H3C S5130S-SI[LI]&S5120V2-SI[LI]&S5110V2-SI&S5000V3-EI&S5000E-X&S3100V3-SI 系列以太网交换机

三层技术-IP 路由配置指导

新华三技术有限公司
http://www.h3c.com

资料版本：6W103-20190822
产品版本：Release 612x 系列

前 言

本配置指导主要介绍路由协议的原理和配置，包括 IPv4、IPv6 网络的多种路由学习技术，以及影响路由选择或者路由表生成的策略。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

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

本书约定

1. 命令行格式约定

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

2. 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 IP路由基础

本手册仅介绍单播路由协议，组播路由协议请参见“IP 组播配置指导”。

1.1 IP路由简介

在网络中路由器根据所收到的报文的目的地址选择一条合适的路径，并将报文转发到下一个路由器。路径中最后一个路由器负责将报文转发给目的主机。路由就是报文在转发过程中的路径信息，用来指导报文转发。

1.1.1 路由表

RIB（Routing Information Base，路由信息库），是一个集中管理路由信息的数据库，包含路由表信息以及路由周边信息（路由迭代信息、路由共享信息以及路由扩展信息）等。

路由器通过对路由表进行优选，把优选路由下发到 FIB（Forwarding Information Base，转发信息库）表中，通过 FIB 表指导报文转发。FIB 表中每条转发项都指明了要到达某子网或某主机的报文应通过路由器的哪个物理接口发送，就可以到达该路径的下一个路由器，或者不需再经过别的路由器便可传送到直接相连的网络中的目的主机。FIB 表的具体内容，请参见“三层技术-IP 业务配置指导”中的“IP 转发基础”。

1.1.2 路由分类

表1-1 路由分类

分类标准	具体分类
根据来源不同	• 直连路由：链路层协议发现的路由，也称为接口路由 • 静态路由：网络管理员手工配置的路由。静态路由配置方便，对系统要求低，适用于拓扑结构简单并且稳定的小型网络。其缺点是每当网络拓扑结构发生变化，都需要手工重新配置，不能自动适应 • 动态路由：路由协议发现的路由
根据路由目的地的不同	• 网段路由：目的地为网段，子网掩码长度小于 32 位 • 主机路由：目的地为主机，子网掩码长度为 32 位
根据目的地与该路由器是否直接相连	• 直接路由：目的地所在网络与路由器直接相连 • 间接路由：目的地所在网络与路由器非直接相连

1.1.3 路由协议分类

路由协议有自己的路由算法，能够自动适应网络拓扑的变化，适用于具有一定规模的网络拓扑。其缺点是配置比较复杂，对系统的要求高于静态路由，并占用一定的网络资源。

对路由协议的分类可采用以下不同标准。

表1-2 路由协议分类

分类标准	具体分类
根据作用范围	• IGP（Interior Gateway Protocol，内部网关协议）：在一个自治系统内部运行，常见的 IGP 协议包括 RIP、OSPF 和 IS-IS • EGP（Exterior Gateway Protocol，外部网关协议）：运行于不同自治系统之间，BGP 是目前最常用的 EGP
根据使用算法	• 距离矢量（Distance-Vector）协议：包括 RIP 和 BGP。其中，BGP 也被称为路径矢量协议（Path-Vector） • 链路状态（Link-State）协议：包括 OSPF 和 IS-IS
根据目的地址类型	• 单播路由协议：包括 RIP、OSPF、BGP 和 IS-IS 等 • 组播路由协议：包括 PIM-SM、PIM-DM 等
根据IP协议版本	• IPv4 路由协议：包括 RIP、OSPF、BGP 和 IS-IS 等 • IPv6 路由协议：包括 RIPng、OSPFv3、IPv6 BGP 和 IPv6 IS-IS 等

AS（Autonomous System，自治系统）是拥有同一选路策略，并在同一技术管理部门下运行的一组路由器。

1.1.4 路由优先级

对于相同的目的地，不同的路由协议、直连路由和静态路由可能会发现不同的路由，但这些路由并不都是最优的。为了判断最优路由，各路由协议、直连路由和静态路由都被赋予了一个优先级，具有较高优先级的路由协议发现的路由将成为最优路由。

除直连路由外，各路由协议的优先级都可由用户手工进行配置。另外，每条静态路由的优先级都可以不相同。缺省的路由优先级如 表 1-3 所示，数值越小表明优先级越高。

表1-3 缺省的路由优先级

路由协议或路由种类	缺省的路由优先级
DIRECT（直连路由）	0
组播静态路由	1
OSPF	10
IS-IS	15
单播静态路由	60
RIP	100
OSPF ASE	150
OSPF NSSA	150
IBGP	255
EBGP	255
UNKNOWN（来自不可信源端的路由）	256

1.1.5 负载分担

对同一路由协议来说，允许配置多条目的地相同且开销也相同的路由。当到同一目的地的路由中，没有更高优先级的路由时，这几条路由都被采纳，在转发去往该目的地的报文时，依次通过各条路径发送，从而实现网络的负载分担。

目前支持负载分担有静态路由/IPv6 静态路由、RIP/RIPng、OSPF/OSPFv3、BGP/IPv6 BGP 和 IS-IS/IPv6 IS-IS。

1.1.6 路由备份

使用路由备份可以提高网络的可靠性。用户可根据实际情况，配置到同一目的地的多条路由，其中优先级最高的一条路由作为主路由，其余优先级较低的路由作为备份路由。

正常情况下，路由器采用主路由转发数据。当链路出现故障时，主路由变为非激活状态，路由器选择备份路由中优先级最高的转发数据，实现从主路由到备份路由的切换；当链路恢复正常时，路由器重新选择路由，由于主路由的优先级最高，路由器选择主路由来发送数据，实现从备份路由到主路由的切换。

1.1.7 路由迭代

对于 BGP 路由（直连 EBGP 路由除外）和静态路由（配置了下一跳）以及多跳 RIP 路由而言，其所携带的下一跳信息可能并不是直接可达，需要找到到达下一跳的直连出接口。路由迭代的过程就是通过路由的下一跳信息来找到直连出接口的过程。

而对于 OSPF 和 IS-IS 等链路状态路由协议而言，其下一跳是直接在路由计算时得到的，不需要进行路由迭代。

路由迭代信息记录并保存路由迭代的结果，包括依赖路由的概要信息、迭代路径、迭代深度等。

1.1.8 路由共享

由于各路由协议采用的路由算法不同，不同的路由协议可能会发现不同的路由。如果网络规模较大，当使用多种路由协议时，往往需要在不同的路由协议间能够共享各自发现的路由。

各路由协议都可以引入其它路由协议的路由、直连路由和静态路由，具体内容请参见本手册中各路由协议模块有关引入外部路由的描述。

路由共享信息记录了路由协议之间的引入关系。

1.1.9 路由扩展

路由扩展属性主要是指 BGP 路由的扩展团体属性以及 OSPF 路由的区域 ID、路由类型和 Router ID 等。同路由共享一样，路由协议可以引入其它路由协议的路由扩展属性。

路由扩展信息记录了各路由协议的路由扩展属性以及路由协议扩展属性之间的引入关系。

1.2 配置路由和标签在RIB中的最大存活时间

1. 功能简介

当协议路由表项较多或协议 GR 时间较长时，由于协议收敛速度较慢，可能会出现协议路由表项提前老化的问题。通过调节路由和标签在 RIB 中的最大存活时间，可以解决上面的问题。

2. 配置限制和指导

该配置在下一次协议进程倒换或者 RIB 进程倒换时才生效。

3. 配置步骤（IPv4）

(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

(4) 配置 IPv4 路由和标签在 RIB 中的最大存活时间。

protocol *protocol* [**instance** *instance-name*] **lifetime** *seconds*

缺省情况下，IPv4 路由和标签在 RIB 中的最大存活时间为 480 秒。

4. 配置步骤（IPv6）

(1) 进入系统视图。

system-view

(2) 进入 RIB 视图。

rib

(3) 创建 RIB IPv6 地址族，并进入 RIB IPv6 地址族视图。

address-family ipv6

(4) 配置 IPv6 路由和标签在 RIB 中的最大存活时间。

protocol *protocol* [**instance** *instance-name*] **lifetime** *seconds*

缺省情况下，IPv6 路由和标签在 RIB 中的最大存活时间为 480 秒。

1.3 配置路由在FIB中的最大存活时间

1. 功能简介

当协议进程倒换或 RIB 进程倒换后，如果协议进程没有配置 GR 或 NSR，需要多保留一段时间 FIB 表项；如果协议进程配置了 GR 或 NSR，需要立刻删除 FIB 表项，避免 FIB 表项长时间存在导致问题。通过调节路由在 FIB 中的最大存活时间，可以解决上面的问题。

2. 配置步骤（IPv4）

(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

(4) 配置 IPv4 路由在 FIB 中的最大存活时间。

fib lifetime *seconds*

缺省情况下，IPv4 路由在 FIB 中的最大存活时间为 600 秒。

3. 配置步骤（IPv6）

(1) 进入系统视图。

system-view

(2) 进入 RIB 视图。

rib

(3) 创建 RIB IPv6 地址族，并进入 RIB IPv6 地址族视图。

address-family ipv6

(4) 配置 IPv6 路由在 FIB 中的最大存活时间。

fib lifetime *seconds*

缺省情况下，IPv6 路由在 FIB 中的最大存活时间为 600 秒。

1.4 配置路由的NSR功能

1. 功能简介

NSR（Nonstop Routing，不间断路由）将路由信息从主进程备份到备进程，在设备发生主备倒换时保证路由信息不丢失，解决了主备倒换期间引发的路由震荡问题，保证转发业务不中断。

路由 NSR 相对于路由协议 NSR 功能，主备倒换时路由收敛速度更快。

2. 配置限制和指导

配置本功能的同时，请配置协议的 GR 或 NSR 功能，否则可能导致路由老化和流量中断。

3. 配置步骤（IPv4）

(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

(4) 配置 IPv4 路由的 NSR 功能。

non-stop-routing

缺省情况下，IPv4 路由的 NSR 功能处于关闭状态。

4. 配置步骤（IPv6）

(1) 进入系统视图。

system-view

(2) 进入 RIB 视图。

rib

(3) 创建 RIB IPv6 地址族，并进入 RIB IPv6 地址族视图。

address-family ipv6

(4) 配置 IPv6 路由的 NSR 功能。

non-stop-routing

缺省情况下，IPv6 路由的 NSR 功能处于关闭状态。

1.5 配置路由不同协议间快速重路由功能

1. 功能简介

当 RIB 表中存在去往同一目的地的多条路由时，路由器会将优先级较高的路由下发到 FIB 表，当该路由的下一跳不可达时，数据流量将会被中断，路由器会重新进行路由优选，优选完毕后，使用新的最优路由来指导报文转发。例如，去往同一个目的地存在一条静态路由和一条 OSPF 路由，缺省情况 OSPF 路由会作为最优路由下发到 FIB 表。当 OSPF 路由的下一跳不可达时，数据流量将会被中断。

通过配置不同协议间快速重路由功能，可以将静态路由的下一跳作为备份下一跳。当路由器检测到网络故障时，将使用备份下一跳替换失效下一跳，通过备份下一跳来指导报文的转发，从而大大缩短了流量中断的时间。

2. 配置限制和指导

使用不同协议间的快速重路由功能生成备份下一跳时可能会造成环路。

3. 配置步骤（IPv4）

(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

(4) 配置 IPv4 路由不同协议间快速重路由功能。

inter-protocol fast-reroute

缺省情况下，不同协议间快速重路由处于关闭状态。

4. 配置步骤（IPv6）

(1) 进入系统视图。

system-view

(2) 进入 RIB 视图。

rib

(3) 创建 RIB IPv6 地址族，并进入 RIB IPv6 地址族视图。

address-family ipv6

(4) 配置 IPv6 路由不同协议间快速重路由功能。

inter-protocol fast-reroute

缺省情况下，不同协议间快速重路由处于关闭状态。

1.6 配置路由快速切换功能

1. 功能简介

在未开启本功能的情况下，当某个物理接口为大量路由（包括等价路由和主备路由的主路由）连接下一跳的出接口时，如果该接口所在的链路故障时，设备需要先删除失效链路对应的所有 ARP/ND 表项，然后通知 FIB 删除失效的 FIB 表项，处理时间过长，流量无法快速切换到可用路径。通过开启本功能，当接口所在的链路故障时，设备首先通知 FIB 删除失效的 FIB 表项，以加快路由的切换、缩短流量中断的时间。

2. 配置步骤（IPv4）

(1) 进入系统视图。

system-view

(2) 配置开启 IPv4 路由快速切换功能。

ip route fast-switchover enable

缺省情况下，IPv4 路由快速切换功能处于关闭状态。

3. 配置步骤（IPv6）

(1) 进入系统视图。

system-view

(2) 配置开启 IPv6 路由快速切换功能。

ipv6 route fast-switchover enable

缺省情况下，IPv6 路由快速切换功能处于关闭状态。

1.7 配置路由按照路由策略进行迭代下一跳查找

1. 功能简介

通过配置按路由策略迭代下一跳，可以对路由迭代的结果进行控制。例如：当路由发生变化时，路由管理需要对非直连的下一跳重新进行迭代。如果不对迭代的结果路由进行任何限制，则路由管理可能会将下一跳迭代到一个错误的转发路径上，从而造成流量丢失。此时，可以通过配置本功能，将错误的依赖路由过滤掉，使路由迭代到通过路由策略过滤的指定依赖路由上。

2. 配置限制和指导

配置路由策略时，如果配置了 apply 子句，apply 子句不会生效。

配置路由策略时，请确保至少有一个正确的依赖路由能够通过该策略的过滤，否则可能导致相关路由不可达，无法正确指导转发。

3. 配置步骤（IPv4）

(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

(4) 配置路由按照路由策略进行迭代下一跳查找。

protocol *protocol* **nexthop recursive-lookup route-policy** *route-policy-name*

缺省情况下，未配置路由按路由策略进行下一跳迭代查找。

4. 配置步骤（IPv6）

(1) 进入系统视图。

system-view

(2) 进入 RIB 视图。

rib

(3) 创建 RIB IPv6 地址族，并进入 RIB IPv6 地址族视图。

address-family ipv6

(4) 配置路由按照路由策略进行迭代下一跳查找。

protocol *protocol* **nexthop recursive-lookup route-policy** *route-policy-name*

缺省情况下，未配置路由按路由策略进行下一跳迭代查找。

1.8 配置设备支持的最大激活路由前缀数

1. 功能简介

配置设备支持的最大 IPv4/IPv6 激活路由前缀数后，当设备上的 IPv4/IPv6 激活路由前缀数超过最大支持的激活路由前缀数目时，可以继续激活新的路由前缀，但会产生一条日志信息提示用户，以便用户及时执行必要的操作，以免 IPv4/IPv6 激活路由前缀占用过多的资源。

2. 配置步骤（IPv4）

(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

(4) 配置最大 IPv4 激活路由前缀数。

routing-table limit *number* **simply-alert**

缺省情况下，不限制设备支持的最大 IPv4 激活路由前缀数。

RIB IPv4 地址族视图下的配置用于控制公网 IPv4 激活路由的总数。

3. 配置步骤（IPv6）

(1) 进入系统视图。

system-view

(2) 进入 RIB 视图。

rib

(3) 创建 RIB IPv6 地址族，并进入 RIB IPv6 地址族视图。

address-family ipv6

(4) 配置最大 IPv6 激活路由前缀数。

routing-table limit *number* **simply-alert**

缺省情况下，不限制设备支持的最大 IPv6 激活路由前缀数。

RIB IPv6 地址族视图下的配置用于控制公网 IPv6 激活路由的总数。

1.9 路由表显示和维护

在任意视图下执行 **display** 命令可以显示路由表信息。在用户视图下执行 **reset** 命令可以清除路由表的统计信息。

表1-4 路由表显示和维护

操作	命令
显示路由表的信息	**display ip routing-table** [**verbose**] **display ip routing-table** [**all-routes**]
显示通过指定基本访问控制列表过滤的路由信息	**display ip routing-table acl** *ipv4-acl-number* [**verbose**]
显示指定目的地址的路由	**display ip routing-table** *ip-address* [*mask-length* | *mask*] [**longer-match**] [**verbose**]
显示指定目的地址范围内的路由	**display ip routing-table** *ip-address1* **to** *ip-address2* [**verbose**]
显示通过指定前缀列表过滤的路由信息	**display ip routing-table prefix-list** *prefix-list-name* [**verbose**]
显示指定协议生成或发现的路由信息	**display ip routing-table protocol** *protocol* [**inactive** | **verbose**]
显示路由表中的综合路由统计信息	**display ip routing-table** [**all-routes**] **statistics**
显示路由表的概要信息	**display ip routing-table summary**
显示IPv6 RIB的路由属性信息	**display ipv6 rib attribute** [*attribute-id*]
显示IPv6 RIB的GR状态信息	**display ipv6 rib graceful-restart**
显示IPv6 RIB的下一跳信息	**display ipv6 rib nib** [**self-originated**] [*nib-id*] [**verbose**] **display ipv6 rib nib protocol** *protocol* [**verbose**]
显示IPv6直连路由下一跳信息	**display ipv6 route-direct nib** [*nib-id*] [**verbose**]

操作	命令
显示IPv6路由表的信息	**display ipv6 routing-table** [**verbose**] **display ipv6 routing-table** [**all-routes**]
显示通过指定基本IPv6 ACL过滤的IPv6路由信息	**display ipv6 routing-table acl** *ipv6-acl-number* [**verbose**]
显示指定目的地址的IPv6路由信息	**display ipv6 routing-table** *ipv6-address* [*prefix-length*] [**longer-match**] [**verbose**]
显示指定目的地址范围内的IPv6路由信息	**display ipv6 routing-table** *ipv6-address1* **to** *ipv6-address2* [**verbose**]
显示通过指定前缀列表过滤的IPv6路由信息	**display ipv6 routing-table prefix-list** *prefix-list-name* [**verbose**]
显示指定协议生成或发现的IPv6路由信息	**display ipv6 routing-table protocol** *protocol* [**inactive** | **verbose**]
显示IPv6路由表中的综合路由统计信息	**display ipv6 routing-table** [**all-routes**] **statistics**
显示IPv6路由表的概要信息	**display ipv6 routing-table summary**
显示RIB的GR状态信息	**display rib graceful-restart**
显示RIB的下一跳信息	**display rib nib** [**self-originated**] [*nib-id*] [**verbose**] **display rib nib protocol** *protocol* [**verbose**]
显示直连路由下一跳信息	**display route-direct nib** [*nib-id*] [**verbose**]
清除路由表中的综合路由统计信息	**reset ip routing-table statistics protocol** { *protocol* | **all** }
清除IPv6路由表中的综合路由统计信息	**reset ipv6 routing-table statistics protocol** { *protocol* | **all** }

目 录

1 静态路由

1.1 静态路由简介

静态路由是一种特殊的路由，由管理员手工配置。当网络结构比较简单时，只需配置静态路由就可以使网络正常工作。

静态路由不能自动适应网络拓扑结构的变化。当网络发生故障或者拓扑发生变化后，必须由网络管理员手工修改配置。

1.2 配置静态路由

(1) 进入系统视图。

system-view

(2) 配置静态路由。

ip route-static *dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* [**recursive-lookup host-route**] } [**permanent** | **track** *track-entry-number*] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

缺省情况下，未配置静态路由。

通过在 Track 模块和静态路由之间建立联动，可以实现静态路由可达性的实时判断。关于 Track 的详细介绍，请参见“可靠性配置指导”中的“Track”。

(3) （可选）配置静态路由向下一跳定时发送 ARP。

ip route-static arp-request interval *interval*

缺省情况下，静态路由不发送 ARP request。

(4) （可选）配置静态路由的缺省优先级。

ip route-static default-preference *default-preference*

缺省情况下，静态路由的缺省优先级为 60。

1.3 配置静态路由配置组

1. 功能简介

当配置多条静态路由时，如果只是前缀不同，每条静态路由都要配置一遍命令，比较繁琐。可以配置静态路由配置组，对静态路由进行批量配置，节省配置工作量。

按配置组配置静态路由时，配置组下的所有前缀会应用相同的下一跳、出接口信息。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建静态路由配置组，并进入静态路由配置组视图。

ip route-static-group *group-name*

缺省情况下，未配置静态路由配置组。

(3) 在静态路由配置组中增加前缀。

prefix *dest-address* { *mask-length* | *mask* }

缺省情况下，静态路由配置组中未配置前缀。

(4) 退回系统视图。

quit

(5) 配置静态路由。

ip route-static group *group-name* { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* [**recursive-lookup host-route**] } [**permanent** | **track** *track-entry-number*] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

缺省情况下，未配置静态路由。

1.4 配置静态路由删除

1. 功能简介

使用 **undo ip route-static** 命令可以删除一条静态路由，而使用 **delete static-routes all** 命令可以删除包括缺省路由在内的所有静态路由。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 删除所有静态路由。

delete static-routes all

1.5 配置静态路由与BFD联动

注意

路由振荡时，使能 BFD 功能可能会加剧振荡，请谨慎使用。

1.5.1 功能简介

BFD（Bidirectional Forwarding Detection，双向转发检测）提供了一个通用的、标准化的、介质无关、协议无关的快速故障检测机制，可以为上层协议（如路由协议等）统一地快速检测两台路由器间双向转发路径的故障。

关于 BFD 的详细介绍，请参见“可靠性配置指导”中的“BFD”。

1.5.2 配置双向检测

1. 功能简介

双向检测，即本端和对端需要同时进行配置，通过控制报文检测两个方向上的链路状态，实现毫秒级别的链路故障检测。

双向检测支持直连下一跳和非直连下一跳。

- 直连下一跳是指下一跳和本端是直连的，配置时必须指定出接口和下一跳。
- 非直连下一跳是指下一跳和本端不是直连的，中间还有其它设备。配置时必须指定下一跳和 BFD 源 IP 地址。

2. 配置直连下一跳双向检测

(1) 进入系统视图。

system-view

(2) 配置静态路由与 BFD 联动。

ip route-static *dest-address* { *mask-length* | *mask* } *interface-type interface-number next-hop-address* **bfd control-packet** [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

缺省情况下，未配置静态路由与 BFD 联动。

3. 配置非直连下一跳双向检测

(1) 进入系统视图。

system-view

(2) 配置静态路由与 BFD 联动。

ip route-static *dest-address* { *mask-length* | *mask* } { *next-hop-address* **bfd control-packet bfd-source** *ip-address* } [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

缺省情况下，未配置静态路由与 BFD 联动。

1.5.3 配置单跳检测

1. 功能简介

单跳检测，即只需要本端进行配置，通过 echo 报文检测链路的状态。echo 报文的目的地址为本端接口地址，发送给下一跳设备后会直接转发回本端。这里所说的“单跳”是 IP 的一跳。

静态路由的出接口为处于 SPOOFING 状态时，不能使用 BFD 进行检测。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 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。

本命令的详细情况请参见“可靠性命令参考”中的“BFD”。

(3) 配置静态路由与 BFD 联动。

ip route-static *dest-address* { *mask-length* | *mask* } *interface-type interface-number next-hop-address* **bfd echo-packet** [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

缺省情况下，未配置静态路由与 BFD 联动。

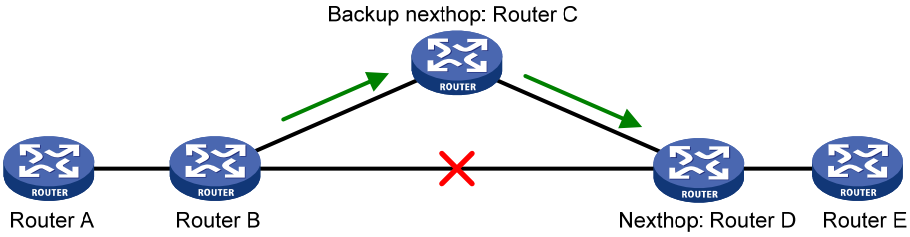
1.6 配置静态路由快速重路由功能

1.6.1 功能简介

当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输才能到达目的地的报文将会丢失或产生路由环路，数据流量将会被中断。

为了尽可能避免网络故障导致的流量中断，网络管理员可以根据需要配置静态路由快速重路由功能。

图1-1 静态路由快速重路由功能示意图



如 图 1-1 所示，通过配置快速重路由功能，网络管理员可以为路由指定备份下一跳，也可以在存在低优先级静态路由的情况下，使能自动快速重路由功能，查找满足条件的低优先级路由的下一跳作为主路由的备份下一跳，当路由器检测到网络故障时，路由器会使用事先配置好的备份下一跳替换失效下一跳，通过备份下一跳来指导报文的转发，从而避免了流量中断。

1.6.2 配置限制和指导

静态路由快速重路由功能不能与静态路由 BFD 功能同时使用。

等价路由不支持配置静态路由快速重路由功能。

配置本功能后，当主链路三层接口 up，主链路由双通变为单通或者不通时，设备会将流量快速地切换到备份路径上转发；当主链路三层接口 down 时，设备会暂时将流量快速地切换到备份路径上转发。同时，设备会重新查找到达目的地址的路由，并将流量切换到查找到的新的路径。如果没有查找到路由，则流量转发会中断。因此，除本配置创建的静态路由外，设备上还需要存在一条到达目的地址的路由。单通现象，即一条链路上的两端，有且只有一端可以收到另一端发来的报文，此链路称为单向链路。

1.6.3 配置手工指定备份下一跳

1. 配置限制和指导

静态路由配置的备份出接口拔出或者删除时，配置的路由会失效。备份出接口和下一跳不能直接修改，且不能和主出接口和下一跳相同。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置静态路由快速重路由功能。

ip route-static *dest-address* { *mask-length* | *mask* } *interface-type interface-number* [*next-hop-address* [**backup-interface** *interface-type interface-number* [**backup-nexthop** *backup-nexthop-address*]]] [**permanent**] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

缺省情况下，静态路由快速重路由功能处于关闭状态。

1.6.4 配置自动查找备份下一跳

(1) 进入系统视图。

system-view

(2) 配置静态路由自动快速重路由功能。

ip route-static fast-reroute auto

缺省情况下，静态路由自动快速重路由功能处于关闭状态。

1.6.5 配置静态路由快速重路由支持BFD检测功能

1. 功能简介

缺省情况下，静态路由通过 ARP 检测主路由的下一跳是否可达。配置本功能后，将使用 BFD（Echo 方式）检测主路由的下一跳是否可达，这种方式可以更快地检测到链路故障。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 BFD Echo 报文源地址。

bfd echo-source-ip *ip-address*

缺省情况下，未配置 BFD Echo 报文源地址。

echo 报文的源 IP 地址用户可以任意指定。建议配置 echo 报文的源 IP 地址不属于该设备任何一个接口所在网段。

本命令的详细情况请参见“可靠性命令参考”中的“BFD”。

(3) 使能静态路由中主用链路的 BFD（Echo 方式）检测功能。

ip route-static primary-path-detect bfd echo

缺省情况下，静态路由中主用链路的 BFD（Echo 方式）检测功能处于关闭状态。

1.7 静态路由显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令查看静态路由配置的运行情况并检验配置结果。

表1-1 静态路由显示和维护

操作	命令
查看静态路由表信息（本命令的详细情况请参见“三层技术-IP路由命令参考”中的“IP路由基础”）	**display ip routing-table protocol static** [**inactive** | **verbose**]
显示静态路由下一跳信息	**display route-static nib** [*nib-id*] [**verbose**]
显示静态路由表信息	**display route-static routing-table** [*ip-address* { *mask-length* | *mask* }]

1.8 静态路由典型配置举例

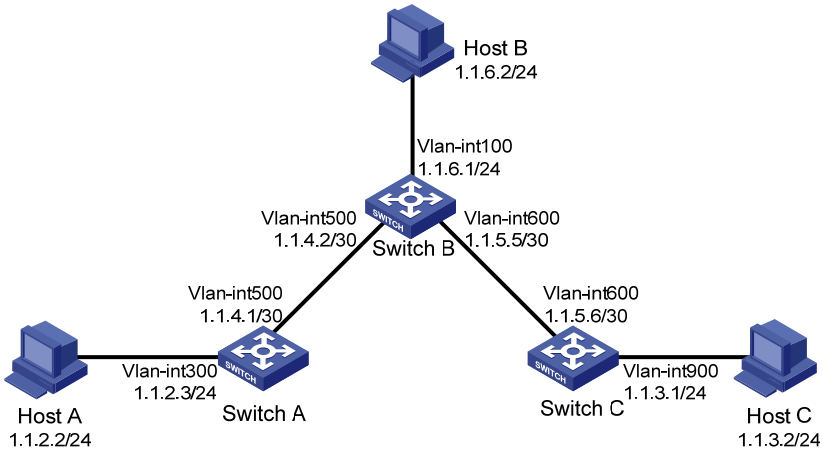
1.8.1 静态路由基本功能配置举例

1. 组网需求

交换机各接口及主机的IP地址和掩码如 图 1-2 所示。要求采用静态路由，使图中任意两台主机之间都能互通。

2. 组网图

图1-2 静态路由基本功能配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置静态路由

在 Switch A 上配置缺省路由。

```
<SwitchA> system-view
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
```

在 Switch B 上配置两条静态路由。

```
<SwitchB> system-view
[SwitchB] ip route-static 1.1.2.0 255.255.255.0 1.1.4.1
[SwitchB] ip route-static 1.1.3.0 255.255.255.0 1.1.5.6
```

在 Switch C 上配置缺省路由。

```
<SwitchC> system-view
[SwitchC] ip route-static 0.0.0.0 0.0.0.0 1.1.5.5
```

(3) 配置主机

配置 Host A 的缺省网关为 1.1.2.3，Host B 的缺省网关为 1.1.6.1，Host C 的缺省网关为 1.1.3.1，具体配置过程略。

4. 验证配置

查看 Switch A 的静态路由信息。

```
[SwitchA] display ip routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/0           Static 60   0            1.1.4.2         Vlan500

Static Routing table Status : <Inactive>
Summary Count : 0
```

查看 Switch B 的静态路由信息。

```
[SwitchB] display ip routing-table protocol static

Summary Count : 2

Static Routing table Status : <Active>
Summary Count : 2

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
1.1.2.0/24          Static 60   0            1.1.4.1         Vlan500
1.1.3.0/24          Static 60   0            1.1.5.6         Vlan600

Static Routing table Status : <Inactive>
Summary Count : 0
```

在 Host B 上使用 **ping** 命令验证 Host A 是否可达（假定主机安装的操作系统为 Windows XP）。

```
C:\Documents and Settings\Administrator>ping 1.1.2.2

Pinging 1.1.2.2 with 32 bytes of data:

Reply from 1.1.2.2: bytes=32 time=1ms TTL=126
Reply from 1.1.2.2: bytes=32 time=1ms TTL=126
Reply from 1.1.2.2: bytes=32 time=1ms TTL=126
Reply from 1.1.2.2: bytes=32 time=1ms TTL=126

Ping statistics for 1.1.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

在 Host B 上使用 **tracert** 命令验证 Host A 是否可达。

```
C:\Documents and Settings\Administrator>tracert 1.1.2.2

Tracing route to 1.1.2.2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  1.1.6.1
  2    <1 ms    <1 ms    <1 ms  1.1.4.1
  3     1 ms    <1 ms    <1 ms  1.1.2.2

Trace complete.
```

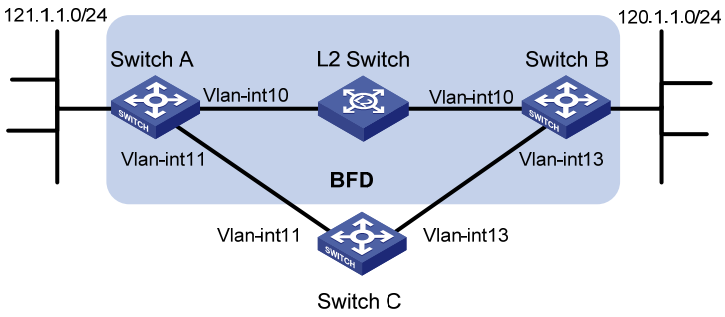
1.8.2 静态路由与BFD联动（直连）配置举例

1. 组网需求

- 在 Switch A 上配置静态路由可以到达 120.1.1.0/24 网段，在 Switch B 上配置静态路由可以到达 121.1.1.0/24 网段，并都使能 BFD 检测功能。
- 在 Switch C 上配置静态路由可以到达 120.1.1.0/24 网段和 121.1.1.0/24 网段。
- 当 Switch A 和 Switch B 通过 L2 Switch 通信的链路出现故障时，BFD 能够快速感知，并且切换到 Switch C 进行通信。

2. 组网图

图1-3 静态路由与 BFD 联动（直连）配置组网图



设备	接口	IP地址	设备	接口	IP地址
Switch A	Vlan-int10	12.1.1.1/24	Switch B	Vlan-int10	12.1.1.2/24
	Vlan-int11	10.1.1.102/24		Vlan-int13	13.1.1.1/24
Switch C	Vlan-int11	10.1.1.100/24			
	Vlan-int13	13.1.1.2/24			

3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置静态路由和 BFD

在 Switch A 上配置静态路由，并使能 BFD 检测功能，使用双向检测方式。

```
<SwitchA> system-view
```

```
[SwitchA] interface vlan-interface 10
[SwitchA-vlan-interface10] bfd min-transmit-interval 500
[SwitchA-vlan-interface10] bfd min-receive-interval 500
[SwitchA-vlan-interface10] bfd detect-multiplier 9
[SwitchA-vlan-interface10] quit
[SwitchA] ip route-static 120.1.1.0 24 vlan-interface 10 12.1.1.2 bfd control-packet
[SwitchA] ip route-static 120.1.1.0 24 vlan-interface 11 10.1.1.100 preference 65
[SwitchA] quit
```

在 Switch B 上配置静态路由，并使能 BFD 检测功能，使用双向检测方式。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 10
[SwitchB-vlan-interface10] bfd min-transmit-interval 500
[SwitchB-vlan-interface10] bfd min-receive-interval 500
[SwitchB-vlan-interface10] bfd detect-multiplier 9
[SwitchB-vlan-interface10] quit
[SwitchB] ip route-static 121.1.1.0 24 vlan-interface 10 12.1.1.1 bfd control-packet
[SwitchB] ip route-static 121.1.1.0 24 vlan-interface 13 13.1.1.2 preference 65
[SwitchB] quit
```

在 Switch C 上配置静态路由。

```
<SwitchC> system-view
[SwitchC] ip route-static 120.1.1.0 24 13.1.1.1
[SwitchC] ip route-static 121.1.1.0 24 10.1.1.102
```

4. 验证配置

下面以 Switch A 为例，Switch B 和 Switch A 类似，不再赘述。

查看 BFD 会话，可以看到 BFD 会话已经创建。

```
<SwitchA> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 Session Working Under Ctrl Mode:

 LD/RD          SourceAddr      DestAddr        State    Holdtime    Interface
 4/7            12.1.1.1        12.1.1.2        Up       2000ms      Vlan10
```

查看静态路由，可以看到 Switch A 经过 L2 Switch 到达 Switch B。

```
<SwitchA> display ip routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
120.1.1.0/24        Static 60   0            12.1.1.2        Vlan10

Static Routing table Status : <Inactive>
Summary Count : 0
```

当 Switch A 和 Switch B 通过 L2 Switch 通信的链路出现故障时：

查看静态路由，可以看到 Switch A 经过 Switch C 到达 Switch B。

```
<SwitchA> display ip routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination/Mask    Proto  Pre  Cost          NextHop         Interface
120.1.1.0/24        Static 65   0             10.1.1.100      Vlan11

Static Routing table Status : <Inactive>
Summary Count : 0
```

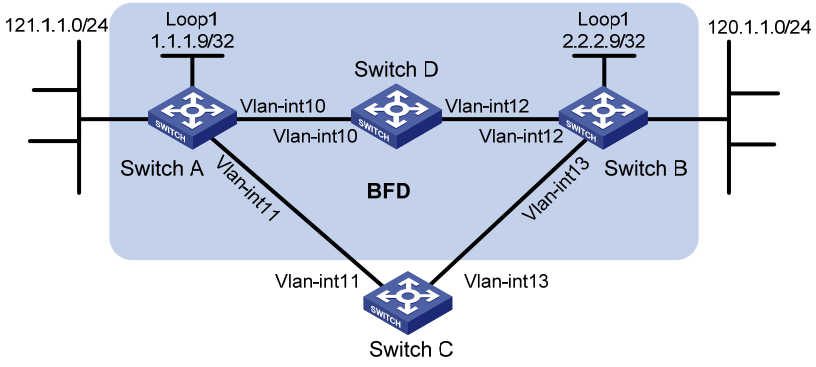
1.8.3 静态路由与BFD联动（非直连）配置举例

1. 组网需求

- 在 Switch A 上配置静态路由可以到达 120.1.1.0/24 网段，在 Switch B 上配置静态路由可以到达 121.1.1.0/24 网段，并都使能 BFD 检测功能。
- 在 Switch C 和 Switch D 上配置静态路由可以到达 120.1.1.0/24 网段和 121.1.1.0/24 网段。
- Switch A 存在到 Switch B 的接口 Loopback1（2.2.2.9/32）的路由，出接口为 Vlan-interface10；Switch B 存在到 Switch A 的接口 Loopback1（1.1.1.9/32）的路由，出接口为 Vlan-interface12；Switch D 存在到 1.1.1.9/32 的路由，出接口为 Vlan-interface10，存在到 2.2.2.9/32 的路由，出接口为 Vlan-interface12。
- 当 Switch A 和 Switch B 通过 Switch D 通信的链路出现故障时，BFD 能够快速感知，并且切换到 Switch C 进行通信。

2. 组网图

图1-4 静态路由与 BFD 联动（非直连）配置组网图



设备	接口	IP地址	设备	接口	IP地址
Switch A	Vlan-int10	12.1.1.1/24	Switch B	Vlan-int12	11.1.1.1/24
	Vlan-int11	10.1.1.102/24		Vlan-int13	13.1.1.1/24
	Loop1	1.1.1.9/32		Loop1	2.2.2.9/32

设备	接口	IP地址	设备	接口	IP地址
Switch C	Vlan-int11	10.1.1.100/24	Switch D	Vlan-int10	12.1.1.2/24
	Vlan-int13	13.1.1.2/24		Vlan-int12	11.1.1.2/24

3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置静态路由和 BFD

在 Switch A 上配置静态路由，并使能 BFD 检测功能，使用双向检测方式。

```
<SwitchA> system-view
[SwitchA] bfd multi-hop min-transmit-interval 500
[SwitchA] bfd multi-hop min-receive-interval 500
[SwitchA] bfd multi-hop detect-multiplier 9
[SwitchA] ip route-static 120.1.1.0 24 2.2.2.9 bfd control-packet bfd-source 1.1.1.9
[SwitchA] ip route-static 120.1.1.0 24 vlan-interface 11 10.1.1.100 preference 65
[SwitchA] quit
```

在 Switch B 上配置静态路由，并使能 BFD 检测功能，使用双向检测方式。

```
<SwitchB> system-view
[SwitchB] bfd multi-hop min-transmit-interval 500
[SwitchB] bfd multi-hop min-receive-interval 500
[SwitchB] bfd multi-hop detect-multiplier 9
[SwitchB] ip route-static 121.1.1.0 24 1.1.1.9 bfd control-packet bfd-source 2.2.2.9
[SwitchB] ip route-static 121.1.1.0 24 vlan-interface 13 13.1.1.2 preference 65
[SwitchB] quit
```

在 Switch C 上配置静态路由。

```
<SwitchC> system-view
[SwitchC] ip route-static 120.1.1.0 24 13.1.1.1
[SwitchC] ip route-static 121.1.1.0 24 10.1.1.102
```

在 Switch D 上配置静态路由。

```
<SwitchD> system-view
[SwitchD] ip route-static 120.1.1.0 24 11.1.1.1
[SwitchD] ip route-static 121.1.1.0 24 12.1.1.1
```

4. 验证配置

下面以 Switch A 为例，Switch B 和 Switch A 类似，不再赘述。

查看 BFD 会话，可以看到 BFD 会话已经创建。

```
<SwitchA> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 Session Working Under Ctrl Mode:

 LD/RD          SourceAddr      DestAddr        State    Holdtime    Interface
 4/7            1.1.1.9         2.2.2.9         Up       2000ms      N/A
```

查看静态路由，可以看到 Switch A 经过 Switch D 到达 Switch B。

```
<SwitchA> display ip routing-table protocol static
```

```
Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
120.1.1.0/24        Static 60   0            12.1.1.2        Vlan10

Static Routing table Status : <Inactive>
Summary Count : 0
```

当 Switch A 和 Switch B 通过 Switch D 通信的链路出现故障时：

查看静态路由，可以看到 Switch A 经过 Switch C 到达 Switch B。

```
<SwitchA> display ip routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
120.1.1.0/24        Static 65   0            10.1.1.100      Vlan11

Static Routing table Status : <Inactive>
Summary Count : 0
```

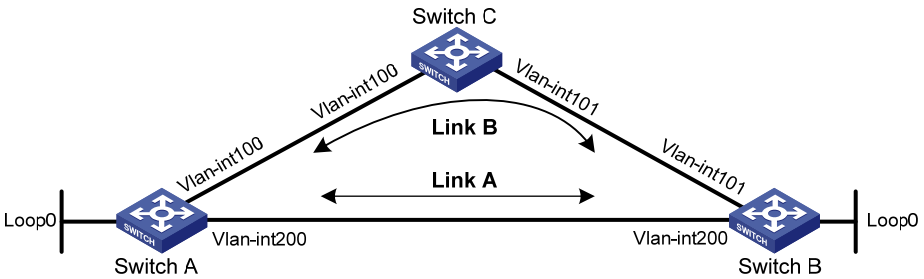
1.8.4 静态路由快速重路由配置举例

1. 组网需求

如 图 1-5 所示，Switch A、Switch B和Switch C通过静态路由实现网络互连。要求当Switch A和Switch B之间的链路A出现单通故障时，业务可以快速切换到链路B上。

2. 组网图

图1-5 静态路由快速重路由配置组网图



设备	接口	IP地址	设备	接口	IP地址
Switch A	Vlan-int100	12.12.12.1/24	Switch B	Vlan-int101	24.24.24.4/24
	Vlan-int200	13.13.13.1/24		Vlan-int200	13.13.13.2/24
	Loop0	1.1.1.1/32		Loop0	4.4.4.4/32

设备	接口	IP地址	设备	接口	IP地址
Switch C	Vlan-int100	12.12.12.2/24			
	Vlan-int101	24.24.24.2/24			

3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置链路 A 上的静态路由快速重路由

静态路由支持快速重路由配置有两种方法，可以任选一种

方法一：配置静态路由快速重路由功能（手工指定备份下一跳）

在 Switch A 上配置静态路由，并指定备份出接口和下一跳。

```
<SwitchA> system-view
[SwitchA] ip route-static 4.4.4.4 32 vlan-interface 200 13.13.13.2 backup-interface
vlan-interface 100 backup-nexthop 12.12.12.2
[SwitchA] ip route-static 4.4.4.4 32 vlan-interface 100 12.12.12.2 preference 70
```

在 Switch B 上配置静态路由，并指定备份出接口和下一跳。

```
<SwitchB> system-view
[SwitchB] ip route-static 1.1.1.1 32 vlan-interface 200 13.13.13.1 backup-interface
vlan-interface 101 backup-nexthop 24.24.24.2
[SwitchB] ip route-static 1.1.1.1 32 vlan-interface 101 24.24.24.2 preference 70
```

方法二：配置静态路由快速重路由功能（自动查找备份下一跳）

在 Switch A 上配置静态路由，并配置静态路由自动快速重路由功能。

```
<SwitchA> system-view
[SwitchA] ip route-static 4.4.4.4 32 vlan-interface 200 13.13.13.2
[SwitchA] ip route-static 4.4.4.4 32 vlan-interface 100 12.12.12.2 preference 70
[SwitchA] ip route-static fast-reroute auto
```

在 Switch B 上配置静态路由，并配置静态路由自动快速重路由功能。

```
<SwitchB> system-view
[SwitchB] ip route-static 1.1.1.1 32 vlan-interface 200 13.13.13.1
[SwitchB] ip route-static 1.1.1.1 32 vlan-interface 101 24.24.24.2 preference 70
[SwitchB] ip route-static fast-reroute auto
```

(3) 配置链路 B 上的静态路由

在 Switch C 上配置静态路由。

```
<SwitchC> system-view
[SwitchC] ip route-static 4.4.4.4 32 vlan-interface 101 24.24.24.4
[SwitchC] ip route-static 1.1.1.1 32 vlan-interface 100 12.12.12.1
```

4. 验证配置

在 Switch A 上查看 4.4.4.4/32 路由，可以看到备份下一跳信息。

```
[SwitchA] display ip routing-table 4.4.4.4 verbose

Summary Count : 1

Destination: 4.4.4.4/32
   Protocol: Static
 Process ID: 0
```

```
  SubProtID: 0x0                    Age: 04h20m37s
       Cost: 0                Preference: 60
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x26000002          LastAs: 0
     AttrID: 0xffffffff         Neighbor: 0.0.0.0
      Flags: 0x1008c         OrigNextHop: 13.13.13.2
      Label: NULL            RealNextHop: 13.13.13.2
    BkLabel: NULL              BkNextHop: 12.12.12.2
  Tunnel ID: Invalid           Interface: Vlan-interface200
BkTunnel ID: Invalid         BkInterface: Vlan-interface100
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A
```

在 Switch B 上查看 1.1.1.1/32 路由，可以看到备份下一跳信息。

```
[SwitchB] display ip routing-table 1.1.1.1 verbose

Summary Count : 1

Destination: 1.1.1.1/32
   Protocol: Static
 Process ID: 0
  SubProtID: 0x0                    Age: 04h20m37s
       Cost: 0                Preference: 60
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x26000002          LastAs: 0
     AttrID: 0xffffffff         Neighbor: 0.0.0.0
      Flags: 0x1008c         OrigNextHop: 13.13.13.1
      Label: NULL            RealNextHop: 13.13.13.1
    BkLabel: NULL              BkNextHop: 24.24.24.2
  Tunnel ID: Invalid           Interface: Vlan-interface200
BkTunnel ID: Invalid         BkInterface: Vlan-interface101
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A
```

2 缺省路由

缺省路由是在路由器没有找到匹配的路由表项时使用的路由。

如果报文的目的地不在路由表中且没有配置缺省路由，那么该报文将被丢弃，将向源端返回一个 ICMP 报文报告该目的地址或网络不可达。

缺省路由有两种生成方式：

- 第一种是网络管理员手工配置。配置请参见“1.2 配置静态路由”，将目的地址与掩码配置为全零（0.0.0.0 0.0.0.0）。
- 第二种是动态路由协议生成（如 OSPFRIP），由路由能力比较强的路由器将缺省路由发布给其它路由器，其它路由器在自己的路由表里生成指向那台路由器的缺省路由。配置请参见各个路由协议手册。

目 录

1 RIP

1.1 RIP简介

RIP（Routing Information Protocol，路由信息协议）是一种基于距离矢量（Distance-Vector）算法的内部网关协议（Interior Gateway Protocol，IGP），它通过 UDP 报文进行路由信息的交换，使用的端口号为 520。RIP 适用于小型网络。

1.1.1 RIP的路由度量值

RIP 使用跳数来衡量到达目的地址的距离，跳数称为度量值。在 RIP 中，路由器到与它直接相连网络的跳数为 0，通过一个路由器可达的网络的跳数为 1，其余依此类推。为限制收敛时间，RIP 规定度量值取 0～15 之间的整数，大于或等于 16 的跳数被定义为无穷大，即目的网络或主机不可达。由于这个限制，使得 RIP 不适合应用于大型网络。

1.1.2 RIP的路由数据库

每个运行 RIP 的路由器管理一个路由数据库，该路由数据库包含了到所有可达目的地的路由项，这些路由项包含下列信息：

- 目的地址：主机或网络的地址。
- 下一跳地址：为到达目的地，需要经过的相邻路由器的接口 IP 地址。
- 出接口：本路由器转发报文的出接口。
- 度量值：本路由器到达目的地的开销。
- 路由时间：从路由项最后一次被更新到现在所经过的时间，路由项每次被更新时，路由时间重置为 0。
- 路由标记（Route Tag）：用于标识外部路由，在路由策略中可根据路由标记对路由信息进行灵活的控制。关于路由策略的详细信息，请参见“三层技术-IP 路由配置指导”中的“路由策略”。

1.1.3 RIP的运行过程

RIP 的运行过程如下：

(1) 路由器启动 RIP 后，便会向相邻的路由器发送请求报文（Request message），相邻的 RIP 路由器收到请求报文后，响应该请求，回送包含本地路由表信息的响应报文（Response message）。

(2) 路由器收到响应报文后，更新本地路由表，同时向相邻路由器发送触发更新报文，通告路由更新信息。相邻路由器收到触发更新报文后，又向其各自的相邻路由器发送触发更新报文。在一连串的触发更新广播后，各路由器都能得到并保持最新的路由信息。

(3) 路由器周期性向相邻路由器发送本地路由表，运行 RIP 协议的相邻路由器在收到报文后，对本地路由进行维护，选择一条最佳路由，再向其各自相邻网络发送更新信息，使更新的路由

最终能达到全局有效。同时，RIP 采用老化机制对超时的路由进行老化处理，以保证路由的实时性和有效性。

1.1.4 RIP防止路由环路的机制

RIP 协议向邻居通告的是自己的路由表，有可能会发生路由环路，可以通过以下机制来避免：

- 计数到无穷（Counting to infinity）：将度量值等于 16 的路由定义为不可达（infinity）。在路由环路发生时，某条路由的度量值将会增加到 16，该路由被认为不可达。
- 触发更新（Triggered Updates）：RIP 通过触发更新来避免在多个路由器之间形成路由环路的可能，而且可以加速网络的收敛速度。一旦某条路由的度量值发生了变化，就立刻向邻居路由器发布更新报文，而不是等到更新周期的到来。
- 水平分割（Split Horizon）：RIP 从某个接口学到的路由，不会从该接口再发回给邻居路由器。这样不但减少了带宽消耗，还可以防止路由环路。
- 毒性逆转（Poison Reverse）：RIP 从某个接口学到路由后，将该路由的度量值设置为 16（不可达），并从原接口发回邻居路由器。利用这种方式，可以清除对方路由表中的无用信息。

1.1.5 RIP的版本

RIP 有两个版本：RIP-1 和 RIP-2。

RIP-1 是有类别路由协议（Classful Routing Protocol），它只支持以广播方式发布协议报文。RIP-1 的协议报文无法携带掩码信息，它只能识别 A、B、C 类这样的自然网段的路由，因此 RIP-1 不支持不连续子网（Discontiguous Subnet）。

RIP-2 是一种无类别路由协议（Classless Routing Protocol），与 RIP-1 相比，它有以下优势：

- 支持路由标记，在路由策略中可根据路由标记对路由进行灵活的控制。
- 报文中携带掩码信息，支持路由聚合和 CIDR（Classless Inter-Domain Routing，无类域间路由）。
- 支持指定下一跳，在广播网上可以选择到最优下一跳地址。
- 支持组播路由发送更新报文，只有 RIP-2 路由器才能收到更新报文，减少资源消耗。
- 支持对协议报文进行验证，并提供明文验证和 MD5 验证两种方式，增强安全性。

RIP-2 有两种报文传送方式：广播方式和组播方式，缺省将采用组播方式发送报文，使用的组播地址为 224.0.0.9。当接口运行 RIP-2 广播方式时，也可接收 RIP-1 的报文。

1.1.6 协议规范

与 RIP 相关的协议规范有：

- RFC 1058：Routing Information Protocol
- RFC 1723：RIP Version 2 - Carrying Additional Information
- RFC 1721：RIP Version 2 Protocol Analysis
- RFC 1722：RIP Version 2 Protocol Applicability Statement
- RFC 1724：RIP Version 2 MIB Extension
- RFC 2082：RIP-2 MD5 Authentication
- RFC 2091：Triggered Extensions to RIP to Support Demand Circuits

- RFC 2453：RIP Version 2

1.2 RIP与硬件适配关系

S5000V3-EI、S5000E-X 系列交换机不支持 RIP。

1.3 RIP配置任务简介

RIP 配置任务如下：

(1) 配置RIP的基本功能

a. 启动RIP

b. （可选）配置接口的工作状态

c. （可选）配置RIP版本

d. 配置RIP邻居

如果在不支持广播或组播报文的链路上运行 RIP，则必须手工指定 RIP 的邻居。

(2) （可选）配置RIP的路由信息控制

- 配置接口附加度量值
- 配置RIP-2 路由聚合
- 禁止RIP接收主机路由
- 配置RIP发布缺省路由
- 配置RIP对接收/发布的路由进行过滤
- 配置RIP协议优先级
- 配置RIP引入外部路由

(3) （可选）调整和优化RIP网络

- 配置RIP定时器
- 配置水平分割和毒性逆转
- 配置RIP触发更新的时间间隔
- 配置RIP报文的发送速率
- 配置RIP报文的最大长度
- 配置RIP发送协议报文的DSCP优先级

(4) （可选）配置RIP网管功能

(5) （可选）提高 RIP 的可靠性

- 配置RIP GR
- 配置RIP NSR
- 配置RIP与BFD联动
- 配置RIP快速重路由功能

(6) （可选）提高RIP的安全性

- 配置RIP-1 报文的零域检查
- 配置源地址检查

1.4 配置RIP的基本功能

1.4.1 配置限制和指导

目前，系统支持 RIP 多进程。当在一台路由器上启动多个 RIP 进程时，需要指定不同的进程号。RIP 进程号是本地概念，不影响与其它路由器之间的报文交换。因此，不同的路由器之间，即使进程号不同也可以进行报文交换。

1.4.2 启动RIP

1. 功能简介

RIP 只在指定网段的接口上运行，指定网段的同时可以配置反码；对于不在指定网段上的接口，RIP 既不在它上面接收和发送路由，也不将它的接口路由发布出去。因此，RIP 启动后必须指定其工作网段。

2. 配置限制和指导

- 启动 RIP 前在接口视图下配置了 RIP 相关命令，这些配置只有在 RIP 启动后才会生效。
- RIP 不支持将同一物理接口下的不同网段使能到不同的 RIP 进程中。
- RIP 不支持在同一物理接口下使能多个 RIP 进程。
- 在指定接口上使能 RIP 的优先级高于在指定网段上使能 RIP。

3. 在指定网段上使能RIP

(1) 进入系统视图。

system-view

(2) 启动 RIP，并进入 RIP 视图。

rip [*process-id*]

缺省情况下，系统没有启动 RIP。

(3) 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。

在单进程情况下，可以使用 **network** 0.0.0.0 命令在所有接口上使能 RIP。在多进程情况下，无法使用 **network** 0.0.0.0 命令。

4. 在指定接口上使能RIP

(1) 进入系统视图。

system-view

(2) 启动 RIP，并进入 RIP 视图。

rip [*process-id*]

缺省情况下，系统没有启动 RIP。

(3) 退回系统视图。

quit

(4) 进入接口视图。

interface *interface-type interface-number*

(5) 在指定接口上使能 RIP。

rip *process-id* **enable** [**exclude-subip**]

缺省情况下，接口上没有使能 RIP。

1.4.3 配置接口的工作状态

1. 功能简介

可对接口的工作状态进行配置，具体包括：

- 配置接口工作在抑制状态，即接口只接收 RIP 报文而不发送 RIP 报文。
- 配置禁止接口接收 RIP 报文。
- 配置禁止接口发送 RIP 报文。

2. 配置限制和指导

silent-interface 命令用来抑制接口，使其只接收 RIP 报文，更新自己的路由表，但不发送 RIP 报文。命令 **silent-interface** 比命令 **rip input** 和 **rip output** 的优先级都高。**silent-interface all** 表示抑制所有接口，在配置该命令后，所有接口都被抑制，**rip input** 和 **rip output** 将不会生效。

3. 配置接口工作在抑制状态

(1) 进入系统视图。

system-view

(2) 进入 RIP 视图。

rip [*process-id*]

(3) 配置抑制接口。

silent-interface { *interface-type interface-number* | **all** }

缺省情况下，允许所有接口发送路由更新报文。

若抑制接口收到非知名端口的单播请求，会发送响应报文。

4. 配置禁止接口接收RIP报文

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置禁止接口接收 RIP 报文。

undo rip input

缺省情况下，允许接口接收 RIP 报文。

5. 配置禁止接口发送RIP报文

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置禁止接口发送 RIP 报文。

undo rip output

缺省情况下，允许接口发送 RIP 报文。

1.4.4 配置RIP版本

1. 功能简介

用户可以在 RIP 视图下配置 RIP 版本，也可在接口上配置 RIP 版本：

- 当全局和接口都没有进行 RIP 版本配置时，接口发送 RIP-1 广播报文，可以接收 RIP-1 广播/单播报文、RIP-2 广播/组播/单播报文。
- 如果接口上配置了 RIP 版本，以接口配置的为准；如果接口没有进行 RIP 版本配置，接口运行的 RIP 版本将以全局配置的版本为准。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 RIP 版本。

- 请依次执行以下命令在 RIP 视图下配置 RIP 版本。

  rip [*process-id*]

  version { **1** | **2** }

  缺省情况下，未配置全局 RIP 版本。接口只能发送 RIP-1 广播报文，可以接收 RIP-1 广播/单播报文、RIP-2 广播/组播/单播报文。

- 请依次执行以下命令在接口视图下配置 RIP 版本。

  interface *interface-type interface-number*

  rip version { **1** | **2** [**broadcast** | **multicast**] }

  缺省情况下，未配置接口运行的 RIP 版本。接口只能发送 RIP-1 广播报文，可以接收 RIP-1 广播/单播报文、RIP-2 广播/组播/单播报文。

1.4.5 配置RIP邻居

1. 功能简介

通常情况下，RIP 使用广播或组播地址发送报文，如果在不支持广播或组播报文的链路上运行 RIP，则必须手工指定 RIP 的邻居。

2. 配置限制和指导

当 RIP 邻居与当前设备直连时不推荐使用 **peer** *ip-address* 命令，因为这样可能会造成对端同时收到同一路由信息的组播（或广播）和单播两种形式的报文。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 RIP 视图。

rip [*process-id*]

(3) 配置 RIP 邻居。

peer *ip-address*

缺省情况下，RIP 不向任何定点地址发送单播更新报文。

(4) 关闭对接收到的 RIP 路由更新报文进行源 IP 地址检查的功能。

undo validate-source-address

缺省情况下，对接收到的 RIP 路由更新报文进行源 IP 地址检查的功能处于使能状态。

当指定的邻居和本地路由器非直接连接，则必须关闭对更新报文的源地址进行检查的功能。

1.5 配置RIP的路由信息控制

1.5.1 配置接口附加度量值

1. 功能简介

附加度量值是在 RIP 路由原来度量值的基础上所增加的度量值（跳数），包括发送附加度量值和接收附加度量值。

- 发送附加度量值：不会改变路由表中的路由度量值，仅当接口发送 RIP 路由信息时才会添加到发送路由上。
- 接收附加度量值：会影响接收到的路由度量值，接口接收到一条合法的 RIP 路由时，在将其加入路由表前会把度量值附加到该路由上，当附加度量值与原路由度量值之和大于 16 时，该条路由的度量值取 16。

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) 配置接口接收 RIP 路由时的附加度量值。

rip metricin [**route-policy** *route-policy-name*] *value*

缺省情况下，接口接收 RIP 路由时的附加路由度量值为 0。

(4) 配置接口发送 RIP 路由时的附加度量值。

rip metricout [**route-policy** *route-policy-name*] *value*

缺省情况下，接口发送 RIP 路由时的附加路由度量值为 1。

1.5.2 配置RIP-2 路由聚合

1. 功能简介

路由聚合是指路由器把同一自然网段内的连续子网的路由聚合成一条路由向外发送，如路由表里有 10.1.1.0/24、10.1.2.0/24、10.1.3.0/24 三条路由，可以通过配置把它们聚合成一条路由 10.1.0.0/16

向外发送，这样邻居路由器只接收到一条路由 10.1.0.0/16，从而减少了路由表的规模，以及网络上的传输流量。

通过配置路由聚合，可以提高网络的可扩展性以及路由器的处理速度。

RIP-2 将多条路由聚合成一条路由时，聚合路由的 Metric 值将取所有路由 Metric 的最小值。

在 RIP-2 中，有两种路由聚合方式：自动路由聚合和手工配置聚合路由。

- 自动路由聚合是指 RIP-2 将同一自然网段内的不同子网的路由聚合成一条自然掩码的路由向外发送，例如，假设路由表里有 10.1.1.0/24、10.1.2.0/24、10.1.3.0/24 三条路由，使能 RIP-2 自动路由聚合功能后，这三条路由聚合成一条自然掩码的路由 10.0.0.0/8 向外发送。
- 手工路由聚合是指用户可在指定接口配置 RIP-2 发布一条聚合路由。如果路由落入聚合路由网段内，则 RIP-2 不发布该路由，只发布配置的聚合路由。例如，假设路由表里有 10.1.1.0/24、10.1.2.0/24、10.1.3.0/24 三条子网连续的路由，在接口 GigabitEthernet1/0/1 配置发布一条聚合路由 10.1.0.0/16 后，这三条路由聚合成一条路由 10.1.0.0/16 向外发送。缺省情况下，RIP-2 的路由将按照自然掩码自动聚合，如果用户在指定接口配置发布一条聚合路由，则必须先关闭自动聚合功能。

2. 配置限制和指导

路由聚合在某些情况会产生路由环路，所以在路由聚合时需要配置出接口为 NULL0 的黑洞路由。报文匹配到黑洞路由时，直接丢弃该报文，避免产生环路。

3. 自动路由聚合

(1) 进入系统视图。

system-view

(2) 进入 RIP 视图。

rip [*process-id*]

