

H3C SecPath M9000 系列 多业务安全网关

MPLS 配置指导(V7)

Copyright © 2021-2024 新华三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。

除新华三技术有限公司的商标外，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

本配置指导主要介绍 MPLS 的相关功能原理及配置。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [资料意见反馈](#)

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。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用 “[]” 括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项选取一个或者不选。
{ 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. 图形界面格式约定

格 式	意 义
< >	带尖括号 “< >” 表示按钮名，如 “单击<确定>按钮”。
[]	带方括号 “[]” 表示窗口名、菜单名和数据表，如 “弹出[新建用户]窗口”。
/	多级菜单用 “/” 隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 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。

4. 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。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

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。

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 技术特点	1-1
1.1.2 MPLS 基本概念	1-1
1.1.3 MPLS 网络结构	1-3
1.1.4 LSP 建立	1-3
1.1.5 MPLS 转发过程	1-5
1.1.6 倒数第二跳弹出	1-5
1.1.7 协议规范	1-6
1.2 MPLS 配置任务简介	1-6
1.3 使能 MPLS 功能	1-6
1.4 配置 MPLS MTU	1-7
1.5 配置设备作为 Egress 节点时为倒数第二跳分配的标签类型	1-8
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 FTN 转发统计功能	1-10
1.9 配置 LSP 的 MPLS 标签转发统计功能	1-11
1.10 开启 MPLS 模块的告警功能	1-11
1.11 MPLS 显示和维护	1-12

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。

1.1.1 MPLS 技术特点

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、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。

1.1.2 MPLS 基本概念

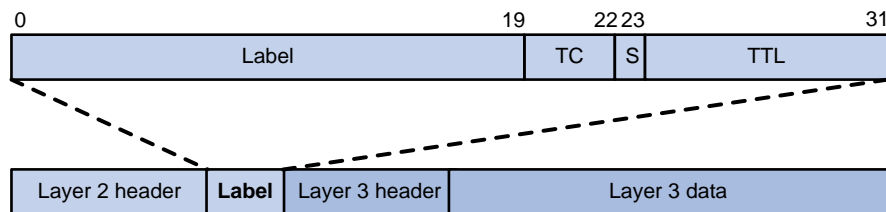
1. 转发等价类

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

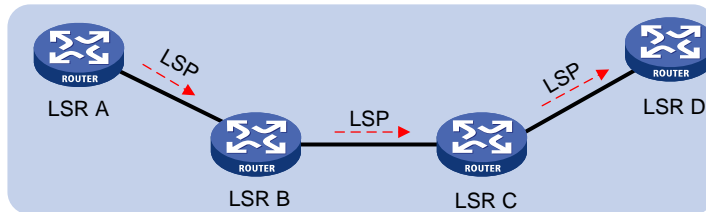
LSR (Label Switching Router, 标签交换路由器) 是具有标签分发能力和标签交换能力的设备, 是 MPLS 网络中的基本元素。

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。

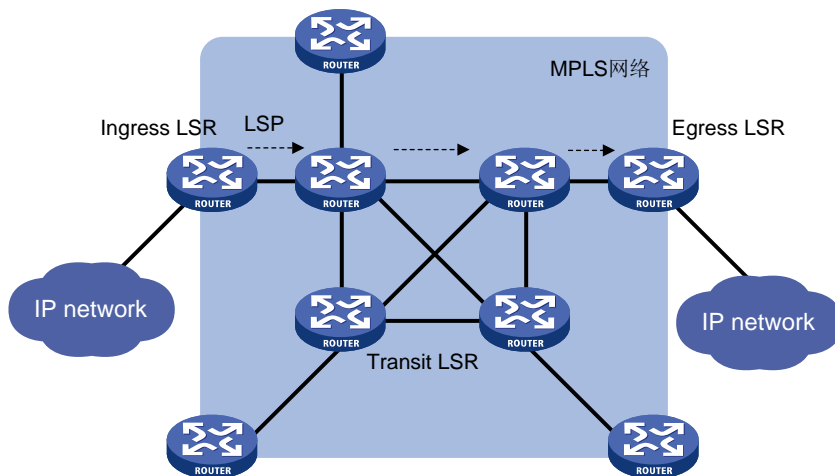
6. 控制平面和转发平面

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。

1.1.3 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。

1.1.4 LSP 建立



说明

M9000 系列产品可建立多条 MPLS LSP，设备最多支持 2 条 MPLS LSP 做等价负载分担，若配置超过 2 条，则只会选择其中一条负载。

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。

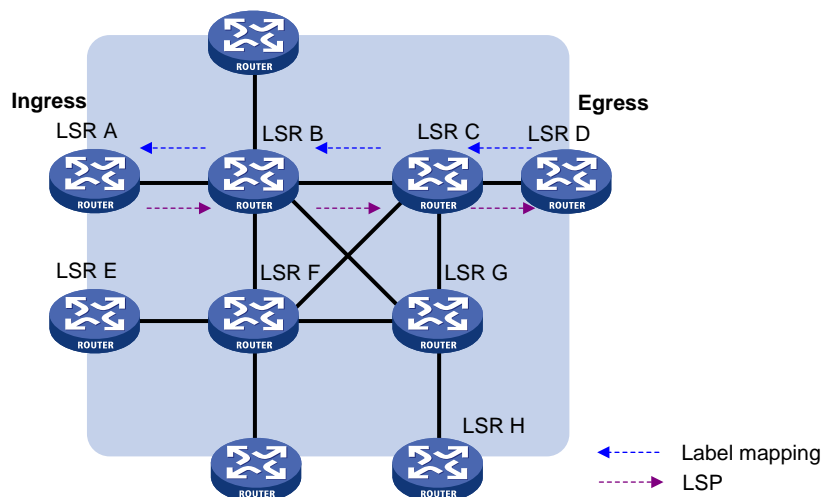


说明

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。

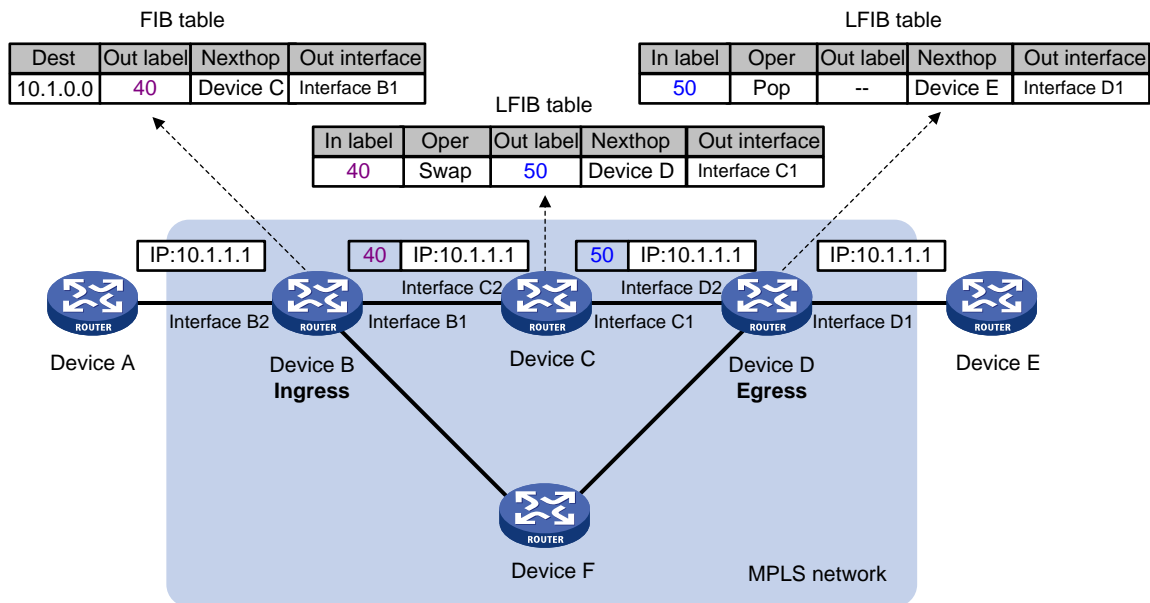
利用标签分发协议动态建立 LSP 的过程如图 1-4 所示。下游 LSR 根据目的地址划分 FEC，为特定 FEC 分配标签，并将 FEC—标签绑定关系通告给上游 LSR；上游 LSR 根据该绑定关系建立标签转发表项。报文转发路径上的所有 LSR 都为该 FEC 建立对应的标签转发表项后，就成功地建立了用于转发属于该 FEC 报文的 LSP。

图1-4 动态 LSP 建立过程



1.1.5 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 (Device 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 (Device C) 和出接口 (Interface B1)，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) **Device 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 (Device D) 和出接口 (Interface C1)，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 (Device 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 (Device E) 和出接口 (Interface D1)，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。

1.1.6 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。

MPLS 通过分配空标签实现倒数第二跳弹出。空标签分为：

- 隐式空标签：取值为 3。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。
- 显式空标签：取值为 0 或 2。0 用于 IPv4 网络；2 用于 IPv6 网络。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。Egress 为 FEC 分配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，并将报文转发给下游 LSR（即 Egress）。Egress 收到标签值为 0 或 2 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。

1.1.7 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

MPLS 配置任务如下：

- (1) [使能 MPLS 功能](#)
- (2) （可选）[配置 MPLS MTU](#)
- (3) （可选）[配置设备作为 Egress 节点时为倒数第二跳分配的标签类型](#)
- (4) （可选）[配置 TTL 复制](#)

开启本功能后，Ingress 节点会将原 IP 报文中的 TTL 值复制到 MPLS 标签的 TTL 域，借助 IP tracer 等工具，可以了解报文在 MPLS 网络中的转发路径。

- (5) （可选）[使能 MPLS 的 TTL 超时消息发送功能](#)
- (6) （可选）[配置 FTN 转发统计功能](#)
- (7) （可选）[配置 LSP 的 MPLS 标签转发统计功能](#)
- (8) （可选）[开启 MPLS 模块的告警功能](#)

1.3 使能MPLS功能

1. 配置准备

在使能 MPLS 功能之前，需要配置单播静态路由或 IGP 协议，保证各 LSR 在网络层互通。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 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 采用点分十进制格式，与 IP 地址格式相同。

LSR ID 在 MPLS 网络内必须唯一，推荐使用 Loopback 接口的 IP 地址作为 LSR ID。

- (3) 进入需要转发 MPLS 报文的接口视图。

```
interface interface-type interface-number
```

- (4) 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。

1.4 配置MPLS MTU

1. 功能简介

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，则直接转发。

2. 硬件适配关系

FG 类单板通过 **hardware fast-forwarding enable** 命令开启硬件转发功能时不支持本功能。有关硬件转发的详细介绍，请参见“三层技术-IP 业务配置指导”中的“快速转发”。

3. 配置限制和指导

MPLS MTU 会影响 IP 入 MPLS 时的流量转发。

不建议将接口 MPLS MTU 值设置过小，否则容易导致因 IP 分片影响性能，严重时甚至出现丢包现象。

配置的 MPLS MTU 值不能大于接口 MTU，否则有可能导致数据转发失败。

如果 MPLS 报文内封装的是 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。

4. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置接口的 MPLS MTU。

```
mpls mtu size
```

缺省情况下，未配置接口的 MPLS MTU 值。此时如果配置了 IP MTU，则根据 IP MTU 进行分片；如果未配置 IP MTU，则根据接口的 MTU 值进行分片。分片的长度不包含 MPLS 标签栈的长度，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。

1.5 配置设备作为Egress节点时为倒数第二跳分配的标签类型

1. 功能简介

请根据实际情况选择 Egress 节点为倒数第二跳分配的标签类型：

- 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，通常情况下不建议使用非空标签。

2. 配置限制和指导

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。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置设备作为 Egress 节点时为倒数第二跳分配的标签类型。

```
mpls label advertise { explicit-null | implicit-null | non-null }
```

缺省情况下，Egress 节点为倒数第二跳分配隐式空标签（`implicit-null`）。

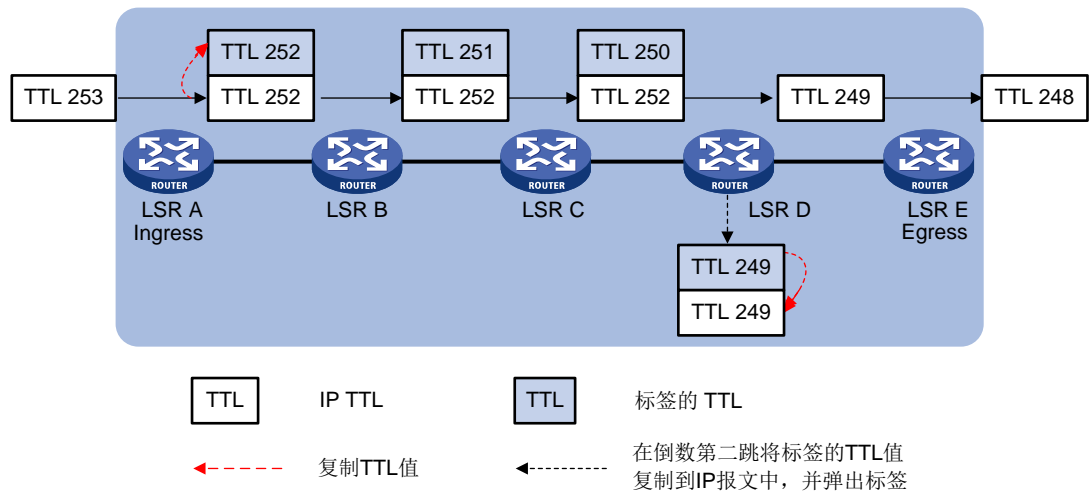
1.6 配置TTL复制

1. 功能简介

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：

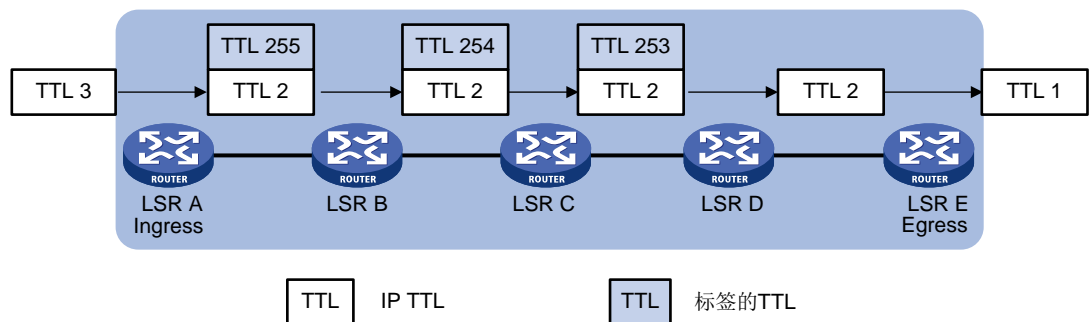
- 使能 TTL 复制功能：Ingress 节点为 IP 报文压入标签时，将原 IP 报文中的 TTL 值复制到新增的标签的 TTL 域。LSR 转发标签报文时，对标签的 TTL 值做减一操作。LSR 弹出报文的标签时，将标签的 TTL 值复制回 IP 报文。使用这种方式时，MPLS 骨干网中的节点对用户网络的报文可见。报文沿着 LSP 传输的过程中，TTL 逐跳递减，Tracert 的结果将反映报文实际经过的路径。

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



2. 硬件适配关系

FG 类单板通过 **hardware fast-forwarding enable** 命令开启硬件转发功能时不支持本功能。有关硬件转发的详细介绍, 请参见“三层技术-IP 业务配置指导”中的“快速转发”。

3. 配置限制和指导

在 MPLS 网络内部, MPLS 报文多层标签之间的 TTL 值总是互相复制。本功能只决定是否将 IP TTL 复制到标签的 TTL 域、是否将标签的 TTL 复制到 IP 的 TTL 域。

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。

4. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 使能 TTL 复制功能。

mpls ttl propagate { public | vpn }

缺省情况下，对于通过公网进行转发的报文，TTL 复制功能处于开启状态；对于通过 VPN 进行转发的报文，TTL 复制功能处于关闭状态。

1.7 使能MPLS的TTL超时消息发送功能

1. 功能简介

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。

2. 硬件适配关系

FG 类单板通过 **hardware fast-forwarding enable** 命令开启硬件转发功能时不支持本功能。有关硬件转发的详细介绍，请参见“三层技术-IP 业务配置指导”中的“快速转发”。

3. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 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FTN转发统计功能

1. 功能简介

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 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。开启该功能后可通过 MIB 查看统计信息。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 进入 RIB 视图。

rib

- (3) 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。

- (4) 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。

- (5) 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。

1.9 配置LSP的MPLS标签转发统计功能

1. 功能简介

LSP 的 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。

本配置用来开启指定 LSP 的 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** 命令查看该 LSP 的 MPLS 标签转发统计信息。

- 对于 RSVP-TE 隧道，通过 **mpls statistics** 命令开启 MPLS 标签转发统计功能后，会自动开启标签转发统计信息的收集功能，统计信息收集的时间间隔为 30 秒。使用 **mpls statistics interval** 命令可以修改统计信息收集的时间间隔。
- 对于其他类型的 LSP，通过 **mpls statistics** 命令开启 MPLS 标签转发统计功能后，还必须执行 **mpls statistics interval** 命令开启统计信息收集功能，并设置统计信息收集的时间间隔。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 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-address mask-length | ipv6 ipv6-address prefix-length } }

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。

- (3) 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。

1.10 开启MPLS模块的告警功能

1. 功能简介

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”。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 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关闭状态。

1.11 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1-1 MPLS 显示和维护

操作	命令
显示ILM表项信息	(独立运行模式) display mpls forwarding ilm [<i>label</i>] [<i>slot slot-number</i> [<i>cpu cpu-number</i>]] (IRF模式) display mpls forwarding ilm [<i>label</i>] [<i>chassis chassis-number slot slot-number</i> [<i>cpu cpu-number</i>]]
显示NHLFE表项信息	(独立运行模式) display mpls forwarding nhlfe [<i>nid</i>] [<i>slot slot-number</i> [<i>cpu cpu-number</i>]] (IRF模式) display mpls forwarding nhlfe [<i>nid</i>] [<i>chassis chassis-number slot slot-number</i> [<i>cpu cpu-number</i>]]
显示使能了MPLS能力接口的MPLS相关信息	display mpls interface [<i>interface-type interface-number</i>]
显示MPLS标签的信息	display mpls label { <i>label-value1</i> [<i>to label-value2</i>] all } [verbose]
显示LSP信息	display mpls lsp [<i>egress</i> <i>in-label label-value</i> <i>ingress</i> <i>outgoing-interface interface-type interface-number</i> <i>protocol</i> { <i>bgp</i> <i>isis</i> <i>ldp</i> <i>local</i> <i>ospf</i> <i>rsvp-te</i> [<i>p2mp</i>] <i>sr-te</i> <i>static</i> <i>static-cr</i> } <i>transit</i>] [<i>vpn-instance vpn-instance-name</i>] [<i>ipv4-address mask-length</i> <i>ipv6</i> [<i>ipv6-address prefix-length</i>]] [verbose]
显示LSP的统计信息	display mpls lsp statistics [<i>ipv6</i>]
显示MPLS的NIB（NextHop Information Base，下一跳信息库）信息	display mpls nib [<i>nib-id</i>]
显示MPLS NHLFE表项索引的使用状态	display mpls nid [<i>nid-value1</i> [<i>to nid-value2</i>]]
显示MPLS汇总信息	display mpls summary
清除指定LSP的MPLS转发统计信息	reset mpls statistics { all [<i>vpn-instance vpn-instance-name</i>] { <i>ipv4 ipv4-address mask-length</i> <i>ipv6 ipv6-address prefix-length</i> } }

