

智能电网-地调接入网解决方案
V100R001C00
部署指南

文档版本 01
发布日期 2011-12-30

版权所有 © 华为技术有限公司 2011。保留一切权利。

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

商标声明



HUAWEI 和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： <http://www.huawei.com>

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 地调接入网方案部署	1
1.1 概述.....	1
1.1.1 地调接入网简介.....	1
1.1.2 典型组网	2
1.1.3 配套版本	4
1.1.4 部署思路	4
1.2 配置接口.....	5
1.3 配置 IGP	6
1.3.1 配置 OSPF 基本功能.....	6
1.3.2 （可选）配置 NSSA 区域	6
1.3.3 配置 OSPF 路由聚合	6
1.3.4 配置 OSPF 引入其他路由	7
1.3.5 （可选）配置 IGP 快速收敛	7
1.4 配置 BGP.....	7
1.4.1 启动 BGP 进程.....	8
1.4.2 配置 BGP 对等体.....	8
1.4.3 （可选）配置 BGP 连接所使用的本地接口	8
1.4.4 配置路由反射器.....	9
1.4.5 配置路由过滤.....	9
1.5 使能 MPLS 基本能力	10
1.5.1 配置 LSR ID.....	10
1.5.2 使能 MPLS.....	11
1.5.3 配置 MPLS LDP.....	11
1.6 配置基本 MPLS L3VPN.....	11
1.6.1 创建 VPN 实例.....	11
1.6.2 配置接口与 VPN 实例绑定.....	12
1.6.3 在 PE 之间建立 MP-IBGP 对等体.....	12
1.6.4 配置 PE 与 CE/MCE 之间的路由交互	13
1.7 （可选）配置 MCE.....	13
1.7.1 配置 VPN 实例.....	13
1.7.2 在接口上绑定 VPN 实例.....	14

1.7.3 配置 PE 和 MCE 之间的路由交互	14
1.7.4 配置 MCE 和 CE 之间的路由交互	14
1.8 配置 HoVPN	15
1.8.1 在 SPE 上创建 VPN 实例	15
1.8.2 配置 UPE 和 SPE 之间的 MP-IBGP 对等体	15
1.8.3 在 SPE 上指定 UPE	15
1.8.4 在 SPE 上发布 VPN 实例的缺省路由	16
1.9 配置跨域 VPN-OptionB	16
1.9.1 配置 UPE 和 ASBR 之间的 MP-IBGP 对等体	16
1.9.2 配置不同 AS 的 ASBR 间的 MP-EBGP 对等体	17
1.10 配置 QoS	17
1.10.1 配置优先级标记	17
1.10.2 (可选) 配置优先级映射	19
1.10.3 配置队列调度	20
1.11 配置可靠性	21
1.11.1 配置 IGP 快速收敛	21
1.11.2 配置 LDP FRR	22
1.11.3 配置 VPN FRR	22
1.11.4 配置 BFD	22
1.12 配置举例	24

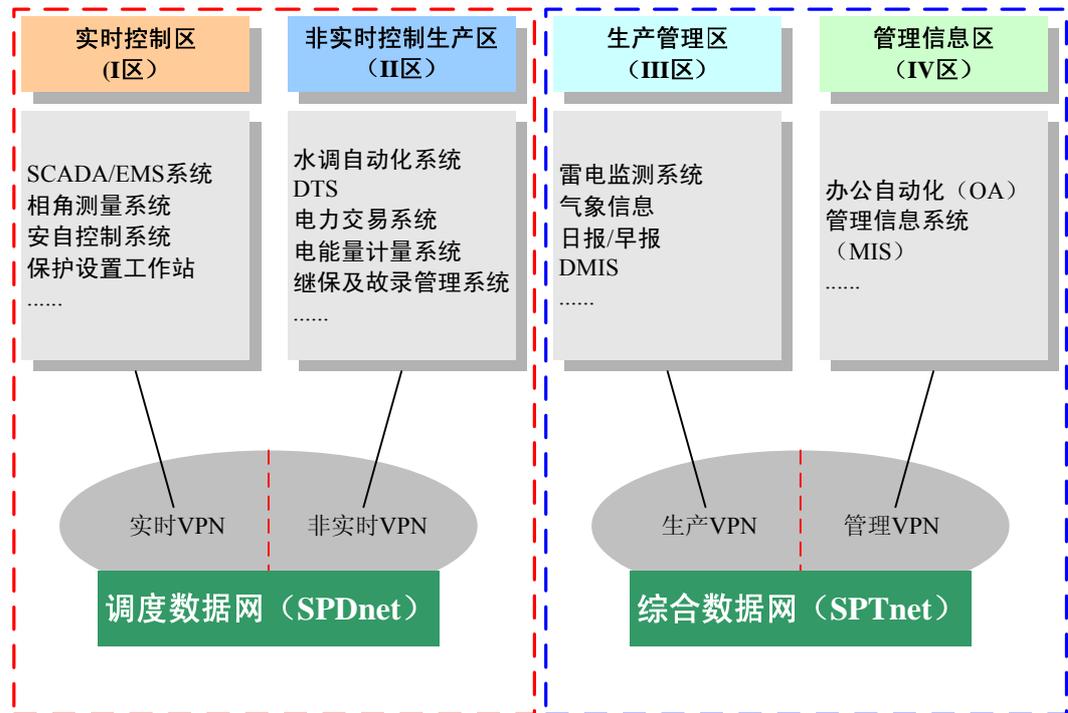
1 地调接入网方案部署

1.1 概述

1.1.1 地调接入网简介

电力系统的生产自动化和信息化依赖于电力数据网。电力数据网又可分为调度数据网（SPDnet）和综合数据网（SPTnet），它们各自承担的职能如图 1-1 所示。

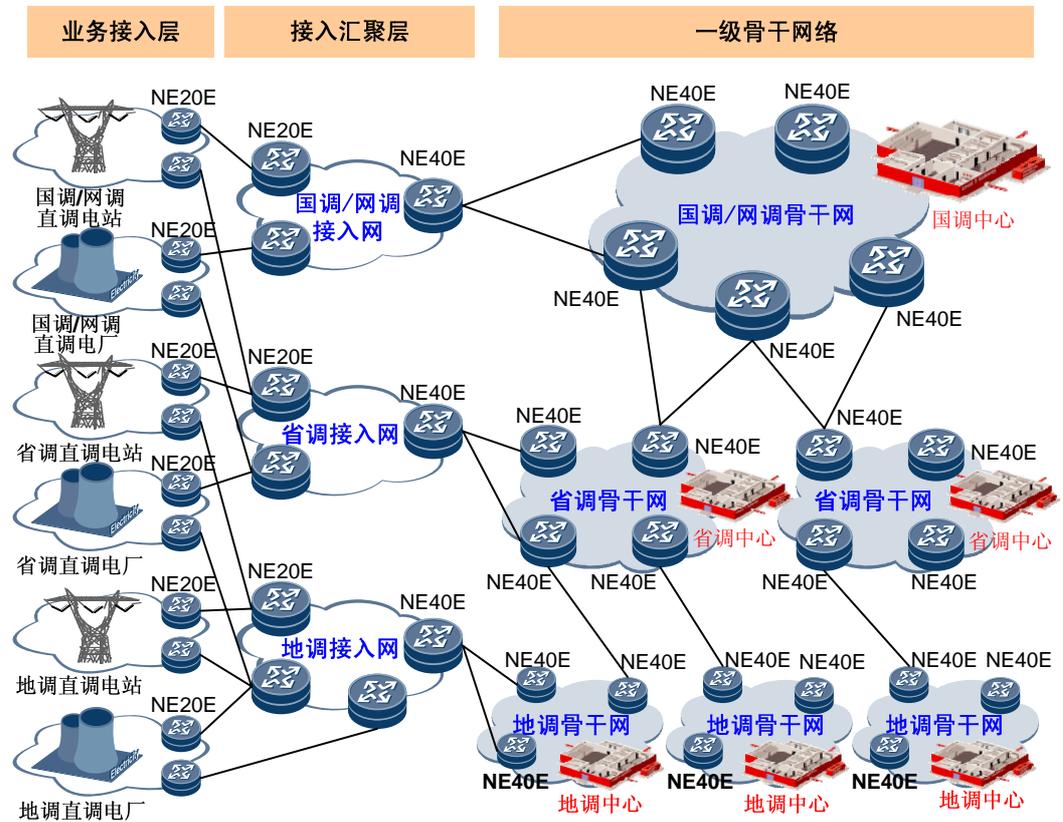
图1-1 电力数据网职能



本章主要描述调度数据网的相关内容。调度数据网是电力的生产控制网络，通过 MPLS VPN 分为实时控制区（I 区）和非控制生产区（II 区），是电力信息化的核心网络之一。

电力调度系统分为国家调度中心（国调）、大区网局级调度控制中心（网调）、省级调度控制中心（省调）、地区调度控制中心（地调）和各级接入网。各级直接管理和调度其下一层调度中心。如图 1-2 所示。

图1-2 调度数据网整体架构

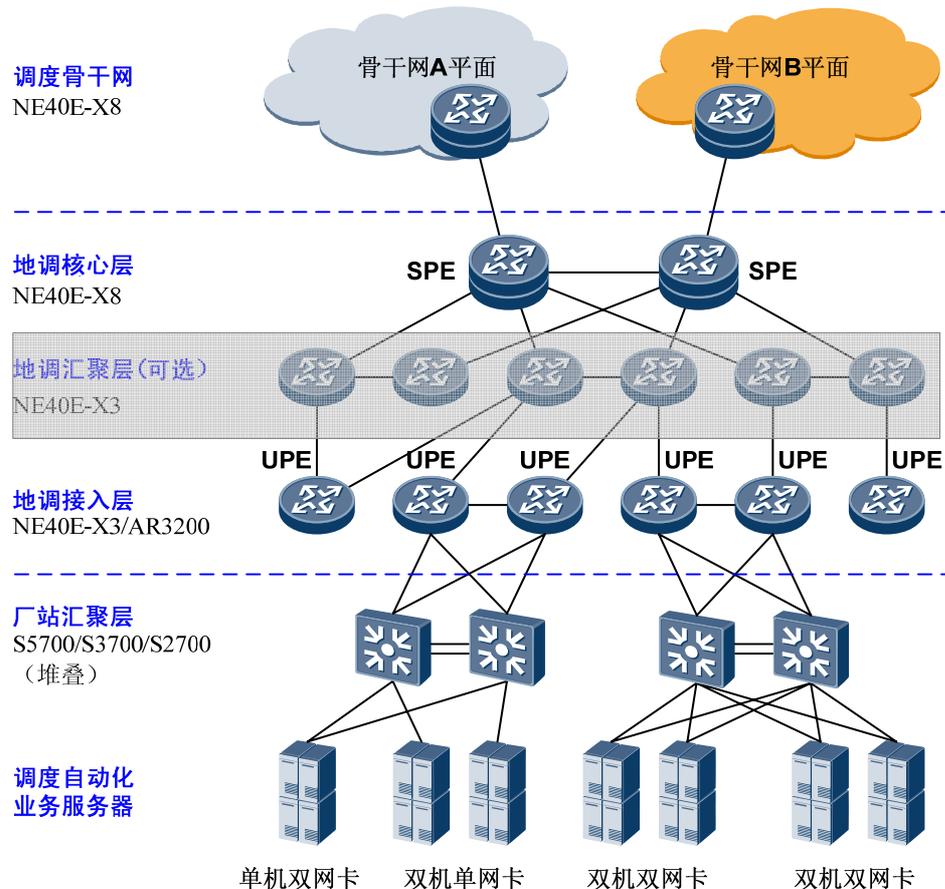


本章只描述地调接入网的组网方案和部署。地调接入网是负责地区电力厂站接入的业务网络，覆盖所属县调、集控站以及 110KV（66KV）、35KV 变电站。

1.1.2 典型组网

地调接入网的典型组网如图 1-3 所示。

图1-3 地调接入网典型组网



地调接入网上行连接骨干网的 A、B 双平面，向下连接各厂站内网。接入网内部可采用两层或三层网络结构。在网络规模较小、传输链路资源不受限制的情况下，接入网核心层节点直接与接入层节点相连。在网络规模较大或传输链路资源受限制的情况下，可在接入网核心层节点与接入层节点间增加一层汇聚节点。

厂站调度自动化业务服务器连接汇聚交换机，汇聚交换机采用二层透传方式将业务汇聚到接入路由器，接入路由器根据业务的不同划分不同的 VLAN。调度自动化业务服务器可选择双机双网卡、双机单网卡、单机双网卡等方式接入，保证接入可靠性。

接入路由器作为 PE，为不同业务构建不同的 VPN，包括实时 VPN、非实时 VPN 和应急 VPN。为了控制 VPN 路由数量，可以采用 HoPE 组网方案，其中接入路由器作为 UPE，核心路由器作为 SPE。

说明

如果接入网的规模过于庞大，还可以采用三层 HoPE 组网，把地调接入网的的汇聚层节点作为 MPE，向下作为 UPE 的 SPE，向上作为 SPE 的 UPE。

1.1.3 配套版本

表1-1 配套产品和版本

部件	产品	版本
地调骨干网路由器	NE40E-X8	V600R003C00
地调接入网核心路由器	NE40E-X8	V600R003C00
地调接入网汇聚路由器	NE40E-X3	V600R003C00
地调接入网接入路由器	NE40E-X3	V600R003C00
	AR3200 系列	V200R001C01
厂站汇聚交换机	S5700/S3700/S2700 系列	V100R006C00

1.1.4 部署思路

前置任务

- 完成各网元/部件的安装调试和线缆连接，各网元上电正常工作。
- 完成各项数据的规划。

配置思路

配置思路	配置注意事项
配置接口	包括接口的物理属性配置、链路层协议配置，以及接口的 IP 地址配置。
配置 IGP	<ul style="list-style-type: none"> • 将接入网的骨干、汇聚区域划为 Area0，各个接入区域可以按照规模情况予以整合，并分为与 Area0 相邻的区域，Area 号顺序分配。 • 为了减少对外发布的路由数量，可以配置 OSPF 路由聚合功能。
配置 BGP	<ul style="list-style-type: none"> • 当地调接入网规模较大，BGP 节点较多时，可以配置路由反射功能。 • 跨域路由传播时，根据电力调度网规范，需要配置路由过滤。
使能 MPLS 基本能力	全局使能 MPLS 和 LDP，在需要转发 MPLS 报文的接口上使能 MPLS 和 LDP。

配置思路	配置注意事项
配置基本 MPLS L3VPN	<ul style="list-style-type: none"> 在 PE 上需要为实时业务、非实时业务和紧急业务分别创建 VPN 实例，并绑定到 VPN Site 接入的接口。 PE 之间需要建立 MP-IBGP 对等体。 PE 和 CE/MCE 之间需要配置路由交互。
(可选) 配置 MCE	如果多个不同 VPN 的 Site 通过同一交换机接入，则需要在该交换机上配置 MCE 功能。
配置 HoVPN	<ul style="list-style-type: none"> 需要在 SPE 上创建 VPN 实例，并指定 UPE。 需要在 UPE 和 SPE 之间建立 MP-IBGP 对等体。 需要在 SPE 上发布 VPN 实例的缺省路由。
配置跨域 VPN-OptionB	<ul style="list-style-type: none"> 需要在 UPE 和 ASBR 之间建立 MP-IBGP 对等体。 需要在不同 AS 的 ASBR 之间建立 MP-EBGP 对等体。
配置 QoS	<p>QoS 采用 Diff-Serv 机制，在 PE（或 UPE）上完成流分类和重标记，在上层网络中按照报文优先级进行队列调度和拥塞控制。</p> <ul style="list-style-type: none"> 实时业务既保证带宽，又保证时延，设为 AF4，保证 60%接口带宽； 非实时业务设为 AF3，保证 30%接口带宽； 应急业务设为 AF2，当其他流量中断时，可使用网络所有带宽。
配置可靠性	<ul style="list-style-type: none"> 通过网络设计，采用节点双设备设置和节点设备间对称连接，备份路径预先设定，为实施快速切换提供网络拓扑基础。 在节点之间部署故障快速检测机制 BFD，迅速检测到链路或者节点故障。 通过 LDP FRR/VPN FRR 等技术，在故障发生时可以快速切换到备用链路。 在故障发生时，通过 IGP 快速收敛，实现路由的快速重新计算。