(3) 使能 RIP-2 自动路由聚合功能。

summary

缺省情况下，RIP-2 自动路由聚合功能处于使能状态。

如果路由表里的路由子网不连续，则需要取消自动路由聚合功能，使得 RIP-2 能够向外发布子网路由和主机路由。

4. 手工配置聚合路由

(1) 进入系统视图。

system-view

(2) 进入 RIP 视图。

rip [*process-id*]

(3) 关闭 RIP-2 自动路由聚合功能。

undo summary

缺省情况下，RIP-2 自动路由聚合功能处于使能状态。

(4) 退回系统视图。

quit

(5) 进入接口视图。

interface *interface-type interface-number*

(6) 配置发布一条聚合路由。

rip summary-address *ip-address* { *mask-length* | *mask* }

缺省情况下，未配置聚合路由。

1.5.3 禁止RIP接收主机路由

1. 功能简介

在某些特殊情况下，路由器会收到大量来自同一网段的主机路由。这些路由对于路由寻址没有多少作用，却占用了大量的资源，此时可配置 RIP 禁止接收主机路由，以节省网络资源。功能仅对 RIPv2 报文携带的路由有效，对 RIPv1 报文携带的路由无效。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 RIP 视图。

rip [*process-id*]

(3) 禁止 RIP 接收主机路由。

undo host-route

缺省情况下，允许 RIP 接收主机路由。

1.5.4 配置RIP发布缺省路由

1. 功能简介

用户可以配置 RIP 以指定度量值向邻居发布一条缺省路由。

- 用户可以在 RIP 视图下配置 RIP 进程的所有接口向邻居发布缺省路由，也可以在接口下配置指定 RIP 接口向邻居发布缺省路由。
- 如果接口没有进行发布缺省路由的相关配置，则以 RIP 进程下的配置为准，否则将以接口配置为准。
- 如果 RIP 进程配置了发布缺省路由，但希望该进程下的某个接口不发送缺省路由（只发布普通路由），可以通过在接口下配置 **rip default-route no-originate** 命令实现。

配置发布缺省路由的 RIP 路由器不接收来自 RIP 邻居的缺省路由。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 RIP 发布缺省路由。

- 请依次执行以下命令在 RIP 视图下配置发布缺省路由。

  rip [*process-id*]

  default-route { **only** | **originate** } [**cost** *cost-value* | **route-policy** *route-policy-name*] *

  缺省情况下，RIP 不向邻居发送缺省路由。

- 请依次执行以下命令在接口视图下配置发布缺省路由。

  interface *interface-type interface-number*

  rip default-route { { **only** | **originate** } [**cost** *cost-value* | **route-policy** *route-policy-name*] * | **no-originate** }

  缺省情况下，RIP 接口是否发布缺省路由以 RIP 进程配置的为准。

1.5.5 配置RIP对接收/发布的路由进行过滤

1. 功能简介

路由过滤就是通过指定访问控制列表或 IP 地址前缀列表，配置入口或出口过滤策略，对接收和发布的路由进行过滤。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 RIP 视图。

rip [*process-id*]

(3) 对接收的路由信息进行过滤。

filter-policy { *ipv4-acl-number* | **gateway** *prefix-list-name* | **prefix-list** *prefix-list-name* [**gateway** *prefix-list-name*] } **import** [*interface-type interface-number*]

缺省情况下，RIP 不对接收的路由信息进行过滤。

本命令对从邻居收到的 RIP 路由进行过滤，没有通过过滤的路由将不被加入路由表，也不向邻居发布该路由。

(4) 对发布的路由信息进行过滤。

filter-policy { *ipv4-acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*] | *interface-type interface-number*]

缺省情况下，RIP 不对发布的路由信息进行过滤。

本命令对本机所有路由的发布进行过滤，包括使用 **import-route** 引入的路由和从邻居学到的 RIP 路由。

1.5.6 配置RIP协议优先级

1. 功能简介

在路由器中可能会运行多个 IGP 路由协议，如果想让 RIP 路由具有比从其它路由协议学来的路由更高的优先级，需要配置小的优先级值。优先级的高低将最后决定 IP 路由表中的路由是通过哪种路由算法获取的最佳路由。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 RIP 视图。

rip [*process-id*]

(3) 配置 RIP 路由的优先级。

preference { *preference* | **route-policy** *route-policy-name* } *

缺省情况下，RIP 路由的优先级为 100。

1.5.7 配置RIP引入外部路由

1. 功能简介

如果在路由器上不仅运行 RIP，还运行着其它路由协议，可以配置 RIP 引入其它协议生成的路由，如 OSPF、静态路由或者直连路由。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 RIP 视图。

rip [*process-id*]

(3) 引入外部路由。

- 配置 RIP 引入直连或静态路由。

  import-route { **direct** | **static** } [**cost** *cost-value* | **route-policy** *route-policy-name* | **tag** *tag*] *

- 配置 RIP 引入 **ospf** 协议或其他 **rip** 进程的路由。

  import-route { **ospf** | **rip** } [*process-id* | **all-processes**] [**allow-direct** | **cost** *cost-value* | **route-policy** *route-policy-name* | **tag** *tag*] *

缺省情况下，RIP 不引入其它路由。

只能引入路由表中状态为 active 的路由，是否为 active 状态可以通过 **display ip routing-table protocol** 命令来查看。

(4) （可选）配置引入路由的缺省度量值。

default cost *cost-value*

缺省情况下，引入路由的缺省度量值为 0。

1.6 调整和优化RIP网络

1.6.1 配置RIP定时器

1. 功能简介

通过调整 RIP 定时器可以改变 RIP 网络的收敛速度。

RIP 受四个定时器的控制，分别是 Update、Timeout、Suppress 和 Garbage-Collect。

- Update 定时器：定义了发送路由更新的时间间隔。
- Timeout 定时器：定义了路由老化时间。如果在老化时间内没有收到关于某条路由的更新报文，则该条路由在路由表中的度量值将会被设置为 16。

- Suppress 定时器：定义了 RIP 路由处于抑制状态的时长。当一条路由的度量值变为 16 时，该路由将进入抑制状态。在被抑制状态，只有来自同一邻居且度量值小于 16 的路由更新才会被路由器接收，取代不可达路由。
- Garbage-Collect 定时器：定义了一条路由从度量值变为 16 开始，直到它从路由表里被删除所经过的时间。在 Garbage-Collect 时间内，RIP 以 16 作为度量值向外发送这条路由的更新，如果 Garbage-Collect 超时，该路由仍没有得到更新，则该路由将从路由表中被彻底删除。

2. 配置限制和指导

定时器值的调整应考虑网络的性能，并在所有运行 RIP 的路由器上进行统一配置，以免增加不必要的网络流量或引起网络路由震荡。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 RIP 视图。

rip [*process-id*]

(3) 配置 RIP 定时器的值。

timers { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* } *

缺省情况下，Garbage-collect 定时器的值为 120 秒，Suppress 定时器的值为 120 秒，Timeout 定时器的值为 180 秒，Update 定时器的值为 30 秒。

1.6.2 配置水平分割和毒性逆转

1. 功能简介

通过配置水平分割或毒性逆转功能可以防止路由环路。

- 配置水平分割可以使得从一个接口学到的路由不能通过此接口向外发布，用于避免相邻路由器间的路由环路。
- 配置毒性逆转后，从一个接口学到的路由还可以从这个接口向外发布，但这些路由的度量值会设置为 16（即不可达），可以用于避免相邻路由器间的路由环路。

2. 配置限制和指导

如果同时配置了水平分割和毒性逆转，则只有毒性逆转功能生效。

3. 配置水平分割

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 使能水平分割功能。

rip split-horizon

缺省情况下，水平分割功能处于使能状态。

4. 配置毒性逆转

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 使能毒性逆转功能。

rip poison-reverse

缺省情况下，毒性逆转功能处于关闭状态。

1.6.3 配置RIP触发更新的时间间隔

1. 功能简介

RIP 路由信息变化后将以触发更新的方式通知邻居设备，加速邻居设备的路由收敛。如果路由信息频繁变化，且每次变化都立即发送触发更新，将会占用大量系统资源，并影响路由器的效率。通过调节触发更新的时间间隔，可以抑制由于路由信息频繁变化带来的影响。本命令在路由信息变化不频繁的情况下将连续触发更新的时间间隔缩小到 *minimum-interval*，而在路由信息变化频繁的情况下可以进行相应惩罚，增加 *incremental-interval*×2^{n-2}（n 为连续触发更新的次数），将等待时间按照配置的惩罚增量延长，最大不超过 *maximum-interval*。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 RIP 视图。

rip [*process-id*]

(3) 配置 RIP 触发更新的时间间隔。

timer triggered *maximum-interval* [*minimum-interval* [*incremental-interval*]]

缺省情况下，发送触发更新的最大时间间隔为 5 秒，最小间隔为 50 毫秒，增量惩罚间隔为 200 毫秒。

1.6.4 配置RIP报文的发送速率

1. 功能简介

RIP 周期性地将路由信息放在 RIP 报文中向邻居发送。

如果路由表里的路由条目数量很多，同时发送大量 RIP 协议报文有可能会对当前设备和网络带宽带来冲击；因此，路由器将 RIP 协议报文分为多个批次进行发送，并且对 RIP 接口每次允许发送的 RIP 协议报文最大个数做出限制。

用户可根据需要配置接口发送 RIP 报文的时间间隔以及接口一次发送 RIP 报文的最大个数。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 RIP 报文的发送速率。

- 请依次执行以下命令在 RIP 视图下配置所有接口的 RIP 报文发送速率。

  rip [*process-id*]

  配置 RIP 报文的发送速率。

  output-delay *time* **count** *count*

  缺省情况下，接口发送 RIP 报文的时间间隔为 20 毫秒，一次最多发送 3 个 RIP 报文。
- 请依次执行以下命令在接口视图下配置某个接口的 RIP 报文发送速率。

  interface *interface-type interface-number*

  配置 RIP 报文的发送速率。

  rip output-delay *time* **count** *count*

  缺省情况下，接口发送 RIP 报文的速率以 RIP 进程配置的为准。

1.6.5 配置RIP报文的最大长度

1. 功能简介

RIP 周期性地将路由信息放在 RIP 报文中向邻居发送，根据 RIP 报文的最大长度来计算报文中发送的最大路由数。通过设置 RIP 报文的最大长度，可以合理利用链路带宽。

在配置认证的情况下，如果配置不当可能会造成报文无法发送，建议用户按照下面进行配置：

- 简单验证方式时，RIP 报文的最大长度不小于 52 字节；
- MD5 验证方式（使用 RFC 2453 规定的报文格式）时，RIP 报文的最大长度不小于 56 字节；
- MD5 验证方式（使用 RFC 2082 规定的报文格式）时，RIP 报文的最大长度不小于 72 字节。

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 RIP 报文的最大长度。

rip max-packet-length *value*

缺省情况下，接口发送 RIP 报文的最大长度为 512 字节。

1.6.6 配置RIP发送协议报文的DSCP优先级

1. 功能简介

DSCP 优先级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 RIP 发送协议报文的 DSCP 优先级。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 RIP 视图。

rip [*process-id*]

(3) 配置 RIP 发送协议报文的 DSCP 优先级。

dscp *dscp-value*

缺省情况下，RIP 发送协议报文的 DSCP 优先级为 48。

1.7 配置RIP网管功能

1. 功能简介

配置 RIP 进程绑定 MIB 功能后，可以通过网管软件对指定的 RIP 进程进行管理。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 RIP 进程绑定 MIB。

rip mib-binding *process-id*

缺省情况下，MIB 绑定在进程号最小的 RIP 进程上。

1.8 配置RIP GR

1. 功能简介

GR（Graceful Restart，平滑重启）是一种在协议重启或主备倒换时 RIP 进行平滑重启，保证转发业务不中断的机制。

GR 有两个角色：

- GR Restarter：发生协议重启或主备倒换事件且具有 GR 能力的设备。
- GR Helper：和 GR Restarter 具有邻居关系，协助完成 GR 流程的设备。

在普通的路由协议重启的情况下，路由器需要重新学习 RIP 路由，并更新 FIB 表，此时会引起网络暂时的中断，基于 RIP 的 GR 可以解决这个问题。

应用了 GR 特性的设备向外发送 RIP 全部路由表请求报文，重新从邻居处学习 RIP 路由，在此期间 FIB 表不变化。在路由协议重启完毕后，设备将重新学到的 RIP 路由下刷给 FIB 表，使该设备的路由信息恢复到重启前的状态。

本配置在 GR Restarter 上进行，启动了 RIP 的设备缺省就是 GR Helper。

2. 配置限制和指导

设备充当 GR Restarter 后不能再配置 RIP NSR 功能。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 RIP 视图。

rip [*process-id*]

(3) 使能 RIP 协议的 GR 能力。

graceful-restart

缺省情况下，RIP 协议的 GR 能力处于关闭状态。

(4) （可选）配置 RIP 协议的 GR 重启间隔时间。

graceful-restart interval *interval*

缺省情况下，RIP 协议的 GR 重启间隔时间为 60 秒。

1.9 配置RIP NSR

1. 功能简介

NSR（Nonstop Routing，不间断路由）通过将 RIP 路由信息从主进程备份到备进程，使设备在发生主备倒换时新主进程可以无缝完成路由的重新生成、下刷，邻接关系不会发生中断，从而避免了主备倒换对转发业务的影响。

GR 特性需要周边设备配合才能完成路由信息的恢复，在网络应用中有一定的限制。NSR 特性不需要周边设备的配合，网络应用更加广泛。

2. 配置限制和指导

设备配置了 RIP NSR 功能后不能再充当 GR Restarter。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 RIP 视图。

rip [*process-id*]

(3) 使能 RIP NSR 功能。

non-stop-routing

缺省情况下，RIP NSR 功能处于关闭状态。

各个进程的 NSR 功能是相互独立的，只对本进程生效。如果存在多个 RIP 进程，建议在各个进程下使能 RIP NSR 功能。

1.10 配置RIP与BFD联动

1.10.1 功能简介

RIP 协议依赖周期性发送路由更新请求作为检测机制，当在指定时间内没有收到路由更新回应时，认为此条路由不再生效，这种方式不能快速响应链路故障。使用 BFD（Bidirectional Forwarding Detection，双向转发检测）检测到链路故障时，RIP 能快速撤销失效路由，减少对其他业务的影响。关于 BFD 的介绍和基本功能配置，请参见“可靠性配置指导”中的“BFD”。

目前 RIP 支持 BFD 提供了下面几种检测方式：

- echo 报文单跳检测方式：直连邻居使用。在对端有 RIP 路由发送时才能建立 BFD 会话。
- 指定目的地址的 echo 报文单跳检测方式：直连邻居使用，并且在接口上直接指定 RIP 邻居的 IP 地址。当该接口使能了 RIP 功能，会建立到指定目的 IP 地址的 BFD 会话。在链路出现单通故障时，本特性可以加快路由收敛速度。链路出现故障时，本端设备不再从该接口收发任何 RIP 报文，链路恢复后，接口将继续发送 RIP 报文。

- control 报文双向检测方式：非直连邻居使用。当两端互有 RIP 路由发送时，且使能 BFD 的接口与接收接口为同一接口，邻居之间才能建立 BFD 会话。

1.10.2 配置限制和指导

rip bfd enable 命令与 **rip bfd enable destination** 命令互斥，不能同时使用。

1.10.3 配置echo报文单跳检测

(1) 进入系统视图。

system-view

(2) 配置 echo 报文源地址。

bfd echo-source-ip *ip-address*

缺省情况下，未配置 echo 报文源地址。

(3) 进入接口视图。

interface *interface-type interface-number*

(4) 使能 RIP 的 BFD 功能。

rip bfd enable

缺省情况下，RIP 的 BFD 功能处于关闭状态。

1.10.4 配置指定目的地址的echo报文单跳检测

1. 配置限制和指导

本特性只检测本端到 RIP 直连邻居的链路的连通状况。配置本特性时，指定的目的地址只能是 RIP 直连邻居的 IP 地址。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 echo 报文源地址。

bfd echo-source-ip *ip-address*

缺省情况下，未配置 echo 报文源地址。

(3) 进入接口视图。

interface *interface-type interface-number*

(4) 使能 RIP 指定目的地址的 BFD 功能。

rip bfd enable destination *ip-address*

缺省情况下，RIP 的 BFD 功能处于关闭状态。

1.10.5 配置control报文双向检测

(1) 进入系统视图。

system-view

(2) 进入 RIP 视图。

rip [*process-id*]

(3) 配置 RIP 邻居。

peer *ip-address*

缺省情况下，RIP 不向任何定点地址发送更新报文。

由于 **peer** 命令与邻居之间没有对应关系，**undo peer** 操作并不能立刻删除邻居，因此不能立刻删除 BFD 会话。

(4) 进入接口视图。

interface *interface-type interface-number*

(5) 使能 RIP 的 BFD 功能。

rip bfd enable

缺省情况下，RIP 的 BFD 功能处于关闭状态。

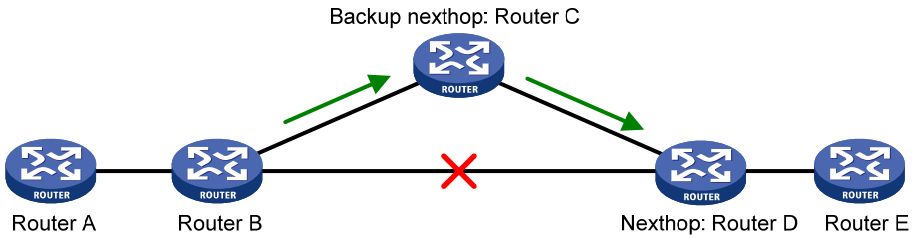
1.11 配置RIP快速重路由功能

1.11.1 功能简介

当 RIP 网络中的链路或某台路由器发生故障时，数据流量将会被中断，直到 RIP 根据新的拓扑网络路由收敛完毕后，被中断的流量才能恢复正常的传输。

为了尽可能缩短网络故障导致的流量中断时间，网络管理员可以根据需要配置 RIP 快速重路由功能。

图1-1 RIP 快速重路由功能示意图



如 图 1-1 所示，通过在Router B上配置快速重路由功能，RIP可以为路由指定备份下一跳，当Router B检测到网络故障时，RIP会使用事先获取好的备份下一跳替换失效下一跳，通过备份下一跳来指导报文的转发，从而大大缩短了流量中断时间。在使用备份下一跳指导报文转发的同时，RIP会根据变化后的网络拓扑重新计算路由，网络收敛完毕后，使用新计算出来的最优路由来指导报文转发。

1.11.2 配置限制和指导

本功能只适合在主链路三层接口 up，主链路由双通变为单通或者不通的情况下使用。在主链路三层接口 down 的情况下，本功能不可用。

单通现象，即一条链路上的两端，有且只有一端可以收到另一端发来的报文，此链路称为单向链路。

RIP 快速重路由功能仅对非迭代 RIP 路由（即从直连邻居学到 RIP 路由）有效。

等价路由不支持快速重路由功能。

1.11.3 开启RIP快速重路由功能

(1) 进入系统视图。

system-view

(2) 配置路由策略。

在路由策略中通过 **apply fast-reroute backup-interface** 命令在路由策略中指定备份下一跳。

详细配置请参见“三层技术-IP 路由配置指导”中的“路由策略”。

(3) 进入 RIP 视图。

rip [*process-id*]

(4) 开启 RIP 快速重路由功能。

fast-reroute route-policy *route-policy-name*

缺省情况下，RIP 快速重路由功能处于关闭状态。

1.11.4 配置RIP快速重路由支持BFD检测功能

1. 功能简介

RIP 协议的快速重路由特性中，主用链路缺省不使用 BFD 进行链路故障检测。配置本功能后，将使用 BFD 进行检测，可以加快 RIP 协议的收敛速度。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 BFD Echo 报文源地址。

bfd echo-source-ip *ip-address*

缺省情况下，未配置 BFD Echo 报文源地址。

echo 报文的源 IP 地址用户可以任意指定。建议配置 echo 报文的源 IP 地址不属于该设备任何一个接口所在网段。

本命令的详细情况请参见“可靠性命令参考”中的“BFD”。

(3) 进入接口视图。

interface *interface-type interface-number*

(4) 使能 RIP 协议中主用链路的 BFD（Echo 方式）检测功能。

rip primary-path-detect bfd echo

缺省情况下，RIP 协议中主用链路的 BFD（Echo 方式）检测功能处于关闭状态。

1.12 提高RIP的安全性

1.12.1 配置RIP-1 报文的零域检查

1. 功能简介

RIP-1 报文中的有些字段必须为零，称之为零域。用户可配置 RIP-1 在接收报文时对零域进行检查，零域值不为零的 RIP-1 报文将不被处理。如果用户能确保所有报文都是可信任的，则可以不进行该项检查，以节省 CPU 处理时间。

由于 RIP-2 的报文没有零域，此项配置对 RIP-2 无效。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 RIP 视图。

rip [*process-id*]

(3) 使能 RIP-1 报文的零域检查功能。

checkzero

缺省情况下，RIP-1 报文的零域检查功能处于使能状态。

1.12.2 配置源地址检查

1. 功能简介

通过配置对接收到的 RIP 路由更新报文进行源 IP 地址检查：

- 对于在接口上接收的报文，RIP 将检查该报文源地址和接收接口的 IP 地址是否处于同一网段，如果不在同一网段则丢弃该报文。
- 对于 PPP 接口上接收的报文，RIP 检查该报文的源地址是否是对端接口的 IP 地址，如果不是则丢弃该报文。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 RIP 视图。

rip [*process-id*]

(3) 使能对接收到的 RIP 路由更新报文进行源 IP 地址检查功能。

validate-source-address

缺省情况下，对接收到的 RIP 路由更新报文进行源 IP 地址检查功能处于使能状态。

1.12.3 配置RIP-2 报文的认证方式

1. 功能简介

在安全性要求较高的网络环境中，可以通过配置报文的认证方式来对 RIP-2 报文进行有效性检查和验证。

RIP-2 支持两种认证方式：简单认证和 MD5 认证。

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 RIP-2 报文的验证方式。

rip authentication-mode { **md5** { **rfc2082** { **cipher** | **plain** } *string key-id* | **rfc2453** { **cipher** | **plain** } *string* } | **simple** { **cipher** | **plain** } *string* }

缺省情况下，未配置 RIP-2 的验证方式。

当 RIP 的版本为 RIP-1 时，虽然在接口视图下仍然可以配置验证方式，但由于 RIP-1 不支持认证，因此该配置不会生效。

1.13 RIP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 RIP 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以重启 RIP 进程或清除指定 RIP 进程的统计信息。

表1-1 RIP 显示和维护

操作	命令
显示RIP的当前运行状态及配置信息	**display rip** [*process-id*]
显示RIP进程的GR状态信息	**display rip** [*process-id*] **graceful-restart**
显示RIP进程的NSR状态信息	**display rip** [*process-id*] **non-stop-routing**
显示RIP数据库的激活路由	**display rip** *process-id* **database** [*ip-address* { *mask-length* | *mask* }]
显示RIP的接口信息	**display rip** *process-id* **interface** [*interface-type interface-number*]
显示RIP进程的邻居信息	**display rip** *process-id* **neighbor** [*interface-type interface-number*]
显示RIP的路由信息	**display rip** *process-id* **route** [*ip-address* { *mask-length* | *mask* } [**verbose**] | **peer** *ip-address* | **statistics**]
重启指定RIP进程	**reset rip** *process-id* **process**
清除RIP进程的统计信息	**reset rip** *process-id* **statistics**

1.14 RIP典型配置举例

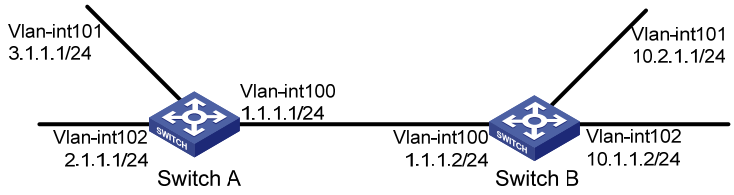
1.14.1 RIP基本功能配置举例

1. 组网需求

- 在 Switch A 和 Switch B 的所有接口上使能 RIP，并使用 RIP-2 进行网络互连。
- 在 Switch B 上配置路由出策略，向 Switch A 发布的路由中过滤掉 10.2.1.0/24；Switch B 上配置入策略，使得 Switch B 只接收路由 2.1.1.0/24。

2. 组网图

图1-2 RIP 基本功能配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置 RIP 基本功能

配置 Switch A，在指定网段上使能 RIP。

```
<SwitchA> system-view
[SwitchA] rip
[SwitchA-rip-1] network 1.0.0.0
[SwitchA-rip-1] network 2.0.0.0
[SwitchA-rip-1] network 3.0.0.0
[SwitchA-rip-1] quit
```

配置 Switch B，在指定接口上使能 RIP。

```
<SwitchB> system-view
[SwitchB] rip
[SwitchB-rip-1] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] rip 1 enable
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] rip 1 enable
[SwitchB-Vlan-interface101] quit
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] rip 1 enable
[SwitchB-Vlan-interface102] quit
```

查看 Switch A 的 RIP 路由表。

```
[SwitchA] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
```

```
              D - Direct, O - Optimal, F - Flush to RIB
------------------------------------------------------------------------------
 Peer 1.1.1.2 on Vlan-interface100
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      10.0.0.0/8              1.1.1.2          1       0       RAOF    11
 Local route
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      1.1.1.0/24              0.0.0.0          0       0       RDOF    -
      2.1.1.0/24              0.0.0.0          0       0       RDOF    -
      3.1.1.0/24              0.0.0.0          0       0       RDOF    -
```

从路由表中可以看出，RIP-1 发布的路由信息使用的是自然掩码。

(3) 配置 RIP 的版本

在 Switch A 上配置 RIP-2。

```
[SwitchA] rip
[SwitchA-rip-1] version 2
[SwitchA-rip-1] undo summary
[SwitchA-rip-1] quit
```

在 Switch B 上配置 RIP-2。

```
[SwitchB] rip
[SwitchB-rip-1] version 2
[SwitchB-rip-1] undo summary
[SwitchB-rip-1] quit
```

查看 Switch A 的 RIP 路由表。

```
[SwitchA] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
------------------------------------------------------------------------------

 Peer 1.1.1.2 on Vlan-interface100
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      10.0.0.0/8              1.1.1.2          1       0       RAOF    50
      10.2.1.0/24             1.1.1.2          1       0       RAOF    16
      10.1.1.0/24             1.1.1.2          1       0       RAOF    16
 Local route
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      1.1.1.0/24              0.0.0.0          0       0       RDOF    -
      2.1.1.0/24              0.0.0.0          0       0       RDOF    -
      3.1.1.0/24              0.0.0.0          0       0       RDOF    -
```

从路由表中可以看出，RIP-2 发布的路由中带有更为精确的子网掩码信息。

说明

由于 RIP 路由信息的老化时间较长，所以在配置 RIP-2 版本后的一段时间里，路由表中可能还会存在 RIP-1 的路由信息。

查看 Switch B 的路由表信息。

```
[SwitchB] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
------------------------------------------------------------------------------
 Peer 1.1.1.1 on Vlan-interface100
      Destination/Mask        Nexthop           Cost    Tag     Flags   Sec
      2.1.1.0/24              1.1.1.1           1       0       RAOF    19
      3.1.1.0/24              1.1.1.1           1       0       RAOF    19
 Local route
      Destination/Mask        Nexthop           Cost    Tag     Flags   Sec
      1.1.1.0/24              0.0.0.0           0       0       RDOF    -
      10.1.1.0/24             0.0.0.0           0       0       RDOF    -
      10.2.1.0/24             0.0.0.0           0       0       RDOF    -
```

(4) 配置 RIP 路由过滤

在 Switch B 配置地址前缀列表。

```
[SwitchB] ip prefix-list aaa index 10 permit 2.1.1.0 24
[SwitchB] ip prefix-list bbb index 10 deny 10.2.1.0 24
[SwitchB] ip prefix-list bbb index 11 permit 0.0.0.0 0 less-equal 32
[SwitchB] rip 1
[SwitchB-rip-1] filter-policy prefix-list aaa import
[SwitchB-rip-1] filter-policy prefix-list bbb export
[SwitchB-rip-1] quit
```

查看路由过滤后 Switch A 的路由信息。

```
[SwitchA] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
------------------------------------------------------------------------------
 Peer 1.1.1.2 on Vlan-interface100
      Destination/Mask        Nexthop           Cost    Tag     Flags   Sec
      10.1.1.0/24             1.1.1.2           1       0       RAOF    19
 Local route
      Destination/Mask        Nexthop           Cost    Tag     Flags   Sec
      1.1.1.0/24              0.0.0.0           0       0       RDOF    -
      2.1.1.0/24              0.0.0.0           0       0       RDOF    -
      3.1.1.0/24              0.0.0.0           0       0       RDOF    -
```

查看 Switch B 的路由表信息。

```
[SwitchB] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
------------------------------------------------------------------------------
 Peer 1.1.1.1 on Vlan-interface100
      Destination/Mask        Nexthop           Cost    Tag     Flags   Sec
      2.1.1.0/24              1.1.1.1           1       0       RAOF    19
 Local route
```

```
Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
1.1.1.0/24              0.0.0.0          0       0       RDOF    -
10.1.1.0/24             0.0.0.0          0       0       RDOF    -
10.2.1.0/24             0.0.0.0          0       0       RDOF    -
```

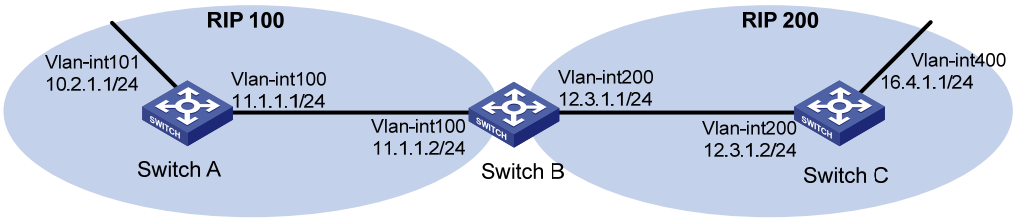
1.14.2 RIP引入外部路由配置举例

1. 组网需求

- Switch B 上运行两个 RIP 进程：RIP 100 和 RIP 200。Switch B 通过 RIP 100 和 Switch A 交换路由信息，通过 RIP 200 和 Switch C 交换路由信息。
- 在 Switch B 上配置 RIP 进程 200 引入外部路由，引入直连路由和 RIP 进程 100 的路由，使得 Switch C 能够学习到达 10.2.1.0/24 和 11.1.1.0/24 的路由，但 Switch A 不能学习到达 12.3.1.0/24 和 16.4.1.0/24 的路由。

2. 组网图

图1-3 RIP 引入外部路由配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置 RIP 基本功能

在 Switch A 上启动 RIP 进程 100，并配置 RIP 版本号为 2。

```
<SwitchA> system-view
[SwitchA] rip 100
[SwitchA-rip-100] network 10.0.0.0
[SwitchA-rip-100] network 11.0.0.0
[SwitchA-rip-100] version 2
[SwitchA-rip-100] undo summary
[SwitchA-rip-100] quit
```

在 Switch B 上启动两个 RIP 进程，进程号分别为 100 和 200，并配置 RIP 版本号为 2。

```
<SwitchB> system-view
[SwitchB] rip 100
[SwitchB-rip-100] network 11.0.0.0
[SwitchB-rip-100] version 2
[SwitchB-rip-100] undo summary
[SwitchB-rip-100] quit
[SwitchB] rip 200
[SwitchB-rip-200] network 12.0.0.0
[SwitchB-rip-200] version 2
[SwitchB-rip-200] undo summary
```

```
[SwitchB-rip-200] quit
```

在 Switch C 上启动 RIP 进程 200，并配置 RIP 版本号为 2。

```
<SwitchC> system-view
[SwitchC] rip 200
[SwitchC-rip-200] network 12.0.0.0
[SwitchC-rip-200] network 16.0.0.0
[SwitchC-rip-200] version 2
[SwitchC-rip-200] undo summary
[SwitchC-rip-200] quit
```

查看 Switch C 的路由表信息。

```
[SwitchC] display ip routing-table

Destinations : 13        Routes : 13

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
12.3.1.0/24         Direct 0    0            12.3.1.2        Vlan200
12.3.1.0/32         Direct 0    0            12.3.1.2        Vlan200
12.3.1.2/32         Direct 0    0            127.0.0.1       InLoop0
12.3.1.255/32       Direct 0    0            12.3.1.2        Vlan200
16.4.1.0/24         Direct 0    0            16.4.1.1        Vlan400
16.4.1.0/32         Direct 0    0            16.4.1.1        Vlan400
16.4.1.1/32         Direct 0    0            127.0.0.1       InLoop0
16.4.1.255/32       Direct 0    0            16.4.1.1        Vlan400
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

(3) 配置 RIP 引入外部路由

在 Switch B 配置 RIP 进程 200 引入外部路由，引入直连路由和 RIP 进程 100 的路由。

```
[SwitchB] rip 200
[SwitchB-rip-200] import-route rip 100
[SwitchB-rip-200] import-route direct
[SwitchB-rip-200] quit
```

查看路由引入后 Switch C 的路由表信息。

```
[SwitchC] display ip routing-table

Destinations : 15        Routes : 15

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.2.1.0/24         RIP    100  1            12.3.1.1        Vlan200
11.1.1.0/24         RIP    100  1            12.3.1.1        Vlan200
12.3.1.0/24         Direct 0    0            12.3.1.2        Vlan200
12.3.1.0/32         Direct 0    0            12.3.1.2        Vlan200
12.3.1.2/32         Direct 0    0            127.0.0.1       InLoop0
12.3.1.255/32       Direct 0    0            12.3.1.2        Vlan200
```

```
16.4.1.0/24          Direct 0    0           16.4.1.1        Vlan400
16.4.1.0/32          Direct 0    0           16.4.1.1        Vlan400
16.4.1.1/32          Direct 0    0           127.0.0.1       InLoop0
16.4.1.255/32        Direct 0    0           16.4.1.1        Vlan400
127.0.0.0/8          Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/32         Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32         Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32   Direct 0    0           127.0.0.1       InLoop0
```

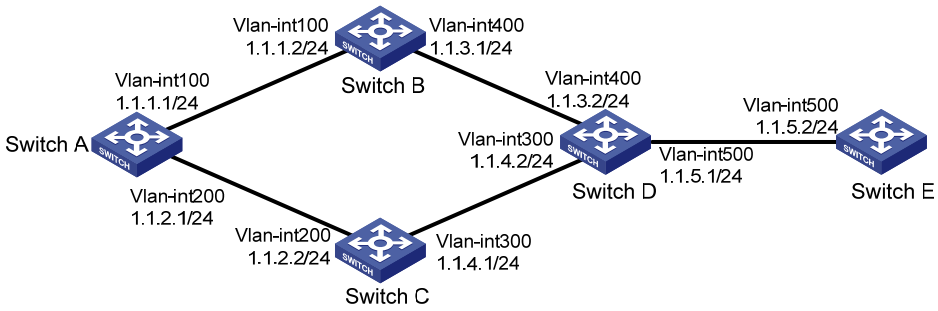
1.14.3 RIP接口附加度量值配置举例

1. 组网需求

- 在 Switch A、Switch B、Switch C、Switch D 和 Switch E 的所有接口上使能 RIP，并使用 RIP-2 进行网络互连。
- Switch A 有两条链路可以到达 Switch D，其中，通过 Switch B 到达 Switch D 的链路比通过 Switch C 到达 Switch D 的链路更加稳定。通过在 Switch A 的 Vlan-interface200 上配置接口接收 RIP 路由的附加度量值，使得 Switch A 优选从 Switch B 学到的 1.1.5.0/24 网段的路由。

2. 组网图

图1-4 RIP 接口附加度量值配置组网图



3. 配置步骤

(1) 配置各接口的地址（略）

(2) 配置 RIP 基本功能

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] rip 1
[SwitchA-rip-1] network 1.0.0.0
[SwitchA-rip-1] version 2
[SwitchA-rip-1] undo summary
[SwitchA-rip-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] rip 1
[SwitchB-rip-1] network 1.0.0.0
[SwitchB-rip-1] version 2
```

```
[SwitchB-rip-1] undo summary
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchB] rip 1
[SwitchC-rip-1] network 1.0.0.0
[SwitchC-rip-1] version 2
[SwitchC-rip-1] undo summary
```

配置 Switch D。

```
<SwitchD> system-view
[SwitchD] rip 1
[SwitchD-rip-1] network 1.0.0.0
[SwitchD-rip-1] version 2
[SwitchD-rip-1] undo summary
```

配置 Switch E。

```
<SwitchE> system-view
[SwitchE] rip 1
[SwitchE-rip-1] network 1.0.0.0
[SwitchE-rip-1] version 2
[SwitchE-rip-1] undo summary
```

在 Switch A 上查看 RIP 数据库的所有激活路由。

```
[SwitchA] display rip 1 database
   1.0.0.0/8, auto-summary
       1.1.1.0/24, cost 0, nexthop 1.1.1.1, RIP-interface
       1.1.2.0/24, cost 0, nexthop 1.1.2.1, RIP-interface
       1.1.3.0/24, cost 1, nexthop 1.1.1.2
       1.1.4.0/24, cost 1, nexthop 1.1.2.2
       1.1.5.0/24, cost 2, nexthop 1.1.1.2
       1.1.5.0/24, cost 2, nexthop 1.1.2.2
```

可以看到，到达网段 1.1.5.0/24 有两条 RIP 路由，下一跳分别是 Switch B（IP 地址为 1.1.1.2）和 Switch C（IP 地址为 1.1.2.2），cost 值都是 2。

(3) 配置 RIP 接口附加度量值

在 Switch A 上配置接口 Vlan-interface200 接收 RIP 路由时的附加度量值为 3。

```
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] rip metricin 3
```

在 Switch A 上查看 RIP 数据库的所有激活路由。

```
[SwitchA-Vlan-interface200] display rip 1 database
   1.0.0.0/8, auto-summary
       1.1.1.0/24, cost 0, nexthop 1.1.1.1, RIP-interface
       1.1.2.0/24, cost 0, nexthop 1.1.2.1, RIP-interface
       1.1.3.0/24, cost 1, nexthop 1.1.1.2
       1.1.4.0/24, cost 2, nexthop 1.1.1.2
       1.1.5.0/24, cost 2, nexthop 1.1.1.2
```

可以看到，到达网段 1.1.5.0/24 的 RIP 路由仅有一条，下一跳是 Switch B（IP 地址为 1.1.1.2），cost 值为 2。

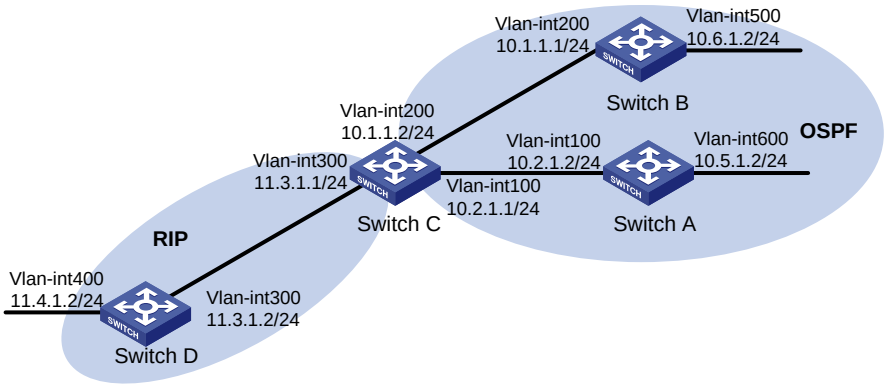
1.14.4 RIP发布聚合路由配置举例

1. 组网需求

- Switch A、Switch B 运行 OSPF，Switch D 运行 RIP，Switch C 同时运行 OSPF 和 RIP。
- 在 Switch C 上配置 RIP 进程引入 OSPF 路由，使 Switch D 有到达 10.1.1.0/24、10.2.1.0/24、10.5.1.0/24 和 10.6.1.0/24 网段的路由。
- 为了减小 Switch D 的路由表规模，在 Switch C 上配置路由聚合，只发布聚合后的路由 10.0.0.0/8。

2. 组网图

图1-5 RIP 发布聚合路由配置组网图



3. 配置步骤

(1) 配置各接口的地址（略）

(2) 配置 OSPF 基本功能

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.5.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 10.6.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 0
```

```
[SwitchC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

(3) 配置 RIP 基本功能

配置 Switch C。

```
[SwitchC] rip 1
[SwitchC-rip-1] network 11.3.1.0
[SwitchC-rip-1] version 2
[SwitchC-rip-1] undo summary
```

配置 Switch D。

```
<SwitchD> system-view
[SwitchD] rip 1
[SwitchD-rip-1] network 11.0.0.0
[SwitchD-rip-1] version 2
[SwitchD-rip-1] undo summary
[SwitchD-rip-1] quit
```

在 Switch C 上配置 RIP 引入外部路由，引入 OSPF 进程 1 的路由和直连路由。

```
[SwitchC-rip-1] import-route direct
[SwitchC-rip-1] import-route ospf 1
[SwitchC-rip-1] quit
```

查看 Switch D 的路由表信息。

```
[SwitchD] display ip routing-table

Destinations : 15        Routes : 15

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.1.1.0/24         RIP    100  1            11.3.1.1        Vlan300
10.2.1.0/24         RIP    100  1            11.3.1.1        Vlan300
10.5.1.0/24         RIP    100  1            11.3.1.1        Vlan300
10.6.1.0/24         RIP    100  1            11.3.1.1        Vlan300
11.3.1.0/24         Direct 0    0            11.3.1.2        Vlan300
11.3.1.0/32         Direct 0    0            11.3.1.2        Vlan300
11.3.1.2/32         Direct 0    0            127.0.0.1       InLoop0
11.4.1.0/24         Direct 0    0            11.4.1.2        Vlan400
11.4.1.0/32         Direct 0    0            11.4.1.2        Vlan400
11.4.1.2/32         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

(4) 在 Switch C 上配置路由聚合，只发布聚合路由 10.0.0.0/8。

```
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] rip summary-address 10.0.0.0 8
```

查看 Switch D 的路由表信息。

```
[SwitchD] display ip routing-table
```

```
Destinations : 12        Routes : 12

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
0.0.0.0/32          Direct 0    0           127.0.0.1       InLoop0
10.0.0.0/8          RIP    100  1           11.3.1.1        Vlan300
11.3.1.0/24         Direct 0    0           11.3.1.2        Vlan300
11.3.1.0/32         Direct 0    0           11.3.1.2        Vlan300
11.3.1.2/32         Direct 0    0           127.0.0.1       InLoop0
11.4.1.0/24         Direct 0    0           11.4.1.2        Vlan400
11.4.1.0/32         Direct 0    0           11.4.1.2        Vlan400
11.4.1.2/32         Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
```

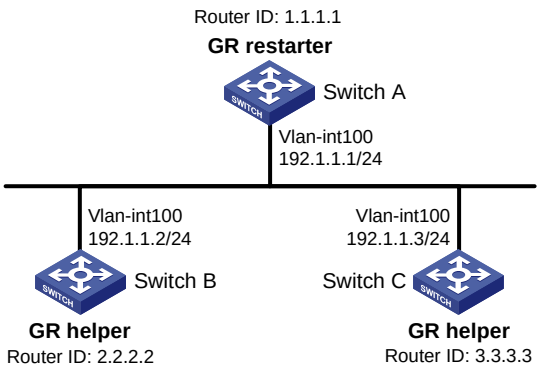
1.14.5 RIP GR配置举例

1. 组网需求

- Switch A、Switch B 和 Switch C 通过 RIPv2 协议实现网络互连。
- Switch A 作为 GR Restarter，Switch B 和 Switch C 作为 GR Helper 并且通过 GR 机制与 Switch A 保持同步。

2. 组网图

图1-6 RIP GR 配置组网图



3. 配置步骤

(1) 配置各路由器接口的 IP 地址和 RIP 协议

请按照上面组网图配置各接口的 IP 地址和子网掩码，具体配置过程略。

配置各路由器之间采用 RIPv2 协议进行互连，确保 Switch A、Switch B 和 Switch C 之间能够在网络层互通，并且各路由器之间能够借助 RIPv2 协议实现动态路由更新。

(2) 配置 RIP GR

使能 Switch A 的 RIP GR 功能。

```
<SwitchA> system-view
```

```
[SwitchA] rip
[SwitchA-rip-1] graceful-restart
```

4. 验证配置

在 Switch A 上触发协议重启或主备倒换后，查看 RIP 的 GR 状态。

```
<SwitchA> display rip graceful-restart
 RIP process: 1
 Graceful Restart capability     : Enabled
 Current GR state                : Normal
 Graceful Restart period         : 60  seconds
 Graceful Restart remaining time : 0   seconds
```

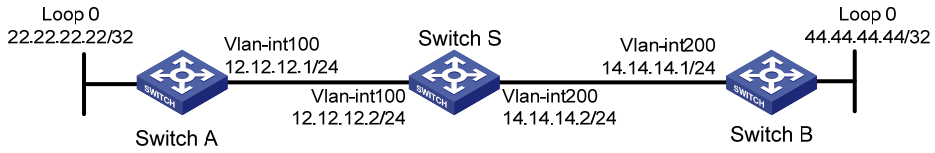
1.14.6 RIP NSR配置举例

1. 组网需求

Switch S、Switch A、Switch B 通过 RIPv2 协议实现网络互连。要求对 Switch S 进行主备倒换时，Switch A 和 Switch B 到 Switch S 的邻居没有中断，Switch A 到 Switch B 的流量没有中断。

2. 组网图

图1-7 RIP NSR 配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址和 RIP 协议

请按照上面组网图配置各接口的 IP 地址和子网掩码，具体配置过程略。

配置各交换机之间采用 RIPv2 协议进行互连，确保 Switch S、Switch A 和 Switch B 之间能够在网络层互通，并且各路由器之间能够借助 RIPv2 协议实现动态路由更新。

(2) 配置 RIP NSR

使能 Switch S 的 RIP NSR 功能。

```
<SwitchS> system-view
[SwitchS] rip 100
[SwitchS-rip-100] non-stop-routing
[SwitchS-rip-100] quit
```

4. 验证配置

Switch S 进行主备倒换。

```
[SwitchS] placement reoptimize
Predicted changes to the placement
Program                          Current location       New location
-------------------------------------------------------------------
lb                               0/0                    0/0
lsm                              0/0                    0/0
```

```
slsp                              0/0                   0/0
rib6                              0/0                   0/0
routepolicy                       0/0                   0/0
rib                               0/0                   0/0
staticroute6                      0/0                   0/0
staticroute                       0/0                   0/0
ospf                              0/0                   1/0
Continue? [y/n]:y
Re-optimization of the placement start. You will be notified on completion
Re-optimization of the placement complete. Use 'display placement' to view the new placement
```

查看 Switch A 上 RIP 协议的邻居和路由。

```
[SwitchA] display rip 1 neighbor
 Neighbor Address: 12.12.12.2
     Interface  : Vlan-interface200
     Version    : RIPv2     Last update: 00h00m13s
     Relay nbr  : No        BFD session: None
     Bad packets: 0         Bad routes : 0
[SwitchA] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
 ------------------------------------------------------------------------------
 Peer 12.12.12.2 on Vlan-interface200
      Destination/Mask        Nexthop           Cost    Tag     Flags   Sec
      14.0.0.0/8              12.12.12.2        1       0       RAOF    16
      44.0.0.0/8              12.12.12.2        2       0       RAOF    16
 Local route
      Destination/Mask        Nexthop           Cost    Tag     Flags   Sec
      12.12.12.0/24           0.0.0.0           0       0       RDOF    -
      22.22.22.22/32          0.0.0.0           0       0       RDOF    -
```

查看 Switch B 上 RIP 协议的邻居和路由。

```
[SwitchB] display rip 1 neighbor
 Neighbor Address: 14.14.14.2
     Interface  : Vlan-interface200
     Version    : RIPv2     Last update: 00h00m32s
     Relay nbr  : No        BFD session: None
     Bad packets: 0         Bad routes : 0
[SwitchB] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
 ------------------------------------------------------------------------------
 Peer 14.14.14.2 on Vlan-interface200
      Destination/Mask        Nexthop           Cost    Tag     Flags   Sec
      12.0.0.0/8              14.14.14.2        1       0       RAOF    1
      22.0.0.0/8              14.14.14.2        2       0       RAOF    1
 Local route
      Destination/Mask        Nexthop           Cost    Tag     Flags   Sec
```

```
44.44.44.44/32          0.0.0.0          0       0       RDOF     -
14.14.14.0/24           0.0.0.0          0       0       RDOF     -
```

通过上面信息可以看出在 Switch S 发生主备倒换的时候，Switch A 和 Switch B 的邻居和路由信息保持不变，从 Switch A 到 Switch B 的流量转发没有受到主备倒换的影响。

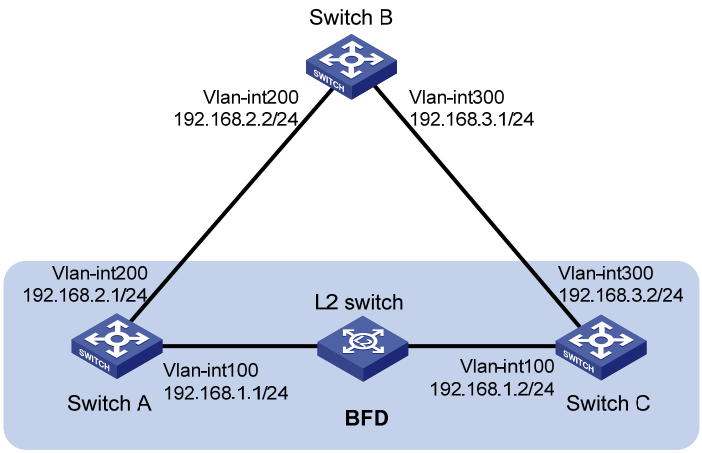
1.14.7 RIP与BFD联动配置举例（echo报文单跳检测）

1. 组网需求

- Switch A、Switch C通过二层交换机互连，它们的接口Vlan-interface100都运行RIP进程1。并且 Switch A 的接口 Vlan-interface100 上还使能了 BFD 检测功能。
- Switch A 通过 Switch B 与 Switch C 互连，Switch A 的接口 Vlan-interface200 运行 RIP 进程 2。Switch C 的接口 Vlan-interface300、Switch B 的接口 Vlan-interface200 和 Vlan-interface300 上都运行 RIP 进程 1。
- Switch C 上配置静态路由，并且将静态路由引入在 RIP 进程中，使 Switch C 有路由发送至 Switch A。Switch A 上学习到 Switch C 发送的静态路由，出接口为与二层交换机相连的接口。
- 在 Switch C 和二层交换机之间的链路发生故障后，BFD 能够快速检测链路中断并通告 RIP 协议。RIP 协议响应 BFD 会话 down，删除与 Switch C 的邻居，并删除从 Switch C 学习的路由。Switch A 上学习到 Switch C 上发送的静态路由，出接口为与 Switch B 相连的接口。

2. 组网图

图1-8 RIP 与 BFD 联动配置组网图（echo 报文单跳检测）



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置 RIP 基本功能

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] rip 1
[SwitchA-rip-1] version 2
[SwitchA-rip-1] undo summary
[SwitchA-rip-1] network 192.168.1.0
```

```
[SwitchA-rip-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] rip bfd enable
[SwitchA-Vlan-interface100] quit
[SwitchA] rip 2
[SwitchA-rip-2] version 2
[SwitchA-rip-2] undo summary
[SwitchA-rip-2] network 192.168.2.0
[SwitchA-rip-2] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] rip 1
[SwitchB-rip-1] version 2
[SwitchB-rip-1] undo summary
[SwitchB-rip-1] network 192.168.2.0
[SwitchB-rip-1] network 192.168.3.0
[SwitchB-rip-1] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] rip 1
[SwitchC-rip-1] version 2
[SwitchC-rip-1] undo summary
[SwitchC-rip-1] network 192.168.1.0
[SwitchC-rip-1] network 192.168.3.0
[SwitchC-rip-1] import-route static
[SwitchC-rip-1] quit
```

(3) 配置 BFD 参数

配置 Switch A。

```
[SwitchA] bfd echo-source-ip 11.11.11.11
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] bfd min-echo-receive-interval 500
[SwitchA-Vlan-interface100] bfd detect-multiplier 7
[SwitchA-Vlan-interface100] quit
[SwitchA] quit
```

(4) Switch C 配置静态路由

```
[SwitchC] ip route-static 120.1.1.1 24 null 0
```

4. 验证配置

查看 Switch A 的 BFD 信息。

```
<SwitchA> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 Session Working Under Echo Mode:

 LD             SourceAddr      DestAddr        State    Holdtime    Interface
 4              192.168.1.1     192.168.1.2     Up       2000ms      Vlan100
```

查看 Switch A 上学到的路由 120.1.1.0/24，可以看到 Switch A 经过 L2 Switch 到达 Switch C。

```
<SwitchA> display ip routing-table 120.1.1.0 24

Summary count : 1

Destination/Mask    Proto   Pre Cost        NextHop         Interface
120.1.1.0/24        RIP     100 1           192.168.1.2     Vlan-interface100
```

当 Switch C 和二层交换机之间的链路发生故障时：

查看 Switch A 上学到的路由 120.1.1.0/24，可以看到 Switch A 经过 Switch B 到达 Switch C。

```
<SwitchA> display ip routing-table 120.1.1.0 24

Summary count : 1

Destination/Mask    Proto   Pre Cost        NextHop         Interface
120.1.1.0/24        RIP     100 1           192.168.2.2     Vlan-interface200
```

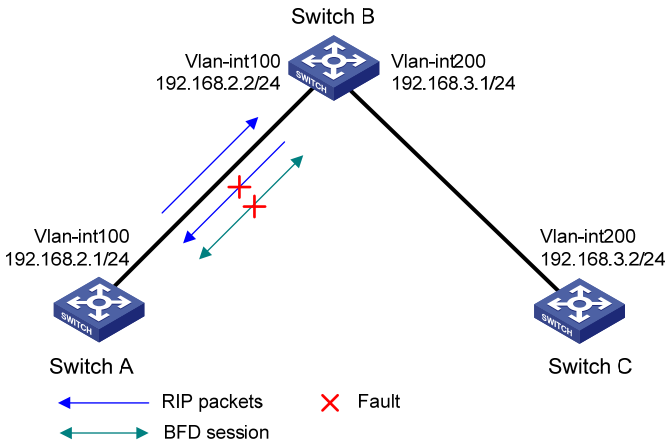
1.14.8 RIP与BFD联动配置举例（指定目的地址的echo报文单跳检测）

1. 组网需求

- Switch A 和 Switch B 互连，Switch A 的接口 Vlan-interface100 和 Switch B 的接口 Vlan-interface100 都运行 RIP 进程 1。Switch A 的接口 Vlan-interface100 上使能了 BFD 检测功能，指定目的地址为 Switch B 的接口 Vlan-interface100 的地址。
- Switch B 与 Switch C 互连，它们的接口 Vlan-interface200 都运行 RIP 进程 1。
- Switch A 和 Switch C 上配置静态路由，并都将静态路由引入 RIP 进程中，其中 Switch A 引入路由的 cost 值比 Switch C 引入的 cost 值小，这样，当 Switch B 上学习到 Switch A 和 Switch C 发送的路由后，会优选 Switch A 的路由，出接口为与 Switch A 连接的接口。
- 在 Switch A 和 Switch B 之间的链路发生单通故障（从 Switch A 到 Switch B 方向报文是通的，但是从 Switch B 到 Switch A 方向的链路不通）后，Switch A 上 BFD 能够快速检测链路故障并通告 RIP 协议。Switch A 上的 RIP 协议响应 BFD 会话 down，删除从接口 Vlan-interface100 学习到的邻居和路由，并不再从该接口接收和发送 RIP 报文。Switch B 上在学自 Switch A 的路由老化后，会优选 Switch C 发送的静态路由，出接口为与 Switch C 连接的接口。

2. 组网图

图1-9 RIP 与 BFD 联动配置组网图（指定目的地址的 echo 报文单跳检测）



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置 RIP 基本功能并且在接口上使能 BFD

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] rip 1
[SwitchA-rip-1] network 192.168.2.0
[SwitchA-rip-1] import-route static
[SwitchA-rip-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] rip bfd enable destination 192.168.2.2
[SwitchA-Vlan-interface100] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] rip 1
[SwitchB-rip-1] network 192.168.2.0
[SwitchB-rip-1] network 192.168.3.0
[SwitchB-rip-1] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] rip 1
[SwitchC-rip-1] network 192.168.3.0
[SwitchC-rip-1] import-route static cost 3
[SwitchC-rip-1] quit
```

(3) 配置接口 BFD 参数

配置 Switch A。

```
[SwitchA] bfd echo-source-ip 11.11.11.11
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] bfd min-echo-receive-interval 500
```

```
[SwitchA-Vlan-interface100] return
```

(4) 配置静态路由

配置 Switch A。

```
[SwitchA] ip route-static 100.1.1.0 24 null 0
```

配置 Switch C。

```
[SwitchC] ip route-static 100.1.1.0 24 null 0
```

4. 验证配置

显示 Switch A 的 BFD 信息。

```
<SwitchA> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working under Echo mode:

 LD              SourceAddr      DestAddr        State    Holdtime    Interface
 3               192.168.2.1     192.168.2.2     Up       2000ms      vlan100
```

显示 Switch B 上学到的路由 100.1.1.0/24。

```
<SwitchB> display ip routing-table 100.1.1.0 24 verbose

Summary Count : 1

Destination: 100.1.1.0/24
   Protocol: RIP
 Process ID: 1
  SubProtID: 0x1                    Age: 00h02m47s
       Cost: 1                Preference: 100
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x12000002          LastAs: 0
     AttrID: 0xffffffff         Neighbor: 192.168.2.1
      Flags: 0x1008c         OrigNextHop: 192.168.2.1
      Label: NULL            RealNextHop: 192.168.2.1
    BkLabel: NULL              BkNextHop: N/A
  Tunnel ID: Invalid           Interface: vlan-interface 100
BkTunnel ID: Invalid         BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A                  PathID: 0x0
```

当 Switch A 和 Switch B 之间的链路发生故障时：

显示 Switch B 上学到的路由 100.1.1.0/24。

```
<SwitchB> display ip routing-table 100.1.1.0 24 verbose

Summary Count : 1

Destination: 100.1.1.0/24
```

```
   Protocol: RIP
 Process ID: 1
  SubProtID: 0x1                    Age: 00h21m23s
       Cost: 4                Preference: 100
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x12000002          LastAs: 0
     AttrID: 0xffffffff         Neighbor: 192.168.3.2
      Flags: 0x1008c         OrigNextHop: 192.168.3.2
      Label: NULL            RealNextHop: 192.168.3.2
    BkLabel: NULL              BkNextHop: N/A
  Tunnel ID: Invalid           Interface: vlan-interface 200
BkTunnel ID: Invalid         BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A                   PathID: 0x0
```

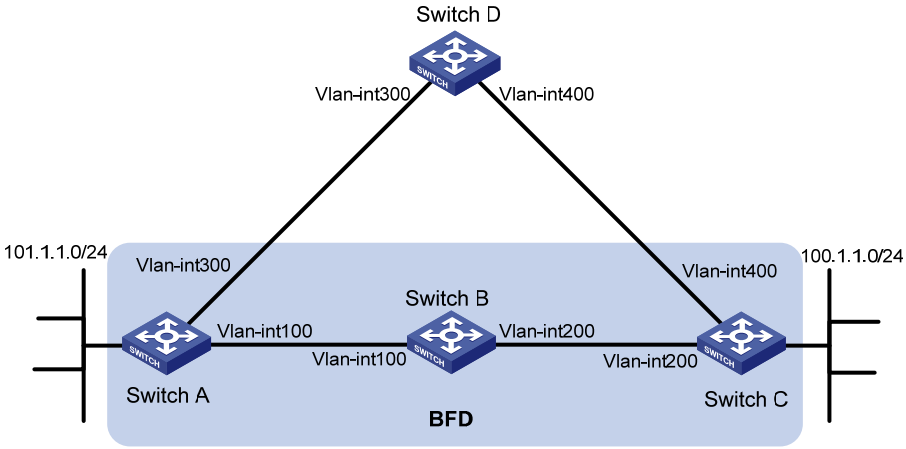
1.14.9 RIP与BFD联动配置举例（control报文双向检测）

1. 组网需求

- Switch A 通过 Switch B 与 Switch C 互连。Switch A 的接口 Vlan-interface100 和 Switch C 的接口 Vlan-interface200 上都运行 RIP 进程 1。分别在 Switch A 和 Switch C 上配置到达对端的静态路由，并在 Switch A 的接口 Vlan-interface100 和 Switch C 的接口 Vlan-interface200 上并使能 BFD 检测功能。
- Switch A 通过 Switch D 与 Switch C 互连。Switch A 的接口 Vlan-interface300 运行 RIP 进程 2。Switch C 的接口 Vlan-interface400、Switch D 的接口 Vlan-interface300 和 Vlan-interface400 上运行 RIP 进程 1。
- 为使 Switch A 与 Switch C 互有路由发送，在 Switch A 与 Switch C 上将到达对端的静态路由引入 RIP 协议中。Switch A 与 Switch C 之间建立 BFD 会话。Switch A 上学习到 Switch C 发送的静态路由，出接口为与 Switch B 连接的接口。
- 在 Switch B 与 Switch C 之间的链路发生故障后，BFD 能够快速检测链路中断并通告 RIP 协议。RIP 协议响应 BFD 会话 down，删除与 Switch C 的邻居，并删除从 Switch C 学习的路由。Switch A 上学习到 Switch C 发送的静态路由，出接口为与 Switch D 连接的接口。

2. 组网图

图1-10 RIP 与 BFD 联动配置组网图（control 报文双向检测）



设备	接口	IP地址	设备	接口	IP地址
Switch A	Vlan-int300	192.168.3.1/24	Switch B	Vlan-int100	192.168.1.2/24
	Vlan-int100	192.168.1.1/24		Vlan-int200	192.168.2.1/24
Switch C	Vlan-int200	192.168.2.2/24	Switch D	Vlan-int300	192.168.3.2/24
	Vlan-int400	192.168.4.2/24		Vlan-int400	192.168.4.1/24

3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置 RIP 基本功能，并引入静态路由，使 Switch A 与 Switch C 互有路由发送

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] rip 1
[SwitchA-rip-1] version 2
[SwitchA-rip-1] undo summary
[SwitchA-rip-1] network 192.168.1.0
[SwitchA-rip-1] network 101.1.1.0
[SwitchA-rip-1] peer 192.168.2.2
[SwitchA-rip-1] undo validate-source-address
[SwitchA-rip-1] import-route static
[SwitchA-rip-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] rip bfd enable
[SwitchA-Vlan-interface100] quit
[SwitchA] rip 2
[SwitchA-rip-2] version 2
[SwitchA-rip-2] undo summary
[SwitchA-rip-2] network 192.168.3.0
[SwitchA-rip-2] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] rip 1
[SwitchC-rip-1] version 2
[SwitchC-rip-1] undo summary
[SwitchC-rip-1] network 192.168.2.0
[SwitchC-rip-1] network 192.168.4.0
[SwitchC-rip-1] network 100.1.1.0
[SwitchC-rip-1] peer 192.168.1.1
[SwitchC-rip-1] undo validate-source-address
[SwitchC-rip-1] import-route static
[SwitchC-rip-1] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] rip bfd enable
[SwitchC-Vlan-interface200] quit
```