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	1-4
1.1.5 LDP GR	1-5
1.1.6 LDP NSR	1-7
1.1.7 LDP 与路由同步	1-7
1.1.8 LDP 快速重路由	1-9
1.1.9 协议规范	1-10
1.2 LDP 配置任务简介	1-10
1.3 使能 LDP 能力	1-11
1.3.1 配置限制和指导	1-11
1.3.2 全局使能 LDP 能力	1-11
1.3.3 在接口上使能 LDP 能力	1-11
1.4 配置 Hello 消息参数	1-12
1.4.1 Hello 消息参数简介	1-12
1.4.2 配置限制和指导	1-12
1.4.3 配置 Link hello 消息参数	1-12
1.4.4 配置 Targeted hello 消息参数	1-12
1.5 配置 LDP 会话参数	1-13
1.5.1 LDP 会话参数简介	1-13
1.5.2 配置限制和指导	1-13
1.5.3 配置基本发现机制的 LDP 会话参数	1-13
1.5.4 配置扩展发现机制的 LDP 会话参数（指定目的地址为 IPv4 地址）	1-14
1.5.5 配置扩展发现机制的 LDP 会话参数（指定目的地址为 IPv6 地址）	1-14
1.6 配置 LDP 倒退机制的延迟时间	1-15
1.7 配置发送的 LDP 报文的 DSCP 优先级	1-15
1.8 配置 LDP 引入 BGP 单播路由	1-16
1.9 配置 LSP 触发策略	1-17
1.10 配置 LDP 标签分发控制方式	1-17
1.11 配置标签通告控制策略	1-18

1.12 配置标签接受控制策略	1-19
1.13 配置 LDP MD5 认证	1-20
1.14 配置 LDP 环路检测	1-21
1.15 配置 LDP 会话保护	1-22
1.16 配置 LDP GR	1-22
1.17 配置 LDP NSR	1-23
1.18 配置 LDP 与路由同步	1-23
1.18.1 配置限制和指导	1-23
1.18.2 配置 LDP 与静态路由同步	1-23
1.18.3 配置 LDP OSPF 同步	1-24
1.18.4 配置 LDP IS-IS 同步	1-25
1.19 配置 LDP 快速重路由	1-26
1.19.1 配置 LDP LFA 快速重路由	1-26
1.19.2 配置 LDP Remote LFA 快速重路由	1-26
1.20 开启 LDP 模块的告警功能	1-27
1.21 LDP 显示和维护	1-27

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。

LDP 协议运行在 IPv4 网络和运行在 IPv6 网络中使用相同格式的 LDP ID，且要求全局唯一。

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（Pseudowire，伪线）划分 FEC。本文只介绍根据目的 IP 地址划分 FEC。

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信息和差错通知，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 协议既可在 IPv4 网络或 IPv6 网络中运行，也可在 IPv4 和 IPv6 并存的网络中运行，LDP 在 IPv4 和 IPv6 网络中的工作过程基本相同。

LDP 工作过程主要包括对等体发现与维护、会话建立与维护、LSP 建立三个阶段。

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。在这种方式下，LSR 周期性地向组播地址 224.0.0.2（IPv4 网络）或 FF02:0:0:0:0:0:0:2（IPv6 网络）发送 LDP 的 Link Hello 消息，以便链路层直接相连的 LSR 发现此 LSR，在 IPv4 和 IPv6 共存的网络中，LSR 会向直连 LSR 同时发送 IPv4 Link Hello 消息和 IPv6 Link Hello 消息，并与邻接 LSR 同时保持 IPv4 Link Hello 邻接关系和 IPv6 Link Hello 邻接关系。
- 扩展发现机制：可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。如果指定的地址为 IPv4 地址，则发送 IPv4 Targeted Hello 消息；如果指定的地址为 IPv6 地址，则发送 IPv6 Targeted Hello 消息。

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未收到新的 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。这一过程可分为两步：

- (1) 建立传输层连接，即在 LSR 之间建立 TCP 连接，在 IPv4 和 IPv6 共存的网络中 LSR 会优先建立 IPv6 TCP 连接，如果长时间没有收到新的 IPv6 Hello 消息，则会尝试建立 IPv4 TCP 连接；
- (2) 通过交换会话初始化消息对 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。

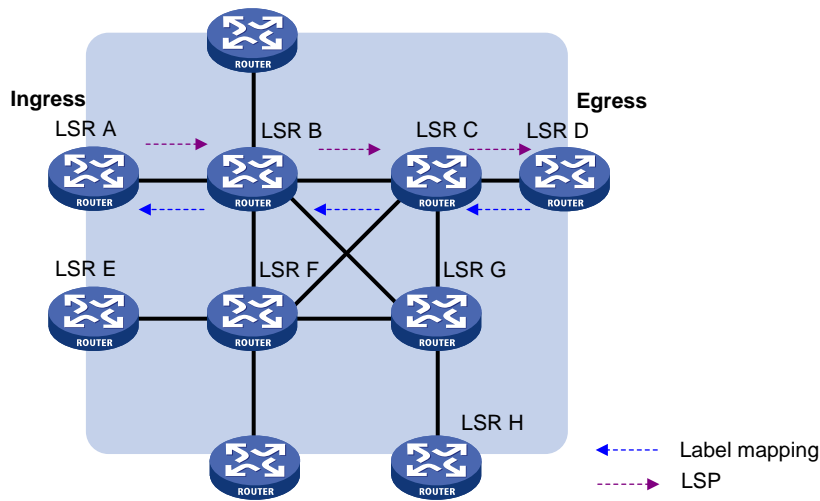
相邻 LSR 之间只会建立一个 LDP 会话，但可在此会话中同时交互 IPv4 FEC—标签映射和 IPv6 FEC—标签映射。

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。

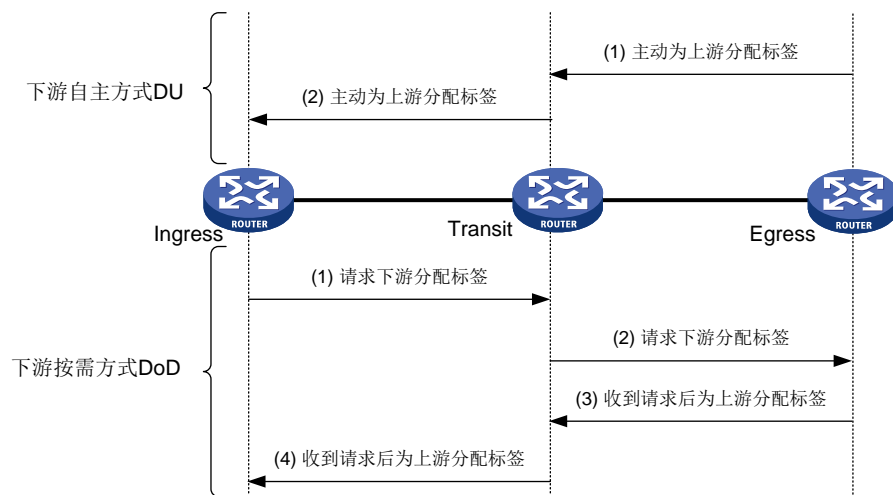
图1-1 动态 LSP 建立过程



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

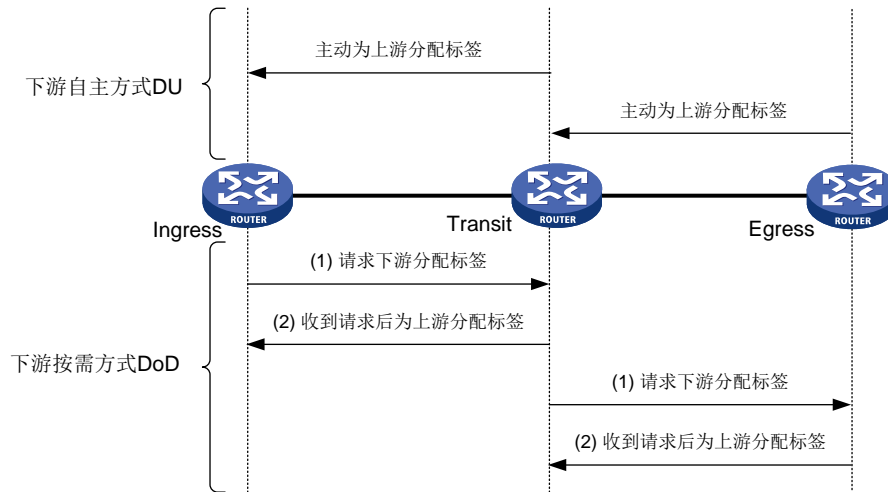
具有标签分发邻接关系的上游 LSR 和下游 LSR 之间必须使用相同的标签通告方式，否则 LSP 无法正常建立。

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：

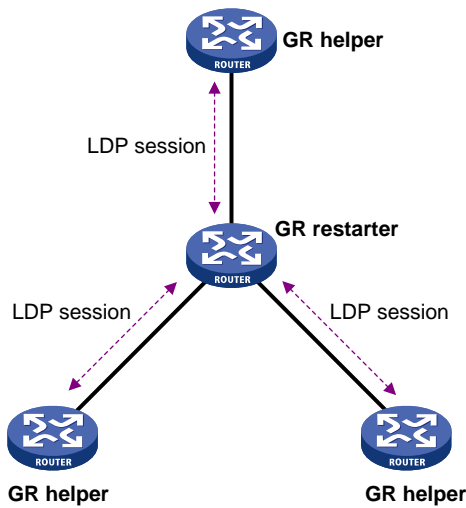
- 自由标签保持方式（Liberal）：对于从邻居 LSR 收到的标签映射，无论邻居 LSR 是不是指定 FEC 的下一跳都保留。这种方式的优点是 LSR 能够迅速适应网络拓扑变化，但是由于需要保留所有不能生成 LSP 的标签，浪费了内存等系统资源。
- 保守标签保持方式（Conservative）：对于从邻居 LSR 收到的标签映射，只有当邻居 LSR 是指定 FEC 的下一跳时才保留。这种方式的优点是节省标签，但是对拓扑变化的响应较慢。

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

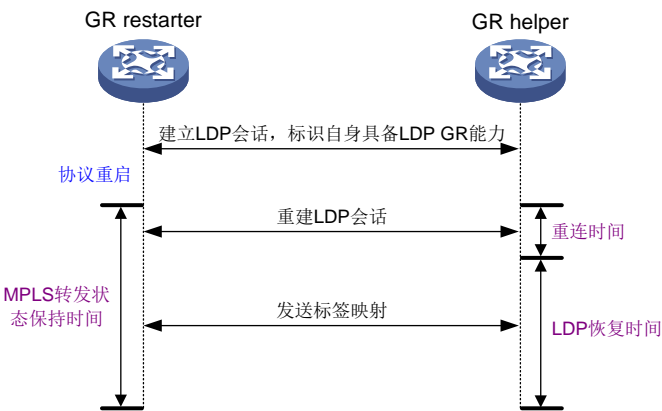


如图 1-4 所示，参与 LDP GR 过程的设备分为以下两种：

- **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

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 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。

1.1.7 LDP 与路由同步

1. LDP 与静态路由同步

LDP 基于静态路由建立 LSP 时，如果 LDP 与静态路由不同步可能导致 MPLS 流量转发中断。LDP 与静态路由不同步包括如下情况：

- 静态路由使用了某条链路，但这条链路上的 LDP LSP 尚未建立。
- 当 LDP 会话 down 时，静态路由继续使用这条链路，而此时这条链路上的 LDP LSP 已经拆除。

开启 LDP 与静态路由同步功能后，只有 LDP 在某条链路上收敛，静态路由的状态才会变为 Active，否则静态路由的状态为 Inactive，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。例如，基于静态路由建立主备 LDP LSP 的组网中，具体的工作机制如下：

- 当主 LSP 出现故障时，静态路由的状态随之变为 Inactive，MPLS 流量切换到备份 LSP。
- 在主 LSP 故障恢复期间，静态路由的状态为 Inactive。当主 LSP 故障恢复时，静态路由的状态随之变为 Active，MPLS 流量回切到主 LSP。

2. LDP 与 IGP 同步

LDP 基于 IGP 最优路由建立 LSP，LDP 与 IGP 不同步可能导致 MPLS 流量转发中断。LDP 与 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。

3. 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。

4. 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

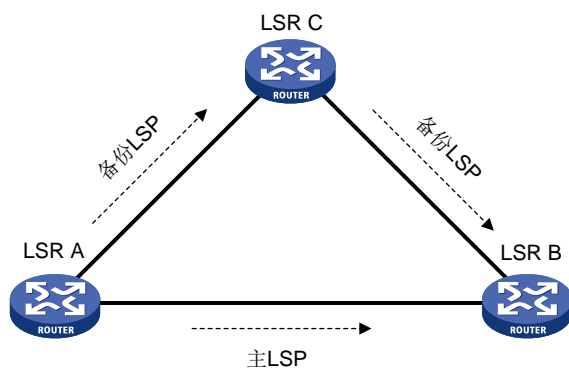
1. LDP LFA 快速重路由

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 LFA（Loop Free Alternate，无环备份）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。IP 快速重路由有两种实现方式：

- IGP 协议自动计算备份下一跳
- 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。

2. LDP Remote LFA 快速重路由

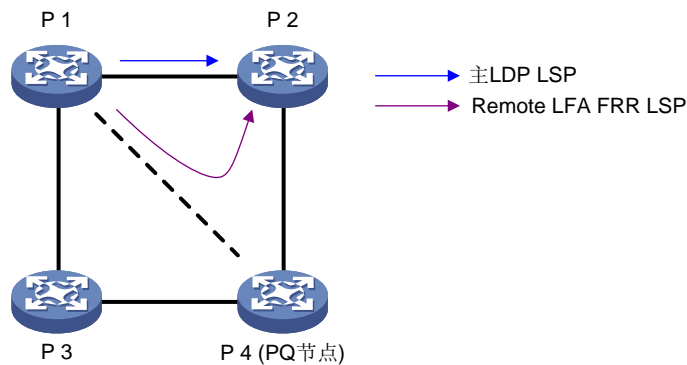
在大型组网中，LDP LFA 快速重路由可能无法计算出备份路径，不能满足可靠性要求，可以通过部署 LDP Remote LFA（Remote Loop Free Alternate，远端无环备份）快速重路由解决该问题。

如图 1-7 所示，P1 为源节点，P2 为目的节点，主 LDP LSP 为 P1→P2，通过 LDP Remote LFA 快速重路由建立 Remote LFA FRR LSP（P1→P4→P2）来保护主 LDP LSP。建立过程为：

- (1) IGP 通过 Remote LFA 算法计算出路由后得到 PQ 节点，PQ 节点为 P4。
- (2) LDP 根据 PQ 节点地址自动创建远端对等体，建立源节点 P1 与 PQ 节点之间的 LDP 远端会话，并在该会话上为目的地址分配标签，从而建立 Remote LFA FRR LSP（P1→P4→P2）以便保护主 LDP LSP。

当主 LDP LSP 发生故障时，P 1 快速将流量切换到 Remote LFA FRR LSP 继续转发，尽量减少流量丢失，从而提高网络可靠性。有关 Remote LFA 的详细介绍，请参见“三层技术-IP 路由配置指导”中的“IS-IS”。

图1-7 LDP Remote LFA 典型组网图



1.1.9 协议规范

与 MPLS 相关的协议规范有：

- RFC 5036: LDP Specification
- draft-ietf-mpls-ldp-ipv6-09.txt

1.2 LDP配置任务简介

LDP 配置任务如下：

- (1) [使能 LDP 能力](#)
- (2) （可选）调整和优化 LDP
 - [配置 Hello 消息参数](#)
 - [配置 LDP 会话参数](#)
 - [配置 LDP 倒退机制的延迟时间](#)
 - [配置发送的 LDP 报文的 DSCP 优先级](#)
- (3) （可选）调整和控制 LSP 的建立
 - [配置 LDP 引入 BGP 单播路由](#)
 - [配置 LSP 触发策略](#)
- (4) （可选）配置 LDP 的标签分发和管理
 - [配置 LDP 标签分发控制方式](#)
 - [配置标签通告控制策略](#)
 - [配置标签接受控制策略](#)
- (5) （可选）[配置 LDP MD5 认证](#)
- (6) （可选）[配置 LDP 环路检测](#)

该功能主要用于存在大量非 TTL 递减设备（如标签控制的 ATM 交换机）的 MPLS 网络。

- (7) (可选) 配置 LDP 高可靠性
 - [配置 LDP 会话保护](#)
 - [配置 LDP GR](#)
 - [配置 LDP NSR](#)
 - [配置 LDP 与路由同步](#)
 - [配置 LDP 快速重路由](#)
- (8) (可选) [开启 LDP 模块的告警功能](#)

1.3 使能LDP能力

1.3.1 配置限制和指导

要使接口的 LDP 能力生效，必须先全局使能 LDP，然后在相应的接口上使能 LDP。

1.3.2 全局使能 LDP 能力

- (1) 进入系统视图。
system-view
- (2) 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
 - 请依次执行以下命令使能指定 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
缺省情况下，LDP 能力处于关闭状态。
- (3) 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。

1.3.3 在接口上使能 LDP 能力

- (1) 进入系统视图。
system-view
- (2) 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。
- (3) 使能接口的 LDP 支持 IPv4 能力。
mpls ldp enable
缺省情况下，接口的 LDP 支持 IPv4 能力处于关闭状态。

- (4) 使能接口的 LDP 支持 IPv6 能力。

```
mpls ldp ipv6 enable
```

缺省情况下，接口的 LDP 支持 IPv6 能力处于关闭状态。

1.4 配置Hello消息参数

1.4.1 Hello 消息参数简介

LDP 的 Hello 消息分为以下几种：

- 用于发现直连邻居的 Link hello 消息，如果在接口上同时使能 LDP 支持 IPv4 能力和 LDP 支持 IPv6 能力，则在接口下配置的 Link Hello 消息参数可同时应用于 IPv4 Link Hello 消息和 IPv6 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。

1.4.2 配置限制和指导

修改 Hello 消息参数，不会对已建立的 LDP 会话生效。如果要求对已建立的会话生效，则需执行 **reset mpls ldp** 命令重启公网或指定 LDP 实例中的所有会话。

1.4.3 配置 Link hello 消息参数

- (1) 进入系统视图。

```
system-view
```

- (2) 进入建立 LDP 会话的接口视图。

```
interface interface-type interface-number
```

- (3) 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。

- (4) 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。

1.4.4 配置 Targeted hello 消息参数

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LDP 视图。

```
mpls ldp
```


- (3) 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 { ipv4-address | ipv6-address }
```

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。

- (4) 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。

- (5) 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

1.5.1 LDP 会话参数简介

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。

1.5.2 配置限制和指导

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。

修改 LDP 会话参数，不会对已建立的 LDP 会话生效。如果要求对已建立的会话生效，则需执行 **reset mpls ldp** 命令重启公网或指定 LDP 实例中的所有会话。

1.5.3 配置基本发现机制的 LDP 会话参数

- (1) 进入系统视图。

```
system-view
```

- (2) 进入建立 LDP 会话的接口视图。

```
interface interface-type interface-number
```

- (3) 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。

- (4) 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。

- (5) 配置 LDP IPv4 传输地址。

```
mpls ldp transport-address { ipv4-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，则本命令指定的传输地址所在的接口需要与同一个 VPN 实例绑定。

- (6) 配置 LDP IPv6 传输地址。

```
mpls ldp transport-address ipv6-address
```

缺省情况下，未配置 LDP IPv6 传输地址。

1.5.4 配置扩展发现机制的 LDP 会话参数（指定目的地址为 IPv4 地址）

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LDP 视图。

```
mpls ldp
```

- (3) 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 ipv4-address
```

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。

- (4) 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。

- (5) 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。

- (6) 配置 LDP 传输地址。

```
mpls ldp transport-address ipv4-address
```

缺省情况下，传输地址是本 LSR 的 LSR ID。

1.5.5 配置扩展发现机制的 LDP 会话参数（指定目的地址为 IPv6 地址）

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LDP 视图。

```
mpls ldp
```

- (3) 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 ipv6-address
```

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。

- (4) 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。

- (5) 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。

- (6) 配置 LDP 传输地址。

```
mpls ldp transport-address ipv6-address
```

缺省情况下，未配置 LDP IPv6 传输地址。

1.6 配置LDP倒退机制的延迟时间

1. 功能简介

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。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LDP 视图或 LDP-VPN 实例视图。

- 进入 LDP 视图。

```
mpls ldp
```

- 请依次执行以下命令进入 LDP-VPN 实例视图。

```
mpls ldp
```

```
vpn-instance vpn-instance-name
```

- (3) 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 配置发送的LDP报文的DSCP优先级

1. 功能简介

DSCP（Differentiated Services Code Point，区分服务编码点）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。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LDP 视图。

```
mpls ldp
```

