图	**address-family ipv4** [**unicast**]	-
使能本地路由器与指定对等体交换IPv4单播路由信息的能力	**peer** { *group-name* | *ip-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv4单播路由信息
引入站点内的VPN路由	**import-route** *protocol* [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]	缺省情况下，BGP不引入且不通告其它协议的路由
（可选）配置对发布的路由信息进行过滤	**filter-policy** { *acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol process-id*]	缺省情况下，不对发布的路由信息进行过滤
（可选）配置对接收的路由信息进行过滤	**filter-policy** { *acl-number* | **prefix-list** *prefix-list-name* } **import**	缺省情况下，不对接收的路由信息进行过滤

1.9 配置Egress PE上私网路由标签操作方式

Egress PE 上私网路由的标签操作方式根据标签查找 FIB 进行转发与根据标签查找出接口进行转发两种：

- 私网标签的 POPGO 转发方式：标签分配时，都明确了标签跟出接口和下一跳的对应关系，弹出标签后，直接从出接口发送。
- 私网标签的 POP 转发方式：忽略标签分配时明确的标签跟出接口和下一跳对应关系，弹出标签后，再查 FIB 表转发。

表1-38 配置 Egress PE 上私网路由标签操作方式

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
配置Egress PE上私网路由的标签操作方式为根据标签查找出接口转发	**vpn popgo**	缺省情况下，Egress PE上私网路由的标签操作方式为根据标签查找FIB进行转发

1.10 配置BGP的AS号替换和SoO属性

不同 Site 的 CE 具有相同的 AS 号时，PE 上需要开启 BGP 的 AS 号替换功能，从而避免路由被丢弃。

使能了 BGP 的 AS 号替换功能后，当 PE 向指定 CE 发布路由时，如果路由的 AS_PATH 中有与 CE 相同的 AS 号，将被替换成 PE 的 AS 号后再发布。

PE 使用不同接口连接同一站点的多个 CE 时，如果配置了 BGP 的 AS 号替换功能，则会导致路由环路。这种情况下，需要在 PE 上通过 **peer soo** 命令为从同一站点不同 CE 学习到的路由添加相同的 SoO 属性，且 PE 向 CE 发布路由时检查 SoO 属性，如果路由的 SoO 属性与为 CE 配置的 SoO 属性相同，则不将该路由发布给 CE，从而避免路由环路。

本配置中各命令的详细介绍，请参见“三层技术-IP 路由命令参考”中的“BGP”。

表1-39 配置 BGP 的 AS 号替换和 SoO 属性

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
进入BGP-VPN实例视图	**ip vpn-instance** *vpn-instance-name*	-
使能BGP的AS号替换功能	**peer** { *ip-address* | *group-name* } **substitute-as**	缺省情况下，BGP的AS号替换功能是被禁止的
进入BGP-VPN IPv4单播地址族视图	**address-family ipv4** [**unicast**]	-
（可选）为BGP对等体/对等体组配置SoO属性	**peer** { *group-name* | *ip-address* } **soo** *site-of-origin*	缺省情况下，没有为BGP对等体/对等体组配置SoO属性

1.11 开启告警功能

开启 L3VPN 模块的告警功能后，在 VPN 实例内的路由数达到告警门限等情况下，L3VPN 模块会产生 RFC 4382 中规定的告警信息。生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。

有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

表1-40 开启告警功能

操作	命令	说明
进入系统视图	**system-view**	-
开启L3VPN模块的告警功能	**snmp-agent trap enable l3vpn**	缺省情况下，L3VPN模块的告警功能处于开启状态

1.12 配置MPLS L3VPN快速重路由

开启 MPLS L3VPN 快速重路由功能的方法有如下两种：

- 在 BGP-VPN IPv4 单播地址族视图下执行 **pic** 命令开启该地址族的快速重路由功能。采用这种方法时，设备会为当前 VPN 实例的所有 BGP 路由自动计算备份下一跳，即只要从不同 BGP 对等体学习到了到达同一目的网络的路由，且这些路由不等价，就会生成主备两条路由。
- 在 BGP-VPN IPv4 单播地址族视图下执行 **fast-reroute route-policy** 命令指定快速重路由引用的路由策略，并在引用的路由策略中，通过 **apply fast-reroute backup-nexthop** 命令指定备份下一跳的地址。采用这种方式时，只有为主路由计算出的备份下一跳地址与指定的地址相同时，才会为其生成备份下一跳；否则，不会为主路由生成备份下一跳。在引用的路由策略中，还可以配置 **if-match** 子句，用来决定哪些路由可以进行快速重路由保护，设备只会为通过 **if-match** 子句过滤的路由生成备份下一跳。

引用路由策略方式的优先级高于通过 **pic** 命令开启 MPLS L3VPN 快速重路由方式。

表1-41 配置 MPLS L3VPN 快速重路由

操作		命令	说明
进入系统视图		**system-view**	-
使能MPLS BFD功能		**mpls bfd enable**	二者选其一 在VPNv4路由备份VPNv4路由、IPv4路由备份VPNv4路由组网中，需要执行**mpls bfd enable**命令，该命令的详细介绍，请参见“MPLS命令参考”中的“MPLS OAM” VPNv4路由备份IPv4路由组网中，若通过Echo方式的BFD会话检测主路由的下一跳是否可达，则需要执行**bfd echo-source-ip**命令，该命令的详细介绍，请参见“可靠性命令参考”中的“BFD”
配置echo报文的源IP地址		**bfd echo-source-ip** *ip-address*	
配置使用BFD检测公网LSP或MPLS TE隧道的连通性	配置使用BFD检测指定FEC对应LSP的连通性	**mpls bfd** *dest-addr mask-length* [**nexthop** *nexthop-address* [**discriminator local** *local-id* **remote** *remote-id*]] [**template** *template-name*]	请根据公网隧道类型选择其一 缺省情况下，未使用BFD检测公网LSP和MPLS TE隧道的连通性 在VPNv4路由备份VPNv4路由、IPv4路由备份VPNv4路由组网中，需要执行本配置；VPNv4路由备份IPv4路由组网中，不需要执行本配置 本配置中各命令的详细介绍，请参见
	配置使用BFD检测当前隧道接口对应MPLS	**interface tunnel** *number* **mode mpls-te**	
		mpls bfd [**discriminator local** *local-id* **remote** *remote-id*] [**template** *template-name*]	

操作		命令	说明
	TE隧道的连通性	**quit**	“MPLS命令参考”中的“MPLS OAM”
创建路由策略，并进入路由策略视图		**route-policy** *route-policy-name* **permit node** *node-number*	缺省情况下，不存在任何路由策略 通过引用路由策略的方式开启MPLS L3VPN快速重路由功能时，必须执行本配置 本命令的详细介绍，请参见“三层技术-IP路由命令参考”中的“路由策略”
配置快速重路由的备份下一跳地址		**apply fast-reroute backup-nexthop** *ip-address*	缺省情况下，没有指定快速重路由的备份下一跳地址 通过引用路由策略的方式开启MPLS L3VPN快速重路由功能时，必须执行本配置 本命令的详细介绍，请参见“三层技术-IP路由命令参考”中的“路由策略”
退回系统视图		**quit**	-
进入BGP视图		**bgp** *as-number*	-
（可选）配置通过Echo方式的BFD会话检测主路由的下一跳是否可达		**primary-path-detect bfd echo**	缺省情况下，通过ARP检测主路由的下一跳是否可达 VPNv4路由备份IPv4路由组网中，可以根据实际情况选择是否执行本配置；其他组网中，无需执行本配置 本命令的详细介绍，请参见“三层技术-IP路由命令参考”中的“BGP”
进入BGP-VPN实例视图		**ip vpn-instance** *vpn-instance-name*	-
进入BGP-VPN IPv4单播地址族视图		**address-family ipv4** [**unicast**]	-
（二者选其一）开启MPLS L3VPN快速重路由功能	开启当前地址族的快速重路由功能	**pic**	缺省情况下，快速重路由功能处于关闭状态 在某些组网情况下，执行**pic**命令为所有BGP路由生成备份下一跳后，可能会导致路由环路，请谨慎使用本命令 本命令的详细介绍，请参见“三层技术-IP路由命令参考”中的“BGP”
	在当前地址族视图下指定快速重路由引用的路由策略	**fast-reroute route-policy** *route-policy-name*	缺省情况下，快速重路由未引用任何路由策略 引用的路由策略中，只有**apply fast-reroute backup-nexthop**和**apply ipv6 fast-reroute backup-nexthop**命令生效，其他**apply**子句不会生效 本命令的详细介绍，请参见“三层技术-IP路由命令参考”中的“BGP”

1.13 MPLS L3VPN显示和维护

1.13.1 复位BGP会话

当 BGP 配置变化后，可以通过软复位或复位 BGP 会话使新的配置生效。软复位 BGP 会话是指在不断开 BGP 邻居关系的情况下，更新 BGP 路由信息；复位 BGP 会话是指断开并重新建立 BGP 邻居关系的情况下，更新 BGP 路由信息。软复位需要 BGP 对等体具备路由刷新能力（支持 ROUTE-REFRESH 消息）。

请在用户视图下进行下列操作。下表中各命令的详细介绍，请参见“三层技术-IP 路由命令参考”中的“BGP”。

表1-42 复位 BGP 会话

操作	命令
手工对VPNv4地址族下的BGP会话进行软复位	**refresh bgp** { *ip-address* | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** } **vpnv4** [**vpn-instance** *vpn-instance-name*]
复位VPNv4地址族下的BGP会话	**reset bgp** { *as-number* | *ip-address* | **all** | **external** | **internal** | **group** *group-name* } **vpnv4** [**vpn-instance** *vpn-instance-name*]

1.13.2 显示MPLS L3VPN的运行状态

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 MPLS L3VPN 的运行情况，通过查看显示信息验证配置的效果。

display bgp group vpnv4、**display bgp peer vpnv4** 和 **display bgp update-group vpnv4** 命令的详细介绍，请参见“三层技术-IP 路由命令参考”中的“BGP”。

表1-43 显示 MPLS L3VPN 的运行状态

操作	命令
显示与VPN实例相关联的IP路由表（本命令的详细介绍请参见“三层技术-IP路由命令参考”中的“IP路由基础命令”）	**display ip routing-table vpn-instance** *vpn-instance-name* [**statistics** | **verbose**]
显示指定VPN实例信息	**display ip vpn-instance** [**instance-name** *vpn-instance-name*]
显示指定VPN实例的FIB信息	**display fib vpn-instance** *vpn-instance-name*
显示指定VPN实例中与指定目的IP地址匹配的FIB信息	**display fib vpn-instance** *vpn-instance-name ip-address* [*mask* | *mask-length*]
显示BGP VPNv4对等体组信息	**display bgp group vpnv4** [**vpn-instance** *vpn-instance-name*] [**group-name** *group-name*]
显示BGP VPNv4对等体信息（MSR 2600/MSR 3600）	**display bgp peer vpnv4** [**vpn-instance** *vpn-instance-name*] [{ *ip-address* | **group-name** *group-name* } **log-info** | [*ip-address*] **verbose**]
显示BGP VPNv4对等体信息（MSR 5600）	**display bgp peer vpnv4** [**vpn-instance** *vpn-instance-name*] [{ *ip-address* | **group-name** *group-name* } **log-info** | [[*ip-address*] **verbose**] [**standby slot** *slot-number*]]

操作	命令
显示BGP VPNv4路由信息（MSR 2600/MSR 3600）	**display bgp routing-table vpnv4** [[**route-distinguisher** *route-distinguisher*] [*network-address* [{ *mask* | *mask-length* } [**longest-match**]] | *network-address* [*mask* | *mask-length*] **advertise-info** | **as-path-acl** *as-path-acl-number* | **community-list** { { *basic-community-list-number* | *comm-list-name* } [**whole-match**] | *adv-community-list-number* }] | [**vpn-instance** *vpn-instance-name*] **peer** *ip-address* { **advertised-routes** | **received-routes** } [*network-address* [*mask* | *mask-length*] | **statistics**] | **statistics**]
显示BGP VPNv4路由信息（MSR 5600）	**display bgp routing-table vpnv4** [[**route-distinguisher** *route-distinguisher*] [*network-address* [{ *mask* | *mask-length* } [**longest-match**]] | *network-address* [*mask* | *mask-length*] **advertise-info** | **as-path-acl** *as-path-acl-number* | **community-list** { { *basic-community-list-number* | *comm-list-name* } [**whole-match**] | *adv-community-list-number* }] | [**vpn-instance** *vpn-instance-name*] **peer** *ip-address* { **advertised-routes** | **received-routes** } [*network-address* [*mask* | *mask-length*] | **statistics**] | **statistics**] [**standby slot** *slot-number*]
显示BGP IPv4单播路由的入标签信息	**display bgp routing-table ipv4** [**unicast**] [**vpn-instance** *vpn-instance-name*] **inlabel**
显示BGP IPv4单播路由的出标签信息（MSR 2600/MSR 3600）	**display bgp routing-table ipv4** [**unicast**] [**vpn-instance** *vpn-instance-name*] **outlabel**
显示BGP IPv4单播路由的出标签信息（MSR 5600）	**display bgp routing-table ipv4** [**unicast**] [**vpn-instance** *vpn-instance-name*] **outlabel** [**standby slot** *slot-number*]
显示所有BGP VPNv4路由的入标签信息	**display bgp routing-table vpnv4 inlabel**
显示所有BGP VPNv4路由的出标签信息（MSR 2600/MSR 3600）	**display bgp routing-table vpnv4 outlabel**
显示所有BGP VPNv4路由的出标签信息（MSR 5600）	**display bgp routing-table vpnv4 outlabel** [**standby slot** *slot-number*]
显示BGP VPNv4地址族下打包组的相关信息	**display bgp update-group vpnv4** [**vpn-instance** *vpn-instance-name*] [*ip-address*]
显示OSPF伪连接信息（MSR 2600/MSR 3600）	**display ospf** [*process-id*] **sham-link** [**area** *area-id*]
显示OSPF伪连接信息（MSR 5600）	**display ospf** [*process-id*] **sham-link** [**area** *area-id*] [**standby slot** *slot-number*]

1.14 MPLS L3VPN典型配置举例

1.14.1 配置MPLS L3VPN示例

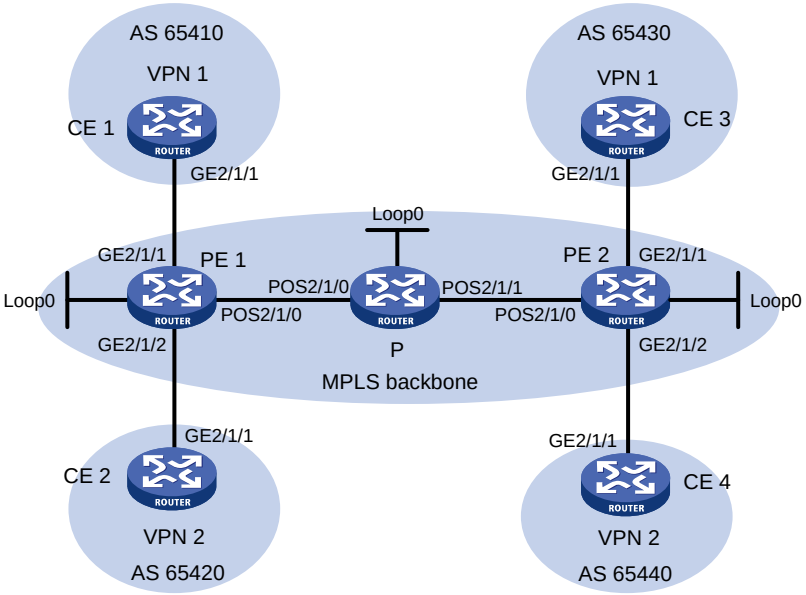
1. 组网需求

- CE 1、CE 3 属于 VPN 1，CE 2、CE 4 属于 VPN 2；
- VPN 1 使用的 VPN Target 属性为 111:1，VPN 2 使用的 VPN Target 属性为 222:2。不同 VPN 用户之间不能互相访问；

- CE 与 PE 之间配置 EBGP 交换 VPN 路由信息；
- PE 与 PE 之间配置 OSPF 实现 PE 内部的互通、配置 MP-IBGP 交换 VPN 路由信息。

2. 组网图

图1-24 配置 MPLS L3VPN 组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	GE2/1/1	10.1.1.1/24	P	Loop0	2.2.2.9/32
PE 1	Loop0	1.1.1.9/32		POS2/1/0	172.1.1.2/24
	GE2/1/1	10.1.1.2/24		POS2/1/1	172.2.1.1/24
	GE2/1/2	10.2.1.2/24	PE 2	Loop0	3.3.3.9/32
	POS2/1/0	172.1.1.1/24		GE2/1/1	10.3.1.2/24
CE 2	GE2/1/1	10.2.1.1/24		GE2/1/2	10.4.1.2/24
CE 3	GE2/1/1	10.3.1.1/24		POS2/1/0	172.2.1.2/24
CE 4	GE2/1/1	10.4.1.1/24			

3. 配置步骤

(1) 在 MPLS 骨干网上配置 IGP 协议，实现骨干网 PE 和 P 的互通

配置 PE 1。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.9 32
[PE1-LoopBack0] quit
[PE1] interface pos 2/1/0
[PE1-Pos2/1/0] ip address 172.1.1.1 24
[PE1-Pos2/1/0] quit
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 172.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

配置 P。

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 2.2.2.9 32
[P-LoopBack0] quit
[P] interface pos 2/1/0
[P-Pos2/1/0] ip address 172.1.1.2 24
[P-Pos2/1/0] quit
[P] interface pos 2/1/1
[P-Pos2/1/1] ip address 172.2.1.1 24
[P-Pos2/1/1] quit
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 172.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 172.2.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

配置 PE 2。

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 3.3.3.9 32
[PE2-LoopBack0] quit
[PE2] interface pos 2/1/0
[PE2-Pos2/1/0] ip address 172.2.1.2 24
[PE2-Pos2/1/0] quit
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 172.2.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

配置完成后，PE 1、P、PE 2 之间应能建立 OSPF 邻居，执行 **display ospf peer** 命令可以看到邻居达到 FULL 状态。执行 **display ip routing-table** 命令可以看到 PE 之间学习到对方的 Loopback 路由。

以 PE 1 为例：

```
[PE1] display ip routing-table protocol ospf

Summary Count : 5

OSPF Routing table Status : <Active>
Summary Count : 3

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
2.2.2.9/32          OSPF   10   1            172.1.1.2       POS2/1/0
3.3.3.9/32          OSPF   10   2            172.1.1.2       POS2/1/0
172.2.1.0/24        OSPF   10   2            172.1.1.2       POS2/1/0
```

```
OSPF Routing table Status : <Inactive>
Summary Count : 2

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
1.1.1.9/32          OSPF   10   0            1.1.1.9         Loop0
172.1.1.0/24        OSPF   10   1            172.1.1.1       POS2/1/0
[PE1] display ospf peer verbose

          OSPF Process 1 with Router ID 1.1.1.9
                  Neighbors

 Area 0.0.0.0 interface 172.1.1.1(POS2/1/0)'s neighbors
 Router ID: 2.2.2.9          Address: 172.1.1.2        GR State: Normal
   State: Full  Mode: Nbr is Master  Priority: 1
   DR: 172.1.1.2  BDR: 172.1.1.1  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 39  sec
   Neighbor is up for 00:00:29
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
```

(2) 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP

配置 PE 1。

```
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] interface pos 2/1/0
[PE1-Pos2/1/0] mpls enable
[PE1-Pos2/1/0] mpls ldp enable
[PE1-Pos2/1/0] quit
```

配置 P。

```
[P] mpls lsr-id 2.2.2.9
[P] mpls ldp
[P-ldp] quit
[P] interface pos 2/1/0
[P-Pos2/1/0] mpls enable
[P-Pos2/1/0] mpls ldp enable
[P-Pos2/1/0] quit
[P] interface pos 2/1/1
[P-Pos2/1/1] mpls enable
[P-Pos2/1/1] mpls ldp enable
[P-Pos2/1/1] quit
```

配置 PE 2。

```
[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls ldp
[PE2-ldp] quit
[PE2] interface pos 2/1/0
```

```
[PE2-Pos2/1/0] mpls enable
[PE2-Pos2/1/0] mpls ldp enable
[PE2-Pos2/1/0] quit
```

上述配置完成后，PE 1、P、PE 2 之间应能建立 LDP 会话，执行 **display mpls ldp peer** 命令可以看到 LDP 会话的状态为 Operational。执行 **display mpls ldp lsp** 命令，可以看到 LDP LSP 的建立情况。

以 PE 1 为例：

```
[PE1] display mpls ldp peer
Total number of peers: 1
Peer LDP ID        State         LAM  Role     GR   MD5  KA Sent/Rcvd
2.2.2.9:0          Operational   DU   Passive  Off  Off  5/5
[PE1] display mpls ldp lsp
        Status codes: * - stale, L - liberal
FECs: 3            Ingress: 2      Transit: 2      Egress: 1

FEC                In/Out Label    Nexthop         OutInterface
1.1.1.9/32         3/-
                   -/1151(L)
2.2.2.9/32         -/3             172.1.1.2       POS2/1/0
                   1151/3          172.1.1.2       POS2/1/0
3.3.3.9/32         -/1150          172.1.1.2       POS2/1/0
                   1150/1150       172.1.1.2       POS2/1/0
```

(3) 在 PE 设备上配置 VPN 实例，将 CE 接入 PE

配置 PE 1。

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 100:1
[PE1-vpn-instance-vpn1] vpn-target 111:1
[PE1-vpn-instance-vpn1] quit
[PE1] ip vpn-instance vpn2
[PE1-vpn-instance-vpn2] route-distinguisher 100:2
[PE1-vpn-instance-vpn2] vpn-target 222:2
[PE1-vpn-instance-vpn2] quit
[PE1] interface gigabitethernet 2/1/1
[PE1-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE1-GigabitEthernet2/1/1] ip address 10.1.1.2 24
[PE1-GigabitEthernet2/1/1] quit
[PE1] interface gigabitethernet 2/1/2
[PE1-GigabitEthernet2/1/2] ip binding vpn-instance vpn2
[PE1-GigabitEthernet2/1/2] ip address 10.2.1.2 24
[PE1-GigabitEthernet2/1/2] quit
```

配置 PE 2。

```
[PE2] ip vpn-instance vpn1
[PE2-vpn-instance-vpn1] route-distinguisher 200:1
[PE2-vpn-instance-vpn1] vpn-target 111:1
[PE2-vpn-instance-vpn1] quit
[PE2] ip vpn-instance vpn2
[PE2-vpn-instance-vpn2] route-distinguisher 200:2
```

```
[PE2-vpn-instance-vpn2] vpn-target 222:2
[PE2-vpn-instance-vpn2] quit
[PE2] interface gigabitethernet 2/1/1
[PE2-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE2-GigabitEthernet2/1/1] ip address 10.3.1.2 24
[PE2-GigabitEthernet2/1/1] quit
[PE2] interface gigabitethernet 2/1/2
[PE2-GigabitEthernet2/1/2] ip binding vpn-instance vpn2
[PE2-GigabitEthernet2/1/2] ip address 10.4.1.2 24
[PE2-GigabitEthernet2/1/2] quit
```

按 图 1-24 配置各CE的接口IP地址，配置过程略。

配置完成后，在 PE 设备上执行 **display ip vpn-instance** 命令可以看到 VPN 实例的配置情况。各 PE 能 ping 通自己接入的 CE。

以 PE 1 和 CE 1 为例：

```
[PE1] display ip vpn-instance
  Total VPN-Instances configured : 2
  VPN-Instance Name               RD                      Create time
  vpn1                            100:1                   2012/02/13 12:49:08
  vpn2                            100:2                   2012/02/13 12:49:20
[PE1] ping -vpn-instance vpn1 10.1.1.1
Ping 10.1.1.1 (10.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 10.1.1.1: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=2.000 ms
56 bytes from 10.1.1.1: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 10.1.1.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 10.1.1.1: icmp_seq=4 ttl=255 time=0.000 ms

--- Ping statistics for 10.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.800/2.000/0.748 ms
```

(4)　在 PE 与 CE 之间建立 EBGP 对等体，引入 VPN 路由

配置 CE 1。

```
<CE1> system-view
[CE1] bgp 65410
[CE1-bgp] peer 10.1.1.2 as-number 100
[CE1-bgp] address-family ipv4 unicast
[CE1-bgp-ipv4] peer 10.1.1.2 enable
[CE1-bgp-ipv4] import-route direct
[CE1-bgp-ipv4] quit
[CE1-bgp] quit
```

另外 3 个 CE 设备（CE 2～CE 4）配置与 CE 1 设备配置类似，配置过程省略。

配置 PE 1。

```
[PE1] bgp 100
[PE1-bgp] ip vpn-instance vpn1
[PE1-bgp-vpn1] peer 10.1.1.1 as-number 65410
[PE1-bgp-vpn1] address-family ipv4 unicast
```

```
[PE1-bgp-ipv4-vpn1] peer 10.1.1.1 enable
[PE1-bgp-ipv4-vpn1] import-route direct
[PE1-bgp-ipv4-vpn1] quit
[PE1-bgp-vpn1] quit
[PE1-bgp] ip vpn-instance vpn2
[PE1-bgp-vpn2] peer 10.2.1.1 as-number 65420
[PE1-bgp-vpn2] address-family ipv4 unicast
[PE1-bgp-ipv4-vpn2] peer 10.2.1.1 enable
[PE1-bgp-ipv4-vpn2] import-route direct
[PE1-bgp-ipv4-vpn2] quit
[PE1-bgp-vpn1] quit
[PE1-bgp] quit
```

PE 2 的配置与 PE 1 类似，配置过程省略。

配置完成后，在 PE 设备上执行 **display bgp peer ipv4 vpn-instance** 命令，可以看到 PE 与 CE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

以 PE 1 与 CE 1 的对等体关系为例：

```
[PE1] display bgp peer ipv4 vpn-instance vpn1

 BGP local router ID: 1.1.1.9
 Local AS number: 100
 Total number of peers: 1                 Peers in established state: 1

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  10.1.1.1             65410        4        4    0       2 00:00:22 Established
```

(5) 在 PE 之间建立 MP-IBGP 对等体

配置 PE 1。

```
[PE1] bgp 100
[PE1-bgp] peer 3.3.3.9 as-number 100
[PE1-bgp] peer 3.3.3.9 connect-interface loopback 0
[PE1-bgp] address-family vpnv4
[PE1-bgp-vpnv4] peer 3.3.3.9 enable
[PE1-bgp-vpnv4] quit
[PE1-bgp] quit
```

配置 PE 2。

```
[PE2] bgp 100
[PE2-bgp] peer 1.1.1.9 as-number 100
[PE2-bgp] peer 1.1.1.9 connect-interface loopback 0
[PE2-bgp] address-family vpnv4
[PE2-bgp-vpnv4] peer 1.1.1.9 enable
[PE2-bgp-vpnv4] quit
[PE2-bgp] quit
```

配置完成后，在 PE 设备上执行 **display bgp peer vpnv4** 命令，可以看到 PE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

```
[PE1] display bgp peer vpnv4
```

```
BGP local router ID: 1.1.1.9
Local AS number: 100
Total number of peers: 1                 Peers in established state: 1

 Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

 3.3.3.9                100        3        6    0       0 00:00:32 Established
```

4. 验证配置

在 PE 设备上执行 **display ip routing-table vpn-instance** 命令，可以看到去往对端 CE 的路由。

以 PE 1 上的 VPN 1 为例：

```
[PE1] display ip routing-table vpn-instance vpn1

Destinations : 13        Routes : 13

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.1.1.0/24         Direct 0    0            10.1.1.2        GE2/1/1
10.1.1.0/32         Direct 0    0            10.1.1.2        GE2/1/1
10.1.1.2/32         Direct 0    0            127.0.0.1       InLoop0
10.1.1.255/32       Direct 0    0            10.1.1.2        GE2/1/1
10.3.1.0/24         BGP    255  0            3.3.3.9         POS2/1/0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

同一 VPN 的 CE 能够相互 Ping 通，不同 VPN 的 CE 不能相互 Ping 通。

例如：CE 1 能够 Ping 通 CE 3（10.3.1.1），但不能 Ping 通 CE 4（10.4.1.1）。

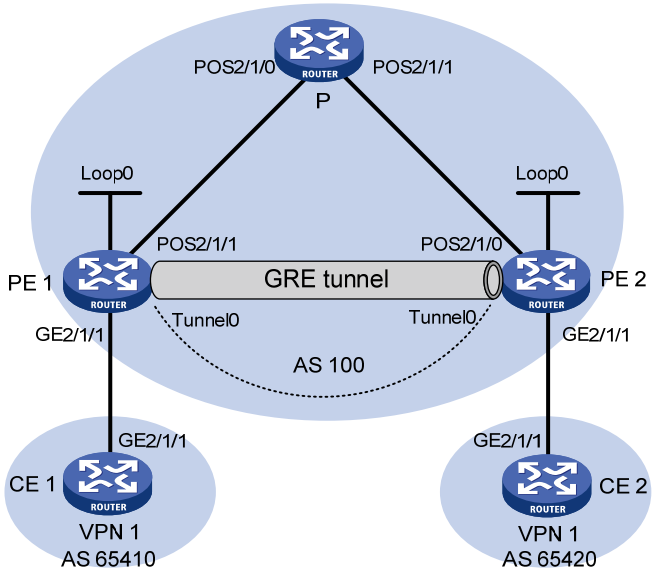
1.14.2 配置MPLS L3VPN采用GRE隧道示例

1. 组网需求

- CE 1 和 CE 2 属于 VPN 1。
- 在运营商骨干网上，PE 设备具备 MPLS 能力，P 设备只提供纯 IP 功能，不具备 MPLS 能力。
- 在骨干网上使用 GRE 隧道封装并转发 VPN 报文，实现 MPLS L3VPN。
- 在 PE 上配置隧道策略，指定 VPN 流量使用的隧道类型为 GRE。（本配置可选）

2. 组网图

图1-25 配置采用 GRE 隧道的 MPLS L3VPN 组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	GE2/1/1	10.1.1.1/24	P	POS2/1/0	172.1.1.2/24
PE 1	Loop0	1.1.1.9/32		POS2/1/1	172.2.1.1/24
	GE2/1/1	10.1.1.2/24	PE 2	Loop0	2.2.2.9/32
	POS2/1/1	172.1.1.1/24		GE2/1/1	10.2.1.2/24
	Tunnel0	20.1.1.1/24		POS2/1/0	172.2.1.2/24
CE 2	GE2/1/1	10.2.1.1/24		Tunnel0	20.1.1.2/24

3. 配置步骤

(1) 在 MPLS 骨干网上配置 IGP 协议，实现骨干网 PE 和 P 的互通

本例中采用 OSPF 发布接口（包括 Loopback 接口）所在网段的路由，具体配置过程略。

配置完成后，PE 1、P、PE 2 之间应能建立 OSPF 邻居，执行 **display ospf peer** 命令可以看到邻居达到 FULL 状态。执行 **display ip routing-table** 命令可以看到 PE 之间学习到对方的 Loopback 路由。

(2) 在 PE 设备上使能 MPLS 基本能力

配置 PE 1。

```
<PE1> system-view
[PE1] mpls lsr-id 1.1.1.9
```

配置 PE 2。

```
<PE2> system-view
[PE2] mpls lsr-id 2.2.2.9
```

(3) 在 PE 设备上配置 VPN 实例，将 CE 接入 PE，并在 PE 上应用隧道策略，指定使用 GRE 隧道转发 VPN 报文

配置 PE 1。

```
[PE1] tunnel-policy gre1
[PE1-tunnel-policy-gre1] select-seq gre load-balance-number 1
[PE1-tunnel-policy-gre1] quit
```

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 100:1
[PE1-vpn-instance-vpn1] vpn-target 100:1 both
[PE1-vpn-instance-vpn1] tnl-policy gre1
[PE1-vpn-instance-vpn1] quit
[PE1] interface gigabitethernet 2/1/1
[PE1-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE1-GigabitEthernet2/1/1] ip address 10.1.1.2 24
[PE1-GigabitEthernet2/1/1] quit
```

配置 PE 2。

```
[PE2] tunnel-policy gre1
[PE2-tunnel-policy-gre1] select-seq gre load-balance-number 1
[PE2-tunnel-policy-gre1] quit
[PE2] ip vpn-instance vpn1
[PE2-vpn-instance-vpn1] route-distinguisher 100:2
[PE2-vpn-instance-vpn1] vpn-target 100:1 both
[PE2-vpn-instance-vpn1] tnl-policy gre1
[PE2-vpn-instance-vpn1] quit
[PE2] interface gigabitethernet 2/1/1
[PE2-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE2-GigabitEthernet2/1/1] ip address 10.2.1.2 24
[PE2-GigabitEthernet2/1/1] quit
```

配置 CE 1。

```
<CE1> system-view
[CE1] interface gigabitethernet 2/1/1
[CE1-GigabitEthernet2/1/1] ip address 10.1.1.1 24
[CE1-GigabitEthernet2/1/1] quit
```

配置 CE2。

```
<CE2> system-view
[CE2] interface gigabitethernet 2/1/1
[CE2-GigabitEthernet2/1/1] ip address 10.2.1.1 24
[CE2-GigabitEthernet2/1/1] quit
```

配置完成后，在 PE 设备上执行 **display ip vpn-instance** 命令可以看到 VPN 实例的配置情况。各 PE 能 ping 通自己接入的 CE。

以 PE 1 为例：

```
[PE1] display ip vpn-instance
  Total VPN-Instances configured : 1
  VPN-Instance Name               RD                      Create time
  vpn1                            100:1                   2012/02/13 15:59:50
[PE1] ping -vpn-instance vpn1 10.1.1.1
Ping 10.1.1.1 (10.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 10.1.1.1: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 10.1.1.1: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 10.1.1.1: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 10.1.1.1: icmp_seq=4 ttl=255 time=0.000 ms
```

```
--- Ping statistics for 10.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.200/1.000/0.400 ms
```

(4) 在 PE 与 CE 之间建立 EBGP 对等体，引入 VPN 路由

配置 CE 1。

```
[CE1] bgp 65410
[CE1-bgp] peer 10.1.1.2 as-number 100
[CE1-bgp] address-family ipv4 unicast
[CE1-bgp-ipv4] peer 10.1.1.2 enable
[CE1-bgp-ipv4] import-route direct
[CE1-bgp-ipv4] quit
[CE1-bgp] quit
```

配置 PE 1。

```
[PE1] bgp 100
[PE1-bgp] ip vpn-instance vpn1
[PE1-bgp-vpn1] peer 10.1.1.1 as-number 65410
[PE1-bgp-vpn1] address-family ipv4 unicast
[PE1-bgp-ipv4-vpn1] peer 10.1.1.1 enable
[PE1-bgp-ipv4-vpn1] peer 10.1.1.1 next-hop-local
[PE1-bgp-ipv4-vpn1] import-route direct
[PE1-bgp-ipv4-vpn1] quit
[PE1-bgp-vpn1] quit
[PE1-bgp] quit
```

CE 2 的配置与 CE 1 类似，PE 2 的配置与 PE 1 类似，配置过程省略。

配置完成后，在 PE 设备上执行 **display bgp peer ipv4 vpn-instance** 命令，可以看到 PE 与 CE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

以 PE 1 为例：

```
[PE1] display bgp peer ipv4 vpn-instance vpn1

 BGP local router ID: 1.1.1.9
 Local AS number: 100
 Total number of peers: 1                 Peers in established state: 1

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  10.1.1.1             65410        4        4    0       2 00:00:13 Established
```

(5) 在 PE 之间建立 MP-IBGP 对等体

配置 PE 1。

```
[PE1] bgp 100
[PE1-bgp] peer 2.2.2.9 as-number 100
[PE1-bgp] peer 2.2.2.9 connect-interface loopback 0
[PE1-bgp] address-family vpnv4
[PE1-bgp-vpnv4] peer 2.2.2.9 enable
[PE1-bgp-vpnv4] quit
[PE1-bgp] quit
```

PE 2 的配置与 PE 1 类似，配置过程省略。

配置完成后，在 PE 设备上执行 **display bgp peer vpnv4** 命令，可以看到 PE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

```
[PE1] display bgp peer vpnv4

 BGP local router ID: 1.1.1.9
 Local AS number: 100
 Total number of peers: 1                 Peers in established state: 1

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  2.2.2.9                100        5        7    0       2 00:00:43 Established
```

(6) 配置 GRE 隧道

配置 PE 1。

```
[PE1] interface tunnel 0 mode gre
[PE1-Tunnel0] source loopback 0
[PE1-Tunnel0] destination 2.2.2.9
[PE1-Tunnel0] ip address 20.1.1.1 24
[PE1-Tunnel0] mpls enable
[PE1-Tunnel0] quit
```

配置 PE 2。

```
[PE2] interface tunnel 0 mode gre
[PE2-Tunnel0] source loopback 0
[PE2-Tunnel0] destination 1.1.1.9
[PE2-Tunnel0] ip address 20.1.1.2 24
[PE2-Tunnel0] mpls enable
[PE2-Tunnel0] quit
```

4. 验证配置

配置完成后，CE 能学到对端 CE 的接口路由。以 CE 1 为例：

```
[CE1] display ip routing-table

Destinations : 13        Routes : 13

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.1.1.0/24         Direct 0    0            10.1.1.1        GE2/1/1
10.1.1.0/32         Direct 0    0            10.1.1.1        GE2/1/1
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.1.1.255/32       Direct 0    0            10.1.1.1        GE2/1/1
10.2.1.0/24         BGP    255  0            10.1.1.2        GE2/1/1
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

CE 1 和 CE 2 之间能够 ping 通。

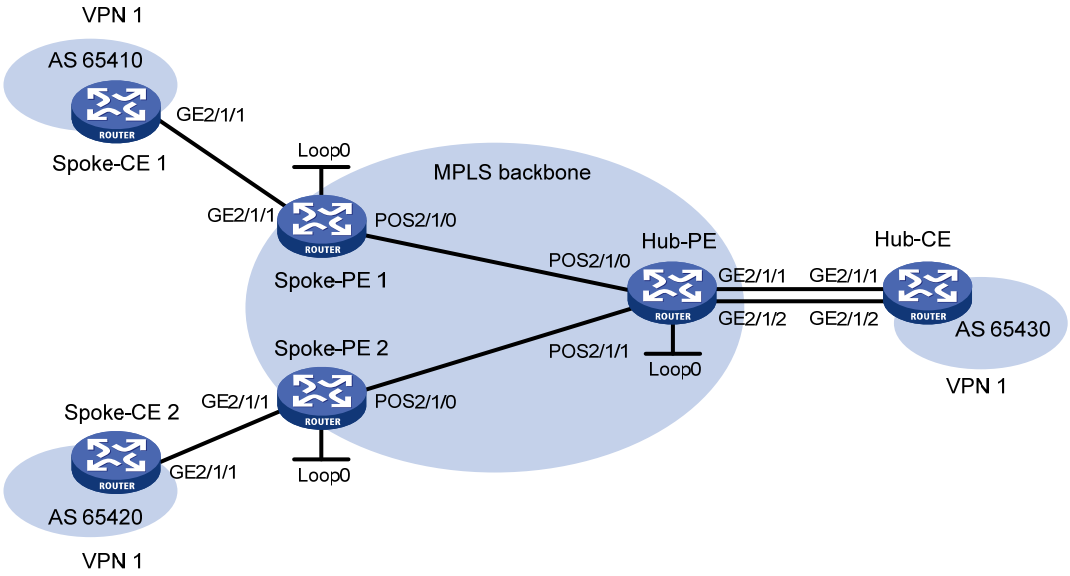
1.14.3 配置Hub&Spoke组网示例

1. 组网需求

- Spoke-CE 之间不能直接通信，只能通过 Hub-CE 转发 Spoke-CE 之间的流量。
- Spoke-CE 与 Spoke-PE 之间、Hub-CE 与 Hub-PE 之间配置 EBGP 交换 VPN 路由信息。
- Spoke-PE 与 Hub-PE 之间配置 OSPF 实现 PE 内部的互通、配置 MP-IBGP 交换 VPN 路由信息。

2. 组网图

图1-26 Hub&Spoke 组网图



设备	接口	IP地址	设备	接口	IP地址
Spoke-CE 1	GE2/1/1	10.1.1.1/24	Hub-CE	GE2/1/1	10.3.1.1/24
Spoke-PE 1	Loop0	1.1.1.9/32		GE2/1/2	10.4.1.1/24
	GE2/1/1	10.1.1.2/24	Hub-PE	Loop0	2.2.2.9/32
	POS2/1/0	172.1.1.1/24		POS2/1/0	172.1.1.2/24
Spoke-CE 2	GE2/1/1	10.2.1.1/24		POS2/1/1	172.2.1.2/24
Spoke-PE 2	Loop0	3.3.3.9/32		GE2/1/1	10.3.1.2/24
	GE2/1/1	10.2.1.2/24		GE2/1/2	10.4.1.2/24
	POS2/1/0	172.2.1.1/24			

3. 配置步骤

(1) 在 MPLS 骨干网上配置 IGP 协议，实现骨干网 Spoke-PE、Hub-PE 之间的互通

配置 Spoke-PE 1。

```
<Spoke-PE1> system-view
[Spoke-PE1] interface loopback 0
[Spoke-PE1-LoopBack0] ip address 1.1.1.9 32
[Spoke-PE1-LoopBack0] quit
[Spoke-PE1] interface pos 2/1/0
[Spoke-PE1-Pos2/1/0] ip address 172.1.1.1 24
[Spoke-PE1-Pos2/1/0] quit
```

```
[Spoke-PE1] ospf
[Spoke-PE1-ospf-1] area 0
[Spoke-PE1-ospf-1-area-0.0.0.0] network 172.1.1.0 0.0.0.255
[Spoke-PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[Spoke-PE1-ospf-1-area-0.0.0.0] quit
[Spoke-PE1-ospf-1] quit
```

配置 Spoke-PE 2。

```
<Spoke-PE2> system-view
[Spoke-PE2] interface loopback 0
[Spoke-PE2-LoopBack0] ip address 3.3.3.9 32
[Spoke-PE2-LoopBack0] quit
[Spoke-PE2] interface pos 2/1/0
[Spoke-PE2-Pos2/1/0] ip address 172.2.1.1 24
[Spoke-PE2-Pos2/1/0] quit
[Spoke-PE2] ospf
[Spoke-PE2-ospf-1] area 0
[Spoke-PE2-ospf-1-area-0.0.0.0] network 172.2.1.0 0.0.0.255
[Spoke-PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[Spoke-PE2-ospf-1-area-0.0.0.0] quit
[Spoke-PE2-ospf-1] quit
```

配置 Hub-PE。

```
<Hub-PE> system-view
[Hub-PE] interface loopback 0
[Hub-PE-LoopBack0] ip address 2.2.2.9 32
[Hub-PE-LoopBack0] quit
[Hub-PE] interface pos 2/1/0
[Hub-PE-Pos2/1/0] ip address 172.1.1.2 24
[Hub-PE-Pos2/1/0] quit
[Hub-PE] interface pos 2/1/1
[Hub-PE-Pos2/1/1] ip address 172.2.1.2 24
[Hub-PE-Pos2/1/1] quit
[Hub-PE] ospf
[Hub-PE-ospf-1] area 0
[Hub-PE-ospf-1-area-0.0.0.0] network 172.1.1.0 0.0.0.255
[Hub-PE-ospf-1-area-0.0.0.0] network 172.2.1.0 0.0.0.255
[Hub-PE-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[Hub-PE-ospf-1-area-0.0.0.0] quit
[Hub-PE-ospf-1] quit
```

配置完成后，Spoke-PE 1、Spoke-PE 2、Hub-PE 之间应能建立 OSPF 邻居，执行 **display ospf peer** 命令可以看到邻居达到 Full 状态。执行 **display ip routing-table** 命令可以看到 PE 之间学习到对方的 Loopback 路由。

(2) 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP

配置 Spoke-PE 1。

```
[Spoke-PE1] mpls lsr-id 1.1.1.9
[Spoke-PE1] mpls ldp
[Spoke-PE1-ldp] quit
[Spoke-PE1] interface pos 2/1/0
```

```
[Spoke-PE1-Pos2/1/0] mpls enable
[Spoke-PE1-Pos2/1/0] mpls ldp enable
[Spoke-PE1-Pos2/1/0] quit
```

配置 Spoke-PE 2。

```
[Spoke-PE2] mpls lsr-id 3.3.3.9
[Spoke-PE2] mpls ldp
[Spoke-PE2-ldp] quit
[Spoke-PE2] interface pos 2/1/0
[Spoke-PE2-Pos2/1/0] mpls enable
[Spoke-PE2-Pos2/1/0] mpls ldp enable
[Spoke-PE2-Pos2/1/0] quit
```

配置 Hub-PE。

```
[Hub-PE] mpls lsr-id 2.2.2.9
[Hub-PE] mpls ldp
[Hub-PE-ldp] quit
[Hub-PE] interface pos 2/1/0
[Hub-PE-Pos2/1/0] mpls enable
[Hub-PE-Pos2/1/0] mpls ldp enable
[Hub-PE-Pos2/1/0] quit
[Hub-PE] interface pos 2/1/1
[Hub-PE-Pos2/1/1] mpls enable
[Hub-PE-Pos2/1/1] mpls ldp enable
[Hub-PE-Pos2/1/1] quit
```

上述配置完成后，Spoke-PE 1、Spoke-PE 2、Hub-PE 之间应能建立 LDP 会话，执行 **display mpls ldp peer** 命令可以看到 LDP 会话的状态为 Operational。执行 **display mpls ldp lsp** 命令，可以看到 LDP LSP 的建立情况。

(3) 在 Spoke-PE 和 Hub-PE 设备上配置 VPN 实例，将 CE 接入 PE

配置 Spoke-PE 1。

```
[Spoke-PE1] ip vpn-instance vpn1
[Spoke-PE1-vpn-instance-vpn1] route-distinguisher 100:1
[Spoke-PE1-vpn-instance-vpn1] vpn-target 111:1 import-extcommunity
[Spoke-PE1-vpn-instance-vpn1] vpn-target 222:2 export-extcommunity
[Spoke-PE1-vpn-instance-vpn1] quit
[Spoke-PE1] interface gigabitethernet 2/1/1
[Spoke-PE1-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[Spoke-PE1-GigabitEthernet2/1/1] ip address 10.1.1.2 24
[Spoke-PE1-GigabitEthernet2/1/1] quit
```

配置 Spoke-PE 2。

```
[Spoke-PE2] ip vpn-instance vpn1
[Spoke-PE2-vpn-instance-vpn1] route-distinguisher 100:2
[Spoke-PE2-vpn-instance-vpn1] vpn-target 111:1 import-extcommunity
[Spoke-PE2-vpn-instance-vpn1] vpn-target 222:2 export-extcommunity
[Spoke-PE2-vpn-instance-vpn1] quit
[Spoke-PE2] interface gigabitethernet 2/1/1
[Spoke-PE2-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[Spoke-PE2-GigabitEthernet2/1/1] ip address 10.2.1.2 24
[Spoke-PE2-GigabitEthernet2/1/1] quit
```

配置 Hub-PE。

```
[Hub-PE] ip vpn-instance vpn1-in
[Hub-PE-vpn-instance-vpn1-in] route-distinguisher 100:3
[Hub-PE-vpn-instance-vpn1-in] vpn-target 222:2 import-extcommunity
[Hub-PE-vpn-instance-vpn1-in] quit
[Hub-PE] ip vpn-instance vpn1-out
[Hub-PE-vpn-instance-vpn1-out] route-distinguisher 100:4
[Hub-PE-vpn-instance-vpn1-out] vpn-target 111:1 export-extcommunity
[Hub-PE-vpn-instance-vpn1-out] quit
[Hub-PE] interface gigabitethernet 2/1/1
[Hub-PE-GigabitEthernet2/1/1] ip binding vpn-instance vpn1-in
[Hub-PE-GigabitEthernet2/1/1] ip address 10.3.1.2 24
[Hub-PE-GigabitEthernet2/1/1] quit
[Hub-PE] interface gigabitethernet 2/1/2
[Hub-PE-GigabitEthernet2/1/2] ip binding vpn-instance vpn1-out
[Hub-PE-GigabitEthernet2/1/2] ip address 10.4.1.2 24
[Hub-PE-GigabitEthernet2/1/2] quit
```

按 图 1-26 配置各CE的接口IP地址，配置过程略。

配置完成后，在 PE 设备上执行 **display ip vpn-instance** 命令可以看到 VPN 实例的配置情况。各 PE 能 ping 通自己接入的 CE。

以 Spoke-PE 1 和 Spoke-CE 1 为例：

```
[Spoke-PE1] display ip vpn-instance
  Total VPN-Instances configured : 1

  VPN-Instance Name               RD                      Create time
  vpn1                            100:1                   2009/04/08 10:55:07
[Spoke-PE1] ping -vpn-instance vpn1 10.1.1.1
Ping 10.1.1.1 (10.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 10.1.1.1: icmp_seq=0 ttl=128 time=1.913 ms
56 bytes from 10.1.1.1: icmp_seq=1 ttl=128 time=2.381 ms
56 bytes from 10.1.1.1: icmp_seq=2 ttl=128 time=1.707 ms
56 bytes from 10.1.1.1: icmp_seq=3 ttl=128 time=1.666 ms
56 bytes from 10.1.1.1: icmp_seq=4 ttl=128 time=2.710 ms

--- Ping statistics for 10.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.666/2.075/2.710/0.406 ms
```

(4) 在 PE 与 CE 之间建立 EBGP 对等体，引入 VPN 路由

配置 Spoke-CE 1。

```
<Spoke-CE1> system-view
[Spoke-CE1] bgp 65410
[Spoke-CE1-bgp] peer 10.1.1.2 as-number 100
[Spoke-CE1-bgp] address-family ipv4
[Spoke-CE1-bgp-ipv4] peer 10.1.1.2 enable
[Spoke-CE1-bgp-ipv4] import-route direct
[Spoke-CE1-bgp-ipv4] quit
[Spoke-CE1-bgp] quit
```

配置 Spoke-CE 2。

```
<Spoke-CE2> system-view
[Spoke-CE2] bgp 65420
[Spoke-CE2-bgp] peer 10.2.1.2 as-number 100
[Spoke-CE2-bgp] address-family ipv4
[Spoke-CE2-bgp-ipv4] peer 10.2.1.2 enable
[Spoke-CE2-bgp-ipv4] import-route direct
[Spoke-CE2-bgp-ipv4] quit
[Spoke-CE2-bgp] quit
```

配置 Hub-CE。

```
<Hub-CE> system-view
[Hub-CE] bgp 65430
[Hub-CE-bgp] peer 10.3.1.2 as-number 100
[Hub-CE-bgp] peer 10.4.1.2 as-number 100
[Hub-CE-bgp] address-family ipv4
[Hub-CE-bgp-ipv4] peer 10.3.1.2 enable
[Hub-CE-bgp-ipv4] peer 10.4.1.2 enable
[Hub-CE-bgp-ipv4] import-route direct
[Hub-CE-bgp-ipv4] quit
[Hub-CE-bgp] quit
```

配置 Spoke-PE 1。

```
[Spoke-PE1] bgp 100
[Spoke-PE1-bgp] ip vpn-instance vpn1
[Spoke-PE1-bgp-vpn1] peer 10.1.1.1 as-number 65410
[Spoke-PE1-bgp-vpn1] address-family ipv4
[Spoke-PE1-bgp-ipv4-vpn1] peer 10.1.1.1 enable
[Spoke-PE1-bgp-ipv4-vpn1] import-route direct
[Spoke-PE1-bgp-ipv4-vpn1] quit
[Spoke-PE1-bgp-vpn1] quit
[Spoke-PE1-bgp] quit
```

配置 Spoke-PE 2。

```
[Spoke-PE2] bgp 100
[Spoke-PE2-bgp] ip vpn-instance vpn1
[Spoke-PE2-bgp-vpn1] peer 10.2.1.1 as-number 65420
[Spoke-PE2-bgp-vpn1] address-family ipv4
[Spoke-PE2-bgp-ipv4-vpn1] peer 10.2.1.1 enable
[Spoke-PE2-bgp-ipv4-vpn1] import-route direct
[Spoke-PE2-bgp-ipv4-vpn1] quit
[Spoke-PE2-bgp-vpn1] quit
[Spoke-PE2-bgp] quit
```

配置 Hub-PE。

```
[Hub-PE] bgp 100
[Hub-PE-bgp] ip vpn-instance vpn1-in
[Hub-PE-bgp-vpn1-in] peer 10.3.1.1 as-number 65430
[Hub-PE-bgp-vpn1-in] address-family ipv4
[Hub-PE-bgp-ipv4-vpn1-in] peer 10.3.1.1 enable
[Hub-PE-bgp-ipv4-vpn1-in] import-route direct
```

```
[Hub-PE-bgp-ipv4-vpn1-in] quit
[Hub-PE-bgp-vpn1-in] quit
[Hub-PE-bgp] ip vpn-instance vpn1-out
[Hub-PE-bgp-vpn1-out] peer 10.4.1.1 as-number 65430
[Hub-PE-bgp-vpn1-out] address-family ipv4
[Hub-PE-bgp-ipv4-vpn1-out] peer 10.4.1.1 enable
[Hub-PE-bgp-ipv4-vpn1-out] import-route direct
[Hub-PE-bgp-ipv4-vpn1-out] quit
[Hub-PE-bgp-vpn1-out] quit
[Hub-PE-bgp] quit
```

配置完成后，在 PE 设备上执行 **display bgp peer ipv4 vpn-instance** 命令，可以看到 PE 与 CE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

(5) 在 Spoke-PE 和 Hub-PE 之间建立 MP-IBGP 对等体

配置 Spoke-PE 1。

```
[Spoke-PE1] bgp 100
[Spoke-PE1-bgp] peer 2.2.2.9 as-number 100
[Spoke-PE1-bgp] peer 2.2.2.9 connect-interface loopback 0
[Spoke-PE1-bgp] address-family vpnv4
[Spoke-PE1-bgp-vpnv4] peer 2.2.2.9 enable
[Spoke-PE1-bgp-vpnv4] quit
[Spoke-PE1-bgp] quit
```

配置 Spoke-PE 2。

```
[Spoke-PE2] bgp 100
[Spoke-PE2-bgp] peer 2.2.2.9 as-number 100
[Spoke-PE2-bgp] peer 2.2.2.9 connect-interface loopback 0
[Spoke-PE2-bgp] address-family vpnv4
[Spoke-PE2-bgp-vpnv4] peer 2.2.2.9 enable
[Spoke-PE2-bgp-vpnv4] quit
[Spoke-PE2-bgp] quit
```

配置 Hub-PE。

```
[Hub-PE] bgp 100
[Hub-PE-bgp] peer 1.1.1.9 as-number 100
[Hub-PE-bgp] peer 1.1.1.9 connect-interface loopback 0
[Hub-PE-bgp] peer 3.3.3.9 as-number 100
[Hub-PE-bgp] peer 3.3.3.9 connect-interface loopback 0
[Hub-PE-bgp] address-family vpnv4
[Hub-PE-bgp-vpnv4] peer 1.1.1.9 enable
[Hub-PE-bgp-vpnv4] peer 3.3.3.9 enable
[Hub-PE-bgp-vpnv4] quit
[Hub-PE-bgp] quit
```

配置完成后，在 PE 设备上执行 **display bgp peer vpnv4** 命令，可以看到 PE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

4. 验证配置

在 PE 设备上执行 **display ip routing-table vpn-instance** 命令，可以看到去往各个 CE 的路由，且 Spoke-PE 上到达对端 Spoke-CE 的路由指向 Hub-PE。以 Spoke-PE 1 为例：

```
[Spoke-PE1] display ip routing-table vpn-instance vpn1
```

```
Routing Tables: vpn1
         Destinations : 8        Routes : 8

Destination/Mask    Proto   Pre  Cost         NextHop         Interface

10.0.0.0/24         BGP     255  0            2.2.2.9         NULL0
10.1.1.0/24         Direct  0    0            10.1.1.2        GE2/1/1
10.1.1.2/32         Direct  0    0            127.0.0.1       InLoop0
10.2.1.0/24         BGP     255  0            2.2.2.9         NULL0
10.3.1.0/24         BGP     255  0            2.2.2.9         NULL0
10.4.1.0/24         BGP     255  0            2.2.2.9         NULL0
127.0.0.0/8         Direct  0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0            127.0.0.1       InLoop0
```

Spoke-CE 1 和 Spoke-CE 2 之间可以 ping 通。从 TTL 值可以推算出 Spoke-CE 1 到 Spoke-CE 2 经过 6 跳（255-250+1），即 Spoke-CE 1 和 Spoke-CE 2 之间的流量需要通过 Hub-CE 转发。以 Spoke-CE 1 为例：

```
[Spoke-CE1] ping 10.2.1.1
Ping 10.2.1.1 (10.2.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 10.2.1.1: icmp_seq=0 ttl=250 time=1.000 ms
56 bytes from 10.2.1.1: icmp_seq=1 ttl=250 time=2.000 ms
56 bytes from 10.2.1.1: icmp_seq=2 ttl=250 time=0.000 ms
56 bytes from 10.2.1.1: icmp_seq=3 ttl=250 time=1.000 ms
56 bytes from 10.2.1.1: icmp_seq=4 ttl=250 time=0.000 ms

--- Ping statistics for 10.2.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.800/2.000/0.748 ms
```

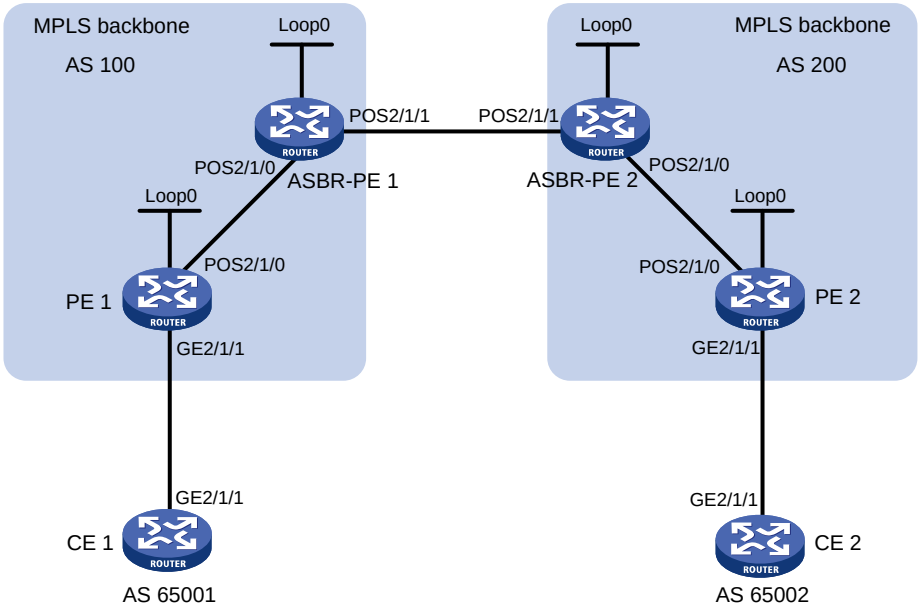
1.14.4 配置跨域VPN-OptionA方式示例

1. 组网需求

- CE 1 和 CE 2 属于同一个 VPN。
- CE 1 通过 AS 100 的 PE 1 接入，CE 2 通过 AS 200 的 PE 2 接入。
- 采用 OptionA 方式实现跨域的 MPLS L3VPN，即，采用 VRF-to-VRF 方式管理 VPN 路由。
- 同一个 AS 内部的 MPLS 骨干网使用 OSPF 作为 IGP。

2. 组网图

图1-27 配置跨域 VPN-OptionA 方式组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	GE2/1/1	10.1.1.1/24	CE 2	GE2/1/1	10.2.1.1/24
PE 1	Loop0	1.1.1.9/32	PE 2	Loop0	4.4.4.9/32
	GE2/1/1	10.1.1.2/24		GE2/1/1	10.2.1.2/24
	POS2/1/0	172.1.1.2/24		POS2/1/0	162.1.1.2/24
ASBR-PE1	Loop0	2.2.2.9/32	ASBR-PE2	Loop0	3.3.3.9/32
	POS2/1/0	172.1.1.1/24		POS2/1/0	162.1.1.1/24
	POS2/1/1	192.1.1.1/24		POS2/1/1	192.1.1.2/24

3. 配置步骤

(1) 在 MPLS 骨干网上配置 IGP 协议，实现骨干网内互通

本例中采用 OSPF 发布接口（包括 Loopback 接口）所在网段的路由，具体配置步骤略。

配置完成后，ASBR-PE 与本 AS 的 PE 之间应能建立 OSPF 邻居，执行 **display ospf peer** 命令可以看到邻居达到 FULL 状态，PE 之间能学习到对方的 Loopback 地址。

ASBR-PE 与本 AS 的 PE 之间能够互相 ping 通。

(2) 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP

配置 PE 1 的 MPLS 基本能力，并在与 ASBR-PE 1 相连的接口上使能 LDP。

```
<PE1> system-view
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] interface pos 2/1/0
[PE1-Pos2/1/0] mpls enable
[PE1-Pos2/1/0] mpls ldp enable
[PE1-Pos2/1/0] quit
```

配置 ASBR-PE 1 的 MPLS 基本能力，并在与 PE 1 相连的接口上使能 LDP。

```
<ASBR-PE1> system-view
```

```
[ASBR-PE1] mpls lsr-id 2.2.2.9
[ASBR-PE1] mpls ldp
[ASBR-PE1-ldp] quit
[ASBR-PE1] interface pos 2/1/0
[ASBR-PE1-Pos2/1/0] mpls enable
[ASBR-PE1-Pos2/1/0] mpls ldp enable
[ASBR-PE1-Pos2/1/0] quit
```

配置 ASBR-PE 2 的 MPLS 基本能力，并在与 PE 2 相连的接口上使能 LDP。

```
<ASBR-PE2> system-view
[ASBR-PE2] mpls lsr-id 3.3.3.9
[ASBR-PE2] mpls ldp
[ASBR-PE2-ldp] quit
[ASBR-PE2] interface pos 2/1/0
[ASBR-PE2-Pos2/1/0] mpls enable
[ASBR-PE2-Pos2/1/0] mpls ldp enable
[ASBR-PE2-Pos2/1/0] quit
```

配置 PE 2 的 MPLS 基本能力，并在与 ASBR-PE 2 相连的接口上使能 LDP。

```
<PE2> system-view
[PE2] mpls lsr-id 4.4.4.9
[PE2] mpls ldp
[PE2-ldp] quit
[PE2] interface pos 2/1/0
[PE2-Pos2/1/0] mpls enable
[PE2-Pos2/1/0] mpls ldp enable
[PE2-Pos2/1/0] quit
```

上述配置完成后，同一 AS 的 PE 和 ASBR-PE 之间应该建立起 LDP 邻居，在各设备上执行 **display mpls ldp peer** 命令可以看到 LDP 会话状态为“Operational”。

(3) 在 PE 设备上配置 VPN 实例，将 CE 接入 PE

说明

同一 AS 内的 ASBR-PE 与 PE 的 VPN 实例的 VPN Target 应能匹配，不同 AS 的 PE 的 VPN 实例的 VPN Target 则不需要匹配。

配置 CE 1。

```
<CE1> system-view
[CE1] interface gigabitethernet 2/1/1
[CE1-GigabitEthernet2/1/1] ip address 10.1.1.1 24
[CE1-GigabitEthernet2/1/1] quit
```

配置 PE 1。

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 100:1
[PE1-vpn-instance-vpn1] vpn-target 100:1 both
[PE1-vpn-instance-vpn1] quit
[PE1] interface gigabitethernet 2/1/1
[PE1-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
```

```
[PE1-GigabitEthernet2/1/1] ip address 10.1.1.2 24
[PE1-GigabitEthernet2/1/1] quit
```

配置 CE 2。

```
<CE2> system-view
[CE2] interface gigabitethernet 2/1/1
[CE2-GigabitEthernet2/1/1] ip address 10.2.1.1 24
[CE2-GigabitEthernet2/1/1] quit
```

配置 PE 2。

```
[PE2] ip vpn-instance vpn1
[PE2-vpn-instance-vpn1] route-distinguisher 200:2
[PE2-vpn-instance-vpn1] vpn-target 200:1 both
[PE2-vpn-instance-vpn1] quit
[PE2] interface gigabitethernet 2/1/1
[PE2-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE2-GigabitEthernet2/1/1] ip address 10.2.1.2 24
[PE2-GigabitEthernet2/1/1] quit
```

配置 ASBR-PE 1：创建 VPN 实例，并将此实例绑定到连接 ASBR-PE 2 的接口（ASBR-PE 1 认为 ASBR-PE 2 是自己的 CE）。

```
[ASBR-PE1] ip vpn-instance vpn1
[ASBR-PE1-vpn-vpn1] route-distinguisher 100:1
[ASBR-PE1-vpn-vpn1] vpn-target 100:1 both
[ASBR-PE1-vpn-vpn1] quit
[ASBR-PE1] interface pos 2/1/1
[ASBR-PE1-Pos2/1/1] ip binding vpn-instance vpn1
[ASBR-PE1-Pos2/1/1] ip address 192.1.1.1 24
[ASBR-PE1-Pos2/1/1] quit
```

配置 ASBR-PE 2：创建 VPN 实例，并将此实例绑定到连接 ASBR-PE 1 的接口（ASBR-PE 2 认为 ASBR-PE 1 是自己的 CE）。

```
[ASBR-PE2] ip vpn-instance vpn1
[ASBR-PE2-vpn-vpn1] route-distinguisher 200:1
[ASBR-PE2-vpn-vpn1] vpn-target 200:1 both
[ASBR-PE2-vpn-vpn1] quit
[ASBR-PE2] interface pos 2/1/1
[ASBR-PE2-Pos2/1/1] ip binding vpn-instance vpn1
[ASBR-PE2-Pos2/1/1] ip address 192.1.1.2 24
[ASBR-PE2-Pos2/1/1] quit
```

上述配置完成后，在各 PE 设备上执行 **display ip vpn-instance** 命令能正确显示 VPN 实例配置。各 PE 能 ping 通各自的 CE。ASBR-PE 之间也能互相 ping 通。

(4) 在 PE 与 CE 之间建立 EBGP 对等体，引入 VPN 路由

配置 CE 1。

```
[CE1] bgp 65001
[CE1-bgp] peer 10.1.1.2 as-number 100
[CE1-bgp] address-family ipv4 unicast
[CE1-bgp-ipv4] peer 10.1.1.2 enable
[CE1-bgp-ipv4] import-route direct
[CE1-bgp-ipv4] quit
```

```
[CE1-bgp] quit
```

配置 PE 1。

```
[PE1] bgp 100
[PE1-bgp] ip vpn-instance vpn1
[PE1-bgp-vpn1] peer 10.1.1.1 as-number 65001
[PE1-bgp-vpn1] address-family ipv4 unicast
[PE1-bgp-ipv4-vpn1] peer 10.1.1.1 enable
[PE1-bgp-ipv4-vpn1] quit
[PE1-bgp-vpn1] quit
[PE1-bgp] quit
```

配置 CE 2。

```
[CE2] bgp 65002
[CE2-bgp] peer 10.2.1.2 as-number 200
[CE2-bgp] address-family ipv4 unicast
[CE2-bgp-ipv4] peer 10.2.1.2 enable
[CE2-bgp-ipv4] import-route direct
[CE2-bgp-ipv4] quit
[CE2-bgp] quit
```

配置 PE 2。

```
[PE2] bgp 200
[PE2-bgp] ip vpn-instance vpn1
[PE2-bgp-vpn1] peer 10.2.1.1 as-number 65002
[PE2-bgp-vpn1] address-family ipv4 unicast
[PE2-bgp-ipv4-vpn1] peer 10.2.1.1 enable
[PE2-bgp-ipv4-vpn1] quit
[PE2-bgp-vpn1] quit
[PE2-bgp] quit
```

(5) PE 与本 AS 的 ASBR-PE 之间建立 MP-IBGP 对等体，ASBR-PE 之间建立 EBGP 对等体

配置 PE 1。

```
[PE1] bgp 100
[PE1-bgp] peer 2.2.2.9 as-number 100
[PE1-bgp] peer 2.2.2.9 connect-interface loopback 0
[PE1-bgp] address-family vpnv4
[PE1-bgp-vpnv4] peer 2.2.2.9 enable
[PE1-bgp-vpnv4] peer 2.2.2.9 next-hop-local
[PE1-bgp-vpnv4] quit
[PE1-bgp] quit
```

配置 ASBR-PE 1。

```
[ASBR-PE1] bgp 100
[ASBR-PE1-bgp] ip vpn-instance vpn1
[ASBR-PE1-bgp-vpn1] peer 192.1.1.2 as-number 200
[ASBR-PE1-bgp-vpn1] address-family ipv4 unicast
[ASBR-PE1-bgp-ipv4-vpn1] peer 192.1.1.2 enable
[ASBR-PE1-bgp-ipv4-vpn1] quit
[ASBR-PE1-bgp-vpn1] quit
[ASBR-PE1-bgp] peer 1.1.1.9 as-number 100
[ASBR-PE1-bgp] peer 1.1.1.9 connect-interface loopback 0
```