1.2 配置接口

接口的配置主要包括接口的物理属性配置、链路层协议配置，以及接口的 IP 地址配置。相关的配置请参考所使用产品的产品文档，本章不做详细介绍。

1.3 配置 IGP

对于 IGP，地调接入网中一般选择 OSPF。可以按照如下原则进行：

- 只启动一个 OSPF 进程。
- 采用分区设计，可以将接入网的骨干、汇聚区域划为 Area0，各个接入区域可以按照规模情况予以整合，并分为与 Area0 相邻的区域，Area 号顺序分配。
- 如果接入区域很少，则可以把所有路由节点都配置为 Area0。
- 如果某些接入区域较大，路由数量较多，可以将该 Area 设置为 NSSA 区域，限制 LSA 在区域间的传播。

1.3.1 配置 OSPF 基本功能

请在需要运行 OSPF 协议的每台路由器上进行以下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf [process-id]**，启动 OSPF 进程，进入 OSPF 视图。

步骤 3 执行命令 **area area-id**，进入 OSPF 区域视图。

步骤 4 执行命令 **network ip-address wildcard-mask [description text]**，配置区域所包含的网段。

----结束

1.3.2 (可选) 配置 NSSA 区域

如果要把某个区域设定为 NSSA 区域，请在 NSSA 区域中所有路由器上进行如下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf [process-id]**，进入 OSPF 视图。

步骤 3 执行命令 **area area-id**，进入 OSPF 区域视图。

步骤 4 执行命令 **nssa [default-route-advertise | flush-waiting-timer interval-value | no-import-route | no-summary | set-n-bit | suppress-forwarding-address | translator-always | translator-interval interval-value | zero-address-forwarding] ***，配置一个区域为 NSSA 区域。

----结束

1.3.3 配置 OSPF 路由聚合

地调接入网中，为了减少对外发布的路由数量，可以配置 OSPF 路由聚合功能，将具有相同前缀的路由信息聚合在一起，只发布一条路由到其它区域。

OSPF 路由聚合有 ABR 聚合和 ASBR 聚合两种方式。

配置 ABR 路由聚合

在 ABR 设备上进行如下配置。

- 步骤 1 执行命令 **system-view**，进入系统视图。
 - 步骤 2 执行命令 **ospf [process-id]**，进入 OSPF 视图。
 - 步骤 3 执行命令 **area area-id**，进入 OSPF 区域视图。
 - 步骤 4 执行命令 **abr-summary ip-address mask [[advertise | not-advertise] | cost cost] ***，配置 OSPF 的 ABR 路由聚合。
- 结束

配置 ASBR 路由聚合

在 ASBR 设备上进行如下配置。

- 步骤 1 执行命令 **system-view**，进入系统视图。
 - 步骤 2 执行命令 **ospf [process-id]**，进入 OSPF 视图。
 - 步骤 3 执行命令 **asbr-summary ip-address mask [not-advertise | tag tag | cost cost | distribute-delay interval] ***，配置 OSPF 的 ASBR 路由聚合。
- 结束

1.3.4 配置 OSPF 引入其他路由

地调接入网中的 OSPF 有可能需要引入骨干网和接入网之间的跨域静态路由。

如果需要 OSPF 引入其他路由，在 ASBR 上进行如下配置。

- 步骤 1 执行命令 **system-view**，进入系统视图。
 - 步骤 2 执行命令 **ospf [process-id]**，进入 OSPF 视图。
 - 步骤 3 执行命令 **import-route { limit limit-number | protocol [process-id] [cost cost | route-policy route-policy-name | tag tag | type type] * }**，引入其它协议的路由信息。
- 如果要引入静态路由，则 *protocol* 选择为 **static**。
- 结束

1.3.5（可选）配置 IGP 快速收敛

请参见“[1.11.1 配置 IGP 快速收敛](#)”。

1.4 配置 BGP

在地调接入网中，BGP 的配置与具体的业务有关，本节只介绍 BGP 的通用配置。实际方案中的具体部署，请参考以下部分：

- [1.6 配置基本 MPLS L3VPN](#)
- [1.8 配置 HoVPN](#)

- 1.9 配置跨域 VPN-OptionB

1.4.1 启动 BGP 进程

在需要启动 BGP 连接的路由器上进行如下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp as-number**，启动 BGP（指定本地 AS 编号），进入 BGP 视图。

步骤 3（可选）执行命令 **router-id ipv4-address**，配置 BGP 的 Router ID。

 说明

为了增加网络的可靠性，建议将 Router ID 手工配置为 Loopback 接口的地址。

----结束

1.4.2 配置 BGP 对等体

在需要启动 BGP 连接的路由器上进行如下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp as-number**，进入 BGP 视图。

步骤 3 执行命令 **peer ipv4-address as-number as-number**，指定对等体 IP 地址及其所属的 AS 号。

对于 IBGP 来说，对等体的 AS 号相同；对于 EBGP 来说，对等体的 AS 号不同。

步骤 4（对于 EBGP，可选）执行命令 **peer { ipv4-address | group-name } ebgp-max-hop [hop-count]**，配置 EBGP 连接的最大跳数。

通常情况下，EBGP 对等体之间必须具有直连的物理链路，如果不满足这一要求，则必须使用 **peer ebgp-max-hop** 命令允许它们之间经过多跳建立 TCP 连接。

步骤 5（可选）执行命令 **peer { ipv4-address | group-name } description description-text**，配置对等体或对等体组的描述信息。

----结束

1.4.3（可选）配置 BGP 连接所使用的本地接口

当指定对等体的 IP 地址为非直连的物理链路时，请在路由器上进行以下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp as-number**，进入 BGP 视图。

步骤 3 执行命令 **peer { ipv4-address | group-name } connect-interface interface-type interface-number [ipv4-source-address]**，指定 BGP 连接所使用的建立 TCP 连接会话的源接口和源地址。

----结束

1.4.4 配置路由反射器

如果地调接入网的规模较大，为了减少 BGP 对等体的数量，可以采用路由反射机制。

根据接入网的规模不同，可以采用一级或两级路由反射规划。

- 两层结构的接入网采用一级路由反射规划，路由反射器为接入网的核心节点，客户为接入节点。
- 三层结构的接入网采用两级路由反射规划，一级路由反射器为接入网核心节点，客户为接入网汇聚节点；二级路由反射器规划为接入网汇聚节点，客户为接入网接入节点。

在作为路由反射器的路由器上进行如下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp as-number**，进入 BGP 视图。

步骤 3 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。

步骤 4 执行命令 **peer { ipv4-address | group-name } reflect-client**，配置路由反射器及其客户。

----结束

1.4.5 配置路由过滤

在接入网和骨干网之间通过 BGP 传播路由时，根据规范需要对路由进行过滤，例如：

- 接入网核心设备只向骨干网发送本 AS 始发的路由。
- 骨干网设备上只接收接入网中只经过一个 AS 的路由。
- 骨干网设备上向接入网发布路由时指定接收者不向其他 AS 传播路由。

上述规范都可以通过配置路由过滤实现。

配置 AS-Path 过滤器

在需要进行路由发布或接收过滤的路由器（例如接入网核心路由器）上进行如下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip as-path-filter { as-path-filter-number | as-path-filter-name } { permit | deny } regular-expression**，配置 AS 路径过滤器。

例如，对于只向骨干网发送本 AS 始发的路由，则可以设置正则表达式为 $^{\wedge}\$$ 。而骨干网设备上只接收接入网中只经过一个 AS 的路由，正则表达式为 $^{\wedge}as-number\$\$$ 。

----结束

配置路由策略

在需要进行路由发布或接收过滤的路由器（例如接入网核心路由器）上进行如下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **route-policy route-policy-name { permit | deny } node node**，创建路由策略的节点，并进入路由策略视图。

步骤 3 执行命令 **if-match as-path-filter { as-path-filter-number | as-path-filter-name } &<1-16>**，配置匹配 AS-Path 过滤器。

对于匹配 AS-Path 过滤器的路由，其路由策略应设置为 **permit**。

步骤 4（可选）执行命令 **apply community { { community-number | aa:nn } &<1-32> | internet | no-advertise | no-export | no-export-subconfed }* [additive]**，设置 BGP 路由信息的团体属性。

例如，如果骨干网设备上向接入网发布路由时，指定接收者不能向其他 AS 传播路由，则可以设置 **no-export** 关键字。

----结束

配置 BGP 路由信息的发布或接收策略

在需要进行路由发布或接收的路由器（例如接入网核心路由器）上进行如下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp as-number**，进入 BGP 视图。

步骤 3 执行命令 **ipv4-family unicast**，进入 IPv4 单播地址族视图。

步骤 4 执行命令 **peer { ipv4-address | group-name } route-policy route-policy-name { export | import }**，配置向指定对等体发布路由时，或者从对等体接收路由时，所使用的路由过滤策略。

----结束

1.5 使能 MPLS 基本能力

BGP/MPLS L3VPN 是基于 MPLS 实现的，因此需要在各级路由器上使能 MPLS 和 LDP，使之具备基本的 MPLS 报文转发能力。需要使能 MPLS 和 LDP 的路由器包括地调接入网中的 UPE、MPE（可能有）、SPE，以及骨干网上的各级节点。

1.5.1 配置 LSR ID

LSR ID 用于标识一个 LSR，配置 LSR ID 是配置其他 MPLS 命令的前提。一般采用路由器的某个 Loopback 接口地址作为 LSR ID。

请在各级路由器上进行如下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mpls lsr-id lsr-id**，配置本节点的 LSR ID。

----结束

1.5.2 使能 MPLS

请在各级路由器上进行如下配置。

- 步骤 1 执行命令 **system-view**，进入系统视图。
- 步骤 2 执行命令 **mpls**，使能本节点的 MPLS，并进入 MPLS 视图。
- 步骤 3 执行命令 **quit**，退回系统视图。
- 步骤 4 执行命令 **interface interface-type interface-number**，配置需要转发 MPLS 报文的接口。
- 步骤 5 执行命令 **mpls**，使能接口的 MPLS。

----结束

1.5.3 配置 MPLS LDP

请在各级路由器上进行如下配置。

- 步骤 1 执行命令 **system-view**，进入系统视图。
- 步骤 2 执行命令 **mpls ldp**，使能全局的 LDP 功能，并进入 MPLS-LDP 视图。
- 步骤 3 执行命令 **quit**，退回系统视图。
- 步骤 4 执行命令 **interface interface-type interface-number**，进入需要建立 LDP 会话的接口视图。
- 步骤 5 执行命令 **mpls ldp**，使能接口的 LDP 功能。

----结束

1.6 配置基本 MPLS L3VPN

1.6.1 创建 VPN 实例

在 UPE 上进行如下配置。

- 步骤 1 执行命令 **system-view**，进入系统视图。
- 步骤 2 执行命令 **ip vpn-instance vpn-instance-name**，创建 VPN 实例，并进入 VPN 实例视图。
- 步骤 3 执行命令 **ipv4-family**，使能 VPN 实例 IPv4 地址族，并进入 VPN 实例 IPv4 地址族视图。
- 步骤 4 执行命令 **route-distinguisher route-distinguisher**，配置 VPN 实例 IPv4 地址族的 RD。

RD 用于区分使用相同地址空间的 IPv4 前缀。同一 VPN 的 RD 必须全局统一，不同 VPN 的 RD 不能相同。

- 步骤 5 执行命令 **vpn-target vpn-target <1-8> [both | export-extcommunity | import-extcommunity]**，为 VPN 实例 IPv4 地址族配置 VPN-target 扩展团体属性。

VPN Target 是 BGP 的扩展团体属性，用来控制 VPN 路由信息的接收和发布。一条 vpn-target 命令最多可以配置 8 个 VPN Target。

----结束

1.6.2 配置接口与 VPN 实例绑定

在 PE 上通过配置接口与 VPN 实例绑定，该接口成为私网接口，从该接口进入的报文使用 VPN 实例中的转发信息进行转发。

在 UPE 上进行如下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface interface-type interface-number**，进入要绑定 VPN 实例的接口视图。

interface-type interface-number 就是 PE 连接 VPN 的 Site 的 CE 的接口。如果多个不同 VPN 的 Site 通过同一个 MCE 设备接入，而 MCE 又通过同一物理接口接入 PE，则需要配置多个子接口，并把子接口与 VPN 实例绑定。

步骤 3 执行命令 **ip binding vpn-instance vpn-instance-name**，将当前接口与 VPN 实例绑定。

步骤 4 执行命令 **ip address ip-address { mask | mask-length }**，配置接口的 IP 地址。

----结束

1.6.3 在 PE 之间建立 MP-IBGP 对等体

MP-IBGP 通过在 BGP 中引入扩展团体属性，使其能够在 PE 设备之间传播 VPNv4 路由。



如果采用 HoVPN 组网，则 UPE 之间不需要直接建立对等体，UPE 只需要和 SPE 建立对等体即可，详细步骤请参见“[1.8.2 配置 UPE 和 SPE 之间的 MP-IBGP 对等体](#)”。

在每个接入 CE 或 MCE 的 PE 上进行如下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp as-number**，进入 BGP 视图。

步骤 3 执行命令 **peer ipv4-address as-number as-number**，将对端 PE 配置为对等体。

步骤 4 执行命令 **peer ipv4-address connect-interface loopback interface-number**，指定建立 TCP 连接的接口。

步骤 5 执行命令 **ipv4-family vpnv4**，进入 BGP-VPNv4 子地址族视图。

步骤 6 执行命令 **peer ipv4-address enable**，使能对等体交换 VPNv4 路由信息的能力。

----结束

1.6.4 配置 PE 与 CE/MCE 之间的路由交互

通过配置 PE 与 CE/MCE 之间的路由交互，可以将 VPN Site 内的 VPN 路由引入到 PE 设备并向远端 PE 进行发布，从而实现各 Site 之间的互通。

PE 和 CE/MCE 间的路由交互可以采用 EBGP、IBGP、静态路由、RIP、OSPF、ISIS，任选一种即可。以下过程以 EBGP 为例进行描述，其余方式请参考相应产品的文档中关于 VPN 的配置指导。

在 PE 上配置 EBGP

- 步骤 1 执行命令 **system-view**，进入系统视图。
- 步骤 2 执行命令 **bgp as-number**，进入 BGP 视图。
- 步骤 3 执行命令 **ipv4-family vpn-instance vpn-instance-name**，进入 BGP-VPN 实例 IPv4 地址族视图。
- 步骤 4 执行命令 **peer ipv4-address as-number as-number**，将 CE 配置为 VPN 私网对等体。
- 步骤 5（可选）执行命令 **import-route direct [med med | route-policy route-policy-name]***，引入到本地 CE 的直连路由。

----结束

在 CE/MCE 上配置 EBGP

- 步骤 1 执行命令 **system-view**，进入系统视图。
- 步骤 2 执行命令 **bgp as-number**，进入 BGP 视图。
- 步骤 3（可选）如果是 MCE 设备，执行命令 **ipv4-family vpn-instance vpn-instance-name**，进入 BGP-VPN 实例视图。
- 步骤 4 执行命令 **peer ipv4-address as-number as-number**，将 PE 配置为对等体。
- 步骤 5 执行命令 **import-route { direct | static | rip process-id | ospf process-id | isis process-id } [med med | route-policy route-policy-name]***，引入本站点的路由。

----结束

1.7（可选）配置 MCE

如果多个不同 VPN 的 Site 通过同一交换机接入，则需要在该交换机上配置 MCE 功能。通过 MCE 功能，可以在一台交换机上实现多个 CE 的功能，实现不同机构或着业务之间的隔离。