- (3) 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。

1.8 配置LDP引入BGP单播路由

1. 功能简介

缺省情况下，LDP 自动引入 IGP 路由（包括已引入到 IGP 的 BGP 路由），并为通过 LSP 触发策略的 IGP 路由和通过 LSP 触发策略的带标签 BGP 路由分配标签，但不自动引入未被引入到 IGP 的 BGP 单播路由。这就导致了在一些特殊的组网环境下，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，则无法通过 LDP 为 BGP 单播路由分配标签，因而无法建立 LDP LSP。

通过配置 LDP 引入 BGP 单播路由，可将 BGP 单播路由强制引入至 LDP，如果该路由通过 LSP 触发策略，则为其分配标签建立 LSP。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LDP 视图或 LDP-VPN 实例视图。

- 进入 LDP 视图。

```
mpls ldp
```

- 请依次执行以下命令进入 LDP-VPN 实例视图。

```
mpls ldp
```

```
vpn-instance vpn-instance-name
```

- (3) 配置 LDP 引入 BGP IPv4 单播路由。

```
import bgp [ as-number ]
```

缺省情况下，LDP 不主动引入 BGP IPv4 单播路由。

- (4) 配置 LDP 引入 BGP IPv6 单播路由。

```
ipv6 import bgp [ as-number ]
```

缺省情况下，LDP 不主动引入 BGP IPv6 单播路由。

1.9 配置LSP触发策略

1. 功能简介

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。对于 Loopback 接口，仅 32 位掩码的路由可以触发 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 IPv4 主机路由或 128 位前缀的 IPv6 主机路由能够触发 LDP 建立 LSP。

2. 配置限制和指导

缺省情况下，只有 32 位掩码的 IPv4 主机路由或 128 位前缀的 IPv6 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。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LDP 视图或 LDP-VPN 实例视图。

- 进入 LDP 视图。

```
mpls ldp
```

- 请依次执行以下命令进入 LDP-VPN 实例视图。

```
mpls ldp
```

```
vpn-instance vpn-instance-name
```

- (3) 配置 IPv4 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 IPv4 主机路由能够触发 LDP 建立 LSP。

- (4) 配置 IPv6 LSP 的触发策略。

```
ipv6 lsp-trigger { all | prefix-list prefix-list-name }
```

缺省情况下，只有引入到 LDP 的 128 位前缀的 IPv6 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

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LDP 视图或 LDP-VPN 实例视图。

- 进入 LDP 视图。

```
mpls ldp
```

- 请依次执行以下命令进入 LDP-VPN 实例视图。

```
mpls ldp
```

```
vpn-instance vpn-instance-name
```

- (3) 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**）。

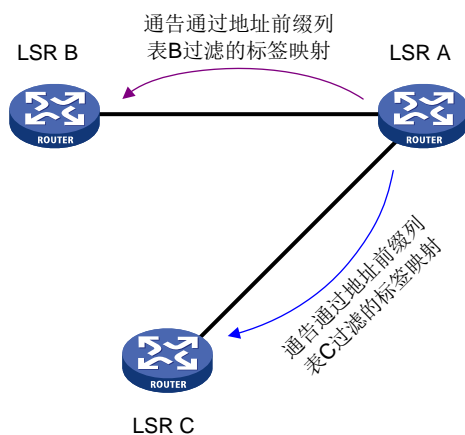
1.11 配置标签通告控制策略

1. 功能简介

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 1-8，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1-8 标签通告控制示意图



2. 配置限制和指导

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”。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LDP 视图或 LDP-VPN 实例视图。

- 进入 LDP 视图。

```
mpls ldp
```

- 。请依次执行以下命令进入 LDP-VPN 实例视图。

```
mpls ldp
```

```
vpn-instance vpn-instance-name
```

- (3) 配置 IPv4 FEC 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 IPv4 地址前缀的标签映射。

- (4) 配置 IPv6 FEC 标签通告控制策略。

```
ipv6 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 IPv6 地址前缀的标签映射。

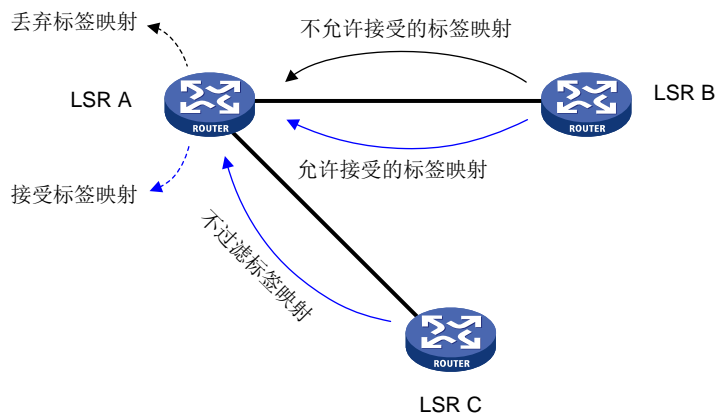
1.12 配置标签接受控制策略

1. 功能简介

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 1-9，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1-9 标签接受控制示意图



2. 配置限制和指导

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”。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LDP 视图或 LDP-VPN 实例视图。

- 进入 LDP 视图。

```
mpls ldp
```

- 请依次执行以下命令进入 LDP-VPN 实例视图。

```
mpls ldp
```

```
vpn-instance vpn-instance-name
```

- (3) 配置 IPv4 FEC 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 IPv4 地址前缀的标签映射。

- (4) 配置 IPv6 FEC 标签接受控制策略。

```
ipv6 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 IPv6 地址前缀的标签映射。

1.13 配置 LDP MD5 认证

1. 功能简介

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。

2. 配置限制和指导

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。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LDP 视图或 LDP-VPN 实例视图。

- 进入 LDP 视图。

```
mpls ldp
```

- 请依次执行以下命令进入 LDP-VPN 实例视图。

```
mpls ldp
```

```
vpn-instance vpn-instance-name
```

- (3) 使能 LDP 的 MD5 认证功能。

```
md5-authentication peer-lsr-id { cipher | plain } string
```

缺省情况下，LDP 的 MD5 认证功能处于关闭状态。

1.14 配置LDP环路检测

1. 功能简介

LDP 环路检测功能用来在 LSP 的建立过程中检测是否存在环路，如果检测到环路则终止 LSP 的建立，从而避免 LSP 环路。该功能主要用于存在大量非 TTL 递减设备（如标签控制的 ATM 交换机）的 MPLS 网络。

开启 LDP 环路检测功能后，将同时使用如下两种方式检测环路，任一方式检测到环路都会终止 LSP 的建立过程：

- 最大跳数环路检测方式：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。Egress 节点发送的标签映射消息和 Ingress 节点发送的标签请求消息中跳数为 1。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。
- 路径向量环路检测方式：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。

Egress 节点发送标签映射消息和 Ingress 节点发送标签请求消息时，本地节点（Egress 或 Ingress 节点）的 LSR ID 不会记录到路径信息中。

2. 配置限制和指导

LSP 经过的所有 LSR 均开启本功能才能够实现环路检测。

LDP 环路检测功能会产生额外处理开销占用带宽，MPLS 网络中大多设备支持 TTL 递减时，可以通过 TTL 递减机制避免报文被无限循环转发，不建议开启本功能。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LDP 视图或 LDP-VPN 实例视图。

- 进入 LDP 视图。

```
mpls ldp
```

- 请依次执行以下命令进入 LDP-VPN 实例视图。

```
mpls ldp
```

```
vpn-instance vpn-instance-name
```

- (3) 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。

- (4) （可选）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。

- (5) （可选）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。

1.15 配置LDP会话保护

1. 功能简介

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 一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 一标签映射等信息，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。

2. 配置限制和指导

LDP 会话保护功能仅支持在 IPv4 网络中进行配置。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LDP 视图。

```
mpls ldp
```

- (3) 使能会话保护功能。

```
session protection [ duration time ] [ peer peer-prefix-list-name ]
```

缺省情况下，会话保护功能处于关闭状态。

1.16 配置LDP GR

1. 配置准备

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。

2. 配置限制和指导

只需要在作为 GR Restarter 的设备上进行以下配置，但由于设备在 GR 过程中的角色不可预知，建议在所有设备上均进行以下配置。

3. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 进入 LDP 视图。

mpls ldp

- (3) 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。

- (4) （可选）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。

- (5) （可选）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。

1.17 配置 LDP NSR

- (1) 进入系统视图。

system-view

- (2) 进入 LDP 视图。

mpls ldp

- (3) 使能 LDP NSR 功能。

non-stop-routing

缺省情况下，LDP NSR 功能处于关闭状态。

1.18 配置 LDP 与路由同步

1.18.1 配置限制和指导

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，在某个接口上关闭 LDP IGP 同步功能。

LDP IGP 同步功能仅支持在 IPv4 网络中进行配置。

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。

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。

1.18.2 配置 LDP 与静态路由同步

- (1) 进入系统视图。

system-view

- (2) 开启 LDP 与静态路由同步功能。

(公网)

```
ip route-static { dest-address { mask-length | mask } | group group-name }  
interface-type interface-number ldp-sync
```

(VPN 网络)

```
ip route-static vpn-instance s-vpn-instance-name dest-address  
{ mask-length | mask } interface-type interface-number ldp-sync
```

```
ip route-static vpn-instance s-vpn-instance-name group group-name  
interface-type interface-number ldp-sync
```

缺省情况下，LDP 与静态路由同步功能处于关闭状态。

有关本命令的详细介绍，请参见“三层技术-IP 路由命令参考”中的“静态路由”。

1.18.3 配置 LDP OSPF 同步

1. 在 OSPF 进程下配置 LDP OSPF 同步

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 OSPF 视图。

```
ospf [ process-id | router-id router-id ] *
```

- (3) 使能 LDP OSPF 同步功能。

```
mpls ldp sync
```

缺省情况下，LDP OSPF 同步功能处于关闭状态。

- (4) (可选) 在接口上关闭 LDP IGP 同步功能。

- a. 退回系统视图。

```
quit
```

- b. 进入接口视图。

```
interface interface-type interface-number
```

- c. 关闭接口的 LDP IGP 同步功能。

```
mpls ldp igp sync disable
```

缺省情况下，接口上的 LDP IGP 同步功能处于开启状态。

- (5) (可选) 配置 LDP OSPF 同步相关参数。

- a. 退回系统视图。

```
quit
```

- b. 进入 LDP 视图。

```
mpls ldp
```

- c. 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。

- d. 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。

2. 在 OSPF 区域下配置 LDP OSPF 同步

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 OSPF 视图。

```
ospf [ process-id | router-id router-id ] *
```

- (3) 进入 OSPF 区域视图。

```
area area-id
```

- (4) 使能 LDP OSPF 同步功能。

```
mpls ldp sync
```

缺省情况下，LDP OSPF 同步功能处于关闭状态。

- (5) （可选）在接口上关闭 LDP IGP 同步功能。

- a. 退回系统视图。

```
quit
```

- b. 进入接口视图。

```
interface interface-type interface-number
```

- c. 关闭接口的 LDP IGP 同步功能。

```
mpls ldp igp sync disable
```

缺省情况下，接口上的 LDP IGP 同步功能处于开启状态。

- (6) （可选）配置 LDP OSPF 同步相关参数。

- a. 退回系统视图。

```
quit
```

- b. 进入 LDP 视图。

```
mpls ldp
```

- c. 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。

- d. 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。

1.18.4 配置 LDP IS-IS 同步

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 IS-IS 视图。

```
isis [ process-id ]
```

- (3) 使能 LDP IS-IS 同步功能。

```
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。

- (4) （可选）在接口上关闭 LDP IGP 同步功能。

- a. 退回系统视图。

```
quit
```

- b. 进入接口视图。

```
interface interface-type interface-number
```

- c. 关闭接口的 LDP IGP 同步功能。

```
mpls ldp igp sync disable
```

缺省情况下，接口上的 LDP IGP 同步功能处于开启状态。

- (5) （可选）配置 LDP IS-IS 同步相关参数。

- a. 退回系统视图。

```
quit
```

- b. 进入 LDP 视图。

```
mpls ldp
```

- c. 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。

- d. 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。

1.19 配置LDP快速重路由

1.19.1 配置 LDP LFA 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”。

1.19.2 配置 LDP Remote LFA 快速重路由

1. 配置限制和指导

在 Remote LFA 组网场景中，请在 PQ 节点配置本功能。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LDP 视图。