配置 Switch D。

```
<SwitchD> system-view
[SwitchD] rip 1
[SwitchD-rip-1] version 2
[SwitchD-rip-1] undo summary
[SwitchD-rip-1] network 192.168.3.0
[SwitchD-rip-1] network 192.168.4.0
```

(3) 配置 BFD 参数

配置 Switch A。

```
[SwitchA] bfd session init-mode active
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] bfd min-transmit-interval 500
[SwitchA-Vlan-interface100] bfd min-receive-interval 500
[SwitchA-Vlan-interface100] bfd detect-multiplier 7
[SwitchA-Vlan-interface100] quit
```

配置 Switch C。

```
[SwitchC] bfd session init-mode active
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] bfd min-transmit-interval 500
[SwitchC-Vlan-interface200] bfd min-receive-interval 500
[SwitchC-Vlan-interface200] bfd detect-multiplier 7
[SwitchC-Vlan-interface200] quit
```

(4) 配置静态路由

配置 Switch A。

```
[SwitchA] ip route-static 192.168.2.0 24 vlan-interface 100 192.168.1.2
[SwitchA] quit
```

配置 Switch C。

```
[SwitchC] ip route-static 192.168.1.0 24 vlan-interface 200 192.168.2.1
```

4. 验证配置

显示 Switch A 的 BFD 信息。

```
<SwitchA> display bfd session
```

```
 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working under Ctrl mode:

 LD/RD              SourceAddr      DestAddr        State     Holdtime     Interface
 513/513            192.168.1.1     192.168.2.2     Up        1700ms       vlan100
```

显示 Switch A 上学到的路由 100.1.1.0/24，可以看到 Switch A 经过 Switch B 到达 Switch C。

```
<SwitchA> display ip routing-table 100.1.1.0 24

Summary count : 1

Destination/Mask    Proto   Pre Cost        NextHop         Interface
100.1.1.0/24        RIP     100 1           192.168.2.2     vlan-interface 100
```

Switch B 和 Switch C 之间的链路发生故障后：

显示 Switch A 上学到的路由 100.1.1.0/24，可以看到 Switch A 经过 Switch D 到达 Switch C。

```
<SwitchA> display ip routing-table 100.1.1.0 24

Summary count : 1

Destination/Mask    Proto   Pre Cost        NextHop         Interface
100.1.1.0/24        RIP     100 2           192.168.3.2     vlan-interface 300
```

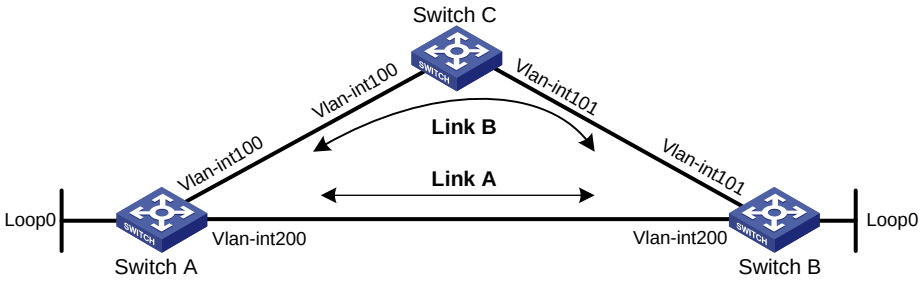
1.14.10 RIP快速重路由配置举例

1. 组网需求

Switch A、Switch B 和 Switch C 通过 RIPv2 协议实现网络互连。要求当 Switch A 和 Switch B 之间的链路出现单通故障时，业务可以快速切换到链路 B 上。

2. 组网图

图1-11 RIP 快速重路由配置组网图



设备	接口	IP地址	设备	接口	IP地址
Switch A	Vlan-int100	12.12.12.1/24	Switch B	Vlan-int101	24.24.24.4/24
	Vlan-int200	13.13.13.1/24		Vlan-int200	13.13.13.2/24
	Loop0	1.1.1.1/32		Loop0	4.4.4.4/32
Switch C	Vlan-int100	12.12.12.2/24			
	Vlan-int101	24.24.24.2/24			

3. 配置步骤

(1) 配置各交换机接口的 IP 地址和 RIPv2 协议

请按照上面组网图配置各接口的 IP 地址和子网掩码，具体配置过程略。

配置各路由器之间采用 RIPv2 协议进行互连，确保 Switch A、Switch B 和 Switch C 之间能够在网络层互通，并且各路由器之间能够借助 RIPv2 协议实现动态路由更新。

具体配置过程略。

(2) 配置 RIP 快速重路由

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ip prefix-list abc index 10 permit 4.4.4.4 32
[SwitchA] route-policy frr permit node 10
[SwitchA-route-policy-frr-10] if-match ip address prefix-list abc
[SwitchA-route-policy-frr-10] apply fast-reroute backup-interface vlan-interface 100
backup-nexthop 12.12.12.2
[SwitchA-route-policy-frr-10] quit
[SwitchA] rip 1
[SwitchA-rip-1] fast-reroute route-policy frr
[SwitchA-rip-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ip prefix-list abc index 10 permit 1.1.1.1 32
[SwitchB] route-policy frr permit node 10
[SwitchB-route-policy-frr-10] if-match ip address prefix-list abc
[SwitchB-route-policy-frr-10] apply fast-reroute backup-interface vlan-interface 101
backup-nexthop 24.24.24.2
[SwitchB-route-policy-frr-10] quit
[SwitchB] rip 1
[SwitchB-rip-1] fast-reroute route-policy frr
[SwitchB-rip-1] quit
```

4. 验证配置

在 Switch A 上查看 4.4.4.4/32 路由，可以看到备份下一跳信息：

```
[SwitchA] display ip routing-table 4.4.4.4 verbose

Summary Count : 1

Destination: 4.4.4.4/32
   Protocol: RIP
 Process ID: 1
  SubProtID: 0x1                    Age: 04h20m37s
       Cost: 1               Preference: 100
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NibID: 0x26000002          LastAs: 0
```

```
     AttrID: 0xffffffff         Neighbor: 13.13.13.2
      Flags: 0x1008c         OrigNextHop: 13.13.13.2
      Label: NULL            RealNextHop: 13.13.13.2
    BkLabel: NULL              BkNextHop: 12.12.12.2
  Tunnel ID: Invalid           Interface: Vlan-interface200
BkTunnel ID: Invalid         BkInterface: Vlan-interface100
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A                  PathID: 0x0
```

在 Switch B 上查看 1.1.1.1/32 路由，可以看到备份下一跳信息：

```
[SwitchB] display ip routing-table 1.1.1.1 verbose

Summary Count : 1

Destination: 1.1.1.1/32
   Protocol: RIP
 Process ID: 1
  SubProtID: 0x1                    Age: 04h20m37s
       Cost: 1               Preference: 100
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NibID: 0x26000002         LastAs: 0
     AttrID: 0xffffffff         Neighbor: 13.13.13.1
      Flags: 0x1008c         OrigNextHop: 13.13.13.1
      Label: NULL            RealNextHop: 13.13.13.1
    BkLabel: NULL              BkNextHop: 24.24.24.2
  Tunnel ID: Invalid           Interface: Vlan-interface200
BkTunnel ID: Invalid         BkInterface: Vlan-interface101
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A                  PathID: 0x0
```

目 录

1 OSPF

1.1 OSPF简介

OSPF（Open Shortest Path First，开放最短路径优先）是 IETF（Internet Engineering Task Force，互联网工程任务组）组织开发的一个基于链路状态的内部网关协议。目前针对 IPv4 协议使用的是 OSPF Version 2。下文中所提到的 OSPF 均指 OSPF Version 2。

1.1.1 OSPF的特点

OSPF 具有如下特点：

- 适应范围广：支持各种规模的网络，最多可支持几百台路由器。
- 快速收敛：在网络的拓扑结构发生变化后立即发送更新报文，使这一变化在自治系统中同步。
- 无自环：由于 OSPF 根据收集到的链路状态用最短路径树算法计算路由，从算法本身保证了不会生成自环路由。
- 区域划分：允许自治系统的网络被划分成区域来管理。路由器链路状态数据库的减小降低了内存的消耗和 CPU 的负担；区域间传送路由信息的减少降低了网络带宽的占用。
- 等价路由：支持到同一目的地址的多条等价路由。
- 路由分级：使用 4 类不同的路由，按优先顺序来说分别是：区域内路由、区域间路由、第一类外部路由、第二类外部路由。
- 支持验证：支持基于区域和接口的报文验证，以保证报文交互和路由计算的安全性。
- 组播发送：在某些类型的链路上以组播地址发送协议报文，减少对其他设备的干扰。

1.1.2 OSPF报文类型

OSPF 协议报文直接封装为 IP 报文，协议号为 89。

OSPF 有五种类型的协议报文：

- Hello 报文：周期性发送，用来发现和维持 OSPF 邻居关系，以及进行 DR（Designated Router，指定路由器）/BDR（Backup Designated Router，备份指定路由器）的选举。
- DD（Database Description，数据库描述）报文：描述了本地 LSDB（Link State DataBase，链路状态数据库）中每一条 LSA（Link State Advertisement，链路状态通告）的摘要信息，用于两台路由器进行数据库同步。
- LSR（Link State Request，链路状态请求）报文：向对方请求所需的 LSA。两台路由器互相交换 DD 报文之后，得知对端的路由器有哪些 LSA 是本地的 LSDB 所缺少的，这时需要发送 LSR 报文向对方请求所需的 LSA。
- LSU（Link State Update，链路状态更新）报文：向对方发送其所需要的 LSA。
- LSAck（Link State Acknowledgment，链路状态确认）报文：用来对收到的 LSA 进行确认。

1.1.3 LSA类型

OSPF 中对链路状态信息的描述都是封装在 LSA 中发布出去，常用的 LSA 有以下几种类型：

- Router LSA（Type-1）：由每个路由器产生，描述路由器的链路状态和开销，在其始发的区域内传播。
- Network LSA（Type-2）：由 DR 产生，描述本网段所有路由器的链路状态，在其始发的区域内传播。
- Network Summary LSA（Type-3）：由 ABR（Area Border Router，区域边界路由器）产生，描述区域内某个网段的路由，并通告给其他区域。
- ASBR Summary LSA（Type-4）：由 ABR 产生，描述到 ASBR（Autonomous System Boundary Router，自治系统边界路由器）的路由，通告给相关区域。
- AS External LSA（Type-5）：由 ASBR 产生，描述到 AS（Autonomous System，自治系统）外部的路由，通告到所有的区域（除了 Stub 区域和 NSSA 区域）。
- NSSA External LSA（Type-7）：由 NSSA（Not-So-Stubby Area）区域内的 ASBR 产生，描述到 AS 外部的路由，仅在 NSSA 区域内传播。
- Opaque LSA：用于 OSPF 的扩展通用机制，目前有 Type-9、Type-10 和 Type-11 三种。其中，Type-9 LSA 仅在本地链路范围进行泛洪，用于支持 GR（Graceful Restart，平滑重启）的 Grace LSA 就是 Type-9 的一种类型；Type-10 LSA 仅在区域范围进行泛洪；Type-11 LSA 可以在一个自治系统范围进行泛洪。

1.1.4 OSPF区域

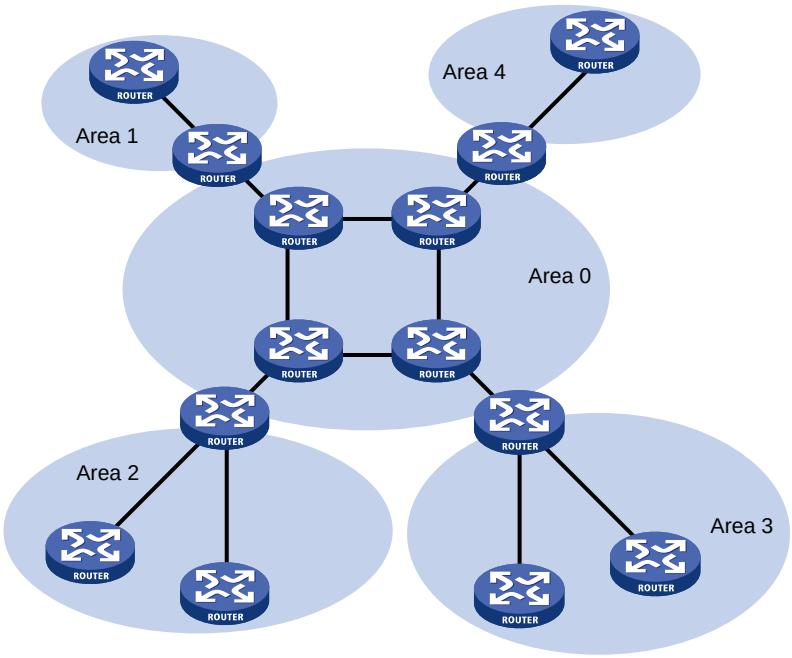
1. 区域划分

随着网络规模日益扩大，当一个大型网络中的路由器都运行 OSPF 协议时，LSDB 会占用大量的存储空间，并使得运行 SPF（Shortest Path First，最短路径优先）算法的复杂度增加，导致 CPU 负担加重。

在网络规模增大之后，拓扑结构发生变化的概率也增大，网络会经常处于“振荡”之中，造成网络中会有大量的 OSPF 协议报文在传递，降低了网络的带宽利用率。更为严重的是，每一次变化都会导致网络中所有的路由器重新进行路由计算。

OSPF协议通过将自治系统划分成不同的区域来解决上述问题。区域是从逻辑上将路由器划分为不同的组，每个组用区域号来标识。如 图 1-1 所示。

图1-1 OSPF 区域划分



区域的边界是路由器，而不是链路。一个路由器可以属于不同的区域，但是一个网段（链路）只能属于一个区域，或者说每个运行 OSPF 的接口必须指明属于哪一个区域。划分区域后，可以在区域边界路由器上进行路由聚合，以减少通告到其他区域的 LSA 数量，还可以将网络拓扑变化带来的影响最小化。

2. 骨干区域（Backbone Area）

OSPF 划分区域之后，并非所有的区域都是平等的关系。其中有一个区域是与众不同的，它的区域号是 0，通常被称为骨干区域。骨干区域负责区域之间的路由，非骨干区域之间的路由信息必须通过骨干区域来转发。对此，OSPF 有两个规定：

- 所有非骨干区域必须与骨干区域保持连通；
- 骨干区域自身也必须保持连通。

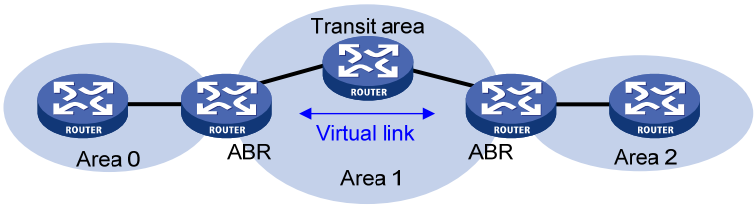
在实际应用中，可能会因为各方面条件的限制，无法满足上面的要求。这时可以通过配置 OSPF 虚连接予以解决。

3. 虚连接（Virtual Link）

虚连接是指在两台 ABR 之间通过一个非骨干区域而建立的一条逻辑上的连接通道。它的两端必须是 ABR，而且必须在两端同时配置方可生效。为虚连接两端提供一条非骨干区域内部路由的区域称为传输区（Transit Area）。

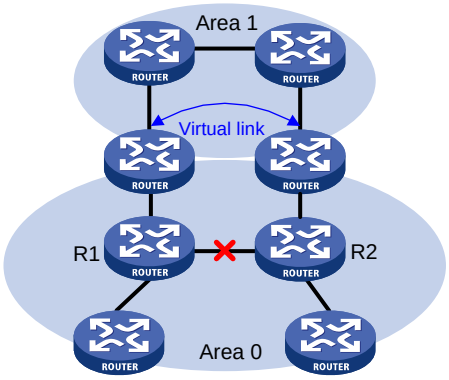
在 图 1-2 中，Area2 与骨干区域之间没有直接相连的物理链路，但可以在ABR上配置虚连接，使Area2通过一条逻辑链路与骨干区域保持连通。

图1-2 虚连接示意图之一



虚连接的另外一个应用是提供冗余的备份链路，当骨干区域因链路故障不能保持连通时，通过虚连接仍然可以保证骨干区域在逻辑上的连通性。如 图 1-3 所示。

图1-3 虚连接示意图之二



虚连接相当于在两个 ABR 之间形成了一个点到点的连接，因此，在这个连接上，和物理接口一样可以配置接口的各参数，如发送 Hello 报文间隔等。

两台 ABR 之间直接传递 OSPF 报文信息，它们之间的 OSPF 路由器只是起到一个转发报文的作用。由于协议报文的目的地址不是中间这些路由器，所以这些报文对于它们而言是透明的，只是当作普通的 IP 报文来转发。

4. Stub区域和Totally Stub区域

Stub 区域是一些特定的区域，该区域的 ABR 会将区域间的路由信息传递到本区域，但不会引入自治系统外部路由，区域中路由器的路由表规模以及 LSA 数量都会大大减少。为保证到自治系统外的路由依旧可达，该区域的 ABR 将生成一条缺省路由 Type-3 LSA，发布给本区域中的其他非 ABR 路由器。

为了进一步减少 Stub 区域中路由器的路由表规模以及 LSA 数量，可以将区域配置为 Totally Stub（完全 Stub）区域，该区域的 ABR 不会将区域间的路由信息和自治系统外部路由信息传递到本区域。为保证到本自治系统的其他区域和自治系统外的路由依旧可达，该区域的 ABR 将生成一条缺省路由 Type-3 LSA，发布给本区域中的其他非 ABR 路由器。

5. NSSA区域和Totally NSSA区域

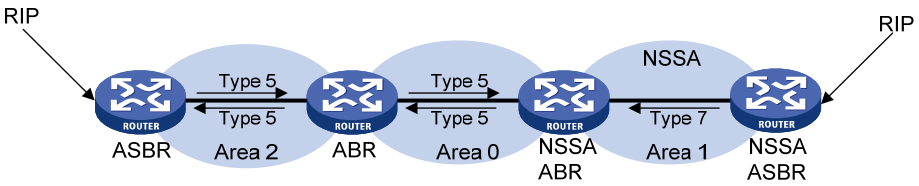
NSSA（Not-So-Stubby Area）区域是 Stub 区域的变形，与 Stub 区域的区别在于 NSSA 区域允许引入自治系统外部路由，由 ASBR 发布 Type-7 LSA 通告给本区域。当 Type-7 LSA 到达 NSSA 的 ABR 时，由 ABR 将 Type-7 LSA 转换成 Type-5 LSA，传播到其他区域。

可以将区域配置为 Totally NSSA（完全 NSSA）区域，该区域的 ABR 不会将区域间的路由信息传递到本区域。为保证到本自治系统的其他区域的路由依旧可达，该区域的 ABR 将生成一条缺省路由 Type-3 LSA，发布给本区域中的其他非 ABR 路由器。

如 图 1-4 所示，运行OSPF协议的自治系统包括 3 个区域：区域 0、区域 1 和区域 2，另外两个自治系统运行RIP协议。区域 1 被定义为NSSA区域，区域 1 接收的RIP路由传播到NSSA ASBR后，由NSSA ASBR产生Type-7 LSA在区域 1 内传播，当Type-7 LSA到达NSSA ABR后，转换成Type-5 LSA传播到区域 0 和区域 2。

另一方面，运行 RIP 的自治系统的 RIP 路由通过区域 2 的 ASBR 产生 Type-5 LSA 在 OSPF 自治系统中传播。但由于区域 1 是 NSSA 区域，所以 Type-5 LSA 不会到达区域 1。

图1-4 NSSA 区域



1.1.5 路由器类型

OSPF 路由器根据在 AS 中的不同位置，可以分为以下四类：

1. 区域内路由器（Internal Router）

该类路由器的所有接口都属于同一个 OSPF 区域。

2. 区域边界路由器ABR

该类路由器可以同时属于两个以上的区域，但其中一个必须是骨干区域。ABR 用来连接骨干区域和非骨干区域，它与骨干区域之间既可以是物理连接，也可以是逻辑上的连接。

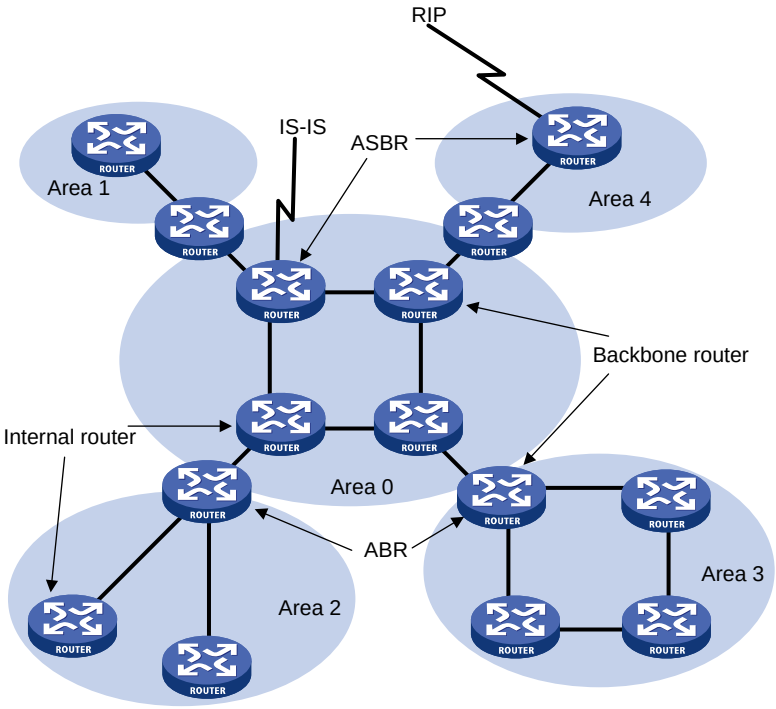
3. 骨干路由器（Backbone Router）

该类路由器至少有一个接口属于骨干区域。因此，所有的 ABR 和位于 Area0 的内部路由器都是骨干路由器。

4. 自治系统边界路由器ASBR

与其他 AS 交换路由信息的路由器称为 ASBR。ASBR 并不一定位于 AS 的边界，它有可能是区域内路由器，也有可能是 ABR。只要一台 OSPF 路由器引入了外部路由的信息，它就成为 ASBR。

图1-5 OSPF 路由器的类型



1.1.6 路由类型

OSPF 将路由分为四类，按照优先级从高到低的顺序依次为：

- 区域内路由（Intra Area）
- 区域间路由（Inter Area）
- 第一类外部路由（Type1 External）：这类路由的可信程度较高，并且和 OSPF 自身路由的开销具有可比性，所以到第一类外部路由的开销等于本路由器到相应的 ASBR 的开销与 ASBR 到该路由目的地址的开销之和。
- 第二类外部路由（Type2 External）：这类路由的可信度比较低，所以 OSPF 协议认为从 ASBR 到自治系统之外的开销远远大于在自治系统之内到达 ASBR 的开销。所以计算路由开销时将主要考虑前者，即到第二类外部路由的开销等于 ASBR 到该路由目的地址的开销。如果计算出开销值相等的两条路由，再考虑本路由器到相应的 ASBR 的开销。

区域内和区域间路由描述的是 AS 内部的网络结构，外部路由则描述了应该如何选择到 AS 以外目的地址的路由。

1.1.7 路由器ID

路由器 ID——即 Router ID，用来在一个自治系统中唯一地标识一台路由器，一台路由器如果要运行 OSPF 协议，则必须存在 Router ID。Router ID 的获取方式有以下两种：

1. 手工指定Router ID

用户可以在创建 OSPF 进程的时候指定 Router ID，配置时，必须保证自治系统中任意两台路由器的 ID 都不相同。通常的做法是将路由器的 ID 配置为与该路由器某个接口的 IP 地址一致。

2. 使用全局Router ID

如果在创建 OSPF 进程的时候没有指定 Router ID，则缺省使用全局 Router ID。建议用户在创建 OSPF 进程的时候手工指定 Router ID，或者选择自动获取 Router ID。

1.1.8 OSPF路由的计算过程

同一个区域内，OSPF 路由的计算过程可简单描述如下：

- 每台 OSPF 路由器根据自己周围的网络拓扑结构生成 LSA，并通过更新报文将 LSA 发送给网络中的其它 OSPF 路由器。
- 每台 OSPF 路由器都会收集其它路由器通告的 LSA，所有的 LSA 放在一起便组成了 LSDB。LSA 是对路由器周围网络拓扑结构的描述，LSDB 则是对整个自治系统的网络拓扑结构的描述。
- OSPF 路由器将 LSDB 转换成一张带权的有向图，这张图便是对整个网络拓扑结构的真实反映。各个路由器得到的有向图是完全相同的。
- 每台路由器根据有向图，使用 SPF 算法计算出一棵以自己为根的最短路径树，这棵树给出了到自治系统中各节点的路由。

1.1.9 OSPF的网络类型

OSPF 根据链路层协议类型将网络分为下列四种类型：

- 广播（Broadcast）类型：当链路层协议是 Ethernet、FDDI 时，缺省情况下，OSPF 认为网络类型是 Broadcast。在该类型的网络中，通常以组播形式（OSPF 路由器的预留 IP 组播地址是 224.0.0.5；OSPF DR/BDR 的预留 IP 组播地址是 224.0.0.6）发送 Hello 报文、LSU 报文和 LSAck 报文；以单播形式发送 DD 报文和 LSR 报文。
- NBMA（Non-Broadcast Multi-Access，非广播多路访问）类型：当链路层协议是帧中继、ATM 或 X.25 时，缺省情况下，OSPF 认为网络类型是 NBMA。在该类型的网络中，以单播形式发送协议报文。
- P2MP（Point-to-MultiPoint，点到多点）类型：没有一种链路层协议会被缺省的认为是 P2MP 类型。P2MP 必须是由其他的网络类型强制更改的，常用做法是将 NBMA 网络改为 P2MP 网络。在该类型的网络中，缺省情况下，以组播形式（224.0.0.5）发送协议报文。可以根据用户需要，以单播形式发送协议报文。
- P2P（Point-to-Point，点到点）类型：当链路层协议是 PPP、HDLC 时，缺省情况下，OSPF 认为网络类型是 P2P。在该类型的网络中，以组播形式（224.0.0.5）发送协议报文。

NBMA 与 P2MP 网络之间的区别如下：

- NBMA 网络是全连通的；P2MP 网络并不需要一定是全连通的。
- NBMA 网络中需要选举 DR 与 BDR；P2MP 网络中没有 DR 与 BDR。
- NBMA 网络采用单播发送报文，需要手工配置邻居；P2MP 网络采用组播方式发送报文，通过配置也可以采用单播发送报文。

1.1.10 DR/BDR

1. DR/BDR简介

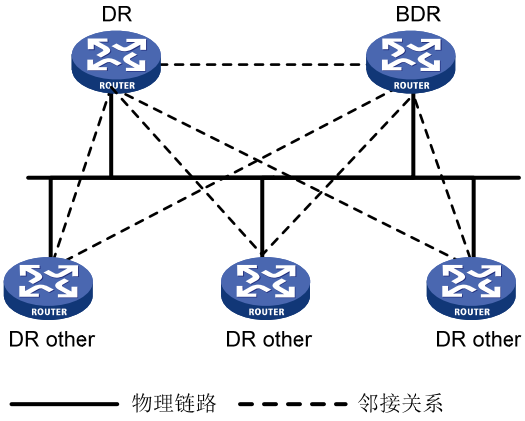
在广播网和 NBMA 网络中，任意两台路由器之间都要交换路由信息。如果网络中有 n 台路由器，则需要建立 n（n-1）/2 个邻接关系。这使得任何一台路由器的路由变化都会导致多次传递，浪费了带宽资源。为解决这一问题，OSPF 提出了 DR 的概念，所有路由器只将信息发送给 DR，由 DR 将网络链路状态发送出去。

另外，OSPF 提出了 BDR 的概念。BDR 是对 DR 的一个备份，在选举 DR 的同时也选举 BDR，BDR 也和本网段内的所有路由器建立邻接关系并交换路由信息。当 DR 失效后，BDR 会立即成为新的 DR。

OSPF 网络中，既不是 DR 也不是 BDR 的路由器为 DR Other。DR Other 仅与 DR 和 BDR 建立邻接关系，DR Other 之间不交换任何路由信息。这样就减少了广播网和 NBMA 网络上各路由器之间邻接关系的数量，同时减少网络流量，节约了带宽资源。

如 图 1-6 所示，进行DR/BDR选举后，5 台路由器之间只需要建立 7 个邻接关系就可以了。

图1-6 DR 和 BDR 示意图



说明

在 OSPF 中，邻居（Neighbor）和邻接（Adjacency）是两个不同的概念。路由器启动后，会通过接口向外发送 Hello 报文，收到 Hello 报文的路由器会检查报文中所定义的参数，如果双方一致就会形成邻居关系。只有当双方成功交换 DD 报文，交换 LSA 并达到 LSDB 同步之后，才形成邻接关系。

---

2. DR/BDR选举过程

DR/BDR 是由同一网段中所有的路由器根据路由器优先级和 Router ID 通过 Hello 报文选举出来的，只有优先级大于 0 的路由器才具有选举资格。

进行 DR/BDR 选举时每台路由器将自己选出的 DR 写入 Hello 报文中，发给网段上每台运行 OSPF 协议的路由器。当处于同一网段的两台路由器同时宣布自己是 DR 时，路由器优先级高者胜出。如果优先级相等，则 Router ID 大者胜出。

需要注意的是：

- 只有在广播或 NBMA 网络中才会选举 DR；在 P2P 或 P2MP 网络中不需要选举 DR。
- DR 是某个网段中的概念，是针对路由器的接口而言的。某台路由器在一个接口上可能是 DR，在另一个接口上有可能是 BDR，或者是 DR Other。
- DR/BDR 选举完毕后，即使网络中加入一台具有更高优先级的路由器，也不会重新进行选举，替换该网段中已经存在的 DR/BDR 成为新的 DR/BDR。DR 并不一定就是路由器优先级最高的路由器接口；同理，BDR 也并不一定就是路由器优先级次高的路由器接口。

1.1.11 协议规范

与 OSPF 相关的协议规范有：

- RFC 1245：OSPF protocol analysis
- RFC 1246：Experience with the OSPF protocol
- RFC 1370：Applicability Statement for OSPF
- RFC 1765：OSPF Database Overflow
- RFC 1793：Extending OSPF to Support Demand Circuits
- RFC 2154：OSPF with Digital Signatures
- RFC 2328：OSPF Version 2
- RFC 3101：OSPF Not-So-Stubby Area (NSSA) Option
- RFC 3166：Request to Move RFC 1403 to Historic Status
- RFC 3509：Alternative Implementations of OSPF Area Border Routers
- RFC 4167：Graceful OSPF Restart Implementation Report
- RFC 4750：OSPF Version 2 Management Information Base
- RFC 4811：OSPF Out-of-Band LSDB Resynchronization
- RFC 4812：OSPF Restart Signaling
- RFC 5088：OSPF Protocol Extensions for Path Computation Element (PCE) Discovery
- RFC 5250：The OSPF Opaque LSA Option
- RFC 5613：OSPF Link-Local Signaling
- RFC 5642：Dynamic Hostname Exchange Mechanism for OSPF
- RFC 5709：OSPFv2 HMAC-SHA Cryptographic Authentication
- RFC 5786：Advertising a Router's Local Addresses in OSPF Traffic Engineering (TE) Extensions
- RFC 6571：Loop-Free Alternate (LFA) Applicability in Service Provider (SP) Networks
- RFC 6860：Hiding Transit-Only Networks in OSPF
- RFC 6987：OSPF Stub Router Advertisement

1.2 OSPF与硬件适配关系

S5110V2-SI、S5000V3-EI 和 S5000E-X 系列交换机不支持 OSPF。

1.3 OSPF配置限制和指导

无论是哪种类型的路由器，都必须先使能 OSPF，否则 OSPF 协议将无法正常运行。在进行各项配置的时候应该先做好网络规划，错误的配置可能会导致相邻路由器之间无法相互传递信息，甚至导致路由信息的阻塞或者产生路由环路。

1.4 OSPF配置任务简介

OSPF 配置任务如下：

(1) 配置OSPF基本功能
- 启动OSPF进程
- 配置OSPF区域
- 使能OSPF功能

(2) （可选）配置OSPF特殊区域
- 配置Stub区域
- 配置NSSA区域
- 配置虚连接

(3) （可选）配置OSPF的网络类型
- 配置OSPF接口网络类型为广播
- 配置OSPF接口网络类型为NBMA
- 配置OSPF接口网络类型为P2MP
- 配置OSPF接口网络类型为P2P

(4) （可选）配置OSPF的路由信息控制
- 配置OSPF区域间路由聚合
- 配置对引入的外部路由信息进行路由聚合
- 配置OSPF对通过接收到的LSA计算出来的路由信息进行过滤
- 配置过滤Type-3 LSA
- 配置OSPF接口的开销值
- 配置OSPF协议的优先级
- 配置NULL0 路由
- 配置OSPF引入外部路由
- 配置OSPF引入缺省路由
- 配置发布一条主机路由

(5) （可选）配置OSPF定时器
- 配置OSPF报文定时器
- 配置接口传送LSA的延迟时间
- 配置OSPF路由计算的时间间隔
- 配置LSA重复到达的最小时间间隔
- 配置LSA重新生成的时间间隔

- 配置OSPF尝试退出overflow状态的定时器时间间隔

(6) （可选）配置OSPF报文相关功能

- 禁止接口收发OSPF报文
- 配置DD报文中的MTU
- 配置OSPF发送协议报文的DSCP优先级
- 配置接口发送OSPF报文的最大长度
- 配置发送LSU报文的速率

(7) （可选）控制LSA的生成、发布与接收

- 配置LSDB中External LSA的最大数量
- 过滤接口出方向的LSA
- 过滤发送给指定邻居的LSA

(8) （可选）加快OSPF路由收敛速度

- 配置ISPF
- 配置前缀抑制
- 配置OSPF的前缀按优先权收敛功能
- 配置PIC

(9) （可选）配置OSPF高级功能

- 配置Stub路由器
- 配置兼容RFC 1583 的外部路由选择规则

(10) （可选）提高 OSPF 网络的可靠性

- 配置OSPF GR
- 配置OSPF NSR
- 配置OSPF与BFD联动
- 配置OSPF快速重路由

(11) （可选）配置 OSPF 安全功能

- 配置OSPF验证
- 配置OSPF GTSM功能

(12) （可选）配置OSPF日志和告警功能

- 配置邻居状态变化的输出开关
- 配置OSPF的日志功能
- 配置OSPF网管功能

1.5 配置OSPF基本功能

1.5.1 启动OSPF进程

(1) 进入系统视图。