```
[ASBR-PE1-bgp] address-family vpnv4
[ASBR-PE1-bgp-vpnv4] peer 1.1.1.9 enable
[ASBR-PE1-bgp-vpnv4] peer 1.1.1.9 next-hop-local
[ASBR-PE1-bgp-vpnv4] quit
[ASBR-PE1-bgp] quit
```

配置 ASBR-PE 2。

```
[ASBR-PE2] bgp 200
[ASBR-PE2-bgp] ip vpn-instance vpn1
[ASBR-PE2-bgp-vpn1] peer 192.1.1.1 as-number 100
[ASBR-PE2-bgp-vpn1] address-family ipv4 unicast
[ASBR-PE2-bgp-ipv4-vpn1] peer 192.1.1.1 enable
[ASBR-PE2-bgp-ipv4-vpn1] quit
[ASBR-PE2-bgp-vpn1] quit
[ASBR-PE2-bgp] peer 4.4.4.9 as-number 200
[ASBR-PE2-bgp] peer 4.4.4.9 connect-interface loopback 0
[ASBR-PE2-bgp] address-family vpnv4
[ASBR-PE2-bgp-vpnv4] peer 4.4.4.9 enable
[ASBR-PE2-bgp-vpnv4] peer 4.4.4.9 next-hop-local
[ASBR-PE2-bgp-vpnv4] quit
[ASBR-PE2-bgp] quit
```

配置 PE 2。

```
[PE2] bgp 200
[PE2-bgp] peer 3.3.3.9 as-number 200
[PE2-bgp] peer 3.3.3.9 connect-interface loopback 0
[PE2-bgp] address-family vpnv4
[PE2-bgp-vpnv4] peer 3.3.3.9 enable
[PE2-bgp-vpnv4] peer 3.3.3.9 next-hop-local
[PE2-bgp-vpnv4] quit
[PE2-bgp] quit
```

4. 验证配置

上述配置完成后，CE 之间能学习到对方的接口路由，CE 1 和 CE 2 能够相互 ping 通。

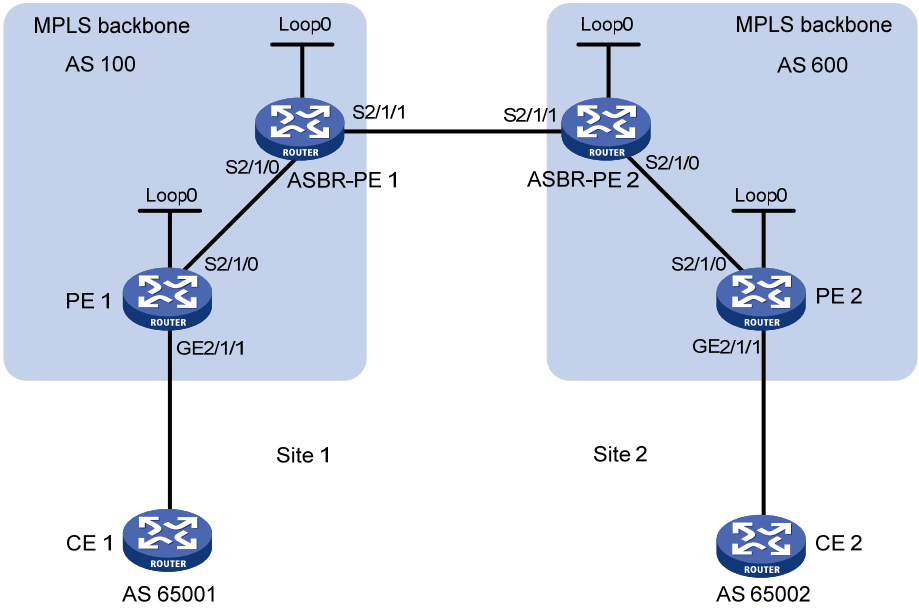
1.14.5 配置跨域VPN-OptionB方式示例

1. 组网需求

- Site 1 和 Site 2 属于同一个 VPN，Site 1 的 CE 1 通过 AS 100 的 PE 1 接入，Site 2 的 CE 2 通过 AS 600 的 PE 2 接入；
- 同一自治系统内的 PE 设备之间运行 IS-IS 作为 IGP；
- PE 1 与 ASBR-PE 1 间通过 MP-IBGP 交换 VPNv4 路由；
- PE 2 与 ASBR-PE 2 间通过 MP-IBGP 交换 VPNv4 路由；
- ASBR-PE 1 与 ASBR-PE 2 间通过 MP-EBGP 交换 VPNv4 路由；
- ASBR 上不对接收的 VPNv4 路由进行 VPN Target 过滤。

2. 组网图

图1-28 配置跨域 VPN-OptionB 方式组网图



设备	接口	IP地址	设备	接口	IP地址
PE 1	Loop0	2.2.2.9/32	PE 2	Loop0	5.5.5.9/32
	GE2/1/1	30.0.0.1/8		GE2/1/1	20.0.0.1/8
	S2/1/0	1.1.1.2/8		S2/1/0	9.1.1.2/8
ASBR-PE 1	Loop0	3.3.3.9/32	ASBR-PE 2	Loop0	4.4.4.9/32
	S2/1/0	1.1.1.1/8		S2/1/0	9.1.1.1/8
	S2/1/1	11.0.0.2/8		S2/1/1	11.0.0.1/8

3. 配置步骤

(1) 配置 PE 1

在 PE 1 上运行 IS-IS。

```
<PE1> system-view
[PE1] isis 1
[PE1-isis-1] network-entity 10.111.111.111.111.00
[PE1-isis-1] quit
```

配置 LSR ID，使能 MPLS 和 LDP。

```
[PE1] mpls lsr-id 2.2.2.9
[PE1] mpls ldp
[PE1-ldp] quit
```

配置接口 Serial2/1/0，在接口上运行 IS-IS，并使能 MPLS 和 LDP。

```
[PE1] interface serial 2/1/0
[PE1-Serial2/1/0] ip address 1.1.1.2 255.0.0.0
[PE1-Serial2/1/0] isis enable 1
[PE1-Serial2/1/0] mpls enable
[PE1-Serial2/1/0] mpls ldp enable
[PE1-Serial2/1/0] quit
```

创建 Loopback0 接口，在接口上运行 IS-IS。

```
[PE1] interface loopback 0
```

```
[PE1-LoopBack0] ip address 2.2.2.9 32
[PE1-LoopBack0] isis enable 1
[PE1-LoopBack0] quit
```

创建一个 VPN 实例，名为 vpn1，配置 RD 和 VPN Target 属性。

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 11:11
[PE1-vpn-instance-vpn1] vpn-target 1:1 2:2 3:3 import-extcommunity
[PE1-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity
[PE1-vpn-instance-vpn1] quit
```

将连接 CE 1 的接口绑定到创建的 VPN 实例。

```
[PE1] interface gigabitethernet 2/1/1
[PE1-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE1-GigabitEthernet2/1/1] ip address 30.0.0.1 8
[PE1-GigabitEthernet2/1/1] quit
```

在 PE 1 上运行 BGP。

```
[PE1] bgp 100
```

配置 IBGP 对等体 3.3.3.9 为 VPNv4 对等体。

```
[PE1-bgp] peer 3.3.3.9 as-number 100
[PE1-bgp] peer 3.3.3.9 connect-interface loopback 0
[PE1-bgp] address-family vpnv4
[PE1-bgp-vpnv4] peer 3.3.3.9 enable
[PE1-bgp-vpnv4] quit
```

将直连路由引入 vpn1 的 VPN 路由表。

```
[PE1-bgp] ip vpn-instance vpn1
[PE1-bgp-vpn1] address-family ipv4 unicast
[PE1-bgp-ipv4-vpn1] import-route direct
[PE1-bgp-ipv4-vpn1] quit
[PE1-bgp-vpn1] quit
[PE1-bgp] quit
```

(2) 配置 ASBR-PE 1

在 ASBR-PE 1 上运行 IS-IS。

```
<ASBR-PE1> system-view
[ASBR-PE1] isis 1
[ASBR-PE1-isis-1] network-entity 10.222.222.222.222.00
[ASBR-PE1-isis-1] quit
```

配置 LSR ID，使能 MPLS 和 LDP。

```
[ASBR-PE1] mpls lsr-id 3.3.3.9
[ASBR-PE1] mpls ldp
[ASBR-PE1-ldp] quit
```

配置接口 Serial2/1/0，在接口上运行 IS-IS，并使能 MPLS 和 LDP。

```
[ASBR-PE1] interface serial 2/1/0
[ASBR-PE1-Serial2/1/0] ip address 1.1.1.1 255.0.0.0
[ASBR-PE1-Serial2/1/0] isis enable 1
[ASBR-PE1-Serial2/1/0] mpls enable
[ASBR-PE1-Serial2/1/0] mpls ldp enable
[ASBR-PE1-Serial2/1/0] quit
```

配置接口 Serial2/1/1，使能 MPLS。

```
[ASBR-PE1] interface serial 2/1/1
[ASBR-PE1-Serial2/1/1] ip address 11.0.0.2 255.0.0.0
[ASBR-PE1-Serial2/1/1] mpls enable
[ASBR-PE1-Serial2/1/1] quit
```

创建 Loopback0 接口，并运行 IS-IS。

```
[ASBR-PE1] interface loopback 0
[ASBR-PE1-LoopBack0] ip address 3.3.3.9 32
[ASBR-PE1-LoopBack0] isis enable 1
[ASBR-PE1-LoopBack0] quit
```

在 ASBR-PE 1 上运行 BGP。

```
[ASBR-PE1] bgp 100
[ASBR-PE1-bgp] peer 2.2.2.9 as-number 100
[ASBR-PE1-bgp] peer 2.2.2.9 connect-interface loopback 0
[ASBR-PE1-bgp] peer 11.0.0.1 as-number 600
[ASBR-PE1-bgp] peer 11.0.0.1 connect-interface serial 2/1/1
```

不对接收的 VPNv4 路由进行 Import VPN-target 过滤。

```
[ASBR-PE1-bgp] address-family vpnv4
[ASBR-PE1-bgp-vpnv4] undo policy vpn-target
```

将 IBGP 对等体 2.2.2.9 和 EBGP 对等体 11.0.0.1 都配置为 VPNv4 对等体。

```
[ASBR-PE1-bgp-vpnv4] peer 11.0.0.1 enable
[ASBR-PE1-bgp-vpnv4] peer 2.2.2.9 enable
[ASBR-PE1-bgp-vpnv4] quit
```

(3) 配置 ASBR-PE 2

在 ASBR-PE 2 上运行 IS-IS。

```
<ASBR-PE2> system-view
[ASBR-PE2] isis 1
[ASBR-PE2-isis-1] network-entity 10.222.222.222.222.00
[ASBR-PE2-isis-1] quit
```

配置 LSR ID，使能 MPLS 和 LDP。

```
[ASBR-PE2] mpls lsr-id 4.4.4.9
[ASBR-PE2] mpls ldp
[ASBR-PE2-ldp] quit
```

配置接口 Serial2/1/0，在接口上运行 IS-IS，并使能 MPLS 和 LDP。

```
[ASBR-PE2] interface serial 2/1/0
[ASBR-PE2-Serial2/1/0] ip address 9.1.1.1 255.0.0.0
[ASBR-PE2-Serial2/1/0] isis enable 1
[ASBR-PE2-Serial2/1/0] mpls enable
[ASBR-PE2-Serial2/1/0] mpls ldp enable
[ASBR-PE2-Serial2/1/0] quit
```

配置接口 Serial2/1/1，使能 MPLS。

```
[ASBR-PE2] interface serial 2/1/1
[ASBR-PE2-Serial2/1/1] ip address 11.0.0.1 255.0.0.0
[ASBR-PE2-Serial2/1/1] mpls enable
[ASBR-PE2-Serial2/1/1] quit
```

创建 Loopback0 接口，并运行 IS-IS。

```
[ASBR-PE2] interface loopback 0
[ASBR-PE2-LoopBack0] ip address 4.4.4.9 32
[ASBR-PE2-LoopBack0] isis enable 1
[ASBR-PE2-LoopBack0] quit
```

在 ASBR-PE 2 上运行 BGP。

```
[ASBR-PE2] bgp 600
[ASBR-PE2-bgp] peer 11.0.0.2 as-number 100
[ASBR-PE2-bgp] peer 11.0.0.2 connect-interface serial 2/1/1
[ASBR-PE2-bgp] peer 5.5.5.9 as-number 600
[ASBR-PE2-bgp] peer 5.5.5.9 connect-interface loopback 0
```

不对接收的 VPNv4 路由进行 Import VPN-target 过滤。

```
[ASBR-PE2-bgp] address-family vpnv4
[ASBR-PE2-bgp-vpnv4] undo policy vpn-target
```

将 IBGP 对等体 5.5.5.9 和 EBGP 对等体 11.0.0.2 都配置为 VPNv4 对等体。

```
[ASBR-PE2-bgp-vpnv4] peer 11.0.0.2 enable
[ASBR-PE2-bgp-vpnv4] peer 5.5.5.9 enable
[ASBR-PE2-bgp-vpnv4] quit
[ASBR-PE2-bgp] quit
```

(4)　配置 PE 2

在 PE 2 上运行 IS-IS。

```
<PE2> system-view
[PE2] isis 1
[PE2-isis-1] network-entity 10.111.111.111.111.00
[PE2-isis-1] quit
```

配置 LSR ID，使能 MPLS 和 LDP。

```
[PE2] mpls lsr-id 5.5.5.9
[PE2] mpls ldp
[PE2-ldp] quit
```

配置接口 Serial2/1/0，在接口上运行 IS-IS，并使能 MPLS 和 LDP。

```
[PE2] interface serial 2/1/0
[PE2-Serial2/1/0] ip address 9.1.1.2 255.0.0.0
[PE2-Serial2/1/0] isis enable 1
[PE2-Serial2/1/0] mpls enable
[PE2-Serial2/1/0] mpls ldp enable
[PE2-Serial2/1/0] quit
```

创建 Loopback0 接口，在接口上运行 IS-IS。

```
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 5.5.5.9 32
[PE2-LoopBack0] isis enable 1
[PE2-LoopBack0] quit
```

创建一个 VPN 实例，名为 vpn1，配置 RD 和 VPN Target 属性。

```
[PE2] ip vpn-instance vpn1
[PE2-vpn-instance-vpn1] route-distinguisher 12:12
[PE2-vpn-instance-vpn1] vpn-target 1:1 2:2 3:3 import-extcommunity
[PE2-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity
```

```
[PE2-vpn-instance-vpn1] quit
```

将连接 CE 1 的接口绑定到创建的 VPN 实例。

```
[PE2] interface gigabitethernet 2/1/1
[PE2-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE2-GigabitEthernet2/1/1] ip address 20.0.0.1 8
[PE2-GigabitEthernet2/1/1] quit
```

在 PE 2 上运行 BGP。

```
[PE2] bgp 600
```

配置 IBGP 对等体 4.4.4.9 为 VPNv4 对等体。

```
[PE2-bgp] peer 4.4.4.9 as-number 600
[PE2-bgp] peer 4.4.4.9 connect-interface loopback 0
[PE2-bgp] address-family vpnv4
[PE2-bgp-vpnv4] peer 4.4.4.9 enable
[PE2-bgp-vpnv4] quit
```

将直连路由引入 vpn1 的 VPN 路由表。

```
[PE2-bgp] ip vpn-instance vpn1
[PE2-bgp-vpn1] address-family ipv4 unicast
[PE2-bgp-ipv4-vpn1] import-route direct
[PE2-bgp-ipv4-vpn1] quit
[PE2-bgp-vpn1] quit
[PE2-bgp] quit
```

4. 验证配置

配置完成后，PE 1 和 PE 2 上连接 CE 的接口 GigabitEthernet2/1/1 之间可以互相 Ping 通。以 PE 1 为例：

```
[PE1] ping -a 30.0.0.1 -vpn-instance vpn1 20.0.0.1
Ping 20.0.0.1 (20.0.0.1) from 30.0.0.1: 56 data bytes, press CTRL_C to break
56 bytes from 20.0.0.1: icmp_seq=0 ttl=255 time=1.208 ms
56 bytes from 20.0.0.1: icmp_seq=1 ttl=255 time=0.867 ms
56 bytes from 20.0.0.1: icmp_seq=2 ttl=255 time=0.551 ms
56 bytes from 20.0.0.1: icmp_seq=3 ttl=255 time=0.566 ms
56 bytes from 20.0.0.1: icmp_seq=4 ttl=255 time=0.570 ms

--- Ping statistics for 20.0.0.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.551/0.752/1.208/0.257 ms
```

1.14.6 配置跨域VPN-OptionC方式示例

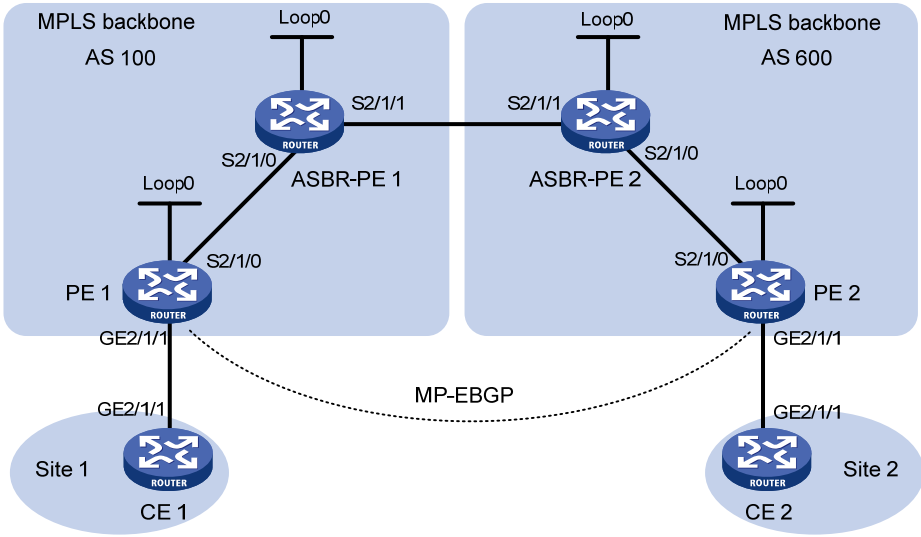
1. 组网需求

- Site 1 和 Site 2 属于同一个 VPN，Site 1 通过 AS 100 的 PE 1 接入，Site 2 通过 AS 600 的 PE 2 接入；
- 同一自治系统内的 PE 设备之间运行 IS-IS 作为 IGP；
- PE 1 与 ASBR-PE 1 间通过 IBGP 交换标签 IPv4 路由；
- PE 2 与 ASBR-PE 2 间通过 IBGP 交换标签 IPv4 路由；
- PE 1 与 PE 2 建立 MP-EBGP 对等体交换 VPNv4 路由；

- ASBR-PE 1 和 ASBR-PE 2 上分别配置路由策略，对从对方接收的路由压入标签；
- ASBR-PE 1 与 ASBR-PE 2 间通过 EBGP 交换标签 IPv4 路由。

2. 组网图

图1-29 配置跨域 VPN-OptionC 方式组网图



设备	接口	IP地址	设备	接口	IP地址
PE 1	Loop0	2.2.2.9/32	PE 2	Loop0	5.5.5.9/32
	GE2/1/1	30.0.0.1/24		GE2/1/1	20.0.0.1/24
	S2/1/0	1.1.1.2/8		S2/1/0	9.1.1.2/8
ASBR-PE 1	Loop0	3.3.3.9/32	ASBR-PE 2	Loop0	4.4.4.9/32
	S2/1/0	1.1.1.1/8		S2/1/0	9.1.1.1/8
	S2/1/1	11.0.0.2/8		S2/1/1	11.0.0.1/8
CE 1	GE2/1/1	30.0.0.2/24	CE 2	GE2/1/1	20.0.0.2/24

3. 配置步骤

(1) 配置 CE 1

配置接口 GigabitEthernet2/1/1 的 IP 地址。

```
<CE1> system-view
[CE1] interface gigabitethernet 2/1/1
[CE1-GigabitEthernet2/1/1] ip address 30.0.0.2 24
[CE1-GigabitEthernet2/1/1] quit
```

配置 CE 1 与 PE 1 建立 EBGP 对等体，并引入 VPN 路由。

```
[CE1] bgp 65001
[CE1-bgp] peer 30.0.0.1 as-number 100
[CE1-bgp] address-family ipv4 unicast
[CE1-bgp-ipv4] peer 30.0.0.1 enable
[CE1-bgp-ipv4] import-route direct
[CE1-bgp-ipv4] quit
[CE1-bgp] quit
```

(2) 配置 PE 1

在 PE 1 上运行 IS-IS。

```
<PE1> system-view
```

```
[PE1] isis 1
[PE1-isis-1] network-entity 10.111.111.111.111.00
[PE1-isis-1] quit
```
配置 LSR ID，使能 MPLS 和 LDP。
```
[PE1] mpls lsr-id 2.2.2.9
[PE1] mpls ldp
[PE1-ldp] quit
```
配置接口 Serial2/1/0，在接口上运行 IS-IS，并使能 MPLS 和 LDP。
```
[PE1] interface serial 2/1/0
[PE1-Serial2/1/0] ip address 1.1.1.2 255.0.0.0
[PE1-Serial2/1/0] isis enable 1
[PE1-Serial2/1/0] mpls enable
[PE1-Serial2/1/0] mpls ldp enable
[PE1-Serial2/1/0] quit
```
创建 Loopback0 接口，在接口上运行 IS-IS。
```
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 2.2.2.9 32
[PE1-LoopBack0] isis enable 1
[PE1-LoopBack0] quit
```
创建 VPN 实例，名称为 vpn1，为其配置 RD 和 VPN Target 属性。
```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 11:11
[PE1-vpn-instance-vpn1] vpn-target 1:1 2:2 3:3 import-extcommunity
[PE1-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity
[PE1-vpn-instance-vpn1] quit
```
配置接口 GigabitEthernet2/1/1 与 VPN 实例 vpn1 绑定，并配置该接口的 IP 地址。
```
[PE1] interface gigabitethernet 2/1/1
[PE1-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE1-GigabitEthernet2/1/1] ip address 30.0.0.1 24
[PE1-GigabitEthernet2/1/1] quit
```
在 PE 1 上运行 BGP。
```
[PE1] bgp 100
```
配置 PE 1 向 IBGP 对等体 3.3.3.9 发布标签路由及从 3.3.3.9 接收标签路由的能力。
```
[PE1-bgp] peer 3.3.3.9 as-number 100
[PE1-bgp] peer 3.3.3.9 connect-interface loopback 0
[PE1-bgp] address-family ipv4 unicast
[PE1-bgp-ipv4] peer 3.3.3.9 enable
[PE1-bgp-ipv4] peer 3.3.3.9 label-route-capability
[PE1-bgp-ipv4] quit
```
配置 PE 1 到 EBGP 对等体 5.5.5.9 的最大跳数为 10。
```
[PE1-bgp] peer 5.5.5.9 as-number 600
[PE1-bgp] peer 5.5.5.9 connect-interface loopback 0
[PE1-bgp] peer 5.5.5.9 ebgp-max-hop 10
```
配置对等体 5.5.5.9 作为 VPNv4 对等体。
```
[PE1-bgp] address-family vpnv4
[PE1-bgp-vpnv4] peer 5.5.5.9 enable
```

```
[PE1-bgp-vpnv4] quit
```
配置 PE 1 与 CE 1 建立 EBGP 对等体，将学习到的 BGP 路由添加到 VPN 实例的路由表中。
```
[PE1-bgp] ip vpn-instance vpn1
[PE1-bgp-vpn1] peer 30.0.0.2 as-number 65001
[PE1-bgp-vpn1] address-family ipv4 unicast
[PE1-bgp-ipv4-vpn1] peer 30.0.0.2 enable
[PE1-bgp-ipv4-vpn1] quit
[PE1-bgp-vpn1] quit
[PE1-bgp] quit
```
(3) 配置 ASBR-PE1

在 ASBR-PE1 上运行 IS-IS。
```
<ASBR-PE1> system-view
[ASBR-PE1] isis 1
[ASBR-PE1-isis-1] network-entity 10.222.222.222.222.00
[ASBR-PE1-isis-1] quit
```
配置 LSR ID，使能 MPLS 和 LDP。
```
[ASBR-PE1] mpls lsr-id 3.3.3.9
[ASBR-PE1] mpls ldp
[ASBR-PE1-ldp] quit
```
配置接口 Serial2/1/0，在接口上运行 IS-IS，并使能 MPLS 和 LDP。
```
[ASBR-PE1] interface serial 2/1/0
[ASBR-PE1-Serial2/1/0] ip address 1.1.1.1 255.0.0.0
[ASBR-PE1-Serial2/1/0] isis enable 1
[ASBR-PE1-Serial2/1/0] mpls enable
[ASBR-PE1-Serial2/1/0] mpls ldp enable
[ASBR-PE1-Serial2/1/0] quit
```
配置接口 Serial2/1/1，并在接口上使能 MPLS。
```
[ASBR-PE1] interface serial 2/1/1
[ASBR-PE1-Serial2/1/1] ip address 11.0.0.2 255.0.0.0
[ASBR-PE1-Serial2/1/1] mpls enable
[ASBR-PE1-Serial2/1/1] quit
```
创建 Loopback0 接口，在接口上运行 IS-IS。
```
[ASBR-PE1] interface loopback 0
[ASBR-PE1-LoopBack0] ip address 3.3.3.9 32
[ASBR-PE1-LoopBack0] isis enable 1
[ASBR-PE1-LoopBack0] quit
```
创建路由策略。
```
[ASBR-PE1] route-policy policy1 permit node 1
[ASBR-PE1-route-policy-policy1-1] apply mpls-label
[ASBR-PE1-route-policy-policy1-1] quit
[ASBR-PE1] route-policy policy2 permit node 1
[ASBR-PE1-route-policy-policy2-1] if-match mpls-label
[ASBR-PE1-route-policy-policy2-1] apply mpls-label
[ASBR-PE1-route-policy-policy2-1] quit
```
在 ASBR-PE 1 上运行 BGP，对向 IBGP 对等体 2.2.2.9 发布的路由应用已配置的路由策略 policy2。
```
[ASBR-PE1] bgp 100
```

```
[ASBR-PE1-bgp] peer 2.2.2.9 as-number 100
[ASBR-PE1-bgp] peer 2.2.2.9 connect-interface loopback 0
[ASBR-PE1-bgp] address-family ipv4 unicast
[ASBR-PE1-bgp-ipv4] peer 2.2.2.9 enable
[ASBR-PE1-bgp-ipv4] peer 2.2.2.9 route-policy policy2 export
```

向 IBGP 对等体 2.2.2.9 发布标签路由及从 2.2.2.9 接收标签路由的能力。

```
[ASBR-PE1-bgp-ipv4] peer 2.2.2.9 label-route-capability
```

引入 IS-IS 进程 1 的路由。

```
[ASBR-PE1-bgp-ipv4] import-route isis 1
[ASBR-PE1-bgp-ipv4] quit
```

对向 EBGP 对等体 11.0.0.1 发布的路由应用已配置的路由策略 policy1。

```
[ASBR-PE1-bgp] peer 11.0.0.1 as-number 600
[ASBR-PE1-bgp] address-family ipv4 unicast
[ASBR-PE1-bgp-ipv4] peer 11.0.0.1 enable
[ASBR-PE1-bgp-ipv4] peer 11.0.0.1 route-policy policy1 export
```

向 EBGP 对等体 11.0.0.1 发布标签路由及从 11.0.0.1 接收标签路由的能力。

```
[ASBR-PE1-bgp-ipv4] peer 11.0.0.1 label-route-capability
[ASBR-PE1-bgp-ipv4] quit
[ASBR-PE1-bgp] quit
```

(4) 配置 ASBR-PE 2

在 ASBR-PE 2 上运行 IS-IS。

```
<ASBR-PE2> system-view
[ASBR-PE2] isis 1
[ASBR-PE2-isis-1] network-entity 10.222.222.222.222.00
[ASBR-PE2-isis-1] quit
```

配置 LSR ID，使能 MPLS 和 LDP。

```
[ASBR-PE2] mpls lsr-id 4.4.4.9
[ASBR-PE2] mpls ldp
[ASBR-PE2-ldp] quit
```

配置接口 Serial2/1/0，在接口上运行 IS-IS，并在接口上使能 MPLS 和 LDP。

```
[ASBR-PE2] interface serial 2/1/0
[ASBR-PE2-Serial2/1/0] ip address 9.1.1.1 255.0.0.0
[ASBR-PE2-Serial2/1/0] isis enable 1
[ASBR-PE2-Serial2/1/0] mpls enable
[ASBR-PE2-Serial2/1/0] mpls ldp enable
[ASBR-PE2-Serial2/1/0] quit
```

创建 Loopback0 接口，在接口上运行 IS-IS。

```
[ASBR-PE2] interface loopback 0
[ASBR-PE2-LoopBack0] ip address 4.4.4.9 32
[ASBR-PE2-LoopBack0] isis enable 1
[ASBR-PE2-LoopBack0] quit
```

配置接口 Serial2/1/1，在接口上使能 MPLS。

```
[ASBR-PE2] interface serial 2/1/1
[ASBR-PE2-Serial2/1/1] ip address 11.0.0.1 255.0.0.0
[ASBR-PE2-Serial2/1/1] mpls enable
[ASBR-PE2-Serial2/1/1] quit
```

创建路由策略。

```
[ASBR-PE2] route-policy policy1 permit node 1
[ASBR-PE2-route-policy-policy1-1] apply mpls-label
[ASBR-PE2-route-policy-policy1-1] quit
[ASBR-PE2] route-policy policy2 permit node 1
[ASBR-PE2-route-policy-policy2-1] if-match mpls-label
[ASBR-PE2-route-policy-policy2-1] apply mpls-label
[ASBR-PE2-route-policy-policy2-1] quit
```

在 ASBR-PE 2 上运行 BGP，向 IBGP 对等体 5.5.5.9 发布标签路由及从 5.5.5.9 接收标签路由的能力。

```
[ASBR-PE2] bgp 600
[ASBR-PE2-bgp] peer 5.5.5.9 as-number 600
[ASBR-PE2-bgp] peer 5.5.5.9 connect-interface loopback 0
[ASBR-PE2-bgp] address-family ipv4 unicast
[ASBR-PE2-bgp-ipv4] peer 5.5.5.9 enable
[ASBR-PE2-bgp-ipv4] peer 5.5.5.9 label-route-capability
```

对向 IBGP 对等体 5.5.5.9 发布的路由应用已配置的路由策略 policy2。

```
[ASBR-PE2-bgp-ipv4] peer 5.5.5.9 route-policy policy2 export
```

引入 IS-IS 进程 1 的路由。

```
[ASBR-PE2-bgp-ipv4] import-route isis 1
[ASBR-PE2-bgp-ipv4] quit
```

对向 EBGP 对等体 11.0.0.2 发布的路由应用已配置的路由策略 policy1。

```
[ASBR-PE2-bgp] peer 11.0.0.2 as-number 100
[ASBR-PE2-bgp] address-family ipv4 unicast
[ASBR-PE2-bgp-ipv4] peer 11.0.0.2 enable
[ASBR-PE2-bgp-ipv4] peer 11.0.0.2 route-policy policy1 export
```

向 EBGP 对等体 11.0.0.2 发布标签路由及从 11.0.0.2 接收标签路由的能力。

```
[ASBR-PE2-bgp-ipv4] peer 11.0.0.2 label-route-capability
[ASBR-PE2-bgp-ipv4] quit
[ASBR-PE2-bgp] quit
```

(5)　配置 PE 2

在 PE 2 上运行 IS-IS。

```
<PE2> system-view
[PE2] isis 1
[PE2-isis-1] network-entity 10.111.111.111.111.00
[PE2-isis-1] quit
```

配置 LSR ID，使能 MPLS 和 LDP。

```
[PE2] mpls lsr-id 5.5.5.9
[PE2] mpls ldp
[PE2-ldp] quit
```

配置接口 Serial2/1/0，在接口上运行 IS-IS，并使能 MPLS 和 LDP。

```
[PE2] interface serial 2/1/0
[PE2-Serial2/1/0] ip address 9.1.1.2 255.0.0.0
[PE2-Serial2/1/0] isis enable 1
[PE2-Serial2/1/0] mpls enable
[PE2-Serial2/1/0] mpls ldp enable
```

```
[PE2-Serial2/1/0] quit
```
创建 Loopback0 接口，在接口上运行 IS-IS。
```
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 5.5.5.9 32
[PE2-LoopBack0] isis enable 1
[PE2-LoopBack0] quit
```
创建 VPN 实例，名称为 vpn1，为其配置 RD 和 VPN Target 属性。
```
[PE2] ip vpn-instance vpn1
[PE2-vpn-instance-vpn1] route-distinguisher 11:11
[PE2-vpn-instance-vpn1] vpn-target 1:1 2:2 3:3 import-extcommunity
[PE2-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity
[PE2-vpn-instance-vpn1] quit
```
配置接口 GigabitEthernet2/1/1 与 VPN 实例 vpn1 绑定，并配置该接口的 IP 地址。
```
[PE2] interface gigabitethernet 2/1/1
[PE2-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE2-GigabitEthernet2/1/1] ip address 20.0.0.1 24
[PE2-GigabitEthernet2/1/1] quit
```
在 PE 2 上运行 BGP。
```
[PE2] bgp 600
```
配置 PE 2 向 IBGP 对等体 4.4.4.9 发布标签路由及从 4.4.4.9 接收标签路由的能力。
```
[PE2-bgp] peer 4.4.4.9 as-number 600
[PE2-bgp] peer 4.4.4.9 connect-interface loopback 0
[PE2-bgp] address-family ipv4 unicast
[PE2-bgp-ipv4] peer 4.4.4.9 enable
[PE2-bgp-ipv4] peer 4.4.4.9 label-route-capability
[PE2-bgp-ipv4] quit
```
配置 PE 2 到 EBGP 对等体 2.2.2.9 的最大跳数为 10。
```
[PE2-bgp] peer 2.2.2.9 as-number 100
[PE2-bgp] peer 2.2.2.9 connect-interface loopback 0
[PE2-bgp] peer 2.2.2.9 ebgp-max-hop 10
```
配置对等体 2.2.2.9 作为 VPNv4 对等体。
```
[PE2-bgp] address-family vpnv4
[PE2-bgp-vpnv4] peer 2.2.2.9 enable
[PE2-bgp-vpnv4] quit
```
配置 PE 2 与 CE 2 建立 EBGP 对等体，将学习到的 BGP 路由添加到 VPN 实例的路由表中。
```
[PE2-bgp] ip vpn-instance vpn1
[PE2-bgp-vpn1] peer 20.0.0.2 as-number 65002
[PE2-bgp-vpn1] address-family ipv4 unicast
[PE2-bgp-ipv4-vpn1] peer 20.0.0.2 enable
[PE2-bgp-ipv4-vpn1] quit
[PE2-bgp-vpn1] quit
[PE2-bgp] quit
```
(6) 配置 CE 2

配置接口 GigabitEthernet2/1/1 的 IP 地址。
```
<CE2> system-view
[CE2] interface gigabitethernet 2/1/1
```

```
[CE2-GigabitEthernet2/1/1] ip address 20.0.0.2 24
[CE2-GigabitEthernet2/1/1] quit
```

配置 CE 2 与 PE 2 建立 EBGP 对等体，并引入 VPN 路由。

```
[CE2] bgp 65002
[CE2-bgp] peer 20.0.0.1 as-number 600
[CE2-bgp] address-family ipv4 unicast
[CE2-bgp-ipv4] peer 20.0.0.1 enable
[CE2-bgp-ipv4] import-route direct
[CE2-bgp-ipv4] quit
[CE2-bgp] quit
```

4. 验证配置

配置完成后，在 CE 1 和 CE 2 上执行 **display ip routing-table** 命令可以查看到到达对方的路由，且 CE 1 和 CE 2 互相可以 ping 通。

1.14.7 配置运营商的运营商示例

1. 组网需求

二级运营商向自己的客户提供 MPLS L3VPN 服务。

在 图 1-30 中：

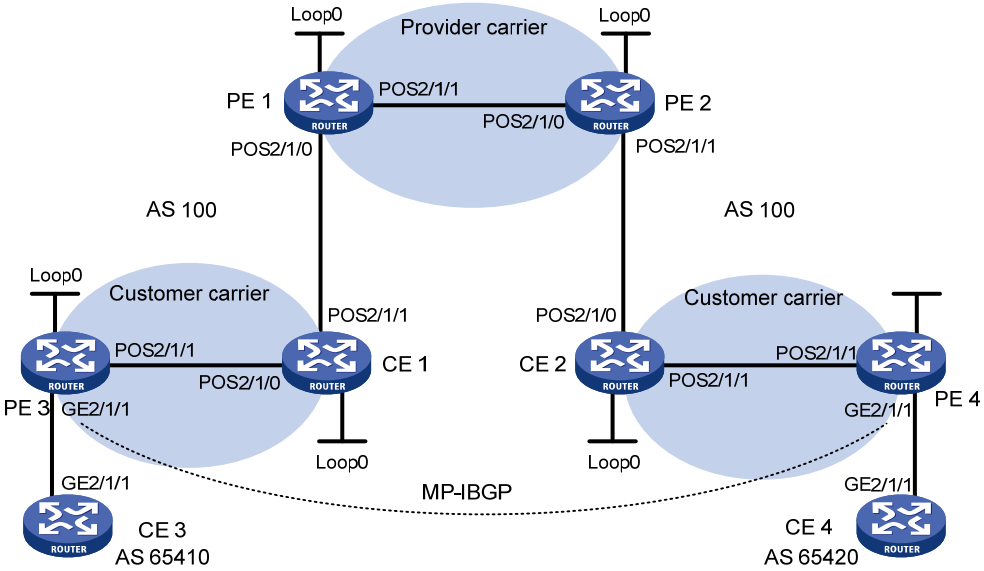
- PE 1 和 PE 2 是一级运营商骨干网的 PE 设备；
- CE 1 和 CE 2 是二级运营商的设备，作为 CE 接入一级运营商的骨干网；
- PE 3 和 PE 4 是二级运营商的设备，为二级运营商的客户提供接入；
- CE 3 和 CE 4 是二级运营商的客户。

运营商的运营商的配置关键在于理解两类路由的交换过程，即：

- 二级运营商 VPN 内部路由在一级运营商骨干网上的交换：一级运营商将二级运营商作为自己的 CE 接入；
- 二级运营商本身客户的 VPN 路由在二级运营商 PE 设备间的交换：需要在二级运营商 PE 设备（PE 3 和 PE 4）间建立 MP-IBGP 对等体关系。

2. 组网图

图1-30 配置 Carriers' carriers 配置组网图



设备	接口	IP地址	设备	接口	IP地址
CE 3	GE2/1/1	100.1.1.1/24	CE 4	GE2/1/1	120.1.1.1/24
PE 3	Loop0	1.1.1.9/32	PE 4	Loop0	6.6.6.9/32
	GE2/1/1	100.1.1.2/24		GE2/1/1	120.1.1.2/24
	POS2/1/1	10.1.1.1/24		POS2/1/1	20.1.1.2/24
CE 1	Loop0	2.2.2.9/32	CE 2	Loop0	5.5.5.9/32
	POS2/1/0	10.1.1.2/24		POS2/1/0	21.1.1.2/24
	POS2/1/1	11.1.1.1/24		POS2/1/1	20.1.1.1/24
PE 1	Loop0	3.3.3.9/32	PE 2	Loop0	4.4.4.9/32
	POS2/1/0	11.1.1.2/24		POS2/1/0	30.1.1.2/24
	POS2/1/1	30.1.1.1/24		POS2/1/1	21.1.1.1/24

3. 配置步骤

(1) 配置一级运营商骨干网的 MPLS L3VPN，使用 IS-IS 作为骨干网的 IGP 协议，PE 1 和 PE 2 之间使能 LDP，并建立 MP-IBGP 对等体关系

配置 PE 1。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 3.3.3.9 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 3.3.3.9
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] isis 1
[PE1-isis-1] network-entity 10.0000.0000.0000.0004.00
[PE1-isis-1] quit
[PE1] interface loopback 0
[PE1-LoopBack0] isis enable 1
[PE1-LoopBack0] quit
[PE1] interface pos 2/1/1
```

```
[PE1-Pos2/1/1] ip address 30.1.1.1 24
[PE1-Pos2/1/1] isis enable 1
[PE1-Pos2/1/1] mpls enable
[PE1-Pos2/1/1] mpls ldp enable
[PE1-Pos2/1/1] mpls ldp transport-address interface
[PE1-Pos2/1/1] quit
[PE1] bgp 100
[PE1-bgp] peer 4.4.4.9 as-number 100
[PE1-bgp] peer 4.4.4.9 connect-interface loopback 0
[PE1-bgp] address-family vpnv4
[PE1-bgp-vpnv4] peer 4.4.4.9 enable
[PE1-bgp-vpnv4] quit
[PE1-bgp] quit
```

PE 2 的配置与 PE 1 类似，配置过程省略。

配置完成后，在 PE 1 或 PE 2 上执行 **display mpls ldp peer** 命令可以看到 LDP 会话建立成功，状态为 Operational；执行 **display bgp peer vpnv4** 命令可以看到 BGP 对等体关系已建立，并达到 Established 状态；执行 **display isis peer** 命令可以看到 IS-IS 邻居关系已建立，状态为 up。

以 PE 1 为例：

```
[PE1] display mpls ldp peer
Total number of peers: 1
Peer LDP ID        State         LAM  Role     GR   MD5  KA Sent/Rcvd
4.4.4.9:0          Operational   DU   Active   Off  Off  8/8
[PE1] display bgp peer vpnv4

 BGP local router ID: 3.3.3.9
 Local AS number: 100
 Total number of peers: 1                 Peers in established state: 1

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  4.4.4.9                100        3        6    0       0 00:00:32 Established
[PE1] display isis peer
                         Peer information for ISIS(1)
                          ---------------------------

 System Id: 0000.0000.0005
 Interface: POS2/1/1               Circuit Id: 0000.0000.0005.02
 State: Up     HoldTime:   8s      Type: L1(L1L2)     PRI: 64

 System Id: 0000.0000.0005
 Interface: POS2/1/1               Circuit Id: 0000.0000.0005.02
 State: Up     HoldTime:   8s      Type: L2(L1L2)     PRI: 64
```

(2) 配置二级运营商网络：使用 IS-IS 作为 IGP 协议，PE 3 和 CE 1、PE 4 和 CE 2 之间分别使能 LDP

配置 PE 3。

```
<PE3> system-view
[PE3] interface loopback 0
```

```
[PE3-LoopBack0] ip address 1.1.1.9 32
[PE3-LoopBack0] quit
[PE3] mpls lsr-id 1.1.1.9
[PE3] mpls ldp
[PE3-ldp] quit
[PE3] isis 2
[PE3-isis-2] network-entity 10.0000.0000.0000.0001.00
[PE3-isis-2] quit
[PE3] interface loopback 0
[PE3-LoopBack0] isis enable 2
[PE3-LoopBack0] quit
[PE3] interface pos 2/1/1
[PE3-Pos2/1/1] ip address 10.1.1.1 24
[PE3-Pos2/1/1] isis enable 2
[PE3-Pos2/1/1] mpls enable
[PE3-Pos2/1/1] mpls ldp enable
[PE3-Pos2/1/1] mpls ldp transport-address interface
[PE3-Pos2/1/1] quit
```

配置 CE 1。

```
<CE1> system-view
[CE1] interface loopback 0
[CE1-LoopBack0] ip address 2.2.2.9 32
[CE1-LoopBack0] quit
[CE1] mpls lsr-id 2.2.2.9
[CE1] mpls ldp
[CE1-ldp] quit
[CE1] isis 2
[CE1-isis-2] network-entity 10.0000.0000.0000.0002.00
[CE1-isis-2] quit
[CE1] interface loopback 0
[CE1-LoopBack0] isis enable 2
[CE1-LoopBack0] quit
[CE1] interface POS 2/1/0
[CE1-Pos2/1/0] ip address 10.1.1.2 24
[CE1-Pos2/1/0] isis enable 2
[CE1-Pos2/1/0] mpls enable
[CE1-Pos2/1/0] mpls ldp enable
[CE1-Pos2/1/0] mpls ldp transport-address interface
[CE1-Pos2/1/0] quit
```

配置完成后，PE 3 和 CE 1 之间应能建立 LDP 和 IS-IS 邻居关系。

PE 4 和 CE 2 之间的配置与 PE 3 和 CE 1 之间的配置类似，配置过程省略。

(3) 配置二级运营商 CE 接入到一级运营商的 PE，并在 PE 上配置 IS-IS 引入 BGP 路由、BGP 引入 IS-IS 路由

配置 PE1。

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 200:1
[PE1-vpn-instance-vpn1] vpn-target 1:1
```

```
[PE1-vpn-instance-vpn1] quit
[PE1] mpls ldp
[PE1-ldp] vpn-instance vpn1
[PE1-ldp-vpn-instance-vpn1] quit
[PE1-ldp] quit
[PE1] isis 2 vpn-instance vpn1
[PE1-isis-2] network-entity 10.0000.0000.0000.0003.00
[PE1-isis-2] import-route bgp
[PE1-isis-2] quit
[PE1] interface pos 2/1/0
[PE1-Pos2/1/0] ip binding vpn-instance vpn1
[PE1-Pos2/1/0] ip address 11.1.1.2 24
[PE1-Pos2/1/0] isis enable 2
[PE1-Pos2/1/0] mpls enable
[PE1-Pos2/1/0] mpls ldp enable
[PE1-Pos2/1/0] mpls ldp transport-address interface
[PE1-Pos2/1/0] quit
[PE1] bgp 100
[PE1-bgp] ip vpn-instance vpn1
[PE1-bgp-vpn1] address-family ipv4 unicast
[PE1-bgp-ipv4-vpn1] import isis 2
[PE1-bgp-ipv4-vpn1] quit
[PE1-bgp-vpn1] quit
[PE1-bgp] quit
```

配置 CE1。

```
[CE1] interface pos 2/1/1
[CE1-Pos2/1/1] ip address 11.1.1.1 24
[CE1-Pos2/1/1] isis enable 2
[CE1-Pos2/1/1] mpls enable
[CE1-Pos2/1/1] mpls ldp enable
[CE1-Pos2/1/1] mpls ldp transport-address interface
[CE1-Pos2/1/1] quit
```

配置完成后，PE 1 和 CE 1 之间应能建立 LDP 和 IS-IS 邻居关系。

PE 2 和 CE 2 之间的配置与 PE 1 和 CE 1 之间的配置类似，配置过程省略。

(4) 配置二级运营商的客户接入 PE

配置 CE 3。

```
<CE3> system-view
[CE3] interface gigabitethernet 2/1/1
[CE3-GigabitEthernet2/1/1] ip address 100.1.1.1 24
[CE3-GigabitEthernet2/1/1] quit
[CE3] bgp 65410
[CE3-bgp] peer 100.1.1.2 as-number 100
[CE3-bgp] address-family ipv4 unicast
[CE3-bgp-ipv4] peer 100.1.1.2 enable
[CE3-bgp-ipv4] import-route direct
[CE3-bgp-ipv4] quit
[CE3-bgp] quit
```

配置 PE 3。

```
[PE3] ip vpn-instance vpn1
[PE3-vpn-instance-vpn1] route-distinguisher 100:1
[PE3-vpn-instance-vpn1] vpn-target 1:1
[PE3-vpn-instance-vpn1] quit
[PE3] interface gigabitethernet 2/1/1
[PE3-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE3-GigabitEthernet2/1/1] ip address 100.1.1.2 24
[PE3-GigabitEthernet2/1/1] quit
[PE3] bgp 100
[PE3-bgp] ip vpn-instance vpn1
[PE3-bgp-vpn1] peer 100.1.1.1 as-number 65410
[PE3-bgp-vpn1] address-family ipv4 unicast
[PE3-bgp-ipv4-vpn1] peer 100.1.1.1 enable
[PE3-bgp-ipv4-vpn1] import-route direct
[PE3-bgp-ipv4-vpn1] quit
[PE3-bgp-vpn1] quit
[PE3-bgp] quit
```

PE 4 和 CE 4 之间的配置与 PE 3 和 CE 3 之间的配置类似，配置过程省略。

(5) 在二级运营商的 PE 之间建立 MP-IBGP 对等体关系，交换二级运营商的客户的 VPN 路由

配置 PE 3。

```
[PE3] bgp 100
[PE3-bgp] peer 6.6.6.9 as-number 100
[PE3-bgp] peer 6.6.6.9 connect-interface loopback 0
[PE3-bgp] address-family vpnv4
[PE3-bgp-vpnv4] peer 6.6.6.9 enable
[PE3-bgp-vpnv4] quit
[PE3-bgp] quit
```

PE 4 的配置与 PE 3 类似，配置过程省略。

4. 验证配置

在 PE 1 和 PE 2 上执行 **display ip routing-table** 命令，可以看到 PE 1 和 PE 2 的公网路由表中只有一级运营商网络的路由。以 PE 1 为例：

```
[PE1] display ip routing-table
Routing Tables: Public
         Destinations : 7        Routes : 7
Destination/Mask    Proto  Pre  Cost      NextHop         Interface
3.3.3.9/32          Direct 0    0         127.0.0.1       InLoop0
4.4.4.9/32          ISIS   15   10        30.1.1.2        POS2/1/1
30.1.1.0/24         Direct 0    0         30.1.1.1        POS2/1/1
30.1.1.1/32         Direct 0    0         127.0.0.1       InLoop0
30.1.1.2/32         Direct 0    0         30.1.1.2        POS2/1/1
127.0.0.0/8         Direct 0    0         127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0         127.0.0.1       InLoop0
```

在 PE 1 和 PE 2 上执行 **display ip routing-table vpn-instance** 命令，可以看到 VPN 路由表中有二级运营商网络的内部路由，但没有二级运营商维护的 VPN 路由。以 PE 1 为例：

```
[PE1] display ip routing-table vpn-instance vpn1
```

```
Routing Tables: vpn1
         Destinations : 11        Routes : 11
Destination/Mask    Proto  Pre  Cost      NextHop         Interface
1.1.1.9/32          ISIS   15   20        11.1.1.1        POS2/1/0
2.2.2.9/32          ISIS   15   10        11.1.1.1        POS2/1/0
5.5.5.9/32          BGP    255  0         4.4.4.9         NULL0
6.6.6.9/32          BGP    255  0         4.4.4.9         NULL0
10.1.1.0/24         ISIS   15   20        11.1.1.1        POS2/1/0
11.1.1.0/24         Direct 0    0         11.1.1.1        POS2/1/0
11.1.1.1/32         Direct 0    0         127.0.0.1       InLoop0
11.1.1.2/32         Direct 0    0         11.1.1.2        POS2/1/0
20.1.1.0/24         BGP    255  0         4.4.4.9         NULL0
21.1.1.0/24         BGP    255  0         4.4.4.9         NULL0
21.1.1.2/32         BGP    255  0         4.4.4.9         NULL0
```

在 CE 1 和 CE 2 上执行 **display ip routing-table** 命令，可以看到公网路由表中有二级运营商网络的内部路由，但没有二级运营商维护的 VPN 路由。以 CE 1 为例：

```
[CE1] display ip routing-table
Routing Tables: Public
         Destinations : 16       Routes : 16
Destination/Mask    Proto  Pre  Cost      NextHop         Interface
1.1.1.9/32          ISIS   15   10        10.1.1.2        POS2/1/0
2.2.2.9/32          Direct 0    0         127.0.0.1       InLoop0
5.5.5.9/32          ISIS   15   74        11.1.1.2        POS2/1/1
6.6.6.9/32          ISIS   15   74        11.1.1.2        POS2/1/1
10.1.1.0/24         Direct 0    0         10.1.1.2        POS2/1/0
10.1.1.1/32         Direct 0    0         10.1.1.1        POS2/1/0
10.1.1.2/32         Direct 0    0         127.0.0.1       InLoop0
11.1.1.0/24         Direct 0    0         11.1.1.1        POS2/1/1
11.1.1.1/32         Direct 0    0         127.0.0.1       InLoop0
11.1.1.2/32         Direct 0    0         11.1.1.2        POS2/1/1
20.1.1.0/24         ISIS   15   74        11.1.1.2        POS2/1/1
21.1.1.0/24         ISIS   15   74        11.1.1.2        POS2/1/1
21.1.1.2/32         ISIS   15   74        11.1.1.2        POS2/1/1
127.0.0.0/8         Direct 0    0         127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0         127.0.0.1       InLoop0
```

在 PE 3 和 PE 4 上执行 **display ip routing-table** 命令，可以看到公网路由表中有二级运营商网络的内部路由。以 PE 3 为例：

```
[PE3] display ip routing-table
Routing Tables: Public
         Destinations : 11       Routes : 11
Destination/Mask    Proto  Pre  Cost      NextHop         Interface
1.1.1.9/32          Direct 0    0         127.0.0.1       InLoop0
2.2.2.9/32          ISIS   15   10        10.1.1.2        POS2/1/1
5.5.5.9/32          ISIS   15   84        10.1.1.2        POS2/1/1
6.6.6.9/32          ISIS   15   84        10.1.1.2        POS2/1/1
10.1.1.0/24         Direct 0    0         10.1.1.1        POS2/1/1
10.1.1.1/32         Direct 0    0         127.0.0.1       InLoop0
10.1.1.2/32         Direct 0    0         10.1.1.2        POS2/1/1
```

```
11.1.1.0/24         ISIS   15   20     10.1.1.2        POS2/1/1
20.1.1.0/24         ISIS   15   84     10.1.1.2        POS2/1/1
21.1.1.0/24         ISIS   15   84     10.1.1.2        POS2/1/1
21.1.1.2/32         ISIS   15   84     10.1.1.2        POS2/1/1
127.0.0.0/8         Direct 0    0      127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0      127.0.0.1       InLoop0
```

在 PE 3 和 PE 4 上执行 **display ip routing-table vpn-instance** 命令，可以看到 VPN 路由表中有远端 VPN 客户的路由。以 PE 3 为例：

```
[PE3] display ip routing-table vpn-instance vpn1
Routing Tables: vpn1
         Destinations : 3        Routes : 3
Destination/Mask    Proto  Pre  Cost      NextHop         Interface
100.1.1.0/24        Direct 0    0         100.1.1.2       GE2/1/1
100.1.1.2/32        Direct 0    0         127.0.0.1       InLoop0
120.1.1.0/24        BGP    255  0         6.6.6.9         NULL0
```

PE 3 和 PE 4 可以相互 Ping 通。

CE 3 和 CE 4 可以互相 Ping 通。

1.14.8 配置嵌套VPN示例

1. 组网需求

运营商向用户提供嵌套VPN服务。如 图 1-31 所示：

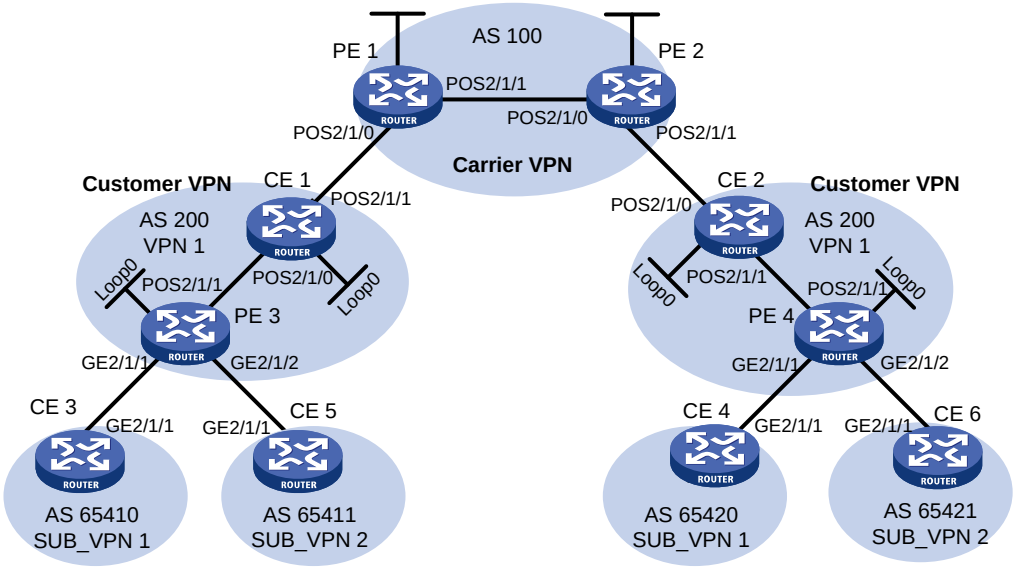
- PE 1 和 PE 2 是运营商骨干网的 PE 设备，支持嵌套 VPN 功能；
- CE 1 和 CE 2 是运营商 CE 设备，接入运营商的骨干网，该 CE 设备支持发送 VPNv4 路由；
- PE 3 和 PE 4 是用户网络内部的 PE 设备，支持 MPLS L3VPN；
- CE 3、CE 4、CE 5 和 CE 6 是用户网络内部子 VPN 的 CE 设备。

配置嵌套 VPN 的关键在于理解子 VPN 路由在运营商 PE 设备上的处理过程：

- 运营商 PE（PE 1 和 PE 2）收到运营商 CE（CE 1 和 CE 2）发送来的 VPNv4 路由时，需要将该 VPNv4 路由的 RD 更换为运营商 CE 所处 VPN 的 RD，同时将运营商 CE 所处 VPN 的 Export Target 添加到路由的扩展团体属性列表中，然后再按照一般的 VPNv4 路由发送出去；
- 为了实现用户网络内部子 VPN 的路由在用户 PE 和运营商 PE 间交换，需要在运营商 PE 和运营商 CE 间建立 MP-EBGP 对等体关系。

2. 组网图

图1-31 嵌套 VPN 组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	Loop0	2.2.2.9/32	CE 2	Loop0	5.5.5.9/32
	POS2/1/0	10.1.1.2/24		POS2/1/0	21.1.1.2/24
	POS2/1/1	11.1.1.1/24		POS2/1/1	20.1.1.1/24
CE 3	GE2/1/1	100.1.1.1/24	CE 4	GE2/1/1	120.1.1.1/24
CE 5	GE2/1/1	110.1.1.1/24	CE 6	GE2/1/1	130.1.1.1/24
PE 1	Loop0	3.3.3.9/32	PE 2	Loop0	4.4.4.9/32
	POS2/1/0	11.1.1.2/24		POS2/1/0	30.1.1.2/24
	POS2/1/1	30.1.1.1/24		POS2/1/1	21.1.1.1/24
PE 3	Loop0	1.1.1.9/32	PE 4	Loop0	6.6.6.9/32
	GE2/1/1	100.1.1.2/24		GE2/1/1	120.1.1.2/24
	GE2/1/2	110.1.1.2/24		GE2/1/2	130.1.1.2/24
	POS2/1/1	10.1.1.1/24		POS2/1/1	20.1.1.2/24

3. 配置步骤

(1) 配置运营商骨干网的 MPLS L3VPN，使用 IS-IS 作为骨干网的 IGP 协议，PE 1 和 PE 2 之间使能 LDP，并建立 MP-IBGP 对等体关系

配置 PE 1。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 3.3.3.9 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 3.3.3.9
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] isis 1
[PE1-isis-1] network-entity 10.0000.0000.0000.0004.00
[PE1-isis-1] quit
[PE1] interface loopback 0
[PE1-LoopBack0] isis enable 1
[PE1-LoopBack0] quit
```

```
[PE1] interface pos 2/1/1
[PE1-Pos2/1/1] ip address 30.1.1.1 24
[PE1-Pos2/1/1] isis enable 1
[PE1-Pos2/1/1] mpls enable
[PE1-Pos2/1/1] mpls ldp enable
[PE1-Pos2/1/1] mpls ldp transport-address interface
[PE1-Pos2/1/1] quit
[PE1] bgp 100
[PE1-bgp] peer 4.4.4.9 as-number 100
[PE1-bgp] peer 4.4.4.9 connect-interface loopback 0
[PE1-bgp] address-family vpnv4
[PE1-bgp-vpnv4] peer 4.4.4.9 enable
[PE1-bgp-vpnv4] quit
[PE1-bgp] quit
```

PE 2 的配置与 PE 1 类似，配置过程略。

配置完成后，在 PE 1 或 PE 2 上执行 **display mpls ldp peer** 命令可以看到 LDP 会话建立成功，LDP 会话状态为 Operational；执行 **display bgp peer vpnv4** 命令可以看到 BGP 对等体关系已建立，并达到 Established 状态；执行 **display isis peer** 命令可以看到 IS-IS 邻居关系已建立，状态为 up。

以 PE 1 为例：

```
[PE1] display mpls ldp peer
Total number of peers: 1
Peer LDP ID        State         LAM  Role     GR   MD5  KA Sent/Rcvd
4.4.4.9:0          Operational   DU   Active   Off  Off  8/8
[PE1] display bgp peer vpnv4

 BGP local router ID: 3.3.3.9
 Local AS number: 100
 Total number of peers: 1                 Peers in established state: 1

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  4.4.4.9                100        3        6    0       0 00:00:32 Established
[PE1] display isis peer
                         Peer information for ISIS(1)
                          ----------------------------

 System Id: 0000.0000.0005
 Interface: POS2/1/1               Circuit Id: 0000.0000.0005.02
 State: Up     HoldTime:   8s      Type: L1(L1L2)     PRI: 64

 System Id: 0000.0000.0005
 Interface: POS2/1/1               Circuit Id: 0000.0000.0005.02
 State: Up     HoldTime:   8s      Type: L2(L1L2)     PRI: 64
```

(2) 配置用户网络：使用 IS-IS 作为 IGP 协议，PE 3 和 CE 1、PE 4 和 CE 2 之间分别使能 LDP

配置 PE 3。

```
<PE3> system-view
```

```
[PE3] interface loopback 0
[PE3-LoopBack0] ip address 1.1.1.9 32
[PE3-LoopBack0] quit
[PE3] mpls lsr-id 1.1.1.9
[PE3] mpls ldp
[PE3-ldp] quit
[PE3] isis 2
[PE3-isis-2] network-entity 10.0000.0000.0000.0001.00
[PE3-isis-2] quit
[PE3] interface loopback 0
[PE3-LoopBack0] isis enable 2
[PE3-LoopBack0] quit
[PE3] interface pos 2/1/1
[PE3-Pos2/1/1] ip address 10.1.1.1 24
[PE3-Pos2/1/1] isis enable 2
[PE3-Pos2/1/1] mpls enable
[PE3-Pos2/1/1] mpls ldp enable
[PE3-Pos2/1/1] quit
```

配置 CE 1。

```
<CE1> system-view
[CE1] interface loopback 0
[CE1-LoopBack0] ip address 2.2.2.9 32
[CE1-LoopBack0] quit
[CE1] mpls lsr-id 2.2.2.9
[CE1] mpls ldp
[CE1-ldp] quit
[CE1] isis 2
[CE1-isis-2] network-entity 10.0000.0000.0000.0002.00
[CE1-isis-2] quit
[CE1] interface loopback 0
[CE1-LoopBack0] isis enable 2
[CE1-LoopBack0] quit
[CE1] interface pos 2/1/0
[CE1-Pos2/1/0] ip address 10.1.1.2 24
[CE1-Pos2/1/0] isis enable 2
[CE1-Pos2/1/0] mpls enable
[CE1-Pos2/1/0] mpls ldp enable
[CE1-Pos2/1/0] quit
```

配置完成后，PE 3 和 CE 1 之间可以建立 LDP 和 IS-IS 邻居关系。

PE 4 和 CE 2 之间的配置与 PE 3 和 CE 1 之间的配置类似，配置过程略。

(3) 配置运营商 CE 接入到运营商的 PE

配置 PE 1。

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 200:1
[PE1-vpn-instance-vpn1] vpn-target 1:1
[PE1-vpn-instance-vpn1] quit
[PE1] interface pos 2/1/0
```

```
[PE1-Pos2/1/0] ip binding vpn-instance vpn1
[PE1-Pos2/1/0] ip address 11.1.1.2 24
[PE1-Pos2/1/0] mpls enable
[PE1-Pos2/1/0] quit
[PE1] bgp 100
[PE1-bgp] ip vpn-instance vpn1
[PE1-bgp-vpn1] peer 11.1.1.1 as-number 200
[PE1-bgp-vpn1] quit
[PE1-bgp] quit
```

配置 CE 1。

```
[CE1] interface pos 2/1/1
[CE1-Pos2/1/1] ip address 11.1.1.1 24
[CE1-Pos2/1/1] mpls enable
[CE1-Pos2/1/1] quit
[CE1] bgp 200
[CE1-bgp] peer 11.1.1.2 as-number 100
[CE1-bgp] quit
```

PE 2 和 CE 2 之间的配置与 PE 1 和 CE 1 之间的配置类似，配置过程省略。

(4) 配置用户 CE 接入用户网络的 PE

配置 CE 3。

```
<CE3> system-view
[CE3] interface gigabitethernet 2/1/1
[CE3-GigabitEthernet2/1/1] ip address 100.1.1.1 24
[CE3-GigabitEthernet2/1/1] quit
[CE3] bgp 65410
[CE3-bgp] peer 100.1.1.2 as-number 200
[CE3-bgp] address-family ipv4 unicast
[CE3-bgp-ipv4] peer 100.1.1.2 enable
[CE3-bgp-ipv4] import-route direct
[CE3-bgp-ipv4] quit
[CE3-bgp] quit
```

配置 CE 5。

```
<CE5> system-view
[CE5] interface gigabitethernet 2/1/1
[CE5-GigabitEthernet2/1/1] ip address 110.1.1.1 24
[CE5-GigabitEthernet2/1/1] quit
[CE5] bgp 65411
[CE5-bgp] peer 110.1.1.2 as-number 200
[CE5-bgp] address-family ipv4 unicast
[CE5-bgp-ipv4] peer 110.1.1.2 enable
[CE5-bgp-ipv4] import-route direct
[CE5-bgp-ipv4] quit
[CE5-bgp] quit
```

配置 PE 3。

```
[PE3] ip vpn-instance SUB_VPN1
[PE3-vpn-instance-SUB_VPN1] route-distinguisher 100:1
[PE3-vpn-instance-SUB_VPN1] vpn-target 2:1
```

```
[PE3-vpn-instance-SUB_VPN1] quit
[PE3] interface gigabitethernet 2/1/1
[PE3-GigabitEthernet2/1/1] ip binding vpn-instance SUB_VPN1
[PE3-GigabitEthernet2/1/1] ip address 100.1.1.2 24
[PE3-GigabitEthernet2/1/1] quit
[PE3] ip vpn-instance SUB_VPN2
[PE3-vpn-instance-SUB_VPN2] route-distinguisher 101:1
[PE3-vpn-instance-SUB_VPN2] vpn-target 2:2
[PE3-vpn-instance-SUB_VPN2] quit
[PE3] interface gigabitethernet 2/1/2
[PE3-GigabitEthernet2/1/2] ip binding vpn-instance SUB_VPN2
[PE3-GigabitEthernet2/1/2] ip address 110.1.1.2 24
[PE3-GigabitEthernet2/1/2] quit
[PE3] bgp 200
[PE3-bgp] ip vpn-instance SUB_VPN1
[PE3-bgp-SUB_VPN1] peer 100.1.1.1 as-number 65410
[PE3-bgp-SUB_VPN1] address-family ipv4 unicast
[PE3-bgp-ipv4-SUB_VPN1] peer 100.1.1.1 enable
[PE3-bgp-ipv4-SUB_VPN1] import-route direct
[PE3-bgp-ipv4-SUB_VPN1] quit
[PE3-bgp-SUB_VPN1] quit
[PE3-bgp] ip vpn-instance SUB_VPN2
[PE3-bgp-SUB_VPN2] peer 110.1.1.1 as-number 65411
[PE3-bgp-SUB_VPN2] address-family ipv4 unicast
[PE3-bgp-ipv4-SUB_VPN2] peer 110.1.1.1 enable
[PE3-bgp-ipv4-SUB_VPN2] import-route direct
[PE3-bgp-ipv4-SUB_VPN2] quit
[PE3-bgp-SUB_VPN2] quit
[PE3-bgp] quit
```

PE 4 和 CE 4，CE 6 之间的配置与 PE 3 和 CE 3，CE 5 之间的配置类似，配置过程省略。

(5)　在运营商的 PE 和运营商 CE 之间建立 MP-EBGP 对等体关系，交换用户的 VPNv4 路由

在 PE 1 上使能嵌套 VPN 功能，并使能 PE 1 与 CE 1 交互 VPNv4 路由的能力。

```
[PE1] bgp 100
[PE1-bgp] address-family vpnv4
[PE1-bgp-vpnv4] nesting-vpn
[PE1-bgp-vpnv4] quit
[PE1-bgp] ip vpn-instance vpn1
[PE1-bgp-vpn1] address-family vpnv4
[PE1-bgp-vpnv4-vpn1] peer 11.1.1.1 enable
[PE1-bgp-vpnv4-vpn1] quit
[PE1-bgp-vpn1] quit
[PE1-bgp] quit
```

在 CE 1 上使能其与 PE 1 交互 VPNv4 路由的能力。

```
[CE1] bgp 200
[CE1-bgp] address-family vpnv4
[CE1-bgp-vpnv4] peer 11.1.1.2 enable
```

在 CE 1 上配置允许本地 AS 号在所接收的路由的 AS_PATH 属性中出现。

```
[CE1-bgp-vpnv4] peer 11.1.1.2 allow-as-loop 2
```

在 CE 1 上配置接收所有 VPNv4 路由。

```
[CE1-bgp-vpnv4] undo policy vpn-target
[CE1-bgp-vpnv4] quit
[CE1-bgp] quit
```

PE 2 和 CE 2 之间的配置与 PE 1 和 CE 1 之间的配置类似，配置过程省略。

(6) 在用户 PE 和运营商 CE 之间建立 MP-IBGP 对等体关系，交换用户内部子 VPN 的 VPNv4 路由

配置 PE 3。

```
[PE3] bgp 200
[PE3-bgp] peer 2.2.2.9 as-number 200
[PE3-bgp] peer 2.2.2.9 connect-interface loopback 0
[PE3-bgp] address-family vpnv4
[PE3-bgp-vpnv4] peer 2.2.2.9 enable
```

配置允许本地 AS 号在所接收的路由的 AS_PATH 属性中出现。

```
[PE3-bgp-vpnv4] peer 2.2.2.9 allow-as-loop 2
[PE3-bgp-vpnv4] quit
[PE3-bgp] quit
```

配置 CE 1。

```
[CE1] bgp 200
[CE1-bgp] peer 1.1.1.9 as-number 200
[CE1-bgp] peer 1.1.1.9 connect-interface loopback 0
[CE1-bgp] address-family vpnv4
[CE1-bgp-vpnv4] peer 1.1.1.9 enable
[CE1-bgp-vpnv4] undo policy vpn-target
[CE1-bgp-vpnv4] quit
[CE1-bgp] quit
```

PE 4 和 CE 2 之间的配置与 PE 3 和 CE 1 之间的配置类似，配置过程省略。

4. 验证配置

在 PE 1 和 PE 2 上执行 **display ip routing-table** 命令，可以看到 PE 1 和 PE 2 的公网路由表中只有运营商网络的路由。以 PE 1 为例：

```
[PE1] display ip routing-table

Destinations : 14        Routes : 14

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
3.3.3.9/32          Direct 0    0            127.0.0.1       InLoop0
4.4.4.9/32          ISIS   15   10           30.1.1.2        POS2/1/1
30.1.1.0/24         Direct 0    0            30.1.1.1        POS2/1/1
30.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.2/32         Direct 0    0            30.1.1.2        POS2/1/1
30.1.1.255/32       Direct 0    0            30.1.1.2        POS2/1/1
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
```

```
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
224.0.0.0/4         Direct 0    0           0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0           0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
```

在 PE 1 和 PE 2 上执行 **display ip routing-table vpn-instance** 命令，可以看到 VPN 路由表中有用户子 VPN 网络的路由。以 PE 1 为例：

```
[PE1] display ip routing-table vpn-instance vpn1

Destinations : 16        Routes : 16

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0           127.0.0.1       InLoop0
11.1.1.0/24         Direct 0    0           11.1.1.1        POS2/1/0
11.1.1.1/32         Direct 0    0           127.0.0.1       InLoop0
11.1.1.2/32         Direct 0    0           11.1.1.2        POS2/1/0
11.1.1.255/32       Direct 0    0           11.1.1.2        POS2/1/0
100.1.1.0/24        BGP    255  0           11.1.1.1        NULL0
110.1.1.0/24        BGP    255  0           11.1.1.1        NULL0
120.1.1.0/24        BGP    255  0           4.4.4.9         NULL0
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
130.1.1.0/24        BGP    255  0           4.4.4.9         NULL0
224.0.0.0/4         Direct 0    0           0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0           0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
```

在 CE 1 和 CE 2 上执行 **display bgp routing-table vpnv4** 命令，可以看到用户网络中 VPNv4 路由表中有所有子 VPN 网络的内部路由。以 CE 1 为例：

```
[CE1] display bgp routing-table vpnv4

BGP Local router ID is 11.11.11.11
Status codes: * - valid, > - best, d - damped, h - history,
              s - suppressed, S - Stale, i - internal, e - external
              Origin: i - IGP, e - EGP, ? - incomplete

Total number of routes from all PEs: 4

Route Distinguisher: 100:1
Total number of routes: 1

    Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* > 100.1.1.0/24       1.1.1.9                                 0      200 65410?

Route Distinguisher: 101:1
Total number of routes: 1
```

```
    Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* > 110.1.1.0/24       1.1.1.9                                0       200 65411?

Route Distinguisher: 200:1
Total number of routes: 1

    Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* > 120.1.1.0/24       11.1.1.2                               0       100 200
                                                                       65420?

Route Distinguisher: 201:1
Total number of routes: 1

    Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* > 130.1.1.0/24       11.1.1.2                               0       100 200
                                                                       65421?
```

在 PE 3 和 PE 4 上执行 **display ip routing-table vpn-instance SUB_VPN1** 命令，可以看到私网路由表中有从运营商 PE 发布到用户网络子 VPN 内部的路由。以 PE 3 为例：

```
[PE3] display ip routing-table vpn-instance SUB_VPN1

Destinations : 13        Routes : 13

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
100.1.1.0/24        Direct 0    0            100.1.1.2       GE2/1/1
100.1.1.0/32        Direct 0    0            100.1.1.2       GE2/1/1
100.1.1.2/32        Direct 0    0            127.0.0.1       InLoop0
100.1.1.255/32      Direct 0    0            100.1.1.2       GE2/1/1
120.1.1.0/24        BGP    255  0            2.2.2.9         NULL0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

在 CE 3 和 CE 4 上执行 **display ip routing-table** 命令，可以看到路由表中有远端子 VPN 的路由。以 CE 3 为例：

```
[CE3] display ip routing-table

Destinations : 13        Routes : 13
```

```
Destination/Mask    Proto   Pre  Cost        NextHop         Interface
0.0.0.0/32          Direct  0    0           127.0.0.1       InLoop0
100.1.1.0/24        Direct  0    0           100.1.1.1       GE2/1/1
100.1.1.0/32        Direct  0    0           100.1.1.1       GE2/1/1
100.1.1.1/32        Direct  0    0           127.0.0.1       InLoop0
100.1.1.255/24      Direct  0    0           100.1.1.1       GE2/1/1
120.1.1.0/24        BGP     255  0           100.1.1.2       GE2/1/1
127.0.0.0/8         Direct  0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct  0    0           127.0.0.1       InLoop0
224.0.0.0/4         Direct  0    0           0.0.0.0         NULL0
224.0.0.0/24        Direct  0    0           0.0.0.0         NULL0
255.255.255.255/32  Direct  0    0           127.0.0.1       InLoop0
```

在 CE 5 和 CE 6 上执行 **display ip routing-table** 命令，可以看到路由表中有远端子 VPN 的路由。以 CE 5 为例：

```
[CE5] display ip routing-table

Destinations : 13        Routes : 13

Destination/Mask    Proto   Pre  Cost        NextHop         Interface
0.0.0.0/32          Direct  0    0           127.0.0.1       InLoop0
110.1.1.0/24        Direct  0    0           110.1.1.1       GE2/1/1
110.1.1.0/32        Direct  0    0           110.1.1.1       GE2/1/1
110.1.1.1/32        Direct  0    0           127.0.0.1       InLoop0
110.1.1.255/32      Direct  0    0           110.1.1.1       GE2/1/1
127.0.0.0/8         Direct  0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct  0    0           127.0.0.1       InLoop0
130.1.1.0/24        BGP     255  0           110.1.1.2       GE2/1/1
224.0.0.0/4         Direct  0    0           0.0.0.0         NULL0
224.0.0.0/24        Direct  0    0           0.0.0.0         NULL0
255.255.255.255/32  Direct  0    0           127.0.0.1       InLoop0
```

CE 3 和 CE 4 可以互相 Ping 通。

CE 5 和 CE 6 可以互相 Ping 通。

CE 3 和 CE 6 不能互相 Ping 通。

1.14.9 配置HoVPN示例

1. 组网需求

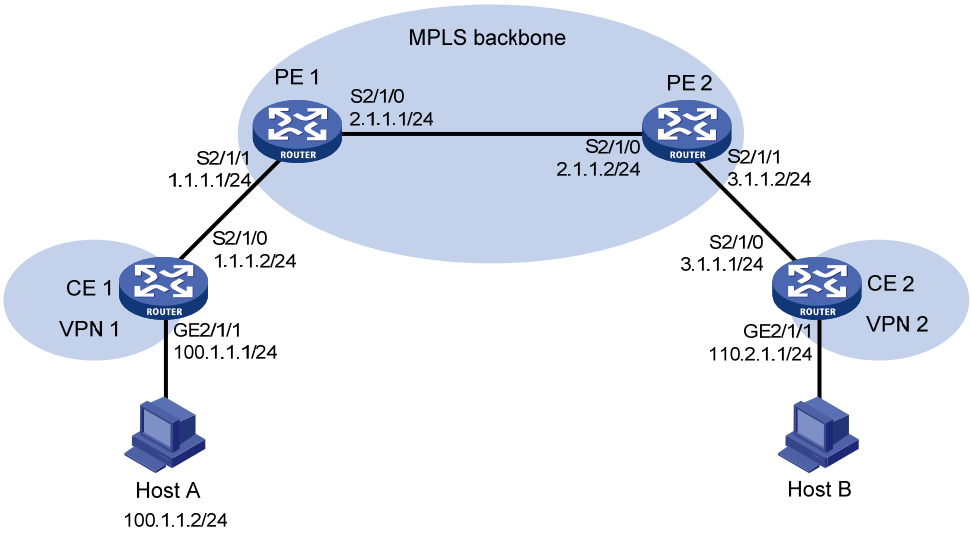
以一个包括省骨干和地市的 MPLS VPN 网络为例：

- SPE 作为省网的 PE 设备，接入地市的 MPLS VPN 网络；
- UPE 作为下层地市网络的 PE 设备，最终接入 VPN 客户。对 UPE 的性能要求低于对 SPE 的性能要求。

- SPE 将通过路由策略的路由发送给 UPE，限制不同 Site 之间的互相访问权限，使得 VPN 1 内的 CE 1 和 CE 3 可以互相访问，VPN 2 内的 CE 2 和 CE 4 不能互相访问。

2. 组网图

图1-32 配置 HoVPN 组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	GE2/1/1	10.2.1.1/24	CE 3	GE2/1/1	10.1.1.1/24
CE 2	GE2/1/1	10.4.1.1/24	CE 4	GE2/1/1	10.3.1.1/24
UPE 1	Loop0	1.1.1.9/32	UPE 2	Loop0	4.4.4.9/32
	GE2/1/1	10.2.1.2/24		GE2/1/1	172.2.1.1/24
	GE2/1/2	10.4.1.2/24		GE2/1/2	10.1.1.2/24
	GE2/1/3	172.1.1.1/24		GE2/1/3	10.3.1.2/24
SPE 1	Loop0	2.2.2.9/32	SPE 2	Loop0	3.3.3.9/32
	GE2/1/1	172.1.1.2/24		GE2/1/1	180.1.1.2/24
	GE2/1/2	180.1.1.1/24		GE2/1/2	172.2.1.2/24

3. 配置步骤

(1) 配置 UPE 1

配置 MPLS 基本能力和 MPLS LDP 能力，建立 LDP LSP。

```
<UPE1> system-view
[UPE1] interface loopback 0
[UPE1-LoopBack0] ip address 1.1.1.9 32
[UPE1-LoopBack0] quit
[UPE1] mpls lsr-id 1.1.1.9
[UPE1] mpls ldp
[UPE1-ldp] quit
[UPE1] interface gigabitethernet 2/1/3
[UPE1-GigabitEthernet2/1/3] ip address 172.1.1.1 24
[UPE1-GigabitEthernet2/1/3] mpls enable
[UPE1-GigabitEthernet2/1/3] mpls ldp enable
[UPE1-GigabitEthernet2/1/3] quit
```

配置 IGP 协议，以 OSPF 为例。

```
[UPE1] ospf
[UPE1-ospf-1] area 0
```

```
[UPE1-ospf-1-area-0.0.0.0] network 172.1.1.0 0.0.0.255
[UPE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[UPE1-ospf-1-area-0.0.0.0] quit
[UPE1-ospf-1] quit
```

配置 VPN 实例 vpn1 和 vpn2，将 CE 1 和 CE 2 接入 UPE 1。

```
[UPE1] ip vpn-instance vpn1
[UPE1-vpn-instance-vpn1] route-distinguisher 100:1
[UPE1-vpn-instance-vpn1] vpn-target 100:1 both
[UPE1-vpn-instance-vpn1] quit
[UPE1] ip vpn-instance vpn2
[UPE1-vpn-instance-vpn2] route-distinguisher 100:2
[UPE1-vpn-instance-vpn2] vpn-target 100:2 both
[UPE1-vpn-instance-vpn2] quit
[UPE1] interface gigabitethernet 2/1/1
[UPE1-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[UPE1-GigabitEthernet2/1/1] ip address 10.2.1.2 24
[UPE1-GigabitEthernet2/1/1] quit
[UPE1] interface gigabitethernet 2/1/2
[UPE1-GigabitEthernet2/1/2] ip binding vpn-instance vpn2
[UPE1-GigabitEthernet2/1/2] ip address 10.4.1.2 24
[UPE1-GigabitEthernet2/1/2] quit
```

配置 UPE 1 与 SPE 1 建立 MP-IBGP 对等体。

```
[UPE1] bgp 100
[UPE1-bgp] peer 2.2.2.9 as-number 100
[UPE1-bgp] peer 2.2.2.9 connect-interface loopback 0
[UPE1-bgp] address-family vpnv4
[UPE1-bgp-vpnv4] peer 2.2.2.9 enable
[UPE1-bgp-vpnv4] quit
```

配置 UPE 1 与 CE 1 建立 EBGP 对等体，并引入 VPN 路由。

```
[UPE1-bgp] ip vpn-instance vpn1
[UPE1-bgp-vpn1] peer 10.2.1.1 as-number 65410
[UPE1-bgp-vpn1] address-family ipv4 unicast
[UPE1-bgp-ipv4-vpn1] peer 10.2.1.1 enable
[UPE1-bgp-ipv4-vpn1] import-route direct
[UPE1-bgp-ipv4-vpn1] quit
[UPE1-bgp-vpn1] quit
```

配置 UPE 1 与 CE 2 建立 EBGP 对等体，并引入 VPN 路由。

```
[UPE1-bgp] ip vpn-instance vpn2
[UPE1-bgp-vpn2] peer 10.4.1.1 as-number 65420
[UPE1-bgp-vpn2] address-family ipv4 unicast
[UPE1-bgp-ipv4-vpn2] peer 10.4.1.1 enable
[UPE1-bgp-ipv4-vpn2] import-route direct
[UPE1-bgp-ipv4-vpn2] quit
[UPE1-bgp-vpn2] quit
[UPE1-bgp] quit
```

(2) 配置 CE 1

```
<CE1> system-view
```

```
[CE1] interface gigabitethernet 2/1/1
[CE1-GigabitEthernet2/1/1] ip address 10.2.1.1 255.255.255.0
[CE1-GigabitEthernet2/1/1] quit
[CE1] bgp 65410
[CE1-bgp] peer 10.2.1.2 as-number 100
[CE1-bgp] address-family ipv4 unicast
[CE1-bgp-ipv4] peer 10.2.1.2 enable
[CE1-bgp-ipv4] import-route direct
[CE1-bgp-ipv4] quit
[CE1-bgp] quit
```

(3) 配置 CE 2

```
<CE2> system-view
[CE2] interface gigabitethernet 2/1/1
[CE2-GigabitEthernet2/1/1] ip address 10.4.1.1 255.255.255.0
[CE2-GigabitEthernet2/1/1] quit
[CE2] bgp 65420
[CE2-bgp] peer 10.4.1.2 as-number 100
[CE2-bgp] address-family ipv4 unicast
[CE2-bgp-ipv4] peer 10.4.1.2 enable
[CE2-bgp-ipv4] import-route direct
[CE2-bgp-ipv4] quit
[CE2-bgp] quit
```

(4) 配置 UPE 2

配置 MPLS 基本能力和 MPLS LDP 能力，建立 LDP LSP。

```
<UPE2> system-view
[UPE2] interface loopback 0
[UPE2-LoopBack0] ip address 4.4.4.9 32
[UPE2-LoopBack0] quit
[UPE2] mpls lsr-id 4.4.4.9
[UPE2] mpls ldp
[UPE2-ldp] quit
[UPE2] interface gigabitethernet 2/1/1
[UPE2-GigabitEthernet2/1/1] ip address 172.2.1.1 24
[UPE2-GigabitEthernet2/1/1] mpls enable
[UPE2-GigabitEthernet2/1/1] mpls ldp enable
[UPE2-GigabitEthernet2/1/1] quit
```

配置 IGP 协议，以 OSPF 为例。

```
[UPE2] ospf
[UPE2-ospf-1] area 0
[UPE2-ospf-1-area-0.0.0.0] network 172.2.1.0 0.0.0.255
[UPE2-ospf-1-area-0.0.0.0] network 4.4.4.9 0.0.0.0
[UPE2-ospf-1-area-0.0.0.0] quit
[UPE2-ospf-1] quit
```

配置 VPN 实例 vpn1 和 vpn2，将 CE 3 和 CE 4 接入 UPE 2。

```
[UPE2] ip vpn-instance vpn1
[UPE2-vpn-instance-vpn1] route-distinguisher 300:1
[UPE2-vpn-instance-vpn1] vpn-target 100:1 both
```

```
[UPE2-vpn-instance-vpn1] quit
[UPE2] ip vpn-instance vpn2
[UPE2-vpn-instance-vpn2] route-distinguisher 400:2
[UPE2-vpn-instance-vpn2] vpn-target 100:2 both
[UPE2-vpn-instance-vpn2] quit
[UPE2] interface gigabitethernet 2/1/2
[UPE2-GigabitEthernet2/1/2] ip binding vpn-instance vpn1
[UPE2-GigabitEthernet2/1/2] ip address 10.1.1.2 24
[UPE2-GigabitEthernet2/1/2] quit
[UPE2] interface gigabitethernet 2/1/3
[UPE2-GigabitEthernet2/1/3] ip binding vpn-instance vpn2
[UPE2-GigabitEthernet2/1/3] ip address 10.3.1.2 24
[UPE2-GigabitEthernet2/1/3] quit
```

配置 UPE 2 与 SPE 2 建立 MP-IBGP 对等体。

```
[UPE2] bgp 100
[UPE2-bgp] peer 3.3.3.9 as-number 100
[UPE2-bgp] peer 3.3.3.9 connect-interface loopback 0
[UPE2-bgp] address-family vpnv4
[UPE2-bgp-vpnv4] peer 3.3.3.9 enable
[UPE2-bgp-vpnv4] quit
```

配置 UPE 2 与 CE 3 建立 EBGP 对等体，并引入 VPN 路由。

```
[UPE2-bgp] ip vpn-instance vpn1
[UPE2-bgp-vpn1] peer 10.1.1.1 as-number 65430
[UPE2-bgp-vpn1] address-family ipv4 unicast
[UPE2-bgp-ipv4-vpn1] peer 10.1.1.1 enable
[UPE2-bgp-ipv4-vpn1] import-route direct
[UPE2-bgp-ipv4-vpn1] quit
[UPE2-bgp-vpn1] quit
```

配置 UPE 2 与 CE 4 建立 EBGP 对等体，并引入 VPN 路由。

```
[UPE2-bgp] ip vpn-instance vpn2
[UPE2-bgp-vpn2] peer 10.3.1.1 as-number 65440
[UPE2-bgp-vpn2] address-family ipv4 unicast
[UPE2-bgp-ipv4-vpn2] peer 10.3.1.1 enable
[UPE2-bgp-ipv4-vpn2] import-route direct
[UPE2-bgp-ipv4-vpn2] quit
[UPE2-bgp-vpn2] quit
[UPE2-bgp] quit
```

(5) 配置 CE 3

```
<CE3> system-view
[CE3] interface gigabitethernet 2/1/1
[CE3-GigabitEthernet2/1/1] ip address 10.1.1.1 255.255.255.0
[CE3-GigabitEthernet2/1/1] quit
[CE3] bgp 65430
[CE3-bgp] peer 10.1.1.2 as-number 100
[CE3-bgp] address-family ipv4 unicast
[CE3-bgp-ipv4] peer 10.1.1.2 enable
[CE3-bgp-ipv4] import-route direct
```

```
[CE3-bgp-ipv4] quit
[CE3-bgp] quit
```

(6) 配置 CE 4

```
<CE4> system-view
[CE4] interface gigabitethernet 2/1/1
[CE4-GigabitEthernet2/1/1] ip address 10.3.1.1 255.255.255.0
[CE4-GigabitEthernet2/1/1] quit
[CE4] bgp 65440
[CE4-bgp] peer 10.3.1.2 as-number 100
[CE4-bgp] address-family ipv4 unicast
[CE4-bgp-ipv4] peer 10.3.1.2 enable
[CE4-bgp-ipv4] import-route direct
[CE4-bgp-ipv4] quit
[CE4-bgp] quit
```

(7) 配置 SPE 1

配置 MPLS 基本能力和 MPLS LDP 能力，建立 LDP LSP。

```
<SPE1> system-view
[SPE1] interface loopback 0
[SPE1-LoopBack0] ip address 2.2.2.9 32
[SPE1-LoopBack0] quit
[SPE1] mpls lsr-id 2.2.2.9
[SPE1] mpls ldp
[SPE1-ldp] quit
[SPE1] interface gigabitethernet 2/1/1
[SPE1-GigabitEthernet2/1/1] ip address 172.1.1.2 24
[SPE1-GigabitEthernet2/1/1] mpls enable
[SPE1-GigabitEthernet2/1/1] mpls ldp enable
[SPE1-GigabitEthernet2/1/1] quit
[SPE1] interface gigabitethernet 2/1/2
[SPE1-GigabitEthernet2/1/2] ip address 180.1.1.1 24
[SPE1-GigabitEthernet2/1/2] mpls enable
[SPE1-GigabitEthernet2/1/2] mpls ldp enable
[SPE1-GigabitEthernet2/1/2] quit
```

配置 IGP 协议，以 OSPF 为例。

```
[SPE1] ospf
[SPE1-ospf-1] area 0
[SPE1-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[SPE1-ospf-1-area-0.0.0.0] network 172.1.1.0 0.0.0.255
[SPE1-ospf-1-area-0.0.0.0] network 180.1.1.0 0.0.0.255
[SPE1-ospf-1-area-0.0.0.0] quit
[SPE1-ospf-1] quit
```

配置 VPN 实例 vpn1 和 vpn2。

```
[SPE1] ip vpn-instance vpn1
[SPE1-vpn-instance-vpn1] route-distinguisher 500:1
[SPE1-vpn-instance-vpn1] vpn-target 100:1 both
[SPE1-vpn-instance-vpn1] quit
[SPE1] ip vpn-instance vpn2
```

```
[SPE1-vpn-instance-vpn2] route-distinguisher 700:1
[SPE1-vpn-instance-vpn2] vpn-target 100:2 both
[SPE1-vpn-instance-vpn2] quit
```

配置 SPE 1 与 SPE 2、UPE 1 建立 MP-IBGP 对等体，并指定 UPE 1 为 UPE。

```
[SPE1] bgp 100
[SPE1-bgp] peer 1.1.1.9 as-number 100
[SPE1-bgp] peer 1.1.1.9 connect-interface loopback 0
[SPE1-bgp] peer 3.3.3.9 as-number 100
[SPE1-bgp] peer 3.3.3.9 connect-interface loopback 0
[SPE1-bgp] address-family vpnv4
[SPE1-bgp-vpnv4] peer 3.3.3.9 enable
[SPE1-bgp-vpnv4] peer 1.1.1.9 enable
[SPE1-bgp-vpnv4] peer 1.1.1.9 upe
[SPE1-bgp-vpnv4] peer 1.1.1.9 next-hop-local
[SPE1-bgp-vpnv4] quit
```

为 VPN 实例 vpn1 和 vpn2 分别创建 BGP-VPN 实例，以便根据 RT 属性将学习到的 VPNv4 路由添加到相应 VPN 实例的 BGP 路由表中。

```
[SPE1-bgp] ip vpn-instance vpn1
[SPE1-bgp-vpn1] quit
[SPE1-bgp] ip vpn-instance vpn2
[SPE1-bgp-vpn2] quit
[SPE1-bgp] quit
```

配置 SPE 1 向 UPE 1 发送通过策略的路由信息，允许 CE 3 的路由发送给 UPE 1。

```
[SPE1] ip prefix-list hope index 10 permit 10.1.1.1 24
[SPE1] route-policy hope permit node 0
[SPE1-route-policy-hope-0] if-match ip address prefix-list hope
[SPE1-route-policy-hope-0] quit
[SPE1] bgp 100
[SPE1-bgp] address-family vpnv4
[SPE1-bgp-vpnv4] peer 1.1.1.9 upe route-policy hope export
```

(8) 配置 SPE 2

配置 MPLS 基本能力和 MPLS LDP 能力，建立 LDP LSP。

```
<SPE2> system-view
[SPE2] interface loopback 0
[SPE2-LoopBack0] ip address 3.3.3.9 32
[SPE2-LoopBack0] quit
[SPE2] mpls lsr-id 3.3.3.9
[SPE2] mpls ldp
[SPE2-ldp] quit
[SPE2] interface gigabitethernet 2/1/1
[SPE2-GigabitEthernet2/1/1] ip address 180.1.1.2 24
[SPE2-GigabitEthernet2/1/1] mpls enable
[SPE2-GigabitEthernet2/1/1] mpls ldp enable
[SPE2-GigabitEthernet2/1/1] quit
[SPE2] interface gigabitethernet 2/1/2
[SPE2-GigabitEthernet2/1/2] ip address 172.2.1.2 24
[SPE2-GigabitEthernet2/1/2] mpls enable
```

```
[SPE2-GigabitEthernet2/1/2] mpls ldp enable
[SPE2-GigabitEthernet2/1/2] quit
```

配置 IGP 协议，以 OSPF 为例。

```
[SPE2] ospf
[SPE2-ospf-1] area 0
[SPE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[SPE2-ospf-1-area-0.0.0.0] network 172.2.1.0 0.0.0.255
[SPE2-ospf-1-area-0.0.0.0] network 180.1.1.0 0.0.0.255
[SPE2-ospf-1-area-0.0.0.0] quit
[SPE2-ospf-1] quit
```

配置 VPN 实例 vpn1 和 vpn2。

```
[SPE2] ip vpn-instance vpn1
[SPE2-vpn-instance-vpn1] route-distinguisher 600:1
[SPE2-vpn-instance-vpn1] vpn-target 100:1 both
[SPE2-vpn-instance-vpn1] quit
[SPE2] ip vpn-instance vpn2
[SPE2-vpn-instance-vpn2] route-distinguisher 800:1
[SPE2-vpn-instance-vpn2] vpn-target 100:2 both
[SPE2-vpn-instance-vpn2] quit
```

配置 SPE 2 与 SPE 1、UPE 2 建立 MP-IBGP 对等体，并指定 UPE 2 为 UPE。

```
[SPE2] bgp 100
[SPE2-bgp] peer 4.4.4.9 as-number 100
[SPE2-bgp] peer 4.4.4.9 connect-interface loopback 0
[SPE2-bgp] peer 2.2.2.9 as-number 100
[SPE2-bgp] peer 2.2.2.9 connect-interface loopback 0
[SPE2-bgp] address-family vpnv4
[SPE2-bgp-vpnv4] peer 2.2.2.9 enable
[SPE2-bgp-vpnv4] peer 4.4.4.9 enable
[SPE2-bgp-vpnv4] peer 4.4.4.9 upe
[SPE2-bgp-vpnv4] peer 4.4.4.9 next-hop-local
[SPE2-bgp-vpnv4] quit
```

为 VPN 实例 vpn1 和 vpn2 分别创建 BGP-VPN 实例，以便根据 RT 属性将学习到的 VPNv4 路由添加到相应 VPN 实例的 BGP 路由表中。

```
[SPE2-bgp] ip vpn-instance vpn1
[SPE2-bgp-vpn1] quit
[SPE2-bgp] ip vpn-instance vpn2
[SPE2-bgp-vpn2] quit
[SPE2-bgp] quit
```

配置 SPE 2 向 UPE 2 发送通过策略的路由信息，允许 CE 1 的路由发送给 UPE 2。

```
[SPE2] ip prefix-list hope index 10 permit 10.2.1.1 24
[SPE2] route-policy hope permit node 0
[SPE2-route-policy-hope-0] if-match ip address prefix-list hope
[SPE2-route-policy-hope-0] quit
[SPE2] bgp 100
[SPE2-bgp] address-family vpnv4
[SPE2-bgp-vpnv4] peer 4.4.4.9 upe route-policy hope export
```

4. 验证配置

上述配置完成后，CE 1 和 CE 3 能够学习到对方的接口路由，CE 1 和 CE 3 能够相互 ping 通；CE 2 和 CE 4 不能学习到对方的接口路由，CE 2 和 CE 4 不能相互 ping 通。

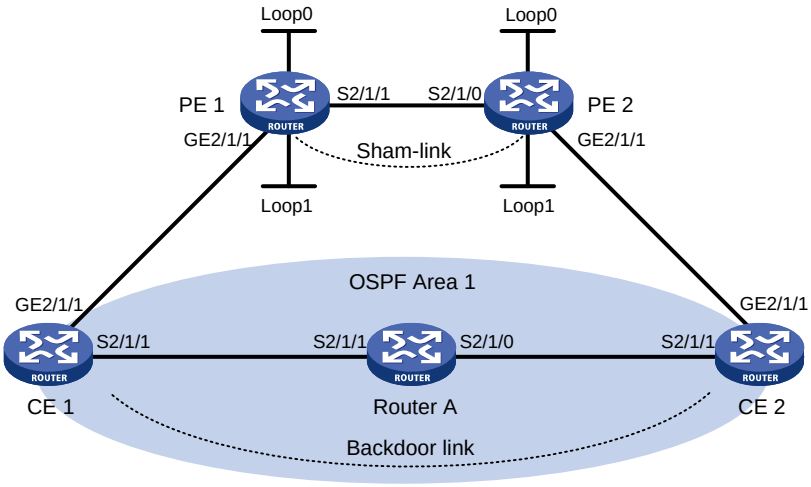
1.14.10 配置OSPF伪连接

1. 组网需求

- CE 1 和 CE 2 都属于 VPN 1，它们分别接入 PE 1 和 PE 2；
- CE 1 和 CE 2 在同一个 OSPF 区域中；
- CE 1 与 CE 2 之间的 VPN 流量通过 MPLS 骨干网转发，不使用 OSPF 的区域内路由。

2. 组网图

图1-33 OSPF 伪连接配置组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	GE2/1/1	100.1.1.1/24	CE 2	GE2/1/1	120.1.1.1/24
	S2/1/1	20.1.1.1/24		S2/1/1	30.1.1.2/24
PE 1	Loop0	1.1.1.9/32	PE 2	Loop0	2.2.2.9/32
	Loop1	3.3.3.3/32		Loop1	5.5.5.5/32
	GE2/1/1	100.1.1.2/24		GE2/1/1	120.1.1.2/24
	S2/1/1	10.1.1.1/24		S2/1/0	10.1.1.2/24
Router A	S2/1/0	30.1.1.1/24			
	S2/1/1	20.1.1.2/24			

3. 配置步骤

(1) 配置用户网络上的 OSPF

在CE 1、Router A、CE 2 上配置普通OSPF，发布 图 1-33 中所示各接口的网段地址。具体配置过程略。

配置完成后，执行 **display ip routing-table** 命令，可以看到 CE 1 和 CE 2 学到了到达对端的路由。

(2) 在骨干网上配置 MPLS L3VPN

配置 PE 1 的 MPLS 基本能力和 MPLS LDP 能力，建立 LDP LSP。

```
<PE1> system-view
[PE1] interface loopback 0
```

```
[PE1-LoopBack0] ip address 1.1.1.9 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] interface serial 2/1/1
[PE1-Serial2/1/1] ip address 10.1.1.1 24
[PE1-Serial2/1/1] mpls enable
[PE1-Serial2/1/1] mpls ldp enable
[PE1-Serial2/1/1] quit
```

配置 PE 1 的 MP-IBGP 对等体为 PE2。

```
[PE1] bgp 100
[PE1-bgp] peer 2.2.2.9 as-number 100
[PE1-bgp] peer 2.2.2.9 connect-interface loopback 0
[PE1-bgp] address-family vpnv4
[PE1-bgp-vpnv4] peer 2.2.2.9 enable
[PE1-bgp-vpnv4] quit
[PE1-bgp] quit
```

配置 PE 1 的 OSPF。

```
[PE1] ospf 1
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

配置 PE 2 的 MPLS 基本能力和 MPLS LDP 能力，建立 LDP LSP。

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 2.2.2.9 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 2.2.2.9
[PE2] mpls ldp
[PE2-ldp] quit
[PE2] interface serial 2/1/1
[PE2-Serial2/1/1] ip address 10.1.1.2 24
[PE2-Serial2/1/1] mpls enable
[PE2-Serial2/1/1] mpls ldp enable
[PE2-Serial2/1/1] quit
```

配置 PE 2 的 MP-IBGP 对等体为 PE1。

```
[PE2] bgp 100
[PE2-bgp] peer 1.1.1.9 as-number 100
[PE2-bgp] peer 1.1.1.9 connect-interface loopback 0
[PE2-bgp] address-family vpnv4
[PE2-bgp-vpnv4] peer 1.1.1.9 enable
[PE2-bgp-vpnv4] quit
[PE2-bgp] quit
```

配置 PE 2 的 OSPF。

```
[PE2] ospf 1
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

(3) 配置 PE 接入 CE

配置 PE 1 接入 CE 1。

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 100:1
[PE1-vpn-instance-vpn1] vpn-target 1:1
[PE1-vpn-instance-vpn1] quit
[PE1] interface gigabitethernet 2/1/1
[PE1-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE1-GigabitEthernet2/1/1] ip address 100.1.1.2 24
[PE1-GigabitEthernet2/1/1] quit
[PE1] ospf 100 vpn-instance vpn1
[PE1-ospf-100] domain-id 10
[PE1-ospf-100] area 1
[PE1-ospf-100-area-0.0.0.1] network 100.1.1.0 0.0.0.255
[PE1-ospf-100-area-0.0.0.1] quit
[PE1-ospf-100] quit
[PE1] bgp 100
[PE1-bgp] ip vpn-instance vpn1
[PE1-bgp-vpn1] address-family ipv4 unicast
[PE1-bgp-ipv4-vpn1] import-route ospf 100
[PE1-bgp-ipv4-vpn1] import-route direct
[PE1-bgp-ipv4-vpn1] quit
[PE1-bgp-vpn1] quit
[PE1-bgp] quit
```

配置 PE 2 接入 CE 2。

```
[PE2] ip vpn-instance vpn1
[PE2-vpn-instance-vpn1] route-distinguisher 100:2
[PE2-vpn-instance-vpn1] vpn-target 1:1
[PE2-vpn-instance-vpn1] quit
[PE2] interface gigabitethernet 2/1/1
[PE2-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE2-GigabitEthernet2/1/1] ip address 120.1.1.2 24
[PE2-GigabitEthernet2/1/1] quit
[PE2] ospf 100 vpn-instance vpn1
[PE2-ospf-100] domain-id 10
[PE2-ospf-100] area 1
[PE2-ospf-100-area-0.0.0.1] network 120.1.1.0 0.0.0.255
[PE2-ospf-100-area-0.0.0.1] quit
[PE2-ospf-100] quit
[PE2] bgp 100
[PE2-bgp] ip vpn-instance vpn1
[PE2-bgp-vpn1] address-family ipv4 unicast
```

```
[PE2-bgp-ipv4-vpn1] import-route ospf 100
[PE2-bgp-ipv4-vpn1] import-route direct
[PE2-bgp-ipv4-vpn1] quit
[PE2-bgp-vpn1] quit
[PE2-bgp] quit
```

完成上述配置后，在 PE 设备上执行 **display ip routing-table vpn-instance** 命令，可以看到去往对端 CE 的路由是通过用户网络的 OSPF 路由，不是通过骨干网的 BGP 路由。

(4) 配置 Sham-link

配置 PE 1。

```
[PE1] interface loopback 1
[PE1-LoopBack1] ip binding vpn-instance vpn1
[PE1-LoopBack1] ip address 3.3.3.3 32
[PE1-LoopBack1] quit
[PE1] ospf 100
[PE1-ospf-100] area 1
[PE1-ospf-100-area-0.0.0.1] sham-link 3.3.3.3 5.5.5.5 cost 10
[PE1-ospf-100-area-0.0.0.1] quit
[PE1-ospf-100] quit
```

配置 PE 2。

```
[PE2] interface loopback 1
[PE2-LoopBack1] ip binding vpn-instance vpn1
[PE2-LoopBack1] ip address 5.5.5.5 32
[PE2-LoopBack1] quit
[PE2] ospf 100
[PE2-ospf-100] area 1
[PE2-ospf-100-area-0.0.0.1] sham-link 5.5.5.5 3.3.3.3 cost 10
[PE2-ospf-100-area-0.0.0.1] quit
[PE2-ospf-100] quit
```

4. 验证配置

完成上述配置后，在 PE 设备上再次执行 **display ip routing-table vpn-instance** 命令，可以看到去往对端 CE 的路由变成了通过骨干网的 BGP 路由，并且有去往 Sham-link 目的地址的路由。

在 CE 设备上执行 **display ip routing-table** 命令，可以看到去往对端 CE 的 OSPF 路由下一跳变为接入 PE 的 Ethernet 接口，即去往对端的 VPN 流量将通过骨干网转发。

在 PE 上执行 **display ospf sham-link** 命令可以看到 Sham-link 的建立情况。

以 PE 1 为例：

```
[PE1] display ospf sham-link

          OSPF Process 100 with Router ID 100.1.1.2
                  Sham link

 Area            Neighbor ID     Source IP       Destination IP  State  Cost
 0.0.0.1         120.1.1.2       3.3.3.3         5.5.5.5         P-2-P  10
```

执行 **display ospf sham-link area** 命令可以看到对端状态为 Full。

```
[PE1] display ospf sham-link area 1
```

```
        OSPF Process 100 with Router ID 100.1.1.2

  Sham link: 3.3.3.3 --> 5.5.5.5
  Neighbor ID: 120.1.1.2     State: Full
  Area: 0.0.0.1
  Cost: 10  State: P-2-P  Type: Sham
  Timers: Hello 10s, Dead 40s, Retransmit 5s, Transmit Delay 1s
  Request list: 0  Retransmit list: 0
```

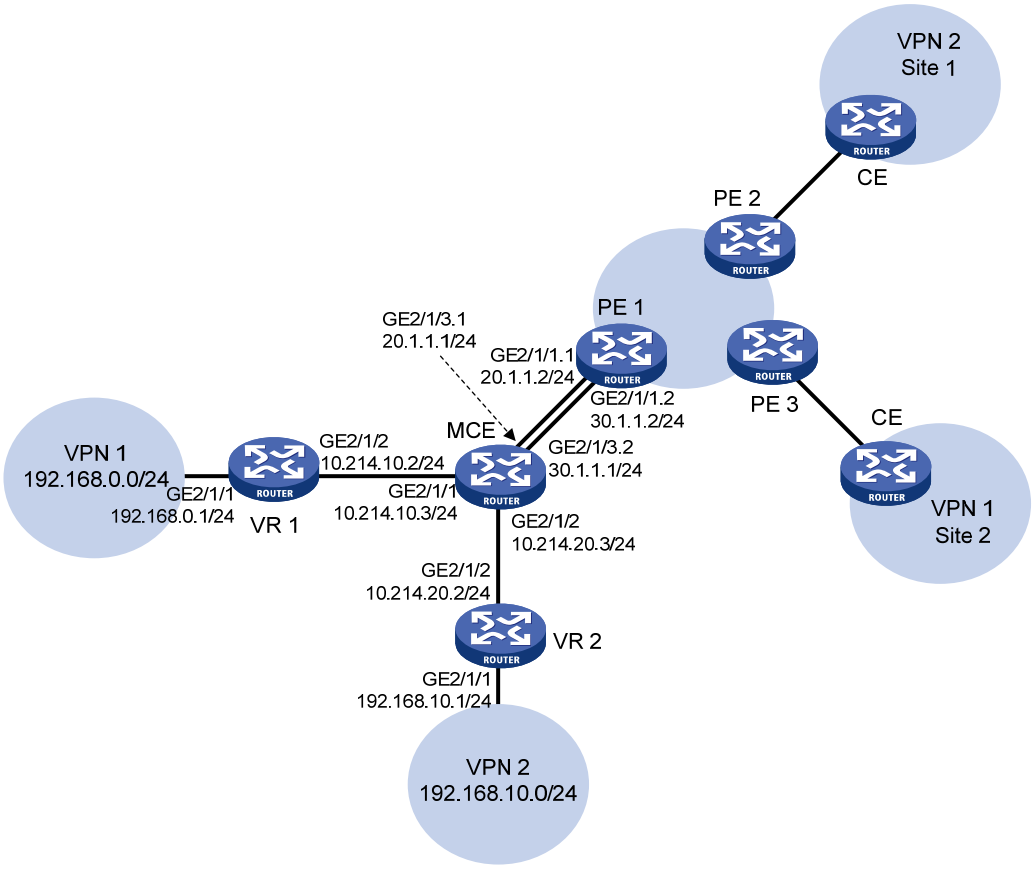
1.14.11 配置MCE示例

1. 组网需求

MCE 设备连接两个 VPN：VPN 1 和 VPN 2。其中，VPN 2 内运行 RIP 路由协议。MCE 设备将两个 VPN 之间的路由隔离，并通过 OSPF 将各 VPN 的路由发布到 PE 1。

2. 组网图

图1-34 配置 MCE 组网图



3. 配置步骤

为区分设备，假设 MCE 系统名为“MCE”，VPN 1 和 VPN 2 的边缘设备分别名为“VR1”和“VR2”，PE 1 系统名为 “PE1”。

(1) 在 MCE 和 PE 1 上配置 VPN 实例

在MCE设备上配置VPN实例，名称分别为vpn1和vpn2，RD分别取值为10:1和20:1，VPN Target取值与RD取相同数值，Export和Import均取此值。

```
<MCE> system-view
[MCE] ip vpn-instance vpn1
[MCE-vpn-instance-vpn1] route-distinguisher 10:1
[MCE-vpn-instance-vpn1] vpn-target 10:1
[MCE-vpn-instance-vpn1] quit
[MCE] ip vpn-instance vpn2
[MCE-vpn-instance-vpn2] route-distinguisher 20:1
[MCE-vpn-instance-vpn2] vpn-target 20:1
[MCE-vpn-instance-vpn2] quit
```

配置接口GigabitEthernet2/1/1与VPN实例vpn1绑定，并配置该接口的地址。

```
[MCE] interface gigabitethernet 2/1/1
[MCE-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[MCE-GigabitEthernet2/1/1] ip address 10.214.10.3 24
[MCE-GigabitEthernet2/1/1] quit
```

配置接口GigabitEthernet2/1/2与VPN实例vpn2绑定，并配置该接口的地址。

```
[MCE] interface gigabitethernet 2/1/2
[MCE-GigabitEthernet2/1/2] ip binding vpn-instance vpn2
[MCE-GigabitEthernet2/1/2] ip address 10.214.20.3 24
[MCE-GigabitEthernet2/1/2] quit
```

在PE 1上配置VPN实例，名称分别为vpn1和vpn2，RD分别取值为30:1和40:1，VPN Target取值分别为10:1和20:1，Export和Import均取此值。

```
<PE1> system-view
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 30:1
[PE1-vpn-instance-vpn1] vpn-target 10:1
[PE1-vpn-instance-vpn1] quit
[PE1] ip vpn-instance vpn2
[PE1-vpn-instance-vpn2] route-distinguisher 40:1
[PE1-vpn-instance-vpn2] vpn-target 20:1
[PE1-vpn-instance-vpn2] quit
```

(2) MCE与Site间路由配置

MCE与VPN 1直接相连，且VPN 1内未使用路由协议，因此可以使用静态路由进行配置。

配置VR1与MCE连接的接口地址为10.214.10.2/24，连接VPN 1接口的地址为192.168.0.1/24。（具体配置过程略）

在VR1上配置缺省路由，指定出方向报文的下一跳地址为10.214.10.3。

```
<VR1> system-view
[VR1] ip route-static 0.0.0.0 0.0.0.0 10.214.10.3
```

在MCE上指定静态路由，去往192.168.0.0/24网段的报文，下一跳地址为10.214.10.2，并将此路由与VPN实例vpn1绑定。

```
[MCE] ip route-static vpn-instance vpn1 192.168.0.0 24 10.214.10.2
```

VPN 2内运行RIP，在MCE上配置RIP进程20，并与VPN实例vpn2绑定，以便将VPN 2内的路由学习到VPN实例vpn2的路由表中。

```
[MCE] rip 20 vpn-instance vpn2
```

发布网段 10.214.20.0 的路由。

```
[MCE-rip-20] network 10.214.20.0
[MCE-rip-20] quit
```

在 VR2 上，配置与 MCE 连接的接口地址为 10.214.20.2/24，连接 VPN 2 接口的地址为 192.168.10.1/24。（配置过程略）

配置 RIP，发布网段 192.168.10.0 和 10.214.20.0 的路由。

```
<VR2> system-view
[VR2] rip 20
[VR2-rip-20] network 192.168.10.0
[VR2-rip-20] network 10.214.20.0
```

在 MCE 上查看 VPN 实例 vpn1 和 vpn2 的路由信息。

```
[MCE] display ip routing-table vpn-instance vpn1

Destinations : 13        Routes : 13

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.214.10.0/24      Direct 0    0            10.214.10.3     GE2/1/1
10.214.10.0/32      Direct 0    0            10.214.10.3     GE2/1/1
10.214.10.3/32      Direct 0    0            127.0.0.1       InLoop0
10.214.10.255/32    Direct 0    0            10.214.10.3     GE2/1/1
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
192.168.0.0/24      Static 60   0            10.214.10.2     GE2/1/1
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
[MCE] display ip routing-table vpn-instance vpn2

Destinations : 13        Routes : 13

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.214.20.0/24      Direct 0    0            10.214.20.3     GE2/1/2
10.214.20.0/32      Direct 0    0            10.214.20.3     GE2/1/2
10.214.20.3/32      Direct 0    0            127.0.0.1       InLoop0
10.214.20.255/32    Direct 0    0            10.214.20.3     GE2/1/2
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
192.168.10.0/24     RIP    100  1            10.214.20.2     GE2/1/2
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

可以看到，MCE 已经通过 RIP 学习到了 VPN 2 内的私网路由，并与 VPN 1 内的路由信息分别维护在两个路由表内，有效地进行了隔离。

(3) MCE 与 PE 间路由配置

MCE 通过子接口与 PE 1 相连。在 MCE 上配置子接口 GigabitEthernet2/1/3.1 与 VPN 实例 vpn1 绑定，配置该子接口终结 VLAN 10，并配置该接口的地址。

```
[MCE] interface gigabitethernet 2/1/3.1
[MCE-GigabitEthernet2/1/3.1] ip binding vpn-instance vpn1
[MCE-GigabitEthernet2/1/3.1] vlan-type dot1q vid 10
[MCE-GigabitEthernet2/1/3.1] ip address 20.1.1.1 24
[MCE-GigabitEthernet2/1/3.1] quit
```

在 MCE 上配置子接口 GigabitEthernet2/1/3.2 与 VPN 实例 vpn2 绑定，配置该子接口终结 VLAN 20，并配置该接口的地址。

```
[MCE] interface gigabitethernet 2/1/3.2
[MCE-GigabitEthernet2/1/3.2] ip binding vpn-instance vpn2
[MCE-GigabitEthernet2/1/3.2] vlan-type dot1q vid 20
[MCE-GigabitEthernet2/1/3.2] ip address 30.1.1.1 24
[MCE-GigabitEthernet2/1/3.2] quit
```

在 PE 1 配置子接口 GigabitEthernet2/1/1.1 与 VPN 实例 vpn1 绑定，配置该子接口终结 VLAN 10，并配置该接口的地址。

```
[PE1] interface gigabitethernet 2/1/1.1
[PE1-GigabitEthernet2/1/1.1] ip binding vpn-instance vpn1
[PE1-GigabitEthernet2/1/1.1] vlan-type dot1q vid 10
[PE1-GigabitEthernet2/1/1.1] ip address 20.1.1.2 24
[PE1-GigabitEthernet2/1/1.1] quit
```

在 PE 1 上配置子接口 GigabitEthernet2/1/1.2 与 VPN 实例 vpn2 绑定，配置该子接口终结 VLAN 20，并配置该接口的地址。

```
[PE1] interface gigabitethernet 2/1/1.2
[PE1-GigabitEthernet2/1/1.2] ip binding vpn-instance vpn2
[PE1-GigabitEthernet2/1/1.2] vlan-type dot1q vid 20
[PE1-GigabitEthernet2/1/1.2] ip address 30.1.1.2 24
[PE1-GigabitEthernet2/1/1.2] quit
```

配置 MCE 和 PE 1 的 Loopback0 接口，用于指定 MCE 和 PE 1 的 Router ID，地址分别为 101.101.10.1 和 100.100.10.1。配置步骤这里省略。

配置 MCE 启动 OSPF 进程 10，该进程绑定到 VPN 实例 vpn1，关闭 OSPF 实例的路由环路检测功能，并配置域 ID 为 10。

```
[MCE] ospf 10 router-id 101.101.10.1 vpn-instance vpn1
[MCE-ospf-10] vpn-instance-capability simple
[MCE-ospf-10] domain-id 10
```

在 Area0 区域发布 20.1.1.0/24 网段路由，并引入 VPN 1 的静态路由。

```
[MCE-ospf-10] area 0
[MCE-ospf-10-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[MCE-ospf-10-area-0.0.0.0] quit
[MCE-ospf-10] import-route static
```

配置 PE 1 启动 OSPF 进程 10，绑定到 VPN 实例 vpn1，域 ID 为 10，在 Area0 区域发布 20.1.1.0/24 网段路由。

```
[PE1] ospf 10 router-id 100.100.10.1 vpn-instance vpn1
[PE1-ospf-10] domain-id 10
[PE1-ospf-10] area 0
[PE1-ospf-10-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[PE1-ospf-10-area-0.0.0.0] quit
[PE1-ospf-10] quit
```

MCE 与 PE 1 间配置 OSPF 进程 20，导入 VPN 实例 vpn2 的路由信息的过程与上面介绍的配置基本一致，不同的是在 MCE 的 OSPF 中配置导入的是 RIP 进程 20 的路由，这里不再赘述。

4. 验证配置

显示 PE 1 上的 VPN 1 路由信息。可以看到，VPN 1 内的静态路由已经引入到 MCE 与 PE 1 间的 OSPF 路由表中。

```
[PE1] display ip routing-table vpn-instance vpn1

Destinations : 13        Routes : 13

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.2        GE2/1/1.1
20.1.1.0/32         Direct 0    0            20.1.1.2        GE2/1/1.1
20.1.1.2/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.255/32       Direct 0    0            20.1.1.2        GE2/1/1.1
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
192.168.0.0/24      O_ASE  150  1            20.1.1.1        GE2/1/1.1
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

显示 PE 1 上的 VPN 2 路由信息。可以看到，VPN 2 内的 RIP 路由已经引入到 MCE 与 PE 1 间的 OSPF 路由表中。

```
[PE1] display ip routing-table vpn-instance vpn2

Destinations : 13        Routes : 13

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Direct 0    0            30.1.1.2        GE2/1/1.2
30.1.1.0/32         Direct 0    0            30.1.1.2        GE2/1/1.2
30.1.1.2/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.255/32       Direct 0    0            30.1.1.2        GE2/1/1.2
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
192.168.10.0/24     O_ASE  150  1            30.1.1.1        GE2/1/1.2
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
```

```
224.0.0.0/24        Direct 0    0           0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
```

至此，通过配置，已经将两个 VPN 实例内的路由信息完整地传播到 PE 1 中，配置完成。

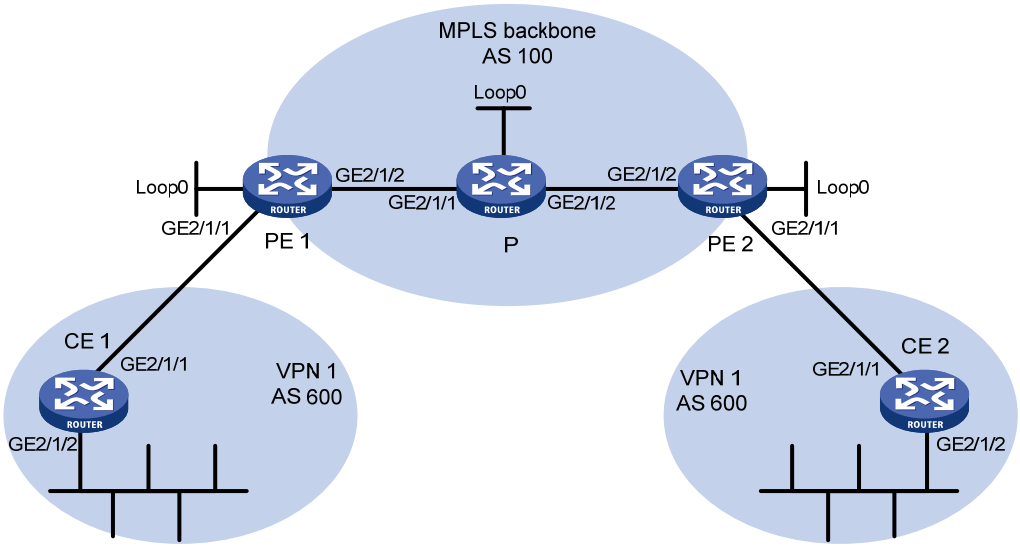
1.14.12 配置BGP的AS号替换

1. 组网需求

如图所示，CE 1 和 CE 2 同属于 VPN 1，分别接入 PE 1 和 PE 2，并且 CE 1 和 CE 2 复用 AS 号 600。

2. 组网图

图1-35 BGP 的 AS 号替换组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	GE2/1/1	10.1.1.1/24	P	Loop0	2.2.2.9/32
	GE2/1/2	100.1.1.1/24		GE2/1/1	20.1.1.2/24
PE 1	Loop0	1.1.1.9/32		GE2/1/2	30.1.1.1/24
	GE2/1/1	10.1.1.2/24	PE 2	Loop0	3.3.3.9/32
	GE2/1/2	20.1.1.1/24		GE2/1/1	10.2.1.2/24
CE 2	GE2/1/1	10.2.1.1/24		GE2/1/2	30.1.1.2/24
	GE2/1/2	200.1.1.1/24			

3. 配置步骤

(1) 配置基本 MPLS L3VPN

- 在 MPLS 骨干网上配置 OSPF，PE 和 P 之间能够学到对方 Loopback 接口的路由；
- 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP；
- PE 之间建立 MP-IBGP 对等体关系，发布 VPN-IPv4 路由；
- 在 PE 2 上配置 VPN 1 的 VPN 实例，接入 CE 2；
- 在 PE 1 上配置 VPN 1 的 VPN 实例，接入 CE 1；
- PE 1 和 CE 1、PE 2 和 CE 2 之间配置 BGP，将 CE 的路由引入 PE。

上述配置可参考“1.14.1 配置MPLS L3VPN示例”，具体配置过程略。

完成上述配置后，在 CE 2 上执行 **display ip routing-table** 命令，可以看到 CE 2 能够学到 CE 1 接入 PE 1 的接口所在网段（10.1.1.0/24）的路由，但没有到达 CE 1 内部 VPN（100.1.1.0/24）的路由。CE 1 上也存在同样的现象。

```
<CE2> display ip routing-table

Destinations : 17        Routes : 17

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.1.1.0/24         BGP    255  0            10.2.1.2        GE2/1/1
10.2.1.0/24         Direct 0    0            10.2.1.1        GE2/1/1
10.2.1.0/32         Direct 0    0            10.2.1.1        GE2/1/1
10.2.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.255/32       Direct 0    0            10.2.1.1        GE2/1/1
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
200.1.1.0/24        Direct 0    0            200.1.1.1       GE2/1/2
200.1.1.0/32        Direct 0    0            200.1.1.1       GE2/1/2
200.1.1.1/32        Direct 0    0            127.0.0.1       InLoop0
200.1.1.255/24      Direct 0    0            200.1.1.1       GE2/1/2
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

在 PE 上执行 **display ip routing-table vpn-instance** 命令，可以看到 PE 的 VPN 实例中有到达对端 CE 内部 VPN 的路由。

以 PE 2 为例：

```
<PE2> display ip routing-table vpn-instance vpn1

Destinations : 15        Routes : 15

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.1.1.0/24         BGP    255  0            1.1.1.9         GE2/1/2
10.2.1.0/24         Direct 0    0            10.2.1.2        GE2/1/1
10.2.1.0/32         Direct 0    0            10.2.1.2        GE2/1/1
10.2.1.2/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.255/32       Direct 0    0            10.2.1.2        GE2/1/1
100.1.1.0/24        BGP    255  0            1.1.1.9         GE2/1/2
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
200.1.1.0/24        BGP    255  0            10.2.1.1        GE2/1/1
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
```

```
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

在 PE 2 上打开 BGP 的 Update 报文调试信息开关，可以看到 PE 2 发布了去往 100.1.1.0/24 的路由，AS 路径信息为“100 600”。

```
<PE2> terminal monitor
<PE2> terminal logging level 7
<PE2> debugging bgp update vpn-instance vpn1 10.2.1.1 ipv4
<PE2> refresh bgp all export ipv4 vpn-instance vpn1
*Jun 13 16:12:52:096 2012 PE2 BGP/7/DEBUG: ;
         BGP.vpn1: Send UPDATE to peer 10.2.1.1 for following destinations:
         Origin       : Incomplete
         AS Path      : 100 600
         Next Hop     : 10.2.1.2
         100.1.1.0/24,
```

在 CE 2 上执行 **display bgp routing-table ipv4 peer received-routes** 命令，可以看到 CE 2 没有接收 100.1.1.0/24 的路由。

```
<CE2> display bgp routing-table ipv4 peer 10.2.1.2 received-routes

 Total number of routes: 2

 BGP local router ID is 200.1.1.1
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >e 10.1.1.0/24        10.2.1.2                               0       100?
*  e 10.2.1.0/24        10.2.1.2        0                      0       100?
```

(2)　配置 BGP 的 AS 号替换功能

在 PE 2 上配置 BGP 的 AS 号替换功能。

```
<PE2> system-view
[PE2] bgp 100
[PE2-bgp] ip vpn-instance vpn1
[PE2-bgp-vpn1] peer 10.2.1.1 substitute-as
[PE2-bgp-vpn1] address-family ipv4 unicast
[PE2-bgp-ipv4-vpn1] peer 10.2.1.1 enable
[PE2-bgp-ipv4-vpn1] quit
[PE2-bgp-vpn1] quit
[PE2-bgp] quit
```

4. 验证配置

可以看到 PE 2 向 CE 2 发布的路由中，100.1.1.0/24 的 AS 路径信息由“100 600”变为“100 100”：

```
*Jun 13 16:15:59:456 2012 PE2 BGP/7/DEBUG;
         BGP.vpn1: Send UPDATE to peer 10.2.1.1 for following destinations:
         Origin       : Incomplete
         AS Path      : 100 100
         Next Hop     : 10.2.1.2
```

```
        100.1.1.0/24,
```

再次查看 CE 2 接收的路由信息和路由表。

```
<CE2> display bgp routing-table ipv4 peer 10.2.1.2 received-routes

 Total number of routes: 3

 BGP local router ID is 200.1.1.1
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >e 10.1.1.0/24        10.2.1.2                               0       100?
*  e 10.2.1.0/24        10.2.1.2        0                      0       100?
* >e 100.1.1.0/24       10.2.1.2                               0       100 100?
<CE2> display ip routing-table

Destinations : 18        Routes : 18

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.1.1.0/24         BGP    255  0            10.2.1.2        GE2/1/1
10.2.1.0/24         Direct 0    0            10.2.1.1        GE2/1/1
10.2.1.0/32         Direct 0    0            10.2.1.1        GE2/1/1
10.2.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.255/32       Direct 0    0            10.2.1.1        GE2/1/1
100.1.1.0/24        BGP    255  0            10.2.1.2        GE2/1/1
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
200.1.1.0/24        Direct 0    0            200.1.1.1       GE2/1/2
200.1.1.0/32        Direct 0    0            200.1.1.1       GE2/1/2
200.1.1.1/32        Direct 0    0            127.0.0.1       InLoop0
200.1.1.255/32      Direct 0    0            200.1.1.1       GE2/1/2
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

在 PE 1 上也配置 BGP 的 AS 号替换功能后，CE 1 和 CE 2 的 Ethernet 接口能够相互 Ping 通。

1.14.13 配置BGP的AS号替换和SoO属性

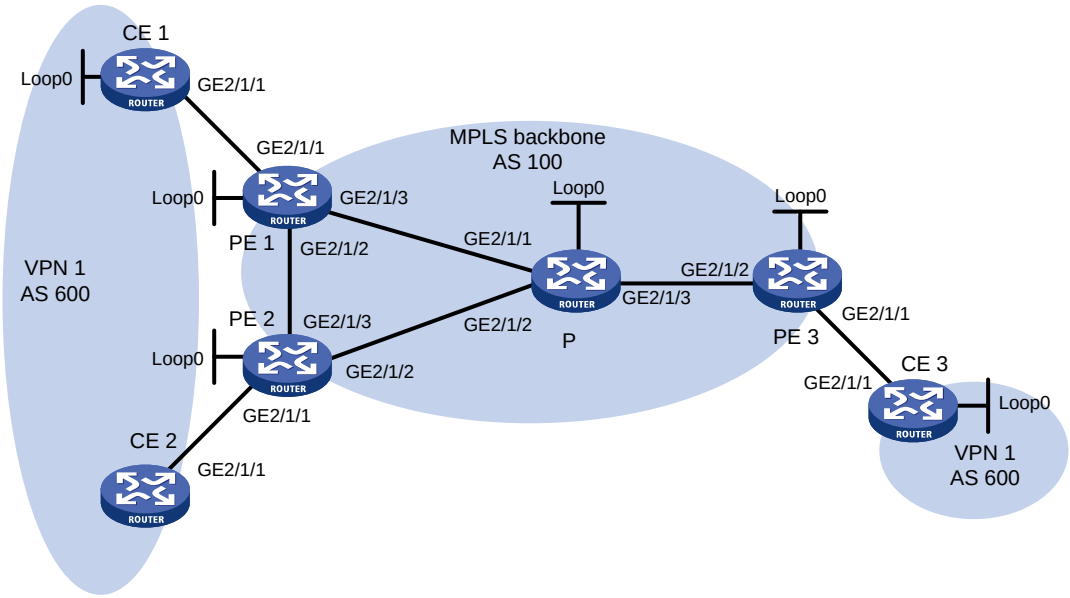
1. 组网需求

- CE 1、CE 2 和 CE 3 同属于 VPN 1，分别接入 PE 1、PE 2 和 PE 3。
- CE 1 和 CE 2 位于同一个站点。
- CE 1、CE 2 和 CE 3 复用 AS 号 600。

- 为了避免路由丢失，在 PE 上配置 AS 号替换；为了避免路由在 CE 1 和 CE 2 之间产生环路，在 PE 1 和 PE 2 上分别为 CE 1 和 CE 2 配置相同的 SoO 属性。

2. 组网图

图1-36 BGP 的 AS 号替换和 SoO 属性组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	Loop0	100.1.1.1/32	CE 3	Loop0	200.1.1.1 /32
	GE2/1/1	10.1.1.1/24		GE2/1/1	10.3.1.1/24
CE 2	GE2/1/1	10.2.1.1/24	PE 2	Loop0	2.2.2.9/32
PE 1	Loop0	1.1.1.9/32		GE2/1/1	10.2.1.2/24
	GE2/1/1	10.1.1.2/24		GE2/1/2	40.1.1.1/24
	GE2/1/2	20.1.1.1/24		GE2/1/3	20.1.1.2/24
	GE2/1/3	30.1.1.1/24	P	Loop0	3.3.3.9/32
PE 3	Loop0	4.4.4.9/32		GE2/1/1	30.1.1.2/24
	GE2/1/1	10.3.1.2/24		GE2/1/2	40.1.1.2/24
	GE2/1/2	50.1.1.2/24		GE2/1/3	50.1.1.1/24

3. 配置步骤

(1) 配置基本 MPLS L3VPN

- 在 MPLS 骨干网上配置 OSPF，PE 和 P 之间能够学到对方 Loopback 接口的路由；
- 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP；
- PE 之间建立 MP-IBGP 对等体关系，发布 VPNv4 路由；
- 在 PE 1 上配置 VPN 1 的 VPN 实例，接入 CE 1；
- 在 PE 2 上配置 VPN 1 的 VPN 实例，接入 CE 2；
- 在 PE 3 上配置 VPN 1 的 VPN 实例，接入 CE 3；
- PE 1 和 CE 1、PE 2 和 CE 2、PE 3 和 CE 3 之间配置 BGP，将 CE 的路由引入 PE。

上述配置可参考“1.14.1 配置MPLS L3VPN示例”，具体配置过程略。

(2) 配置 BGP 的 AS 号替换功能

在PE 1、PE 2 和PE 3 上配置BGP的AS号替换功能，具体配置参见“1.14.12 配置BGP的AS号替换”。

查看 CE 2 接收的路由信息，可以看到 CE 1 发来的路由 100.1.1.1/32。可见，由于 CE 1 和 CE 2 位于同一站点，造成了路由环路。

```
<CE2> display bgp routing-table ipv4 peer 10.2.1.2 received-routes

Total number of routes: 6

 BGP local router ID is 1.1.1.9
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >e 10.1.1.0/24        10.2.1.2                               0       100?
*    10.2.1.0/24        10.2.1.2        0                      0       100?
*    10.2.1.1/32        10.2.1.2        0                      0       100?
* >e 10.3.1.0/24        10.2.1.2                               0       100?
* >e 100.1.1.1/32       10.2.1.2                               0       100 100?
* >e 200.1.1.1/32       10.2.1.2                               0       100 100?
```

(3) 配置 BGP 的 SoO 属性

在 PE 1 上为对等体 CE 1 配置 SoO 属性为 1:100。

```
<PE1> system-view
[PE1] bgp 100
[PE1-bgp] ip vpn-instance vpn1
[PE1-bgp-vpn1] address-family ipv4
[PE1-bgp-ipv4-vpn1] peer 10.1.1.1 soo 1:100
```

在 PE 2 上为对等体 CE 2 配置 SoO 属性为 1:100。

```
<PE2> system-view
[PE2] bgp 100
[PE2-bgp] ip vpn-instance vpn1
[PE2-bgp-vpn1] address-family ipv4
[PE2-bgp-ipv4-vpn1] peer 10.2.1.1 soo 1:100
```

4. 验证配置

由于配置的 SoO 属性相同，PE 2 不会将 CE 1 发过来的路由发布给 CE 2。查看 CE 2 路由表，不会再看到 100.1.1.1/32 路由。

```
<CE2> display ip routing-table

Destinations : 14        Routes : 14

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.2.1.0/24         Direct 0    0            10.2.1.1        GE2/1/1
10.2.1.0/32         Direct 0    0            10.2.1.1        GE2/1/1
10.2.1.1/32         Direct 0    0            127.0.0.1       Inloop0
```

```
10.2.1.255/32       Direct 0    0           10.2.1.1        GE2/1/1
10.3.1.0/24         BGP    255  0           10.2.1.2        GE2/1/1
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
200.1.1.1/32        BGP    255  0           10.2.1.2        GE2/1/1
224.0.0.0/4         Direct 0    0           0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0           0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
```

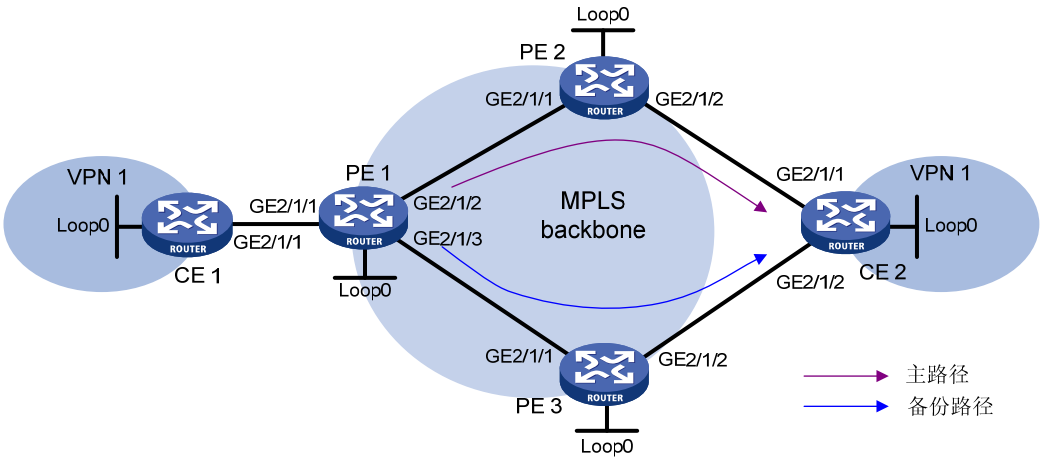
1.14.14 配置MPLS L3VPN快速重路由示例一

1. 组网需求

- CE 1 和 CE 2 属于 VPN 1。
- CE 与 PE 之间配置 EBGP 交换 VPN 路由信息。
- PE 与 PE 之间配置 OSPF 实现 PE 内部的互通、配置 MP-IBGP 交换 VPNv4 路由信息。
- 在 PE 1 上配置 MPLS L3VPN 快速重路由功能。PE 1 和 PE 2 之间的路径正常工作时，CE 1 通过路径 CE 1—PE 1—PE 2—CE 2 将流量转发给 CE 2；PE 1 通过 BFD 检测出 PE 1 到 PE 2 的公网 LSP 出现故障后，将流量切换到备份路径，即 CE 1 通过路径 CE 1—PE 1—PE 3—CE 2 将流量转发给 CE 2，从而缩短故障恢复时间。

2. 组网图

图1-37 MPLS L3VPN 快速重路由示例一组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	Loop0	5.5.5.5/32	PE 1	Loop0	1.1.1.1/32
	GE2/1/1	10.2.1.1/24		GE2/1/1	10.2.1.2/24
PE 2	Loop0	2.2.2.2/32		GE2/1/2	172.1.1.1/24
	GE2/1/1	172.1.1.2/24		GE2/1/3	172.2.1.1/24
	GE2/1/2	10.1.1.2/24	CE 2	Loop0	4.4.4.4/32
PE 3	Loop0	3.3.3.3/32		GE2/1/1	10.1.1.1/24
	GE2/1/1	172.2.1.3/24		GE2/1/2	10.3.1.1/24
	GE2/1/2	10.3.1.2/24			

3. 配置步骤

(1)　配置各路由器接口的 IP 地址、BGP 路由协议和 MPLS L3VPN

请按照上面的组网图配置各接口的 IP 地址和子网掩码。

完成MPLS L3VPN基本配置，具体配置过程请参见“1.14.1 配置MPLS L3VPN示例”。

(2)　配置 MPLS L3VPN 快速重路由

在 PE 1 上配置使用 BFD 检测到达 2.2.2.2/32（PE 1 到达 PE 2）的公网 LSP 的连通性。

```
<PE1> system-view
[PE1] mpls bfd enable
[PE1] mpls bfd 2.2.2.2 32
```

在 PE 1 上创建路由策略 frr，为路由 4.4.4.4/32 指定快速重路由的备份下一跳地址为 3.3.3.3（PE 3 的地址）。

```
[PE1] ip prefix-list abc index 10 permit 4.4.4.4 32
[PE1] route-policy frr permit node 10
[PE1-route-policy] if-match ip address prefix-list abc
[PE1-route-policy] apply fast-reroute backup-nexthop 3.3.3.3
[PE1-route-policy] quit
```

在 PE 1 上配置 VPN 实例 vpn1 的快速重路由功能引用路由策略 frr。

```
[PE1] bgp 100
[PE1-bgp] ip vpn-instance vpn1
[PE1-bgp-vpn1] address-family ipv4 unicast
[PE1-bgp-ipv4-vpn1] fast-reroute route-policy frr
[PE1-bgp-ipv4-vpn1] quit
[PE1-bgp-vpn1] quit
```

在 PE 1 上配置从 PE 2 接收到的 BGP VPNv4 路由的首选值为 100，大于从 PE 3 接收到的路由的首选值 0，以保证 PE 1 优选从 PE 2 接收到的路由。

```
[PE1-bgp] address-family vpnv4
[PE1-bgp-vpnv4] peer 2.2.2.2 preferred-value 100
[PE1-bgp-vpnv4] quit
[PE1-bgp] quit
```

在 PE 2 上使能 MPLS BFD 功能。

```
<PE2> system-view
[PE2] mpls bfd enable
```

4. 验证配置

在 PE 1 上查看私网路由 4.4.4.4/32，可以看到备份下一跳信息。

```
[PE1] display ip routing-table vpn-instance vpn1 4.4.4.4 32 verbose

Summary Count : 1

Destination: 4.4.4.4/32
   Protocol: BGP             Process ID: 0
  SubProtID: 0x1                    Age: 00h00m03s
       Cost: 0              Preference: 255
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active Adv
```

```
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x102               OrigAs: 300
      NibID: 0x15000002          LastAs: 300
     AttrID: 0x2                Neighbor: 2.2.2.2
      Flags: 0x110060       OrigNextHop: 2.2.2.2
      Label: 1146           RealNextHop: 172.1.1.2
    BkLabel: 1275             BkNextHop: 172.2.1.3
  Tunnel ID: Invalid          Interface: GE2/1/2
BkTunnel ID: Invalid        BkInterface: GE2/1/3
   FtnIndex: 0x0
```

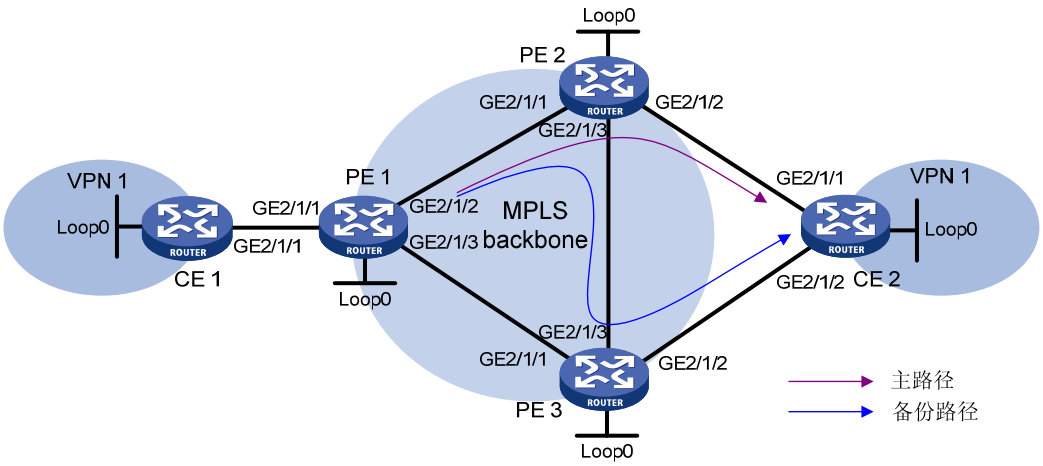
1.14.15 配置MPLS L3VPN快速重路由示例二

1. 组网需求

- CE 1 和 CE 2 属于 VPN 1。
- CE 与 PE 之间配置 EBGP 交换 VPN 路由信息。
- PE 与 PE 之间配置 OSPF 实现 PE 内部的互通、配置 MP-IBGP 交换 VPNv4 路由信息。
- 在 PE 2 上配置 MPLS L3VPN 快速重路由功能。PE 2 和 CE 2 之间的路径正常工作时，CE 1 通过路径 CE 1—PE 1—PE 2—CE 2 将流量转发给 CE 2；PE 2 通过 BFD 检测出 PE 2 到 CE 2 这条路径出现故障后，将流量切换到备份路径，即 CE 1 通过路径 CE 1—PE 1—PE 2—PE3—CE 2 将流量转发给 CE 2，从而缩短故障恢复时间。

2. 组网图

图1-38 配置 MPLS L3VPN 快速重路由示例二组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	Loop0	5.5.5.5/32	PE 2	Loop0	2.2.2.2/32
	GE2/1/1	10.2.1.1/24		GE2/1/1	172.1.1.2/24
PE 1	Loop0	1.1.1.1/32		GE2/1/2	10.1.1.2/24
	GE2/1/1	10.2.1.2/24		GE2/1/3	172.3.1.2/24
	GE2/1/2	172.1.1.1/24	PE 3	Loop0	3.3.3.3/32
	GE2/1/3	172.2.1.1/24		GE2/1/1	172.2.1.3/24
CE 2	Loop0	4.4.4.4/32		GE2/1/2	10.3.1.2/24
	GE2/1/1	10.1.1.1/24		GE2/1/3	172.3.1.3/24
	GE2/1/2	10.3.1.1/24			

3. 配置步骤

(1)　配置各路由器接口的 IP 地址、BGP 路由协议和 MPLS L3VPN

请按照上面的组网图配置各接口的 IP 地址和子网掩码。

完成MPLS L3VPN基本配置，具体配置过程请参见“1.14.1 配置MPLS L3VPN示例”。

(2)　配置 MPLS L3VPN 快速重路由

在 PE 2 上配置 BFD echo 报文的源 IP 地址为 12.1.1.1。

```
<PE2> system-view
[PE2] bfd echo-source-ip 12.1.1.1
```

在 PE 2 上创建路由策略 frr，为路由 4.4.4.4/32 指定快速重路由的备份下一跳地址为 3.3.3.3（PE 3 的地址）。

```
[PE2] ip prefix-list abc index 10 permit 4.4.4.4 32
[PE2] route-policy frr permit node 10
[PE2-route-policy] if-match ip address prefix-list abc
[PE2-route-policy] apply fast-reroute backup-nexthop 3.3.3.3
[PE2-route-policy] quit
```

在 PE 2 上配置通过 Echo 方式的 BFD 会话检测主路由的下一跳是否可达。

```
[PE2] bgp 100
[PE2-bgp] primary-path-detect bfd echo
```

在 PE 2 上配置 VPN 实例 vpn1 的快速重路由功能引用路由策略 frr。

```
[PE2-bgp] ip vpn-instance vpn1
[PE2-bgp-vpn1] address-family ipv4 unicast
[PE2-bgp-ipv4-vpn1] fast-reroute route-policy frr
```

在 PE 2 上配置从 CE 2 接收到的 BGP 路由的首选值为 200，大于从 PE 3 接收到的路由的首选值 0，以保证 PE 2 优选从 CE 2 接收到的路由。

```
[PE2-bgp-ipv4-vpn1] peer 10.1.1.1 preferred-value 200
[PE2-bgp-vpn1] quit
[PE2-bgp] quit
```

4. 验证配置

在 PE 2 上查看私网路由 4.4.4.4/32，可以看到备份下一跳信息。

```
[PE2] display ip routing-table vpn-instance vpn1 4.4.4.4 32 verbose

Summary Count : 1

Destination: 4.4.4.4/32
   Protocol: BGP             Process ID: 0
  SubProtID: 0x2                    Age: 01h54m24s
       Cost: 0              Preference: 10
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active Adv
  OrigTblID: 0x0               OrigVrf: vpn1
    TableID: 0x102              OrigAs: 300
      NibID: 0x15000002         LastAs: 300
     AttrID: 0x0              Neighbor: 10.1.1.1
      Flags: 0x10060       OrigNextHop: 10.1.1.1
```

```
      Label: NULL           RealNextHop: 10.1.1.1
    BkLabel: 1275             BkNextHop: 172.3.1.3
  Tunnel ID: Invalid          Interface: GE2/1/2
BkTunnel ID: 0x409          BkInterface: GE2/1/3
   FtnIndex: 0x0
```

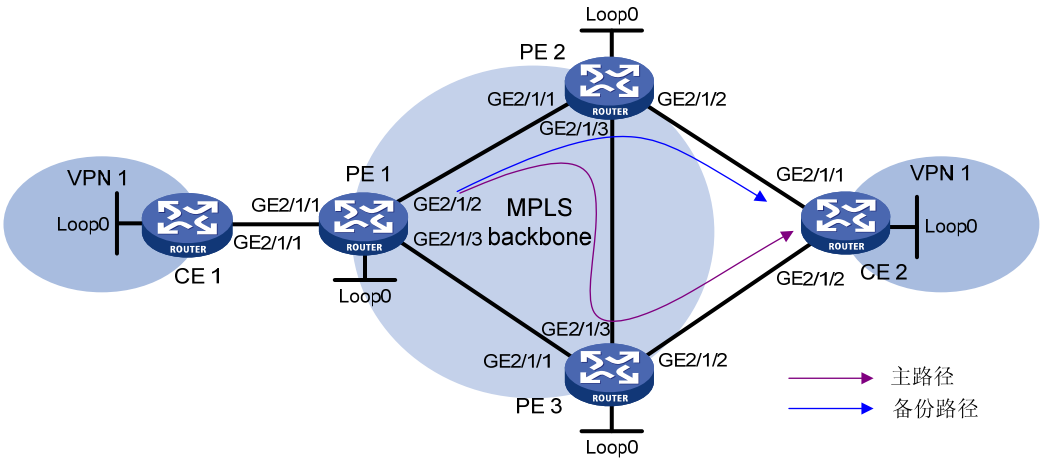
1.14.16 配置MPLS L3VPN快速重路由示例三

1. 组网需求

- CE 1 和 CE 2 属于 VPN 1；
- CE 与 PE 之间配置 EBGP 交换 VPN 路由信息；
- PE 与 PE 之间配置 OSPF 实现 PE 内部的互通、配置 MP-IBGP 交换 VPNv4 路由信息。
- 在 PE 2 上配置 MPLS L3VPN 快速重路由功能。PE 2 和 PE 3 之间的路径正常工作时，CE 1 通过路径 CE 1—PE 1—PE 2—PE 3—CE 2 将流量转发给 CE 2；PE 2 通过 BFD 检测出 PE 2 到 PE 3 这条路径出现故障后，将流量切换到备份路径，即 CE 1 通过路径 CE 1—PE 1—PE 2—CE 2 将流量转发给 CE 2，从而缩短故障恢复时间。

2. 组网图

图1-39 配置 MPLS L3VPN 快速重路由示例三组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	Loop0	5.5.5.5/32	PE 2	Loop0	2.2.2.2/32
	GE2/1/1	10.2.1.1/24		GE2/1/1	172.1.1.2/24
PE 1	Loop0	1.1.1.1/32		GE2/1/2	10.1.1.2/24
	GE2/1/1	10.2.1.2/24		GE2/1/3	172.3.1.2/24
	GE2/1/2	172.1.1.1/24	PE 3	Loop0	3.3.3.3/32
	GE2/1/3	172.2.1.1/24		GE2/1/1	172.2.1.3/24
CE 2	Loop0	4.4.4.4/32		GE2/1/2	10.3.1.2/24
	GE2/1/1	10.1.1.1/24		GE2/1/3	172.3.1.3/24
	GE2/1/2	10.3.1.1/24			

3. 配置步骤

(1) 配置各路由器接口的 IP 地址、BGP 路由协议和 MPLS L3VPN

请按照上面的组网图配置各接口的 IP 地址和子网掩码。

完成MPLS L3VPN基本配置, 具体配置过程请参见“1.14.1 配置MPLS L3VPN示例”。

(2) 配置 MPLS L3VPN 快速重路由

在 PE 2 上配置使用 BFD 检测到达 3.3.3.3/32（PE 2 到达 PE 3）的公网 LSP 的连通性。

```
<PE2> system-view
[PE2] mpls bfd enable
[PE2] mpls bfd 3.3.3.3 32
```

在 PE 2 上创建路由策略 frr，为路由 4.4.4.4/32 指定快速重路由的备份下一跳地址为 10.1.1.1（CE 2 的地址）。

```
[PE2] ip prefix-list abc index 10 permit 4.4.4.4 32
[PE2] route-policy frr permit node 10
[PE2-route-policy] if-match ip address prefix-list abc
[PE2-route-policy] apply fast-reroute backup-nexthop 10.1.1.1
[PE2-route-policy] quit
```

在 PE 2 上配置 VPN 实例 vpn1 的快速重路由功能引用路由策略 frr。

```
[PE2] bgp 100
[PE2-bgp] ip vpn-instance vpn1
[PE2-bgp-vpn1] address-family ipv4 unicast
[PE2-bgp-ipv4-vpn1] fast-reroute route-policy frr
[PE2-bgp-ipv4-vpn1] quit
[PE2-bgp-vpn1] quit
```

在 PE 2 上配置从 PE 3 接收到的 BGP VPNv4 路由的首选值为 200，大于从 CE 2 接收到的 IPv4 单播路由的首选值 0，以保证 PE 2 优选从 PE 3 接收到的路由。

```
[PE2-bgp] address-family vpnv4
[PE2-bgp-vpnv4] peer 3.3.3.3 preferred-value 200
[PE2-bgp-vpnv4] quit
[PE2-bgp] quit
```

在 PE 3 上使能 MPLS BFD 功能。

```
<PE3> system-view
[PE3] mpls bfd enable
```

4. 验证配置

在 PE 2 上查看私网路由 4.4.4.4/32，可以看到备份下一跳信息。

```
[PE2] display ip routing-table vpn-instance vpn1 4.4.4.4 32 verbose

Summary Count : 1

Destination: 4.4.4.4/32
   Protocol: BGP             Process ID: 0
  SubProtID: 0x1                    Age: 00h00m04s
       Cost: 0              Preference: 255
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x102              OrigAs: 300
      NibID: 0x15000004         LastAs: 300
     AttrID: 0x1              Neighbor: 3.3.3.3
      Flags: 0x110060       OrigNextHop: 3.3.3.3
      Label: 1275           RealNextHop: 172.3.1.3
```

```
     BkLabel: NULL              BkNextHop: 10.1.1.1
   Tunnel ID: 0x409             Interface: GE2/1/3
BkTunnel ID: Invalid         BkInterface: GE2/1/2
   FtnIndex: 0x0
```

2 IPv6 MPLS L3VPN

2.1 IPv6 MPLS L3VPN简介

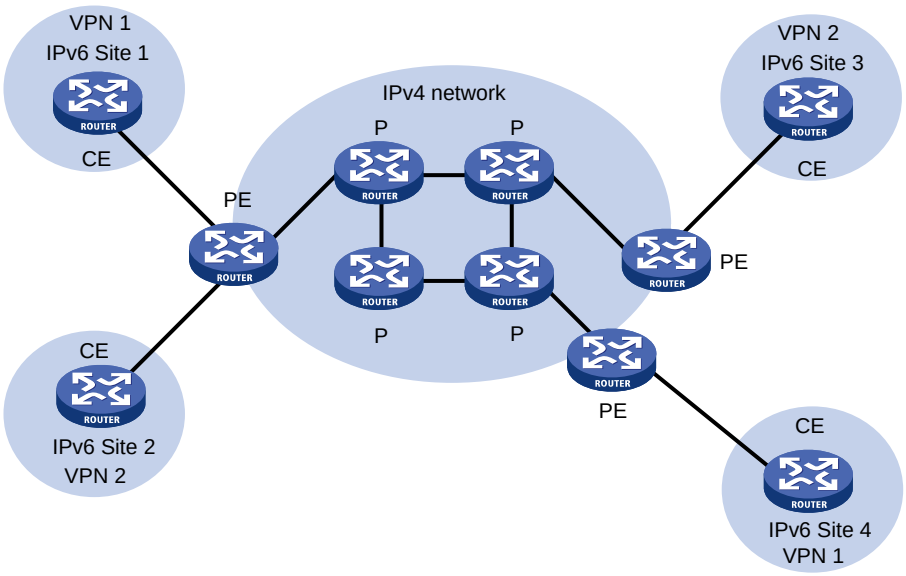
2.1.1 IPv6 MPLS L3VPN概述

MPLS L3VPN 应用于 IPv4 组网环境，利用 BGP 在服务提供商骨干网上发布 VPN 的 IPv4 路由，利用 MPLS 在服务提供商骨干网上转发 VPN 的 IPv4 报文。

IPv6 MPLS L3VPN 的原理与 MPLS L3VPN 相同，所不同的是 IPv6 MPLS L3VPN 利用 BGP 在服务提供商骨干网上发布 VPN 的 IPv6 路由，利用 MPLS 在服务提供商骨干网上转发 VPN 的 IPv6 报文。

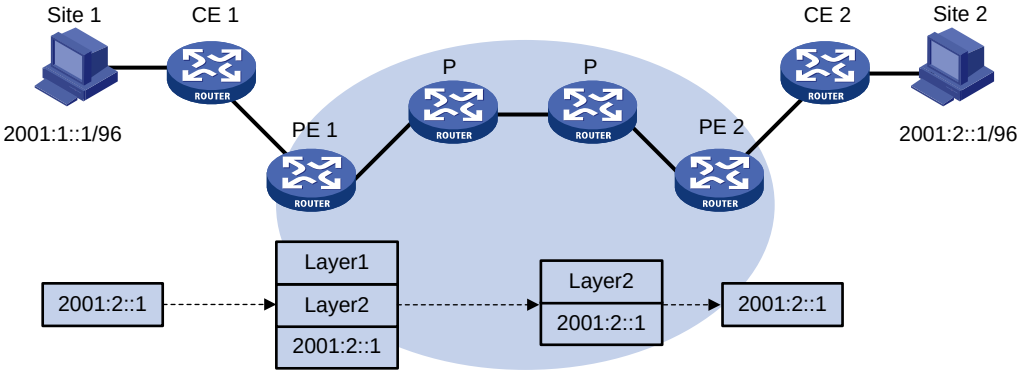
IPv6 MPLS L3VPN的典型组网环境如 图 2-1 所示。目前，IPv6 MPLS L3VPN组网中服务提供商骨干网应为IPv4 网络。VPN内部及CE和PE之间运行IPv6 协议，骨干网中PE和P设备之间运行IPv4 协议。PE需要同时支持IPv4 和IPv6 协议，连接CE的接口上使用IPv6 协议，连接骨干网的接口上使用IPv4 协议。

图2-1 IPv6 MPLS L3VPN 应用组网图



2.1.2 IPv6 MPLS L3VPN的报文转发

图2-2 IPv6 MPLS L3VPN 报文转发示意图



如 图 2-2 所示，IPv6 MPLS L3VPN的报文转发过程为：

(1) Site 1 发出一个目的地址为 2001:2::1 的 IPv6 报文，由 CE 1 将报文发送至 PE 1。

(2) PE 1 根据报文到达的接口及目的地址查找 VPN 实例的路由表项，匹配后将报文转发出去，同时打上公网和私网两层标签。

(3) MPLS 网络利用报文的外层标签，将报文传送到 PE 2。（报文在到达 PE 2 前一跳时已经被剥离外层标签，到达 PE 2 时仅含内层标签）

(4) PE 2 根据内层标签和目的地址查找 VPN 实例的路由表项，确定报文的出接口，将报文转发至 CE 2。

(5) CE 2 根据正常的 IPv6 转发过程将报文传送到目的地。

2.1.3 IPv6 MPLS L3VPN的路由发布

VPN 路由信息的发布过程包括三部分：本地 CE 到入口 PE、入口 PE 到出口 PE、出口 PE 到远端 CE。完成这三部分后，本地 CE 与远端 CE 之间将建立可达路由，VPN 私网路由信息能够在骨干网上发布。

1. 本地CE到入口PE的路由信息交换

CE 使用 IPv6 静态路由、RIPng、OSPFv3、IPv6 IS-IS、EBGP 或 IBGP 路由协议，将本站点的 VPN 路由发布给 PE。CE 发布给 PE 的是标准的 IPv6 路由。

2. 入口PE到出口PE的路由信息交换

PE 从 CE 学到 VPN 的 IPv6 路由信息后，为这些标准 IPv6 路由增加 RD 和 VPN Target 属性，形成 VPN-IPv6 路由，存放到为 CE 创建的 VPN 实例的路由表中，并触发 MPLS 为其分配私网标签。

入口 PE 通过 MP-BGP 把 VPN-IPv6 路由发布给出口 PE。出口 PE 根据 VPN-IPv6 路由的 Export Target 属性与自己维护的 VPN 实例的 Import Target 属性，决定是否将该路由加入到 VPN 实例的路由表。

PE 之间通过 IGP 来保证内部的连通性。

3. 出口PE到远端CE的路由信息交换

与本地 CE 到入口 PE 的路由信息交换相同，远端 CE 有多种方式可以从出口 PE 学习 VPN 路由，包括 IPv6 静态路由、RIPng、OSPFv3、IPv6 IS-IS、EBGP 或 IBGP 路由协议。

2.1.4 IPv6 MPLS L3VPN支持的组网方案及功能

目前，IPv6 MPLS L3VPN 支持如下组网方案及功能：

- 基本的 VPN 组网方案
- 跨域 VPN-OptionA
- 跨域 VPN-OptionC
- 运营商的运营商
- Multi-VPN-Instance CE
- BGP 的 AS 号替换和 SoO 组网

2.1.5 协议规范

与 IPv6 MPLS L3VPN 相关的协议规范有：

- RFC 4659：BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN

2.2 IPv6 MPLS L3VPN配置任务简介

表2-1 IPv6 MPLS L3VPN 配置任务简介

配置任务	说明	详细配置
配置基本IPv6 MPLS L3VPN	必选	2.3
配置IPv6跨域VPN	可选	2.4
配置Multi-VPN-Instance CE	可选	2.5
配置BGP的AS号替换和SoO属性	可选	2.6

2.3 配置基本IPv6 MPLS L3VPN

2.3.1 基本IPv6 MPLS L3VPN配置任务简介

配置 IPv6 MPLS L3VPN 的关键在于管理 VPN 私网路由在 MPLS 骨干网上的发布，包括 PE-CE 间的路由发布管理以及 PE-PE 间的路由发布管理。

表2-2 基本 IPv6 MPLS L3VPN 配置任务简介

配置任务		说明	详细配置
配置VPN实例	创建VPN实例	必选	2.3.3 1.
	配置VPN实例与接口关联	必选	2.3.3 2.
	配置VPN实例的路由相关属性	可选	2.3.3 3.
配置PE-CE间的路由交换		必选	2.3.4
配置PE-PE间的路由交换		必选	2.3.5
配置BGP-VPNv6子地址族下的路由特性		可选	2.3.6

2.3.2 配置准备

在配置基本 IPv6 MPLS L3VPN 之前，需完成以下任务：

- 对 MPLS 骨干网（PE、P）配置 IGP，实现骨干网的 IP 连通性
- 对 MPLS 骨干网（PE、P）配置 MPLS 基本能力
- 对 MPLS 骨干网（PE、P）配置 MPLS LDP，建立 LDP LSP

2.3.3 配置VPN实例

VPN 实例不仅可以隔离 VPN 私网路由与公网路由，还可以隔离不同 VPN 实例的路由，这一特点使得 VPN 实例的使用不限于 MPLS L3VPN。

配置 VPN 实例的操作是在 PE 或 MCE 设备上进行的。

1. 创建VPN实例

VPN 实例在实现中与 Site 关联。VPN 实例不是直接对应于 VPN，一个 VPN 实例综合了和它所对应 Site 的 VPN 成员关系和路由规则。

表2-3 创建 VPN 实例

操作	命令	说明
进入系统视图	**system-view**	-
创建VPN实例，并进入VPN实例视图	**ip vpn-instance** *vpn-instance-name*	缺省情况下，设备上不存在任何VPN实例
配置VPN实例的RD	**route-distinguisher** *route-distinguisher*	缺省情况下，未指定VPN实例的RD
（可选）配置VPN实例的描述信息	**description** *text*	缺省情况下，为指定VPN实例的描述信息 描述信息用于描述VPN实例，可以用来记录VPN实例与某个VPN的关系等信息
（可选）配置VPN实例的ID	**vpn-id** *vpn-id*	缺省情况下，没有指定VPN实例的ID
（可选）配置VPN实例的SNMP上下文	**snmp context-name** *context-name*	缺省情况下，没有指定VPN实例的SNMP上下文

MSR 系列路由器各款型对于本节所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR 2600	VPN实例	最多可配置VPN数量为1023
MSR 3600		• MSR3600-28/3600-51 最多可配置 VPN 数量为 1023 • MSR 36-10/MSR 36-20/MSR 36-40/MSR 36-60 最多可配置 VPN 数量为 2047
MSR 5600		最多可配置VPN数量为4095

2. 配置VPN实例与接口关联

说明

执行 **ip binding vpn-instance** 命令将删除接口上已经配置的 IPv6 地址，因此需要重新配置接口的 IPv6 地址。

VPN 实例配置完成后，还需要与连接 CE 的接口进行关联。

表2-4 配置 VPN 实例与接口关联

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
将当前接口与VPN实例关联	**ip binding vpn-instance** *vpn-instance-name*	缺省情况下，接口不关联任何VPN实例

3. 配置VPN实例的路由相关属性

表2-5 配置 VPN 实例的路由相关属性

<table>
<tr><th colspan="2">操作</th><th>命令</th><th>说明</th></tr>
<tr><td colspan="2">进入系统视图</td><td>system-view</td><td>-</td></tr>
<tr><td rowspan="3">进入VPN实例视图或IPv6 VPN视图</td><td>进入VPN实例视图</td><td>ip vpn-instance vpn-instance-name</td><td rowspan="3">VPN实例视图下配置的路由相关属性既可以用于IPv4 VPN，也可以用于IPv6 VPN
既可以在VPN实例视图下，也可以在IPv6 VPN视图下，配置IPv6 VPN的路由相关属性。如果同时在两个视图下配置了路由相关属性，则IPv6 VPN采用IPv6 VPN视图下配置的路由相关属性</td></tr>
<tr><td rowspan="2">进入IPv6 VPN视图</td><td>ip vpn-instance vpn-instance-name</td></tr>
<tr><td>address-family ipv6</td></tr>
<tr><td colspan="2">配置VPN Target</td><td>vpn-target vpn-target&<1-8> [both | export-extcommunity | import-extcommunity]</td><td>缺省情况下，没有指定VPN实例的VPN Target</td></tr>
<tr><td colspan="2">配置支持的最大激活路由前缀数</td><td>routing-table limit number { warn-threshold | simply-alert }</td><td>本命令的缺省情况与设备的型号有关，具体请参见命令手册
配置一个VPN实例可以支持的最大激活路由前缀数，可以防止PE路由器上保存过多的激活路由前缀信息
一个PE路由器最多可以支持的激活路由前缀数与设备的型号有关，具体请参见命令手册</td></tr>
</table>

操作	命令	说明
应用入方向路由策略	**import route-policy** *route-policy*	缺省情况下，接收所有VPN Target属性匹配的路由 执行本配置时，需要创建路由策略。路由策略的详细介绍，请参见“三层技术-IP路由配置指导”中的“路由策略”
应用出方向路由策略	**export route-policy** *route-policy*	缺省情况下，不对发布的路由进行过滤 执行本配置时，需要创建路由策略。路由策略的详细介绍，请参见“三层技术-IP路由配置指导”中的“路由策略”
配置VPN实例的隧道策略	**tnl-policy** *tunnel-policy-name*	缺省情况下，隧道策略为按照LSP隧道－>GRE隧道－>CR-LSP隧道的优先级顺序选择隧道，负载分担条数为1 为VPN实例配置隧道策略之前必须先创建隧道策略，否则将采用缺省策略 隧道策略的创建及配置方法，请参见“MPLS配置指导”中的“隧道策略”

2.3.4 配置PE-CE间的路由交换

PE-CE 间路由交换可以使用 IPv6 静态路由、RIPng、OSPFv3、IPv6 IS-IS、EBGP 和 IBGP 路由协议。根据实际组网情况选择一种进行配置即可。

1. 配置PE-CE间使用IPv6 静态路由

表2-6 配置 PE-CE 间使用 IPv6 静态路由

操作	命令	说明
进入系统视图	**system-view**	-
为指定VPN实例配置IPv6静态路由	**ipv6 route-static vpn-instance** *s-vpn-instance-name ipv6-address prefix-length* { *interface-type interface-number* [*next-hop-address*] | *nexthop-address* [**public**] | **vpn-instance** *d-vpn-instance-name nexthop-address* } [**permanent**] [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*]	缺省情况下，没有配置IPv6静态路由 该配置在PE上进行，CE上的配置方法与普通IPv6静态路由相同 有关IPv6静态路由的配置请参见“三层技术-IP路由配置指导”中的“IPv6静态路由”

2. 配置PE-CE间使用RIPng

一个 RIPng 进程只能属于一个 VPN 实例。如果在启动 RIPng 进程时不绑定到 VPN 实例，则该进程属于公网进程。有关 RIPng 的介绍和详细配置，请参见“三层技术-IP 路由配置指导”中的“RIPng”。

表2-7 配置 PE-CE 间使用 RIPng

操作	命令	说明
进入系统视图	**system-view**	-
创建PE-CE间的RIPng实例，并进入RIPng视图	**ripng** [*process-id*] **vpn-instance** *vpn-instance-name*	该配置在PE上进行，CE上配置普通RIPng即可
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
在接口上使能RIPng路由协议	**ripng** *process-id* **enable**	缺省情况下，接口禁用RIPng路由协议

3. 配置PE-CE间使用OSPFv3

一个 OSPFv3 进程只能属于一个 VPN 实例。如果在启动 OSPFv3 进程时不绑定到 VPN 实例，则该进程属于公网进程。有关 OSPFv3 的介绍和详细配置，请参见“三层技术-IP 路由配置指导”中的“OSPFv3”。

表2-8 配置 PE-CE 间使用 OSPFv3

操作	命令	说明
进入系统视图	**system-view**	-
创建PE-CE间的OSPFv3实例，并进入OSPFv3视图	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	该配置在PE上进行，CE上配置普通OSPFv3即可 一个VPN实例中最多可以启动的OSPFv3进程数没有限制，没有最大值，与设备内存有关 删除VPN实例后，相关的所有OSPFv3进程也将全部被删除
配置Router ID	**router-id** *router-id*	-
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
在接口上使能OSPFv3	**ospfv3** *process-id* **area** *area-id* [**instance** *instance-id*]	缺省情况下，接口上没有使能OSPFv3 该配置在PE上进行

4. 配置PE-CE间使用IPv6 IS-IS

一个 IPv6 IS-IS 进程只能属于一个 VPN 实例。如果在启动 IPv6 IS-IS 进程时不绑定到 VPN 实例，则该进程属于公网进程。有关 IPv6 IS-IS 的介绍和详细配置，请参见“三层技术-IP 路由配置指导”中的“IPv6 IS-IS”。

表2-9 配置 PE-CE 间使用 IPv6 IS-IS

操作	命令	说明
进入系统视图	**system-view**	-
创建PE-CE间的IPv6 IS-IS实例，并进入IS-IS视图	**isis** [*process-id*] **vpn-instance** *vpn-instance-name*	该配置在PE上进行，CE上配置普通IPv6 IS-IS即可
配置网络实体名称	**network-entity** *net*	缺省情况下，没有配置网络实体名称
使能IS-IS进程的IPv6能力	**ipv6 enable**	缺省情况下，没有使能IS-IS路由进程的IPv6能力
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能接口IS-IS路由进程的IPv6能力，并指定要关联的IS-IS进程号	**isis ipv6 enable** [*process-id*]	缺省情况下，接口上没有使能IS-IS路由进程的IPv6能力

5. 配置PE-CE间使用EBGP

(1) PE 上的配置

表2-10 PE 上的配置

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
进入BGP-VPN实例视图	**ip vpn-instance** *vpn-instance-name*	-
将CE配置为VPN私网EBGP对等体	**peer** { *group-name* | *ipv6-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体
创建BGP-VPN IPv6单播地址族，并进入BGP-VPN IPv6单播地址族视图	**address-family ipv6** [**unicast**]	缺省情况下，没有创建BGP-VPN IPv6单播地址族 BGP-VPN IPv6单播地址族视图下的配置命令与BGP IPv6单播地址族视图下的配置命令相同。本文只列举了部分配置命令，更多的配置命令请参见“三层技术-IP路由配置指导”中的“BGP”
使能本地路由器与指定对等体交换IPv6单播路由信息的能力	**peer** { *group-name* | *ipv6-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv6单播路由信息

操作	命令	说明
引入本端CE路由	**import-route** *protocol* [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]	PE需要将到本端CE的路由引入VPN路由表中，以发布给对端PE
（可选）配置对发布的路由信息进行过滤	**filter-policy** { *acl6-number* | **prefix-list** *ipv6-prefix-name* } **export** [*protocol process-id*]	缺省情况下，不对发布的路由信息进行过滤
（可选）配置对接收的路由信息进行过滤	**filter-policy** { *acl6-number* | **prefix-list** *ipv6-prefix-name* } **import**	缺省情况下，不对接收的路由信息进行过滤

(2) CE 上的配置

表2-11 CE 上的配置

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
将PE配置为EBGP对等体	**peer** { *group-name* | *ipv6-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体
创建BGP IPv6单播地址族，并进入BGP IPv6单播地址族视图	**address-family ipv6** [**unicast**]	缺省情况下，BGP IPv6单播地址族
使能本地路由器与指定对等体交换IPv6单播路由信息的能力	**peer** { *group-name* | *ipv6-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv6单播路由信息
（可选）配置路由引入	**import-route** *protocol* [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]	CE需要将自己所能到达的VPN网段地址发布给接入的PE，通过PE发布给对端CE

6. 配置PE-CE间使用IBGP

提示

PE 和 CE 之间使用 IBGP 路由协议只适用于基本的 IPv6 MPLS L3VPN 组网环境，跨域 VPN 和运营商的运营商组网中，PE 和 CE 之间不能配置 IBGP。

(1) PE 上的配置

表2-12 PE 上的配置

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-

操作	命令	说明
进入BGP-VPN实例视图	**ip vpn-instance** *vpn-instance-name*	BGP-VPN实例视图下的配置任务与BGP视图下的相同，有关介绍和详细配置，请参见“三层技术-IP路由配置指导”中的“BGP”
将CE配置为VPN私网IBGP对等体	**peer** { *group-name* | *ipv6-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体
创建BGP-VPN IPv6单播地址族，并进入BGP-VPN IPv6单播地址族视图	**address-family ipv6** [**unicast**]	缺省情况下，没有创建BGP-VPN IPv6单播地址族
使能本地路由器与指定对等体/对等体组交换IPv6单播路由信息的能力	**peer** { *group-name* | *ipv6-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv6单播路由信息
将CE配置为路由反射器的客户端	**peer** { *group-name* | *ipv6-address* } **reflect-client**	缺省情况下，没有配置路由发射器及其客户端 缺省情况下PE不会向IBGP对等体（包括VPNv6的IBGP对等体）发送从IBGP对等体CE学习的路由，只有将CE配置为路由反射器的客户端后，才能向其它IBGP对等体发送从该CE学习的路由 配置路由反射器后不会修改路由的下一跳。如果需要修改下一跳，则需在路由的接收端通过入策略进行修改
（可选）允许路由反射器在客户机之间反射路由	**reflect between-clients**	缺省情况下，允许路由反射器在客户机之间反射路由
（可选）配置路由反射器的集群ID	**reflector cluster-id** { *cluster-id* | *ip-address* }	缺省情况下，每个路由反射器都使用自己的Router ID作为集群ID 如果一个集群中配置了多个路由反射器，请使用本命令为所有的路由反射器配置相同的集群ID，以避免产生路由环路

(2) CE 上的配置

表2-13 CE 上的配置

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
将PE配置为IBGP对等体	**peer** { *group-name* | *ipv6-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体
创建BGP IPv6单播地址族，并进入BGP IPv6单播地址族视图	**address-family ipv6** [**unicast**]	缺省情况下，没有创建BGP IPv6单播地址族

操作	命令	说明
使能本地路由器与指定对等体/对等体组交换IPv6单播路由信息的能力	**peer** { *group-name* | *ipv6-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv6单播路由信息
（可选）配置路由引入	**import-route** *protocol* [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]	CE需要将自己所能到达的VPN网段地址发布给接入的PE，通过PE发布给对端CE

2.3.5 配置PE-PE间的路由交换

表2-14 配置 PE-PE 间的路由交换

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
将对端PE配置为对等体	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体
指定与对等体/对等体组创建BGP会话时建立TCP连接使用的源接口	**peer** { *group-name* | *ip-address* } **connect-interface** *interface-type interface-number*	缺省情况下，BGP使用到达BGP对等体的最佳路由的出接口作为与对等体/对等体组创建BGP会话时建立TCP连接的源接口
创建BGP VPNv6地址族，并进入BGP VPNv6地址族视图	**address-family vpnv6**	缺省情况下，没有创建BGP VPNv6地址族
使能本地路由器与指定对等体交换VPNv6路由信息的能力	**peer** { *group-name* | *ip-address* } **enable**	缺省情况下，本地路由器不能与对等体交换VPNv6路由信息

2.3.6 配置BGP VPNv6 路由

BGP VPNv6 路由的属性需要在 BGP VPNv6 地址族视图下配置。BGP VPNv6 路由的很多配置都与 BGP IPv6 单播路由相同，详细配置请参见“三层技术-IP 路由配置指导”中的“BGP”。

表2-15 配置 BGP VPNv6 路由

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
进入BGP VPNv6地址族视图	**address-family vpnv6**	-
配置对发布的路由信息进行过滤	**filter-policy** { *acl6-number* | **prefix-list** *ipv6-prefix-name* } **export** [*protocol process-id*]	缺省情况下，不对发布的路由信息进行过滤

操作	命令	说明
配置对接收的路由信息进行过滤	**filter-policy** { *acl6-number* | **prefix-list** *ipv6-prefix-name* } **import**	缺省情况下，不对接收的路由信息进行过滤
为对等体/对等体组设置基于ACL的BGP路由过滤策略	**peer** { *group-name* | *ip-address* } **filter-policy** *acl6-number* { **export** | **import** }	缺省情况下，没有设置基于ACL的BGP路由过滤策略
为对等体/对等体组设置基于IPv6地址前缀列表的BGP路由过滤策略	**peer** { *group-name* | *ip-address* } **prefix-list** *ipv6-prefix-name* { **export** | **import** }	缺省情况下，没有设置基于IPv6地址前缀列表的BGP路由过滤策略
为从对等体/对等体组接收的路由分配首选值	**peer** { *group-name* | *ip-address* } **preferred-value** *value*	缺省情况下，从对等体/对等体组接收的路由的首选值为0
向指定EBGP对等体/对等体组发送BGP更新消息时只携带公有AS号，不携带私有AS号	**peer** { *group-name* | *ip-address* } **public-as-only**	缺省情况下，向EBGP对等体/对等体组发送BGP更新消息时，既可以携带公有AS号，又可以携带私有AS号
对来自对等体/对等体组的路由或发布给对等体/对等体组的路由应用路由策略	**peer** { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** }	缺省情况下，没有为对等体/对等体组指定路由策略
对接收到的VPNv6路由使能VPN-Target过滤功能	**policy vpn-target**	缺省情况下，对接收到的VPNv6路由使能VPN-Target过滤功能
配置将本机作为路由反射器，并将对等体作为路由反射器的客户	**peer** { *group-name* | *ip-address* } **reflect-client**	缺省情况下，没有配置路由反射器及其客户
设置允许从指定对等体/对等体组收到的路由数量	**peer** { *group-name* | *ip-address* } **route-limit** *prefix-number* [{ **alert-only** | **discard** | **reconnect** *reconnect-time* } | *percentage-value*] *	缺省情况下，不限制从对等体/对等体组接收的路由数量
允许路由反射器在客户机之间反射路由	**reflect between-clients**	缺省情况下，允许路由反射器在客户机之间反射路由
配置路由反射器的集群ID	**reflector cluster-id** { *cluster-id* | *ip-address* }	缺省情况下，每个路由反射器都使用自己的Router ID作为集群ID 如果一个集群中配置了多个路由反射器，请使用本命令为所有的路由反射器配置相同的集群ID，以避免产生路由环路
创建路由反射器的反射策略	**rr-filter** *extended-community-number*	缺省情况下，路由反射器不会对反射的路由进行过滤 执行本命令后，只有与本命令配置的扩展团体属性号匹配的IBGP路由才会被反射 通过在不同的路由反射器上配置不同的反射策略，可以实现路由反射器之间的负载分担
为BGP对等体/对等体组配置SoO属性	**peer** { *group-name* | *ip-address* } **soo** *site-of-origin*	缺省情况下，没有为BGP对等体/对等体组配置SoO属性

2.4 配置IPv6跨域VPN

如果承载 IPv6 VPN 路由的 MPLS 骨干网跨越多个 AS，就需要配置跨域 VPN。

跨域VPN有三种解决方案，具体介绍请参见“1.1.6 跨域VPN”。目前，IPv6 MPLS L3VPN只支持VPN-OptionA和VPN-OptionC。请根据实际组网情况，选择合适的跨域VPN方案。

2.4.1 配置准备

在配置跨域 VPN 之前，需完成以下任务：

- 为各 AS 的 MPLS 骨干网分别配置 IGP，实现同一 AS 内骨干网的 IP 连通性
- 为各 AS 的 MPLS 骨干网分别配置 MPLS 基本能力
- 为各 AS 的 MPLS 骨干网分别配置 MPLS LDP，建立 LDP LSP

2.4.2 配置IPv6 跨域VPN-OptionA

IPv6 跨域 VPN-OptionA 的实现比较简单，当 PE 上的 VPN 数量及 VPN 路由数量都比较少时可以采用这种方案。

IPv6 跨域 VPN-OptionA 的配置可以描述为：

- 对各 AS 分别进行基本 IPv6 MPLS L3VPN 配置。
- 对于 ASBR-PE，将对端 ASBR-PE 看作自己的 CE 配置即可。即：IPv6 跨域 VPN-OptionA 方式需要在 PE 和 ASBR-PE 上分别配置 IPv6 VPN 实例，前者用于接入 CE，后者用于接入对端 ASBR-PE。

具体配置方法，请参见“2.3 配置基本IPv6 MPLS L3VPN”。

在 IPv6 跨域 VPN-OptionA 方式中，对于同一个 IPv6 VPN，同一 AS 内的 ASBR-PE 和 PE 上配置的 VPN Target 应能匹配，即 VPN Target 的配置应能保证 PE（或 ASBR-PE）发送的 VPN 路由能够被 ASBR-PE（或 PE）接受；不同 AS 的 PE 上配置的 VPN Target 则不需要匹配。

2.4.3 配置IPv6 跨域VPN-OptionC

1. 配置PE

同一AS内的PE和ASBR-PE之间建立普通的IBGP对等体关系，不同AS的PE之间建立MP-EBGP对等体关系。

同一 AS 内的 PE 和 ASBR-PE 之间应能够交换带标签的路由。

表2-16 配置 PE

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
配置本AS的ASBR-PE为IBGP对等体	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体
将另一AS的PE配置为EBGP对等体	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体

操作	命令	说明
进入BGP IPv4单播地址族视图	**address-family ipv4** [**unicast**]	-
使能与本AS的ASBR-PE交换BGP IPv4单播路由的能力	**peer** { *group-name* | *ip-address* } **enable**	缺省情况下，不能与本AS的ASBR-PE交换BGP IPv4单播路由
配置与本AS的ASBR-PE之间能够交换带标签的路由	**peer** { *group-name* | *ip-address* } **label-route-capability**	缺省情况下，不向IPv4对等体/对等体组发送标签路由
退回BGP视图	**quit**	-
进入BGP VPNv6地址族视图	**address-family vpnv6**	-
使能本地路由器与指定对等体交换VPNv6路由信息的能力	**peer** *ip-address* **enable**	缺省情况下，本地路由器不能与对等体交换VPNv6路由信息

2. 配置ASBR-PE

在跨域VPN-OptionC方式中，需要建立一条跨域的VPN LSP，相关PE、ASBR之间发布公网路由时携带MPLS标签信息。此跨域VPN LSP的建立同IPv4 MPLS VPN相同，配置方式参见“1.4.3 配置跨域VPN-OptionC”。

3. 配置路由策略

配置在 ASBR-PE 上应用路由策略：

- 对于从本 AS 的 PE 接收的路由，在向对端 ASBR-PE 发布时，分配 MPLS 标签；
- 对于向本 AS 的 PE 发布的路由，如果是带标签的路由，为其分配新的 MPLS 标签。

IPv6 跨域VPN路由策略的配置与IPv4 MPLS VPN相同，配置方式参见“1.4.3 配置跨域VPN-OptionC”。

2.5 配置Multi-VPN-Instance CE

Multi-VPN-Instance CE 可以看作一种通过路由隔离实现业务隔离的组网方案。配置 MCE 的关键为：

- 配置 MCE 与站点之间的路由交换
- 配置 MCE 与 PE 之间的路由交换

在 MCE 组网方案中，路由计算时需要关闭 PE 上的路由环路检测功能，防止路由丢失；同时禁止各路由协议互操作功能，以节省系统资源。

2.5.1 配置准备

在配置 Multi-VPN-Instance CE 之前，需完成以下任务：

- 创建 VPN 实例、在 MCE 上将连接站点和 PE 的接口与 VPN 实例绑定
- 配置相关接口的链路层协议和网络层协议，保证路由可达

2.5.2 配置MCE与站点之间的路由交换

1. 配置MCE与站点之间使用IPv6 静态路由

MCE 可以通过 IPv6 静态路由与 Site 连接。传统 CE 配置的 IPv6 静态路由对全局生效，无法解决多 VPN 间的地址重叠问题。以太网交换机提供的 MCE 功能可以将 IPv6 静态路由与 VPN 实例相绑定，将各 IPv6 VPN 之间的 IPv6 静态路由进行隔离。

表2-17 配置 MCE 与站点之间使用 IPv6 静态路由

操作	命令	说明
进入系统视图	**system-view**	-
为指定VPN实例配置IPv6静态路由	**ipv6 route-static vpn-instance** *s-vpn-instance-name ipv6-address prefix-length* { *interface-type interface-number* [*next-hop-address*] | *nexthop-address* [**public**] | **vpn-instance** *d-vpn-instance-name nexthop-address* } [**permanent**] [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*]	缺省情况下，没有配置IPv6静态路由 该配置在MCE上进行，站点上的配置方法与普通IPv6静态路由相同
（可选）配置IPv6静态路由的缺省优先级	**ipv6 route-static default-preference** *default-preference-value*	缺省情况下，IPv6静态路由的缺省优先级为60

2. 配置MCE与站点之间使用RIPng

一个 RIPng 进程只能属于一个 IPv6 VPN 实例。如果在启动 RIPng 进程时不绑定到 IPv6 VPN 实例，则该进程属于公网进程。通过在 MCE 上将 RIPng 进程与 IPv6 VPN 实例绑定，可以使不同 IPv6 VPN 内的私网路由通过不同的 RIPng 进程在 Site 和 MCE 间进行交互，保证了私网路由的隔离和安全。有关 RIPng 的介绍和详细配置，请参见“三层技术-IP 路由配置指导”中的“RIPng”。

表2-18 配置 MCE 与站点之间使用 RIPng

操作	命令	说明
进入系统视图	**system-view**	-
创建MCE与站点间的RIPng实例，并进入RIPng视图	**ripng** [*process-id*] **vpn-instance** *vpn-instance-name*	该配置在MCE上进行，站点上配置普通RIPng即可
引入由PE发布的远端站点的路由	**import-route** *protocol* [*process-id*] [**allow-ibgp**] [**allow-direct** | **cost** *cost* | **route-policy** *route-policy-name*] *	缺省情况下，RIPng未引入其它路由
（可选）配置引入路由的缺省度量值	**default cost** *value*	缺省情况下，引入路由的缺省度量值为0
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
在接口上使能RIPng路由协议	**ripng** *process-id* **enable**	缺省情况下，接口禁用RIPng路由协议

3. 配置MCE与站点之间使用OSPFv3

一个 OSPFv3 进程只能属于一个 IPv6 VPN 实例。如果在启动 OSPFv3 进程时不绑定到 IPv6 VPN 实例，则该进程属于公网进程。

通过在 MCE 上将 OSPFv3 进程与 IPv6 VPN 实例绑定，可以使不同 IPv6 VPN 内的私网路由通过不同的 OSPFv3 进程在 Site 和 MCE 间进行交互，保证了私网路由的隔离和安全。

有关 OSPFv3 的介绍和详细配置，请参见“三层技术-IP 路由配置指导”中的“OSPFv3”。

表2-19 配置 MCE 与站点之间使用 OSPFv3

操作	命令	说明
进入系统视图	**system-view**	-
创建MCE与站点间的OSPFv3实例，并进入OSPFv3视图	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	该配置在MCE上进行，站点上配置普通OSPFv3即可 一个VPN实例中最多可以启动的OSPFv3进程数没有限制，没有最大值，与设备内存有关 删除VPN实例后，相关的所有OSPFv3进程也将全部被删除
配置Router ID	**router-id** *router-id*	-
引入由PE发布的远端站点的路由	**import-route** *protocol* [*process-id* | **all-processes** | **allow-ibgp**] [**allow-direct** | **cost** *cost* | **route-policy** *route-policy-name* | **type** *type*] *	缺省情况下，没有引入其他协议的路由信息
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
在接口上使能OSPFv3	**ospfv3** *process-id* **area** *area-id* [**instance** *instance-id*]	缺省情况下，接口上没有使能OSPFv3

4. 配置MCE与站点之间使用IPv6 IS-IS

一个IPv6 IS-IS进程只能属于一个IPv6 VPN实例。如果在启动IPv6 IS-IS进程时不绑定到IPv6 VPN实例，则该进程属于公网进程。

通过在 MCE 上将 IPv6 IS-IS 进程与 IPv6 VPN 实例绑定，可以使不同 IPv6 VPN 内的私网路由通过不同的 IPv6 IS-IS 进程在 Site 和 MCE 间进行交互，保证了私网路由的隔离和安全。

有关 IPv6 IS-IS 的介绍和详细配置，请参见“三层技术-IP 路由配置指导”中的“IPv6 IS-IS”。

表2-20 配置 MCE 与站点之间使用 IPv6 IS-IS

操作	命令	说明
进入系统视图	**system-view**	-
创建MCE与站点间的IPv6 IS-IS实例，并进入IS-IS视图	**isis** [*process-id*] **vpn-instance** *vpn-instance-name*	该配置在MCE上进行，站点上配置普通IPv6 IS-IS即可
配置网络实体名称	**network-entity** *net*	缺省情况下，没有配置网络实体名称

操作	命令	说明
使能IS-IS进程的IPv6能力	**ipv6 enable**	缺省情况下，没有使能IS-IS路由进程的IPv6能力
（可选）引入由PE发布的远端站点的路由	**ipv6 import-route** *protocol* [*process-id*] [**allow-ibgp**] [**allow-direct** | **cost** *cost* | [**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *	缺省情况下，IPv6 IS-IS不引入其它协议的路由信息 如果**ipv6 import-route**命令中不指定引入的级别，则默认为引入路由到Level-2路由表中
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能接口IS-IS路由进程的IPv6能力，并指定要关联的IS-IS进程号	**isis ipv6 enable** [*process-id*]	缺省情况下，接口上没有使能IS-IS路由进程的IPv6能力

5. 配置MCE与站点之间使用EBGP

MCE 与站点间使用 EBGP 交换路由信息时，需要在 MCE 上为每个 IPv6 VPN 实例配置 IPv6 BGP 对等体，并在站点上引入相应 IPv6 VPN 内的 IGP 路由信息。

MCE 使用 EBGP 交换路由信息时，还可以通过 Filter-policy 对接收/发布的路由进行过滤。

有关 IPv6 BGP 协议的配置，请参见“三层技术-IP 路由配置指导”中的“BGP”。

(1) MCE 上的配置

表2-21 配置 MCE 与站点之间使用 EBGP

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
进入BGP-VPN实例视图	**ip vpn-instance** *vpn-instance-name*	-
配置IPv6 BGP对等体的AS号	**peer** { *group-name* | *ipv6-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体
进入BGP-VPN IPv6单播地址族视图	**address-family ipv6** [**unicast**]	-
使能本地路由器与指定对等体交换IPv6单播路由信息的能力	**peer** { *group-name* | *ipv6-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv6单播路由信息
引入由PE发布的远端站点的路由	**import-route** *protocol* [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]	缺省情况下，BGP不引入且不通告其它协议的路由
（可选）配置对发布的路由信息进行过滤	**filter-policy** { *acl6-number* | **prefix-list** *ipv6-prefix-name* } **export** [*protocol process-id*]	缺省情况下，不对发布的路由信息进行过滤
（可选）配置对接收的路由信息进行过滤	**filter-policy** { *acl6-number* | **prefix-list** *ipv6-prefix-name* } **import**	缺省情况下，不对接收的路由信息进行过滤

(2) 站点上的配置

表2-22 站点上的配置

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
将MCE配置为EBGP对等体	**peer** { *group-name* | *ipv6-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体
进入BGP IPv6单播地址族视图	**address-family ipv6** [**unicast**]	-
使能本地路由器与指定对等体交换IPv6单播路由信息的能力	**peer** { *group-name* | *ipv6-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv6单播路由信息
引入VPN内的IGP路由	**import-route** *protocol* [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]	缺省情况下，BGP不引入且不通告其它协议的路由 站点需要将自己所能到达的IPv6 VPN网段地址发布给接入的MCE

6. 配置MCE与站点间使用IBGP

MCE 与站点间使用 IBGP 交换路由信息时，需要在 MCE 上为每个 VPN 实例配置 BGP 对等体，并在站点上引入相应 VPN 内的 IGP 路由信息。

(1) MCE 上的配置

表2-23 配置 MCE 与站点之间使用 IBGP

操作	命令	说明
进入系统视图	**system-view**	-
启动BGP，并进入BGP视图	**bgp** *as-number*	缺省情况下，系统没有运行BGP
进入BGP-VPN实例视图	**ip vpn-instance** *vpn-instance-name*	-
配置IBGP对等体	**peer** { *group-name* | *ipv6-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体和对等体组
进入BGP-VPN IPv6单播地址族视图	**address-family ipv6** [**unicast**]	-
使能本地路由器与指定对等体交换IPv6单播路由信息的能力	**peer** { *group-name* | *ipv6-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv6单播路由信息

操作	命令	说明
（可选）配置本地设备作为路由反射器，对端设备作为路由反射器的客户端	**peer** { *group-name* | *ipv6-address* } **reflect-client**	缺省情况下，没有配置路由反射器及其客户端 将站点配置为IBGP对等体时，从该站点学习的BGP路由不会向其它IBGP对等体（包括VPNv6对等体）发送。只有将站点配置为路由反射器的客户端后，才能向其它IBGP对等体发送从该站点学习的路由
引入由PE发布的远端站点的路由	**import-route** *protocol* [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]	缺省情况下，BGP不引入且不通告其它协议的路由
（可选）配置对发布的路由信息进行过滤	**filter-policy** { *acl6-number* | **prefix-list** *ipv6-prefix-name* } **export** [*protocol process-id*]	缺省情况下，不对发布的路由信息进行过滤
（可选）配置对接收的路由信息进行过滤	**filter-policy** { *acl6-number* | **prefix-list** *ipv6-prefix-name* } **import**	缺省情况下，不对接收的路由信息进行过滤

(2) 站点上的配置

表2-24 站点上的配置

操作	命令	说明
进入系统视图	**system-view**	-
启动BGP，并进入BGP视图	**bgp** *as-number*	缺省情况下，系统没有运行BGP
将MCE配置为IBGP对等体	**peer** { *group-name* | *ipv6-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体和对等体组
进入BGP IPv6单播地址族视图	**address-family ipv6** [**unicast**]	-
使能本地路由器与指定对等体交换IPv6单播路由信息的能力	**peer** { *group-name* | *ipv6-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv6单播路由信息
配置引入VPN内的IGP路由	**import-route** *protocol* [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]	缺省情况下，BGP不引入且不通告其它协议的路由 站点需要将自己所能到达的VPN网段地址发布给接入的MCE

2.5.3 配置MCE与PE之间的路由交换

由于在 MCE 设备上已经将站点内的私网路由信息与 IPv6 VPN 实例进行了绑定，因此，只需要在 MCE 与 PE 之间将接口与 IPv6 VPN 实例进行绑定、进行简单的路由配置、并将 MCE 上维护的站点内的 IPv6 VPN 路由引入到 MCE-PE 间的路由协议中，便可以实现私网 VPN 路由信息的传播。

本节中的配置均在MCE上进行，PE上的配置与基本IPv6 MPLS L3VPN组网中PE上的配置相同，详细介绍请参见“2.3.4 配置PE-CE间的路由交换”。

1. 配置MCE与PE之间使用IPv6 静态路由

表2-25 配置 MCE 与 PE 之间使用 IPv6 静态路由

操作	命令	说明
进入系统视图	**system-view**	-
为指定VPN实例配置IPv6静态路由	**ipv6 route-static vpn-instance** *s-vpn-instance-name ipv6-address prefix-length* { *interface-type interface-number* [*next-hop-address*] | *nexthop-address* [**public**] | **vpn-instance** *d-vpn-instance-name nexthop-address* } [**permanent**] [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*]	缺省情况下，没有配置IPv6静态路由
（可选）配置IPv6静态路由的缺省优先级	**ipv6 route-static default-preference** *default-preference-value*	缺省情况下，IPv6静态路由的缺省优先级为60

2. 配置MCE与PE之间使用RIPng

表2-26 配置 MCE 与 PE 之间使用 RIPng

操作	命令	说明
进入系统视图	**system-view**	-
创建MCE与PE间的RIPng实例，并进入RIPng视图	**ripng** [*process-id*] **vpn-instance** *vpn-instance-name*	-
引入站点内的VPN路由	**import-route** *protocol* [*process-id*] [**allow-ibgp**] [**allow-direct** | **cost** *cost* | **route-policy** *route-policy-name*] *	缺省情况下，RIPng未引入其它路由
（可选）配置引入路由的缺省度量值	**default cost** *value*	缺省情况下，引入路由的缺省度量值为0
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
在指定的网络接口上使能RIPng	**ripng** *process-id* **enable**	缺省情况下，接口禁用RIPng

3. 配置MCE与PE之间使用OSPFv3

表2-27 配置 MCE 与 PE 之间使用 OSPFv3

操作	命令	说明
进入系统视图	**system-view**	-
创建MCE与PE间的OSPFv3实例，并进入OSPFv3视图	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	-

操作	命令	说明
配置Router ID	**router-id** *router-id*	-
引入站点内的VPN路由	**import-route** *protocol* [*process-id* | **all-processes** | **allow-ibgp**] [**allow-direct** | **cost** *cost* | **route-policy** *route-policy-name* | **type** *type*] *	缺省情况下，没有引入其他协议的路由信息
（可选）配置对发布的路由进行过滤	**filter-policy** { *acl6-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*]]	缺省情况下，没有对发布的路由信息进行过滤
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
在接口上使能OSPFv3	**ospfv3** *process-id* **area** *area-id* [**instance** *instance-id*]	缺省情况下，接口上没有使能OSPFv3

4. 配置MCE与PE之间使用IPv6 IS-IS

表2-28 配置 MCE 与 PE 之间使用 IPv6 IS-IS

操作	命令	说明
进入系统视图	**system-view**	-
创建MCE与PE间的IPv6 IS-IS实例，并进入IS-IS视图	**isis** [*process-id*] **vpn-instance** *vpn-instance-name*	-
配置网络实体名称	**network-entity** *net*	缺省情况下，没有配置网络实体名称
使能IS-IS进程的IPv6能力	**ipv6 enable**	缺省情况下，没有使能IS-IS路由进程的IPv6能力
（可选）引入站点内的VPN路由	**ipv6 import-route** *protocol* [*process-id*] [**allow-ibgp**] [**allow-direct** | **cost** *cost* | [**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *	缺省情况下，IPv6 IS-IS不引入其它协议的路由信息 如果**ipv6 import-route**命令中不指定引入的级别，则默认为引入路由到Level-2路由表中
（可选）对发布的路由进行过滤	**ipv6 filter-policy** { *acl6-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } **export** [*protocol* [*process-id*]]	缺省情况下，IPv6 IS-IS不对发布的路由信息进行过滤
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能接口IS-IS路由进程的IPv6能力，并指定要关联的IS-IS进程号	**isis ipv6 enable** [*process-id*]	缺省情况下，接口上没有使能IS-IS路由进程的IPv6能力

5. 配置MCE与PE之间使用EBGP

表2-29 配置 MCE 与 PE 之间使用 EBGP

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
进入BGP-VPN实例视图	**ip vpn-instance** *vpn-instance-name*	-
将PE配置为EBGP对等体	**peer** { *group-name* | *ipv6-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体
进入BGP-VPN IPv6单播地址族视图	**address-family ipv6** [**unicast**]	-
使能本地路由器与指定对等体交换IPv6单播路由信息的能力	**peer** { *group-name* | *ipv6-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv6单播路由信息
引入站点内的VPN路由	**import-route** *protocol* [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]	缺省情况下，BGP不引入且不通告其它协议的路由
（可选）配置对发布的路由信息进行过滤	**filter-policy** { *acl6-number* | **prefix-list** *ipv6-prefix-name* } **export** [*protocol process-id*]	缺省情况下，不对发布的路由信息进行过滤
（可选）配置对接收的路由信息进行过滤	**filter-policy** { *acl6-number* | **prefix-list** *ipv6-prefix-name* } **import**	缺省情况下，不对接收的路由信息进行过滤

6. 配置MCE与PE之间使用IBGP

表2-30 配置 MCE 与 PE 之间使用 IBGP

操作	命令	说明
进入系统视图	**system-view**	-
启动BGP，并进入BGP视图	**bgp** *as-number*	缺省情况下，系统没有运行BGP
进入BGP-VPN实例视图	**ip vpn-instance** *vpn-instance-name*	-
将PE配置为IBGP对等体	**peer** { *group-name* | *ipv6-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体和对等体组
进入BGP-VPN IPv6单播地址族视图	**address-family ipv6** [**unicast**]	-
使能本地路由器与指定对等体交换IPv6单播路由信息的能力	**peer** { *group-name* | *ipv6-address* } **enable**	缺省情况下，本地路由器不能与对等体交换IPv6单播路由信息
引入站点内的VPN路由	**import-route** *protocol* [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]	缺省情况下，BGP不引入且不通告其它协议的路由

操作	命令	说明
（可选）配置对发布的路由信息进行过滤	**filter-policy** { *acl6-number* | **prefix-list** *ipv6-prefix-name* } **export** [*protocol process-id*]	缺省情况下，不对发布的路由信息进行过滤
（可选）配置对接收的路由信息进行过滤	**filter-policy** { *acl6-number* | **prefix-list** *ipv6-prefix-name* } **import**	缺省情况下，不对接收的路由信息进行过滤

2.6 配置BGP的AS号替换和SoO属性

不同 Site 的 CE 具有相同的 AS 号时，PE 上需要开启 BGP 的 AS 号替换功能，从而避免路由被丢弃。

使能了 BGP 的 AS 号替换功能后，当 PE 向指定 CE 发布路由时，如果路由的 AS_PATH 中有与 CE 相同的 AS 号，将被替换成 PE 的 AS 号后再发布。

PE 使用不同接口连接同一站点的多个 CE 时，如果配置了 BGP 的 AS 号替换功能，则会导致路由环路。这种情况下，需要在 PE 上通过 **peer soo** 命令为从同一站点不同 CE 学习到的路由添加相同的 SoO 属性，且 PE 向 CE 发布路由时检查 SoO 属性，如果路由的 SoO 属性与为 CE 配置的 SoO 属性相同，则不将该路由发布给 CE，从而避免路由环路。

本配置中各命令的详细介绍，请参见“三层技术-IP 路由命令参考”中的“BGP”。

表2-31 配置 BGP 的 AS 号替换和 SoO 属性

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
进入BGP-VPN实例视图	**ip vpn-instance** *vpn-instance-name*	-
使能BGP的AS号替换功能	**peer** { *group-name* | *ipv6-address* } **substitute-as**	缺省情况下，BGP的AS号替换功能是被禁止的
进入BGP-VPN IPv6单播地址族视图	**address-family ipv6** [**unicast**]	-
（可选）为BGP对等体/对等体组配置SoO属性	**peer** { *group-name* | *ipv6-address* } **soo** *site-of-origin*	缺省情况下，没有为BGP对等体/对等体组配置SoO属性

2.7 IPv6 MPLS L3VPN显示和维护

2.7.1 复位BGP会话

当 BGP 配置变化后，可以通过软复位或复位 BGP 会话使新的配置生效。软复位 BGP 会话是指在不断开 BGP 邻居关系的情况下，更新 BGP 路由信息；复位 BGP 会话是指断开并重新建立 BGP 邻居关系的情况下，更新 BGP 路由信息。软复位需要 BGP 对等体具备路由刷新能力（支持 ROUTE-REFRESH 消息）。

请在用户视图下进行下列操作。下表中各命令的详细介绍，请参见“三层技术-IP 路由命令参考”中的“BGP”。

表2-32 复位 BGP 会话

操作	命令
手工对VPNv6地址族下的BGP会话进行软复位	**refresh bgp** { *ip-address* | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** } **vpnv6**
复位VPNv6地址族下的BGP会话	**reset bgp** { *as-number* | *ip-address* | **all** | **external** | **internal** | **group** *group-name* } **vpnv6**

2.7.2 显示IPv6 MPLS L3VPN的运行状态

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 IPv6 MPLS L3VPN 的运行情况，通过查看显示信息验证配置的效果。

display bgp group vpnv6、**display bgp peer vpnv6** 和 **display bgp update-group vpnv6** 命令的详细介绍，请参见“三层技术-IP 路由命令参考”中的“BGP”。

表2-33 显示 IPv6 MPLS L3VPN 的运行状态

操作	命令
显示与VPN实例相关联的IPv6路由表（本命令的详细介绍请参见“三层技术-IP路由命令参考”中的“IP路由基础命令”）	**display ipv6 routing-table vpn-instance** *vpn-instance-name* [**verbose**]
显示指定VPN实例信息	**display ip vpn-instance** [**instance-name** *vpn-instance-name*]
显示指定VPN实例的IPv6 FIB信息	**display ipv6 fib vpn-instance** *vpn-instance-name* [**acl6** *acl6-number* | **ipv6-prefix** *ipv6-prefix-name*]
显示指定VPN实例中与指定目的IPv6地址匹配的IPv6 FIB信息	**display ipv6 fib vpn-instance** *vpn-instance-name ipv6-address* [*prefix-length*]
显示BGP VPNv6对等体组的信息	**display bgp group vpnv6** [**group-name** *group-name*]
显示BGP VPNv6对等体的信息（MSR 2600/MSR 3600）	**display bgp peer vpnv6** [{ *ip-address* | **group-name** *group-name* } **log-info** | [*ip-address*] **verbose**]
显示BGP VPNv6对等体的信息（MSR 5600）	**display bgp peer vpnv6** [{ *ip-address* | **group-name** *group-name* } **log-info** | [[*ip-address*] **verbose**] [**standby slot** *slot-number*]]
显示BGP VPNv6路由信息（MSR 2600/MSR 3600）	**display bgp routing-table vpnv6** [[**route-distinguisher** *route-distinguisher*] [*network-address prefix-length* [**advertise-info**] | **as-path-acl** *as-path-acl-number* | **community-list** { { *basic-community-list-number* | *comm-list-name* } [**whole-match**] | *adv-community-list-number* }] | **peer** *ip-address* { **advertised-routes** | **received-routes** } [*network-address prefix-length* | **statistics**] | **statistics**]

操作	命令
显示BGP VPNv6路由信息（MSR 5600）	**display bgp routing-table vpnv6** [[**route-distinguisher** *route-distinguisher*] [*network-address prefix-length* [**advertise-info**] | **as-path-acl** *as-path-acl-number* | **community-list** { { *basic-community-list-number* | *comm-list-name* } [**whole-match**] | *adv-community-list-number* }] | **peer** *ip-address* { **advertised-routes** | **received-routes** } [*network-address prefix-length* | **statistics**] | **statistics**] [**standby slot** *slot-number*]
显示所有BGP VPNv6路由的入标签信息	**display bgp routing-table vpnv6 inlabel**
显示所有BGP VPNv6路由的出标签信息（MSR 2600/MSR 3600）	**display bgp routing-table vpnv6 outlabel**
显示所有BGP VPNv6路由的出标签信息（MSR 5600）	**display bgp routing-table vpnv6 outlabel** [**standby slot** *slot-number*]
显示BGP VPNv6地址族下打包组的相关信息	**display bgp update-group vpnv6** [*ip-address*]

2.8 IPv6 MPLS L3VPN典型配置举例

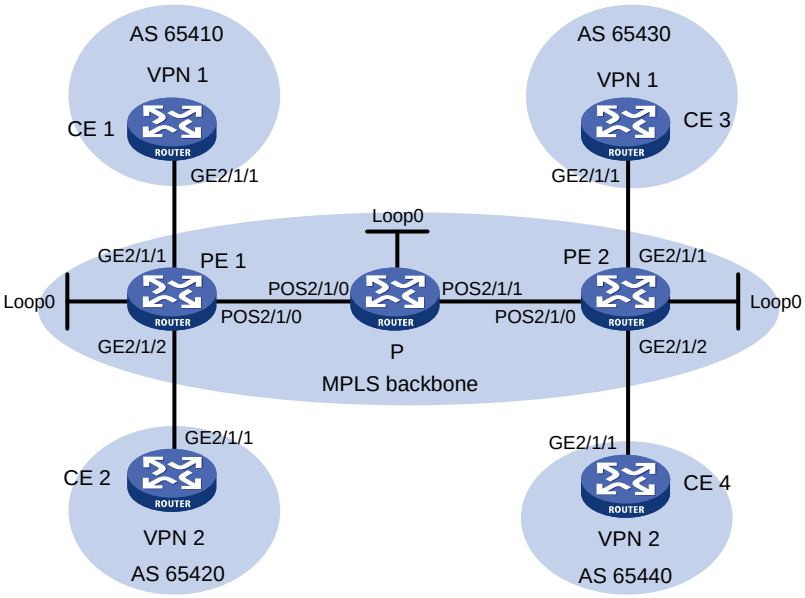
2.8.1 配置IPv6 MPLS L3VPN示例

1. 组网需求

- CE 1、CE 3 属于 VPN 1，CE 2、CE 4 属于 VPN 2；
- VPN 1 使用的 VPN Target 属性为 111:1，VPN 2 使用的 VPN Target 属性为 222:2。不同 VPN 用户之间不能互相访问；
- CE 与 PE 之间配置 EBGP 交换 VPN 路由信息；
- PE 与 PE 之间配置 OSPF 实现 PE 内部的互通、配置 MP-IBGP 交换 VPN 路由信息。

2. 组网图

图2-3 配置 IPv6 MPLS L3VPN 组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	GE2/1/1	2001:1::1/96	P	Loop0	2.2.2.9/32
PE 1	Loop0	1.1.1.9/32		POS2/1/0	172.1.1.2/24
	GE2/1/1	2001:1::2/96		POS2/1/1	172.2.1.1/24
	GE2/1/2	2001:2::2/96	PE 2	Loop0	3.3.3.9/32
	POS2/1/0	172.1.1.1/24		GE2/1/1	2001:3::2/96
CE 2	GE2/1/1	2001:2::1/96		GE2/1/2	2001:4::2/96
CE 3	GE2/1/1	2001:3::1/96		POS2/1/0	172.2.1.2/24
CE 4	GE2/1/1	2001:4::1/96			

3. 配置步骤

(1) 在 MPLS 骨干网上配置 IGP 协议，实现骨干网 PE 和 P 的互通

配置 PE 1。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.9 32
[PE1-LoopBack0] quit
[PE1] interface pos 2/1/0
[PE1-Pos2/1/0] ip address 172.1.1.1 24
[PE1-Pos2/1/0] quit
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 172.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

配置 P。

```
<P> system-view
[P] interface loopback 0
```

```
[P-LoopBack0] ip address 2.2.2.9 32
[P-LoopBack0] quit
[P] interface pos 2/1/0
[P-Pos2/1/0] ip address 172.1.1.2 24
[P-Pos2/1/0] quit
[P] interface pos 2/1/1
[P-Pos2/1/1] ip address 172.2.1.1 24
[P-Pos2/1/1] quit
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 172.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 172.2.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

配置 PE 2。

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 3.3.3.9 32
[PE2-LoopBack0] quit
[PE2] interface pos 2/1/0
[PE2-Pos2/1/0] ip address 172.2.1.2 24
[PE2-Pos2/1/0] quit
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 172.2.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

配置完成后，PE 1、P、PE 2 之间应能建立 OSPF 邻居，执行 **display ospf peer** 命令可以看到邻居达到 FULL 状态。执行 **display ip routing-table** 命令可以看到 PE 之间学习到对方的 Loopback 路由。

以 PE 1 为例：

```
[PE1] display ip routing-table protocol ospf

Summary Count : 5

OSPF Routing table Status : <Active>
Summary Count : 3

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
2.2.2.9/32          OSPF   10   1            172.1.1.2       POS2/1/0
3.3.3.9/32          OSPF   10   2            172.1.1.2       POS2/1/0
172.2.1.0/24        OSPF   10   2            172.1.1.2       POS2/1/0

OSPF Routing table Status : <Inactive>
Summary Count : 2
```

```
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
1.1.1.9/32          OSPF   10   0            1.1.1.9         Loop0
172.1.1.0/24        OSPF   10   1            172.1.1.1       POS2/1/0
[PE1] display ospf peer verbose

          OSPF Process 1 with Router ID 1.1.1.9
                  Neighbors

 Area 0.0.0.0 interface 172.1.1.1(POS2/1/0)'s neighbors
 Router ID: 2.2.2.9          Address: 172.1.1.2        GR State: Normal
   State: Full  Mode: Nbr is Master  Priority: 1
   DR: 172.1.1.2  BDR: 172.1.1.1  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 39  sec
   Neighbor is up for 00:00:29
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
```

(2) 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP

配置 PE 1。

```
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] interface pos 2/1/0
[PE1-Pos2/1/0] mpls enable
[PE1-Pos2/1/0] mpls ldp enable
[PE1-Pos2/1/0] quit
```

配置 P。

```
[P] mpls lsr-id 2.2.2.9
[P] mpls ldp
[P-ldp] quit
[P] interface pos 2/1/0
[P-Pos2/1/0] mpls enable
[P-Pos2/1/0] mpls ldp enable
[P-Pos2/1/0] quit
[P] interface pos 2/1/1
[P-Pos2/1/1] mpls enable
[P-Pos2/1/1] mpls ldp enable
[P-Pos2/1/1] quit
```

配置 PE 2。

```
[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls ldp
[PE2-ldp] quit
[PE2] interface pos 2/1/0
[PE2-Pos2/1/0] mpls enable
[PE2-Pos2/1/0] mpls ldp enable
[PE2-Pos2/1/0] quit
```

上述配置完成后，PE 1、P、PE 2 之间应能建立 LDP 会话，执行 **display mpls ldp peer** 命令可以看到 LDP 会话状态为 Operational。执行 **display mpls ldp lsp** 命令，可以看到 LDP LSP 的建立情况。

以 PE 1 为例：

```
[PE1] display mpls ldp peer
Total number of peers: 1
Peer LDP ID        State         LAM  Role     GR   MD5  KA Sent/Rcvd
2.2.2.9:0          Operational   DU   Passive  Off  Off  5/5
[PE1] display mpls ldp lsp
        Status codes: * - stale, L - liberal
FECs: 3            Ingress: 2      Transit: 2      Egress: 1

FEC                In/Out Label    Nexthop         OutInterface
1.1.1.9/32         3/-
                   -/1151(L)
2.2.2.9/32         -/3             172.1.1.2       POS2/1/0
                   1151/3          172.1.1.2       POS2/1/0
3.3.3.9/32         -/1150          172.1.1.2       POS2/1/0
                   1150/1150       172.1.1.2       POS2/1/0
```

(3) 在 PE 设备上配置 IPv6 VPN 实例，将 CE 接入 PE

配置 PE 1。

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 100:1
[PE1-vpn-instance-vpn1] vpn-target 111:1
[PE1-vpn-instance-vpn1] quit
[PE1] ip vpn-instance vpn2
[PE1-vpn-instance-vpn2] route-distinguisher 100:2
[PE1-vpn-instance-vpn2] vpn-target 222:2
[PE1-vpn-instance-vpn2] quit
[PE1] interface gigabitethernet 2/1/1
[PE1-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE1-GigabitEthernet2/1/1] ipv6 address 2001:1::2 96
[PE1-GigabitEthernet2/1/1] quit
[PE1] interface gigabitethernet 2/1/2
[PE1-GigabitEthernet2/1/2] ip binding vpn-instance vpn2
[PE1-GigabitEthernet2/1/2] ipv6 address 2001:2::2 96
[PE1-GigabitEthernet2/1/2] quit
```

配置 PE 2。

```
[PE2] ip vpn-instance vpn1
[PE2-vpn-instance-vpn1] route-distinguisher 200:1
[PE2-vpn-instance-vpn1] vpn-target 111:1
[PE2-vpn-instance-vpn1] quit
[PE2] ip vpn-instance vpn2
[PE2-vpn-instance-vpn2] route-distinguisher 200:2
[PE2-vpn-instance-vpn2] vpn-target 222:2
[PE2-vpn-instance-vpn2] quit
[PE2] interface gigabitethernet 2/1/1
```

```
[PE2-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE2-GigabitEthernet2/1/1] ipv6 address 2001:3::2 96
[PE2-GigabitEthernet2/1/1] quit
[PE2] interface gigabitethernet 2/1/2
[PE2-GigabitEthernet2/1/2] ip binding vpn-instance vpn2
[PE2-GigabitEthernet2/1/2] ipv6 address 2001:4::2 96
[PE2-GigabitEthernet2/1/2] quit
```

按 图 2-3 配置各CE的接口IP地址，配置过程略。

配置完成后，在 PE 设备上执行 **display ip vpn-instance** 命令可以看到 VPN 实例的配置情况。各 PE 能 ping 通自己接入的 CE。

以 PE 1 和 CE 1 为例：

```
[PE1] display ip vpn-instance
  Total VPN-Instances configured : 2
  VPN-Instance Name               RD                      Create time
  vpn1                            100:1                   2012/02/13 12:49:08
  vpn2                            100:2                   2012/02/13 12:49:20
[PE1] ping ipv6 -vpn-instance vpn1 2001:1::1
Ping6(56 bytes) 2001:1::2 --> 2001:1::1, press CTRL_C to break
56 bytes from 2001:1::1, icmp_seq=0 hlim=64 time=9.000 ms
56 bytes from 2001:1::1, icmp_seq=1 hlim=64 time=1.000 ms
56 bytes from 2001:1::1, icmp_seq=2 hlim=64 time=0.000 ms
56 bytes from 2001:1::1, icmp_seq=3 hlim=64 time=0.000 ms
56 bytes from 2001:1::1, icmp_seq=4 hlim=64 time=0.000 ms

--- Ping6 statistics for 2001:1::1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/2.000/9.000/3.521 ms
```

(4) 在 PE 与 CE 之间建立 EBGP 对等体，引入 VPN 路由

配置 CE 1。

```
<CE1> system-view
[CE1] bgp 65410
[CE1-bgp] peer 2001:1::2 as-number 100
[CE1-bgp] address-family ipv6 unicast
[CE1-bgp-ipv6] peer 2001:1::2 enable
[CE1-bgp-ipv6] import-route direct
[CE1-bgp-ipv6] quit
[CE1-bgp] quit
```

另外 3 个 CE 设备（CE 2～CE 4）配置与 CE 1 设备配置类似，配置过程省略。

配置 PE 1。

```
[PE1] bgp 100
[PE1-bgp] ip vpn-instance vpn1
[PE1-bgp-vpn1] peer 2001:1::1 as-number 65410
[PE1-bgp-vpn1] address-family ipv6 unicast
[PE1-bgp-ipv6-vpn1] peer 2001:1::1 enable
[PE1-bgp-ipv6-vpn1] import-route direct
[PE1-bgp-ipv6-vpn1] quit
```

```
[PE1-bgp-vpn1] quit
[PE1-bgp] ip vpn-instance vpn2
[PE1-bgp-vpn2] peer 2001:2::1 as-number 65420
[PE1-bgp-vpn2] address-family ipv6 unicast
[PE1-bgp-ipv6-vpn2] peer 2001:2::1 enable
[PE1-bgp-ipv6-vpn2] import-route direct
[PE1-bgp-ipv6-vpn2] quit
[PE1-bgp-vpn2] quit
[PE1-bgp] quit
```

PE 2 的配置与 PE 1 类似，配置过程省略。

配置完成后，在 PE 设备上执行 **display bgp peer ipv6 vpn-instance** 命令，可以看到 PE 与 CE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

(5) 在 PE 之间建立 MP-IBGP 对等体

配置 PE 1。

```
[PE1] bgp 100
[PE1-bgp] peer 3.3.3.9 as-number 100
[PE1-bgp] peer 3.3.3.9 connect-interface loopback 0
[PE1-bgp] address-family vpnv6
[PE1-bgp-vpnv6] peer 3.3.3.9 enable
[PE1-bgp-vpnv6] quit
[PE1-bgp] quit
```

配置 PE 2。

```
[PE2] bgp 100
[PE2-bgp] peer 1.1.1.9 as-number 100
[PE2-bgp] peer 1.1.1.9 connect-interface loopback 0
[PE2-bgp] address-family vpnv6
[PE2-bgp-vpnv6] peer 1.1.1.9 enable
[PE2-bgp-vpnv6] quit
[PE2-bgp] quit
```

配置完成后，在 PE 设备上执行 **display bgp peer vpnv6** 命令，可以看到 PE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

4. 验证配置

在 PE 设备上执行 **display ipv6 routing-table vpn-instance** 命令，可以看到去往对端 CE 的路由。

以 PE 1 为例：

```
[PE1] display ipv6 routing-table vpn-instance vpn1

Destinations : 6 Routes : 6

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: 2001:1::/96                            Protocol  : Direct
NextHop    : ::                                     Preference: 0
```

```
Interface  : GE2/1/1                                    Cost      : 0

Destination: 2001:1::2/128                              Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 2001:3::/96                                Protocol  : BGP4+
NextHop    : ::FFFF:3.3.3.9                             Preference: 255
Interface  : POS2/1/0                                   Cost      : 0

Destination: FE80::/10                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0

Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0
[PE1] display ipv6 routing-table vpn-instance vpn2

Destinations : 6 Routes : 6

Destination: ::1/128                                    Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 2001:2::/96                                Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : GE2/1/2                                    Cost      : 0

Destination: 2001:2::2/128                              Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 2001:4::/96                                Protocol  : BGP4+
NextHop    : ::FFFF:3.3.3.9                             Preference: 255
Interface  : POS2/1/0                                   Cost      : 0

Destination: FE80::/10                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0

Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0
```

同一 VPN 的 CE 能够相互 Ping 通，不同 VPN 的 CE 不能相互 Ping 通。例如：CE 1 能够 Ping 通 CE 3（2001:3::1），但不能 Ping 通 CE 4（2001:4::1）。

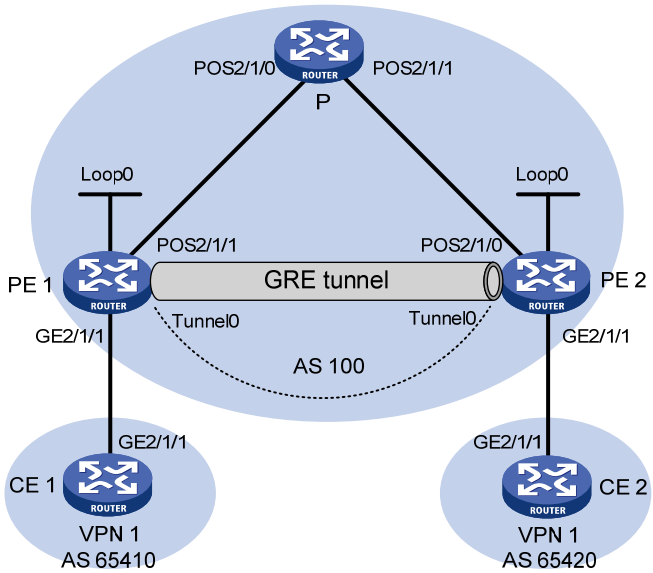
2.8.2 配置IPv6 MPLS L3VPN采用GRE隧道示例

1. 组网需求

- CE 1 和 CE 2 属于 VPN 1。
- 在运营商骨干网上，PE 设备具备 MPLS 能力，P 设备只提供纯 IP 功能，不具备 MPLS 能力。
- 在骨干网上使用 GRE 隧道封装并转发 VPN 报文，实现 IPv6 MPLS L3VPN。
- 在 PE 上配置隧道策略，指定 VPN 流量使用的隧道类型为 GRE。（本配置可选）

2. 组网图

图2-4 配置采用 GRE 隧道的 IPv6 MPLS L3VPN 组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	GE2/1/1	2001:1::1/96	P	POS2/1/0	172.1.1.2/24
PE 1	Loop0	1.1.1.9/32		POS2/1/1	172.2.1.1/24
	GE2/1/1	2001:1::2/96	PE 2	Loop0	2.2.2.9/32
	POS2/1/1	172.1.1.1/24		GE2/1/1	2001:2::2/96
	Tunnel0	20.1.1.1/24		POS2/1/0	172.2.1.2/24
CE 2	GE2/1/1	2001:2::1/96		Tunnel0	20.1.1.2/24

3. 配置步骤

(1) 在 MPLS 骨干网上配置 IGP 协议，实现骨干网 PE 和 P 的互通

本例中采用 OSPF 发布接口（包括 Loopback 接口）所在网段的路由，具体配置过程略。

配置完成后，PE 1、P、PE 2 之间应能建立 OSPF 邻居，执行 **display ospf peer** 命令可以看到邻居达到 FULL 状态。执行 **display ip routing-table** 命令可以看到 PE 之间学习到对方的 Loopback 路由。

(2) 在 PE 设备上使能 MPLS 基本能力

配置 PE 1。

```
<PE1> system-view
[PE1] mpls lsr-id 1.1.1.9
```

配置 PE 2。

```
<PE2> system-view
```

```
[PE2] mpls lsr-id 2.2.2.9
```

(3) 在 PE 设备上配置 VPN 实例，将 CE 接入 PE，并在 PE 上应用隧道策略，指定使用 GRE 隧道转发 VPN 报文

配置 PE 1。

```
[PE1] tunnel-policy gre1
[PE1-tunnel-policy-gre1] select-seq gre load-balance-number 1
[PE1-tunnel-policy-gre1] quit
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 100:1
[PE1-vpn-instance-vpn1] vpn-target 100:1 both
[PE1-vpn-instance-vpn1] tnl-policy gre1
[PE1-vpn-instance-vpn1] quit
[PE1] interface gigabitethernet 2/1/1
[PE1-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE1-GigabitEthernet2/1/1] ipv6 address 2001:1::2 96
[PE1-GigabitEthernet2/1/1] quit
```

配置 PE 2。

```
[PE2] tunnel-policy gre1
[PE2-tunnel-policy-gre1] select-seq gre load-balance-number 1
[PE2-tunnel-policy-gre1] quit
[PE2] ip vpn-instance vpn1
[PE2-vpn-instance-vpn1] route-distinguisher 100:2
[PE2-vpn-instance-vpn1] vpn-target 100:1 both
[PE2-vpn-instance-vpn1] tnl-policy gre1
[PE2-vpn-instance-vpn1] quit
[PE2] interface gigabitethernet 2/1/1
[PE2-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE2-GigabitEthernet2/1/1] ipv6 address 2001:2::2 96
[PE2-GigabitEthernet2/1/1] quit
```

配置 CE 1。

```
<CE1> system-view
[CE1] interface gigabitethernet 2/1/1
[CE1-GigabitEthernet2/1/1] ipv6 address 2001:1::1 96
[CE1-GigabitEthernet2/1/1] quit
```

配置 CE2。

```
<CE2> system-view
[CE2] interface gigabitethernet 2/1/1
[CE2-GigabitEthernet2/1/1] ipv6 address 2001:2::1 96
[CE2-GigabitEthernet2/1/1] quit
```

配置完成后，在 PE 设备上执行 **display ip vpn-instance** 命令可以看到 VPN 实例的配置情况。各 PE 能 ping 通自己接入的 CE。

以 PE 1 为例：

```
[PE1] display ip vpn-instance
  Total VPN-Instances configured : 1
  VPN-Instance Name               RD                      Create time
  vpn1                            100:1                   2012/02/13 15:59:50
```

```
[PE1] ping ipv6 -vpn-instance vpn1 2001:1::1
Ping6(56 bytes) 2001:1::2 --> 2001:1::1, press CTRL_C to break
56 bytes from 2001:1::1, icmp_seq=0 hlim=64 time=0.000 ms
56 bytes from 2001:1::1, icmp_seq=1 hlim=64 time=1.000 ms
56 bytes from 2001:1::1, icmp_seq=2 hlim=64 time=0.000 ms
56 bytes from 2001:1::1, icmp_seq=3 hlim=64 time=1.000 ms
56 bytes from 2001:1::1, icmp_seq=4 hlim=64 time=0.000 ms

--- Ping6 statistics for 2001:1::1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.400/1.000/0.490 ms
```

(4) 在 PE 与 CE 之间建立 EBGP 对等体，引入 VPN 路由

配置 CE 1。

```
[CE1] bgp 65410
[CE1-bgp] peer 2001:1::2 as-number 100
[CE1-bgp] address-family ipv6 unicast
[CE1-bgp-ipv6] peer 2001:1::2 enable
[CE1-bgp-ipv6] import-route direct
[CE1-bgp-ipv6] quit
```

配置 PE 1。

```
[PE1] bgp 100
[PE1-bgp] ip vpn-instance vpn1
[PE1-bgp-vpn1] peer 2001:1::1 as-number 65410
[PE1-bgp-vpn1] address-family ipv6 unicast
[PE1-bgp-ipv6-vpn1] peer 2001:1::1 enable
[PE1-bgp-ipv6-vpn1] import-route direct
[PE1-bgp-ipv6-vpn1] quit
[PE1-bgp-vpn1] quit
[PE1-bgp] quit
```

CE 2 的配置与 CE 1 类似，PE 2 的配置与 PE 1 类似，配置过程省略。

配置完成后，在 PE 设备上执行 **display bgp peer ipv6 vpn-instance** 命令，可以看到 PE 与 CE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

以 PE 1 为例：

```
[PE1] display bgp peer ipv6 vpn-instance vpn1

 BGP local router ID : 1.1.1.9
 Local AS number : 100
 Total number of peers : 1             Peers in established state : 1

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State
  2001:1::1            65410        5        5    0       1 00:02:03 Established
```

(5) 在 PE 之间建立 MP-IBGP 对等体

配置 PE 1。

```
[PE1] bgp 100
[PE1-bgp] peer 2.2.2.9 as-number 100
[PE1-bgp] peer 2.2.2.9 connect-interface loopback 0
```

```
[PE1-bgp] address-family vpnv6
[PE1-bgp-vpnv6] peer 2.2.2.9 enable
[PE1-bgp-vpnv6] quit
[PE1-bgp] quit
```

PE 2 的配置与 PE 1 类似，配置过程省略。

配置完成后，在 PE 设备上执行 **display bgp peer vpnv6** 命令，可以看到 PE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

```
[PE1] display bgp peer vpnv6

 BGP local router ID : 1.1.1.9
 Local AS number : 100
 Total number of peers : 1           Peers in established state : 1

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State
  2.2.2.9                100        3        3    0       1 00:00:34 Established
```

(6) 配置 GRE 隧道

配置 PE 1。

```
[PE1] interface tunnel 0 mode gre
[PE1-Tunnel0] source loopback 0
[PE1-Tunnel0] destination 2.2.2.9
[PE1-Tunnel0] ip address 20.1.1.1 24
[PE1-Tunnel0] mpls enable
[PE1-Tunnel0] quit
```

配置 PE 2。

```
[PE2] interface tunnel 0 mode gre
[PE2-Tunnel0] source loopback 0
[PE2-Tunnel0] destination 1.1.1.9
[PE2-Tunnel0] ip address 20.1.1.2 24
[PE2-Tunnel0] mpls enable
[PE2-Tunnel0] quit
```

4. 验证配置

配置完成后，CE 能学到对端 CE 的接口路由。CE 之间能够 ping 通。

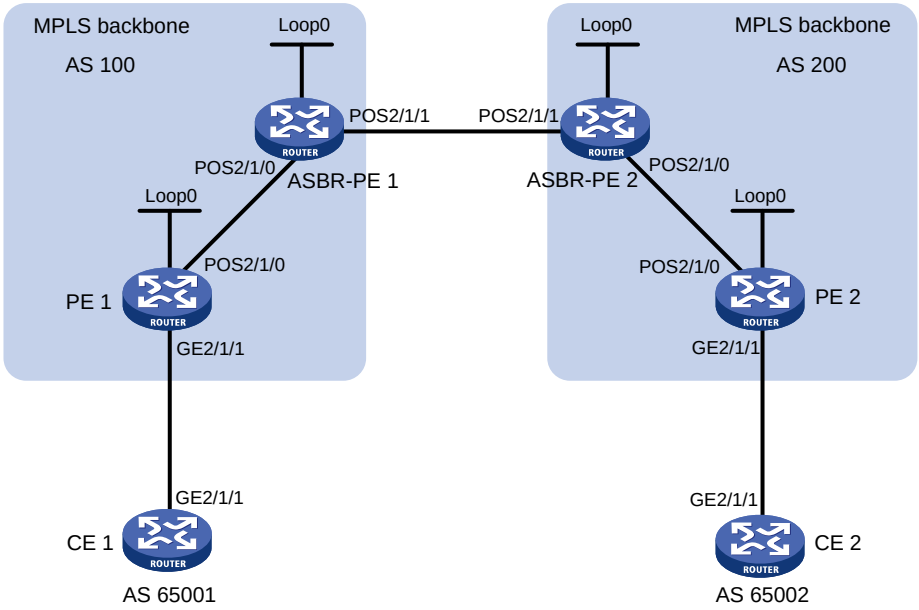
2.8.3 配置IPv6 跨域VPN-OptionA方式示例

1. 组网需求

- CE 1 和 CE 2 属于同一个 VPN。
- CE 1 通过 AS100 的 PE 1 接入，CE2 通过 AS200 的 PE 2 接入。
- 采用 OptionA 方式实现跨域的 IPv6 MPLS L3VPN，即采用 VRF-to-VRF 方式管理 VPN 路由。
- 同一个 AS 内部的 MPLS 骨干网使用 OSPF 作为 IGP。

2. 组网图

图2-5 配置跨域 VPN-OptionA 方式组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	GE2/1/1	2001:1::1/96	CE 2	GE2/1/1	2001:2::1/96
PE 1	Loop0	1.1.1.9/32	PE 2	Loop0	4.4.4.9/32
	GE2/1/1	2001:1::2/96		GE2/1/1	2001:2::2/96
	POS2/1/0	172.1.1.2/24		POS2/1/0	162.1.1.2/24
ASBR-PE1	Loop0	2.2.2.9/32	ASBR-PE2	Loop0	3.3.3.9/32
	POS2/1/0	172.1.1.1/24		POS2/1/0	162.1.1.1/24
	POS2/1/1	2002:1::1/96		POS2/1/1	2002:1::2/96

3. 配置步骤

(1) 在 MPLS 骨干网上配置 IGP 协议，实现骨干网内互通

本例中采用 OSPF 发布接口（包括 Loopback 接口）所在网段的路由，具体配置步骤略。

配置完成后，ASBR-PE 与本 AS 的 PE 之间应能建立 OSPF 邻居，执行 **display ospf peer** 命令可以看到邻居达到 FULL 状态，ASBR-PE 与本 AS 的 PE 之间能学习到对方的 Loopback 地址。

ASBR-PE 与本 AS 的 PE 之间能够互相 ping 通。

(2) 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP

配置 PE 1 的 MPLS 基本能力，并在与 ASBR-PE 1 相连的接口上使能 LDP。

```
<PE1> system-view
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] interface pos 2/1/0
[PE1-Pos2/1/0] mpls enable
[PE1-Pos2/1/0] mpls ldp enable
[PE1-Pos2/1/0] quit
```

配置 ASBR-PE 1 的 MPLS 基本能力，并在与 PE 1 相连的接口上使能 LDP。

```
<ASBR-PE1> system-view
```

```
[ASBR-PE1] mpls lsr-id 2.2.2.9
[ASBR-PE1] mpls ldp
[ASBR-PE1-ldp] quit
[ASBR-PE1] interface pos 2/1/0
[ASBR-PE1-Pos2/1/0] mpls enable
[ASBR-PE1-Pos2/1/0] mpls ldp enable
[ASBR-PE1-Pos2/1/0] quit
```

配置 ASBR-PE 2 的 MPLS 基本能力，并在与 PE 2 相连的接口上使能 LDP。

```
<ASBR-PE2> system-view
[ASBR-PE2] mpls lsr-id 3.3.3.9
[ASBR-PE2] mpls ldp
[ASBR-PE2-ldp] quit
[ASBR-PE2] interface pos 2/1/0
[ASBR-PE2-Pos2/1/0] mpls enable
[ASBR-PE2-Pos2/1/0] mpls ldp enable
[ASBR-PE2-Pos2/1/0] quit
```

配置 PE 2 的 MPLS 基本能力，并在与 ASBR-PE 2 相连的接口上使能 LDP。

```
<PE2> system-view
[PE2] mpls lsr-id 4.4.4.9
[PE2] mpls ldp
[PE2-ldp] quit
[PE2] interface pos 2/1/0
[PE2-Pos2/1/0] mpls enable
[PE2-Pos2/1/0] mpls ldp enable
[PE2-Pos2/1/0] quit
```

上述配置完成后，同一 AS 的 PE 和 ASBR-PE 之间应该建立起 LDP 邻居，在各设备上执行 **display mpls ldp peer** 命令可以看到 LDP 会话状态为“Operational”。

(3) 在 PE 设备上配置 VPN 实例，将 CE 接入 PE

说明

同一 AS 内的 ASBR-PE 与 PE 的 VPN 实例的 VPN Target 应能匹配，不同 AS 的 PE 的 VPN 实例的 VPN Target 则不需要匹配。

配置 CE 1。

```
<CE1> system-view
[CE1] interface gigabitethernet 2/1/1
[CE1-GigabitEthernet2/1/1] ipv6 address 2001:1::1 96
[CE1-GigabitEthernet2/1/1] quit
```

配置 PE 1。

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 100:1
[PE1-vpn-instance-vpn1] vpn-target 100:1 both
[PE1-vpn-instance-vpn1] quit
[PE1] interface gigabitethernet 2/1/1
[PE1-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
```

```
[PE1-GigabitEthernet2/1/1] ipv6 address 2001:1::2 96
[PE1-GigabitEthernet2/1/1] quit
```

配置 CE 2。

```
<CE2> system-view
[CE2] interface gigabitethernet 2/1/1
[CE2-GigabitEthernet2/1/1] ipv6 address 2001:2::1 96
[CE2-GigabitEthernet2/1/1] quit
```

配置 PE 2。

```
[PE2] ip vpn-instance vpn1
[PE2-vpn-instance-vpn1] route-distinguisher 200:2
[PE2-vpn-instance-vpn1] vpn-target 200:1 both
[PE2-vpn-instance-vpn1] quit
[PE2] interface gigabitethernet 2/1/1
[PE2-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE2-GigabitEthernet2/1/1] ipv6 address 2001:2::2 96
[PE2-GigabitEthernet2/1/1] quit
```

配置 ASBR-PE 1：创建 VPN 实例，并将此实例绑定到连接 ASBR-PE 2 的接口（ASBR-PE 1 认为 ASBR-PE 2 是自己的 CE）。

```
[ASBR-PE1] ip vpn-instance vpn1
[ASBR-PE1-vpn-vpn1] route-distinguisher 100:1
[ASBR-PE1-vpn-vpn1] vpn-target 100:1 both
[ASBR-PE1-vpn-vpn1] quit
[ASBR-PE1] interface pos 2/1/1
[ASBR-PE1-Pos2/1/1] ip binding vpn-instance vpn1
[ASBR-PE1-Pos2/1/1] ipv6 address 2002:1::1 96
[ASBR-PE1-Pos2/1/1] quit
```

配置 ASBR-PE 2：创建 VPN 实例，并将此实例绑定到连接 ASBR-PE 1 的接口（ASBR-PE 2 认为 ASBR-PE 1 是自己的 CE）。

```
[ASBR-PE2] ip vpn-instance vpn1
[ASBR-PE2-vpn-vpn1] route-distinguisher 200:1
[ASBR-PE2-vpn-vpn1] vpn-target 200:1 both
[ASBR-PE2-vpn-vpn1] quit
[ASBR-PE2] interface pos 2/1/1
[ASBR-PE2-Pos2/1/1] ip binding vpn-instance vpn1
[ASBR-PE2-Pos2/1/1] ipv6 address 2002:1::2 96
[ASBR-PE2-Pos2/1/1] quit
```

上述配置完成后，在各 PE 设备上执行 **display ip vpn-instance** 命令能正确显示 VPN 实例配置。各 PE 能 ping 通各自的 CE。ASBR-PE 之间也能互相 ping 通。

(4) 在 PE 与 CE 之间建立 EBGP 对等体，引入 VPN 路由

配置 CE 1。

```
[CE1] bgp 65001
[CE1-bgp] peer 2001:1::2 as-number 100
[CE1-bgp] address-family ipv6 unicast
[CE1-bgp-ipv6] peer 2001:1::2 enable
[CE1-bgp-ipv6] import-route direct
[CE1-bgp-ipv6] quit
```

```
[CE1-bgp] quit
```

配置 PE 1。

```
[PE1] bgp 100
[PE1-bgp] ip vpn-instance vpn1
[PE1-bgp-vpn1] peer 2001:1::1 as-number 65001
[PE1-bgp-vpn1] address-family ipv6 unicast
[PE1-bgp-ipv6-vpn1] peer 2001:1::1 enable
[PE1-bgp-ipv6-vpn1] quit
[PE1-bgp-vpn1] quit
[PE1-bgp] quit
```

配置 CE 2。

```
[CE2] bgp 65002
[CE2-bgp] peer 2001:2::2 as-number 200
[CE2-bgp] address-family ipv6
[CE2-bgp-ipv6] peer 2001:2::2 enable
[CE2-bgp-ipv6] import-route direct
[CE2-bgp-ipv6] quit
[CE2-bgp] quit
```

配置 PE 2。

```
[PE2] bgp 200
[PE2-bgp] ip vpn-instance vpn1
[PE2-bgp-vpn1] peer 2001:2::1 as-number 65002
[PE2-bgp-vpn1] address-family ipv6 unicast
[PE2-bgp-ipv6-vpn1] peer 2001:2::1 enable
[PE2-bgp-ipv6-vpn1] quit
[PE2-bgp-vpn1] quit
[PE2-bgp] quit
```

(5) PE 与本 AS 的 ASBR-PE 之间建立 IBGP 对等体，ASBR-PE 之间建立 EBGP 对等体

配置 PE 1。

```
[PE1] bgp 100
[PE1-bgp] peer 2.2.2.9 as-number 100
[PE1-bgp] peer 2.2.2.9 connect-interface loopback 0
[PE1-bgp] address-family vpnv6
[PE1-bgp-vpnv6] peer 2.2.2.9 enable
[PE1-bgp-vpnv6] quit
[PE1-bgp] quit
```

配置 ASBR-PE 1。

```
[ASBR-PE1] bgp 100
[ASBR-PE1-bgp] ip vpn-instance vpn1
[ASBR-PE1-bgp-vpn1] peer 2002:1::2 as-number 200
[ASBR-PE1-bgp-vpn1] address-family ipv6 unicast
[ASBR-PE1-bgp-ipv6-vpn1] peer 2002:1::2 enable
[ASBR-PE1-bgp-ipv6-vpn1] quit
[ASBR-PE1-bgp-vpn1] quit
[ASBR-PE1-bgp] peer 1.1.1.9 as-number 100
[ASBR-PE1-bgp] peer 1.1.1.9 connect-interface loopback 0
[ASBR-PE1-bgp] address-family vpnv6
```

```
[ASBR-PE1-bgp-vpnv6] peer 1.1.1.9 enable
[ASBR-PE1-bgp-vpnv6] quit
[ASBR-PE1-bgp] quit
```

配置 ASBR-PE 2。

```
[ASBR-PE2] bgp 200
[ASBR-PE2-bgp] ip vpn-instance vpn1
[ASBR-PE2-bgp-vpn1] peer 2002:1::1 as-number 100
[ASBR-PE2-bgp-vpn1] address-family ipv6 unicast
[ASBR-PE2-bgp-ipv6-vpn1] peer 2002:1::1 enable
[ASBR-PE2-bgp-ipv6-vpn1] quit
[ASBR-PE2-bgp-vpn1] quit
[ASBR-PE2-bgp] peer 4.4.4.9 as-number 200
[ASBR-PE2-bgp] peer 4.4.4.9 connect-interface loopback 0
[ASBR-PE2-bgp] address-family vpnv6
[ASBR-PE2-bgp-vpnv6] peer 4.4.4.9 enable
[ASBR-PE2-bgp-vpnv6] quit
[ASBR-PE2-bgp] quit
```

配置 PE 2。

```
[PE2] bgp 200
[PE2-bgp] peer 3.3.3.9 as-number 200
[PE2-bgp] peer 3.3.3.9 connect-interface loopback 0
[PE2-bgp] address-family vpnv6
[PE2-bgp-vpnv6] peer 3.3.3.9 enable
[PE2-bgp-vpnv6] quit
[PE2-bgp] quit
```

4. 验证配置

上述配置完成后，CE 之间能学习到对方的接口路由，CE 1 和 CE 2 能够相互 ping 通。

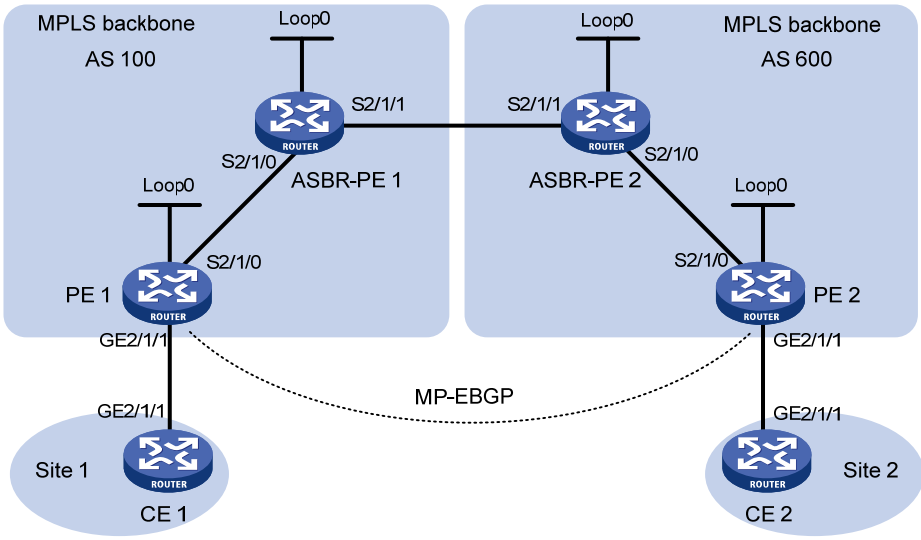
2.8.4 配置IPv6 跨域VPN-OptionC方式示例

1. 组网需求

- Site 1 和 Site 2 属于同一个 VPN，Site 1 通过 AS 100 的 PE 1 接入，Site 2 通过 AS 600 的 PE 2 接入；
- 同一自治系统内的 PE 设备之间运行 IS-IS 作为 IGP；
- PE 1 与 ASBR-PE 1 间通过 IBGP 交换带标签的 IPv4 路由；
- PE 2 与 ASBR-PE 2 间通过 IBGP 交换带标签的 IPv4 路由；
- PE 1 与 PE 2 建立 MP-EBGP 对等体交换 VPNv6 路由；
- ASBR-PE 1 和 ASBR-PE 2 上分别配置路由策略，对从对方接收的路由压入标签；
- ASBR-PE 1 与 ASBR-PE 2 间通过 EBGP 交换带标签的 IPv4 路由。

2. 组网图

图2-6 配置 IPv6 跨域 VPN-OptionC 方式组网图



设备	接口	IP地址	设备	接口	IP地址
PE 1	Loop0	2.2.2.9/32	PE 2	Loop0	5.5.5.9/32
	GE2/1/1	2001::1/64		GE2/1/1	2002::1/64
	S2/1/0	1.1.1.2/8		S2/1/0	9.1.1.2/8
ASBR-PE 1	Loop0	3.3.3.9/32	ASBR-PE 2	Loop0	4.4.4.9/32
	S2/1/0	1.1.1.1/8		S2/1/0	9.1.1.1/8
	S2/1/1	11.0.0.2/8		S2/1/1	11.0.0.1/8
CE 1	GE2/1/1	2001::2/64	CE 1	GE2/1/1	2002::2/64

3. 配置步骤

(1) 配置 CE 1

配置接口 GigabitEthernet2/1/1 的 IPv6 地址。

```
<CE1> system-view
[CE1] interface gigabitethernet 2/1/1
[CE1-GigabitEthernet2/1/1] ipv6 address 2001::2 64
[CE1-GigabitEthernet2/1/1] quit
```

配置 CE 1 与 PE 1 建立 EBGP 对等体，并引入 VPN 路由。

```
[CE1] bgp 65001
[CE1-bgp] peer 2001::1 as-number 100
[CE1-bgp] address-family ipv6 unicast
[CE1-bgp-ipv6] peer 2001::1 enable
[CE1-bgp-ipv6] import-route direct
[CE1-bgp-ipv6] quit
[CE1-bgp] quit
```

(2) 配置 PE 1

在 PE 1 上运行 IS-IS。

```
<PE1> system-view
[PE1] isis 1
[PE1-isis-1] network-entity 10.111.111.111.111.00
[PE1-isis-1] quit
```

配置 LSR ID，使能 MPLS 和 LDP。

```
[PE1] mpls lsr-id 2.2.2.9
[PE1] mpls ldp
[PE1-ldp] quit
```

配置接口 Serial2/1/0，在接口上运行 IS-IS，并使能 MPLS 和 LDP。

```
[PE1] interface serial 2/1/0
[PE1-Serial2/1/0] ip address 1.1.1.2 255.0.0.0
[PE1-Serial2/1/0] isis enable 1
[PE1-Serial2/1/0] mpls enable
[PE1-Serial2/1/0] mpls ldp enable
[PE1-Serial2/1/0] quit
```

创建 Loopback0 接口，在接口上运行 IS-IS。

```
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 2.2.2.9 32
[PE1-LoopBack0] isis enable 1
[PE1-LoopBack0] quit
```

创建 VPN 实例，名称为 vpn1，为其配置 RD 和 VPN Target 属性。

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 11:11
[PE1-vpn-instance-vpn1] vpn-target 3:3 import-extcommunity
[PE1-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity
[PE1-vpn-instance-vpn1] quit
```

配置接口 GigabitEthernet2/1/1 与 VPN 实例 vpn1 绑定，并配置该接口的 IPv6 地址。

```
[PE1] interface gigabitethernet 2/1/1
[PE1-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE1-GigabitEthernet2/1/1] ipv6 address 2001::1 64
[PE1-GigabitEthernet2/1/1] quit
```

在 PE 1 上运行 BGP。

```
[PE1] bgp 100
```

配置 PE 1 向 IBGP 对等体 3.3.3.9 发布标签路由及从 3.3.3.9 接收标签路由的能力。

```
[PE1-bgp] peer 3.3.3.9 as-number 100
[PE1-bgp] peer 3.3.3.9 connect-interface loopback 0
[PE1-bgp] address-family ipv4 unicast
[PE1-bgp-ipv4] peer 3.3.3.9 enable
[PE1-bgp-ipv4] peer 3.3.3.9 label-route-capability
[PE1-bgp-ipv4] quit
```

配置 PE 1 到 EBGP 对等体 5.5.5.9 的最大跳数为 10。

```
[PE1-bgp] peer 5.5.5.9 as-number 600
[PE1-bgp] peer 5.5.5.9 connect-interface loopback 0
[PE1-bgp] peer 5.5.5.9 ebgp-max-hop 10
```

配置对等体 5.5.5.9 作为 VPNv6 对等体。

```
[PE1-bgp] address-family vpnv6
[PE1-bgp-vpnv6] peer 5.5.5.9 enable
[PE1-bgp-vpnv6] quit
```

配置 PE 1 与 CE 1 建立 EBGP 对等体，将学习到的 BGP 路由添加到 VPN 实例的路由表中。

```
[PE1-bgp] ip vpn-instance vpn1
```

```
[PE1-bgp-vpn1] peer 2001::2 as-number 65001
[PE1-bgp-vpn1] address-family ipv6 unicast
[PE1-bgp-ipv6-vpn1] peer 2001::2 enable
[PE1-bgp-ipv6-vpn1] quit
[PE1-bgp-vpn1] quit
[PE1-bgp] quit
```

(3) 配置 ASBR-PE1

在 ASBR-PE1 上运行 IS-IS。

```
<ASBR-PE1> system-view
[ASBR-PE1] isis 1
[ASBR-PE1-isis-1] network-entity 10.222.222.222.222.00
[ASBR-PE1-isis-1] quit
```

配置 LSR ID，使能 MPLS 和 LDP。

```
[ASBR-PE1] mpls lsr-id 3.3.3.9
[ASBR-PE1] mpls ldp
[ASBR-PE1-ldp] quit
```

配置接口 Serial2/1/0，在接口上运行 IS-IS，并使能 MPLS 和 LDP。

```
[ASBR-PE1] interface serial 2/1/0
[ASBR-PE1-Serial2/1/0] ip address 1.1.1.1 255.0.0.0
[ASBR-PE1-Serial2/1/0] isis enable 1
[ASBR-PE1-Serial2/1/0] mpls enable
[ASBR-PE1-Serial2/1/0] mpls ldp enable
[ASBR-PE1-Serial2/1/0] quit
```

配置接口 Serial2/1/1，并在接口上使能 MPLS。

```
[ASBR-PE1] interface serial 2/1/1
[ASBR-PE1-Serial2/1/1] ip address 11.0.0.2 255.0.0.0
[ASBR-PE1-Serial2/1/1] mpls
[ASBR-PE1-Serial2/1/1] quit
```

创建 Loopback0 接口，在接口上运行 IS-IS。

```
[ASBR-PE1] interface loopback 0
[ASBR-PE1-LoopBack0] ip address 3.3.3.9 32
[ASBR-PE1-LoopBack0] isis enable 1
[ASBR-PE1-LoopBack0] quit
```

创建路由策略。

```
[ASBR-PE1] route-policy policy1 permit node 1
[ASBR-PE1-route-policy-policy1-1] apply mpls-label
[ASBR-PE1-route-policy-policy1-1] quit
[ASBR-PE1] route-policy policy2 permit node 1
[ASBR-PE1-route-policy-policy2-1] if-match mpls-label
[ASBR-PE1-route-policy-policy2-1] apply mpls-label
[ASBR-PE1-route-policy-policy2-1] quit
```

在 ASBR-PE 1 上运行 BGP，对向 IBGP 对等体 2.2.2.9 发布的路由应用已配置的路由策略 policy2。

```
[ASBR-PE1] bgp 100
[ASBR-PE1-bgp] peer 2.2.2.9 as-number 100
[ASBR-PE1-bgp] peer 2.2.2.9 connect-interface loopback 0
[ASBR-PE1-bgp] address-family ipv4 unicast
```

```
[ASBR-PE1-bgp-ipv4] peer 2.2.2.9 enable
[ASBR-PE1-bgp-ipv4] peer 2.2.2.9 route-policy policy2 export
```
向 IBGP 对等体 2.2.2.9 发布标签路由及从 2.2.2.9 接收标签路由的能力。
```
[ASBR-PE1-bgp-ipv4] peer 2.2.2.9 label-route-capability
```
引入 IS-IS 进程 1 的路由。
```
[ASBR-PE1-bgp-ipv4] import-route isis 1
[ASBR-PE1-bgp-ipv4] quit
```
对向 EBGP 对等体 11.0.0.1 发布的路由应用已配置的路由策略 policy1。
```
[ASBR-PE1-bgp] peer 11.0.0.1 as-number 600
[ASBR-PE1-bgp] address-family ipv4 unicast
[ASBR-PE1-bgp-ipv4] peer 11.0.0.1 enable
[ASBR-PE1-bgp-ipv4] peer 11.0.0.1 route-policy policy1 export
```
向 EBGP 对等体 11.0.0.1 发布标签路由及从 11.0.0.1 接收标签路由的能力。
```
[ASBR-PE1-bgp-ipv4] peer 11.0.0.1 label-route-capability
[ASBR-PE1-bgp-ipv4] quit
[ASBR-PE1-bgp] quit
```
(4)　配置 ASBR-PE 2

在 ASBR-PE 2 上运行 IS-IS。
```
<ASBR-PE2> system-view
[ASBR-PE2] isis 1
[ASBR-PE2-isis-1] network-entity 10.333.333.333.333.00
[ASBR-PE2-isis-1] quit
```
配置 LSR ID，使能 MPLS 和 LDP。
```
[ASBR-PE2] mpls lsr-id 4.4.4.9
[ASBR-PE2] mpls ldp
[ASBR-PE2-ldp] quit
```
配置接口 Serial2/1/0，在接口上运行 IS-IS，并在接口上使能 MPLS 和 LDP。
```
[ASBR-PE2] interface serial 2/1/0
[ASBR-PE2-Serial2/1/0] ip address 9.1.1.1 255.0.0.0
[ASBR-PE2-Serial2/1/0] isis enable 1
[ASBR-PE2-Serial2/1/0] mpls enable
[ASBR-PE2-Serial2/1/0] mpls ldp enable
[ASBR-PE2-Serial2/1/0] quit
```
创建 Loopback0 接口，在接口上运行 IS-IS。
```
[ASBR-PE2] interface loopback 0
[ASBR-PE2-LoopBack0] ip address 4.4.4.9 32
[ASBR-PE2-LoopBack0] isis enable 1
[ASBR-PE2-LoopBack0] quit
```
配置接口 Serial2/1/1，在接口上使能 MPLS。
```
[ASBR-PE2] interface serial 2/1/1
[ASBR-PE2-Serial2/1/1] ip address 11.0.0.1 255.0.0.0
[ASBR-PE2-Serial2/1/1] mpls enable
[ASBR-PE2-Serial2/1/1] quit
```
创建路由策略。
```
[ASBR-PE2] route-policy policy1 permit node 1
```

```
[ASBR-PE2-route-policy-policy1-1] apply mpls-label
[ASBR-PE2-route-policy-policy1-1] quit
[ASBR-PE2] route-policy policy2 permit node 1
[ASBR-PE2-route-policy-policy2-1] if-match mpls-label
[ASBR-PE2-route-policy-policy2-1] apply mpls-label
[ASBR-PE2-route-policy-policy2-1] quit
```

在 ASBR-PE 2 上运行 BGP，向 IBGP 对等体 5.5.5.9 发布标签路由及从 5.5.5.9 接收标签路由的能力。

```
[ASBR-PE2] bgp 600
[ASBR-PE2-bgp] peer 5.5.5.9 as-number 600
[ASBR-PE2-bgp] peer 5.5.5.9 connect-interface loopback 0
[ASBR-PE2-bgp] address-family ipv4 unicast
[ASBR-PE2-bgp-ipv4] peer 5.5.5.9 enable
[ASBR-PE2-bgp-ipv4] peer 5.5.5.9 label-route-capability
```

对向 IBGP 对等体 5.5.5.9 发布的路由应用已配置的路由策略 policy2。

```
[ASBR-PE2-bgp-ipv4] peer 5.5.5.9 route-policy policy2 export
```

引入 IS-IS 进程 1 的路由。

```
[ASBR-PE2-bgp-ipv4] import-route isis 1
[ASBR-PE2-bgp-ipv4] quit
```

对向 EBGP 对等体 11.0.0.2 发布的路由应用已配置的路由策略 policy1。

```
[ASBR-PE2-bgp] peer 11.0.0.2 as-number 100
[ASBR-PE2-bgp] address-family ipv4 unicast
[ASBR-PE2-bgp-ipv4] peer 11.0.0.2 enable
[ASBR-PE2-bgp-ipv4] peer 11.0.0.2 route-policy policy1 export
```

向 EBGP 对等体 11.0.0.2 发布标签路由及从 11.0.0.2 接收标签路由的能力。

```
[ASBR-PE2-bgp-ipv4] peer 11.0.0.2 label-route-capability
[ASBR-PE2-bgp-ipv4] quit
[ASBR-PE2-bgp] quit
```

(5) 配置 PE 2

在 PE 2 上运行 IS-IS。

```
<PE2> system-view
[PE2] isis 1
[PE2-isis-1] network-entity 10.444.444.444.444.00
[PE2-isis-1] quit
```

配置 LSR ID，使能 MPLS 和 LDP。

```
[PE2] mpls lsr-id 5.5.5.9
[PE2] mpls ldp
[PE2-ldp] quit
```

配置接口 Serial2/1/0，在接口上运行 IS-IS，并使能 MPLS 和 LDP。

```
[PE2] interface serial 2/1/0
[PE2-Serial2/1/0] ip address 9.1.1.2 255.0.0.0
[PE2-Serial2/1/0] isis enable 1
[PE2-Serial2/1/0] mpls enable
[PE2-Serial2/1/0] mpls ldp enable
[PE2-Serial2/1/0] quit
```

创建 Loopback0 接口，在接口上运行 IS-IS。

```
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 5.5.5.9 32
[PE2-LoopBack0] isis enable 1
[PE2-LoopBack0] quit
```

创建 VPN 实例，名称为 vpn1，为其配置 RD 和 VPN Target 属性。

```
[PE2] ip vpn-instance vpn1
[PE2-vpn-instance-vpn1] route-distinguisher 11:11
[PE2-vpn-instance-vpn1] vpn-target 3:3 import-extcommunity
[PE2-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity
[PE2-vpn-instance-vpn1] quit
```

配置接口 GigabitEthernet2/1/1 与 VPN 实例 vpn1 绑定，并配置该接口的 IPv6 地址。

```
[PE2] interface gigabitethernet 2/1/1
[PE2-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE2-GigabitEthernet2/1/1] ipv6 address 2002::1 64
[PE2-GigabitEthernet2/1/1] quit
```

在 PE 2 上运行 BGP。

```
[PE2] bgp 600
```

配置 PE 2 向 IBGP 对等体 4.4.4.9 发布标签路由及从 4.4.4.9 接收标签路由的能力。

```
[PE2-bgp] peer 4.4.4.9 as-number 600
[PE2-bgp] peer 4.4.4.9 connect-interface loopback 0
[PE2-bgp] address-family ipv4 unicast
[PE2-bgp-ipv4] peer 4.4.4.9 enable
[PE2-bgp-ipv4] peer 4.4.4.9 label-route-capability
[PE2-bgp-ipv4] quit
```

配置 PE 2 到 EBGP 对等体 2.2.2.9 的最大跳数为 10。

```
[PE2-bgp] peer 2.2.2.9 as-number 100
[PE2-bgp] peer 2.2.2.9 connect-interface loopback 0
[PE2-bgp] peer 2.2.2.9 ebgp-max-hop 10
```

配置对等体 2.2.2.9 作为 VPNv6 对等体。

```
[PE2-bgp] address-family vpnv6
[PE2-bgp-vpnv6] peer 2.2.2.9 enable
[PE2-bgp-vpnv6] quit
```

配置 PE 2 与 CE 2 建立 EBGP 对等体，将学习到的 BGP 路由添加到 VPN 实例的路由表中。

```
[PE2-bgp] ip vpn-instance vpn1
[PE2-bgp-vpn1] peer 2002::2 as-number 65002
[PE2-bgp-vpn1] address-family ipv6 unicast
[PE2-bgp-ipv6-vpn1] peer 2002::2 enable
[PE2-bgp-ipv6-vpn1] quit
[PE2-bgp-vpn1] quit
[PE2-bgp] quit
```

(6) 配置 CE 2

配置接口 GigabitEthernet2/1/1 的 IPv6 地址。

```
<CE2> system-view
[CE2] interface gigabitethernet 2/1/1
[CE2-GigabitEthernet2/1/1] ipv6 address 2002::2 64
[CE2-GigabitEthernet2/1/1] quit
```

配置 CE 2 与 PE 2 建立 EBGP 对等体，并引入 VPN 路由。

```
[CE2] bgp 65002
[CE2-bgp] peer 2002::1 as-number 600
[CE2-bgp] address-family ipv6 unicast
[CE2-bgp-ipv6] peer 2002::1 enable
[CE2-bgp-ipv6] import-route direct
[CE2-bgp-ipv6] quit
[CE2-bgp] quit
```

4. 验证配置

配置完成后，在 CE 1 和 CE 2 上执行 **display ipv6 routing-table** 命令可以查看到到达对方的路由，且 CE 1 和 CE 2 互相可以 ping 通。

2.8.5 配置运营商的运营商示例

1. 组网需求

在 图 2-7 中：

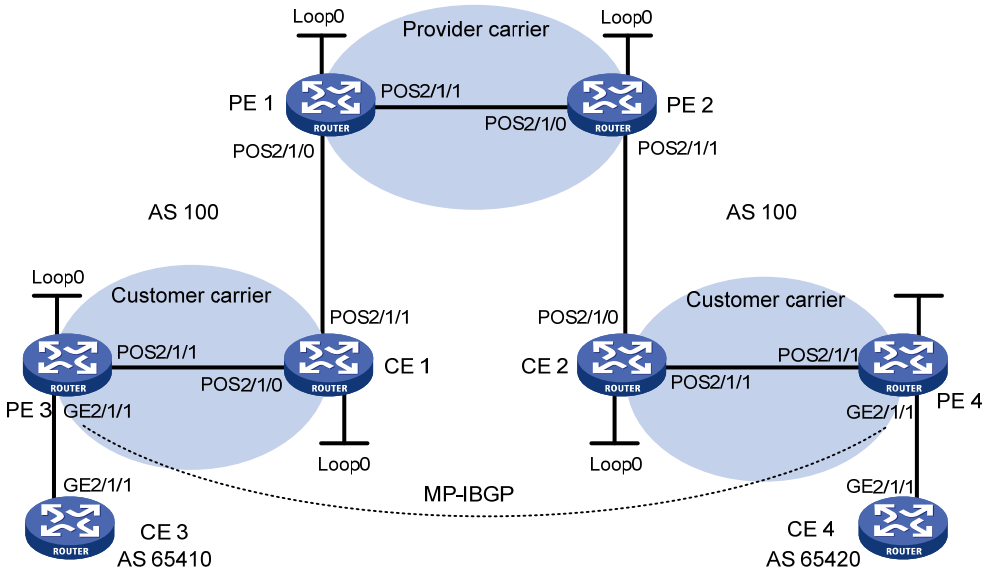
- PE 1 和 PE 2 是一级运营商骨干网的 PE 设备，为二级运营商提供 VPN 服务；
- CE 1 和 CE 2 是同一个二级运营商的设备，作为 CE 接入一级运营商的骨干网；
- PE 3 和 PE 4 是二级运营商的 PE 设备，为二级运营商的客户提供 IPv6 MPLS L3VPN 服务；
- CE 3 和 CE 4 是二级运营商的客户。

配置运营商的运营商关键在于配置两类路由的交换：

- 二级运营商 VPN 内部路由在一级运营商骨干网上的交换：一级运营商将二级运营商作为自己的 CE 接入；
- 二级运营商本身客户的 VPN 路由在二级运营商 PE 设备间的交换：需要在二级运营商 PE 设备（PE 3 和 PE 4）间建立 MP-IBGP 对等体关系。

2. 组网图

图2-7 配置 Carriers’ carriers 组网图



设备	接口	IP地址	设备	接口	IP地址

CE 3	GE2/1/1	2001:1::1/96	CE 4	GE2/1/1	2001:2::1/96
PE 3	Loop0	1.1.1.9/32	PE 4	Loop0	6.6.6.9/32
	GE2/1/1	2001:1::2/96		GE2/1/1	2001:2::2/96
	POS2/1/1	10.1.1.1/24		POS2/1/1	20.1.1.2/24
CE 1	Loop0	2.2.2.9/32	CE 2	Loop0	5.5.5.9/32
	POS2/1/0	10.1.1.2/24		POS2/1/0	21.1.1.2/24
	POS2/1/1	11.1.1.1/24		POS2/1/1	20.1.1.1/24
PE 1	Loop0	3.3.3.9/32	PE 2	Loop0	4.4.4.9/32
	POS2/1/0	11.1.1.2/24		POS2/1/0	30.1.1.2/24
	POS2/1/1	30.1.1.1/24		POS2/1/1	21.1.1.1/24

3. 配置步骤

(1) 配置一级运营商骨干网的 MPLS L3VPN，使用 IS-IS 作为骨干网的 IGP 协议，PE 1 和 PE 2 之间使能 LDP，并建立 MP-IBGP 对等体关系

配置 PE 1。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 3.3.3.9 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 3.3.3.9
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] isis 1
[PE1-isis-1] network-entity 10.0000.0000.0000.0004.00
[PE1-isis-1] quit
[PE1] interface loopback 0
[PE1-LoopBack0] isis enable 1
[PE1-LoopBack0] quit
[PE1] interface pos 2/1/1
[PE1-Pos2/1/1] ip address 30.1.1.1 24
[PE1-Pos2/1/1] isis enable 1
[PE1-Pos2/1/1] mpls enable
[PE1-Pos2/1/1] mpls ldp enable
[PE1-Pos2/1/1] mpls ldp transport-address interface
[PE1-Pos2/1/1] quit
[PE1] bgp 100
[PE1-bgp] peer 4.4.4.9 as-number 100
[PE1-bgp] peer 4.4.4.9 connect-interface loopback 0
[PE1-bgp] address-family vpnv4
[PE1-bgp-vpnv4] peer 4.4.4.9 enable
[PE1-bgp-vpnv4] quit
[PE1-bgp] quit
```

PE 2 的配置与 PE 1 类似，配置过程省略。

配置完成后，在 PE 1 或 PE 2 上执行 **display mpls ldp peer** 命令可以看到 LDP 会话建立成功；执行 **display bgp peer vpnv4** 命令可以看到 BGP 对等体关系已建立，并达到 Established 状态；执行 **display isis peer** 命令可以看到 IS-IS 邻居关系已建立，状态为 up。

以 PE 1 为例：

```
[PE1] display mpls ldp peer
```

```
Total number of peers: 1
Peer LDP ID        State         LAM  Role     GR   MD5  KA Sent/Rcvd
4.4.4.9:0          Operational   DU   Active   Off  Off  8/8
[PE1] display bgp peer vpnv4

 BGP local router ID: 3.3.3.9
 Local AS number: 100
 Total number of peers: 1                 Peers in established state: 1

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  4.4.4.9                100        3        6    0       0 00:00:32 Established
[PE1] display isis peer
                         Peer information for ISIS(1)
                          ---------------------------

 System Id: 0000.0000.0005
 Interface: POS2/1/1               Circuit Id: 0000.0000.0005.02
 State: Up     HoldTime:   8s      Type: L1(L1L2)     PRI: 64

 System Id: 0000.0000.0005
 Interface: POS2/1/1               Circuit Id: 0000.0000.0005.02
 State: Up     HoldTime:   8s      Type: L2(L1L2)     PRI: 64
```

(2) 配置二级运营商网络：使用 IS-IS 作为 IGP 协议，PE 3 和 CE 1、PE 4 和 CE 2 之间分别使能 LDP

配置 PE 3。

```
<PE3> system-view
[PE3] interface loopback 0
[PE3-LoopBack0] ip address 1.1.1.9 32
[PE3-LoopBack0] quit
[PE3] mpls lsr-id 1.1.1.9
[PE3] mpls ldp
[PE3-ldp] quit
[PE3] isis 2
[PE3-isis-2] network-entity 10.0000.0000.0000.0001.00
[PE3-isis-2] quit
[PE3] interface loopback 0
[PE3-LoopBack0] isis enable 2
[PE3-LoopBack0] quit
[PE3] interface pos 2/1/1
[PE3-Pos2/1/1] ip address 10.1.1.1 24
[PE3-Pos2/1/1] isis enable 2
[PE3-Pos2/1/1] mpls enable
[PE3-Pos2/1/1] mpls ldp enable
[PE3-Pos2/1/1] mpls ldp transport-address interface
[PE3-Pos2/1/1] quit
```

配置 CE 1。

```
<CE1> system-view
[CE1] interface loopback 0
[CE1-LoopBack0] ip address 2.2.2.9 32
[CE1-LoopBack0] quit
[CE1] mpls lsr-id 2.2.2.9
[CE1] mpls ldp
[CE1-ldp] quit
[CE1] isis 2
[CE1-isis-2] network-entity 10.0000.0000.0000.0002.00
[CE1-isis-2] quit
[CE1] interface loopback 0
[CE1-LoopBack0] isis enable 2
[CE1-LoopBack0] quit
[CE1] interface pos 2/1/0
[CE1-Pos2/1/0] ip address 10.1.1.2 24
[CE1-Pos2/1/0] isis enable 2
[CE1-Pos2/1/0] mpls enable
[CE1-Pos2/1/0] mpls ldp enable
[CE1-Pos2/1/0] mpls ldp transport-address interface
[CE1-Pos2/1/0] quit
```

配置完成后，PE 3 和 CE 1 之间应能建立 LDP 和 IS-IS 邻居关系。

PE 4 和 CE 2 之间的配置与 PE 3 和 CE 1 之间的配置类似，配置过程省略。

(3) 配置二级运营商 CE 接入到一级运营商的 PE

配置 PE 1。

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 200:1
[PE1-vpn-instance-vpn1] vpn-target 1:1
[PE1-vpn-instance-vpn1] quit
[PE1] mpls ldp
[PE1-ldp] vpn-instance vpn1
[PE1-ldp-vpn-instance-vpn1] quit
[PE1-ldp] quit
[PE1] isis 2 vpn-instance vpn1
[PE1-isis-2] network-entity 10.0000.0000.0000.0003.00
[PE1-isis-2] import-route bgp allow-ibgp
[PE1-isis-2] quit
[PE1] interface pos 2/1/0
[PE1-Pos2/1/0] ip binding vpn-instance vpn1
[PE1-Pos2/1/0] ip address 11.1.1.2 24
[PE1-Pos2/1/0] isis enable 2
[PE1-Pos2/1/0] mpls enable
[PE1-Pos2/1/0] mpls ldp enable
[PE1-Pos2/1/0] mpls ldp transport-address interface
[PE1-Pos2/1/0] quit
[PE1] bgp 100
[PE1-bgp] ip vpn-instance vpn1
[PE1-bgp-vpn1] address-family ipv4 unicast
```

```
[PE1-bgp-ipv4-vpn1] import isis 2
[PE1-bgp-ipv4-vpn1] quit
[PE1-bgp-vpn1] quit
[PE1-bgp] quit
```

配置 CE1。

```
[CE1] interface pos 2/1/1
[CE1-Pos2/1/1] ip address 11.1.1.1 24
[CE1-Pos2/1/1] isis enable 2
[CE1-Pos2/1/1] mpls enable
[CE1-Pos2/1/1] mpls ldp enable
[CE1-Pos2/1/1] mpls ldp transport-address interface
[CE1-Pos2/1/1] quit
```

配置完成后，PE 1 和 CE 1 之间应能建立 LDP 和 IS-IS 邻居关系。

PE 2 和 CE 2 之间的配置与 PE 1 和 CE 1 之间的配置类似，配置过程省略。

(4) 配置二级运营商的客户接入 PE

配置 CE 3。

```
<CE3> system-view
[CE3] interface gigabitethernet 2/1/1
[CE3-GigabitEthernet2/1/1] ipv6 address 2001:1::1 96
[CE3-GigabitEthernet2/1/1] quit
[CE3] bgp 65410
[CE3-bgp] peer 2001:1::2 as-number 100
[CE3-bgp] address-family ipv6
[CE3-bgp-ipv6] peer 2001:1::2 enable
[CE3-bgp-ipv6] import-route direct
[CE3-bgp-ipv6] quit
[CE3-bgp] quit
```

配置 PE 3。

```
[PE3] ip vpn-instance vpn1
[PE3-vpn-instance-vpn1] route-distinguisher 100:1
[PE3-vpn-instance-vpn1] vpn-target 1:1
[PE3-vpn-instance-vpn1] quit
[PE3] interface gigabitethernet 2/1/1
[PE3-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
[PE3-GigabitEthernet2/1/1] ipv6 address 2001:1::2 96
[PE3-GigabitEthernet2/1/1] quit
[PE3] bgp 100
[PE3-bgp] ip vpn-instance vpn1
[PE3-bgp-vpn1] peer 2001:1::1 as-number 65410
[PE3-bgp-vpn1] address-family ipv6 unicast
[PE3-bgp-ipv6-vpn1] peer 2001:1::1 enable
[PE3-bgp-ipv6-vpn1] import-route direct
[PE3-bgp-ipv6-vpn1] quit
[PE3-bgp-vpn1] quit
[PE3-bgp] quit
```

PE 4 和 CE 4 之间的配置与 PE 3 和 CE 3 之间的配置类似，配置过程省略。

(5) 在二级运营商的 PE 之间建立 MP-IBGP 对等体关系，交换二级运营商的客户的 VPN 路由

配置 PE 3。

```
[PE3] bgp 100
[PE3-bgp] peer 6.6.6.9 as-number 100
[PE3-bgp] peer 6.6.6.9 connect-interface loopback 0
[PE3-bgp] address-family vpnv6
[PE3-bgp-vpnv6] peer 6.6.6.9 enable
[PE3-bgp-vpnv6] quit
[PE3-bgp] quit
```

PE 4 的配置与 PE 3 类似，配置过程省略。

4. 验证配置

在 PE 1 和 PE 2 上执行 **display ip routing-table** 命令，可以看到 PE 1 和 PE 2 的公网路由表中只有一级运营商网络的路由。以 PE 1 为例：

```
[PE1] display ip routing-table
Routing Tables: Public
         Destinations : 7        Routes : 7
Destination/Mask    Proto  Pre  Cost      NextHop         Interface
3.3.3.9/32          Direct 0    0         127.0.0.1       InLoop0
4.4.4.9/32          ISIS   15   10        30.1.1.2        POS2/1/1
30.1.1.0/24         Direct 0    0         30.1.1.1        POS2/1/1
30.1.1.1/32         Direct 0    0         127.0.0.1       InLoop0
30.1.1.2/32         Direct 0    0         30.1.1.2        POS2/1/1
127.0.0.0/8         Direct 0    0         127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0         127.0.0.1       InLoop0
```

在 PE 1 和 PE 2 上执行 **display ip routing-table vpn-instance** 命令，可以看到 VPN 路由表中有二级运营商网络的内部路由。以 PE 1 为例：

```
[PE1] display ip routing-table vpn-instance vpn1
Routing Tables: vpn1
         Destinations : 11        Routes : 11
Destination/Mask    Proto  Pre  Cost      NextHop         Interface
1.1.1.9/32          ISIS   15   20        11.1.1.1        POS2/1/0
2.2.2.9/32          ISIS   15   10        11.1.1.1        POS2/1/0
5.5.5.9/32          BGP    255  0         4.4.4.9         NULL0
6.6.6.9/32          BGP    255  0         4.4.4.9         NULL0
10.1.1.0/24         ISIS   15   20        11.1.1.1        POS2/1/0
11.1.1.0/24         Direct 0    0         11.1.1.1        POS2/1/0
11.1.1.1/32         Direct 0    0         127.0.0.1       InLoop0
11.1.1.2/32         Direct 0    0         11.1.1.2        POS2/1/0
20.1.1.0/24         BGP    255  0         4.4.4.9         NULL0
21.1.1.0/24         BGP    255  0         4.4.4.9         NULL0
21.1.1.2/32         BGP    255  0         4.4.4.9         NULL0
```

在 CE 1 和 CE 2 上执行 **display ip routing-table** 命令，可以看到公网路由表中有二级运营商网络的内部路由。以 CE 1 为例：

```
[CE1] display ip routing-table
Routing Tables: Public
         Destinations : 16       Routes : 16
```

```
Destination/Mask    Proto  Pre  Cost   NextHop         Interface
1.1.1.9/32          ISIS   15   10     10.1.1.2        POS2/1/0
2.2.2.9/32          Direct 0    0      127.0.0.1       InLoop0
5.5.5.9/32          ISIS   15   74     11.1.1.2        POS2/1/1
6.6.6.9/32          ISIS   15   74     11.1.1.2        POS2/1/1
10.1.1.0/24         Direct 0    0      10.1.1.2        POS2/1/0
10.1.1.1/32         Direct 0    0      10.1.1.1        POS2/1/0
10.1.1.2/32         Direct 0    0      127.0.0.1       InLoop0
11.1.1.0/24         Direct 0    0      11.1.1.1        POS2/1/1
11.1.1.1/32         Direct 0    0      127.0.0.1       InLoop0
11.1.1.2/32         Direct 0    0      11.1.1.2        POS2/1/1
20.1.1.0/24         ISIS   15   74     11.1.1.2        POS2/1/1
21.1.1.0/24         ISIS   15   74     11.1.1.2        POS2/1/1
21.1.1.2/32         ISIS   15   74     11.1.1.2        POS2/1/1
127.0.0.0/8         Direct 0    0      127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0      127.0.0.1       InLoop0
```

在 PE 3 和 PE 4 上执行 **display ip routing-table** 命令，可以看到公网路由表中有二级运营商网络的内部路由。以 PE 3 为例：

```
[PE3] display ip routing-table
Routing Tables: Public
         Destinations : 11       Routes : 11
Destination/Mask    Proto  Pre  Cost   NextHop         Interface
1.1.1.9/32          Direct 0    0      127.0.0.1       InLoop0
2.2.2.9/32          ISIS   15   10     10.1.1.2        POS2/1/1
5.5.5.9/32          ISIS   15   84     10.1.1.2        POS2/1/1
6.6.6.9/32          ISIS   15   84     10.1.1.2        POS2/1/1
10.1.1.0/24         Direct 0    0      10.1.1.1        POS2/1/1
10.1.1.1/32         Direct 0    0      127.0.0.1       InLoop0
10.1.1.2/32         Direct 0    0      10.1.1.2        POS2/1/1
11.1.1.0/24         ISIS   15   20     10.1.1.2        POS2/1/1
20.1.1.0/24         ISIS   15   84     10.1.1.2        POS2/1/1
21.1.1.0/24         ISIS   15   84     10.1.1.2        POS2/1/1
21.1.1.2/32         ISIS   15   84     10.1.1.2        POS2/1/1
127.0.0.0/8         Direct 0    0      127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0      127.0.0.1       InLoop0
```

在 PE 3 和 PE 4 上执行 **display ipv6 routing-table vpn-instance** 命令，可以看到 VPN 路由表中有对端 VPN 客户的路由。以 PE 3 为例：

```
[PE3] display ipv6 routing-table vpn-instance vpn1

Destinations : 6 Routes : 6

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: 2001:1::/96                            Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : GE2/1/1                                Cost      : 0
```

```
Destination: 2001:1::2/128                              Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 2001:2::/96                                Protocol  : BGP4+
NextHop    : ::FFFF:606:609                             Preference: 0
Interface  : NULL0                                      Cost      : 0

Destination: FE80::/10                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0

Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0
```

PE 3 和 PE 4 可以相互 Ping 通。

CE 3 和 CE 4 可以互相 Ping 通。

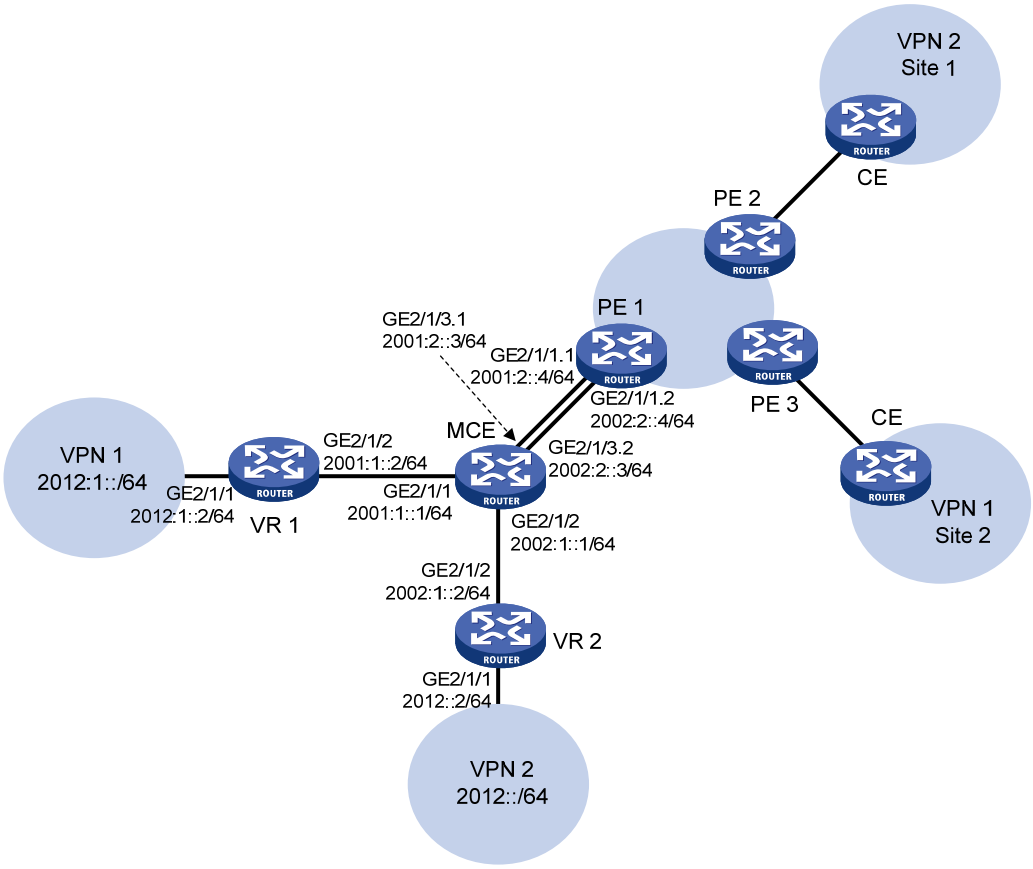
2.8.6 配置IPv6 MCE示例

1. 组网需求

MCE 设备连接两个 VPN：VPN 1 和 VPN 2，VPN 2 内运行 RIPng 路由协议。MCE 设备将两个 VPN 之间的路由隔离，并通过 OSPFv3 将各 VPN 的路由发布到 PE 1。

2. 组网图

图2-8 配置 IPv6 MCE 组网图



3. 配置步骤

为区分设备，假设 MCE 系统名为“MCE”，VPN 1 和 VPN 2 的边缘设备分别名为“VR1”和“VR2”，PE 1 系统名为 “PE1”。

(1) 在 MCE 和 PE 1 上配置 VPN 实例

在 MCE 设备上配置 VPN 实例，名称分别为 vpn1 和 vpn2，RD 分别取值为 10:1 和 20:1，VPN Target 取值与 RD 取相同数值，Export 和 Import 均取此值。

```
<MCE> system-view
[MCE] ip vpn-instance vpn1
[MCE-vpn-instance-vpn1] route-distinguisher 10:1
[MCE-vpn-instance-vpn1] vpn-target 10:1
[MCE-vpn-instance-vpn1] quit
[MCE] ip vpn-instance vpn2
[MCE-vpn-instance-vpn2] route-distinguisher 20:1
[MCE-vpn-instance-vpn2] vpn-target 20:1
[MCE-vpn-instance-vpn2] quit
```

配置接口 GigabitEthernet2/1/1 与 VPN 实例 vpn1 绑定，并配置该接口的 IPv6 地址。

```
[MCE] interface gigabitethernet 2/1/1
[MCE-GigabitEthernet2/1/1] ip binding vpn-instance vpn1
```

```
[MCE-GigabitEthernet2/1/1] ipv6 address 2001:1::1 64
[MCE-GigabitEthernet2/1/1] quit
```

配置接口 GigabitEthernet2/1/2 与 VPN 实例 vpn2 绑定，并配置该接口的 IPv6 地址。

```
[MCE] interface gigabitethernet 2/1/2
[MCE-GigabitEthernet2/1/2] ip binding vpn-instance vpn2
[MCE-GigabitEthernet2/1/2] ipv6 address 2002:1::1 64
[MCE-GigabitEthernet2/1/2] quit
```

在 PE 1 上配置 VPN 实例，名称分别为 vpn1 和 vpn2，RD 分别取值为 30:1 和 40:1，VPN Target 取值分别为 10:1 和 20:1，Export 和 Import 均取此值。

```
<PE1> system-view
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 30:1
[PE1-vpn-instance-vpn1] vpn-target 10:1
[PE1-vpn-instance-vpn1] quit
[PE1] ip vpn-instance vpn2
[PE1-vpn-instance-vpn2] route-distinguisher 40:1
[PE1-vpn-instance-vpn2] vpn-target 20:1
[PE1-vpn-instance-vpn2] quit
```

(2) MCE 与 Site 间路由配置

MCE 与 VPN 1 直接相连，且 VPN 1 内未使用路由协议，因此可以使用 IPv6 静态路由进行配置。

配置 VR1 与 MCE 连接的接口地址为 2001:1::2/64，连接 VPN 1 接口的地址为 2012:1::2/64。（具体配置过程略）

在 VR1 上配置缺省路由，指定出方向报文的下一跳地址为 2001:1::1。

```
<VR1> system-view
[VR1] ipv6 route-static :: 0 2001:1::1
```

在 MCE 上指定 IPv6 静态路由，去往 2012:1::/64 网段的报文，下一跳地址为 2001:1::2，并将此路由与 VPN 实例 vpn1 绑定。

```
[MCE] ipv6 route-static vpn-instance vpn1 2012:1:: 64 2001:1::2
```

VPN 2 内运行 RIPng，在 MCE 上配置 RIPng 进程 20，并与 VPN 实例 vpn2 绑定，以便将 VPN 2 内的路由学习到 vpn2 实例的路由表中。

```
[MCE] ripng 20 vpn-instance vpn2
```

配置 RIPng 发布 2002:1::/64 网段路由。

```
[MCE] interface gigabitethernet 2/1/2
[MCE-GigabitEthernet2/1/2] ripng 20 enable
[MCE-GigabitEthernet2/1/2] quit
```

在 VR 2 上，配置与 MCE 连接的接口地址为 2002:1::2/64。（具体配置过程略）

在 VR 2 上配置 RIPng 发布 2012::/64 和 2002:1::/64 网段路由。

```
<VR2> system-view
[VR2] ripng 20
[VR2-ripng-20] quit
[VR2] interface gigabitethernet 2/1/1
[VR2-GigabitEthernet2/1/1] ripng 20 enable
[VR2-GigabitEthernet2/1/1] quit
[VR2] interface gigabitethernet 2/1/2
[VR2-GigabitEthernet2/1/2] ripng 20 enable
```

```
[VR2-GigabitEthernet2/1/2] quit
```
在 MCE 上查看 VPN 实例 vpn1 和 vpn2 的路由信息。
```
[MCE] display ipv6 routing-table vpn-instance vpn1

Destinations : 6 Routes : 6

Destination: ::1/128                                    Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 2001:1::/64                                Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : GE2/1/1                                    Cost      : 0

Destination: 2001:1::1/128                              Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 2012:1::/64                                Protocol  : Static
NextHop    : 2001:1::2                                  Preference: 60
Interface  : GE2/1/1                                    Cost      : 0

Destination: FE80::/10                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0

Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0
[MCE] display ipv6 routing-table vpn-instance vpn2

Destinations : 6 Routes : 6

Destination: ::1/128                                    Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 2002:1::/64                                Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : GE2/1/2                                    Cost      : 0

Destination: 2002:1::1/128                              Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 2012::/64                                  Protocol  : RIPng
NextHop    : FE80::20C:29FF:FE40:701                    Preference: 100
Interface  : GE2/1/2                                    Cost      : 1
```

```
Destination: FE80::/10                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0

Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0
```

可以看到，MCE 已经通过 RIPng 学习到了 VPN 2 内的私网路由，并与 VPN 1 内的路由信息分别维护在两个路由表内，有效地进行了隔离。

(3) MCE 与 PE 间路由配置

MCE 通过子接口与 PE 1 相连。在 MCE 上配置子接口 GigabitEthernet2/1/3.1 与 VPN 实例 vpn1 绑定，配置该子接口终结 VLAN 10，并配置该接口的 IPv6 地址。

```
[MCE] interface gigabitethernet 2/1/3.1
[MCE-GigabitEthernet2/1/3.1] ip binding vpn-instance vpn1
[MCE-GigabitEthernet2/1/3.1] vlan-type dot1q vid 10
[MCE-GigabitEthernet2/1/3.1] ipv6 address 2001:2::3 64
[MCE-GigabitEthernet2/1/3.1] quit
```

在 MCE 上配置子接口 GigabitEthernet2/1/3.2 与 VPN 实例 vpn2 绑定，配置该子接口终结 VLAN 20，并配置该接口的 IPv6 地址。

```
[MCE] interface gigabitethernet 2/1/3.2
[MCE-GigabitEthernet2/1/3.2] ip binding vpn-instance vpn2
[MCE-GigabitEthernet2/1/3.2] vlan-type dot1q vid 20
[MCE-GigabitEthernet2/1/3.2] ipv6 address 2002:2::3 64
[MCE-GigabitEthernet2/1/3.2] quit
```

在 PE 1 配置子接口 GigabitEthernet2/1/1.1 与 VPN 实例 vpn1 绑定，配置该子接口终结 VLAN 10，并配置该接口的 IPv6 地址。

```
[PE1] interface gigabitethernet 2/1/1.1
[PE1-GigabitEthernet2/1/1.1] ip binding vpn-instance vpn1
[PE1-GigabitEthernet2/1/1.1] vlan-type dot1q vid 10
[PE1-GigabitEthernet2/1/1.1] ipv6 address 2001:2::4 64
[PE1-GigabitEthernet2/1/1.1] quit
```

在 PE 1 上配置子接口 GigabitEthernet2/1/1.2 与 VPN 实例 vpn2 绑定，配置该子接口终结 VLAN 20，并配置该接口的 IPv6 地址。

```
[PE1] interface gigabitethernet 2/1/1.2
[PE1-GigabitEthernet2/1/1.2] ip binding vpn-instance vpn2
[PE1-GigabitEthernet2/1/1.2] vlan-type dot1q vid 20
[PE1-GigabitEthernet2/1/1.2] ipv6 address 2002:2::4 64
[PE1-GigabitEthernet2/1/1.2] quit
```

配置 MCE 和 PE 1 的 Loopback0 接口，用于指定 MCE 和 PE 1 的 Router ID，地址分别为 101.101.10.1 和 100.100.10.1。配置步骤这里省略。

配置 MCE 启动 OSPFv3 进程 10，绑定到 VPN 实例 vpn1，并引入 VPN 1 的 IPv6 静态路由。

```
[MCE] ospfv3 10 vpn-instance vpn1
[MCE-ospf-10] router-id 101.101.10.1
[MCE-ospf-10] import-route static
```

```
[MCE-ospf-10] quit
```

在子接口 GigabitEthernet2/1/3.1 上使能 OSPFv3。

```
[MCE] interface gigabitethernet 2/1/3.1
[MCE-GigabitEthernet2/1/3.1] ospfv3 10 area 0.0.0.0
[MCE-GigabitEthernet2/1/3.1] quit
```

配置 PE 1 启动 OSPFv3 进程 10，绑定到 VPN 实例 vpn1。

```
[PE1] ospfv3 10 vpn-instance vpn1
[PE1-ospf-10] router-id 100.100.10.1
[PE1-ospf-10] quit
```

在子接口 GigabitEthernet2/1/1.1 上使能 OSPFv3。

```
[PE1] interface gigabitethernet 2/1/1.1
[PE1-GigabitEthernet2/1/1.1] ospfv3 10 area 0.0.0.0
[PE1-GigabitEthernet2/1/1.1] quit
```

MCE 与 PE 1 间配置 OSPFv3 进程 20，引入 VPN 实例 vpn2 的路由信息的过程与上面介绍的配置基本一致，不同的是在 MCE 的 OSPFv3 中配置引入的是 RIPng 进程 20 的路由，这里不再赘述。

4. 验证配置

显示 PE 1 上 VPN 实例 vpn1 的路由信息。可以看到，PE 1 通过 OSPFv3 学习到了 VPN 1 内的私网路由。

```
[PE1] display ipv6 routing-table vpn-instance vpn1

Destinations : 6 Routes : 6

Destination: ::1/128                                    Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 2001:2::/64                                Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : GE2/1/1.1                                  Cost      : 0

Destination: 2001:2::4/128                              Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 2012:1::/64                                Protocol  : OSPFv3
NextHop    : FE80::200:5EFF:FE01:1C05                   Preference: 15
Interface  : GE2/1/1.1                                  Cost      : 10

Destination: FE80::/10                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0

Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0
```

通过下面的显示信息可以看出，PE 1 通过 OSPFv3 学习到了 VPN 2 内的私网路由。

```
[PE1] display ipv6 routing-table vpn-instance vpn2

Destinations : 6 Routes : 6

Destination: ::1/128                                    Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 2002:2::/64                                Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : GE2/1/1.2                                  Cost      : 0

Destination: 2002:2::4/128                              Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 2012::/64                                  Protocol  : OSPFv3
NextHop    : FE80::200:5EFF:FE01:1C06                   Preference: 15
Interface  : GE2/1/1.2                                  Cost      : 10

Destination: FE80::/10                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0

Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0
```

至此，通过配置，已经将两个 VPN 实例内的路由信息完整地传播到 PE 1 中，配置完成。

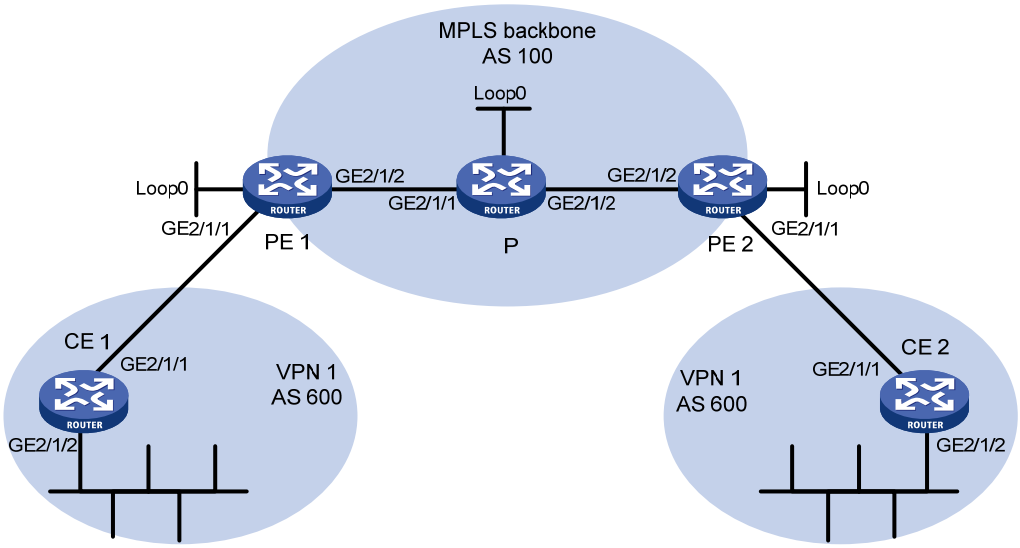
2.8.7 配置BGP的AS号替换

1. 组网需求

CE 1 和 CE 2 同属于 VPN 1，分别接入 PE 1 和 PE 2，并且 CE 1 和 CE 2 复用 AS 号 600。

2. 组网图

图2-9 BGP 的 AS 号替换组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	GE2/1/1	10:1::2/96	P	Loop0	2.2.2.9/32
	GE2/1/2	100::1/96		GE2/1/1	20.1.1.2/24
PE 1	Loop0	10.1.1.1/32		GE2/1/2	30.1.1.1/24
	GE2/1/1	10:1::1/96	PE 2	Loop0	10.1.1.2/32
	GE2/1/2	20.1.1.1/24		GE2/1/1	10:2::1/96
CE 2	GE2/1/1	10:2::2/96		GE2/1/2	30.1.1.2/24
	GE2/1/2	200::1/96			

3. 配置步骤

(1) 配置基本 IPv6 MPLS L3VPN

- 在 MPLS 骨干网上配置 OSPF，PE 和 P 之间能够学到对方 Loopback 接口的路由；
- 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP；
- PE 之间建立 MP-IBGP 对等体关系，交换 VPNv6 路由；
- 在 PE 1 上配置 VPN 1 的 VPN 实例，接入 CE 1；
- 在 PE 2 上配置 VPN 1 的 VPN 实例，接入 CE 2；
- PE 1 和 CE 1、PE 2 和 CE 2 之间配置 BGP，将 CE 的路由引入 PE。

上述配置可参考“2.8.1 配置IPv6 MPLS L3VPN示例”，具体配置过程略。

完成上述配置后，在 CE 2 上执行 **display ipv6 routing-table** 命令，可以看到没有到达 CE 1 内部 VPN（100::/96）的路由。CE 1 上也存在同样的现象。

```
<CE2> display ipv6 routing-table

Destinations : 6 Routes : 6

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: 10:2::/96                              Protocol  : Direct
```

```
NextHop    : ::                                    Preference: 0
Interface  : GE2/1/1                               Cost      : 0

Destination: 10:2::2/128                           Protocol  : Direct
NextHop    : ::1                                   Preference: 0
Interface  : InLoop0                               Cost      : 0

Destination: 200::/96                              Protocol  : Static
NextHop    : ::                                    Preference: 60
Interface  : NULL0                                 Cost      : 0

Destination: FE80::/10                             Protocol  : Direct
NextHop    : ::                                    Preference: 0
Interface  : NULL0                                 Cost      : 0

Destination: FF00::/8                              Protocol  : Direct
NextHop    : ::                                    Preference: 0
Interface  : NULL0                                 Cost      : 0
```

在 PE 上执行 **display ipv6 routing-table vpn-instance** 命令，可以看到 PE 的 VPN 实例中有到达对端 CE 内部 VPN 的路由。以 PE 2 为例：

```
<PE2> display ipv6 routing-table vpn-instance vpn1

Destinations : 7 Routes : 7

Destination: ::1/128                               Protocol  : Direct
NextHop    : ::1                                   Preference: 0
Interface  : InLoop0                               Cost      : 0

Destination: 10:2::/96                             Protocol  : Direct
NextHop    : ::                                    Preference: 0
Interface  : GE2/1/1                               Cost      : 0

Destination: 10:2::1/128                           Protocol  : Direct
NextHop    : ::1                                   Preference: 0
Interface  : InLoop0                               Cost      : 0

Destination: 100::/96                              Protocol  : BGP4+
NextHop    : ::FFFF:10.1.1.1                       Preference: 255
Interface  : GE2/1/2                               Cost      : 0

Destination: 200::/96                              Protocol  : BGP4+
NextHop    : 10:2::2                               Preference: 255
Interface  : GE2/1/1                               Cost      : 0

Destination: FE80::/10                             Protocol  : Direct
NextHop    : ::                                    Preference: 0
Interface  : NULL0                                 Cost      : 0
```

```
Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0
```

在 PE 2 上打开 BGP 的 Update 报文调试信息开关，可以看到 PE 2 发布了去往 100::/96 的路由，AS 路径信息为“100 600”。

```
<PE2> terminal monitor
<PE2> terminal logging level 7
<PE2> debugging bgp update vpn-instance vpn1 10:2::2 ipv6
<PE2> refresh bgp all export ipv6 vpn-instance vpn1
*Jun 13 16:12:52:096 2012 PE2 BGP/7/DEBUG;
         BGP_IPV6.vpn1: Send UPDATE to update-group 0 for following destinations:
         Origin       : Incomplete
         AS path      : 100 600
         Next hop     : ::FFFF:10.1.1.1
         100::/96,


*Jun 27 23:59:30:085 2013 H3C BGP/7/DEBUG;
 BGP.vpn1: Send UPDATE MSG to peer 10:2::2(IPv6-UNC) NextHop: 10:2::1.
```

在 CE 2 上执行 **display bgp routing-table ipv6 peer received-routes** 命令，可以看到 CE 2 没有接收 100::/96 的路由。

```
<CE2> display bgp routing-table ipv6 peer 10:2::1 received-routes

 Total number of routes: 0
```

(2)　配置 BGP 的 AS 号替换功能

在 PE 1 上配置 BGP 的 AS 号替换功能。

```
<PE1> system-view
[PE1] bgp 100
[PE1-bgp] ip vpn-instance vpn1
[PE1-bgp-vpn1] peer 10:1::2 substitute-as
[PE1-bgp-vpn1] quit
[PE1-bgp] quit
```

在 PE 2 上配置 BGP 的 AS 号替换功能。

```
<PE2> system-view
[PE2] bgp 100
[PE2-bgp] ip vpn-instance vpn1
[PE2-bgp-vpn1] peer 10:2::2 substitute-as
[PE2-bgp-vpn1] quit
[PE2-bgp] quit
```

4. 验证配置

可以看到 PE 2 向 CE 2 发布的路由中，100::/96 的 AS 路径信息由“100 600”变为“100 100”。

```
*Jun 27 18:07:34:420 2013 PE2 BGP/7/DEBUG;
         BGP_IPV6.vpn1: Send UPDATE to peer 10:2::2 for following destinations:
         Origin       : Incomplete
```

```
        AS path       : 100 100
        Next hop      : 10:2::1
        100::/96,
```

再次查看 CE 2 接收的路由信息和路由表，可以看到 CE 2 学习到了路由 100::/96。

```
<CE2> display bgp routing-table ipv6 peer 10:2::1 received-routes

 Total number of routes: 1

 BGP local router ID is 12.1.1.3
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

* >e Network : 100::                                    PrefixLen : 96
     NextHop : 10:2::1                                 LocPrf    :
     PrefVal : 0                                       OutLabel  : NULL
     MED     :
     Path/Ogn: 100 100?

<CE2> display ipv6 routing-table

Destinations : 7 Routes : 7

Destination: ::1/128                                   Protocol  : Direct
NextHop    : ::1                                       Preference: 0
Interface  : InLoop0                                   Cost      : 0

Destination: 10:2::/96                                 Protocol  : Direct
NextHop    : ::                                        Preference: 0
Interface  : GE2/1/1                                   Cost      : 0

Destination: 10:2::2/128                               Protocol  : Direct
NextHop    : ::1                                       Preference: 0
Interface  : InLoop0                                   Cost      : 0

Destination: 100::/96                                  Protocol  : BGP4+
NextHop    : 10:2::1                                   Preference: 255
Interface  : GE2/1/1                                   Cost      : 0

Destination: 200::/96                                  Protocol  : Static
NextHop    : ::                                        Preference: 60
Interface  : NULL0                                     Cost      : 0

Destination: FE80::/10                                 Protocol  : Direct
NextHop    : ::                                        Preference: 0
Interface  : NULL0                                     Cost      : 0

Destination: FF00::/8                                  Protocol  : Direct
```

```
NextHop    : ::                                    Preference: 0
Interface  : NULL0                                 Cost      : 0
```

CE 1 和 CE 2 的 GigabitEthernet2/1/2 接口地址之间能够相互 Ping 通。

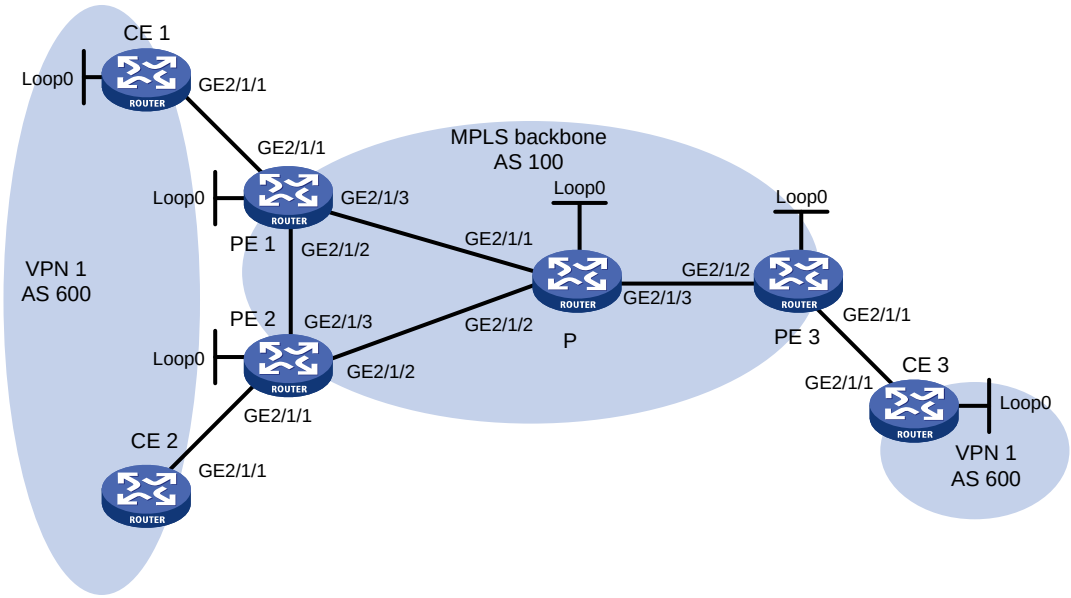
2.8.8 配置BGP的AS号替换和SoO属性

1. 组网需求

- CE 1、CE 2 和 CE 3 同属于 VPN 1，分别接入 PE 1、PE 2 和 PE 3。
- CE 1 和 CE 2 位于同一个站点。
- CE 1、CE 2 和 CE 3 复用 AS 号 600。
- 为了避免路由丢失，在 PE 上配置 AS 号替换；为了避免路由在 CE 1 和 CE 2 之间产生环路，在 PE 1 和 PE 2 上分别为 CE 1 和 CE 2 配置相同的 SoO 属性。

2. 组网图

图2-10 BGP 的 AS 号替换和 SoO 属性组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	Loop0	100::1/96	CE 3	Loop0	200::1/96
	GE2/1/1	10:1::1/96		GE2/1/1	10:3::1/96
CE 2	GE2/1/1	10:2::1/96	PE 2	Loop0	2.2.2.9/32
PE 1	Loop0	1.1.1.9/32		GE2/1/1	10:2::2/96
	GE2/1/1	10:1::2/96		GE2/1/2	40.1.1.1/24
	GE2/1/2	20.1.1.1/24		GE2/1/3	20.1.1.2/24
	GE2/1/3	30.1.1.1/24	P	Loop0	3.3.3.9/32
PE 3	Loop0	4.4.4.9/32		GE2/1/1	30.1.1.2/24
	GE2/1/1	10:3::2/96		GE2/1/2	40.1.1.2/24
	GE2/1/2	50.1.1.2/24		GE2/1/3	50.1.1.1/24

3. 配置步骤

(1) 配置基本 IPv6 MPLS L3VPN

- 在 MPLS 骨干网上配置 OSPF，PE 和 P 之间能够学到对方 Loopback 接口的路由；

- 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP；
- PE 之间建立 MP-IBGP 对等体关系，发布 VPNv6 路由；
- 在 PE 1 上配置 VPN 1 的 VPN 实例，接入 CE 1；
- 在 PE 2 上配置 VPN 1 的 VPN 实例，接入 CE 2；
- 在 PE 3 上配置 VPN 1 的 VPN 实例，接入 CE 3；
- PE 1 和 CE 1、PE 2 和 CE 2、PE 3 和 CE 3 之间配置 BGP，将 CE 的路由引入 PE。

上述配置可参考“2.8.1 配置IPv6 MPLS L3VPN示例”，具体配置过程略。

(2) 配置 BGP 的 AS 号替换功能

在PE 1、PE 2 和PE 3 上配置BGP的AS号替换功能，具体配置参见“2.8.7 配置BGP的AS号替换”。

查看 CE 2 接收的路由信息，可以看到 CE 1 发来的路由 100::/96。可见，由于 CE 1 和 CE 2 位于同一站点，造成了路由环路。

```
<CE2> display bgp routing-table ipv6 peer 10:2::2 received-routes

 Total number of routes: 2

 BGP local router ID is 12.1.1.3
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

* >e Network : 100::                                    PrefixLen : 96
     NextHop : 10:2::2                                 LocPrf    :
     PrefVal : 0                                       OutLabel  : NULL
     MED     :
     Path/Ogn: 100 100?
* >e Network : 200::                                    PrefixLen : 96
     NextHop : 10:2::2                                 LocPrf    :
     PrefVal : 0                                       OutLabel  : NULL
     MED     :
     Path/Ogn: 100 100?
```

(3) 配置 BGP 的 SoO 属性

在 PE 1 上为对等体 CE 1 配置 SoO 属性为 1:100。

```
<PE1> system-view
[PE1] bgp 100
[PE1-bgp] ip vpn-instance vpn1
[PE1-bgp-vpn1] address-family ipv6
[PE1-bgp-ipv6-vpn1] peer 10:1::1 soo 1:100
```

在 PE 2 上为对等体 CE 2 配置 SoO 属性为 1:100。

```
[PE2] bgp 100
[PE2-bgp] ip vpn-instance vpn1
[PE2-bgp-vpn1] address-family ipv6
[PE2-bgp-ipv6-vpn1] peer 10:2::1 soo 1:100
```

4. 验证配置

由于配置的 SoO 属性相同，PE 2 不会将 CE 1 发过来的路由发布给 CE 2。查看 CE 2 路由表，不会再看到 100::/96 路由。

```
<CE2> display ipv6 routing-table

Destinations : 4 Routes : 4

Destination: ::1/128                                    Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 10:2::/96                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : GE2/1/1                                    Cost      : 0

Destination: 10:2::1/128                                Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 200::/96                                   Protocol  : Static
NextHop    : ::                                         Preference: 60
Interface  : NULL0                                      Cost      : 0
```

目 录

1 MPLS L2VPN ····· 1-1
1.1 MPLS L2VPN简介 ····· 1-1
1.1.1 基本概念 ····· 1-1
1.1.2 基本网络架构 ····· 1-2
1.1.3 远程连接的配置方法和工作原理 ····· 1-3
1.1.4 本地交换的配置方法和工作原理 ····· 1-5
1.1.5 PW数据封装类型 ····· 1-6
1.1.6 控制字功能 ····· 1-7
1.1.7 异构网络互连（Interworking） ····· 1-8
1.1.8 PW冗余保护 ····· 1-8
1.1.9 多段PW ····· 1-9
1.1.10 PW连通校验VCCV ····· 1-11
1.2 MPLS L2VPN配置任务简介 ····· 1-11
1.3 使能L2VPN ····· 1-12
1.4 配置AC ····· 1-12
1.4.1 配置AC侧接口 ····· 1-12
1.5 配置交叉连接 ····· 1-14
1.6 配置PW ····· 1-14
1.6.1 配置PW模板 ····· 1-14
1.6.2 配置静态PW ····· 1-14
1.6.3 配置LDP PW ····· 1-15
1.6.4 配置BGP PW ····· 1-15
1.6.5 配置CCC远程连接 ····· 1-17
1.7 配置AC与交叉连接关联 ····· 1-18
1.7.1 配置AC侧三层接口与交叉连接关联 ····· 1-18
1.8 配置PW冗余保护 ····· 1-19
1.8.1 配置静态PW的冗余保护 ····· 1-19
1.8.2 配置LDP PW的冗余保护 ····· 1-20
1.9 配置异构网络互连 ····· 1-20
1.10 MPLS L2VPN显示和维护 ····· 1-21
1.11 MPLS L2VPN典型配置举例 ····· 1-22
1.11.1 本地交换配置举例 ····· 1-22
1.11.2 本地交换IP异构配置举例 ····· 1-23

1.11.3 静态PW配置举例 ····· 1-25
1.11.4 LDP PW配置举例 ····· 1-28
1.11.5 LDP方式IP异构连接配置举例 ····· 1-31
1.11.6 BGP PW配置举例 ····· 1-35
1.11.7 CCC远程连接配置举例 ····· 1-39
1.11.8 域内多段PW配置举例 ····· 1-42
1.11.9 域间多段PW配置举例 ····· 1-45

1 MPLS L2VPN

MPLS L2VPN 既可以提供点到点的连接，也可以提供多点间的连接。本章只介绍提供点到点连接的 MPLS L2VPN 技术。

1.1 MPLS L2VPN简介

MPLS L2VPN 是基于 MPLS 的二层 VPN（Virtual Private Network，虚拟专用网络）技术，是 PWE3（Pseudo Wire Emulation Edge-to-Edge，边缘到边缘的伪线仿真）的一种实现方式。MPLS L2VPN 将用户的二层数据（如以太网数据帧、ATM 信元等）封装成可以在 IP 或 MPLS 网络中传送的分组，通过 IP 路径或 MPLS 隧道转发封装后的分组，接收端解封装分组后恢复原来的二层数据，从而实现用户二层数据跨越 MPLS 或 IP 网络透明地传送。从用户的角度来看，MPLS 或 IP 网络是一个二层交换网络，可以在用户网络的不同站点（Site）间建立二层连接。

利用 MPLS L2VPN，运营商可以在统一的 MPLS 或 IP 骨干网上为不同的数据链路层提供 VPN 服务，包括 Ethernet、VLAN、PPP、ATM、Frame Relay 等，使得数据链路层业务可以穿越 MPLS 或 IP 骨干网传送。以 Ethernet 类型的用户网络为例，通过 MPLS L2VPN 连接的 Ethernet 节点感知不到 MPLS 或 IP 骨干网的存在，就好像节点之间直接通过以太网相连。

1.1.1 基本概念

- CE（Customer Edge，用户网络边缘）设备

直接与服务提供商网络相连的用户网络侧设备。

- PE（Provider Edge，服务提供商网络边缘）设备

与 CE 相连的服务提供商网络侧设备。PE 主要负责 VPN 业务的接入，完成报文从用户网络到公网隧道、从公网隧道到用户网络的映射与转发。

- AC（Attachment Circuit，接入电路）

连接 CE 和 PE 的物理电路或虚拟电路，例如 Frame Relay 的 DLCI、ATM 的 VPI/VCI、Ethernet 接口、VLAN、物理接口上的 PPP 连接。

- PW（Pseudowire，伪线）

两个 PE 之间的虚拟双向连接。MPLS PW 由一对方向相反的单向 LSP 构成。

- 公网隧道（Tunnel）

穿越 IP 或 MPLS 骨干网、用来承载 PW 的隧道。一条公网隧道可以承载多条 PW，公网隧道可以是 LSP、MPLS TE、GRE 隧道等。

- 交叉连接（Cross connect）

由两条物理电路或虚拟电路串连而成的一条连接，从一条物理、虚拟电路收到的报文直接交换到另一条物理、虚拟电路转发。交叉连接包括三种方式：AC 到 AC 交叉连接、AC 到 PW 交叉连接、PW 到 PW 交叉连接。

- Site ID

用户网络站点在 VPN 内的唯一标识。不同 VPN 内站点的 Site ID 可以相同。

- RD（Route Distinguisher，路由标识符）

RD 用来区分不同 VPN 内 Site ID 相同的站点。在 Site ID 前增加 RD，通过 RD+Site ID 可以唯一标识网络中的一个站点。

- 标签块

标签块是一组标签的集合，包含以下参数：

  - LB（Label Base，初始标签）：标签块的标签初始值。该值为 PE 设备自动选取，不可手动修改。
  - LR（Label Range，标签范围）：标签块包含的标签数目。LB 和 LR 确定了标签块中包含哪些标签。例如，LB 为 1000、LR 为 5，则该标签块包含的标签为 1000～1004。
  - LO（Label-block Offset，标签块偏移）：VPN 网络中站点的数量增加，原有的标签块大小无法满足要求时，PE 无需撤销原有的标签块，只要在原有标签块的基础上再分配一个新的标签块就可以扩大标签范围，满足扩展需要。在这种情况下，PE 通过 LO 来标识某个标签块在所有为站点分配的标签块中的位置，并根据 LO 来判断从哪个标签块中分配标签。LO 的取值为之前分配的所有标签块大小的总合。例如，PE 为站点分配的第一个标签块的 LR 为 10、LO 为 0，则第二个标签块的 LO 为 10；如果第二个标签块的 LR 为 20，则第三个标签块的 LO 为 30。

标签块通过 LB/LO/LR 来表示，即 LB 为 1000、LO 为 10、LR 为 5 的标签块可以表示为 1000/10/5。

假设，某个 VPN 网络中原有站点数量为 10，PE 为其分配第一个标签块 LB1/0/10。站点数量增加到 25 时，PE 可以保留分配的第一个标签块，并补充分配第二个标签块 LB2/10/15，从而满足 VPN 网络扩展的要求。其中，LB1 和 LB2 为 PE 随机选取的初始标签值。

- VPN target

MPLS L2VPN 使用 BGP 扩展团体属性——VPN Target（也称为 Route Target）来控制 BGP L2VPN 信息的发布。

PE 上的 VPN target 属性分为以下两种，每一种都可以包括多个属性值：

  - Export target 属性：本地 PE 在通过 BGP 的 Update 消息将 L2VPN 信息（如本地 Site ID、RD、标签块等）发送给远端 PE 时，将 Update 消息中携带的 VPN target 属性设置为 Export target。
  - Import target 属性：PE 收到其它 PE 发布的 Update 消息时，将消息中携带的 VPN target 属性与本地配置的 Import target 属性进行比较，只有二者中存在相同的属性值时，才会接收该消息中的 L2VPN 信息。

也就是说，VPN target 属性定义了本地发送的 L2VPN 信息可以为哪些 PE 所接收，PE 可以接收哪些远端 PE 发送来的 L2VPN 信息。

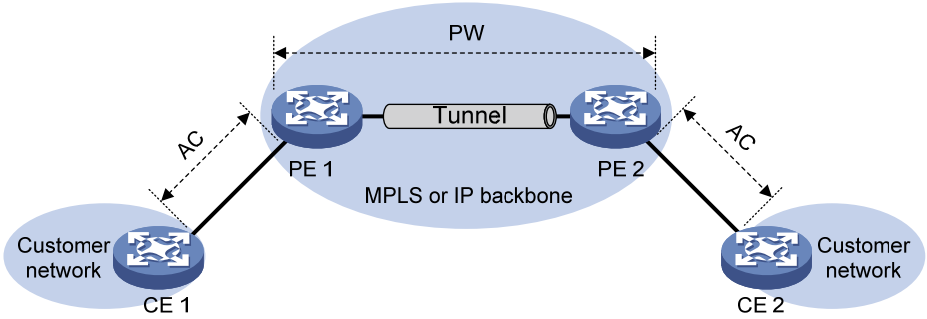
1.1.2 基本网络架构

MPLS L2VPN 的组网架构分为远程连接和本地交换两种。

1. 远程连接组网架构

如 图 1-1 所示，MPLS L2VPN的远程连接组网是指通过穿越IP或MPLS骨干网络的PW连接两端的用户网络。

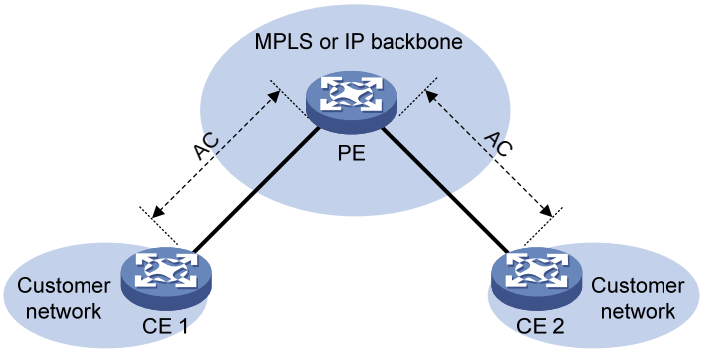
图1-1 远程连接组网图



2. 本地交换组网架构

如 图 1-2 所示，本地交换是MPLS L2VPN提供的一种比较特殊的连接，它是指将同一个用户网络两个站点的CE连接到同一个PE上，两个CE直接通过PE进行用户报文的交换。

图1-2 本地交换组网图



1.1.3 远程连接的配置方法和工作原理

要想通过 MPLS L2VPN 的远程连接转发报文，需要完成以下工作：

- 建立公网隧道，公网隧道用来承载 PE 之间的一条或多条 PW。
- 建立用来传送特定用户网络报文的 PW，PW 标签标识了报文所属的用户网络。
- 建立用来连接 CE 和 PE 的 AC，AC 的报文匹配规则（显式配置或隐含的规则）决定了从 CE 接收到的哪些报文属于一个特定的用户网络。
- 将 AC 和 PW 关联，以便 PE 确定从 AC 接收到的报文向哪条 PW 转发，从 PW 接收到的报文向哪条 AC 转发。

完成上述配置后，PE 从 AC 接收到用户网络的报文后，根据 AC 关联的 PW 为报文封装 PW 标签，并通过公网隧道将报文转发给远端 PE；远端 PE 从公网隧道接收到报文后，根据 PW 标签判断报文所属的 PW，并将还原后的原始报文转发给与该 PW 关联的 AC。

1. 建立公网隧道

公网隧道用来承载 PW，可以是 LSP 隧道、MPLS TE 隧道和 GRE 隧道等。不同隧道的建立方式不同，详细介绍请参见相关手册。

当两个 PE 之间存在多条公网隧道时，可以通过配置隧道策略，确定如何选择隧道。隧道策略的详细介绍，请参见“MPLS 配置指导”中的“隧道策略”。

说明

如果 PW 建立在 LSP 或 MPLS TE 隧道之上，则 PW 上传送的报文将包括两层标签：内层标签为 PW 标签，用来决定报文所属的 PW，从而将报文转发给正确的 CE；外层标签为公网 LSP 或 MPLS TE 隧道标签，用来保证报文在 MPLS 网络正确传送。

2. 建立PW

建立 PW 是指两端的 PE 设备分别为对方分配 PW 标签，以便建立方向相反的一对单向 LSP。

PW 的建立方式有以下几种：

- 静态方式

静态方式建立 PW 是指在两端的 PE 上分别手工指定远端 PE 地址、PW 的入标签、出标签等信息，以便建立 PW。采用静态方式建立的 PW，称为静态 PW。

采用此方式时，不需要使用 PW 信令协议传递 PW 标签等信息，消耗的网络资源比较少，但是需要手工在两端 PE 上配置入标签和出标签，配置比较复杂。

- LDP 方式

LDP 方式建立 PW 是指在两端的 PE 上分别手工指定远端 PE 地址后，通过 LDP 协议向该远端 PE 通告本端 PE 为 PW 分配的 PW 标签等信息，以便建立 PW。采用 LDP 方式建立的 PW，称为 LDP PW。

为了在 PE 之间交换 PW 和 PW 标签的绑定关系，LDP 定义了一种新的 FEC 类型——PW ID FEC。该 FEC 通过 PW ID 和 PW type 来标识一条 PW。其中，PW ID 为 PW 在两个 PE 之间的标识；PW type 表明 PW 上传送数据的封装类型，如 ATM、帧中继、Ethernet、VLAN 等。

PE 发送标签映射消息时，在消息中携带 PW ID FEC 及相应的 PW 标签，就可以将 PE 为该 PW 分配的 PW 标签通告给远端 PE。两端 PE 均收到对端通告的 PW 标签后，便成功在这两个 PE 之间建立起一条 PW。

与静态方式相比，LDP 方式配置比较简单，但是消耗的网络资源比较多。

- BGP 方式

BGP 方式建立 PW 是指通过 BGP 协议通告本端 PE 分配的 PW 标签块等信息，以便远端 PE 自动发现该 PE，并与其建立 PW。采用 BGP 方式建立的 PW，称为 BGP PW。

采用 BGP 方式建立 PW 的过程为：PE 将自己分配的标签块通过扩展的 BGP Update 消息通告给同一个 VPN 内的所有 PE，每个 PE 都根据其他 PE 通告的标签块计算 PW 出标签、根据自己分配的标签块计算 PW 入标签。两端 PE 分别计算出 PW 入标签和 PW 出标签后，便在二者之间建立了 BGP PW。

BGP 方式具有如下特点：

  - 无需手工指定远端 PE 的地址，在通过 BGP 发布标签块信息的同时可以自动发现远端 PE，简化了配置。
  - 通过发布标签块信息可以实现一次为多个 PW 分配标签，减少了 VPN 部署和扩容时的配置工作量，但是耗费的标签资源较多。

- CCC 方式

CCC（Circuit Cross Connect，电路交叉连接）方式建立 PW 是指通过在 PE 设备上手工指定入标签和出标签而建立一条静态连接。CCC 方式建立的 PW 称为 CCC PW，或 CCC 远程连接。

CCC 远程连接不需要公网隧道来承载，它通过在 PE 之间的 P 设备上配置两条方向相反的静态 LSP，来实现报文跨越公网传送。通过 CCC 远程连接转发二层用户报文时，只需为用户报文封装一层标签。

CCC 远程连接对 P 设备上 LSP 的使用是独占性的。P 设备上的 LSP 只用于传递这个 CCC 远程连接的数据，不能用于其他连接，也不能用于 MPLS L3VPN。

3. 建立AC

AC 是 CE 与 PE 之间的物理电路或虚拟电路，它可以是以太网链路、用 DLCI 标识的帧中继虚电路等。建立 AC 就是在 PE 和 CE 上配置链路层协议，以便在 PE 和 CE 之间建立链路层连接，如 PPP 连接。

AC 在 PE 上的表现形式有如下几种：

- 三层物理接口：用来做端口透传，即物理接口上接收到的所有报文都关联到同一条 PW。这种方式称为端口模式，如以太网端口透传、ATM 信元端口透传、Frame Relay 端口透传。
- 三层子接口：将子接口对应的链路（如 VLAN、ATM VPC、ATM VCC、Frame Relay 的 DLCI）上接收到的报文关联到同一条 PW。采用这种方式时，VLAN 在接口范围内唯一，而不是整设备范围内唯一。
- VLAN 虚接口：将从一个 VLAN 上接收到的所有报文关联到同一条 PW。采用这种方式时，VLAN 整设备范围内唯一。

说明

VLAN 整设备范围内唯一是指不区分接口，无论从哪个接口接收到的报文，只要 Tag 相同就关联到同一条 PW；VLAN 接口范围内唯一是指从不同接口接收到的带有相同 Tag 的报文，可以关联到不同的 PW。

---

4. 将AC和PW关联

通过命令行将 AC 连接对应的三层物理接口、三层子接口、VLAN 虚接口与 PW 关联，即可实现从该 AC 接收到的报文通过关联的 PW 转发，从关联的 PW 上接收到的报文通过该 AC 转发。

1.1.4 本地交换的配置方法和工作原理

要想实现报文的本地交换，需要完成以下工作：

(1) 在同一台 PE 上建立两条 AC

两个CE连接到同一个PE时，在PE和两个CE之间配置链路层协议，以便PE与两个CE分别建立AC连接。详细介绍请参见“1.1.3 3. 建立AC”。

(2) 将两个 AC 关联

通过命令行将两条 AC 连接对应的三层物理接口、三层子接口、VLAN 虚接口关联，即可实现从一个 AC 接收到的报文被转发到与其关联的另一个 AC。

1.1.5 PW数据封装类型

MPLS L2VPN可以在PW上传递不同数据链路层协议的二层用户报文。为二层报文封装PW标签前，PE对不同链路层协议的二层报文的处理方式有所不同。PW数据封装类型（PW type）用来标识PE对二层报文的处理方式。PW数据封装类型与AC的链路类型（PE—CE之间的链路类型）密切相关，其对应关系如 表 1-1 所示。

表1-1 AC 链路类型及 PW 数据封装类型对应关系表

AC 链路类型	PW 数据封装类型
以太网	Ethernet
	VLAN
PPP	PPP
HDLC	HDLC

1. Ethernet over MPLS

Ethernet over MPLS 是指利用 MPLS L2VPN 连接以太网，通过 PW 在 MPLS 骨干网上传送 Ethernet 报文。

Ethernet over MPLS 对应的 PW 数据封装类型有两种：

- Ethernet 数据封装类型下，PW 上传输的帧不能带服务提供商网络为了区分用户而要求用户压入的 P-Tag，该 Tag 又称为服务定界符。对于 CE 侧的报文，如果从 CE 收到带有 P-Tag 的报文，则将其去除后再压入 PW 标签和公网隧道封装转发；如果从 CE 收到不带 P-Tag 的报文，则直接压入 PW 标签和公网隧道封装后转发。对于 PE 发送给 CE 的报文，如果 **ac interface** 命令配置的接入模式为 VLAN，则添加 P-Tag 后转发给 CE；如果配置的接入模式为 Ethernet，则不添加 P-Tag，直接转发给 CE；不允许重写或去除已经存在的任何 Tag。
- VLAN 数据封装类型下，PW 上传输的帧必须带 P-Tag。对于 CE 侧的报文，从 CE 收到带有 P-Tag 的报文后，如果远端 PE 不要求 Ingress 改写 P-Tag，则保留 P-Tag，如果远端 PE 要求 Ingress 改写 P-Tag，则将 P-Tag 改写为远端 PE 期望的 VLAN Tag（Tag 可能是值为 0 的空 Tag），再压入 PW 标签和公网隧道封装后转发；从 CE 收到不带 P-Tag 的报文后，如果远端 PE 不要求 Ingress 改写 P-Tag，则添加值为 0 的空 P-Tag，如果远端 PE 要求 Ingress 改写 P-Tag，则添加一个远端 PE 期望的 VLAN Tag（Tag 可能是值为 0 的空 Tag）后，再压入 PW 标签和公网隧道封装后转发。对于 PE 发送给 CE 的报文，如果 **ac interface** 命令配置的接入模式为 VLAN，转发给 CE 时重写或保留 P-Tag；如果配置的接入模式为 Ethernet，则去除 P-Tag 后转发给 CE。

说明

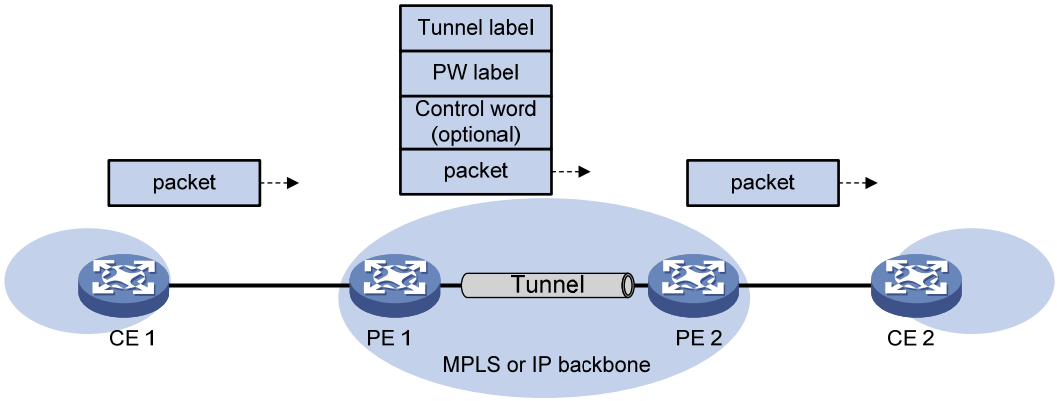
接入模式分为 Ethernet 和 VLAN 两种，可以通过 **ac interface** 命令来配置。详细介绍请参见“MPLS 命令参考”中的“MPLS L2VPN”。

Ethernet over MPLS 有如下几种方式：

- 端口模式

通过命令行将三层以太网接口与 PW 关联。这样，从该接口收到的所有报文都通过关联的 PW 传送到远端 PE。缺省情况下，端口模式中 PW 的数据封装类型为 Ethernet。

图1-3 Ethernet 的端口模式



- VLAN 模式

通过命令行将三层以太网子接口或 VLAN 接口与 PW 关联。这样，接收到的所有属于特定 VLAN 的报文都通过关联的 PW 传送到远端 PE，远端 PE 可以根据连接的用户网络的需要修改 VLAN tag。缺省情况下，VLAN 模式中 PW 的数据封装类型为 VLAN。

2. PPP/HDLC over MPLS

PPP/HDLC over MPLS 是指利用 MPLS L2VPN 连接 PPP 或 HDLC 网络，通过 PW 在 MPLS 骨干网上传送 PPP 或 HDLC 报文。

PPP over MPLS 对应的 PW 数据封装类型为 PPP；HDLC over MPLS 对应的 PW 数据封装类型为 HDLC。

PPP/HDLC over MPLS 只支持端口模式，即通过命令行将配置了 PPP 或 HDLC 封装的三层接口与 PW 关联。PE 从三层接口接收到 PPP/HDLC 报文后，查找与该接口关联的 PW，对 PPP/HDLC 报文进行封装后，通过该 PW 将封装后的报文传递给远端 PE；远端 PE 去掉外层封装，还原出 PPP/HDLC 报文，并将其转发给用户网络。

1.1.6 控制字功能

控制字字段位于 MPLS 标签栈和二层数据之间，用来携带额外的二层数据帧的控制信息，如序列号等。控制字具有如下功能：

- 避免报文乱序：在多路径转发的情况下，报文有可能产生乱序，此时可以通过控制字的序列号字段对报文进行排序重组。
- 传送特定二层数据帧的标记：如帧中继的 FECN（Forward Explicit Congestion Notification，前向显式拥塞通知）比特和 BECN（Backward Explicit Congestion Notification，后向显示拥塞通知）比特等。
- 指示净载荷长度：如果 PW 上传送报文的净载荷长度小于 64 字节，则需要对报文进行填充，以避免报文发送失败。此时，通过控制字的载荷长度字段可以确定原始载荷的长度，以便从填充后的报文中正确获取原始的报文载荷。

对于某些 PW 数据封装类型（如帧中继 DLCI 类型、ATM AAL5 SDU VCC 类型），PW 上传递的报文必须携带控制字字段，不能通过配置来控制。对于某些 PW 数据封装类型（如 Ethernet、VLAN），控制字字段是可选的，由两端的配置共同决定是否携带控制字：如果两端 PE 上都使能了控制字功能，则报文中携带控制字字段；否则，报文中不携带控制字字段。

1.1.7 异构网络互连（Interworking）

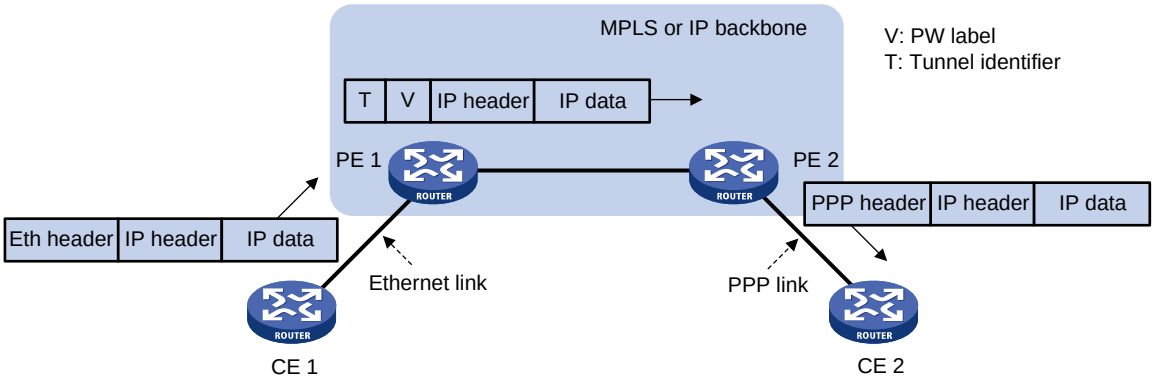
CE 接入 PE 的链路类型多种多样，如 ATM、FR、HDLC、Ethernet、PPP 等。不同接入链路类型的 CE 之间可以通过 MPLS L2VPN 网络互相通信，即 MPLS L2VPN 可以连接异构的网络。

目前，本地交换、静态 PW、LDP PW 和 CCC 远程连接可以连接异构的网络。

说明

MPLS L2VPN 连接异构网络有两种方式：Ethernet interworking 和 IP interworking。目前，设备只支持 IP interworking 方式，本文只介绍这种方式。

图1-4 MPLS L2VPN 连接异构网络示意图



如 图 1-4 所示，以Ethernet和PPP链路类型为例，MPLS L2VPN连接异构网络的报文转发过程为：

(1) CE 1 将目的地址为 CE 2 的以太网数据帧发送给 PE 1。

(2) PE 1 判断接收到的以太网数据帧内封装的是否为 IP 报文。若是，则删除以太网头、添加 PW 标签 V 和隧道标识 T 后，将报文沿隧道转发给远端 PE 2。否则，丢弃该报文。

(3) PE 2 根据 PW 标签 V 获取报文的出接口，弹出 PW 标签后为报文添加 PPP 头，将 PPP 数据帧发送给 CE 2。

MPLS L2VPN 连接异构网络时，链路层协商报文不会在网络中传递，CE 之间无法直接建立二层连接。因此，PE 需要与接入的 CE 建立二层连接，例如，PPP 链路中 PE 需要与 CE 进行 PPP 协商，以建立 PPP 连接。

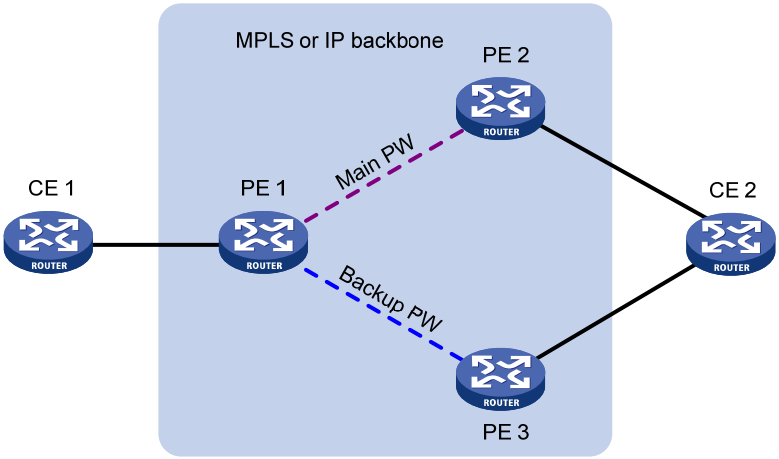
1.1.8 PW冗余保护

如果两个 CE 之间只存在一条 PW，则当 PE 节点、PE 与 CE 之间的链路、或 PE 之间的 PW 出现故障时，CE 之间将无法通信。PW 冗余保护功能通过部署主备两条 PW，实现当主 PW 出现故障后，

将流量立即切换到备份 PW，使得流量转发得以继续。目前，只有静态 PW 和 LDP PW 支持 PW 冗余保护功能。

如 图 1-5 所示，在两个CE之间建立两条PW链路，正常情况下，CE使用主PW与远端CE通信；当PE 1 检测出到PE 2 的PW不可用（可能是PE 2 节点故障，也可能是PW故障，或PE 2 与CE 2 之间的链路故障），PE 1 将启用备份PW，通过备份PW将CE 1 的报文转发给PE 3，再由PE 3 转发给CE 2。CE 2 接收到报文后，通过更新MAC地址表项等方式将发送给CE 1 的报文切换到备份PW转发，从而保证通信不会中断。

图1-5 MPLS L2VPN 的 PW 冗余保护



MPLS L2VPN 根据控制平面的 LDP 会话状态，或者数据平面连通性检测结果等来判断当前使用的 PW 是否可以继续使用。在当前使用的 PW 不可用的情况下，将流量切换到备用的另一条 PW 上。在以下情况下，将启用备份 PW：

- 承载主 PW 的公网隧道被拆除或通过 BFD 等检测机制检测到公网隧道出现故障，导致主 PW 的状态变为 down；
- 控制平面拆除主 PW（如主 PW 两端 PE 之间的 LDP 会话 down 导致主 PW 被删除），或利用 BFD 等链路检测机制检测到主 PW 故障；
- 执行命令手工切换主备 PW。

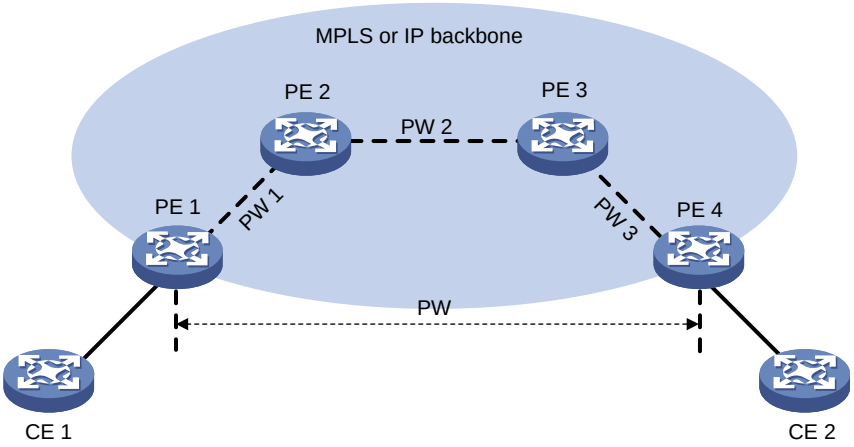
控制平面和数据平面的介绍，请参见“MPLS 配置指导”中的“MPLS 基础”。

1.1.9 多段PW

多段 PW 是指将两条或多条静态 PW 或 LDP PW 串连（concatenated）起来，形成一条端到端的 PW。通过在同一个交叉连接下创建两条 PW，可以实现将该交叉连接下的两条 PW 串连。PE 从一条 PW 接收到报文后，剥离报文的隧道标识和 PW 标签，封装上与该 PW 串连的另一条 PW 的 PW 标签，并通过承载该 PW 的公网隧道转发该报文，从而实现报文在两条 PW 之间的转发。目前，只有静态 PW 和 LDP PW 支持多段 PW 功能。

如 图 1-6 所示，通过在PE 2 上将PW 1 和PW 2 串连、在PE 3 上将PW 2 和PW 3 串连，可以建立从PE 1 到PE 4 的端到端PW，实现报文沿着PW 1、PW 2 和PW 3 形成的多段PW在PE 1 和PE 4 之间转发。

图1-6 多段 PW 示意图



多段 PW 分为：

- 域内多段 PW：即在一个自治系统内部署多段 PW。
- 域间多段 PW：即跨越自治系统部署多段 PW。

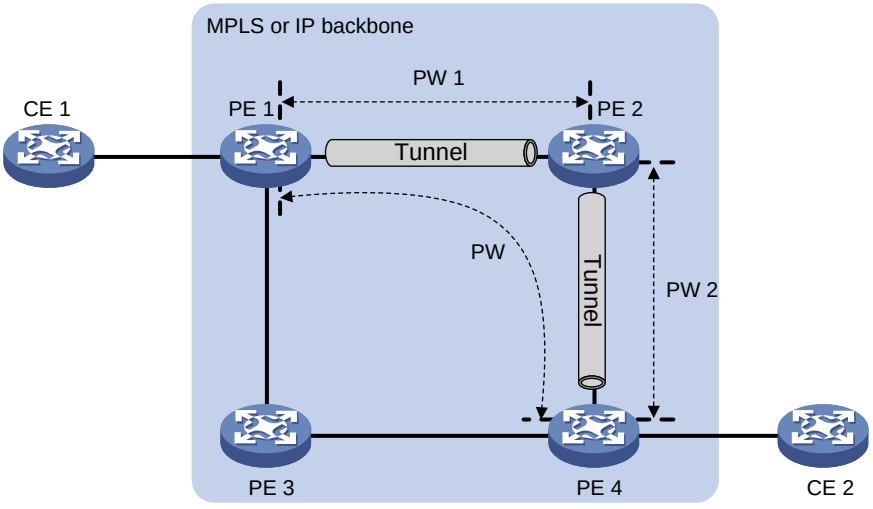
1. 域内多段PW

在一个自治系统内部署多段 PW，可以实现两个 PE 之间不存在端到端公网隧道的情况下，在这两个 PE 之间建立端到端 PW。

如 图 1-7 所示，PE 1 和PE 4 之间没有建立公网隧道，PE 1 和PE 2、PE 2 和PE 4 之间已经建立了公网隧道。通过在PE 1 与PE 2、PE 2 与PE 4 之间分别建立一条PW（PW 1 和PW 2），在PE 2 上将这两条PW串连，可以实现在PE 1 和PE 4 之间建立一条由两段PW组成的端到端域内多段PW。

通过建立域内多段 PW 可以充分利用已有的公网隧道，减少端到端公网隧道数量。

图1-7 域内多段 PW



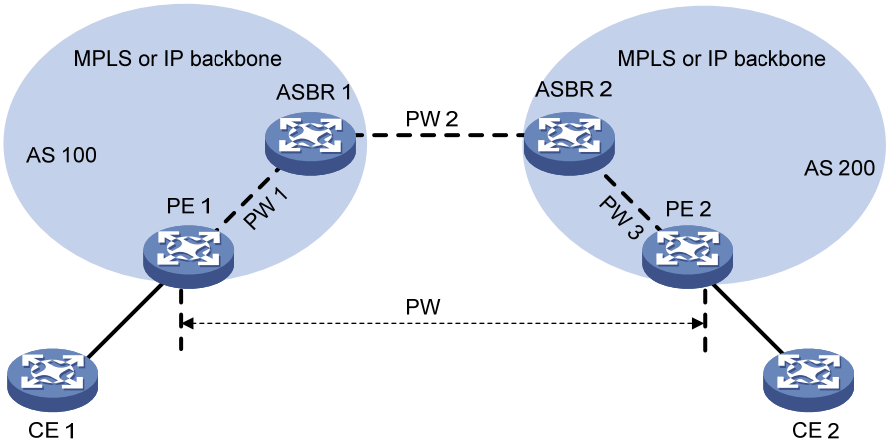
2. 域间多段PW

域间多段PW可以提供穿越多个自治系统的端到端PW，可以作为跨自治系统的Option B解决方案。

如 图 1-8 所示，在PE 1 与ASBR 1、ASBR 1 与ASBR 2、ASBR 2 与PE 2 之间分别建立PW 1、PW

2 和PW 3，在ASBR 1 上将PW 1 与PW 2 串连，在ASBR 2 上将PW 2 与PW 3 串连后，即可建立从PE 1 到PE 2 的跨域PW，实现报文的跨域传送。

图1-8 域间多段 PW



1.1.10 PW连通校验VCCV

VCCV（Virtual Circuit Connectivity Verification，虚电路连通性验证）是 L2VPN 的一种 OAM（Operation, Administration and Maintenance，操作、管理和维护）功能，用于确认 PW 数据平面的连通性。VCCV 有两种方式：

- 按需方式：执行 **ping mpls pw** 命令手工触发 PW 检测。
- 自动方式：配置通过 BFD 或 Raw-BFD 检测 PW 后，系统主动完成 PW 检测。

VCCV 的详细介绍，请参见“MPLS 配置指导”中的“MPLS OAM”。

1.2 MPLS L2VPN配置任务简介

在 MPLS L2VPN 组网中，需要进行以下配置：

- 配置 IGP（Interior Gateway Protocol，内部网关协议），实现骨干网的 IP 连通性。
- 配置 MPLS 基本功能、LDP、GRE 或 MPLS TE 等，在骨干网上建立公网隧道。
- 在两端的 PE 设备上配置 MPLS L2VPN，如建立 PW、将 AC 与 PW 关联。

本文只介绍 PE 设备上的 MPLS L2VPN 相关配置。

在不同的场景下，MPLS L2VPN 的配置有所不同：

- 远程连接：在该场景下，需要配置 AC、在交叉连接视图/自动发现交叉连接视图下配置 PW、在交叉连接视图/自动发现交叉连接视图下配置 AC 与该交叉连接关联，以便关联同一交叉连接视图/自动发现交叉连接视图下的 AC 和 PW。
- 本地交换：在该场景下，需要配置 AC、在交叉连接视图下配置两条 AC 分别与该交叉连接关联，以便关联同一交叉连接视图下的两条 AC。
- 多段 PW：在该场景下，需要在交叉连接视图下配置两条 PW，以便将这两条 PW 串连起来。

表1-2 MPLS L2VPN 配置任务简介

操作		说明	详细配置
使能L2VPN		必选	1.3
配置AC	配置AC侧接口	可选 配置多段PW时，无需进行本配置	1.4.1
配置交叉连接		必选	1.5
配置PW	配置PW模板	可选	1.6.1
	配置静态PW	根据MPLS L2VPN的实现方式，选择相应的配置方法 配置本地交换时，无需进行本配置	1.6.2
	配置LDP PW		1.6.3
	配置BGP PW		1.6.4
	配置CCC远程连接		1.6.5
配置AC与交叉连接关联	配置AC侧接口与交叉连接关联	可选 配置多段PW时，无需进行本配置	1.7.1
配置PW冗余保护		可选	1.8
配置异构网络互连		可选	1.9

1.3 使能L2VPN

执行本配置前，需要先通过 **mpls lsr-id** 命令配置本节点的 LSR ID，并在 PE 连接公网的接口上通过 **mpls enable** 命令使能该接口的 MPLS 能力。**mpls lsr-id** 命令和 **mpls enable** 命令的详细介绍，请参见“MPLS 命令参考”中的“MPLS 基础”。

表1-3 使能 L2VPN

操作	命令	说明
进入系统视图	**system-view**	-
使能L2VPN功能	**l2vpn enable**	缺省情况下，L2VPN功能处于关闭状态

1.4 配置AC

1.4.1 配置AC侧接口

AC 侧接口指的是 PE 上连接 CE 的接口。配置 MPLS L2VPN 时，需要配置 AC 侧接口，以便在 PE 和 CE 之间建立二层链路。

由于 PE 从 AC 侧接口接收到的报文直接通过关联的 PW 转发，无需进行网络层处理，因此 AC 侧接口上不需要配置 IP 地址。

1. 封装类型为Ethernet或VLAN时的接口配置

AC 侧接口为三层以太网接口（包括三层以太网接口、三层虚拟以太网接口、VE-L2VPN 接口）时，PW 数据封装类型和 AC 接入模式缺省均为 Ethernet；AC 侧接口为三层以太网子接口、VLAN 接口时，PW 数据封装类型和 AC 接入模式缺省均为 VLAN。

PW 数据封装类型和 AC 接入模式决定了报文转发过程中 PE 对报文中 VLAN Tag 的处理方式。两端设备上配置的 PW 数据封装类型和 AC 接入模式需要匹配，以便正确处理报文中的 VLAN Tag。

表1-4 封装类型为 Ethernet 或 VLAN 时的接口配置

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
（可选）配置缺省下一跳的IP地址或MAC地址	**default-nexthop** { **ip** *ip-address* | **mac** { *mac-address* | **broadcast** } }	MPLS L2VPN支持连接异构网络时，必选；其他情况下，无需执行本命令 缺省情况下，未指定缺省下一跳信息 VLAN接口下，不支持本配置

2. 封装类型为PPP时的接口配置

表1-5 封装类型为 PPP 时的接口配置

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** { **serial** | **pos** } *number*	-
配置接口的链路协议类型	**link-protocol ppp**	缺省情况下，接口的链路协议类型为PPP
（可选）配置IPCP无地址协商	**ppp ipcp ignore local-ip**	MPLS L2VPN支持异构网络时，二者必选其一；其他情况下，无需执行本命令 缺省情况下，不支持IPCP无地址协商，未指定IPCP代理IP地址
（可选）指定IPCP代理IP地址	**ppp ipcp proxy** *ip-address*	

3. 封装类型为HDLC时的接口配置

表1-6 封装类型为 HDLC 时的接口配置

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** { **serial** | **pos** } *number*	-
配置接口的链路协议类型	**link-protocol hdlc**	缺省情况下，接口的链路协议类型为PPP

1.5 配置交叉连接

表1-7 配置交叉连接

操作	命令	说明
进入系统视图	**system-view**	-
创建一个交叉连接组，并进入交叉连接组视图	**xconnect-group** *group-name*	缺省情况下，设备上不存在任何交叉连接组
（可选）设置交叉连接组的描述信息	**description** *text*	缺省情况下，未配置交叉连接组的描述信息
（可选）开启当前的交叉连接组	**undo shutdown**	缺省情况下，交叉连接组处于开启状态
创建一个交叉连接，并进入交叉连接视图	**connection** *connection-name*	缺省情况下，设备上不存在任何L2VPN交叉连接
配置PW的MTU值	**mtu** *mtu*	缺省情况下，PW的MTU值为1500字节 如果采用LDP信令协议建立PW，则要求PW两端的PE上为PW配置相同的MTU值。否则，PW无法up

1.6 配置PW

1.6.1 配置PW模板

在 PW 模板中可以指定 PW 的属性，如 PW 的数据封装类型、是否使用控制字等。具有相同属性的 PW 可以通过引用相同的 PW 模板，实现对 PW 属性的配置，从而简化配置。

表1-8 配置 PW 模板

操作	命令	说明
进入系统视图	**system-view**	-
创建PW模板，并进入PW模板视图	**pw-class** *class-name*	缺省情况下，设备上不存在任何PW模板
（可选）使能控制字功能	**control-word enable**	缺省情况下，未使能控制字功能
（可选）PW数据封装类型	**pw-type** { **ethernet** | **vlan** }	缺省情况下，PW数据封装类型为VLAN

1.6.2 配置静态PW

表1-9 配置静态 PW

操作	命令	说明
进入系统视图	**system-view**	-
进入交叉连接组视图	**xconnect-group** *group-name*	-
进入交叉连接视图	**connection** *connection-name*	-

操作	命令	说明
配置静态PW，并进入交叉连接PW视图	**peer** *ip-address* **pw-id** *pw-id* **in-label** *label-value* **out-label** *label-value* [**pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *	缺省情况下，未配置静态PW

1.6.3 配置LDP PW

在配置LDP PW之前，需要在PE上使能全局和接口的MPLS LDP能力，详细配置方法请参见“MPLS配置指导”中的“LDP”。

表1-10 配置 LDP PW

操作	命令	说明
进入系统视图	**system-view**	-
进入交叉连接组视图	**xconnect-group** *group-name*	-
进入交叉连接视图	**connection** *connection-name*	-
配置LDP PW，并进入交叉连接PW视图	**peer** *ip-address* **pw-id** *pw-id* [**pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *	缺省情况下，未配置LDP PW

说明

如果 LDP PW 两端的 PE 不是直连的，则创建 PW 后，本端 PE 会自动使用 Targeted hello 来发现远端 PE，以建立 LDP 会话，并在这个会话上交换 PW ID FEC 与 PW 标签的映射。

1.6.4 配置BGP PW

配置 BGP PW 时，需要在 PE 上进行以下配置：

- 配置 BGP 发布 MPLS L2VPN 标签块信息
- 建立 BGP PW

1. 配置BGP发布MPLS L2VPN标签块信息

建立 BGP PW 时，需要在 PE 设备上进行 BGP 相关配置，以便 PE 通过 BGP 发布 MPLS L2VPN 的标签块信息。

下表中 **peer as-number**、**peer enable**、**peer allow-as-loop**、**peer reflect-client**、**reflect between-clients** 和 **reflector cluster-id** 命令的详细介绍，请参见“三层技术-IP 路由命令参考”中的“BGP”。

表1-11 配置 BGP 发布 MPLS L2VPN 标签块信息

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
启动BGP，并进入BGP视图	**bgp** *as-number*	缺省情况下，系统没有运行BGP
将远端PE配置为对等体	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	缺省情况下，设备上不存在任何BGP对等体
创建BGP L2VPN地址族，并进入BGP L2VPN地址族视图	**address-family l2vpn**	缺省情况下，没有创建BGP L2VPN地址族
使能本地路由器与指定对等体/对等体组交换BGP L2VPN信息的能力	**peer** { *group-name* | *ip-address* } **enable**	缺省情况下，本地路由器不能与对等体/对等体组交换BGP L2VPN信息
使能本地路由器与指定对等体/对等体组交换MPLS L2VPN标签块信息的能力	**peer** { *group-name* | *ip-address* } **signaling** [**non-standard**]	缺省情况下，本地路由器具有与BGP L2VPN对等体/对等体组交换标签块信息的能力，并且采用RFC 4761中定义的MP_REACH_NLRI格式交换标签块信息
（可选）配置对于从对等体/对等体组接收的BGP消息，允许本地AS号在该消息的AS_PATH属性中出现，并配置允许出现的次数	**peer** { *group-name* | *ip-address* } **allow-as-loop** [*number*]	缺省情况下，不允许本地AS号在接收消息的AS_PATH属性中出现
（可选）对接收到的BGP L2VPN信息使能VPN-Target过滤功能	**policy vpn-target**	缺省情况下，对接收到的BGP L2VPN信息使能VPN-Target过滤功能
（可选）配置本机作为路由反射器，对等体/对等体组作为路由反射器的客户机	**peer** { *group-name* | *ip-address* } **reflect-client**	缺省情况下，没有配置路由反射器及其客户机
（可选）允许路由反射器在客户机之间反射L2VPN信息	**reflect between-clients**	缺省情况下，允许路由反射器在客户机之间反射L2VPN信息
（可选）配置路由反射器的集群ID	**reflector cluster-id** { *cluster-id* | *ip-address* }	缺省情况下，每个路由反射器都使用自己的Router ID作为集群ID
（可选）创建路由反射器的反射策略	**rr-filter** *extended-community-number*	缺省情况下，路由反射器不会对反射的L2VPN信息进行过滤
（可选）返回用户视图	**return**	-
（可选）手工对L2VPN地址族下的BGP会话进行软复位	**refresh bgp** { *ip-address* | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** } **l2vpn**	本命令的详细介绍，请参见“三层技术-IP路由命令参考”中的“BGP”
（可选）复位L2VPN地址族下的BGP会话	**reset bgp** { *as-number* | *ip-address* | **all** | **external** | **group** *group-name* | **internal** } **l2vpn**	本命令的详细介绍，请参见“三层技术-IP路由命令参考”中的“BGP”

2. 建立BGP PW

表1-12 建立 BGP PW

操作	命令	说明
进入系统视图	**system-view**	-
进入交叉连接组视图	**xconnect-group** *group-name*	-

操作	命令	说明
指定交叉连接组采用BGP方式自动发现邻居、建立PW，并进入交叉连接组自动发现视图	**auto-discovery bgp**	缺省情况下，交叉连接组不会采用BGP方式自动发现邻居并建立PW
为当前交叉连接组的BGP方式配置RD	**route-distinguisher** *route-distinguisher*	缺省情况下，没有为交叉连接组的BGP方式指定RD
为当前交叉连接组的BGP方式配置Route Target属性	**vpn-target** *vpn-target*&<1-8> [**both** | **export-extcommunity** | **import-extcommunity**]	缺省情况下，没有为交叉连接组的BGP方式指定Route Target属性
（可选）指定引用的PW模板	**pw-class** *class-name*	缺省情况下，不引用任何PW模板
（可选）配置PW的MTU值	**mtu** *mtu*	缺省情况下，PW的MTU值为1500字节
创建本地站点，并进入站点视图	**site** *site-id* [**range** *range-value*] [**default-offset** *defalut-offset*]	缺省情况下，设备上不存在任何本地站点
创建交叉连接，并进入自动发现交叉连接视图	**connection remote-site-id** *remote-site-id*	缺省情况下，设备上不存在任何交叉连接 执行本命令创建交叉连接后，将同时创建连接当前站点和指定远端站点的一条PW，该PW与该交叉连接关联
（可选）指定引用的隧道策略	**tunnel-policy** *tunnel-policy-name*	缺省情况下，不引用任何隧道策略

1.6.5 配置CCC远程连接

配置 CCC 远程连接时，需要在 PE 和 P 上分别进行如下配置：

- 在两端 PE 上分别通过 **ccc** 命令指定入标签和出标签等。
- 在 PE 之间的所有 P 设备上执行 **static-lsp transit** 命令为两个数据传输方向分别配置一条静态 LSP，专门用于传输 CCC 远程连接的数据。**static-lsp transit** 命令的详细介绍，请参见“MPLS 命令参考”中的“静态 LSP”。

创建 CCC 远程连接时，需要确保：

- 为某一台设备指定的出标签必须与为其下一跳指定的入标签相同。
- 两端 PE 上 CCC 远程连接的封装类型、控制字功能等配置保持一致，否则可能会导致报文转发失败。

表1-13 配置 CCC 远程连接

操作	命令	说明
进入系统视图	**system-view**	-
进入交叉连接组视图	**xconnect-group** *group-name*	-
进入交叉连接视图	**connection** *connection-name*	-

操作	命令	说明
创建一条CCC远程连接	**ccc in-label** *in-label-value* **out-label** *out-label-value* { **nexthop** *nexthop* | **out-interface** *interface-type interface-number* } [**pw-class** *class-name*]	缺省情况下，设备上不存在任何CCC远程连接 只有出接口连接的链路是点到点链路时，才能够使用**out-interface**参数指定出接口。如果出接口连接的链路不是点到点链路，如出接口类型为三层以太网接口、VLAN接口或三层聚合接口，则必须使用**nexthop**参数指定下一跳IP地址

1.7 配置AC与交叉连接关联

提示

本配置与以太网链路聚合功能互斥。三层或二层以太网接口加入聚合组后，不能再将该接口与交叉连接关联；反之亦然。

配置 AC 与交叉连接关联的方法与 AC 在 PE 上的表现形式有关：

- AC 为三层接口时，需要配置 AC 侧三层接口与交叉连接关联。

1.7.1 配置AC侧三层接口与交叉连接关联

配置 AC 侧三层接口与交叉连接关联后，从接口接收到的报文将通过关联该交叉连接的 PW 或另一条 AC 转发。

表1-14 配置 AC 侧三层接口与非 BGP 方式交叉连接关联

操作	命令	说明
进入系统视图	**system-view**	-
进入交叉连接组视图	**xconnect-group** *group-name*	-
进入交叉连接视图	**connection** *connection-name*	-
将AC侧接口与交叉连接关联	**ac interface** *interface-type interface-number*	缺省情况下，接口没有与交叉连接关联

表1-15 配置 AC 侧三层接口与 BGP 方式交叉连接关联

操作	命令	说明
进入系统视图	**system-view**	-
进入交叉连接组视图	**xconnect-group** *group-name*	-
进入交叉连接组自动发现视图	**auto-discovery bgp**	-
进入站点视图	**site** *site-id* [**range** *range-value*] [**default-offset** *defalut-offset-value*]	-

操作	命令	说明
进入自动发现交叉连接视图	**connection remote-site-id** *remote-site-id*	-
将AC侧接口与交叉连接关联	**ac interface** *interface-type interface-number*	缺省情况下，接口没有与交叉连接关联

1.8 配置PW冗余保护

PW 冗余保护的配置包括以下几部分：

- 为主 PW 创建备份 PW。
- 配置 PW 冗余保护倒换的回切模式，即主 PW 恢复后，流量是否从备份 PW 回切到主 PW；以及回切模式下的回切等待时间，即主 PW 恢复后，流量从备份 PW 回切到主 PW 的等待时间。
- 手工将指定 PW 的流量倒换到它的冗余备份 PW 上，以方便管理员对网络流量进行管理。

1.8.1 配置静态PW的冗余保护

表1-16 配置静态 PW 的冗余保护

操作	命令	说明
进入系统视图	**system-view**	-
进入交叉连接组视图	**xconnect-group** *group-name*	-
进入交叉连接视图	**connection** *connection-name*	-
（可选）配置PW冗余保护倒换的回切模式，以及回切模式下的回切等待时间	**revertive** { **wtr** *wtr-time* | **never** }	缺省情况下，开启回切功能，即主PW恢复后，流量会从备份PW回切到主PW；回切等待时间为0，即主PW恢复后，流量会立即从备份PW回切到主PW
进入交叉连接PW视图	**peer** *ip-address* **pw-id** *pw-id* [**in-label** *label-value* **out-label** *label-value*] [**pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *	-
配置备份的静态PW，并进入交叉连接备份PW视图	**backup-peer** *ip-address* **pw-id** *pw-id* **in-label** *label-value* **out-label** *label-value* [**pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *	缺省情况下，未配置备份的静态PW
返回用户视图	**return**	-
将指定PW的流量手工倒换到它的冗余备份PW上	**l2vpn switchover peer** *ip-address* **pw-id** *pw-id*	-

1.8.2 配置LDP PW的冗余保护

表1-17 配置 LDP PW 的冗余保护

操作	命令	说明
进入系统视图	**system-view**	-
进入交叉连接组视图	**xconnect-group** *group-name*	-
进入交叉连接视图	**connection** *connection-name*	-
（可选）配置PW冗余保护倒换的回切模式，以及回切模式下的回切等待时间	**revertive** { **wtr** *wtr-time* | **never** }	缺省情况下，开启回切功能，即主PW恢复后，流量会从备份PW回切到主PW；回切等待时间为0，即主PW恢复后，流量会立即从备份PW回切到主PW。
进入交叉连接PW视图	**peer** *ip-address* **pw-id** *pw-id* [**pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *	-
配置备份的LDP PW，并进入交叉连接备份PW视图	**backup-peer** *ip-address* **pw-id** *pw-id* [**pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *	缺省情况下，未配置备份的LDP PW
返回用户视图	**return**	-
将指定PW的流量手工倒换到它的冗余备份PW上	**l2vpn switchover peer** *ip-address* **pw-id** *pw-id*	-

1.9 配置异构网络互连

异构网络互连功能对链路层协议及 PE 配置具有如下要求：

(1) CE 接入 PE 的链路类型为 Ethernet 或 VLAN 时

- PE 和 CE 所在的以太网或 VLAN 网络内只能存在 PE 和 CE 两台三层设备。
- 对于 CE 发送的所有 ARP 请求，PE 都会采用自己的 MAC 地址进行应答。
- PE 上需要通过 **default-nexthop** 命令配置缺省下一跳信息，以便 PE 正确地为发送给 CE 的报文封装链路层头。缺省下一跳信息为单播 MAC 地址（CE 的 MAC 地址）或广播 MAC 地址时，PE 发送给 CE 的报文将以该 MAC 地址作为目的 MAC 地址；缺省下一跳信息为 IP 地址（CE 的 IP 地址）时，PE 通过免费 ARP 将 IP 地址解析为 MAC 地址，解析到的 MAC 地址将作为 PE 发送给 CE 报文的目的 MAC 地址。
- CE 连接 PE 的接口上配置路由协议的操作方式为点对点操作方式，例如通过 **ospf network-type p2p** 命令配置 OSPF 接口的网络类型为 P2P（Point-to-Point，点到点）。
- 在 PE 上取消支持连接异构网络的配置时，需要通过 **reset arp** 命令清除 CE 上的 ARP 表项，以便 CE 能学到新的 ARP 表项，避免流量被错误地丢弃。

(2) CE 接入 PE 的链路类型为 PPP 时

PE 上需要配置 **ppp ipcp ignore local-ip**，以支持 IPCP 无地址协商；或配置 **ppp ipcp proxy**，以使用指定的 IP 地址与 CE 进行 IPCP 协商。

表1-18 配置异构网络互连

操作	命令	说明
进入系统视图	**system-view**	-
进入交叉连接组视图	**xconnect-group** *group-name*	-
进入交叉连接视图	**connection** *connection-name*	-
使能交叉连接的异构互连功能	**interworking ipv4**	缺省情况下，交叉连接不支持异构互连功能

1.10 MPLS L2VPN显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 MPLS L2VPN 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可以复位 BGP 会话。

display bgp group l2vpn、**display bgp peer l2vpn**、**display bgp update-group l2vpn** 和 **reset bgp l2vpn** 命令的详细介绍，请参见“三层技术-IP 路由命令参考”中的“BGP”。

表1-19 MPLS L2VPN 显示和维护

操作	命令
显示LDP协议通告的PW标签相关信息	**display l2vpn ldp** [**peer** *ip-address* [**pw-id** *pw-id*] | **xconnect-group** *group-name*] [**verbose**]
显示交叉连接的转发信息（MSR 2600/MSR 3600）	**display l2vpn forwarding** { **ac** | **pw** } [**xconnect-group** *group-name*] [**verbose**]
显示交叉连接的转发信息（MSR 5600）	**display l2vpn forwarding** { **ac** | **pw** } [**xconnect-group** *group-name*] [**slot** *slot-number*] [**verbose**]
显示与交叉连接关联的三层接口的L2VPN信息	**display l2vpn interface** [**xconnect-group** *group-name* | *interface-type interface-number*]
显示L2VPN的PW信息	**display l2vpn pw** [**xconnect-group** *group-name*] [**protocol** { **bgp** | **ldp** | **static** }] [**verbose**]
显示PW模板的信息	**display l2vpn pw-class** [*class-name*]
显示交叉连接组的信息	**display l2vpn xconnect-group** [**name** *group-name*] [**verbose**]
显示MPLS L2VPN的标签块信息	**display l2vpn bgp** [**peer** *ip-address* | **local**] [**xconnect-group** *group-name*] [**verbose**]
显示BGP L2VPN对等体组的信息	**display bgp group l2vpn** [**group-name** *group-name*]
显示BGP协议的MPLS L2VPN标签块信息	**display bgp l2vpn signaling** [**peer** *ip-address* { **advertised** | **received** } [**statistics**] | **route-distinguisher** *route-distinguisher* [**site-id** *site-id* [**label-offset** *label-offset* [**advertise-info**]]] | **statistics**]
显示BGP L2VPN对等体的信息	**display bgp peer l2vpn** [**group-name** *group-name* **log-info** | *ip-address* { **log-info** | **verbose** } | **verbose**]
显示BGP L2VPN地址族下打包组的相关信息	**display bgp update-group l2vpn** [*ip-address*]

操作	命令
复位L2VPN地址族下的BGP会话	**reset bgp** { *as-number* | *ip-address* | **all** | **external** | **group** *group-name* | **internal** } **l2vpn**

1.11 MPLS L2VPN典型配置举例

1.11.1 本地交换配置举例

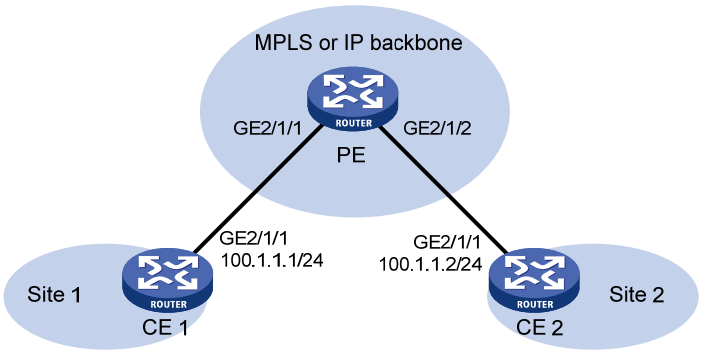
1. 组网需求

用户网络有两个站点，站点 CE 分别为 CE 1 和 CE 2。

通过在骨干网的 PE 上配置本地交换，连接 CE 1 的接口 GigabitEthernet2/1/1 与 CE 2 的接口 GigabitEthernet2/1/1，实现通过三层接口连接二层网络。

2. 组网图

图1-9 本地交换配置组网图



3. 配置步骤

(1) 配置 CE 1

```
<CE1> system-view
[CE1] interface gigabitethernet 2/1/1
[CE1-GigabitEthernet2/1/1] ip address 100.1.1.1 24
[CE1-GigabitEthernet2/1/1] quit
```

(2) 配置 CE 2

```
<CE2> system-view
[CE2] interface gigabitethernet 2/1/1
[CE2-GigabitEthernet2/1/1] ip address 100.1.1.2 24
[CE2-GigabitEthernet2/1/1] quit
```

(3) 配置 PE

使能 L2VPN。

```
<PE> system-view
[PE] l2vpn enable
```

创建交叉连接组 vpn1，在该交叉连接组内创建名称为 vpn1 的交叉连接，并将接口 GigabitEthernet2/1/1 和接口 GigabitEthernet2/1/2 关联，用来实现报文在这两个接口之间的本地交换。

```
[PE] xconnect-group vpn1
[PE-xcg-vpn1] connection vpn1
[PE-xcg-vpn1-vpn1] ac interface gigabitethernet 2/1/1
[PE-xcg-vpn1-vpn1] ac interface gigabitethernet 2/1/2
[PE-xcg-vpn1-vpn1] quit
```

4. 验证配置

在 PE 上查看 AC 转发表项，可以看到两条 AC 表项。

```
[PE] display l2vpn forwarding ac
Total number of cross-connections: 1
Total number of ACs: 2

AC                                  Xconnect-group                  Link ID
GE2/1/1                             vpn1                            0
GE2/1/2                             vpn1                            1
```

CE 1 与 CE 2 之间能够 ping 通。

1.11.2 本地交换IP异构配置举例

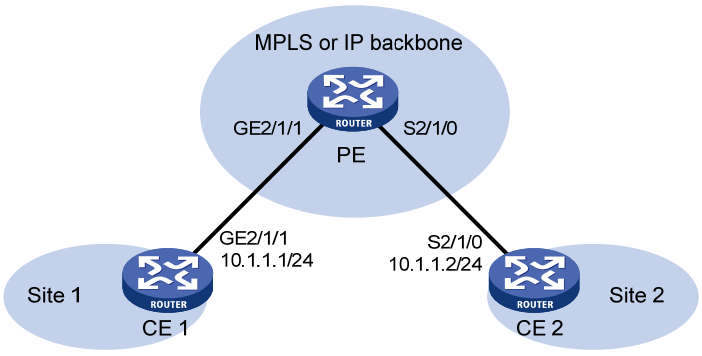
1. 组网需求

用户网络有两个站点，站点 CE 分别为 CE 1 和 CE 2。CE 1 与 PE 之间通过以太网接口相连。CE 2 与 PE 之间通过 Serial 接口相连，链路层封装 PPP。

通过在骨干网的 PE 上配置本地交换和异构网络互连，实现 CE 1 的接口 GigabitEthernet2/1/1 与 CE 2 的接口 Serial2/1/0 本地异构互联。

2. 组网图

图1-10 本地交换 IP 异构配置组网图



3. 配置步骤

(1) 配置 CE 1

```
<CE1> system-view
[CE1] interface gigabitethernet 2/1/1
```

```
[CE1-GigabitEthernet2/1/1] ip address 10.1.1.1 24
[CE1-GigabitEthernet2/1/1] quit
```

(2) 配置 CE 2

```
<CE2> system-view
[CE2] interface serial 2/1/0
[CE2-Serial2/1/0] link-protocol ppp
[CE2-Serial2/1/0] ip address 10.1.1.2 24
[CE2-Serial2/1/0] quit
```

(3) 配置 PE

使能 L2VPN。

```
<PE> system-view
[PE] l2vpn enable
```

在接入 CE 1 的接口 GigabitEthernet2/1/1 上配置缺省下一跳的 IP 地址为 10.1.1.1。此接口不需配置 IP 地址。

```
[PE] interface gigabitethernet 2/1/1
[PE-GigabitEthernet2/1/1] default-nexthop ip 10.1.1.1
[PE-GigabitEthernet2/1/1] quit
```

在接入 CE2 的接口 Serial2/1/0 上配置 IPCP 代理 IP 地址为远端 CE 1 的 IP 地址。此接口不需配置 IP 地址。

```
[PE] interface serial 2/1/0
[PE-Serial2/1/0] link-protocol ppp
[PE-Serial2/1/0] ppp ipcp proxy 10.1.1.1
[PE-Serial2/1/0] quit
```

创建交叉连接组 vpn1，在该交叉连接组内创建名称为 vpn1 的交叉连接，使能该交叉连接的异构互连功能，并将接口 GigabitEthernet2/1/1 和接口 Serial2/1/0 关联，以实现报文在这两个接口之间的本地交换。

```
[PE] xconnect-group vpn1
[PE-xcg-vpn1] connection vpn1
[PE-xcg-vpn1-vpn1] interworking ipv4
[PE-xcg-vpn1-vpn1] ac interface gigabitethernet 2/1/1
[PE-xcg-vpn1-vpn1] ac interface serial 2/1/0
[PE-xcg-vpn1-vpn1] quit
[PE-xcg-vpn1] quit
```

4. 验证配置

在 PE 上查看 AC 转发表项，可以看到两条 AC 表项。

```
[PE] display l2vpn forwarding ac
Total number of cross-connections: 1
Total number of ACs: 2

AC                              Xconnect-group                  Link ID
GE2/1/1                         vpn1                            0
S2/1/0                          vpn1                            1
```

CE 1 与 CE 2 之间能够 ping 通。

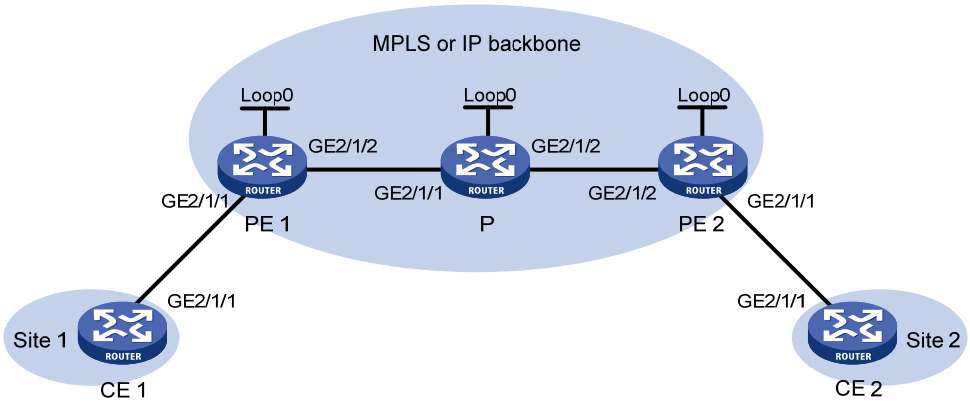
1.11.3 静态PW配置举例

1. 组网需求

用户网络有若干个站点，希望通过在骨干网上建立静态 PW，实现站点 1 与站点 2 互联。

2. 组网图

图1-11 静态 PW 配置组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	GE2/1/1	100.1.1.1/24	P	Loop0	192.4.4.4/32
PE 1	Loop0	192.2.2.2/32		GE2/1/1	10.1.1.2/24
	GE2/1/1	-		GE2/1/2	10.2.2.2/24
	GE2/1/2	10.1.1.1/24	PE 2	Loop0	192.3.3.3/32
CE 2	GE2/1/1	100.1.1.2/24		GE2/1/1	-
				GE2/1/2	10.2.2.1/24

3. 配置步骤

(1) 配置 CE 1

```
<CE1> system-view
[CE1] interface gigabitethernet 2/1/1
[CE1-GigabitEthernet2/1/1] ip address 100.1.1.1 24
[CE1-GigabitEthernet2/1/1] quit
```

(2) 配置 PE 1

配置 LSR ID。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 192.2.2.2 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 192.2.2.2
```

使能 L2VPN。

```
[PE1] l2vpn enable
```

全局使能 LDP。

```
[PE1] mpls ldp
[PE1-ldp] quit
```

配置连接 P 的接口 GigabitEthernet2/1/2，在此接口上使能 LDP。

```
[PE1] interface gigabitethernet 2/1/2
```

```
[PE1-GigabitEthernet2/1/2] ip address 10.1.1.1 24
[PE1-GigabitEthernet2/1/2] mpls enable
[PE1-GigabitEthernet2/1/2] mpls ldp enable
[PE1-GigabitEthernet2/1/2] quit
```

在 PE 1 上运行 OSPF，用于建立 LSP。

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 192.2.2.2 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

创建交叉连接组 vpna，在该交叉连接组内创建名称为 svc 的交叉连接，将接口 GigabitEthernet2/1/1 与此交叉连接关联，并在交叉连接内创建静态 PW，以便将 AC 和 PW 关联。

```
[PE1] xconnect-group vpna
[PE1-xcg-vpna] connection svc
[PE1-xcg-vpna-svc] ac interface gigabitethernet 2/1/1
[PE1-xcg-vpna-svc] peer 192.3.3.3 pw-id 3 in-label 100 out-label 200
[PE1-xcg-vpna-svc-192.3.3.3-3] quit
[PE1-xcg-vpna-svc] quit
[PE1-xcg-vpna] quit
```

(3) 配置 P

配置 LSR ID。

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 192.4.4.4 32
[P-LoopBack0] quit
[P] mpls lsr-id 192.4.4.4
```

全局使能 LDP。

```
[P] mpls ldp
[P-ldp] quit
```

配置连接 PE 1 的接口 GigabitEthernet2/1/1，在此接口上使能 LDP。

```
[P] interface gigabitethernet 2/1/1
[P-GigabitEthernet2/1/1] ip address 10.1.1.2 24
[P-GigabitEthernet2/1/1] mpls enable
[P-GigabitEthernet2/1/1] mpls ldp enable
[P-GigabitEthernet2/1/1] quit
```

配置连接 PE 2 的接口 GigabitEthernet2/1/2，在此接口上使能 LDP。

```
[P] interface gigabitethernet 2/1/2
[P-GigabitEthernet2/1/2] ip address 10.2.2.2 24
[P-GigabitEthernet2/1/2] mpls enable
[P-GigabitEthernet2/1/2] mpls ldp enable
[P-GigabitEthernet2/1/2] quit
```

在 P 上运行 OSPF，用于建立 LSP。

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.2 0.0.0.255
```

```
[P-ospf-1-area-0.0.0.0] network 10.2.2.2 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 192.4.4.4 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

(4) 配置 PE 2

配置 LSR ID。

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 192.3.3.3 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 192.3.3.3
```

使能 L2VPN。

```
[PE2] l2vpn enable
```

全局使能 LDP。

```
[PE2] mpls ldp
[PE2-ldp] quit
```

配置连接 P 的接口 GigabitEthernet2/1/2，在此接口上使能 LDP。

```
[PE2] interface gigabitethernet 2/1/2
[PE2-GigabitEthernet2/1/2] ip address 10.2.2.1 24
[PE2-GigabitEthernet2/1/2] mpls enable
[PE2-GigabitEthernet2/1/2] mpls ldp enable
[PE2-GigabitEthernet2/1/2] quit
```

在 PE 2 上运行 OSPF，用于建立 LSP。

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 10.2.2.1 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 192.3.3.3 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

创建交叉连接组 vpna，在该交叉连接组内创建名称为 svc 的交叉连接，将接口 GigabitEthernet2/1/1 与此交叉连接关联，并在交叉连接内创建静态 PW，以便将 AC 和 PW 关联。

```
[PE2] xconnect-group vpna
[PE2-xcg-vpna] connection svc
[PE2-xcg-vpna-svc] ac interface gigabitethernet 2/1/1
[PE2-xcg-vpna-svc] peer 192.2.2.2 pw-id 3 in-label 200 out-label 100
[PE2-xcg-vpna-svc-192.2.2.2-3] quit
[PE2-xcg-vpna-svc] quit
[PE2-xcg-vpna] quit
```

(5) 配置 CE 2

```
<CE2> system-view
[CE2] interface gigabitethernet 2/1/1
[CE2-GigabitEthernet2/1/1] ip address 100.1.1.2 24
[CE2-GigabitEthernet2/1/1] quit
```

4. 验证配置

在 PE 1 上查看 PW 信息，可以看到建立了一条静态 PW。

```
[PE1] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1, 1 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpna
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
192.3.3.3       3          100/200         Static M     0          Up
```

在 PE 2 上也可以看到静态 PW 的信息。

```
[PE2] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1, 1 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpna
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
192.2.2.2       3          200/100         Static M     0          Up
```

CE 1 与 CE 2 之间能够 ping 通。

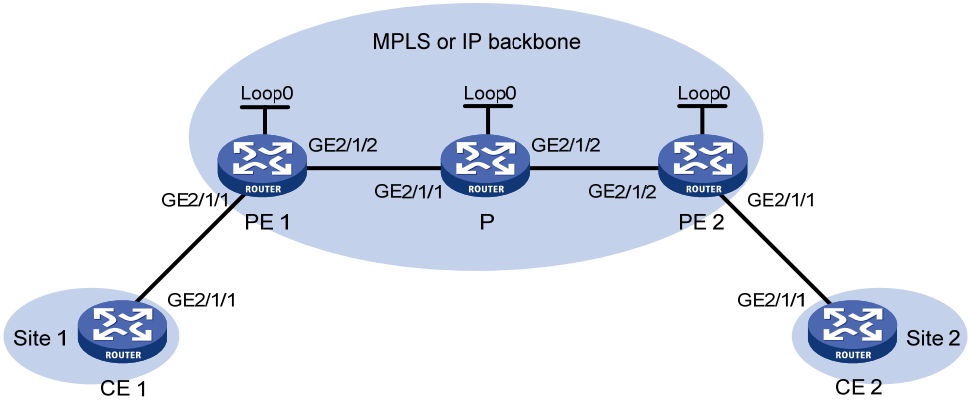
1.11.4 LDP PW配置举例

1. 组网需求

用户网络有若干个站点，希望通过在骨干网上建立 LDP PW，实现站点 1 与站点 2 互联。

2. 组网图

图1-12 LDP PW 配置组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	GE2/1/1	100.1.1.1/24	P	Loop0	192.4.4.4/32
PE 1	Loop0	192.2.2.2/32		GE2/1/1	10.1.1.2/24
	GE2/1/1	-		GE2/1/2	10.2.2.2/24
	GE2/1/2	10.1.1.1/24	PE 2	Loop0	192.3.3.3/32
CE 2	GE2/1/1	100.1.1.2/24		GE2/1/1	-
				GE2/1/2	10.2.2.1/24

3. 配置步骤

(1) 配置 CE 1

```
<CE1> system-view
[CE1] interface gigabitethernet 2/1/1
```

```
[CE1-GigabitEthernet2/1/1] ip address 100.1.1.1 24
[CE1-GigabitEthernet2/1/1] quit
```

(2) 配置 PE 1

配置 LSR ID。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 192.2.2.2 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 192.2.2.2
```

使能 L2VPN。

```
[PE1] l2vpn enable
```

全局使能 LDP。

```
[PE1] mpls ldp
[PE1-ldp] quit
```

配置连接 P 的接口 GigabitEthernet2/1/2，在此接口上使能 LDP。

```
[PE1] interface gigabitethernet 2/1/2
[PE1-GigabitEthernet2/1/2] ip address 10.1.1.1 24
[PE1-GigabitEthernet2/1/2] mpls enable
[PE1-GigabitEthernet2/1/2] mpls ldp enable
[PE1-GigabitEthernet2/1/2] quit
```

在 PE 1 上运行 OSPF，用于建立 LSP。

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 192.2.2.2 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

创建交叉连接组 vpna，在该交叉连接组内创建名称为 ldp 的交叉连接，将接口 GigabitEthernet2/1/1 与此交叉连接关联，并在交叉连接内创建 LDP PW，以便将 AC 和 PW 关联。

```
[PE1] xconnect-group vpna
[PE1-xcg-vpna] connection ldp
[PE1-xcg-vpna-ldp] ac interface gigabitethernet 2/1/1
[PE1-xcg-vpna-ldp] peer 192.3.3.3 pw-id 3
[PE1-xcg-vpna-ldp-192.3.3.3-3] quit
[PE1-xcg-vpna-ldp] quit
[PE1-xcg-vpna] quit
```

(3) 配置 P

配置 LSR ID。

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 192.4.4.4 32
[P-LoopBack0] quit
[P] mpls lsr-id 192.4.4.4
```

全局使能 LDP。

```
[P] mpls ldp
[P-ldp] quit
```

配置连接 PE 1 的接口 GigabitEthernet2/1/1，在此接口上使能 LDP。

```
[P] interface gigabitethernet 2/1/1
[P-GigabitEthernet2/1/1] ip address 10.1.1.2 24
[P-GigabitEthernet2/1/1] mpls enable
[P-GigabitEthernet2/1/1] mpls ldp enable
[P-GigabitEthernet2/1/1] quit
```

配置连接 PE 2 的接口 GigabitEthernet2/1/2，在此接口上使能 LDP。

```
[P] interface gigabitethernet 2/1/2
[P-GigabitEthernet2/1/2] ip address 10.2.2.2 24
[P-GigabitEthernet2/1/2] mpls enable
[P-GigabitEthernet2/1/2] mpls ldp enable
[P-GigabitEthernet2/1/2] quit
```

在 P 上运行 OSPF，用于建立 LSP。

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.2 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.2.2.2 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 192.4.4.4 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

(4) 配置 PE 2

配置 LSR ID。

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 192.3.3.3 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 192.3.3.3
```

使能 L2VPN。

```
[PE2] l2vpn enable
```

全局使能 LDP。

```
[PE2] mpls ldp
[PE2-ldp] quit
```

配置连接 P 的接口 GigabitEthernet2/1/2，在此接口上使能 LDP。

```
[PE2] interface gigabitethernet 2/1/2
[PE2-GigabitEthernet2/1/2] ip address 10.2.2.1 24
[PE2-GigabitEthernet2/1/2] mpls enable
[PE2-GigabitEthernet2/1/2] mpls ldp enable
[PE2-GigabitEthernet2/1/2] quit
```

在 PE 2 上运行 OSPF，用于建立 LSP。

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 192.3.3.3 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 10.2.2.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

创建交叉连接组 vpna，在该交叉连接组内创建名称为 ldp 的交叉连接，将接口 GigabitEthernet2/1/1 与此交叉连接关联，并在交叉连接内创建 LDP PW，以便将 AC 和 PW 关联。

```
[PE2] xconnect-group vpna
[PE2-xcg-vpna] connection ldp
[PE2-xcg-vpna-ldp] ac interface gigabitethernet 2/1/1
[PE2-xcg-vpna-ldp] peer 192.2.2.2 pw-id 3
[PE2-xcg-vpna-ldp-192.2.2.2-3] quit
[PE2-xcg-vpna-ldp] quit
[PE2-xcg-vpna] quit
```

(5) 配置 CE 2

```
<CE2> system-view
[CE2] interface gigabitethernet 2/1/1
[CE2-GigabitEthernet2/1/1] ip address 100.1.1.2 24
[CE2-GigabitEthernet2/1/1] quit
```

4. 验证配置

在 PE 1 上查看 PW 信息，可以看到建立了一条 LDP PW。

```
[PE1] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1, 1 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpna
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
192.3.3.3       3          1279/1279       LDP    M     1          Up
```

在 PE 2 上也可以看到 LDP PW 信息。

```
[PE2] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1, 1 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpna
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
192.2.2.2       3          1279/1279       LDP    M     1          Up
```

CE 1 与 CE 2 之间能够 ping 通。

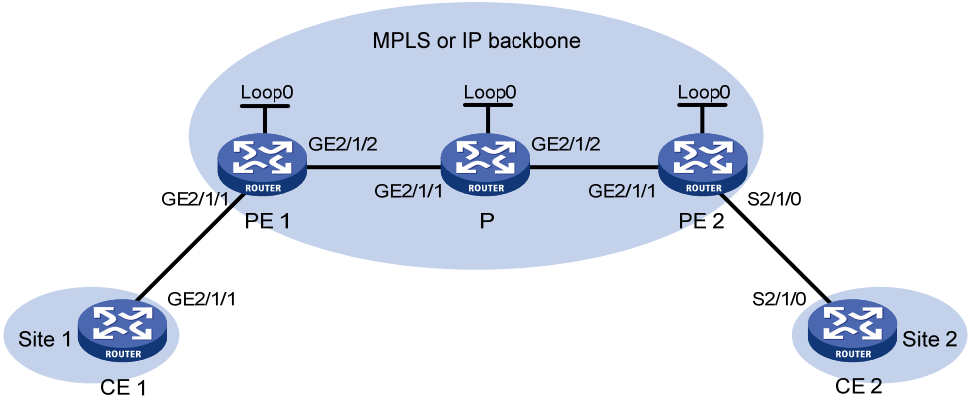
1.11.5 LDP方式IP异构连接配置举例

1. 组网需求

用户网络有若干个站点，CE 1 与 PE 1 之间通过以太网接口相连。CE 2 与 PE 2 之间通过 Serial 接口相连，链路层封装 PPP。通过在骨干网上建立 LDP PW，并配置异构网络互连，实现 CE 1 的接口 GigabitEthernet2/1/1 与 CE 2 的接口 Serial2/1/0 异构互联。

2. 组网图

图1-13 LDP 方式 IP 异构配置组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	GE2/1/1	100.1.1.1/24	P	Loop0	192.4.4.4/32
PE 1	Loop0	192.2.2.2/32		GE2/1/1	10.1.1.2/24
	GE2/1/1	-		GE2/1/2	10.2.2.2/24
	GE2/1/2	10.1.1.1/24	PE 2	Loop0	192.3.3.3/32
CE 2	S2/1/0	100.1.1.2/24		S2/1/0	-
				GE2/1/1	10.2.2.1/24

3. 配置步骤

(1) 配置 CE 1

```
<CE1> system-view
[CE1] interface gigabitethernet 2/1/1
[CE1-GigabitEthernet2/1/1] ip address 100.1.1.1 24
[CE1-GigabitEthernet2/1/1] quit
```

(2) 配置 PE 1

配置 LSR ID。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 192.2.2.2 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 192.2.2.2
```

使能 L2VPN。

```
[PE1] l2vpn enable
```

全局使能 LDP。

```
[PE1] mpls ldp
[PE1-ldp] quit
```

在接入 CE 1 的接口 GigabitEthernet2/1/1 上配置缺省下一跳的 IP 地址为 100.1.1.1。此接口不需配置 IP 地址。

```
[PE1] interface gigabitethernet 2/1/1
[PE1-GigabitEthernet2/1/1] default-nexthop ip 100.1.1.1
[PE1-GigabitEthernet2/1/1] quit
```

配置连接 P 的接口 GigabitEthernet2/1/2，在此接口上使能 LDP。

```
[PE1] interface gigabitethernet 2/1/2
```

```
[PE1-GigabitEthernet2/1/2] ip address 10.1.1.1 24
[PE1-GigabitEthernet2/1/2] mpls enable
[PE1-GigabitEthernet2/1/2] mpls ldp enable
[PE1-GigabitEthernet2/1/2] quit
```

在 PE 1 上运行 OSPF，用于建立 LSP。

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 192.2.2.2 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

创建交叉连接组 vpna，在该交叉连接组内创建名称为 ldp 的交叉连接，使能该交叉连接的异构互连功能，将接口 GigabitEthernet2/1/1 与此交叉连接关联，并在交叉连接内创建 LDP PW，以便将 AC 和 PW 关联。

```
[PE1] xconnect-group vpna
[PE1-xcg-vpna] connection ldp
[PE1-xcg-vpna-ldp] interworking ipv4
[PE1-xcg-vpna-ldp] ac interface gigabitethernet 2/1/1
[PE1-xcg-vpna-ldp] peer 192.3.3.3 pw-id 3
[PE1-xcg-vpna-ldp-192.3.3.3-3] quit
[PE1-xcg-vpna-ldp] quit
[PE1-xcg-vpna] quit
```

(3) 配置 P

配置 LSR ID。

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 192.4.4.4 32
[P-LoopBack0] quit
[P] mpls lsr-id 192.4.4.4
```

全局使能 LDP。

```
[P] mpls ldp
[P-ldp] quit
```

配置连接 PE 1 的接口 GigabitEthernet2/1/1，在此接口上使能 LDP。

```
[P] interface gigabitethernet 2/1/1
[P-GigabitEthernet2/1/1] ip address 10.1.1.2 24
[P-GigabitEthernet2/1/1] mpls enable
[P-GigabitEthernet2/1/1] mpls ldp enable
[P-GigabitEthernet2/1/1] quit
```

配置连接 PE 2 的接口 GigabitEthernet2/1/2，在此接口上使能 LDP。

```
[P] interface gigabitethernet 2/1/2
[P-GigabitEthernet2/1/2] ip address 10.2.2.2 24
[P-GigabitEthernet2/1/2] mpls enable
[P-GigabitEthernet2/1/2] mpls ldp enable
[P-GigabitEthernet2/1/2] quit
```

在 P 上运行 OSPF，用于建立 LSP。

```
[P] ospf
```

```
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.2 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.2.2.2 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 192.4.4.4 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

(4) 配置 PE 2

配置 LSR ID。

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 192.3.3.3 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 192.3.3.3
```

使能 L2VPN。

```
[PE2] l2vpn enable
```

全局使能 LDP。

```
[PE2] mpls ldp
[PE2-ldp] quit
```

配置连接 P 的接口 GigabitEthernet2/1/1，在此接口上使能 LDP。

```
[PE2] interface gigabitethernet 2/1/1
[PE2-GigabitEthernet2/1/1] ip address 10.2.2.1 24
[PE2-GigabitEthernet2/1/1] mpls enable
[PE2-GigabitEthernet2/1/1] mpls ldp enable
[PE2-GigabitEthernet2/1/1] quit
```

在 PE 2 上运行 OSPF，用于建立 LSP。

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 192.3.3.3 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 10.2.2.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

在接入 CE 2 的接口 Serial2/1/0 上配置 IPCP 代理 IP 地址为远端 CE 1 的 IP 地址。此接口不需配置 IP 地址。

```
[PE2] interface serial 2/1/0
[PE2-Serial2/1/0] link-protocol ppp
[PE2-Serial2/1/0] ppp ipcp proxy 100.1.1.1
[PE2-Serial2/1/0] quit
```

创建交叉连接组 vpna，在该交叉连接组内创建名称为 ldp 的交叉连接，使能该交叉连接的异构互连功能，将接口 Serial2/1/0 与此交叉连接关联，并在交叉连接内创建 LDP PW，以便将 AC 和 PW 关联。

```
[PE2] xconnect-group vpna
[PE2-xcg-vpna] connection ldp
[PE2-xcg-vpna-ldp] interworking ipv4
[PE2-xcg-vpna-ldp] ac interface serial 2/1/0
[PE2-xcg-vpna-ldp] peer 192.2.2.2 pw-id 3
[PE2-xcg-vpna-ldp-192.2.2.2-3] quit
```

```
[PE2-xcg-vpna-ldp] quit
[PE2-xcg-vpna] quit
```

(5) 配置 CE 2

```
<CE2> system-view
[CE2] interface serial 2/1/0
[CE2-Serial2/1/0] link-protocol ppp
[CE2-Serial2/1/0] ip address 100.1.1.2 24
[CE2-Serial2/1/0] quit
```

4. 验证配置

在 PE 1 上查看 PW 信息，可以看到建立了一条 LDP PW。

```
[PE1] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1, 1 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpna
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
192.3.3.3       3          1279/1279       LDP    M     1          Up
```

在 PE 2 上也可以看到 LDP PW 信息。

```
[PE2] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1, 1 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpna
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
192.2.2.2       3          1279/1279       LDP    M     1          Up
```

CE 1 与 CE 2 之间能够 ping 通。

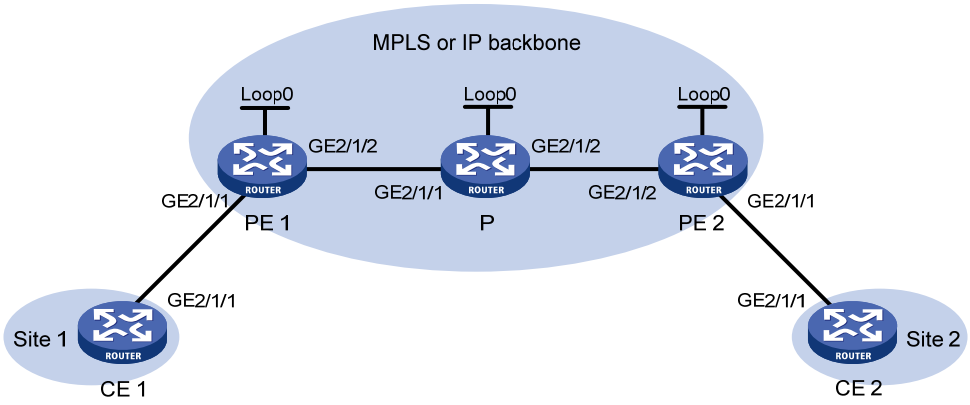
1.11.6 BGP PW配置举例

1. 组网需求

用户网络有若干个站点，希望通过在骨干网上建立 BGP PW，实现站点 1 与站点 2 互联。

2. 组网图

图1-14 BGP PW 配置组网图



设备	接口	IP地址	设备	接口	IP地址

CE 1	GE2/1/1	100.1.1.1/24	P	Loop0	192.4.4.4/32
PE 1	Loop0	192.2.2.2/32		GE2/1/1	10.1.1.2/24
	GE2/1/1	-		GE2/1/2	10.2.2.2/24
	GE2/1/2	10.1.1.1/24	PE 2	Loop0	192.3.3.3/32
CE 2	GE2/1/1	100.1.1.2/24		GE2/1/1	-
				GE2/1/2	10.2.2.1/24

3. 配置步骤

(1) 配置 CE 1

```
<CE1> system-view
[CE1] interface gigabitethernet 2/1/1
[CE1-GigabitEthernet2/1/1] ip address 100.1.1.1 24
[CE1-GigabitEthernet2/1/1] quit
```

(2) 配置 PE 1

配置 LSR ID。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 192.2.2.2 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 192.2.2.2
```

使能 L2VPN。

```
[PE1] l2vpn enable
```

全局使能 LDP。

```
[PE1] mpls ldp
[PE1-ldp] quit
```

配置连接 P 的接口 GigabitEthernet2/1/2，在此接口上使能 LDP。

```
[PE1] interface gigabitethernet 2/1/2
[PE1-GigabitEthernet2/1/2] ip address 10.1.1.1 24
[PE1-GigabitEthernet2/1/2] mpls enable
[PE1-GigabitEthernet2/1/2] mpls ldp enable
[PE1-GigabitEthernet2/1/2] quit
```

在 PE 1 上运行 OSPF，用于建立 LSP。

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 192.2.2.2 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

在 PE 1 和 PE 2 之间建立 IBGP 连接，并配置在二者之间通过 BGP 发布 L2VPN 信息。

```
[PE1] bgp 100
[PE1-bgp] peer 192.3.3.3 as-number 100
[PE1-bgp] peer 192.3.3.3 connect-interface loopback 0
[PE1-bgp] address-family l2vpn
[PE1-bgp-l2vpn] peer 192.3.3.3 enable
[PE1-bgp-l2vpn] quit
[PE1-bgp] quit
```

创建交叉连接组 vpnb，在该交叉连接组内创建本地站点 1，在本地站点 1 和远端站点 2 之间建立 BGP PW，并将接口 GigabitEthernet2/1/1 与此 PW 关联。

```
[PE1] xconnect-group vpnb
[PE1-xcg-vpnb] auto-discovery bgp
[PE1-xcg-vpnb-auto] route-distinguisher 2:2
[PE1-xcg-vpnb-auto] vpn-target 2:2 export-extcommunity
[PE1-xcg-vpnb-auto] vpn-target 2:2 import-extcommunity
[PE1-xcg-vpnb-auto] site 1 range 10 default-offset 0
[PE1-xcg-vpnb-auto-1] connection remote-site-id 2
[PE1-xcg-vpnb-auto-1-2] ac interface gigabitethernet 2/1/1
[PE1-xcg-vpnb-auto-1-2] return
```

(3) 配置 P

配置 LSR ID。

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 192.4.4.4 32
[P-LoopBack0] quit
[P] mpls lsr-id 192.4.4.4
```

全局使能 LDP。

```
[P] mpls ldp
[P-ldp] quit
```

配置连接 PE 1 的接口 GigabitEthernet2/1/1，在此接口上使能 LDP。

```
[P] interface gigabitethernet 2/1/1
[P-GigabitEthernet2/1/1] ip address 10.1.1.2 24
[P-GigabitEthernet2/1/1] mpls enable
[P-GigabitEthernet2/1/1] mpls ldp enable
[P-GigabitEthernet2/1/1] quit
```

配置连接 PE 2 的接口 GigabitEthernet2/1/2，在此接口上使能 LDP。

```
[P] interface gigabitethernet 2/1/2
[P-GigabitEthernet2/1/2] ip address 10.2.2.2 24
[P-GigabitEthernet2/1/2] mpls enable
[P-GigabitEthernet2/1/2] mpls ldp enable
[P-GigabitEthernet2/1/2] quit
```

在 P 上运行 OSPF，用于建立 LSP。

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.2 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.2.2.2 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 192.4.4.4 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

(4) 配置 PE 2

配置 LSR ID。

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 192.3.3.3 32
```

```
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 192.3.3.3
```
使能 L2VPN。
```
[PE2] l2vpn enable
```
全局使能 LDP。
```
[PE2] mpls ldp
[PE2-ldp] quit
```
配置连接 P 的接口 GigabitEthernet2/1/2，在此接口上使能 LDP。
```
[PE2] interface gigabitethernet 2/1/2
[PE2-GigabitEthernet2/1/2] ip address 10.2.2.1 24
[PE2-GigabitEthernet2/1/2] mpls enable
[PE2-GigabitEthernet2/1/2] mpls ldp enable
[PE2-GigabitEthernet2/1/2] quit
```
在 PE 2 上运行 OSPF，用于建立 LSP。
```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 192.3.3.3 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 10.2.2.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```
在 PE 1 和 PE 2 之间建立 IBGP 连接，并配置在二者之间通过 BGP 发布 L2VPN 信息。
```
[PE2] bgp 100
[PE2-bgp] peer 192.2.2.2 as-number 100
[PE2-bgp] peer 192.2.2.2 connect-interface loopback 0
[PE2-bgp] address-family l2vpn
[PE2-bgp-l2vpn] peer 192.2.2.2 enable
[PE2-bgp-l2vpn] quit
[PE2-bgp] quit
```
创建交叉连接组 vpnb，在该交叉连接组内创建本地站点 2，在本地站点 2 和远端站点 1 之间建立 BGP PW，并将接口 GigabitEthernet2/1/1 与此 PW 关联。
```
[PE2] xconnect-group vpnb
[PE2-xcg-vpnb] auto-discovery bgp
[PE2-xcg-vpnb-auto] route-distinguisher 2:2
[PE2-xcg-vpnb-auto] vpn-target 2:2 export-extcommunity
[PE2-xcg-vpnb-auto] vpn-target 2:2 import-extcommunity
[PE2-xcg-vpnb-auto] site 2 range 10 default-offset 0
[PE2-xcg-vpnb-auto-2] connection remote-site-id 1
[PE2-xcg-vpnb-auto-2-1] ac interface gigabitethernet 2/1/1
[PE2-xcg-vpnb-auto-2-1] return
```
(5) 配置 CE 2
```
<CE2> system-view
[CE2] interface gigabitethernet 2/1/1
[CE2-GigabitEthernet2/1/1] ip address 100.1.1.2 24
[CE2-GigabitEthernet2/1/1] quit
```
4. 验证配置
在 PE 1 上查看 PW 信息，可以看到建立了一条 BGP PW。

```
<PE1> display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1, 1 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpnb
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
192.3.3.3       2                 1036/1025       BGP     M     1        Up
```

在 PE 2 上也可以看到 PW 信息。

```
<PE2> display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1, 1 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpnb
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
192.2.2.2       1                 1025/1036       BGP     M     1        Up
```

CE 1 与 CE 2 之间能够 ping 通。

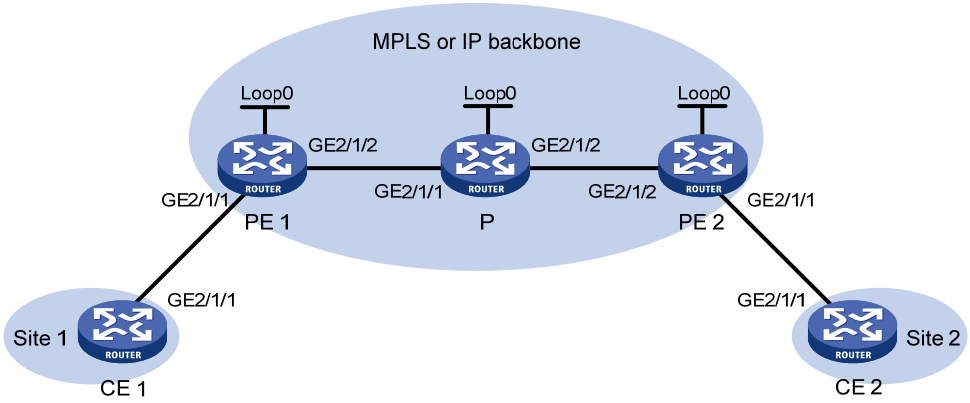
1.11.7 CCC远程连接配置举例

1. 组网需求

用户网络有若干个站点，希望通过在骨干网上建立 CCC 远程连接，实现站点 1 与站点 2 互联。

2. 组网图

图1-15 CCC 远程连接配置组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	GE2/1/1	100.1.1.1/24	P	Loop0	192.4.4.4/32
PE 1	Loop0	192.2.2.2/32		GE2/1/1	10.1.1.2/24
	GE2/1/1	-		GE2/1/2	10.2.2.2/24
	GE2/1/2	10.1.1.1/24	PE 2	Loop0	192.3.3.3/32
CE 2	GE2/1/1	100.1.1.2/24		GE2/1/1	-
				GE2/1/2	10.2.2.1/24

3. 配置步骤

(1) 配置 CE 1

```
<CE1> system-view
[CE1] interface gigabitethernet 2/1/1
```

```
[CE1-GigabitEthernet2/1/1] ip address 100.1.1.1 24
[CE1-GigabitEthernet2/1/1] quit
```

(2) 配置 PE 1

配置 LSR ID。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 192.2.2.2 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 192.2.2.2
```

使能 L2VPN。

```
[PE1] l2vpn enable
```

配置连接 P 的接口 GigabitEthernet2/1/2，在此接口上使能 MPLS。

```
[PE1] interface gigabitethernet 2/1/2
[PE1-GigabitEthernet2/1/2] ip address 10.1.1.1 24
[PE1-GigabitEthernet2/1/2] mpls enable
[PE1-GigabitEthernet2/1/2] quit
```

在 PE 1 上运行 OSPF，用于发布路由。

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 192.2.2.2 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

创建交叉连接组 ccc，在该交叉连接组内创建 CCC 远程连接（入标签为 101、出标签为 201、下一跳地址为 10.1.1.2），并将接口 GigabitEthernet2/1/1 与此 CCC 远程连接关联。

```
[PE1] xconnect-group ccc
[PE1-xcg-ccc] connection ccc
[PE1-xcg-ccc-ccc] ccc in-label 101 out-label 201 nexthop 10.1.1.2
[PE1-xcg-ccc-ccc] ac interface gigabitethernet 2/1/1
[PE1-xcg-ccc-ccc] quit
[PE1-xcg-ccc] quit
```

(3) 配置 P

配置 LSR ID。

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 192.4.4.4 32
[P-LoopBack0] quit
[P] mpls lsr-id 192.4.4.4
```

配置连接 PE 1 的接口 GigabitEthernet2/1/1，在此接口上使能 MPLS。

```
[P] interface gigabitethernet 2/1/1
[P-GigabitEthernet2/1/1] ip address 10.1.1.2 24
[P-GigabitEthernet2/1/1] mpls enable
[P-GigabitEthernet2/1/1] quit
```

配置连接 PE 2 的接口 GigabitEthernet2/1/2，在此接口上使能 MPLS。

```
[P] interface gigabitethernet 2/1/2
[P-GigabitEthernet2/1/2] ip address 10.2.2.2 24
```

```
[P-GigabitEthernet2/1/2] mpls enable
[P-GigabitEthernet2/1/2] quit
```

配置一条静态 LSP 用于转发由 PE 1 去往 PE 2 的报文。

```
[P] static-lsp transit pe1-pe2 in-label 201 nexthop 10.2.2.1 out-label 202
```

配置另一条静态 LSP 用于转发由 PE 2 去往 PE 1 的报文。

```
[P] static-lsp transit pe2-pe1 in-label 102 nexthop 10.1.1.1 out-label 101
```

在 P 上运行 OSPF，用于发布路由。

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.2 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.2.2.2 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 192.4.4.4 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

(4) 配置 PE 2

配置 LSR ID。

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 192.3.3.3 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 192.3.3.3
```

使能 L2VPN。

```
[PE2] l2vpn enable
```

配置连接 P 的接口 GigabitEthernet2/1/2，在此接口上使能 MPLS。

```
[PE2] interface gigabitethernet 2/1/2
[PE2-GigabitEthernet2/1/2] ip address 10.2.2.1 24
[PE2-GigabitEthernet2/1/2] mpls enable
[PE2-GigabitEthernet2/1/2] quit
```

在 PE 2 上运行 OSPF，用于发布路由。

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 10.2.2.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 192.3.3.3 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

创建交叉连接组 ccc，在该交叉连接组内创建 CCC 远程连接（入标签为 202、出标签为 102、下一跳地址为 10.2.2.2），并将接口 GigabitEthernet2/1/1 与此 CCC 远程连接关联。

```
[PE2] xconnect-group ccc
[PE2-xcg-ccc] connection ccc
[PE2-xcg-ccc-ccc] ccc in-label 202 out-label 102 nexthop 10.2.2.2
[PE2-xcg-ccc-ccc] ac interface gigabitethernet 2/1/1
[PE2-xcg-ccc-ccc] quit
[PE2-xcg-ccc] quit
```

(5) 配置 CE 2

```
<CE2> system-view
[CE2] interface gigabitethernet 2/1/1
```

```
[CE2-GigabitEthernet2/1/1] ip address 100.1.1.2 24
[CE2-GigabitEthernet2/1/1] quit
```

4. 验证配置

在 PE 1 上查看 PW 信息，可以看到建立了一条 PW 连接。PW ID/Rmt Site 字段为“-”，Protoc 字段为“Static”，表示该 PW 连接为 CCC 远程连接。

```
[PE1] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1, 1 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: ccc
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
10.1.1.2        -                 101/201         Static  M     0        Up
```

在 PE 2 上也可以看到 PW 信息。

```
[PE2] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1, 1 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: ccc
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
10.2.2.2        -                 202/102         Static  M     0        Up
```

CE 1 与 CE 2 之间能够 ping 通。

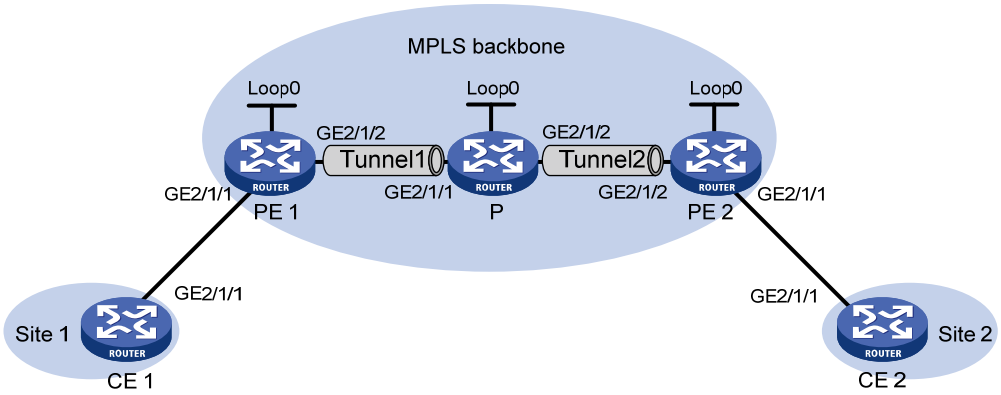
1.11.8 域内多段PW配置举例

1. 组网需求

在 图 1-16 中，PE 1 和P、P和PE 2 之间分别建立了一条MPLS TE隧道，但是在PE 1 和PE 2 之间未建立MPLS TE隧道。通过配置域内多段PW：P与PE 1 之间建立LDP PW、P与PE 2 之间建立静态PW、在P上将两条PW关联，可以实现在PE 1 和PE 2 之间不存在公网隧道的情况下间接在PE 1 和PE 2 之间建立连接，确保CE 1 和CE 2 的二层报文跨越骨干网传送。

2. 组网图

图1-16 域内多段 PW 配置组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	GE2/1/1	100.1.1.1/24	P	Loop0	192.4.4.4/32
PE 1	Loop0	192.2.2.2/32		GE2/1/1	23.1.1.2/24

	GE2/1/2	23.1.1.1/24		GE2/1/2	26.2.2.2/24
CE 2	GE2/1/1	100.1.1.2/24	PE 2	Loop0	192.3.3.3/32
				GE2/1/2	26.2.2.1/24

3. 配置步骤

(1) 配置 CE 1

```
<CE1> system-view
[CE1] interface gigabitethernet 2/1/1
[CE1-GigabitEthernet2/1/1] ip address 100.1.1.1 24
[CE1-GigabitEthernet2/1/1] quit
```

(2) 配置 PE 1

配置 LSR ID。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 192.2.2.2 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 192.2.2.2
```

使能 L2VPN。

```
[PE1] l2vpn enable
```

配置 MPLS TE，以便在 PE 1 和 P 之间建立 MPLS TE 隧道。详细配置过程，请参见“MPLS 配置指导”中的“MPLS TE”。

创建交叉连接组 vpn1，在该交叉连接组内创建名称为 ldp 的交叉连接，将接口 GigabitEthernet2/1/1 与此交叉连接关联，并在交叉连接内创建 LDP PW，以实现 AC 和 PW 关联。

```
[PE1] xconnect-group vpn1
[PE1-xcg-vpn1] connection ldp
[PE1-xcg-vpn1-ldp] ac interface gigabitethernet 2/1/1
[PE1-xcg-vpn1-ldp] peer 192.4.4.4 pw-id 1000
[PE1-xcg-vpn1-ldp-192.4.4.4-1000] quit
[PE1-xcg-vpn1-ldp] quit
[PE1-xcg-vpn1] quit
```

(3) 配置 P

配置 LSR ID。

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 192.4.4.4 32
[P-LoopBack0] quit
[P] mpls lsr-id 192.4.4.4
```

使能 L2VPN。

```
[P] l2vpn enable
```

创建 PW 模版，配置 PW 数据封装类型为 Ethernet。

```
[P] pw-class pwa
[P-pw-pwa] pw-type ethernet
[P-pw-pwa] quit
```

配置 MPLS TE，以便在 PE 1 和 P、P 和 PE 2 之间建立 MPLS TE 隧道。详细配置过程，请参见“MPLS 配置指导”中的“MPLS TE”。

创建交叉连接组 vpn1，在该交叉连接组内创建名称为 ldpsvc 的交叉连接，在交叉连接内创建一条 LDP PW 和一条静态 PW，将这两条 PW 关联，以便建立多段 PW。

```
[P] xconnect-group vpn1
[P-xcg-vpn1] connection ldpsvc
[P-xcg-vpn1-ldpsvc] peer 192.2.2.2 pw-id 1000 pw-class pwa
[P-xcg-vpn1-ldpsvc-192.2.2.2-1000] quit
[P-xcg-vpn1-ldpsvc] peer 192.3.3.3 pw-id 1000 in-label 100 out-label 200 pw-class pwa
[P-xcg-vpn1-ldpsvc-192.3.3.3-1000] quit
[P-xcg-vpn1-ldpsvc] quit
[P-xcg-vpn1] quit
```

(4) 配置 PE 2

配置 LSR ID。

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 192.3.3.3 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 192.3.3.3
```

使能 L2VPN。

```
[PE2] l2vpn enable
```

配置 MPLS TE，以便在 P 和 PE 2 之间建立 MPLS TE 隧道。详细配置过程，请参见“MPLS 配置指导”中的“MPLS TE”。

创建交叉连接组 vpn1，在该交叉连接组内创建名称为 svc 的交叉连接，将接口 GigabitEthernet2/1/1 与此交叉连接关联，并在交叉连接内创建静态 PW，以实现 AC 和 PW 关联。

```
[PE2] xconnect-group vpn1
[PE2-xcg-vpn1] connection svc
[PE2-xcg-vpn1-svc] ac interface gigabitethernet 2/1/1
[PE2-xcg-vpn1-svc] peer 192.4.4.4 pw-id 1000 in-label 200 out-label 100
[PE2-xcg-vpn1-svc-192.4.4.4-1000] quit
[PE2-xcg-vpn1-svc] quit
[PE2-xcg-vpn1] quit
```

(5) 配置 CE 2

```
<CE2> system-view
[CE2] interface gigabitethernet 2/1/1
[CE2-GigabitEthernet2/1/1] ip address 100.1.1.2 24
[CE2-GigabitEthernet2/1/1] quit
```

4. 验证配置

在 P 上查看 PW 信息，可以看到建立了两条 PW 连接，构成了多段 PW。

```
[P] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 2, 2 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpn1
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
192.2.2.2       1000       1279/1150       LDP    M     0          Up
192.3.3.3       1000       100/200         Static M     1          Up
```

在 PE 1 上也可以看到 PW 信息。

```
[PE1] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1, 1 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpn1
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
192.4.4.4       1000       1150/1279       LDP    M     1          Up
```

在 PE 2 上也可以看到 PW 信息。

```
[PE2] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1, 1 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpn1
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
192.4.4.4       1000       200/100         Static M     1          Up
```

CE 1 与 CE 2 之间能够 ping 通。

1.11.9 域间多段PW配置举例

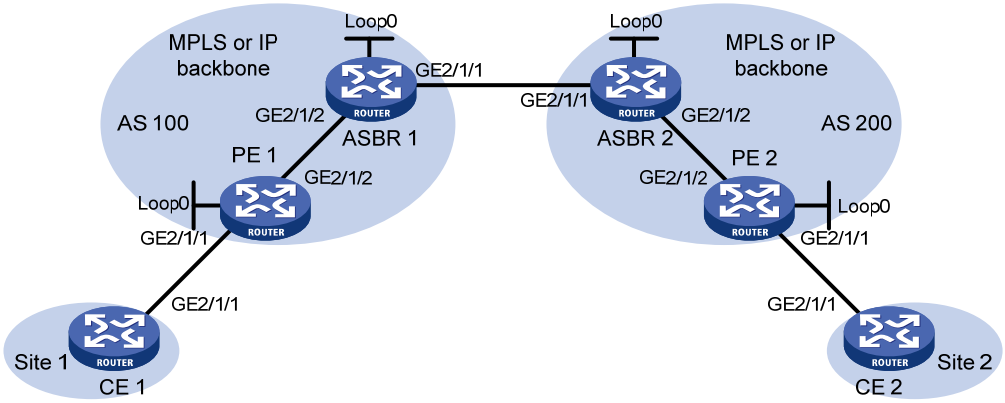
1. 组网需求

PE 1 和 ASBR 1 属于 AS 100，PE 2 和 ASBR 2 属于 AS 200。采用多段 PW 功能作为跨域 Option B 的解决方案，跨越 AS 域在 PE 1 和 PE 2 之间建立连接，实现 CE 1 和 CE 2 的二层报文跨越骨干网传递。具体需求如下：

- PE 1 和 ASBR 1、PE 2 和 ASBR 2 之间分别建立 LDP PW，并通过 LDP 建立承载该 PW 的公网隧道。
- ASBR 1 和 ASBR 2 之间建立 LDP PW，并在二者之间通过 BGP 发布带标签的 IPv4 路由，以通过 BGP 建立承载该 PW 的公网隧道。
- 在 ASBR 1 和 ASBR 2 上分别将两条隧道关联，以便建立多段 PW。

2. 组网图

图1-17 域间多段 PW 配置组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	GE2/1/1	100.1.1.1/24	ASBR 1	Loop0	192.2.2.2/32
PE 1	Loop0	192.1.1.1/32		GE2/1/2	23.1.1.2/24

	GE2/1/2	23.1.1.1/24		GE2/1/1	26.2.2.2/24
PE 2	Loop0	192.4.4.4/32	ASBR 2	Loop0	192.3.3.3/32
	GE2/1/2	22.2.2.1/24		GE2/1/1	26.2.2.3/24
CE 2	GE2/1/1	100.1.1.2/24		GE2/1/2	22.2.2.3/24

3. 配置步骤

(1) 配置 CE 1

```
<CE1> system-view
[CE1] interface gigabitethernet 2/1/1
[CE1-GigabitEthernet2/1/1] ip address 100.1.1.1 24
[CE1-GigabitEthernet2/1/1] quit
```

(2) 配置 PE 1

配置 LSR ID。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 192.1.1.1 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 192.1.1.1
```

使能 L2VPN。

```
[PE1] l2vpn enable
```

全局使能 LDP。

```
[PE1] mpls ldp
[PE1-ldp] quit
```

配置连接 ASBR1 的接口 GigabitEthernet2/1/2，在此接口上使能 LDP。

```
[PE1] interface gigabitethernet 2/1/2
[PE1-GigabitEthernet2/1/2] ip address 23.1.1.1 24
[PE1-GigabitEthernet2/1/2] mpls enable
[PE1-GigabitEthernet2/1/2] mpls ldp enable
[PE1-GigabitEthernet2/1/2] quit
```

在 PE 1 上运行 OSPF，用于建立 LSP。

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 23.1.1.1 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 192.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

创建交叉连接组 vpn1，在该交叉连接组内创建名称为 ldp 的交叉连接，将接口 GigabitEthernet2/1/1 与此交叉连接关联，并在交叉连接内创建 LDP PW，以实现 AC 和 PW 关联。

```
[PE1] xconnect-group vpn1
[PE1-xcg-vpn1] connection ldp
[PE1-xcg-vpn1-ldp] ac interface gigabitethernet 2/1/1
[PE1-xcg-vpn1-ldp] peer 192.2.2.2 pw-id 1000
[PE1-xcg-vpn1-ldp-192.2.2.2-1000] quit
[PE1-xcg-vpn1-ldp] quit
[PE1-xcg-vpn1] quit
```

(3) 配置 ASBR 1

配置 LSR ID。

```
<ASBR1> system-view
[ASBR1] interface loopback 0
[ASBR1-LoopBack0] ip address 192.2.2.2 32
[ASBR1-LoopBack0] quit
[ASBR1] mpls lsr-id 192.2.2.2
```

使能 L2VPN。

```
[ASBR1] l2vpn enable
```

全局使能 LDP。

```
[ASBR1] mpls ldp
[ASBR1-ldp] quit
```

配置连接 PE 1 的接口 GigabitEthernet2/1/2，在此接口上使能 LDP。

```
[ASBR1] interface gigabitethernet 2/1/2
[ASBR1-GigabitEthernet2/1/2] ip address 23.1.1.2 24
[ASBR1-GigabitEthernet2/1/2] mpls enable
[ASBR1-GigabitEthernet2/1/2] mpls ldp enable
[ASBR1-GigabitEthernet2/1/2] quit
```

配置连接 ASBR 2 的接口 GigabitEthernet2/1/1。

```
[ASBR1] interface gigabitethernet 2/1/1
[ASBR1-GigabitEthernet2/1/1] ip address 26.2.2.2 24
[ASBR1-GigabitEthernet2/1/1] mpls enable
[ASBR1-GigabitEthernet2/1/1] quit
```

在 ASBR 1 上运行 OSPF，用于建立域内 LSP。

```
[ASBR1] ospf
[ASBR1-ospf-1] area 0
[ASBR1-ospf-1-area-0.0.0.0] network 23.1.1.2 0.0.0.255
[ASBR1-ospf-1-area-0.0.0.0] network 192.2.2.2 0.0.0.0
[ASBR1-ospf-1-area-0.0.0.0] quit
[ASBR1-ospf-1] quit
```

在 ASBR 1 上配置 BGP 发布带标签的单播路由。

```
[ASBR1] bgp 100
[ASBR1-bgp] peer 26.2.2.3 as-number 200
[ASBR1-bgp] address-family ipv4 unicast
[ASBR1-bgp-ipv4] import-route direct
[ASBR1-bgp-ipv4] peer 26.2.2.3 enable
[ASBR1-bgp-ipv4] peer 26.2.2.3 route-policy policy1 export
[ASBR1-bgp-ipv4] peer 26.2.2.3 label-route-capability
[ASBR1-bgp-ipv4] quit
[ASBR1-bgp] quit
[ASBR1] route-policy policy1 permit node 1
[ASBR1-route-policy-policy1-1] apply mpls-label
[ASBR1-route-policy-policy1-1] quit
```

创建交叉连接组 vpn1，在该交叉连接组内创建名称为 ldp 的交叉连接，在交叉连接内创建两条 LDP PW，将这两条 PW 关联，以便建立多段 PW。

```
[ASBR1] xconnect-group vpn1
[ASBR1-xcg-vpn1] connection ldp
```

```
[ASBR1-xcg-vpn1-ldp] peer 192.1.1.1 pw-id 1000
[ASBR1-xcg-vpn1-ldp-192.1.1.1-1000] quit
[ASBR1-xcg-vpn1-ldp] peer 192.3.3.3 pw-id 1000
[ASBR1-xcg-vpn1-ldp-192.3.3.3-1000] quit
[ASBR1-xcg-vpn1-ldp] quit
[ASBR1-xcg-vpn1] quit
```

(4) 配置 ASBR 2

配置 LSR ID。

```
<ASBR2> system-view
[ASBR2] interface loopback 0
[ASBR2-LoopBack0] ip address 192.3.3.3 32
[ASBR2-LoopBack0] quit
[ASBR2] mpls lsr-id 192.3.3.3
```

使能 L2VPN。

```
[ASBR2] l2vpn enable
```

全局使能 LDP。

```
[ASBR2] mpls ldp
[ASBR2-ldp] quit
```

配置连接 PE 2 的接口 GigabitEthernet2/1/2，在此接口上使能 LDP。

```
[ASBR2] interface gigabitethernet 2/1/2
[ASBR2-GigabitEthernet2/1/2] ip address 22.2.2.3 24
[ASBR2-GigabitEthernet2/1/2] mpls enable
[ASBR2-GigabitEthernet2/1/2] mpls ldp enable
[ASBR2-GigabitEthernet2/1/2] quit
```

配置连接 ASBR 1 的接口 GigabitEthernet2/1/1。

```
[ASBR2] interface gigabitethernet 2/1/1
[ASBR2-GigabitEthernet2/1/1] ip address 26.2.2.3 24
[ASBR2-GigabitEthernet2/1/1] mpls enable
[ASBR2-GigabitEthernet2/1/1] quit
```

在 ASBR 2 上运行 OSPF，用于建立域内 LSP。

```
[ASBR2] ospf
[ASBR2-ospf-1] area 0
[ASBR2-ospf-1-area-0.0.0.0] network 22.2.2.3 0.0.0.255
[ASBR2-ospf-1-area-0.0.0.0] network 192.3.3.3 0.0.0.0
[ASBR2-ospf-1-area-0.0.0.0] quit
[ASBR2-ospf-1] quit
```

在 ASBR 2 上配置 BGP 发布带标签的单播路由。

```
[ASBR2] bgp 200
[ASBR2-bgp] peer 26.2.2.2 as-number 100
[ASBR2-bgp] address-family ipv4 unicast
[ASBR2-bgp-ipv4] import-route direct
[ASBR2-bgp-ipv4] peer 26.2.2.2 enable
[ASBR2-bgp-ipv4] peer 26.2.2.2 route-policy policy1 export
[ASBR2-bgp-ipv4] peer 26.2.2.2 label-route-capability
[ASBR2-bgp-ipv4] quit
[ASBR2-bgp] quit
```

```
[ASBR2] route-policy policy1 permit node 1
[ASBR2-route-policy-policy1-1] apply mpls-label
[ASBR2-route-policy-policy1-1] quit
```

创建交叉连接组 vpn1，在该交叉连接组内创建名称为 ldp 的交叉连接，在交叉连接内创建两条 LDP PW，将这两条 PW 关联，以便建立多段 PW。

```
[ASBR2] xconnect-group vpn1
[ASBR2-xcg-vpn1] connection ldp
[ASBR2-xcg-vpn1-ldp] peer 192.2.2.2 pw-id 1000
[ASBR2-xcg-vpn1-ldp-192.2.2.2-1000] quit
[ASBR2-xcg-vpn1-ldp] peer 192.4.4.4 pw-id 1000
[ASBR2-xcg-vpn1-ldp-192.4.4.4-1000] quit
[ASBR2-xcg-vpn1-ldp] quit
[ASBR2-xcg-vpn1] quit
```

(5) 配置 PE 2

配置 LSR ID。

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 192.4.4.4 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 192.4.4.4
```

使能 L2VPN。

```
[PE2] l2vpn enable
```

全局使能 LDP。

```
[PE2] mpls ldp
[PE2-ldp] quit
```

配置连接 ASBR 2 的接口 GigabitEthernet2/1/2，在此接口上使能 LDP。

```
[PE2] interface gigabitethernet 2/1/2
[PE2-GigabitEthernet2/1/2] ip address 22.2.2.1 24
[PE2-GigabitEthernet2/1/2] mpls enable
[PE2-GigabitEthernet2/1/2] mpls ldp enable
[PE2-GigabitEthernet2/1/2] quit
```

在 PE 2 上运行 OSPF，用于建立 LSP。

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 192.4.4.4 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 22.2.2.1 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

创建交叉连接组 vpn1，在该交叉连接组内创建名称为 ldp 的交叉连接，将接口 GigabitEthernet2/1/1 与此交叉连接关联，并在交叉连接内创建 LDP PW，以实现 AC 和 PW 关联。

```
[PE2] xconnect-group vpn1
[PE2-xcg-vpn1] connection ldp
[PE2-xcg-vpn1-ldp] ac interface gigabitethernet 2/1/1
[PE2-xcg-vpn1-ldp] peer 192.3.3.3 pw-id 1000
[PE2-xcg-vpn1-ldp-192.3.3.3-1000] quit
[PE2-xcg-vpn1-ldp] quit
```

```
[PE2-xcg-vpn1] quit
```

(6) 配置 CE 2

```
<CE2> system-view
[CE2] interface gigabitethernet 2/1/1
[CE2-GigabitEthernet2/1/1] ip address 100.1.1.2 24
[CE2-GigabitEthernet2/1/1] quit
```

4. 验证配置

在 PE 1 上查看 PW 信息，可以看到已经建立了 LDP PW。

```
[PE1] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1, 1 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpn1
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
192.2.2.2       1000       1151/1279       LDP    M     1          Up
```

在 ASBR 1 上查看 PW 信息，可以看到建立了两条 PW 连接，构成了多段 PW。

```
[ASBR1] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 2, 2 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpn1
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
192.1.1.1       1000       1279/1151       LDP    M     0          Up
192.3.3.3       1000       1278/1151       LDP    M     1          Up
```

在 ASBR 2 上查看 PW 信息，可以看到建立了两条 PW 连接，构成了多段 PW。

```
[ASBR2] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 2, 2 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpn1
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
192.2.2.2       1000       1151/1278       LDP    M     0          Up
192.4.4.4       1000       1150/1279       LDP    M     1          Up
```

在 PE 2 上也可以看到 PW 信息。

```
[PE2] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1, 1 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpn1
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
192.3.3.3       1000       1279/1150       LDP    M     1          Up
```

CE 1 与 CE 2 之间能够 ping 通。

目 录

1 MPLS OAM 1-1
1.1 MPLS OAM简介 1-1
1.1.1 MPLS Ping 1-1
1.1.2 MPLS Trace route 1-1
1.1.3 周期性MPLS Trace route 1-1
1.1.4 MPLS BFD 1-2
1.1.5 协议规范 1-2
1.2 配置LSP隧道的MPLS OAM功能 1-2
1.2.1 配置MPLS Ping功能 1-3
1.2.2 配置MPLS Trace route功能 1-3
1.2.3 使能LSP的周期性Trace route功能 1-3
1.2.4 配置使用BFD检测LSP 1-3
1.3 配置MPLS TE隧道的MPLS OAM功能 1-4
1.3.1 配置MPLS Ping功能 1-4
1.3.2 配置MPLS Trace route功能 1-5
1.3.3 配置使用BFD检测MPLS TE隧道 1-5
1.4 配置PW的MPLS OAM功能 1-6
1.4.1 配置MPLS Ping功能 1-6
1.4.2 配置使用BFD检测PW 1-7
1.5 MPLS OAM显示和维护 1-8
1.6 MPLS OAM典型配置举例 1-8
1.6.1 BFD检测LSP配置举例 1-8

1 MPLS OAM

1.1 MPLS OAM简介

MPLS OAM（Operations, Administration and Maintenance，操作、管理和维护）功能为 MPLS 网络提供了数据平面连通性检测、数据平面与控制平面一致性校验、故障点定位等多种错误管理（Fault Management）工具。MPLS OAM 利用这些错误管理工具对 LSP、MPLS TE 隧道和 MPLS PW 进行检测和故障定位，降低了 MPLS 网络的管理和维护的复杂度，提高了 MPLS 网络的可用性。

MPLS OAM 提供的错误管理工具分为如下两类：

- 手工按需检测工具（on-demand 工具）：根据需要手工触发的检测工具，如 MPLS ping、MPLS Trace route。
- 系统主动检测工具（proactive 工具）：系统主动启动、无需手工触发的检测工具，如周期性 MPLS Trace route、MPLS BFD。

1.1.1 MPLS Ping

用来对 LSP 隧道、MPLS TE 隧道或 PW 的连通性进行手工检测。MPLS Ping 的工作机制是：在 Ingress 节点为 MPLS Echo Request 报文压入待检测隧道对应的标签；经过隧道将该报文转发到 Egress 节点；Egress 节点处理该报文后，回应 MPLS Echo Reply 报文；如果 Ingress 节点接收到表示成功的 MPLS Echo Reply 报文，则说明该隧道可以用于数据转发；如果 Ingress 节点接收到带有错误码的 MPLS Echo Reply 报文，则说明该隧道存在故障。

1.1.2 MPLS Trace route

用来查看 LSP 隧道或 MPLS TE 隧道从 Ingress 节点到 Egress 节点所经过的路径，以便对 LSP 隧道或 MPLS TE 隧道的错误点进行定位。MPLS Trace route 功能通过沿着隧道连续发送 TTL 从 1 到某个值的 MPLS Echo Request 报文，让隧道经过的每一跳收到该报文后，返回 MPLS Echo Reply 报文。这样，Ingress 节点可以收集到隧道上每一跳的信息，从而定位出故障节点。同时，MPLS Trace route 功能还可用于收集整条隧道上每个节点的重要信息，如下游分配的标签等。

1.1.3 周期性MPLS Trace route

周期性 MPLS Trace route 功能，即周期性地对 LSP 隧道进行 Trace route 主动检测，用来对 LSP 隧道的错误点进行定位，对数据平面和控制平面一致性进行校验，并将发现的错误记录到系统日志（System Log Messages）中。管理员可以通过查看日志信息，了解 LSP 隧道是否出现故障。

如果同时配置了 BFD 自动检测 LSP 功能和周期性 MPLS Trace route 功能，则周期性 MPLS Trace route 检测到数据平面与控制平面不一致时，会拆除 BFD 会话，并基于控制平面重新建立 BFD 会话。

1.1.4 MPLS BFD

MPLS BFD 功能通过 BFD 会话来主动检测 LSP 隧道、MPLS TE 隧道或 PW 的连通性。当 BFD 检测到连通故障后，触发设备及时进行相应地处理，如快速重路由或路径保护倒换，使得流量转发得以继续。

MPLS BFD 功能的工作机制是：在待检测隧道的 Ingress 节点和 Egress 节点之间建立 BFD 会话；在 Ingress 节点为 BFD 控制报文压入隧道对应的标签；沿着隧道转发 BFD 控制报文；根据收到的 Egress 节点的 BFD 控制报文来判断隧道的状态。

可以通过两种方式建立检测 LSP 隧道、MPLS TE 隧道或 PW 的 BFD 会话：

- 静态方式：通过命令行手工指定本地和远端的标识符，根据指定的标识符建立 BFD 会话。
- 动态方式：不需要手工指定本地和远端的标识符，系统自动运行 MPLS Ping 来协商标识符，并根据协商好的标识符建立 BFD 会话。

对于 LSP 隧道和 MPLS TE 隧道，采用静态方式时，Egress 节点通过反向隧道转发 BFD 控制报文；采用动态方式时，如果存在反向隧道，则 Egress 节点通过反向隧道转发 BFD 控制报文，否则，通过 IP 路由转发 BFD 控制报文。因此，静态方式用来检测两台设备间从本地到远端和从远端到本地的一对 LSP 隧道或 MPLS TE 隧道；动态方式用来检测两台设备间从本地到远端的一条单向 LSP 隧道或 MPLS TE 隧道。

由于 PW 是一条双向隧道，对于 PW，静态方式和动态方式的作用相同，都是用来检测一条 PW。

1.1.5 协议规范

与 MPLS OAM 相关的协议规范有：

- RFC 4379：Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
- RFC 5085：Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires
- RFC 5885：Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)

1.2 配置LSP隧道的MPLS OAM功能

LSP 隧道的连通性检测方式分为以下两种：

- 按需方式：执行 **ping mpls ipv4** 命令或 **tracert mpls ipv4** 命令手工触发 LSP 检测。
- 主动方式：配置 LSP 的周期性 Trace route 或 BFD 检测 LSP 功能后，系统主动完成 LSP 检测。

1.2.1 配置MPLS Ping功能

表1-1 配置 MPLS ping 功能

操作	命令	说明
通过MPLS Ping功能检测IPv4地址前缀类型LSP的连通性	**ping mpls** [**-a** *source-ip* | **-c** *count* | **-exp** *exp-value* | **-h** *ttl-value* | **-m** *wait-time* | **-r** *reply-mode* | **-rtos** *tos-value* | **-s** *packet-size* | **-t** *time-out* | **-v**] * **ipv4** *dest-addr mask-length* [**destination** *start-address* [*end-address* [*address-increment*]]]	可在任意视图下配置本命令

1.2.2 配置MPLS Trace route功能

表1-2 配置 MPLS Trace route 功能

操作	命令	说明
通过MPLS Trace route功能查看IPv4地址前缀类型LSP从Ingress节点到Egress节点所经过的路径	**tracert mpls** [**-a** *source-ip* | **-exp** *exp-value* | **-h** *ttl-value* | **-r** *reply-mode* | **-rtos** *tos-value* | **-t** *time-out* | **-v** | **fec-check**] * **ipv4** *dest-addr mask-length* [**destination** *start-address* [*end-address* [*address-increment*]]]	可在任意视图下配置本命令

1.2.3 使能LSP的周期性Trace route功能

表1-3 使能 LSP 的周期性 Trace route 功能

操作	命令	说明
进入系统视图	**system-view**	-
使能指定FEC对应LSP的周期性Trace route功能	**mpls periodic-tracert** *dest-addr mask-length* [**-a** *source-ip* | **-exp** *exp-value* | **-h** *ttl-value* | **-m** *wait-time* | **-rtos** *tos-value* | **-t** *time-out* | **-u** *retry-attempt* | **fec-check**] *	缺省情况下，LSP的周期性Trace route功能处于关闭状态

1.2.4 配置使用BFD检测LSP

要想在本地和远端设备之间建立检测LSP的BFD会话，本地和远端设备上需要进行的配置如 表 1-4 所示。

表1-4 本地和远端设备上的配置

BFD 会话建立方式	节点类型	是否需要执行 **mpls bfd enable** 命令	是否需要执行 **mpls bfd** 命令	是否需要通过 **discriminator** 参数指定标识符
静态方式	本地	是	是	是
	远端	是	是	是
动态方式	本地	是	是	否
	远端	是	否	-

配置使用 BFD 检测 LSP 时，需要注意：

- 配置静态方式 BFD 会话时，两端设备上配置的本地和远端标识符必须匹配，即本地设备上配置的本地标识符与远端设备上配置的远端标识符相同；本地设备上配置的远端标识符与远端设备上配置的本地标识符相同。
- BFD 会话的源地址为本端设备的 MPLS LSR ID。因此，配置 BFD 检测 LSP 功能前，需要先在本端设备上配置 MPLS LSR ID，并确保远端设备上存在到达 MPLS LSR ID 的路由。
- 为某一个 FEC 配置 BFD 检测时，要么指定下一跳创建会话，要么不指定下一跳自动为每个下一跳分别创建一个 BFD 会话，不能同时配置两种方式。
- 通过静态方式建立 BFD 会话时，Ingress 和 Egress 节点均工作在主动（Active）模式；通过动态方式建立 BFD 会话时，Ingress 节点工作在被动（Passive）模式，Egress 节点工作在主动（Active）模式。在 Ingress 节点和 Egress 节点上执行 **bfd session init-mode** 命令不会改变节点的工作模式。

表1-5 使用 BFD 检测 LSP

操作	命令	说明
进入系统视图	**system-view**	-
使能MPLS BFD功能	**mpls bfd enable**	缺省情况下，MPLS BFD功能处于关闭状态
使用BFD检测指定FEC对应LSP的连通性	**mpls bfd** *dest-addr mask-length* [**nexthop** *nexthop-address* [**discriminator local** *local-id* **remote** *remote-id*]] [**template** *template-name*]	缺省情况下，未使用BFD检测FEC对应LSP的连通性

1.3 配置MPLS TE隧道的MPLS OAM功能

MPLS TE 隧道的连通性检测方式分为以下两种：

- 按需方式：执行 **ping mpls te** 命令或 **tracert mpls te** 命令手工触发 MPLS TE 隧道检测。
- 主动方式：配置 BFD 检测 MPLS TE 隧道功能后，系统主动完成 MPLS TE 隧道检测。

1.3.1 配置MPLS Ping功能

表1-6 配置 MPLS ping 功能

操作	命令	说明
通过MPLS Ping功能检测MPLS TE隧道的连通性	**ping mpls** [**-a** *source-ip* | **-c** *count* | **-exp** *exp-value* | **-h** *ttl-value* | **-m** *wait-time* | **-r** *reply-mode* | **-rtos** *tos-value* | **-s** *packet-size* | **-t** *time-out* | **-v**] * **te tunnel** *interface-number*	可在任意视图下配置本命令

1.3.2 配置MPLS Trace route功能

表1-7 配置 MPLS Trace route 功能

操作	命令	说明
通过MPLS Trace route功能查看MPLS TE隧道从Ingress节点到Egress节点所经过的路径	**tracert mpls** [**-a** *source-ip* | **-exp** *exp-value* | **-h** *ttl-value* | **-r** *reply-mode* | **-rtos** *tos-value* | **-t** *time-out* | **-v** | **fec-check**] * **te tunnel** *interface-number*	可在任意视图下配置本命令

1.3.3 配置使用BFD检测MPLS TE隧道

要想在本地和远端设备之间建立检测MPLS TE隧道的BFD会话，本地和远端设备上需要进行的配置如 表 1-8 所示。

表1-8 本地和远端设备上的配置

BFD 会话建立方式	节点类型	是否需要执行 **mpls bfd enable** 命令	是否需要执行 **mpls bfd** 命令	是否需要通过 **discriminator** 参数指定标识符
静态方式	本地	是	是	是
	远端	是	是	是
动态方式	本地	是	是	否
	远端	是	否	-

配置使用 BFD 检测 MPLS TE 隧道时，需要注意：

- 配置静态方式 BFD 会话时，两端设备上配置的本地和远端标识符必须匹配，即本地设备上配置的本地标识符与远端设备上配置的远端标识符相同；本地设备上配置的远端标识符与远端设备上配置的本地标识符相同。
- BFD 会话的源地址为本端设备的 MPLS LSR ID。因此，配置 BFD 检测 MPLS TE 隧道功能前，需要先在本端设备上配置 MPLS LSR ID，并确保远端设备上存在到达 MPLS LSR ID 的路由。
- 通过静态方式建立 BFD 会话时，Ingress 和 Egress 节点均工作在主动（Active）模式；通过动态方式建立 BFD 会话时，Ingress 节点工作在被动（Passive）模式，Egress 节点工作在主动（Active）模式。在 Ingress 节点和 Egress 节点上执行 **bfd session init-mode** 命令不会改变节点的工作模式。
- 如果在 MPLS TE 隧道上同时使用了 FRR 和 BFD 检测 TE 隧道功能，则为了保证 FRR 切换不会导致检测 TE 隧道的 BFD 会话 down，需要配置检测 TE 隧道的 BFD 会话的检测周期大于 FRR 触发机制（如 BFD 检测 RSVP 邻居）的检测周期。

表1-9 配置使用 BFD 检测 MPLS TE 隧道

操作	命令	说明
进入系统视图	**system-view**	-
使能MPLS BFD功能	**mpls bfd enable**	缺省情况下，MPLS BFD功能处于关闭状态

操作	命令	说明
进入MPLS TE隧道对应的Tunnel接口视图	**interface tunnel** *number*	-
配置使用BFD检测当前隧道接口对应MPLS TE隧道的连通性	**mpls bfd** [**discriminator local** *local-id* **remote** *remote-id*] [**template** *template-name*]	缺省情况下，未使用BFD检测隧道接口对应MPLS TE隧道的连通性

1.4 配置PW的MPLS OAM功能

VCCV（Virtual Circuit Connectivity Verification，虚电路连通性验证）是一种 L2VPN PW OAM 功能，用于确认 PW 数据平面的连通性。VCCV 有两种方式：

- 按需方式：执行 **ping mpls pw** 命令手工触发 PW 检测。
- 主动方式：配置通过 BFD 或 Raw-BFD 检测 PW 后，系统主动完成 PW 检测。

用来检测 PW 连通性的报文统称为 VCCV 报文。PE 通过 CC（Control Channel，控制通道）来传送 VCCV 报文。

CC 有以下几种类型：

- **control-word** 类型：通过控制字，即 PW-ACH（PW Associated Channel Header，PW 随路通道首部），标识 VCCV 报文。只有 PW 支持控制字时，才能选择这种类型。控制字的详细介绍，请参见“MPLS 配置指导”中的“MPLS L2VPN”。
- **router-alert** 类型：通过在 PW 标签之前携带 MPLS 路由器告警标签来标识 VCCV 报文。

CV（Connectivity Verification，连通性验证）类型，即检测工具类型，分为如下几种：

- LSP Ping 类型：采用 MPLS ping 检测 PW 的连通性。
- BFD 方式：采用 BFD 检测 PW 的连通性，BFD 报文的封装方式为 IP/UDP Encapsulation (with IP/UDP Headers)。
- Raw-BFD 方式：采用 BFD 检测 PW 的连通性，BFD 报文的封装方式为 PW-ACH Encapsulation (without IP/UDP Headers)，即封装在 VCCV 控制通道内的 BFD 控制报文不携带 IP 和 UDP 头。只有控制通道类型为 **control-word** 时，指定本参数才会生效。

1.4.1 配置MPLS Ping功能

执行本配置前，需要先：

(1) 创建 PW 模板，并在 PW 模板视图下通过 **vccv cc** 命令配置 VCCV 控制通道类型。

(2) 创建 PW，并指定该 PW 引用上述步骤中创建的 PW 模板。

表1-10 配置 MPLS ping 功能

操作	命令	说明
通过MPLS Ping功能检测PW的连通性	**ping mpls** [**-a** *source-ip* | **-c** *count* | **-exp** *exp-value* | **-h** *ttl-value* | **-m** *wait-time* | **-r** *reply-mode* | **-rtos** *tos-value* | **-s** *packet-size* | **-t** *time-out* | **-v**] * **pw** *ip-address* **pw-id** *pw-id*	可在任意视图下配置本命令

1.4.2 配置使用BFD检测PW

使用 BFD 检测 PW 功能的配置步骤为：

(1) 使能 MPLS BFD 功能。

(2) 创建 PW 模板，并在 PW 模板视图下配置使用 BFD 检测 PW 的连通性。

(3) 创建 PW，并指定该 PW 引用上述步骤中创建的 PW 模板。

从上述步骤中可以看出，使用 BFD 检测 PW 功能并不是直接在 PW 上配置，而是通过引用 PW 模板间接来配置。

完成上述配置后，最终是否使用 BFD 检测 PW 的连通性、BFD 报文采用何种封装方式以及采用何种 VCCV 控制通道，由两端的配置共同决定：

- 如果两端 PE 上都配置了 BFD 检测 PW 且 BFD 报文封装方式相同，则采用该封装方式检测 PW；否则，不使用 BFD 检测 PW 的连通性。
- 如果两端 PE 上配置了相同的 VCCV 控制通道类型，则使用该 VCCV 控制通道；否则，不使用任何 VCCV 控制通道，这样会导致无法建立 BFD 会话。

1. 配置使用BFD检测MPLS L2VPN的PW

本配置可以用来检测 MPLS L2VPN 的静态 PW 和 LDP PW。

表1-11 配置使用 BFD 检测 MPLS L2VPN 的 PW

操作	命令	说明
进入系统视图	**system-view**	-
使能MPLS BFD功能	**mpls bfd enable**	缺省情况下，MPLS BFD功能处于关闭状态
创建PW模板，并进入PW模板视图	**pw-class** *class-name*	缺省情况下，设备上不存在任何PW模板
配置使用BFD检测PW的连通性	**vccv bfd** [**raw-bfd**] [**template** *template-name*]	缺省情况下，未使用BFD检测PW的连通性 执行本命令时如果指定了**raw-bfd**参数，则需要配置控制通道类型为**control-word**
配置VCCV控制通道类型	**vccv cc** { **control-word** | **router-alert** }	缺省情况下，没有指定VCCV控制通道类型
退回系统视图	**quit**	-
进入交叉连接组视图	**xconnect-group** *group-name*	-
进入交叉连接视图	**connection** *connection-name*	-
配置PW，引用已创建的PW模板，并进入PW视图	**peer** *ip-address* **pw-id** *pw-id* [**in-label** *label-value* **out-label** *label-value*] **pw-class** *class-name* [**tunnel-policy** *tunnel-policy-name*]	缺省情况下，未配置PW
（可选）配置检测PW的BFD会话的本地标识符和远端标识符	**bfd discriminator local** *local-id* **remote** *remote-id*	缺省情况下，没有指定检测PW的BFD会话的本地标识符和远端标识符 本端PE上配置的标识符需要和对端PE上配置的标识符相对应

操作	命令	说明
（可选）配置备份PW，引用已创建的PW模板，并进入备份PW视图	**backup-peer** *ip-address* **pw-id** *pw-id* [**in-label** *label-value* **out-label** *label-value*] **pw-class** *class-name* [**tunnel-policy** *tunnel-policy-name*]	缺省情况下，未配置备份PW
（可选）配置检测备份PW的BFD会话的本地标识符和远端标识符	**bfd discriminator local** *local-id* **remote** *remote-id*	缺省情况下，没有指定检测备份PW的BFD会话的本地标识符和远端标识符 本端PE上配置的标识符需要和对端PE上配置的标识符相对应

1.5 MPLS OAM显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 MPLS OAM 的运行情况，通过查看显示信息验证配置的效果。

表1-12 MPLS OAM 显示和维护

操作	命令
显示LSP隧道或MPLS TE隧道的BFD检测信息	**display mpls bfd** [**ipv4** *dest-addr mask-length* | **te tunnel** *tunnel-number*]
显示PW的BFD检测信息	**display l2vpn pw bfd** [**peer** *peer-ip* **pw-id** *pw-id*]

1.6 MPLS OAM典型配置举例

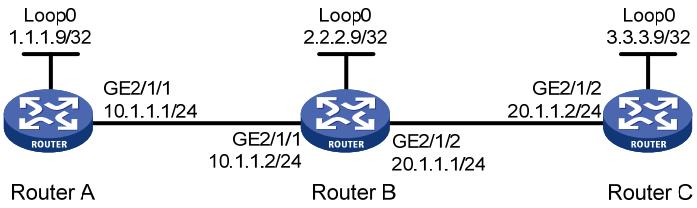
1.6.1 BFD检测LSP配置举例

1. 组网需求

利用 LDP 建立 1.1.1.9/32 到 3.3.3.9/32、3.3.3.9/32 到 1.1.1.9/32 两条 LSP 后，使用 BFD 检测 LSP 隧道的连通性。

2. 组网图

图1-1 BFD 检测 LSP 配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址

按照上图配置各接口 IP 地址和掩码，包括三层以太网接口和 Loopback 接口，具体配置过程略。

(2) 配置 OSPF，以保证各设备之间路由可达

配置 Router A。

```
<RouterA> system-view
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[RouterA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

配置 Router B。

```
<RouterB> system-view
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

配置 Router C。

```
<RouterC> system-view
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[RouterC-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

(3) 使能 MPLS 和 LDP 功能

配置 Router A。

```
[RouterA] mpls lsr-id 1.1.1.9
[RouterA] mpls ldp
[RouterA-ldp] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mpls enable
[RouterA-GigabitEthernet2/1/1] mpls ldp enable
[RouterA-GigabitEthernet2/1/1] quit
```

配置 Router B。

```
[RouterB] mpls lsr-id 2.2.2.9
[RouterB] mpls ldp
[RouterB-ldp] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mpls enable
[RouterB-GigabitEthernet2/1/1] mpls ldp enable
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] mpls enable
[RouterB-GigabitEthernet2/1/2] mpls ldp enable
[RouterB-GigabitEthernet2/1/2] quit
```

配置 Router C。

```
[RouterC] mpls lsr-id 3.3.3.9
[RouterC] mpls ldp
[RouterC-ldp] quit
[RouterC] interface gigabitethernet 2/1/2
[RouterC-GigabitEthernet2/1/2] mpls enable
[RouterC-GigabitEthernet2/1/2] mpls ldp enable
[RouterC-GigabitEthernet2/1/2] quit
```

(4) 使能 MPLS BFD 功能，并配置通过 BFD 检测 LSP 的连通性

配置 Router A。

```
[RouterA] mpls bfd enable
[RouterA] mpls bfd 3.3.3.9 32
```

配置 Router C。

```
[RouterC] mpls bfd enable
[RouterC] mpls bfd 1.1.1.9 32
```

4. 验证配置

配置完成后，在设备 Router A 和 Router C 上执行 **display mpls bfd** 命令，可以看到检测 LSP 的 BFD 会话的建立情况。以 Router A 为例。

```
[RouterA] display mpls bfd
 Total number of sessions: 2, 2 up, 0 down, 0 init

 FEC Type: LSP
 FEC Info:
   Destination: 1.1.1.9
   Mask Length: 32
 NHLFE ID: -
 Local Discr: 513                    Remote Discr: 513
 Source IP: 1.1.1.9                  Destination IP: 3.3.3.9
 Session State: Up                   Session Role: Active
 Template Name: -

 FEC Type: LSP
 FEC Info:
   Destination: 3.3.3.9
   Mask Length: 32
 NHLFE ID: 1042
 Local Discr: 514                    Remote Discr: 514
 Source IP: 1.1.1.9                  Destination IP: 127.0.0.1
 Session State: Up                   Session Role: Passive
 Template Name: -
```

以上显示信息表示，Router A 和 Router C 之间建立了两个 BFD 会话，分别用来检测 3.3.3.9/32 到 1.1.1.9/32、1.1.1.9/32 到 3.3.3.9/32 两条 LSP。

目 录

1 MPLS保护倒换 ····· 1-1
1.1 MPLS保护倒换简介 ····· 1-1
1.1.1 保护倒换的触发方式 ····· 1-1
1.1.2 保护倒换方式 ····· 1-1
1.1.3 路径切换方式 ····· 1-2
1.2 协议规范 ····· 1-2
1.3 MPLS保护倒换配置任务简介 ····· 1-2
1.4 开启MPLS保护倒换功能 ····· 1-3
1.5 创建保护组 ····· 1-3
1.6 配置保护组的属性 ····· 1-4
1.7 配置保护组外部倒换 ····· 1-5
1.8 配置PSC控制报文发送时间间隔 ····· 1-5
1.9 MPLS保护倒换显示和维护 ····· 1-5
1.10 MPLS保护倒换配置举例 ····· 1-6

1 MPLS保护倒换

1.1 MPLS保护倒换简介

MPLS PS（Protection Switching，保护倒换）是 MPLS TE 隧道的一种端到端线性保护机制。它通过将一条 MPLS TE 隧道（工作隧道）与另一条 MPLS TE 隧道（保护隧道）关联，形成一个保护组，实现工作隧道故障后，流量可以快速倒换到保护隧道，以保证流量的不中断传输。

1.1.1 保护倒换的触发方式

除了工作隧道发生故障外，还可以通过其他方法触发流量在工作隧道和保护隧道之间进行倒换。MPLS PS 支持的保护倒换触发方式有如下几种：

(1) 外部倒换：通过手工配置命令触发保护倒换。外部倒换的优先级由高到低为：

- 清除倒换（Clear）：清除所有已执行的外部倒换命令。
- 锁定倒换（Lockout of Protection）：流量锁定在工作隧道上传输。
- 强制倒换（Forced Switch）：强制将流量从工作隧道倒换到保护隧道上传输。
- 手工倒换（Manual Switch）：手动将流量从工作隧道倒换到保护隧道上传输，如果保护隧道存在故障，则不进行流量倒换。

(2) 信令倒换（Signal Fail）：通过信令协议触发保护倒换。目前，可以触发保护倒换的信令包括使用 MPLS BFD 检测 MPLS TE 隧道、通过链路层检测接口的 Up/Down 状态。MPLS BFD 检测 MPLS TE 隧道的详细介绍请参见“MPLS 配置指导”中的“MPLS OAM”。

外部倒换命令及信令倒换优先级从高到低依次为：

- 清除倒换
- 锁定倒换
- 强制倒换
- 保护隧道的信令倒换，即通过信令协议检测到保护隧道发生故障
- 工作隧道的信令倒换，即通过信令协议检测到工作隧道发生故障
- 信令清除倒换，即通过信令协议检测到工作隧道或保护隧道故障恢复
- 手工倒换

如果同时存在多种触发方式，则由优先级高的触发方式决定当前传输流量的隧道。

1.1.2 保护倒换方式

MPLS PS 支持如下保护倒换方式：

- 1:1 保护倒换：正常情况下，流量在工作隧道上传输；当隧道的头节点或尾节点通过检测机制（如 MPLS BFD）发现工作隧道发生故障或执行外部倒换命令时，通知头节点根据保护倒换状态决定流量在工作隧道或保护隧道上传输。
- 1+1 保护倒换：在正常情况下，流量在工作隧道、保护隧道上都传输，隧道的尾节点选择从工作隧道上接收流量；当隧道的头节点或尾节点通过检测机制（如 MPLS BFD）发现工作隧道

发生故障或执行外部倒换命令时，通知隧道的尾节点根据保护倒换状态决定从工作隧道或保护隧道上接收流量。

1.1.3 路径切换方式

MPLS TE 隧道为双向隧道时，该隧道可以采用如下方式切换流量转发路径：

- 单向路径切换：外部倒换命令或信令倒换触发一个方向的流量进行保护倒换时，只切换该方向流量的转发隧道，另一个方向的转发隧道不受影响。
- 双向路径切换：外部倒换命令或信令倒换触发一个方向的流量进行保护倒换时，不仅切换该方向流量的转发隧道，还通过 PSC（Protection State Coordination，保护状态协调）控制报文通知远端切换另一个方向流量的转发隧道。

1:1 保护倒换支持单向路径切换和双向路径切换；1+1 保护倒换只支持双向路径切换。

1.2 协议规范

与 MPLS 保护倒换相关的协议规范有：

- RFC 6372：MPLS Transport Profile (MPLS-TP) Survivability Framework
- RFC 6378：MPLS Transport Profile (MPLS-TP) Linear Protection

1.3 MPLS保护倒换配置任务简介

在配置 MPLS 保护倒换之前，需要先创建两条 MPLS TE 隧道：一条作为工作隧道，一条作为保护隧道。MPLS TE 隧道的创建方法，请参见“MPLS 配置指导”中的“MPLS TE”。

表1-1 MPLS 保护倒换配置任务简介

操作		说明	详细配置
开启MPLS保护倒换功能		必选	1.4
创建保护组		必选	1.5
配置保护组的属性		可选	1.6
配置保护组外部倒换命令		可选	1.7
配置保护组信令倒换		可选	设备自动支持根据接口状态进行保护倒换，无需配置 若要通过MPLS OAM机制检测工作隧道或保护隧道的状态，则需要对工作隧道或保护隧道进行MPLS OAM相关配置，配置方法请参见“MPLS配置指导”中的“MPLS OAM”
配置PSC控制报文的发送时间间隔		可选	1.8
配置流量通过保护组转发	配置静态路由使流量沿Tunnel-Bundle接口转发	必选	详细配置，请参见“MPLS配置指导”中的“MPLS TE”
	配置策略路由使流量沿Tunnel-Bundle接口转发		
	配置自动路由发布使流量沿Tunnel-Bundle接口转发		

1.4 开启MPLS保护倒换功能

只有开启 MPLS 保护倒换功能后，才能执行 MPLS 保护倒换的其他命令。

表1-2 开启 MPLS 保护倒换功能

操作	命令	说明
进入系统视图	**system-view**	-
开启MPLS保护倒换功能，并进入MPLS保护倒换视图	**mpls protection**	缺省情况下，MPLS保护倒换功能处于关闭状态

1.5 创建保护组

创建保护倒换模式的 Tunnel-Bundle 接口，并为该 Tunnel-Bundle 接口指定两个成员接口（一个作为工作隧道和一个作为保护隧道），设备上将创建一个 MPLS TE 保护组。在 MPLS TE 保护组内，设备根据外部倒换命令、信令倒换，决定转发流量使用的隧道。

执行本配置时，需要注意：

- 配置 Tunnel-Bundle 接口的 IP 地址和隧道目的端地址后，至少有一个成员接口处于 up 状态，Tunnel-Bundle 接口才能 up。
- 建议为成员接口和 Tunnel-Bundle 接口配置相同的目的端地址。如果不同，则需要确保通过成员接口能够到达 Tunnel-Bundle 接口的目的端地址；否则，会导致流量转发不通。
- 为 Tunnel-Bundle 接口指定的成员接口必须是 MPLS TE 隧道接口。
- 成员接口只能用来转发出接口为 Tunnel-Bundle 接口的流量，不能转发其他流量。

表1-3 创建保护组

操作	命令	说明
进入系统视图	**system-view**	-
创建保护倒换模式的隧道捆绑接口（Tunnel-Bundle接口），并进入Tunnel-Bundle接口视图	**interface tunnel-bundle** *number* **protection** { **oneplusone** | **onetoone** }	缺省情况下，设备上不存在任何Tunnel-Bundle接口
为Tunnel-Bundle接口指定主用成员接口	**member interface tunnel** *tunnel-number*	缺省情况下，未指定主用成员接口 主用成员接口对应的MPLS TE隧道为工作隧道
为Tunnel-Bundle接口指定备用成员接口	**member interface tunnel** *tunnel-number* **protection**	缺省情况下，未指定备用成员接口 备用成员接口对应的MPLS TE隧道为保护隧道
配置Tunnel-Bundle接口的IPv4地址	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	缺省情况下，未配置Tunnel-Bundle接口的IPv4地址

操作	命令	说明
配置Tunnel-Bundle接口的隧道目的端地址	**destination** *ip-address*	缺省情况下，未指定Tunnel-Bundle接口的隧道目的端地址
（可选）设置当前接口的描述信息	**description** *text*	缺省情况下，接口的描述信息为“*接口名* Interface”，比如：“Tunnel-Bundle1 Interface”
（可选）配置接口的期望带宽	**bandwidth** *bandwidth-value*	缺省值为64kbps
（可选）指定转发当前接口流量的业务处理板（MSR 5600）	**service slot** *slot-number*	缺省情况下，没有指定转发当前接口流量的业务处理板
（可选）恢复当前接口的缺省配置	**default**	-
（可选）打开当前接口	**undo shutdown**	缺省情况下，隧道捆绑接口处于UP状态

1.6 配置保护组的属性

缺省情况下，若工作隧道出现故障，则立即将流量切换到保护隧道上传输，从而防止因工作隧道故障引起的流量中断。工作隧道故障恢复后，流量立即从保护隧道回切到工作隧道。但在网络抖动的情况下，立即倒换、立即回切可能会导致流量频繁在工作隧道和保护隧道之间倒换，影响流量的正常转发，并增加了设备的负担。

可以通过如下几种方式解决上述问题：

- 配置保护组的倒换延迟时间：工作隧道出现故障时，等待倒换延迟时间超时后，再将流量切换至保护隧道传输。若在倒换延迟时间内，工作隧道恢复正常，则不会进行倒换。
- 配置保护组不回切：工作隧道故障恢复后，流量继续在保护隧道上传输，如果保护隧道未出现故障，则流量不会回切到工作隧道。
- 配置保护组延迟回切：工作隧道故障恢复后，如果在回切时间超时时，工作隧道仍然处于正常状态，则将流量从保护隧道回切到工作隧道。

表1-4 配置保护组的属性

操作	命令	说明
进入系统视图	**system-view**	-
进入保护倒换模式的Tunnel-Bundle接口视图	**interface tunnel-bundle** *number* [**protection** { **oneplusone** | **onetoone** }]	-
配置检测到工作隧道发生故障后的倒换延迟时间	**protection holdoff** *holdoff-time*	缺省情况下，倒换延迟时间为0，即检测到工作隧道故障后立即将流量倒换到保护隧道传输
配置保护组的回切模式和回切等待时间	**protection revertive** { **never** | **wtr** [*wtr-time*] }	缺省情况下，工作隧道故障恢复后，流量会立即从保护隧道回切到工作隧道

操作	命令	说明
配置保护组采用双向路径切换方式	**protection switching-mode bidirectional**	本命令仅支持在1:1保护倒换方式的Tunnel-Bundle接口下配置。缺省情况下，1:1保护倒换方式的保护组采用单向路径切换方式 1+1保护倒换方式只支持双向路径切换方式

1.7 配置保护组外部倒换

通过配置保护组外部倒换，可根据需求对保护倒换的触发方式进行手动的控制。

表1-5 配置保护组外部倒换

操作	命令	说明
进入系统视图	**system-view**	-
进入保护组Tunnel-Bundle接口视图	**interface tunnel-bundle** *number* [**protection** { **onetoone** | **oneplusone** }]	Tunnel-Bundle接口已经创建的情况下，进入Tunnel-Bundle接口视图无需指定模式
配置外部倒换方式	**protection switch** { **clear** | **force** | **lock** | **manual** }	缺省情况下，未配置外部倒换命令

1.8 配置PSC控制报文发送时间间隔

采用双向路径切换时，两个方向的隧道需要同时进行切换，因此隧道两端的设备需要周期性发送 PSC 控制报文来协调隧道两端的保护状态，以达到双向隧道同时切换的目的。

可以根据需要修改 PSC 控制报文的发送时间间隔，避免协议报文占用过多的带宽和设备资源。

表1-6 配置 PSC 控制报文发送时间间隔

操作	命令	说明
进入系统视图	**system-view**	-
进入MPLS保护倒换视图	**mpls protection**	-
配置PSC控制报文的发送时间间隔	**psc message-interval** *interval*	缺省情况下，PSC控制报文的发送时间间隔为5秒

1.9 MPLS保护倒换显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 MPLS 保护倒换的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可以清除 Tunnel-Bundle 接口统计信息。

表1-7 MPLS 保护倒换显示和维护

操作	命令
显示隧道捆绑接口的相关信息	**display interface** [**tunnel-bundle** [*number*]] [**brief** [**description** | **down**]]
显示MPLS保护组的转发状态信息（MSR 2600/MSR 3600）	**display mpls forwarding protection** [**tunnel-bundle** *number*]
显示MPLS保护组的转发状态信息（MSR 5600）	**display mpls forwarding protection** [**tunnel-bundle** *number*] [**slot** *slot-number*]
显示MPLS保护组的当前运行状态和相关信息	**display mpls protection** [**tunnel-bundle** *number*] [**verbose**]
显示Tunnel-Bundle接口及其成员接口的信息	**display tunnel-bundle** [*number*]
清除接口的统计信息	**reset counters interface** [**tunnel-bundle** [*number*]]

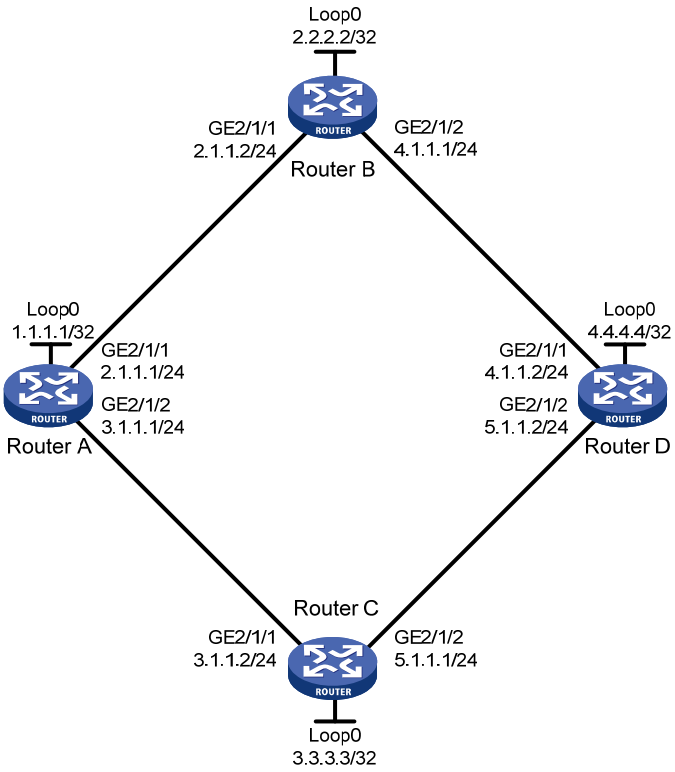
1.10 MPLS保护倒换配置举例

1. 组网需求

- 设备 Router A、Router B、Router C 和 Router D 运行 IS-IS；
- Router A 上存在两条到达 Router D 的 MPLS TE 隧道，分别为 Tunnel 1 和 Tunnel 2。Tunnel 1 采用的路径为 Router A—Router B—Router D；Tunnel 2 采用的路径为 Router A—Router C—Router D。
- 在 Router A 上创建 MPLS 保护组，Tunnel 1 作为工作隧道，Tunnel 2 作为保护隧道，在两条隧道之间实现保护倒换。

2. 组网图

图1-1 MPLS 保护倒换配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址

按照 图 1-1 配置各接口的IP地址和掩码，具体配置过程略。

(2) 在 Router A 上创建 MPLS TE 隧道

创建两条到达 Router D 的 MPLS TE 隧道，分别为 Tunnel 1 和 Tunnel 2，具体配置过程请参见“MPLS 配置指导”中的“MPLS TE”。

配置完成后，在 Router A 上执行 **display mpls tunnel all** 命令可以看到两条 MPLS TE 隧道的信息。

```
<RouterA> display mpls tunnel all
Destination      Type     Tunnel/NHLFE      VPN Instance
4.4.4.4          CRLSP    Tunnel1           -
4.4.4.4          CRLSP    Tunnel2           -
```

执行 **display interface tunnel** 命令可以看到隧道接口状态为 UP，以 Tunnel 1 为例：

```
<RouterA> display interface tunnel 1
Tunnel1
Current state: UP
Line protocol state: UP
Description: Tunnel1 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1496
```

```
Internet Address is 10.1.10.1/24 Primary
Tunnel source unknown, destination 4.4.4.4
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

(3) 配置保护组对应的 Tunnel-Bundle 接口

开启 MPLS 保护倒换功能。

```
<RouterA> system-view
[RouterA] mpls protection
[RouterA-mpls-protection] quit
```

创建 1:1 保护倒换模式的 Tunnel-Bundle 接口，为接口配置任意的 IP 地址（本例中为 101.1.101.1/24），并配置隧道目的端地址为 4.4.4.4（Router D 的 LSR ID）。

```
[RouterA] interface tunnel-bundle 0 protection onetoone
[RouterA-Tunnel-Bundle0] destination 4.4.4.4
[RouterA-Tunnel-Bundle0] ip address 101.1.101.1 24
```

为 Tunnel-Bundle 接口指定主用成员接口为 Tunnel1 接口，备用成员接口为 Tunnel2 接口。

```
[RouterA-Tunnel-Bundle0] member interface tunnel 1
[RouterA-Tunnel-Bundle0] member interface tunnel 2 protection
[RouterA-Tunnel-Bundle0] quit
```

(4) 配置通过 BFD 检测工作隧道和保护隧道

使能 MPLS BFD 功能。

```
[RouterA] mpls bfd enable
```

在主用成员接口上配置使用 BFD 检测工作隧道的连通性。

```
[RouterA] interface tunnel 1
[RouterA-Tunnel1] mpls bfd
[RouterA-Tunnel1] quit
```

在备用成员接口上配置使用 BFD 检测保护隧道的连通性。

```
[RouterA] interface tunnel 2
[RouterA-Tunnel2] mpls bfd
[RouterA-Tunnel2] quit
```

执行 **display bfd session** 命令可以看到用于检测 MPLS TE 隧道的 BFD 会话信息。

```
[RouterA] display bfd session
 Total Session Num: 2     Up Session Num: 2     Init Mode: Active

 IPv4 Session Working Under Ctrl Mode:

LD/RD          SourceAddr      DestAddr        State    Holdtime    Interface
513/513        1.1.1.1         127.0.0.1       Up       2297ms      Tunnel1
514/514        1.1.1.1         127.0.0.1       Up       1127ms      Tunnel2
```

(5) 配置静态路由使流量沿 Tunnel-Bundle 接口转发

在 Router A 上配置静态路由，使得到达目的地址 4.4.4.4/32 的流量通过接口 Tunnel-Bundle0 转发。

```
[RouterA] ip route-static 4.4.4.4 32 tunnel-bundle 0 preference 1
```

4. 验证配置

配置完成后，在 Router A 上执行 **display tunnel-bundle** 命令，可以查看到 Tunnel-Bundle 接口及其成员接口的信息。

```
[RouterA] display tunnel-bundle
Tunnel-Bundle Name     : Tunnel-Bundle 0
Bundle State           : Up
Bundle Attributes      :
  Bundle Mode          : 1:1
  Tunnel Type          : CR-LSP
  Tunnel Destination   : 4.4.4.4
Bundle Members :
  Member         State        Weight    Role
  Tunnel1        Up           1         Working
  Tunnel2        Up           1         Protection
```

在 Router A 上执行 **display mpls tunnel all** 命令，可以看到 Tunnel-bundle 接口对应捆绑隧道的信息。

```
[RouterA] display mpls tunnel all
Destination      Type     Tunnel/NHLFE      VPN Instance
4.4.4.4          CRLSP    Tunnel-Bundle0    -
```

在 Router A 上执行 **display mpls lsp protocol local verbose** 可以查看到 Tunnel-Bundle 接口对应的本地 LSP 的信息。

```
[RouterA] display mpls lsp protocol local verbose
Destination  : 4.4.4.4
FEC          : TunBDL0
Protocol     : TE
LSR Type     : Ingress
Service      : -
NHLFE ID     : 536870912
State        : Active
Out-Interface: Tun1
BkInterface  : Tun2
```

在 Router A 上执行 **display mpls protection** 可以查看到保护组信息。

```
[RouterA] display mpls protection
Total number of protection-groups: 1
Group    Type         Work-tunnel ID    Protect-tunnel ID    State
0     Tunnel-bundle      1                 2                N
```