```
mpls ldp
```

- (3) 开启设备根据 Targeted Hello 消息自动建立 LDP Targeted 会话的功能。

```
accept target-hello { all | prefix-list prefix-list-name }
```

缺省情况下，设备根据 Targeted Hello 消息自动建立 LDP Targeted 会话的功能处于关闭状态。

1.20 开启LDP模块的告警功能

1. 功能简介

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”。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 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。

1.21 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。

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

表1-1 显示 LDP 运行状态

操作	命令
显示LDP发现过程相关信息	display mpls ldp discovery [vpn-instance <i>vpn-instance-name</i>] [[interface <i>interface-type</i> <i>interface-number</i> peer <i>peer-lsr-id</i>] [ipv6] targeted-peer { <i>ipv4-address</i> <i>ipv6-address</i> }] [verbose]
显示通过LDP学习到的FEC—标签映射信息	display mpls ldp fec [vpn-instance <i>vpn-instance-name</i>] [<i>ipv4-address mask-length</i> <i>ipv6-address prefix-length</i>] [ipv6] [summary]]
显示接口的LDP IGP同步信息	display mpls ldp igp sync [interface <i>interface-type</i> <i>interface-number</i>]
显示使能了LDP能力的接口的LDP相关信息	display mpls ldp interface [vpn-instance <i>vpn-instance-name</i>] [<i>interface-type</i> <i>interface-number</i>] [ipv6]
显示LDP协议生成的LSP信息，即LDP LSP信息	display mpls ldp lsp [vpn-instance <i>vpn-instance-name</i>] [<i>ipv4-address mask-length</i> <i>ipv6-address prefix-length</i>] [ipv6]
显示LDP的运行参数	display mpls ldp parameter [vpn-instance <i>vpn-instance-name</i>]

操作	命令
显示LDP对等体和LDP会话信息	display mpls ldp peer [vpn-instance <i>vpn-instance-name</i>] [<i>peer-lsr-id</i>] [verbose]
显示LDP运行数据汇总信息	display mpls ldp summary [all vpn-instance <i>vpn-instance-name</i>]
重启LDP会话	reset mpls ldp [vpn-instance <i>vpn-instance-name</i>] [peer <i>peer-id</i>]

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 多角色主机	1-7
1.1.7 OSPF VPN 扩展	1-8
1.1.8 BGP 的 AS 号替换和 SoO 属性	1-10
1.1.9 MPLS L3VPN 快速重路由	1-11
1.1.10 VPN 引入等价路由	1-13
1.1.11 协议规范	1-14
1.2 vSystem 相关说明	1-14
1.3 MPLS L3VPN 配置准备	1-15
1.4 配置 VPN 实例	1-15
1.4.1 创建 VPN 实例	1-15
1.4.2 配置 VPN 实例与三层接口关联	1-16
1.4.3 配置 VPN 实例的路由相关属性	1-16
1.5 配置 PE-CE 间的路由交换	1-17
1.5.1 配置 PE-CE 间使用静态路由	1-17
1.5.2 配置 PE-CE 间使用 RIP	1-17
1.5.3 配置 PE-CE 间使用 OSPF	1-18
1.5.4 配置 PE-CE 间使用 IS-IS	1-19
1.5.5 配置 PE-CE 间使用 EBGP	1-20
1.6 配置 PE-PE 间的路由交换	1-21
1.7 配置 BGP VPNv4 路由	1-22
1.7.1 功能简介	1-22
1.7.2 控制 BGP VPNv4 路由的发布、接收和保存	1-22
1.7.3 配置 BGP VPNv4 路由的首选值	1-22
1.7.4 配置 BGP VPNv4 路由反射	1-23
1.7.5 配置 BGP VPNv4 路由过滤	1-24
1.7.6 配置 BGP VPNv4 路由衰减	1-25

1.7.7 提高邻居路由参与优选时的优先级	1-25
1.8 配置多角色主机	1-26
1.8.1 功能简介	1-26
1.8.2 配置并应用策略路由	1-26
1.8.3 配置静态路由	1-26
1.9 配置 Egress PE 上私网路由标签操作方式	1-27
1.10 配置 MPLS L3VPN 快速重路由	1-27
1.10.1 功能简介	1-27
1.10.2 配置限制和指导	1-27
1.10.3 通过路由策略配置快速重路由功能	1-28
1.10.4 开启 BGP-VPN IPv4 单播地址族的快速重路由功能	1-29
1.11 配置 OSPF 伪连接.....	1-29
1.11.1 功能简介	1-29
1.11.2 配置准备	1-29
1.11.3 发布 Loopback 接口的路由	1-30
1.11.4 创建伪连接.....	1-30
1.12 配置 BGP 的 AS 号替换和 SoO 属性	1-31
1.13 配置 RT-Filter 功能	1-31
1.14 配置 BGP Add-Path	1-33
1.15 配置路由信息引入功能	1-34
1.16 开启 VPN 引入等价路由功能	1-35
1.17 配置优先发送指定路由的撤销消息	1-35
1.18 开启告警功能.....	1-36
1.19 MPLS L3VPN 显示和维护	1-36
1.19.1 复位 BGP 会话	1-36
1.19.2 显示和维护 MPLS L3VPN 的运行状态	1-37
2 IPv6 MPLS L3VPN	2-1
2.1 IPv6 MPLS L3VPN 简介	2-1
2.1.1 IPv6 MPLS L3VPN 典型组网环境.....	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 协议规范	2-3
2.2 vSystem 相关说明	2-3
2.3 IPv6 MPLS L3VPN 配置限制和指导.....	2-3
2.4 IPv6 MPLS L3VPN 配置任务简介	2-3
2.5 IPv6 MPLS L3VPN 配置准备	2-4

2.6 配置 VPN 实例	2-4
2.6.1 创建 VPN 实例	2-4
2.6.2 配置 VPN 实例与三层接口关联	2-4
2.6.3 配置 VPN 实例的路由相关属性	2-5
2.7 配置 PE-CE 间的路由交换	2-6
2.7.1 配置 PE-CE 间使用 IPv6 静态路由	2-6
2.7.2 配置 PE-CE 间使用 RIPng	2-6
2.7.3 配置 PE-CE 间使用 OSPFv3	2-7
2.7.4 配置 PE-CE 间使用 IPv6 IS-IS	2-9
2.7.5 配置 PE-CE 间使用 EBGp	2-9
2.8 配置 PE-PE 间的路由交换	2-11
2.9 配置 BGP VPNv6 路由	2-11
2.9.1 功能简介	2-11
2.9.2 配置 BGP VPNv6 路由的首选值	2-11
2.9.3 配置允许从指定对等体/对等体组收到的路由数量	2-12
2.9.4 配置 BGP VPNv6 路由属性	2-12
2.9.5 配置 BGP VPNv6 路由过滤	2-13
2.9.6 提高邻居路由参与优选时的优先级	2-14
2.10 配置多角色主机	2-14
2.10.1 功能简介	2-14
2.10.2 配置并应用策略路由	2-14
2.10.3 配置静态路由	2-15
2.11 配置 OSPFv3 伪连接	2-15
2.11.1 配置准备	2-15
2.11.2 发布 Loopback 接口的路由	2-15
2.11.3 创建伪连接	2-16
2.12 配置 BGP 的 AS 号替换和 SoO 属性	2-16
2.13 配置 BGP Add-Path	2-17
2.14 配置路由信息引入功能	2-18
2.15 配置优先发送指定路由的撤销消息	2-19
2.16 IPv6 MPLS L3VPN 显示和维护	2-19
2.16.1 复位 BGP 会话	2-19
2.16.2 显示 IPv6 MPLS L3VPN 的运行状态	2-20

1 MPLS L3VPN

1.1 MPLS L3VPN简介

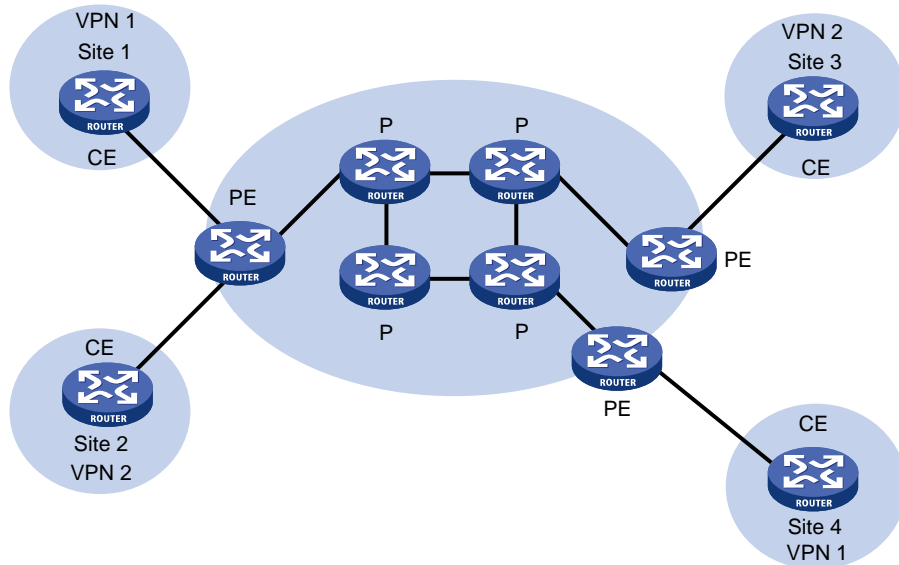
MPLS L3VPN 是一种三层 VPN 技术，它使用 BGP 在服务提供商骨干网上发布用户站点的私网路由，使用 MPLS 在服务提供商骨干网上转发用户站点之间的私网报文，从而实现通过服务提供商的骨干网连接属于同一个 VPN、位于不同地理位置的用户站点。MPLS L3VPN 组网方式灵活，可扩展性好，并能够方便地支持 MPLS QoS 和 MPLS TE，因此得到了广泛的应用。

1.1.1 MPLS L3VPN 基本网络架构

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。

图1-1 MPLS L3VPN 基本网络架构



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）、Route Target 属性、路由过滤策略** 等。

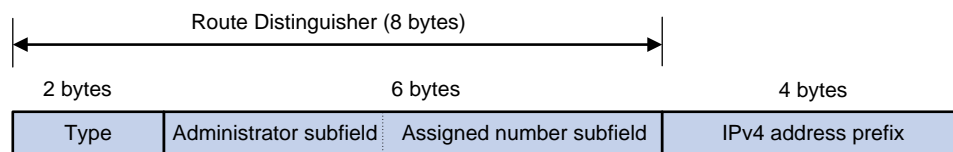
3. VPN-IPv4 地址

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. Route Target 属性

MPLS L3VPN 使用 BGP 扩展团体属性——Route Target (也称为 VPN Target) 来控制 VPN 路由信息的发布。

Route 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。

Route 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, Route 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、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。

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。

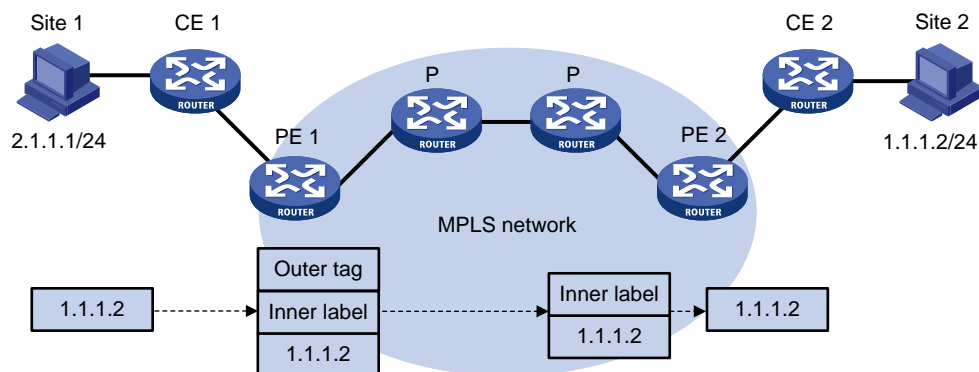


提示

目前，MPLS L3VPN 不支持采用 GRE over IPv6 隧道作为公网隧道。

- 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 根据私网标签可以确定报文所属的 VPN 实例，通过查找该 VPN 实例的路由表，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所属的 VPN 实例，通过查找该 VPN 实例的路由表，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。

1.1.5 MPLS L3VPN 常见组网方案

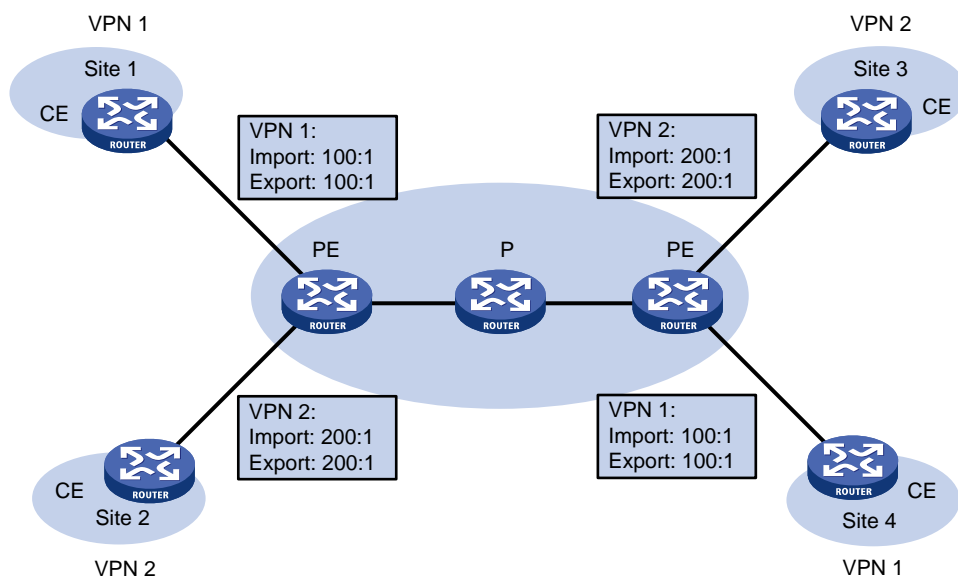
在 MPLS L3VPN 网络中，通过 Route Target 属性来控制 VPN 路由信息在各 Site 之间的发布和接收。VPN Export Target 和 Import Target 的设置相互独立，并且都可以设置多个值，能够实现灵活的 VPN 访问控制，从而实现多种 VPN 组网方案。

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 Route Target，作为该 VPN 的 Export Target 和 Import Target，且此 Route 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 Route Target 值为 100:1，为 VPN 2 分配的 Route 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。

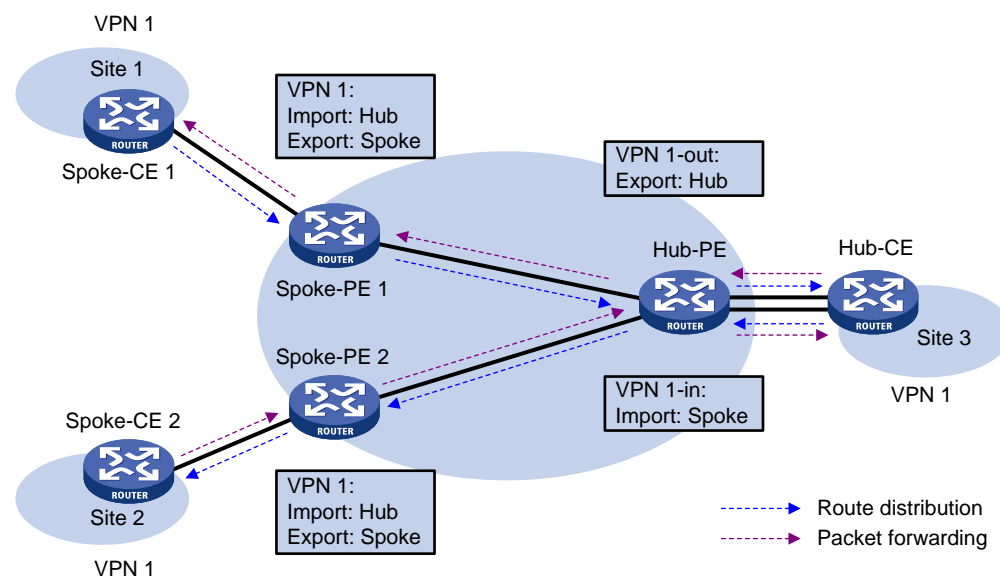
对于这种组网，Route Target 设置规则为：

- Spoke-PE：Export Target 为 “Spoke”，Import Target 为 “Hub”；
- Hub-PE：Hub-PE 上需要使用两个接口连接 Hub-CE，两个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 Route 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。

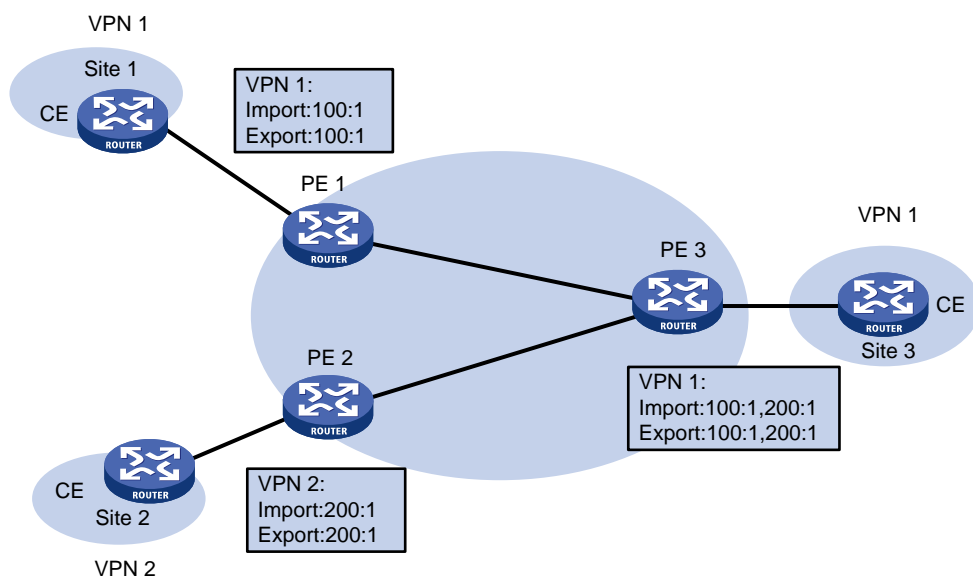
Spoke 站点之间通过 Hub 站点完成路由交互后，Spoke 站点之间的通信将通过 Hub 站点进行。

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 Route 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。

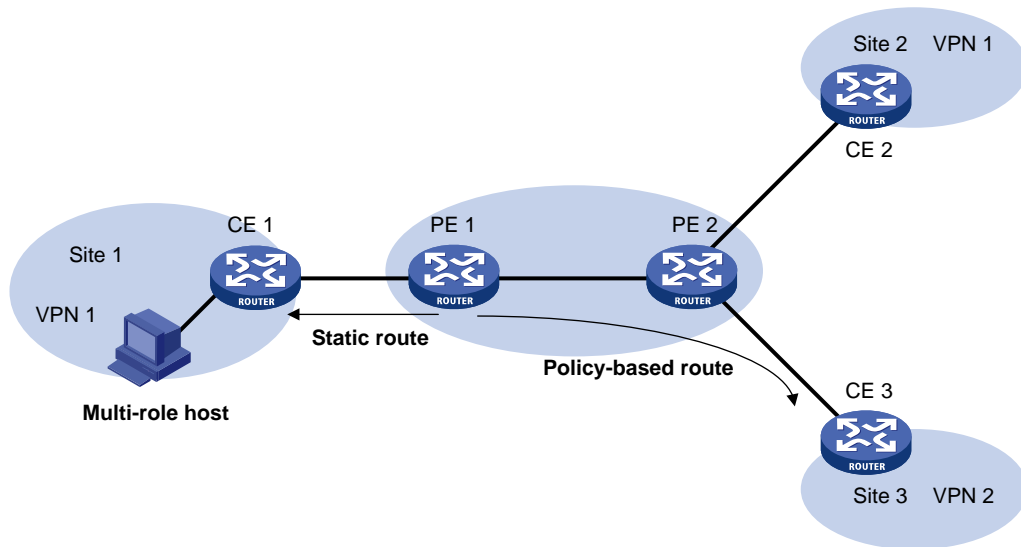
1.1.6 多角色主机

Site 所属的 VPN 由 PE 上连接 Site 的接口关联的 VPN 实例决定，即 PE 从同一个接口接收到的来自 Site 的报文都通过同一个 VPN 实例转发。在实际组网中，Site 内的某些主机或服务器可能需要

访问多个 VPN，而其他主机或服务器只需访问某个 VPN。虽然可以通过设置多个逻辑接口来实现上述需求，但会增加额外的配置负担，使用起来也有局限性。

多角色主机功能通过在 PE 上配置策略路由，使得来自 Site 内某些主机或服务器的报文可以访问多个 VPN。这些主机或服务器称为多角色主机。

图1-7 多角色主机示意图



如图 1-7 所示，多角色主机组网中，PE 上需要进行如下配置：

- 将连接 Site 的接口与某个 VPN 实例关联。
- 配置策略路由，实现对于来自多角色主机的报文，在关联 VPN 实例的路由表内查找不到路由时，在其它 VPN 实例的路由表内查找路由，从而保证 Site 发送给 PE 的报文不仅可以转发到关联的 VPN，还可以转发到其它的 VPN。
- 为其它的 VPN 实例配置静态路由，指定到达多角色主机的路由的下一跳为关联 VPN 实例内 CE 的 IP 地址，从而实现 PE 将其它 VPN 发送的报文转发到该 Site。

在多角色主机组网中，应保证多角色主机所能访问的所有 VPN 内 IP 地址不能重叠。

1.1.7 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

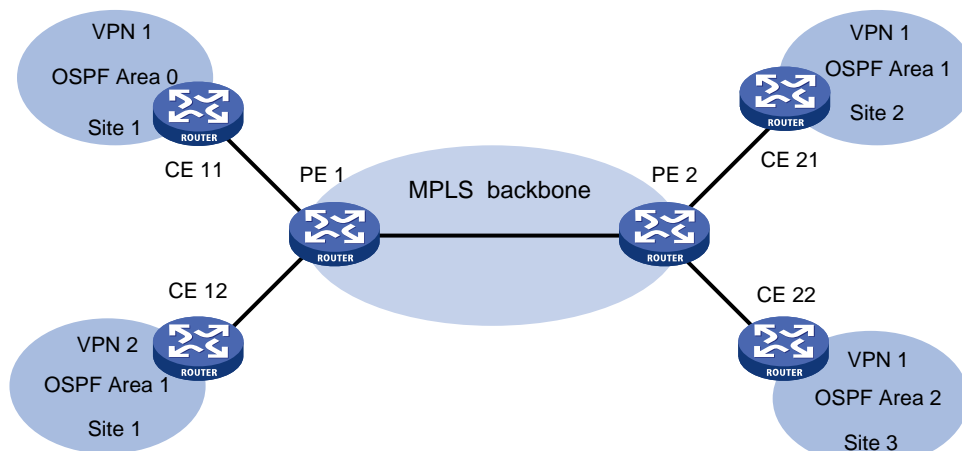
PE 与 CE 之间的 OSPF 区域可以是非骨干区域，也可以是骨干区域。

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1-8 BGP/OSPF 交互示意图



以图 1-8 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。

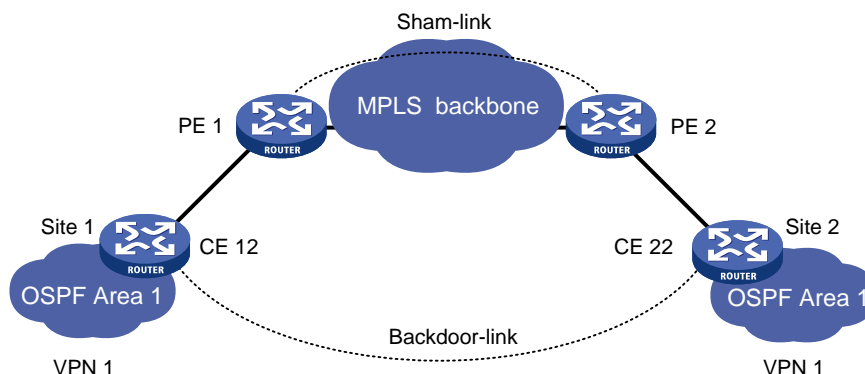
4. OSPF 伪连接

如图 1-9 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1-9 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。

1.1.8 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。

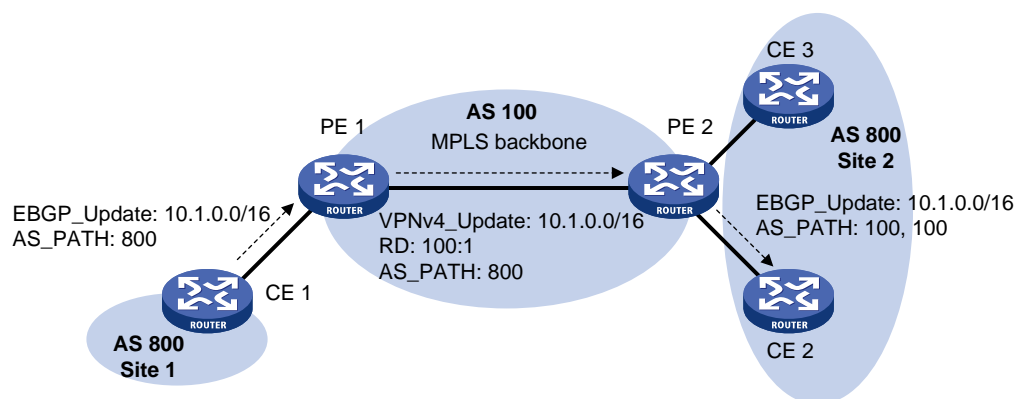
如果物理位置不同的 CE 复用相同的 AS 号，则需要在 PE 上配置 BGP 的 AS 号替换功能，当 PE 向指定对等体（CE）发布路由时，如果路由的 AS_PATH 中存在 CE 所在的 AS 号，则 PE 将该 AS 号替换成 PE 的 AS 号后，再发布该路由，以保证私网路由能够正确发布。



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1-10 BGP AS 号替换和 SoO 应用示意图



在图 1-10 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 1-10 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”。

1.1.9 MPLS L3VPN 快速重路由

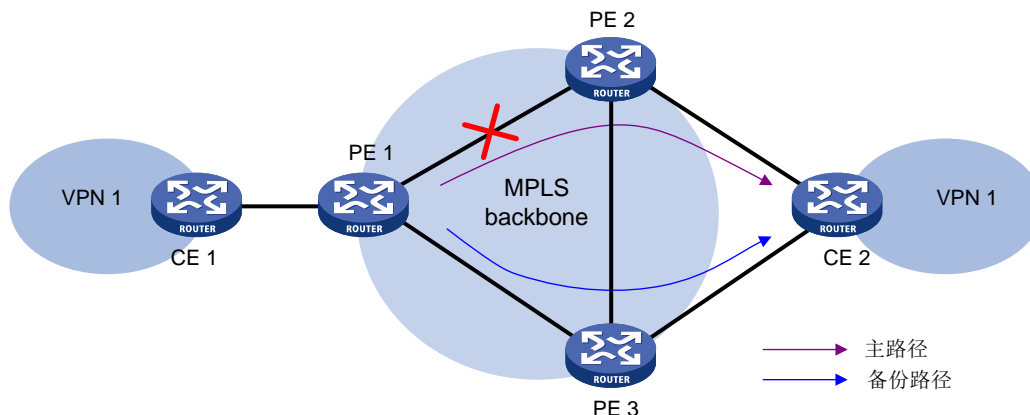
MPLS L3VPN FRR（Fast Reroute，快速重路由）功能用来在 CE 双归属（即一个 CE 同时连接两个 PE）的组网环境下，通过为流量转发的主路径指定一条备份路径，并通过 BFD 检测主路径的状态，实现当主路径出现故障时，将流量迅速切换到备份路径，大大缩短了故障恢复时间。在使用备份路径转发报文的同时，会重新进行路由优选，优选完毕后，使用新的最优路由来转发报文。

MPLS L3VPN 快速重路由的路径备份方式分为如下几种：

- VPNv4 路由备份 VPNv4 路由
- VPNv4 路由备份 IPv4 路由
- IPv4 路由备份 VPNv4 路由

1. VPNv4 路由备份 VPNv4 路由

图1-11 VPNv4 路由备份 VPNv4 路由示意图



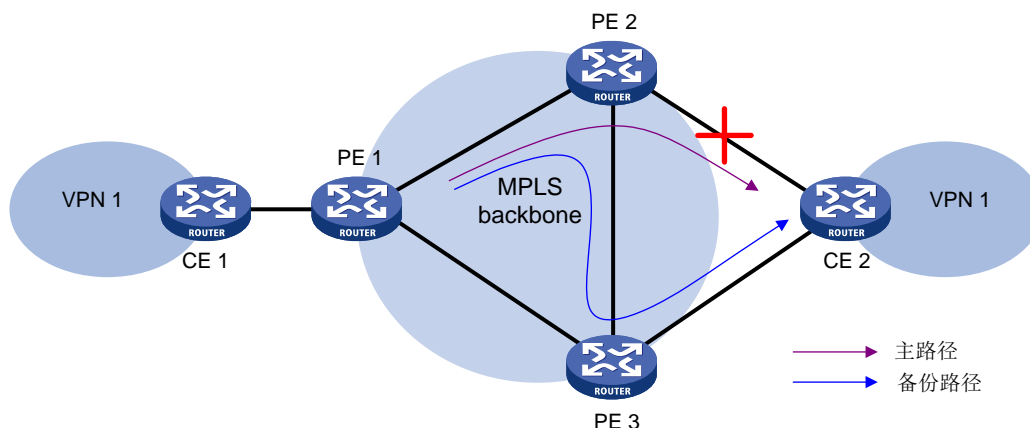
如图 1-11 所示，在入节点 PE 1 上指定 VPN 1 的 FRR 备份下一跳为 PE 3，则 PE 1 接收到 PE 2 和 PE 3 发布的到达 CE 2 的 VPNv4 路由后，PE 1 会记录这两条 VPNv4 路由，并将 PE 2 发布的 VPNv4 路由当作主路径，PE 3 发布的 VPNv4 路由当作备份路径。

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。

2. VPNv4 路由备份 IPv4 路由

图1-12 VPNv4 路由备份 IPv4 路由示意图

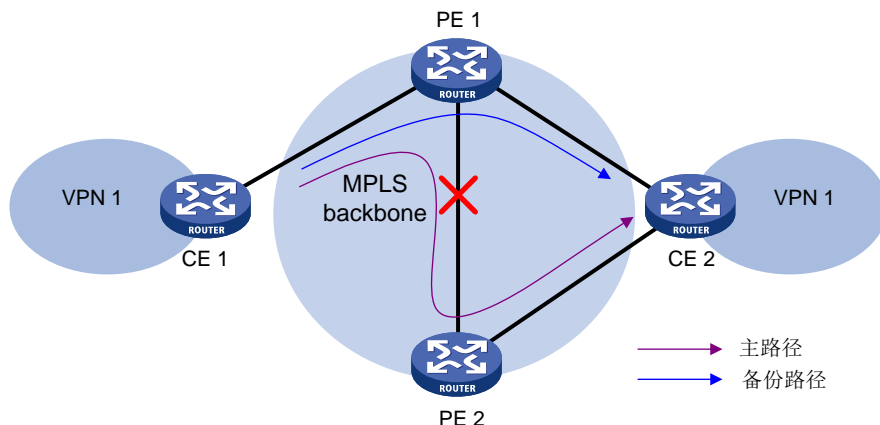


如图 1-12 所示，在出节点 PE 2 上指定 VPN 1 的 FRR 备份下一跳为 PE 3，则 PE 2 接收到 CE 2 发布的 IPv4 路由和 PE 3 发布的到达 CE 2 的 VPNv4 路由后，PE 2 会记录这两条路由，并将 CE 2 发布的 IPv4 路由当作主路径，PE 3 发布的到达 CE 2 的 VPNv4 路由当作备份路径。同时，PE 2 通过 ARP 或 Echo 方式的 BFD 会话检测 PE 2—CE 2 这条路径的状态。当此路径正常工作时，CE 1 和 CE 2 通过主路径 CE 1—PE 1—PE 2—CE 2 通信。当 PE 2 检测到路径 PE 2—CE 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1-13 IPv4 路由备份 VPNv4 路由示意图



如图 1-13 所示，在 PE 1 上指定 VPN 1 的 FRR 备份下一跳为 CE 2，则 PE 1 接收到 CE 2 发布的 IPv4 路由和 PE 2 发布的到达 CE 2 的 VPNv4 路由后，PE 1 会记录这两条路由，并将 PE 2 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。

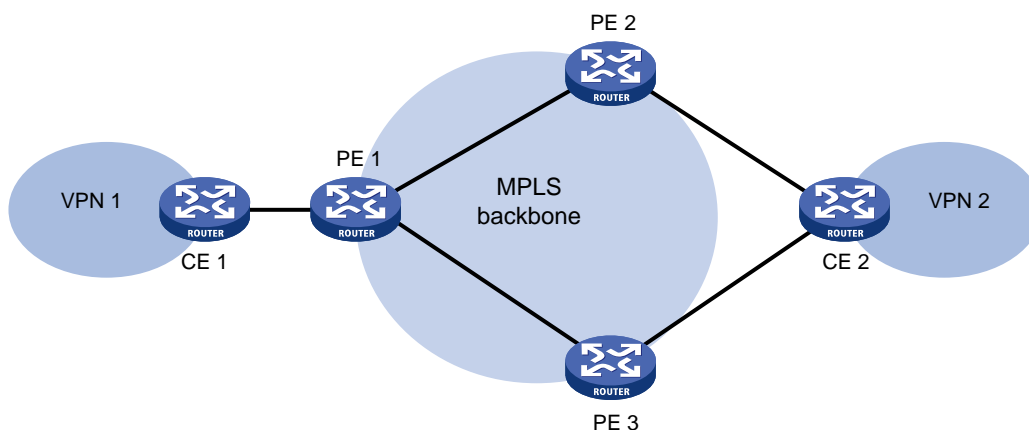
在 PE 1 上配置 BFD 检测 LSP 或 MPLS TE 隧道功能，通过 BFD 检测 PE 1 到 PE 2 之间公网隧道的状态。当公网隧道正常工作时，CE 1 和 CE 2 通过主路径 CE 1—PE 1—PE 2—CE 2 通信。当 PE 1 检测到该公网隧道出现故障时，PE 1 将通过备份路径 CE 1—PE 1—CE 2 转发 CE 1 访问 CE 2 的流量。

在这种备份方式中，PE 1 负责主路径检测和流量切换。

1.1.10 VPN 引入等价路由

VPN 引入等价路由功能用于将前缀和 RD 均相同的多条路由全部引入到 VPN 实例的路由表中。如果在开启本功能的同时配置了 **balance** 命令或 MPLS L3VPN 快速重路由功能，则这些路由之间可以进行负载分担或 MPLS L3VPN 快速重路由。**balance** 命令的详细介绍，请参见“三层技术-IP 路由命令参考”中的“BGP”。

图1-14 VPN 引入等价路由示意图



如图 1-14 所示,在 PE 1 上存在 RD 为 1:1 的 VPN 实例 VPN1,CE 1 通过该 VPN 实例接入骨干网;在 PE 2 和 PE 3 上均存在 RD 为 1:2 的 VPN 实例 VPN2,CE 2 通过该 VPN 实例接入骨干网;VPN1 和 VPN2 能够相互访问。

CE 2 上发布一条路由后,PE 2 和 PE 3 均通过 VPNv4 路由将该路由发布给 PE 1,路由的 RD 为 1:2。缺省情况下,对于前缀和 RD 均相同的多条路由,BGP 只会将最优路由学习到 VPN 实例的路由表中。因此,在 PE 1 上,VPN 实例 VPN1 的 BGP 路由表中只会存在一条到达 CE 2 的路由。在 PE 1 的 VPN 实例 VPN1 中开启 VPN 引入等价路由功能后,BGP 会把前缀和 RD 均相同的两条路由全部学习到该 VPN 实例中,这两条路由之间可以进行负载分担或 MPLS L3VPN 快速重路由。

1.1.11 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 vSystem相关说明

非缺省 vSystem 支持本特性的部分功能,包括在非缺省 vSystem 的系统视图下配置 RD 和 Route Target,以及在 vSystem IPv4 地址族视图下配置 Route Target。



说明

非缺省 vSystem 对具体命令的支持情况,请见本特性的命令参考。有关 vSystem 的详细介绍请参见“虚拟化技术配置指导”中的“vSystem”。

1.3 MPLS L3VPN配置准备

在配置 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

1.4 配置VPN实例

配置 VPN 实例的操作是在 PE 设备上进行的。

1.4.1 创建 VPN 实例

1. 功能简介

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。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 VPN 实例的 MPLS 标签范围。