```
system-view
```

(2) （可选）配置全局 Router ID。

router id *router-id*

缺省情况下，未配置全局 Router ID。

未配置全局路由器 ID 时，按照下面的规则进行选择：

- 如果存在配置 IP 地址的 Loopback 接口，则选择 Loopback 接口地址中最大的作为 Router ID。
- 如果没有配置IP地址的Loopback接口，则从其他接口的IP地址中选择最大的作为Router ID（不考虑接口的 up/down 状态）。

(3) 进入 OSPF 视图。

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

缺省情况下，系统没有运行 OSPF。

(4) （可选）配置 OSPF 进程描述。

description *text*

缺省情况下，未配置进程描述。

建议用户为每个 OSPF 进程配置进程描述信息，帮助识别进程的用途，以便于记忆和管理。

1.5.2 配置OSPF区域

(1) 进入系统视图。

system-view

(2) （可选）配置全局 Router ID。

router id *router-id*

缺省情况下，未配置全局 Router ID。

(3) 进入 OSPF 视图。

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

缺省情况下，系统没有运行 OSPF。

(4) （可选）配置 OSPF 进程描述。

description *text*

缺省情况下，未配置进程描述。

建议用户为每个 OSPF 进程配置进程描述信息，帮助识别进程的用途，以便于记忆和管理。

(5) 创建 OSPF 区域，并进入 OSPF 区域。

area *area-id*

(6) （可选）配置区域描述。

description *text*

缺省情况下，未配置区域描述。

建议用户为每个区域配置区域描述信息，帮助识别区域的用途，以便于记忆和管理。

(7) （可选）配置允许将区域下的接口从标准拓扑中分离。

capability default-exclusion

缺省情况下，OSPF 区域下的接口自动加入标准拓扑 **base**。

需要在本设备和邻居设备上同时配置本命令，否则会影响邻居关系的建立。

1.5.3 使能OSPF功能

1. 功能简介

要在路由器上使能 OSPF 功能，必须先创建 OSPF 进程、指定该进程关联的区域以及区域包括的网段；对于当前路由器来说，如果某个路由器的接口 IP 地址落在某个区域的网段内，则该接口属于这个区域并使能了 OSPF 功能，OSPF 将把这个接口的直连路由宣告出去。

OSPF 支持多进程，即可以在一台路由器上通过为不同的 OSPF 进程指定不同的进程号来启动多个 OSPF 进程。OSPF 进程号是本地概念，不影响与其它路由器之间的报文交换。因此，不同的路由器之间，即使进程号不同也可以进行报文交换。

2. 配置限制和指导

可以在指定接口上使能 OSPF，或者在指定网段上使能 OSPF。在指定接口上使能 OSPF 的优先级高于在指定网段上使能 OSPF。

在接口上使能 OSPF 时，如果不存在进程和区域，则创建对应的进程和区域；在接口上关闭 OSPF 时，不删除已经创建的进程和区域。

3. 在指定网段上使能OSPF

(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) 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。

一个网段只能属于一个区域。

4. 在指定接口上使能OSPF

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置接口使能 OSPF。

ospf *process-id* **area** *area-id* [**exclude-subip**]

缺省情况下，未配置接口使能 OSPF。

1.6 配置OSPF特殊区域

1.6.1 功能简介

网络管理员对整个网络划分区域完毕后，可以根据组网需要进一步将区域配置成 Stub 区域或 NSSA 区域。

当非骨干区域不能与骨干区域保持连通，或者骨干区域因为各方面条件的限制无法保持连通时，可以通过配置 OSPF 虚连接予以解决。

1.6.2 配置Stub区域

1. 功能简介

对于位于 AS 边缘的一些非骨干区域，我们可以在该区域的所有路由器上配置 **stub** 命令，把该区域配置为 Stub 区域。这样，描述自治系统外部路由的 Type-5 LSA 不会在 Stub 区域里泛洪，减小了路由表的规模。ABR 生成一条缺省路由，所有到达自治系统外部的报文都交给 ABR 进行转发。

如果想进一步减少 Stub 区域路由表规模以及路由信息传递的数量，那么在 ABR 上配置 **stub** 命令时指定 **no-summary** 参数，可以将该区域配置为 Totally Stub 区域。这样，自治系统外部路由和区域间的路由信息都不会传递到本区域，所有目的地是自治系统外和区域外的报文都交给 ABR 进行转发。

Stub 区域和 Totally Stub 区域内不能存在 ASBR，即自治系统外部的路由不能在本区域内传播。

2. 配置限制和指导

骨干区域不能配置成 Stub 区域或 Totally Stub 区域。

如果要将一个区域配置成 Stub 区域，则该区域中的所有路由器必须都要配置 **stub** 命令。

如果要将一个区域配置成 Totally Stub 区域，该区域中的所有路由器必须配置 **stub** 命令，该区域的 ABR 路由器需要配置 **stub no-summary** 命令。

3. 配置步骤

(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) 配置当前区域为 Stub 区域。

stub [**default-route-advertise-always** | **no-summary**] *

缺省情况下，没有区域被设置为 Stub 区域。

(5) （可选）配置 ABR 发送到 Stub 区域缺省路由的开销。

default-cost *cost-value*

缺省情况下，ABR 发送到 Stub 区域缺省路由的开销为 1。

本命令只有在 Stub 区域和 Totally Stub 区域的 ABR 上配置才能生效。

1.6.3 配置NSSA区域

1. 功能简介

Stub 区域不能引入外部路由，为了在允许将自治系统外部路由通告到 OSPF 路由域内部的同时，保持其余部分的 Stub 区域的特征，网络管理员可以将区域配置为 NSSA 区域。NSSA 区域也是位于 AS 边缘的非骨干区域。

配置 **nssa** 命令时指定 **no-summary** 参数可以将该区域配置为 Totally NSSA 区域，该区域的 ABR 不会将区域间的路由信息传递到本区域。

2. 配置限制和指导

骨干区域不能配置成 NSSA 区域或 Totally NSSA 区域。

如果要将一个区域配置成 NSSA 区域，则该区域中的所有路由器必须都要配置 **nssa** 命令。

如果要将一个区域配置成 Totally NSSA 区域，该区域中的所有路由器必须配置 **nssa** 命令，该区域的 ABR 路由器需要配置 **nssa no-summary** 命令。

3. 配置步骤

(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) 配置当前区域为 NSSA 区域。

nssa [**default-route-advertise** [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **type** *type*] * | **no-import-route** | **no-summary** | **suppress-fa** | [[[**translate-always**] [**translate-ignore-checking-backbone**]] | **translate-never**] | **translator-stability-interval** *value*] *

缺省情况下，没有区域被设置为 NSSA 区域。

(5) （可选）配置发送到 NSSA 区域缺省路由的开销。

default-cost *cost-value*

缺省情况下，发送到 NSSA 区域的缺省路由的开销为 1。

本命令只有在 NSSA 区域和 Totally NSSA 区域的 ABR/ASBR 上配置才能生效。

1.6.4 配置虚连接

1. 功能简介

在划分区域之后，非骨干区域之间的 OSPF 路由更新是通过骨干区域来完成交换的。对此，OSPF 要求所有非骨干区域必须与骨干区域保持连通，并且骨干区域自身也要保持连通。

但在实际应用中，可能会因为各方面条件的限制，无法满足这个要求。这时可以通过在 ABR 上配置 OSPF 虚连接予以解决。

2. 配置限制和指导

虚连接不能穿过 Stub 区域和 Totally Stub 区域；虚连接不能穿过 NSSA 区域和 Totally NSSA 区域。

3. 配置步骤

(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) 创建并配置虚连接。

vlink-peer *router-id* [**dead** *seconds* | **hello** *seconds* | { { **hmac-md5** | **md5** } *key-id* { **cipher** | **plain** } *string* | **simple** { **cipher** | **plain** } *string* } | **retransmit** *seconds* | **trans-delay** *seconds*] *

为使虚连接生效，在虚连接的两端都需配置此命令，并且两端配置的 **hello**、**dead** 参数必须一致。

1.7 配置OSPF的网络类型

1.7.1 配置限制和指导

OSPF 的网络类型有四种：广播、NBMA、P2MP 和 P2P。用户可以根据需要更改接口的网络类型，例如：

- 当广播网络中有部分路由器不支持组播时，可以将网络类型更改为 NBMA。
- 如果一网段内只有两台路由器运行 OSPF 协议，也可将接口类型配置为 P2P，节省网络开销。

如果接口配置为广播、NBMA 或者 P2MP 网络类型，只有双方接口在同一网段才能建立邻居关系。

1.7.2 配置OSPF接口网络类型为广播

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置 OSPF 接口网络类型为广播。

ospf network-type broadcast

缺省情况下，接口的网络类型为广播类型。

(4) （可选）配置 OSPF 接口的路由器优先级。

ospf dr-priority *priority*

缺省情况下，接口的路由器优先级为 1。

1.7.3 配置OSPF接口网络类型为NBMA

1. 配置限制和指导

把接口类型配置为 NBMA 后，由于无法通过广播 Hello 报文的形式动态发现相邻路由器，必须手工为接口指定相邻接口的 IP 地址、该相邻接口是否有选举权等（*dr-priority* 参数的值仅表示路由器是否具有 DR 选举权，为 0 表示不具有 DR 选举权，大于 0 时表示具有 DR 选举权）。

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 OSPF 接口的网络类型为 NBMA。

ospf network-type nbma

缺省情况下，接口的网络类型为广播类型。

(4) （可选）配置 OSPF 接口的路由器优先级。

ospf dr-priority *priority*

缺省情况下，接口的路由器优先级为 1。

本命令设置的优先级用于实际的 DR 选举。

(5) 退回系统视图。

quit

(6) 进入 OSPF 视图。

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

(7) 配置 NBMA 网络的邻居。

peer *ip-address* [**dr-priority** *priority*]

缺省情况下，未配置邻居。

如果在配置邻居时将优先级指定为 0，则本地路由器认为该邻居不具备选举权，不向该邻居发送 Hello 报文。本地路由器是 DR 或 BDR 的情况除外。

1.7.4 配置OSPF接口网络类型为P2MP

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置 OSPF 接口的网络类型为 P2MP。

ospf network-type p2mp [**unicast**]

缺省情况下，接口的网络类型为广播类型。

(4) 退回系统视图。

quit

(5) 进入 OSPF 视图。

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

(6) 配置 P2MP 单播网络的邻居。

peer *ip-address* [**cost** *cost-value*]

缺省情况下，未配置邻居。

如果接口类型为 P2MP 单播，必须配置本命令。

1.7.5 配置OSPF接口网络类型为P2P

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置 OSPF 接口的网络类型为 P2P。

ospf network-type p2p [**peer-address-check**]

缺省情况下，接口的网络类型为广播类型。

1.8 配置OSPF的路由信息控制

通过本节的配置，可以控制 OSPF 的路由信息的发布与接收，并引入路由信息。

1.8.1 配置OSPF区域间路由聚合

1. 功能简介

OSPF 区域间路由聚合是指 ABR 将具有相同前缀的路由信息聚合，只发布一条路由到其它区域。

AS 被划分成不同的区域后，每一个区域通过 OSPF 区域边界路由器（ABR）相连，区域间可以通过路由聚合来减少路由信息，减小路由表的规模，提高路由器的运算速度。

ABR 在计算出一个区域的区域内路由之后，根据聚合相关设置，将其中多条 OSPF 路由聚合成一条发送到区域之外。例如，某个区域内有三条区域内路由 19.1.1.0/24，19.1.2.0/24，19.1.3.0/24，如果在 ABR 上配置了路由聚合，将三条路由聚合成一条 19.1.0.0/16，则 ABR 就只生成一条聚合后的 Type-3 LSA，并发布给其它区域的路由器，这样既可以减少其它区域中 LSDB 的规模，也减小了因为网络拓扑变化带来的影响。

2. 配置步骤

(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) 配置 ABR 路由聚合。

abr-summary *ip-address* { *mask-length* | *mask* } [**advertise** | **not-advertise**] [**cost** *cost-value*]

缺省情况下，ABR 不对路由进行聚合。

1.8.2 配置对引入的外部路由信息进行路由聚合

1. 功能简介

ASBR 引入外部路由后，每一条路由都会放在单独的一条 Type-5 LSA 中向外宣告；通过配置路由聚合，路由器只把聚合后的路由放在 Type-5 LSA 中向外宣告，减少了 LSDB 中 LSA 的数量。

在 ASBR 上配置路由聚合后，将对聚合地址范围内的 Type-5 LSA 进行聚合；如果 ASBR 在 NSSA 区域里面，将对聚合地址范围内的 Type-7 LSA 进行聚合。

2. 配置限制和指导

如果本地路由器同时是 ASBR 和 ABR，并且是 NSSA 区域的转换路由器，将对由 Type-7 LSA 转化成的 Type-5 LSA 进行聚合处理；如果不是 NSSA 区域的转换路由器，则不进行聚合处理。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 配置 ASBR 路由聚合。

asbr-summary *ip-address* { *mask-length* | *mask* } [**cost** *cost-value* | **not-advertise** | **nssa-only** | **tag** *tag*] *

缺省情况下，ASBR 不对路由进行聚合。

1.8.3 配置OSPF对通过接收到的LSA计算出来的路由信息进行过滤

1. 功能简介

OSPF 是基于链路状态的动态路由协议，路由信息是根据接收到的 LSA 计算出来的，可以对通过接收到的 LSA 计算出来的 OSPF 路由信息进行过滤。

一共有四种过滤方式：

- 基于要加入到路由表的路由信息的目的地址进行过滤，可以通过配置访问控制列表或 IP 地址前缀列表来指定过滤条件；
- 基于要加入到路由表的路由信息的下一跳进行过滤，可以通过在命令中配置 **gateway** 参数来指定过滤条件；
- 基于要加入到路由表的路由信息的目的地址和下一跳进行过滤，可以通过配置访问控制列表或 IP 地址前缀列表指定过滤目的地址的条件，同时配置 **gateway** 参数来指定过滤下一跳的条件；
- 基于路由策略对要加入到路由表的路由信息进行过滤，可以通过在命令中配置 **route-policy** 参数来指定过滤条件。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 配置 OSPF 对通过接收到的 LSA 计算出来的路由信息进行过滤。

filter-policy { *ipv4-acl-number* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name* | **prefix-list** *prefix-list-name* [**gateway** *prefix-list-name*] | **route-policy** *route-policy-name* } **import**

缺省情况下，OSPF 不对通过接收到的 LSA 计算出来的路由信息进行过滤。

1.8.4 配置过滤Type-3 LSA

1. 功能简介

通过在 ABR 上配置 Type-3 LSA 过滤，可以对进入 ABR 所在区域或 ABR 向其它区域发布的 Type-3 LSA 进行过滤。

2. 配置步骤

(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) 配置对 Type-3 LSA 进行过滤。

filter { *ipv4-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } { **export** | **import** }

缺省情况下，不对 Type-3 LSA 进行过滤。

1.8.5 配置OSPF接口的开销值

1. 功能简介

OSPF 有两种方式来配置接口的开销值：

- 在接口视图下直接配置开销值；
- 配置接口的带宽参考值，OSPF 根据带宽参考值自动计算接口的开销值，计算公式为：接口开销＝带宽参考值÷接口期望带宽（接口期望带宽通过命令 **bandwidth** 进行配置，具体情况请参见接口分册命令参考中的介绍）。当计算出来的开销值大于 65535 时，开销取最大值 65535；当计算出来的开销值小于 1 时，开销取最小值 1。

2. 配置接口的开销值

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 设置 OSPF 接口的开销值。

ospf cost *cost-value*

缺省情况下，接口按照当前的带宽自动计算接口运行 OSPF 协议所需的开销。对于 Loopback 接口，缺省值为 0。

3. 配置带宽参考值

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 配置带宽参考值。

bandwidth-reference *value*

缺省情况下，带宽参考值为 100Mbps。

1.8.6 配置OSPF协议的优先级

1. 功能简介

由于路由器上可能同时运行多个动态路由协议，就存在各个路由协议之间路由信息共享和选择的问题。系统为每一种路由协议设置一个优先级，在不同协议发现同一条路由时，优先级高的路由将被优先选择。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 配置 OSPF 协议的路由优先级。

preference [**ase**] { *preference* | **route-policy** *route-policy-name* } *

缺省情况下，OSPF 协议对自治系统内部路由的优先级为 10，对自治系统外部路由的优先级为 150。

1.8.7 配置NULL0 路由

1. 功能简介

本命令用来配置是否产生 NULL0 路由以及产生 NULL0 路由的优先级。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 配置 NULL0 路由以及 NULL0 路由的优先级。

discard-route { **external** { *preference* | **suppression** } | **internal** { *preference* | **suppression** } } *

缺省情况下，产生引入聚合 NULL0 路由和区域间聚合 NULL0 路由，且 NULL0 路由优先级为 255。

1.8.8 配置OSPF引入外部路由

1. 功能简介

如果在路由器上不仅运行 OSPF，还运行着其它路由协议，可以配置 OSPF 引入其它协议生成的路由，将这些路由信息通过 Type5 LSA 或 Type7 LSA 向外宣告。

OSPF 还可以对引入的路由进行过滤，只将满足过滤条件的外部路由转换为 Type5 LSA 或 Type7 LSA 发布出去。

2. 配置限制和指导

只能引入路由表中状态为 active 的路由，是否为 active 状态可以通过 **display ip routing-table protocol** 命令来查看。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 配置 OSPF 引入外部路由。

import-route { **direct** | **static** } [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

import-route { **ospf** | **rip** } [*process-id* | **all-processes**] [**allow-direct** | **cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

缺省情况下，不引入外部路由。

(4) （可选）配置对引入的路由进行过滤。

filter-policy { *ipv4-acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*]]

缺省情况下，不对引入的路由信息进行过滤。

(5) 配置路由引入时的参数缺省值（开销、标记、类型）。

default { **cost** *cost-value* | **tag** *tag* | **type** *type* } *

缺省情况下，OSPF 引入的路由的度量值为 1，引入的路由的标记为 1，引入的路由类型为 2。

1.8.9 配置OSPF引入缺省路由

1. 功能简介

OSPF 不能通过 **import-route** 命令从其它协议引入缺省路由，如果想把缺省路由引入到 OSPF 路由区域，必须执行本配置。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 配置 OSPF 引入缺省路由。

default-route-advertise [[**always** | **permit-calculate-other**] | **cost** *cost-value* | **route-policy** *route-policy-name* | **type** *type*] *

缺省情况下，不引入缺省路由。

(4) 配置路由引入时的参数缺省值（开销、标记、类型）。

default { **cost** *cost-value* | **tag** *tag* | **type** *type* } *

缺省情况下，OSPF 引入的路由的度量值为 1，引入的路由的标记为 1，引入的路由类型为 2。

1.8.10 配置发布一条主机路由

(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) 配置并发布一条主机路由。

host-advertise *ip-address cost*

缺省情况下，OSPF 不发布所包含网段之外的主机路由。

1.9 配置OSPF定时器

1.9.1 功能简介

通过改变 OSPF 的报文定时器，可以调整 OSPF 网络的收敛速度以及协议报文带来的网络负荷。在一些低速链路上，需要考虑接口传送 LSA 的延迟时间。

1.9.2 配置OSPF报文定时器

1. 功能简介

用户可以在接口上配置下列 OSPF 报文定时器：

- Hello 定时器：接口向邻居发送 Hello 报文的时间间隔，OSPF 邻居之间的 Hello 定时器的值要保持一致。
- Poll 定时器：在 NBMA 网络中，路由器向状态为 down 的邻居路由器发送轮询 Hello 报文的时间间隔。

- 邻居失效时间：在邻居失效时间内，如果接口还没有收到邻居发送的 Hello 报文，路由器就会宣告该邻居无效。
- 接口重传 LSA 的时间间隔：路由器向它的邻居通告一条 LSA 后，需要对方进行确认。若在重传间隔时间内没有收到对方的确认报文，就会向邻居重传这条 LSA。

2. 配置限制和指导

Hello 报文中包含 Hello 定时器和邻居失效时间，对于不同的网络类型，Hello 定时器和邻居失效时间的缺省值不同。修改网络类型时，Hello 定时器和邻居失效时间将恢复为对应网络类型下的缺省值。请确保邻居路由器两端的 Hello 定时器和邻居失效时间的值保持一致，否则将影响 OSPF 邻居关系的建立。

3. 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 Hello 定时器。

ospf timer hello *seconds*

缺省情况下，P2P、Broadcast 类型接口发送 Hello 报文的时间间隔为 10 秒，P2MP、NBMA 类型接口发送 Hello 报文的时间间隔为 30 秒。

(4) 配置 Poll 定时器。

ospf timer poll *seconds*

缺省情况下，发送轮询 Hello 报文的时间间隔为 120 秒。

轮询 Hello 报文的时间间隔至少应为 Hello 时间间隔的 4 倍。

(5) 配置邻居失效时间。

ospf timer dead *seconds*

缺省情况下，P2P、Broadcast 类型接口的 OSPF 邻居失效时间为 40 秒，P2MP、NBMA 类型接口的 OSPF 邻居失效时间为 120 秒。

邻居失效时间应至少为 Hello 时间间隔的 4 倍。

(6) 配置接口重传 LSA 的时间间隔。

ospf timer retransmit *seconds*

缺省情况下，时间间隔为 5 秒。

相邻路由器重传 LSA 时间间隔的值不要设置得太小，否则将会引起不必要的重传。通常应该大于一个报文在两台路由器之间传送一个来回的时间。

1.9.3 配置接口传送LSA的延迟时间

1. 功能简介

考虑到 OSPF 报文在链路上传送时也需要花费时间，所以 LSA 的老化时间（age）在传送之前要增加一定的延迟时间，在低速链路上需要对该项配置进行重点考虑。

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) 配置接口传送 LSA 的延迟时间。

ospf trans-delay *seconds*

缺省情况下，接口传送 LSA 的延迟时间为 1 秒。

1.9.4 配置OSPF路由计算的时间间隔

1. 功能简介

当 OSPF 的 LSDB 发生改变时，需要重新计算最短路径。如果网络频繁变化，且每次变化都立即计算最短路径，将会占用大量系统资源，并影响路由器的效率。通过调节路由计算的时间间隔，可以抑制由于网络频繁变化带来的影响。

本命令在网络变化不频繁的情况下将连续路由计算的时间间隔缩小到 *minimum-interval*，而在网络变化频繁的情况下可以进行相应惩罚，增加 *incremental-interval*×2^{n-2}（n 为连续触发路由计算的次数），将等待时间按照配置的惩罚增量延长，最大不超过 *maximum-interval*。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 配置 OSPF 路由计算的时间间隔。

spf-schedule-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

缺省情况下，OSPF 路由计算的最大时间间隔为 5 秒，最小时间间隔为 50 毫秒，时间间隔惩罚增量为 200 毫秒。

1.9.5 配置LSA重复到达的最小时间间隔

1. 功能简介

如果在重复到达的最小时间间隔内连续收到一条 LSA 类型、LS ID、生成路由器 ID 均相同的 LSA 则直接丢弃，这样就可以抑制网络频繁变化可能导致的占用过多带宽资源和路由器资源。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 配置 LSA 重复到达的最小时间间隔。

lsa-arrival-interval *interval*

缺省情况下，OSPF LSA 重复到达的最小时间间隔为 1000 毫秒。

1.9.6 配置LSA重新生成的时间间隔

1. 功能简介

通过调节 LSA 重新生成的时间间隔，可以抑制网络频繁变化可能导致的占用过多带宽资源和路由器资源。

本命令在网络变化不频繁的情况下将 LSA 重新生成时间间隔缩小到 *minimum-interval*，而在网络变化频繁的情况下可以进行相应惩罚，增加 *incremental-interval*×2^{n-2}（n 为连续触发路由计算的次数），将等待时间按照配置的惩罚增量延长，最大不超过 *maximum-interval*。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 配置 LSA 重新生成的时间间隔。

lsa-generation-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

缺省情况下，最大时间间隔为 5 秒，最小时间间隔为 50 毫秒，惩罚增量为 200 毫秒。

1.9.7 配置OSPF尝试退出overflow状态的定时器时间间隔

1. 功能简介

网络中出现过多 LSA，会占用大量系统资源。当设置的 LSDB 中 External LSA 的最大数量达到上限时，LSDB 会进入 overflow 状态，在 overflow 状态中，不再接收 External LSA，同时删除自己生成的 External LSA，对于已经收到的 External LSA 则不会删除。这样就可以减少 LSA 从而节省系统资源。

通过配置可以调整 OSPF 退出 overflow 状态的时间。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 配置 OSPF 尝试退出 overflow 状态的定时器时间间隔。

lsdb-overflow-interval *interval*

缺省情况下，OSPF 尝试退出 overflow 定时器间隔是 300 秒，配置为 0 时，表示不退出 Overflow 状态。

1.10 配置OSPF报文相关功能

1.10.1 禁止接口收发OSPF报文

1. 功能简介

如果要使 OSPF 路由信息不被某一网络中的路由器获得，可以禁止接口收发 OSPF 报文。

将运行 OSPF 协议的接口指定为 Silent 状态后，该接口的直连路由仍可以由同一路由器的其它接口通过 Router-LSA 发布出去，但 OSPF 报文将被阻塞，接口上无法建立邻居关系。这样可以增强 OSPF 的组网适应能力，减少系统资源的消耗。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 禁止接口收发 OSPF 报文。

silent-interface { *interface-type interface-number* | **all** }

缺省情况下，允许接口收发 OSPF 报文。

不同的进程可以对同一接口禁止收发 OSPF 报文，但本命令只对本进程已经使能的 OSPF 接口起作用，对其它进程的接口不起作用。

1.10.2 配置DD报文中的MTU

1. 功能简介

一般情况下，接口发送 DD 报文时不使用接口的实际 MTU 值，而是用 0 代替。进行此配置后，将使用接口的实际 MTU 值填写 DD 报文 Interface MTU 字段。

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 DD 报文中 MTU 域的值为发送该报文接口的 MTU 值。

ospf mtu-enable

缺省情况下，接口发送的 DD 报文中 MTU 域的值为 0。

1.10.3 配置OSPF发送协议报文的DSCP优先级

1. 功能简介

DSCP 优先级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 OSPF 发送协议报文的 DSCP 优先级。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 配置 OSPF 发送协议报文的 DSCP 优先级。

dscp *dscp-value*

缺省情况下，OSPF 发送协议报文的 DSCP 优先级值为 48。

1.10.4 配置接口发送OSPF报文的最大长度

1. 功能简介

本功能用于需要对接口发送 OSPF 报文的大小进行限制的场景。

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) 配置接口发送 OSPF 报文的最大长度。

ospf packet-size *value*

缺省情况下，接口发送 OSPF 报文的最大长度为本接口的 IP MTU 值。

1.10.5 配置发送LSU报文的速率

1. 功能简介

在与邻居进行 LSDB 同步的过程中，需要发送大量的 LSU 报文时，邻居设备会在短时间内收到大量的 LSU 报文，处理这些突发的大量 LSU 报文时，可能会出现如下情况：

- 占用较多的系统资源，导致邻居设备设备性能下降。
- 邻居设备可能会将维持邻居关系的 Hello 报文丢弃，导致邻居关系断开。重新建立邻居关系的过程中，需要交互的 LSU 数量将会更大，从而加剧设备性能的下降。

配置本功能后，路由器将 LSU 报文分为多个批次进行发送，对 OSPF 接口每次允许发送的 LSU 报文的最大个数做出限制；同时，在指定的时间间隔内，所有运行 OSPF 的接口发送 LSU 的最大个数不能超过限定值，即对整机发送 LSU 的速率进行限制，从而避免上述情况的发生。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启 OSPF 限制 LSU 发送速率功能。

ospf lsu-flood-control [*interval count*]

缺省情况下，OSPF 不对 LSU 的发送速率进行限制。

调整 OSPF 对 LSU 的发送速率时，如果配置不当可能会造成路由异常等情况，请谨慎配置。通常情况下，建议使用缺省值。

(3) 进入 OSPF 视图。

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

(4) （可选）配置接口发送 LSU 报文的时间间隔和一次发送 LSU 报文的最大个数。

transmit-pacing interval *interval* **count** *count*

缺省情况下，OSPF 接口发送 LSU 报文的时间间隔为 20 毫秒，一次最多发送 3 个 LSU 报文。

用户可根据需要配置 OSPF 接口发送 LSU 报文的时间间隔以及接口一次发送 LSU 报文的最大个数。

1.11 控制LSA的生成、发布与接收

1.11.1 配置LSDB中External LSA的最大数量

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 配置 LSDB 中 External LSA 的最大数量。

lsdb-overflow-limit *number*

缺省情况下，不对 LSDB 中 External LSA 的最大条目数进行限制。

1.11.2 过滤接口出方向的LSA

1. 功能简介

通过该功能，不希望让邻居接收到的 LSA 可在本端接口出方向上被过滤掉，从而减小邻居 LSDB 的规模，并节省带宽。

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) 配置过滤接口出方向的 LSA。

ospf database-filter { **all** | { **ase** [**acl** *ipv4-acl-number*] | **nssa** [**acl** *ipv4-acl-number*] | **summary** [**acl** *ipv4-acl-number*] } * }

缺省情况下，不对接口出方向的 LSA 进行过滤。

1.11.3 过滤发送给指定邻居的LSA

1. 功能简介

在 P2MP 网络中，一台路由器可以有多个接口的网络类型为 P2MP 的 OSPF 邻居。当两台路由器之间存在多条 P2MP 链路时，不希望让某个指定邻居收到的 LSA，通过该功能可在本地被过滤掉。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 配置过滤发送给接口的网络类型为 P2MP 的邻居的 LSA。

database-filter peer *ip-address* { **all** | { **ase** [**acl** *ipv4-acl-number*] | **nssa** [**acl** *ipv4-acl-number*] | **summary** [**acl** *ipv4-acl-number*] } * }

缺省情况下，不对发送给接口的网络类型为 P2MP 的邻居的 LSA 进行过滤。

1.12 加快OSPF路由收敛速度

1.12.1 配置ISPF

1. 功能简介

ISPF（Incremental Shortest Path First，增量最短路径优先）是对 OSPF 中最短路径树的增量计算，当网络的拓扑结构发生变化，即影响到最短路径树的结构时，只对受影响的部分节点进行重新计算拓扑结构，只对最短路径树中受影响的部分进行修正，而不需要重建整棵最短路径树。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 开启增量 SPF 计算功能。

ispf enable

缺省情况下，增量 SPF 计算功能处于使能状态。

1.12.2 配置前缀抑制

1. 功能简介

OSPF 使能网段时会将接口上匹配该网段的所有网段路由与主机路由都通过 LSA 发布，但有些时候主机路由或网段路由是不希望被发布的。通过前缀抑制配置，可以减少 LSA 中携带不需要的前缀，即不发布某些网段路由和主机路由，从而提高网络安全性，加快路由收敛。

当使能前缀抑制时，具体情况如下：

- P2P 或 P2MP 类型网络：Type-1 LSA 中不发布接口的主地址，即 Type-1 LSA 中链路类型为 3 的 Stub 链路被抑制，不生成接口路由，但其他路由信息可以正常计算，不会影响流量转发。
- 广播类型或者 NBMA 网络：DR 发布的 Type-2 LSA 的掩码字段会填成 32 位，即不生成网段路由，但其他路由信息可以正常计算，不会影响流量转发。另外，如果没有邻居，发布的 Type-1 LSA 中也不发布接口的主地址，即 Type-1 LSA 中链路类型为 3 的 Stub 链路被抑制。

2. 配置限制和指导

如果需要抑制前缀发布，建议整个 OSPF 网络都配置本命令。

3. 配置全局前缀抑制

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 配置前缀抑制功能。

prefix-suppression

缺省情况下，不抑制 OSPF 进程进行前缀发布。

不能抑制从地址、LoopBack 接口以及处于抑制状态的接口对应的前缀。

4. 配置接口前缀抑制

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置接口的前缀抑制功能。

ospf prefix-suppression [**disable**]

缺省情况下，不抑制接口进行前缀发布。

不能抑制从地址对应的前缀。

1.12.3 配置OSPF的前缀按优先权收敛功能

1. 功能简介

通过策略指定优先权，不同前缀按优先权顺序下发，由高到低分为 4 个优先权（Critical、High、Medium 和 Low），如果一条路由符合多个收敛优先权的匹配规则，则这些收敛优先权中最高者当选为路由的收敛优先权。

OSPF 路由的 32 位主机路由为 Medium 优先权，其它为 Low 优先权。

2. 配置步骤

(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 OSPF 的前缀按优先权快速收敛功能。

prefix-priority route-policy *route-policy-name*

缺省情况下，OSPF 的前缀按优先权快速收敛功能处于关闭状态。

1.12.4 配置PIC

1. 功能简介

PIC（Prefix Independent Convergence，前缀无关收敛），即收敛时间与前缀数量无关，加快收敛速度。传统的路由计算快速收敛都与前缀数量相关，收敛时间与前缀数量成正比。

2. 配置限制和指导

PIC 和 OSPF 快速重路由功能同时配置时，OSPF 快速重路由功能生效。

目前只支持区域间路由以及外部路由的 PIC 功能。

3. 使能PIC功能

(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 PIC 功能。

pic [**additional-path-always**]

缺省情况下，前缀无关收敛功能处于使能状态。

4. 配置PIC支持BFD检测功能（Ctrl方式）

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 使能 OSPF 协议中主用链路的 BFD（Ctrl 方式）检测功能。

ospf primary-path-detect bfd ctrl

缺省情况下，OSPF 协议中主用链路的 BFD（Ctrl 方式）检测功能处于关闭状态。

配置本功能后，可以加快 OSPF 协议的收敛速度。使用 control 报文双向检测方式时，需要建立 OSPF 邻居的两端设备均支持 BFD 配置。

5. 配置PIC支持BFD检测功能（Echo方式）

(1) 进入系统视图。

system-view

(2) 配置 BFD Echo 报文源地址。

bfd echo-source-ip *ip-address*

缺省情况下，未配置 BFD Echo 报文源地址。

echo 报文的源 IP 地址用户可以任意指定。建议配置 echo 报文的源 IP 地址不属于该设备任何一个接口所在网段。

本命令的详细情况请参见“可靠性命令参考”中的“BFD”。

(3) 进入接口视图。

interface *interface-type interface-number*

(4) 使能 OSPF 协议中主用链路的 BFD（Echo 方式）检测功能。

ospf primary-path-detect bfd echo

缺省情况下，OSPF 协议中主用链路的 BFD（Echo 方式）检测功能处于关闭状态。

配置本功能后，可以加快 OSPF 协议的收敛速度。使用 echo 报文单跳检测方式时，仅需要一端设备支持 BFD 配置。

1.13 配置OSPF高级功能

1.13.1 配置Stub路由器

1. 功能简介

Stub 路由器用来控制流量，它告知其他 OSPF 路由器不要使用这个 Stub 路由器来转发数据，但可以拥有一个到 Stub 路由器的路由。

通过将当前路由器配置为 Stub 路由器，在该路由器发布的 Router-LSA 中，当链路类型取值为 3 表示连接到 Stub 网络时，链路度量值不变；当链路类型为 1、2、4 分别表示通过 P2P 链路与另一路由器相连、连接到传送网络、虚连接时，链路度量值将设置为最大值 65535。通过增加 **include-stub** 参数可以将路由器发布的 Router-LSA 中，链路类型为 3 的 Stub 链路度量值设置为最大值 65535。这样其邻居计算出这条路由的开销就会很大，如果邻居上有到这个目的地址开销更小的路由，则数据不会通过这个 Stub 路由器转发。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 配置当前路由器为 Stub 路由器。

stub-router [**external-lsa** [*max-metric-value*] | **include-stub** | **on-startup** *seconds* | **summary-lsa** [*max-metric-value*]] *

缺省情况下，当前路由器没有被配置为 Stub 路由器。

Stub 路由器与 Stub 区域无关。

1.13.2 配置兼容RFC 1583 的外部路由选择规则

1. 功能简介

当有多条路径可以到达同一个外部路由时，在选择最优路由的问题上，RFC 2328 中定义的选路规则与 RFC 1583 的有所不同，进行此配置可以兼容 RFC 1583 中定义的规则。

具体的选路规则如下：

(1) 当 RFC 2328 兼容 RFC 1583 时，所有到达 ASBR 的路由优先级相同。当 RFC 2328 不兼容 RFC 1583 时，非骨干区的区域内路由优先级最高，区域间路由与骨干区区域内路由优先级相同，优选非骨干区的区域内路由，尽量减少骨干区的负担；

(2) 若存在多条优先级相同的路由时，按开销值优选，优选开销值小的路由；

(3) 若存在多条开销值相同路由时，按路由来源区域的区域 ID 选择，优选区域 ID 大的路由。

2. 配置限制和指导

为了避免路由环路，同一路由域内的路由器建议统一配置相同选择规则。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 配置兼容 RFC 1583 的外部路由选择规则。

rfc1583 compatible

缺省情况下，兼容 RFC 1583 的路由选择优先规则的功能处于开启状态。

1.14 配置OSPF GR

1.14.1 功能简介

GR（Graceful Restart，平滑重启）是一种通过备份 OSPF 配置信息，在协议重启或主备倒换时 OSPF 进行平滑重启，从邻居那里获得邻居关系，并对 LSDB 进行同步，从而保证转发业务不中断的机制。

GR 有两个角色：

- GR Restarter：发生协议重启或主备倒换事件且具有 GR 能力的设备。
- GR Helper：和 GR Restarter 具有邻居关系，协助完成 GR 流程的设备。

目前有两种方式实现 OSPF GR 技术：

- 一种是基于 IETF 标准，GR Restarter 通过向 GR Helper 发送一种称为 Grace LSA 的 9 类 Opaque LSA 来控制 GR 的交互过程。
- 另外一种是非 IETF 标准，GR Restarter 与 GR Helper 之间是通过相互发送携带 LLS 与 OOB 扩展信息的 OSPF 报文来完成 GR 的交互过程。

一台设备可以同时充当 GR Restarter 和 GR Helper。

1.14.2 配置限制和指导

设备充当 GR Restarter 后不能再配置 OSPF NSR 功能。

1.14.3 配置GR Restarter

1. 配置IETF标准GR Restarter

(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 Opaque LSA 发布接收能力。

opaque-capability enable

缺省情况下，OSPF 的 Opaque LSA 发布接收能力处于开启状态。

(4) 使能 OSPF 协议的 IETF 标准 GR 能力。

graceful-restart ietf [**global** | **planned-only**] *

缺省情况下，OSPF 协议的 IETF 标准 GR 能力处于关闭状态。

(5) （可选）配置 OSPF 协议的 GR 重启间隔时间。

graceful-restart interval *interval*

缺省情况下，OSPF 协议的 GR 重启间隔时间为 120 秒。

2. 配置非IETF标准GR Restarter

(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 OSPF 本地链路信令能力。

enable link-local-signaling

缺省情况下，OSPF 本地链路信令能力处于关闭状态。

(4) 使能 OSPF 带外同步能力。

enable out-of-band-resynchronization

缺省情况下，OSPF 带外同步能力处于关闭状态。

(5) 使能 OSPF 协议的非 IETF 标准 GR 能力。

graceful-restart [**nonstandard**] [**global** | **planned-only**] *

缺省情况下，OSPF 协议的非 IETF 标准 GR 能力处于关闭状态。

(6) （可选）配置 OSPF 协议的 GR 重启间隔时间。

graceful-restart interval *interval*

缺省情况下，OSPF 协议的 GR 重启间隔时间为 120 秒。

1.14.4 配置GR Helper

1. 配置IETF标准GR Helper

(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 Opaque LSA 发布接收能力。

opaque-capability enable

缺省情况下，OSPF 的 Opaque LSA 发布接收能力处于开启状态。

(4) 使能 GR Helper 能力。

graceful-restart helper enable [**planned-only**]

缺省情况下，OSPF 的 GR Helper 能力处于开启状态。

(5) （可选）配置 GR Helper 严格检查 LSA 能力。

graceful-restart helper strict-lsa-checking

缺省情况下，OSPF 协议的 GR Helper 严格 LSA 检查能力处于关闭状态。

执行本配置后，当检查到 GR Helper 设备的 LSA 发生变化时，Helper 设备退出 GR Helper 模式。

2. 配置非IETF标准GR Helper

(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 OSPF 本地链路信令能力。

enable link-local-signaling

缺省情况下，OSPF 本地链路信令能力处于关闭状态。

(4) 使能 OSPF 带外同步能力。

enable out-of-band-resynchronization

缺省情况下，OSPF 带外同步能力处于关闭状态。

(5) 使能 GR Helper 能力。

graceful-restart helper enable

缺省情况下，OSPF 的 GR Helper 能力处于开启状态。

(6) （可选）配置 GR Helper 严格检查 LSA 能力。

graceful-restart helper strict-lsa-checking

缺省情况下，OSPF 协议的 GR Helper 严格 LSA 检查能力处于关闭状态。

执行本配置后，当检查到 GR Helper 设备的 LSA 发生变化时，Helper 设备退出 GR Helper 模式。

1.14.5 以GR方式重启OSPF进程

1. 功能简介

设备进行主备倒换或者进行如下操作均可以以 GR 方式重启 OSPF 进程。

2. 配置步骤

请在用户视图下执行本命令，以 GR 方式重启 OSPF 进程。

reset ospf [*process-id*] **process graceful-restart**

1.15 配置OSPF NSR

1. 功能简介

NSR（Nonstop Routing，不间断路由）通过将 OSPF 链路状态信息从主进程备份到备进程，使设备在发生主备倒换时可以自行完成链路状态的恢复和路由的重新生成，邻接关系不会发生中断，从而避免了主备倒换对转发业务的影响。

GR 特性需要周边设备配合才能完成路由信息的恢复，在网络应用中有一定的限制。NSR 特性不需要周边设备的配合，网络应用更加广泛。

2. 配置限制和指导

设备配置了 GR NSR 功能后不能再充当 GR Restarter。

3. 配置步骤

(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 OSPF NSR 功能。

non-stop-routing

缺省情况下，OSPF NSR 功能处于关闭状态。

各个进程的 NSR 功能是相互独立的，只对本进程生效。如果存在多个 OSPF 进程，建议在各个进程下使能 OSPF NSR 功能。

1.16 配置OSPF与BFD联动

1.16.1 功能简介

BFD（Bidirectional Forwarding Detection，双向转发检测）能够为 OSPF 邻居之间的链路提供快速检测功能。当邻居之间的链路出现故障时，加快 OSPF 协议的收敛速度。关于 BFD 的介绍和基本功能配置，请参见“可靠性配置指导”中的“BFD”。

OSPF 使用 BFD 来进行快速故障检测时，提供两种检测方式：

- control 报文双向检测：需要建立 OSPF 邻居的两端设备均支持 BFD 配置。
- echo 报文单跳检测：仅需要一端设备支持 BFD 配置。

1.16.2 control报文双向检测

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 使能 OSPF 的 BFD 功能。

ospf bfd enable

缺省情况下，OSPF 的 BFD 功能处于关闭状态。

创建 BFD 会话的通信双方必须处于特定区域的同一网段。

1.16.3 echo报文单跳检测

(1) 进入系统视图。

system-view

(2) 配置 echo 报文源地址。

bfd echo-source-ip *ip-address*

缺省情况下，未配置 echo 报文源地址。

(3) 进入接口视图。

interface *interface-type interface-number*

(4) 使能 OSPF 的 BFD 功能。

ospf bfd enable echo

缺省情况下，OSPF 的 BFD 功能处于关闭状态。

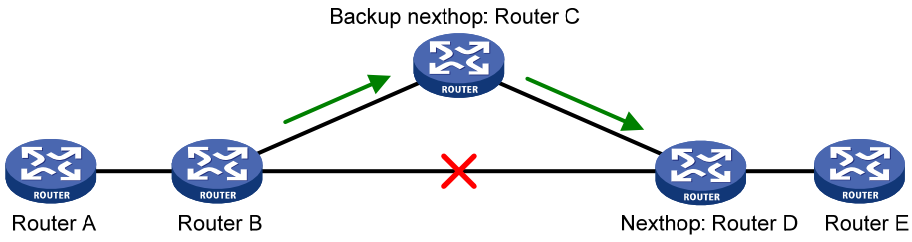
1.17 配置OSPF快速重路由

1.17.1 功能简介

当 OSPF 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输才能到达目的地的报文将会丢失或产生路由环路，数据流量将会被中断，直到 OSPF 根据新的拓扑网络路由收敛完毕后，被中断的流量才能恢复正常的传输。

为了尽可能缩短网络故障导致的流量中断时间，网络管理员可以根据需要配置 OSPF 快速重路由功能。

图1-7 OSPF 快速重路由功能示意图



如 图 1-7 所示，通过在Router B上使能快速重路由功能，OSPF将为路由计算或指定备份下一跳，当Router B检测到网络故障时，OSPF会使用事先获取的备份下一跳替换失效下一跳，通过备份下一跳来指导报文的转发，从而大大缩短了流量中断时间。在使用备份下一跳指导报文转发的同时，OSPF会根据变化后的网络拓扑重新计算最短路径，网络收敛完毕后，使用新计算出来的最优路由来指导报文转发。

网络管理员可以配置给所有 OSPF 路由通过 LFA（Loop Free Alternate）算法选取备份下一跳，也可以在路由策略中指定备份下一跳，为符合过滤条件的路由指定备份下一跳。

1.17.2 配置限制和指导

OSPF 快速重路由功能和 PIC 同时配置时，OSPF 快速重路由功能生效。

1.17.3 配置通过LFA算法选取备份下一跳信息

1. 配置限制和指导

OSPF 快速重路由功能（通过 LFA 算法选取备份下一跳信息）不能与 **vlink-peer** 命令同时使用。

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) （可选）配置接口参与 LFA 计算。

ospf fast-reroute lfa-backup

缺省情况下，接口参与 LFA 计算，能够被选为备份接口。

(4) 退回系统视图。

quit

(5) 进入 OSPF 视图。

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

(6) 配置 OSPF 快速重路由功能（通过 LFA 算法选取备份下一跳信息）。

fast-reroute lfa [**abr-only**]

缺省情况下，OSPF 快速重路由功能处于关闭状态。

abr-only 表示仅选取到 ABR 设备的路由作为备份下一跳。

1.17.4 配置通过路由策略指定备份下一跳

1. 功能简介

网络管理员可以通过 **apply fast-reroute backup-interface** 命令在路由策略中指定备份下一跳，为符合过滤条件的路由指定备份下一跳，关于 **apply fast-reroute backup-interface** 命令以及路由策略的相关配置，请参见“三层技术-IP 路由配置指导”中的“路由策略”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 配置 OSPF 快速重路由功能（通过路由策略指定备份下一跳）。

fast-reroute route-policy *route-policy-name*

缺省情况下，OSPF 快速重路由功能处于关闭状态。

1.17.5 配置OSPF快速重路由支持BFD检测功能（Ctrl方式）

1. 功能简介

OSPF 协议的快速重路由特性中，主用链路缺省不使用 BFD 进行链路故障检测。配置本功能后，将使用 BFD 进行检测，可以加快 OSPF 协议的收敛速度。使用 control 报文双向检测方式时，需要建立 OSPF 邻居的两端设备均支持 BFD 配置。

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) 使能 OSPF 协议中主用链路的 BFD（Ctrl 方式）检测功能。

ospf primary-path-detect bfd ctrl

缺省情况下，OSPF 协议中主用链路的 BFD 检测功能（Ctrl 方式）处于关闭状态。

1.17.6 配置OSPF快速重路由支持BFD检测功能（Echo方式）

1. 功能简介

OSPF 协议的快速重路由特性中，主用链路缺省不使用 BFD 进行链路故障检测。配置本功能后，将使用 BFD 进行检测，可以加快 OSPF 协议的收敛速度。使用 echo 报文单跳检测方式时，仅需要一端设备支持 BFD 配置。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 BFD Echo 报文源地址。

bfd echo-source-ip *ip-address*

缺省情况下，未配置 BFD Echo 报文源地址。

echo 报文的源 IP 地址用户可以任意指定。建议配置 echo 报文的源 IP 地址不属于该设备任何一个接口所在网段。

本命令的详细情况请参见“可靠性命令参考”中的“BFD”。

(3) 进入接口视图。

interface *interface-type interface-number*

(4) 使能 OSPF 协议中主用链路的 BFD（Echo 方式）检测功能。

ospf primary-path-detect bfd echo

缺省情况下，OSPF 协议中主用链路的 BFD（Echo 方式）检测功能处于关闭状态。

1.18 配置OSPF验证

1.18.1 功能简介

从安全性角度来考虑，为了避免路由信息外泄或者 OSPF 路由器受到恶意攻击，OSPF 提供报文验证功能。

OSPF 路由器建立邻居关系时，在发送的报文中会携带配置好的口令，接收报文时进行验证，只有通过验证的报文才能接收，否则将不会接收报文，不能正常建立邻居。

如果区域验证和接口验证都进行了配置，以接口验证的配置为准。

1.18.2 配置区域验证

(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) 配置 OSPF 区域的验证模式。请选择其中一项进行配置。

- 配置 OSPF 区域使用 HMAC-MD5/MD5 验证模式。

  authentication-mode { **hmac-md5** | **md5** } *key-id* { **cipher** | **plain** } *string*

- 配置 OSPF 区域使用简单验证模式。

  authentication-mode simple { **cipher** | **plain** } *string*

缺省情况下，未配置区域验证模式。

一个区域中所有路由器的验证模式和验证密钥必须一致。

1.18.3 配置接口验证

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置 OSPF 接口的验证模式。请选择其中一项进行配置。

- 配置 OSPF 区域使用 HMAC-MD5/MD5 验证模式。

  ospf authentication-mode { **hmac-md5** | **md5** } *key-id* { **cipher** | **plain** } *string*

- 配置 OSPF 区域使用简单验证模式。

  ospf authentication-mode simple { **cipher** | **plain** } *string*

缺省情况下，接口不对 OSPF 报文进行验证。

邻居路由器两端接口的验证模式和验证密钥必须一致。

1.19 配置OSPF GTSM功能

1.19.1 功能简介

GTSM（Generalized TTL Security Mechanism，通用 TTL 安全保护机制）是一种简单易行的、对基于 IP 协议的上层业务进行保护的安全机制。开启 OSPF 报文的 GTSM 功能后，当设备收到来自 OSPF 普通邻居或虚连接邻居的报文时，会判断报文的 TTL 是否在 255-“*hop-count*”+1 到 255 之间。如果在，就上送报文；如果不在，则直接丢弃报文。以使设备避免受到 CPU 利用（CPU-utilization）等类型的攻击（如 CPU 过载），增强系统的安全性。

开启 GTSM 功能的方式有两种：一种是在 OSPF 区域视图下开启，另一种是在接口视图下开启。在 OSPF 区域视图下开启 GTSM 功能会对该区域中所有使能 OSPF 的接口生效；接口视图下开启 GTSM 功能只对当前接口生效。在接口视图下配置的 **hops** 参数的优先级高于在 OSPF 区域视图下配置的 **hops** 参数。

1.19.2 配置限制和指导

开启 OSPF GTSM 功能时，要求本设备和邻居设备上同时配置本特性，指定的 *hop-count* 值可以不同，只要能够满足合法性检查即可。

1.19.3 配置区域GTSM功能

1. 配置限制和指导

该命令对区域中所有使能 OSPF 的接口都会生效，并且只会对来自 OSPF 普通邻居和虚连接邻居的报文进行安全检测。

2. 配置步骤

(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) 开启区域的 OSPF GTSM 功能。

ttl-security [**hops** *hop-count*]

缺省情况下，区域的 OSPF GTSM 功能处于关闭状态。

1.19.4 配置接口GTSM功能

1. 配置限制和指导

该命令只对当前接口生效，并且只会对来自 OSPF 普通邻居和虚连接邻居的报文进行安全检测。

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) 配置开启接口的 OSPF GTSM 功能。

ospf ttl-security [**hops** *hop-count* | **disable**]

缺省情况下，接口的 OSPF GTSM 功能处于关闭状态。

1.20 配置OSPF日志和告警功能

1.20.1 配置邻居状态变化的输出开关

1. 功能简介

打开邻居状态变化的输出开关后，OSPF 邻居状态变化时会生成日志信息发送到设备的信息中心，通过设置信息中心的参数，最终决定日志信息的输出规则（即是否允许输出以及输出方向）。（有关信息中心参数的配置请参见“网络管理和监控配置指导”中的“信息中心”。）

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 打开邻居状态变化的输出开关。

log-peer-change

缺省情况下，邻居状态变化的输出开关处于打开状态。

1.20.2 配置OSPF的日志功能

1. 功能简介

OSPF 的日志信息包括路由计算、邻居、路由、LSA 老化、生成和接收 LSA 的日志信息。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPF 视图。

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

(3) 配置 OSPF 的日志信息个数。

event-log { **lsa-flush** | **peer** | **spf** } **size** *count*

缺省情况下，路由计算、邻居和 LSA 老化的日志信息个数为 10。

1.20.3 配置OSPF网管功能

1. 功能简介

配置 OSPF 进程绑定 MIB 功能后，可以通过网管软件对指定的 OSPF 进程进行管理。

开启 OSPF 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”。）

通过调整 OSPF 在指定时间间隔内允许输出的告警信息条数，可以避免网络出现大量告警信息时对资源的消耗。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 OSPF 进程绑定公有 MIB。

ospf mib-binding *process-id*

缺省情况下，MIB 绑定在进程号最小的 OSPF 进程上。

(3) 开启 OSPF 的告警功能。

snmp-agent trap enable ospf [**authentication-failure** | **bad-packet** | **config-error** | **grhelper-status-change** | **grrestarter-status-change** | **if-state-change** | **lsa-maxage** | **lsa-originate** | **lsdb-approaching-overflow** | **lsdb-overflow** | **neighbor-state-change** | **nssatranslator-status-change** | **retransmit** | **virt-authentication-failure** | **virt-bad-packet** | **virt-config-error** | **virt-retransmit** | **virtgrhelper-status-change** | **virtif-state-change** | **virtneighbor-state-change**] *

缺省情况下，OSPF 的告警功能处于开启状态。

(4) 进入 OSPF 视图。

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

(5) 配置 OSPF 在指定时间间隔内允许输出的告警信息条数。

snmp trap rate-limit interval *trap-interval* **count** *trap-number*

缺省情况下，OSPF 在 10 秒内允许输出 7 条告警信息。

1.21 OSPF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 OSPF 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 OSPF 的统计信息、重启 OSPF 进程或重新向 OSPF 引入外部路由。

表1-1 OSPF 显示和维护

操作	命令
显示OSPF的ABR聚合信息	**display ospf** [*process-id*] [**area** *area-id*] **abr-summary** [*ip-address* { *mask-length* | *mask* }] [**verbose**]
显示区域中FRR备份下一跳候选列表	**display ospf** [*process-id*] [**area** *area-id*] **fast-reroute lfa-candidate**

操作	命令
显示OSPF区域中的拓扑信息	**display ospf** [*process-id*] [**area** *area-id*] **spf-tree** [**verbose**]
显示OSPF的进程信息	**display ospf** [*process-id*] [**verbose**]
显示OSPF ABR及ASBR信息	**display ospf** [*process-id*] **abr-asbr** [**verbose**]
显示OSPF的ASBR聚合信息	**display ospf** [*process-id*] **asbr-summary** [*ip-address* { *mask-length* | *mask* }]
显示OSPF的日志信息	**display ospf** [*process-id*] **event-log** { **lsa-flush** | **peer** | **spf** }
显示OSPF进程的GR状态信息	**display ospf** [*process-id*] **graceful-restart** [**verbose**]
显示OSPF接口信息	**display ospf** [*process-id*] **interface** [*interface-type interface-number* | **verbose**]
显示OSPF的LSDB信息	**display ospf** [*process-id*] [**area** *area-id*] **lsdb** { **asbr** | **network** | **nssa** | **opaque-area** | **opaque-link** | **router** | **summary** } [*link-state-id*] [**originate-router** *advertising-router-id* | **self-originate**] **display ospf** [*process-id*] **lsdb** [**brief** | **originate-router** *advertising-router-id* | **self-originate**] **display ospf** [*process-id*] **lsdb** { **ase** | **opaque-as ase** } [*link-state-id*] [**originate-router** *advertising-router-id* | **self-originate**]
显示进程中的下一跳信息	**display ospf** [*process-id*] **nexthop**
显示OSPF的NSR阶段信息	**display ospf** [*process-id*] **non-stop-routing status**
显示OSPF邻居的信息	**display ospf** [*process-id*] **peer** [**verbose**] [*interface-type interface-number*] [*neighbor-id*]
显示OSPF各区域邻居的统计信息	**display ospf** [*process-id*] **peer statistics**
显示OSPF请求列表	**display ospf** [*process-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*]
显示OSPF重传列表	**display ospf** [*process-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*]
显示OSPF路由表的信息	**display ospf** [*process-id*] **routing** [*ip-address* { *mask-length* | *mask* }] [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*] [**verbose**]
显示OSPF的统计信息	**display ospf** [*process-id*] **statistics** [**error** | **packet** [*interface-type interface-number*]]
显示OSPF虚连接信息	**display ospf** [*process-id*] **vlink**
显示全局Router ID	**display router id**
清除OSPF的日志信息	**reset ospf** [*process-id*] **event-log** [**lsa-flush** | **peer** | **spf**]
重启OSPF进程	**reset ospf** [*process-id*] **process** [**graceful-restart**]
重新向OSPF引入外部路由	**reset ospf** [*process-id*] **redistribution**
清除OSPF的统计信息	**reset ospf** [*process-id*] **statistics**

1.22 OSPF典型配置举例

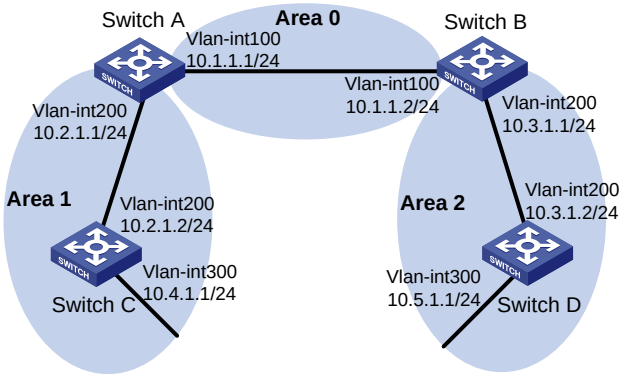
1.22.1 OSPF基本功能配置举例

1. 组网需求

- 所有的交换机都运行 OSPF，并将整个自治系统划分为 3 个区域。
- 其中 Switch A 和 Switch B 作为 ABR 来转发区域之间的路由。
- 配置完成后，每台交换机都应学到 AS 内的到所有网段的路由。

2. 组网图

图1-8 OSPF 基本功能配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置 OSPF 基本配置

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] router id 10.2.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] router id 10.3.1.1
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] area 2
[SwitchB-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
```

```
[SwitchB-ospf-1-area-0.0.0.2] quit
[SwitchB-ospf-1] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] router id 10.4.1.1
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] network 10.4.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

配置 Switch D。

```
<SwitchD> system-view
[SwitchD] router id 10.5.1.1
[SwitchD] ospf
[SwitchD-ospf-1] area 2
[SwitchD-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] network 10.5.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] quit
[SwitchD-ospf-1] quit
```

4. 验证配置

查看 Switch A 的 OSPF 邻居。

```
[SwitchA] display ospf peer verbose

          OSPF Process 1 with Router ID 10.2.1.1
                  Neighbors

 Area 0.0.0.0 interface 10.1.1.1(Vlan-interface100)'s neighbors
 Router ID: 10.3.1.1         Address: 10.1.1.2         GR State: Normal
   State: Full  Mode: Nbr is master  Priority: 1
   DR: 10.1.1.1  BDR: 10.1.1.2  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 37  sec
   Neighbor is up for 06:03:59
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 5

 Area 0.0.0.1 interface 10.2.1.1(Vlan-interface200)'s neighbors
 Router ID: 10.4.1.1         Address: 10.2.1.2         GR State: Normal
   State: Full  Mode: Nbr is master  Priority: 1
   DR: 10.2.1.1  BDR: 10.2.1.2  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 32  sec
   Neighbor is up for 06:03:12
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 5
```

查看 Switch A 的 OSPF 路由信息。

```
[SwitchA] display ospf routing

          OSPF Process 1 with Router ID 10.2.1.1
                  Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 10.2.1.0/24        1        Transit 10.2.1.1        10.2.1.1        0.0.0.1
 10.3.1.0/24        2        Inter   10.1.1.2        10.3.1.1        0.0.0.0
 10.4.1.0/24        2        Stub    10.2.1.2        10.4.1.1        0.0.0.1
 10.5.1.0/24        3        Inter   10.1.1.2        10.3.1.1        0.0.0.0
 10.1.1.0/24        1        Transit 10.1.1.1        10.2.1.1        0.0.0.0

 Total nets: 5
 Intra area: 3  Inter area: 2  ASE: 0  NSSA: 0
```

查看 Switch D 的 OSPF 路由信息。

```
[SwitchD] display ospf routing

          OSPF Process 1 with Router ID 10.5.1.1
                  Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 10.2.1.0/24        3        Inter   10.3.1.1        10.3.1.1        0.0.0.2
 10.3.1.0/24        1        Transit 10.3.1.2        10.3.1.1        0.0.0.2
 10.4.1.0/24        4        Inter   10.3.1.1        10.3.1.1        0.0.0.2
 10.5.1.0/24        1        Stub    10.5.1.1        10.5.1.1        0.0.0.2
 10.1.1.0/24        2        Inter   10.3.1.1        10.3.1.1        0.0.0.2

 Total nets: 5
 Intra area: 2  Inter area: 3  ASE: 0  NSSA: 0
```

在 Switch D 上使用 Ping 进行测试连通性。

```
[SwitchD] ping 10.4.1.1
Ping 10.4.1.1 (10.4.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 10.4.1.1: icmp_seq=0 ttl=253 time=1.549 ms
56 bytes from 10.4.1.1: icmp_seq=1 ttl=253 time=1.539 ms
56 bytes from 10.4.1.1: icmp_seq=2 ttl=253 time=0.779 ms
56 bytes from 10.4.1.1: icmp_seq=3 ttl=253 time=1.702 ms
56 bytes from 10.4.1.1: icmp_seq=4 ttl=253 time=1.471 ms

--- Ping statistics for 10.4.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.779/1.408/1.702/0.323 ms
```

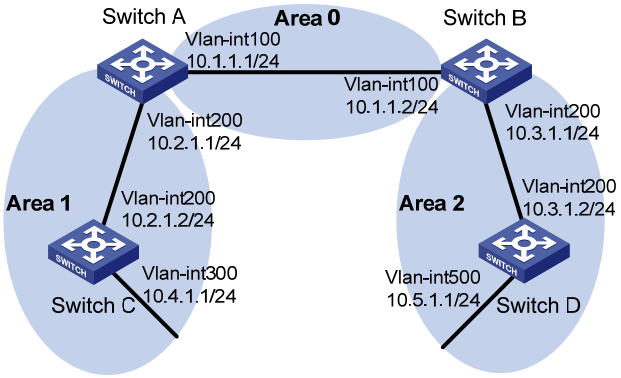
1.22.2 OSPF引入自治系统外部路由配置举例

1. 组网需求

- 所有的交换机都运行 OSPF，整个自治系统划分为 3 个区域。
- 其中 Switch A 和 Switch B 作为 ABR 来转发区域之间的路由。
- 在 Switch C 上配置为 ASBR 引入外部路由（静态路由），且路由信息可正确的在 AS 内传播。

2. 组网图

图1-9 OSPF 引入自治系统外部路由配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置OSPF（同前例“1.22.1 OSPF基本功能配置举例”）

(3) 配置引入自治系统外部路由

在 Switch C 上配置一条到目的网段 3.1.2.0/24 的静态路由。

```
<SwitchC> system-view
[SwitchC] ip route-static 3.1.2.1 24 10.4.1.2
```

在 Switch C 上配置 OSPF 引入静态路由。

```
[SwitchC] ospf 1
[SwitchC-ospf-1] import-route static
```

4. 验证配置

查看 Switch D 的 ABR/ASBR 信息。

```
<SwitchD> display ospf abr-asbr

          OSPF Process 1 with Router ID 10.5.1.1
                 Routing Table to ABR and ASBR


                Topology base (MTID 0)
 Type     Destination     Area            Cost     Nexthop         RtType
 Intra    10.3.1.1        0.0.0.2         10       10.3.1.1        ABR
 Inter    10.4.1.1        0.0.0.2         22       10.3.1.1        ASBR
```

查看 Switch D 的 OSPF 路由表。

```
<SwitchD> display ospf routing
```

```
          OSPF Process 1 with Router ID 10.5.1.1
                  Routing Table

                Topology base (MTID 0)

Routing for network
Destination        Cost     Type    NextHop         AdvRouter       Area
10.2.1.0/24        22       Inter   10.3.1.1        10.3.1.1        0.0.0.2
10.3.1.0/24        10       Transit 10.3.1.2        10.3.1.1        0.0.0.2
10.4.1.0/24        25       Inter   10.3.1.1        10.3.1.1        0.0.0.2
10.5.1.0/24        10       Stub    10.5.1.1        10.5.1.1        0.0.0.2
10.1.1.0/24        12       Inter   10.3.1.1        10.3.1.1        0.0.0.2

Routing for ASEs
Destination        Cost     Type    Tag         NextHop         AdvRouter
3.1.2.0/24         1        Type2   1           10.3.1.1        10.4.1.1

Total nets: 6
Intra area: 2  Inter area: 3  ASE: 1  NSSA: 0
```

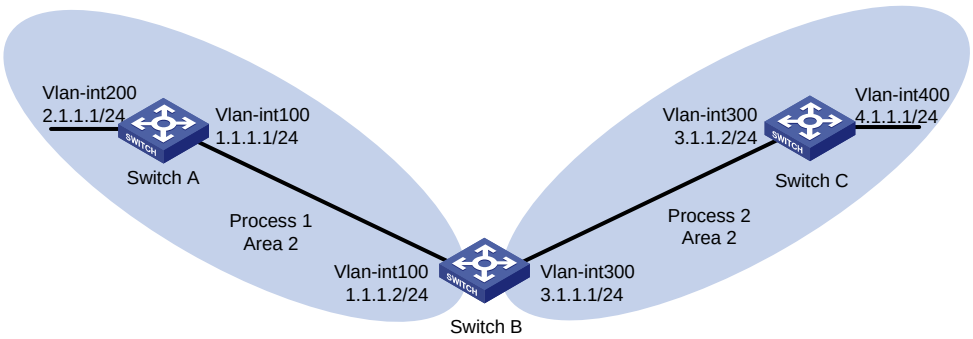
1.22.3 OSPF发布ASBR聚合路由配置举例

1. 组网需求

- Switch A、Switch B 和 Switch C 位于 Area 2 内。
- Switch B 上运行两个 OSPF 进程：1 和 2。Switch B 通过进程 1 和 Switch A 交换路由信息，通过进程 2 和 Switch C 交换路由信息。
- 在 Switch A 的接口 Vlan-interface200 上配置地址 2.1.2.1/24、2.1.3.1/24、2.1.4.1/24，并在 Switch B 上配置 OSPF 进程 2 引入直连路由和 OSPF 进程 1 的路由，使得 Switch C 能够学习到达 2.1.2.0/24、2.1.3.0/24 和 2.1.4.0/24 的路由。
- 为了减小 Switch C 的路由表规模，在 Switch B 上配置 ASBR 路由聚合，只发布聚合后的路由 2.0.0.0/8。

2. 组网图

图1-10 OSPF 发布 ASBR 聚合路由配置组网图



3. 配置步骤

(1) 配置接口的 IP 地址（略）

(2) 配置 OSPF

在 Switch A 上启动 OSPF 进程 1。

```
<SwitchA> system-view
[SwitchA] router id 11.2.1.1
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ip address 2.1.2.1 24
[SwitchA-Vlan-interface200] ip address 2.1.3.1 24 sub
[SwitchA-Vlan-interface200] ip address 2:1.4.1 24 sub
[SwitchA-Vlan-interface200] quit
[SwitchA] ospf 1
[SwitchA-ospf-1] area 2
[SwitchA-ospf-1-area-0.0.0.2] network 1.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.2] network 2.1.0.0 0.0.255.255
[SwitchA-ospf-1-area-0.0.0.2] quit
[SwitchA-ospf-1] quit
```

在 Switch B 上启动两个 OSPF 进程，进程号分别为 1 和 2。

```
<SwitchB> system-view
[SwitchB] router id 11.2.1.2
[SwitchB] ospf 1
[SwitchB-ospf-1] area 2
[SwitchB-ospf-1-area-0.0.0.2] network 1.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.2] quit
[SwitchB-ospf-1] quit
[SwitchB] ospf 2
[SwitchB-ospf-2] area 2
[SwitchB-ospf-2-area-0.0.0.2] network 3.3.3.0 0.0.0.255
[SwitchB-ospf-2-area-0.0.0.2] quit
[SwitchB-ospf-2] quit
```

在 Switch C 上启动 OSPF 进程 2。

```
<SwitchC> system-view
[SwitchC] router id 11.1.1.2
[SwitchC] ospf 2
[SwitchC-ospf-2] area 2
[SwitchC-ospf-2-area-0.0.0.2] network 3.3.3.0 0.0.0.255
[SwitchC-ospf-2-area-0.0.0.2] network 4.4.0.0 0.0.255.255
[SwitchC-ospf-2-area-0.0.0.2] quit
[SwitchC-ospf-2] quit
```

(3) 配置 OSPF 引入外部路由

在 Switch B 上配置 OSPF 进程 2 引入直连路由和 OSPF 进程 1 的路由。

```
[SwitchB] ospf 2
[SwitchB-ospf-2]import-route direct
[SwitchB-ospf-2]import-route ospf 1
```

查看路由引入后 Switch C 的路由表信息。

```
[SwitchC] display ip routing-table
```

```
Destinations : 28       Routes : 28

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
1.1.1.0/24         OSPF    150 1           3.1.1.1         Vlan300
2.1.2.0/24         OSPF    150 1           3.1.1.1         Vlan300
2.1.3.0/24         OSPF    150 1           3.1.1.1         Vlan300
2.1.4.0/24         OSPF    150 1           3.1.1.1         Vlan300
3.1.1.0/24         Direct  0   0           3.1.1.2         Vlan300
3.1.1.0/32         Direct  0   0           3.1.1.2         Vlan300
3.1.1.2/32         Direct  0   0           127.0.0.1       InLoop0
3.1.1.255/32       Direct  0   0           3.1.1.2         Vlan300
4.1.1.0/24         Direct  0   0           4.1.1.1         Loop101
4.1.1.0/32         Direct  0   0           4.1.1.1         Loop101
4.1.1.1/32         Direct  0   0           127.0.0.1       InLoop0
4.1.1.255/32       Direct  0   0           4.1.1.1         Loop101
4.1.2.0/24         Direct  0   0           4.1.2.1         Loop102
4.1.2.0/32         Direct  0   0           4.1.2.1         Loop102
4.1.2.1/32         Direct  0   0           127.0.0.1       InLoop0
4.1.2.255/32       Direct  0   0           4.1.2.1         Loop102
4.1.3.0/24         Direct  0   0           4.1.3.1         Loop103
4.1.3.0/32         Direct  0   0           4.1.3.1         Loop103
4.1.3.1/32         Direct  0   0           127.0.0.1       InLoop0
4.1.3.255/32       Direct  0   0           4.1.3.1         Loop103
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

(4) 配置 OSPF 发布 ASBR 聚合路由

在 Switch B 上配置 OSPF 进程 2 发布 ASBR 聚合路由 2.0.0.0/8。

```
[SwitchB] ospf 2
[SwitchB-ospf-2] asbr-summary 2.0.0.0 8
[SwitchB-ospf-2] quit
```

查看路由聚合后 Switch C 的路由表信息。

```
[SwitchC]display ip routing-table

Destinations : 26       Routes : 26

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
1.1.1.0/24         OSPF    150 1           3.1.1.1         Vlan300
2.0.0.0/8          OSPF    150 1           3.1.1.1         Vlan300
3.1.1.0/24         Direct  0   0           3.1.1.2         Vlan300
3.1.1.0/32         Direct  0   0           3.1.1.2         Vlan300
```

```
3.1.1.2/32          Direct  0   0           127.0.0.1       InLoop0
3.1.1.255/32        Direct  0   0           3.1.1.2         Vlan300
4.1.1.0/24          Direct  0   0           4.1.1.1         Loop101
4.1.1.0/32          Direct  0   0           4.1.1.1         Loop101
4.1.1.1/32          Direct  0   0           127.0.0.1       InLoop0
4.1.1.255/32        Direct  0   0           4.1.1.1         Loop101
4.1.2.0/24          Direct  0   0           4.1.2.1         Loop102
4.1.2.0/32          Direct  0   0           4.1.2.1         Loop102
4.1.2.1/32          Direct  0   0           127.0.0.1       InLoop0
4.1.2.255/32        Direct  0   0           4.1.2.1         Loop102
4.1.3.0/24          Direct  0   0           4.1.3.1         Loop103
4.1.3.0/32          Direct  0   0           4.1.3.1         Loop103
4.1.3.1/32          Direct  0   0           127.0.0.1       InLoop0
4.1.3.255/32        Direct  0   0           4.1.3.1         Loop103
127.0.0.0/8         Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
224.0.0.0/4         Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24        Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
```

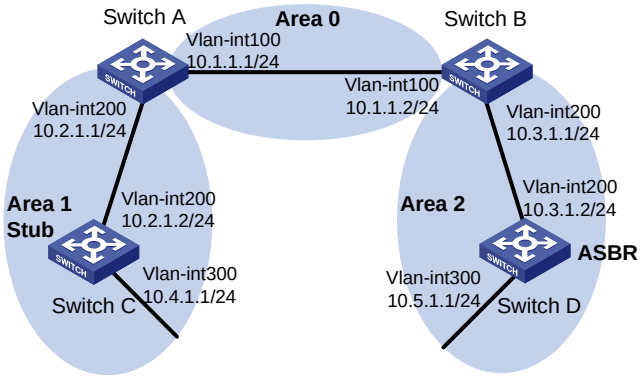
1.22.4 OSPF Stub区域配置举例

1. 组网需求

- 所有的交换机都运行 OSPF，整个自治系统划分为 3 个区域。
- 其中 Switch A 和 Switch B 作为 ABR 来转发区域之间的路由，Switch D 作为 ASBR 引入了外部路由（静态路由）。
- 要求将 Area1 配置为 Stub 区域，减少通告到此区域内的 LSA 数量，但不影响路由的可达性。

2. 组网图

图1-11 OSPF Stub 区域配置组网图



3. 配置步骤

(1) 配置接口的 IP 地址（略）

(2) 配置OSPF（同前例“1.22.1 OSPF基本功能配置举例”）

(3) 配置 Switch D 引入静态路由

```
<SwitchD> system-view
[SwitchD] ip route-static 3.1.2.1 24 10.5.1.2
[SwitchD] ospf
[SwitchD-ospf-1] import-route static
[SwitchD-ospf-1] quit
```

查看 Switch C 的 ABR/ASBR 信息。

```
<SwitchC> display ospf abr-asbr

          OSPF Process 1 with Router ID 10.4.1.1
                  Routing Table to ABR and ASBR


                Topology base (MTID 0)
 Type        Destination     Area            Cost  Nexthop         RtType
 Intra       10.2.1.1        0.0.0.1         3     10.2.1.1        ABR
 Inter       10.5.1.1        0.0.0.1         7     10.2.1.1        ASBR
```

查看 Switch C 的 OSPF 路由表，可以看到路由表中存在 AS 外部的路由。

```
<SwitchC> display ospf routing

          OSPF Process 1 with Router ID 10.4.1.1
                   Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 10.2.1.0/24        3        Transit 0.0.0.0         10.2.1.1        0.0.0.1
 10.3.1.0/24        7        Inter   10.2.1.1        10.2.1.1        0.0.0.1
 10.4.1.0/24        3        Stub    10.4.1.1        10.4.1.1        0.0.0.1
 10.5.1.0/24        17       Inter   10.2.1.1        10.2.1.1        0.0.0.1
 10.1.1.0/24        5        Inter   10.2.1.1        10.2.1.1        0.0.0.1

 Routing for ASEs
 Destination        Cost     Type    Tag         NextHop         AdvRouter
 3.1.2.0/24         1        Type2   1           10.2.1.1        10.5.1.1

 Total nets: 6
 Intra area: 2  Inter area: 3  ASE: 1  NSSA: 0
```

(4) 配置 Area1 为 Stub 区域

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] stub
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] stub
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

查看 Switch C 的 OSPF 路由表，已经看不到 AS 外部的路由，取而代之的是一条缺省路由。

```
[SwitchC] display ospf routing

          OSPF Process 1 with Router ID 10.4.1.1
                  Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 0.0.0.0/0          4        Inter   10.2.1.1        10.2.1.1        0.0.0.1
 10.2.1.0/24        3        Transit 0.0.0.0         10.2.1.1        0.0.0.1
 10.3.1.0/24        7        Inter   10.2.1.1        10.2.1.1        0.0.0.1
 10.4.1.0/24        3        Stub    10.4.1.1        10.4.1.1        0.0.0.1
 10.5.1.0/24        17       Inter   10.2.1.1        10.2.1.1        0.0.0.1
 10.1.1.0/24        5        Inter   10.2.1.1        10.2.1.1        0.0.0.1

 Total nets: 6
 Intra area: 2  Inter area: 4  ASE: 0  NSSA: 0
```

配置 Area1 为 Totally Stub 区域。

```
[SwitchA] ospf
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] stub no-summary
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

查看 Switch C 的 OSPF 路由表，可以看到路由表项进一步减少，只保留了一条通往区域外部的缺省路由。

```
[SwitchC] display ospf routing

          OSPF Process 1 with Router ID 10.4.1.1
                  Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 0.0.0.0/0          4        Inter   10.2.1.1        10.2.1.1        0.0.0.1
 10.2.1.0/24        3        Transit 0.0.0.0         10.4.1.1        0.0.0.1
 10.4.1.0/24        3        Stub    10.4.1.1        10.4.1.1        0.0.0.1
```

```
Total nets: 3
Intra area: 2  Inter area: 1  ASE: 0  NSSA: 0
```

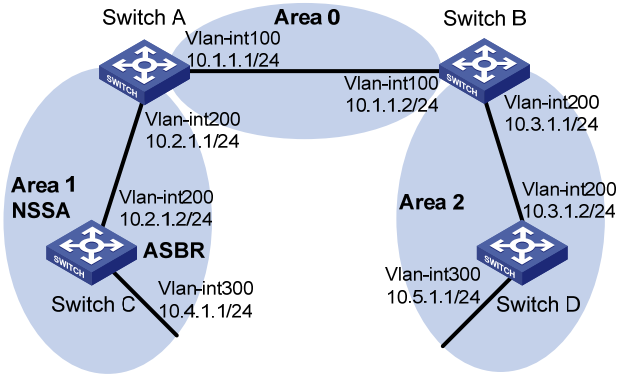
1.22.5 OSPF NSSA区域配置举例

1. 组网需求

- 所有的交换机都运行 OSPF，整个自治系统划分为 3 个区域。
- 其中 Switch A 和 Switch B 作为 ABR 来转发区域之间的路由。
- 要求将 Area1 配置为 NSSA 区域，同时将 Switch C 配置为 ASBR 引入外部路由（静态路由），且路由信息可正确的在 AS 内传播。

2. 组网图

图1-12 OSPF NSSA 区域配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置OSPF（同前例“1.22.1 OSPF基本功能配置举例”）

(3) 配置 Area1 区域为 NSSA 区域

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] nssa
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] nssa
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

查看 Switch C 的 OSPF 路由表。

```
[SwitchC] display ospf routing
```

```
          OSPF Process 1 with Router ID 10.4.1.1
                  Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 10.2.1.0/24        3        Transit 10.2.1.2        10.4.1.1        0.0.0.1
 10.3.1.0/24        7        Inter   10.2.1.1        10.2.1.1        0.0.0.1
 10.4.1.0/24        3        Stub    10.4.1.1        10.4.1.1        0.0.0.1
 10.5.1.0/24        17       Inter   10.2.1.1        10.2.1.1        0.0.0.1
 10.1.1.0/24        5        Inter   10.2.1.1        10.2.1.1        0.0.0.1

 Total nets: 5
 Intra area: 2  Inter area: 3  ASE: 0  NSSA: 0
```

(4) 配置 Switch C 引入静态路由

```
[SwitchC] ip route-static 3.1.3.1 24 10.4.1.2
[SwitchC] ospf
[SwitchC-ospf-1] import-route static
[SwitchC-ospf-1] quit
```

查看 Switch D 的 OSPF 路由表，可以看到 NSSA 区域引入了一条 AS 外部路由。

```
<SwitchD> display ospf routing

                Topology base (MTID 0)

          OSPF Process 1 with Router ID 10.5.1.1
                  Routing Table

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 10.2.1.0/24        22       Inter   10.3.1.1        10.3.1.1        0.0.0.2
 10.3.1.0/24        10       Transit 10.3.1.2        10.3.1.1        0.0.0.2
 10.4.1.0/24        25       Inter   10.3.1.1        10.3.1.1        0.0.0.2
 10.5.1.0/24        10       Stub    10.5.1.1        10.5.1.1        0.0.0.2
 10.1.1.0/24        12       Inter   10.3.1.1        10.3.1.1        0.0.0.2

 Routing for ASEs
 Destination        Cost     Type    Tag         NextHop         AdvRouter
 3.1.3.0/24         1        Type2   1           10.3.1.1        10.2.1.1

 Total nets: 6
 Intra area: 2  Inter area: 3  ASE: 1  NSSA: 0
```

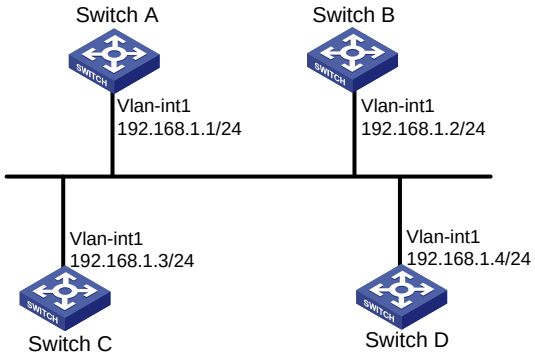
1.22.6 OSPF的DR选择配置举例

1. 组网需求

- Switch A、Switch B、Switch C、Switch D 在同一网段，运行 OSPF 协议；

- 配置 Switch A 为 DR，Switch C 为 BDR。

图1-13 OSPF 的 DR 选择配置组网图



2. 配置思路

(1) 配置各接口的 IP 地址

(2) 配置 OSPF 基本功能

(3) 改变交换机接口的路由器优先级使 Switch A 成为 DR，Switch C 成为 BDR。

3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置 OSPF 基本功能

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] router id 3.3.3.3
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

配置 Switch D。

```
<SwitchD> system-view
[SwitchD] router id 4.4.4.4
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

查看 Switch A 的邻居信息。

```
[SwitchA] display ospf peer verbose

          OSPF Process 1 with Router ID 1.1.1.1
                  Neighbors

 Area 0.0.0.0 interface 192.168.1.1(Vlan-interface1)'s neighbors
 Router ID: 2.2.2.2          Address: 192.168.1.2      GR State: Normal
   State: 2-Way  Mode: None  Priority: 1
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 38  sec
   Neighbor is up for 00:01:31
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled

 Router ID: 3.3.3.3          Address: 192.168.1.3      GR State: Normal
   State: Full  Mode: Nbr is master  Priority: 1
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 31  sec
   Neighbor is up for 00:01:28
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled

 Router ID: 4.4.4.4          Address: 192.168.1.4      GR State: Normal
   State: Full  Mode: Nbr is master  Priority: 1
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 31  sec
   Neighbor is up for 00:01:28
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled
```

可以看到 Switch D 为 DR，Switch C 为 BDR。

(3) 配置接口上的路由器优先级

配置 Switch A。

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ospf dr-priority 100
[SwitchA-Vlan-interface1] quit
```

配置 Switch B。

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ospf dr-priority 0
[SwitchB-Vlan-interface1] quit
```

配置 Switch C。

```
[SwitchC] interface vlan-interface 1
[SwitchC-Vlan-interface1] ospf dr-priority 2
[SwitchC-Vlan-interface1] quit
```

查看 Switch D 的邻居信息。

```
<SwitchD> display ospf peer verbose

          OSPF Process 1 with Router ID 4.4.4.4
                  Neighbors

 Area 0.0.0.0 interface 192.168.1.4(Vlan-interface1)'s neighbors
 Router ID: 1.1.1.1      Address: 192.168.1.1      GR State: Normal
   State: Full  Mode:Nbr is  slave  Priority: 100
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 31  sec
   Neighbor is up for 00:11:17
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled

 Router ID: 2.2.2.2      Address: 192.168.1.2      GR State: Normal
   State: Full  Mode:Nbr is  slave  Priority: 0
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 35  sec
   Neighbor is up for 00:11:19
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled

 Router ID: 3.3.3.3      Address: 192.168.1.3      GR State: Normal
   State: Full  Mode:Nbr is  slave  Priority: 2
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 33  sec
   Neighbor is up for 00:11:15
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled
```

可以看到，网络中 DR/BDR 并没有改变。

说明

网络中 DR/BDR 已经存在的情况下，接口上的路由器优先级的配置并不会立即生效。

(4) 重启 OSPF 进程

重启 Switch D 的进程。

```
<SwitchD> reset ospf 1 process
Warning : Reset OSPF process? [Y/N]:y
```

查看 Switch D 的邻居信息。

```
<SwitchD> display ospf peer verbose

          OSPF Process 1 with Router ID 4.4.4.4
                 Neighbors

 Area 0.0.0.0 interface 192.168.1.4(Vlan-interface1)'s neighbors
 Router ID: 1.1.1.1          Address: 192.168.1.1      GR State: Normal
   State: Full  Mode: Nbr is slave  Priority: 100
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 39  sec
   Neighbor is up for 00:01:40
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled

 Router ID: 2.2.2.2          Address: 192.168.1.2      GR State: Normal
   State: 2-Way  Mode: None  Priority: 0
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 35  sec
   Neighbor is up for 00:01:44
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled

 Router ID: 3.3.3.3          Address: 192.168.1.3      GR State: Normal
   State: Full  Mode: Nbr is slave  Priority: 2
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 39  sec
   Neighbor is up for 00:01:41
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled
```

可以看到 Switch A 成为 DR，Switch C 为 BDR。

说明

如果邻居的状态是 Full，这说明它和邻居之间形成了邻接关系；

如果邻居的状态是 2-Way，则说明它们都不是 DR 或 BDR，两者之间不需要交换 LSA。

查看 OSPF 接口的状态。

```
[SwitchA] display ospf interface

          OSPF Process 1 with Router ID 1.1.1.1
                  Interfaces

 Area: 0.0.0.0
 IP Address      Type      State   Cost  Pri   DR             BDR
 192.168.1.1     Broadcast DR      1     100   192.168.1.1    192.168.1.3

[SwitchB] display ospf interface

          OSPF Process 1 with Router ID 2.2.2.2
                  Interfaces

 Area: 0.0.0.0
 IP Address      Type      State    Cost  Pri   DR             BDR
 192.168.1.2     Broadcast DROther  1     0     192.168.1.1    192.168.1.3
```