在作为 MCE 的交换机上进行如下配置。

1.7.1 配置 VPN 实例

- 步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip vpn-instance** *vpn-instance-name*, 创建 VPN 实例, 并进入 VPN 实例视图。

步骤 3 执行命令 **route-distinguisher** *route-distinguisher*, 配置 VPN 实例 IPv4 地址族的 RD。

----结束

1.7.2 在接口上绑定 VPN 实例

步骤 1 执行命令 **system-view**, 进入系统视图。

步骤 2 执行命令 **interface vlanif** *interface-number*, 进入要绑定 VPN 实例的 VLAN 接口视图。

步骤 3 执行命令 **ip binding vpn-instance** *vpn-instance-name*, 将当前接口与 VPN 实例绑定。

步骤 4 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }, 配置接口的 IP 地址。

----结束

1.7.3 配置 PE 和 MCE 之间的路由交互

请参见“1.6.4 配置 PE 与 CE/MCE 之间的路由交互”。

1.7.4 配置 MCE 和 CE 之间的路由交互

MCE 与 CE 之间的路由交互可以采用 EBGP、IBGP、静态路由、RIP、OSPF、ISIS, 任选一种即可。以下过程以 EBGP 为例进行描述, 其余方式请参考相应产品的文档中关于 VPN 的配置指导。

在 MCE 上配置 EBGP

步骤 1 执行命令 **system-view**, 进入系统视图。

步骤 2 执行命令 **bgp** *as-number*, 进入 BGP 视图。

步骤 3 执行命令 **ipv4-family vpn-instance** *vpn-instance-name*, 进入 BGP-VPN 实例 IPv4 地址族视图。

步骤 4 执行命令 **peer** *ipv4-address* **as-number** *as-number*, 将 CE 配置为 VPN 私网对等体。

步骤 5 (可选) 执行命令 **import-route direct** [**med** *med* | **route-policy** *route-policy-name*]*, 引入到本地 CE 的直连路由。

----结束

在 CE 上配置 EBGP

步骤 1 执行命令 **system-view**, 进入系统视图。

步骤 2 执行命令 **bgp** *as-number*, 进入 BGP 视图。

步骤 3 执行命令 **peer** *ipv4-address* **as-number** *as-number*, 将 MCE 配置为对等体。

步骤 4 执行命令 **import-route { direct | static | rip process-id | ospf process-id | isis process-id } [med med | route-policy route-policy-name]***，引入本站点的路由。

----结束

1.8 配置 HoVPN

当地调接入网中采用 HoPE 组网方案时，地调接入路由器作为 UPE，地调核心路由器作为 SPE。此时需要进行 HoVPN 的配置。

1.8.1 在 SPE 上创建 VPN 实例

当使用 HoPE 组网方案时，SPE 上也需要配置各个 VPN 的 VPN 实例，但不需要绑定接口。在 SPE 上进行如下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip vpn-instance vpn-instance-name**，创建 VPN 实例，并进入 VPN 实例视图。

步骤 3 执行命令 **ipv4-family**，使能 VPN 实例 IPv4 地址族，并进入 VPN 实例 IPv4 地址族视图。

步骤 4 执行命令 **route-distinguisher route-distinguisher**，配置 VPN 实例 IPv4 地址族的 RD。

RD 用于区分使用相同地址空间的 IPv4 前缀。同一 VPN 的 RD 必须全局统一，不同 VPN 的 RD 不能相同。

步骤 5 执行命令 **vpn-target vpn-target <1-8> [both | export-extcommunity | import-extcommunity]**，为 VPN 实例 IPv4 地址族配置 VPN-target 扩展团体属性。

VPN Target 是 BGP 的扩展团体属性，用来控制 VPN 路由信息的接收和发布。一条 vpn-target 命令最多可以配置 8 个 VPN Target。

----结束

1.8.2 配置 UPE 和 SPE 之间的 MP-IBGP 对等体

在 UPE 和 SPE 上分别进行如下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bgp as-number**，进入 BGP 视图。

步骤 3 执行命令 **peer ipv4-address as-number as-number**，将 SPE（UPE）配置为对等体。

步骤 4 执行命令 **ipv4-family vpnv4**，进入 BGP-VPNv4 子地址族视图。

步骤 5 执行命令 **peer ipv4-address enable**，使能对等体交换 VPNv4 路由信息的能力。

----结束

1.8.3 在 SPE 上指定 UPE

在 SPE 上进行如下配置。

- 步骤 1 执行命令 **system-view**，进入系统视图。
 - 步骤 2 执行命令 **bgp as-number**，进入 BGP 视图。
 - 步骤 3 执行命令 **ipv4-family vpnv4 [unicast]**，进入 BGP-VPNv4 子地址族视图。
 - 步骤 4 执行命令 **peer { ipv4-address | group-name } upe**，将对等体指定为自己的 UPE。
- 结束

1.8.4 在 SPE 上发布 VPN 实例的缺省路由

SPE 向 UPE 发布一条下一跳地址为本地地址的缺省路由，用以指导 UPE 上的 VPN 报文转发。

在 SPE 上进行如下配置。

- 步骤 1 执行命令 **system-view**，进入系统视图。
- 步骤 2 执行命令 **bgp as-number**，进入 BGP 视图。
- 步骤 3 执行命令 **ipv4-family vpnv4**，进入 BGP-VPNv4 子地址族视图。
- 步骤 4 执行命令 **peer { ipv4-address | group-name } default-originate vpn-instance vpn-instance-name**，向 UPE 发送指定 VPN 实例的缺省路由。

执行此命令后，不论本地路由表中是否存在缺省路由，SPE 都会向 UPE 发布一条下一跳地址为本地地址的缺省路由。

----结束

1.9 配置跨域 VPN-OptionB

在电力的调度数据网，调度骨干网和各级调度接入网分属不同的 AS 域，例如 A 平面的调度骨干网 AS 号为 20000，各级调度接入网的编号则是 2XXYY 格式，XX 为国网省编码，YY 为各地区编码。因此在构建 MPLS VPN 时，需要进行跨域 VPN 部署。

根据 RFC2547bis，跨域 VPN 有 OptionA (VRF-to-VRF)、OptionB (MP-EBGP) 和 OptionC (Multi-hop MP-EBGP) 三种部署方式。而根据电力调度网的相关规范，在电力调度网中，主要采用 OptionB 方式。

在 OptionB 方式下，两个 ASBR 之间运行 MP-EBGP 协议，MP-EBGP 协议将一个域内的所有的 VPN 信息传递给另外一个域，传递的是私网路由和标签信息。对端的 ASBR 收到 VPN 路由信息后，在本地保存，再继续向自己域内的 PE 设备扩散。

1.9.1 配置 UPE 和 ASBR 之间的 MP-IBGP 对等体

由于 ASBR 同时又是 HoVPN 中的 SPE，因此，其配置过程请参见“[1.8.2 配置 UPE 和 SPE 之间的 MP-IBGP 对等体](#)”。如果上述配置已完成，则本步骤无需重复。

1.9.2 配置不同 AS 的 ASBR 间的 MP-EBGP 对等体

在地调接入网中，核心路由器作为本接入网 AS 域的 ASBR，而骨干网中的地调节点作为骨干网 AS 域的 ASBR，两者之间运行 MP-EBGP 协议交换 VPN 路由信息。

在各 ASBR 上进行如下配置。

- 步骤 1 执行命令 **system-view**，进入系统视图。
- 步骤 2 执行命令 **bgp as-number**，进入 BGP 视图。
- 步骤 3 执行命令 **peer ipv4-address as-number as-number**，指定对端 ASBR 为自己的 EBGP 对等体。
- 步骤 4 执行命令 **ipv4-family vpnv4 [unicast]**，进入 BGP-VPNv4 子地址族视图。
- 步骤 5 执行命令 **peer ipv4-address enable**，使能与对端 ASBR 交换 VPNv4 路由的能力。

----结束

1.10 配置 QoS

在电力调度网中，QoS 采用 Diff-Serv 机制，在 PE（或 UPE）上完成流分类和重标记，在上层网络中按照报文优先级进行队列调度和拥塞控制。

网络业务分类按 VPN 划分，确保安全区 I（控制区）中的业务优先传输。例如在 PE（或 UPE）配置 DSCP 标记如下：

- 实时业务既保证带宽，又保证时延，设为 AF4，保证 60%接口带宽；
- 非实时业务设为 AF3，保证 30%接口带宽；
- 应急业务设为 AF2，当其他流量中断时，可使用网络所有带宽。



注意

本文只以 NE40E 为例说明基本的配置思路。如果是其他型号的路由器（例如 AR3200 路由器），基本的配置思路相似，但是配置方式和配置命令可能有所不同。请参考具体产品的使用文档。

1.10.1 配置优先级标记

配置 ACL

在 PE（或 UPE）上进行如下配置。

- 步骤 1 执行命令 **system-view**，进入系统视图。
- 步骤 2 执行命令 **acl [number] acl-number [match-order { auto | config }]**，创建一个高级访问控制列表。

步骤 3 执行命令 **rule permit ip vpn-instance** *vpn-instance-name*，配置基于 VPN 实例的匹配规则。

 说明

需要为实时业务 VPN、非实时业务 VPN 和紧急业务 VPN 各创建一个 ACL。

----结束

配置流分类

在 PE（或 UPE）上进行如下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **traffic classifier** *classifier-name*，创建流分类并进入流分类视图。

步骤 3 执行命令 **if-match acl** *acl-number*，定义基于 ACL 的匹配规则。

 说明

这里的 ACL 就是上面用于匹配 VPN 实例的 ACL。

----结束

配置流行为

在 PE（或 UPE）上进行如下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **quit**，返回系统视图。

步骤 3 执行命令 **traffic behavior** *behavior-name*，创建流行为并进入流行为视图。

步骤 4 执行命令 **remark dscp** *dscp-value*，指定报文的 DSCP 值。

- 实时业务 VPN 的报文，DSCP 值为 AF41；
- 非实时业务 VPN 的报文，DSCP 值为 AF31；
- 紧急业务 VPN 的报文，DSCP 值为 AF21。

步骤 5 执行命令 **service-class** *service-class* **color** *color*，配置报文的服务等级。

配置本步骤的目的是使得报文在 PE/UPE 上可以直接进入指定服务等级的队列，而不需根据报文头中的优先级字段查 BA 表来确定服务等级。

----结束

配置流策略并关联流分类和流行为

在 PE（或 UPE）上进行如下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **traffic policy** *policy-name*，创建流策略并进入流策略视图。

- 步骤 3 执行命令 **classifier classifier-name behavior behavior-name**，关联流分类和流行为。
----结束

在接口上应用流策略

在 PE（或 UPE）上进行如下配置。

- 步骤 1 执行命令 **system-view**，进入系统视图。
步骤 2 执行命令 **interface interface-type interface-number**，进入接口视图。

说明

这里的接口是指 VPN 的 CE/MCE 接入的接口。

- 步骤 3 执行命令 **traffic-policy policy-name inbound**，在接口入方向应用流策略。
----结束



上述基于 ACL 的流分类是考虑到有可能一个接口下可能有多个 VPN 接入，因此需要通过 ACL 进行细分。如果一个接口下只有一个 VPN 接入时，可以不需要配置 ACL，直接使用 **if-match any** 命令来配置流分类，再配置流行为和流策略之后，直接将流策略应用到指定接口即可。

1.10.2（可选）配置优先级映射

当路由器收到一个带有 DSCP 优先级的报文之后，首先需要将 DSCP 优先级映射为内部的服务等级（EF、AF1~4、BE、CS 等）以及报文颜色（Green、Yellow、Red），然后根据服务等级进行优先级调度。

路由器中，缺省已经定义了 DSCP 优先级和内部服务等级的映射关系（名为 default 的 DS 域的配置），如果没有特殊需求，采用系统缺省的映射关系即可。如果有特殊需求，可以自定义 DSCP 优先级和服务等级的映射关系。

在 PE/UPE 之外的所有路由器上进行如下配置。

- 步骤 1 执行命令 **system-view**，进入系统视图。
步骤 2 执行命令 **diffserv domain { ds-domain-name | default }**，定义 DS 域并进入 DS 域视图。
步骤 3 执行命令 **ip-dscp-inbound dscp-value phb service-class [color]**，配置 DSCP 优先级和内部服务等级的映射关系。
步骤 4 执行命令 **quit**，退回到系统视图。
步骤 5 执行命令 **interface interface-type interface-number**，进入接口视图。

这里的接口是指报文的入方向接口。

步骤 6 执行命令 **trust upstream { 5p3d | ds-domain-name | default }**，在接口上绑定 DS 域。

----结束

1.10.3 配置队列调度

当不同业务的报文在 PE/UPE 上被标记了 DSCP 优先级之后，主干网络中的路由器将根据报文的 DSCP 优先级进行优先级队列调度，以保证不同业务的带宽和优先级。因此需要在主干网络中（包括 PE/UPE）的所有路由器上配置优先级队列调度。

配置队列调度主要包括两个方面：

- 拥塞管理：配置不同优先级报文所使用的队列调度方式，以及所占用的带宽。
- 拥塞避免：配置当出现拥塞时，对于报文的丢弃策略。

不同的路由器对于队列调度有不同的配置方式，以下以 NE40E 为例说明队列调度的配置方式。

（可选）配置 WRED 模板

如果对于报文的丢弃策略采用 WRED 方式，则需要配置 WRED 模板；如果采用尾丢弃策略，则不需要配置 WRED 模板。

在所有路由器（包括 PE/UPE）上进行如下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **port-wred port-wred-name**，创建类队列 WRED 模板并进入 WRED 视图。

步骤 3 执行命令 **color { green | yellow | red } low-limit low-limit-percentage high-limit high-limit-percentage discard-percentage discard-percentage**，配置不同颜色的报文的高低门限百分比和丢弃概率。

----结束

配置队列调度

在所有路由器（包括 PE/UPE）上进行如下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

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

这里的接口是指报文的出方向接口。

步骤 3 执行命令 **port-queue cos-value { { pq | wfq weight weight-value | lpq } | shaping { shaping-value | shaping-percentage shaping-percentage-value } | port-wred wred-name } * outbound**，在接口上为不同业务等级的类队列配置调度策略，并在调度策略中应用配置好的 WRED 模板。

本步骤中，需要注意如下几点：

- 如果队列的拥塞避免策略为尾丢弃，则不需要指定 **port-wred wred-name**；如果拥塞避免策略为 WRED，则需要指定 **port-wred wred-name**。

- 如果在队列调度时, 还需要实时流量整形, 则可以指定 **shaping** 关键字及相关参数。
 - 对于实时业务、非实时业务、紧急业务的队列调度配置如下:
 - 实时业务: **port-queue af4 wfq weight 60 outband**
 - 非实时业务: **port-queue af3 wfq weight 30 outband**
 - 紧急业务: **port-queue af2 wfq weight 10 outband**
- 结束

1.11 配置可靠性

地调接入网的可靠性策略可以分为以下几个方面:

- 通过网络设计, 采用节点双设备设置和节点设备间对称连接, 备份路径预先设定, 为实施快速切换提供网络拓扑基础。
- 在节点之间部署故障快速检测机制 BFD, 迅速检测到链路或者节点故障。
- 通过 LDP FRR/VPN FRR 等技术, 在故障发生时可以快速切换到备用链路。
- 在故障发生时, 通过 IGP 快速收敛, 实现路由的快速重新计算。