```
mpls per-vrf-label range minimum maximum
```

- (3) 创建 VPN 实例，并进入 VPN 实例视图。

```
ip vpn-instance vpn-instance-name
```

- (4) 配置 VPN 实例的 RD。

```
route-distinguisher route-distinguisher
```

缺省情况下，未配置 VPN 实例的 RD。

- (5) （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。

- (6) （可选）配置 VPN 实例的 ID。

```
vpn-id vpn-id
```

缺省情况下，未配置 VPN 实例的 ID。

- (7) （可选）配置 VPN 实例的 SNMP 上下文。

```
snmp context-name context-name
```

缺省情况下，未配置 VPN 实例的 SNMP 上下文。

1.4.2 配置 VPN 实例与三层接口关联

1. 配置限制和指导

如果主接口已经与 VSI 或 MPLS L2VPN 的交叉连接关联，则该接口或其子接口无法与 VPN 实例进行关联。

如果子接口已经与 VSI 或 MPLS L2VPN 的交叉连接关联，则该子接口无法与 VPN 实例进行关联。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置接口与指定的 VPN 实例关联。

```
ip binding vpn-instance vpn-instance-name
```

缺省情况下，接口未关联 VPN 实例，即接口属于公网。



注意

配置或取消接口与 VPN 实例关联后，该接口上的 IP 地址、路由协议等配置将被删除。

执行本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。

1.4.3 配置 VPN 实例的路由相关属性

1. 配置限制和指导

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。

VPN 实例视图和 VPN 实例 IPv4 地址族视图下配置的路由相关属性均能用于 IPv4 VPN。如果同时配置二者，则 IPv4 VPN 采用 VPN 实例 IPv4 地址族视图下的配置。

2. 配置准备

在对 VPN 实例应用入方向或出方向路由策略时，还需要创建并配置路由策略，配置方法请参见“三层技术-IP 路由配置指导”中的“路由策略”。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 VPN 实例视图或 VPN 实例 IPv4 地址族视图。

- o 进入 VPN 实例视图。

```
ip vpn-instance vpn-instance-name
```

- o 请依次执行以下命令进入 VPN 实例 IPv4 地址族视图。

```
ip vpn-instance vpn-instance-name
```

```
address-family ipv4
```

- (3) 配置 VPN 实例的 Route Target。

```
vpn-target vpn-target&<1-8> [ both | export-extcommunity |  
import-extcommunity ]
```

缺省情况下，未配置 VPN 实例的 Route Target。

- (4) 配置 VPN 实例支持的最大激活路由前缀数。

```
routing-table limit number { warn-threshold | simply-alert }
```

缺省情况下，未限制 VPN 实例支持的最多激活路由前缀数。

通过本配置可以防止 PE 路由器上保存过多的激活路由前缀信息。

- (5) 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 Route Target 属性匹配的路由通过。

- (6) 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。

- (7) 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→CRLSP→SRLSP 隧道的优先级顺序选择隧道，负载分担条数为 1。

如果本配置中指定的隧道策略尚未创建，则采用缺省策略。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”。

1.5 配置 PE-CE 间的路由交换

1.5.1 配置 PE-CE 间使用静态路由

1. 功能简介

本配置在 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. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 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 ] | vpn-instance  
d-vpn-instance-name next-hop-address }
```

1.5.2 配置 PE-CE 间使用 RIP

1. 功能简介

本配置在 PE 上进行，CE 上配置普通 RIP 即可。

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”。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 PE-CE 间的 RIP 实例，并进入 RIP 视图。

```
rip [ process-id ] vpn-instance vpn-instance-name
```

- (3) 配置引入 BGP 路由。

```
import-route bgp [ as-number ] [ allow-ibgp ] [ cost cost-value |  
route-policy route-policy-name | tag tag ] *
```

缺省情况下，没有引入其他协议的路由信息。

- (4) 在指定网段上使能 RIP。

```
network network-address [ wildcard-mask ]
```

缺省情况下，没有网段使能 RIP。

1.5.3 配置 PE-CE 间使用 OSPF

1. 功能简介

本配置在 PE 上进行，CE 上配置普通 OSPF 即可。

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”。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 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
```

参数	使用说明
router-id router-id	VPN实例绑定的OSPF进程不使用系统视图下配置的公网Router ID，因此在启动进程时需要手工配置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
vpn-instance vpn-instance-name	<ul style="list-style-type: none">• 一个 OSPF 进程只能属于一个 VPN 实例• 删除 VPN 实例后，相关的所有 OSPF 进程也将全部被删除

- (3) 配置引入 BGP 路由。

```
import-route bgp [ as-number ] [ allow-ibgp ] [ cost cost-value |  
nssa-only | 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。

若在设备上配置 OSPF 实例引入 BGP 路由，则该 OSPF 实例下未配置

vpn-instance-capability simple 命令时，设备会将从 MP-IBGP 对等体学习到的 VPNv4 路由引入到 OSPF 实例，无需指定 **allow-ibgp** 参数；否则，只有指定

allow-ibgp 参数，设备才会将从 MP-IBGP 对等体学习到的 VPNv4 路由引入到 OSPF 实例。

- (4) (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。

域标识符的作用	域标识符配置注意事项
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	<ul style="list-style-type: none">每个 OSPF 进程只能配置一个主标识符，不同进程的域标识符可以相同同一个 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

- (5) (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。

- (6) 配置 OSPF 区域，并进入 OSPF 区域视图。

area *area-id*

- (7) 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。

1.5.4 配置 PE-CE 间使用 IS-IS

1. 功能简介

本配置在 PE 上进行，CE 上配置普通 IS-IS 即可。

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”。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 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*

一个 IS-IS 进程只能属于一个 VPN 实例。

- (3) 配置网络实体名称。

network-entity *net*

缺省情况下，未配置 NET。

- (4) 进入 IS-IS IPv4 单播地址族视图。

address-family **ipv4**

- (5) 配置引入 BGP 路由。

```

import-route bgp [ as-number ] [ allow-ibgp ] [ cost cost-value |
cost-type { external | internal } | [ level-1 | level-1-2 | level-2 ] |
route-policy route-policy-name | tag tag ] *
import-route bgp [ as-number ] [ allow-ibgp ] inherit-cost [ [ level-1 |
level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *

```

缺省情况下，没有引入其他协议的路由信息。

- (6) 退回系统视图。

```

quit
quit

```

- (7) 进入接口视图。

```

interface interface-type interface-number

```

- (8) 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。

1.5.5 配置 PE-CE 间使用 EBGp

1. 配置 PE

- (1) 进入系统视图。

```

system-view

```

- (2) 启动 BGP 实例，并进入 BGP 实例视图。

```

bgp as-number [ instance instance-name ]

```

缺省情况下，没有运行 BGP。

- (3) 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 实例视图下的相同，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”。

- (4) 将 CE 配置为 VPN 私网 EBGp 对等体。

```

peer { group-name | ip-address [ mask-length ] } as-number as-number

```

本命令的详细介绍请参见“三层技术-IP 路由配置指导”中的“BGP”。

- (5) 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 ]

```

- (6) 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 [ mask-length ] } 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。

- (7) 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 需要将要到本端 CE 的路由引入 VPN 路由表中，以发布给对端 PE。

- (8) 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 [mask-length] } 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。

Hub&Spoke 组网中,如果在 Hub-PE 和 Hub-CE 之间运行 EBGp,则需要在 Hub-PE 上执行本配置,否则 Hub-PE 不能接受 Hub-CE 返回的路由更新信息。

## 2. 配置 CE

- (1) 进入系统视图。

```
system-view
```

- (2) 启动 BGP 实例,并进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

缺省情况下,没有运行 BGP。

- (3) 将 PE 配置为对等体。

```
peer { group-name | ip-address [mask-length] } as-number as-number
```

- (4) 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]
```

- (5) 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 [mask-length] } 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。

- (6) 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。

## 1.6 配置 PE-PE 间的路由交换

- (1) 进入系统视图。

```
system-view
```

- (2) 启动 BGP 实例,并进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

缺省情况下,没有运行 BGP。

- (3) 将对端 PE 配置为对等体。

```
peer { group-name | ip-address [mask-length] } as-number as-number
```

- (4) (可选) 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 [mask-length] } 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。

- (5) 创建 BGP VPNv4 地址族,并进入 BGP VPNv4 地址族视图。

```
address-family vpnv4
```



- (6) 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 [mask-length] } enable
```

缺省情况下，本地路由器不能与对等体交换 VPNv4 路由信息。

## 1.7 配置BGP VPNv4路由

### 1.7.1 功能简介

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”。

### 1.7.2 控制 BGP VPNv4 路由的发布、接收和保存

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (3) 进入 BGP VPNv4 地址族视图。

```
address-family vpnv4
```

- (4) 向对等体/对等体组发送缺省路由。

```
peer { group-name | ipv4-address [mask-length] }
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。

- (5) 设置允许从指定对等体/对等体组收到的路由数量。

```
peer { group-name | ipv4-address [mask-length] } 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。

- (6) 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 | ipv4-address [mask-length] } 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。

### 1.7.3 配置 BGP VPNv4 路由的首选值

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (3) 进入 BGP VPNv4 地址族视图。

```
address-family vpnv4
```

- (4) 为从指定对等体/对等体组接收的路由分配首选值。

```
peer { group-name | ipv4-address [mask-length] } 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。

## 1.7.4 配置 BGP VPNv4 路由反射

### 1. 功能简介

为保证 IBGP 对等体之间的连通性，需要在 IBGP 对等体之间建立全连接关系。当 IBGP 对等体数目很多时，网络资源和 CPU 资源的消耗都很大。

利用路由反射可以解决这一问题。在一个 AS 内，其中一台路由器作为 RR（Route Reflector，路由反射器），作为客户机（Client）的路由器与路由反射器之间建立 IBGP 连接。路由反射器从客户机接收到路由后，将其传递（反射）给所有其他的客户机，从而保证客户机之间不需要建立 IBGP 连接，就可以学习到彼此的路由。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (3) 进入 BGP VPNv4 地址族视图。

```
address-family vpnv4
```

- (4) 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 | ipv4-address [mask-length] } reflect-client
```

缺省情况下，未配置路由反射器及其客户。

- (5) （可选）允许从对等体/对等体组收到的路由反射给客户机。

```
peer { group-name | ipv4-address [mask-length] } reflect-route
```

缺省情况下，允许从对等体/对等体组收到的路由反射给客户机。

- (6) （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。

- (7) （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。

- (8) （可选）创建路由反射器的反射策略。

```
rr-filter ext-comm-list-number
```

缺省情况下，路由反射器不会对反射的路由进行过滤。

- (9) （可选）允许路由反射器反射路由时修改路由属性。

```
reflect change-path-attribute
```

缺省情况下，不允许路由反射器反射路由时修改路由属性。

## 1.7.5 配置 BGP VPNv4 路由过滤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (3) 进入 BGP VPNv4 地址族视图。

```
address-family vpnvpn4
```

- (4) 配置对发布的路由信息进行过滤。

```
filter-policy { ipv4-acl-number | name ipv4-acl-name | prefix-list prefix-list-name } export [direct | { isis | ospf | rip } process-id | static]
```

缺省情况下，不对发布的路由信息进行过滤。

- (5) 配置对接收的路由信息进行过滤。

```
filter-policy { ipv4-acl-number | name ipv4-acl-name | 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) 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 | ipv4-address [mask-length] } as-path-acl as-path-acl-number { export | import }
```

缺省情况下，未配置基于 AS 路径过滤列表的 BGP 路由过滤策略。

- (7) 为对等体/对等体组设置基于 ACL 的 BGP 路由过滤策略。

```
peer { group-name | ipv4-address [mask-length] } filter-policy { ipv4-acl-number | name ipv4-acl-name } { export | import }
```

缺省情况下，未配置基于 ACL 的 BGP 路由过滤策略。

- (8) 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 | ipv4-address [mask-length] } prefix-list prefix-list-name { export | import }
```