说明

如果 OSPF 接口的状态是 DROther，则说明它既不是 DR，也不是 BDR。

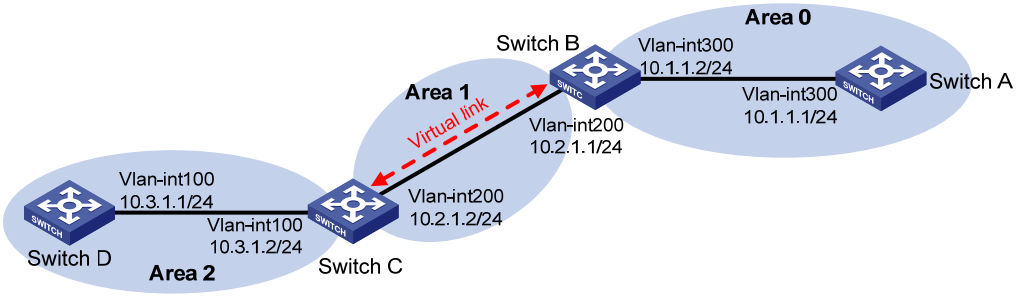
1.22.7 OSPF虚连接配置举例

1. 组网需求

- Area 2 与 Area 0 没有直接相连。Area 1 被用作传输区域（Transit Area）来连接 Area 2 和 Area 0。Switch B 和 Switch C 之间配置一条虚连接。
- 配置完成后，Switch B 能够学到 Area 2 中的路由。

2. 组网图

图1-14 OSPF 虚链路配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置 OSPF 基本功能

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ospf 1 router-id 1.1.1.1
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ospf 1 router-id 2.2.2.2
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] area 1
[SwitchB-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.1] quit
[SwitchB-ospf-1] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ospf 1 router-id 3.3.3.3
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] area 2
[SwitchC-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.2] quit
[SwitchC-ospf-1] quit
```

配置 Switch D。

```
<SwitchD> system-view
[SwitchD] ospf 1 router-id 4.4.4.4
```

```
[SwitchD-ospf-1] area 2
[SwitchD-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] quit
[SwitchD-ospf-1] quit
```

查看 Switch B 的 OSPF 路由表。

```
[SwitchB] display ospf routing

          OSPF Process 1 with Router ID 2.2.2.2
                  Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 10.2.1.0/24        2        Transit 10.2.1.1        3.3.3.3         0.0.0.1
 10.1.1.0/24        2        Transit 10.1.1.2        2.2.2.2         0.0.0.0
 Total nets: 2
 Intra area: 2  Inter area: 0  ASE: 0  NSSA: 0
```

说明

由于 Area 0 没有与 Area 2 直接相连，所以 Switch B 的路由表中没有 Area 2 的路由。

(3) 配置虚连接

配置 Switch B。

```
[SwitchB] ospf
[SwitchB-ospf-1] area 1
[SwitchB-ospf-1-area-0.0.0.1] vlink-peer 3.3.3.3
[SwitchB-ospf-1-area-0.0.0.1] quit
[SwitchB-ospf-1] quit
```

配置 Switch C。

```
[SwitchC] ospf 1
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] vlink-peer 2.2.2.2
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

查看 Switch B 的 OSPF 路由表。

```
[SwitchB] display ospf routing

          OSPF Process 1 with Router ID 2.2.2.2
                  Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 10.2.1.0/24        2        Transit 10.2.1.1        3.3.3.3         0.0.0.1
```

```
10.3.1.0/24        5        Inter   10.2.1.2        3.3.3.3         0.0.0.0
10.1.1.0/24        2        Transit 10.1.1.2        2.2.2.2         0.0.0.0

Total nets: 3
Intra area: 2  Inter area: 1  ASE: 0  NSSA: 0
```

可以看到，Switch B 已经学到了 Area 2 的路由 10.3.1.0/24。

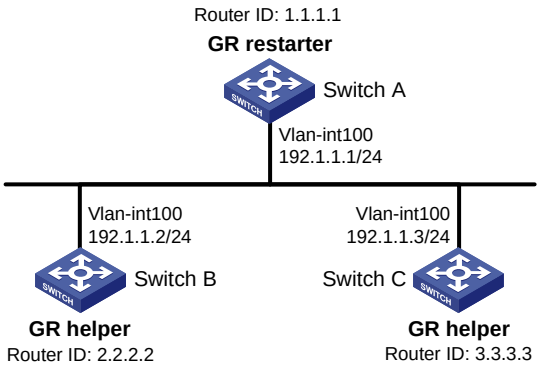
1.22.8 OSPF GR配置举例

1. 组网需求

- Switch A、Switch B 和 Switch C 既属于同一自治系统，也属于同一 OSPF 域，通过 OSPF 协议实现网络互连，并提供 GR 机制。
- Switch A 作为非 IETF 标准 GR Restarter，Switch B 和 Switch C 作为 GR Helper 并且通过 GR 机制与 Switch A 保持带外同步。

2. 组网图

图1-15 OSPF GR 配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置 OSPF 基本功能

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] router id 1.1.1.1
[SwitchA] ospf 100
[SwitchA-ospf-100] area 0
[SwitchA-ospf-100-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[SwitchA-ospf-100-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] router id 2.2.2.2
[SwitchB] ospf 100
[SwitchB-ospf-100] area 0
[SwitchB-ospf-100-area-0.0.0.0] network 192.1.1.0 0.0.0.255
```

```
[SwitchB-ospf-100-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] router id 3.3.3.3
[SwitchC] ospf 100
[SwitchC-ospf-100] area 0
[SwitchC-ospf-100-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[SwitchC-ospf-100-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

(3) 配置 OSPF GR

配置 Switch A 作为非 IETF 标准 GR Restarter，即使能 OSPF 进程 100 的本地链路信令能力、OSPF 带外同步能力和非 IETF 标准 GR 能力。

```
[SwitchA-ospf-100] enable link-local-signaling
[SwitchA-ospf-100] enable out-of-band-resynchronization
[SwitchA-ospf-100] graceful-restart
[SwitchA-ospf-100] quit
```

配置 Switch B 作为 GR Helper，即使能 OSPF 进程 100 的本地链路信令能力和 OSPF 带外同步能力。

```
[SwitchB-ospf-100] enable link-local-signaling
[SwitchB-ospf-100] enable out-of-band-resynchronization
```

配置 Switch C 作为 GR Helper，即使能 OSPF 进程 100 的本地链路信令能力和 OSPF 带外同步能力。

```
[SwitchC-ospf-100] enable link-local-signaling
[SwitchC-ospf-100] enable out-of-band-resynchronization
```

4. 验证配置

打开 Switch A 的 OSPF 平滑启动事件调试信息开关。在 Switch A 上以 GR 方式重启 OSPF 进程。

```
<SwitchA> debugging ospf event graceful-restart
<SwitchA> terminal monitor
<SwitchA> terminal logging level 7
<SwitchA> reset ospf 100 process graceful-restart
Reset OSPF process? [Y/N]:y
%Oct 21 15:29:28:727 2011 SwitchA OSPF/5/OSPF_NBR_CHG: OSPF 100 Neighbor
192.1.1.2(Vlan-interface100) from Full to Down.
%Oct 21 15:29:28:729 2011 SwitchA OSPF/5/OSPF_NBR_CHG: OSPF 100 Neighbor
192.1.1.3(Vlan-interface100) from Full to Down.
*Oct 21 15:29:28:735 2011 SwitchA OSPF/7/DEBUG:
OSPF 100 nonstandard GR Started for OSPF Router
*Oct 21 15:29:28:735 2011 SwitchA OSPF/7/DEBUG:
OSPF 100 created GR wait timer,timeout interval is 40(s).
*Oct 21 15:29:28:735 2011 SwitchA OSPF/7/DEBUG:
OSPF 100 created GR Interval timer,timeout interval is 120(s).
*Oct 21 15:29:28:758 2011 SwitchA OSPF/7/DEBUG:
OSPF 100 created OOB Progress timer for neighbor 192.1.1.3.
*Oct 21 15:29:28:766 2011 SwitchA OSPF/7/DEBUG:
OSPF 100 created OOB Progress timer for neighbor 192.1.1.2.
```

```
%Oct 21 15:29:29:902 2011 SwitchA OSPF/5/OSPF_NBR_CHG: OSPF 100 Neighbor
192.1.1.2(Vlan-interface100) from Loading to Full.
*Oct 21 15:29:29:902 2011 SwitchA OSPF/7/DEBUG:
OSPF 100 deleted OOB Progress timer for neighbor 192.1.1.2.
%Oct 21 15:29:30:897 2011 SwitchA OSPF/5/OSPF_NBR_CHG: OSPF 100 Neighbor
192.1.1.3(Vlan-interface100) from Loading to Full.
*Oct 21 15:29:30:897 2011 SwitchA OSPF/7/DEBUG:
OSPF 100 deleted OOB Progress timer for neighbor 192.1.1.3.
*Oct 21 15:29:30:911 2011 SwitchA OSPF/7/DEBUG:
OSPF GR: Process 100 Exit Restart,Reason : DR or BDR change,for neighbor : 192.1.1.3.
*Oct 21 15:29:30:911 2011 SwitchA OSPF/7/DEBUG:
OSPF 100 deleted GR Interval timer.
*Oct 21 15:29:30:912 2011 SwitchA OSPF/7/DEBUG:
OSPF 100 deleted GR wait timer.
%Oct 21 15:29:30:920 2011 SwitchA OSPF/5/OSPF_NBR_CHG: OSPF 100 Neighbor
192.1.1.2(Vlan-interface100) from Full to Down.
%Oct 21 15:29:30:921 2011 SwitchA OSPF/5/OSPF_NBR_CHG: OSPF 100 Neighbor
192.1.1.3(Vlan-interface100) from Full to Down.
%Oct 21 15:29:33:815 2011 SwitchA OSPF/5/OSPF_NBR_CHG: OSPF 100 Neighbor
192.1.1.3(Vlan-interface100) from Loading to Full.
%Oct 21 15:29:35:578 2011 SwitchA OSPF/5/OSPF_NBR_CHG: OSPF 100 Neighbor
192.1.1.2(Vlan-interface100) from Loading to Full.
```

从上面的信息可以看出 Switch A 完成了 GR。

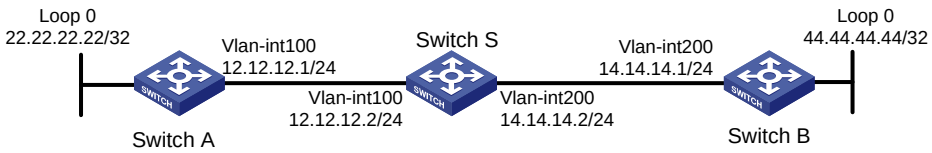
1.22.9 OSPF NSR配置举例

1. 组网需求

Switch S、Switch A、Switch B 属于同一 OSPF 区域，通过 OSPF 协议实现网络互连。要求对 Switch S 进行主备倒换时，Switch A 和 Switch B 到 Switch S 的邻居没有中断，Switch A 到 Switch B 的流量没有中断。

2. 组网图

图1-16 OSPF NSR 配置组网图



3. 配置步骤

(1) 配置各路由器接口的 IP 地址和 OSPF 协议

请按照上面组网图配置各接口的 IP 地址和子网掩码，具体配置过程略。

配置各交换机之间采用 OSPF 协议进行互连，确保 Switch S、Switch A 和 Switch B 之间能够在网络层互通，并且各交换机之间能够借助 OSPF 协议实现动态路由更新。具体配置过程略。

(2) 配置 OSPF NSR

使能 Switch S 的 OSPF NSR 功能。

```
<SwitchS> system-view
[SwitchS] ospf 100
[SwitchS-ospf-100] non-stop-routing
[SwitchS-ospf-100] quit
```

4. 验证配置

Switch S 进行主备倒换。

```
[SwitchS] placement reoptimize
Predicted changes to the placement
Program                           Current location       New location
-------------------------------------------------------------------
rib                               0/0                    0/0
staticroute                       0/0                    0/0
ospf                              0/0                    0/0
Continue? [y/n]:y
Re-optimization of the placement start. You will be notified on completion
Re-optimization of the placement complete. Use 'display placement' to view the new placement
```

查看 Switch A 上 OSPF 协议的邻居和路由。

```
<SwitchA> display ospf peer

          OSPF Process 1 with Router ID 2.2.2.1
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 3.3.3.1         12.12.12.2      1   37         Full/BDR          Vlan100
<SwitchA> display ospf routing

          OSPF Process 1 with Router ID 2.2.2.1
                  Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 44.44.44.44/32     2        Stub    12.12.12.2      4.4.4.1         0.0.0.0
 14.14.14.0/24      2        Transit 12.12.12.2      4.4.4.1         0.0.0.0
 22.22.22.22/32     0        Stub    22.22.22.22     2.2.2.1         0.0.0.0
 12.12.12.0/24      1        Transit 12.12.12.1      2.2.2.1         0.0.0.0

 Total nets: 4
 Intra area: 4  Inter area: 0  ASE: 0  NSSA: 0
```

查看 Switch B 上 OSPF 协议的邻居和路由。

```
<SwitchB> display ospf peer

          OSPF Process 1 with Router ID 4.4.4.1
               Neighbor Brief Information
```

```
 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 3.3.3.1         14.14.14.2      1   39         Full/BDR          Vlan200
<SwitchB> display ospf routing

          OSPF Process 1 with Router ID 4.4.4.1
                  Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 44.44.44.44/32     0        Stub    44.44.44.44     4.4.4.1         0.0.0.0
 14.14.14.0/24      1        Transit 14.14.14.1      4.4.4.1         0.0.0.0
 22.22.22.22/32     2        Stub    14.14.14.2      2.2.2.1         0.0.0.0
 12.12.12.0/24      2        Transit 14.14.14.2      2.2.2.1         0.0.0.0

 Total nets: 4
 Intra area: 4  Inter area: 0  ASE: 0  NSSA: 0
```

通过上面信息可以看出在 Switch S 发生主备倒换的时候，Switch A 和 Switch B 的邻居和路由信息保持不变，从 Switch A 到 Switch B 的流量转发没有受到主备倒换的影响。

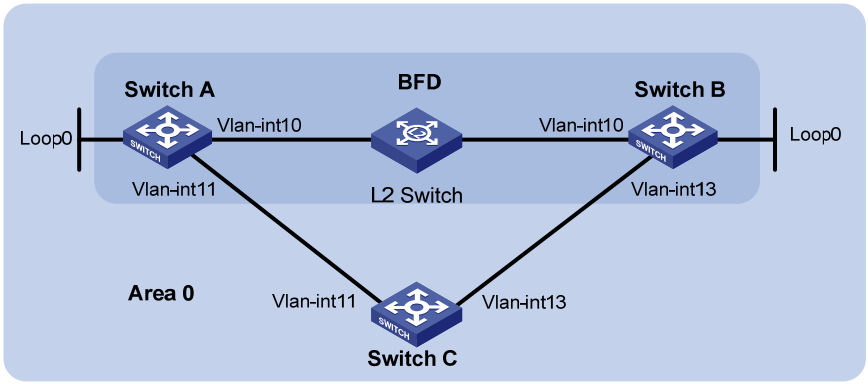
1.22.10 OSPF与BFD联动配置举例

1. 组网需求

- Switch A、Switch B 和 Switch C 上运行 OSPF，网络层相互可达。
- 当 Switch A 和 Switch B 通过 L2 Switch 通信的链路出现故障时 BFD 能够快速感知通告 OSPF 协议，并且切换到 Switch C 进行通信。

2. 组网图

图1-17 OSPF 与 BFD 联动配置组网图



设备	接口	IP地址	设备	接口	IP地址
Switch A	Vlan-int10	192.168.0.102/24	Switch B	Vlan-int10	192.168.0.100/24

设备	接口	IP地址	设备	接口	IP地址
	Vlan-int11	10.1.1.102/24		Vlan-int13	13.1.1.1/24
	Loop0	121.1.1.1/32		Loop0	120.1.1.1/32
Switch C	Vlan-int11	10.1.1.100/24			
	Vlan-int13	13.1.1.2/24			

3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置 OSPF 基本功能

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 121.1.1.1 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 120.1.1.1 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

(3) 配置 BFD 功能

在 Switch A 上使能 BFD 检测功能，并配置 BFD 参数。

```
[SwitchA] bfd session init-mode active
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ospf bfd enable
[SwitchA-Vlan-interface10] bfd min-transmit-interval 500
[SwitchA-Vlan-interface10] bfd min-receive-interval 500
[SwitchA-Vlan-interface10] bfd detect-multiplier 7
[SwitchA-Vlan-interface10] quit
```

在 Switch B 上使能 BFD 检测功能，并配置 BFD 参数。

```
[SwitchB] bfd session init-mode active
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] ospf bfd enable
[SwitchB-Vlan-interface10] bfd min-transmit-interval 500
[SwitchB-Vlan-interface10] bfd min-receive-interval 500
[SwitchB-Vlan-interface10] bfd detect-multiplier 6
[SwitchB-Vlan-interface10] quit
```

4. 验证配置

下面以 Switch A 为例，Switch B 和 Switch A 类似，不再赘述。

显示 Switch A 的 BFD 信息。

```
<SwitchA> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 Session Working Under Ctrl Mode:

 LD/RD          SourceAddr      DestAddr        State    Holdtime    Interface
 3/1            192.168.0.102   192.168.0.100   Up       1700ms      Vlan10
```

在 Switch A 上查看 120.1.1.1/32 的路由信息，可以看出 Switch A 和 Switch B 是通过 L2 Switch 进行通信的。

```
<SwitchA> display ip routing-table 120.1.1.1 verbose

Summary Count : 1

Destination: 120.1.1.1/32
   Protocol: O_INTRA
 Process ID: 1
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 1              Preference: 10
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                   State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NibID: 0x26000002         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c       OrigNextHop: 192.168.0.100
      Label: NULL          RealNextHop: 192.168.0.100
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid         Interface: Vlan-interface10
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                PathID: 0x0
```

当 Switch A 和 Switch B 通过 L2 Switch 通信的链路出现故障时：

在 Switch A 上查看 120.1.1.1/32 的路由信息，可以看出 Switch A 和 Switch B 已经切换到 Switch C 进行通信。

```
<SwitchA> display ip routing-table 120.1.1.1 verbose
```

```
Summary Count : 1

Destination: 120.1.1.1/32
   Protocol: O_INTRA
 Process ID: 1
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 2              Preference: 10
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                   State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NibID: 0x26000002         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c       OrigNextHop: 10.1.1.100
      Label: NULL          RealNextHop: 10.1.1.100
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid         Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0
```

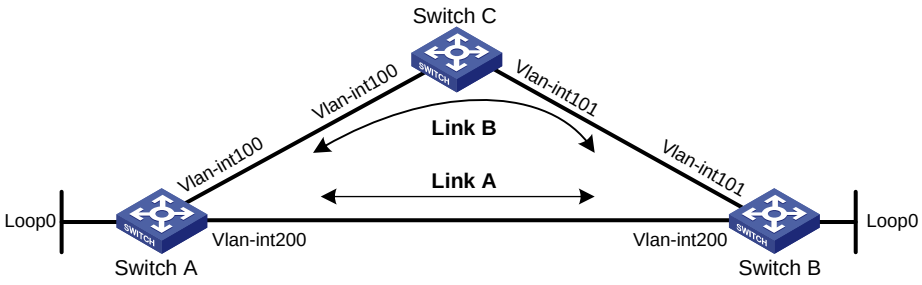
1.22.11 OSPF快速重路由配置举例

1. 组网需求

如 图 1-18 所示，Switch A、Switch B和Switch C属于同一OSPF区域，通过OSPF协议实现网络互连。要求当Switch A和Switch B之间的链路出现故障时，业务可以快速切换到链路B上。

2. 组网图

图1-18 OSPF 快速重路由配置组网图



设备	接口	IP地址	设备	接口	IP地址
Switch A	Vlan-int100	12.12.12.1/24	Switch B	Vlan-int101	24.24.24.4/24
	Vlan-int200	13.13.13.1/24		Vlan-int200	13.13.13.2/24
	Loop0	1.1.1.1/32		Loop0	4.4.4.4/32
Switch C	Vlan-int100	12.12.12.2/24			
	Vlan-int101	24.24.24.2/24			

3. 配置步骤

(1) 配置各交换机接口的 IP 地址和 OSPF 协议

请按照上面组网图配置各接口的 IP 地址和子网掩码，具体配置过程略。

配置各交换机之间采用 OSPF 协议进行互连，确保 Switch A、Switch B 和 Switch C 之间能够在网络层互通，并且各交换机之间能够借助 OSPF 协议实现动态路由更新。

具体配置过程略。

(2) 配置 OSPF 快速重路由

OSPF 支持快速重路由配置有两种配置方法，可以任选一种。

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

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ospf 1
[SwitchA-ospf-1] fast-reroute lfa
[SwitchA-ospf-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ospf 1
[SwitchB-ospf-1] fast-reroute lfa
[SwitchB-ospf-1] quit
```

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

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ip prefix-list abc index 10 permit 4.4.4.4 32
[SwitchA] route-policy frr permit node 10
[SwitchA-route-policy-frr-10] if-match ip address prefix-list abc
[SwitchA-route-policy-frr-10] apply fast-reroute backup-interface vlan-interface 100
backup-nexthop 12.12.12.2
[SwitchA-route-policy-frr-10] quit
[SwitchA] ospf 1
[SwitchA-ospf-1] fast-reroute route-policy frr
[SwitchA-ospf-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ip prefix-list abc index 10 permit 1.1.1.1 32
[SwitchB] route-policy frr permit node 10
[SwitchB-route-policy-frr-10] if-match ip address prefix-list abc
[SwitchB-route-policy-frr-10] apply fast-reroute backup-interface vlan-interface 101
backup-nexthop 24.24.24.2
[SwitchB-route-policy-frr-10] quit
[SwitchB] ospf 1
[SwitchB-ospf-1] fast-reroute route-policy frr
[SwitchB-ospf-1] quit
```

4. 验证配置

在 Switch A 上查看 4.4.4.4/32 网段路由，可以看到备份下一跳信息。

```
[SwitchA] display ip routing-table 4.4.4.4 verbose

Summary Count : 1

Destination: 4.4.4.4/32
   Protocol: O_INTRA
 Process ID: 1
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 1              Preference: 10
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Active Adv
  OrigTblID: 0x0              OrigVrf: default-vrf
    TableID: 0x2               OrigAs: 0
      NibID: 0x26000002        LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c       OrigNextHop: 13.13.13.2
      Label: NULL          RealNextHop: 13.13.13.2
    BkLabel: NULL            BkNextHop: 12.12.12.2
  Tunnel ID: Invalid         Interface: Vlan-interface200
BkTunnel ID: Invalid       BkInterface: Vlan-interface100
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                PathID: 0x0
```

在 Switch B 上查看 1.1.1.1/32 网段路由，可以看到备份下一跳信息。

```
[SwitchB] display ip routing-table 1.1.1.1 verbose

Summary Count : 1

Destination: 1.1.1.1/32
   Protocol: O_INTRA
 Process ID: 1
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 1              Preference: 10
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Active Adv
  OrigTblID: 0x0              OrigVrf: default-vrf
    TableID: 0x2               OrigAs: 0
      NibID: 0x26000002        LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c       OrigNextHop: 13.13.13.1
      Label: NULL          RealNextHop: 13.13.13.1
    BkLabel: NULL            BkNextHop: 24.24.24.2
  Tunnel ID: Invalid         Interface: Vlan-interface200
BkTunnel ID: Invalid       BkInterface: Vlan-interface101
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                PathID: 0x0
```

1.23 常见配置错误举例

1.23.1 OSPF邻居无法建立

1. 故障现象

OSPF 邻居无法建立。

2. 分析

如果物理连接和下层协议正常，则检查接口上配置的 OSPF 参数，必须保证与相邻路由器的参数一致，区域号相同，网段与掩码也必须一致（点到点与虚连接的网段与掩码可以不同）。

3. 处理过程

(1) 使用 **display ospf peer** 命令查看 OSPF 邻居状态。

(2) 使用 **display ospf interface** 命令查看 OSPF 接口的信息。

(3) 检查物理连接及下层协议是否正常运行，可通过 **ping** 命令测试。若从本地路由器 Ping 对端路由器不通，则表明物理连接和下层协议有问题。

(4) 检查 OSPF 定时器，在同一接口上邻居失效时间应至少为 Hello 报文发送时间间隔的 4 倍。

(5) 如果是 NBMA 网络，则应该使用 **peer ip-address** 命令手工指定邻居。

(6) 如果网络类型为广播网或 NBMA，则至少有一个接口的路由器优先级大于零。

1.23.2 OSPF路由信息不正确

1. 故障现象

OSPF 不能发现其他区域的路由。

2. 分析

应保证骨干区域与所有的区域相连接。若一台路由器配置了两个以上的区域，则至少有一个区域应与骨干区域相连。骨干区域不能配置成 Stub 区域。

在 Stub 区域内的路由器不能接收外部 AS 的路由。如果一个区域配置成 Stub 区域，则与这个区域相连的所有路由器都应将此区域配置成 Stub 区域。

3. 处理过程

(1) 使用 **display ospf peer** 命令查看 OSPF 邻居状态。

(2) 使用 **display ospf interface** 命令查看 OSPF 接口的信息。

(3) 使用 **display ospf lsdb** 查看 LSDB 的信息是否完整。

(4) 使用 **display current-configuration configuration ospf** 命令查看区域是否配置正确。若配置了两个以上的区域，则至少有一个区域与骨干区域相连。

(5) 如果某区域是 Stub 区域，则该区域中的所有路由器都要配置 **stub** 命令；如果某区域是 NSSA 区域，则该区域中的所有路由器都要配置 **nssa** 命令。

(6) 如果配置了虚连接，使用 **display ospf vlink** 命令查看 OSPF 虚连接是否正常。

目 录

1 策略路由

1.1 策略路由简介

与单纯依照 IP 报文的目的地址查找路由表进行转发不同，策略路由是一种依据用户制定的策略进行路由转发的机制。策略路由可以对于满足一定条件（ACL 规则）的报文，执行指定的操作（设置报文的下一跳）。

1.1.1 报文的转发流程

报文到达后，其后续的转发流程如下：

- 首先根据配置的策略路由转发。
- 若找不到匹配的节点，或虽然找到了匹配的节点但指导报文转发失败时，根据路由表中除缺省路由之外的路由来转发报文。
- 若转发失败，则再根据缺省路由来转发报文。

1.1.2 策略路由类型

根据作用对象的不同，策略路由可分为以下三种类型：

- 本地策略路由：对设备本身产生的报文（比如本地发出的 ping 报文）起作用，指导其发送。
- 转发策略路由：对接口接收的报文起作用，指导其转发。

1.1.3 策略简介

策略用来定义报文的匹配规则，以及对报文执行的操作。策略由节点组成。

一个策略可以包含一个或者多个节点。节点的构成如下：

- 每个节点由节点编号来标识。节点编号越小节点的优先级越高，优先级高的节点优先被执行。
- 每个节点的具体内容由 **if-match** 子句和 **apply** 子句来指定。**if-match** 子句定义该节点的匹配规则，**apply** 子句定义该节点的动作。
- 每个节点对报文的处理方式由匹配模式决定。匹配模式分为 **permit**（允许）和 **deny**（拒绝）两种。

应用策略后，系统将根据策略中定义的匹配规则和操作，对报文进行处理：系统按照优先级从高到低的顺序依次匹配各节点，如果报文满足这个节点的匹配规则，就执行该节点的动作；如果报文不满足这个节点的匹配规则，就继续匹配下一个节点；如果报文不能满足策略中任何一个节点的匹配规则，则根据路由表来转发报文。

1. if-match子句关系

目前，策略路由支持通过 **if-match acl** 子句设置 ACL 匹配规则，在一个节点中只能配置一条 **if-match acl** 子句。

2. apply子句关系

目前，策略路由仅提供了一种 **apply** 子句，即 **apply next-hop**，用来设置报文转发的下一跳。

3. 节点的匹配模式与节点的if-match子句、apply子句的关系

一个节点的匹配模式与这个节点的**if-match**子句、**apply**子句的关系如 表 1-1 所示。

表1-1 节点的匹配模式、if-match 子句、apply 子句三者之间的关系

是否满足所有 **if-match** 子句	节点匹配模式	
	permit（允许模式）	**deny**（拒绝模式）
是	• 如果节点配置了 **apply** 子句，则执行此节点 **apply** 子句，如果节点指导报文转发成功，则不再匹配下一节点 • 如果节点未配置 **apply** 子句，则不会执行任何动作，且不再匹配下一节点，报文将根据路由表来进行转发	不执行此节点**apply**子句，不再匹配下一节点，报文将根据路由表来进行转发
否	不执行此节点**apply**子句，继续匹配下一节点	不执行此节点**apply**子句，继续匹配下一节点

说明

如果一个节点中未配置任何 **if-match** 子句，则认为所有报文都满足该节点的匹配规则，按照“报文满足所有 **if-match** 子句”的情况进行后续处理。

1.1.4 策略路由与Track联动

策略路由通过与 Track 联动，增强了应用的灵活性和对网络环境变化的动态感知能力。

策略路由可以在配置报文的下一跳时与 Track 项关联，根据 Track 项的状态来动态地决定策略的可用性。策略路由配置仅在关联的 Track 项状态为 Positive 或 NotReady 时生效。关于策略路由与 Track 联动的详细介绍和相关配置，请参见“可靠性配置指导”中的“Track”。

1.1.5 策略路由配置限制和指导

对于目的地址是本机的 IP 报文，如果用户配置的策略路由中的 ACL 规格包含这类报文，且某些 IP 报文设备无法识别，ACL 匹配成功之后，策略路由会将这些报文直接转发出去。

1.2 策略路由配置任务简介

策略路由配置任务如下：

(1) 配置策略

a. 创建策略节点

b. 配置策略节点的匹配规则

c. 配置策略节点的动作

(2) 应用策略

请选择以下至少一项任务进行配置：

- 对本地报文应用策略

对接口转发的报文应用策略

1.3 配置策略

1.3.1 创建策略节点

(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*

1.3.2 配置策略节点的匹配规则

1. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入策略节点视图。

policy-based-route *policy-name* [**deny** | **permit**] **node** *node-number*

(3) 设置 ACL 匹配规则。

if-match acl { *acl-number* | **name** *acl-name* }

缺省情况下，未设置 ACL 匹配规则。

策略路由不支持匹配二层信息的 ACL 匹配规则。

设置 ACL 匹配规则时，对于 ACL 规则的 permit/deny 动作以及 time-range 指定的规则生效时间段等的处理机制不再生效。

1.3.3 配置策略节点的动作

1. 功能简介

用户通过配置 **apply** 子句指导策略节点的动作。目前，策略路由仅提供了一种 **apply** 子句，即 **apply next-hop**，用来设置报文转发的下一跳。

2. 配置限制和指导

在设置报文转发的下一跳时，对于配置接口出方向策略路由，仅支持直连下一跳，且仅支持一个下一跳。

策略路由通过查询 FIB 表中是否存在下一跳或缺省下一跳地址对应的条目，判断设置的报文转发下一跳或缺省下一跳地址是否可用。策略路由周期性检查 FIB 表，设备到下一跳的路径发生变化时，策略路由无法及时感知，可能会导致通信发生短暂中断。

3. 配置指导报文转发类动作

(1) 进入系统视图。

system-view

(2) 进入策略节点视图。

policy-based-route *policy-name* [**deny** | **permit**] **node** *node-number*

(3) 设置报文转发的下一跳。

apply next-hop { *ip-address* [**direct**] [**track** *track-entry-number*] }&<1-2>

缺省情况下，未设置报文转发的下一跳。

用户通过一次或多次配置本命令可以同时配置多个下一跳，每个节点最多可以配置 2 个下一跳，这些下一跳起到主备的作用。

1.4 应用策略

1.4.1 对本地报文应用策略

1. 功能简介

通过本配置，可以将已经配置的策略应用到本地，指导设备本身产生报文的发送。应用策略时，该策略必须已经存在，否则配置将失败。

2. 配置限制和指导

- 对本地报文只能应用一个策略。应用新的策略前必须删除本地原来已经应用的策略。
- 若无特殊需求，建议用户不要对本地报文应用策略。否则，有可能会对本地报文的发送造成不必要的影响（如 ping、telnet 服务的失效）。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 对本地报文应用策略。

ip local policy-based-route *policy-name*

缺省情况下，未对本地报文应用策略。

1.4.2 对接口转发的报文应用策略

1. 功能简介

通过本配置，可以将已经配置的策略应用到接口，指导接口接收的所有报文的转发。应用策略时，该策略必须已经存在，否则配置将失败。

2. 配置限制和指导

- 对接口转发的报文应用策略时，一个接口只能应用一个策略。应用新的策略前必须删除接口上原来已经应用的策略。
- 一个策略可以同时被多个接口应用。

3. 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) 对接口转发的报文应用策略。

ip policy-based-route *policy-name*

缺省情况下，未对接口转发的报文应用策略。

1.5 策略路由显示和维护

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

在用户视图下执行 **reset** 命令可以清除策略路由的统计信息。

表1-2 策略路由显示和维护

操作	命令
显示已经配置的策略	**display ip policy-based-route** [**policy** *policy-name*]
显示接口下转发策略路由的配置信息和统计信息	**display ip policy-based-route interface** *interface-type interface-number* [**slot** *slot-number*]
显示本地策略路由的配置信息和统计信息	**display ip policy-based-route local** [**slot** *slot-number*]
显示已经应用的策略路由信息	**display ip policy-based-route setup**
清除策略路由的统计信息	**reset ip policy-based-route statistics** [**policy** *policy-name*]

1.6 策略路由典型配置举例

1.6.1 基于报文协议类型的本地策略路由配置举例

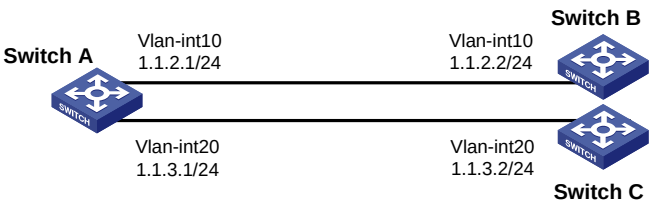
1. 组网需求

Switch A 分别与 Switch B 和 Switch C 直连（保证 Switch B 和 Switch C 之间路由完全不可达）。通过策略路由控制 Switch A 产生的报文：

- 指定所有 TCP 报文的下一跳为 1.1.2.2；
- 其它报文仍然按照查找路由表的方式进行转发。

2. 组网图

图1-1 基于报文协议类型的本地策略路由的配置举例组网图



3. 配置步骤

(1) 配置 Switch A

创建 VLAN 10 和 VLAN 20。

```
<SwitchA> system-view
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] vlan 20
[SwitchA-vlan20] quit
```

配置接口 Vlan-interface10 和 Vlan-interface20 的 IP 地址。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ip address 1.1.2.1 24
[SwitchA-Vlan-interface10] quit
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ip address 1.1.3.1 24
[SwitchA-Vlan-interface20] quit
```

定义访问控制列表 ACL 3101，用来匹配 TCP 报文。

```
[SwitchA] acl advanced 3101
[SwitchA-acl-ipv4-adv-3101] rule permit tcp
[SwitchA-acl-ipv4-adv-3101] quit
```

定义 5 号节点，指定所有 TCP 报文的下一跳为 1.1.2.2。

```
[SwitchA] policy-based-route aaa permit node 5
[SwitchA-pbr-aaa-5] if-match acl 3101
[SwitchA-pbr-aaa-5] apply next-hop 1.1.2.2
[SwitchA-pbr-aaa-5] quit
```

在 Switch A 上应用本地策略路由。

```
[SwitchA] ip local policy-based-route aaa
```

(2) 配置 Switch B

创建 VLAN 10

```
<SwitchB> system-view
[SwitchB] vlan 10
[SwitchB-vlan10] quit
```

配置接口 Vlan-interface10 的 IP 地址。

```
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] ip address 1.1.2.2 24
```

(3) 配置 Switch C

#创建 VLAN 20

```
<SwitchC> system-view
[SwitchC] vlan 20
[SwitchC-vlan20] quit
```

配置接口 Vlan-interface20 的 IP 地址。

```
[SwitchC] interface vlan-interface 20
[SwitchC-Vlan-interface20] ip address 1.1.3.2 24
```

4. 验证配置

从 Switch A 上通过 Telnet 方式登录 Switch B（1.1.2.2/24），结果成功。

从 Switch A 上通过 Telnet 方式登录 Switch C（1.1.3.2/24），结果失败。

从 Switch A 上 ping Switch C（1.1.3.2/24），结果成功。

由于 Telnet 使用的是 TCP 协议，ping 使用的是 ICMP 协议，所以由以上结果可证明：Switch A 发出的 TCP 报文的下一跳为 1.1.2.2，接口 Vlan-interface20 不发送 TCP 报文，但可以发送非 TCP 报文，策略路由设置成功。

1.6.2 基于报文协议类型的转发策略路由配置举例

1. 组网需求

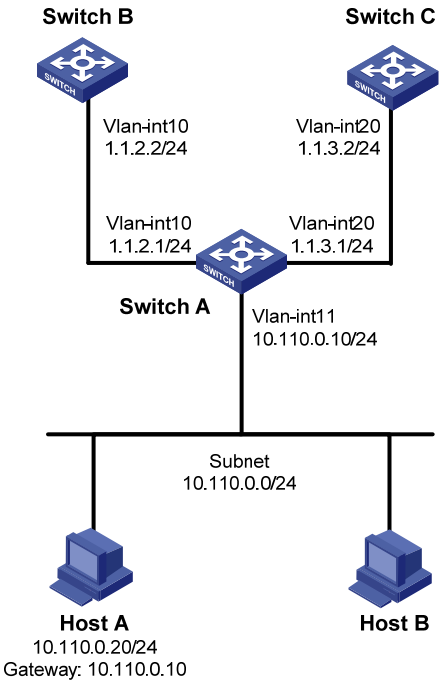
Switch A 分别与 Switch B 和 Switch C 直连（保证 Switch B 和 Switch C 之间路由完全不可达）。

通过策略路由控制从 Switch A 的接口 Vlan-interface11 接收的报文：

- 指定所有 TCP 报文的下一跳为 1.1.2.2；
- 其它报文仍然按照查找路由表的方式进行转发。

2. 组网图

图1-2 基于报文协议类型的转发策略路由的配置举例组网图



3. 配置步骤

配置前请确保 Switch B 和 Host A，Switch C 和 Host A 之间路由可达。

(1) 配置 Switch A

创建 VLAN 10 和 VLAN 20。

```
<SwitchA> system-view
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] vlan 20
[SwitchA-vlan20] quit
```

配置接口 Vlan-interface10 和 Vlan-interface20 的 IP 地址。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ip address 1.1.2.1 24
[SwitchA-Vlan-interface10] quit
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ip address 1.1.3.1 24
[SwitchA-Vlan-interface20] quit
```

定义访问控制列表 ACL 3101，用来匹配 TCP 报文。

```
[SwitchA] acl advanced 3101
[SwitchA-acl-ipv4-adv-3101] rule permit tcp
[SwitchA-acl-ipv4-adv-3101] quit
```

定义 5 号节点，指定所有 TCP 报文的下一跳为 1.1.2.2。

```
[SwitchA] policy-based-route aaa permit node 5
[SwitchA-pbr-aaa-5] if-match acl 3101
[SwitchA-pbr-aaa-5] apply next-hop 1.1.2.2
[SwitchA-pbr-aaa-5] quit
```

在接口 Vlan-interface11 上应用转发策略路由，处理此接口接收的报文。

```
[SwitchA] interface vlan-interface 11
[SwitchA-Vlan-interface11] ip address 10.110.0.10 24
[SwitchA-Vlan-interface11] ip policy-based-route aaa
[SwitchA-Vlan-interface11] quit
```

4. 验证配置

从 Host A 上通过 Telnet 方式登录 Switch B，结果成功。

从 Host A 上通过 Telnet 方式登录 Switch C，结果失败。

从 Host A 上 ping Switch C，结果成功。

由于 Telnet 使用的是 TCP 协议，ping 使用的是 ICMP 协议，所以由以上结果可证明：从 Switch A 的接口 Vlan-interface11 接收的 TCP 报文的下一跳为 1.1.2.2，接口 Vlan-interface20 不转发 TCP 报文，但可以转发非 TCP 报文，策略路由设置成功。

目 录

1 IPv6 静态路由

1.1 IPv6静态路由简介

静态路由是一种特殊的路由，由管理员手工配置。当网络结构比较简单时，只需配置静态路由就可以使网络正常工作。

静态路由不能自动适应网络拓扑结构的变化。当网络发生故障或者拓扑发生变化后，必须由网络管理员手工修改配置。

IPv6 静态路由与 IPv4 静态路由类似，适合于一些结构比较简单的 IPv6 网络。

1.2 配置IPv6静态路由

(1) 进入系统视图。

system-view

(2) 配置 IPv6 静态路由。

ipv6 route-static *ipv6-address prefix-length* { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* } [**permanent**] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

缺省情况下，未配置 IPv6 静态路由。

(3) 缺省情况下，未配置 IPv6 静态路由。（可选）配置 IPv6 静态路由的缺省优先级。

ipv6 route-static default-preference *default-preference*

缺省情况下，IPv6 静态路由的缺省优先级为 60。

1.3 配置IPv6静态路由删除

1. 功能简介

使用 **undo ipv6 route-static** 命令可以删除一条 IPv6 静态路由，而使用 **delete ipv6 static-routes all** 命令可以删除包括缺省路由在内的所有 IPv6 静态路由。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 删除所有 IPv6 静态路由。

delete ipv6 static-routes all

1.4 配置IPv6静态路由与BFD联动

1.4.1 功能简介

BFD（Bidirectional Forwarding Detection，双向转发检测）提供了一个通用的、标准化的、介质无关、协议无关的快速故障检测机制，可以为上层协议（如路由协议等）统一地快速检测两台路由器间双向转发路径的故障。使能 IPv6 与 BFD 联动功能后，BFD 将对 IPv6 静态路由的下一跳可达性进行快速检测。当检测到下一跳不可达时，相应的 IPv6 静态路由将会被删除。

关于 BFD 的详细介绍，请参见“可靠性配置指导”中的“BFD”。

1.4.2 配置限制和指导

路由振荡时，使能 BFD 功能可能会加剧振荡，请谨慎使用。

1.4.3 配置双向检测

1. 功能简介

双向检测，即本端和对端需要同时进行配置，通过控制报文检测两个方向上的链路状态，实现毫秒级别的链路故障检测。

双向检测支持直连下一跳和非直连下一跳：

- 直连下一跳是指下一跳和本端是直连的，配置时必须指定出接口和下一跳。
- 非直连下一跳是指下一跳和本端不是直连的，中间还有其它设备。配置时必须指定下一跳和 BFD 源 IPv6 地址。

2. 配置直连下一跳双向检测

(1) 进入系统视图。

system-view

(2) 配置静态路由与 BFD 联动。

ipv6 route-static *ipv6-address prefix-length interface-type interface-number next-hop-address* **bfd control-packet** [**bfd-source** *ipv6-address*] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

缺省情况下，未配置 IPv6 静态路由与 BFD 联动。

3. 配置非直连下一跳双向检测

(1) 进入系统视图。

system-view

(2) 配置静态路由与 BFD 联动。

ipv6 route-static *ipv6-address prefix-length* { *next-hop-address* **bfd control-packet bfd-source** *ipv6-address* } [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

缺省情况下，未配置 IPv6 静态路由与 BFD 联动。

1.4.4 配置单跳检测

1. 功能简介

单跳检测，即只需要本端进行配置，通过 echo 报文检测链路的状态。echo 报文的目的地址为本端接口地址，发送给下一跳设备后会直接转发回本端。这里所说的“单跳”是 IPv6 的一跳。

2. 配置限制和指导

IPv6 静态路由的出接口为处于 SPOOFING 状态时，不能使用 BFD 进行检测。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 echo 报文的源 IPv6 地址。

bfd echo-source-ipv6 *ipv6-address*

缺省情况下，未配置 echo 报文的源 IPv6 地址。

echo 报文源 IPv6 地址仅支持全球单播地址。

本命令的详细情况请参见“可靠性命令参考”中的“BFD”。

(3) 配置静态路由与 BFD 联动。

ipv6 route-static *ipv6-address prefix-length interface-type interface-number next-hop-address* **bfd echo-packet** [**bfd-source** *ipv6-address*] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

缺省情况下，未配置 IPv6 静态路由与 BFD 联动。

下一跳 IPv6 地址必须为全球单播地址。

1.5 IPv6静态路由显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令查看 IPv6 静态路由配置的运行情况并检验配置结果。

表1-1 IPv6 静态路由显示和维护

操作	命令
显示IPv6静态路由下一跳信息	**display ipv6 route-static nib** [*nib-id*] [**verbose**]
显示IPv6静态路由表信息	**display ipv6 route-static routing-table** [*ipv6-address prefix-length*]
查看IPv6静态路由表信息（本命令的详细情况请参见“三层技术-IP路由命令参考”中的“IP路由基础”）	**display ipv6 routing-table protocol static** [**inactive** | **verbose**]

1.6 IPv6静态路由典型配置举例

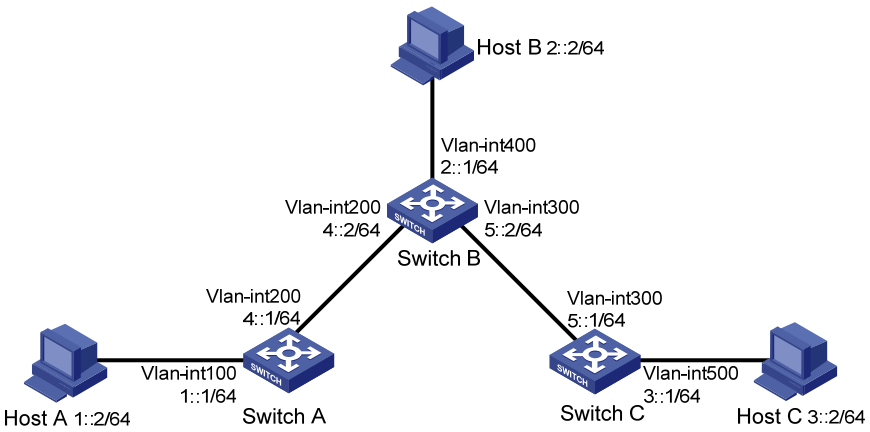
1.6.1 IPv6 静态路由基本功能配置举例

1. 组网要求

要求各交换机之间配置 IPv6 静态路由后，可以使所有主机和交换机之间互通。

2. 组网图

图1-1 IPv6 静态路由基本功能配置组网图



3. 配置步骤

(1) 配置各 VLAN 虚接口的 IPv6 地址（略）

(2) 配置 IPv6 静态路由

在 Switch A 上配置 IPv6 缺省路由。

```
<SwitchA> system-view
[SwitchA] ipv6 route-static :: 0 4::2
```

在 Switch B 上配置两条 IPv6 静态路由。

```
<SwitchB> system-view
[SwitchB] ipv6 route-static 1:: 64 4::1
[SwitchB] ipv6 route-static 3:: 64 5::1
```

在 Switch C 上配置 IPv6 缺省路由。

```
<SwitchC> system-view
[SwitchC] ipv6 route-static :: 0 5::2
```

(3) 配置主机地址和网关

根据组网图配置好各主机的 IPv6 地址，并将 Host A 的缺省网关配置为 1::1，Host B 的缺省网关配置为 2::1，Host C 的缺省网关配置为 3::1。

4. 验证配置

查看 Switch A 的 IPv6 静态路由信息。

```
[SwitchA] display ipv6 routing-table protocol static

Summary Count : 1
```

```
Static Routing table Status : <Active>
Summary Count : 1

Destination: ::                                         Protocol  : Static
NextHop    : 4::2                                       Preference: 60
Interface  : Vlan-interface200                          Cost      : 0

Static Routing table Status : <Inactive>
Summary Count : 0
```

查看 Switch B 的 IPv6 静态路由信息。

```
[SwitchB] display ipv6 routing-table protocol static

Summary Count : 2

Static Routing table Status : <Active>
Summary Count : 2

Destination: 1::/64                                     Protocol  : Static
NextHop    : 4::1                                       Preference: 60
Interface  : Vlan-interface200                          Cost      : 0

Destination: 3::/64                                     Protocol  : Static
NextHop    : 5::1                                       Preference: 60
Interface  : Vlan-interface300                          Cost      : 0

Static Routing table Status : <Inactive>
Summary Count : 0
```

使用 Ping 进行验证。

```
[SwitchA] ping ipv6 3::1
Ping6(56 data bytes) 4::1 --> 3::1, press CTRL_C to break
56 bytes from 3::1, icmp_seq=0 hlim=62 time=0.700 ms
56 bytes from 3::1, icmp_seq=1 hlim=62 time=0.351 ms
56 bytes from 3::1, icmp_seq=2 hlim=62 time=0.338 ms
56 bytes from 3::1, icmp_seq=3 hlim=62 time=0.373 ms
56 bytes from 3::1, icmp_seq=4 hlim=62 time=0.316 ms

--- Ping6 statistics for 3::1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.316/0.416/0.700/0.143 ms
```

1.6.2 IPv6 静态路由与BFD联动（直连）配置举例

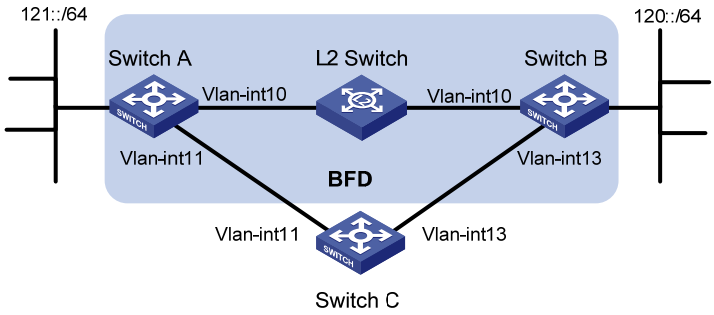
1. 组网需求

- 在 Switch A 上配置 IPv6 静态路由可以到达 120::/64 网段，在 Switch B 上配置 IPv6 静态路由可以到达 121::/64 网段，并都使能 BFD 检测功能。
- 在 Switch C 上配置 IPv6 静态路由可以到达 120::/64 网段和 121::/64 网段。

- 当 Switch A 和 Switch B 通过 L2 Switch 通信的链路出现故障时，BFD 能够快速感知，并且切换到 Switch C 进行通信。

2. 组网图

图1-2 IPv6 静态路由与 BFD 联动（直连）配置组网图



设备	接口	IPv6地址	设备	接口	IPv6地址
Switch A	Vlan-int10	12::1/64	Switch B	Vlan-int10	12::2/64
	Vlan-int11	10::102/64		Vlan-int13	13::1/64
Switch C	Vlan-int11	10:: 100/64			
	Vlan-int13	13::2/64			

3. 配置步骤

(1) 配置各接口的 IPv6 地址（略）

(2) 配置 IPv6 静态路由和 BFD

在 Switch A 上配置静态路由，并使能 BFD 检测功能，使用双向检测方式。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 10
[SwitchA-vlan-interface10] bfd min-transmit-interval 500
[SwitchA-vlan-interface10] bfd min-receive-interval 500
[SwitchA-vlan-interface10] bfd detect-multiplier 9
[SwitchA-vlan-interface10] quit
[SwitchA] ipv6 route-static 120:: 64 vlan-interface 10 12::2 bfd control-packet
[SwitchA] ipv6 route-static 120:: 64 10::100 preference 65
[SwitchA] quit
```

在 Switch B 上配置 IPv6 静态路由，并使能 BFD 检测功能，使用双向检测方式。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 10
[SwitchB-vlan-interface10] bfd min-transmit-interval 500
[SwitchB-vlan-interface10] bfd min-receive-interval 500
[SwitchB-vlan-interface10] bfd detect-multiplier 9
[SwitchB-vlan-interface10] quit
[SwitchB] ipv6 route-static 121:: 64 vlan-interface 10 12::1 bfd control-packet
[SwitchB] ipv6 route-static 121:: 64 13::2 preference 65
[SwitchB] quit
```

在 Switch C 上配置静态路由。

```
<SwitchC> system-view
```

```
[SwitchC] ipv6 route-static 120:: 64 13::1
[SwitchC] ipv6 route-static 121:: 64 10::102
```

4. 验证配置

下面以 Switch A 为例，Switch B 和 Switch A 类似，不再赘述。

查看 BFD 会话，可以看到 BFD 会话已经创建。

```
<SwitchA> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv6 Session Working Under Ctrl Mode:

       Local Discr: 513                Remote Discr: 33
         Source IP: 12::1
    Destination IP: 12::2
     Session State: Up                      Interface: Vlan10
         Hold Time: 2012ms
```

查看静态路由，可以看到 Switch A 经过 L2 Switch 到达 Switch B。

```
<SwitchA> display ipv6 routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination: 120::/64                                  Protocol  : Static
NextHop    : 12::2                                     Preference: 60
Interface  : Vlan10                                    Cost      : 0

Direct Routing table Status : <Inactive>
Summary Count : 0
```

当 Switch A 和 Switch B 通过 L2 Switch 通信的链路出现故障时：

查看 IPv6 静态路由，可以看到 Switch A 经过 Switch C 到达 Switch B。

```
<SwitchA> display ipv6 routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination: 120::/64                                  Protocol  : Static
NextHop    : 10::100                                   Preference: 65
Interface  : Vlan11                                    Cost      : 0

Static Routing table Status : < Inactive>
Summary Count : 0
```

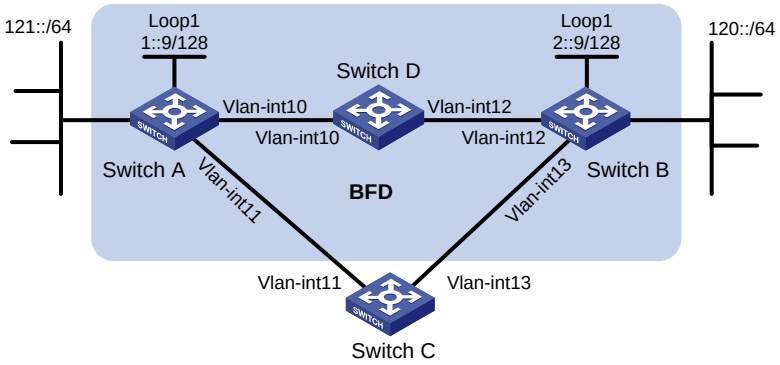
1.6.3 IPv6 静态路由与BFD联动（非直连）配置举例

1. 组网需求

- 在 Switch A 上配置 IPv6 静态路由可以到达 120::/64 网段，在 Switch B 上配置 IPv6 静态路由可以到达 121::/64 网段，并都使能 BFD 检测功能。
- 在 Switch C 和 Switch D 上配置 IPv6 静态路由可以到达 120::/64 网段和 121::/64 网段。
- Switch A 存在到 Switch B 的接口 Loopback1（2::9/128）的路由，出接口为 Vlan-interface10；Switch B 存在到 Switch A 的接口 Loopback1（1::9/128）的路由，出接口为 Vlan-interface12；Switch D 存在到 1::9/128 的路由，出接口为 Vlan-interface10，存在到 2::9/128 的路由，出接口为 Vlan-interface12。
- 当 Switch A 和 Switch B 通过 Switch D 通信的链路出现故障时，BFD 能够快速感知，并且切换到 Switch C 进行通信。

2. 组网图

图1-3 IPv6 静态路由与 BFD 联动（非直连）配置组网图



设备	接口	IPv6地址	设备	接口	IPv6地址
Switch A	Vlan-int10	12::1/64	Switch B	Vlan-int12	11::2/64
	Vlan-int11	10::102/64		Vlan-int13	13::1/64
	Loop1	1::9/128		Loop1	2::9/128
Switch C	Vlan-int11	10::100/64	Switch D	Vlan-int10	12::2/64
	Vlan-int13	13::2/64		Vlan-int12	11::1/64

3. 配置步骤

(1) 配置各接口的 IPv6 地址（略）

(2) 配置 IPv6 静态路由和 BFD

在 Switch A 上配置 IPv6 静态路由，并使能 BFD 检测功能，使用双向检测方式。

```
<SwitchA> system-view
[SwitchA] bfd multi-hop min-transmit-interval 500
[SwitchA] bfd multi-hop min-receive-interval 500
[SwitchA] bfd multi-hop detect-multiplier 9
[SwitchA] ipv6 route-static 120:: 64 2::9 bfd control-packet bfd-source 1::9
[SwitchA] ipv6 route-static 120:: 64 10::100 preference 65
[SwitchA] ipv6 route-static 2::9 128 12::2
[SwitchA] quit
```

在 Switch B 上配置 IPv6 静态路由，并使能 BFD 检测功能，使用双向检测方式。

```
<SwitchB> system-view
[SwitchB] bfd multi-hop min-transmit-interval 500
[SwitchB] bfd multi-hop min-receive-interval 500
[SwitchB] bfd multi-hop detect-multiplier 9
[SwitchB] ipv6 route-static 121:: 64 1::9 bfd control-packet bfd-source 2::9
[SwitchB] ipv6 route-static 121:: 64 13::2 preference 65
[SwitchB] ipv6 route-static 1::9 128 11::1
[SwitchB] quit
```

在 Switch C 上配置静态路由。

```
<SwitchC> system-view
[SwitchC] ipv6 route-static 120:: 64 13::1
[SwitchC] ipv6 route-static 121:: 64 10::102
```

在 Switch D 上配置静态路由。

```
<SwitchD> system-view
[SwitchD] ipv6 route-static 120:: 64 11::2
[SwitchD] ipv6 route-static 121:: 64 12::1
[SwitchD] ipv6 route-static 2::9 128 11::2
[SwitchD] ipv6 route-static 1::9 128 12::1
```

4. 验证配置

下面以 Switch A 为例，Switch B 和 Switch A 类似，不再赘述。

查看 BFD 会话，可以看到 BFD 会话已经创建。

```
<SwitchA> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv6 Session Working Under Ctrl Mode:

       Local Discr: 513                 Remote Discr: 33
         Source IP: 1::9
    Destination IP: 2::9
     Session State: Up                      Interface: N/A
         Hold Time: 2012ms
```

查看 IPv6 静态路由，可以看到 Switch A 经过 Switch D 到达 Switch B。

```
<SwitchA> display ipv6 routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination: 120::/64                                  Protocol  : Static
NextHop    : 2::9                                      Preference: 60
Interface  : Vlan10                                    Cost      : 0

Static Routing table Status : <Inactive>
```

```
Summary Count : 0
```

当 Switch A 和 Switch B 通过 Switch D 通信的链路出现故障时：

查看 IPv6 静态路由，可以看到 Switch A 经过 Switch C 到达 Switch B。

```
<SwitchA> display ipv6 routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination: 120::/64                                   Protocol  : Static
NextHop    : 10::100                                    Preference: 65
Interface  : Vlan11                                     Cost      : 0

Static Routing table Status : <Inactive>
Summary Count : 0
```

2 IPv6 缺省路由

IPv6 缺省路由是在路由器没有找到匹配的 IPv6 路由表项时使用的路由。

IPv6 缺省路由有两种生成方式：

- 第一种是网络管理员手工配置。配置请参见“1.2 配置IPv6 静态路由”，指定的目的地址为::/0（前缀长度为 0）。
- 第二种是动态路由协议生成（如 OSPFv3 和 RIPng），由路由能力比较强的路由器将 IPv6 缺省路由发布给其它路由器，其它路由器在自己的路由表里生成指向那台路由器的缺省路由。配置请参见各个路由协议手册。

目 录

1 RIPng

1.1 RIPng简介

RIPng（RIP next generation，下一代 RIP 协议）是基于距离矢量（Distance-Vector）算法的协议。它通过 UDP 报文交换路由信息，使用的端口号为 521。RIPng 是对原来的 IPv4 网络中 RIP-2 协议的扩展，大多数 RIP 的概念都可以用于 RIPng。

1.1.1 RIPng的路由度量值

RIPng 使用跳数来衡量到达目的地址的距离（也称为度量值或开销）。在 RIPng 中，从一个路由器到其直连网络的跳数为 0，通过与其相连的路由器到达另一个网络的跳数为 1，其余以此类推。当跳数大于或等于 16 时，目的网络或主机就被定义为不可达。

1.1.2 RIPng的路由数据库

每个运行 RIPng 的路由器都管理一个路由数据库，该路由数据库包含了到所有可达目的地的路由项，这些路由项包含下列信息：

- 目的地址：主机或网络的 IPv6 地址。
- 下一跳地址：为到达目的地，需要经过的相邻路由器的接口 IPv6 地址。
- 出接口：转发 IPv6 报文通过的出接口。
- 度量值：本路由器到达目的地的开销。
- 路由时间：从路由项最后一次被更新到现在所经过的时间，路由项每次被更新时，路由时间重置为 0。
- 路由标记（Route Tag）：用于标识外部路由，以便在路由策略中根据 Tag 对路由进行灵活的控制。关于路由策略的详细信息，请参见“三层技术-IP 路由配置指导”中的“路由策略”。

1.1.3 RIPng报文及路由发布过程

RIPng 有两种报文：Request 报文和 Response 报文，并采用组播方式发送报文，使用链路本地地址 FF02::9 作为 RIPng 路由更新的目的地址；使用链路本地地址 FE80::/10 作为 RIPng 路由更新的源地址。