注意

本节涉及的可靠性功能, 均以 NE40E 为例进行说明, 在其他设备上有可能不支持, 请以所使用设备的实际情况为准。

1.11.1 配置 IGP 快速收敛

为了保证 OSPF 的快速收敛, 提高网络可靠性, 可以配置 IGP FC 功能。

- 步骤 1 执行命令 **system-view**, 进入系统视图。
- 步骤 2 执行命令 **ospf [process-id]**, 进入 OSPF 视图。
- 步骤 3 执行命令 **prefix-priority { critical | high | medium } ip-prefix ip-prefix-name**, 配置 OSPF 路由的收敛优先级。
- 步骤 4 执行命令 **lsa-originate-interval { 0 | { intelligent-timer max-interval start-interval hold-interval | other-type interval } * }**, 配置 LSA 的更新时间间隔。
- 步骤 5 执行命令 **lsa-arrival-interval { interval | intelligent-timer max-interval start-interval hold-interval }**, 配置 LSA 被接收的时间间隔。
- 步骤 6 执行命令 **spf-schedule-interval { interval1 | intelligent-timer max-interval start-interval hold-interval | millisecond interval2 }**, 设置 SPF 计算间隔。

----结束

1.11.2 配置 LDP FRR

LDP FRR 通过建立一条备用 LSP，来保证在主用 LSP 故障时，可以快速切换到备用 LSP 进行 MPLS 报文转发，这样可以在网络收敛之前的短时间内保证流量不中断。

LDP FRR 有 Manual 和 Auto 两种配置方式，在调度接入网中建议采用 LDP Auto FRR。

在 LSP 的 Ingress 或 Transit 节点进行如下配置。

- 步骤 1 执行命令 **system-view**，进入系统视图。
- 步骤 2 执行命令 **mpls ldp**，进入 MPLS LDP 视图。
- 步骤 3 执行命令 **auto-frr lsp-trigger { all | host | ip-prefix ip-prefix-name | none }**，配置触发 LDP 建立备份 LSP 的策略。

缺省情况下，32 位地址的备份路由触发 LDP 建立备份 LSP。

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

----结束

1.11.3 配置 VPN FRR

VPN FRR 是在 CE 双归属的 VPN 网络环境中，当 PE 设备发生故障时使 VPN 业务快速切换的技术。

VPN FRR 利用基于 VPN 的私网路由快速切换技术，通过预先在远端 PE 中设置指向主用 PE 和备用 PE 的主备用转发项，并结合 PE 故障快速探测，在 VPN 路由收敛完成之前，先将 VPN 流量切换到备份路径上。

VPN FRR 有 Manual 和 Auto 两种配置方式，在调度接入网中建议采用 VPN Auto FRR。

在 PE（或者 UPE）上进行如下配置。

- 步骤 1 执行命令 **system-view**，进入系统视图。
- 步骤 2 执行命令 **bgp as-number**，进入 BGP 视图。
- 步骤 3 执行命令 **ipv4-family vpn-instance vpn-instance-name**，进入 BGP-VPN 实例 IPv4 地址族视图。
- 步骤 4 执行命令 **auto-frr**，使能 VPN Auto FRR 功能。

----结束

1.11.4 配置 BFD

BFD 是一种应用广泛的快速检测协议，BFD 用来对任何媒介、任何协议层进行实时地检测。在地调接入网中，建议部署 BFD for OSPF、BFD for BGP、BFD for LDP LSP。

BFD 可与 LDP FRR、VPN FRR 等联动，在故障发生时触发快速切换。

- BFD 与 LDP FRR 的联动基于 BFD 对 LDP LSP 的检测实现。
- BFD 与 VPN FRR 的联动，需要在两个 PE 设备之间配置 BFD 多跳检测。

配置 BFD for OSPF

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd**，使能全局的 BFD 能力，并进入 BFD 视图。

步骤 3 执行命令 **quit**，返回系统视图。

步骤 4 执行命令 **ospf [process-id]**，进入 OSPF 视图。

步骤 5 执行命令 **bfd all-interfaces enable**，打开 OSPF BFD 特性的开关，建立 BFD 会话。

当配置了全局 BFD 特性，且邻居状态为 Full 时，OSPF 为该进程下所有满足上述条件的接口都建立默认的 BFD 参数值。如果需要阻止某些接口创建 BFD 会话，请在接口视图下执行命令 **ospf bfd block**。

如果需要配置 BFD 参数请执行 **bfd all-interfaces { min-rx-interval receive-interval | min-tx-interval transmit-interval | detect-multiplier multiplier-value } *命令**，指定需要建立 BFD 会话的各个参数值。

----结束

配置 BFD for BGP

在 BGP 对等体的两侧分别进行以下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd**，使能全局的 BFD 能力，并进入 BFD 视图。

步骤 3 执行命令 **quit**，返回系统视图。

步骤 4 执行命令 **bgp as-number**，进入 BGP 视图。

步骤 5 (可选) 执行命令 **peer { group-name | ipv4-address } bfd { min-tx-interval min-tx-interval | min-rx-interval min-rx-interval | detect-multiplier multiplier } *命令**，指定需要建立 BFD 会话的各个参数值。

步骤 6 执行命令 **peer { group-name | ipv4-address } bfd enable**，配置对等体或对等体组的 BFD 功能，建立 BFD 会话。

----结束

配置 BFD for LDP LSP

在被检测 LSP 的源端进行下列配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd**，使能全局的 BFD 能力，并进入 BFD 视图。

步骤 3 执行命令 **quit**，返回系统视图。

步骤 4 执行命令 **mpls**，进入 MPLS 视图。

步骤 5 执行命令 **mpls bfd enable**，使能 LDP LSP 动态创建 BFD 会话的能力。

步骤 6 执行命令 **mpls bfd-trigger [host [nexthop next-hop-address | outgoing-interface interface-type interface-number] * | fec-list list-name]**，配置动态 BFD 检测 LDP LSP 的触发策略。

----结束

在被检测 LSP 的目的端进行下列配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd**，使能全局的 BFD 能力，并进入 BFD 视图。

步骤 3 执行命令 **mpls-passive**，使能被动创建 BFD 会话功能。

----结束

配置 BFD for VPN FRR

在 VPN 的两端 PE（或 UPE）上分别进行如下配置。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **bfd**，使能全局的 BFD 能力，并进入 BFD 视图。

步骤 3 执行命令 **quit**，返回系统视图。

步骤 4 执行命令 **bfd cfg-name bind peer-ip peer-ip [vpn-instance vpn-instance-name] [source-ip source-ip]**，创建 BFD 会话。

peer-ip 是对端 PE（或 UPE）的 IP 地址。*source-ip* 是本端 PE（或 UPE）的 IP 地址。

步骤 5 执行命令 **discriminator local discr-value**，配置本地标识符。

步骤 6 执行命令 **discriminator remote discr-value**，配置远端标识符。

BFD 会话两端设备的本地标识符和远端标识符需要分别对应，本端的本地标识符与对端的远端标识符相同，否则会话无法正确建立。并且本地标识符和远端标识符配置成功后不可修改。

步骤 7 执行命令 **commit**，提交配置。

----结束

1.12 配置举例

组网需求

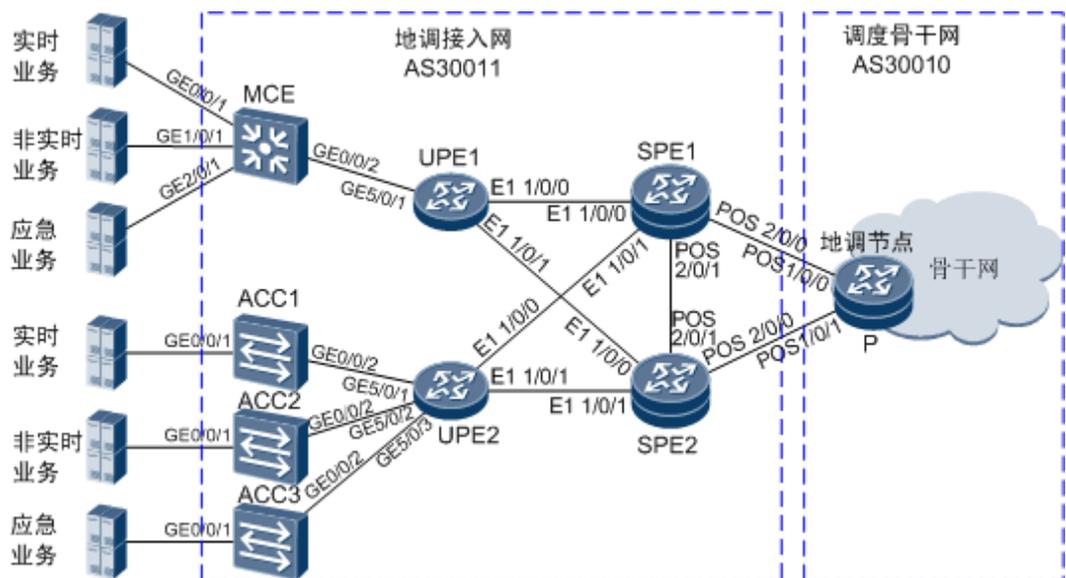
某地的地调接入网负责接入地区电力厂站，以覆盖所属县调、集控站以及 110KV（66KV）、35KV 变电站。

接入网采用接入和核心两层网络结构。接入网的核心路由器采用双节点，并上行连接骨干网中的地调节点，接入网的接入路由器向下连接各厂站内网。

厂站调度自动化业务服务器直接连接交换机，交换机作为 CE 接入到接入路由器，接入路由器根据业务的不同划分不同的 VLAN。在某些厂站，使用一台交换机接入多种业务。

接入路由器作为 PE，为不同业务构建不同的 VPN，包括实时 VPN、非实时 VPN 和应急 VPN。为了控制 VPN 路由数量，采用 HoPE 组网方案，其中接入路由器作为 UPE，核心路由器作为 SPE。

图1-4 地调接入网配置组网图



数据准备

表1-2 数据规划表

配置项	配置子项	数据
VLAN	MCE	实时业务下行 VLAN: 11
		实时业务上行 VLAN: 101
		非实时业务下行 VLAN: 12
	非实时业务上行 VLAN: 102	
	紧急业务下行 VLAN: 13	
	紧急业务上行 VLAN: 103	
	ACC1	实时业务 VLAN: 11
	ACC2	非实时业务 VLAN: 12
	ACC3	紧急业务 VLAN: 13

配置项	配置子项	数据
设备 IP 地址	MCE1	VLANIF 11: 192.11.1.1/24 VLANIF 12: 192.12.1.1/24 VLANIF 13: 192.13.1.1/24 VLANIF 101: 192.101.1.2/24 VLANIF 102: 192.102.1.2/24 VLANIF 103: 192.103.1.2/24
	UPE1	VLANIF 101: 192.101.1.1/24 VLANIF 102: 192.102.1.1/24 VLANIF 103: 192.103.1.1/24 E1 1/0/0: 11.100.1.2/24 E1 1/0/1: 11.100.2.2/24 LoopBack0: 11.3.3.3/32
	UPE2	VLANIF 11: 192.11.2.1/24 VLANIF 12: 192.11.2.1/24 VLANIF 13: 192.13.2.1/24 E1 1/0/0: 11.100.3.2/24 E1 1/0/1: 11.100.4.2/24 LoopBack0: 11.4.4.4/32
	SPE1	E1 1/0/0: 11.100.1.1/24 E1 1/0/1: 11.100.3.1/24 POS2/0/0: 100.1.1.2/24 POS2/0/1: 11.101.1.1/24 LoopBack0: 11.1.1.1/32
	SPE2	E1 1/0/0: 11.100.2.1/24 E1 1/0/1: 11.100.4.1/24 POS2/0/0: 100.1.2.2/24 POS2/0/1: 11.101.1.2/24 LoopBack0: 11.2.2.2/32
	P	POS1/0/0: 100.1.1.1/24 POS1/0/1: 100.1.2.1/24 LoopBack0: 10.1.1.1/32
	路由	接入网 AS
骨干网 AS		30010
RR		SPE1 和 SPE2 双反射 VPN 路由

配置项	配置子项	数据
VPN	实时业务 VPN	VPN 实例名: rt RD: 30011:11 VPN-Target (import) : 30011:11 VPN-Target (export) : 30011:11
	非实时业务 VPN	VPN 实例名: nrt RD: 30011:12 VPN-Target (import) : 30011:12 VPN-Target (export) : 30011:12
	紧急业务 VPN	VPN 实例名: eng RD: 30011:13 VPN-Target (import) : 30011:13 VPN-Target (export) : 30011:13
QoS	实时业务	服务等级: AF4 带宽: 60%
	非实时业务	服务等级: AF3 带宽: 30%
	紧急业务	服务等级: AF2 带宽: 10%

操作步骤

步骤 1 配置接口和 VLAN

配置 ACC1。

```
[ACC1] vlan-batch 11
[ACC1] interface GigabitEthernet 0/0/1
[ACC1-GigabitEthernet0/0/1] port link-type access
[ACC1-GigabitEthernet0/0/1] port default vlan 11
[ACC1-GigabitEthernet0/0/1] quit
[ACC1] interface GigabitEthernet 0/0/2
[ACC1-GigabitEthernet0/0/2] port link-type trunk
[ACC1-GigabitEthernet0/0/2] port trunk allow-pass vlan 11
[ACC1-GigabitEthernet0/0/2] quit
```

配置 ACC2。

```
[ACC2] vlan-batch 12
[ACC2] interface GigabitEthernet 0/0/1
[ACC2-GigabitEthernet0/0/1] port link-type access
[ACC2-GigabitEthernet0/0/1] port default vlan 12
[ACC2-GigabitEthernet0/0/1] quit
```

```
[ACC2] interface GigabitEthernet 0/0/2
[ACC2-GigabitEthernet0/0/2] port link-type trunk
[ACC2-GigabitEthernet0/0/2] port trunk allow-pass vlan 12
[ACC2-GigabitEthernet0/0/2] quit
```

配置 ACC3。

```
[ACC3] vlan-batch 13
[ACC3] interface GigabitEthernet 0/0/1
[ACC3-GigabitEthernet0/0/1] port link-type access
[ACC3-GigabitEthernet0/0/1] port default vlan 13
[ACC3-GigabitEthernet0/0/1] quit
[ACC3] interface GigabitEthernet 0/0/2
[ACC3-GigabitEthernet0/0/2] port link-type trunk
[ACC3-GigabitEthernet0/0/2] port trunk allow-pass vlan 13
[ACC3-GigabitEthernet0/0/2] quit
```

配置 MCE。

```
[MCE] vlan-batch 11 12 13 101 102 103
[MCE] interface GigabitEthernet 0/0/1
[MCE-GigabitEthernet0/0/1] port link-type access
[MCE-GigabitEthernet0/0/1] port default vlan 11
[MCE-GigabitEthernet0/0/1] quit
[MCE] interface GigabitEthernet 1/0/1
[MCE-GigabitEthernet1/0/1] port link-type access
[MCE-GigabitEthernet1/0/1] port default vlan 12
[MCE-GigabitEthernet1/0/1] quit
[MCE] interface GigabitEthernet 2/0/1
[MCE-GigabitEthernet2/0/1] port link-type access
[MCE-GigabitEthernet2/0/1] port default vlan 13
[MCE-GigabitEthernet2/0/1] quit
[MCE] interface GigabitEthernet 0/0/2
[MCE-GigabitEthernet0/0/2] port link-type trunk
[MCE-GigabitEthernet0/0/2] port trunk allow-pass vlan 101 102 103
[MCE-GigabitEthernet0/0/2] quit
```

说明

MCE 上的 VLANIF 接口为业务接口，其 IP 地址将在后续绑定 VPN 实例后配置。

配置 UPE1。

```
[UPE1] vlan-batch 101 102 103
[UPE1] interface GigabitEthernet 5/0/1
[UPE1-GigabitEthernet5/0/1] port link-type trunk
[UPE1-GigabitEthernet5/0/1] port trunk allow-pass vlan 101 102 103
[UPE1-GigabitEthernet5/0/1] quit
[UPE1] interface loopback 0
[UPE1-LoopBack0] ip address 11.3.3.3 255.255.255.255
[UPE1-LoopBack0] quit
[UPE1] controller e1 1/0/0
[UPE1-E1 1/0/0] using e1
[UPE1-E1 1/0/0] clock slave
[UPE1-E1 1/0/0] quit
[UPE1] interface Serial 1/0/0:0
[UPE1-Serial1/0/0:0] ip address 11.100.1.2 255.255.255.0
[UPE1-Serial1/0/0:0] quit
```

```
[UPE1] controller e1 1/0/1
[UPE1-E1 1/0/1] using e1
[UPE1-E1 1/0/1] clock slave
[UPE1-E1 1/0/1] quit
[UPE1] interface Serial 1/0/1:0
[UPE1-Serial1/0/1:0] ip address 11.100.2.2 255.255.255.0
[UPE1-Serial1/0/1:0] quit
```