缺省情况下，未配置基于地址前缀列表的 BGP 路由过滤策略。

- (9) 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 | ipv4-address [mask-length] } 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。

- (10) 配置对接收到的 VPNv4 路由进行 Route Target 过滤。

```
policy vpn-target
```

缺省情况下，对接收到的 VPNv4 路由进行 Route Target 过滤，即只将 Export Route Target 属性与本地 Import Route Target 属性匹配的 VPNv4 路由加入到路由表。

## 1.7.6 配置 BGP VPNv4 路由衰减

### 1. 功能简介

通过配置 BGP VPNv4 路由衰减，可以抑制不稳定的路由信息，不允许这类路由参与路由选择。

### 2. 配置限制和指导

本配置仅对 IBGP 路由生效。

配置本功能后，IBGP 邻居 down 了之后，来自该邻居的 VPNv4 路由不会被删除，而是进行路由衰减。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (3) 进入 BGP VPNv4 地址族视图。

```
address-family vpnvpn4
```

- (4) 配置 IBGP 路由衰减。

```
dampening ibgp [half-life-reachable half-life-unreachable reuse
suppress ceiling | route-policy route-policy-name] *
```

缺省情况下，未配置 IBGP 路由衰减。

## 1.7.7 提高邻居路由参与优选时的优先级

### 1. 功能简介

VPNv4 地址族支持 IPv4 和 IPv6 邻居共存，设备上可能存在从 IPv4 邻居和 IPv6 邻居学习到相同前缀的路由，通过配置本功能可以控制路由优先级顺序。

对于 L3VPN 支持 IPv4 和 IPv6 双栈场景，VPNv4 地址族存在从 IPv4 邻居和 IPv6 邻居学习的相同前缀的路由，可能存在从 IPv6 邻居学习的路由被优选，导致从 IPv4 学习的路由不能发布的问题。因此在业务演进过程中需要在 VPNv4 地址族 IPv4 邻居上配置本功能，保证 IPv4 邻居学习的路由被优选。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (3) 进入 BGP VPNv4 地址族视图。

```
address-family vpnvpn4
```

- (4) 为指定对等体/对等体组设置高优先级，路由选路时优选从该对等体/对等体组学习到的路由。

```
peer { group-name | ipv4-address [mask-length] | ipv6-address
[prefix-length] } high-priority
```

缺省情况下，BGP 不为指定对等体/对等体组设置高优先级，选路规则不发生变化。

## 1.8 配置多角色主机

### 1.8.1 功能简介

多角色主机特性的配置都在多角色主机所属 Site 接入的 PE 上进行，主要包括如下配置：

- 配置并应用策略路由：使得多角色主机发送的报文可以发送到多个 VPN。
- 配置静态路由：使得其他 VPN 返回的报文能够发送给多角色主机。

### 1.8.2 配置并应用策略路由

- (1) 进入系统视图。

```
system-view
```

- (2) 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
```

- (3) 配置策略节点的匹配规则。

详细介绍请参见“三层技术-IP 路由配置指导”中的“策略路由”。

缺省情况下，未配置策略节点的匹配规则，所有报文都满足该节点的匹配规则。

本配置用来匹配来自多角色主机的报文。

- (4) 设置报文在指定 VPN 实例中进行转发。

```
apply access-vpn vpn-instance vpn-instance-name<1-4>
```

缺省情况下，未设置报文在指定 VPN 实例中进行转发。

本配置中需要指定多个 VPN 实例，第一个为多角色主机所属的 VPN 实例，其余为需要访问的其他 VPN 实例。对于满足匹配规则的报文，根据第一个可用的 VPN 实例转发表进行转发。

- (5) 退回系统视图。

```
quit
```

- (6) 进入接入 CE 的接口视图。

```
interface interface-type interface-number
```

- (7) 对接口转发的报文应用策略。

```
ip policy-based-route policy-name
```

缺省情况下，对接口转发的报文未应用策略。

### 1.8.3 配置静态路由

- (1) 进入系统视图。

```
system-view
```

- (2) 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 } vpn-instance d-vpn-instance-name
next-hop-address
```

其中，*d-vpn-instance-name* 为多角色主机所属的 VPN 实例，*next-hop-address* 为多角色主机所在 Site 的 CE 设备的地址。

## 1.9 配置Egress PE上私网路由标签操作方式

### 1. 功能简介

Egress PE 上私网路由的标签操作方式分为：

- 私网标签的 POPGO 转发方式：弹出标签后，直接从出接口发送。
- 私网标签的 POP 转发方式：弹出标签后，再查 FIB 表转发。

### 2. 配置限制和指导

私网标签的 POPGO 转发方式和每 VPN 实例标签申请方式互斥，即不能同时执行 **vpn popgo** 和 **label-allocation-mode per-vrf** 命令。**label-allocation-mode** 命令的详细介绍请参见“三层技术-IP 路由命令参考”中的“BGP”。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (3) 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MPLS L3VPN快速重路由

### 1.10.1 功能简介

开启 MPLS L3VPN 快速重路由功能的方法有如下两种：

- 在路由策略中指定快速重路由的备份下一跳，并在 BGP-VPN IPv4 单播地址族视图下配置快速重路由引用该路由策略。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。
- 在 BGP-VPN IPv4 单播地址族视图下开启该地址族的快速重路由功能。采用这种方式时，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。

路由策略方式的优先级高于开启地址族快速重路由功能方式。

### 1.10.2 配置限制和指导

在某些组网情况下，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，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。

### 1.10.3 通过路由策略配置快速重路由功能

- (1) 进入系统视图。

**system-view**

- (2) 配置 BFD 检测。

- o 配置 echo 报文的源 IP 地址。

**bfd echo-source-ip** *ip-address*

缺省情况下，未配置 echo 报文的源 IP 地址。

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，则需要执行本命令。本命令的详细介绍，请参见“可靠性命令参考”中的“BFD”。

- (3) 配置路由策略。

- a. 创建路由策略，并进入路由策略视图。

**route-policy** *route-policy-name* **permit** **node** *node-number*

- b. 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，未配置快速重路由的备份下一跳地址。

- c. 退回系统视图。

**quit**

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“路由策略”。

- (4) 进入 BGP 实例视图。

**bgp** *as-number* [**instance** *instance-name*]

- (5) （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”。

- (6) 进入 BGP-VPN 实例视图。

**ip vpn-instance** *vpn-instance-name*

- (7) 进入 BGP-VPN IPv4 单播地址族视图。

**address-family ipv4** [**unicast**]

- (8) 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** 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”。



## 1.10.4 开启 BGP-VPN IPv4 单播地址族的快速重路由功能

- (1) 进入系统视图。

**system-view**

- (2) 配置 BFD 检测。

- 配置 echo 报文的源 IP 地址。

**bfd echo-source-ip ip-address**

缺省情况下，未配置 echo 报文的源 IP 地址。

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，则需要执行本命令。本命令的详细介绍，请参见“可靠性命令参考”中的“BFD”。

- (3) 进入 BGP 实例视图。

**bgp as-number [ instance instance-name ]**

- (4) （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”。

- (5) 进入 BGP-VPN 实例视图。

**ip vpn-instance vpn-instance-name**

- (6) 进入 BGP-VPN IPv4 单播地址族视图。

**address-family ipv4 [ unicast ]**

- (7) 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。

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”。

## 1.11 配置 OSPF 伪连接

### 1.11.1 功能简介

在 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。

### 1.11.2 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）
- 在用户 CE 所在局域网内配置 OSPF



### 1.11.3 发布 Loopback 接口的路由

- (1) 进入系统视图。  
**system-view**
- (2) 创建 Loopback 接口，并进入 Loopback 接口视图。  
**interface loopback** *interface-number*
- (3) 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。
- (4) 配置 Loopback 接口的地址。  
**ip address** *ip-address* { *mask-length* | *mask* }  
缺省情况下，未配置 Loopback 接口的地址。
- (5) 退回系统视图。  
**quit**
- (6) 进入 BGP 实例视图。  
**bgp** *as-number* [ **instance** *instance-name* ]
- (7) 进入 BGP-VPN 实例视图。  
**ip vpn-instance** *vpn-instance-name*
- (8) 进入 BGP-VPN IPv4 单播地址族视图。  
**address-family ipv4** [ **unicast** ]
- (9) 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。

### 1.11.4 创建伪连接

- (1) 进入系统视图。  
**system-view**
- (2) 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。
- (3) 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。
- (4) 进入 OSPF 区域视图。  
**area** *area-id*
- (5) 创建一条 OSPF 伪连接。

```
sham-link source-ip-address destination-ip-address [cost cost-value |
dead dead-interval | hello hello-interval | { { hmac-md5 | hmac-sha-256
| md5 } key-id { cipher | plain } string | keychain keychain-name | simple
{ cipher | plain } string } | retransmit retrans-interval | trans-delay
delay | ttl-security hops hop-count] *
```

## 1.12 配置BGP的AS号替换和SoO属性

### 1. 功能简介

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”。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (3) 进入 BGP-VPN 实例视图。

```
ip vpn-instance vpn-instance-name
```

- (4) 使能 BGP 的 AS 号替换功能。

```
peer { ipv4-address [mask-length] | group-name } substitute-as
```

缺省情况下，BGP 的 AS 号替换功能处于关闭状态。

- (5) 进入 BGP-VPN IPv4 单播地址族视图。

```
address-family ipv4 [unicast]
```

- (6) （可选）为 BGP 对等体/对等体组配置 SoO 属性。

```
peer { group-name | ipv4-address [mask-length] } 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。

## 1.13 配置RT-Filter功能

### 1. 功能简介

在 MPLS L3VPN 组网中，通过 RT-Filter 功能可以从源头上减少路由信息的数量。配置 RT-Filter 功能后，PE 使用 RT-Filter 地址族将本地的 Import Target 属性发布给远端 PE。远端 PE 根据接收

到的 Import target 属性直接对路由进行过滤，只发布通过 Import target 属性过滤的路由，从而减少发布的路由信息数量。

RT-Filter 功能通常和路由反射器功能配合使用，以解决路由反射器上存在大量路由的问题。

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”。

## 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (3) 进入 BGP IPv4 RT-Filter 地址族视图。

```
address-family ipv4 rtfilter
```

- (4) 允许本地路由器与指定对等体/对等体组交换路由信息。

```
peer { group-name | ipv4-address [mask-length] } enable
```

缺省情况下，本地路由器不能与对等体/对等体组交换路由信息。

- (5) （可选）向对等体/对等体组发送缺省路由。

```
peer { group-name | ipv4-address [mask-length] }
default-route-advertise [route-policy route-policy-name]
```

缺省情况下，不向对等体/对等体组发送缺省路由。

- (6) （可选）为从对等体/对等体组接收的路由分配首选值。

```
peer { group-name | ipv4-address [mask-length] } 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。

- (7) （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 | ipv4-address [mask-length] } reflect-client
```

缺省情况下，未配置路由反射器及其客户机。

- (8) （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。

- (9) （可选）配置路由反射器的集群 ID。

```
reflector cluster-id { cluster-id | ipv4-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。

- (10) （可选）为指定对等体/对等体组设置高优先级，路由选路时优选从该对等体/对等体组学习到的路由。

```
peer { group-name | ipv4-address [mask-length] } high-priority
```

缺省情况下，BGP 不为指定对等体/对等体组设置高优先级，选路规则不发生变化。

## 1.14 配置BGP Add-Path

### 1. 功能简介

缺省情况下，BGP 只发布一条最优路由。如果最优路由所在路径出现网络故障，数据流量将会被中断，直到 BGP 根据新的网络拓扑路由收敛后，被中断的流量才能恢复正常的传输。

配置了 Add-Path（Additional Paths）功能后，BGP 可以向邻居发送本地前缀相同下一跳不同的多条路由。网络出现故障后，次优路由可以成为新的最优路由，这样就缩短了流量中断时间。

Add-Path 能力包括接收和发送两种。为了让对等体间的 Add-Path 能力协商成功，必须一端使能接收能力，另一端使能发送能力。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP VPNv4 地址族视图或 BGP-VPN VPNv4 地址族视图。

- 依次执行以下命令进入 BGP VPNv4 地址族视图。

```
bgp as-number [instance instance-name]
address-family vpnv4
```

- 依次执行以下命令进入 BGP-VPN VPNv4 地址族视图。

```
bgp as-number [instance instance-name]
ip vpn-instance vpn-instance-name
address-family vpnv4
```

- (3) 配置 Add-Path 功能。

- 在 BGP VPNv4 地址族视图下：

```
peer { group-name | ipv4-address [mask-length] | ipv6-address
[prefix-length] } additional-paths { receive | send } *
```

- 在 BGP-VPN VPNv4 地址族视图下：

```
peer { group-name | ipv4-address [mask-length] } additional-paths
{ receive | send } *
```

缺省情况下，未配置 Add-Path 功能。

- (4) 配置向指定对等体/对等体组发送的 Add-Path 优选路由的最大条数。

- 在 BGP VPNv4 地址族视图下：

```
peer { group-name | ipv4-address [mask-length] | ipv6-address
[prefix-length] } advertise additional-paths best number
```

- 在 BGP-VPN VPNv4 地址族视图下：

```
peer { group-name | ipv4-address [mask-length] } advertise
additional-paths best number
```

缺省情况下，向指定对等体/对等体组发送的 Add-Path 优选路由的最大条数为 1。

- (5) 配置 Add-Path 优选路由的最大条数。

```
additional-paths select-best best-number
```

缺省情况下，Add-Path 优选路由的最大条数为 1。

- (6) (可选) 配置路由延迟优选时间。

```
route-select delay delay-value
```

缺省情况下, 延迟时间为 0 秒, 即路由优选不延迟。

## 1.15 配置路由信息引入功能

### 1. 功能简介

在 BGP/MPLS L3VPN 组网中, 只有 Route Target 属性匹配的 VPN 实例之间才可以通信。通过配置本功能可以实现:

- 将公网或其他 VPN 实例的路由信息引入到指定 VPN 实例中, 从而使指定 VPN 用户可以获取访问公网或其他 VPN 的路由。
- 将指定 VPN 实例的路由信息引入到公网中, 从而使公网获取指定 VPN 的路由, 以便转发用户流量。

在流量智能调控场景中, 不同租户的流量被划分到不同的 VPN 中。为了使租户流量可以流向公网, 则需要配置本功能将公网的路由信息引入到指定 VPN 实例中。

### 2. 将公网或其他 VPN 实例的路由信息引入到指定 VPN 实例中

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 VPN 实例视图。

```
ip vpn-instance vpn-instance-name
```

- (3) 进入 VPN 实例 IPv4 地址族视图。

```
address-family ipv4
```

- (4) 将公网或其他 VPN 实例的路由信息引入到指定 VPN 实例中。

```
route-replicate from { public | vpn-instance vpn-instance-name }
protocol { bgp as-number | direct | static | { isis | ospf | rip } process-id }
[advertise] [route-policy route-policy-name]
```

缺省情况下, 公网或其他 VPN 实例的路由信息不能引入到指定 VPN 实例中。

### 3. 将指定 VPN 实例的路由信息引入到公网中

- (1) 进入系统视图。

```
system-view
```

- (2) 进入公网实例视图。

```
ip public-instance
```

- (3) 进入公网实例 IPv4 地址族视图。

```
address-family ipv4
```

- (4) 将指定 VPN 实例的路由信息引入到公网中。

```
route-replicate from vpn-instance vpn-instance-name protocol { bgp
as-number | direct | static | { isis | ospf | rip } process-id } [advertise]
[route-policy route-policy-name]
```

缺省情况下, VPN 实例的路由信息不能引入到公网中。

## 1.16 开启VPN引入等价路由功能

### 1. 功能简介

缺省情况下，对于前缀和 RD 均相同的多条路由，BGP 只会将最优路由引入到 VPN 实例的路由表中。开启 VPN 引入等价路由功能后，BGP 可以把前缀和 RD 均相同的多条路由全部引入到 VPN 实例的路由表中，以便在这些路由之间进行负载分担或 MPLS L3VPN 快速重路由。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 相应视图。

- o 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- o 进入 BGP IPv4 单播地址族视图。

```
bgp as-number [instance instance-name]
```

```
address-family ipv4 [unicast]
```

- o 进入 BGP IPv6 单播地址族视图。

```
bgp as-number [instance instance-name]
```

```
address-family ipv6 [unicast]
```

- o 依次执行以下命令进入 BGP-VPN IPv4 单播地址族视图。

```
bgp as-number [instance instance-name]
```

```
ip vpn-instance vpn-instance-name
```

```
address-family ipv4 [unicast]
```

- o 依次执行以下命令进入 BGP-VPN IPv6 单播地址族视图。

```
bgp as-number [instance instance-name]
```

```
ip vpn-instance vpn-instance-name
```

```
address-family ipv6 [unicast]
```

- (3) 开启 VPN 引入等价路由功能。

```
vpn-route cross multipath
```

缺省情况下，VPN 引入等价路由功能处于关闭状态，对于前缀和 RD 均相同的多条路由，只会将最优路由引入到 VPN 实例的路由表中。

BGP IPv4 单播地址族视图和 BGP IPv6 单播地址族视图下配置本命令后，会将多条路由全部引入到公网实例的路由表中。

## 1.17 配置优先发送指定路由的撤销消息

### 1. 功能简介

当 BGP 路由器需要撤销大量路由时，撤销所有的路由会耗费一定时间，导致有些流量不能快速切换到有效路径。对于某些重要的、不希望长时间中断的流量，可以通过本配置，确保 BGP 路由器

优先发送这些路由的撤销消息，以便将指定流量快速地切换到有效路径上，最大限度地减少流量中断时间。

## 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (3) 创建 BGP VPNv4 地址族，并进入 BGP VPNv4 地址族视图。

```
address-family vpnv4
```

- (4) 配置优先发送指定路由的撤销消息。

```
update-first route-policy route-policy-name
```

缺省情况下，不支持优先发送指定路由的撤销消息。

## 1.18 开启告警功能

### 1. 功能简介

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”。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 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。

## 1.19 MPLS L3VPN显示和维护



说明

非缺省 vSystem 不支持部分显示和维护命令，具体情况请见本特性的命令参考。

### 1.19.1 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1-1 复位 BGP 会话

| 操作                                   | 命令                                                                                                                                                                                                                                                                                            |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 手工对BGP IPv4 RT-Filter地址族下的BGP会话进行软复位 | <b>refresh bgp</b> [ <b>instance</b> <i>instance-name</i> ] { <i>ipv4-address</i> [ <i>mask-length</i> ]   <b>all</b>   <b>external</b>   <b>group</b> <i>group-name</i>   <b>internal</b> } { <b>export</b>   <b>import</b> } <b>ipv4 rtfilter</b>                                           |
| 手工对VPNv4地址族下的BGP会话进行软复位              | <b>refresh bgp</b> [ <b>instance</b> <i>instance-name</i> ] { <i>ipv4-address</i> [ <i>mask-length</i> ]   <b>all</b>   <b>external</b>   <b>group</b> <i>group-name</i>   <b>internal</b> } { <b>export</b>   <b>import</b> } <b>vpnvp4</b> [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] |
| 复位BGP IPv4 RT-Filter地址族下的BGP会话       | <b>reset bgp</b> [ <b>instance</b> <i>instance-name</i> ] { <i>as-number</i>   <i>ipv4-address</i> [ <i>mask-length</i> ]   <b>all</b>   <b>external</b>   <b>internal</b>   <b>group</b> <i>group-name</i> } <b>ipv4 rtfilter</b>                                                            |
| 复位VPNv4地址族下的BGP会话                    | <b>reset bgp</b> [ <b>instance</b> <i>instance-name</i> ] { <i>as-number</i>   <i>ipv4-address</i> [ <i>mask-length</i> ]   <b>all</b>   <b>external</b>   <b>internal</b>   <b>group</b> <i>group-name</i> } <b>vpnvp4</b> [ <b>vpn-instance</b> <i>vpn-instance-name</i> ]                  |