当 RIPng 路由器启动后或者需要更新部分路由表项时，便会发出 Request 报文，向邻居请求需要的路由信息。

Response 报文包含本地路由表的信息，一般在下列情况下产生：

- 对某个 Request 报文进行响应
- 作为更新报文周期性地发出
- 在路由发生变化时触发更新

收到 Request 报文的 RIPng 路由器会以 Response 报文形式发回给请求路由器。

收到 Response 报文的路由器会更新自己的 RIPng 路由表。为了保证路由的准确性，RIPng 路由器会对收到的 Response 报文进行有效性检查，比如源 IPv6 地址是否是链路本地地址，端口号是否正确等，没有通过检查的报文会被忽略。

1.1.4 协议规范

与 RIPng 相关的规范有：

- RFC 2080：RIPng for IPv6
- RFC 2081：RIPng Protocol Applicability Statement

1.2 RIPng与硬件适配关系

S5000V3-EI、S5000E-X 系列交换机不支持 RIPng。

1.3 RIPng配置任务简介

RIPng 配置任务如下：

(1) 配置RIPng的基本功能

(2) （可选）配置RIPng的路由信息控制
- 配置接口附加度量值
- 配置RIPng路由聚合
- 配置RIPng发布缺省路由
- 配置RIPng对接收/发布的路由进行过滤
- 配置RIPng协议优先级
- 配置RIPng引入外部路由

(3) （可选）调整和优化RIPng网络
- 配置RIPng定时器
- 配置水平分割和毒性逆转
- 配置RIPng报文的发送速率
- 配置RIPng触发更新的时间间隔

(4) （可选）提高 RIPng 的可靠性
- 配置RIPng GR
- 配置RIPng NSR
- 配置RIPng快速重路由

(5) （可选）提高RIPng的安全性
- 配置RIPng报文的零域检查
- 配置IPsec

1.4 配置RIPng的基本功能

(1) 进入系统视图。

system-view

(2) 进入 RIPng 视图。

ripng [*process-id*]

缺省情况下，系统没有运行 RIPng。

(3) 退回系统视图。

quit

(4) 进入接口视图。

interface *interface-type interface-number*

(5) 在接口上使能 RIPng 路由协议。

ripng *process-id* **enable**

缺省情况下，接口上的 RIPng 功能处于关闭状态。

如果接口没有使能 RIPng，那么 RIPng 进程在该接口上既不发送也不接收 RIPng 路由。

1.5 配置RIPng的路由信息控制

1.5.1 配置接口附加度量值

1. 功能简介

附加度量值是在 RIPng 路由原来度量值的基础上所增加的度量值（跳数），包括发送附加度量值和接收附加度量值。

- 发送附加度量值：不会改变路由表中的路由度量值，仅当接口发送 RIPng 路由信息时才会添加到发送路由上。
- 接收附加度量值：会影响接收到的路由度量值，接口接收到一条合法的 RIPng 路由时，在将其加入路由表前会把附加度量值加到该路由上。

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) 设置接口接收 RIPng 路由时的附加度量值。

ripng metricin *value*

缺省情况下，接口接收 RIPng 路由时的附加度量值为 0。

(4) 设置接口发送 RIPng 路由时的附加度量值。

ripng metricout *value*

缺省情况下，接口发送 RIPng 路由时的附加度量值为 1。

1.5.2 配置RIPng路由聚合

1. 功能简介

RIPng 的路由聚合是在接口上实现的，在接口上配置路由聚合，此时可以将 RIPng 要在这个接口上发布出去的路由按最长匹配原则聚合后发布出去。

RIPng 路由聚合可提高网络的可扩展性和效率，缩减路由表。

RIPng 将多条路由聚合成一条路由时，聚合路由的 Metric 值将取所有路由 Metric 的最小值。

例如，RIPng 从接口发布出去的路由有两条：11:11:11::24 Metric=2 和 11:11:12::34 Metric=3，在此接口上配置的聚合路由为 11::0/16，则最终发布出去的路由为 11::0/16 Metric=2。

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 RIPng 在接口发布聚合的 IPv6 地址，并指定被聚合的路由的 IPv6 前缀。

ripng summary-address *ipv6-address prefix-length*

缺省情况下，未配置 RIPng 在接口发布聚合的 IPv6 地址。

1.5.3 配置RIPng发布缺省路由

1. 功能简介

用户可以配置 RIP 以指定度量值向邻居发布一条缺省路由。

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 RIPng 发布缺省路由。

ripng default-route { **only** | **originate** } [**cost** *cost-value* | **route-policy** *route-policy-name*] *

缺省情况下，RIPng 进程不发布缺省路由。

缺省路由将被强制通过指定接口的路由更新报文发布出去，该路由的发布不考虑其是否已经存在于本设备的 IPv6 路由表中。

1.5.4 配置RIPng对接收/发布的路由进行过滤

1. 功能简介

用户可通过使用 IPv6 ACL 和 IPv6 前缀列表对接收到的路由信息进行过滤，只有通过过滤的路由才能被加入到 RIPng 路由表；此外，还可对本机所有要发布的路由进行过滤，包括从其它路由协议引入的路由和从邻居学到的 RIPng 路由，只有通过过滤的路由才能被发布给 RIPng 邻居。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 RIPng 视图。

ripng [*process-id*]

(3) 对接收的路由信息进行过滤。

filter-policy { *ipv6-acl-number* | **prefix-list** *prefix-list-name* } **import**

缺省情况下，RIPng 不对接收的路由信息进行过滤。

(4) 对发布的路由信息进行过滤。

filter-policy { *ipv6-acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*]]

缺省情况下，RIPng 不对发布的路由信息进行过滤。

1.5.5 配置RIPng协议优先级

1. 功能简介

任何路由协议都具备特有的协议优先级，在设备进行路由选择时能够在不同的协议中选择最佳路由。可以手工设置 RIPng 协议的优先级，设置的值越小，其优先级越高。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 RIPng 视图。

ripng [*process-id*]

(3) 配置 RIPng 路由的优先级。

preference { *preference* | **route-policy** *route-policy-name* } *

缺省情况下，RIPng 路由的优先级为 100。

1.5.6 配置RIPng引入外部路由

(1) 进入系统视图。

system-view

(2) 进入 RIPng 视图。

ripng [*process-id*]

(3) 引入外部路由。

- 配置 RIPng 引入直连或静态路由。

  import-route { **direct** | **static** } [**cost** *cost-value* | **route-policy** *route-policy-name*] *

- 配置 RIPng 引入 **ospfv3** 协议或其他 **ripng** 进程的路由。

  import-route { **ospfv3** | **ripng** } [*process-id*] [**allow-direct** | **cost** *cost-value* | **route-policy** *route-policy-name*] *

缺省情况下，RIPng 不引入其它路由。

(4) （可选）配置引入路由的缺省度量值。

default cost *cost-value*

缺省情况下，引入路由的缺省度量值为 0。

1.6 调整和优化RIPng网络

1.6.1 配置RIPng定时器

1. 功能简介

用户可通过调节 RIPng 定时器来调整 RIPng 路由协议的性能，以满足网络需要。

2. 配置限制和指导

在配置 RIPng 定时器时需要注意，定时器值的调整应考虑网络的性能，并在所有运行 RIPng 的路由器上进行统一配置，避免增加不必要的网络流量。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 RIPng 视图。

ripng [*process-id*]

(3) 配置 RIPng 定时器的值。

timers { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* } *

缺省情况下，Update 定时器的值为 30 秒，Timeout 定时器的值为 180 秒，Suppress 定时器的值为 120 秒，Garbage-collect 定时器的值为 120 秒。

1.6.2 配置水平分割和毒性逆转

1. 配置限制和指导

- 如果同时配置了水平分割和毒性逆转，则只有毒性逆转功能生效。
- 配置水平分割可以使得从一个接口学到的路由不能通过此接口向外发布，用于避免相邻路由器间的路由环路。因此，建议不要关闭水平分割。
- 配置毒性逆转可以使得从一个接口学到的路由还可以从这个接口向外发布，但此时这些路由的度量值已设置为 16，即不可达。

2. 配置水平分割

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 使能水平分割功能。

ripng split-horizon

缺省情况下，水平分割功能处于使能状态。

3. 配置毒性逆转

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 使能毒性逆转功能。

ripng poison-reverse

缺省情况下，毒性逆转功能处于关闭状态。

1.6.3 配置RIPng报文的发送速率

1. 功能简介

RIPng 周期性地将路由信息放在 RIPng 报文中向邻居发送。

如果路由表里的路由条目数量很多，同时发送大量 RIPng 协议报文有可能会对当前设备和网络带宽带来冲击；因此，路由器将 RIPng 协议报文分为多个批次进行发送，并且对 RIPng 接口每次允许发送的 RIPng 协议报文最大个数做出限制。

用户可根据需要配置接口发送 RIPng 报文的时间间隔以及接口一次发送 RIPng 报文的最大个数。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 RIPng 报文的发送速率。

- 请依次执行以下命令在 RIP 视图下配置 RIPng 报文发送速率。

  ripng [*process-id*]

  output-delay *time* **count** *count*

  缺省情况下，接口发送 RIPng 报文的时间间隔为 20 毫秒，一次最多发送 3 个 RIPng 报文。

- 请依次执行以下命令在接口视图下配置 RIPng 报文发送速率。

  interface *interface-type interface-number*

  ripng output-delay *time* **count** *count*

  缺省情况下，接口发送 RIPng 报文的速率以 RIPng 进程配置的为准。

1.6.4 配置RIPng触发更新的时间间隔

1. 功能简介

RIPng 路由信息变化后将以触发更新的方式通知邻居设备，加速邻居设备的路由收敛。如果路由信息频繁变化，且每次变化都立即发送触发更新，将会占用大量系统资源，并影响路由器的效率。通过调节触发更新的时间间隔，可以抑制由于路由信息频繁变化带来的影响。本命令在路由信息变化不频繁的情况下将连续触发更新的时间间隔缩小到 *minimum-interval*，而在路由信息变化频繁

的情况下可以进行相应惩罚，增加 *incremental-interval*×2^{n-2}（n 为连续触发更新的次数），将等待时间按照配置的惩罚增量延长，最大不超过 *maximum-interval*。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 RIPng 视图。

ripng [*process-id*]

(3) 配置 RIPng 触发更新的时间间隔。

timer triggered *maximum-interval* [*minimum-interval* [*incremental-interval*]]

缺省情况下，发送触发更新的最大时间间隔为 5 秒，最小间隔为 50 毫秒，增量惩罚间隔为 200 毫秒。

1.7 配置RIPng GR

1. 功能简介

GR（Graceful Restart，平滑重启）是一种在协议重启或主备倒换时 RIPng 进行平滑重启，保证转发业务不中断的机制。

GR 有两个角色：

- GR Restarter：发生协议重启或主备倒换事件且具有 GR 能力的设备。
- GR Helper：和 GR Restarter 具有邻居关系，协助完成 GR 流程的设备。

在普通的路由协议重启的情况下，路由器需要重新学习 RIPng 路由，并更新 FIB 表，此时会引起网络暂时的中断，基于 RIPng 的 GR 可以解决这个问题。

应用了 GR 特性的设备向外发送 RIPng 全部路由表请求报文，重新从邻居处学习 RIPng 路由，在此期间 FIB 表不变化。在路由协议重启完毕后，设备将重新学到的 RIPng 路由下刷给 FIB 表，使该设备的路由信息恢复到重启前的状态。

本配置在 GR Restarter 上进行。启动了 RIPng 的设备缺省就是 GR Helper。

2. 配置限制和指导

设备充当 GR Restarter 后不能再配置 RIPng NSR 功能。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 RIPng 视图。

ripng [*process-id*]

(3) 使能 RIPng 协议的 GR 能力。

graceful-restart

缺省情况下，RIPng 协议的 GR 能力处于关闭状态。

(4) （可选）配置 RIPng 协议的 GR 重启间隔时间。

graceful-restart interval *interval*

缺省情况下，RIPng 协议的 GR 重启间隔时间为 60 秒。

1.8 配置RIPng NSR

1. 功能简介

NSR（Nonstop Routing，不间断路由）通过将 RIPng 路由信息从主进程备份到备进程，使设备在发生主备倒换时新主进程可以无缝完成路由的重新生成、下刷，邻接关系不会发生中断，从而避免了主备倒换对转发业务的影响。

GR 特性需要周边设备配合才能完成路由信息的恢复，在网络应用中有一定的限制。NSR 特性不需要周边设备的配合，网络应用更加广泛。

2. 配置限制和指导

各个进程的 NSR 功能是相互独立的，只对本进程生效。如果存在多个 RIPng 进程，建议在各个进程下使能 RIPng NSR 功能。

设备配置了 RIPng NSR 功能后不能在充当 GR Restarter。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 RIPng 视图。

ripng [*process-id*]

(3) 使能 RIPng NSR 功能。

non-stop-routing

缺省情况下，RIPng NSR 功能处于关闭状态。

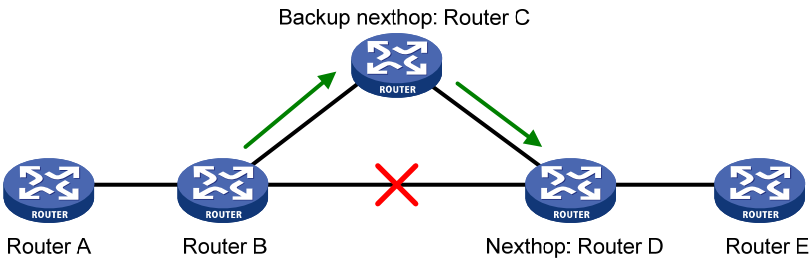
1.9 配置RIPng快速重路由

1.9.1 功能简介

在部署了备份链路的 RIPng 网络中，当主用链路发生故障时，RIPng 会对路由进行重新计算，在路由收敛完成后，流量可以通过备份链路进行传输。在路由收敛期间，数据流量将会被中断。

为了尽可能缩短网络故障导致的流量中断时间，网络管理员可以根据需要配置 RIPng 快速重路由功能。

图1-1 RIPng 快速重路由功能示意图



如 图 1-1 所示，通过在Router B上配置快速重路由功能，RIPng可以为路由指定备份下一跳，当Router B检测到主用下一跳地址无法到达时，会直接使用备份下一跳地址来指导报文的转发，从而大大缩短了流量路径切换的时间。在快速切换流量传输路径的同时，RIPng会根据变化后的网络拓扑重新计算路由，在路由收敛完毕后，使用新计算出来的最优路由来指导报文转发。

1.9.2 配置限制和指导

- 本功能只适合在主链路三层接口 up，主链路由双通变为单通或者不通的情况下使用。在主链路三层接口 down 的情况下，本功能不可用。单通现象，即一条链路上的两端，有且只有一端可以收到另一端发来的报文，此链路称为单向链路。
- RIPng 快速重路由功能仅对非迭代 RIPng 路由（即从直连邻居学到 RIPng 路由）有效。
- 等价路由不支持快速重路由功能。

1.9.3 配置RIPng快速重路由功能

(1) 进入系统视图。

system-view

(2) 配置路由策略。

在路由策略中通过 **apply ipv6 fast-reroute backup-interface** 命令在路由策略中指定备份下一跳。详细配置请参见“三层技术-IP 路由配置指导”中的“路由策略”。

(3) 进入 RIPng 视图。

ripng [*process-id*]

(4) 开启 RIPng 快速重路由功能。

fast-reroute route-policy *route-policy-name*

缺省情况下，RIPng 快速重路由功能处于关闭状态。

1.9.4 配置RIPng快速重路由支持BFD检测功能

1. 功能简介

RIPng 协议的快速重路由特性中，主用链路缺省不使用 BFD 进行链路故障检测。配置本功能后，将使用 BFD（Echo 方式）进行检测，可以加快 RIPng 协议的收敛速度。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 BFD Echo 报文源地址。

bfd echo-source-ipv6 *ipv6-address*

缺省情况下，未配置 BFD Echo 报文源地址。

echo 报文的源 IPv6 地址用户可以任意指定。建议配置 echo 报文的源 IPv6 地址不属于该设备任何一个接口所在网段。

本命令的详细介绍请参见“可靠性命令参考”中的“BFD”。

(3) 进入接口视图。

interface *interface-type interface-number*

(4) 使能 RIPng 协议中主用链路的 BFD（Echo 方式）检测功能。

ripng primary-path-detect bfd echo

缺省情况下，RIPng 协议中主用链路的 BFD（Echo 方式）检测功能处于关闭状态。

1.10 提高RIPng的安全性

1.10.1 配置RIPng报文的零域检查

1. 功能简介

RIPng 报文头部中的一些字段必须配置为 0，也称为零域。使能 RIPng 报文的零域检查功能后，如果报文头部零域中的值不为零，这些报文将被丢弃，不做处理。如果能确保所有报文都是可信任的，则不需要进行该项检查，以节省 CPU 处理时间。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 RIPng 视图。

ripng [*process-id*]

(3) 使能对 RIPng 报文头部的零域检查功能。

checkzero

缺省情况下，RIPng 报文的零域检查功能处于使能状态。

1.10.2 配置IPsec保护RIPng报文

1. 功能简介

在安全性要求较高的网络环境中，可以通过配置基于 IPsec 安全框架的认证方式来对 RIPng 报文进行有效性检查和验证。IPsec 安全框架的具体情况请参见“安全配置指导”中的“IPsec”。

设备在发送的报文中会携带配置好的 IPsec 安全框架的 SPI（Security Parameter Index，安全参数索引）值，接收报文时通过 SPI 值进行 IPsec 安全框架匹配：只有安全框架匹配的报文才能接收；否则将不会接收报文，从而不能正常建立邻居和学习路由。

2. 配置限制和指导

RIPng 支持在进程和接口下配置 IPsec 安全框架。进程下配置的 IPsec 安全框架对该进程下的所有报文有效，接口下的 IPsec 安全框架只对接口下的报文有效。当接口和接口所在进程均配置了 IPsec 安全框架时，接口下的配置生效。

3. RIPng进程上应用IPsec安全框架

(1) 进入系统视图。

system-view

(2) 进入 RIPng 视图。

ripng [*process-id*]

(3) 配置 RIPng 进程应用 IPsec 安全框架。

enable ipsec-profile *profile-name*

缺省情况下，RIPng 进程没有应用 IPsec 安全框架。

4. 接口上应用IPsec安全框架

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置使能了 RIPng 的接口上应用 IPsec 安全框架。

ripng ipsec-profile *profile-name*

缺省情况下，RIPng 接口没有应用 IPsec 安全框架。

1.11 RIPng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 RIPng 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以重启 RIPng 进程或清除指定 RIPng 进程的统计信息。

表1-1 RIPng 显示和维护

操作	命令
显示RIPng进程的GR状态信息	**display ripng** [*process-id*] **graceful-restart**
显示RIPng进程的NSR状态信息	**display ripng** [*process-id*] **non-stop-routing**
显示RIPng进程的配置信息	**display ripng** [*process-id*]
显示RIPng发布数据库中的路由	**display ripng** *process-id* **database** [*ipv6-address prefix-length*]
显示指定RIPng进程的接口信息	**display ripng** *process-id* **interface** [*interface-type interface-number*]
显示RIPng进程的邻居信息	**display ripng** *process-id* **neighbor** [*interface-type interface-number*]

操作	命令
显示指定RIPng进程的路由信息	**display ripng** *process-id* **route** [*ipv6-address prefix-length* [**verbose**] | **peer** *ipv6-address* | **statistics**]
重启指定RIPng进程	**reset ripng** *process-id* **process**
清除RIPng进程的统计信息	**reset ripng** *process-id* **statistics**

1.12 RIPng典型配置举例

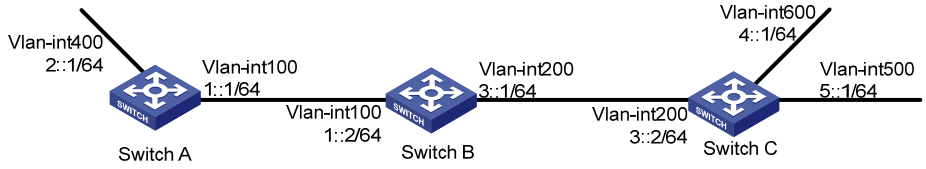
1.12.1 RIPng基本功能配置举例

1. 组网需求

- Switch A、Switch B 和 Switch C 相连并通过 RIPng 来学习网络中的 IPv6 路由信息。
- 在 Switch B 上对接收的 Switch A 的路由（2::/64）进行过滤，使其不加入到 Switch B 的 RIPng 进程的路由表中，发布给 Switch A 的路由只有（4::/64）。

2. 组网图

图1-2 RIPng 基本功能配置组网图



3. 配置步骤

(1) 配置各接口的 IPv6 地址（略）

(2) 配置 RIPng 的基本功能

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ripng 1
[SwitchA-ripng-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ripng 1 enable
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 400
[SwitchA-Vlan-interface400] ripng 1 enable
[SwitchA-Vlan-interface400] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ripng 1
[SwitchB-ripng-1] quit
[SwitchB] interface vlan-interface 200
```

```
[SwitchB-Vlan-interface200] ripng 1 enable
[SwitchB-Vlan-interface200] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ripng 1 enable
[SwitchB-Vlan-interface100] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ripng 1
[SwitchC-ripng-1] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] ripng 1 enable
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 500
[SwitchC-Vlan-interface500] ripng 1 enable
[SwitchC-Vlan-interface500] quit
[SwitchC] interface vlan-interface 600
[SwitchC-Vlan-interface600] ripng 1 enable
[SwitchC-Vlan-interface600] quit
```

查看 Switch B 的 RIPng 路由表。

```
[SwitchB] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D – Direct
                O - Optimal, F - Flush to RIB
 ------------------------------------------------------------------

 Peer FE80::20F:E2FF:FE23:82F5 on Vlan-interface100
 Destination 2::/64,
     via FE80::20F:E2FF:FE23:82F5, cost 1, tag 0, AOF, 6 secs
 Peer FE80::20F:E2FF:FE00:100  on Vlan-interface200
 Destination 4::/64,
     via FE80::20F:E2FF:FE00:100, cost 1, tag 0, AOF, 11 secs
 Destination 5::/64,
     via FE80::20F:E2FF:FE00:100, cost 1, tag 0, AOF, 11
 Local route
 Destination 1::/64,
     via ::, cost 0, tag 0, DOF
 Destination 3::/64,
     via ::, cost 0, tag 0, DOF
```

查看 Switch A 的 RIPng 路由表。

```
[SwitchA] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D – Direct
                O - Optimal, F - Flush to RIB
 ------------------------------------------------------------------

 Peer FE80::200:2FF:FE64:8904 on Vlan-interface100
 Destination 3::/64,
     via FE80::200:2FF:FE64:8904, cost 1, tag 0, AOF, 31 secs
 Destination 4::/64,
     via FE80::200:2FF:FE64:8904, cost 2, tag 0, AOF, 31 secs
```

```
 Destination 5::/64,
     via FE80::200:2FF:FE64:8904, cost 2, tag 0, AOF, 31 secs
 Local route
 Destination 2::/64,
     via ::, cost 0, tag 0, DOF
 Destination 1::/64,
     via ::, cost 0, tag 0, DOF
```

(3) 配置 Switch B 对接收和发布的路由进行过滤

```
[SwitchB] ipv6 prefix-list aaa permit 4:: 64
[SwitchB] ipv6 prefix-list bbb deny 2:: 64
[SwitchB] ipv6 prefix-list bbb permit :: 0 less-equal 128
[SwitchB] ripng 1
[SwitchB-ripng-1] filter-policy prefix-list aaa export
[SwitchB-ripng-1] filter-policy prefix-list bbb import
[SwitchB-ripng-1] quit
```

查看 Switch B 和 Switch A 的 RIPng 路由表。

```
[SwitchB] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D – Direct
                O - Optimal, F - Flush to RIB
 ------------------------------------------------------------------

 Peer FE80::1:100 on Vlan-interface100

 Peer FE80::3:200 on Vlan-interface200
 Destination 4::/64,
     via FE80::2:200, cost 1, tag 0, AOF, 11 secs
 Destination 5::/64,
     via FE80::2:200, cost 1, tag 0, AOF, 11 secs
 Local route
 Destination 1::/64,
     via ::, cost 0, tag 0, DOF
 Destination 3::/64,
     via ::, cost 0, tag 0, DOF
[SwitchA] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D – Direct
                O - Optimal, F - Flush to RIB
 ------------------------------------------------------------------

 Peer FE80::2:100 on Vlan-interface100
 Destination 4::/64,
     via FE80::1:100, cost 2, tag 0, AOF, 2 secs
```

1.12.2 RIPng引入外部路由配置举例

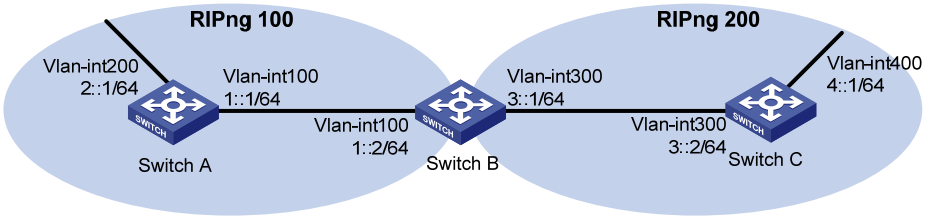
1. 组网需求

- Switch B 上运行两个 RIPng 进程：RIPng100 和 RIPng200。Switch B 通过 RIPng100 和 Switch A 交换路由信息，通过 RIPng200 和 Switch C 交换路由信息。

- 要求在 Switch B 上配置路由引入，将两个不同进程的 RIPng 路由相互引入到对方的 RIPng 进程中。

2. 组网图

图1-3 RIPng 引入外部路由配置组网图



3. 配置步骤

(1) 配置各接口的 IPv6 地址（略）

(2) 配置 RIPng

在 Switch A 上启动 RIPng 进程 100。

```
<SwitchA> system-view
[SwitchA] ripng 100
[SwitchA-ripng-100] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ripng 100 enable
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ripng 100 enable
[SwitchA-Vlan-interface200] quit
```

在 Switch B 上启动两个 RIPng 进程，进程号分别为 100 和 200。

```
<SwitchB> system-view
[SwitchB] ripng 100
[SwitchB-ripng-100] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ripng 100 enable
[SwitchB-Vlan-interface100] quit
[SwitchB] ripng 200
[SwitchB-ripng-200] quit
[SwitchB] interface vlan-interface 300
[SwitchB-Vlan-interface300] ripng 200 enable
[SwitchB-Vlan-interface300] quit
```

在 Switch C 上启动 RIPng 进程 200。

```
<SwitchC> system-view
[SwitchC] ripng 200
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] ripng 200 enable
[SwitchC-Vlan-interface300] quit
[SwitchC] interface vlan-interface 400
[SwitchC-Vlan-interface400] ripng 200 enable
```

```
[SwitchC-Vlan-interface400] quit
```

查看 Switch A 的路由表信息。

```
[SwitchA] display ipv6 routing-table

Destinations : 7 Routes : 7

Destination: ::1/128                                    Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 1::/64                                     Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : Vlan100                                    Cost      : 0

Destination: 1::1/128                                   Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 2::/64                                     Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : Vlan200                                    Cost      : 0

Destination: 2::1/128                                   Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: FE80::/10                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0

Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0
```

(3) 配置 RIPng 引入外部路由

在 Switch B 上将两个不同 RIPng 进程的路由相互引入到对方的路由表中。

```
[SwitchB] ripng 100
[SwitchB-ripng-100] import-route ripng 200
[SwitchB-ripng-100] quit
[SwitchB] ripng 200
[SwitchB-ripng-200] import-route ripng 100
[SwitchB-ripng-200] quit
```

查看路由引入后 Switch A 的路由表信息。

```
[SwitchA] display ipv6 routing-table

Destinations : 8 Routes : 8

Destination: ::1/128                                    Protocol  : Direct
```

```
NextHop    : ::1                                   Preference: 0
Interface  : InLoop0                               Cost      : 0

Destination: 1::/64                                Protocol  : Direct
NextHop    : ::                                    Preference: 0
Interface  : Vlan100                               Cost      : 0

Destination: 1::1/128                              Protocol  : Direct
NextHop    : ::1                                   Preference: 0
Interface  : InLoop0                               Cost      : 0

Destination: 2::/64                                Protocol  : Direct
NextHop    : ::                                    Preference: 0
Interface  : Vlan200                               Cost      : 0

Destination: 2::1/128                              Protocol  : Direct
NextHop    : ::1                                   Preference: 0
Interface  : InLoop0                               Cost      : 0

Destination: 4::/64                                Protocol  : RIPng
NextHop    : FE80::200:BFF:FE01:1C02               Preference: 100
Interface  : Vlan100                               Cost      : 1

Destination: FE80::/10                             Protocol  : Direct
NextHop    : ::                                    Preference: 0
Interface  : NULL0                                 Cost      : 0

Destination: FF00::/8                              Protocol  : Direct
NextHop    : ::                                    Preference: 0
Interface  : NULL0                                 Cost      : 0
```

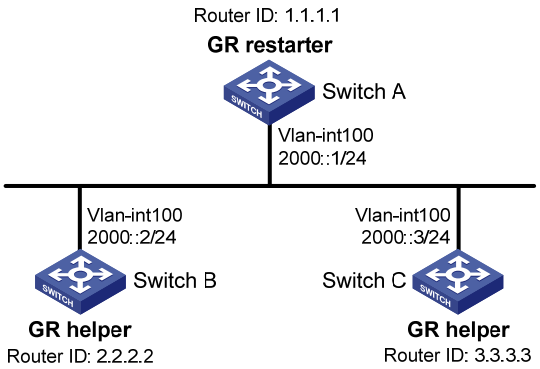
1.12.3 RIPng GR配置举例

1. 组网需求

- Switch A、Switch B 和 Switch C 通过 RIPng 协议实现网络互连。
- Switch A 作为 GR Restarter，Switch B 和 Switch C 作为 GR Helper 并且通过 GR 机制与 Switch A 保持同步。

2. 组网图

图1-4 RIPng GR 配置组网图



3. 配置步骤

(1) 配置各路由器接口的 IPv6 地址和 RIPng 协议

请按照上面组网图配置各接口的 IPv6 地址，具体配置过程略。

配置各路由器之间采用 RIPng 协议进行互连，确保 Router A、Router B 和 Router C 之间能够在网络层互通，并且各路由器之间能够借助 RIPng 协议实现动态路由更新。

(2) 配置 RIPng GR

使能 Switch A 的 RIPng GR 功能。

```
<SwitchA> system-view
[SwitchA] ripng 1
[SwitchA-ripng-1] graceful-restart
```

4. 验证配置

在 Switch A 上触发协议重启或主备倒换后，查看 RIPng 的 GR 状态。

```
<SwitchA> display ripng 1 graceful-restart
RIPng process: 1
 Graceful Restart capability     : Enabled
 Current GR state                : Normal
 Graceful Restart period         : 60  seconds
 Graceful Restart remaining time: 0   seconds
```

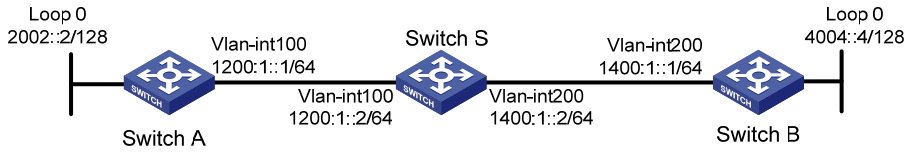
1.12.4 RIPng NSR配置举例

1. 组网需求

Switch S、Switch A、Switch B 通过 RIPng 协议实现网络互连。要求对 Switch S 进行主备倒换时，Switch A 和 Switch B 到 Switch S 的邻居没有中断，Switch A 到 Switch B 的流量没有中断。

2. 组网图

图1-5 RIPng NSR 配置组网图



3. 配置步骤

(1) 配置各接口的 IPv6 地址和 RIPng 协议

请按照上面组网图配置各接口的 IPv6 地址，具体配置过程略。

配置各交换机之间采用 RIPng 协议进行互连，确保 Switch S、Switch A 和 Switch D 之间能够在网络层互通，并且各路由器之间能够借助 RIPng 协议实现动态路由更新。

(2) 配置 RIPng NSR

使能 Switch S 的 RIPng NSR 功能。

```
<SwitchS> system-view
[SwitchS] ripng 1
[SwitchS-ripng-1] non-stop-routing
[SwitchS-ripng-1] quit
```

4. 验证配置

Switch S 进行主备倒换。

```
[SwitchS] placement reoptimize
Predicted changes to the placement
Program                          Current location       New location
-------------------------------------------------------------------------
lb                               0/0                    0/0
lsm                              0/0                    0/0
slsp                             0/0                    0/0
rib6                             0/0                    0/0
routepolicy                      0/0                    0/0
rib                              0/0                    0/0
staticroute6                     0/0                    0/0
staticroute                      0/0                    0/0
ospf                             0/0                    1/0
Continue? [y/n]:y
Re-optimization of the placement start. You will be notified on completion
Re-optimization of the placement complete. Use 'display placement' to view the new placement
```

查看 Switch A 上 RIPng 协议的邻居和路由。

```
[SwitchA] display ripng 1 neighbor
 Neighbor Address: FE80::AE45:5CE7:422E:2867
     Interface  : Vlan-interface100
     Version    : RIPng version 1     Last update: 00h00m23s
     Bad packets: 0                   Bad routes : 0
[SwitchA] display ripng 1 route
```

```
  Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D - Direct
               O - Optimal, F - Flush to RIB
 ------------------------------------------------------------------
 Peer FE80::AE45:5CE7:422E:2867 on Vlan-interface100
 Destination 1400:1::/64,
     via FE80::AE45:5CE7:422E:2867, cost 1, tag 0, AOF, 1 secs
 Destination 4004::4/128,
     via FE80::AE45:5CE7:422E:2867, cost 2, tag 0, AOF, 1 secs
 Local route
 Destination 2002::2/128,
     via ::, cost 0, tag 0, DOF
 Destination 1200:1::/64,
     via ::, cost 0, tag 0, DOF
```

查看 Switch B 上 RIPng 协议的邻居和路由。

```
[SwitchB] display ripng 1 neighbor
 Neighbor Address: FE80::20C:29FF:FECE:6277
     Interface  : Vlan-interface200
     Version    : RIPng version 1     Last update: 00h00m18s
     Bad packets: 0                   Bad routes : 0
[SwitchB] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D - Direct
               O - Optimal, F - Flush to RIB
 ------------------------------------------------------------------
 Peer FE80::20C:29FF:FECE:6277 on Vlan-interface200
 Destination 2002::2/128,
     via FE80::20C:29FF:FECE:6277, cost 2, tag 0, AOF, 24 secs
 Destination 1200:1::/64,
     via FE80::20C:29FF:FECE:6277, cost 1, tag 0, AOF, 24 secs
 Local route
 Destination 4004::4/128,
     via ::, cost 0, tag 0, DOF
 Destination 1400:1::/64,
     via ::, cost 0, tag 0, DOF
```

通过上面信息可以看出在 Switch S 发生主备倒换的时候，Switch A 和 Switch B 的邻居和路由信息保持不变，从 Switch A 到 Switch B 的流量转发没有受到主备倒换的影响。

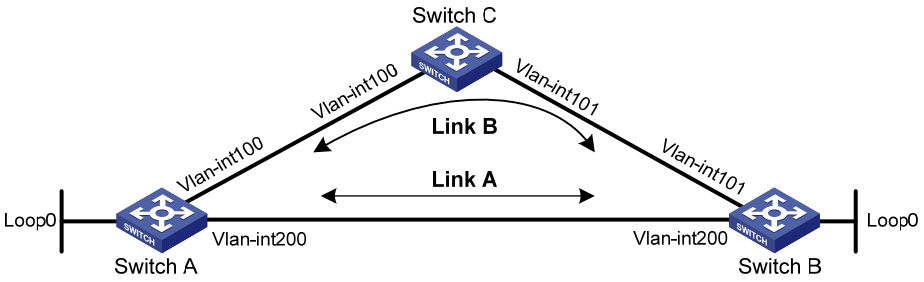
1.12.5 RIPng快速重路由配置举例

1. 组网需求

Switch A、Switch B 和 Switch C 通过 RIPng 协议实现网络互连。要求当 Switch A 和 Switch B 之间的链路出现单通故障时，业务可以快速切换到链路 B 上。

2. 组网图

图1-6 RIPng 快速重路由配置组网图



设备	接口	IP地址	设备	接口	IP地址
Switch A	Vlan-int100	1::1/64	Switch B	Vlan-int101	3::1/64
	Vlan-int200	2::1/64		Vlan-int200	2::2/64
	Loop0	10::1/128		Loop0	20::1/128
Switch C	Vlan-int100	1::2/64			
	Vlan-int101	3::2/64			

3. 配置步骤

(1) 配置各路由器接口的 IPv6 地址和 RIPng 协议

请按照上面组网图配置各接口的 IP 地址和子网掩码，具体配置过程略。

配置各交换机之间采用 RIPng 协议进行互连，确保 Switch A、Switch B 和 Switch C 之间能够在网络层互通，并且各交换机之间能够借助 RIPng 协议实现动态路由更新。

具体配置过程略。

(2) 配置 RIPng 快速重路由

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ipv6 prefix-list abc index 10 permit 20::1 128
[SwitchA] route-policy frr permit node 10
[SwitchA-route-policy-frr-10] if-match ipv6 address prefix-list abc
[SwitchA-route-policy-frr-10] apply ipv6 fast-reroute backup-interface vlan-interface
100 backup-nexthop 1::2
[SwitchA-route-policy-frr-10] quit
[SwitchA] ripng 1
[SwitchA-ripng-1] fast-reroute route-policy frr
[SwitchA-ripng-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ipv6 prefix-list abc index 10 permit 10::1 128
[SwitchB] route-policy frr permit node 10
[SwitchB-route-policy-frr-10] if-match ipv6 address prefix-list abc
[SwitchB-route-policy-frr-10] apply ipv6 fast-reroute backup-interface vlan-interface
101 backup-nexthop 3::2
[SwitchB-route-policy-frr-10] quit
```

```
[SwitchB] ripng 1
[SwitchB-ripng-1] fast-reroute route-policy frr
[SwitchB-ripng-1] quit
```

4. 验证配置

在 Switch A 上查看 20::1/128 的路由信息，可以看到备份下一跳信息。

```
[SwitchA] display ipv6 routing-table 20::1 128 verbose

Summary count : 1

Destination: 20::1/128
   Protocol: RIPng
 Process ID: 1
  SubProtID: 0x0                  Age: 00h17m42s
       Cost: 1              Preference: 100
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Inactive Adv
  OrigTblID: 0x0              OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x22000003         LastAs: 0
     AttrID: 0xffffffff       Neighbor: FE80::34CD:9FF:FE2F:D02
      Flags: 0x41          OrigNextHop: FE80::34CD:9FF:FE2F:D02
      Label: NULL          RealNextHop: FE80::34CD:9FF:FE2F:D02
   BkLabel: NULL            BkNextHop: FE80::7685:45FF:FEAD:102
  Tunnel ID: Invalid          Interface: Vlan-interface200
BkTunnel ID: Invalid       BkInterface: Vlan-interface100
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                PathID: 0x0
```

在 Switch B 上查看 10::1/128 的路由信息，可以看到备份下一跳信息。

```
[SwitchB] display ipv6 routing-table 10::1 128 verbose

Summary count : 1

Destination: 10::1/128
   Protocol: RIPng
 Process ID: 1
  SubProtID: 0x0                  Age: 00h22m34s
       Cost: 1              Preference: 100
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Inactive Adv
  OrigTblID: 0x0              OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x22000001         LastAs: 0
     AttrID: 0xffffffff       Neighbor: FE80::34CC:E8FF:FE5B:C02
      Flags: 0x41          OrigNextHop: FE80::34CC:E8FF:FE5B:C02
      Label: NULL          RealNextHop: FE80::34CC:E8FF:FE5B:C02
    BkLabel: NULL            BkNextHop: FE80::7685:45FF:FEAD:102
  Tunnel ID: Invalid          Interface: Vlan-interface200
```

```
BkTunnel ID: Invalid          BkInterface: Vlan-interface101
   FtnIndex: 0x0             TrafficIndex: N/A
  Connector: N/A                   PathID: 0x0
```

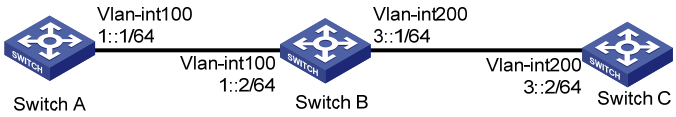
1.12.6 RIPng IPsec安全框架配置举例

1. 组网需求

- Switch A、Switch B 和 Switch C 相连并通过 RIPng 来学习网络中的 IPv6 路由信息。
- 要求配置 IPsec 安全框架对 Switch A、Switch B 和 Switch C 之间的 RIPng 报文进行有效性检查和验证。

2. 组网图

图1-7 RIPng IPsec 安全框架配置组网图



3. 配置步骤

(1) 配置各接口的 IPv6 地址（略）

(2) 配置 RIPng 基本功能

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ripng 1
[SwitchA-ripng-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ripng 1 enable
[SwitchA-Vlan-interface100] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ripng 1
[SwitchB-ripng-1] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ripng 1 enable
[SwitchB-Vlan-interface200] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ripng 1 enable
[SwitchB-Vlan-interface100] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ripng 1
[SwitchC-ripng-1] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] ripng 1 enable
[SwitchC-Vlan-interface200] quit
```

(3) 配置 RIPng IPsec 安全框架

配置 Switch A。创建名为 protrf1 的安全提议，报文封装形式采用传输模式，安全协议采用 ESP 协议。创建一条安全框架 profile001，协商方式为 manual，配置 SPI 和密钥。

```
[SwitchA] ipsec transform-set protrf1
[SwitchA-ipsec-transform-set-protrf1] esp encryption-algorithm 3des-cbc
[SwitchA-ipsec-transform-set-protrf1] esp authentication-algorithm md5
[SwitchA-ipsec-transform-set-protrf1] encapsulation-mode transport
[SwitchA-ipsec-transform-set-protrf1] quit
[SwitchA] ipsec profile profile001 manual
[SwitchA-ipsec-profile-profile001-manual] transform-set protrf1
[SwitchA-ipsec-profile-profile001-manual] sa spi inbound esp 256
[SwitchA-ipsec-profile-profile001-manual] sa spi outbound esp 256
[SwitchA-ipsec-profile-profile001-manual] sa string-key inbound esp simple abc
[SwitchA-ipsec-profile-profile001-manual] sa string-key outbound esp simple abc
[SwitchA-ipsec-profile-profile001-manual] quit
```

配置 Switch B。创建名为 protrf1 的安全提议，报文封装形式采用传输模式，安全协议采用 ESP 协议。创建一条安全框架 profile001，协商方式为 manual，配置 SPI 和密钥。

```
[SwitchB] ipsec transform-set protrf1
[SwitchB-ipsec-transform-set-protrf1] esp encryption-algorithm 3des-cbc
[SwitchB-ipsec-transform-set-protrf1] esp authentication-algorithm md5
[SwitchB-ipsec-transform-set-protrf1] encapsulation-mode transport
[SwitchB-ipsec-transform-set-protrf1] quit
[SwitchB] ipsec profile profile001 manual
[SwitchB-ipsec-profile-profile001-manual] transform-set protrf1
[SwitchB-ipsec-profile-profile001-manual] sa spi inbound esp 256
[SwitchB-ipsec-profile-profile001-manual] sa spi outbound esp 256
[SwitchB-ipsec-profile-profile001-manual] sa string-key inbound esp simple abc
[SwitchB-ipsec-profile-profile001-manual] sa string-key outbound esp simple abc
[SwitchB-ipsec-profile-profile001-manual] quit
```

配置 Switch C。创建名为 protrf1 的安全提议，报文封装形式采用传输模式，安全协议采用 ESP 协议。创建一条安全框架 profile001，协商方式为 manual，配置 SPI 和密钥。

```
[SwitchC] ipsec transform-set protrf1
[SwitchC-ipsec-transform-set-protrf1] esp encryption-algorithm 3des-cbc
[SwitchC-ipsec-transform-set-protrf1] esp authentication-algorithm md5
[SwitchC-ipsec-transform-set-protrf1] encapsulation-mode transport
[SwitchC-ipsec-transform-set-protrf1] quit
[SwitchC] ipsec profile profile001 manual
[SwitchC-ipsec-profile-profile001-manual] transform-set protrf1
[SwitchC-ipsec-profile-profile001-manual] sa spi inbound esp 256
[SwitchC-ipsec-profile-profile001-manual] sa spi outbound esp 256
[SwitchC-ipsec-profile-profile001-manual] sa string-key inbound esp simple abc
[SwitchC-ipsec-profile-profile001-manual] sa string-key outbound esp simple abc
[SwitchC-ipsec-profile-profile001-manual] quit
```

(4) RIPng 进程上应用 IPsec 安全框架

配置 Switch A。

```
[SwitchA] ripng 1
[SwitchA-ripng-1] enable ipsec-profile profile001
[SwitchA-ripng-1] quit
```

配置 Switch B。

```
[SwitchB] ripng 1
[SwitchB-ripng-1] enable ipsec-profile profile001
[SwitchB-ripng-1] quit
```

配置 Switch C。

```
[SwitchC] ripng 1
[SwitchC-ripng-1] enable ipsec-profile profile001
[SwitchC-ripng-1] quit
```

4. 验证配置

以上配置完成后，Switch A、Switch B 和 Switch C 之间的 RIPng 报文将被加密传输。

目 录

1 OSPFv3

1.1 OSPFv3简介

OSPFv3 是 OSPF（Open Shortest Path First，开放最短路径优先）版本 3 的简称，主要提供对 IPv6 的支持。

1.1.1 OSPFv3 和OSPFv2 的异同点

OSPFv3 和 OSPFv2 在很多方面是相同的：

- Router ID，Area ID 仍然是 32 位的。
- 相同类型的报文：Hello 报文，DD（Database Description，数据库描述）报文，LSR（Link State Request，链路状态请求）报文，LSU（Link State Update，链路状态更新）报文和 LSAck（Link State Acknowledgment，链路状态确认）报文。
- 相同的邻居发现机制和邻接形成机制。
- 相同的 LSA 扩散机制和老化机制。

OSPFv3 和 OSPFv2 的不同主要有：

- OSPFv3 是基于链路运行；OSPFv2 是基于网段运行。在配置 OSPFv3 时，不需要考虑是否配置在同一网段，只要在同一链路，就可以直接建立联系。
- OSPFv3 在同一条链路上可以运行多个实例，即一个接口可以使能多个 OSPFv3 进程（使用不同的实例）。
- OSPFv3 是通过 Router ID 来标识邻居；OSPFv2 则是通过 IPv4 地址来标识邻居。

关于 OSPF 版本 2 的介绍，请参见“三层技术-IP 路由”中的“OSPF”。

1.1.2 OSPFv3 的协议报文

和 OSPFv2 一样，OSPFv3 也有五种报文类型，如下：

- Hello 报文：周期性发送，用来发现和维持 OSPFv3 邻居关系，以及进行 DR（Designated Router，指定路由器）/BDR（Backup Designated Router，备份指定路由器）的选举。
- DD（Database Description，数据库描述）报文：描述了本地 LSDB（Link State DataBase，链路状态数据库）中每一条 LSA（Link State Advertisement，链路状态通告）的摘要信息，用于两台路由器进行数据库同步。
- LSR（Link State Request，链路状态请求）报文：向对方请求所需的 LSA。两台路由器互相交换 DD 报文之后，得知对端的路由器有哪些 LSA 是本地的 LSDB 所缺少的，这时需要发送 LSR 报文向对方请求所需的 LSA。
- LSU（Link State Update，链路状态更新）报文：向对方发送其所需要的 LSA。
- LSAck（Link State Acknowledgment，链路状态确认）报文：用来对收到的 LSA 进行确认。

1.1.3 OSPFv3 的LSA类型

LSA（Link State Advertisement，链路状态通告）是 OSPFv3 协议计算和维护路由信息的主要来源，常用的 LSA 有以下几种类型：

- Router LSA（Type-1）：由每个路由器生成，描述本路由器的链路状态和开销，只在路由器所处区域内传播。
- Network LSA（Type-2）：由广播网络和 NBMA（Non-Broadcast Multi-Access，非广播多路访问）网络的 DR（Designated Router，指定路由器）生成，描述本网段接口的链路状态，只在 DR 所处区域内传播。
- Inter-Area-Prefix LSA（Type-3）：由 ABR（Area Border Router，区域边界路由器）生成，在与该 LSA 相关的区域内传播，描述一条到达本自治系统内其他区域的 IPv6 地址前缀的路由。
- Inter-Area-Router LSA（Type-4）：由 ABR 生成，在与该 LSA 相关的区域内传播，描述一条到达本自治系统内的 ASBR（Autonomous System Boundary Router，自治系统边界路由器）的路由。
- AS External LSA（Type-5）：由 ASBR 生成，描述到达其它 AS（Autonomous System，自治系统）的路由，传播到整个 AS（Stub 区域和 NSSA 区域除外）。缺省路由也可以用 AS External LSA 来描述。
- NSSA LSA（Type-7）：由 NSSA（Not-So-Stubby Area）区域内的 ASBR 生成，描述到 AS 外部的路由，仅在 NSSA 区域内传播。
- Link LSA（Type-8）：路由器为每一条链路生成一个 Link-LSA，在本地链路范围内传播，描述该链路上所连接的 IPv6 地址前缀及路由器的 Link-local 地址。
- Intra-Area-Prefix LSA（Type-9）：包含路由器上的 IPv6 前缀信息，Stub 区域信息或穿越区域（Transit Area）的网段信息，该 LSA 在区域内传播。由于 Router LSA 和 Network LSA 不再包含地址信息，导致了 Intra-Area-Prefix LSA 的引入。
- Grace LSA（Type-11）：由 Restarter 在重启时候生成的，在本地链路范围内传播。这个 LSA 描述了重启设备的重启原因和重启时间间隔，目的是通知邻居本设备将进入 GR（Graceful Restart，平滑重启）。

1.1.4 协议规范

与 OSPFv3 相关的协议规范有：

- RFC 2328：OSPF Version 2
- RFC 3101：OSPF Not-So-Stubby Area (NSSA) Option
- RFC 4552：Authentication/Confidentiality for OSPFv3
- RFC 5187：OSPFv3 Graceful Restart
- RFC 5329：Traffic Engineering Extensions to OSPF Version 3
- RFC 5340：OSPF for IPv6
- RFC 5523：OSPFv3-Based Layer 1 VPN Auto-Discovery
- RFC 5643：Management Information Base for OSPFv3
- RFC 6506：Supporting Authentication Trailer for OSPFv3

- RFC 6565：OSPFv3 as a Provider Edge to Customer Edge (PE-CE) Routing Protocol
- RFC 6969：OSPFv3 Instance ID Registry Update
- RFC 7166：Supporting Authentication Trailer for OSPFv3

1.2 OSPFv3与硬件适配关系

S5110V2-SI、S5000V3-EI 和 S5000E-X 系列交换机不支持 OSPFv3。

1.3 OSPFv3配置任务简介

OSPFv3 配置任务如下：

(1) 使能OSPFv3 功能

(2) （可选）配置OSPFv3 的区域属性
- 配置OSPFv3 的Stub区域
- 配置OSPFv3 的NSSA区域
- 配置OSPFv3 的虚连接

  所有非骨干区域必须与骨干区域保持连通，并且骨干区域自身也要保持连通。无法满足这个要求时，可以通过在 ABR 上配置 OSPFv3 虚连接予以解决。

(3) （可选）配置OSPFv3 的网络类型
- 配置OSPFv3 接口的网络类型为广播
- 配置OSPFv3 接口的网络类型为NBMA
- 配置OSPFv3 接口的网络类型为P2MP
- 配置OSPFv3 接口的网络类型为P2P

(4) （可选）配置OSPFv3 的路由信息控制
- 配置OSPFv3 区域间路由聚合
- 配置对引入的外部路由信息进行路由聚合
- 过滤通过接收到的LSA计算出来的路由信息
- 配置过滤Inter-Area-Prefix-LSA
- 配置OSPFv3 接口的开销值
- 配置OSPFv3 协议的优先级
- 配置OSPFv3 引入外部路由
- 配置OSPFv3 引入缺省路由

(5) （可选）配置OSPFv3 定时器
- 配置OSPFv3 报文定时器
- 配置接口的LSA传输延迟时间
- 配置SPF计算时间间隔
- 配置LSA重新生成的时间间隔
- 配置接口发送LSU报文的时间间隔和一次发送LSU报文的最大个数

(6) （可选）配置接口的DR优先级

(7) （可选）配置OSPFv3 报文相关功能
   - 忽略DD报文中的MTU检查
   - 禁止接口收发OSPFv3 报文

(8) （可选）配置前缀抑制

(9) （可选）配置Stub路由器

(10) （可选）提高 OSPF 网络的可靠性
   - 配置OSPFv3 GR
   - 配置OSPFv3 NSR
   - 配置OSPFv3 与BFD联动
   - 配置OSPFv3 快速重路由

(11) （可选）应用IPsec安全框架保护OSPFv3 报文

(12) （可选）配置OSPFv3 日志和告警功能
   - 配置邻居状态变化的输出开关
   - 配置OSPFv3 的日志信息个数
   - 配置OSPFv3 网管功能

1.4 使能OSPFv3功能

1. 功能简介

要在路由器上使能 OSPFv3 功能，必须先创建 OSPFv3 进程、指定该进程的 Router ID 并在接口上使能 OSPFv3 功能。

在一台路由器上可以创建多个 OSPFv3 进程，OSPFv3 进程是本地概念。不同的路由器之间，即使进程不同也可以进行报文交换。

Router ID 用来在一个自治系统中唯一的标识一台路由器。在 OSPFv3 中，用户必须手工配置一个 Router ID，而且必须保证自治系统中任意两台路由器的 Router ID 都不相同。因此，为了保证 OSPFv3 运行的稳定性，在进行网络规划时，应确定路由器 ID 的划分并手工配置。

2. 配置限制和指导

如果在同一台路由器上运行了多个 OSPFv3 进程，必须为不同的进程指定不同的 Router ID。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 启动 OSPFv3，并进入 OSPFv3 视图。

ospfv3 [*process-id*]

缺省情况下，系统没有运行 OSPFv3。

(3) 配置路由器的 Router ID。

router-id *router-id*

缺省情况下，运行 OSPFv3 协议的路由器没有 Router ID。

(4) 进入接口视图。

interface *interface-type interface-number*

(5) 在接口上使能 OSPFv3 功能。

ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

缺省情况下，接口上的 OSPFv3 功能处于关闭状态。

1.5 配置OSPFv3的区域属性

1.5.1 功能简介

OSPFv3 支持 Stub 区域、NSSA 区域和虚连接的配置，其原理及应用环境与 OSPFv2 相同。

OSPFv3 划分区域后，可以减少网络中 LSA 的数量，OSPFv3 的扩展性也得以增强。对于位于 AS 边缘的一些非骨干区域，为了更多的缩减其路由表规模和降低 LSA 的数量，可以将它们配置为 Stub 区域。

Stub 区域不能引入外部路由，为了在允许将自治系统外部路由通告到 OSPFv3 路由域内部的同时，保持其余部分的 Stub 区域的特征，网络管理员可以将区域配置为 NSSA 区域。NSSA 区域也是位于 AS 边缘的非骨干区域。

在划分区域之后，非骨干区域之间的 OSPFv3 路由更新是通过骨干区域来交换完成的。对此，OSPFv3 要求所有非骨干区域必须与骨干区域保持连通，并且骨干区域自身也要保持连通。但在实际应用中，可能会因为各方面条件的限制，无法满足这个要求。这时可以通过配置 OSPFv3 虚连接予以解决。

1.5.2 配置OSPFv3 的Stub区域

1. 配置限制和指导

对于位于 Stub 区域中的所有路由器都必须执行本配置。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 进入 OSPFv3 区域视图。

area *area-id*

(4) 配置一个区域为 Stub 区域。

stub [**default-route-advertise-always** | **no-summary**] *

缺省情况下，没有区域被配置为 Stub 区域。

参数 **no-summary** 只能在 ABR 上配置。指定 **no-summary** 参数后，ABR 只向区域内发布一条描述缺省路由的 Inter-Area-Prefix-LSA。

(5) （可选）配置发送到 Stub 区域的缺省路由的开销值。

default-cost *cost-value*

缺省情况下，发送到 Stub 区域的缺省路由的开销值为 1。

1.5.3 配置OSPFv3 的NSSA区域

1. 配置限制和指导

对于位于 NSSA 区域中的所有路由器都必须执行本配置。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 进入 OSPFv3 区域视图。

area *area-id*

(4) 配置一个区域为 NSSA 区域。

nssa [**default-route-advertise** [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] * | **no-import-route** | **no-summary** | [**translate-always** | **translate-never**] | **suppress-fa** | **translator-stability-interval** *value*] *

缺省情况下，没有区域被配置为 NSSA 区域。

指定 **no-summary** 参数可以将该区域配置为 Totally NSSA 区域，该区域的 ABR 不会将区域间的路由信息传递到本区域。

(5) （可选）配置发送到 NSSA 区域的缺省路由的开销值。

default-cost *cost-value*

缺省情况下，发送到 NSSA 区域的缺省路由的开销值为 1。

本命令只有在 NSSA 区域和 Totally NSSA 区域的 ABR/ASBR 上配置才能生效。

1.5.4 配置OSPFv3 的虚连接

1. 功能简介

对于没有和骨干区域直接相连的非骨干区域，或者不连续的骨干区域，可以使用该配置建立逻辑上的连通性。

2. 配置限制和指导

虚连接的两端必须是 ABR，而且必须在两端同时配置才可生效。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 进入 OSPFv3 区域视图。

area *area-id*

(4) 创建并配置虚连接。

vlink-peer *router-id* [**dead** *seconds* | **hello** *seconds* | **instance** *instance-id* | **ipsec-profile** *profile-name* | **retransmit** *seconds* | **trans-delay** *seconds*] *

1.6 配置OSPFv3的网络类型

1.6.1 配置限制和指导

OSPFv3 根据链路层协议类型将网络分为四种不同的类型：广播、NBMA、P2MP 和 P2P。接口的网络类型根据物理接口而定，用户可以根据需要配置 OSPFv3 接口的网络类型：

- 如果在广播网络上有不支持组播地址的路由器，可以将接口的网络类型改为 NBMA。
- 如果一网段内只有两台路由器运行 OSPFv3 协议，也可将接口类型配置为 P2P，节省网络开销。

1.6.2 配置OSPFv3 接口的网络类型为广播

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置 OSPFv3 接口的网络类型。

ospfv3 network-type broadcast [**instance** *instance-id*]

缺省情况下，接口的网络类型为广播类型。

1.6.3 配置OSPFv3 接口的网络类型为NBMA

1. 配置限制和指导

当路由器的接口类型为 NBMA 时，由于无法通过广播 Hello 报文的形式发现相邻路由器，必须手工指定相邻路由器的本地链路地址、该相邻路由器是否有 DR 选举权等。

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 OSPFv3 接口的网络类型为 NBMA。

ospfv3 network-type nbma [**instance** *instance-id*]

缺省情况下，接口的网络类型为广播类型。

(4) （可选）配置 OSPFv3 接口的路由优先级。

ospfv3 dr-priority *priority*

缺省情况下，接口的路由优先级为 1。

本命令设置的优先级用于实际的 DR 选举。

(5) 配置 NBMA 网络的邻居。

ospfv3 peer *ipv6-address* [**cost** *cost-value* | **dr-priority** *priority*] [**instance** *instance-id*]

缺省情况下，未指定邻居接口的链路本地地址。

1.6.4 配置OSPFv3 接口的网络类型为P2MP

1. 配置限制和指导

当路由器的接口的网络类型为 P2MP，且在 P2MP 网络中接口选择单播形式发送报文时，由于无法通过广播 Hello 报文的形式发现相邻路由器，必须手工指定相邻路由器的本地链路地址。

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 OSPFv3 接口的网络类型为 P2MP。

ospfv3 network-type p2mp [**unicast**] [**instance** *instance-id*]

缺省情况下，接口的网络类型为广播类型。

(4) 配置 P2MP（单播）网络的邻居。

ospfv3 peer *ipv6-address* [**cost** *cost-value* | **dr-priority** *priority*] [**instance** *instance-id*]

缺省情况下，未指定邻居接口的链路本地地址。

1.6.5 配置OSPFv3 接口的网络类型为P2P

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置 OSPFv3 接口的网络类型为 P2P。

ospfv3 network-type p2p [**instance** *instance-id*]

缺省情况下，接口的网络类型为广播类型。

1.7 配置OSPFv3的路由信息控制

1.7.1 配置OSPFv3 区域间路由聚合

1. 功能简介

如果一个区域中存在多个连续的网段，则可以在 ABR 上配置路由聚合将它们聚合成一个网段，ABR 只发送一条聚合后的 LSA，所有落入本命令指定的聚合网段范围的 LSA 将不再会被单独发送出去，这样可减小其它区域中 LSDB 的规模。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 进入 OSPFv3 区域视图。

area *area-id*

(4) 配置 ABR 路由聚合。

abr-summary *ipv6-address prefix-length* [**not-advertise**] [**cost** *cost-value*]

缺省情况下，ABR 不对路由进行聚合。

1.7.2 配置对引入的外部路由信息进行路由聚合

1. 功能简介

如果引入的路由中存在多个连续的网段，则可以在 ASBR 上配置路由聚合将它们聚合成一个网段。

如果本地路由器是 ASBR，配置 ASBR 路由聚合可对引入的聚合地址范围内的 Type-5 LSA 描述的路由进行聚合；当配置了 NSSA 区域时，对引入的聚合地址范围内的 Type-7 LSA 描述的路由进行聚合。

如果本地路由器同时是 ASBR 和 ABR，并且是 NSSA 区域的转换路由器，则对由 Type-7 LSA 转化成的 Type-5 LSA 描述的路由进行聚合处理；如果不是 NSSA 区域的转换路由器，则不进行聚合处理。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 配置 ASBR 路由聚合。

asbr-summary *ipv6-address prefix-length* [**cost** *cost-value* | **not-advertise** | **nssa-only** | **tag** *tag*] *

缺省情况下，ASBR 不对引入的路由进行聚合。

1.7.3 过滤通过接收到的LSA计算出来的路由信息

1. 功能简介

OSPFv3 接收到 LSA 后，可以根据一定的过滤条件来决定是否将计算后得到的路由信息加入到本地路由表中。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 过滤通过接收到的 LSA 计算出来的路由信息。

filter-policy { *ipv6-acl-number* [**gateway** *prefix-list-name*] | **prefix-list** *prefix-list-name* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name* | **route-policy** *route-policy-name* } **import**

缺省情况下，不对通过接收到的 LSA 计算出来的路由信息进行过滤。

本命令只对 OSPFv3 计算出来的路由进行过滤，没有通过过滤的路由将不被加入到本地路由表中，从而不能用于转发报文。

1.7.4 配置过滤Inter-Area-Prefix-LSA

1. 配置限制和指导

此命令只在 ABR 路由器上有效，对区域内部路由器无效。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 进入 OSPFv3 区域视图。

area *area-id*

(4) 配置对 Inter-Area-Prefix-LSA 进行过滤。

filter { *ipv6-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } { **export** | **import** }

缺省情况下，不对 Inter-Area-Prefix-LSA 进行过滤。

1.7.5 配置OSPFv3 接口的开销值

1. 功能简介

OSPFv3 有两种方式来配置接口的开销值：

- 第一种方法是在接口视图下直接配置开销值；
- 第二种方法是配置接口的带宽参考值，OSPFv3 根据带宽参考值自动计算接口的开销值，计算公式为：接口开销＝带宽参考值（100Mbps）÷接口带宽（Mbps），当计算出来的开销值大于 65535，开销取最大值 65535；当计算出来的开销值小于 1 时，开销取最小值 1。

2. 配置接口的开销值

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置 OSPFv3 接口的开销值。

ospfv3 cost *cost-value* [**instance** *instance-id*]

缺省情况下，OSPFv3 根据接口的带宽自动计算链路开销，对于 VLAN 接口，缺省值为 1；对于 Loopback 接口，缺省取值为 0。

3. 配置带宽参考值

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 配置带宽参考值。

bandwidth-reference *value*

缺省情况下，带宽参考值为 100Mbps。

1.7.6 配置OSPFv3 协议的优先级

1. 功能简介

由于路由器上可能同时运行多个动态路由协议，就存在各个路由协议之间路由信息共享和选择的问题。系统为每一种路由协议设置一个优先级，在不同协议发现同一条路由时，优先级高的路由将被优选。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 配置 OSPFv3 协议的路由优先级。

preference [**ase**] { *preference* | **route-policy** *route-policy-name* } *

缺省情况下，对于自治系统内部路由，OSPFv3 协议的路由优先级为 10；对于自治系统外部路由，OSPFv3 协议的路由优先级为 150。

1.7.7 配置OSPFv3 引入外部路由

1. 配置限制和指导

由于 OSPFv3 是基于链路状态的路由协议，不能直接对发布的 LSA 进行过滤，所以只能在 OSPFv3 引入路由时进行过滤，只有符合条件的路由才能转换成 LSA 发布出去。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 引入外部路由信息。

import-route { **direct** | **static** } [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

import-route { **ospfv3** | **ripng** } [*process-id* | **all-processes**]

缺省情况下，不引入外部路由信息。

(4) （可选）对引入的外部路由信息进行过滤。

filter-policy { *ipv6-acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*]]

缺省情况下，不对引入的路由信息进行过滤。

本命令只对本设备使用 **import-route** 引入的路由起作用。如果没有配置 **import-route** 命令来引入其它外部路由（包括不同进程的 OSPFv3 路由），则本命令失效。

(5) 配置路由引入的全局标记。

default tag *tag*

缺省情况下，路由引入的全局标记为 1。

1.7.8 配置OSPFv3 引入缺省路由

1. 功能简介

OSPFv3 不能通过 **import-route** 命令从其它协议引入缺省路由，如果想把缺省路由引入到 OSPFv3 路由区域，必须要使用下面命令配置 OSPFv3 引入缺省路由。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 配置 OSPFv3 引入缺省路由。

default-route-advertise [[**always** | **permit-calculate-other**] | **cost** *cost-value* | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

缺省情况下，未引入缺省路由。

(4) 配置路由引入的全局标记。

default tag *tag*

缺省情况下，路由引入的全局标记为 1。

1.8 配置OSPFv3定时器

1.8.1 配置OSPFv3 报文定时器

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置接口发送 hello 报文的时间间隔。

ospfv3 timer hello *seconds* [**instance** *instance-id*]

缺省情况下，P2P、Broadcast 网络类型接口发送 Hello 报文的时间间隔的值为 10 秒；P2MP、NBMA 类型接口发送 Hello 报文的时间间隔为 30 秒。

(4) 配置相邻路由器间失效时间。

ospfv3 timer dead *seconds* [**instance** *instance-id*]

缺省情况下，P2P、Broadcast 网络类型接口的 OSPFv3 邻居失效时间为 40 秒；P2MP、NBMA 类型接口的 OSPFv3 邻居失效的时间为 120 秒。

相邻路由器间失效时间的值不要设置得太小，否则邻居很容易失效。

(5) 配置轮询定时器。

ospfv3 timer poll *seconds* [**instance** *instance-id*]

缺省情况下，发送轮询 Hello 报文的时间间隔为 120 秒。

(6) 配置相邻路由器重传 LSA 的时间间隔。

ospfv3 timer retransmit *interval* [**instance** *instance-id*]

缺省情况下，LSA 的重传时间间隔为 5 秒。

相邻路由器重传 LSA 时间间隔的值不要设置得太小，否则将会引起不必要的重传。

1.8.2 配置接口的LSA传输延迟时间

1. 功能简介

LSA 在本路由器的链路状态数据库（LSDB）中会随时间老化（每秒钟加 1），但在网络的传输过程中却不会，所以有必要在发送之前将 LSA 的老化时间增加一定的延迟时间。此配置对低速率的网络尤其重要。

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) 配置接口的 LSA 传输延迟时间。

ospfv3 trans-delay *seconds* [**instance** *instance-id*]

缺省情况下，接口的 LSA 传输延迟时间为 1 秒。

1.8.3 配置SPF计算时间间隔

1. 功能简介

当 OSPFv3 的 LSDB 发生改变时，需要重新计算最短路径。如果网络频繁变化，且每次变化都立即计算最短路径，将会占用大量系统资源，并影响路由器的效率。通过调节 SPF 计算时间间隔，可以抑制由于网络频繁变化带来的影响。

本命令在网络变化不频繁的情况下将连续路由计算的时间间隔缩小到 *minimum-interval*，而在网络变化频繁的情况下可以进行相应惩罚，增加 *incremental-interval*×2^{n-2}（n 为连续触发路由计算的次数），将等待时间按照配置的惩罚增量延长，最大不超过 *maximum-interval*。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 配置 SPF 计算时间间隔。

spf-schedule-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

缺省情况下，SPF 计算的最大时间间隔为 5 秒，最小时间间隔为 50 毫秒，时间间隔惩罚增量为 200 毫秒。

1.8.4 配置LSA重新生成的时间间隔

1. 功能简介

通过调节 LSA 重新生成的时间间隔，可以抑制网络频繁变化可能导致的占用过多带宽资源和路由器资源。

本命令在网络变化不频繁的情况下将 LSA 重新生成时间间隔缩小到 *minimum-interval*，而在网络变化频繁的情况下可以进行相应惩罚，增加 *incremental-interval*×2^{n-2}（n 为连续触发路由计算的次数），将等待时间按照配置的惩罚增量延长，最大不超过 *maximum-interval*。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 配置 LSA 重新生成的时间间隔。

lsa-generation-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

缺省情况下，最大时间间隔为 5 秒，最小时间间隔为 0 毫秒，惩罚增量为 0 毫秒。

1.8.5 配置接口发送LSU报文的时间间隔和一次发送LSU报文的最大个数

1. 功能简介

如果路由器路由表里的路由条目很多，在与邻居进行 LSDB 同步时，可能需要发送大量 LSU，有可能会对当前设备和网络带宽带来影响；因此，路由器将 LSU 报文分为多个批次进行发送，并且对 OSPFv3 接口每次允许发送的 LSU 报文的最大个数做出限制。

用户可根据需要配置 OSPFv3 接口发送 LSU 报文的时间间隔以及接口一次发送 LSU 报文的最大个数。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 配置接口发送 LSU 报文的时间间隔和一次发送 LSU 报文的最大个数。

transmit-pacing interval *interval* **count** *count*

缺省情况下，OSPFv3 接口发送 LSU 报文的时间间隔为 20 毫秒，一次最多发送 3 个 LSU 报文。

1.9 配置接口的DR优先级

1. 功能简介

路由器接口的 DR 优先级将影响接口在选举 DR 时所具有的资格，优先级为 0 的路由器不会被选举为 DR 或 BDR。

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) 配置接口的 DR 优先级。

ospfv3 dr-priority *priority* [**instance** *instance-id*]

缺省情况下，接口的 DR 优先级为 1。

1.10 配置OSPFv3报文相关功能

1.10.1 忽略DD报文中的MTU检查

1. 功能简介

在 LSA 数量不多的情况下，没有必要去检查 MTU 大小，可以设置忽略 DD 报文中的 MTU 检查，从而提高性能。

2. 配置限制和指导

双方的接口 MTU 必须相同才能建立邻居关系。

3. 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) 忽略 DD 报文中的 MTU 检查。

ospfv3 mtu-ignore [**instance** *instance-id*]

缺省情况下，接口在进行 DD 报文交换时执行 MTU 检查。

1.10.2 禁止接口收发OSPFv3 报文

1. 功能简介

当运行 OSPFv3 协议的接口被配置为 Silent 状态后，该接口的直连路由仍可以由同一路由器的其他接口通过 Intra-Area-Prefix-LSA 发布，但 OSPFv3 报文将被阻塞，接口上不会建立 OSPFv3 邻居关系。这一特性可以增强 OSPFv3 的组网适应能力。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 禁止接口收发 OSPFv3 报文。

silent-interface { *interface-type interface-number* | **all** }

缺省情况下，允许接口收发 OSPFv3 报文。

不同的进程可以对同一接口禁止收发 OSPFv3 报文，但本命令只对本进程已经使能的 OSPFv3 接口起作用，不对其它进程的接口起作用。

1.11 配置前缀抑制

1.11.1 功能简介

接口使能 OSPFv3 后，会将接口下的所有网段路由都通过 LSA 发布，但有时候网段路由是不希望被发布的。通过前缀抑制配置，可以减少 LSA 中携带不需要的前缀，即不发布某些网段路由，从而提高网络安全性，加快路由收敛。

当使能前缀抑制时，Type-8 LSA 中不发布处于抑制的接口前缀信息；对于广播网或者 NBMA 网络，DR 在生成引用 Type-2 LSA 的 Type-9 LSA 时，不发布处于抑制的接口前缀信息；对于 P2P 或 P2MP 网络，生成引用 Type-1 LSA 的 Type-9 LSA 时，不发布处于抑制的接口前缀信息。

1.11.2 配置限制和指导

如果需要抑制前缀发布，建议整个 OSPFv3 网络都配置本命令，否则会有互通问题。

1.11.3 配置全局前缀抑制

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 配置前缀抑制功能。

prefix-suppression

缺省情况下，不抑制 OSPFv3 进程进行前缀发布。

不能抑制 LoopBack 接口和处于 silent-interface 状态接口对应的前缀。

1.11.4 配置接口前缀抑制

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置接口的前缀抑制功能。

ospfv3 prefix-suppression [**disable**] [**instance** *instance-id*]

缺省情况下，不抑制接口进行前缀发布。

1.12 配置Stub路由器

1. 功能简介

Stub 路由器用来控制流量，它告知其他 OSPFv3 路由器不要使用这个 Stub 路由器来转发数据，但可以拥有一个到 Stub 路由器的路由。

将当前路由器配置为 Stub 路由器的功能，可通过 R-bit 和 max-metric 两种模式来实现：

- R-bit 模式：通过清除该路由器发布 Type-1 LSA 中 options 域的 R-bit，使其他路由器只能计算到该路由器本身而不会通过该路由器来转发数据。
- max-metric 模式：该路由器发布的 Type-1 LSA 的链路度量值将设为最大值 65535，这样其邻居计算出这条路由的开销就会很大，如果邻居上有到这个目的地址开销更小的路由，则数据不会通过这个 Stub 路由器转发。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 配置当前路由器为 Stub 路由器。请选择其中一项进行配置。

- 配置当前路由器为 Stub 路由器，且发布的 Type-1 LSA 中的 options 域的 R-bit 将被清除。

  stub-router r-bit [**include-stub** | **on-startup** *seconds*] *

- 配置当前路由器为 Stub 路由器，且发布的 Type-1 LSA 的链路度量值将设置为最大值 65535。

  stub-router max-metric [**external-lsa** [*max-metric-value*] | **summary-lsa** [*max-metric-value*] | **include-stub** | **on-startup** *seconds*] *

缺省情况下，当前路由器没有被配置为 Stub 路由器。

Stub 路由器与 Stub 区域无关。

1.13 配置OSPFv3 GR

1.13.1 功能简介

GR（Graceful Restart，平滑重启）是一种在协议重启或主备倒换时保证转发业务不中断的机制。GR 有两个角色：

- GR Restarter：发生协议重启或主备倒换事件且具有 GR 能力的设备。
- GR Helper：和 GR Restarter 具有邻居关系，协助完成 GR 流程的设备。

支持 OSPFv3 的 GR Restarter 能力的设备主备倒换后，为了实现设备转发业务的不中断，它必须完成下列两项任务：

- 重启过程 GR Restarter 转发表项保持稳定；
- 重启流程结束后重建所有邻居关系，重新获取完整的网络拓扑信息。

设备（GR Restarter）主备倒换后，首先向邻居发送 Grace LSA 通告邻居本设备进入 GR；邻居收到 Grace-LSA 后，如果支持 GR Helper 能力则进入 Helper 模式（此时该邻居称为 GR Helper）。GR Restarter 重新建立邻居，GR Helper 帮助 GR Restarter 进行 LSDB 的同步。同步完成之后，GR 流程结束，进入正常的 OSPFv3 流程。这样就能实现设备在主备倒换时转发业务正常进行。

1.13.2 配置限制和指导

设备充当 GR Restarter 后不能再配置 OSPFv3 NSR 功能。

1.13.3 配置GR Restarter

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 使能 GR 能力。

graceful-restart enable [**global** | **planned-only**] *

缺省情况下，OSPFv3 协议的 GR Restarter 能力处于关闭状态。

(4) （可选）配置 GR 重启时间间隔。

graceful-restart interval *interval*

缺省情况下，OSPFv3 协议的 GR 重启间隔时间为 120 秒。

1.13.4 配置GR Helper

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 使能 GR Helper 能力。

graceful-restart helper enable [**planned-only**]

缺省情况下，OSPFv3 的 GR Helper 能力处于开启状态。

(4) 使能 LSA 严格检查能力。

graceful-restart helper strict-lsa-checking

缺省情况下，OSPFv3 协议的 GR Helper 严格 LSA 检查能力处于关闭状态。

1.13.5 以GR方式重启OSPFv3 进程

1. 功能简介

设备进行主备倒换或者进行如下操作均可以以 GR 方式重启 OSPFv3 进程。

2. 配置步骤

请在用户视图下执行本命令，以 GR 方式重启 OSPFv3 进程。

reset ospfv3 [*process-id*] **process graceful-restart**

1.14 配置OSPFv3 NSR

1. 功能简介

NSR（Nonstop Routing，不间断路由）通过将 OSPFv3 链路状态信息从主进程备份到备进程，使设备在发生主备倒换时可以自行完成链路状态的恢复和路由的重新生成，邻接关系不会发生中断，从而避免了主备倒换对转发业务的影响。

GR 特性需要周边设备配合才能完成路由信息的恢复，在网络应用中有一定的限制。NSR 特性不需要周边设备的配合，网络应用更加广泛。

2. 配置限制和指导

设备配置了 OSPFv3 NSR 功能后不能再充当 GR Restarter。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 使能 OSPFv3 NSR 功能。

non-stop-routing

缺省情况下，OSPFv3 NSR 功能处于关闭状态。

各个进程的 NSR 功能是相互独立的，只对本进程生效。如果存在多个 OSPFv3 进程，建议在各个进程下使能 OSPFv3 NSR 功能。

1.15 配置OSPFv3与BFD联动

1. 功能简介

BFD（Bidirectional Forwarding Detection，双向转发检测）能够为 OSPFv3 邻居之间的链路提供快速检测功能。当邻居之间的链路出现故障时，加快 OSPFv3 协议的收敛速度。关于 BFD 的介绍和基本功能配置，请参见“可靠性配置指导”中的“BFD”。

OSPFv3 使用 BFD 来进行快速故障检测时，可以通过 Hello 报文动态发现邻居，将邻居地址通知 BFD 就开始建立会话。BFD 会话建立前处于 down 状态，此时 BFD 控制报文以不小于 1 秒的时间间隔周期发送以减少控制报文流量，直到会话建立以后才会以协商的时间间隔发送以实现快速检测。

进行配置 BFD 之前，需要配置 OSPFv3 功能。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 配置路由器的 ID。

router-id *router-id*

(4) 退出 OSPFv3 视图。

quit

(5) 进入接口视图。

interface *interface-type interface-number*

(6) 在接口上使能 OSPFv3。

ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

(7) 在指定接口上使能 OSPFv3 BFD。

ospfv3 bfd enable [**instance** *instance-id*]

缺省情况下，运行 OSPFv3 的接口的 BFD 功能处于关闭状态。

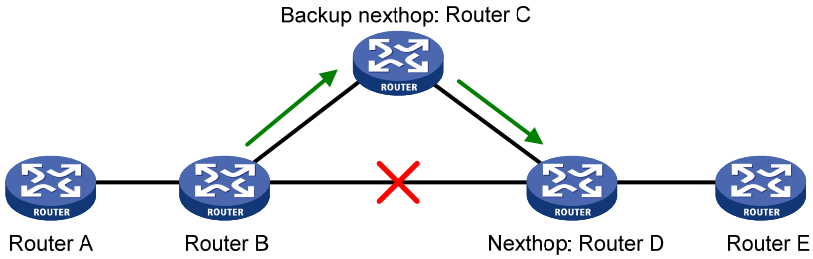
1.16 配置OSPFv3快速重路由

1.16.1 功能简介

在部署了备份链路的 OSPFv3 网络中，当主用链路发生故障时，OSPFv3 会对路由进行重新计算，在路由收敛完成后，流量可以通过备份链路进行传输。在路由收敛期间，数据流量将会被中断。

为了尽可能缩短网络故障导致的流量中断时间，网络管理员可以根据需要配置 OSPFv3 快速重路由功能。

图1-1 OSPFv3 快速重路由功能示意图



如 图 1-1 所示，通过在Router B上使能快速重路由功能，OSPFv3 将为路由计算或指定备份下一跳，当Router B检测到主用下一跳地址无法到达时，会直接使用备份下一跳地址来指导报文的转发，从

而大大缩短了流量路径切换的时间。在快速切换流量传输路径的同时，OSPFv3 会根据变化后的网络拓扑重新计算路由，在路由收敛完毕后，使用新计算出来的最优路由来指导报文转发。

在为快速重路由功能指定备份下一跳地址时，可以采用以下两种方式：

- 通过 LFA（Loop Free Alternate）算法选取备份下一跳地址。
- 在路由策略中指定备份下一跳，为符合过滤条件的路由指定备份下一跳地址。

1.16.2 配置通过LFA算法选取备份下一跳

1. 配置限制和指导

OSPFv3 快速重路由功能（通过 LFA 算法选取备份下一跳信息）使能后，不能配置 **vlink-peer** 命令。

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) （可选）禁止接口参与 LFA 计算。

ospfv3 fast-reroute lfa-backup exclude

缺省情况下，接口参与 LFA 计算，有资格被选为备份接口。

(4) 退回系统视图。

quit

(5) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(6) 配置 OSPFv3 快速重路由功能（通过 LFA 算法选取备份下一跳信息）。

fast-reroute lfa [**abr-only**]

缺省情况下，OSPFv3 快速重路由功能处于关闭状态。

abr-only 表示只有到 ABR 设备的路由才能作为备份下一跳。

1.16.3 配置通过路由策略指定备份下一跳

1. 功能简介

网络管理员可以通过 **apply ipv6 fast-reroute backup-interface** 命令在路由策略中指定备份下一跳，为符合过滤条件的路由指定备份下一跳，关于 **apply ipv6 fast-reroute backup-interface** 命令以及路由策略的相关配置，请参见“三层技术-IP 路由配置指导”中的“路由策略”。

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) （可选）禁止接口参与 LFA 计算。

ospfv3 fast-reroute lfa-backup exclude

缺省情况下，接口参与 LFA 计算，有资格被选为备份接口。

(4) 退回系统视图。

quit

(5) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(6) 配置 OSPFv3 快速重路由功能（通过路由策略指定备份下一跳）。

fast-reroute route-policy *route-policy-name*

缺省情况下，OSPFv3 快速重路由功能处于关闭状态。

1.16.4 配置OSPFv3 快速重路由支持BFD检测功能（Ctrl方式）

1. 功能简介

OSPFv3 协议的快速重路由特性中，主用链路缺省不使用 BFD 进行链路故障检测。配置本功能后，将使用 BFD 进行检测，可以更快速的发现主用链路的故障，从而加快 OSPFv3 协议的收敛速度。

使用 control 报文双向检测方式时，需要建立 OSPF 邻居的两端设备均支持 BFD 配置。

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) 使能 OSPFv3 协议中主用链路的 BFD 检测功能。

ospfv3 primary-path-detect bfd ctrl [**instance** *instance-id*]

缺省情况下，OSPFv3 协议中主用链路的 BFD 检测功能（Ctrl 方式）处于关闭状态。

1.16.5 配置OSPFv3 快速重路由支持BFD检测功能（Echo方式）

1. 功能简介

OSPFv3 协议的快速重路由特性中，主用链路缺省不使用 BFD 进行链路故障检测。配置本功能后，将使用 BFD 进行检测，可以更快速的发现主用链路的故障，从而加快 OSPFv3 协议的收敛速度。

使用 echo 报文单跳检测方式时，仅需要一端设备支持 BFD 配置。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 BFD Echo 报文源地址。

bfd echo-source-ipv6 *ipv6-address*

缺省情况下，未配置 BFD Echo 报文源地址。

echo 报文的源 IPv6 地址用户可以任意指定。建议配置 echo 报文的源 IPv6 地址不属于该设备任何一个接口所在网段。

本命令的详细情况请参见“可靠性命令参考”中的“BFD”。

(3) 进入接口视图。

interface *interface-type interface-number*

(4) 使能 OSPFv3 协议中主用链路的 BFD 检测功能。

ospfv3 primary-path-detect bfd echo [**instance** *instance-id*]

缺省情况下，OSPFv3 协议中主用链路的 BFD 检测功能（Echo 方式）处于关闭状态。

1.17 应用IPsec安全框架保护OSPFv3报文

1.17.1 功能简介

从安全性角度来考虑，为了避免路由信息外泄或者对设备进行恶意攻击，OSPFv3 提供基于 IPsec 的报文验证功能。IPsec 安全框架的具体情况请参见“安全配置指导”中的“IPsec”。

设备在发送的报文中会携带配置好的 IPsec 安全框架的 SPI（Security Parameter Index，安全参数索引）值，接收报文时通过 SPI 值进行 IPsec 安全框架匹配：只有能够匹配的报文才能接收；否则将不会接收报文，从而不能正常建立邻居和学习路由。

1.17.2 配置限制和指导

OSPFv3 支持在区域、接口和虚连接下配置 IPsec 安全框架。

- 当需要保护区域内的所有报文时，可以在区域下配置 IPsec 安全框架，此时区域内所有路由器都需要配置相同的 IPsec 安全框架。
- 当需要保护区域下某些接口的报文时，可以在接口下配置 IPsec 安全框架，此时直连邻居接口需要配置相同的 IPsec 安全框架。
- 当需要保护虚连接的报文时，可以配置虚连接应用 IPsec 安全框架，此时虚连接上的两个邻居需要配置相同的 IPsec 安全框架。

当接口和接口所在区域均配置了 IPsec 安全框架时，接口下的生效；当虚连接和区域 0 均配置了 IPsec 安全框架时，虚连接的生效。

1.17.3 在OSPFv3 区域上应用IPsec安全框架

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 进入 OSPFv3 区域视图。

area *area-id*

(4) 配置 OSPFv3 区域应用 IPsec 安全框架。

enable ipsec-profile *profile-name*

缺省情况下，OSPFv3 区域没有应用 IPsec 安全框架。

1.17.4 在OSPFv3 接口上应用IPsec安全框架

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置使能了 OSPFv3 的接口上应用 IPsec 安全框架。

ospfv3 ipsec-profile *profile-name*

缺省情况下，OSPFv3 接口没有应用 IPsec 安全框架。

1.17.5 在OSPFv3 虚连接上应用IPsec安全框架

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 进入 OSPFv3 区域视图。

area *area-id*

(4) 配置 OSPFv3 虚连接应用 IPsec 安全框架。

vlink-peer *router-id* [**dead** *seconds* | **hello** *seconds* | **instance** *instance-id* | **retransmit** *seconds* | **trans-delay** *seconds* | **ipsec-profile** *profile-name*] *

缺省情况下，OSPFv3 虚连接没有应用 IPsec 安全框架。

1.18 配置OSPFv3日志和告警功能

1.18.1 配置邻居状态变化的输出开关

1. 功能简介

打开邻居状态变化的输出开关后，OSPFv3 邻居状态变化时会生成日志信息发送到设备的信息中心，通过设置信息中心的参数，最终决定日志信息的输出规则（即是否允许输出以及输出方向）。（有关信息中心参数的配置请参见“网络管理和监控配置指导”中的“信息中心”。）

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 配置邻居状态变化的输出开关。

log-peer-change

缺省情况下，邻居状态变化的输出开关处于打开状态。

1.18.2 配置OSPFv3 的日志信息个数

1. 功能简介

OSPFv3 的日志信息包括路由计算、邻居和 LSA 老化的日志信息。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(3) 配置保存 OSPFv3 的日志信息的最大个数。

event-log { **lsa-flush** | **peer** | **spf** } **size** *count*

缺省情况下，路由计算、邻居和 LSA 老化的日志信息个数均为 10 个。

1.18.3 配置OSPFv3 网管功能

1. 功能简介

配置 OSPFv3 进程绑定 MIB 功能后，可以通过网管软件对指定的 OSPFv3 进程进行管理。

开启 OSPFv3 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”。）

通过调整 OSPFv3 在指定时间间隔内允许输出的告警信息条数，可以避免网络出现大量告警信息时对资源的消耗。

OSPFv3 使用 MIB（Management Information Base，管理信息库）为 NMS（Network Management System，网络管理系统）提供对 OSPFv3 实例的管理，但标准 OSPFv3 MIB 中定义的 MIB 为单实例管理对象，无法对多个 OSPFv3 实例进行管理。因此，参考 RFC 4750 中对 OSPF 多实例的管理方法，为管理 OSPFv3 的 SNMP 实体定义一个上下文名称，以此来区分不同的 OSPFv3 实例，实现对多个 OSPFv3 实例进行管理。由于上下文名称只是 SNMPv3 独有的概念，对于 SNMPv1/v2c，会将团体名映射为上下文名称以对不同协议进行区分。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 OSPFv3 进程绑定 MIB。

ospfv3 mib-binding *process-id*

缺省情况下，MIB 绑定在进程号最小的 OSPFv3 进程上。

(3) 开启 OSPFv3 的告警功能。

snmp-agent trap enable ospfv3 [**grrestarter-status-change** | **grhelper-status-change** | **if-state-change** | **if-cfg-error** | **if-bad-pkt** | **neighbor-state-change** | **nssatranslator-status-change** | **virtif-bad-pkt** | **virtif-cfg-error** |**virtif-state-change** | **virtgrhelper-status-change** | **virtneighbor-state-chang**] *

缺省情况下，OSPFv3 的告警功能处于开启状态。

(4) 进入 OSPFv3 视图。

ospfv3 [*process-id*]

(5) 配置管理 OSPFv3 的 SNMP 实体所使用的上下文名称。

snmp context-name *context-name*

缺省情况下，未配置管理 OSPFv3 的 SNMP 实体所使用的上下文名称。

(6) （可选）配置 OSPFv3 在指定时间间隔内允许输出的告警信息条数。

snmp trap rate-limit interval *trap-interval* **count** *trap-number*

缺省情况下，OSPFv3 模块在 10 秒内允许输出 7 条告警信息。

1.19 OSPFv3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 OSPFv3 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 OSPFv3 的统计信息、重启 OSPFv3 进程或者重新向 OSPFv3 引入外部路由。

表1-1 OSPFv3 显示和维护

操作	命令
显示OSPFv3的ABR聚合信息	**display ospfv3** [*process-id*] [**area** *area-id*] **abr-summary** [*ipv6-address prefix-length*] [**verbose**]
显示OSPFv3邻居信息	**display ospfv3** [*process-id*] [**area** *area-id*] **peer** [[*interface-type interface-number*] [**verbose**] | *peer-router-id* | **statistics**]
显示OSPFv3请求列表的信息	**display ospfv3** [*process-id*] [**area** *area-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*]
显示OSPFv3重传列表的信息	**display ospfv3** [*process-id*] [**area** *area-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*]
显示OSPFv3区域的拓扑信息	**display ospfv3** [*process-id*] [**area** *area-id*] **spf-tree** [**verbose**]
显示OSPFv3的进程信息	**display ospfv3** [*process-id*] [**verbose**]
显示到OSPFv3的区域边界路由器和自治系统边界路由器的路由信息	**display ospfv3** [*process-id*] **abr-asbr**
显示OSPFv3的ASBR聚合信息	**display ospfv3** [*process-id*] **asbr-summary** [*ipv6-address prefix-length*] [**verbose**]
显示OSPFv3路由计算的日志信息	**display ospfv3** [*process-id*] **event-log** { **lsa-flush** | **peer** | **spf** }
显示OSPFv3进程的GR状态信息	**display ospfv3** [*process-id*] **graceful-restart** [**verbose**]
显示OSPFv3的接口信息	**display ospfv3** [*process-id*] **interface** [*interface-type interface-number* | **verbose**]

操作	命令
显示OSPFv3的链路状态数据库信息	**display ospfv3** [*process-id*] **lsdb** [{ **external** | **grace** | **inter-prefix** | **inter-router** | **intra-prefix** | **link** | **network** | **nssa** | **router** | **unknown** [*type*] } [*link-state-id*] [**originate-router** *router-id* | **self-originate**] | **statistics** | **total** | **verbose**]
显示OSPFv3的路由下一跳信息	**display ospfv3** [*process-id*] **nexthop**
显示OSPFv3进程的NSR状态信息	**display ospfv3** [*process-id*] **non-stop-routing**
显示OSPFv3路由表信息	**display ospfv3** [*process-id*] **routing** [*ipv6-address prefix-length*]
显示OSPFv3的报文统计信息	**display ospfv3** [*process-id*] **statistics** [**error**]
显示OSPFv3的虚连接信息	**display ospfv3** [*process-id*] **vlink**
清除OSPFv3的日志信息	**reset ospfv3** [*process-id*] **event-log** [**lsa-flush** | **peer** | **spf**]
重启OSPFv3进程	**reset ospfv3** [*process-id*] **process** [**graceful-restart**]
重新向OSPFv3引入外部路由	**reset ospfv3** [*process-id*] **redistribution**
清除OSPFv3的统计信息	**reset ospfv3** [*process-id*] **statistics**

1.20 OSPFv3配置举例

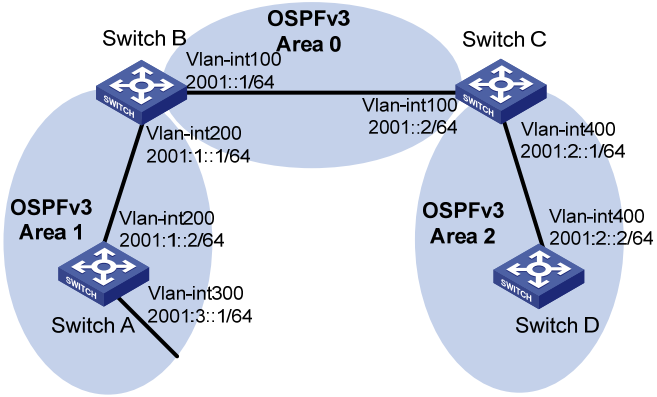
1.20.1 OSPFv3 Stub区域配置举例

1. 组网需求

- 所有的交换机都运行 OSPFv3，整个自治系统划分为 3 个区域。其中 Switch B 和 Switch C 作为 ABR 来转发区域之间的路由。
- 要求将 Area 2 配置为 Stub 区域，减少通告到此区域内的 LSA 数量，但不影响路由的可达性。

2. 组网图

图1-2 OSPFv3 Stub 区域配置组网图



3. 配置步骤

(1) 配置各接口的 IPv6 地址（略）

(2) 配置 OSPFv3 基本功能

配置 Switch A，启动 OSPFv3，并配置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] ospfv3
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 300
[SwitchA-Vlan-interface300] ospfv3 1 area 1
[SwitchA-Vlan-interface300] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ospfv3 1 area 1
[SwitchA-Vlan-interface200] quit
```

配置 Switch B，启动 OSPFv3，并配置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] ospfv3
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ospfv3 1 area 0
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ospfv3 1 area 1
[SwitchB-Vlan-interface200] quit
```

配置 Switch C，启动 OSPFv3，并配置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] ospfv3
[SwitchC-ospfv3-1] router-id 3.3.3.3
[SwitchC-ospfv3-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] ospfv3 1 area 0
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 400
[SwitchC-Vlan-interface400] ospfv3 1 area 2
[SwitchC-Vlan-interface400] quit
```

配置 Switch D，启动 OSPFv3，并配置其 Router ID 为 4.4.4.4。

```
<SwitchD> system-view
[SwitchD] ospfv3
[SwitchD-ospfv3-1] router-id 4.4.4.4
[SwitchD-ospfv3-1] quit
[SwitchD] interface vlan-interface 400
[SwitchD-Vlan-interface400] ospfv3 1 area 2
[SwitchD-Vlan-interface400] quit
```

查看 Switch B 的 OSPFv3 邻居状态。

```
[SwitchB] display ospfv3 peer
```

```
              OSPFv3 Process 1 with Router ID 2.2.2.2

 Area: 0.0.0.0
--------------------------------------------------------------------------
 Router ID       Pri State            Dead-Time InstID Interface
 3.3.3.3         1   Full/BDR         00:00:40  0      Vlan100

 Area: 0.0.0.1
--------------------------------------------------------------------------
 Router ID       Pri State            Dead-Time InstID Interface
 1.1.1.1         1   Full/DR          00:00:40  0      Vlan200
```

查看 Switch C 的 OSPFv3 邻居状态。

```
[SwitchC] display ospfv3 peer

              OSPFv3 Process 1 with Router ID 3.3.3.3

 Area: 0.0.0.0
--------------------------------------------------------------------------
 Router ID       Pri State            Dead-Time InstID Interface
 2.2.2.2         1   Full/DR          00:00:40  0      Vlan100

 Area: 0.0.0.2
--------------------------------------------------------------------------
 Router ID       Pri State            Dead-Time InstID Interface
 4.4.4.4         1   Full/BDR         00:00:40  0      Vlan400
```

查看 Switch D 的 OSPFv3 路由表信息。

```
[SwitchD] display ospfv3 routing

              OSPFv3 Process 1 with Router ID 4.4.4.4
--------------------------------------------------------------------------
 I  - Intra area route,  E1 - Type 1 external route,  N1 - Type 1 NSSA route
 IA - Inter area route,  E2 - Type 2 external route,  N2 - Type 2 NSSA route
 *  - Selected route

 *Destination: 2001::/64
  Type       : IA                                    Cost     : 2
  NextHop    : FE80::F40D:0:93D0:1                   Interface: Vlan400
  AdvRouter  : 3.3.3.3                               Area     : 0.0.0.2
  Preference : 10

 *Destination: 2001:1::/64
  Type       : IA                                    Cost     : 3
  NextHop    : FE80::F40D:0:93D0:1                   Interface: Vlan400
  AdvRouter  : 3.3.3.3                               Area     : 0.0.0.2
  Preference : 10

 *Destination: 2001:2::/64
```

```
 Type       : I                                        Cost     : 1
 Nexthop    : ::                                       Interface: Vlan400
 AdvRouter  : 4.4.4.4                                  Area     : 0.0.0.2
 Preference : 10

*Destination: 2001:3::/64
 Type       : IA                                       Cost     : 4
 NextHop    : FE80::F40D:0:93D0:1                      Interface: Vlan400
 AdvRouter  : 3.3.3.3                                  Area     : 0.0.0.2
 Preference : 10

 Total: 4
 Intra area: 1         Inter area: 3         ASE: 0         NSSA: 0
```

(3) 配置 Stub 区域

配置 Switch D 的 Stub 区域。

```
[SwitchD] ospfv3
[SwitchD-ospfv3-1] area 2
[SwitchD-ospfv3-1-area-0.0.0.2] stub
```

配置 Switch C 的 Stub 区域，设置发送到 Stub 区域的缺省路由的开销为 10。

```
[SwitchC] ospfv3
[SwitchC-ospfv3-1] area 2
[SwitchC-ospfv3-1-area-0.0.0.2] stub
[SwitchC-ospfv3-1-area-0.0.0.2] default-cost 10
```

查看 Switch D 的 OSPFv3 路由表信息，可以看到路由表中多了一条缺省路由，它的开销值为直连路由的开销和所配置的开销值之和。

```
[SwitchD] display ospfv3 routing

               OSPFv3 Process 1 with Router ID 4.4.4.4
------------------------------------------------------------------------
 I  - Intra area route,  E1 - Type 1 external route,  N1 - Type 1 NSSA route
 IA - Inter area route,  E2 - Type 2 external route,  N2 - Type 2 NSSA route
 *  - Selected route

 *Destination: ::/0
  Type       : IA                                       Cost     : 11
  NextHop    : FE80::F40D:0:93D0:1                      Interface: Vlan400
  AdvRouter  : 4.4.4.4                                  Area     : 0.0.0.2
  Preference : 10

 *Destination: 2001::/64
  Type       : IA                                       Cost     : 2
  NextHop    : FE80::F40D:0:93D0:1                      Interface: Vlan400
  AdvRouter  : 3.3.3.3                                  Area     : 0.0.0.2
  Preference : 10

 *Destination: 2001:1::/64
  Type       : IA                                       Cost     : 3
```

```
 NextHop    : FE80::F40D:0:93D0:1                    Interface: Vlan400
 AdvRouter  : 3.3.3.3                                Area     : 0.0.0.2
 Preference : 10

*Destination: 2001:2::/64
 Type       : I                                      Cost     : 1
 Nexthop    : ::                                     Interface: Vlan400
 AdvRouter  : 4.4.4.4                                Area     : 0.0.0.2
 Preference : 10

*Destination: 2001:3::/64
 Type       : IA                                     Cost     : 4
 NextHop    : FE80::F40D:0:93D0:1                    Interface: Vlan400
 AdvRouter  : 3.3.3.3                                Area     : 0.0.0.2
 Preference : 10

 Total: 5
 Intra area: 1         Inter area: 4         ASE: 0         NSSA: 0
```

(4) 配置 Totally Stub 区域

配置 Switch C，设置 Area 2 为 Totally Stub 区域。

```
[SwitchC-ospfv3-1-area-0.0.0.2] stub no-summary
```

查看 Switch D 的 OSPFv3 路由表，可以发现路由表项数目减少了，其他非直连路由都被抑制，只有缺省路由被保留。

```
[SwitchD] display ospfv3 routing

               OSPFv3 Process 1 with Router ID 4.4.4.4
------------------------------------------------------------------------
 I  - Intra area route,  E1 - Type 1 external route,  N1 - Type 1 NSSA route
 IA - Inter area route,  E2 - Type 2 external route,  N2 - Type 2 NSSA route
 *  - Selected route

 *Destination: ::/0
  Type       : IA                                     Cost     : 11
  NextHop    : FE80::F40D:0:93D0:1                    Interface: Vlan400
  AdvRouter  : 4.4.4.4                                Area     : 0.0.0.2
  Preference : 10

 *Destination: 2001:2::/64
  Type       : I                                      Cost     : 1
  Nexthop    : ::                                     Interface: Vlan400
  AdvRouter  : 4.4.4.4                                Area     : 0.0.0.2
  Preference : 10

 Total: 2
 Intra area: 1         Inter area: 1         ASE: 0         NSSA: 0
```

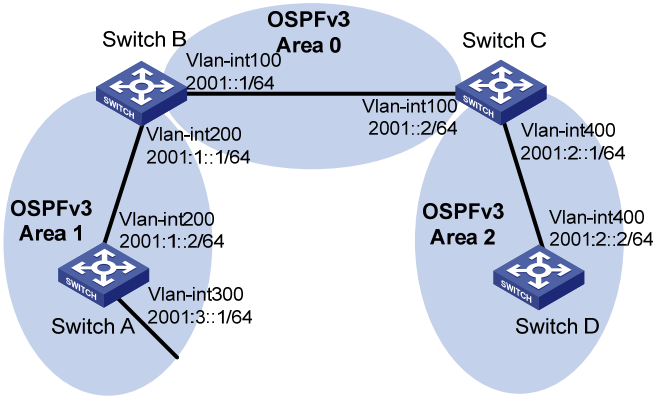
1.20.2 OSPFv3 NSSA区域配置举例

1. 组网需求

- 所有的交换机都运行 OSPFv3，整个自治系统划分为 3 个区域。其中 Switch B 和 Switch C 作为 ABR 来转发区域之间的路由。
- 要求将 Area 1 配置为 NSSA 区域，同时将 Switch A 配置为 ASBR 引入外部路由（静态路由），且路由信息可正确的在 AS 内传播。

2. 组网图

图1-3 OSPFv3 NSSA 区域配置组网图



3. 配置步骤

(1) 配置各接口的 IPv6 地址（略）

(2) 配置OSPFv3 基本功能（同前例“1.20.1 OSPFv3 Stub区域配置举例”）

(3) 配置 Area 1 为 NSSA 区域

配置 Switch A 的 NSSA 区域。

```
[SwitchA] ospfv3
[SwitchA-ospfv3-1] area 1
[SwitchA-ospfv3-1-area-0.0.0.1] nssa
[SwitchA-ospfv3-1-area-0.0.0.1] quit
[SwitchA-ospfv3-1] quit
```

配置 Switch B 的 NSSA 区域。

```
[SwitchB] ospfv3
[SwitchB-ospfv3-1] area 1
[SwitchB-ospfv3-1-area-0.0.0.1] nssa
[SwitchB-ospfv3-1-area-0.0.0.1] quit
[SwitchB-ospfv3-1] quit
```

查看 Switch A 的 OSPFv3 路由表信息。

```
[SwitchA] display ospfv3 1 routing

                OSPFv3 Process 1 with Router ID 1.1.1.1
------------------------------------------------------------------------
 I  - Intra area route,  E1 - Type 1 external route,  N1 - Type 1 NSSA route
```

```
IA - Inter area route,  E2 - Type 2 external route,  N2 - Type 2 NSSA route
*  - Selected route

*Destination: 2001::/64
 Type       : IA                                    Cost     : 2
 NextHop    : FE80::20C:29FF:FE74:59C6              Interface: Vlan200
 AdvRouter  : 2.2.2.2                               Area     : 0.0.0.1
 Preference : 10

*Destination: 2001:1::/64
 Type       : I                                     Cost     : 1
 Nexthop    : ::                                    Interface: Vlan200
 AdvRouter  : 1.1.1.1                               Area     : 0.0.0.1
 Preference : 10

*Destination: 2001:2::/64
 Type       : IA                                    Cost     : 3
 NextHop    : FE80::20C:29FF:FE74:59C6              Interface: Vlan200
 AdvRouter  : 2.2.2.2                               Area     : 0.0.0.1
 Preference : 10

 Total: 3
 Intra area: 1         Inter area: 2         ASE: 0         NSSA: 0
```

(4) 配置 Switch A 引入静态路由

配置 Switch A 上的静态路由，并配置 OSPFv3 引入静态路由。

```
[SwitchA] ipv6 route-static 1234:: 64 null 0
[SwitchA] ospfv3 1
[SwitchA-ospfv3-1] import-route static
[SwitchA-ospfv3-1] quit
```

查看 Switch D 的 OSPFv3 路由表，可以看到 NSSA 区域引入的一条 AS 外部的路由。

```
[SwitchD] display ospfv3 1 routing

              OSPFv3 Process 1 with Router ID 4.4.4.4
------------------------------------------------------------------------
 I  - Intra area route,  E1 - Type 1 external route,  N1 - Type 1 NSSA route
 IA - Inter area route,  E2 - Type 2 external route,  N2 - Type 2 NSSA route
 *  - Selected route

 *Destination: 2001::/64
  Type       : IA                                    Cost     : 2
  NextHop    : FE80::20C:29FF:FEB9:F2EF              Interface: Vlan400
  AdvRouter  : 3.3.3.3                               Area     : 0.0.0.2
  Preference : 10

 *Destination: 2001:1::/64
  Type       : IA                                    Cost     : 3
  NextHop    : FE80::20C:29FF:FEB9:F2EF              Interface: Vlan400
  AdvRouter  : 3.3.3.3                               Area     : 0.0.0.2
```

```
 Preference : 10

*Destination: 2001:2::/64
 Type       : I                                    Cost     : 1
 NextHop    : ::                                   Interface: Vlan400
 AdvRouter  : 4.4.4.4                              Area     : 0.0.0.2
 Preference : 10

*Destination: 1234::/64
 Type       : E2                                   Cost     : 1
 NextHop    : FE80::20C:29FF:FEB9:F2EF             Interface: Vlan400
 AdvRouter  : 2.2.2.2                              Area     : 0.0.0.2
 Preference : 10

Total: 4
Intra area: 1         Inter area: 2         ASE: 1         NSSA: 0
```

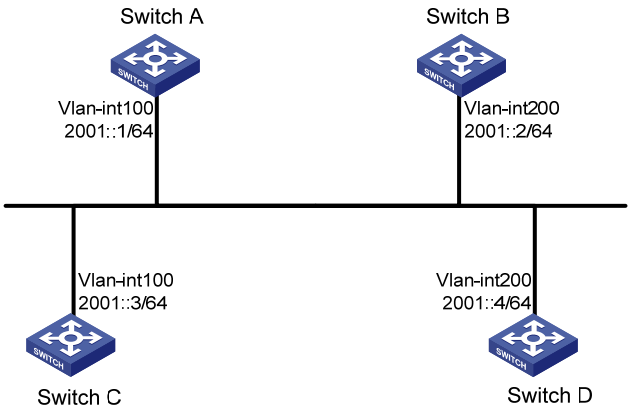
1.20.3 OSPFv3 的DR选择配置举例

1. 组网需求

- Switch A 的优先级配置为 100，它是网络上的最高优先级，所以 Switch A 被选为 DR；
- Switch C 的优先级配置为 2，它是优先级次高的，被选为 BDR；
- Switch B 的优先级配置为 0，这意味着它将无法成为 DR；
- Switch D 没有配置优先级，取缺省值 1。

2. 组网图

图1-4 OSPFv3 的 DR 选择配置组网图



3. 配置步骤

(1) 配置各接口的 IPv6 地址（略）

(2) 配置 OSPFv3 基本功能

配置 Switch A，启动 OSPFv3，并配置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] ospfv3
```

```
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 1 area 0
[SwitchA-Vlan-interface100] quit
```

配置 Switch B，启动 OSPFv3，并配置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] ospfv3
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ospfv3 1 area 0
[SwitchB-Vlan-interface200] quit
```

配置 Switch C，启动 OSPFv3，并配置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] ospfv3
[SwitchC-ospfv3-1] router-id 3.3.3.3
[SwitchC-ospfv3-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] ospfv3 1 area 0
[SwitchC-Vlan-interface100] quit
```

配置 Switch D，启动 OSPFv3，并配置其 Router ID 为 4.4.4.4。

```
<SwitchD> system-view
[SwitchD] ospfv3
[SwitchD-ospfv3-1] router-id 4.4.4.4
[SwitchD-ospfv3-1] quit
[SwitchD] interface vlan-interface 200
[SwitchD-Vlan-interface200] ospfv3 1 area 0
[SwitchD-Vlan-interface200] quit
```

查看 Switch A 的邻居信息，可以看到 DR 优先级（缺省为 1）以及邻居状态，此时优先级相等，Router ID 大者被选为 DR，可以看到 Switch D 为 DR，Switch C 为 BDR。

```
[SwitchA] display ospfv3 peer

              OSPFv3 Process 1 with Router ID 1.1.1.1

 Area: 0.0.0.0
--------------------------------------------------------------------------
 Router ID       Pri State             Dead-Time InstID Interface
 2.2.2.2         1   2-Way/DROther     00:00:36  0      Vlan200
 3.3.3.3         1   Full/BDR          00:00:35  0      Vlan100
 4.4.4.4         1   Full/DR           00:00:33  0      Vlan200
```

查看 Switch D 的邻居信息，可以看到 Switch D 和其他邻居之间的邻居状态都为 Full。

```
[SwitchD] display ospfv3 peer

              OSPFv3 Process 1 with Router ID 4.4.4.4

 Area: 0.0.0.0
```

```
------------------------------------------------------------------------------
 Router ID       Pri State            Dead-Time InstID Interface
 1.1.1.1         1   Full/DROther     00:00:30  0      Vlan100
 2.2.2.2         1   Full/DROther     00:00:37  0      Vlan200
 3.3.3.3         1   Full/BDR         00:00:31  0      Vlan100
```

(3) 配置接口的 DR 优先级

配置 Switch A 的接口 Vlan-interface100 的 DR 优先级为 100。

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 dr-priority 100
[SwitchA-Vlan-interface100] quit
```

配置 Switch B 的接口 Vlan-interface200 的 DR 优先级为 0。

```
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ospfv3 dr-priority 0
[SwitchB-Vlan-interface200] quit
```

配置 Switch C 的接口 Vlan-interface100 的 DR 优先级为 2。

```
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] ospfv3 dr-priority 2
[SwitchC-Vlan-interface100] quit
```

显示 Switch A 的邻居信息，可以看到 DR 优先级已经更新，但 DR/BDR 并未改变。

```
[SwitchA] display ospfv3 peer

              OSPFv3 Process 1 with Router ID 1.1.1.1

 Area: 0.0.0.0
------------------------------------------------------------------------------
 Router ID       Pri State            Dead-Time InstID Interface
 2.2.2.2         0   2-Way/DROther    00:00:36  0      Vlan200
 3.3.3.3         2   Full/BDR         00:00:35  0      Vlan200
 4.4.4.4         1   Full/DR          00:00:33  0      Vlan200
```

显示 Switch D 的邻居信息，可以看到 Switch D 仍然为 DR。

```
[SwitchD] display ospfv3 peer

              OSPFv3 Process 1 with Router ID 4.4.4.4

 Area: 0.0.0.0
------------------------------------------------------------------------------
 Router ID       Pri State            Dead-Time InstID Interface
 1.1.1.1         100 Full/DROther     00:00:30  0      Vlan100
 2.2.2.2         0   Full/DROther     00:00:37  0      Vlan200
 3.3.3.3         2   Full/BDR         00:00:31  0      Vlan100
```

(4) 重新进行 DR/BDR 选择

将所有接口进行一次 **shutdown** 和 **undo shutdown**，使 OSPFv3 进行 DR/BDR 的重新选举。

查看 Switch A 的邻居信息，可以看到 Switch C 为 BDR。

```
[SwitchA] display ospfv3 peer
```

```
                OSPFv3 Process 1 with Router ID 1.1.1.1

 Area: 0.0.0.0
--------------------------------------------------------------------------
 Router ID       Pri State            Dead-Time InstID Interface
 2.2.2.2         0   Full/DROther     00:00:36  0      Vlan200
 3.3.3.3         2   Full/BDR         00:00:35  0      Vlan100
 4.4.4.4         1   Full/DROther     00:00:33  0      Vlan200
```

查看 Switch D 的邻居信息，可以看到 Switch A 为 DR。

```
[SwitchD] display ospfv3 peer

                OSPFv3 Process 1 with Router ID 4.4.4.4

 Area: 0.0.0.0
--------------------------------------------------------------------------
 Router ID       Pri State            Dead-Time InstID Interface
 1.1.1.1         100 Full/DR          00:00:30  0      Vlan100
 2.2.2.2         0   2-Way/DROther    00:00:37  0      Vlan200
 3.3.3.3         2   Full/BDR         00:00:31  0      Vlan100
```

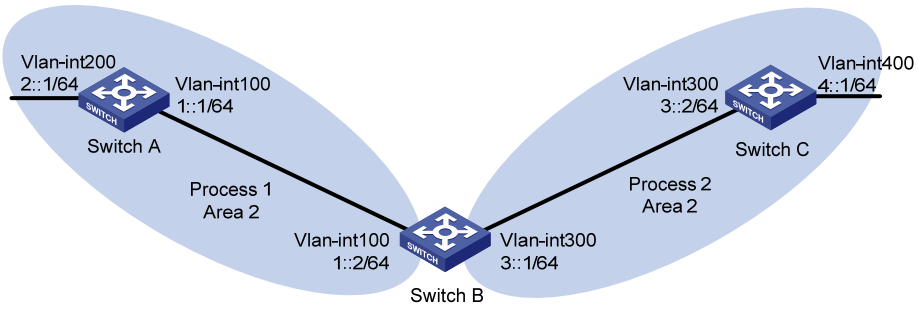
1.20.4 OSPFv3 引入外部路由配置举例

1. 组网需求

- Switch A、Switch B 和 Switch C 位于 Area 2 内；
- Switch B 上运行两个 OSPFv3 进程：OSPFv3 1 和 OSPFv3 2。Switch B 通过 OSPFv3 1 和 Switch A 交换路由信息，通过 OSPFv3 2 和 Switch C 交换路由信息；
- 在 Switch B 上配置 OSPFv3 进程 2 引入外部路由，引入直连路由和 OSPFv3 进程 1 的路由，并将引入的外部路由的缺省度量值设置为 3，使得 Switch C 能够学习到达 1::0/64 和 2::0/64 的路由，但 Switch A 不能学习到达 3::0/64 和 4::0/64 的路由。

2. 组网图

图1-5 OSPFv3 引入外部路由配置组网图



3. 配置步骤

(1) 配置各接口的 IPv6 地址（略）

(2) 配置 OSPFv3

在 Switch A 上启动 OSPFv3 进程 1。

```
<SwitchA> system-view
[SwitchA] ospfv3 1
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 1 area 2
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ospfv3 1 area 2
[SwitchA-Vlan-interface200] quit
```

在 Switch B 上启动两个 OSPFv3 进程，进程号分别为 1 和 2。

```
<SwitchB> system-view
[SwitchB] ospfv3 1
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ospfv3 1 area 2
[SwitchB-Vlan-interface100] quit
[SwitchB] ospfv3 2
[SwitchB-ospfv3-2] router-id 3.3.3.3
[SwitchB-ospfv3-2] quit
[SwitchB] interface vlan-interface 300
[SwitchB-Vlan-interface300] ospfv3 2 area 2
[SwitchB-Vlan-interface300] quit
```

在 Switch C 上启动 OSPFv3 进程 2。

```
<SwitchC> system-view
[SwitchC] ospfv3 2
[SwitchC-ospfv3-2] router-id 4.4.4.4
[SwitchC-ospfv3-2] quit
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] ospfv3 2 area 2
[SwitchC-Vlan-interface300] quit
[SwitchC] interface vlan-interface 400
[SwitchC-Vlan-interface400] ospfv3 2 area 2
[SwitchC-Vlan-interface400] quit
```

查看 Switch C 的路由表信息。

```
[SwitchC] display ipv6 routing-table

Destinations : 7 Routes : 7

Destination: ::1/128                                    Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 3::/64                                     Protocol  : Direct
NextHop    : ::                                         Preference: 0
```

```
Interface  : Vlan300                                  Cost      : 0

Destination: 3::2/128                                 Protocol  : Direct
NextHop    : ::1                                      Preference: 0
Interface  : InLoop0                                  Cost      : 0

Destination: 4::/64                                   Protocol  : Direct
NextHop    : ::                                       Preference: 0
Interface  : Vlan400                                  Cost      : 0

Destination: 4::1/128                                 Protocol  : Direct
NextHop    : ::1                                      Preference: 0
Interface  : InLoop0                                  Cost      : 0

Destination: FE80::/10                                Protocol  : Direct
NextHop    : ::                                       Preference: 0
Interface  : NULL0                                    Cost      : 0

Destination: FF00::/8                                 Protocol  : Direct
NextHop    : ::                                       Preference: 0
Interface  : NULL0
```

(3) 配置 OSPFv3 引入外部路由

在 Switch B 上配置 OSPFv3 引入外部路由,，引入直连路由和 OSPFv3 进程 1 的路由。

```
[SwitchB] ospfv3 2
[SwitchB-ospfv3-2] default cost 3
[SwitchB-ospfv3-2] import-route ospfv3 1
[SwitchB-ospfv3-2] import-route direct
[SwitchB-ospfv3-2] quit
```

查看路由引入后 Switch C 的路由表信息。

```
[SwitchC] display ipv6 routing-table

Destinations : 9 Routes : 9

Destination: ::1/128                                  Protocol  : Direct
NextHop    : ::1                                      Preference: 0
Interface  : InLoop0                                  Cost      : 0

Destination: 1::/64                                   Protocol  : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03                  Preference: 150
Interface  : Vlan300                                  Cost      : 3

Destination: 2::/64                                   Protocol  : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03                  Preference: 150
Interface  : Vlan300                                  Cost      : 3

Destination: 3::/64                                   Protocol  : Direct
NextHop    : ::                                       Preference: 0
Interface  : Vlan300                                  Cost      : 0
```

```
Destination: 3::2/128                                   Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 4::/64                                     Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : Vlan400                                    Cost      : 0

Destination: 4::1/128                                   Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: FE80::/10                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0

Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0
```

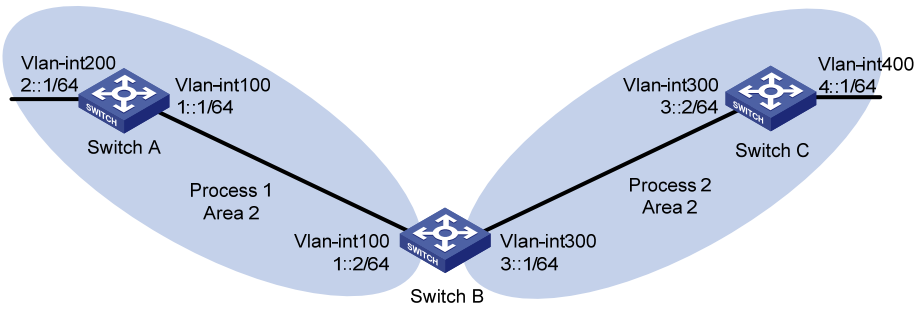
1.20.5 OSPFv3 发布ASBR聚合路由配置举例

1. 组网需求

- Switch A、Switch B 和 Switch C 位于 Area 2 内；
- Switch B 上运行两个 OSPFv3 进程：1 和 2。Switch B 通过进程 1 和 Switch A 交换路由信息，通过进程 2 和 Switch C 交换路由信息；
- 在 Switch A 的接口 Vlan-interface200 上配置地址 2:1:1::1/64、2:1:2::1/64、2:1:3::1/64，并在 Switch B 上配置 OSPFv3 进程 2 引入直连路由和 OSPFv3 进程 1 的路由，使得 Switch C 能够学习到达 2::/64、2:1:1::/64、2:1:2::/64、2:1:3::/64 的路由；
- 为了减小 Switch C 的路由表规模，在 Switch B 上配置 ASBR 聚合路由，只发布聚合后的路由 2::/16。

2. 组网图

图1-6 OSPFv3 发布 ASBR 聚合路由配置组网图



3. 配置步骤

(1) 配置各接口的 IPv6 地址（略）

(2) 配置 OSPFv3

在 Switch A 上启动 OSPFv3 进程 1。

```
<SwitchA> system-view
[SwitchA] ospfv3 1
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 1 area 2
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ipv6 address 2:1:1::1 64
[SwitchA-Vlan-interface200] ipv6 address 2:1:2::1 64
[SwitchA-Vlan-interface200] ipv6 address 2:1:3::1 64
[SwitchA-Vlan-interface200] ospfv3 1 area 2
[SwitchA-Vlan-interface200] quit
```

在 Switch B 上启动两个 OSPFv3 进程，进程号分别为 1 和 2。

```
<SwitchB> system-view
[SwitchB] ospfv3 1
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ospfv3 1 area 2
[SwitchB-Vlan-interface100] quit
[SwitchB] ospfv3 2
[SwitchB-ospfv3-2] router-id 3.3.3.3
[SwitchB-ospfv3-2] quit
[SwitchB] interface vlan-interface 300
[SwitchB-Vlan-interface300] ospfv3 2 area 2
[SwitchB-Vlan-interface300] quit
```

在 Switch C 上启动 OSPFv3 进程 2。

```
<SwitchC> system-view
[SwitchC] ospfv3 2
[SwitchC-ospfv3-2] router-id 4.4.4.4
[SwitchC-ospfv3-2] quit
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] ospfv3 2 area 2
[SwitchC-Vlan-interface300] quit
[SwitchC] interface vlan-interface 400
[SwitchC-Vlan-interface400] ospfv3 2 area 2
[SwitchC-Vlan-interface400] quit
```

(3) 配置 OSPFv3 引入外部路由

在 Switch B 上配置 OSPFv3 进程 2 引入直连路由和 OSPFv3 进程 1 的路由。

```
[SwitchB] ospfv3 2
[SwitchB-ospfv3-2] import-route ospfv3 1
```

```
[SwitchB-ospfv3-2] import-route direct
[SwitchB-ospfv3-2] quit
```

查看路由引入后 Switch C 的路由表信息。

```
[SwitchC] display ipv6 routing-table

Destinations : 12 Routes : 12

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: 1::/64                                 Protocol  : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03                Preference: 150
Interface  : Vlan300                                Cost      : 1

Destination: 2::/64                                 Protocol  : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03                Preference: 150
Interface  : Vlan300                                Cost      : 1

Destination: 2:1:1::/64                             Protocol  : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03                Preference: 150
Interface  : Vlan300                                Cost      : 1

Destination: 2:1:2::/64                             Protocol  : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03                Preference: 150
Interface  : Vlan300                                Cost      : 1

Destination: 2:1:3::/64                             Protocol  : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03                Preference: 150
Interface  : Vlan300                                Cost      : 1

Destination: 3::/64                                 Protocol  : Direct
NextHop    : 3::2                                   Preference: 0
Interface  : Vlan300                                Cost      : 0

Destination: 3::2/128                               Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: 4::/64                                 Protocol  : Direct
NextHop    : 4::1                                   Preference: 0
Interface  : Vlan400                                Cost      : 0

Destination: 4::1/128                               Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: FE80::/10                              Protocol  : Direct
```

```
NextHop    : ::                                    Preference: 0
Interface  : NULL0                                 Cost      : 0

Destination: FF00::/8                              Protocol  : Direct
NextHop    : ::                                    Preference: 0
Interface  : NULL0
```

(4) 配置 OSPFv3 发布 ASBR 聚合路由

在 Switch B 上配置 OSPFv3 进程 2 发布 ASBR 聚合路由 2::/16。

```
[SwitchB] ospfv3 2
[SwitchB-ospfv3-2] asbr-summary 2:: 16
[SwitchB-ospfv3-2] quit
```

查看路由聚合后 Switch C 的路由表信息。

```
[SwitchC] display ipv6 routing-table

Destinations : 9 Routes : 9

Destination: ::1/128                               Protocol  : Direct
NextHop    : ::1                                   Preference: 0
Interface  : InLoop0                               Cost      : 0

Destination: 1::/64                                Protocol  : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03               Preference: 150
Interface  : Vlan300                               Cost      : 1

Destination: 2::/16                                Protocol  : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03               Preference: 150
Interface  : Vlan300                               Cost      : 1

Destination: 3::/64                                Protocol  : Direct
NextHop    : 3::2                                  Preference: 0
Interface  : Vlan300                               Cost      : 0

Destination: 3::2/128                              Protocol  : Direct
NextHop    : ::1                                   Preference: 0
Interface  : InLoop0                               Cost      : 0

Destination: 4::/64                                Protocol  : Direct
NextHop    : 4::1                                  Preference: 0
Interface  : Vlan400                               Cost      : 0

Destination: 4::1/128                              Protocol  : Direct
NextHop    : ::1                                   Preference: 0
Interface  : InLoop0                               Cost      : 0

Destination: FE80::/10                             Protocol  : Direct
NextHop    : ::                                    Preference: 0
Interface  : NULL0                                 Cost      : 0
```

```
Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0
```

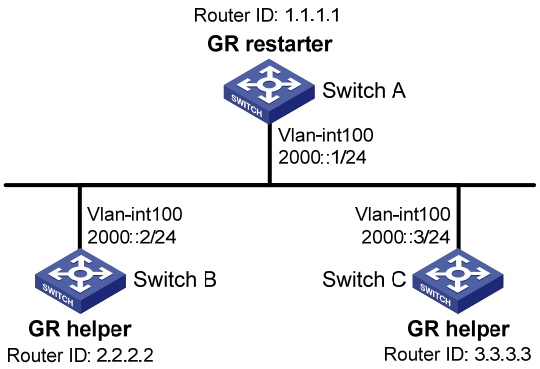
1.20.6 OSPFv3 GR配置举例

1. 组网需求

- Switch A、Switch B 和 Switch C 既属于同一自治系统，也属于同一 OSPFv3 区域，通过 OSPFv3 协议实现网络互连，并提供 GR 机制。
- Switch A 作为 GR Restarter，Switch B 和 Switch C 作为 GR Helper 并且通过 GR 机制与 Switch A 保持同步。

2. 组网图

图1-7 OSPFv3 GR 配置组网图



3. 配置步骤

(1) 配置各接口的 IPv6 地址（略）

(2) 配置 OSPFv3 基本功能

配置 Switch A，启动 OSPFv3，并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] ospfv3 1
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] graceful-restart enable
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 1 area 1
[SwitchA-Vlan-interface100] quit
```

配置 Switch B，启动 OSPFv3，并设置其 Router ID 为 2.2.2.2。缺省情况下，Switch B 的 GR helper 能力处于开启状态。

```
<SwitchB> system-view
[SwitchB] ospfv3 1
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ospfv3 1 area 1
```

```
[SwitchB-Vlan-interface100] quit
```

配置 Switch C，启动 OSPFv3，并设置其 Router ID 为 3.3.3.3。缺省情况下，Switch C 的 GR helper 能力处于开启状态。

```
<SwitchC> system-view
[SwitchC] ospfv3 1
[SwitchC-ospfv3-1] router-id 3.3.3.3
[SwitchC-ospfv3-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] ospfv3 1 area 1
[SwitchC-Vlan-interface100] quit
```

4. 验证配置

运行稳定后，在 Switch A 上主备倒换进入 OSPFv3 协议的 GR 进程。

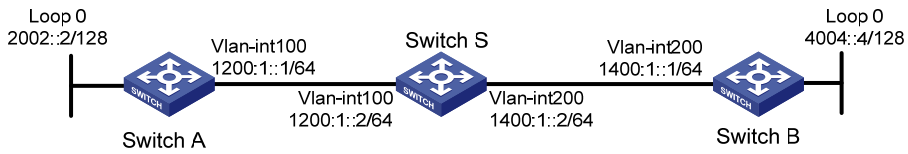
1.20.7 OSPFv3 NSR配置举例

1. 组网需求

- Switch A、Switch B 和 Switch S 既属于同一自治系统，也属于同一 OSPFv3 区域，通过 OSPFv3 协议实现网络互连。Switch S 为分布式设备，提供 NSR 机制；
- 当 Switch S 进行主备倒换时，Switch A 和 Switch B 与 Switch S 的邻居没有中断，Switch A 到 Switch B 的流量没有中断。

2. 组网图

图1-8 OSPFv3 NSR 配置组网图



3. 配置步骤

(1) 配置各接口的 IPv6 地址（略）

(2) 配置 OSPFv3 基本功能

配置 Switch A，启动 OSPFv3，并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] ospfv3 1
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 1 area 1
[SwitchA-Vlan-interface100] quit
```

配置 Switch B，启动 OSPFv3，并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] ospfv3 1
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
```

```
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ospfv3 1 area 1
[SwitchB-Vlan-interface200] quit
```

配置 Switch S，启动 OSPFv3，并设置其 Router ID 为 3.3.3.3。使能 NSR 能力。

```
<SwitchS> system-view
[SwitchS] ospfv3 1
[SwitchS-ospfv3-1] router-id 3.3.3.3
[SwitchS-ospfv3-1] non-stop-routing
[SwitchS-ospfv3-1] quit
[SwitchS] interface vlan-interface 100
[SwitchS-Vlan-interface100] ospfv3 1 area 1
[SwitchS-Vlan-interface100] quit
[SwitchS] interface vlan-interface 200
[SwitchS-Vlan-interface200] ospfv3 1 area 1
[SwitchS-Vlan-interface200] quit
```

4. 验证配置

运行稳定后，在 Switch S 上主备倒换进入 OSPFv3 协议的 NSR 阶段，保证倒换期间流量正常转发，倒换后平滑升级。

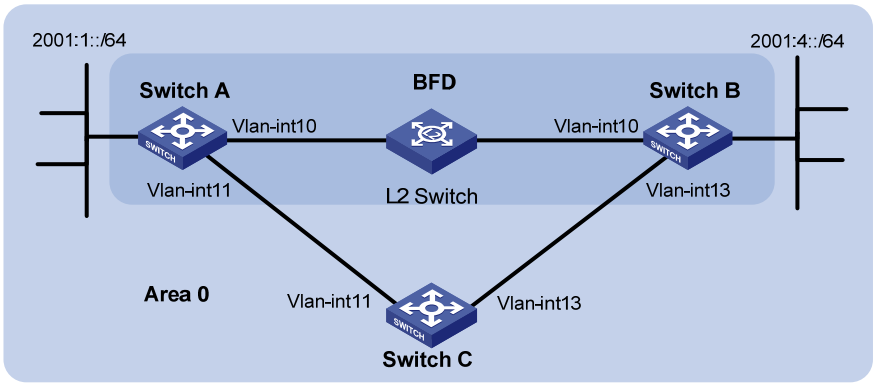
1.20.8 OSPFv3 与BFD联动配置举例

1. 组网需求

- Switch A、Switch B 和 Switch C 上运行 OSPFv3，网络层相互可达。
- 当 Switch A 和 Switch B 通过 L2 Switch 通信的链路出现故障时 BFD 能够快速感知通告 OSPFv3 协议，并且切换到 Switch C 进行通信。

2. 组网图

图1-9 OSPFv3 与 BFD 联动配置组网图



设备	接口	IPv6地址	设备	接口	IPv6地址
Switch A	Vlan-int10	2001::1/64	Switch B	Vlan-int10	2001::2/64
	Vlan-int11	2001:2::1/64		Vlan-int13	2001:3::2/64
Switch C	Vlan-int11	2001:2::2/64			
	Vlan-int13	2001:3::1/64			

3. 配置步骤

(1) 配置各接口的 IPv6 地址（略）

(2) 配置 OSPFv3 基本功能

配置 Switch A，启动 OSPFv3，并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] ospfv3
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ospfv3 1 area 0
[SwitchA-Vlan-interface10] quit
[SwitchA] interface vlan-interface 11
[SwitchA-Vlan-interface11] ospfv3 1 area 0
[SwitchA-Vlan-interface11] quit
```

配置 Switch B，启动 OSPFv3，并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] ospfv3
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] ospfv3 1 area 0
[SwitchB-Vlan-interface10] quit
[SwitchB] interface vlan-interface 13
[SwitchB-Vlan-interface13] ospfv3 1 area 0
[SwitchB-Vlan-interface13] quit
```

配置 Switch C，启动 OSPFv3，并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] ospfv3
[SwitchC-ospfv3-1] router-id 3.3.3.3
[SwitchC-ospfv3-1] quit
[SwitchC] interface vlan-interface 11
[SwitchC-Vlan-interface11] ospfv3 1 area 0
[SwitchC-Vlan-interface11] quit
[SwitchC] interface vlan-interface 13
[SwitchC-Vlan-interface13] ospfv3 1 area 0
[SwitchC-Vlan-interface13] quit
```

(3) 配置 BFD 功能

在 Switch A 上使能 BFD 检测功能，并配置 BFD 参数。

```
[SwitchA] bfd session init-mode active
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ospfv3 bfd enable
[SwitchA-Vlan-interface10] bfd min-transmit-interval 500
[SwitchA-Vlan-interface10] bfd min-receive-interval 500
[SwitchA-Vlan-interface10] bfd detect-multiplier 7
[SwitchA-Vlan-interface10] return
```

在 Switch B 上使能 BFD 检测功能，并配置 BFD 参数。

```
[SwitchB] bfd session init-mode active
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] ospfv3 bfd enable
[SwitchB-Vlan-interface10] bfd min-transmit-interval 500
[SwitchB-Vlan-interface10] bfd min-receive-interval 500
[SwitchB-Vlan-interface10] bfd detect-multiplier 6
```

4. 验证配置

下面以 Switch A 为例，Switch B 和 Switch A 类似，不再赘述。

显示 Switch A 的 BFD 信息。

```
<SwitchA> display bfd session

 Total Session Num: 1            Init Mode: Active

 IPv6 Session Working Under Ctrl Mode:

     Local Discr: 1441               Remote Discr: 1450
      Source IP: FE80::20F:FF:FE00:1202（Switch A 接口 Vlan-interface10 的链路本地地址）
 Destination IP: FE80::20F:FF:FE00:1200（Switch B 接口 Vlan-interface10 的链路本地地址）
   Session State: Up                     Interface: Vlan10
      Hold Time: 2319ms
```

在 Switch A 上查看 2001:4::0/64 的路由信息，可以看出 Switch A 和 Switch B 是通过 L2 Switch 进行通信的。

```
<SwitchA> display ipv6 routing-table 2001:4::0 64

Summary Count : 1

Destination: 2001:4::/64                                Protocol  : O_INTRA
NextHop    : FE80::20F:FF:FE00:1200                     Preference: 10
Interface  : Vlan10                                     Cost      : 1
```

当 Switch A 和 Switch B 通过 L2 Switch 通信的链路出现故障时：

在 Switch A 上查看 2001:4::0/64 的路由信息，可以看出 Switch A 和 Switch B 已经切换到 Switch C 进行通信。

```
<SwitchA> display ipv6 routing-table 2001:4::0 64

Summary Count : 1

Destination: 2001:4::/64                                Protocol  : O_INTRA
NextHop    : FE80::BAAF:67FF:FE27:DCD0                  Preference: 10
Interface  : Vlan11                                     Cost      : 2
```

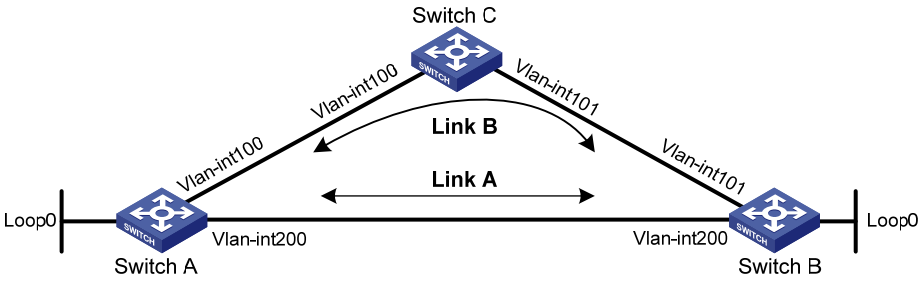
1.20.9 OSPFv3 快速重路由配置举例

1. 组网需求

如 图 1-10 所示，Switch A、Switch B和Switch C属于同一OSPF区域，通过OSPFv3 协议实现网络互连。要求当Switch A和Switch B之间的链路出现故障时，业务可以快速切换到链路B上。

2. 组网图

图1-10 OSPFv3 快速重路由配置组网图



设备	接口	IP地址	设备	接口	IP地址
Switch A	Vlan-int100	1::1/64	Switch B	Vlan-int101	3::1/64
	Vlan-int200	2::1/64		Vlan-int200	2::2/64
	Loop0	10::1/128		Loop0	20::1/128
Switch C	Vlan-int100	1::2/64			
	Vlan-int101	3::2/64			

3. 配置步骤

(1) 配置各交换机接口的 IP 地址和 OSPFv3 协议

请按照上面组网图配置各接口的 IP 地址和子网掩码，具体配置过程略。

配置各交换机之间采用 OSPFv3 协议进行互连，确保 Switch A、Switch B 和 Switch C 之间能够在网络层互通，并且各交换机之间能够借助 OSPFv3 协议实现动态路由更新。

具体配置过程略。

(2) 配置 OSPFv3 快速重路由

OSPFv3 支持快速重路由的配置方法有两种，一种是通过 LFA 算法选取备份下一跳，另一种是在路由策略中指定备份下一跳，两种方法任选一种。

方法一：使能 Switch A 和 Switch B 的 OSPFv3 快速重路由功能（通过 LFA 算法选取备份下一跳信息）

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ospfv3 1
[SwitchA-ospfv3-1] fast-reroute lfa
[SwitchA-ospfv3-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ospfv3 1
[SwitchB-ospfv3-1] fast-reroute lfa
[SwitchB-ospfv3-1] quit
```

方法二：使能 Switch A 和 Switch B 的 OSPFv3 快速重路由功能（通过路由策略指定备份下一跳）

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ipv6 prefix-list abc index 10 permit 20::1 128
[SwitchA] route-policy frr permit node 10
[SwitchA-route-policy-frr-10] if-match ipv6 address prefix-list abc
[SwitchA-route-policy-frr-10] apply ipv6 fast-reroute backup-interface vlan-interface
100 backup-nexthop 1::2/64
[SwitchA-route-policy-frr-10] quit
[SwitchA] ospfv3 1
[SwitchA-ospfv3-1] fast-reroute route-policy frr
[SwitchA-ospfv3-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ipv6 prefix-list abc index 10 permit 10::1 128
[SwitchB] route-policy frr permit node 10
[SwitchB-route-policy-frr-10] if-match ipv6 address prefix-list abc
[SwitchB-route-policy-frr-10] apply ipv6 fast-reroute backup-interface vlan-interface
101 backup-nexthop 3::2/64
[SwitchB-route-policy-frr-10] quit
[SwitchB] ospfv3 1
[SwitchB-ospfv3-1] fast-reroute route-policy frr
[SwitchB-ospfv3-1] quit
```

4. 验证配置

在 Switch A 上查看 20::1/128 的路由信息，可以看到备份下一跳信息。

```
[SwitchA] display ipv6 routing-table 20::1 128 verbose

Summary count : 1

Destination: 20::1/128
   Protocol: O_INTRA
 Process ID: 1
  SubProtID: 0x1                  Age: 00h03m45s
       Cost: 6              Preference: 10
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Active Adv
  OrigTblID: 0x0              OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x23000005         LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10041       OrigNextHop: FE80::7685:45FF:FEAD:102
      Label: NULL          RealNextHop: FE80::7685:45FF:FEAD:102
    BkLabel: NULL            BkNextHop: FE80::34CD:9FF:FE2F:D02
  Tunnel ID: Invalid         Interface: Vlan-interface200
BkTunnel ID: Invalid       BkInterface: Vlan-interface100
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                PathID: 0x0
```

在 Switch B 上查看 10::1/128 的路由信息，可以看到备份下一跳信息。

```
[SwitchB] display ipv6 routing-table 10::1 128 verbose
```

```
Summary count : 1

Destination: 10::1/128
   Protocol: O_INTRA
 Process ID: 1
  SubProtID: 0x1                  Age: 00h03m10s
       Cost: 1              Preference: 10
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Active Adv
  OrigTblID: 0x0              OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x23000006         LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10041       OrigNextHop: FE80::34CC:E8FF:FE5B:C02
      Label: NULL          RealNextHop: FE80::34CC:E8FF:FE5B:C02
    BkLabel: NULL            BkNextHop: FE80::7685:45FF:FEAD:102
  Tunnel ID: Invalid         Interface: Vlan-interface200
BkTunnel ID: Invalid       BkInterface: Vlan-interface101
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                PathID: 0x0
```

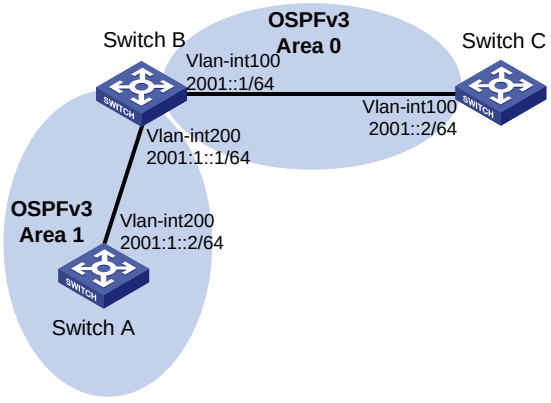
1.20.10 OSPFv3 IPsec安全框架配置举例

1. 组网需求

- 所有的交换机都运行 OSPFv3，整个自治系统划分为 2 个区域。
- 要求配置 IPsec 安全框架对 Switch A、Switch B 和 Switch C 之间的 OSPFv3 报文进行有效性检查和验证。

2. 组网图

图1-11 OSPFv3 IPsec 安全框架配置组网图



3. 配置步骤

(1) 配置各接口的 IPv6 地址（略）

(2) 配置 OSPFv3 基本功能

配置 Switch A，启动 OSPFv3，并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] ospfv3 1
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ospfv3 1 area 1
[SwitchA-Vlan-interface200] quit
```

配置 Switch B，启动 OSPFv3，并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] ospfv3 1
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ospfv3 1 area 0
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ospfv3 1 area 1
[SwitchB-Vlan-interface200] quit
```

配置 Switch C，启动 OSPFv3，并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] ospfv3 1
[SwitchC-ospfv3-1] router-id 3.3.3.3
[SwitchC-ospfv3-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] ospfv3 1 area 0
[SwitchC-Vlan-interface100] quit
```

(3) 配置 OSPFv3 IPsec 安全框架

配置 Switch A。创建名为 trans 的安全提议，报文封装形式采用传输模式，安全协议采用 ESP 协议。创建一条安全框架 profile001，协商方式为 manual，配置 SPI 和密钥。

```
[SwitchA] ipsec transform-set trans
[SwitchA-ipsec-transform-set-trans] encapsulation-mode transport
[SwitchA-ipsec-transform-set-trans] protocol esp
[SwitchA-ipsec-transform-set-trans] esp encryption-algorithm aes-cbc-128
[SwitchA-ipsec-transform-set-trans] esp authentication-algorithm sha1
[SwitchA-ipsec-transform-set-trans] quit
[SwitchA] ipsec profile profile001 manual
[SwitchA-ipsec-profile-manual-profile001] transform-set trans
[SwitchA-ipsec-profile-manual-profile001] sa spi outbound esp 123456
[SwitchA-ipsec-profile-manual-profile001] sa spi inbound esp 123456
[SwitchA-ipsec-profile-manual-profile001] sa string-key outbound esp simple abcdefg
[SwitchA-ipsec-profile-manual-profile001] sa string-key inbound esp simple abcdefg
[SwitchA-ipsec-profile-manual-profile001] quit
```

配置 Switch B。创建名为 trans 的安全提议，报文封装形式采用传输模式，安全协议采用 ESP 协议。创建一条安全框架 profile001，协商方式为 manual，配置 SPI 和密钥。创建一条安全框架 profile002，协商方式为 manual，配置 SPI 和密钥。

```
[SwitchB] ipsec transform-set trans
[SwitchB-ipsec-transform-set-trans] encapsulation-mode transport
[SwitchB-ipsec-transform-set-trans] protocol esp
[SwitchB-ipsec-transform-set-trans] esp encryption-algorithm aes-cbc-128
[SwitchB-ipsec-transform-set-trans] esp authentication-algorithm sha1
[SwitchB-ipsec-transform-set-trans] quit
[SwitchB] ipsec profile profile001 manual
[SwitchB-ipsec-profile-manual-profile001] transform-set trans
[SwitchB-ipsec-profile-manual-profile001] sa spi outbound esp 123456
[SwitchB-ipsec-profile-manual-profile001] sa spi inbound esp 123456
[SwitchB-ipsec-profile-manual-profile001] sa string-key outbound esp simple abcdefg
[SwitchB-ipsec-profile-manual-profile001] sa string-key inbound esp simple abcdefg
[SwitchB-ipsec-profile-manual-profile001] quit
[SwitchB] ipsec profile profile002 manual
[SwitchB-ipsec-profile-manual-profile002] transform-set trans
[SwitchB-ipsec-profile-manual-profile002] sa spi outbound esp 256
[SwitchB-ipsec-profile-manual-profile002] sa spi inbound esp 256
[SwitchB-ipsec-profile-manual-profile002] sa string-key outbound esp simple byebye
[SwitchB-ipsec-profile-manual-profile001] sa string-key inbound esp simple byebye
[SwitchB-ipsec-profile-manual-profile001] quit
```

配置 Switch C。创建名为 trans 的安全提议，报文封装形式采用传输模式，安全协议采用 ESP 协议。创建一条安全框架 profile002，协商方式为 manual，配置 SPI 和密钥。

```
[SwitchC] ipsec transform-set trans
[SwitchC-ipsec-transform-set-trans] encapsulation-mode transport
[SwitchC-ipsec-transform-set-trans] protocol esp
[SwitchC-ipsec-transform-set-trans] esp encryption-algorithm aes-cbc-128
[SwitchC-ipsec-transform-set-trans] esp authentication-algorithm sha1
[SwitchC-ipsec-transform-set-trans] quit
[SwitchC] ipsec profile profile002 manual
[SwitchC-ipsec-profile-manual-profile002] transform-set trans
[SwitchC-ipsec-profile-manual-profile002] sa spi outbound esp 256
[SwitchC-ipsec-profile-manual-profile002] sa spi inbound esp 256
[SwitchC-ipsec-profile-manual-profile002] sa string-key outbound esp simple byebye
[SwitchC-ipsec-profile-manual-profile001] sa string-key inbound esp simple byebye
[SwitchC-ipsec-profile-manual-profile001] quit
```

(4) 配置 OSPFv3 区域上应用 IPsec 安全框架

配置 Switch A。

```
[SwitchA] ospfv3 1
[SwitchA-ospfv3-1] area 1
[SwitchA-ospfv3-1-area-0.0.0.1] enable ipsec-profile profile001
[SwitchA-ospfv3-1-area-0.0.0.1] quit
[SwitchA-ospfv3-1] quit
```

配置 Switch B。

```
[SwitchB] ospfv3 1
[SwitchB-ospfv3-1] area 0
[SwitchB-ospfv3-1-area-0.0.0.0] enable ipsec-profile profile002
[SwitchB-ospfv3-1-area-0.0.0.0] quit
```

```
[SwitchB-ospfv3-1] area 1
[SwitchB-ospfv3-1-area-0.0.0.1] enable ipsec-profile profile001
[SwitchB-ospfv3-1-area-0.0.0.1] quit
[SwitchB-ospfv3-1] quit
```

配置 Switch C。

```
[SwitchC] ospfv3 1
[SwitchC-ospfv3-1] area 0
[SwitchC-ospfv3-1-area-0.0.0.0] enable ipsec-profile profile002
[SwitchC-ospfv3-1-area-0.0.0.0] quit
[SwitchC-ospfv3-1] quit
```

4. 验证配置

以上配置完成后，Switch A、Switch B 和 Switch C 之间的 OSPFv3 报文将被加密传输。

目 录

1 IPv6 策略路由

1.1 IPv6策略路由简介

与单纯依照 IPv6 报文的目的地址查找路由表进行转发不同，策略路由是一种依据用户制定的策略进行路由转发的机制。策略路由可以对于满足一定条件（ACL 规则）的报文，执行指定的操作（设置报文的下一跳）。

1.1.1 IPv6 报文的转发流程

报文到达后，其后续的转发流程如下：

- 首先根据配置的策略路由转发。
- 若找不到匹配的节点，或虽然找到了匹配的节点但指导 IPv6 报文转发失败时，根据路由表中除缺省路由之外的路由来转发报文。
- 若转发失败，则根据缺省路由来转发报文。

1.1.2 IPv6 策略路由类型

根据作用对象的不同，策略路由可分为本地策略路由和转发策略路由：

- 本地策略路由：对设备本身产生的报文（比如本地发出的 ping 报文）起作用，指导其发送。
- 转发策略路由：对接口接收的报文起作用，指导其转发。

1.1.3 IPv6 策略简介

IPv6 策略用来定义报文的匹配规则，以及对报文执行的操作。IPv6 策略由节点组成。

一个 IPv6 策略可以包含一个或者多个节点。节点的构成如下：

- 每个节点由节点编号来标识。节点编号越小节点的优先级越高，优先级高的节点优先被执行。
- 每个节点的具体内容由 **if-match** 子句和 **apply** 子句来指定。**if-match** 子句定义该节点的匹配规则，**apply** 子句定义该节点的动作。
- 每个节点对报文的处理方式由匹配模式决定。匹配模式分为 **permit**（允许）和 **deny**（拒绝）两种。

应用 IPv6 策略后，系统将根据 IPv6 策略中定义的匹配规则和操作，对报文进行处理：系统按照优先级从高到低的顺序依次匹配各节点，如果报文满足这个节点的匹配规则，就执行该节点的动作；如果报文不满足这个节点的匹配规则，就继续匹配下一个节点；如果报文不能满足 IPv6 策略中任何一个节点的匹配规则，则根据路由表来转发报文。

1. if-match子句关系

目前，IPv6 策略路由支持通过 **if-match acl** 子句设置 ACL 匹配规则，在一个节点中只能配置一条 **if-match acl** 子句。

2. apply子句关系

目前，IPv6 策略路由仅提供了一种 **apply** 子句，即 **apply next-hop**，用来设置报文转发的下一跳。

3. 节点的匹配模式与节点的if-match子句、apply子句的关系

一个节点的匹配模式与这个节点的**if-match**子句、**apply**子句的关系如 表 1-1 所示。

表1-1 节点的匹配模式、if-match 子句、apply 子句三者之间的关系

是否满足所有 **if-match** 子句	节点匹配模式	
	permit（允许模式）	**deny**（拒绝模式）
是	• 如果节点配置了 **apply** 子句，则执行此节点 **apply** 子句，不再匹配下一节点，如果节点指导报文转发成功，则不再匹配下一节点 • 如果节点未配置 **apply** 子句，则不会执行任何动作，且不再匹配下一节点，报文将根据路由表来进行转发	不执行此节点**apply**子句，不再匹配下一节点，报文将根据路由表来进行转发
否	不执行此节点**apply**子句，继续匹配下一节点	不执行此节点**apply**子句，继续匹配下一节点

说明

如果一个节点中未配置任何 **if-match** 子句，则认为所有报文都满足该节点的匹配规则，按照“报文满足所有 **if-match** 子句”的情况进行后续处理。

1.1.4 策略路由与Track联动

策略路由通过与 Track 联动，增强了应用的灵活性和对网络环境变化的动态感知能力。

策略路由可以在配置报文的下一跳时与 Track 项关联，根据 Track 项的状态来动态地决定策略的可用性。策略路由配置仅在关联的 Track 项状态为 Positive 或 NotReady 时生效。关于策略路由与 Track 联动的详细介绍和相关配置，请参见“可靠性配置指导”中的“Track”。

1.2 IPv6策略路由配置任务简介

IPv6 策略路由配置任务如下：

(1) 配置IPv6 策略

a. 创建IPv6 策略节点

b. 配置IPv6 策略节点的匹配规则

c. 配置IPv6 策略节点的动作

(2) 应用IPv6 策略

请选择以下至少一项任务进行配置：

- 对本地报文应用IPv6 策略
- 对接口转发的报文应用IPv6 策略

1.3 配置IPv6策略

1.3.1 创建IPv6 策略节点

(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*

1.3.2 配置IPv6 策略节点的匹配规则

(1) 进入系统视图。

system-view

(2) 进入 IPv6 策略节点视图。

ipv6 policy-based-route *policy-name* [**deny** | **permit**] **node** *node-number*

(3) 设置 ACL 匹配规则。

if-match acl { *ipv6-acl-number* | **name** *ipv6-acl-name* }

缺省情况下，未设置 ACL 匹配规则。

IPv6 策略路由不支持匹配二层信息的 ACL 匹配规则。

设置 ACL 匹配规则时，对于 ACL 规则的 permit/deny 动作以及 time-range 指定的规则生效时间段等的处理机制不再生效。

1.3.3 配置IPv6 策略节点的动作

1. 功能简介

用户通过配置 **apply** 子句指导 IPv6 策略节点的动作。目前，IPv6 策略路由仅提供了一种 **apply** 子句，即 **apply next-hop**，用来设置报文转发的下一跳。

2. 配置限制和指导

IPv6 策略路由通过查询 FIB 表中是否存在下一跳地址对应的条目，判断设置的报文转发下一跳地址是否可用。IPv6 策略路由周期性检查 FIB 表，设备到下一跳的路径发生变化时，IPv6 策略路由无法及时感知，可能会导致通信发生短暂中断。

3. 配置指导报文转发类动作

(1) 进入系统视图。

system-view

(2) 进入 IPv6 策略节点视图。

ipv6 policy-based-route *policy-name* [**deny** | **permit**] **node** *node-number*

(3) 设置报文转发的下一跳。

apply next-hop { *ipv6-address* [**direct**] [**track** *track-entry-number*] } &<1-2>

缺省情况下，未设置报文转发的下一跳。

用户通过一次或多次配置本命令可以同时配置多个下一跳，每个节点最多可以配置 2 个下一跳，这些下一跳起到主备的作用。

1.4 应用IPv6策略

1.4.1 对本地报文应用IPv6 策略

1. 功能简介

通过本配置，可以将已经配置的 IPv6 策略应用到本地，指导设备本身产生 IPv6 报文的发送。应用 IPv6 策略时，该 IPv6 策略必须已经存在，否则配置将失败。

2. 配置限制和指导

对本地报文只能应用一个 IPv6 策略。应用新的 IPv6 策略前必须删除本地原来已经应用的 IPv6 策略。

若无特殊需求，建议用户不要对本地报文应用 IPv6 策略。否则，有可能会对本地报文的发送造成不必要的影响（如 ping、telnet 服务的失效）。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 对本地报文应用 IPv6 策略。

ipv6 local policy-based-route *policy-name*

缺省情况下，未对本地报文应用 IPv6 策略。

1.4.2 对接口转发的报文应用IPv6 策略

1. 功能简介

通过本配置，可以将已经配置的 IPv6 策略应用到接口，指导接口接收的所有 IPv6 报文的转发。应用 IPv6 策略时，该 IPv6 策略必须已经存在，否则配置将失败。

2. 配置限制和指导

对接口转发的报文应用 IPv6 策略时，一个接口只能应用一个 IPv6 策略。应用新的 IPv6 策略前必须删除接口上原来已经应用的 IPv6 策略。

一个 IPv6 策略可以同时被多个接口应用。

3. 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) 对接口转发的报文应用 IPv6 策略。

ipv6 policy-based-route *policy-name*

缺省情况下，未对接口转发的报文应用 IPv6 策略。

1.5 IPv6策略路由显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 IPv6 策略路由配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，用户可以执行 **reset** 命令可以清除 IPv6 策略路由的统计信息。

表1-2 IPv6 策略路由显示和维护

操作	命令
显示已经配置的IPv6策略	**display ipv6 policy-based-route** [**policy** *policy-name*]
显示接口下IPv6转发策略路由的配置信息和统计信息	**display ipv6 policy-based-route interface** *interface-type interface-number* [**slot** *slot-number*]
显示IPv6本地策略路由的配置信息和统计信息	**display ipv6 policy-based-route local** [**slot** *slot-number*]
显示已经应用的IPv6策略路由信息	**display ipv6 policy-based-route setup**
清除IPv6策略路由的统计信息	**reset ipv6 policy-based-route statistics** [**policy** *policy-name*]

1.6 IPv6策略路由典型配置举例

1.6.1 基于报文协议类型的IPv6 本地策略路由配置举例

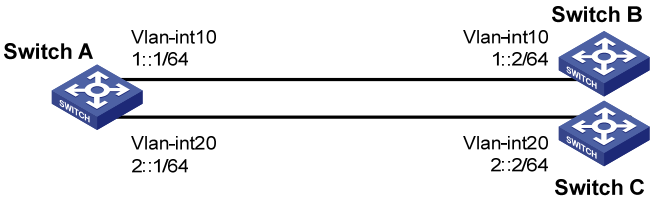
1. 组网需求

Switch A 分别与 Switch B 和 Switch C 直连（保证 Switch B 和 Switch C 之间路由完全不可达）。通过策略路由控制 Switch A 产生的报文：

- 指定所有 TCP 报文的下一跳为 1::2；
- 其它 IPv6 报文仍然按照查找路由表的方式进行转发。

2. 组网图

图1-1 基于报文协议类型的本地策略路由的配置举例组网图



3. 配置步骤

(1) 配置 Switch A

创建 VLAN 10 和 VLAN 20。

```
<SwitchA> system-view
[SwitchA] vlan 10
```

```
[SwitchA-vlan10] quit
[SwitchA] vlan 20
[SwitchA-vlan20] quit
```

配置接口 Vlan-interface10 和 Vlan-interface20 的 IPv6 地址。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ipv6 address 1::1 64
[SwitchA-Vlan-interface10] quit
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ipv6 address 2::1 64
[SwitchA-Vlan-interface20] quit
```

定义访问控制列表 ACL 3001，用来匹配 TCP 报文。

```
[SwitchA] acl ipv6 advanced 3001
[SwitchA-acl-ipv6-adv-3001] rule permit tcp
[SwitchA-acl-ipv6-adv-3001] quit
```

定义 5 号节点，指定所有 TCP 报文的下一跳为 1::2。

```
[SwitchA] ipv6 policy-based-route aaa permit node 5
[SwitchA-pbr6-aaa-5] if-match acl 3001
[SwitchA-pbr6-aaa-5] apply next-hop 1::2
[SwitchA-pbr6-aaa-5] quit
```

在 Switch A 上应用本地策略路由。

```
[SwitchA] ipv6 local policy-based-route aaa
```

(2) 配置 Switch B

创建 VLAN 10

```
<SwitchB> system-view
[SwitchB] vlan 10
[SwitchB-vlan10] quit
```

配置接口 Vlan-interface10 的 IP 地址。

```
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] ipv6 address 1::2 64
```

(3) 配置 Switch C

#创建 VLAN 20

```
<SwitchC> system-view
[SwitchC] vlan 20
[SwitchC-vlan20] quit
```

配置接口 Vlan-interface20 的 IP 地址。

```
[SwitchC] interface vlan-interface 20
[SwitchC-Vlan-interface20] ipv6 address 2::2 64
```

4. 验证配置

从 Switch A 上通过 Telnet 方式登录 Switch B（1::2/64），结果成功。

从 Switch A 上通过 Telnet 方式登录 Switch C（2::2/64），结果失败。

从 Switch A 上 ping Switch C（2::2/64），结果成功。

由于 Telnet 使用的是 TCP 协议，ping 使用的是 ICMP6 协议，所以由以上结果可证明：Switch A 发出的 TCP 报文的下一跳为 1::2，接口 Vlan-interface20 不发送 TCP 报文，但可以发送非 TCP 报文，策略路由设置成功。

1.6.2 基于报文协议类型的IPv6 转发策略路由配置举例

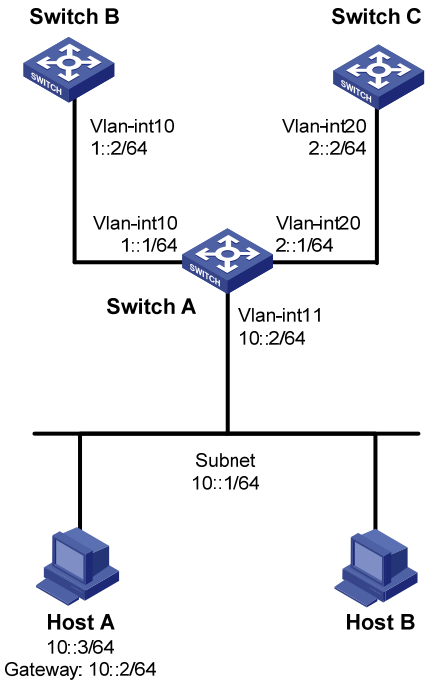
1. 组网需求

Switch A 分别与 Switch B 和 Switch C 直连（保证 Switch B 和 Switch C 之间路由完全不可达）。通过策略路由控制从 Switch A 的接口 Vlan-interface11 接收的报文：

- 指定所有 TCP 报文的下一跳为 1::2；
- 其它 IPv6 报文仍然按照查找路由表的方式进行转发。

2. 组网图

图1-2 基于报文协议类型的 IPv6 转发策略路由配置举例组网图



3. 配置步骤

(1) 配置 Switch A

创建 VLAN 10 和 VLAN 20。

```
<SwitchA> system-view
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] vlan 20
[SwitchA-vlan20] quit
```

配置动态路由协议 RIPng。

```
[SwitchA] ripng 1
[SwitchA-ripng-1] quit
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ipv6 address 1::1 64
[SwitchA-Vlan-interface10] ripng 1 enable
[SwitchA-Vlan-interface10] quit
```

```
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ipv6 address 2::1 64
[SwitchA-Vlan-interface20] ripng 1 enable
[SwitchA-Vlan-interface20] quit
```

定义访问控制列表 ACL 3001，用来匹配 TCP 报文。

```
[SwitchA] acl ipv6 advanced 3001
[SwitchA-acl-ipv6-adv-3001] rule permit tcp
[SwitchA-acl-ipv6-adv-3001] quit
```

定义 5 号节点，指定所有 TCP 报文的下一跳为 1::2。

```
[SwitchA] ipv6 policy-based-route aaa permit node 5
[SwitchA-pbr6-aaa-5] if-match acl 3001
[SwitchA-pbr6-aaa-5] apply next-hop 1::2
[SwitchA-pbr6-aaa-5] quit
```

在接口 Vlan-interface11 上应用转发策略路由，处理此接口接收的报文。

```
[SwitchA] interface vlan-interface 11
[SwitchA-Vlan-interface11] ipv6 address 10::2 64
[SwitchA-Vlan-interface11] undo ipv6 nd ra halt
[SwitchA-Vlan-interface11] ripng 1 enable
[SwitchA-Vlan-interface11] ipv6 policy-based-route aaa
```

(2) 配置 Switch B

创建 VLAN 10

```
<SwitchB> system-view
[SwitchB] vlan 10
[SwitchB-vlan10] quit
```

配置动态路由协议 RIPng。

```
[SwitchB] ripng 1
[SwitchB-ripng-1] quit
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] ipv6 address 1::2 64
[SwitchB-Vlan-interface10] ripng 1 enable
[SwitchB-Vlan-interface10] quit
```

(3) 配置 Switch C

#创建 VLAN 20

```
<SwitchC> system-view
[SwitchC] vlan 20
[SwitchC-vlan20] quit
```

配置动态路由协议 RIPng。

```
[SwitchC] ripng 1
[SwitchC-ripng-1] quit
[SwitchC] interface vlan-interface 20
[SwitchC-Vlan-interface20] ipv6 address 2::2 64
[SwitchC-Vlan-interface20] ripng 1 enable
[SwitchC-Vlan-interface20] quit
```

4. 验证配置

在 Host A 上安装 IPv6 协议栈，并将 IPv6 地址配置为 10::3。

```
C:\>ipv6 install
Installing...
Succeeded.
C:\>ipv6 adu 4/10::3
```

从 Host A 上通过 Telnet 方式登录 Router B，结果成功。

从 Host A 上通过 Telnet 方式登录 Router C，结果失败。

从 Host A 上 ping Router C，结果成功。

由于 Telnet 使用的是 TCP 协议，ping 使用的是 ICMP 协议，所以由以上结果可证明：从 Switch A 的接口 Vlan-interface11 接收的 TCP 报文的下一跳为 1::2，接口 Vlan-interface20 不转发 TCP 报文，但可以转发非 TCP 报文，策略路由设置成功。

目 录

1 路由策略

1.1 路由策略简介

路由策略是为了改变网络流量所经过的途径而修改路由信息的技术，主要通过改变路由属性（包括可达性）来实现。路由策略可以用来控制路由的发布、控制路由的接收、管理引入的路由和设置路由的属性。

1.1.1 路由策略的实现

路由策略的实现步骤如下：

(1) 首先要定义将要实施路由策略的路由信息的特征，即定义一组匹配规则。可以灵活使用过滤器来定义各种匹配规则。

(2) 然后再将匹配规则应用于路由的发布、接收和引入等过程的路由策略中。

1.1.2 过滤器

过滤器可以看作是路由策略过滤路由的工具，单独配置的过滤器没有任何过滤效果，只有在路由协议的相关命令中应用这些过滤器，才能够达到预期的过滤效果。

1. 访问控制列表

访问控制列表可以指定 IP 地址和子网范围，用于匹配路由信息的目的网段地址或下一跳地址。

ACL 的相关内容请参见“ACL 和 QoS 配置指导”中的“ACL”。

2. 地址前缀列表

地址前缀列表的作用类似于 ACL，但比它更为灵活，且更易于用户理解。使用地址前缀列表过滤路由信息时，其匹配对象为路由信息的目的地址。

一个地址前缀列表由前缀列表名标识。每个前缀列表可以包含多个表项，每个表项可以独立指定一个网络前缀形式的匹配范围，并用一个索引号来标识，索引号指明了在地址前缀列表中进行匹配检查的顺序。

每个表项之间是“或”的关系，在匹配的过程中，路由器按升序依次检查由索引号标识的各个表项，只要有某一表项满足条件，就意味着通过该地址前缀列表的过滤（不再对下一个表项进行匹配）。

3. 路由策略

路由策略是一种比较复杂的过滤器，它不仅可以匹配路由信息的某些属性，还可以在条件满足时改变路由信息的属性。路由策略可以使用前面几种过滤器定义自己的匹配规则。

一个路由策略可以由多个节点构成，每个节点是匹配检查的一个单元。在匹配过程中，系统按节点序号升序依次检查各个节点。不同节点间是“或”的关系，如果通过了其中一个节点，就意味着通过该路由策略，不再对其他节点进行匹配（配置了 **continue** 子句的情况除外）。

每个节点对路由信息的处理方式由匹配模式决定。匹配模式分为 **permit** 和 **deny** 两种。

- **permit**：指定节点的匹配模式为允许模式。当路由信息通过该节点的过滤后，将执行该节点的 **apply** 子句，不进入下一个节点的匹配（配置了 **continue** 子句的情况除外）；如果路由信息没有通过该节点过滤，将进入下一个节点继续匹配。
- **deny**：指定节点的匹配模式为拒绝模式（此模式下 **apply** 子句和 **continue** 子句不会被执行）。当路由信息通过该节点的过滤后，将被拒绝通过该节点，不进入下一个节点的匹配；如果路由信息没有通过该节点的过滤，将进入下一个节点继续匹配。

每个节点可以由一组 **if-match**、**apply** 和 **continue** 子句组成。

- **if-match** 子句：定义匹配规则，匹配对象是路由信息的一些属性。同一节点中的不同 **if-match** 子句是“与”的关系，只有满足节点内所有 **if-match** 子句指定的匹配条件，才能通过该节点的匹配。
- **apply** 子句：指定动作，也就是在通过节点的匹配后，对路由信息的一些属性进行设置。
- **continue** 子句：用来配置下一个执行节点。当路由成功匹配当前路由策略节点（必须是 **permit** 节点）时，可以指定路由继续匹配同一路由策略内的下一个节点，这样可以组合路由策略各个节点的 **if-match** 子句和 **apply** 子句，增强路由策略的灵活性。

if-match、**apply** 和 **continue** 子句可以根据应用进行设置，都是可选的。

- 如果只过滤路由，不设置路由的属性，则不需要使用 **apply** 子句。
- 如果某个 **permit** 节点未配置任何 **if-match** 子句，则该节点匹配所有的路由。
- 通常在多个 **deny** 节点后设置一个不含 **if-match** 子句和 **apply** 子句的 **permit** 节点，用于允许其它的路由通过。

1.2 路由策略配置任务简介

路由策略配置任务如下：

(1) （可选）配置过滤器

- 配置IPv4 地址前缀列表
- 配置IPv6 地址前缀列表

(2) 配置路由策略

a. 创建路由策略

b. 配置if-match子句

c. 配置apply子句

d. 配置continue子句

1.3 配置IPv4地址前缀列表

1. 配置限制和指导

如果所有表项都是**deny**模式，则任何路由都不能通过该过滤列表。要允许其它所有IPv4路由通过，需要在多条 **deny** 模式的表项后定义一条 **permit** 0.0.0.0 0 **less-equal** 32 表项。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 IPv4 地址前缀列表。

ip prefix-list *prefix-list-name* [**index** *index-number*] { **deny** | **permit** } *ip-address mask-length* [**greater-equal** *min-mask-length*] [**less-equal** *max-mask-length*]

1.4 配置IPv6地址前缀列表

1. 配置限制和指导

如果所有表项都是**deny**模式，则任何路由都不能通过该过滤列表。要允许其它所有IPv6路由通过，需要在多条 **deny** 模式的表项后定义一条 **permit** :: 0 **less-equal** 128 表项。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 IPv6 地址前缀列表。

ipv6 prefix-list *prefix-list-name* [**index** *index-number*] { **deny** | **permit** } *ipv6-address* { **inverse** *inverse-prefix-length* | *prefix-length* [**greater-equal** *min-prefix-length*] [**less-equal** *max-prefix-length*] }

1.5 配置路由策略

1.5.1 创建路由策略

1. 功能简介

路由策略中至少应该有一个节点的匹配模式是**permit**。如果路由策略的所有节点都是**deny**模式，则没有路由信息能通过该路由策略。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建路由策略，并进入该路由策略视图。

route-policy *route-policy-name* { **deny** | **permit** } **node** *node-number*

1.5.2 配置if-match子句

1. 功能简介

在一个节点中，可以没有 **if-match** 子句，也可以有多个 **if-match** 子句。当不指定 **if-match** 子句时，如果该节点的匹配模式为允许模式，则所有路由信息都会通过该节点的过滤；如果该节点的匹配模式为拒绝模式，则所有路由信息都会被拒绝。

2. 配置限制和指导

如果配置了多条相同类型的 **if-match** 子句，设备在显示路由策略时，会将这些 **if-match** 子句合并为一条 **if-match** 子句。如果合并后的 **if-match** 子句超过命令行最大长度，则这些相同类型的 **if-match** 子句会分成多条显示，这些子句之间是“或”的关系，即满足一个匹配条件，就认

为匹配该 **if-match** 语句，例如出现多条 **if-match community** 子句时，各个子句的团体属性之间是“或”的关系，即满足其中一个团体属性，就认为匹配 **if-match community** 子句。

如果一个节点中 **if-match** 子句只指定了 IPv6 ACL，没有指定 IPv4 ACL，所有的 IPv4 路由信息都会匹配这个节点。如果一个节点中 **if-match** 子句只指定 IPv4 ACL，没有指定 IPv6 ACL，所有的 IPv6 路由信息都会匹配这个节点。

如果 **if-match** 子句对应的 ACL 不存在，则默认满足该匹配条件。如果 **if-match** 子句对应的 ACL 中没有匹配的 ACL 规则或者 ACL 规则处于非激活状态，则默认不满足该匹配条件。

如果 **if-match** 子句对应的前缀列表、团体属性列表或扩展团体属性列表不存在，则默认满足该匹配条件。如果 **if-match** 子句对应的前缀列表、团体属性列表或扩展团体属性列表中没有匹配的规则，则默认不满足该匹配条件。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入路由策略视图。

route-policy *route-policy-name* { **deny** | **permit** } **node** *node-number*

(3) 配置通过 ACL 或 IP 地址前缀列表匹配路由。

（IPv4 网络）

if-match ip { **address** | **next-hop** | **route-source** } { **acl** *ipv4-acl-number* | **prefix-list** *prefix-list-name* }

（IPv6 网络）

if-match ipv6 { **address** | **next-hop** | **route-source** } { **acl** *ipv6-acl-number* | **prefix-list** *prefix-list-name* }

缺省情况下，未配置通过 ACL 或 IP 地址前缀列表匹配路由。

路由策略使用非 VPN 的 ACL 进行路由过滤。

(4) 配置基于路由信息的匹配条件。

- 配置路由信息的路由开销匹配条件。

  if-match cost *cost-value*

- 配置路由信息的出接口匹配条件。

  if-match interface { *interface-type interface-number* }&<1-16>

- 配置路由信息类型匹配条件。

  if-match route-type { **external-type1** | **external-type1or2** | **external-type2** | **internal** | **nssa-external-type1** | **nssa-external-type1or2** | **nssa-external-type2** } *

- 配置 IGP 路由信息标记的匹配条件。

  if-match tag *tag-value*

缺省情况下，未配置基于路由信息的匹配条件。

1.5.3 配置apply子句

(1) 进入系统视图。

system-view

(2) 进入路由策略视图。

route-policy *route-policy-name* { **deny** | **permit** } **node** *node-number*

(3) 配置路由开销。

- 配置路由信息的路由开销。

  apply cost [**+** | **-**] *cost-value*

  缺省情况下，未配置路由信息的路由开销。

- 配置路由信息的开销类型。

  apply cost-type { **type-1** | **type-2** }

  缺省情况下，未配置路由信息的开销类型。

(4) 配置路由信息的下一跳地址。

（IPv4 网络）

apply ip-address next-hop *ip-address* [**public**]

（IPv6 网络）

apply ipv6 next-hop *ipv6-address*

缺省情况下，未配置路由信息的下一跳地址。

对于引入的路由，使用本命令设置下一跳地址无效。

(5) 配置路由优先级。

- 配置路由的 IP 优先级。

  apply ip-precedence { *value* | **clear** }

  缺省情况下，未配置路由的 IP 优先级。

- 配置路由协议的优先级。

  apply preference *preference*

  缺省情况下，未配置路由协议的优先级。

- 配置路由收敛优先级。

  apply prefix-priority { **critical** | **high** | **medium** }

  缺省情况下，路由收敛优先级为低（Low）。

(6) 配置 IGP 路由信息的标记。

apply tag *tag-value*

缺省情况下，未配置 IGP 路由信息的标记。

(7) 配置快速重路由备份。

（IPv4 网络）

apply fast-reroute { **backup-interface** *interface-type interface-number* [**backup-nexthop** *ip-address*] | **backup-nexthop** *ip-address* }

（IPv6 网络）

apply ipv6 fast-reroute { **backup-interface** *interface-type interface-number* [**backup-nexthop** *ipv6-address*] | **backup-nexthop** *ipv6-address* }

缺省情况下，未配置快速重路由备份。

1.5.4 配置continue子句

1. 配置限制和指导

当配置 **continue** 子句的多个节点配置相同的 **apply** 子句（没有叠加属性）只是子句的值不相同时，以最后一个节点的 **apply** 子句为准；如果配置的是有叠加属性的 **apply** 子句（命令 **apply as-path** 不指定参数 **replace**/命令 **apply cost** 指定参数**+**或**-**/命令 **apply community** 指定参数 **additive**/命令 **apply extcommunity** 指定参数 **additive**），属性会全部叠加到路由上。

当配置 **continue** 子句的多个节点配置 **apply community** 子句时，使用命令行 **apply comm-list delete** 不能删除前面节点中配置的团体属性。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入路由策略视图。

route-policy *route-policy-name* { **deny** | **permit** } **node** *node-number*

(3) 配置下一个执行节点。

continue [*node-number*]

缺省情况下，未配置下一个执行节点。

下一个执行节点序列号必须大于当前节点序列号。

1.6 路由策略显示和维护

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

在用户视图下执行 **reset** 命令可以清除路由策略的统计信息。

表1-1 路由策略显示和维护

操作	命令
显示IPv4地址前缀列表的统计信息	**display ip prefix-list** [**name** *prefix-list-name*]
显示IPv6地址前缀列表的统计信息	**display ipv6 prefix-list** [**name** *prefix-list-name*]
显示路由策略信息	**display route-policy** [**name** *route-policy-name*]
清除IPv4地址前缀列表的统计信息	**reset ip prefix-list** [*prefix-list-name*]
清除IPv6地址前缀列表的统计信息	**reset ipv6 prefix-list** [*prefix-list-name*]

1.7 路由策略典型配置举例

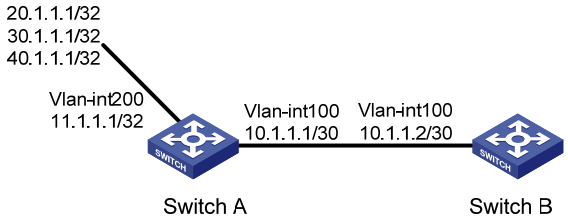
1.7.1 在RIP中引入静态路由时应用路由策略配置举例

1. 组网需求

- Switch A 与 Switch B 通信，都运行 RIP 协议。
- 使能 Switch A 上的 RIP 协议，配置三条静态路由。
- 设置在引入静态路由时应用路由策略，使三条静态路由部分引入、部分被屏蔽掉——20.1.1.1/32 和 40.1.1.1/32 网段的路由是可见的，30.1.1.1/32 网段的路由则被屏蔽。
- 通过在 Switch B 上查看 RIP 路由表，验证路由策略是否生效。

2. 组网图

图1-1 在 RIP 中引入静态路由时应用路由策略配置举例



3. 配置步骤

(1) 配置 Switch A

配置接口 vlan-interface 100 和 vlan-interface 200 的 IP 地址。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 100
[SwitchA-vlan-interface100] ip address 10.1.1.1 30
[SwitchA-vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-vlan-interface200] ip address 11.1.1.1 32
[SwitchA-vlan-interface200] quit
```

在接口 vlan-interface 100 下使能 RIP。

```
[SwitchA] interface vlan-interface 100
[SwitchA-vlan-interface100] rip 1 enable
[SwitchA-vlan-interface100] quit
```

配置三条静态路由，其下一跳为 11.1.1.2，保证静态路由为 active 状态。

```
[SwitchA] ip route-static 20.1.1.1 32 11.1.1.2
[SwitchA] ip route-static 30.1.1.1 32 11.1.1.2
[SwitchA] ip route-static 40.1.1.1 32 11.1.1.2
```

配置路由策略。

```
[SwitchA] ip prefix-list a index 10 permit 30.1.1.1 32
[SwitchA] route-policy static2rip deny node 0
[SwitchA-route-policy-static2rip-0] if-match ip address prefix-list a
[SwitchA-route-policy-static2rip-0] quit
```

```
[SwitchA] route-policy static2rip permit node 10
[SwitchA-route-policy-static2rip-10] quit
```

启动 RIP 协议，同时应用路由策略 static2rip 对引入的静态路由进行过滤。

```
[SwitchA] rip
[SwitchA-rip-1] import-route static route-policy static2rip
```

(2) 配置 Switch B

配置接口 vlan-interface 100 的 IP 地址。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 100
[SwitchB-vlan-interface100] ip address 10.1.1.2 30
```

启动 RIP 协议。

```
[SwitchB] rip
[SwitchB-rip-1] quit
```

在接口下使能 RIP。

```
[SwitchB] interface vlan-interface 100
[SwitchB-vlan-interface100] rip 1 enable
[SwitchB-vlan-interface100] quit
```

4. 验证配置

查看 Switch B 的 RIP 路由表。

```
<H3C>display  ip routing-table
Destinations : 14       Routes : 14
Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/32          Direct  0   0           127.0.0.1       InLoop0
10.1.1.0/30         Direct  0   0           10.1.1.2        Vlan100
10.1.1.0/32         Direct  0   0           10.1.1.2        Vlan100
10.1.1.2/32         Direct  0   0           127.0.0.1       InLoop0
10.1.1.3/32         Direct  0   0           10.1.1.2        Vlan100
20.0.0.0/8          RIP     100 1           10.1.1.1        Vlan100
40.0.0.0/8          RIP     100 1           10.1.1.1        Vlan100
127.0.0.0/8         Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
224.0.0.0/4         Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24        Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

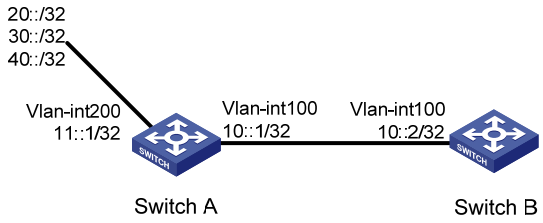
1.7.2 在IPv6 路由引入中应用路由策略配置举例

1. 组网需求

- 在 Switch A 和 Switch B 上使能 RIPng。
- 在 Switch A 上配置三条静态路由，并设置在引入静态路由时应用路由策略，使三条静态路由部分引入、部分被屏蔽掉——20::/32 和 40::/32 网段的路由是可见的，30::/32 网段的路由则被屏蔽。
- 通过在 Switch B 上查看 RIPng 路由表，验证路由策略是否生效。

2. 组网图

图1-2 在 IPv6 路由引入中应用路由策略配置组网图



3. 配置步骤

(1) 配置 Switch A

配置接口 Vlan-interface100 和 Vlan-interface200 的 IPv6 地址。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ipv6 address 10::1 32
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ipv6 address 11::1 32
[SwitchA-Vlan-interface200] quit
```

在接口下使能 RIPng。

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ripng 1 enable
[SwitchA-Vlan-interface100] quit
```

配置三条静态路由，其下一跳为 11::2，保证静态路由为 active 状态。

```
[SwitchA] ipv6 route-static 20:: 32 11::2
[SwitchA] ipv6 route-static 30:: 32 11::2
[SwitchA] ipv6 route-static 40:: 32 11::2
```

配置路由策略。

```
[SwitchA] ipv6 prefix-list a index 10 permit 30:: 32
[SwitchA] route-policy static2ripng deny node 0
[SwitchA-route-policy-static2ripng-0] if-match ipv6 address prefix-list a
[SwitchA-route-policy-static2ripng-0] quit
[SwitchA] route-policy static2ripng permit node 10
[SwitchA-route-policy-static2ripng-10] quit
```

启动 RIPng 协议并引入静态路由。

```
[SwitchA] ripng
[SwitchA-ripng-1] import-route static route-policy static2ripng
```

(2) 配置 Switch B

配置接口 Vlan-interface100 的 IPv6 地址。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ipv6 address 10::2 32
```

启动 RIPng 协议。

```
[SwitchB] ripng
[SwitchB-ripng-1] quit
```

在接口下使能 RIPng。

```
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ripng 1 enable
[SwitchB-Vlan-interface100] quit
```

4. 验证配置

查看 Switch B 的 RIPng 路由表。

```
[SwitchB] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
 ----------------------------------------------------------------

 Peer FE80::7D58:0:CA03:1 on Vlan-interface 100
 Destination 20::/32,
     via FE80::7D58:0:CA03:1, cost 1, tag 0, A, 8 secs
 Destination 40::/32,
     via FE80::7D58:0:CA03:1, cost 1, tag 0, A, 3 secs
 Local route
 Destination 10::/32,
     via ::, cost 0, tag 0, DOF
```