 说明

UPE1 上的 VLANIF 接口为业务接口，其 IP 地址将在后续绑定 VPN 实例后配置。

配置 UPE2。

```
[UPE2] vlan-batch 11 12 13
[UPE2] interface GigabitEthernet 5/0/1
[UPE2-GigabitEthernet5/0/1] port link-type trunk
[UPE2-GigabitEthernet5/0/1] port trunk allow-pass vlan 11
[UPE2-GigabitEthernet5/0/1] quit
[UPE2] interface GigabitEthernet 5/0/2
[UPE2-GigabitEthernet5/0/2] port link-type trunk
[UPE2-GigabitEthernet5/0/2] port trunk allow-pass vlan 12
[UPE2-GigabitEthernet5/0/2] quit
[UPE2] interface GigabitEthernet 5/0/3
[UPE2-GigabitEthernet5/0/3] port link-type trunk
[UPE2-GigabitEthernet5/0/3] port trunk allow-pass vlan 13
[UPE2-GigabitEthernet5/0/3] quit
[UPE2] interface loopback 0
[UPE2-LoopBack0] ip address 11.4.4.4 255.255.255.255
[UPE2-LoopBack0] quit
[UPE2] controller e1 1/0/0
[UPE2-E1 1/0/0] using e1
[UPE2-E1 1/0/0] clock slave
[UPE2-E1 1/0/0] quit
[UPE2] interface Serial 1/0/0:0
[UPE2-Serial1/0/0:0] ip address 11.100.3.2 255.255.255.0
[UPE2-Serial1/0/0:0] quit
[UPE2] controller e1 1/0/1
[UPE2-E1 1/0/1] using e1
[UPE2-E1 1/0/1] clock slave
[UPE2-E1 1/0/1] quit
[UPE2] interface Serial 1/0/1:0
[UPE2-Serial1/0/1:0] ip address 11.100.4.2 255.255.255.0
[UPE2-Serial1/0/1:0] quit
```

 说明

UPE2 上的 VLANIF 接口为业务接口，其 IP 地址将在后续绑定 VPN 实例后配置。

配置 SPE1。

```
[SPE1] interface loopback 0
[SPE1-LoopBack0] ip address 11.1.1.1 255.255.255.255
[SPE1-LoopBack0] quit
[SPE1] controller e1 1/0/0
[SPE1-E1 1/0/0] using e1
[SPE1-E1 1/0/0] clock master
[SPE1-E1 1/0/0] quit
[SPE1] interface Serial 1/0/0:0
```

```
[SPE1-Serial1/0/0:0] ip address 11.100.1.1 255.255.255.0
[SPE1-Serial1/0/0:0] quit
[SPE1] controller e1 1/0/1
[SPE1-E1 1/0/1] using e1
[SPE1-E1 1/0/1] clock master
[SPE1-E1 1/0/1] quit
[SPE1] interface Serial 1/0/1:0
[SPE1-Serial1/0/1:0] ip address 11.100.3.1 255.255.255.0
[SPE1-Serial1/0/1:0] quit
[SPE1] interface pos 2/0/0
[SPE1-Pos2/0/0] link-protocol ppp
[SPE1-Pos2/0/0] ip address 100.1.1.2 255.255.255.0
[SPE1-Pos2/0/0] quit
[SPE1] interface pos 2/0/1
[SPE1-Pos2/0/1] link-protocol ppp
[SPE1-Pos2/0/1] ip address 11.101.1.1 255.255.255.0
[SPE1-Pos2/0/1] quit
```

配置 SPE2。

```
[SPE2] interface loopback 0
[SPE2-LoopBack0] ip address 11.2.2.2 255.255.255.255
[SPE2-LoopBack0] quit
[SPE2] controller e1 1/0/0
[SPE2-E1 1/0/0] using e1
[SPE2-E1 1/0/0] clock master
[SPE2-E1 1/0/0] quit
[SPE2] interface Serial 1/0/0:0
[SPE2-Serial1/0/0:0] ip address 11.100.2.1 255.255.255.0
[SPE2-Serial1/0/0:0] quit
[SPE2] controller e1 1/0/1
[SPE2-E1 1/0/1] using e1
[SPE2-E1 1/0/1] clock master
[SPE2-E1 1/0/1] quit
[SPE2] interface Serial 1/0/1:0
[SPE2-Serial1/0/1:0] ip address 11.100.4.1 255.255.255.0
[SPE2-Serial1/0/1:0] quit
[SPE2] interface pos 2/0/0
[SPE2-Pos2/0/0] link-protocol ppp
[SPE2-Pos2/0/0] ip address 100.1.2.2 255.255.255.0
[SPE2-Pos2/0/0] quit
[SPE2] interface pos 2/0/1
[SPE2-Pos2/0/1] link-protocol ppp
[SPE2-Pos2/0/1] ip address 11.101.1.2 255.255.255.0
[SPE2-Pos2/0/1] quit
```

配置 P。

```
[P] interface loopback 0
[P-LoopBack0] ip address 10.1.1.1 255.255.255.255
[P-LoopBack0] quit
[P] interface pos 1/0/0
[P-Pos1/0/0] link-protocol ppp
[P-Pos1/0/0] ip address 100.1.1.1 255.255.255.0
[P-Pos1/0/0] quit
[P] interface pos 1/0/1
[P-Pos1/0/1] link-protocol ppp
```

```
[P-Pos1/0/1] ip address 100.1.2.1 255.255.255.0  
[P-Pos1/0/1] quit
```

步骤 2 配置 IGP

UPE1 配置 OSPF。

```
[UPE1] router id 11.3.3.3  
[UPE1] ospf 1  
[UPE1-ospf-1] area 1  
[UPE1-ospf-1-area-0.0.0.1] network 11.100.1.2 0.0.0.255  
[UPE1-ospf-1-area-0.0.0.1] network 11.100.2.2 0.0.0.255  
[UPE1-ospf-1-area-0.0.0.1] network 11.3.3.3 0.0.0.0  
[UPE1-ospf-1-area-0.0.0.1] quit  
[UPE1-ospf-1] quit
```

UPE2 配置 OSPF。

```
[UPE2] router id 11.4.4.4  
[UPE2] ospf 1  
[UPE2-ospf-1] area 2  
[UPE2-ospf-1-area-0.0.0.2] network 11.100.3.2 0.0.0.255  
[UPE2-ospf-1-area-0.0.0.2] network 11.100.4.2 0.0.0.255  
[UPE2-ospf-1-area-0.0.0.2] network 11.3.3.3 0.0.0.0  
[UPE2-ospf-1-area-0.0.0.2] quit  
[UPE2-ospf-1] quit
```

SPE1 配置 OSPF。

```
[SPE1] router id 11.1.1.1  
[SPE1] ospf 1  
[SPE1] import-route static cost 1000 type 1  
[SPE1] asbr-summary 11.0.0.0 255.0.0.0  
[SPE1-ospf-1] area 0  
[SPE1-ospf-1-area-0.0.0.0] network 11.101.1.1 0.0.0.255  
[SPE1-ospf-1-area-0.0.0.0] network 11.1.1.1 0.0.0.0  
[SPE1-ospf-1-area-0.0.0.0] quit  
[SPE1-ospf-1] area 1  
[SPE1-ospf-1-area-0.0.0.1] network 11.100.1.1 0.0.0.255  
[SPE1-ospf-1-area-0.0.0.1] quit  
[SPE1-ospf-1] area 2  
[SPE1-ospf-1-area-0.0.0.2] network 11.100.3.1 0.0.0.255  
[SPE1-ospf-1-area-0.0.0.2] quit  
[SPE1-ospf-1] quit
```

SPE2 配置 OSPF。

```
[SPE2] router id 11.2.2.2  
[SPE2] ospf 1  
[SPE2] import-route static cost 1000 type 1  
[SPE2] asbr-summary 11.0.0.0 255.0.0.0  
[SPE2-ospf-1] area 0  
[SPE2-ospf-1-area-0.0.0.0] network 11.101.1.2 0.0.0.255  
[SPE2-ospf-1-area-0.0.0.0] network 11.2.2.2 0.0.0.0  
[SPE2-ospf-1-area-0.0.0.0] quit  
[SPE2-ospf-1] area 1  
[SPE2-ospf-1-area-0.0.0.1] network 11.100.2.1 0.0.0.255  
[SPE2-ospf-1-area-0.0.0.1] quit
```

```
[SPE2-ospf-1] area 2
[SPE2-ospf-1-area-0.0.0.2] network 11.100.4.1 0.0.0.255
[SPE2-ospf-1-area-0.0.0.2] quit
[SPE2-ospf-1] quit

# 配置 SPE1 的跨域公网静态路由。

[SPE1] ip route-static 10.0.0.0 255.0.0.0 pos 2/0/0 100.1.1.1

# 配置 SPE2 的跨域公网静态路由。

[SPE2] ip route-static 10.0.0.0 255.0.0.0 pos 2/0/0 100.1.2.1

# 配置 P 的跨域公网静态路由。

[P] ip route-static 11.0.0.0 255.0.0.0 pos 1/0/0 100.1.1.2 preference 60
[P] ip route-static 11.0.0.0 255.0.0.0 pos 1/0/1 100.1.2.2 preference 100
```

 说明

P 所在 AS 的 IGP 配置，本处省略。

步骤 3 使能 MPLS 基本能力

使能 UPE1 的 MPLS 基本能力。

```
[UPE1] mpls lsr-id 11.3.3.3
[UPE1] mpls
[UPE1-mppls] quit
[UPE1] mpls ldp
[UPE1-mppls-ldp] quit
[UPE1] interface serial 1/0/0:0
[UPE1-Serial1/0/0:0] mpls
[UPE1-Serial1/0/0:0] mpls ldp
[UPE1-Serial1/0/0:0] quit
[UPE1] interface serial 1/0/1:0
[UPE1-Serial1/0/1:0] mpls
[UPE1-Serial1/0/1:0] mpls ldp
[UPE1-Serial1/0/1:0] quit
```

使能 UPE2 的 MPLS 基本能力。

```
[UPE2] mpls lsr-id 11.4.4.4
[UPE2] mpls
[UPE2-mppls] quit
[UPE2] mpls ldp
[UPE2-mppls-ldp] quit
[UPE2] interface serial 1/0/0:0
[UPE2-Serial1/0/0:0] mpls
[UPE2-Serial1/0/0:0] mpls ldp
[UPE2-Serial1/0/0:0] quit
[UPE2] interface serial 1/0/1:0
[UPE2-Serial1/0/1:0] mpls
[UPE2-Serial1/0/1:0] mpls ldp
[UPE2-Serial1/0/1:0] quit
```

使能 SPE1 的 MPLS 基本能力。

```
[SPE1] mpls lsr-id 11.1.1.1
[SPE1] mpls
```

```
[SPE1-mpls] quit
[SPE1] mpls ldp
[SPE1-mpls-ldp] quit
[SPE1] interface serial 1/0/0:0
[SPE1-Serial1/0/0:0] mpls
[SPE1-Serial1/0/0:0] mpls ldp
[SPE1-Serial1/0/0:0] quit
[SPE1] interface serial 1/0/1:0
[SPE1-Serial1/0/1:0] mpls
[SPE1-Serial1/0/1:0] mpls ldp
[SPE1-Serial1/0/1:0] quit
[SPE1] interface pos 2/0/0
[SPE1-Pos2/0/0] mpls
[SPE1-Pos2/0/0] mpls ldp
[SPE1-Pos2/0/0] quit
[SPE1] interface pos 2/0/1
[SPE1-Pos2/0/1] mpls
[SPE1-Pos2/0/1] mpls ldp
[SPE1-Pos2/0/1] quit
```

使能 SPE2 的 MPLS 基本能力。

```
[SPE2] mpls lsr-id 11.2.2.2
[SPE2] mpls
[SPE2-mpls] quit
[SPE2] mpls ldp
[SPE2-mpls-ldp] quit
[SPE2] interface serial 1/0/0:0
[SPE2-Serial1/0/0:0] mpls
[SPE2-Serial1/0/0:0] mpls ldp
[SPE2-Serial1/0/0:0] quit
[SPE2] interface serial 1/0/1:0
[SPE2-Serial1/0/1:0] mpls
[SPE2-Serial1/0/1:0] mpls ldp
[SPE2-Serial1/0/1:0] quit
[SPE2] interface pos 2/0/0
[SPE2-Pos2/0/0] mpls
[SPE2-Pos2/0/0] mpls ldp
[SPE2-Pos2/0/0] quit
[SPE2] interface pos 2/0/1
[SPE2-Pos2/0/1] mpls
[SPE2-Pos2/0/1] mpls ldp
[SPE2-Pos2/0/1] quit
```

使能 P 的 MPLS 基本能力。

```
[P] mpls lsr-id 10.1.1.1
[P] mpls
[P-mpls] quit
[P] mpls ldp
[P-mpls-ldp] quit
[P] interface pos 1/0/0
[P-Pos1/0/0] mpls
[P-Pos1/0/0] mpls ldp
[P-Pos1/0/0] quit
[P] interface pos 1/0/1
[P-Pos1/0/1] mpls
```

```
[P-Pos1/0/1] mpls ldp
[P-Pos1/0/1] quit
```

步骤 4 配置基本 MPLS L3VPN

UPE1 上配置 VPN 实例。

```
[UPE1] ip vpn-instance rt
[UPE1-vpn-instance-rt] route-distinguisher 30011:11
[UPE1-vpn-instance-rt-af-ipv4] vpn-target 30011:11 both
[UPE1-vpn-instance-rt-af-ipv4] quit
[UPE1-vpn-instance-rt] quit
[UPE1] ip vpn-instance nrt
[UPE1-vpn-instance-nrt] route-distinguisher 30011:12
[UPE1-vpn-instance-nrt-af-ipv4] vpn-target 30011:12 both
[UPE1-vpn-instance-nrt-af-ipv4] quit
[UPE1-vpn-instance-nrt] quit
[UPE1] ip vpn-instance eng
[UPE1-vpn-instance-eng] route-distinguisher 30011:13
[UPE1-vpn-instance-eng-af-ipv4] vpn-target 30011:13 both
[UPE1-vpn-instance-eng-af-ipv4] quit
[UPE1-vpn-instance-eng] quit
```

UPE1 上将 VPN 实例绑定到接口。

```
[UPE1] interface vlanif 101
[UPE1-Vlanif101] ip binding vpn-instance rt
[UPE1-Vlanif101] ip address 192.101.1.1 255.255.255.0
[UPE1-Vlanif101] quit
[UPE1] interface vlanif 102
[UPE1-Vlanif102] ip binding vpn-instance nrt
[UPE1-Vlanif102] ip address 192.102.1.1 255.255.255.0
[UPE1-Vlanif102] quit
[UPE1] interface vlanif 103
[UPE1-Vlanif103] ip binding vpn-instance eng
[UPE1-Vlanif103] ip address 192.103.1.1 255.255.255.0
[UPE1-Vlanif103] quit
```

配置 UPE1 和 MCE 之间的路由交互。

```
[UPE1] bgp 30011
[UPE1-bgp] ipv4-family vpn-instance rt
[UPE1-bgp-rt] peer 192.101.1.2 as-number 30011
[UPE1-bgp-rt] import-route direct
[UPE1-bgp-rt] quit
[UPE1-bgp] ipv4-family vpn-instance nrt
[UPE1-bgp-nrt] peer 192.102.1.2 as-number 30011
[UPE1-bgp-nrt] import-route direct
[UPE1-bgp-nrt] quit
[UPE1-bgp] ipv4-family vpn-instance eng
[UPE1-bgp-eng] peer 192.103.1.2 as-number 30011
[UPE1-bgp-eng] import-route direct
[UPE1-bgp-eng] quit
```

配置 MCE 的 VPN 实例。

```
[MCE] ip vpn-instance rt
[MCE-vpn-instance-rt] route-distinguisher 30011:11
```

```
[MCE-vpn-instance-rt] vpn-target 30011:11 export-extcommunity
[MCE-vpn-instance-rt] vpn-target 30011:11 import-extcommunity
[MCE-vpn-instance-rt] quit
[MCE] ip vpn-instance nrt
[MCE-vpn-instance-nrt] route-distinguisher 30011:12
[MCE-vpn-instance-nrt] vpn-target 30011:12 export-extcommunity
[MCE-vpn-instance-nrt] vpn-target 30011:12 import-extcommunity
[MCE-vpn-instance-nrt] quit
[MCE] ip vpn-instance eng
[MCE-vpn-instance-eng] route-distinguisher 30011:13
[MCE-vpn-instance-eng] vpn-target 30011:13 export-extcommunity
[MCE-vpn-instance-eng] vpn-target 30011:13 import-extcommunity
[MCE-vpn-instance-eng] quit
```

MCE 上将 VPN 实例绑定到接口。

```
[MCE] interface vlanif 11
[MCE-Vlanif11] ip binding vpn-instance rt
[MCE-Vlanif11] ip address 192.11.1.1 255.255.255.0
[MCE-Vlanif11] quit
[MCE] interface vlanif 12
[MCE-Vlanif12] ip binding vpn-instance nrt
[MCE-Vlanif12] ip address 192.12.1.1 255.255.255.0
[MCE-Vlanif12] quit
[MCE] interface vlanif 13
[MCE-Vlanif13] ip binding vpn-instance eng
[MCE-Vlanif13] ip address 192.13.1.1 255.255.255.0
[MCE-Vlanif13] quit
[MCE] interface vlanif 101
[MCE-Vlanif101] ip binding vpn-instance rt
[MCE-Vlanif101] ip address 192.101.1.2 255.255.255.0
[MCE-Vlanif101] quit
[MCE] interface vlanif 102
[MCE-Vlanif102] ip binding vpn-instance nrt
[MCE-Vlanif102] ip address 192.102.1.2 255.255.255.0
[MCE-Vlanif102] quit
[MCE] interface vlanif 103
[MCE-Vlanif103] ip binding vpn-instance eng
[MCE-Vlanif103] ip address 192.103.1.2 255.255.255.0
[MCE-Vlanif103] quit
```

配置 MCE 和 UPE1 之间的路由交互。

```
[MCE] bgp 30011
[MCE-bgp] ipv4-family vpn-instance rt
[MCE-bgp-rt] peer 192.101.1.1 as-number 30011
[MCE-bgp-rt] import-route direct
[MCE-bgp-rt] quit
[MCE-bgp] ipv4-family vpn-instance nrt
[MCE-bgp-nrt] peer 192.102.1.1 as-number 30011
[MCE-bgp-nrt] import-route direct
[MCE-bgp-nrt] quit
[MCE-bgp] ipv4-family vpn-instance eng
[MCE-bgp-eng] peer 192.103.1.1 as-number 30011
[MCE-bgp-eng] import-route direct
[MCE-bgp-eng] quit
```

UPE2 上配置 VPN 实例。

```
[UPE2] ip vpn-instance rt
[UPE2-vpn-instance-rt] route-distinguisher 30011:11
[UPE2-vpn-instance-rt-af-ipv4] vpn-target 30011:11 both
[UPE2-vpn-instance-rt-af-ipv4] quit
[UPE2-vpn-instance-rt] quit
[UPE2] ip vpn-instance nrt
[UPE2-vpn-instance-nrt] route-distinguisher 30011:12
[UPE2-vpn-instance-nrt-af-ipv4] vpn-target 30011:12 both
[UPE2-vpn-instance-nrt-af-ipv4] quit
[UPE2-vpn-instance-nrt] quit
[UPE2] ip vpn-instance eng
[UPE2-vpn-instance-eng] route-distinguisher 30011:13
[UPE2-vpn-instance-eng-af-ipv4] vpn-target 30011:13 both
[UPE2-vpn-instance-eng-af-ipv4] quit
[UPE2-vpn-instance-eng] quit
```

UPE2 上将 VPN 实例绑定到接口。

```
[UPE2] interface vlanif 11
[UPE2-Vlanif11] ip binding vpn-instance rt
[UPE2-Vlanif11] ip address 192.11.2.1 24
[UPE2-Vlanif11] quit
[UPE2] interface vlanif 12
[UPE2-Vlanif12] ip binding vpn-instance nrt
[UPE2-Vlanif12] ip address 192.12.2.1 24
[UPE2-Vlanif12] quit
[UPE2] interface vlanif 13
[UPE2-Vlanif13] ip binding vpn-instance eng
[UPE2-Vlanif13] ip address 192.13.2.1 24
[UPE2-Vlanif13] quit
```

步骤 5 配置 HoVPN

配置 UPE1 上的 MP-IBGP 对等体。

```
[UPE1] bgp 30011
[UPE1-bgp] peer 11.1.1.1 as-number 30011
[UPE1-bgp] peer 11.1.1.1 connect-interface loopback 0
[UPE1-bgp] peer 11.2.2.2 as-number 30011
[UPE1-bgp] peer 11.2.2.2 connect-interface loopback 0
[UPE1-bgp] ipv4-family vpnv4
[UPE1-bgp-af-vpnv4] peer 11.1.1.1 enable
[UPE1-bgp-af-vpnv4] peer 11.2.2.2 enable
[UPE1-bgp-af-vpnv4] quit
```

配置 UPE2 上的 MP-IBGP 对等体。

```
[UPE2] bgp 30011
[UPE2-bgp] peer 11.1.1.1 as-number 30011
[UPE2-bgp] peer 11.1.1.1 connect-interface loopback 0
[UPE2-bgp] peer 11.2.2.2 as-number 30011
[UPE2-bgp] peer 11.2.2.2 connect-interface loopback 0
[UPE2-bgp] ipv4-family vpnv4
[UPE2-bgp-af-vpnv4] peer 11.1.1.1 enable
[UPE2-bgp-af-vpnv4] peer 11.2.2.2 enable
```

```
[UPE2-bgp-af-vpn4] quit

# 配置 SPE1 上的 MP-IBGP 对等体。

[SPE1] bgp 30011
[SPE1-bgp] peer 11.2.2.2 as-number 30011
[SPE1-bgp] peer 11.2.2.2 connect-interface loopback 0
[SPE1-bgp] peer 11.3.3.3 as-number 30011
[SPE1-bgp] peer 11.3.3.3 connect-interface loopback 0
[SPE1-bgp] peer 11.4.4.4 as-number 30011
[SPE1-bgp] peer 11.4.4.4 connect-interface loopback 0
[SPE1-bgp] ipv4-family vpnv4
[SPE1-bgp-af-vpn4] peer 11.2.2.2 enable
[SPE1-bgp-af-vpn4] peer 11.2.2.2 reflect-client
[SPE1-bgp-af-vpn4] peer 11.3.3.3 enable
[SPE1-bgp-af-vpn4] peer 11.3.3.3 reflect-client
[SPE1-bgp-af-vpn4] peer 11.4.4.4 enable
[SPE1-bgp-af-vpn4] peer 11.4.4.4 reflect-client
[SPE1-bgp-af-vpn4] quit

# 配置 SPE2 上的 MP-IBGP 对等体。

[SPE2] bgp 30011
[SPE2-bgp] peer 11.1.1.1 as-number 30011
[SPE2-bgp] peer 11.1.1.1 connect-interface loopback 0
[SPE2-bgp] peer 11.3.3.3 as-number 30011
[SPE2-bgp] peer 11.3.3.3 connect-interface loopback 0
[SPE2-bgp] peer 11.4.4.4 as-number 30011
[SPE2-bgp] peer 11.4.4.4 connect-interface loopback 0
[SPE2-bgp] ipv4-family vpnv4
[SPE2-bgp-af-vpn4] peer 11.1.1.1 enable
[SPE2-bgp-af-vpn4] peer 11.1.1.1 reflect-client
[SPE2-bgp-af-vpn4] peer 11.3.3.3 enable
[SPE2-bgp-af-vpn4] peer 11.3.3.3 reflect-client
[SPE2-bgp-af-vpn4] peer 11.4.4.4 enable
[SPE2-bgp-af-vpn4] peer 11.4.4.4 reflect-client
[SPE2-bgp-af-vpn4] quit

# 配置 SPE1 的 VPN 实例。

[SPE1] ip vpn-instance rt
[SPE1-vpn-instance-rt] route-distinguisher 30011:11
[SPE1-vpn-instance-rt-af-ipv4] vpn-target 30011:11 both
[SPE1-vpn-instance-rt-af-ipv4] quit
[SPE1-vpn-instance-rt] quit
[SPE1] ip vpn-instance nrt
[SPE1-vpn-instance-nrt] route-distinguisher 30011:12
[SPE1-vpn-instance-nrt-af-ipv4] vpn-target 30011:12 both
[SPE1-vpn-instance-nrt-af-ipv4] quit
[SPE1-vpn-instance-nrt] quit
[SPE1] ip vpn-instance eng
[SPE1-vpn-instance-eng] route-distinguisher 30011:13
[SPE1-vpn-instance-eng-af-ipv4] vpn-target 30011:13 both
[SPE1-vpn-instance-eng-af-ipv4] quit
[SPE1-vpn-instance-eng] quit

# 配置 SPE2 的 VPN 实例。
```

```
[SPE2] ip vpn-instance rt
[SPE2-vpn-instance-rt] route-distinguisher 30011:11
[SPE2-vpn-instance-rt-af-ipv4] vpn-target 30011:11 both
[SPE2-vpn-instance-rt-af-ipv4] quit
[SPE2-vpn-instance-rt] quit
[SPE2] ip vpn-instance nrt
[SPE2-vpn-instance-nrt] route-distinguisher 30011:12
[SPE2-vpn-instance-nrt-af-ipv4] vpn-target 30011:12 both
[SPE2-vpn-instance-nrt-af-ipv4] quit
[SPE2-vpn-instance-nrt] quit
[SPE2] ip vpn-instance eng
[SPE2-vpn-instance-eng] route-distinguisher 30011:13
[SPE2-vpn-instance-eng-af-ipv4] vpn-target 30011:13 both
[SPE2-vpn-instance-eng-af-ipv4] quit
[SPE2-vpn-instance-eng] quit
```

在 SPE1 上指定 UPE 并发布 VPN 缺省路由。

```
[SPE1] bgp 30011
[SPE1-bgp] ipv4-family vpnv4
[SPE1-bgp-af-vpnv4] peer 11.3.3.3 upe
[SPE1-bgp-af-vpnv4] peer 11.3.3.3 default-originate vpn-instance rt
[SPE1-bgp-af-vpnv4] peer 11.3.3.3 default-originate vpn-instance nrt
[SPE1-bgp-af-vpnv4] peer 11.3.3.3 default-originate vpn-instance eng
[SPE1-bgp-af-vpnv4] peer 11.4.4.4 upe
[SPE1-bgp-af-vpnv4] peer 11.4.4.4 default-originate vpn-instance rt
[SPE1-bgp-af-vpnv4] peer 11.4.4.4 default-originate vpn-instance nrt
[SPE1-bgp-af-vpnv4] peer 11.4.4.4 default-originate vpn-instance eng
[SPE1-bgp-af-vpnv4] quit
```

在 SPE2 上指定 UPE 并发布 VPN 缺省路由。

```
[SPE2] bgp 30011
[SPE2-bgp] ipv4-family vpnv4
[SPE2-bgp-af-vpnv4] peer 11.3.3.3 upe
[SPE2-bgp-af-vpnv4] peer 11.3.3.3 default-originate vpn-instance rt
[SPE2-bgp-af-vpnv4] peer 11.3.3.3 default-originate vpn-instance nrt
[SPE2-bgp-af-vpnv4] peer 11.3.3.3 default-originate vpn-instance eng
[SPE2-bgp-af-vpnv4] peer 11.4.4.4 upe
[SPE2-bgp-af-vpnv4] peer 11.4.4.4 default-originate vpn-instance rt
[SPE2-bgp-af-vpnv4] peer 11.4.4.4 default-originate vpn-instance nrt
[SPE2-bgp-af-vpnv4] peer 11.4.4.4 default-originate vpn-instance eng
[SPE2-bgp-af-vpnv4] quit
```

步骤 6 配置跨域 VPN-OptionB 方式

说明

骨干网接入 VPN Site（例如地区调度中心的数据中心）的 PE（组网图中未列出）上，需要进行 L3VPN 的配置，此处省略。

配置 SPE1（AS 30011 的 ASBR）上 MP-EBGP 对等体。

```
[SPE1] bgp 30011
[SPE1-bgp] peer 10.1.1.1 as-number 30010
[SPE1-bgp] peer 10.1.1.1 connect-interface loopback 0
[SPE1-bgp] ipv4-family vpnv4
[SPE1-bgp-af-vpnv4] peer 10.1.1.1 enable
```

```
[SPE1-bgp-af-vpn4] quit

# 配置 SPE2（AS 30011 的 ASBR）上的 MP-EBGP 对等体。

[SPE2] bgp 30011
[SPE2-bgp] peer 10.1.1.1 as-number 30010
[SPE2-bgp] peer 10.1.1.1 connect-interface loopback 0
[SPE2-bgp] ipv4-family vpnv4
[SPE2-bgp-af-vpn4] peer 10.1.1.1 enable
[SPE2-bgp-af-vpn4] quit

# 配置 P（AS 30010 的 ASBR）上的 MP-EBGP 对等体。

[P] bgp 30010
[P-bgp] peer 11.1.1.1 as-number 30011
[P-bgp] peer 11.1.1.1 connect-interface loopback 0
[P-bgp] peer 11.2.2.2 as-number 30011
[P-bgp] peer 11.2.2.2 connect-interface loopback 0
[P-bgp] ipv4-family vpnv4
[P-bgp-af-vpn4] peer 11.1.1.1 enable
[P-bgp-af-vpn4] peer 11.2.2.2 enable
[P-bgp-af-vpn4] quit

# 配置 SPE1 上的路由过滤。

[SPE1] ip as-path-filter 10 permit ^$
[SPE1] route-policy as30011_export_to_as30010 permit node 10
[SPE1-route-policy] if-match as-path-filter 10
[SPE1-route-policy] quit
[SPE1] bgp 30011
[SPE1-bgp] ipv4-family vpnv4
[SPE1-bgp-af-vpn4] peer 10.1.1.1 route-policy as30011_export_to_as30010 export

# 配置 SPE2 上的路由过滤。

[SPE2] ip as-path-filter 10 permit ^$
[SPE2] route-policy as30011_export_to_as30010 permit node 10
[SPE2-route-policy] if-match as-path-filter 10
[SPE2-route-policy] quit
[SPE2] bgp 30011
[SPE2-bgp] ipv4-family vpnv4
[SPE2-bgp-af-vpn4] peer 10.1.1.1 route-policy as30011_export_to_as30010 export

# 配置 P 上的路由过滤。

[P] ip as-path-filter 10 permit ^30011$
[P] ip as-path-filter 20 permit ^30010$
[P] route-policy as30010_import_from_as30011 permit node 10
[P-route-policy] if-match as-path-filter 10
[P-route-policy] quit
[P] route-policy as30010_export_to_as30011 permit node 10
[P-route-policy] if-match as-path-filter 20
[P-route-policy] apply community no-export
[P-route-policy] quit
[P] bgp 30010
[P-bgp] ipv4-family vpnv4
[P-bgp-af-vpn4] peer 11.1.1.1 route-policy as30010_import_from_as30011 import
[P-bgp-af-vpn4] peer 11.2.2.2 route-policy as30010_import_from_as30011 import
```

```
[P-bgp-af-vpnv4]peer 11.1.1.1 route-policy as30010_export_to_as30011 export
[P-bgp-af-vpnv4]peer 11.2.2.2 route-policy as30010_export_to_as30011 export
[P-bgp-af-vpnv4] quit
```

步骤7 配置 QoS

在 UPE1 上配置优先级标记。

```
[UPE1] acl 3000
[UPE1-acl-adv-3000] rule permit ip vpn-instance rt
[UPE1-acl-adv-3000] quit
[UPE1] acl 3001
[UPE1-acl-adv-3001] rule permit ip vpn-instance nrt
[UPE1-acl-adv-3001] quit
[UPE1] acl 3002
[UPE1-acl-adv-3002] rule permit ip vpn-instance eng
[UPE1-acl-adv-3002] quit
[UPE1] traffic classifier rt
[UPE1-classifier-rt] if-match acl 3000
[UPE1-classifier-rt] quit
[UPE1] traffic classifier nrt
[UPE1-classifier-nrt] if-match acl 3001
[UPE1-classifier-nrt] quit
[UPE1] traffic classifier eng
[UPE1-classifier-eng] if-match acl 3002
[UPE1-classifier-eng] quit
[UPE1] traffic behavior rt
[UPE1-behavior-rt] remark dscp af41
[UPE1-behavior-rt] quit
[UPE1] traffic behavior nrt
[UPE1-behavior-nrt] remark dscp af31
[UPE1-behavior-nrt] quit
[UPE1] traffic behavior eng
[UPE1-behavior-eng] remark dscp af21
[UPE1-behavior-eng] quit
[UPE1] traffic policy vpn
[UPE1-trafficpolicy-vpn] classifier rt behavior rt
[UPE1-trafficpolicy-vpn] classifier nrt behavior nrt
[UPE1-trafficpolicy-vpn] classifier eng behavior eng
[UPE1-trafficpolicy-vpn] quit
[UPE1] interface GigabitEthernet 5/0/1
[UPE1-GigabitEthernet5/0/1] traffic-policy vpn inbound
[UPE1-GigabitEthernet5/0/1] quit
```

在 UPE2 上配置优先级标记。

```
[UPE2] traffic classifier rt
[UPE2-classifier-rt] if-match any
[UPE2-classifier-rt] quit
[UPE2] traffic behavior rt
[UPE2-behavior-rt] remark dscp af41
[UPE2-behavior-rt] quit
[UPE2] traffic policy rt
[UPE2-trafficpolicy-rt] classifier rt behavior rt
[UPE2-trafficpolicy-rt] quit
[UPE2] interface GigabitEthernet 5/0/1
[UPE2-GigabitEthernet5/0/1] traffic-policy rt inbound
```

```
[UPE2-GigabitEthernet5/0/1] quit
[UPE2] traffic classifier nrt
[UPE2-classifier-nrt] if-match any
[UPE2-classifier-nrt] quit
[UPE2] traffic behavior nrt
[UPE2-behavior-nrt] remark dscp af31
[UPE2-behavior-nrt] quit
[UPE2] traffic policy nrt
[UPE2-trafficpolicy-nrt] classifier nrt behavior nrt
[UPE2-trafficpolicy-nrt] quit
[UPE2] interface GigabitEthernet 5/0/2
[UPE2-GigabitEthernet5/0/2] traffic-policy nrt inbound
[UPE2-GigabitEthernet5/0/2] quit
[UPE2] traffic classifier eng
[UPE2-classifier-eng] if-match any
[UPE2-classifier-eng] quit
[UPE2] traffic behavior eng
[UPE2-behavior-eng] remark dscp af21
[UPE2-behavior-eng] quit
[UPE2] traffic policy eng
[UPE2-trafficpolicy-eng] classifier eng behavior eng
[UPE2-trafficpolicy-eng] quit
[UPE2] interface GigabitEthernet 5/0/3
[UPE2-GigabitEthernet5/0/3] traffic-policy eng inbound
[UPE2-GigabitEthernet5/0/3] quit
```

配置 UPE1 的优先级队列调度。

```
[UPE1] interface GigabitEthernet 5/0/1
[UPE1-GigabitEthernet5/0/1] trust upstream default
[UPE1-GigabitEthernet5/0/1] port-queue af4 wfq weight 60 outbound
[UPE1-GigabitEthernet5/0/1] port-queue af3 wfq weight 30 outbound
[UPE1-GigabitEthernet5/0/1] port-queue af2 wfq weight 10 outbound
[UPE1-GigabitEthernet5/0/1] quit
[UPE1] interface serial 1/0/0:0
[UPE1-Serial1/0/0:0] trust upstream default
[UPE1-Serial1/0/0:0] port-queue af4 wfq shaping cir percentage 60 pir percentage 61
[UPE1-Serial1/0/0:0] port-queue af3 wfq shaping cir percentage 30 pir percentage 31
[UPE1-Serial1/0/0:0] port-queue af2 wfq shaping cir percentage 10 pir percentage 11
[UPE1-Serial1/0/0:0] quit
[UPE1] interface serial 1/0/1:0
[UPE1-Serial1/0/1:0] trust upstream default
[UPE1-Serial1/0/1:0] port-queue af4 wfq shaping cir percentage 60 pir percentage 61
[UPE1-Serial1/0/1:0] port-queue af3 wfq shaping cir percentage 30 pir percentage 31
[UPE1-Serial1/0/1:0] port-queue af2 wfq shaping cir percentage 10 pir percentage 11
[UPE1-Serial1/0/1:0] quit
```

说明

网络中所有路由器和所有接口的优先级队列调度配置均与此相同，本处不再重复。而不同接口上的队列调度命令可能有所不同，请根据实际情况来进行配置。

步骤 8 配置可靠性

UPE1 上配置 LDP Auto FRR。

```
[UPE1] mpls ldp
[UPE1-mpls-ldp] auto-frr lsp-trigger all
```

```
[UPE1-mp1s-1dp] quit

# UPE2 上配置 LDP Auto FRR。

[UPE2] mp1s ldp
[UPE2-mp1s-1dp] auto-frr lsp-trigger all
[UPE2-mp1s-1dp] quit

# UPE1 配置 BFD for OSPF。

[UPE1] bfd
[UPE1-bfd] quit
[UPE1] ospf 1
[UPE1-ospf-1] bfd all-interfaces enable
[UPE1-ospf-1] quit

# UPE2 配置 BFD for OSPF。

[UPE2] bfd
[UPE2-bfd] quit
[UPE2] ospf 1
[UPE2-ospf-1] bfd all-interfaces enable
[UPE2-ospf-1] quit

# SPE1 配置 BFD for OSPF。

[SPE1] bfd
[SPE1-bfd] quit
[SPE1] ospf 1
[SPE1-ospf-1] bfd all-interfaces enable
[SPE1-ospf-1] quit

# SPE2 配置 BFD for OSPF。

[SPE2] bfd
[SPE2-bfd] quit
[SPE2] ospf 1
[SPE2-ospf-1] bfd all-interfaces enable
[SPE2-ospf-1] quit

# UPE1 上配置 BFD for BGP。

[UPE1] bgp 30011
[UPE1-bgp] peer 11.1.1.1 bfd enable
[UPE1-bgp] peer 11.2.2.2 bfd enable
[UPE1-bgp] quit

# UPE2 上配置 BFD for BGP。

[UPE2] bgp 30011
[UPE2-bgp] peer 11.1.1.1 bfd enable
[UPE2-bgp] peer 11.2.2.2 bfd enable
[UPE2-bgp] quit

# SPE1 上配置 BFD for BGP。

[SPE1] bgp 30011
[SPE1-bgp] peer 11.2.2.2 bfd enable
[SPE1-bgp] peer 11.3.3.3 bfd enable
[SPE1-bgp] peer 11.4.4.4 bfd enable
```

```
[SPE1-bgp] peer 10.1.1.1 bfd enable
[SPE1-bgp] quit
```

SPE2 上配置 BFD for BGP。

```
[SPE2] bgp 30011
[SPE2-bgp] peer 11.1.1.1 bfd enable
[SPE2-bgp] peer 11.3.3.3 bfd enable
[SPE2-bgp] peer 11.4.4.4 bfd enable
[SPE2-bgp] peer 10.1.1.1 bfd enable
[SPE2-bgp] quit
```

P 上配置 BFD for BGP。

```
[P] bgp 30010
[P-bgp] peer 11.1.1.1 bfd enable
[P-bgp] peer 11.2.2.2 bfd enable
[P-bgp] quit
```

UPE1 上配置 BFD for LDP LSP。

```
[UPE1] bfd
[UPE1-bfd] mpls-passive
[UPE1-bfd] quit
[UPE1] mpls
[UPE1-mpls] mpls bfd enable
[UPE1-mpls] mpls bfd-trigger all
[UPE1-mpls] quit
```

UPE2 上配置 BFD for LDP LSP。

```
[UPE2] bfd
[UPE2-bfd] mpls-passive
[UPE2-bfd] quit
[UPE2] mpls
[UPE2-mpls] mpls bfd enable
[UPE2-mpls] mpls bfd-trigger all
[UPE2-mpls] quit
```

----结束

配置文件

- ACC1 的配置文件

```
#
sysname ACC1
#
vlan batch 11
#
interface GigabitEthernet0/0/1
port link-type access
port default vlan 11
#
interface GigabitEthernet0/0/2
port link-type trunk
port trunk allow-pass vlan 11
#
```

```
return
```

- ACC2 的配置文件

```
#
sysname ACC2
#
vlan batch 12
#
interface GigabitEthernet0/0/1
port link-type access
port default vlan 12
#
interface GigabitEthernet0/0/2
port link-type trunk
port trunk allow-pass vlan 12
#
return
```

- ACC3 的配置文件

```
#
sysname ACC2
#
vlan batch 13
#
interface GigabitEthernet0/0/1
port link-type access
port default vlan 13
#
interface GigabitEthernet0/0/2
port link-type trunk
port trunk allow-pass vlan 13
#
return
```

- MCE 的配置文件

```
#
sysname MCE
#
vlan batch 11 12 13 101 102 103
#
ip vpn-instance rt
route-distinguisher 30011:11
vpn-target 30011:11 export-extcommunity
vpn-target 30011:11 import-extcommunity
ip vpn-instance nrt
route-distinguisher 30011:12
vpn-target 30011:12 export-extcommunity
vpn-target 30011:12 import-extcommunity
ip vpn-instance eng
route-distinguisher 30011:13
vpn-target 30011:13 export-extcommunity
vpn-target 30011:13 import-extcommunity
#
interface Vlanif11
ip binding vpn-instance rt
ip address 192.11.1.1 255.255.255.0
```

```
#
interface Vlanif12
 ip binding vpn-instance nrt
 ip address 192.12.1.1 255.255.255.0
#
interface Vlanif13
 ip binding vpn-instance eng
 ip address 192.13.1.1 255.255.255.0
#
interface Vlanif101
 ip binding vpn-instance rt
 ip address 192.101.1.2 255.255.255.0
#
interface Vlanif102
 ip binding vpn-instance nrt
 ip address 192.102.1.2 255.255.255.0
#
interface Vlanif103
 ip binding vpn-instance eng
 ip address 192.103.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 11
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 101 102 103
#
interface GigabitEthernet1/0/1
 port link-type access
 port default vlan 12
#
interface GigabitEthernet2/0/1
 port link-type access
 port default vlan 13
#
bgp 30011
#
 ipv4-family vpn-instance rt
  peer 192.101.1.1 as-number 30011
  import-route direct
#
 ipv4-family vpn-instance nrt
  peer 192.102.1.1 as-number 30011
  import-route direct
#
 ipv4-family vpn-instance eng
  peer 192.103.1.1 as-number 30011
  import-route direct
#
return
● UPE1 的配置文件
#
sysname UPE1
```

```
#
router id 11.3.3.3
#
vlan batch 101 to 103
#
ip vpn-instance rt
ipv4-family
route-distinguisher 30011:11
vpn-target 30011:11 export-extcommunity
vpn-target 30011:11 import-extcommunity
ip vpn-instance nrt
ipv4-family
route-distinguisher 30011:12
vpn-target 30011:12 export-extcommunity
vpn-target 30011:12 import-extcommunity
ip vpn-instance eng
ipv4-family
route-distinguisher 30011:13
vpn-target 30011:13 export-extcommunity
vpn-target 30011:13 import-extcommunity
#
bfd
mpls-passive
#
mpls lsr-id 11.3.3.3
mpls
mpls bfd enable
mpls bfd-trigger all
#
mpls ldp
auto-frr lsp-trigger all
#
acl number 3000
rule 5 permit ip vpn-instance rt
#
acl number 3001
rule 5 permit ip vpn-instance nrt
#
acl number 3002
rule 5 permit ip vpn-instance eng
#
traffic classifier rt operator or
if-match acl 3000
#
traffic classifier nrt operator or
if-match acl 3001
#
traffic classifier eng operator or
if-match acl 3002
#
traffic behavior rt
remark dscp af41
#
traffic behavior nrt
remark dscp af31
```

```
#
traffic behavior eng
  remark dscp af21
#
traffic policy vpn
  classifier rt behavior rt
  classifier nrt behavior nrt
  classifier eng behavior eng
#
controller E1 1/0/0
  clock slave
  using e1
  undo shutdown
#
controller E1 1/0/1
  clock slave
  using e1
  undo shutdown
#
interface Vlanif101
  ip binding vpn-instance rt
  ip address 192.101.1.1 255.255.255.0
#
interface Vlanif102
  ip binding vpn-instance nrt
  ip address 192.102.1.1 255.255.255.0
#
interface Vlanif103
  ip binding vpn-instance eng
  ip address 192.103.1.1 255.255.255.0
#
interface Serial1/0/0:0
  link-protocol ppp
  ip address 11.100.1.2 255.255.255.0
  mpls
  mpls ldp
  trust upstream default
  port-queue af2 wfq shaping cir percentage 10 pir percentage 11
  port-queue af3 wfq shaping cir percentage 30 pir percentage 31
  port-queue af4 wfq shaping cir percentage 60 pir percentage 61
#
interface Serial1/0/1:0
  link-protocol ppp
  ip address 11.100.2.2 255.255.255.0
  mpls
  mpls ldp
  trust upstream default
  port-queue af2 wfq shaping cir percentage 10 pir percentage 11
  port-queue af3 wfq shaping cir percentage 30 pir percentage 31
  port-queue af4 wfq shaping cir percentage 60 pir percentage 61
#
interface GigabitEthernet5/0/1
  port link-type trunk
  port trunk allow-pass vlan 101 102 103
  traffic-policy vpn inbound
```

```
trust upstream default
port-queue af3 wfq weight 30 outbound
port-queue af4 wfq weight 60 outbound
#
interface LoopBack0
 ip address 11.3.3.3 255.255.255.255
#
bgp 30011
peer 11.1.1.1 as-number 30011
peer 11.1.1.1 connect-interface loopback 0
peer 11.1.1.1 bfd enable
peer 11.2.2.2 as-number 30011
peer 11.2.2.2 connect-interface loopback 0
peer 11.2.2.2 bfd enable
#
ipv4-family vpvv4
peer 11.1.1.1 enable
peer 11.2.2.2 enable
#
ipv4-family vpn-instance rt
peer 192.101.1.2 as-number 30011
import-route direct
#
ipv4-family vpn-instance nrt
peer 192.102.1.2 as-number 30011
import-route direct
#
ipv4-family vpn-instance eng
peer 192.103.1.2 as-number 30011
import-route direct
#
#
ospf 1
bfd all-interfaces enable
area 0.0.0.1
network 11.100.1.0 0.0.0.255
network 11.100.2.0 0.0.0.255
network 11.3.3.3 0.0.0.0
#
return
```

● UPE2 的配置文件

```
#
sysname UPE2
#
router id 11.4.4.4
#
vlan batch 11 to 13
#
ip vpn-instance rt
ipv4-family
route-distinguisher 30011:11
vpn-target 30011:11 export-extcommunity
vpn-target 30011:11 import-extcommunity
ip vpn-instance nrt
ipv4-family
```

```
route-distinguisher 30011:12
vpn-target 30011:12 export-extcommunity
vpn-target 30011:12 import-extcommunity
ip vpn-instance eng
ipv4-family
route-distinguisher 30011:13
vpn-target 30011:13 export-extcommunity
vpn-target 30011:13 import-extcommunity
#
bfd
mpls-passive
#
mpls lsr-id 11.4.4.4
mpls
mpls bfd enable
mpls bfd-trigger all
#
mpls ldp
auto-frr lsp-trigger all
#
traffic classifier rt operator or
if-match any
#
traffic classifier nrt operator or
if-match any
#
traffic classifier eng operator or
if-match any
#
traffic behavior rt
remark dscp af41
#
traffic behavior nrt
remark dscp af31
#
traffic behavior eng
remark dscp af21
#
traffic policy rt
classifier rt behavior rt
#
traffic policy nrt
classifier nrt behavior nrt
#
traffic policy eng
classifier eng behavior eng
#
controller E1 1/0/0
clock slave
using e1
undo shutdown
#
controller E1 1/0/1
clock slave
using e1
```

```
undo shutdown
#
interface Vlanif11
 ip binding vpn-instance rt
 ip address 192.11.2.1 255.255.255.0
#
interface Vlanif12
 ip binding vpn-instance nrt
 ip address 192.12.2.1 255.255.255.0
#
interface Vlanif13
 ip binding vpn-instance eng
 ip address 192.13.2.1 255.255.255.0
#
interface Serial1/0/0:0
 link-protocol ppp
 ip address 11.100.3.2 255.255.255.0
 mpls
 mpls ldp
 trust upstream default
 port-queue af2 wfq shaping cir percentage 10 pir percentage 11
 port-queue af3 wfq shaping cir percentage 30 pir percentage 31
 port-queue af4 wfq shaping cir percentage 60 pir percentage 61
#
interface Serial1/0/1:0
 link-protocol ppp
 ip address 11.100.4.2 255.255.255.0
 mpls
 mpls ldp
 trust upstream default
 port-queue af2 wfq shaping cir percentage 10 pir percentage 11
 port-queue af3 wfq shaping cir percentage 30 pir percentage 31
 port-queue af4 wfq shaping cir percentage 60 pir percentage 61
#
interface GigabitEthernet5/0/1
 port link-type trunk
 port trunk allow-pass vlan 11
 traffic-policy rt inbound
 trust upstream default
 port-queue af3 wfq weight 30 outbound
 port-queue af4 wfq weight 60 outbound
#
interface GigabitEthernet5/0/2
 port link-type trunk
 port trunk allow-pass vlan 12
 traffic-policy nrt inbound
 trust upstream default
 port-queue af3 wfq weight 30 outbound
 port-queue af4 wfq weight 60 outbound
#
interface GigabitEthernet5/0/3
 port link-type trunk
 port trunk allow-pass vlan 13
 traffic-policy eng inbound
 trust upstream default
```

```
port-queue af3 wfq weight 30 outbound
port-queue af4 wfq weight 60 outbound
#
interface LoopBack0
 ip address 11.4.4.4 255.255.255.255
#
bgp 30011
 peer 11.1.1.1 as-number 30011
 peer 11.1.1.1 connect-interface loopback 0
 peer 11.1.1.1 bfd enable
 peer 11.2.2.2 as-number 30011
 peer 11.2.2.2 connect-interface loopback 0
 peer 11.2.2.2 bfd enable
#
ipv4-family vpv4
 peer 11.1.1.1 enable
 peer 11.2.2.2 enable
#
ipv4-family vpn-instance rt
 import-route direct
#
ipv4-family vpn-instance nrt
 import-route direct
#
ipv4-family vpn-instance eng
 import-route direct
#
#
ospf 1
 bfd all-interfaces enable
 area 0.0.0.2
  network 11.100.3.0 0.0.0.255
  network 11.100.4.0 0.0.0.255
  network 11.4.4.4 0.0.0.0
#
return
```

● SPE1 的配置文件

```
#
sysname SPE1
#
router id 11.1.1.1
#
ip vpn-instance rt
 ipv4-family
  route-distinguisher 30011:11
  vpn-target 30011:11 export-extcommunity
  vpn-target 30011:11 import-extcommunity
ip vpn-instance nrt
 ipv4-family
  route-distinguisher 30011:12
  vpn-target 30011:12 export-extcommunity
  vpn-target 30011:12 import-extcommunity
ip vpn-instance eng
 ipv4-family
  route-distinguisher 30011:13
```

```
vpn-target 30011:13 export-extcommunity
vpn-target 30011:13 import-extcommunity
#
bfd
#
mpls lsr-id 11.1.1.1
mpls
#
mpls ldp
#
controller E1 1/0/0
clock master
using e1
undo shutdown
#
controller E1 1/0/1
clock master
using e1
undo shutdown
#
interface Serial1/0/0:0
link-protocol ppp
ip address 11.100.1.1 255.255.255.0
mpls
mpls ldp
trust upstream default
port-queue af2 wfq shaping cir percentage 10 pir percentage 11
port-queue af3 wfq shaping cir percentage 30 pir percentage 31
port-queue af4 wfq shaping cir percentage 60 pir percentage 61
#
interface Serial1/0/1:0
link-protocol ppp
ip address 11.100.3.1 255.255.255.0
mpls
mpls ldp
trust upstream default
port-queue af2 wfq shaping cir percentage 10 pir percentage 11
port-queue af3 wfq shaping cir percentage 30 pir percentage 31
port-queue af4 wfq shaping cir percentage 60 pir percentage 61
#
interface Pos2/0/0
link-protocol ppp
ip address 100.1.1.2 255.255.255.0
mpls
mpls ldp
trust upstream default
port-queue af2 wfq shaping cir percentage 10 pir percentage 11
port-queue af3 wfq shaping cir percentage 30 pir percentage 31
port-queue af4 wfq shaping cir percentage 60 pir percentage 61
#
interface Pos2/0/1
link-protocol ppp
ip address 11.101.1.1 255.255.255.0
mpls
mpls ldp
```

```
trust upstream default
port-queue af2 wfq shaping cir percentage 10 pir percentage 11
port-queue af3 wfq shaping cir percentage 30 pir percentage 31
port-queue af4 wfq shaping cir percentage 60 pir percentage 61
#
interface LoopBack0
 ip address 11.1.1.1 255.255.255.255
#
bgp 30011
 peer 11.2.2.2 as-number 30011
 peer 11.2.2.2 connect-interface loopback 0
 peer 11.2.2.2 bfd enable
 peer 11.3.3.3 as-number 30011
 peer 11.3.3.3 connect-interface loopback 0
 peer 11.3.3.3 bfd enable
 peer 11.4.4.4 as-number 30011
 peer 11.4.4.4 connect-interface loopback 0
 peer 11.4.4.4 bfd enable
 peer 10.1.1.1 as-number 30010
 peer 10.1.1.1 connect-interface loopback 0
#
ipv4-family vpnv4
 peer 11.2.2.2 enable
 peer 11.2.2.2 reflect-client
 peer 11.3.3.3 enable
 peer 11.3.3.3 reflect-client
 peer 11.3.3.3 upe
 peer 11.3.3.3 default-originate vpn-instance rt
 peer 11.3.3.3 default-originate vpn-instance nrt
 peer 11.3.3.3 default-originate vpn-instance eng
 peer 11.4.4.4 enable
 peer 11.4.4.4 reflect-client
 peer 11.4.4.4 upe
 peer 11.4.4.4 default-originate vpn-instance rt
 peer 11.4.4.4 default-originate vpn-instance nrt
 peer 11.4.4.4 default-originate vpn-instance eng
 peer 10.1.1.1 enable
 peer 10.1.1.1 route-policy as30011_export_to_as30010 export
 peer 10.1.1.1 bfd enable
#
ipv4-family vpn-instance rt
 import-route direct
#
ipv4-family vpn-instance nrt
 import-route direct
#
ipv4-family vpn-instance eng
 import-route direct
#
#
ospf 1
 bfd all-interfaces enable
 import-route static cost 1000 type 1
 asbr-summary 11.0.0.0 255.0.0.0
 area 0.0.0.0
```

```
network 11.101.1.0 0.0.0.255
network 11.1.1.1 0.0.0.0
area 0.0.0.1
network 11.100.1.0 0.0.0.255
area 0.0.0.2
network 11.100.3.1 0.0.0.255
#
ip route-static 10.0.0.0 255.0.0.0 pos 2/0/0 100.1.1.1
#
route-policy as30011_export_to_as30010 permit node 10
if-match as-path-filter 10
#
ip as-path-filter 10 permit ^$
#
return
```

- SPE2 的配置文件

```
#
sysname SPE2
#
router id 11.2.2.2
#
ip vpn-instance rt
ipv4-family
route-distinguisher 30011:11
vpn-target 30011:11 export-extcommunity
vpn-target 30011:11 import-extcommunity
ip vpn-instance nrt
ipv4-family
route-distinguisher 30011:12
vpn-target 30011:12 export-extcommunity
vpn-target 30011:12 import-extcommunity
ip vpn-instance eng
ipv4-family
route-distinguisher 30011:13
vpn-target 30011:13 export-extcommunity
vpn-target 30011:13 import-extcommunity
#
bfd
#
mpls lsr-id 11.2.2.2
mpls
#
mpls ldp
#
controller E1 1/0/0
clock master
using e1
undo shutdown
#
controller E1 1/0/1
clock master
using e1
undo shutdown
#
interface Serial1/0/0:0
```

```
link-protocol ppp
ip address 11.100.2.1 255.255.255.0
mpls
mpls ldp
trust upstream default
port-queue af2 wfq shaping cir percentage 10 pir percentage 11
port-queue af3 wfq shaping cir percentage 30 pir percentage 31
port-queue af4 wfq shaping cir percentage 60 pir percentage 61
#
interface Serial1/0/1:0
link-protocol ppp
ip address 11.100.4.1 255.255.255.0
mpls
mpls ldp
trust upstream default
port-queue af2 wfq shaping cir percentage 10 pir percentage 11
port-queue af3 wfq shaping cir percentage 30 pir percentage 31
port-queue af4 wfq shaping cir percentage 60 pir percentage 61
#
interface Pos2/0/0
link-protocol ppp
ip address 100.1.2.2 255.255.255.0
mpls
mpls ldp
trust upstream default
port-queue af2 wfq shaping cir percentage 10 pir percentage 11
port-queue af3 wfq shaping cir percentage 30 pir percentage 31
port-queue af4 wfq shaping cir percentage 60 pir percentage 61
#
interface Pos2/0/1
link-protocol ppp
ip address 11.101.1.2 255.255.255.0
mpls
mpls ldp
trust upstream default
port-queue af2 wfq shaping cir percentage 10 pir percentage 11
port-queue af3 wfq shaping cir percentage 30 pir percentage 31
port-queue af4 wfq shaping cir percentage 60 pir percentage 61
#
interface LoopBack0
ip address 11.2.2.2 255.255.255.255
#
bgp 30011
peer 11.1.1.1 as-number 30011
peer 11.1.1.1 connect-interface loopback 0
peer 11.1.1.1 bfd enable
peer 11.3.3.3 as-number 30011
peer 11.3.3.3 connect-interface loopback 0
peer 11.3.3.3 bfd enable
peer 11.4.4.4 as-number 30011
peer 11.4.4.4 connect-interface loopback 0
peer 11.4.4.4 bfd enable
peer 10.1.1.1 as-number 30010
peer 10.1.1.1 connect-interface loopback 0
peer 10.1.1.1 bfd enable
```

```
#
ipv4-family vpnv4
 peer 11.1.1.1 enable
 peer 11.1.1.1 reflect-client
 peer 11.3.3.3 enable
 peer 11.3.3.3 reflect-client
 peer 11.3.3.3 upe
 peer 11.3.3.3 default-originate vpn-instance rt
 peer 11.3.3.3 default-originate vpn-instance nrt
 peer 11.3.3.3 default-originate vpn-instance eng
 peer 11.4.4.4 enable
 peer 11.4.4.4 reflect-client
 peer 11.4.4.4 upe
 peer 11.4.4.4 default-originate vpn-instance rt
 peer 11.4.4.4 default-originate vpn-instance nrt
 peer 11.4.4.4 default-originate vpn-instance eng
 peer 10.1.1.1 enable
 peer 10.1.1.1 route-policy as30011_export_to_as30010 export
#
ipv4-family vpn-instance rt
 import-route direct
#
ipv4-family vpn-instance nrt
 import-route direct
#
ipv4-family vpn-instance eng
 import-route direct
#
#
ospf 1
 bfd all-interfaces enable
 import-route static cost 1000 type 1
 asbr-summary 11.0.0.0 255.0.0.0
 area 0.0.0.0
  network 11.101.1.2 0.0.0.255
  network 11.2.2.2 0.0.0.0
 area 0.0.0.1
  network 11.100.2.1 0.0.0.255
 area 0.0.0.2
  network 11.100.4.1 0.0.0.255
#
 ip route-static 10.0.0.0 255.0.0.0 pos 2/0/0 100.1.2.1
#
 route-policy as30011_export_to_as30010 permit node 10
  if-match as-path-filter 10
#
 ip as-path-filter 10 permit ^$
#
return
● P 的配置文件
#
 sysname P
#
 router id 10.1.1.1
#
```

```
bfd
#
mpls lsr-id 10.1.1.1
mpls
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
ip address 100.1.1.1 255.255.255.0
mpls
mpls ldp
trust upstream default
port-queue af2 wfq shaping cir percentage 10 pir percentage 11
port-queue af3 wfq shaping cir percentage 30 pir percentage 31
port-queue af4 wfq shaping cir percentage 60 pir percentage 61
#
interface Pos1/0/1
link-protocol ppp
ip address 100.1.2.1 255.255.255.0
mpls
mpls ldp
trust upstream default
port-queue af2 wfq shaping cir percentage 10 pir percentage 11
port-queue af3 wfq shaping cir percentage 30 pir percentage 31
port-queue af4 wfq shaping cir percentage 60 pir percentage 61
#
interface LoopBack0
ip address 10.1.1.1 255.255.255.255
#
bgp 30010
peer 11.1.1.1 as-number 30011
peer 11.1.1.1 connect-interface loopback 0
peer 11.1.1.1 bfd enable
peer 11.2.2.2 as-number 30011
peer 11.2.2.2 connect-interface loopback 0
peer 11.2.2.2 bfd enable
#
ipv4-family vpnv4
peer 11.1.1.1 enable
peer 11.1.1.1 route-policy as30010_import_from_as30011 import
peer 11.1.1.1 route-policy as30010_export_to_as30011 export
peer 11.2.2.2 enable
peer 11.2.2.2 route-policy as30010_import_from_as30011 import
peer 11.2.2.2 route-policy as30010_export_to_as30011 export
#
ipv4-family vpn-instance rt
import-route direct
#
ipv4-family vpn-instance nrt
import-route direct
#
ipv4-family vpn-instance eng
import-route direct
#
```

```
#
ip route-static 11.0.0.0 255.0.0.0 pos 1/0/0 100.1.1.2 preference 60
ip route-static 11.0.0.0 255.0.0.0 pos 1/0/1 100.1.2.2 preference 100
#
route-policy as30010_import_from_as30011 permit node 10
if-match as-path-filter 10
route-policy as30010_export_to_as30011 permit node 10
if-match as-path-filter 20
apply community no-export
#
ip as-path-filter 10 permit ^30011$
ip as-path-filter 20 permit ^30010$
#
return
```