### 1.19.2 显示和维护 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。在用户视图下执行 **reset** 命令清除 BGP VPNv4 路由的相关信息。

**display bgp group vpnvp4**、**display bgp peer vpnvp4** 和 **display bgp update-group vpnvp4** 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1-2 显示 MPLS L3VPN 的运行状态

| 操作                         | 命令                                                                                                                                                                                                                                                                                           |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 显示BGP VPNv4路由衰减参数          | <b>display bgp</b> [ <b>instance</b> <i>instance-name</i> ] <b>dampening parameter vpnvp4</b>                                                                                                                                                                                                |
| 显示BGP IPv4 RT-Filter对等体组信息 | <b>display bgp</b> [ <b>instance</b> <i>instance-name</i> ] <b>group ipv4 rtfilter</b> [ <b>group-name</b> <i>group-name</i> ]                                                                                                                                                               |
| 显示BGP VPNv4对等体组信息          | <b>display bgp</b> [ <b>instance</b> <i>instance-name</i> ] <b>group vpnvp4</b> [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] [ <b>group-name</b> <i>group-name</i> ]                                                                                                                     |
| 显示BGP IPv4 RT-Filter的信息    | <b>display bgp</b> [ <b>instance</b> <i>instance-name</i> ] <b>ipv4 rtfilter</b> [ <b>peer</b> <i>ipv4-address</i> [ <b>statistics</b> ]   <b>statistics</b> ]                                                                                                                               |
| 显示BGP IPv4 RT-Filter对等体信息  | <b>display bgp</b> [ <b>instance</b> <i>instance-name</i> ] <b>peer ipv4 rtfilter</b> [ <i>ipv4-address mask-length</i>   { <i>ipv4-address</i>   <b>group-name</b> <i>group-name</i> } <b>log-info</b>   [ <i>ipv4-address</i> ] <b>verbose</b> ]                                           |
| 显示BGP VPNv4对等体信息           | <b>display bgp</b> [ <b>instance</b> <i>instance-name</i> ] <b>peer vpnvp4</b> [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] [ <i>ipv4-address mask-length</i>   { <i>ipv4-address</i>   <b>group-name</b> <i>group-name</i> } <b>log-info</b>   [ <i>ipv4-address</i> ] <b>verbose</b> ] |



| 操作                                                        | 命令                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 显示衰减的BGP VPNv4路由信息                                        | <b>display bgp [ instance <i>instance-name</i> ]<br/>routing-table dampened vpnv4</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 显示BGP VPNv4路由的震荡统计信息                                      | <b>display bgp [ instance <i>instance-name</i> ]<br/>routing-table flap-info vpnv4 [ <i>ipv4-address</i><br/>[ { <i>mask</i> / <i>mask-length</i> } [ <b>longest-match</b> ] ]  <br/>as-path-acl <i>as-path-acl-number</i> ]</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 显示BGP IPv4单播路由的入标签信息                                      | <b>display bgp [ instance <i>instance-name</i> ]<br/>routing-table ipv4 [ <b>unicast</b> ] [ <b>vpn-instance</b><br/><i>vpn-instance-name</i> ] inlabel</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 显示BGP IPv4单播路由的出标签信息                                      | <b>display bgp [ instance <i>instance-name</i> ]<br/>routing-table ipv4 [ <b>unicast</b> ] [ <b>vpn-instance</b><br/><i>vpn-instance-name</i> ] outlabel</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 显示BGP IPv4 RT-Filter路由信息                                  | <b>display bgp [ instance <i>instance-name</i> ]<br/>routing-table ipv4 rtfilter [ <b>default-rt</b><br/>[ <b>advertise-info</b> ]   [ <b>origin-as</b> <i>as-number</i> ]<br/>[ <b>route-target</b> [ <b>advertise-info</b> ] ]   <b>peer</b><br/><i>ipv4-address</i> { <b>advertised-routes</b>  <br/><b>received-routes</b> } [ <b>default-rt</b>   [ <b>origin-as</b><br/><i>as-number</i> ] [ <b>route-target</b> ]   <b>statistics</b> ]  <br/><b>statistics</b> ]</b>                                                                                                                                                                                                                                                                                                                                    |
| 显示BGP VPNv4路由信息                                           | <b>display bgp [ instance <i>instance-name</i> ]<br/>routing-table vpnv4 [ [ <b>route-distinguisher</b><br/><i>route-distinguisher</i> ] [ <i>ipv4-address</i><br/>[ { <i>mask-length</i>   <i>mask</i> } [ <b>longest-match</b> ] ]  <br/><i>ipv4-address</i> [ <i>mask-length</i>   <i>mask</i> ] <b>advertise-info</b><br/>  <b>as-path-acl</b> <i>as-path-acl-number</i>   <b>community-list</b><br/>{ { <i>basic-community-list-number</i>   <i>comm-list-name</i> }<br/>[ <b>whole-match</b> ]   <i>adv-community-list-number</i> } ]  <br/>[ <b>vpn-instance</b> <i>vpn-instance-name</i> ] <b>peer</b><br/><i>ipv4-address</i> { <b>advertised-routes</b>  <br/><b>received-routes</b> } [ <i>ipv4-address</i> [ <i>mask-length</i>  <br/><i>mask</i> ]   <b>statistics</b> ]   <b>statistics</b> ]</b> |
| 显示BGP VPNv4路由的入标签信息                                       | <b>display bgp [ instance <i>instance-name</i> ]<br/>routing-table vpnv4 inlabel</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 显示BGP VPNv4路由的出标签信息                                       | <b>display bgp [ instance <i>instance-name</i> ]<br/>routing-table vpnv4 outlabel</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 显示BGP IPv4 RT-Filter地址族下打包组的相关信息                          | <b>display bgp [ instance <i>instance-name</i> ] update-group<br/>ipv4 rtfilter [ <i>ipv4-address</i> ]</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 显示BGP VPNv4地址族下打包组的相关信息                                   | <b>display bgp [ instance <i>instance-name</i> ] update-group<br/>vpnv4 [ <b>vpn-instance</b> <i>vpn-instance-name</i> ]<br/>[ <i>ipv4-address</i> ]</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 显示指定VPN实例的FIB信息                                           | <b>display fib vpn-instance <i>vpn-instance-name</i></b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 显示指定VPN实例中与指定目的IP地址匹配的FIB信息                               | <b>display fib vpn-instance <i>vpn-instance-name</i><br/>ip-address [ <i>mask-length</i>   <i>mask</i> ]</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 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”） | <b>display ip routing-table vpn-instance<br/><i>vpn-instance-name</i> [ <b>statistics</b>   <b>verbose</b> ]</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 显示指定VPN实例信息                                               | <b>display ip vpn-instance [ <i>instance-name</i><br/><i>vpn-instance-name</i> ]</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 显示OSPF伪连接信息                                               | <b>display ospf [ <i>process-id</i> ] sham-link [ <i>area</i><br/><i>area-id</i> ]</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| 操作                              | 命令                                                                                                                                                                                                                                                    |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 显示VPN peer的信息                   | <b>display vpn-peer</b> [ <b>peer-id</b> <i>vpn-peer-id</i>   <b>peer-name</b> <i>vpn-peer-name</i>   <b>verbose</b> ]                                                                                                                                |
| 清除BGP VPNv4路由的衰减信息,并解除对BGP路由的抑制 | <b>reset bgp</b> [ <b>instance</b> <i>instance-name</i> ] <b>dampening vpnv4</b> [ <i>ipv4-address</i> [ <i>mask</i>   <i>mask-length</i> ] ]                                                                                                         |
| 清除BGP VPNv4路由的震荡统计信息            | <b>reset bgp</b> [ <b>instance</b> <i>instance-name</i> ] <b>flap-info vpnv4</b> [ <i>ipv4-address</i> [ <i>mask</i>   <i>mask-length</i> ]   <b>as-path-acl</b> <i>as-path-acl-number</i>   <b>peer</b> <i>ipv4-address</i> [ <i>mask-length</i> ] ] |

## 2 IPv6 MPLS L3VPN

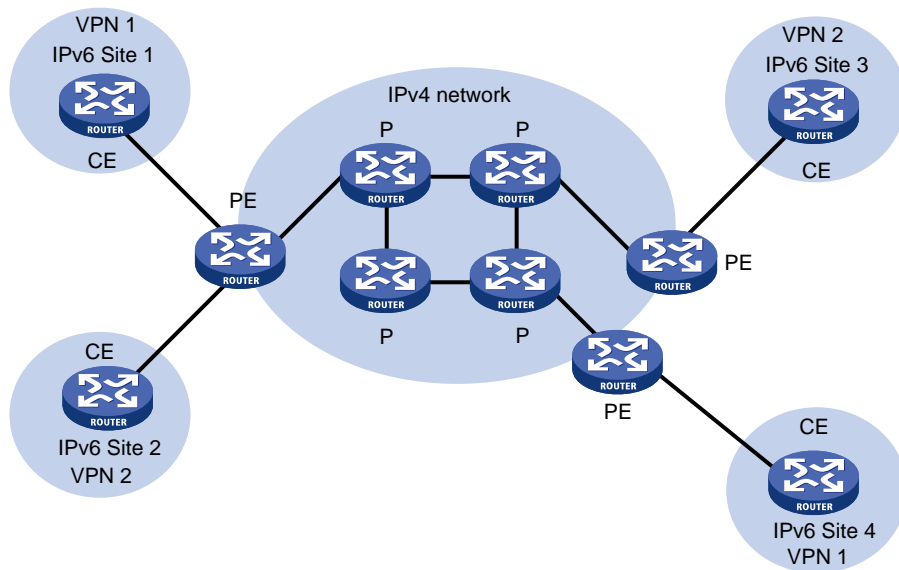
### 2.1 IPv6 MPLS L3VPN简介

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(即 6VPE, IPv6 VPN Provider Edge)的工作原理与 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。

#### 2.1.1 IPv6 MPLS L3VPN 典型组网环境

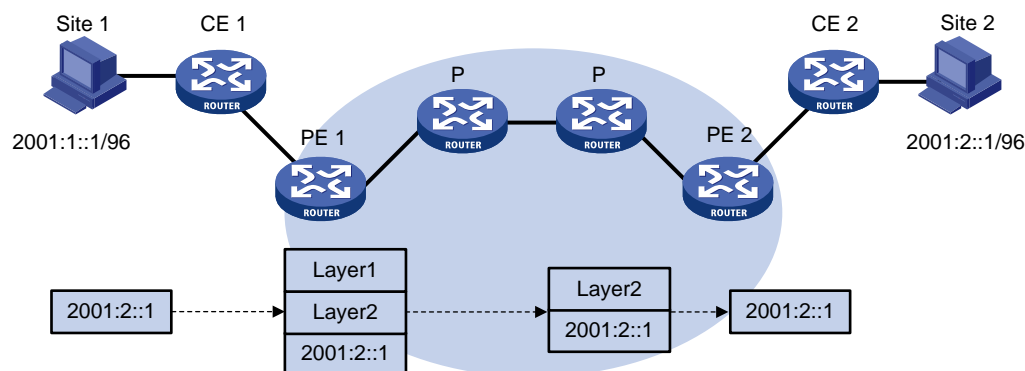
IPv6 MPLS L3VPN 的典型组网环境如图 2-1 所示。目前，IPv6 MPLS L3VPN 组网中服务提供商骨干网应为 IPv4 网络。VPN 内部及 CE 和 PE 之间运行 IPv6 协议，骨干网中 PE 和 P 设备之间运行 IPv4 协议。PE 需要同时支持 IPv4 和 IPv6 协议，连接 CE 的接口上使用 IPv6 协议，连接骨干网的接口上使用 IPv4 协议。

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 Route 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 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
- RFC 6565: OSPFv3 as a Provider Edge to Customer Edge (PE-CE) Routing Protocol

## 2.2 vSystem相关说明

非缺省 vSystem 支持本特性的部分功能，包括在非缺省 vSystem 的系统视图下配置 RD 和 Route Target，以及在 vSystem IPv6 地址族视图下配置 Route Target。



说明

非缺省 vSystem 对具体命令的支持情况，请见本特性的命令参考。有关 vSystem 的详细介绍请参见“虚拟化技术配置指导”中的“vSystem”。

## 2.3 IPv6 MPLS L3VPN配置限制和指导

IPv6 MPLS L3VPN 的公网隧道可以是 LSP 隧道、MPLS TE 隧道和 GRE 隧道等。目前，IPv6 MPLS L3VPN 不支持采用 GRE over IPv6 隧道作为公网隧道。

## 2.4 IPv6 MPLS L3VPN配置任务简介

除特殊说明外，IPv6 MPLS L3VPN 的配置均在 PE 设备上执行。IPv6 MPLS L3VPN 配置任务如下：

### (1) 配置 IPv6 MPLS L3VPN 基本功能

- a. [配置 VPN 实例](#)
- b. [配置 PE-CE 间的路由交换](#)
- c. [配置 PE-PE 间的路由交换](#)
- d. （可选）[配置 BGP VPNv6 路由](#)

### (2) 配置 IPv6 MPLS L3VPN 高级组网

请根据实际情况选择以下任务进行配置：

#### o [配置多角色主机](#)

多角色主机功能通过在 PE 上配置策略路由，使得来自 Site 内某些主机或服务器的报文可以访问多个 VPN。

- (3) （可选）[配置 OSPFv3 伪连接](#)
- (4) （可选）[配置 BGP 的 AS 号替换和 SoO 属性](#)
- (5) （可选）[配置 BGP Add-Path](#)
- (6) （可选）[配置路由信息引入功能](#)
- (7) （可选）[配置优先发送指定路由的撤销消息](#)

## 2.5 IPv6 MPLS L3VPN配置准备

在配置 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

## 2.6 配置VPN实例

### 2.6.1 创建 VPN 实例

#### 1. 功能简介

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。

#### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 VPN 实例的 MPLS 标签范围。

```
mpls per-vrf-label range minimum maximum
```

- (3) 创建 VPN 实例，并进入 VPN 实例视图。

```
ip vpn-instance vpn-instance-name
```

- (4) 配置 VPN 实例的 RD。

```
route-distinguisher route-distinguisher
```

缺省情况下，未配置 VPN 实例的 RD。

- (5) （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。

- (6) （可选）配置 VPN 实例的 ID。

```
vpn-id vpn-id
```

缺省情况下，未配置 VPN 实例的 ID。

- (7) （可选）配置 VPN 实例的 SNMP 上下文。

```
snmp context-name context-name
```

缺省情况下，未配置 VPN 实例的 SNMP 上下文。

### 2.6.2 配置 VPN 实例与三层接口关联

#### 1. 配置限制和指导

如果主接口已经与 VSI 或 MPLS L2VPN 的交叉连接关联，则该接口或其子接口无法与 VPN 实例进行关联。

如果子接口已经与 VSI 或 MPLS L2VPN 的交叉连接关联，则该子接口无法与 VPN 实例进行关联。

## 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置接口与指定 VPN 实例关联。

```
ip binding vpn-instance vpn-instance-name
```

缺省情况下，接口未关联 VPN 实例，接口属于公网。



注意

配置或取消接口与 VPN 实例关联后，该接口上的 IP 地址、路由协议等配置将被删除。

---

执行本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。

## 2.6.3 配置 VPN 实例的路由相关属性

### 1. 配置限制和指导

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。

VPN 实例视图和 VPN 实例 IPv6 地址族视图下配置的路由相关属性均能用于 IPv6 VPN。如果同时配置二者，则 IPv6 VPN 采用 VPN 实例 IPv6 地址族视图下的配置。

### 2. 配置准备

在对 VPN 实例应用入方向或出方向路由策略时，还需要创建并配置路由策略，配置方法请参见“三层技术-IP 路由配置指导”中的“路由策略”。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 VPN 实例视图或 VPN 实例 IPv6 地址族视图。

- 进入 VPN 实例视图。

```
ip vpn-instance vpn-instance-name
```

- 请依次执行以下命令进入 VPN 实例 IPv6 地址族视图。

```
ip vpn-instance vpn-instance-name
```

```
address-family ipv6
```

- (3) 配置 Route Target。

```
vpn-target vpn-target [both | export-extcommunity | import-extcommunity]
```

缺省情况下，未配置 VPN 实例的 Route Target。

- (4) 配置支持的最大激活路由前缀数。

```
routing-table limit number { warn-threshold | simply-alert }
```

缺省情况下，未限制 VPN 实例支持的最多激活路由前缀数。

通过本配置可以防止 PE 路由器上保存过多的激活路由前缀信息。

- (5) 应用入方向路由策略。

```
import route-policy route-policy
```

缺省情况下，接收所有 Route Target 属性匹配的路由。

- (6) 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。

- (7) 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→CRLSP→SRLSP 隧道的优先级顺序选择隧道，负载分担条数为 1。

如果本配置中指定的隧道策略尚未创建，则采用缺省策略。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”。

## 2.7 配置 PE-CE 间的路由交换

### 2.7.1 配置 PE-CE 间使用 IPv6 静态路由

#### 1. 功能简介

本配置在 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. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 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 }
```

### 2.7.2 配置 PE-CE 间使用 RIPng

#### 1. 功能简介

本配置在 PE 上进行，CE 上配置普通 RIPng 即可。

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”。

#### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 PE-CE 间的 RIPng 实例，并进入 RIPng 视图。



```
ripng [process-id] vpn-instance vpn-instance-name
```

一个 RIPng 进程只能属于一个 VPN 实例。

- (3) 配置引入 BGP 路由。

```
import-route bgp4+ [as-number] [allow-ibgp] [cost cost-value |
route-policy route-policy-name] *
```

缺省情况下，没有引入其他协议的路由信息。

- (4) 退回系统视图。

```
quit
```

- (5) 进入接口视图。

```
interface interface-type interface-number
```

- (6) 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。

## 2.7.3 配置 PE-CE 间使用 OSPFv3

### 1. 功能简介

本配置在 PE 上进行，CE 上配置普通 OSPFv3 即可。

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”。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 PE-CE 间的 OSPFv3 实例，并进入 OSPFv3 视图。

```
ospfv3 [process-id | vpn-instance vpn-instance-name] *
```

一个 OSPFv3 进程只能属于一个 VPN 实例。

删除 VPN 实例后，相关的所有 OSPFv3 进程也将全部被删除。

- (3) 配置 Router ID。

```
router-id router-id
```

- (4) 配置引入 BGP 路由。

```
import-route bgp4+ [as-number] [allow-ibgp] [cost cost-value |
nssa-only | 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。

若在设备上配置 OSPFv3 实例引入 BGP 路由，则该 OSPFv3 实例下未配置

**vpn-instance-capability simple** 命令时，设备会将从 MP-IBGP 对等体学习到的

VPNv6 路由引入到 OSPFv3 实例，无需指定 **allow-ibgp** 参数；否则，只有指定

**allow-ibgp** 参数，设备才会将从 MP-IBGP 对等体学习到的 VPNv6 路由引入到 OSPFv3 实例。

- (5) （可选）配置 OSPFv3 路由属性。

- a. 配置 OSPFv3 域标识符。

**domain-id** { *domain-id* [ **secondary** ] | **null** }

缺省情况下，OSPFv3 域标识符为 0。

| 域标识符的作用                                                                  | 域标识符配置注意事项                                                                                                               |
|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| OSPFv3进程的域标识符包含在此进程生成的路由中，在将OSPFv3路由引入BGP时，域标识符被附加到BGP路由上，作为BGP的扩展团体属性传递 | <ul style="list-style-type: none"><li>不同 OSPFv3 进程的域标识符可以相同</li><li>同一 VPN 的所有 OSPFv3 进程应配置相同的域标识符，以保证路由发布的正确性</li></ul> |

- b. 配置 OSPFv3 扩展团体属性的类型编码。

**ext-community-type** { **domain-id** *type-code1* | **route-type** *type-code2* | **router-id** *type-code3* }

缺省情况下，OSPFv3 扩展团体属性 Domain ID 的类型编码是 0x0005，Route Type 的类型编码是 0x0306，Router ID 的类型编码是 0x0107。

- c. 在 PE 上配置 VPN 引入路由的外部路由标记值。

**route-tag** *tag-value*

缺省情况下，若本端配置了 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。

- d. 配置 PE 上不设置 OSPFv3 LSA 的 DN 位。

**disable-dn-bit-set**

缺省情况下，将 BGP 路由引入 OSPFv3，并生成 OSPFv3 LSA 时，设备为生成的 LSA 设置 DN 位。

配置该命令后，可能会导致路由环路，需谨慎使用。

- e. 配置 PE 上忽略 OSPFv3 LSA 的 DN 位检查。

**disable-dn-bit-check**

缺省情况下，PE 上检查 OSPFv3 LSA 的 DN 位。

配置该命令后，可能会导致路由环路，需谨慎使用。

- f. 在 PE 上使能 OSPFv3 LSA 的外部路由标记检查。

**route-tag-check enable**

缺省情况下，PE 上不检查 OSPFv3 LSA 的外部路由标记，通过 DN 位检查避免路由环路。

该命令是为了兼容旧的协议（RFC 4577），现在不建议使用。

- g. 退回系统视图。

**quit**

- (6) 进入接口视图。

**interface** *interface-type interface-number*

- (7) 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。

配置本命令时, 需要确保 OSPFv3 进程所属的 VPN 实例与接口绑定的 VPN 实例相同, 否则, 命令会执行失败。

## 2.7.4 配置 PE-CE 间使用 IPv6 IS-IS

### 1. 功能简介

该配置在 PE 上进行, CE 上配置普通 IPv6 IS-IS 即可。

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”。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 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
```

一个 IPv6 IS-IS 进程只能属于一个 VPN 实例。

- (3) 配置网络实体名称。

```
network-entity net
```

缺省情况下, 未配置网络实体名称。

- (4) 创建并进入 IS-IS IPv6 单播地址族视图。

```
address-family ipv6 [unicast]
```

- (5) 配置引入 BGP 路由。

```
import-route bgp4+ [as-number] [allow-ibgp] [[cost cost-value |
inherit-cost] | [level-1 | level-1-2 | level-2] | route-policy
route-policy-name | tag tag] *
```

缺省情况下, 没有引入其他协议的路由信息。

- (6) 退回系统视图。

```
quit
```

```
quit
```

- (7) 进入接口视图。

```
interface interface-type interface-number
```

- (8) 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。

## 2.7.5 配置 PE-CE 间使用 EBGp

### 1. 配置 PE

- (1) 进入系统视图。

```
system-view
```

- (2) 启动 BGP 实例, 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

缺省情况下，没有运行 BGP。

- (3) 进入 BGP-VPN 实例视图。

```
ip vpn-instance vpn-instance-name
```

- (4) 将 CE 配置为 VPN 私网 EBGp 对等体。

```
peer { group-name | ipv6-address [prefix-length] } as-number as-number
```

- (5) 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]
```

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。本文只列举了部分命令，更多的命令请参见“三层技术-IP 路由配置指导”中的“BGP”。

- (6) 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 [prefix-length] } 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。

- (7) 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。

- (8) （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 | ipv6-address [prefix-length] } 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。

Hub&Spoke 组网中，如果在 Hub-PE 和 Hub-CE 之间运行 EBGp，则需要在 Hub-PE 上执行本配置，否则 Hub-PE 不能接受 Hub-CE 返回的路由更新信息。

## 2. 配置 CE

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (3) 将 PE 配置为 EBGp 对等体。

```
peer { group-name | ipv6-address [prefix-length] } as-number as-number
```

- (4) 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]
```

- (5) 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 [prefix-length] } 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。

- (6) 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。

## 2.8 配置PE-PE间的路由交换

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (3) 将对端 PE 配置为对等体。

```
peer { group-name | ipv4-address [mask-length] } as-number as-number
```

- (4) 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 | ipv4-address [mask-length] } 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。

- (5) 创建 BGP VPNv6 地址族，并进入 BGP VPNv6 地址族视图。

```
address-family vpn6
```

- (6) 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 | ipv4-address [mask-length] } enable
```

缺省情况下，本地路由器不能与对等体交换 VPNv6 路由信息。

## 2.9 配置BGP VPNv6路由

### 2.9.1 功能简介

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”。

### 2.9.2 配置 BGP VPNv6 路由的首选值

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (3) 进入 BGP VPNv6 地址族视图。

```
address-family vpn6
```

- (4) 为从对等体/对等体组接收的路由分配首选值。

```
peer { group-name | ipv4-address [mask-length] } 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。

### 2.9.3 配置允许从指定对等体/对等体组收到的路由数量

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (3) 进入 BGP VPNv6 地址族视图。

```
address-family vpn6
```

- (4) 设置允许从指定对等体/对等体组收到的路由数量。

```
peer { group-name | ipv4-address [mask-length] } 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。

### 2.9.4 配置 BGP VPNv6 路由属性

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (3) 进入 BGP VPNv6 地址族视图。

```
address-family vpn6
```

- (4) 配置 AS\_PATH 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 | ipv4-address [mask-length] } 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。

- 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 | ipv4-address [mask-length] } 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。

- (5) 配置向对等体/对等体组发布路由时不改变下一跳。

```
peer { group-name | ipv4-address [mask-length] } next-hop-invariable
```

缺省情况下，向对等体/对等体组发布路由时会将自己的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 VPNv6 路由，则需要在路由反射器上通过本命令配置向 BGP 邻居和反射客户通告 VPNv6 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。

- (6) 配置向对等体/对等体组发布团体属性。

**peer** { *group-name* | *ipv4-address* [ *mask-length* ] } **advertise-community**  
缺省情况下，不向对等体/对等体组发布团体属性。

- (7) 为 BGP 对等体/对等体组配置 SoO 属性。

**peer** { *group-name* | *ipv4-address* [ *mask-length* ] } **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。

## 2.9.5 配置 BGP VPNv6 路由过滤

- (1) 进入系统视图。

**system-view**

- (2) 进入 BGP 实例视图。

**bgp** *as-number* [ **instance** *instance-name* ]

- (3) 进入 BGP VPNv6 地址族视图。

**address-family** *vpn**v6*

- (4) 配置对发布的路由信息进行过滤。

**filter-policy** { *ipv6-acl-number* | **name** *ipv6-acl-name* | **prefix-list** *ipv6-prefix-name* } **export** [ **direct** | { **isisv6** | **ospfv3** | **ripng** } *process-id* | **static** ]

缺省情况下，不对发布的路由信息进行过滤。

- (5) 配置对接收的路由信息进行过滤。

**filter-policy** { *ipv6-acl-number* | **name** *ipv6-acl-name* | **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) 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* | *ipv4-address* [ *mask-length* ] } **as-path-acl** *as-path-acl-number* { **export** | **import** }

缺省情况下，未配置基于 AS 路径过滤列表的 BGP 路由过滤策略。

- (7) 为对等体/对等体组设置基于 ACL 的 BGP 路由过滤策略。

**peer** { *group-name* | *ipv4-address* [ *mask-length* ] } **filter-policy** { *ipv6-acl-number* | **name** *ipv6-acl-name* } { **export** | **import** }

缺省情况下，未配置基于 ACL 的 BGP 路由过滤策略。

- (8) 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* | *ipv4-address* [ *mask-length* ] } **prefix-list** *ipv6-prefix-name* { **export** | **import** }

缺省情况下，未配置基于 IPv6 地址前缀列表的 BGP 路由过滤策略。

- (9) 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* | *ipv4-address* [ *mask-length* ] } **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。

- (10) 配置对接收到的 VPNv6 路由进行 Route Target 过滤。

**policy vpn-target**

缺省情况下，对接收到的 VPNv6 路由进行 Route Target 过滤，即只将 Export Route Target 属性与本地 Import Route Target 属性匹配的 VPNv6 路由加入到路由表。

## 2.9.6 提高邻居路由参与优选时的优先级

### 1. 功能简介

VPNv4 地址族支持 IPv4 和 IPv6 邻居共存，设备上可能存在从 IPv4 邻居和 IPv6 邻居学习到相同前缀的路由，通过配置本功能可以控制路由优先级顺序。

对于 L3VPN 支持 IPv4 和 IPv6 双栈场景，VPNv6 地址族存在从 IPv4 邻居和 IPv6 邻居学习的相同前缀的路由，可能存在从 IPv4 邻居学习的路由被优选，导致从 IPv6 学习的路由不能发布的问题。因此在业务演进过程中需要在 VPNv6 地址族 IPv6 邻居上配置本功能，保证 IPv6 邻居学习的路由被优选。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (3) 进入 BGP VPNv6 地址族视图。

```
address-family vpn6
```

- (4) 为指定对等体/对等体组设置高优先级，路由选路时优选从该对等体/对等体组学习到的路由。

```
peer { group-name | ipv4-address [mask-length] | ipv6-address [prefix-length] } high-priority
```

缺省情况下，BGP 不为指定对等体/对等体组设置高优先级，选路规则不发生变化。

## 2.10 配置多角色主机

### 2.10.1 功能简介

多角色主机特性的配置都在多角色主机所属 Site 接入的 PE 上进行，主要包括如下配置：

- 配置并应用策略路由：使得多角色主机发送的报文可以发送到多个 VPN。
- 配置静态路由：使得其他 VPN 返回的报文能够发送给多角色主机。

### 2.10.2 配置并应用策略路由

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 IPv6 策略节点，并进入 IPv6 策略节点视图。

```
ipv6 policy-based-route policy-name { deny | permit } node node-number
```

- (3) 配置 IPv6 策略节点的匹配规则。

详细介绍请参见“三层技术-IP 路由配置指导”中的“IPv6 策略路由”



缺省情况下，未配置 IPv6 策略节点的匹配规则，所有报文都满足该节点的匹配规则。

本配置用来匹配来自多角色主机的报文。

- (4) 设置报文在指定 VPN 实例中进行转发。

```
apply access-vpn vpn-instance vpn-instance-name <1-4>
```

缺省情况下，未设置报文在指定 VPN 实例中进行转发。

本配置中需要指定多个 VPN 实例，第一个为多角色主机所属的 VPN 实例，其余为需要访问的其他 VPN 实例。报文满足匹配规则后，将根据第一个可用的 VPN 实例转发表进行转发。

- (5) 退回系统视图。

```
quit
```

- (6) 进入接入 CE 的接口视图。

```
interface interface-type interface-number
```

- (7) 对接口转发的报文应用策略。

```
ipv6 policy-based-route policy-name
```

缺省情况下，对接口转发的报文没有应用策略。

### 2.10.3 配置静态路由

- (1) 进入系统视图。

```
system-view
```

- (2) 为指定 VPN 实例配置静态路由。

```
ipv6 route-static vpn-instance s-vpn-instance-name ipv6-address
prefix-length vpn-instance d-vpn-instance-name nexthop-address
```

其中，*d-vpn-instance-name* 为多角色主机所属的 VPN 实例，*next-hop-address* 为多角色主机所在 Site 的 CE 设备的地址。

## 2.11 配置 OSPFv3 伪连接

### 2.11.1 配置准备

在配置 OSPF 伪连接之前，需完成以下任务：

- 配置基本 IPv6 MPLS L3VPN（PE-CE 间使用 OSPFv3）
- 在用户 CE 所在局域网内配置 OSPFv3

### 2.11.2 发布 Loopback 接口的路由

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 Loopback 接口，并进入 Loopback 接口视图。

```
interface loopback interface-number
```

- (3) 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。

- (4) 配置 Loopback 接口的 IPv6 地址。

配置方法，请参见“三层技术-IP 业务配置指导”中的“IPv6 基础”。

缺省情况下，未配置 Loopback 接口的 IPv6 地址。

- (5) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (6) 进入 BGP-VPN 实例视图。

```
ip vpn-instance vpn-instance-name
```

- (7) 进入 BGP-VPN IPv6 单播地址族视图。

```
address-family ipv6 [unicast]
```

- (8) 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。

### 2.11.3 创建伪连接

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 OSPFv3 视图。

```
ospfv3 [process-id | vpn-instance vpn-instance-name] *
```

- (3) 进入 OSPFv3 区域视图。

```
area area-id
```

- (4) 创建一条 OSPFv3 伪连接。

```
sham-link source-ipv6-address destination-ipv6-address [cost cost-value | dead dead-interval | hello hello-interval | instance instance-id | ipsec-profile profile-name | keychain keychain-name | retransmit retrans-interval | trans-delay delay] *
```

## 2.12 配置BGP的AS号替换和SoO属性

### 1. 功能简介

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”。

## 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (3) 进入 BGP-VPN 实例视图。

```
ip vpn-instance vpn-instance-name
```

- (4) 使能 BGP 的 AS 号替换功能。

```
peer { group-name | ipv6-address [prefix-length] } substitute-as
```

缺省情况下，BGP 的 AS 号替换功能处于关闭状态。

- (5) 进入 BGP-VPN IPv6 单播地址族视图。

```
address-family ipv6 [unicast]
```

- (6) （可选）为 BGP 对等体/对等体组配置 SoO 属性。

```
peer { group-name | ipv6-address [prefix-length] } 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。

## 2.13 配置BGP Add-Path

### 1. 功能简介

缺省情况下，BGP 只发布一条最优路由。如果最优路由所在路径出现网络故障，数据流量将会被中断，直到 BGP 根据新的网络拓扑路由收敛后，被中断的流量才能恢复正常的传输。

配置了 Add-Path（Additional Paths）功能后，BGP 可以向邻居发送本地前缀相同下一跳不同的多条路由。网络出现故障后，次优路由可以成为新的最优路由，这样就缩短了流量中断时间。

Add-Path 能力包括接收和发送两种。为了让对等体间的 Add-Path 能力协商成功，必须一端使能接收能力，另一端使能发送能力。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (3) 进入 BGP VPNv6 地址族视图。

```
address-family vpnv6
```

- (4) 配置 Add-Path 功能。

```
peer { group-name | ipv4-address [mask-length] | ipv6-address [prefix-length] } additional-paths { receive | send } *
```

缺省情况下，未配置 Add-Path 功能。

- (5) 配置向指定对等体/对等体组发送的 Add-Path 优选路由的最大条数。

```
peer { group-name | ipv4-address [mask-length] | ipv6-address [prefix-length] } advertise additional-paths best number
```

缺省情况下，向指定对等体/对等体组发送的 Add-Path 优选路由的最大条数为 1。

- (6) 配置 Add-Path 优选路由的最大条数。

```
additional-paths select-best best-number
```

缺省情况下，Add-Path 优选路由的最大条数为 1。

## 2.14 配置路由信息引入功能

### 1. 功能简介

在 IPv6 BGP/IPv6 MPLS L3VPN 组网中，只有 Route Target 属性匹配的 VPN 实例之间才可以通信。通过配置本功能可以实现：

- 将公网或其他 VPN 实例的路由信息引入到指定 VPN 实例中，从而使指定 VPN 用户可以获取访问公网或其他 VPN 的路由。
- 将指定 VPN 实例的路由信息引入到公网中，从而使公网获取指定 VPN 的路由，以便转发用户流量。

在流量智能调控场景中，不同租户的流量被划分到不同的 VPN 中。为了使租户流量可以流向公网，则需要将公网的路由信息引入到指定 VPN 实例中。

### 2. 将公网或其他 VPN 实例的路由信息引入到指定 VPN 实例中

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 VPN 实例视图。

```
ip vpn-instance vpn-instance-name
```

- (3) 进入 VPN 实例 IPv6 地址族视图。

```
address-family ipv6
```

- (4) 将公网或其他 VPN 实例的路由信息引入到指定 VPN 实例中。

```
route-replicate from { public | vpn-instance vpn-instance-name }
protocol { bgp4+ as-number | direct | static | { isisv6 | ospfv3 | ripng }
process-id } [advertise] [route-policy route-policy-name]
```

缺省情况下，公网或其他 VPN 实例的路由信息不能引入到指定 VPN 实例中。

### 3. 将指定 VPN 实例的路由信息引入到公网中

- (1) 进入系统视图。

```
system-view
```

- (2) 进入公网实例视图。

```
ip public-instance
```

- (3) 进入公网实例 IPv6 地址族视图。

```
address-family ipv6
```

- (4) 将指定 VPN 实例的路由信息引入到公网中。

```
route-replicate from vpn-instance vpn-instance-name protocol { bgp4+
as-number | direct | static | { isisv6 | ospfv3 | ripng } process-id }
[advertise] [route-policy route-policy-name]
```

缺省情况下，VPN 实例的路由信息不能引入到公网中。

## 2.15 配置优先发送指定路由的撤销消息

### 1. 功能简介

当 BGP 路由器需要撤销大量路由时，撤销所有的路由会耗费一定时间，导致有些流量不能快速切换到有效路径。对于某些重要的、不希望长时间中断的流量，可以通过本配置，确保 BGP 路由器优先发送这些路由的撤销消息，以便将指定流量快速地切换到有效路径上，最大限度地减少流量中断时间。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 BGP 实例视图。

```
bgp as-number [instance instance-name]
```

- (3) 创建 BGP VPNv6 地址族，并进入 BGP VPNv6 地址族视图。

```
address-family vpnv6
```

- (4) 配置优先发送指定路由的撤销消息。

```
update-first route-policy route-policy-name
```

缺省情况下，不支持优先发送指定路由的撤销消息。

## 2.16 IPv6 MPLS L3VPN显示和维护



说明

非缺省 vSystem 不支持部分显示和维护命令，具体情况请见本特性的命令参考。

### 2.16.1 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2-1 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 | <pre>refresh bgp [ instance instance-name ] { ipv4-address [ mask-length ]   all   external   group group-name   internal } { export   import } vpnv6</pre> |

| 操作                | 命令                                                                                                                                                                                                                        |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 复位VPNv6地址族下的BGP会话 | <b>reset bgp</b> [ <b>instance</b> <i>instance-name</i> ] { <i>as-number</i>   <i>ipv4-address</i> [ <i>mask-length</i> ]   <b>all</b>   <b>external</b>   <b>internal</b>   <b>group</b> <i>group-name</i> } <b>vpn6</b> |

## 2.16.2 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 vpn6**、**display bgp peer vpn6** 和 **display bgp update-group vpn6** 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2-2 显示 IPv6 MPLS L3VPN 的运行状态

| 操作                                                          | 命令                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 显示BGP VPNv6对等体组的信息                                          | <b>display bgp</b> [ <b>instance</b> <i>instance-name</i> ] <b>group vpn6</b> [ <b>group-name</b> <i>group-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 显示BGP VPNv6对等体的信息                                           | <b>display bgp</b> [ <b>instance</b> <i>instance-name</i> ] <b>peer vpn6</b> [ <i>ipv4-address</i> <i>mask-length</i>   { <i>ipv4-address</i>   <b>group-name</b> <i>group-name</i> } <b>log-info</b>   [ <i>ipv4-address</i> ] <b>verbose</b> ]                                                                                                                                                                                                                                                                                                                                                            |
| 显示BGP VPNv6路由信息                                             | <b>display bgp</b> [ <b>instance</b> <i>instance-name</i> ] <b>routing-table vpn6</b> [ [ <b>route-distinguisher</b> <i>route-distinguisher</i> ] [ <i>ipv6-address</i> <i>prefix-length</i> ] <b>advertise-info</b>   <b>as-path-acl</b> <i>as-path-acl-number</i>   <b>community-list</b> { { <i>basic-community-list-number</i>   <i>comm-list-name</i> }   [ <b>whole-match</b> ]   <i>adv-community-list-number</i> } ]   <b>peer</b> <i>ipv4-address</i> { <b>advertised-routes</b>   <b>received-routes</b> } [ <i>ipv6-address</i> <i>prefix-length</i>   <b>statistics</b> ]   <b>statistics</b> ] |
| 显示所有BGP VPNv6路由的入标签信息                                       | <b>display bgp</b> [ <b>instance</b> <i>instance-name</i> ] <b>routing-table vpn6 inlabel</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 显示所有BGP VPNv6路由的出标签信息                                       | <b>display bgp</b> [ <b>instance</b> <i>instance-name</i> ] <b>routing-table vpn6 outlabel</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 显示BGP VPNv6地址族下打包组的相关信息                                     | <b>display bgp</b> [ <b>instance</b> <i>instance-name</i> ] <b>update-group vpn6</b> [ <i>ipv4-address</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 显示指定VPN实例信息                                                 | <b>display ip vpn-instance</b> [ <b>instance-name</b> <i>vpn-instance-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 显示指定VPN实例的IPv6 FIB信息                                        | <b>display ipv6 fib vpn-instance</b> <i>vpn-instance-name</i> [ <i>ipv6-address</i> [ <i>prefix-length</i> ] ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 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”） | <b>display ipv6 routing-table vpn-instance</b> <i>vpn-instance-name</i> [ <b>verbose</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 显示OSPFv3伪连接信息                                               | <b>display ospfv3</b> [ <i>process-id</i> ] [ <b>area</b> <i>area-id</i> ] <b>sham-link</b> [ <b>verbose</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 显示VPN peer的信息                                               | <b>display vpn-peer</b> [ <b>peer-id</b> <i>vpn-peer-id</i>   <b>peer-name</b> <i>vpn-peer-name</i> ] <b>verbose</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |