H3C SR6600_SR6600-X 系列路由器

典型配置案例集

新华三技术有限公司
http://www.h3c.com

软件版本：R8128
资料版本：6W101-20220817

Copyright © 2022 新华三技术有限公司及其许可者 版权所有，保留一切权利。

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

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

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

环境保护

本产品符合关于环境保护方面的设计要求，产品的存放、使用和弃置应遵照相关国家法律、法规要求进行。

前 言

本配置指导主要介绍 H3C SR6600_SR6600-X 系列路由器 典型配置案例。

前言部分包含如下内容：

- 读者对象
- 本书约定
- 资料意见反馈

读者对象

本手册主要适用于如下工程师：

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

本书约定

1. 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。

2. 各类标志

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

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

3. 图标约定

本书使用的图标及其含义如下：

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

4. 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！

1 典型配置举例 导读

H3C SR6600_SR6600-X 系列路由器 典型配置举例共包括 42 个文档，介绍了 SR6600_SR6600-X 系列路由器常用特性的典型配置举例，包含组网需求、配置步骤和验证配置等内容。

1.1 适用款型及软件版本

本手册所描述的内容适用于 SR6600_SR6600-X 系列路由器 Release 8128 及其以上版本。

1.2 内容简介

手册包含的文档列表如下：

编号	名称
1	H3C SR6600_SR6600-X系列路由器 策略路由典型配置举例
2	H3C SR6600_SR6600-X系列路由器 镜像典型配置举例
3	H3C SR6600_SR6600-X系列路由器 路由策略配置举例
4	H3C SR6600_SR6600-X系列路由器 双向PIM典型配置举例
5	H3C SR6600_SR6600-X系列路由器 以太网链路聚合典型配置举例
6	H3C SR6600_SR6600-X系列路由器 以太网OAM典型配置举例
7	H3C SR6600_SR6600-X系列路由器 帧中继典型配置举例
8	H3C SR6600_SR6600-X系列路由器 组播VPN典型配置
9	H3C SR6600_SR6600-X系列路由器 AAA典型配置举例
10	H3C SR6600_SR6600-X系列路由器 ACL典型配置举例
11	H3C SR6600_SR6600-X系列路由器 ATM典型配置举例
12	H3C SR6600_SR6600-X系列路由器 BFD典型配置举例
13	H3C SR6600_SR6600-X系列路由器 BGP基础配置举例
14	H3C SR6600_SR6600-X系列路由器 BGP路由属性控制路由选择配置举例
15	H3C SR6600_SR6600-X系列路由器 CPOS接口典型配置举例
16	H3C SR6600_SR6600-X系列路由器 EAA典型配置举例
17	H3C SR6600_SR6600-X系列路由器 GRE和OSPF结合使用典型配置举例
18	H3C SR6600_SR6600-X系列路由器 HoVPN典型配置举例
19	H3C SR6600_SR6600-X系列路由器 IGMP典型配置举例
20	H3C SR6600_SR6600-X系列路由器 IPsec配置举例
21	H3C SR6600_SR6600-X系列路由器 IPv6 IS-IS典型配置举例

编号	名称
22	H3C SR6600_SR6600-X系列路由器 IPv6 over IPv4 GRE隧道典型配置举例
23	H3C SR6600_SR6600-X系列路由器 IS-IS典型配置举例
24	H3C SR6600_SR6600-X系列路由器 IS-IS路由聚合典型配置举例
25	H3C SR6600_SR6600-X系列路由器 MPLS基础典型配置举例
26	H3C SR6600_SR6600-X系列路由器 MPLS L3VPN典型配置举例
27	H3C SR6600_SR6600-X系列路由器 MPLS OAM典型配置举例
28	H3C SR6600_SR6600-X系列路由器 MPLS TE典型配置举例
29	H3C SR6600_SR6600-X系列路由器 NAT典型配置举例
30	H3C SR6600_SR6600-X系列路由器 NetStream典型配置举例
31	H3C SR6600_SR6600-X系列路由器 NQA典型配置举例
32	H3C SR6600_SR6600-X系列路由器 NTP典型配置举例
33	H3C SR6600_SR6600-X系列路由器 OSPF典型配置举例
34	H3C SR6600_SR6600-X系列路由器 OSPFv3典型配置举例
35	H3C SR6600_SR6600-X系列路由器 Portal典型配置举例
36	H3C SR6600_SR6600-X系列路由器 POS接口典型配置举例
37	H3C SR6600_SR6600-X系列路由器 PPP典型配置案例
38	H3C SR6600_SR6600-X系列路由器 RBAC典型配置举例
39	H3C SR6600_SR6600-X系列路由器 Sampler结合IPv4 Netstream典型配置举例
40	H3C SR6600_SR6600-X系列路由器 SNMP典型配置举例
41	H3C SR6600_SR6600-X系列路由器 SSH典型配置举例
42	H3C SR6600_SR6600-X系列路由器 VRRP典型配置举例

H3C SR6600/SR6600-X 系列路由器

策略路由配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 使用限制 1
4 IPv4 策略路由配置举例 1
4.1 组网需求 1
4.2 配置思路 2
4.3 使用版本 2
4.4 配置步骤 2
4.5 验证配置 3
4.6 配置文件 3
5 IPv6 策略路由配置举例 4
5.1 组网需求 4
5.2 配置思路 5
5.3 使用版本 5
5.4 配置步骤 5
5.5 验证配置 6
5.6 配置文件 6
6 相关资料 7

1 简介

本文档介绍了策略路由的配置举例。

普通报文是根据目的 IP 地址来查找路由表转发的，策略路由是一种依据用户制定的策略进行路由选择的机制。策略路由可以基于到达报文的源地址、目的地址、IP 优先级、协议类型等字段灵活地进行路由选择。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文假设您已了解策略路由特性。

3 使用限制

配置重定向到下一跳时，不能将 IPv4 规则重定向到 IPv6 地址，反之亦然。

4 IPv4 策略路由配置举例

4.1 组网需求

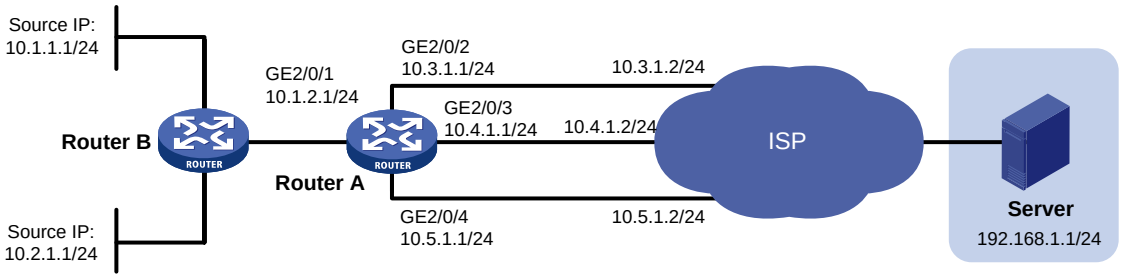
如图 1 所示，缺省情况下，Router A 的接口 GigabitEthernet2/0/1 上收到的所有访问 Server 的报文根据路由表转发的下一跳均为 10.4.1.2。

现要求在 Router A 上配置 IPv4 策略路由，对于访问 Server 的报文实现如下要求：

(1) 首先匹配接口 GigabitEthernet2/0/1 上收到的源 IP 地址为 10.2.1.1 的报文，将该报文的下一跳重定向到 10.5.1.2；

(2) 其次匹配接口 GigabitEthernet2/0/1 上收到的 HTTP 报文，将该报文的下一跳重定向到 10.3.1.2。

图1 IPv4 策略路由特性典型配置组网图



4.2 配置思路

- 为了确保能同时满足对于两种不同类型的报文重定向到不同的下一跳，需要配置两个访问控制列表，一个用于匹配接口 GigabitEthernet2/0/1 上收到的源 IP 地址为 10.2.1.1 的报文，另一个用于匹配接口 GigabitEthernet2/0/1 上收到的 HTTP 报文，并在策略路由中创建两个节点，分别对匹配上的报文进行重定向；
- 同一条策略路由中，创建的节点编号越小，优先级越高。为了确保接口 GigabitEthernet2/0/1 上收到源 IP 地址为 10.2.1.1 的 HTTP 报文下一跳能优先被重定向到 10.5.1.2，需要在策略路由中配置该策略使用较小的节点编号（本例中使用 0 号节点，另一策略使用 1 号节点）。

4.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.4 配置步骤

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] ip address 10.1.2.1 255.255.255.0
[RouterA-GigabitEthernet2/0/1] quit
```

请参考以上方法配置图 1 中其它接口的 IP 地址，配置步骤这里省略。

配置静态路由，保证三条路径都可达，并且缺省下一跳为 10.4.1.2。

```
[RouterA] ip route-static 192.168.1.0 24 10.3.1.2
[RouterA] ip route-static 192.168.1.0 24 10.4.1.2 preference 40
[RouterA] ip route-static 192.168.1.0 24 10.5.1.2
```

定义访问控制列表 ACL 3005，用于匹配源 IP 地址为 10.2.1.1 的报文。

```
[RouterA] acl advanced 3005
[RouterA-acl-ipv4-adv-3005] rule 0 permit ip source 10.2.1.1 0
[RouterA-acl-ipv4-adv-3005] quit
```

定义访问控制列表 ACL 3006，用于匹配 HTTP 报文。

```
[RouterA] acl advanced 3006
[RouterA-acl-ipv4-adv-3006] rule 0 permit tcp destination-port eq www
[RouterA-acl-ipv4-adv-3006] quit
```

创建策略路由 pbr1 的 0 号节点，将匹配 ACL 3005 的报文下一跳重定向到 10.5.1.2。

```
[RouterA] policy-based-route pbr1 permit node 0
[RouterA-pbr-pbr1-0] if-match acl 3005
[RouterA-pbr-pbr1-0] apply next-hop 10.5.1.2
[RouterA-pbr-pbr1-0] quit
```

创建策略路由 pbr1 的 1 号节点，将匹配 ACL 3006 的报文下一跳重定向到 10.3.1.2。

```
[RouterA] policy-based-route pbr1 permit node 1
[RouterA-pbr-pbr1-1] if-match acl 3006
[RouterA-pbr-pbr1-1] apply next-hop 10.3.1.2
[RouterA-pbr-pbr1-1] quit
```

在 Router A 的接口 GigabitEthernet2/0/1 上应用策略。

```
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] ip policy-based-route pbr1
[RouterA-GigabitEthernet2/0/1] quit
```

4.5 验证配置

通过 **display ip policy-based-route** 命令可以查看到当前策略路由配置已经配置成功：

```
[RouterA] display ip policy-based-route policy pbr1
Policy name: pbr1
  node 0 permit:
    if-match acl 3005
    apply next-hop 10.5.1.2
  node 1 permit:
    if-match acl 3006
    apply next-hop 10.3.1.2
```

通过 **tracert** 命令查看以下报文的转发路径（使用 Tracert 功能需要在中间设备上开启 ICMP 超时报文发送功能，在目的端开启 ICMP 目的不可达报文发送功能）：

- 源 IP 为 10.1.1.1 的非 HTTP 报文，根据路由表进行转发，下一跳为 10.4.1.2。

```
<Router> tracert -a 10.1.1.1 192.168.1.1
traceroute to 192.168.1.1 (192.168.1.1) from 10.1.1.1, 30 hops at most, 40 bytes
 each packet, press CTRL_C to break
 1  10.1.2.1 (10.1.2.1)  2.178 ms  1.364 ms  1.058 ms
 2  10.4.1.2 (10.4.1.2)  1.548 ms  1.248 ms  1.112 ms
 3  192.168.1.1 (192.168.1.1)  1.594 ms  1.321 ms  1.093 ms
```

- 源 IP 为 10.2.1.1 的报文，重定向到 10.5.1.2 进行转发。

```
<Router> tracert -a 10.2.1.1 192.168.1.1
traceroute to 192.168.1.1 (192.168.1.1) from 10.2.1.1, 30 hops at most, 40 bytes
 each packet, press CTRL_C to break
 1  10.1.2.1 (10.1.2.1)  1.721 ms  1.226 ms  1.050 ms
 2  10.5.1.2 (10.5.1.2)  4.494 ms  1.385 ms  1.170 ms
 3  192.168.1.1 (192.168.1.1)  1.448 ms  1.304 ms  1.093 ms
```

4.6 配置文件

```
#
policy-based-route pbr1 permit node 0
 if-match acl 3005
 apply next-hop 10.5.1.2
#
policy-based-route pbr1 permit node 1
 if-match acl 3006
 apply next-hop 10.3.1.2
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.1.2.1 255.255.255.0
 ip policy-based-route pbr1
```

```
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.3.1.1 255.255.255.0
#
interface GigabitEthernet2/0/3
 port link-mode route
 ip address 10.4.1.1 255.255.255.0
#
interface GigabitEthernet2/0/4
 port link-mode route
 ip address 10.5.1.1 255.255.255.0
#
 ip route-static 192.168.1.0 24 10.3.1.2
 ip route-static 192.168.1.0 24 10.4.1.2 preference 40
 ip route-static 192.168.1.0 24 10.5.1.2
#
acl advanced 3005
 rule 0 permit ip source 10.2.1.1 0
#
acl advanced 3006
 rule 0 permit tcp destination-port eq www
#
```

5 IPv6 策略路由配置举例

5.1 组网需求

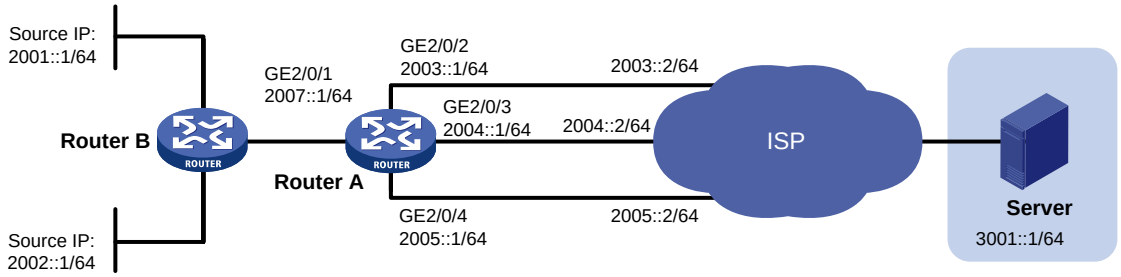
如图 2 所示缺省情况下，Router A 的接口 GigabitEthernet2/0/1 上收到的所有访问 Server 的报文根据路由表转发的下一跳均为 2004::2。

现要求在 Router A 上配置 IPv4 策略路由，对于访问 Server 的报文实现如下要求：

(1) 首先匹配接口 GigabitEthernet2/0/1 上收到的源 IPv6 地址为 2002::1 的报文，将该报文的下一跳重定向到 2005::2；

(2) 其次匹配接口 GigabitEthernet2/0/1 上收到的 HTTP 报文，将该报文的下一跳重定向到 2003::2。

图2 IPv6 策略路由特性典型配置组网图



5.2 配置思路

- 为了确保能同时满足对于两种不同类型的报文重定向到不同的下一跳，需要配置两个访问控制列表，一个用于匹配接口 GigabitEthernet2/0/1 上收到的源 IPv6 地址为 2002::1 的报文，另一个用于匹配接口 GigabitEthernet2/0/1 上收到的 HTTP 报文，并在策略路由中创建两个节点，分别对匹配上的报文进行重定向；
- 同一条策略路由中，创建的节点编号越小，优先级越高。为了确保接口 GigabitEthernet2/0/1 上收到源 IPv6 地址为 2002::1 的 HTTP 报文下一跳能优先被重定向到 2005::2，需要在策略路由中配置该策略使用较小的节点编号（本例中使用 0 号节点，另一策略使用 1 号节点）。

5.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

5.4 配置步骤

#配置接口 GigabitEthernet2/0/1 的 IPv6 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] ipv6 address 2007::1 64
[RouterA-GigabitEthernet2/0/1] quit
```

#请参考以上方法配置图 2 中其它接口的 IPv6 地址，配置步骤这里省略。

配置静态路由，保证三条路径都可达，并且缺省下一跳为 2004::2/64。

```
[RouterA] ipv6 route-static 3001::1 64 2003::2
[RouterA] ipv6 route-static 3001::1 64 2004::2 preference 40
[RouterA] ipv6 route-static 3001::1 64 2005::2
```

定义 IPv6 访问控制列表 IPv6 ACL 3005，用于匹配源 IPv6 地址为 2002::1 的报文。

```
[RouterA] acl ipv6 advanced 3005
[RouterA-acl6-adv-3005] rule 0 permit ipv6 source 2002::1/128
[RouterA-acl6-adv-3005] quit
```

定义 IPv6 访问控制列表 IPv6 ACL 3006，用于匹配 GigabitEthernet2/0/1 端口上收到的 HTTP 报文。

```
[RouterA] acl ipv6 advanced 3006
[RouterA-acl6-adv-3006] rule 0 permit tcp destination-port eq www
[RouterA-acl6-adv-3006] quit
```

创建 IPv6 策略路由 pbr1 的 0 号结点，将匹配 IPv6 ACL 3005 的报文下一跳重定向到 2005::2。

```
[RouterA] ipv6 policy-based-route pbr1 permit node 0
[RouterA-pbr6-pbr1-0] if-match acl 3005
[RouterA-pbr6-pbr1-0] apply next-hop 2005::2
[RouterA-pbr6-pbr1-0] quit
```

创建 IPv6 策略路由 pbr1 的 1 号结点，将匹配 IPv6 ACL 3006 的报文下一跳重定向到 2003::2。

```
[RouterA] ipv6 policy-based-route pbr1 permit node 1
[RouterA-pbr6-pbr1-1] if-match acl 3006
[RouterA-pbr6-pbr1-1] apply next-hop 2003::2
[RouterA-pbr6-pbr1-1] quit
```

在 Router A 的接口 GigabitEthernet2/0/1 上应用策略。

```
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] ipv6 policy-based-route pbr1
[RouterA-GigabitEthernet2/0/1] quit
```

5.5 验证配置

通过 **display ipv6 policy-based-route** 命令可以查看到当前 IPv6 策略路由配置已经生效：

```
[RouterA] display ipv6 policy-based-route policy pbr1
Policy name: pbr1
  node 0 permit:
    if-match acl 3005
    apply next-hop 2005::2
  node 1 permit:
    if-match acl 3006
    apply next-hop 2003::2
```

当 RouterA 收到源 IPv6 地址为 2002::1 的报文时，有如下结果：

- 当 2005::2 可达时，报文被重定向到 2005::2；
- 当 2005::2 不可达时，报文会根据普通的路由表转发到下一跳 2004::2。

当 RouterA 收到 HTTP 报文时，有如下结果：

- 当 2003::2 可达时，报文被重定向到 2003::2；
- 当 2003::2 不可达时，报文会根据普通的路由表转发到下一跳 2004::2。

5.6 配置文件

```
#
ipv6 policy-based-route pbr1 permit node 0
 if-match acl 3005
 apply next-hop 2005::2
#
ipv6 policy-based-route pbr1 permit node 1
 if-match acl 3006
 apply next-hop 2003::2
#
interface GigabitEthernet2/0/1
 port link-mode route
 ipv6 policy-based-route pbr1
 ipv6 address 2007::1/64
#
interface GigabitEthernet2/0/2
 port link-mode route
 ipv6 address 2003::1 64
#
interface GigabitEthernet2/0/3
 port link-mode route
 ipv6 address 2004::1 64
```

```
#
interface GigabitEthernet2/0/4
 port link-mode route
 ipv6 address 2005::1 64
#
 ipv6 route-static 3001:: 64 2003::2
 ipv6 route-static 3001:: 64 2004::2 preference 40
 ipv6 route-static 3001:: 64 2005::2
#
acl ipv6 advanced 3005
 rule 0 permit ipv6 source 2002::1/128
#
 acl ipv6 advanced 3006
 rule 0 permit tcp destination-port eq www
#
```

6 相关资料

- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由配置指导-R7607
- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

镜像配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 本地端口镜像典型配置举例 1
3.1 组网需求 1
3.2 使用版本 1
3.3 配置注意事项 2
3.4 配置步骤 2
3.5 验证配置 2
3.6 配置文件 3
4 相关资料 4

1 简介

本文介绍了端口镜像的典型配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

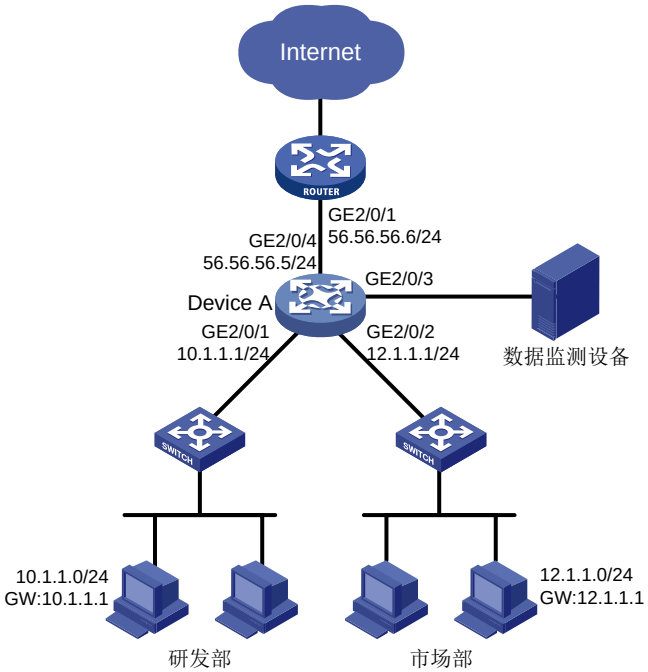
本文假设您已了解镜像特性。

3 本地端口镜像典型配置举例

3.1 组网需求

如图 1 所示，某公司内部各部门使用不同网段的 IP 地址，其中研发部使用 10.1.1.0/24 网段，市场部使用 12.1.1.0/24 网段。现要求通过配置本地端口镜像功能，使用数据监测设备对研发部和市场部访问 Internet 的流量以及两个部门之间互访的流量进行监控。

图1 本地端口镜像组网图



3.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.3 配置注意事项

- 本地镜像组需要配置源端口、目的端口才能生效。其中目的端口不能是现有镜像组的成员端口。
- 目的端口收到的报文包括复制自源端口的报文和来自其它端口的正常转发报文。为了保证数据监测设备只对源端口的报文进行分析，请将目的端口只用于端口镜像，不作其它用途。

3.4 配置步骤

配置 GigabitEthernet2/0/1 接口 IP 地址为 10.1.1.1。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 10.1.1.1 24
[DeviceA-GigabitEthernet2/0/1] quit
```

请参考以上方法配置图 1 中其它接口的 IP 地址，配置步骤这里省略。

创建本地镜像组。

```
[DeviceA] mirroring-group 1 local
```

将 GigabitEthernet2/0/1 和 GigabitEthernet2/0/2 配置为镜像源端口，对这两个端口接收的报文进行镜像。

```
[DeviceA] mirroring-group 1 mirroring-port gigabitethernet 2/0/1 gigabitethernet 2/0/2
inbound
```

将 GigabitEthernet2/0/3 配置为镜像目的端口。

```
[DeviceA] mirroring-group 1 monitor-port gigabitethernet 2/0/3
```

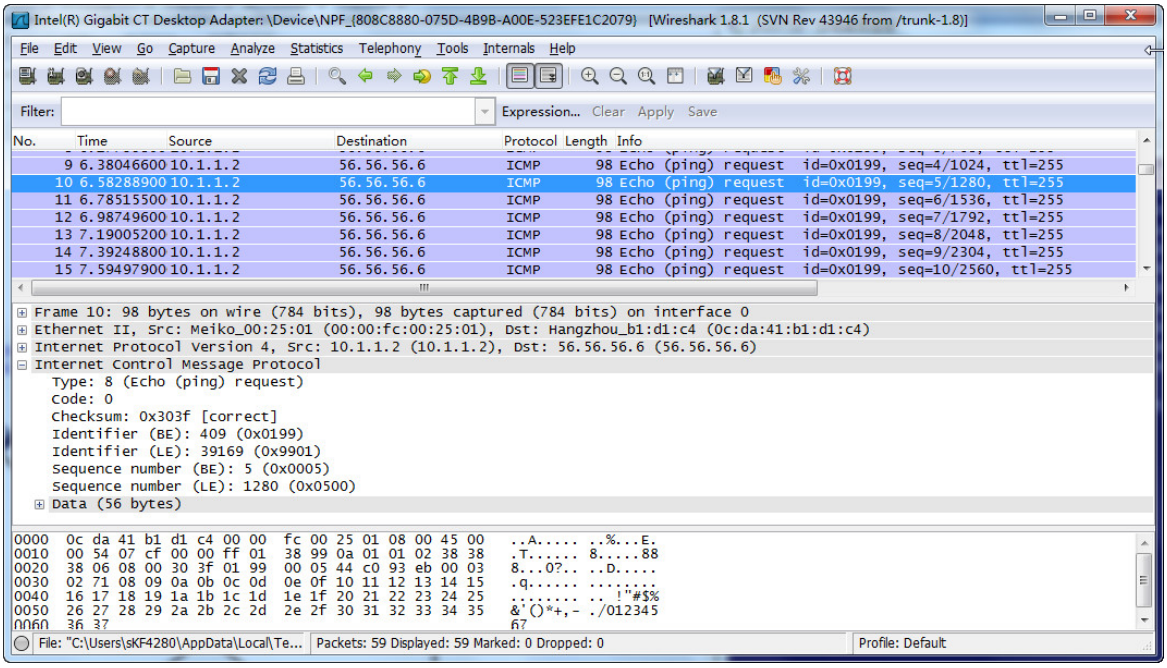
3.5 验证配置

在完成上述配置后，在 DeviceA 上显示镜像组 1 的配置信息。

```
[DeviceA] display mirroring-group 1
Mirroring group 1:
    Type: Local
    Status: Active
    Mirroring port:
        GigabitEthernet2/0/1  Inbound
        GigabitEthernet2/0/2  Inbound
    Monitor port: GigabitEthernet2/0/3
```

以研发部某台主机 10.1.1.2 通过 ping 方式访问 56.56.56.6 为例，进行镜像测试，数据监测设备的抓包数据如图 2 所示。

图2 Wireshark 的抓包数据



以上抓包信息表明，配置的本地镜像功能生效，数据监测设备可以成功对需要监控的流量进行监控。

3.6 配置文件

```
#
 mirroring-group 1 local
#
interface GigabitEthernet2/0/1
 ip address 10.1.1.1 255.255.255.0
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet2/0/2
 ip address 12.1.1.1 255.255.255.0
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet2/0/3
 port link-mode bridge
 undo stp enable
 mirroring-group 1 monitor-port
#
interface GigabitEthernet2/0/4
 port link-mode route
 ip address 56.56.56.5 255.255.255.0
#
```

4 相关资料

- H3C SR6600 SR6600-X 路由器 网络管理和监控配置指导-R7607
- H3C SR6600 SR6600-X 路由器 网络管理和监控命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

路由策略配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 配置举例 1
3.1 组网需求 1
3.2 配置思路 2
3.3 使用版本 2
3.4 配置步骤 2
3.4.1 配置各接口的 IP 地址 2
3.4.2 在 AS 100 内配置 OSPF 基本功能，保证设备间路由可达 2
3.4.3 配置 BGP 基本功能 3
3.4.4 配置路由策略 6
3.5 验证配置 6
3.6 配置文件 8
4 相关资料 11

1 简介

本文档介绍路由策略配置举例。

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。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解路由策略特性。

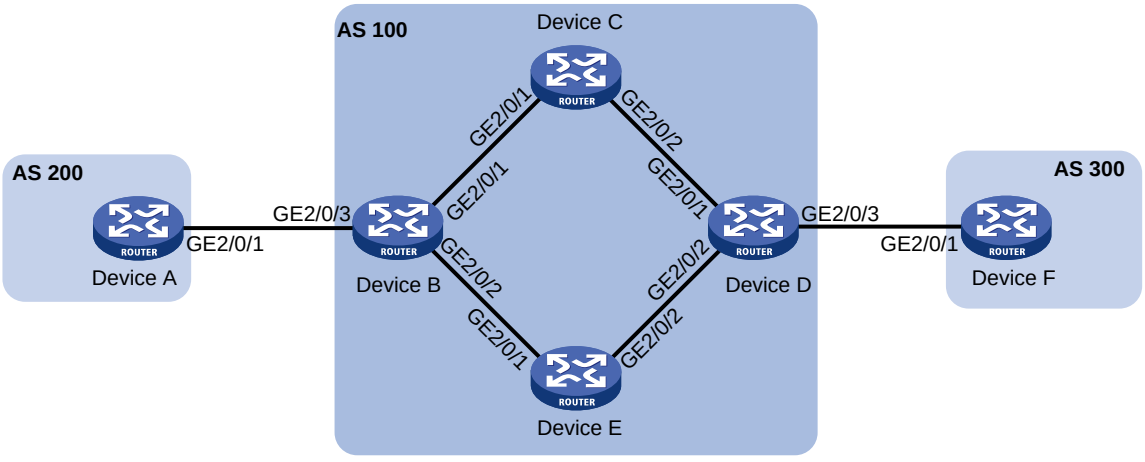
3 配置举例

3.1 组网需求

如图 1 所示，某公司的两个部门相距较远，Device A 和 Device F 分别作为这两个部门的出口设备，AS 100 内部使用 OSPF 作为 IGP。现要求：

- 通过部署 BGP，使两个部门可以通信；
- 通过配置路由策略，将 Device B<—>Device C<—>Device D 链路作为主链路，负责转发 Device A 和 Device F 之间的流量；当主链路断开时，自动切换到 Device B<—>Device E<—>Device D 这条路径进行通信。

图1 路由策略配置组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	GE2/0/1	120.1.0.1/24	Device D	GE2/0/1	10.2.0.101/24
Device B	GE2/0/1	10.1.0.101/24		GE2/0/2	13.1.1.101/24
	GE2/0/2	192.168.0.101/24		GE2/0/3	120.2.0.2/24

设备	接口	IP地址	设备	接口	IP地址
	GE2/0/3	120.1.0.2/24	Device E	GE2/0/1	192.168.0.102/24
Device C	GE2/0/1	10.1.0.102/24		GE2/0/2	13.1.1.102/24
	GE2/0/2	10.2.0.102/24	Device F	GE2/0/1	120.2.0.1/24

3.2 配置思路

- 为了使 Device B<—>Device C<—>Device D 成为主链路，需要：
  - 在 Device B 上配置路由策略来调整 AS 100 前往 AS 200 两条路径的本地优先级
    - Device D—> Device C—> Device B 的本地优先级为 200；
    - Device D—> Device E—> Device B 的本地优先级为缺省值 100；
  - 在 Device D 上配置路由策略来调整 AS 100 前往 AS 300 两条路径的本地优先级
    - Device B—> Device C—> Device D 的本地优先级为 200；
    - Device B—> Device E—> Device D 的本地优先级为缺省值 100。
- 为了使 AS 100 内通信的报文使用 BGP 而不是 OSPF 选路，需要将 IBGP 路由优先级配置高于 OSPF 路由优先级。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置步骤

3.4.1 配置各接口的 IP 地址

配置 Device A 各接口的 IP 地址

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 120.1.0.1 24
[DeviceA-GigabitEthernet2/0/1] quit
```

请参考以上方法配置其它相关接口的 IP 地址，配置步骤这里省略。

3.4.2 在 AS 100 内配置 OSPF 基本功能，保证设备间路由可达

1. 配置 Device B

```
<DeviceB> system-view
[DeviceB] ospf
[DeviceB-ospf-1] import-route direct
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

2. 配置 Device C

```
<DeviceC> system-view
[DeviceC] ospf
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 10.2.0.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] quit
[DeviceC-ospf-1] quit
```

3. 配置 Device D

```
<DeviceD> system-view
[DeviceD] ospf
[DeviceD-ospf-1] import-route direct
[DeviceD-ospf-1] area 0
[DeviceD-ospf-1-area-0.0.0.0] network 10.2.0.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] quit
[DeviceD-ospf-1] quit
```

4. 配置 Device E

```
<DeviceE> system-view
[DeviceE] ospf
[DeviceE-ospf-1] area 0
[DeviceE-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] quit
[DeviceE-ospf-1] quit
```

3.4.3 配置 BGP 基本功能

1. 配置 Device A

启动 BGP，指定本地 AS 号为 200，指定 BGP 路由器的 Router ID 为 1.1.1.1。

```
[DeviceA] bgp 200
[DeviceA-bgp] router-id 1.1.1.1
```

配置 Device A 和 Device B 建立 EBGP 连接。

```
[DeviceA-bgp] peer 120.1.0.2 as-number 100
```

创建 BGP IPv4 单播地址族，并进入 BGP IPv4 单播地址族视图。

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

使能 Device A 与对等体 120.1.0.2 交换 IPv4 单播路由信息的能力。

```
[DeviceA-bgp-ipv4] peer 120.1.0.2 enable
```

在 BGP IPv4 单播地址族视图下，将本地路由表中到达 120.1.0.0/24 网段的路由添加到 BGP 路由表中。

```
[DeviceA-bgp-ipv4] network 120.1.0.0 255.255.255.0
[DeviceA-bgp-ipv4] quit
```

2. 配置 Device B

启动 BGP，指定本地 AS 号为 100，指定 BGP 路由器的 Router ID 为 2.2.2.2。

```
[DeviceB] bgp 100
```

```
[DeviceB-bgp] router-id 2.2.2.2
```
配置 Device B 和 Device A 建立 EBGP 连接。
```
[DeviceB-bgp] peer 120.1.0.1 as-number 200
```
配置 Device B 和 Device D 建立 IBGP 连接。
```
[DeviceB-bgp] peer 10.2.0.101 as-number 100
[DeviceB-bgp] peer 13.1.1.101 as-number 100
```
创建 BGP IPv4 单播地址族，并进入 BGP IPv4 单播地址族视图。
```
[DeviceB-bgp] address-family ipv4 unicast
```
使能 Device B 与对等体 10.2.0.101 交换 IPv4 单播路由信息的能力。
```
[DeviceB-bgp-ipv4] peer 10.2.0.101 enable
```
在 BGP IPv4 单播地址族视图下，配置向对等体 10.2.0.101 发布 BGP 路由时，将下一跳属性修改为自身的地址。
```
[DeviceB-bgp-ipv4] peer 10.2.0.101 next-hop-local
```
使能 Device B 与对等体 13.1.1.101 交换 IPv4 单播路由信息的能力。
```
[DeviceB-bgp-ipv4] peer 13.1.1.101 enable
```
在 BGP IPv4 单播地址族视图下，配置向对等体 13.1.1.101 发布 BGP 路由时，将下一跳属性修改为自身的地址。
```
[DeviceB-bgp-ipv4] peer 13.1.1.101 next-hop-local
```
使能 Device B 与对等体 120.1.0.1 交换 IPv4 单播路由信息的能力。
```
[DeviceB-bgp-ipv4] peer 120.1.0.1 enable
[DeviceB-bgp-ipv4] quit
```
3. 配置 Device D

启动 BGP，指定本地 AS 号为 100，指定 BGP 路由器的 Router ID 为 4.4.4.4。
```
[DeviceD] bgp 100
[DeviceD-bgp] router-id 4.4.4.4
```
配置 Device D 和 Device B 建立 IBGP 连接。
```
[DeviceD-bgp] peer 10.1.0.101 as-number 100
[DeviceD-bgp] peer 192.168.0.101 as-number 100
```
配置 Device D 和 Device F 建立 EBGP 连接。
```
[DeviceD-bgp] peer 120.2.0.1 as-number 300
```
创建 BGP IPv4 单播地址族，并进入 BGP IPv4 单播地址族视图。
```
[DeviceD-bgp] address-family ipv4 unicast
```
使能 Device D 与对等体 10.1.0.101 交换 IPv4 单播路由信息的能力。
```
[DeviceD-bgp-ipv4] peer 10.1.0.101 enable
```
在 BGP IPv4 单播地址族视图下，配置向对等体 10.1.0.101 发布 BGP 路由时，将下一跳属性修改为自身的地址。
```
[DeviceD-bgp-ipv4] peer 10.1.0.101 next-hop-local
```
使能 Device D 与对等体 192.168.0.101 交换 IPv4 单播路由信息的能力。
```
[DeviceD-bgp-ipv4] peer 192.168.0.101 enable
```
在 BGP IPv4 单播地址族视图下，配置向对等体 192.168.0.101 发布 BGP 路由时，将下一跳属性修改为自身的地址。
```
[DeviceD-bgp-ipv4] peer 192.168.0.101 next-hop-local
```
使能 Device D 与对等体 120.2.0.1 交换 IPv4 单播路由信息的能力。
```
[DeviceD-bgp-ipv4] peer 120.2.0.1 enable
```

```
[DeviceD-bgp-ipv4] quit
```

4. 配置 Device F

#启动 BGP，指定本地 AS 号为 300，指定 BGP 路由器的 Router ID 为 6.6.6.6。

```
<DeviceF> system-view
[DeviceF] bgp 300
[DeviceF-bgp] router-id 6.6.6.6
```

配置 Device F 和 Device D 建立 EBGP 连接。

```
[DeviceF-bgp] peer 120.2.0.2 as-number 100
```

创建 BGP IPv4 单播地址族，并进入 BGP IPv4 单播地址族视图。

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

在 BGP IPv4 单播地址族视图下，将本地路由表中到达 120.2.0.0/24 网段的路由添加到 BGP 路由表中。

```
[DeviceF-bgp-ipv4] network 120.2.0.0 255.255.255.0
```

使能 Device F 与对等体 120.2.0.2 交换 IPv4 单播路由信息的能力。

```
[DeviceF-bgp-ipv4] peer 120.2.0.2 enable
[DeviceF-bgp-ipv4] quit
```

完成以上配置后，在 Device B 上通过命令 **display bgp peer** 查看 BGP 对等体信息。

```
[DeviceB] display bgp peer ipv4

 BGP local router ID: 2.2.2.2
 Local AS number: 100
 Total number of peers: 3                 Peers in established state: 3

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  10.2.0.101             100        6        4    0       1 00:00:56 Established
  13.1.1.101             100        6        5    0       1 00:00:56 Established
  120.1.0.1              200        6        5    0       1 00:00:56 Established
```

以上信息可以看到 Device B 与 Device D 建立 IBGP 连接，Device B 与 Device A 建立 EBGP 连接，且均处于 Established 状态。

完成以上配置后，从 Device A 上 ping Device F 的 IP 地址。

```
[DeviceA] ping 120.2.0.1
Ping 120.2.0.1 (120.2.0.1): 56 data bytes, press CTRL_C to break
56 bytes from 120.2.0.1: icmp_seq=0 ttl=252 time=1.189 ms
56 bytes from 120.2.0.1: icmp_seq=1 ttl=252 time=1.095 ms
56 bytes from 120.2.0.1: icmp_seq=2 ttl=252 time=1.086 ms
56 bytes from 120.2.0.1: icmp_seq=3 ttl=252 time=1.097 ms
56 bytes from 120.2.0.1: icmp_seq=4 ttl=252 time=1.089 ms

--- Ping statistics for 120.2.0.1 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.086/1.111/1.189/0.039 ms
```

以上显示信息表明 Device A 和 Device F 之间路由可达。

3.4.4 配置路由策略

1. 配置 Device B

创建 ACL 2000，允许源 IP 地址为 120.1.0.0/24 的报文通过。

```
[DeviceB] acl basic 2000
[DeviceB-acl-ipv4-basic-2000] rule permit source 120.1.0.0 0.0.0.255
[DeviceB-acl-ipv4-basic-2000] quit
```

配置路由策略，将从对等体 120.1.0.1 学习到的路由发布给对等体 10.2.0.101 时，设置本地优先级为 200。

```
[DeviceB] route-policy local-pre permit node 10
[DeviceB-route-policy-local-pre-10] if-match ip address acl 2000
[DeviceB-route-policy-local-pre-10] apply local-preference 200
[DeviceB-route-policy-local-pre-10] quit
[DeviceB] bgp 100
[DeviceB-bgp] address-family ipv4 unicast
[DeviceB-bgp-ipv4] peer 10.2.0.101 route-policy local-pre export
```

配置 EBGP 路由优先级为 255，配置 IBGP 路由优先级为 100，配置本地路由优先级为 130，使 IBGP 路由优先级优于 OSPF 路由。

```
[DeviceB-bgp-ipv4] preference 255 100 130
[DeviceB-bgp-ipv4] quit
```

2. 配置 Device D

创建 ACL 2000，允许源 IP 地址为 120.2.0.0/24 的报文通过。

```
[DeviceD] acl basic 2000
[DeviceD-acl-ipv4-basic-2000] rule permit source 120.2.0.0 0.0.0.255
[DeviceD-acl-ipv4-basic-2000] quit
```

配置路由策略，将从对等体 120.2.0.1 学习到的路由发布给对等体 10.1.0.101 时，设置本地优先级为 200。

```
[DeviceD] route-policy local-pre permit node 10
[DeviceD-route-policy-local-pre-10] if-match ip address acl 2000
[DeviceD-route-policy-local-pre-10] apply local-preference 200
[DeviceD-route-policy-local-pre-10] quit
[DeviceD] bgp 100
[DeviceD-bgp] address-family ipv4 unicast
[DeviceD-bgp-ipv4] peer 10.1.0.101 route-policy local-pre export
```

#配置 EBGP 路由优先级为 255，配置 IBGP 路由优先级为 100，配置本地路由优先级为 130，使 IBGP 路由优先级优于 OSPF 路由。

```
[DeviceD-bgp-ipv4] preference 255 100 130
[DeviceD-bgp-ipv4] quit
```

3.5 验证配置

在 Device B 上使用 **`display bgp routing-table ipv4`** 命令查看 BGP 路由表，可以看到 2 条 120.2.0.0/24 的路由，本地路由优先级分别为 100 和 200。

```
[DeviceB]display bgp routing-table ipv4
```

```
 Total number of routes: 3

 BGP local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >e 120.1.0.0/24       120.1.0.1       0                     0       200i
* >i 120.2.0.0/24       10.2.0.101      0          200        0       300i
*  i                    13.1.1.101      0          100        0       300i
```

在 Device A 上 tracert Device F，查看到报文传输路径是 Device A—> Device B—> Device C—> Device D—> Device F

```
[DeviceA] tracert 120.2.0.1
traceroute to 120.2.0.1 (120.2.0.1), 30 hops at most, 52 bytes each packet, pres
s CTRL_C to break
 1  120.1.0.2 (120.1.0.2)  2.208 ms  1.119 ms  1.085 ms
 2  10.1.0.102 (10.1.0.102)  1.083 ms  1.100 ms  1.085 ms
 3  10.2.0.101 (10.2.0.101)  2.364 ms  1.099 ms  1.086 ms
 4  120.2.0.1 (120.2.0.1)  3.825 ms  3.693 ms  4.008 ms
```

主链路断开后再查看 Device B 的 BGP 路由表，存在 1 条 120.2.0.0/24 的路由。

```
[DeviceB]display bgp routing-table ipv4

 Total number of routes: 2

 BGP local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >e 120.1.0.0/24       120.1.0.1       0                     0       200i
* >i 120.2.0.0/24       13.1.1.101      0          100        0       300i
```

再次在 Device A 上 tracert Device F，查看到报文传输路径是 Device A—> Device B—> Device E—> Device D—> Device F

```
[DeviceA] tracert 120.2.0.1
traceroute to 120.2.0.1 (120.2.0.1), 30 hops at most, 52 bytes each packet, pres
s CTRL_C to break
 1  120.1.0.2 (120.1.0.2)  2.308 ms  1.127 ms  1.091 ms
 2  192.168.0.102 (192.168.0.102)  1.086 ms  1.102 ms  1.096 ms
 3  13.1.1.101 (13.1.1.101)  2.451 ms  2.087 ms  1.092 ms
 4  120.2.0.1 (120.2.0.1)  3.533 ms  3.818 ms  4.002 ms
```

以上信息表明主备链路切换成功。

3.6 配置文件

- Device A：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 120.1.0.1 255.255.255.0
#
bgp 200
 router-id 1.1.1.1
 peer 120.1.0.2 as-number 100
 #
 address-family ipv4 unicast
  network 120.1.0.0 255.255.255.0
  peer 120.1.0.2 enable
#
```

- Device B：

```
#
ospf 1
import-route direct
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.1.0.101 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 192.168.0.101 255.255.255.0
#
interface GigabitEthernet2/0/3
 port link-mode route
 ip address 120.1.0.2 255.255.255.0
#
bgp 100
 router-id 2.2.2.2
 peer 10.2.0.101 as-number 100
 peer 13.1.1.101 as-number 100
 peer 120.1.0.1 as-number 200
#
 address-family ipv4 unicast
  preference 255 100 130
  peer 10.2.0.101 enable
  peer 10.2.0.101 next-hop-local
  peer 10.2.0.101 route-policy local-pre export
  peer 13.1.1.101 enable
```

```
  peer 13.1.1.101 next-hop-local
  peer 120.1.0.1 enable
#
route-policy local-pre permit node 10
 if-match ip address acl 2000
 apply local-preference 200
#
acl basic 2000
 rule 0 permit source 120.1.0.0 0.0.0.255
#
```

- Device C：

```
#
ospf 1
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 10.2.0.0 0.0.0.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.1.0.102 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.2.0.102 255.255.255.0
#
```

- Device D：

```
#
ospf 1
 import-route direct
 area 0.0.0.0
  network 10.2.0.0 0.0.0.255
  network 13.1.1.0 0.0.0.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.2.0.101 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 13.1.1.101 255.255.255.0
#
interface GigabitEthernet2/0/3
 port link-mode route
 ip address 120.2.0.2 255.255.255.0
#
bgp 100
 router-id 4.4.4.4
 peer 10.1.0.101 as-number 100
```

```
 peer 120.2.0.1 as-number 300
 peer 192.168.0.101 as-number 100
#
 address-family ipv4 unicast
  preference 255 100 130
  peer 10.1.0.101 enable
  peer 10.1.0.101 next-hop-local
  peer 10.1.0.101 route-policy local-pre export
  peer 192.168.0.101 enable
  peer 192.168.0.101 next-hop-local
  peer 120.2.0.1 enable
#
route-policy local-pre permit node 10
 if-match ip address acl 2000
 apply local-preference 200
#
#
acl basic 2000
 rule 0 permit source 120.2.0.0 0.0.0.255
#
```

- Device E：

```
#
ospf 1
 area 0.0.0.0
  network 13.1.1.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 192.168.0.102 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 13.1.1.102 255.255.255.0
#
```

- Device F：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 120.2.0.1 255.255.255.0
#
bgp 300
 router-id 6.6.6.6
 peer 120.2.0.2 as-number 100
 #
 address-family ipv4 unicast
  network 120.2.0.0 255.255.255.0
  peer 120.2.0.2 enable
```

#

4 相关资料

- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由配置指导-R7607
- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

双向 PIM 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 配置举例 1
3.1 组网需求 1
3.2 配置思路 2
3.3 使用版本 3
3.4 配置注意事项 3
3.5 配置步骤 3
3.5.1 Router A 的配置 3
3.5.2 Router B 的配置 4
3.5.3 Router C 的配置 5
3.6 验证配置 6
3.7 配置文件 11
4 相关资料 13

1 简介

本文档介绍了双向 PIM 配置举例。

双向 PIM（Bidirectional Protocol Independent Multicast，双向协议无关组播）通过建立以 RP（Rendezvous Point，汇集点）为中心、分别连接组播源和接收者的双向 RPT（Rendezvous Point Tree，共享树），使组播数据沿着双向 RPT 从组播源经由 RP 转发到接收者。适用于一个组播组中同时对应多个接收者和多个组播源的组网，例如多方电视电话会议。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文假设您已了解双向 PIM 特性。

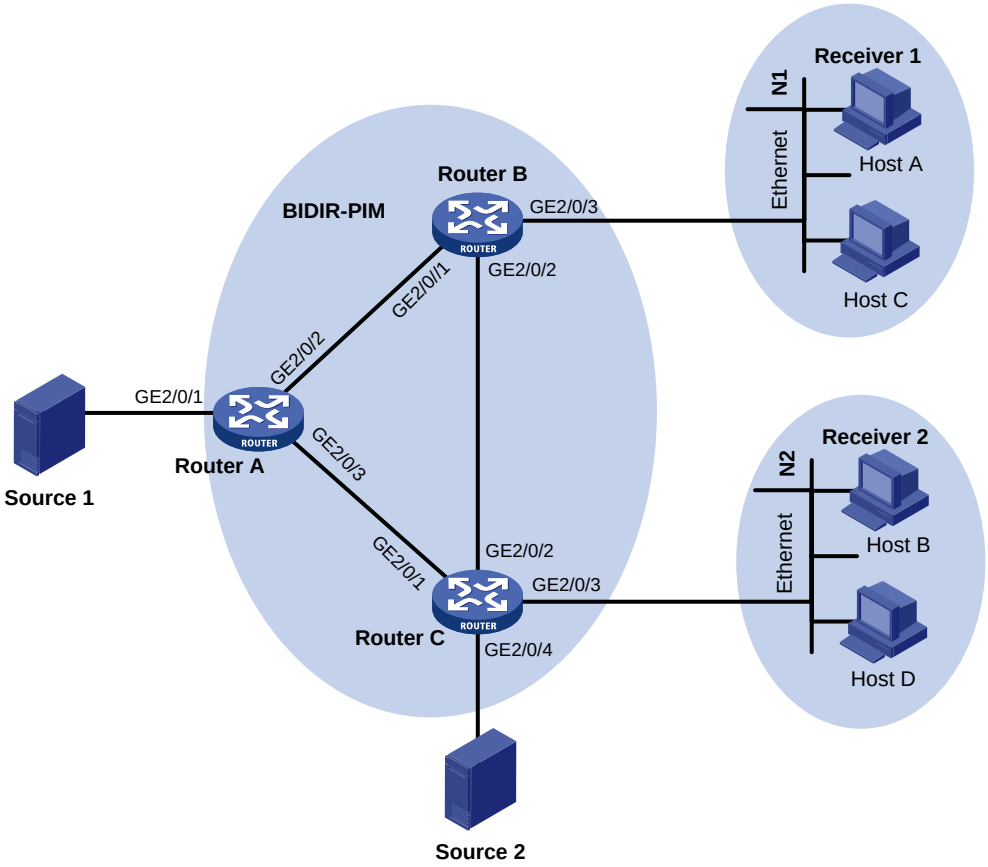
3 配置举例

3.1 组网需求

如图 1 所示，路由器 Router A、Router B 和 Router C 上均运行 OSPF 协议，单播路由正常。接收者通过组播方式接收视频点播信息，组播源 Source 1 和 Source 2 都向组播组 225.1.1.1 发送组播信息，末梢用户网络 N1 和 N2 中的 Host A 和 Host B 均为该组播信息的接收者。

要求在该网络中采用双向 PIM 协议实现组播数据的分发，以减少路由器所维护的组播转发表项数量；同时为了避免因单一 RP 故障而使通信中断，该网络采用动态 RP 和静态 RP 配合方式，来起到 RP 的备份。

图1 双向 PIM 配置组网图



设备	接口	IP地址	设备	接口	IP地址
Router A	GE2/0/1	10.10.1.1/24	Router C	GE2/0/1	10.13.1.3/24
	GE2/0/2	10.12.1.1/24		GE2/0/2	10.23.1.3/24
	GE2/0/3	10.13.1.1/24		GE2/0/3	10.102.1.1/24
				GE2/0/4	10.33.1.3/24
Router B	GE2/0/1	10.12.1.2/24	Source1	-	10.10.1.2/24
	GE2/0/2	10.23.1.2/24	Source2	-	10.33.1.4/24
	GE2/0/3	10.101.1.1/24			

3.2 配置思路

- 选择一台设备的接口作为服务于双向 PIM 的 C-RP，并为该双向 PIM 域指定一个 C-BSR，以负责在双向 PIM 域中收集并发布 RP 信息，C-RP 和 C-BSR 可以由同一接口来充当，也可以配置在不同设备上。本例中指定 Router A 的 GE2/0/2 接口作为 C-RP 和 C-BSR。
- 由于本网络中只配置了一个 C-RP，为了避免因单一节点故障而引起的通信中断，可以再配置一个服务于双向 PIM 的静态 RP 进行备份。本例中通过将静态 RP 的 IP 地址指定为该网络中某网段内但实际不存在的一个地址，从而形成 RPL，连接到 RPL 上的所有接口都可以充当 RP，以提供可靠的备份功能。本例中将实际不存在的地址 10.13.1.4/24 配置为静态 RP 的地址，从而连接到对应 RPL 的路由器 Router A、Router C 都可以提供 RP 的功能。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置注意事项

- 同一台设备相同实例的所有接口上启用的 PIM 模式必须相同。
- 双向 PIM 域内的所有路由器上都必须配置完全相同的静态 RP。
- 双向 PIM 域内的所有路由器的接口都必须使能 PIM-SM。
- 在边界设备连接用户网络的接口上必须使能 IGMP 功能，以建立和维护各组播组的成员关系。

3.5 配置步骤

3.5.1 Router A 的配置

(1) 使能组播路由功能

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
```

(2) 配置各接口及接口地址，并使能 PIM-SM

配置连接组播源 Source 1 的接口及接口地址，使能 PIM-SM。

```
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] ip address 10.10.1.1 24
[RouterA-GigabitEthernet2/0/1] pim sm
[RouterA-GigabitEthernet2/0/1] quit
```

配置连接 Router B 的接口及接口地址，使能 PIM-SM。

```
[RouterA] interface gigabitethernet 2/0/2
[RouterA-GigabitEthernet2/0/2] ip address 10.12.1.1 24
[RouterA-GigabitEthernet2/0/2] pim sm
[RouterA-GigabitEthernet2/0/2] quit
```

配置连接 Router C 的接口及接口地址，使能 PIM-SM。

```
[RouterA] interface gigabitethernet 2/0/3
[RouterA-GigabitEthernet2/0/3] ip address 10.13.1.1 24
[RouterA-GigabitEthernet2/0/3] pim sm
[RouterA-GigabitEthernet2/0/3] quit
```

(3) 配置 C-RP 和静态 RP

指定接口 GigabitEthernet 2/0/2 的 IP 地址为 C-BSR 和 C-RP。

```
[RouterA] pim
[RouterA-pim] c-bsr 10.12.1.1
[RouterA-pim] c-rp 10.12.1.1 bidir
```

指定 IP 地址 10.13.1.4 为静态 RP 的 IP 地址。

```
[RouterA-pim] static-rp 10.13.1.4 bidir
```

使能双向 PIM。

```
[RouterA-pim] bidir-pim enable
```

```
[RouterA-pim] quit
```
配置单播路由协议，以建立正确的单播路由表项。
```
[RouterA] ospf 1
[RouterA-ospf-1] import-route direct
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

3.5.2 Router B 的配置

(1) 使能组播路由功能
```
<RouterB> system-view
[RouterB] multicast routing
[RouterB-mrib] quit
```
(2) 配置各接口及接口地址，并使能 PIM-SM

配置连接 Router A 的接口及接口地址，使能 PIM-SM。
```
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] ip address 10.12.1.2 24
[RouterB-GigabitEthernet2/0/1] pim sm
[RouterB-GigabitEthernet2/0/1] quit
```
配置连接 Router C 的接口及接口地址，使能 PIM-SM。
```
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] ip address 10.23.1.2 24
[RouterB-GigabitEthernet2/0/2] pim sm
[RouterB-GigabitEthernet2/0/2] quit
```
配置连接网络 N1 的接口及接口地址，使能 PIM-SM 和 IGMP（缺省情况下，IGMP 的版本为 IGMPv2）。
```
[RouterB] interface gigabitethernet 2/0/3
[RouterB-GigabitEthernet2/0/3] ip address 10.101.1.1 24
[RouterB-GigabitEthernet2/0/3] pim sm
[RouterB-GigabitEthernet2/0/3] igmp enable
[RouterB-GigabitEthernet2/0/3] quit
```
(3) 配置静态 RP。指定 IP 地址 10.13.1.4 为静态 RP 的 IP 地址。
```
[RouterB] pim
[RouterB-pim] static-rp 10.13.1.4 bidir
```
(4) 使能双向 PIM
```
[RouterB-pim] bidir-pim enable
[RouterB-pim] quit
```
(5) 配置单播路由协议，以建立正确的单播路由表项
```
[RouterB] ospf 1
[RouterB-ospf-1] import-route direct
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

3.5.3 Router C 的配置

(1) 使能组播路由功能

```
<RouterC> system-view
[RouterC] multicast routing
[RouterC-mrib] quit
```

(2) 配置各接口及接口地址，并使能 PIM-SM

配置连接组播源 Source 2 的接口及接口地址，使能 PIM-SM。

```
[RouterC] interface gigabitethernet 2/0/4
[RouterC-GigabitEthernet2/0/4] ip address 10.33.1.3 24
[RouterC-GigabitEthernet2/0/4] pim sm
[RouterC-GigabitEthernet2/0/4] quit
```

配置连接 Router A 的接口及接口地址，使能 PIM-SM

```
[RouterC] interface gigabitethernet 2/0/1
[RouterC-GigabitEthernet2/0/1] ip address 10.13.1.3 24
[RouterC-GigabitEthernet2/0/1] pim sm
[RouterC-GigabitEthernet2/0/1] quit
```

配置连接 Router B 的接口及接口地址，使能 PIM-SM。

```
[RouterC] interface gigabitethernet 2/0/2
[RouterC-GigabitEthernet2/0/2] ip address 10.23.1.3 24
[RouterC-GigabitEthernet2/0/2] pim sm
[RouterC-GigabitEthernet2/0/2] quit
```

配置连接网络 N2 的接口及接口地址，使能 PIM-SM 和 IGMP（缺省情况下，IGMP 的版本为 IGMPv2）。

```
[RouterC] interface gigabitethernet 2/0/3
[RouterC-GigabitEthernet2/0/3] ip address 10.102.1.1 24
[RouterC-GigabitEthernet2/0/3] pim sm
[RouterC-GigabitEthernet2/0/3] igmp enable
[RouterC-GigabitEthernet2/0/3] quit
```

(3) 配置静态 RP。指定 IP 地址 10.13.1.4 为静态 RP 的 IP 地址

```
[RouterC] pim
[RouterC-pim] static-rp 10.13.1.4 bidir
```

(4) 使能双向 PIM

```
[RouterC-pim] bidir-pim enable
[RouterC-pim] quit
```

(5) 配置单播路由协议，以建立正确的单播路由表项

```
[RouterC] ospf 1
[RouterC-ospf-1] import-route direct
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

3.6 验证配置

(1) 按照如上配置后，查看配置信息发现 Router A、Router B 和 Router C 之间建立了 PIM 邻居关系。

查看 Router A 上的 PIM 邻居信息。

```
[RouterA] display pim neighbor
 Total Number of Neighbors = 2

 Neighbor        Interface          Uptime   Expires  DR-Priority Mode
 10.12.1.2       GE2/0/2            00:02:27 00:01:45 1           B
 10.13.1.3       GE2/0/3            00:02:27 00:01:19 1           B
```

查看 Router B 上的 PIM 邻居信息。

```
[RouterB] display pim neighbor
 Total Number of Neighbors = 2

 Neighbor        Interface          Uptime   Expires  DR-Priority Mode
 10.12.1.1       GE2/0/1            00:03:05 00:01:44 1           B
 10.23.1.3       GE2/0/3            00:13:49 00:01:29 1           B
```

查看 Router C 上的 PIM 邻居信息。

```
[RouterC] display pim neighbor
 Total Number of Neighbors = 2

 Neighbor        Interface          Uptime   Expires  DR-Priority Mode
 10.13.1.1       GE2/0/1            00:03:28 00:01:39 1           B
 10.23.1.2       GE2/0/2            00:14:05 00:01:36 1           B
```

(2) 通过使用 **display pim bsr-info** 命令可以查看 PIM-SM 域中的 BSR 信息。

查看 Router A 上 PIM-SM 域中的 BSR 信息。

```
[RouterA] display pim bsr-info
 Scope: non-scoped
     State: Elected
     Bootstrap timer: 00:01:18
     Elected BSR address: 10.12.1.1
       Priority: 64
       Hash mask length: 30
       Uptime: 00:04:01
     Candidate BSR address: 10.12.1.1
       Priority: 64
       Hash mask length: 30
```

查看 Router B 上 PIM-SM 域中的 BSR 信息。

```
[RouterB] display pim bsr-info
 Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:00:26
     Elected BSR address: 10.12.1.1
       Priority: 64
       Hash mask length: 30
```

```
      Uptime: 00:10:41
```

查看 Router C 上 PIM-SM 域中的 BSR 信息。

```
[RouterC] display pim bsr-info
 Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:02:08
     Elected BSR address: 10.12.1.1
       Priority: 64
       Hash mask length: 30
       Uptime: 00:15:41
```

(3) 通过使用 **display pim rp-info** 命令可以查看 PIM-SM 域中的 RP 信息。

查看 Router A 上所有组播组对应的 RP 信息。

```
[RouterA] display pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4 [B]
       RP address               Priority  HoldTime  Uptime    Expires
       10.12.1.1 (local)        192       180       00:06:01  00:02:58

 Static RP information:
       RP address               ACL   Mode    Preferred
       10.13.1.4                ----  bidir   No
```

查看 Router B 上所有组播组对应的 RP 信息。

```
[RouterB] display pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4 [B]
       RP address               Priority  HoldTime  Uptime    Expires
       10.12.1.1                192       180       00:06:33  00:02:26

 Static RP information:
       RP address               ACL   Mode    Preferred
       10.13.1.4                ----  bidir   No
```

查看 Router C 上所有组播组对应的 RP 信息。

```
[RouterC] display pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4 [B]
       RP address               Priority  HoldTime  Uptime    Expires
       10.12.1.1                192       180       00:06:51  00:02:05

Static RP information:
       RP address               ACL   Mode    Preferred
       10.13.1.4                ----  bidir   No
```

(4) 通过使用 **display pim df-info** 命令可以查看双向 PIM 的 DF 信息。

查看 Router A 上双向 PIM 的 DF 信息

```
[RouterA] display pim df-info
```

```
RP address: 10.12.1.1
 Interface           State   DF-Pref    DF-Metric  DF-Uptime DF-Address
 GE2/0/1             Win     0          0          00:01:09  10.10.1.1 (local)
 GE2/0/2             -       -          -          -         -
 GE2/0/3             Win     0          0          00:01:10  10.13.1.1 (local)

RP address: 10.13.1.4
 Interface           State   DF-Pref    DF-Metric  DF-Uptime DF-Address
 GE2/0/1             Win     0          0          00:00:07  10.10.1.1 (local)
 GE2/0/2             Win     0          0          00:00:07  10.12.1.1 (local)
 GE2/0/3             -       -          -          -         -
```

查看 Router B 上双向 PIM 的 DF 信息。

```
[RouterB] display pim df-info
RP address: 10.12.1.1
 Interface           State   DF-Pref    DF-Metric  DF-Uptime DF-Address
 GE2/0/1             -       -          -          -         -
 GE2/0/2             Win     0          0          00:01:46  10.23.1.2 (local)
 GE2/0/3             Win     0          0          00:01:45  10.101.1.1 (local)

RP address: 10.13.1.4
 Interface           State   DF-Pref    DF-Metric  DF-Uptime DF-Address
 GE2/0/1             Lose    0          0          00:00:44  10.12.1.1
 GE2/0/2             Lose    0          0          00:00:53  10.23.1.3
 GE2/0/3             Win     10         2          00:00:53  10.101.1.1 (local)
```

查看 Router C 上双向 PIM 的 DF 信息。

```
[RouterC] display pim df-info
RP address: 10.12.1.1
 Interface           State   DF-Pref    DF-Metric  DF-Uptime DF-Address
 GE2/0/3             Win     10         2          00:02:07  10.102.1.1 (local)
 GE2/0/4             Win     10         2          00:02:06  10.33.1.3 (local)
 GE2/0/1             Lose    0          0          00:02:07  10.13.1.1
 GE2/0/2             Lose    0          0          00:02:07  10.23.1.2

RP address: 10.13.1.4
 Interface           State   DF-Pref    DF-Metric  DF-Uptime DF-Address
 GE2/0/3             Win     0          0          00:01:24  10.102.1.1 (local)
 GE2/0/4             Win     0          0          00:01:23  10.33.1.3 (local)
 GE2/0/1             -       -          -          -         -
 GE2/0/2             Win     0          0          00:01:24  10.23.1.3 (local)
```

(5) 通过使用 **display multicast forwarding df-info** 命令可以查看组播转发的 DF 信息

查看 Router A 上组播转发的 DF 信息

```
[RouterA] display multicast forwarding df-info
Total 2 RPs, 2 matched

00001. RP address: 10.12.1.1
     Flags: 0x0
     Uptime: 00:02:42
```

```
     RPF interface: GigabitEthernet2/0/2
     List of 2 DF interfaces:
       1: GigabitEthernet2/0/1
       2: GigabitEthernet2/0/3

00002. RP address: 10.13.1.4
     Flags: 0x0
     Uptime: 00:01:41
     RPF interface: GigabitEthernet2/0/3
     List of 2 DF interfaces:
       1: GigabitEthernet2/0/1
       2: GigabitEthernet2/0/2
```

查看 Router B 上组播转发的 DF 信息。

```
[RouterB] display multicast forwarding df-info
Total 2 RPs, 2 matched

00001. RP address: 10.12.1.1
     Flags: 0x0
     Uptime: 00:03:18
     RPF interface: GigabitEthernet2/0/1
     List of 2 DF interfaces:
       1: GigabitEthernet2/0/2
       2: GigabitEthernet2/0/3

00002. RP address: 10.13.1.4
     Flags: 0x0
     Uptime: 00:02:24
     RPF interface: GigabitEthernet2/0/2
     List of 1 DF interfaces:
       1: GigabitEthernet2/0/3
```

查看 Router C 上组播转发的 DF 信息。

```
[RouterC] display multicast forwarding df-info
Total 2 RPs, 2 matched

00001. RP address: 10.12.1.1
     Flags: 0x0
     Uptime: 00:03:38
     RPF interface: GigabitEthernet2/0/2
     List of 2 DF interfaces:
       1: GigabitEthernet2/0/3
       2: GigabitEthernet2/0/4

00002. RP address: 10.13.1.4
     Flags: 0x0
     Uptime: 2d:18h
     RPF interface: GigabitEthernet2/0/1
     List of 3 DF interfaces:
       1: GigabitEthernet2/0/3
```

```
        2: GigabitEthernet2/0/4
        3: GigabitEthernet2/0/2
```

(6) Host A 和 Host B 指定加入组播组 G（225.1.1.1）后，Source 1 和 Source 2 都向组播组 225.1.1.1 发送组播信息，查看各路由器上的 PIM 路由表信息，可以看出（*，G）表项总数、PIM 的模式、入接口、上游邻居、RPF 邻居和下游接口信息。

查看 Router A 上的 PIM 路由表信息。

```
[RouterA] display pim routing-table
 Total 1 (*, G) entry; 0 (S, G) entry

 (*, 225.1.1.1)
     RP: 10.12.1.1 (local)
     Protocol: pim-bidir, Flag: WC LOC ACT
     UpTime: 00:21:59
     Upstream interface: GigabitEthernet2/0/2
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/0/2
             Protocol: pim-bidir, UpTime: 00:21:59, Expires: -
         2: GigabitEthernet2/0/3
             Protocol: pim-bidir, UpTime: 00:03:26, Expires: -
```

查看 Router B 上的 PIM 路由表信息。

```
[RouterB] display pim routing-table
 Total 1 (*, G) entry; 0 (S, G) entry

 (*, 225.1.1.1)
     RP: 10.12.1.1
     Protocol: pim-bidir, Flag: WC LOC ACT
     UpTime: 00:23:47
     Upstream interface: GigabitEthernet2/0/1
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 3
         1: GigabitEthernet2/0/1
             Protocol: pim-bidir, UpTime: 00:23:47, Expires: -
         2: GigabitEthernet2/0/2
             Protocol: pim-bidir, UpTime: 00:21:56, Expires: -
         3: GigabitEthernet2/0/3
             Protocol: igmp, UpTime: 00:23:47, Expires: -
```

查看 Router C 上的 PIM 路由表信息。

```
[RouterC] display pim routing-table
 Total 1 (*, G) entry; 0 (S, G) entry

 (*, 225.1.1.1)
     RP: 10.12.1.1
```

```
    Protocol: pim-bidir, Flag: WC ACT
    UpTime: 00:01:45
    Upstream interface: GigabitEthernet2/0/2
        Upstream neighbor: 10.23.1.2
        RPF prime neighbor: 10.23.1.2
    Downstream interface(s) information:
    Total number of downstreams: 2
        1: GigabitEthernet2/0/3
            Protocol: igmp, UpTime: 00:01:05, Expires: -
        2: GigabitEthernet2/0/2
            Protocol: pim-bidir, UpTime: 00:00:53, Expires: -
```

3.7 配置文件

- Router A：

```
#
ospf 1
 import-route direct
 area 0.0.0.0
  network 10.0.0.0 0.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.10.1.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.12.1.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/3
 port link-mode route
 ip address 10.13.1.1 255.255.255.0
 pim sm
#
multicast routing
#
pim
 c-bsr 10.12.1.1
 c-rp 10.12.1.1 bidir
 static-rp 10.13.1.4 bidir
 bidir-pim enable
#
```

- Router B：

```
#
ospf 1
 import-route direct
```

```
 area 0.0.0.0
  network 10.0.0.0 0.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 combo enable copper
 ip address 10.12.1.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/2
 port link-mode route
 combo enable copper
 ip address 10.23.1.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/3
 port link-mode route
 combo enable copper
 ip address 10.101.1.1 255.255.255.0
 pim sm
 igmp enable
#
multicast routing
#
pim
 static-rp 10.13.1.4 bidir
 bidir-pim enable
#
```

- Router C：

```
#
ospf 1
 import-route direct
 area 0.0.0.0
  network 10.0.0.0 0.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.13.1.3 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.23.1.3 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/3
 port link-mode route
 ip address 10.102.1.1 255.255.255.0
```

```
 pim sm
 igmp enable
#
interface GigabitEthernet2/0/4
 port link-mode route
 ip address 10.33.1.3 255.255.255.0
 pim sm
#
multicast routing
#
pim
 static-rp 10.13.1.4 bidir
 bidir-pim enable
#
```

4 相关资料

- H3C SR6600 SR6600-X 路由器 IP 组播配置指导-R7607
- H3C SR6600 SR6600-X 路由器 IP 组播命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

以太网链路聚合配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1

2 配置前提 1

3 三层链路聚合配置举例 1

3.1 组网需求 1

3.2 使用版本 1

3.3 配置注意事项 1

3.4 配置步骤 2

3.4.1 Device A 的配置 2

3.4.2 Device B 的配置 2

3.5 验证配置 2

3.6 配置文件 3

4 三层聚合负载分担配置举例 4

4.1 组网需求 4

4.2 使用版本 4

4.3 配置注意事项 4

4.4 配置步骤 5

4.4.1 Device A 的配置 5

4.4.2 Device B 的配置 5

4.5 验证配置 5

4.6 配置文件 6

5 端口聚合与 Cisco 互通配置举例 7

5.1 组网需求 7

5.2 配置思路 7

5.3 使用版本 7

5.4 配置注意事项 7

5.5 配置步骤 8

5.5.1 Device A 的配置 8

5.5.2 Device B 的配置 8

5.6 验证配置 8

5.7 配置文件 10

6 相关资料 11

1 简介

本文档介绍以太网链路聚合特性的配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

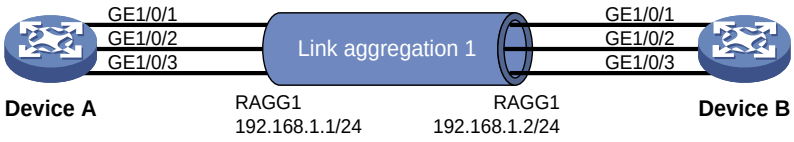
本文档假设您已了解以太网链路聚合特性。

3 三层链路聚合配置举例

3.1 组网需求

如图 1 所示，Device A 与 Device B 通过以太网链路互连。要求在 Device A 和 Device B 上分别配置三层链路聚合组，并为对应的三层聚合接口配置 IP 地址和子网掩码，从而提高两设备之间的带宽与可靠性。

图1　三层聚合配置示例图



3.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.3 配置注意事项

链路聚合分为静态聚合和动态聚合两种模式，用户可根据这两种模式的特点，结合具体组网情况选择其中一种进行配置。

- 静态聚合组在完成配置后，端口的选中/非选中状态不受网络环境的影响，比较稳定，但不能根据对端的状态调整成员端口的选中/非选中状态。
- 动态聚合组能够根据对端和本端的信息调整端口的选中/非选中状态，比较灵活，但其成员端口的选中/非选中状态容易受网络环境的影响。

3.4 配置步骤

3.4.1 Device A 的配置

创建三层聚合接口 1。（根据具体情况选择下面两种方式之一）

- 采用静态聚合模式

```
<DeviceA> system-view
[DeviceA] interface route-aggregation 1
```

- 采用动态聚合模式

```
<DeviceA> system-view
[DeviceA] interface route-aggregation 1
[DeviceA-Route-Aggregation1] link-aggregation mode dynamic
```

为三层聚合接口 1 配置 IP 地址和子网掩码。

```
[DeviceA-Route-Aggregation1] ip address 192.168.1.1 24
[DeviceA-Route-Aggregation1] quit
```

将接口 GigabitEthernet1/0/1～GigabitEthernet1/0/3 加入聚合组 1。

```
[DeviceA] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[DeviceA-if-range] port link-aggregation group 1
[DeviceA-if-range] quit
```

3.4.2 Device B 的配置

Device B 上的配置与 Device A 相同，配置过程略。

3.5 验证配置

通过 **display link-aggregation verbose** 命令来显示聚合组的相关信息，以验证配置是否成功。

- 采用静态聚合模式的聚合组信息

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status  Priority Oper-Key
--------------------------------------------------------------------------------
  GE1/0/1          S       32768    1
  GE1/0/2          S       32768    1
  GE1/0/3          S       32768    1
```

结果说明：本端加入到静态聚合组内的成员端口都处于 Selected 状态，与对端对应端口是否是 Selected 状态无关。

- 采用动态聚合模式的聚合组信息

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port             Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  GE1/0/1          S       32768    1         {ACDEF}
  GE1/0/2          S       32768    1         {ACDEF}
  GE1/0/3          S       32768    1         {ACDEF}
Remote:
  Actor            Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE1/0/1          1       32768    1         0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/2          2       32768    1         0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/3          3       32768    1         0x8000, 000f-e267-57ad {ACDEF}
```

结果说明：本端和对端设备上聚合组内的成员端口都处于 Selected 状态。原因是在动态链路聚合中通过 LACP 协议报文交互，可使两端聚合组内的成员端口选中状态达成一致，可顺利实现对用户数据的转发。

3.6 配置文件

- Device A：

```
#
```

  - 采用静态聚合模式

```
#
interface route-aggregation1
 ip address 192.168.1.1 255.255.255.0
#
```

  - 采用动态聚合模式

```
#
interface route-aggregation1
 ip address 192.168.1.1 255.255.255.0
 link-aggregation mode dynamic
#
interface GigabitEthernet1/0/1
 port link-mode route
 port link-aggregation group 1
#
```

```
interface GigabitEthernet1/0/2
 port link-mode route
 port link-aggregation group 1
#
interface GigabitEthernet1/0/3
 port link-mode route
 port link-aggregation group 1
#
```

- Device B：

Device B 上的配置文件与 Device A 类似。

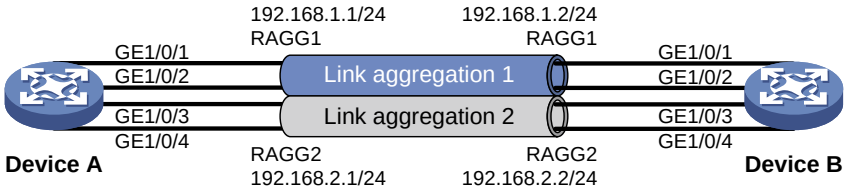
4 三层聚合负载分担配置举例

4.1 组网需求

如图 2 所示：

- Device A 与 Device B 通过各自的三层以太网接口 GigabitEthernet1/0/1～GigabitEthernet1/0/4 相互连接。
- 在 Device A 和 Device B 上分别配置两个三层静态链路聚合组，并为对应的三层聚合接口都配置 IP 地址和子网掩码。
- 通过在聚合组 1 上按照源 IP 地址进行聚合负载分担、在聚合组 2 上按照目的 IP 地址进行聚合负载分担的方式，来实现数据流量在各成员端口间的负载分担。

图2 三层聚合负载分担配置组网图



4.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.3 配置注意事项

聚合负载分担类型支持全局配置或在聚合组内配置两种方式；对于一个聚合组来说，优先采用该聚合组内的配置。本例在聚合组内配置。

4.4 配置步骤

4.4.1 Device A 的配置

创建三层聚合接口 1，配置该接口对应的聚合组内按照源 IP 地址进行聚合负载分担，并为其配置 IP 地址和子网掩码。

```
<DeviceA> system-view
[DeviceA] interface route-aggregation 1
[DeviceA-Route-Aggregation1] link-aggregation load-sharing mode source-ip
[DeviceA-Route-Aggregation1] ip address 192.168.1.1 24
[DeviceA-Route-Aggregation1] quit
```

创建三层聚合接口 2，配置该接口对应的聚合组内按照目的 IP 地址进行聚合负载分担，并为其配置 IP 地址和子网掩码。

```
[DeviceA] interface route-aggregation 2
[DeviceA-Route-Aggregation2] link-aggregation load-sharing mode destination-ip
[DeviceA-Route-Aggregation2] ip address 192.168.2.1 24
[DeviceA-Route-Aggregation2] quit
```

将接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 加入聚合组 1，接口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 加入聚合组 2。

```
[DeviceA] interface range gigabitethernet 1/0/1 gigabitethernet 1/0/2
[DeviceA-if-range] port link-aggregation group 1
[DeviceA-if-range] quit
[DeviceA] interface range gigabitethernet 1/0/3 gigabitethernet 1/0/4
[DeviceA-if-range] port link-aggregation group 2
[DeviceA-if-range] quit
```

4.4.2 Device B 的配置

Device B 的配置与 Device A 相同，配置过程略。

4.5 验证配置

查看 Device A 上所有聚合组的详细信息。

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status  Priority Oper-Key
--------------------------------------------------------------------------------
  GE1/0/1          S       32768    1
  GE1/0/2          S       32768    1
```

```
Aggregate Interface: Route-Aggregation2
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status  Priority Oper-Key
--------------------------------------------------------------------------------
  GE1/0/3          S       32768    2
  GE1/0/4          S       32768    2
```

以上信息表明，聚合组 1 和聚合组 2 都是负载分担类型的三层静态聚合组，各包含有两个选中端口。

查看 Device A 上所有聚合接口所对应聚合组内采用的聚合负载分担类型。

```
[DeviceA] display link-aggregation load-sharing mode interface
Route-Aggregation1 Load-Sharing Mode:
source-ip address

Route-Aggregation2 Load-Sharing Mode:
destination-ip address
```

以上信息表明，三层聚合组 1 按照报文的源 IP 地址进行聚合负载分担，三层聚合组 2 按照报文的目的 IP 地址进行聚合负载分担。

4.6 配置文件

- Device A：

```
#
interface Route-Aggregation1
 ip address 192.168.1.1 255.255.255.0
 link-aggregation load-sharing mode source-ip
#
interface Route-Aggregation2
 ip address 192.168.2.1 255.255.255.0
 link-aggregation load-sharing mode destination-ip
#
interface GigabitEthernet1/0/1
 port link-mode route
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-mode route
 port link-aggregation group 1
#
interface GigabitEthernet1/0/3
 port link-mode route
 port link-aggregation group 2
#
interface GigabitEthernet1/0/4
 port link-mode route
 port link-aggregation group 2
#
```

- Device B：

Device B 上的配置文件与 Device A 类似。

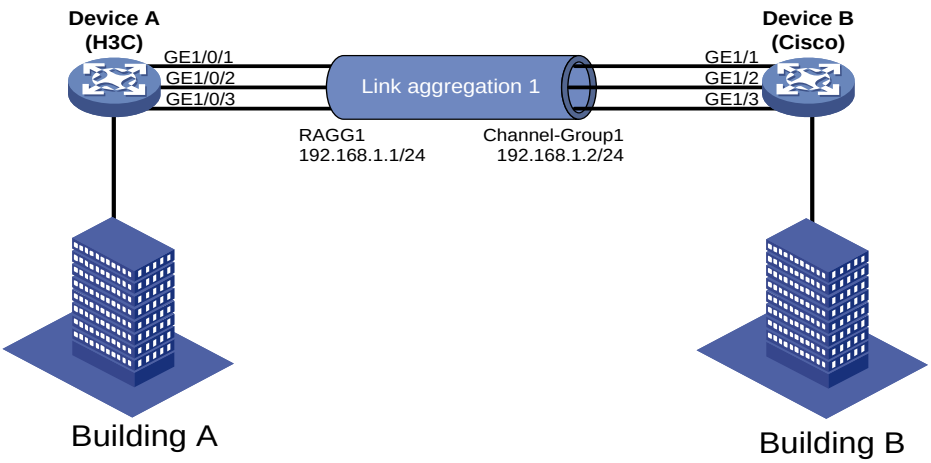
5 端口聚合与 Cisco 互通配置举例

5.1 组网需求

如图 3 所示：

- 两个楼宇之间分别使用 H3C Device A（简称 Device A）与 Cisco Device B（简称 Device B）通过各自的三层以太网接口相互连接。
- 为提高设备间链路带宽与可靠性，并考虑不同厂商设备互联的兼容性，配置动态链路聚合，在 Device A 和 Device B 上分别配置三层链路聚合组，并为对应的三层聚合接口配置 IP 地址和子网掩码。

图3 三层链路聚合配置示例图



5.2 配置思路

- Device A：创建三层聚合接口，配置该接口为动态聚合模式。将端口加入到聚合接口中。
- Device B：创建通道组，配置封装协议为 LACP，并配置 LACP 工作模式为主动(Active)。

5.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

5.4 配置注意事项

- 由于静态聚合组中端口选中状态不受对端端口是否在聚合组中及是否处于选中状态的影响。这样有可能导致两端设备所确定的 Selected 状态端口不一致，当两端都支持配置静态和动态聚合组的情况下，建议用户优选动态聚合组。

- 对于 Cisco 设备，需配置通道组为 LACP 协议，并将通道组类型配置为 Active。关于更多通道组端口状态请查阅 Cisco 相关资料。

5.5 配置步骤

5.5.1 Device A 的配置

创建三层聚合接口 1，并采用动态聚合模式。

```
<DeviceA> system
[DeviceA] interface route-aggregation 1
[DeviceA-Route-Aggregation1] link-aggregation mode dynamic
```

为三层聚合接口 1 配置 IP 地址和子网掩码。

```
[DeviceA-Route-Aggregation1] ip address 192.168.1.1 24
[DeviceA-Route-Aggregation1] quit
```

将接口 GigabitEthernet1/0/1～GigabitEthernet1/0/3 加入聚合组 1。

```
[DeviceA] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[DeviceA-if-range] port link-aggregation group 1
[DeviceA-if-range] quit
```

5.5.2 Device B 的配置

为端口通道接口 1 配置 IP 地址和子网掩码。

```
DeviceB>enable
DeviceB#configure terminal
DeviceB(config)#interface port-channel 1
DeviceB(config-if)#ip address 192.168.1.2 255.255.255.0
```

将通道协议模式配置为 LACP（缺省为 PagP 模式）。

```
DeviceB(config-if)#channel-protocol lacp
DeviceB(config-if)#exit
```

进入以太网接口视图。

```
DeviceB(config)#interface range gigabitethernet 1/1 – 3
```

#将端口批量加入通道组。

```
DeviceB(config-if-range)#no switchport
DeviceB(config-if-range)#channel-group 1 mode active
DeviceB(config-if-range)#exit
```

5.6 验证配置

(1) Device A

通过 **display link-aggregation verbose** 命令来显示聚合组的相关信息，以验证配置是否成功。

```
 [DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
```

```
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port             Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  GE1/0/1          S       32768    1         {ACDEF}
  GE1/0/2          S       32768    1         {ACDEF}
  GE1/0/3          S       32768    1         {ACDEF}
Remote:
  Actor            Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE1/0/1          1       32768    1         0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/2          2       32768    1         0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/3          3       32768    1         0x8000, 000f-e267-57ad {ACDEF}
```

结果说明：本端和对端设备上聚合组内的成员端口都处于 Selected 状态。原因是在动态链路聚合中通过 LACP 协议报文交互，可使两端聚合组内的成员端口选中状态达成一致，可顺利实现对用户数据的转发。

(2) Device B

通过 **show etherchannel summary** 与 show etherchannel port-channel 命令来显示端口聚合的简要信息，以验证配置是否成功。

```
DeviceB#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)           LACP   Gi1/1(P) Gi1/2(P) Gi1/3(P)
DeviceB#show etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 1
```

```
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po1    (Primary Aggregator)
------------

Age of the Port-channel   = 00d:00h:26m:35s
Logical slot/port   = 2/1       Number of ports = 3
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel
Protocol            =   LACP
Port Security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi1/1    Active             0
  0     00     Gi1/2    Active             0
  0     00     Gi1/3    Active             0
Time since last port bundled:    00d:00h:12m:13s    Gi0/2
```

5.7 配置文件

- Device A：

```
#
interface route-aggregation1
 ip address 192.168.1.1 255.255.255.0
 link-aggregation mode dynamic
#
interface GigabitEthernet1/0/1
 port link-mode route
port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-mode route
port link-aggregation group 1
#
interface GigabitEthernet1/0/3
 port link-mode route
port link-aggregation group 1
#
```

- Device B：

```
Building configuration...

Current configuration : 1444 bytes
!
```

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
!
!
!
interface GigabitEthernet1/1
 no switchport
 channel-protocol lacp
 channel-group 1 mode active
!
interface GigabitEthernet1/2
 no switchport
 channel-protocol lacp
 channel-group 1 mode active
!
interface GigabitEthernet1/3
 no switchport
 channel-group 1 mode active
!
interface Port-channel 1
 no switchport
 channel-protocol lacp
 ip address 192.168.1.2 255.255.255.0
略
```

6 相关资料

- H3C SR6600 SR6600-X 路由器 二层技术-以太网交换配置指导-R7607
- H3C SR6600 SR6600-X 路由器 二层技术-以太网交换命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

以太网 OAM 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 配置举例 1
3.1 组网需求 1
3.2 配置思路 1
3.3 使用版本 2
3.4 配置注意事项 2
3.5 配置步骤 2
3.5.1 Device A 的配置 2
3.5.2 Device B 的配置 2
3.6 验证配置 2
3.7 配置文件 4
4 相关资料 4

1 简介

本文档介绍了使用以太网 OAM 监控链路性能的典型配置举例。

以太网 OAM 是一种监控网络故障的工具，可以监控两台直连设备之间的链路状态。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解以太网 OAM 特性。

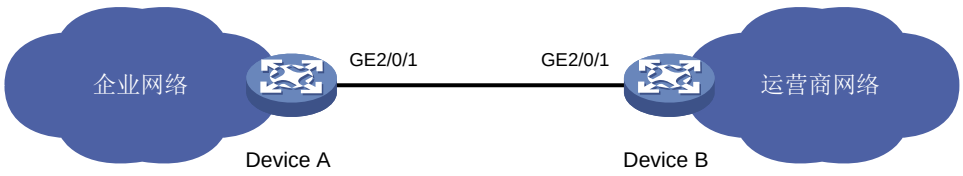
3 配置举例

3.1 组网需求

如图 1 所示，企业网络和运营商网络通过各自边缘设备 Device A 和 Device B 进行相连。使用以太网 OAM 功能，监控 Device A 和 Device B 间链路的状态，从而可确定运营商所提供的网络链路可靠性是否符合与企业用户签订的 SLA（Service Level Agreement），具体需求：

- 实现自动检测 Device A 和 Device B 之间链路的连通性；
- 网络管理员可以查看是否 Device A 和 Device B 之间链路是否发生紧急链路事件；
- 网络管理员可以通过观察一般链路事件统计信息动态地了解链路状态。

图1 以太网 OAM 组网示意图



3.2 配置思路

为了在 Device A 和 Device B 之间链路上成功建立以太网 OAM 连接，至少需要保证链路两端至少有一个接口的以太网 OAM 的连接模式为 Active 模式。由于本设备的所有接口的以太网 OAM 的连接模式缺省情况为 Active 模式，所以可以省去此配置。本案例以在 Device A 的 XGE2/0/1 上配置以太网 OAM 的连接模式为 Active 模式，在 Device B 的 XGE2/0/1 上配置以太网 OAM 的连接模式为 Passive 模式为例。

以太网 OAM 功能可以监控的一般链路事件包括错误信号事件、错误帧事件、错误帧周期事件及错误帧秒事件。缺省情况下，开启了以太网 OAM 功能的接口的一般链路事件检测参数均采用全局配置，您可以根据实际网络情况对其中某些事件的检测参数进行修改，以满足您对这些事件的检测精度。本案例以对错误帧事件的检测参数进行修改为例。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置注意事项

不允许在已使能以太网 OAM 功能的接口上更改以太网 OAM 的连接模式。如需更改，请先关闭该接口上的以太网 OAM 功能。

3.5 配置步骤

3.5.1 Device A 的配置

配置接口 Ten-GigabitEthernet2/0/1 的以太网 OAM 的连接模式为 Active 模式（缺省情况下，所有接口的以太网 OAM 的连接模式都为 Active 模式），并开启以太网 OAM 功能。

```
<DeviceA> system-view
[DeviceA] interface ten-gigabitethernet 2/0/1
[DeviceA-Ten-GigabitEthernet2/0/1] undo shutdown
[DeviceA-Ten-GigabitEthernet2/0/1] oam mode active
[DeviceA-Ten-GigabitEthernet2/0/1] oam enable
```

在接口 Ten-GigabitEthernet2/0/1 上配置错误帧事件的检测窗口为 20000 毫秒，检测阈值为 10 次。

```
[DeviceA-Ten-GigabitEthernet2/0/1] oam errored-frame window 200
[DeviceA-Ten-GigabitEthernet2/0/1] oam errored-frame threshold 10
[DeviceA-Ten-GigabitEthernet2/0/1] quit
```

3.5.2 Device B 的配置

配置接口 Ten-GigabitEthernet2/0/1 的以太网 OAM 的连接模式为 Passive 模式，并开启以太网 OAM 功能。

```
<DeviceB> system-view
[DeviceB] interface ten-gigabitethernet 2/0/1
[DeviceB-Ten-GigabitEthernet2/0/1] undo shutdown
[DeviceB-Ten-GigabitEthernet2/0/1] oam mode passive
[DeviceB-Ten-GigabitEthernet2/0/1] oam enable
[DeviceB-Ten-GigabitEthernet2/0/1] quit
```

3.6 验证配置

显示 Device A 上的全局以及未采用缺省配置的接口上的以太网 OAM 配置信息。

```
[DeviceA] display oam configuration
---------------- [Global] ----------------
 OAM timers
   Hello timer        : 1000 milliseconds
   Keepalive timer    : 5000 milliseconds
 Link monitoring
   Errored symbol period
     Window           : 100 x 1000000 symbols
```

```
    Threshold        : 1 error symbols
  Errored frame
    Window           : 10 x 100 milliseconds
    Threshold        : 1 error frames
  Errored frame period
    Window           : 1000 x 10000 frames
    Threshold        : 1 error frames
  Errored frame seconds
    Window           : 600 x 100 milliseconds
    Threshold        : 1 error seconds

----------- [Ten-GigabitEthernet2/0/1] -----------
 OAM timers
  Hello timer        : 1000 milliseconds
  Keepalive timer    : 5000 milliseconds
 Link monitoring
  Errored symbol period
    Window           : 100 x 1000000 symbols
    Threshold        : 1 error symbols
  Errored frame
    Window           : 200 x 100 milliseconds
    Threshold        : 10 error frames
  Errored frame period
    Window           : 1000 x 10000 frames
    Threshold        : 1 error frames
  Errored frame seconds
    Window           : 600 x 100 milliseconds
    Threshold        : 1 error seconds
```

显示 Device A 上以太网 OAM 的紧急链路事件统计信息。

```
[DeviceA] display oam critical-event
----------- [Ten-GigabitEthernet2/0/1] -----------
 Local link status   : UP
 Event statistics
  Link fault         : Not occurred
  Dying gasp         : Not occurred
  Critical event     : Not occurred
```

以上信息表明：Device A 与 Device B 之间的链路连通正常，尚未发生任何紧急链路事件。

通过 Device A 显示本端的一般链路事件统计信息。

```
[DeviceA] display oam link-event local
----------- [Ten-GigabitEthernet2/0/1] -----------
 Link status: UP
 OAM local errored frame event
  Event time stamp        : 5789 x 100 milliseconds
  Errored frame window    : 200 x 100 milliseconds
  Errored frame threshold : 10 error frames
  Errored frame           : 13 error frames
  Error running total     : 350 error frames
  Event running total     : 17 events
```

上面的显示信息表明从 OAM 连接建立后，Device A 上总共发生了 350 次错误帧，其中错误帧事件有 17 次，链路的性能不稳定。

说明

当链路检测结果为链路性能不稳定，请咨询 H3C 技术支援人员。

3.7 配置文件

- Device A

```
#
interface Ten-GigabitEthernet2/0/1
 port link-mode bridge
 oam errored-frame window 200
 oam errored-frame threshold 10
 oam enable
```

- Device B

```
#
interface Ten-GigabitEthernet2/0/1
 port link-mode bridge
 oam mode passive
 oam enable
```

4 相关资料

- H3C SR6600 SR6600-X 路由器 可靠性配置指导-R7607
- H3C SR6600 SR6600-X 路由器 可靠性命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

帧中继配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
2.1 组网需求 1
2.2 配置思路 1
2.3 使用版本 2
2.4 配置注意事项 2
2.5 配置步骤 2
2.5.1 配置 Device A 2
2.5.2 配置 Device B 2
2.5.3 配置 Device C 3
2.6 验证配置 3
2.7 配置文件 4
3 相关资料 5

1 简介

本文档介绍了帧中继网络互连局域网的典型配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

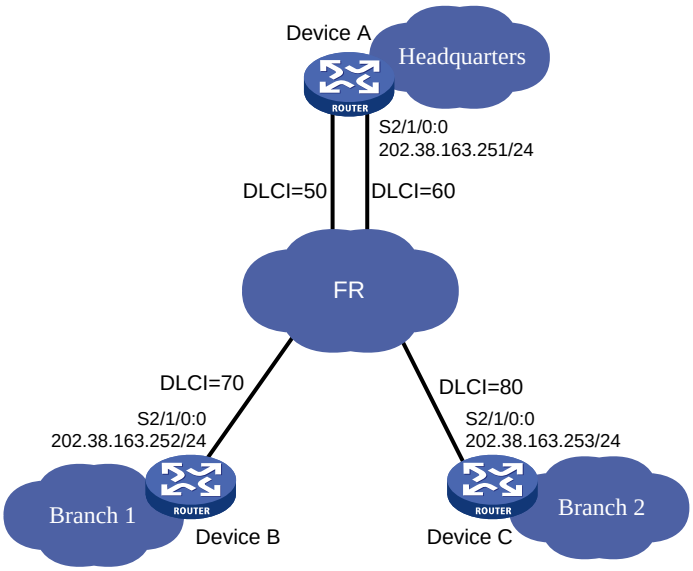
本文假设您已了解帧中继特性。

2.1 组网需求

如图 1 所示，公司总部和分支机构通过帧中继网络相连，帧中继网络与 Device A 相连的 2 条虚电路 DLCI 分别为 50 和 60，与 Device B 相连的虚电路 DLCI 为 70，与 Device C 相连的虚电路 DLCI 为 80。

要求实现：Device A 可以通过帧中继网络分别与 Device B、Device C 通信。

图1 通过帧中继网络互连局域网配置组网图



2.2 配置思路

- 由于 DTE 是终端设备，DCE 是网络设备，所以帧中继网络中的设备工作在帧中继的 DCE 方式，Device A、Device B、Device C 只能工作在帧中继的 DTE 方式。
- 为防止网络拓扑变化，选择运行 InARP 动态建立各路由器上接口 Serial2/1/0:0 的帧中继地址映射。

2.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

2.4 配置注意事项

- 当帧中继接口类型是 DCE 或 NNI 时，需要为接口（不论是主接口还是子接口）手动创建虚电路。
- 当帧中继接口类型是 DTE 时，如果接口是主接口，则系统会根据对端设备自动确定虚电路，也可以手工配置虚电路；如果是子接口，则必须手动为接口指定虚电路。
- 如果要在 DTE 侧手工配置虚电路，则配置的虚电路号必须与相连的 DCE 侧保持一致。
- 虚电路号在一个主接口及其所有子接口上是唯一的。

2.5 配置步骤

2.5.1 配置 Device A

配置接口 Serial2/1/0:0 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface Serial 2/1/0:0
[DeviceA-Serial2/1/0:0] ip address 202.38.163.251 255.255.255.0
```

封装接口 Serial2/1/0:0 的链路层协议为帧中继。

```
[DeviceA-Serial2/1/0:0] link-protocol fr
```

配置帧中继接口类型为 DTE（缺省为该类型）。

```
[DeviceA-Serial2/1/0:0] fr interface-type dte
```

配置动态建立帧中继地址映射，即允许接口 Serial2/1/0:0 上的所有虚电路上都进行逆向地址解析（缺省帧中继 InARP 功能处于使能状态）。

```
[DeviceA-Serial2/1/0:0] fr inarp ip
```

2.5.2 配置 Device B

配置接口 Serial2/1/0:0 的 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface Serial 2/1/0:0
[DeviceB-Serial2/1/0:0] ip address 202.38.163.252 255.255.255.0
```

封装接口 Serial2/1/0:0 的链路层协议为帧中继。

```
[DeviceB-Serial2/1/0:0] link-protocol fr
```

配置帧中继接口类型为 DTE（缺省为该类型）。

```
[DeviceB-Serial2/1/0:0] fr interface-type dte
```

配置动态建立帧中继地址映射，即允许接口 Serial2/1/0:0 上的所有虚电路上都进行逆向地址解析（缺省帧中继 InARP 功能处于使能状态）。

```
[DeviceB-Serial2/1/0:0] fr inarp ip
```

2.5.3 配置 Device C

配置接口 Serial2/1/0:0 的 IP 地址。

```
<DeviceC> system-view
[DeviceC] interface Serial 2/1/0:0
[DeviceC-Serial2/1/0:0] ip address 202.38.163.253 255.255.255.0
```

封装接口 Serial2/1/0:0 的链路层协议为帧中继。

```
[DeviceC-Serial2/1/0:0] link-protocol fr
```

配置帧中继接口类型为 DTE（缺省为该类型）。

```
[DeviceC-Serial2/1/0:0] fr interface-type dte
```

配置动态建立帧中继地址映射，即允许接口 Serial2/1/0:0 上的所有虚电路上都进行逆向地址解析（缺省帧中继 InARP 功能处于使能状态）。

```
[DeviceC-Serial2/1/0:0] fr inarp ip
```

2.6 验证配置

(1) 查看各帧中继接口的信息。

在 Device A 上查看帧中继 InARP 报文统计信息。

```
<DeviceA> display fr inarp
Frame relay InARP statistics for interface Serial2/1/0:0 (DTE)
  Recvd InARP request  Sent InARP reply  Sent InARP request  Recvd InARP reply
  0                    0                 0                  0
```

在 Device B 上查看帧中继 InARP 报文统计信息。

```
<DeviceB> display fr inarp
Frame relay InARP statistics for interface Serial2/1/0:0 (DTE)
  Recvd InARP request  Sent InARP reply  Sent InARP request  Recvd InARP reply
  0                    0                 0                  0
```

在 Device C 上查看帧中继 InARP 报文统计信息。

```
<DeviceC> display fr inarp
Frame relay InARP statistics for interface Serial2/1/0:0 (DTE)
  Recvd InARP request  Sent InARP reply  Sent InARP request  Recvd InARP reply
  0                    0                 0                  0
```

(2) Device A 可以分别与 Device B、Device C 互相 Ping 通。

在 Device A 上 Ping Device B 对端接口的 IP 地址。

```
<DeviceA> ping 202.38.163.252
  PING 202.38.163.252: 56   data bytes, press CTRL_C to break
    Reply from 202.38.163.252: bytes=56 Sequence=1 ttl=252 time=8 ms
    Reply from 202.38.163.252: bytes=56 Sequence=2 ttl=252 time=7 ms
    Reply from 202.38.163.252: bytes=56 Sequence=3 ttl=252 time=7 ms
    Reply from 202.38.163.252: bytes=56 Sequence=4 ttl=252 time=6 ms
    Reply from 202.38.163.252: bytes=56 Sequence=5 ttl=252 time=7 ms

  --- 202.38.163.252  ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
```

```
round-trip min/avg/max = 6/7/8 ms
```

在 Device B 上 Ping Device A 对端接口的 IP 地址。

```
<DeviceB> ping 202.38.163.251
  PING 202.38.163.251: 56   data bytes, press CTRL_C to break
    Reply from 202.38.163.251: bytes=56 Sequence=1 ttl=252 time=8 ms
    Reply from 202.38.163.251: bytes=56 Sequence=2 ttl=252 time=7 ms
    Reply from 202.38.163.251: bytes=56 Sequence=3 ttl=252 time=7 ms
    Reply from 202.38.163.251: bytes=56 Sequence=4 ttl=252 time=6 ms
    Reply from 202.38.163.251: bytes=56 Sequence=5 ttl=252 time=7 ms

  --- 202.38.163.251  ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 6/7/8 ms
```

在 Device A 上 Ping Device C 对端接口的 IP 地址。

```
<DeviceA> ping 202.38.163.253
  PING 202.38.163.253: 56   data bytes, press CTRL_C to break
    Reply from 202.38.163.253: bytes=56 Sequence=1 ttl=252 time=7 ms
    Reply from 202.38.163.253: bytes=56 Sequence=2 ttl=252 time=7 ms
    Reply from 202.38.163.253: bytes=56 Sequence=3 ttl=252 time=8 ms
    Reply from 202.38.163.253: bytes=56 Sequence=4 ttl=252 time=7 ms
    Reply from 202.38.163.253: bytes=56 Sequence=5 ttl=255 time=6 ms

  --- 202.38.163.253  ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 6/7/8 ms
```

在 Device C 上 Ping Device A 对端接口的 IP 地址。

```
<DeviceA> ping 202.38.163.251
  PING 202.38.163.251: 56   data bytes, press CTRL_C to break
    Reply from 202.38.163.251: bytes=56 Sequence=1 ttl=252 time=7 ms
    Reply from 202.38.163.251: bytes=56 Sequence=2 ttl=252 time=7 ms
    Reply from 202.38.163.251: bytes=56 Sequence=3 ttl=252 time=8 ms
    Reply from 202.38.163.251: bytes=56 Sequence=4 ttl=252 time=7 ms
    Reply from 202.38.163.251: bytes=56 Sequence=5 ttl=255 time=6 ms

  --- 202.38.163.251  ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 6/7/8 ms
```

2.7 配置文件

- Device A：

```
#
interface Serial2/1/0:0
 link-protocol fr
 fr interface-type dte
 fr inarp ip
 ip address 202.38.163.251 255.255.255.0
#
```

- Device B：

```
#
interface Serial2/1/0:0
 link-protocol fr
 fr interface-type dte
 fr inarp ip
 ip address 202.38.163.252 255.255.255.0
#
```

- Device C：

```
#
interface Serial2/1/0:0
 link-protocol fr
 fr interface-type dte
 fr inarp ip
 ip address 202.38.163.253 255.255.255.0
#
```

3 相关资料

- H3C SR6600 SR6600-X 路由器 二层技术-广域网接入配置指导-R7607
- H3C SR6600 SR6600-X 路由器 二层技术-广域网接入命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

组播 VPN 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1

2 配置前提 1

3 单 AS 内 MDT 模式 MVPN 配置举例 1

3.1 组网需求 1

3.2 配置思路 2

3.3 使用版本 2

3.4 配置注意事项 2

3.5 配置步骤 2

3.5.1 配置各设备接口 IP 地址 2

3.5.2 配置路由及基本 MPLS L3VPN 2

3.5.3 配置组播路由相关功能及 MDT 模式 MVPN 2

3.6 验证配置 5

3.7 配置文件 6

4 A 类跨 AS 的 MDT 模式 MVPN 配置举例 8

4.1 组网需求 8

4.2 配置思路 9

4.3 使用版本 9

4.4 配置注意事项 9

4.5 配置步骤 10

4.5.1 配置各设备接口 IP 地址 10

4.5.2 配置路由和 OptionA 方式的跨域 MPLS L3VPN 10

4.5.3 配置组播路由相关功能及 MDT 模式 MVPN 10

4.6 验证配置 14

4.7 配置文件 15

5 C 类跨 AS 的 MDT 模式 MVPN 配置举例 18

5.1 组网需求 18

5.2 配置思路 19

5.3 使用版本 19

5.4 配置步骤 19

5.4.1 配置各设备接口 IP 地址 19

5.4.2 配置路由和 OptionC 方式的跨域 MPLS L3VPN 20

5.4.3 配置组播路由相关功能及 MDT 模式 MVPN 20

5.5 验证配置 24
5.6 配置文件 24
6 相关资料 28

1 简介

本文档介绍组播 VPN 的典型配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

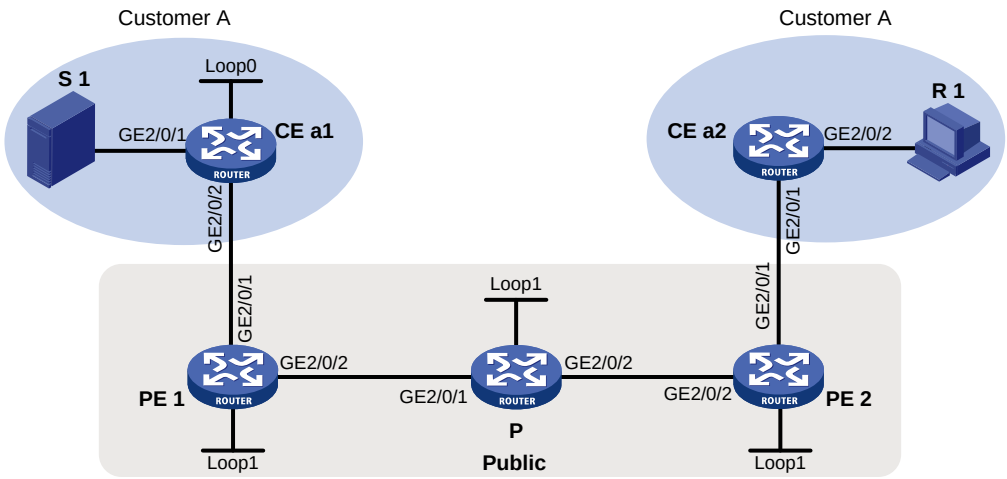
本文档假设您已了解组播 VPN 特性。

3 单 AS 内 MDT 模式 MVPN 配置举例

3.1 组网需求

如图 1 所示，Customer A 有位于两地的分支机构，这两个分支机构已通过同一个运营商的 MPLS L3VPN 网络实现了两地间单播路由信息的正常交互。目前 Customer A 中的组播源与接收者分别位于不同的分支机构中，且各分支机构内运行的 PIM 协议模式为 PIM-SM。现要求通过 MDT 模式 MVPN 技术，实现组播接收者能够正常接收到组播源发来的组播数据。

图1 配置单 AS 内 MDT 模式 MVPN 组网图



设备	接口	IP地址	设备	接口	IP地址
S 1	-	10.11.3.2/24	PE 2	GE2/0/2	192.168.2.2/24
PE 1	GE2/0/2	192.168.1.2/24		GE2/0/1	10.11.2.1/24
	GE2/0/1	10.11.1.1/24		Loop1	1.1.1.2/32
	Loop1	1.1.1.1/32	CE a1	GE2/0/1	10.11.3.1/24
P	GE2/0/1	192.168.1.1/24		GE2/0/2	10.11.1.2/24
	GE2/0/2	192.168.2.1/24		Loop0	2.2.2.2/32
	Loop1	3.3.3.3/32	CE a2	GE2/0/2	10.11.4.1/24
R 1	-	10.11.4.2/24		GE2/0/1	10.11.2.2/24

3.2 配置思路

为了实现上述组网需求，需要在公网的各设备上运行 PIM 协议（与私网中的 PIM 协议模式相互独立），并在各 PE 设备上配置 MDT 模式 MVPN。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置注意事项

- 配置 MDT 模式 MVPN 时，只有在指定了 Default-Group 和 MVPN 源接口，并获取到 MVPN 源接口的公网 IP 地址之后，MTI 才会生效。
- 属于同一 VPN 的所有接口（包括 PE 上绑定 VPN 实例的接口）上必须运行相同模式的 PIM 协议。
- 在不同的 PE 上，应该为相同 MDT 模式 MVPN 实例指定相同的 Default-Group。
- MVPN 源接口必须与建立 BGP 对等体时所使用的源接口相同，否则将无法获取正确的路由信息。

3.5 配置步骤

3.5.1 配置各设备接口 IP 地址

按图 1 配置各设备上的接口 IP 地址和子网掩码。

```
<CEa1> system-view
[CEa1] interface gigabitethernet 2/0/1
[CEa1-GigabitEthernet2/0/1] ip address 10.11.3.1 24
[CEa1-GigabitEthernet2/0/1] quit
[CEa1] interface loopback 0
[CEa1-LoopBack0] ip address 2.2.2.2 32
[CEa1-LoopBack0] quit
[CEa1] interface gigabitethernet 2/0/2
[CEa1-GigabitEthernet2/0/2] ip address 10.11.1.2 24
[CEa1-GigabitEthernet2/0/2] quit
```

PE 1、P、PE 2 和 CE a2 的配置与 CE a1 相似，配置过程略。

3.5.2 配置路由及基本 MPLS L3VPN

配置路由协议及基本 MPLS L3VPN，实现两地间单播路由信息互通。具体配置请参见“MPLS 配置指导”中的“MPLS L3VPN”。

3.5.3 配置组播路由相关功能及 MDT 模式 MVPN

(1) 在公网实例中使能 IP 组播路由、公网接口上配置 PIM-SM 功能（包括 LoopBack 接口）

在 PE 1 上使能 IP 组播路由，在公网接口上配置 PIM-SM。

```
<PE1> system-view
[PE1] multicast routing
[PE1-mrib] quit
[PE1] interface gigabitethernet 2/0/2
[PE1-GigabitEthernet2/0/2] pim sm
[PE1-GigabitEthernet2/0/2] quit
[PE1] interface loopback 1
[PE1-LoopBack1] pim sm
[PE1-LoopBack1] quit
```

在 P 上使能 IP 组播路由，在公网接口上配置 PIM-SM，并将 LoopBack 1 接口指定为公网的 C-BSR 和 C-RP，其中 C-RP 服务于公网实例中所有组播组。

```
<P> system-view
[P] multicast routing
[P-mrib] quit
[P] interface gigabitethernet 2/0/1
[P-GigabitEthernet2/0/1] pim sm
[P-GigabitEthernet2/0/1] quit
[P] interface gigabitethernet 2/0/2
[P-GigabitEthernet2/0/2] pim sm
[P-GigabitEthernet2/0/2] quit
[P] interface loopback 1
[P-LoopBack1] pim sm
[P-LoopBack1] quit
[P] pim
[P-pim] c-bsr 3.3.3.3
[P-pim] c-rp 3.3.3.3
[P-pim] quit
```

在 PE 2 上使能 IP 组播路由，在公网接口上配置 PIM-SM。

```
<PE2> system-view
[PE2] multicast routing
[PE2-mrib] quit
[PE2] interface gigabitethernet 2/0/2
[PE2-GigabitEthernet2/0/2] pim sm
[PE2-GigabitEthernet2/0/2] quit
[PE2] interface loopback 1
[PE2-LoopBack1] pim sm
[PE2-LoopBack1] quit
```

(2) 在 VPN 私网实例中使能 IP 组播路由、私网接口上配置 PIM-SM 功能，并在连接有接收者的 CE 上配置 IGMP

在 CE a1 上使能 IP 组播路由，在各接口上配置 PIM-SM，并将 LoopBack 0 接口指定为私网的 C-BSR 和 C-RP，其中 C-RP 服务于 Customer A 实例中所有组播组。

```
<CEa1> system-view
[CEa1] multicast routing
[CEa1-mrib] quit
[CEa1] interface gigabitethernet 2/0/1
[CEa1-GigabitEthernet2/0/1] pim sm
```

```
[CEa1-GigabitEthernet2/0/1] quit
[CEa1] interface gigabitethernet 2/0/2
[CEa1-GigabitEthernet2/0/2] pim sm
[CEa1-GigabitEthernet2/0/2] quit
[CEa1] interface loopback 0
[CEa1-LoopBack0] pim sm
[CEa1-LoopBack0] quit
[CEa1] pim
[CEa1-pim] c-bsr 2.2.2.2
[CEa1-pim] c-rp 2.2.2.2
[CEa1-pim] quit
```

在 CE a2 上使能 IP 组播路由，在连接有接收者的接口上使能 IGMP，其余各接口上配置 PIM-SM。

```
<CEa2> system-view
[CEa2] multicast routing
[CEa2-mrib] quit
[CEa2] interface gigabitethernet 2/0/1
[CEa2-GigabitEthernet2/0/1] pim sm
[CEa2-GigabitEthernet2/0/1] quit
[CEa2] interface gigabitethernet 2/0/2
[CEa2-GigabitEthernet2/0/2] igmp enable
[CEa2-GigabitEthernet2/0/2] quit
```

在 PE 1 上配置 VPN 实例 Customer A，将接口 GigabitEthernet2/0/1 与该实例其进行关联，并使能该实例中的 IP 组播路由及在关联接口上配置 PIM-SM。

```
[PE1] ip vpn-instance customerA
[PE1-vpn-instance-customerA] route-distinguisher 100:1
[PE1-vpn-instance-customerA] vpn-target 100:1
[PE1-vpn-instance-customerA] quit
[PE1] interface gigabitethernet 2/0/1
[PE1-GigabitEthernet2/0/1] ip binding vpn-instance customerA
[PE1-GigabitEthernet2/0/1] quit
[PE1] multicast routing vpn-instance customerA
[PE1-mrib-customerA] quit
[PE1] interface gigabitethernet 2/0/1
[PE1-GigabitEthernet2/0/1] pim sm
[PE1-GigabitEthernet2/0/1] quit
```

在 PE 2 上配置 VPN 实例 Customer A，将接口 GigabitEthernet2/0/1 与该实例其进行关联，并使能该实例中的 IP 组播路由及在关联接口上配置 PIM-SM。

```
[PE2] ip vpn-instance customerA
[PE2-vpn-instance-customerA] route-distinguisher 100:1
[PE2-vpn-instance-customerA] vpn-target 100:1
[PE2-vpn-instance-customerA] quit
[PE2] interface gigabitethernet 2/0/1
[PE2-GigabitEthernet2/0/1] ip binding vpn-instance customerA
[PE2-GigabitEthernet2/0/1] quit
[PE2] multicast routing vpn-instance customerA
[PE2-mrib-customerA] quit
```

```
[PE2] interface gigabitethernet 2/0/1
[PE2-GigabitEthernet2/0/1] pim sm
[PE2-GigabitEthernet2/0/1] quit
```

(3) 创建 MDT 模式 MVPN 实例，进入 MVPN IPv4 地址族视图并指定 Default-Group、MD 源接口和 Data-Group 范围

在 PE 1 上创建 MDT 模式 MVPN 实例 customerA，进入 MVPN IPv4 地址族视图并指定 Default-Group、MVPN 源接口和 Data-Group 范围。

```
[PE1] multicast-vpn vpn-instance customerA mode mdt
[PE1-mvpn-customerA] address-family ipv4
[PE1-mvpn-customerA-ipv4] default-group 239.1.1.1
[PE1-mvpn-customerA-ipv4] source loopback 1
[PE1-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[PE1-mvpn-customerA-ipv4] quit
[PE1-mvpn-customerA] quit
```

在 PE 2 上创建 MDT 模式 MVPN 实例 customerA，进入 MVPN IPv4 地址族视图并指定 Default-Group、MVPN 源接口和 Data-Group 范围。

```
[PE2] multicast-vpn vpn-instance customerA mode mdt
[PE2-mvpn-customerA] address-family ipv4
[PE2-mvpn-customerA-ipv4] default-group 239.1.1.1
[PE2-mvpn-customerA-ipv4] source loopback 1
[PE2-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[PE2-mvpn-customerA-ipv4] quit
[PE2-mvpn-customerA] quit
```

3.6 验证配置

按照如上配置后，通过在 PE 及 P 设备上执行 **display pim routing-table** 命令，可以检查公网 Default-MDT 建立情况，以 P 设备为例：

```
[P]display pim routing-table
 Total 1 (*, G) entry; 2 (S, G) entry

 (*, 239.1.1.1)
     RP: 3.3.3.3 (local)
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 02:54:43
     Upstream interface: Register
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 2
         1: GigabitEthernet2/0/1
             Protocol: pim-sm, UpTime: 02:54:43, Expires: -
         2: GigabitEthernet2/0/2
             Protocol: pim-sm, UpTime: 02:33:57, Expires: -

 (1.1.1.1, 239.1.1.1)
```

```
     RP: 3.3.3.3 (local)
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 01:57:13
     Upstream interface: GigabitEthernet2/0/1
         Upstream neighbor: 192.168.1.2
         RPF prime neighbor: 192.168.1.2
     Downstream interface(s) information: None

(1.1.1.2, 239.1.1.1)
     RP: 3.3.3.3 (local)
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 01:57:13
     Upstream interface: GigabitEthernet2/0/2
         Upstream neighbor: 192.168.2.2
         RPF prime neighbor: 192.168.2.2
     Downstream interface(s) information: None
```

由此可见，公网 P 设备上已建立 RPT（*，239.1.1.1）和两棵相互独立的 SPT 树，这三棵树共同组成了该公网上的 Default-MDT。

3.7 配置文件

- PE 1：

```
#
ip vpn-instance customerA
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 pim sm
#
interface GigabitEthernet2/0/1
 ip binding vpn-instance customerA
 ip address 10.11.1.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/2
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
multicast routing
#
multicast routing vpn-instance customerA
#
multicast-vpn vpn-instance customerA mode mdt
 address-family ipv4
```

```
  source LoopBack1
  default-group 239.1.1.1
  data-group 225.1.1.0 255.255.255.240
#
```

- PE 2：

```
#
ip vpn-instance customerA
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
interface LoopBack1
 ip address 1.1.1.2 255.255.255.255
 pim sm
#
interface GigabitEthernet2/0/1
 ip binding vpn-instance customerA
 ip address 10.11.2.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/2
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
multicast routing
#
multicast routing vpn-instance customerA
#
multicast-vpn vpn-instance customerA mode mdt
 address-family ipv4
  source LoopBack1
  default-group 239.1.1.1
  data-group 225.1.1.0 255.255.255.240
#
```

- P：

```
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 pim sm
#
interface GigabitEthernet2/0/1
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/2
 ip address 192.168.2.1 255.255.255.0
 pim sm
```

```
#
multicast routing
#
pim
 c-bsr 3.3.3.3
 c-rp 3.3.3.3
#
```

- CE a1：

```
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
 pim sm
#
interface GigabitEthernet2/0/1
 ip address 10.11.3.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/2
 ip address 10.11.1.2 255.255.255.0
 pim sm
#
multicast routing
#
pim
 c-bsr 2.2.2.2
 c-rp 2.2.2.2
#
```

- CE a2：

```
#
interface GigabitEthernet2/0/1
 ip address 10.11.2.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/2
 ip address 10.11.4.1 255.255.255.0
 igmp enable
#
multicast routing
#
```

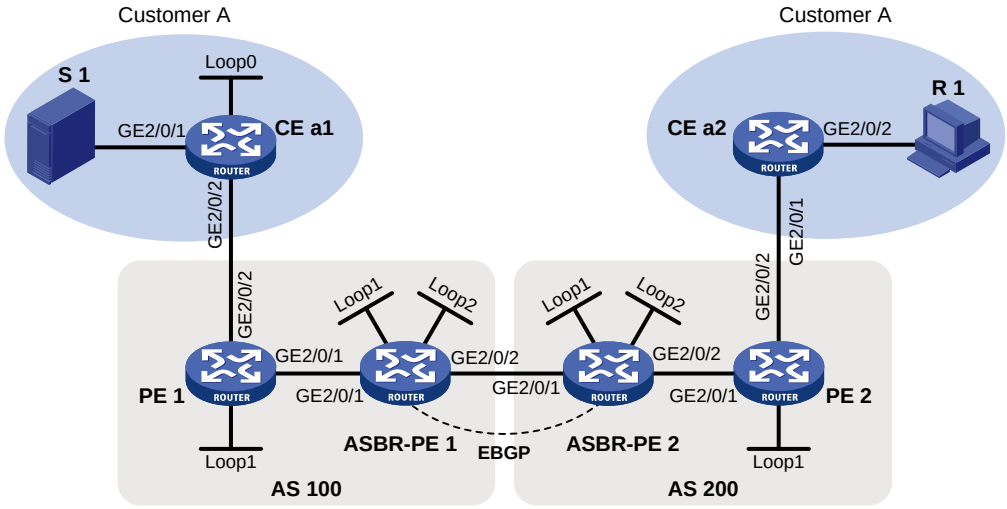
4 A 类跨 AS 的 MDT 模式 MVPN 配置举例

4.1 组网需求

如图 2 所示，Customer A 有位于两地的分支机构，这两个分支机构跨越了两个运营商网络，并已通过跨域 VPN-OptionA 方案实现了两地间单播路由信息的正常交互。目前 Customer A 中的组播源

与接收者分别位于不同的分支机构中，且各分支机构内运行的 PIM 协议模式为 PIM-SM。现要求通过 MDT 模式 MVPN 技术，实现组播接收者能够正常接收到组播源发来的组播数据。

图2 配置 A 类跨 AS 的 MDT 模式 MVPN 组网图



设备	接口	IP地址	设备	接口	IP地址
S 1	-	10.11.3.2/24	R 1	-	10.11.4.2/24
PE 1	GE2/0/1	192.168.1.2/24	ASBR-PE 2	GE2/0/1	192.168.2.2/24
	GE2/0/2	10.11.1.1/24		GE2/0/2	192.168.3.2/24
	Loop1	1.1.1.1/32		Loop1	1.1.1.3/32
ASBR-PE 1	GE2/0/1	192.168.1.1/24		Loop2	22.22.22.22/32
	GE2/0/2	192.168.2.1/24	PE 2	GE2/0/1	192.168.3.1/24
	Loop1	1.1.1.2/32		GE2/0/2	10.11.2.1/24
	Loop2	11.11.11.11/32		Loop1	1.1.1.4/32
CE a1	GE2/0/1	10.11.3.1/24	CE a2	GE2/0/1	10.11.2.2/24
	GE2/0/2	10.11.1.2/24		GE2/0/2	10.11.4.1/24
	Loop0	2.2.2.2/32			

4.2 配置思路

为了实现上述组网需求，需要在每个 AS 内各建立一个独立的 MDT 模式 MVPN。

4.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.4 配置注意事项

- 各 AS 内部运行的公网 PIM 模式可以不同，但属于同一 VPN 的所有接口（包括 ASBR 上绑定 VPN 实例的接口）上必须运行统一的 PIM 模式。
- 对于同一 AS 内的相同 MDT 模式 MVPN 实例，应为其指定相同的 Default-Group，对于不同 AS 的相同 VPN 实例，为其 MDT 模式 MVPN 实例指定的 Default-Group 可以不同。

4.5 配置步骤

4.5.1 配置各设备接口 IP 地址

按图 2 配置各设备上的接口 IP 地址和子网掩码。

```
<CEa1> system-view
[CEa1] interface gigabitethernet 2/0/1
[CEa1-GigabitEthernet2/0/1] ip address 10.11.3.1 24
[CEa1-GigabitEthernet2/0/1] quit
[CEa1] interface loopback 0
[CEa1-LoopBack0] ip address 2.2.2.2 32
[CEa1-LoopBack0] quit
[CEa1] interface gigabitethernet 2/0/2
[CEa1-GigabitEthernet2/0/2] ip address 10.11.1.2 24
[CEa1-GigabitEthernet2/0/2] quit
```

PE 1、ASBR-PE 1、ASBR-PE 2、PE 2 和 CE a2 的配置与 CE a1 相似，配置过程略。

4.5.2 配置路由和 OptionA 方式的跨域 MPLS L3VPN

配置路由协议及 OptionA 方式的跨域 MPLS L3VPN，实现两地间单播路由信息互通。具体配置请参见“MPLS 配置指导”中的“MPLS L3VPN”。

4.5.3 配置组播路由相关功能及 MDT 模式 MVPN

(1) 在各 AS 的公网实例中使能 IP 组播路由、公网接口上配置 PIM-SM 功能（包括 LoopBack 接口）

在 PE 1 上使能 IP 组播路由，在公网接口上配置 PIM-SM。

```
<PE1> system-view
[PE1] multicast routing
[PE1-mrib] quit
[PE1] interface gigabitethernet 2/0/1
[PE1-GigabitEthernet2/0/1] pim sm
[PE1-GigabitEthernet2/0/1] quit
[PE1] interface loopback 1
[PE1-LoopBack1] pim sm
[PE1-LoopBack1] quit
```

在 ASBR-PE 1 上使能 IP 组播路由，在公网接口上配置 PIM-SM，并将 LoopBack 2 接口指定为 AS 100 公网的 C-BSR 和 C-RP，其中 C-RP 服务于该公网实例中所有组播组。

```
<ASBR-PE1> system-view
[ASBR-PE1] multicast routing
[ASBR-PE1-mrib] quit
[ASBR-PE1] interface gigabitethernet 2/0/1
[ASBR-PE1-GigabitEthernet2/0/1] pim sm
[ASBR-PE1-GigabitEthernet2/0/1] quit
[ASBR-PE1] interface loopback 1
[ASBR-PE1-LoopBack1] pim sm
```

```
[ASBR-PE1-LoopBack1] quit
[ASBR-PE1] interface loopback 2
[ASBR-PE1-LoopBack2] pim sm
[ASBR-PE1-LoopBack2] quit
[ASBR-PE1] pim
[ASBR-PE1-pim] c-bsr 11.11.11.11
[ASBR-PE1-pim] c-rp 11.11.11.11
[ASBR-PE1-pim] quit
```

在 PE 2 上使能 IP 组播路由，在公网接口上配置 PIM-SM。

```
<PE2> system-view
[PE2] multicast routing
[PE2-mrib] quit
[PE2] interface gigabitethernet 2/0/1
[PE2-GigabitEthernet2/0/1] pim sm
[PE2-GigabitEthernet2/0/1] quit
[PE2] interface loopback 1
[PE2-LoopBack1] pim sm
[PE2-LoopBack1] quit
```

在配置 ASBR-PE 2 上使能 IP 组播路由，在公网接口上配置 PIM-SM，并将 LoopBack 2 接口指定为 AS 200 公网的 C-BSR 和 C-RP，其中 C-RP 服务于该公网实例中所有组播组。

```
<ASBR-PE2> system-view
[ASBR-PE2] multicast routing
[ASBR-PE2-mrib] quit
[ASBR-PE2] interface gigabitethernet 2/0/2
[ASBR-PE2-GigabitEthernet2/0/2] pim sm
[ASBR-PE2-GigabitEthernet2/0/2] quit
[ASBR-PE2] interface loopback 1
[ASBR-PE2-LoopBack1] pim sm
[ASBR-PE2-LoopBack1] quit
[ASBR-PE2] interface loopback 2
[ASBR-PE2-LoopBack2] pim sm
[ASBR-PE2-LoopBack2] quit
[ASBR-PE2] pim
[ASBR-PE2-pim] c-bsr 22.22.22.22
[ASBR-PE2-pim] c-rp 22.22.22.22
[ASBR-PE2-pim] quit
```

(2) 在 VPN 私网实例中使能 IP 组播路由、私网接口上配置 PIM-SM 功能，并在连接有接收者的 CE 上配置 IGMP

说明

同一 AS 内的 ASBR 与 PE 的 VPN 实例的 VPN Target 应能匹配，不同 AS 的 PE 的 VPN 实例的 VPN Target 则不需要匹配。

在 CE a1 上使能 IP 组播路由，在各接口上配置 PIM-SM，并将 LoopBack 0 接口指定为私网的 C-BSR 和 C-RP，其中 C-RP 服务于 Customer A 实例中所有组播组。

```
<CEa1> system-view
[CEa1] multicast routing
[CEa1-mrib] quit
[CEa1] interface gigabitethernet 2/0/1
[CEa1-GigabitEthernet2/0/1] pim sm
[CEa1-GigabitEthernet2/0/1] quit
[CEa1] interface gigabitethernet 2/0/2
[CEa1-GigabitEthernet2/0/2] pim sm
[CEa1-GigabitEthernet2/0/2] quit
[CEa1] interface loopback 0
[CEa1-LoopBack0] pim sm
[CEa1-LoopBack0] quit
[CEa1] pim
[CEa1-pim] c-bsr 2.2.2.2
[CEa1-pim] c-rp 2.2.2.2
[CEa1-pim] quit
```

在 CE a2 上使能 IP 组播路由，在连接有接收者的接口上使能 IGMP，其余各接口上配置 PIM-SM。

```
<CEa2> system-view
[CEa2] multicast routing
[CEa2-mrib] quit
[CEa2] interface gigabitethernet 2/0/1
[CEa2-GigabitEthernet2/0/1] pim sm
[CEa2-GigabitEthernet2/0/1] quit
[CEa2] interface gigabitethernet 2/0/2
[CEa2-GigabitEthernet2/0/2] igmp enable
[CEa2-GigabitEthernet2/0/2] quit
```

在 PE 1 上配置 VPN 实例 Customer A，将接口 GigabitEthernet2/0/2 与该实例其进行关联，并使能该实例中的 IP 组播路由及在关联接口上配置 PIM-SM。

```
[PE1] ip vpn-instance customerA
[PE1-vpn-instance-customerA] route-distinguisher 100:1
[PE1-vpn-instance-customerA] vpn-target 100:1
[PE1-vpn-instance-customerA] quit
[PE1] interface gigabitethernet 2/0/2
[PE1-GigabitEthernet2/0/2] ip binding vpn-instance customerA
[PE1-GigabitEthernet2/0/2] quit
[PE1] multicast routing vpn-instance customerA
[PE1-mrib-customerA] quit
[PE1] interface gigabitethernet 2/0/2
[PE1-GigabitEthernet2/0/2] pim sm
[PE1-GigabitEthernet2/0/2] quit
```

在 PE 2 上配置 VPN 实例 Customer A，将接口 GigabitEthernet2/0/2 与该实例其进行关联，并使能该实例中的 IP 组播路由及在关联接口上配置 PIM-SM

```
[PE2] ip vpn-instance customerA
[PE2-vpn-instance] route-distinguisher 200:1
[PE2-vpn-instance] vpn-target 200:1
[PE2-vpn-instance] quit
```

```
[PE2] interface gigabitethernet 2/0/2
[PE2-GigabitEthernet2/0/2] ip binding vpn-instance customerA
[PE2-GigabitEthernet2/0/2] quit
[PE2] multicast routing vpn-instance customerA
[PE2-mrib-customerA] quit
[PE2] interface gigabitethernet 2/0/2
[PE2-GigabitEthernet2/0/2] pim sm
[PE2-GigabitEthernet2/0/2] quit
```

在 ASBR-PE 1 上配置 VPN 实例 Customer A，将接口 GigabitEthernet2/0/2 与该实例其进行关联，并使能该实例中的 IP 组播路由及在关联接口上配置 PIM-SM。

```
[ASBR-PE1] ip vpn-instance customerA
[ASBR-PE1-vpn-instance-customerA] route-distinguisher 100:1
[ASBR-PE1-vpn-instance-customerA] vpn-target 100:1
[ASBR-PE1-vpn-instance-customerA] quit
[ASBR-PE1] interface gigabitethernet 2/0/2
[ASBR-PE1-GigabitEthernet2/0/2] ip binding vpn-instance customerA
[ASBR-PE1-GigabitEthernet2/0/2] quit
[ASBR-PE1] multicast routing vpn-instance customerA
[ASBR-PE1-mrib-customerA] quit
[ASBR-PE1] interface gigabitethernet 2/0/2
[ASBR-PE1-GigabitEthernet2/0/2] pim sm
[ASBR-PE1-GigabitEthernet2/0/2] quit
```

在 ASBR-PE 2 上配置 VPN 实例 Customer A，将接口 GigabitEthernet2/0/1 与该实例其进行关联，并使能该实例中的 IP 组播路由及在关联接口上配置 PIM-SM。

```
[ASBR-PE2] ip vpn-instance customerA
[ASBR-PE2-vpn-vpn-customerA] route-distinguisher 200:1
[ASBR-PE2-vpn-vpn-customerA] vpn-target 200:1
[ASBR-PE2-vpn-vpn-customerA] quit
[ASBR-PE2] interface gigabitethernet 2/0/1
[ASBR-PE2-GigabitEthernet2/0/1] ip binding vpn-instance customerA
[ASBR-PE2-GigabitEthernet2/0/1] quit
[ASBR-PE2] multicast routing vpn-instance customerA
[ASBR-PE2-mrib-customerA] quit
[ASBR-PE2] interface gigabitethernet 2/0/1
[ASBR-PE2-GigabitEthernet2/0/1] pim sm
[ASBR-PE2-GigabitEthernet2/0/1] quit
```

(3) 在每个 AS 内各建立一个独立的 MDT 模式 MVPN 实例，并指定 Default-Group、MD 源接口和 Data-Group 范围

在 PE1 上创建 MDT 模式 MVPN 实例 customerA，进入 MVPN IPv4 地址族视图并指定 Default-Group、MVPN 源接口和 Data-Group 范围。

```
[PE1] multicast-vpn vpn-instance customerA mode mdt
[PE1-mvpn-customerA] address-family ipv4
[PE1-mvpn-customerA-ipv4] default-group 239.1.1.1
[PE1-mvpn-customerA-ipv4] source loopback 1
[PE1-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[PE1-mvpn-customerA-ipv4] quit
```

```
[PE1-mvpn-customerA] quit
```

在 ASBR-PE 1 上创建 MDT 模式 MVPN 实例 customerA，进入 MVPN IPv4 地址族视图并指定 Default-Group、MVPN 源接口和 Data-Group 范围。

```
[ASBR-PE1] multicast-vpn vpn-instance customerA mode mdt
[ASBR-PE1-mvpn-customerA] address-family ipv4
[ASBR-PE1-mvpn-customerA-ipv4] default-group 239.1.1.1
[ASBR-PE1-mvpn-customerA-ipv4] source loopback 1
[ASBR-PE1-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[ASBR-PE1-mvpn-customerA-ipv4] quit
[ASBR-PE1-mvpn-customerA] quit
```

在 PE 2 上创建 Multicast tunnel 类型的业务环回组 1，并选择一个未被使用的端口，将其加入该业务环回组。

```
[PE2] service-loopback group 1 type multicast-tunnel
[PE2] interface ten-gigabitethernet 1/0/4
[PE2-Ten-GigabitEthernet1/0/4] port service-loopback group 1
[PE2-Ten-GigabitEthernet1/0/4] quit
```

在 ASBR-PE 2 上创建 MDT 模式 MVPN 实例 customerA，进入 MVPN IPv4 地址族视图并指定 Default-Group、MVPN 源接口和 Data-Group 范围。

```
[ASBR-PE2] multicast-vpn vpn-instance customerA mode mdt
[ASBR-PE2-mvpn-customerA] address-family ipv4
[ASBR-PE2-mvpn-customerA-ipv4] default-group 239.1.1.1
[ASBR-PE2-mvpn-customerA-ipv4] source loopback 1
[ASBR-PE2-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[ASBR-PE2-mvpn-customerA-ipv4] quit
[ASBR-PE2-mvpn-customerA] quit
```

4.6 验证配置

按照如上配置后，通过在 PE 及 ASBR-PE 设备上执行 **display pim routing-table** 命令，可以检查各 AS 的公网 Default-MDT 建立情况，以 ASBR-PE 1 设备为例：

```
[ASBR-PE1]display pim routing-table
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, 239.1.1.1)
     RP: 11.11.11.11 (local)
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 02:54:43
     Upstream interface: Register
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/0/1
             Protocol: pim-sm, UpTime: 02:54:43, Expires: -

 (1.1.1.1, 239.1.1.1)
```

```
RP: 11.11.11.11 (local)
Protocol: pim-sm, Flag: SPT LOC ACT
UpTime: 01:57:13
Upstream interface: GigabitEthernet2/0/1
    Upstream neighbor: 192.168.1.2
    RPF prime neighbor: 192.168.1.2
Downstream interface(s) information: None
```

由此可见，公网 ASBR-PE 1 设备上已建立 RPT（*，239.1.1.1）和 SPT(1.1.1.1, 239.1.1.1)，这两棵树共同组成了 AS 100 公网上的 Default-MDT。

4.7 配置文件

- PE 1：

```
#
ip vpn-instance customerA
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 pim sm
#
interface GigabitEthernet2/0/1
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/2
 ip binding vpn-instance customerA
 ip address 10.11.1.1 255.255.255.0
 pim sm
#
multicast routing
#
multicast routing vpn-instance customerA
#
multicast-vpn vpn-instance customerA mode mdt
 address-family ipv4
  source LoopBack1
  default-group 239.1.1.1
  data-group 225.1.1.0 255.255.255.240
#
```

- PE 2：

```
#
ip vpn-instance customerA
 route-distinguisher 200:1
 vpn-target 200:1 import-extcommunity
```

```
 vpn-target 200:1 export-extcommunity
#
interface LoopBack1
 ip address 1.1.1.4 255.255.255.255
 pim sm
#
interface GigabitEthernet2/0/1
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/2
 ip binding vpn-instance customerA
 ip address 10.11.2.1 255.255.255.0
 pim sm
#
multicast routing
#
multicast routing vpn-instance customerA
#
multicast-vpn vpn-instance customerA mode mdt
 address-family ipv4
  source LoopBack1
  default-group 239.1.1.1
  data-group 225.1.1.0 255.255.255.240
#
```

- ASBR-PE 1：

```
#
ip vpn-instance customerA
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
interface LoopBack1
 ip address 1.1.1.2 255.255.255.255
 pim sm
#
interface LoopBack2
 ip address 11.11.11.11 255.255.255.255
 pim sm
#
interface GigabitEthernet2/0/1
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/2
 ip binding vpn-instance customerA
 ip address 192.168.2.1 255.255.255.0
 pim sm
```

```
#
multicast routing
#
multicast routing vpn-instance customerA
#
pim
 c-bsr 11.11.11.11
 c-rp 11.11.11.11
#
multicast-vpn vpn-instance customerA mode mdt
 address-family ipv4
  source LoopBack1
  default-group 239.1.1.1
  data-group 225.1.1.0 255.255.255.240
#
```

- ASBR-PE 2：

```
#
ip vpn-instance customerA
 route-distinguisher 200:1
 vpn-target 200:1 import-extcommunity
 vpn-target 200:1 export-extcommunity
#
interface LoopBack1
 ip address 1.1.1.3 255.255.255.255
 pim sm
#
interface LoopBack2
 ip address 22.22.22.22 255.255.255.255
 pim sm
#
interface GigabitEthernet2/0/1
 ip binding vpn-instance customerA
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/2
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
multicast routing
#
multicast routing vpn-instance customerA
#
pim
 c-bsr 22.22.22.22
 c-rp 22.22.22.22
#
multicast-vpn vpn-instance customerA mode mdt
```

```
 address-family ipv4
  source LoopBack1
  default-group 239.1.1.1
  data-group 225.1.1.0 255.255.255.240
#
```

- CE a1：

```
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
 pim sm
#
interface GigabitEthernet2/0/1
 ip address 10.11.3.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/2
 ip address 10.11.1.2 255.255.255.0
 pim sm
#
multicast routing
#
pim
 c-bsr 2.2.2.2
 c-rp 2.2.2.2
#
```

- CE a2：

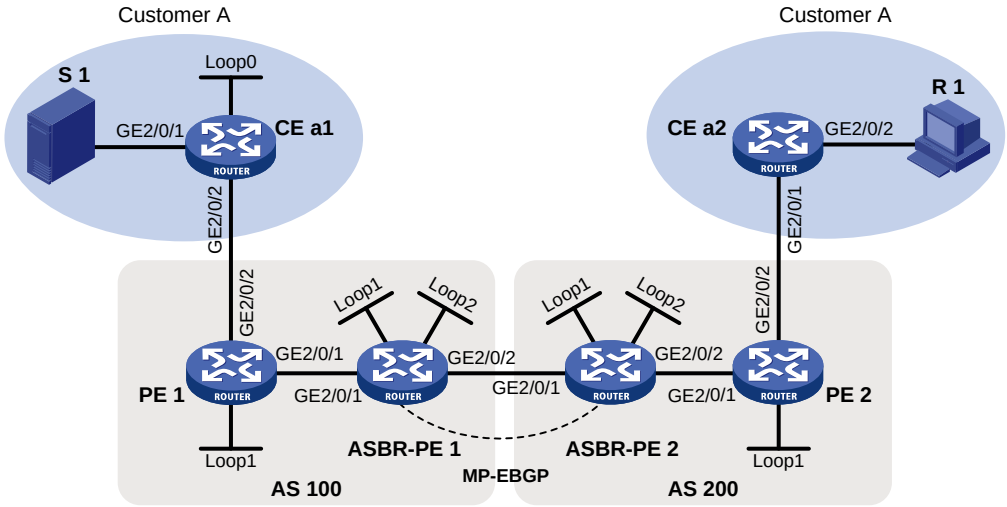
```
#
interface GigabitEthernet2/0/1
 ip address 10.11.2.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/2
 ip address 10.11.4.1 255.255.255.0
 igmp enable
#
multicast routing
#
```

5 C 类跨 AS 的 MDT 模式 MVPN 配置举例

5.1 组网需求

如图 3 所示，Customer A 有位于两地的分支机构，这两个分支机构跨越了两个运营商网络，并已通过跨域 VPN-OptionC 方案实现了两地间单播路由信息的正常交互。目前 Customer A 中的组播源与接收者分别位于不同的分支机构中，且各分支机构内运行的 PIM 协议模式为 PIM-SM。现要求通过 MDT 模式 MVPN 技术，实现组播接收者能够正常接收到组播源发来的组播数据。

图3 配置 C 类跨 AS 的 MDT 模式 MVPN 组网图



设备	接口	IP地址	设备	接口	IP地址
S 1	-	10.11.3.2/24	R 1	-	10.11.4.2/24
PE 1	GE2/0/1	192.168.1.2/24	ASBR-PE2	GE2/0/1	192.168.2.2/24
	GE2/0/2	10.11.1.1/24		GE2/0/2	192.168.3.2/24
	Loop1	1.1.1.1/32		Loop1	1.1.1.3/32
ASBR-PE1	GE2/0/1	192.168.1.1/24		Loop2	22.22.22.22/32
	GE2/0/2	192.168.2.1/24	PE 2	GE2/0/1	192.168.3.1/24
	Loop1	1.1.1.2/32		GE2/0/2	10.11.2.1/24
	Loop2	11.11.11.11/32		Loop1	1.1.1.4/32
CE a1	GE2/0/1	10.11.3.1/24	CE a2	GE2/0/1	10.11.2.2/24
	GE2/0/2	10.11.1.2/24		GE2/0/2	10.11.4.1/24
	Loop0	2.2.2.2/32			

5.2 配置思路

- 为了实现上述组网需求，需要在所有 AS 内统一建立一个 MDT 模式 MVPN 实例。
- 为了使公网 PIM-SM 域之间组播源信息的共享，需要在各公网 PIM-SM 域的 RP 之间建立 MSDP 对等体。

5.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

5.4 配置步骤

5.4.1 配置各设备接口 IP 地址

按图 3 配置各设备上的接口 IP 地址和子网掩码。

```
<CEa1> system-view
[CEa1] interface gigabitethernet 2/0/1
[CEa1-GigabitEthernet2/0/1] ip address 10.11.3.1 24
[CEa1-GigabitEthernet2/0/1] quit
```

```
[CEa1] interface loopback 0
[CEa1-LoopBack0] ip address 2.2.2.2 32
[CEa1-LoopBack0] quit
[CEa1] interface gigabitethernet 2/0/2
[CEa1-GigabitEthernet2/0/2] ip address 10.11.1.2 24
[CEa1-GigabitEthernet2/0/2] quit
```

PE 1、ASBR-PE 1、ASBR-PE 2、PE 2 和 CE a2 的配置与 CE a1 相似，配置过程略。

5.4.2 配置路由和 OptionC 方式的跨域 MPLS L3VPN

配置路由协议及 OptionC 方式的跨域 MPLS L3VPN，实现两地间单播路由信息互通。具体配置请参见“MPLS 配置指导”中的“MPLS L3VPN”。

5.4.3 配置组播路由相关功能及 MDT 模式 MVPN

(1) 在各 AS 的公网实例中使能 IP 组播路由、公网接口上配置 PIM-SM 功能（包括 LoopBack 接口），并将各 AS 配置为独立的 PIM-SM 域

在 PE 1 上使能 IP 组播路由，在公网接口上配置 PIM-SM。

```
<PE1> system-view
[PE1] multicast routing
[PE1-mrib] quit
[PE1] interface gigabitethernet 2/0/1
[PE1-GigabitEthernet2/0/1] pim sm
[PE1-GigabitEthernet2/0/1] quit
[PE1] interface loopback 1
[PE1-LoopBack1] pim sm
[PE1-LoopBack1] quit
```

在 ASBR-PE 1 上使能 IP 组播路由，在公网接口上配置 PIM-SM，并将 LoopBack 2 接口指定为 AS 100 公网的 C-BSR 和 C-RP，其中 C-RP 服务于该公网实例中所有组播组。。

使能 IP 组播路由，及配置 PIM-SM。

```
<ASBR-PE1> system-view
[ASBR-PE1] multicast routing
[ASBR-PE1-mrib] quit
[ASBR-PE1] interface gigabitethernet 2/0/1
[ASBR-PE1-GigabitEthernet2/0/1] pim sm
[ASBR-PE1-GigabitEthernet2/0/1] quit
[ASBR-PE1] interface gigabitethernet 2/0/2
[ASBR-PE1-GigabitEthernet2/0/2] pim sm
[ASBR-PE1-GigabitEthernet2/0/2] quit
[ASBR-PE1] interface loopback 1
[ASBR-PE1-LoopBack1] pim sm
[ASBR-PE1-LoopBack1] quit
[ASBR-PE1] interface loopback 2
[ASBR-PE1-LoopBack2] pim sm
[ASBR-PE1-LoopBack2] quit
[ASBR-PE1] pim
[ASBR-PE1-pim] c-bsr 11.11.11.11
```

```
[ASBR-PE1-pim] c-rp 11.11.11.11
[ASBR-PE1-pim] quit
```

在 ASBR-PE 1 上配置 BSR 的服务边界，将 AS 100 配置为独立的 PIM-SM 域。

```
[ASBR-PE1] interface gigabitethernet 2/0/2
[ASBR-PE1-GigabitEthernet2/0/2] pim bsr-boundary
[ASBR-PE1-GigabitEthernet2/0/2] quit
```

在 PE 2 上使能 IP 组播路由，在公网接口上配置 PIM-SM。

```
<PE2> system-view
[PE2] multicast routing
[PE2-mrib] quit
[PE2] interface gigabitethernet 2/0/1
[PE2-GigabitEthernet2/0/1] pim sm
[PE2-GigabitEthernet2/0/1] quit
[PE2] interface loopback 1
[PE2-LoopBack1] pim sm
[PE2-LoopBack1] quit
```

在 ASBR-PE 2 上使能 IP 组播路由，在公网接口上配置 PIM-SM，并将 LoopBack 2 接口指定为 AS 200 公网的 C-BSR 和 C-RP，其中 C-RP 服务于该公网实例中所有组播组。

```
<ASBR-PE2> system-view
[ASBR-PE2] multicast routing
[ASBR-PE2-mrib] quit
[ASBR-PE2] interface gigabitethernet 2/0/1
[ASBR-PE2-GigabitEthernet2/0/1] pim sm
[ASBR-PE2-GigabitEthernet2/0/1] quit
[ASBR-PE2] interface gigabitethernet 2/0/2
[ASBR-PE2-GigabitEthernet2/0/2] pim sm
[ASBR-PE2-GigabitEthernet2/0/2] quit
[ASBR-PE2] interface loopback 1
[ASBR-PE2-LoopBack1] pim sm
[ASBR-PE2-LoopBack1] quit
[ASBR-PE2] interface loopback 2
[ASBR-PE2-LoopBack2] pim sm
[ASBR-PE2-LoopBack2] quit
[ASBR-PE2] pim
[ASBR-PE2-pim] c-bsr 22.22.22.22
[ASBR-PE2-pim] c-rp 22.22.22.22
[ASBR-PE2-pim] quit
```

在 ASBR-PE 2 上配置 BSR 的服务边界，将 AS 200 配置为独立的 PIM-SM 域。

```
[ASBR-PE2] interface gigabitethernet 2/0/1
[ASBR-PE2-GigabitEthernet2/0/1] pim bsr-boundary
[ASBR-PE2-GigabitEthernet2/0/1] quit
```

(2) 在各公网 PIM-SM 域的 RP 之间建立 MSDP 对等体，从而实现各 AS 公网 PIM-SM 域之间组播源信息的共享

在 ASBR-PE 1 上配置 MSDP 对等体。

```
[ASBR-PE1] msdp
[ASBR-PE1-msdp] encap-data-enable
```

```
[ASBR-PE1-msdp] peer 192.168.2.2 connect-interface gigabitethernet 2/0/2
```

在 ASBR-PE 2 上配置 MSDP 对等体。

```
[ASBR-PE2] msdp
[ASBR-PE2-msdp] encap-data-enable
[ASBR-PE2-msdp] peer 192.168.2.1 connect-interface gigabitethernet 2/0/1
```

(3) 在 VPN 私网实例中使能 IP 组播路由、私网接口上配置 PIM-SM 功能，并在连接有接收者的 CE 上配置 IGMP

说明

对于同一个 VPN，不同 AS 的 PE 上为该 VPN 实例配置的 VPN Target 需要匹配。

在 CE a1 上使能 IP 组播路由，在各接口上配置 PIM-SM，并将 LoopBack 0 接口指定为私网的 C-BSR 和 C-RP，其中 C-RP 服务于 Customer A 实例中所有组播组。

```
<CEa1> system-view
[CEa1] multicast routing
[CEa1-mrib] quit
[CEa1] interface gigabitethernet 2/0/1
[CEa1-GigabitEthernet2/0/1] pim sm
[CEa1-GigabitEthernet2/0/1] quit
[CEa1] interface gigabitethernet 2/0/2
[CEa1-GigabitEthernet2/0/2] pim sm
[CEa1-GigabitEthernet2/0/2] quit
[CEa1] interface loopback 0
[CEa1-LoopBack0] pim sm
[CEa1-LoopBack0] quit
[CEa1] pim
[CEa1-pim] c-bsr 2.2.2.2
[CEa1-pim] c-rp 2.2.2.2
[CEa1-pim] quit
```

在配置 CE a2 上使能 IP 组播路由，在连接有接收者的接口上使能 IGMP，其余各接口上配置 PIM-SM。

```
<CEa2> system-view
[CEa2] multicast routing
[CEa2-mrib] quit
[CEa2] interface gigabitethernet 2/0/1
[CEa2-GigabitEthernet2/0/1] pim sm
[CEa2-GigabitEthernet2/0/1] quit
[CEa2] interface gigabitethernet 2/0/2
[CEa2-GigabitEthernet2/0/2] igmp enable
[CEa2-GigabitEthernet2/0/2] quit
```

在配置 PE 1 上配置 VPN 实例 Customer A，将接口 GigabitEthernet2/0/2 与该实例其进行关联，并使能该实例中的 IP 组播路由及在关联接口上配置 PIM-SM。

```
[PE1] ip vpn-instance customerA
[PE1-vpn-instance-customerA] route-distinguisher 100:1
[PE1-vpn-instance-customerA] vpn-target 100:1
```

```
[PE1-vpn-instance-customerA] quit
[PE1] interface gigabitethernet 2/0/2
[PE1-GigabitEthernet2/0/2] ip binding vpn-instance customerA
[PE1-GigabitEthernet2/0/2] quit
[PE1] multicast routing vpn-instance customerA
[PE1-mrib-customerA] quit
[PE1] interface gigabitethernet 2/0/2
[PE1-GigabitEthernet2/0/2] pim sm
[PE1-GigabitEthernet2/0/2] quit
```

在 PE 2 上配置 VPN 实例 Customer A，将接口 GigabitEthernet2/0/2 与该实例其进行关联，并使能该实例中的 IP 组播路由及在关联接口上配置 PIM-SM

```
[PE2] ip vpn-instance customerA
[PE2-vpn-instance-customerA] route-distinguisher 200:1
[PE2-vpn-instance-customerA] vpn-target 100:1
[PE2-vpn-instance] quit
[PE2] interface gigabitethernet 2/0/2
[PE2-GigabitEthernet2/0/2] ip binding vpn-instance customerA
[PE2-GigabitEthernet2/0/2] quit
[PE2] multicast routing vpn-instance customerA
[PE2-mrib-customerA] quit
[PE2] interface gigabitethernet 2/0/2
[PE2-GigabitEthernet2/0/2] pim sm
[PE2-GigabitEthernet2/0/2] quit
```

(4) 在所有 AS 内统一建立一个 MDT 模式 MVPN 实例，并指定 Default-Group、MVPN 源接口和 Data-Group 范围

在 PE 1 上创建 MDT 模式 MVPN 实例 customerA，进入 MVPN IPv4 地址族视图并指定 Default-Group、MVPN 源接口和 Data-Group 范围。

```
[PE1] multicast-vpn vpn-instance customerA mode mdt
[PE1-mvpn-customerA] address-family ipv4
[PE1-mvpn-customerA-ipv4] default-group 239.1.1.1
[PE1-mvpn-customerA-ipv4] source loopback 1
[PE1-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[PE2-mvpn-customerA-ipv4] quit
[PE1-mvpn-customerA] quit
```

在 PE 2 上创建 MDT 模式 MVPN 实例 customerA，进入 MVPN IPv4 地址族视图并指定 Default-Group、MVPN 源接口和 Data-Group 范围。

```
[PE2] multicast-vpn vpn-instance customerA mode mdt
[PE2-mvpn-customerA] address-family ipv4
[PE2-mvpn-customerA-ipv4] default-group 239.1.1.1
[PE2-mvpn-customerA-ipv4] source loopback 1
[PE2-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[PE2-mvpn-customerA-ipv4] quit
[PE2-mvpn-customerA] quit
```

5.5 验证配置

按照如上配置后，通过在 PE 及 ASBR-PE 设备上执行 **display pim routing-table** 命令，可以检查公网 Default-MDT 建立情况，以 ASBR-PE 1 设备为例：

```
[ASBR-PE1]display pim routing-table
 Total 1 (*, G) entry; 2 (S, G) entry

 (*, 239.1.1.1)
     RP: 3.3.3.3 (local)
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 02:54:43
     Upstream interface: Register
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/0/1
             Protocol: pim-sm, UpTime: 02:54:43, Expires: -

 (1.1.1.1, 239.1.1.1)
     RP: 3.3.3.3 (local)
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 01:57:13
     Upstream interface: GigabitEthernet2/0/1
         Upstream neighbor: 192.168.1.2
         RPF prime neighbor: 192.168.1.2
     Downstream interface(s) information: None

(1.1.1.4, 239.1.1.1)
     RP: 3.3.3.3 (local)
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 01:57:13
     Upstream interface: GigabitEthernet2/0/2
         Upstream neighbor: 192.168.2.2
         RPF prime neighbor: 192.168.2.2
     Downstream interface(s) information: None
```

由此可见，公网 ASBR-PE 1 设备上已建立 RPT（*，239.1.1.1）和两棵相互独立的 SPT 树，这三棵树共同组成了该公网 MDT 模式 MVPN 实例上的 Default-MDT。

5.6 配置文件

- PE 1：

```
#
ip vpn-instance customerA
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
```

```
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 pim sm
#
interface GigabitEthernet2/0/1
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/2
 ip binding vpn-instance customerA
 ip address 10.11.1.1 255.255.255.0
 pim sm
#
multicast routing
#
multicast routing vpn-instance customerA
#
multicast-vpn vpn-instance customerA mode mdt
 address-family ipv4
  source LoopBack1
  default-group 239.1.1.1
  data-group 225.1.1.0 255.255.255.240
#
```

- PE 2：

```
#
ip vpn-instance customerA
 route-distinguisher 200:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
interface LoopBack1
 ip address 1.1.1.4 255.255.255.255
 pim sm
#
interface GigabitEthernet2/0/1
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/2
 ip binding vpn-instance customerA
 ip address 10.11.2.1 255.255.255.0
 pim sm
#
multicast routing
#
multicast routing vpn-instance customerA
#
```

```
multicast-vpn vpn-instance customerA mode mdt
 address-family ipv4
  source LoopBack1
  default-group 239.1.1.1
  data-group 225.1.1.0 255.255.255.240
#
```

- ASBR-PE 1：

```
#
interface LoopBack1
 ip address 1.1.1.2 255.255.255.255
 pim sm
#
interface LoopBack2
 ip address 11.11.11.11 255.255.255.255
 pim sm
#
interface GigabitEthernet2/0/1
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/2
 ip address 192.168.2.1 255.255.255.0
 pim sm
 pim bsr-boundary
#
multicast routing
#
pim
 c-bsr 11.11.11.11
 c-rp 11.11.11.11
#
msdp
 encap-data-enable
 peer 192.168.2.2 connect-interface GigabitEthernet2/0/2
#
```

- ASBR-PE 2：

```
#
interface LoopBack1
 ip address 1.1.1.3 255.255.255.255
 pim sm
#
interface LoopBack2
 ip address 22.22.22.22 255.255.255.255
 pim sm
#
interface GigabitEthernet2/0/1
 ip address 192.168.2.2 255.255.255.0
```

```
 pim sm
 pim bsr-boundary
#
interface GigabitEthernet2/0/2
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
multicast routing
#
pim
 c-bsr 22.22.22.22
 c-rp 22.22.22.22
#
msdp
 encap-data-enable
 peer 192.168.2.1 connect-interface GigabitEthernet2/0/1
#
```

- CE a1：

```
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
 pim sm
#
interface GigabitEthernet2/0/1
 ip address 10.11.3.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/2
 ip address 10.11.1.2 255.255.255.0
 pim sm
#
multicast routing
#
pim
 c-bsr 2.2.2.2
 c-rp 2.2.2.2
#
```

- CE a2：

```
#
interface GigabitEthernet2/0/1
 ip address 10.11.2.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/2
 ip address 10.11.4.1 255.255.255.0
 igmp enable
#
```

```
multicast routing
#
```

6 相关资料

- H3C SR6600 SR6600-X 路由器 IP 组播配置指导-R7607
- H3C SR6600 SR6600-X 路由器 IP 组播命令参考-R7607
- H3C SR6600 SR6600-X 路由器 MPLS 配置指导-R7607
- H3C SR6600 SR6600-X 路由器 MPLS 命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

AAA 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1

2 配置前提 1

3 Telnet 用户的 HWTACACS 认证和授权配置举例 1

3.1 组网需求 1

3.2 配置思路 1

3.3 使用版本 2

3.4 配置步骤 2

3.4.1 配置 HWTACACS 2

3.4.2 配置 Device 5

3.5 验证配置 6

3.6 配置文件 6

4 SSH 用户的 RADIUS 认证和授权配置举例 7

4.1 组网需求 7

4.2 **配置思路** 7

4.3 使用版本 8

4.4 配置步骤 8

4.4.1 配置 RADIUS 服务器 8

4.4.2 配置 Device 10

4.5 验证配置 11

4.6 配置文件 13

5 相关资料 14

1 简介

本文档介绍了 Telnet、SSH 用户通过 AAA 服务器进行登录认证和授权的配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文假设您已了解 AAA 特性。

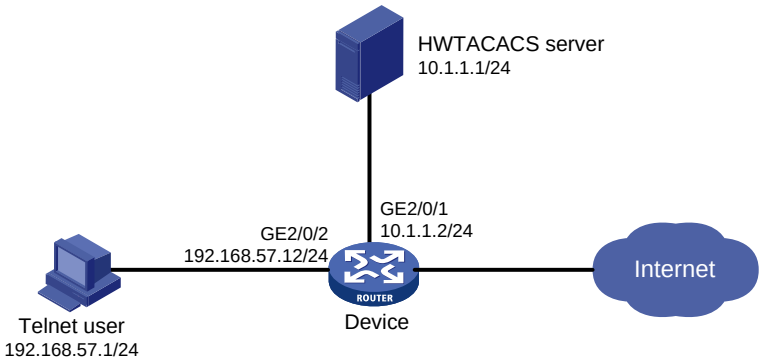
3 Telnet 用户的 HWTACACS 认证和授权配置举例

3.1 组网需求

如图 1 所示，通过在作为 NAS 的 Device 上配置远程 HWTACACS 认证、授权功能，实现 Telnet 用户的安全登录。要求在 Device 上配置实现：

- HWTACACS 服务器对登录 Device 的 Telnet 用户进行认证和授权，登录用户名为 *user*@bbb，密码为 aabbcc；
- 用户通过认证后可执行系统所有功能和资源的相关 **display** 命令。

图1 Telnet 用户的远端 HWTACACS 认证和授权配置组网图



3.2 配置思路

- 为了使 HWTACACS 服务器能够识别合法的用户，在 HWTACACS 服务器上添加合法的 Telnet 用户名和密码。
- 为了使用户通过认证后可执行系统所有功能和资源的相关 **display** 命令，在 HWTACACS 服务器上设置用户角色为 network-operator。
- 由于本例中用户登录 Device 要通过 AAA 处理，因此 Telnet 用户登录的用户界面认证方式配置为 scheme。

- 为了实现通过 HWTACACS 来进行认证和授权，需要在 Device 上配置 HWTACACS 方案并指定相应的认证和授权服务器，并将其应用于 Telnet 用户所属的 ISP 域。
- 为了在 Device 和 HWTACACS 服务器之间安全地传输用户密码，并且能在 Device 上验证服务器响应报文未被篡改，在 Device 和 HWTACACS 服务器上都要设置交互报文时所使用的共享密钥。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置步骤

3.4.1 配置 HWTACACS

说明

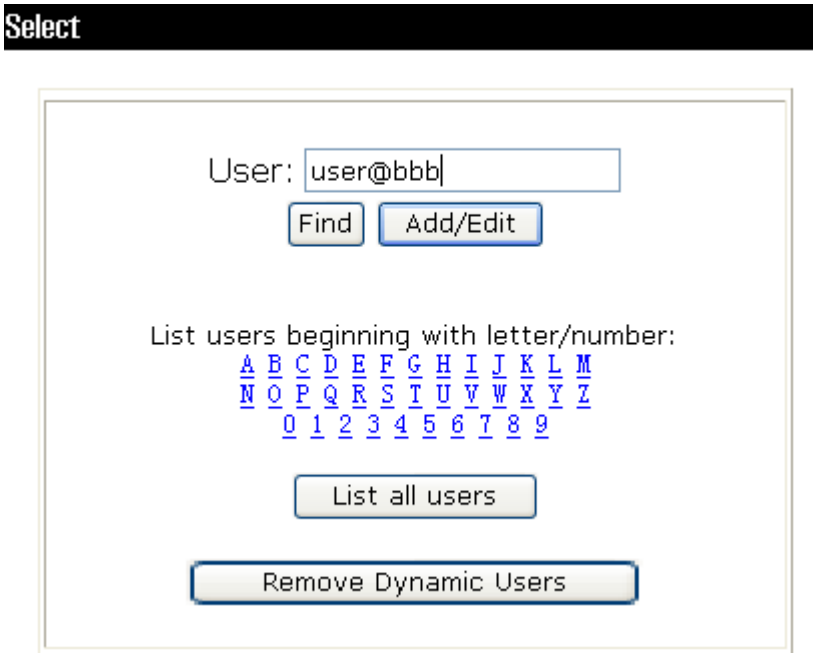
本文以 HWTACACS 服务器 ACS 4.0 为例，说明该例中 HWTACACS 的基本配置。

1. 增加设备管理用户

登录进入 HWTACACS 管理平台，点击左侧导航栏“User-Setup”增加设备管理用户。

- 在界面上输入用户名“user@bbb”；
- 点击按钮“Add/Edit”进入用户编辑页面。

图2 用户创建界面

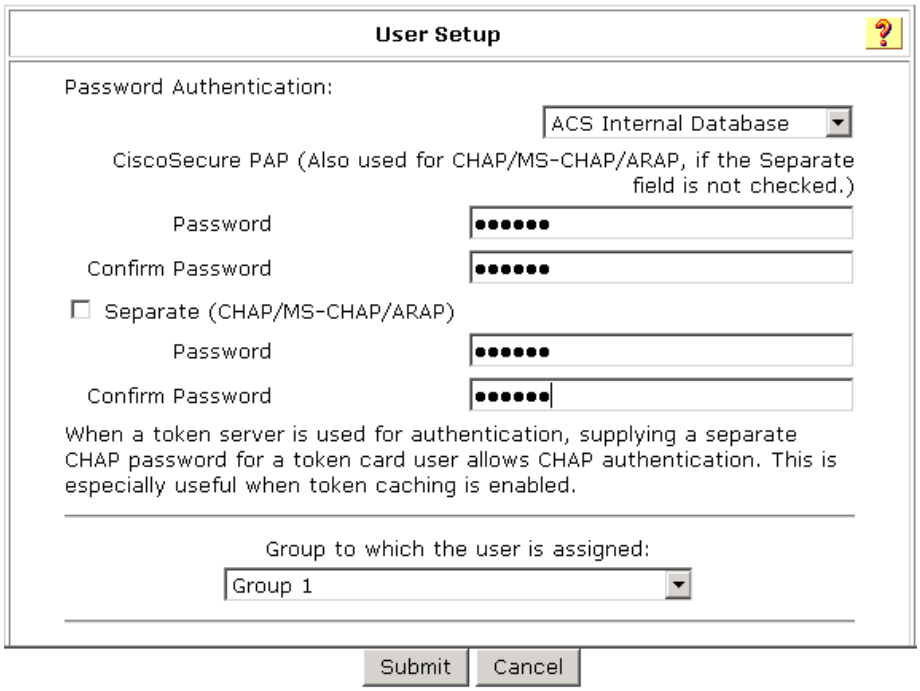


2. 配置设备管理用户

在用户编辑页面上配置设备管理用户。

- 配置用户密码“aabbcc”；
- 为用户选择组“Group 1”；
- 单击“Submit”完成操作。

图3 用户密码配置界面

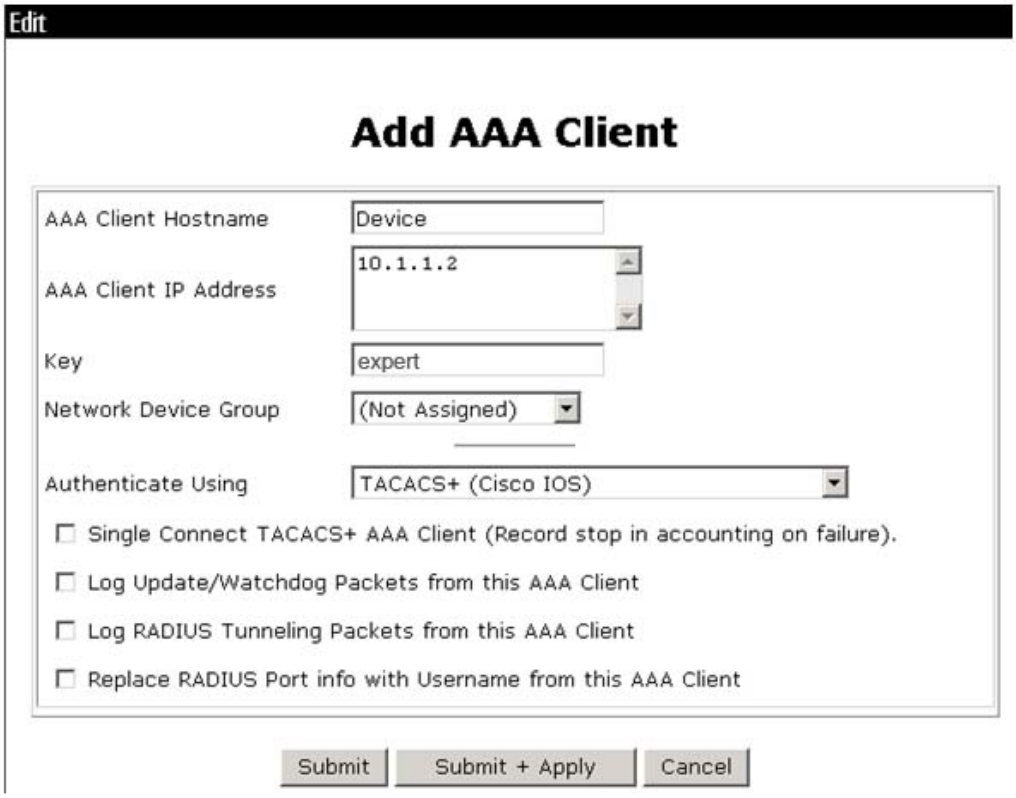


3. 配置网络

点击左侧导航栏“Network Configuration”，在“AAA Client Hostname”处任意命名（本例为“Device”）后开始配置网络。

- “AAA Client IP Address”一栏填写 Device 与 HWTACACS 服务器相连的接口的 IP 地址“10.1.1.2”。
- “Key”一栏填写 HWTACACS 服务器和设备通信时的共享密钥“expert”，必须和 Device 上 HWTACACS 方案里配置的认证、授权和计费共享密钥相同。
- 在“Authenticate Using”的下拉框里选择“TACACS+ (Cisco IOS)”。
- 单击“Submit+Apply”按钮完成配置。

图4 网络配置界面



4. 设置组

单击左侧导航栏“Group Setup”，选取“Group 1”（与配置设备管理用户时为用户选择的组一致），单击“Edit Settings”进入编辑区。

- 在多选框中选择“Shell”（用户可以执行命令）；
- 在多选框中选择“Custom attributes”，并在文本框中输入：roles=\”network-operator\”；
- 单击“Submit”后完成操作。

图5 选择组界面

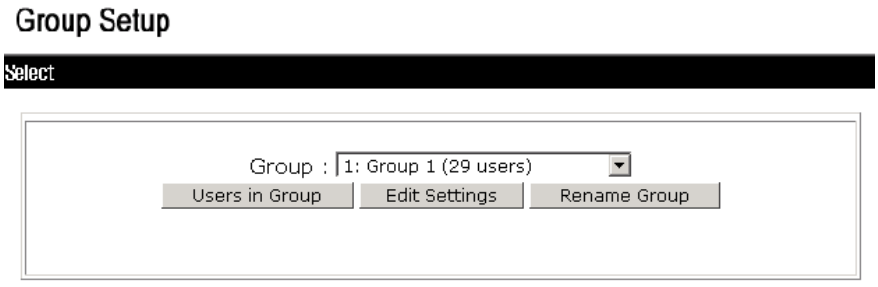
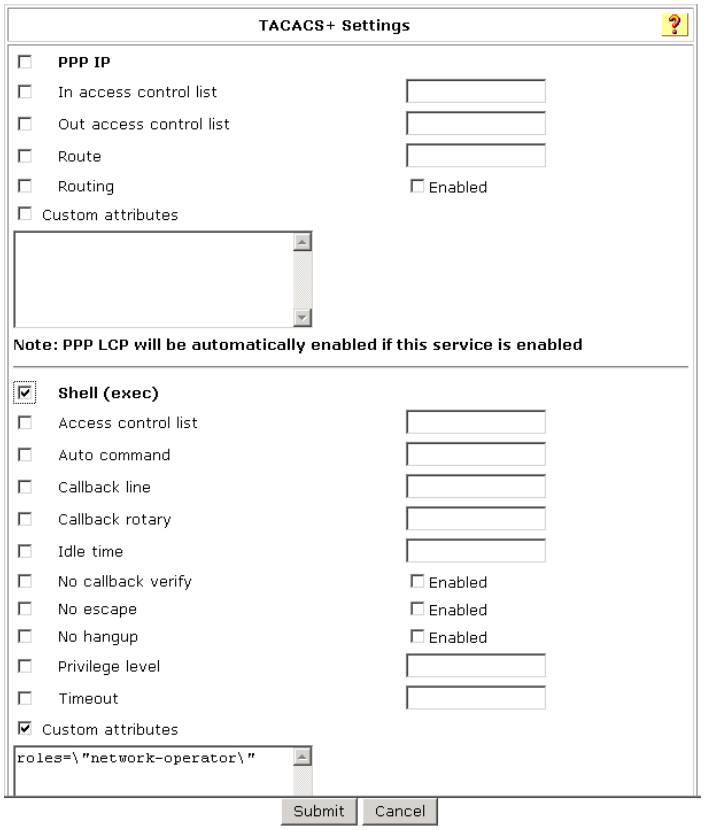


图6 组配置界面



3.4.2 配置 Device

配置接口 GigabitEthernet2/0/2 的 IP 地址。

```
<Device> system-view
[Device] interface GigabitEthernet 2/0/2
[Device-GigabitEthernet2/0/2] ip address 192.168.57.12 255.255.255.0
[Device-GigabitEthernet2/0/2] quit
```

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
[Device] interface GigabitEthernet 2/0/1
[Device-GigabitEthernet2/0/1] ip address 10.1.1.2 255.255.255.0
[Device-GigabitEthernet2/0/1] quit
```

开启 Device 的 Telnet 服务器功能。

```
[Device] telnet server enable
```

配置 Telnet 用户登录的用户界面采用 scheme 方式。

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

配置 HWTACACS 方案 hwtac。

```
[Device] hwtacacs scheme hwtac
```

配置主认证、授权和计费服务器的 IP 地址为 10.1.1.1，认证、授权和计费的端口号为 49（HWTACACS 服务器的认证、授权和计费端口为 TCP 端口 49）。

```
[Device-hwtacacs-hwtac] primary authentication 10.1.1.1 49
[Device-hwtacacs-hwtac] primary authorization 10.1.1.1 49
[Device-hwtacacs-hwtac] primary accounting 10.1.1.1 49
```

配置与认证、授权和计费服务器交互报文时的共享密钥均为明文 expert。

```
[Device-hwtacacs-hwtac] key authentication simple expert
[Device-hwtacacs-hwtac] key authorization simple expert
[Device-hwtacacs-hwtac] key accounting simple expert
[Device-hwtacacs-hwtac] quit
```

配置 ISP 域的 AAA 方案，为 login 用户配置 AAA 认证方法为 HWTACACS 认证、授权和计费。

```
[Device] domain bbb
[Device-isp-bbb] authentication login hwtacacs-scheme hwtac
[Device-isp-bbb] authorization login hwtacacs-scheme hwtac
[Device-isp-bbb] accounting login hwtacacs-scheme hwtac
[Device-isp-bbb] quit
```

3.5 验证配置

Telnet 用户可以使用用户名 user@bbb 和密码 aabbcc 通过认证，并且获得用户角色 network-operator（用户通过认证后可执行系统所有功能和资源的相关 **display** 命令）。

3.6 配置文件

```
#
 telnet server enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 192.168.57.12 255.255.255.0
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.1.1.2 255.255.255.0
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
hwtacacs scheme hwtac
 primary authentication 10.1.1.1
 primary authorization 10.1.1.1
 primary accounting 10.1.1.1
 key authentication cipher $c$3$6ps2/dT38b2K2MDCMCDGYxrvyJNR+/jiKw==
 key authorization cipher $c$3$xEldxJraE8Yof3rHHlVIgyCIb/uLlrZbgg==
 key accounting cipher $c$3$kySCJbNA8DSs+l3HCqxunl8SE4me3vue5g==
#
```

```
 domain bbb
  authentication login hwtacacs-scheme hwtac
  authorization login hwtacacs-scheme hwtac
  accounting login hwtacacs-scheme hwtac
#
```

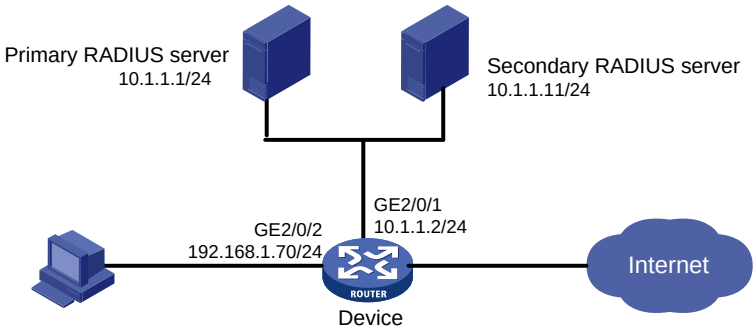
4 SSH 用户的 RADIUS 认证和授权配置举例

4.1 组网需求

如图 7 所示，通过在作为 NAS 的 Device 上配置远程 RADIUS 认证、授权功能，实现 SSH 用户的安全登录。在网络架构上采用主从 RADIUS 服务器的方式来提高用户认证的稳定性。要求在 Device 上配置实现：

- 使用 RADIUS 服务器对登录 Device 的 SSH 用户进行认证和授权，登录用户名为 hello@bbb，密码为 aabbcc；
- Device 向 RADIUS 服务器发送的用户名带域名，服务器根据用户名携带的域名来区分提供给用户的服务。
- 用户通过认证后可执行系统所有功能和资源的相关 **display** 命令。

图7 SSH 用户的远端 RADIUS 认证和授权配置组网图



4.2 配置思路

- 为了使主/从 RADIUS 服务器能够识别合法的用户，在主/从 RADIUS 服务器上添加合法的用户名和密码。
- 为了使用户通过认证后可执行系统所有功能和资源的相关 **display** 命令，在主/从 RADIUS 服务器上设置用户角色为 network-operator。
- 因为 SSH 用户登录 Device 要通过 AAA 处理，因此 SSH 用户登录的用户界面认证方式配置为 scheme。
- 为了实现通过 RADIUS 来进行认证和授权，需要在 Device 上配置 RADIUS 方案并指定相应的主/从认证和授权服务器，并将其应用于 SSH 用户所属的 ISP 域。

- 为了在 Device 和主/从 RADIUS 服务器之间安全地传输用户密码，并且能在 Device 上验证主/从 RADIUS 服务器响应报文未被篡改，在 Device 和主/从 RADIUS 服务器上都要设置交互报文时所使用的共享密钥。

4.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.4 配置步骤

4.4.1 配置 RADIUS 服务器

说明

- 本节以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.0(E0102)、iMC EIA 7.0(E0201)），说明该例中 RADIUS 服务器的基本配置。
- 主从 RADIUS 服务器设置相同，本节以主 RADIUS 服务器设置为例。

1. 增加接入设备

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击“增加”按钮，进入增加接入设备页面。

- 设置与 Device 交互报文时使用的认证和授权共享密钥为“expert”；
- 设置认证及计费的端口号分别为“1812”（RADIUS 服务器的认证端口为 UDP 端口 1812）和“1813”（RADIUS 服务器的计费端口为 UDP 端口 1813）；
- 选择业务类型为“设备管理业务”；
- 选择接入设备类型为“H3C(General)”；
- 选择或手工增加接入设备，添加 IP 地址为 10.1.1.2 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图8 增加接入设备

2. 增加设备管理用户

选择“用户”页签，单击导航树中的[接入用户管理视图/设备管理用户]菜单项，进入设备管理用户列表页面，在该页面中单击<增加>按钮，进入增加设备管理用户页面。

- 输入用户名“hello@bbb”和密码。
- 选择服务类型为“SSH”。
- 输入用户角色名“network-operator”
- 添加所管理设备的 IP 地址，IP 地址范围为“10.1.1.0～10.1.1.255”。
- 单击<确定>按钮完成操作。

说明

添加的所管理设备的 IP 地址范围要包含添加的接入设备的 IP 地址。

图9 增加设备管理用户

4.4.2 配置 Device

配置接口 GigabitEthernet2/0/2 的 IP 地址。

```
<Device> system-view
[Device] interface GigabitEthernet 2/0/2
[Device-GigabitEthernet2/0/2] ip address 192.168.1.70 255.255.255.0
[Device-GigabitEthernet2/0/2] quit
```

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
[Device] interface GigabitEthernet 2/0/1
[Device-GigabitEthernet2/0/1] ip address 10.1.1.2 255.255.255.0
[Device-GigabitEthernet2/0/1] quit
```

生成 RSA 及 DSA 密钥对。

```
[Device] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.
Create the key pair successfully.
```

```
[Device] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

使能 SSH 服务器功能。

```
[Device] ssh server enable
```

配置 SSH 用户登录采用 AAA 认证方式。

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

创建 RADIUS 方案 rad。

```
[Device] radius scheme rad
```

配置主认证服务器的 IP 地址为 10.1.1.1，认证端口号为 1812。

```
[Device-radius-rad] primary authentication 10.1.1.1 1812
```

配置从认证服务器的 IP 地址为 10.1.1.11，认证端口号为 1812。

```
[Device-radius-rad] secondary authentication 10.1.1.11 1812
```

配置主计费服务器的 IP 地址为 10.1.1.1，计费端口号为 1813。

```
[Device-radius-rad] primary accounting 10.1.1.1 1813
```

配置从计费服务器的 IP 地址为 10.1.1.11，计费端口号为 1813。

```
[Device-radius-rad] secondary accounting 10.1.1.11 1813
```

配置与认证和计费服务器交互报文时的共享密钥为明文 expert。

```
[Device-radius-rad] key authentication simple expert
[Device-radius-rad] key accounting simple expert
```

配置向 RADIUS 服务器发送的用户名要携带域名。

```
[Device-radius-rad] user-name-format with-domain
[Device-radius-rad] quit
```

创建 ISP 域 bbb，为 login 用户配置 AAA 认证方法为 RADIUS 认证、授权和计费。

```
[Device] domain bbb
[Device-isp-bbb] authentication login radius-scheme rad
[Device-isp-bbb] authorization login radius-scheme rad
[Device-isp-bbb] accounting login radius-scheme rad
[Device-isp-bbb] quit
```

4.5 验证配置

用户向 Device 发起 SSH 连接，在 SSH 客户端按照提示输入用户名 hello@bbb 和密码 aabbcc 通过认证，并且获得用户角色 network-operator（用户通过认证后可执行系统所有功能和资源的相关 **display** 命令）。

主服务器可达时，设备与主 RADIUS 服务器进行交互。

显示主服务器可达时的 RADIUS 方案的配置信息。

```
<Sysname> display radius scheme
Total 1 RADIUS schemes

--------------------------------------------------------------------
RADIUS scheme name: rad
  Index: 0
  Primary authentication server:
    IP   : 10.1.1.1                               Port: 1812
    VPN  : Not configured
    State: Active
    Test profile: Not configured
  Primary accounting server:
    IP   : 10.1.1.1                               Port: 1813
    VPN  : Not configured
    State: Active
  Second authentication server:
    IP   : 10.1.1.11                              Port: 1812
    VPN  : Not configured
    State: Active
    Test profile: Not configured
  Second accounting server:
    IP   : 10.1.1.11                              Port: 1813
    VPN  : Not configured
    State: Active
  Accounting-On function                    : Disabled
    extended function                       : Disabled
    retransmission times                    : 50
    retransmission interval(seconds)        : 3
  Timeout Interval(seconds)                 : 3
  Retransmission Times                      : 3
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes)              : 5
  Realtime Accounting Interval(seconds)     : 720
  NAS IP Address                            : Not configured
  VPN                                       : Not configured
  User Name Format                          : with-domain
  Data flow unit                            : Byte
  Packet unit                               : One
  Attribute 15 check-mode                   : Strict
  Attribute 25                              : Standard
  Attribute Remanent-Volume unit            : Kilo
--------------------------------------------------------------------
```

主服务器不可达时，再查看 RADIUS 方案的配置信息，会发现主服务器的状态从 active 变为 block。此时，设备变成与从 RADIUS 服务器进行交互。

显示主服务器不可达时的 RADIUS 方案的配置信息。

```
<Sysname> display radius scheme
Total 1 RADIUS schemes
```

```
------------------------------------------------------------------
RADIUS scheme name: rad
  Index: 0
  Primary authentication server:
    IP   : 10.1.1.1                                Port: 1812
    VPN  : Not configured
    State: Block
    Test profile: Not configured
  Primary accounting server:
    IP   : 10.1.1.1                                Port: 1813
    VPN  : Not configured
    State: Block
  Second authentication server:
    IP   : 10.1.1.11                               Port: 1812
    VPN  : Not configured
    State: Active
    Test profile: Not configured
  Second accounting server:
    IP   : 10.1.1.11                               Port: 1813
    VPN  : Not configured
    State: Active
  Accounting-On function                     : Disabled
    extended function                        : Disabled
    retransmission times                     : 50
    retransmission interval(seconds)         : 3
  Timeout Interval(seconds)                  : 3
  Retransmission Times                       : 3
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes)               : 5
  Realtime Accounting Interval(seconds)      : 720
  NAS IP Address                             : Not configured
  VPN                                        : Not configured
  User Name Format                           : with-domain
  Data flow unit                             : Byte
  Packet unit                                : One
  Attribute 15 check-mode                    : Strict
  Attribute 25                               : Standard
  Attribute Remanent-Volume unit             : Kilo
------------------------------------------------------------------
```

4.6 配置文件

```
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 192.168.1.70 255.255.255.0
#
```

```
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.1.1.2 255.255.255.0
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
 ssh server enable
#
radius scheme rad
 primary authentication 10.1.1.1
 primary accounting 10.1.1.1
 secondary authentication 10.1.1.11
 secondary accounting 10.1.1.11
 key authentication cipher $c$3$63G7LzIQElGq4aFGTiYQafU+loQxS/cbLg==
 key accounting cipher $c$3$tUIVlyGISJ5X/yiTFWrmh8nyjBIF+1LFzQ==
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
 accounting login radius-scheme rad
#
```

5 相关资料

- H3C SR6600 SR6600-X 路由器 安全配置指导-R7607
- H3C SR6600 SR6600-X 路由器 安全命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

ACL 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1

2 配置前提 1

3 配置设备的 FTP 访问权限典型配置举例 1

3.1 组网需求 1

3.2 使用版本 1

3.3 配置思路 2

3.4 配置步骤 2

3.5 验证配置 2

3.6 配置文件 3

4 通过 IP 地址过滤流量典型配置举例 4

4.1 组网需求 4

4.2 使用版本 5

4.3 配置思路 5

4.4 配置步骤 5

4.5 验证配置 6

4.6 配置文件 7

5 通过指定的 TCP 协议过滤流量典型配置举例 8

5.1 组网需求 8

5.2 使用版本 8

5.3 配置思路 9

5.4 配置步骤 9

5.5 验证配置 10

5.6 配置文件 10

6 相关资料 11

1 简介

本文档介绍了 ACL（Access Control List，访问控制列表）的配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文假设您已了解 ACL 特性。

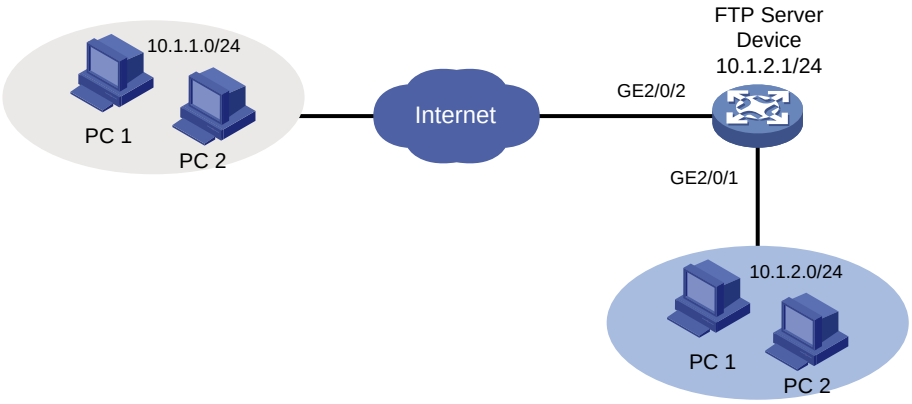
3 配置设备的 FTP 访问权限典型配置举例

3.1 组网需求

如图 1 所示，当设备作为 FTP 服务器时，需要为网络中的不同用户设置不同的 FTP 访问权限：

- 10.1.2.0/24 网段的用户任意时间都可以访问 FTP 服务器；
- 10.1.1.0/24 网段的用户只能在工作时间（周一至周五的 8:30～18:00）访问 FTP 服务器；
- 符合访问条件的用户可以获得 level-15 的用户访问权限，不符合条件的用户不能访问 FTP 服务器。

图1 配置设备的 FTP 访问权限组网图



3.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.3 配置思路

- 为了根据 FTP 用户的 IP 地址来区分不同的访问权限，需要创建 ACL 配置规则只允许源地址为 10.1.2.0/24 和 10.1.1.0/24 的报文通过，并指定 10.1.1.0/24 网段的生效时间段；
- 为实现 FTP 服务器区分用户权限，需要将 ACL 规则与 FTP 服务功能关联。

3.4 配置步骤

配置时间段 ftp，时间范围为周一至周五的 8:30～18:00。

```
<Device> system-view
[Device] time-range ftp 8:30 to 18:00 working-day
```

创建 IPv4 基本 ACL 2000，定义规则允许源 IP 地址为 10.1.2.0/24 的报文通过。

```
[Device] acl basic 2000
[Device-acl-ipv4-basic-2000] rule permit source 10.1.2.0 0.0.0.255
```

定义规则为在 ftp 时间段内允许源 IP 地址为 10.1.1.0/24 的报文通过。

```
[Device-acl-ipv4-basic-2000] rule permit source 10.1.1.0 0.0.0.255 time-range ftp
[Device-acl-ipv4-basic-2000] quit
```

开启设备的 FTP 服务器功能。

```
[Device] ftp server enable
```

新增 FTP 用户。

```
[Device] local-user ftp
[Device-luser-manage-ftp] service-type ftp
```

配置 FTP 用户密码。

```
[Device-luser-manage-ftp] password simple 123456
```

配置 FTP 用户的访问权限为 level-15。

```
[Device-luser-manage-ftp] authorization-attribute user-role level-15
[Device-luser-manage-ftp] quit
```

配置 FTP 服务器关联 ACL 2000 设置 FTP 用户的访问权限。

```
[Device] ftp server acl 2000
```

3.5 验证配置

工作时间，在 IP 地址为 10.1.2.100 的主机上尝试登录 FTP 服务器：

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>ftp 10.1.2.1
Connected to 10.1.2.1.
220 FTP service ready.
User (10.1.2.1:(none)): ftp
331 Password required for ftp.
Password:
230 User logged in.
```

在根据提示信息正确输入 FTP 用户名和密码后，提示登入成功。

工作时间，在 IP 地址为 10.1.1.100 的主机上尝试登录 FTP 服务器：

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>ftp 10.1.2.1
Connected to 10.1.2.1.
220 FTP service ready.
User (10.1.2.1:(none)): ftp
331 Password required for ftp.
Password:
230 User logged in.
```

在根据提示信息正确输入 FTP 用户名和密码后，提示登入成功。

非工作时间，在 IP 地址为 10.1.2.100 的主机上尝试登录 FTP 服务器：

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>ftp 10.1.2.1
Connected to 10.1.2.1.
220 FTP service ready.
User (10.1.2.1:(none)): ftp
331 Password required for ftp.
Password:
230 User logged in.
```

在根据提示信息正确输入 FTP 用户名和密码后，提示登入成功。

非工作时间，在 IP 地址为 10.1.1.100 的主机上尝试登录 FTP 服务器：

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>ftp 10.1.2.1
ftp>
ftp> ls
Not connected.
```

没有提示要求输入用户名和密码，执行 FTP 命令后，提示没有 FTP 连接成功。

3.6 配置文件

```
#
 time-range ftp 08:30 to 18:00 working-day
#
acl basic 2000
 rule 0 permit source 10.1.2.0 0.0.0.255
 rule 5 permit source 10.1.1.0 0.0.0.255 time-range ftp
#
local-user ftp class manage
 password hash $h$6$FtGf7gkM3iOdT35z$D5/M4eLL9HT14yFuii5QlCWk0nEG6JQxIvxa3vvVcoP
EbUIhJS3P6JVGa/8BDYxU1vYVH1LyNqxNB+fX2DpvPA==
 service-type ftp
 authorization-attribute user-role level-15
```

```
 authorization-attribute user-role network-operator
#
 ftp server enable
 ftp server acl 2000
```

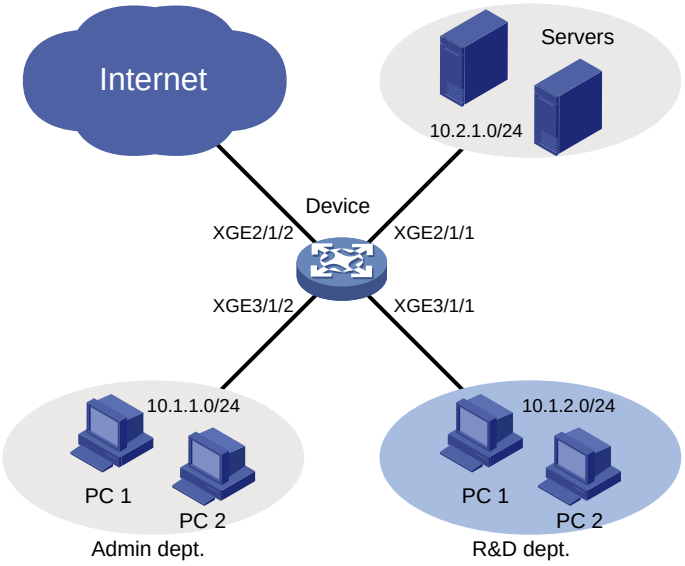
4 通过 IP 地址过滤流量典型配置举例

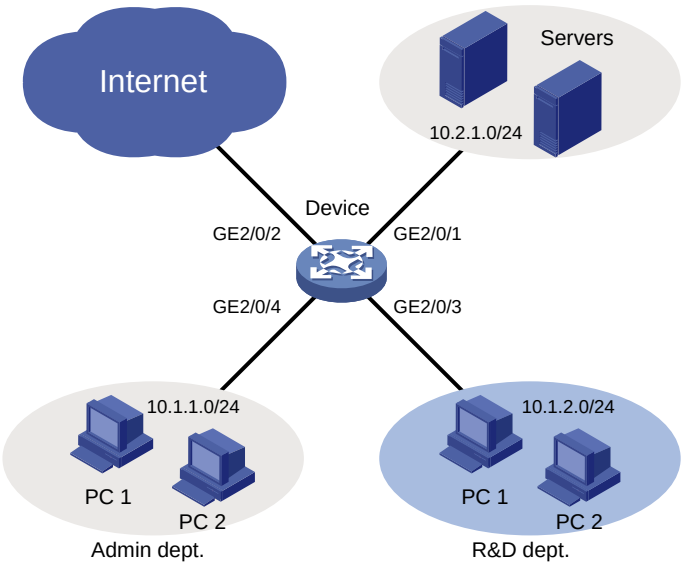
4.1 组网需求

如图 2 所示，某公司的网络分成管理部、研发部和服务器三个区域，通过 Device 设备与 Internet 连接。现要求通过 ACL 实现：

- 管理部任意时间都可以访问 Internet 和服务器，但不能访问研发部；
- 研发部在工作时间（周一至周五的 8:30～18:00）只能访问服务器，不能访问 Internet 和管理部；非工作时间可以访问 Internet 和服务器，但不能访问管理部。

图2 通过 IP 地址过滤流量配置组网图





4.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.3 配置思路

- 为实现管理部不能访问研发部，需要创建 ACL 配置规则拒绝目的地址为 10.1.2.0/24 的报文，在 Device 的 Ten-GigabitEthernet3/1/2 的入方向进行过滤；
- 为实现研发部在工作时间只能访问服务器，需要创建 ACL 配置规则只允许目的地址为 10.2.1.0/24 的报文通过，并指定规则的生效时间段，在 Device 的 Ten-GigabitEthernet3/1/1 的入方向上进行过滤；
- 为实现研发部在非工作时间不能访问管理部，需要创建 ACL 配置规则拒绝目的地址为 10.1.1.0/24 的报文，在 Device 的 Ten-GigabitEthernet3/1/1 的入方向上进行过滤；
- 缺省情况下，ACL 规则的匹配顺序为配置顺序，因此在此例中，需要先创建指定时间段内只允许目的地址为 10.2.1.0/24 报文通过的规则，再创建指定时间段内拒绝其他报文通过的规则。

4.4 配置步骤

(1) 配置管理部的网络权限

创建 IPv4 高级 ACL 3000。

```
<Device> system-view
[Device] acl advanced 3000
```

创建规则，过滤目的地址为 10.1.2.0/24 网段的报文。

```
[Device-acl-ipv4-adv-3000] rule deny ip destination 10.1.2.0 0.0.0.255
[Device-acl-ipv4-adv-3000] quit
```

配置包过滤功能，应用 IPv4 高级 ACL 3000 对端口 GigabitEthernet2/0/4 收到的 IP 报文进行过滤。

```
[Device] interface gigabitethernet 2/0/4
[Device-GigabitEthernet2/0/4] packet-filter 3000 inbound
[Device-GigabitEthernet2/0/4] quit
```

(2) 配置研发部的网络权限

配置时间段 worktime，指定周一至周五的 8:30～18:00 为工作时间。

```
[Device] time-range worktime 8:30 to 18:00 working-day
```

创建 IPv4 高级 ACL 3001。

```
[Device] acl advanced 3001
```

创建规则，允许时间段内目的地址为 10.2.1.0/24 网段的报文通过。

```
[Device-acl-ipv4-adv-3001] rule permit ip destination 10.2.1.0 0.0.0.255 time-range
worktime
```

创建规则，过滤时间段内其他的报文。

```
[Device-acl-ipv4-adv-3001] rule deny ip time-range worktime
```

创建规则，过滤目的地址为 10.1.1.0/24 网段的报文。

```
[Device-acl-ipv4-adv-3001] rule deny ip destination 10.1.1.0 0.0.0.255
[Device-acl-ipv4-adv-3001] quit
```

配置包过滤功能，应用 IPv4 高级 ACL 3001 对端口 GigabitEthernet2/0/3 收到的 IP 报文进行过滤。

```
[Device] interface gigabitethernet 2/0/3
[Device-GigabitEthernet2/0/3] packet-filter 3001 inbound
[Device-GigabitEthernet2/0/3] quit
```

4.5 验证配置

执行 **display packet-filter** 命令查看包过滤功能的应用状态。

```
[Device] display packet-filter interface inbound
Interface: GigabitEthernet2/0/3
 In-bound policy:
  IPv4 ACL 3001
Interface: GigabitEthernet2/0/4
 In-bound policy:
  IPv4 ACL 3000
```

上述信息显示 GigabitEthernet2/0/3 和 GigabitEthernet2/0/4 端口上已经正确应用了包过滤功能。

在周一的上午 9:30，从研发部的某台电脑上 ping Internet 上某个网站，结果无法 ping 通。

```
C:\>ping www.google.com

Pinging www.google.com [173.194.127.242] with 32 bytes of data:

Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50

Ping statistics for 173.194.127.242:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

```
    Minimum = 30ms, Maximum = 30ms, Average = 30ms
C:\>
```

在周一的上午 9:30，从管理部的某台电脑上 ping Internet 上某个网站，结果可以 ping 通。

```
C:\>ping www.google.com

Pinging www.google.com [173.194.127.242] with 32 bytes of data:

Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50

Ping statistics for 173.194.127.242:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 30ms, Maximum = 30ms, Average = 30ms
C:\>
```

在周一的晚上 19:30，从研发部的某台电脑上 ping Internet 上某个网站，结果可以 ping 通。

```
C:\>ping www.google.com

Pinging www.google.com [173.194.127.242] with 32 bytes of data:

Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50

Ping statistics for 173.194.127.242:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 30ms, Maximum = 30ms, Average = 30ms
C:\>
```

4.6 配置文件

```
#
interface GigabitEthernet2/0/3
 port link-mode route
 packet-filter 3001 inbound
#
interface GigabitEthernet2/0/4
 port link-mode route
 packet-filter 3000 inbound
#
 time-range worktime 08:30 to 18:00 working-day
#
acl advanced 3000
 rule 0 deny ip destination 10.1.2.0 0.0.0.255
```

```
#
acl advanced 3001
 rule 0 permit ip destination 10.2.1.0 0.0.0.255 time-range worktime
 rule 5 deny ip time-range worktime
 rule 10 deny ip destination 10.1.1.0 0.0.0.255
```

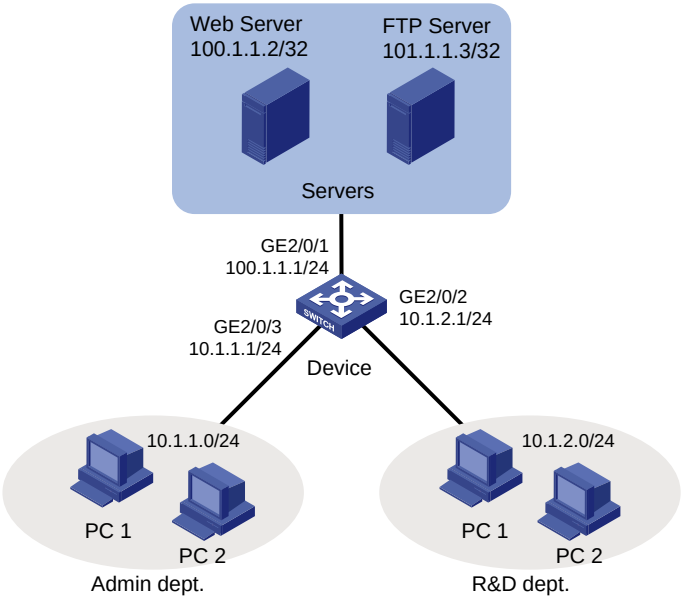
5 通过指定的 TCP 协议过滤流量典型配置举例

5.1 组网需求

如图 3 所示，某公司的网络分成管理部、研发部和服务器三个区域，通过 Device 设备互相连接。现要求通过 ACL 实现：

- Web 服务器只能向管理部的主机提供 HTTP 服务；
- FTP 服务器只能向研发部的主机提供 FTP 服务；
- 在主机与 Web 服务器之间进行通信时，仅允许由主机向服务器发起和建立 TCP 连接，不允许由服务器向主机发起 TCP 连接；在主机与 FTP 服务器之间进行通信时，不对 TCP 连接发起方进行限制。

图3 通过 IP 地址过滤流量配置组网图



5.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

5.3 配置思路

- 为了实现主机与 Web 服务器之间进行通信时，仅允许由主机向 Web 服务器发起和建立 TCP 连接，需要在高级 ACL 的规则中，指定 **established** 参数，用于匹配 TCP 报文头中 ACK 或 RST 置位的报文，即在已建立的 TCP 连接上传输的报文。
- 由于 TCP 连接发起方一般使用大于 1023 的 TCP 端口号，因此，由 Web 服务器向主机发送的端口号大于 1023、且 ACK 或 RST 位置位的报文，应视作已经存在的 TCP 连接，应该允许通过。其余的由 Web 服务器向主机发送的 TCP 报文都应拒绝通过。
- 要过滤 FTP 报文，需要同时拒绝 FTP 数据报文（TCP 端口号 20）和控制报文（TCP 端口号 21）通过。
- 要过滤 HTTP 服务，需要配置拒绝 TCP 目的端口号为 80 的报文（HTTP）通过的规则。

5.4 配置步骤

(1) 配置管理部的网络权限

创建 IPv4 高级 ACL 3000。

```
<Device> system-view
[Device] acl advanced 3000
```

创建规则，允许源地址为 100.1.1.1/32、目的地址为 10.1.1.0/24 网段、目的 TCP 端口号大于 1023、且 ACK 或 RST 位置位的报文通过。

```
[Device-acl-ipv4-adv-3000] rule permit tcp established source 100.1.1.1 0 destination
10.1.1.0 0.0.0.255 destination-port gt 1023
```

创建规则，拒绝源地址为 100.1.1.1/32、目的地址为 10.1.1.0/24 网段的 TCP 报文通过。

```
[Device-acl-ipv4-adv-3000] rule deny tcp source 100.1.1.1 0 destination 10.1.1.0
0.0.0.255
```

创建规则，拒绝源地址为 101.1.1.1/32 的 FTP 报文通过。

```
[Device-acl-ipv4-adv-3000] rule deny tcp source 101.1.1.1 0 source-port range 20 21
[Device-acl-ipv4-adv-3000] quit
```

配置包过滤功能，应用 IPv4 高级 ACL 3000 对端口 GigabitEthernet2/0/3 发出的报文进行过滤。

```
[Device] interface gigabitethernet 2/0/3
[Device-GigabitEthernet2/0/3] packet-filter 3000 outbound
[Device-GigabitEthernet2/0/3] quit
```

(2) 配置研发部的网络权限

创建 IPv4 高级 ACL 3001，配置规则拒绝源地址为 100.1.1.1/32 的 HTTP 报文通过。

```
[Device] acl advanced 3001
[Device-acl-ipv4-adv-3001] rule deny tcp source 100.1.1.1 0 source-port eq 80
[Device-acl-ipv4-adv-3001] quit
```

配置包过滤功能，应用 IPv4 高级 ACL 3001 对端口 GigabitEthernet2/0/2 发出的报文进行过滤。

```
[Device] interface gigabitethernet 2/0/2
[Device-GigabitEthernet2/0/2] packet-filter 3001 outbound
[Device-GigabitEthernet2/0/2] quit
```

5.5 验证配置

执行 **display packet-filter** 命令查看包过滤功能的应用状态。

```
[Device] display packet-filter interface outbound
Interface: GigabitEthernet2/0/2
 Out-bound policy:
  IPv4 ACL 3001
Interface: GigabitEthernet2/0/3
 Out-bound policy:
  IPv4 ACL 3000
```

上述信息显示 GigabitEthernet2/0/2 和 GigabitEthernet2/0/3 端口上已经正确应用了包过滤功能。

在管理部的主机执行 **telnet** 101.1.1.1 21 命令测试是否可以访问 FTP 服务器的 21 端口。

```
C:\>telnet 101.1.1.1 21
Connecting To 101.1.1.1...Could not open connection to the host, on port 21:
 Connect failed

C:\>
```

上述信息显示管理部的主机无法访问 FTP 服务器的 21 端口。

在管理部某台主机上设置共享文件夹，然后从 Web 服务器上 ping 该主机，可以 ping 通，但是无法访问共享文件夹。

```
C:\>ping 10.1.1.110

Pinging 10.1.1.110 with 32 bytes of data:
Reply from 10.1.1.110: bytes=32 time=2ms TTL=128
Reply from 10.1.1.110: bytes=32 time=14ms TTL=128
Reply from 10.1.1.110: bytes=32 time=1ms TTL=128
Reply from 10.1.1.110: bytes=32 time=1ms TTL=128

Ping statistics for 10.1.1.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 14ms, Average = 4ms

C:\>
```

在研发部的主机执行 **telnet** 100.1.1.1 80 命令测试是否可以访问 Web 服务器的 80 端口。

```
C:\>telnet 100.1.1.1 80
Connecting To 100.1.1.1...Could not open connection to the host, on port 80:
 Connect failed

C:\>
```

上述信息显示管理部的主机无法访问 FTP 服务器的 21 端口。

5.6 配置文件

```
#
interface GigabitEthernet2/0/2
```

```
 port link-mode route
 packet-filter 3001 outbound
#
interface GigabitEthernet2/0/3
 port link-mode route
 packet-filter 3000 outbound
#
acl advanced 3000
 rule 0 permit tcp source 100.1.1.1 0 destination 10.1.1.0 0.0.0.255 destination-port gt 1023
established
 rule 5 deny tcp source 100.1.1.1 0 destination 10.1.1.0 0.0.0.255
 rule 10 deny tcp source 101.1.1.1 0 source-port range ftp-data ftp
#
acl advanced 3001
 rule 0 deny tcp source 100.1.1.1 0 source-port eq www
```

6 相关资料

- H3C SR6600 SR6600-X 路由器 ACL 和 QoS 配置指导-R7607
- H3C SR6600 SR6600-X 路由器 ACL 和 QoS 命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

ATM 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 IPoA 典型配置指导 1
3.1 组网需求 1
3.2 配置思路 1
3.3 使用版本 2
3.4 配置注意事项 2
3.5 配置步骤 2
3.6 验证配置 3
3.7 配置文件 3
4 相关资料 4

1 简介

本文档介绍了 ATM 特性的 IPoA 应用的典型配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

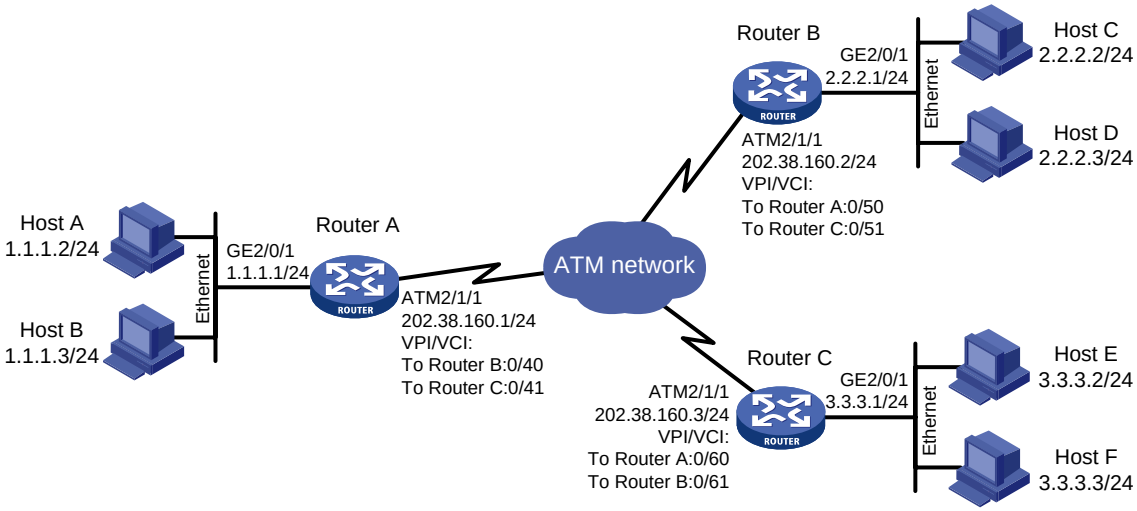
本文假设您已了解 ATM 特性。

3 IPoA 典型配置指导

3.1 组网需求

如图 1 所示，Router A 是某公司的总部的出口网关、Router B 和 Router C 分别是位于城市 B 和城市 C 的分公司的出口网关。为了安全、高效的传输总部及各个分公司的之间的数据，公司决定采用 IPoA 接入技术实现三个公司局域网之间的互访。

图1 IPoA 组网图



3.2 配置思路

在 ATM 上承载 IP 协议报文时，要想使高层协议能通过对端设备的 IP 地址寻址到对端设备，用户必须将本端的 PVC 与对端设备的 IP 地址关联起来，即配置 PVC 映射的 IP 地址。这样，系统就知道到达某个 IP 地址的报文通过哪个 PVC 进行发送了。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置注意事项

- ATM 接口只支持手工配置的 PVC（Permanent Virtual Circuit，永久虚电路），不支持通过信令建立的 SVC（Switched Virtual Circuit，交换虚电路）。
- ATM P2P 子接口只允许配置一个 PVC。
- 同一 PVC 下只能映射一个 IP 地址，且静态 IP 地址映射、default 映射和 InARP 映射三者同时只能配置其中一个。相同接口下不同的 PVC 不能映射到同一个 IP 地址。同一个接口下的 PVC 最多只能配置一个 default 映射。
- 如果是两台路由器接口直连，本端上映射到对端 IP 地址的 PVC 的 VPI/VCI 值必须和对端上映射到本端 IP 地址的 PVC 的 VPI/VCI 值相同。

3.5 配置步骤

(1) 配置 Router A

进入 ATM 接口，并为其配置 IP 地址。

```
<RouterA> system-view
[RouterA] interface atm 2/1/1
[RouterA-ATM2/1/1] ip address 202.38.160.1 255.255.255.0
```

创建 PVC，并指定承载 IP 协议。

```
[RouterA-ATM2/1/1] pvc to_b 0/40
[RouterA-ATM2/1/1-pvc-to_b-0/40] map ip 202.38.160.2
[RouterA-ATM2/1/1-pvc-to_b-0/40] quit
[RouterA-ATM2/1/1] pvc to_c 0/41
[RouterA-ATM2/1/1-pvc-to_c-0/41] map ip 202.38.160.3
```

(2) 配置 Router B

进入 ATM 接口，并为其配置 IP 地址。

```
<RouterB> system-view
[RouterB] interface atm 2/1/1
[RouterB-ATM2/1/1] ip address 202.38.160.2 255.255.255.0
```

创建 PVC，并指定承载 IP 协议。

```
[RouterB-ATM2/1/1] pvc to_a 0/50
[RouterB-ATM2/1/1-pvc-to_a-0/50] map ip 202.38.160.1
[RouterB-ATM2/1/1-pvc-to_a-0/50] quit
[RouterB-ATM2/1/1] pvc to_c 0/51
[RouterB-ATM2/1/1-pvc-to_c-0/51] map ip 202.38.160.3
```

(3) 配置 Router C

进入 ATM 接口，并为其配置 IP 地址。

```
<RouterC> system-view
[RouterC] interface atm 2/1/1
[RouterC-ATM2/1/1] ip address 202.38.160.3 255.255.255.0
```

创建 PVC，并指定承载 IP 协议。

```
[RouterC-ATM2/1/1] pvc to_a 0/60
[RouterC-ATM2/1/1-pvc-to_a-0/60] map ip 202.38.160.1
[RouterC-ATM2/1/1-pvc-to_a-0/60] quit
[RouterC-ATM2/1/1] pvc to_b 0/61
[RouterC-ATM2/1/1-pvc-to_b-0/61] map ip 202.38.160.2
```

3.6 验证配置

在 Router A 上通过 **display atm map-info** 命令所有接口下所有 PVC 的映射信息，发现 PVC 的状态为 UP。

```
<RouterA> display atm map-info
ATM2/1/1
  PVC 0/40:
   Protocol: IP, IP address: 202.38.160.2, State: UP
  PVC 0/41:
   Protocol: IP, IP address: 202.38.160.3, State: UP
```

Router A 和 Router B 可以互相 ping 通对方。

```
[RouterA] ping 202.38.160.2
Ping 202.38.160.2 (202.38.160.2): 56 data bytes, press CTRL_C to break
56 bytes from 202.38.160.2: icmp_seq=0 ttl=255 time=76.007 ms
56 bytes from 202.38.160.2: icmp_seq=1 ttl=255 time=8.790 ms
56 bytes from 202.38.160.2: icmp_seq=2 ttl=255 time=1.630 ms
56 bytes from 202.38.160.2: icmp_seq=3 ttl=255 time=0.841 ms
56 bytes from 202.38.160.2: icmp_seq=4 ttl=255 time=1.012 ms
--- Ping statistics for 202.38.160.2---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.841/17.656/76.007/29.326 ms
```

3.7 配置文件

- Router A：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 1.1.1.1 255.255.255.0
#
interface ATM2/1/1
ip address 202.38.160.1 255.255.255.0
 pvc to_b 0/40
  map ip 202.38.160.2
 pvc to_c 0/41
  map ip 202.38.160.3
#
```

- Router B：

```
#
interface GigabitEthernet2/0/1
```

```
 port link-mode route
 ip address 2.2.2.1 255.255.255.0
#
interface ATM2/1/1
ip address 202.38.160.2 255.255.255.0
 pvc to_a 0/50
  map ip 202.38.160.1
 pvc to_c 0/51
  map ip 202.38.160.3
#
```

- Router C：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 3.3.3.1 255.255.255.0
#
interface ATM2/1/1
ip address 202.38.160.3 255.255.255.0
 pvc to_a 0/60
  map ip 202.38.160.1
 pvc to_c 0/61
  map ip 202.38.160.2
#
```

4 相关资料

- H3C SR6600 SR6600-X 路由器 二层技术-广域网接入配置指导-R7607
- H3C SR6600 SR6600-X 路由器 二层技术-广域网接入命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

BFD 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1

2 配置前提 1

3 使用限制 1

4 VRRP 与 BFD、Track 联动配置举例 1

4.1 组网需求 1

4.2 配置思路 2

4.3 使用版本 3

4.4 配置注意事项 3

4.5 配置步骤 3

4.5.1 配置各接口的 IP 地址 3

4.5.2 配置上行设备 Device E 和 Device F 到 VRRP 组虚拟 IP 的静态路由 3

4.5.3 配置 VRRP 备份组 3

4.5.4 配置 BFD 功能 4

4.5.5 配置 Track 项 4

4.6 验证配置 5

4.7 配置文件 9

5 静态路由与 BFD 联动配置举例 11

5.1 组网需求 11

5.2 配置思路 11

5.3 使用版本 11

5.4 配置步骤 12

5.4.1 配置各接口的 IP 地址 12

5.4.2 配置静态路由 12

5.4.3 配置 Device A 的 BFD 功能 12

5.5 验证配置 13

5.6 配置文件 13

6 RIP 与 BFD 联动配置举例 15

6.1 组网需求 15

6.2 配置思路 15

6.3 使用版本 16

6.4 配置步骤 16

6.4.1 配置各接口的 IP 地址 16

6.4.2 配置 RIP 基本功能 ····· 16
6.4.3 配置 Device A 的 BFD 参数 ····· 17
6.5 验证配置 ····· 17
6.6 配置文件 ····· 18
7 OSPF 与 BFD 联动配置举例 ····· 20
7.1 组网需求 ····· 20
7.2 配置思路 ····· 20
7.3 使用版本 ····· 21
7.4 配置步骤 ····· 21
7.4.1 配置各接口的 IP 地址 ····· 21
7.4.2 配置 OSPF 基本功能 ····· 21
7.4.3 配置 BFD 功能 ····· 22
7.5 验证配置 ····· 22
7.6 配置文件 ····· 25
8 IS-IS 与 BFD 联动配置举例 ····· 26
8.1 组网需求 ····· 26
8.2 配置思路 ····· 27
8.3 使用版本 ····· 27
8.4 配置步骤 ····· 27
8.4.1 配置各接口的 IP 地址 ····· 27
8.4.2 配置 IS-IS 基本功能 ····· 27
8.4.3 配置 BFD 功能 ····· 28
8.5 验证配置 ····· 29
8.6 配置文件 ····· 31
9 BGP 与 BFD 联动配置举例 ····· 32
9.1 组网需求 ····· 32
9.2 配置思路 ····· 33
9.3 使用版本 ····· 33
9.4 配置步骤 ····· 33
9.4.1 配置各接口的 IP 地址 ····· 33
9.4.2 在 AS 100 内配置 OSPF 功能，保证设备间路由可达 ····· 34
9.4.3 配置 BGP 功能 ····· 34
9.4.4 配置路由策略 ····· 36
9.4.5 配置 BFD 功能 ····· 37
9.5 验证配置 ····· 37
9.6 配置文件 ····· 40

10 策略路由与 BFD 联动配置举例 ····· 43
10.1 组网需求 ····· 43
10.2 配置思路 ····· 44
10.3 使用版本 ····· 44
10.4 配置步骤 ····· 44
10.4.1 配置各接口的 IP 地址 ····· 44
10.4.2 配置静态路由 ····· 44
10.4.3 配置 Device A 上的路由策略 ····· 44
10.4.4 配置 BFD 功能，并创建和 BFD 会话关联的 Track 项 11，检测 Device B 是否可达 ····· 45
10.5 验证配置 ····· 45
10.6 配置文件 ····· 46
11 BFD 单跳检测三层链路配置举例 ····· 47
11.1 组网需求 ····· 47
11.2 使用版本 ····· 48
11.3 配置步骤 ····· 48
11.3.1 配置 Device A ····· 48
11.3.2 配置 Device B ····· 48
11.4 验证配置 ····· 49
11.5 配置文件 ····· 50
12 BFD 检测三层静态聚合组配置举例 ····· 51
12.1 组网需求 ····· 51
12.2 使用版本 ····· 51
12.3 配置注意事项 ····· 51
12.4 配置步骤 ····· 51
12.4.1 配置 Device A ····· 51
12.4.2 配置 Device B ····· 52
12.5 验证配置 ····· 53
12.6 配置文件 ····· 57
13 相关资料 ····· 58

1 简介

本文档介绍了 BFD 配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文假设您已了解 BFD 特性、VRRP 特性、Track 特性以及 OSPF、IS-IS 等路由协议。

3 使用限制

IP 隧道（如 IPv6 over IPv4 隧道）不支持 BFD 检测。

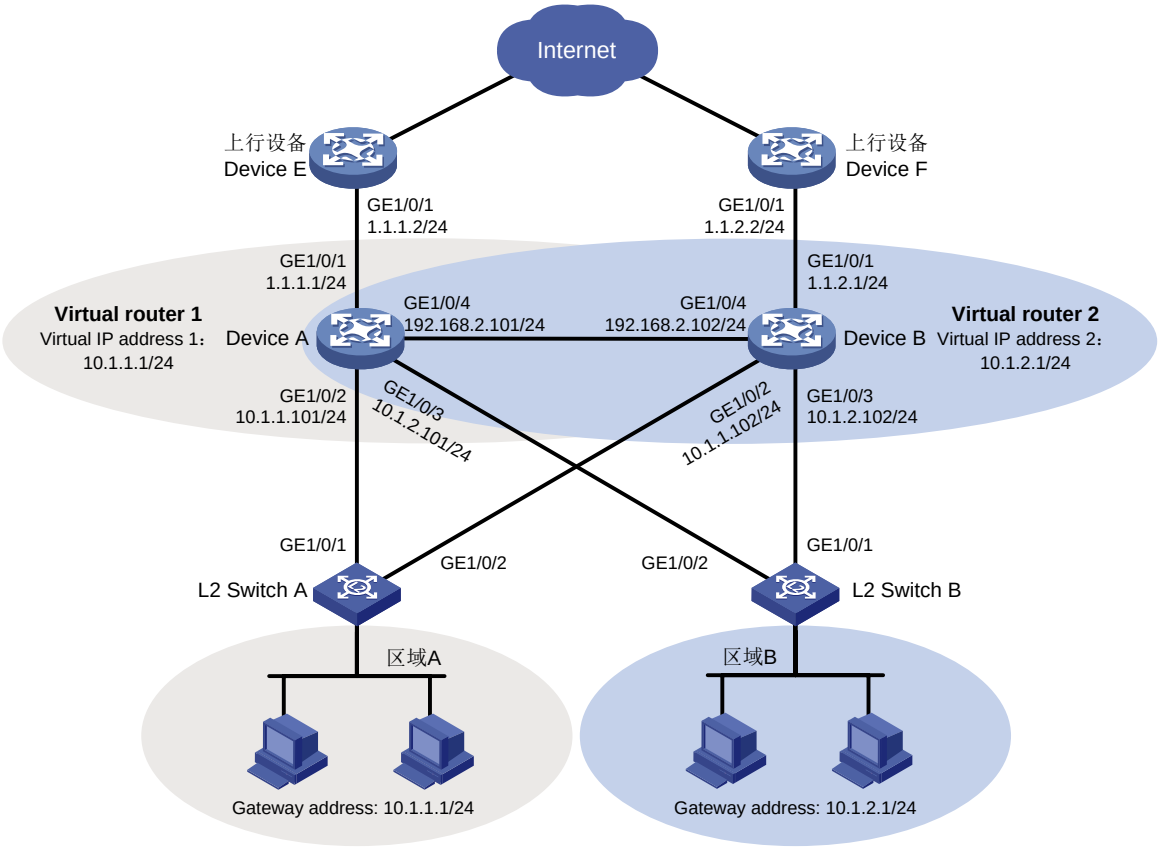
4 VRRP 与 BFD、Track 联动配置举例

4.1 组网需求

如图 1所示，区域 A 和区域 B 用户所在网络的出口处部署了两台汇聚层设备（Device A 和 Device B）。现要求使用 VRRP 与 BFD、Track 联动功能，实现以下需求：

- 在 Device A 和 Device B 上分别配置两个 VRRP 备份组，Device A 是 VRRP 备份组 1 中的 Master 设备，Device B 是 VRRP 备份组 2 中的 Master 设备；
- 在正常情况下，区域 A 的用户将 VRRP 备份组 1 作为缺省网关，通过 Device A 进行数据转发，区域 B 用户将 VRRP 备份组 2 作为缺省网关，通过 Device B 进行数据转发。当一台网关设备出现故障时，另一台网关设备能够迅速承担受影响区域内主机流量的转发任务；
- 当网关设备 Device A（Device B）自身出现故障，或其上行接口出现故障时，局域网中的主机可以通过另一台设备网关设备 Device B（Device A）继续通信，避免通信中断；当 Device A（Device B）故障恢复后，继续承担网关功能；
- 当 Device A 或 Device B 的下行链路出现故障时，局域网中的主机通过接入设备 L2 Switch A 或 L2 Switch B 的 GigabitEthernet1/0/2 端口将数据转发给网关设备继续通信，避免通信中断；当 Device A 或 Device B 的下行链路故障恢复后，继续由 L2 Switch A 或 L2 Switch B 的 GigabitEthernet1/0/1 端口将数据发送给网关设备。

图1 VRRP 与 BFD、Track 联动配置组网图



4.2 配置思路

- 为了实现不同区域中用户数据流的负载分担，需要在 Device A 和 Device B 上分别创建两个 VRRP 备份组，并配置区域 A 内的主机都将 VRRP 备份组 1 作为网关，区域 B 内的主机都将 VRRP 备份组 2 作为网关；
- 为使 Device A 优先被选举为 VRRP 备份组 1 的 Master 设备，需要为其在 VRRP 备份组 1 中配置较高的优先级；为使 Device B 优先被选举为 VRRP 备份组 2 的 Master 设备，需要为其在 VRRP 备份组 2 中配置较高的优先级；
- 配置两个 VRRP 备份组都工作在抢占模式，以保证原 Master 设备故障恢复后，能再次抢占成为 Master；
- 通过 Device A 与 Device B 上配置 BFD 功能监视其上行接口的状态，当监测到其上行接口故障时，Device A 或 Device B 的优先级会自动降低指定的数额，使 VRRP 备份组 1 内 Device B 的优先级高于 Device A，或 VRRP 备份组 2 内 Device A 的优先级高于 Device B，从而实现主备切换；

4.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.4 配置注意事项

- 请务必保证备份组中的所有设备上配置的 VRRP 版本一致，否则备份组无法正常工作。
- 为了避免对端发送大量的 ICMP 重定向报文造成网络拥塞，建议不要将 BFD echo 报文的源 IP 地址配置为属于该设备任何一个接口所在网段。
- 建议将备份组的虚拟 IP 地址和备份组中设备下行接口的 IP 地址配置为同一网段，否则可能导致局域网内的主机无法访问外部网络。

4.5 配置步骤

4.5.1 配置各接口的 IP 地址

(1) 配置 Device A 各接口的 IP 地址

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 1.1.1.1 24
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 请参考以上方法配置图 1 中其它接口的 IP 地址，配置步骤这里省略

4.5.2 配置上行设备 Device E 和 Device F 到 VRRP 组虚拟 IP 的静态路由

(1) 配置 Device E

配置 Device E 到 VRRP 备份组 1 和 VRRP 备份组 2 的虚拟 IP 地址的静态路由。

```
<DeviceE> system-view
[DeviceE] ip route-static 10.1.1.0 255.255.255.0 1.1.1.1
[DeviceE] ip route-static 10.1.2.0 255.255.255.0 1.1.1.1
```

(2) 配置 Device F

配置 Device F 到 VRRP 备份组 1 和 VRRP 备份组 2 的虚拟 IP 地址的静态路由。

```
<DeviceE> system-view
[DeviceF] ip route-static 10.1.1.0 255.255.255.0 1.1.2.1
[DeviceF] ip route-static 10.1.2.0 255.255.255.0 1.1.2.1
```

4.5.3 配置 VRRP 备份组

(1) 配置 Device A

配置 VRRP 备份组 1 的虚拟 IP 地址为 10.1.1.1，抢占延时为 5s。并且 VRRP 备份组 1 中 Device A 的优先级为 110，高于 Device B，成为 VRRP 备份组 1 的 Master。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] vrrp vrid 1 virtual-ip 10.1.1.1
[DeviceA-GigabitEthernet1/0/2] vrrp vrid 1 priority 110
[DeviceA-GigabitEthernet1/0/2] vrrp vrid 1 preempt-mode delay 500
```

```
[DeviceA-GigabitEthernet1/0/2] quit
```

配置 VRRP 备份组 2 的虚拟 IP 地址为 10.1.2.1，抢占延时为 5s。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] vrrp vrid 2 virtual-ip 10.1.2.1
[DeviceA-GigabitEthernet1/0/3] vrrp vrid 2 preempt-mode delay 500
[DeviceA–GigabitEthernet1/0/3] quit
```

(2) 配置 Device B

配置 VRRP 备份组 1 的虚拟 IP 地址为 10.1.1.1，抢占延时为 5s。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] vrrp vrid 1 virtual-ip 10.1.1.1
[DeviceB-GigabitEthernet1/0/2] vrrp vrid 1 preempt-mode delay 500
[DeviceB-GigabitEthernet1/0/2] quit
```

配置 VRRP 备份组 2 的虚拟 IP 地址为 10.1.2.1，抢占延时为 5s。并且 VRRP 备份组 2 中 Device B 的优先级为 110，高于 Device A，成为 VRRP 备份组 2 的 Master。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] vrrp vrid 2 virtual-ip 10.1.2.1
[DeviceB-GigabitEthernet1/0/3] vrrp vrid 2 priority 110
[DeviceB-GigabitEthernet1/0/3] vrrp vrid 2 preempt-mode delay 500
[DeviceB–GigabitEthernet1/0/3] quit
```

4.5.4 配置 BFD 功能

(1) 配置 Device A

配置 BFD echo 报文方式的 Source IP，IP 地址可以任意指定，不要与实际接口地址相同。

```
[DeviceA] bfd echo-source-ip 10.10.10.10
```

(2) 配置 Device B

配置 BFD echo 报文方式的 Source IP，IP 地址可以任意指定，不要与实际接口地址相同。

```
[DeviceB] bfd echo-source-ip 11.11.11.11
```

4.5.5 配置 Track 项

(1) 配置 Device A

创建和 BFD 会话关联的 Track 项 1，检测上行设备 Device E 是否可达。

```
[DeviceA] track 1 bfd echo interface gigabitethernet 1/0/1 remote ip 1.1.1.2 local ip
1.1.1.1
```

配置备份组 1 监视 Track 项 1 的状态，当 Track 项状态为 Negative 时，Device A 在 VRRP 备份组 1 中的优先级减小 20，低于 Device B，以便 Device B 抢占成为 Master。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] vrrp vrid 1 track 1 priority reduced 20
[DeviceA-GigabitEthernet1/0/2] quit
```

(2) 配置 Device B

创建和 BFD 会话关联的 Track 项 1，检测上行设备 Device F 是否可达。

```
[DeviceB] track 1 bfd echo interface gigabitethernet 1/0/1 remote ip 1.1.2.2 local ip
1.1.2.1
```

配置备份组 2 监视 Track 项 1 的状态，当 Track 项状态为 Negative 时，Device B 在 VRRP 备份组 2 中的优先级减小 20，低于 Device A，以便 Device A 抢占成为 Master。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] vrrp vrid 2 track 1 priority reduced 20
[DeviceB-GigabitEthernet1/0/3] quit
```

4.6 验证配置

(1) 网关设备 Device A、Device B 和链路均正常工作时，验证局域网内主机是否可以与外部网络通信

检查区域 A 的主机到目的端 1.1.1.2 是否可达。

```
<host A> ping 1.1.1.2
PING 1.1.1.2 (1.1.1.2): 56 data bytes
56 bytes from 1.1.1.2: seq=0 ttl=128 time=22.43 ms
56 bytes from 1.1.1.2: seq=1 ttl=128 time=7.17 ms
56 bytes from 1.1.1.2: seq=2 ttl=128 time=8.91 ms
56 bytes from 1.1.1.2: seq=3 ttl=128 time=7.45 ms
56 bytes from 1.1.1.2: seq=4 ttl=128 time=9.11 ms

--- 1.1.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.17/11.01/22.43 ms
```

检查区域 B 的主机到目的端 1.1.2.2 是否可达。

```
<host C> ping 1.1.2.2
PING 1.1.2.2 (1.1.2.2): 56 data bytes
56 bytes from 1.1.2.2: seq=0 ttl=128 time=22.43 ms
56 bytes from 1.1.2.2: seq=1 ttl=128 time=7.17 ms
56 bytes from 1.1.2.2: seq=2 ttl=128 time=8.91 ms
56 bytes from 1.1.2.2: seq=3 ttl=128 time=7.45 ms
56 bytes from 1.1.2.2: seq=4 ttl=128 time=9.11 ms

--- 1.1.2.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.17/11.01/22.43 ms
```

以上显示信息表示网关设备 Device A、Device B 和链路均正常工作时，区域 A 的主机和区域 B 的主机都可以访问 Internet。

查看 Device A 的 BFD 会话。

```
[DeviceA] 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
 65            1.1.1.1         1.1.1.2         Up       500ms       XGE1/0/1
```

以上显示信息表示 BFD 会话已经建立。

显示 Device A 上备份组的详细信息。

```
[DeviceA] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
   Interface GigabitEthernet1/0/2
     VRID           : 1                 Adver Timer  : 100
     Admin Status   : Up                State        : Master
     Config Pri     : 110               Running Pri  : 110
     Preempt Mode   : Yes               Delay Time   : 500
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 10.1.1.101
   VRRP Track Information:
     Track Object   : 1                 State : Positive   Pri Reduced : 20

   Interface GigabitEthernet1/0/3
     VRID           : 2                 Adver Timer  : 100
     Admin Status   : Up                State        : Backup
     Config Pri     : 100               Running Pri  : 100
     Preempt Mode   : Yes               Delay Time   : 500
     Become Master  : 3600ms left
     Auth Type      : None
     Virtual IP     : 10.1.2.1
     Master IP      : 10.1.2.102
```

显示 Device B 上备份组的详细信息。

```
[DeviceB] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
   Interface GigabitEthernet1/0/2
     VRID           : 1                 Adver Timer  : 100
     Admin Status   : Up                State        : Backup
     Config Pri     : 100               Running Pri  : 100
     Preempt Mode   : Yes               Delay Time   : 500
     Become Master  : 3100ms left
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Master IP      : 10.1.1.101

   Interface GigabitEthernet1/0/3
     VRID           : 2                 Adver Timer  : 100
     Admin Status   : Up                State        : Master
     Config Pri     : 110               Running Pri  : 110
     Preempt Mode   : Yes               Delay Time   : 500
     Auth Type      : None
     Virtual IP     : 10.1.2.1
     Virtual MAC    : 0000-5e00-0102
```

```
    Master IP      : 10.1.2.102
  VRRP Track Information:
    Track Object   : 1                    State : Positive   Pri Reduced : 20
```

以上显示信息表示在备份组 1 中 Device A 为 Master，Device B 为 Backup，缺省网关为 10.1.1.1/24 的主机通过 Device A 访问 Internet；备份组 2 中 Device A 为 Backup，Device B 为 Master，缺省网关为 10.1.2.1/24 的主机通过 Device B 访问 Internet。

(2) 当 Device A 监视的上行设备或上行链路状态为 down 时，验证局域网内主机是否可以与外部网络通信

检查区域 A 的主机到目的端 1.1.1.2 是否可达。

```
<host A> ping 1.1.1.2
PING 1.1.1.2 (1.1.1.2): 56 data bytes
56 bytes from 1.1.1.2: seq=0 ttl=128 time=22.43 ms
56 bytes from 1.1.1.2: seq=1 ttl=128 time=7.17 ms
56 bytes from 1.1.1.2: seq=2 ttl=128 time=8.91 ms
56 bytes from 1.1.1.2: seq=3 ttl=128 time=7.45 ms
56 bytes from 1.1.1.2: seq=4 ttl=128 time=9.11 ms

--- 1.1.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.17/11.01/22.43 ms
```

检查区域 B 的主机到目的端 1.1.1.2 是否可达。

```
<host C> ping 1.1.2.2
PING 1.1.2.2 (1.1.2.2): 56 data bytes
56 bytes from 1.1.2.2: seq=0 ttl=128 time=22.43 ms
56 bytes from 1.1.2.2: seq=1 ttl=128 time=7.17 ms
56 bytes from 1.1.2.2: seq=2 ttl=128 time=8.91 ms
56 bytes from 1.1.2.2: seq=3 ttl=128 time=7.45 ms
56 bytes from 1.1.2.2: seq=4 ttl=128 time=9.11 ms

--- 1.1.2.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.17/11.01/22.43 ms
```

以上显示信息表示当 Device A 监视的上行设备或上行链路状态为 down 时，区域 A 的主机和区域 B 的主机都可以访问 Internet。

查看 Device A 上的 BFD 会话。

```
[DeviceA] display bfd session
 Total Session Num: 1     Up Session Num: 0     Init Mode: Active

 IPv4 Session Working Under Echo Mode:

 LD             SourceAddr      DestAddr        State    Holdtime    Interface
 65             1.1.1.1         1.1.1.2         Down       /         XGE1/0/1
```

以上显示信息表示 BFD 会话已经终止。

显示 Device B 上备份组的详细信息。

```
[DeviceB] display vrrp verbose
IPv4 Virtual Router Information:
```

```
 Running Mode      : Standard
 Total number of virtual routers : 2
   Interface GigabitEthernet1/0/2
     VRID            : 1                   Adver Timer  : 100
     Admin Status    : Up                  State        : Master
     Config Pri      : 100                 Running Pri  : 100
     Preempt Mode    : Yes                 Delay Time   : 500
     Auth Type       : None
     Virtual IP      : 10.1.1.1
     Virtual MAC     : 0000-5e00-0101
     Master IP       : 10.1.1.102

   Interface GigabitEthernet1/0/2
     VRID            : 2                   Adver Timer  : 100
     Admin Status    : Up                  State        : Master
     Config Pri      : 110                 Running Pri  : 110
     Preempt Mode    : Yes                 Delay Time   : 500
     Auth Type       : None
     Virtual IP      : 10.1.2.1
     Virtual MAC     : 0000-5e00-0102
     Master IP       : 10.1.2.102
   VRRP Track Information:
     Track Object    : 1                   State : Positive   Pri Reduced : 20
```

以上显示信息表示当 Device A 监视的上行设备或上行链路状态为 down 时，Device B 抢占成为 VRRP 备份组 1 的 Master，区域 A 的主机通过 Device B 与外界通信。

当上行设备或上行链路状态恢复为 UP 后，查看 Device A 上的 BFD 会话。

```
[DeviceA] 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
 65             1.1.1.1         1.1.1.2         Up       1000ms      XGE1/0/1
```

以上显示信息表示 BFD 会话已经恢复。

当上行设备或上行链路状态恢复为 UP 后，显示 Device A 上备份组的详细信息。

```
[DeviceA] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
   Interface GigabitEthernet1/0/2
     VRID            : 1                   Adver Timer  : 100
     Admin Status    : Up                  State        : Master
     Config Pri      : 110                 Running Pri  : 110
     Preempt Mode    : Yes                 Delay Time   : 500
     Auth Type       : None
     Virtual IP      : 10.1.1.1
```

```
    Virtual MAC     : 0000-5e00-0101
    Master IP       : 10.1.1.101
  VRRP Track Information:
    Track Object    : 1                    State : Positive   Pri Reduced : 20

  Interface GigabitEthernet1/0/3
    VRID            : 2                    Adver Timer  : 100
    Admin Status    : Up                   State        : Backup
    Config Pri      : 100                  Running Pri  : 100
    Preempt Mode    : Yes                  Delay Time   : 500
    Become Master   : 3550ms left
    Auth Type       : None
    Virtual IP      : 10.1.2.1
    Master IP       : 10.1.2.102
```

以上显示信息表示当上行设备或上行链路状态恢复为 UP 后，Device A 在 VRRP 备份组 1 中恢复为原来的优先级并抢占成为该备份组的 Master，区域 B 内的主机通过 Device A 与外界通信。

4.7 配置文件

- Device A：

```
#
 bfd echo-source-ip 10.10.10.10
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.1.1.101 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.1
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode delay 500
 vrrp vrid 1 track 1 reduced 20
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 10.1.2.101 255.255.255.0
vrrp vrid 2 virtual-ip 10.1.2.1
 vrrp vrid 2 preempt-mode delay 500
#
interface GigabitEthernet1/0/4
 port link-mode route
 ip address 192.168.2.101 255.255.255.0
#
 track 1 bfd echo interface GigabitEthernet1/0/1 remote ip 1.1.1.2 local ip 1.1.1.1
```

- Device B：

```
#
 bfd echo-source-ip 11.11.11.11
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 1.1.2.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.1.1.102 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.1
 vrrp vrid 1 preempt-mode delay 500
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 10.1.2.102 255.255.255.0
 vrrp vrid 2 virtual-ip 10.1.2.1
 vrrp vrid 2 priority 110
 vrrp vrid 2 preempt-mode delay 500
 vrrp vrid 2 track 1 reduced 20
#
interface GigabitEthernet1/0/4
 port link-mode route
 ip address 192.168.2.102 255.255.255.0
#
 track 1 bfd echo interface GigabitEthernet1/0/1 remote ip 1.1.2.2 local ip 1.1.2.1
```

- Device E：

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 1.1.1.2 255.255.255.0
#
 ip route-static 10.1.1.0 255.255.255.0 1.1.1.1
 ip route-static 10.1.2.0 255.255.255.0 1.1.1.1
#
```

- Device F：

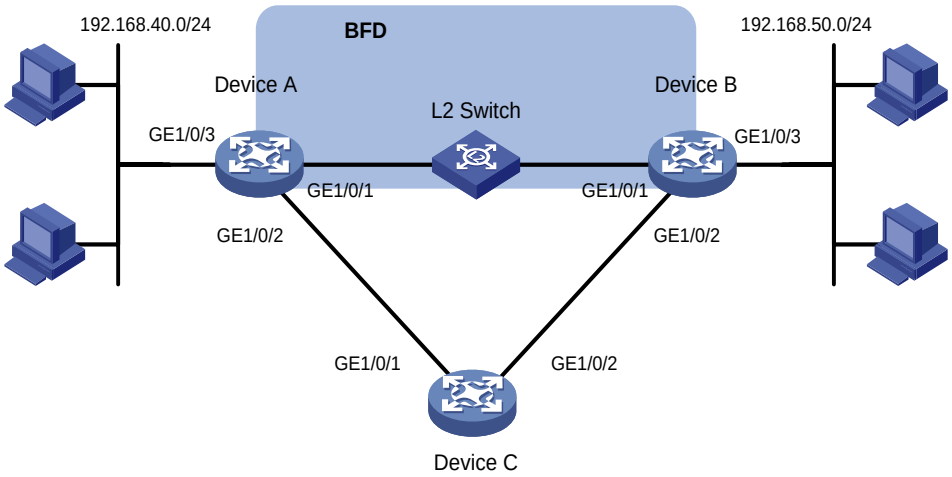
```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 1.1.2.2 255.255.255.0
#
 ip route-static 10.1.1.0 255.255.255.0 1.1.2.1
 ip route-static 10.1.2.0 255.255.255.0 1.1.2.1
#
```

5 静态路由与 BFD 联动配置举例

5.1 组网需求

某公司内部网络如图 2 所示，从 Device A 到 Device B 有两条转发路径，下一跳分别为 Device B 和 Device C。由于 Device A 和 Device B 之间物理距离较远，通过一个二层交换机 L2 Switch 作为中继。假设 Device B 不支持 BFD，要求在 Device A 上使用静态路由与 BFD 联动技术，实现当 Device B 与二层交换机 L2 Switch 之间的链路出现故障（如链路 down）时，Device A 能快速感知，并将流量切换到 Device C 的链路上。

图2 静态路由与 BFD 联动配置组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	XGE1/0/1	192.168.10.101/24	Device B	XGE1/0/1	192.168.10.102/24
	XGE1/0/2	192.168.20.101/24		XGE1/0/2	192.168.30.101/24
	XGE1/0/3	192.168.40.101/24		XGE1/0/3	192.168.50.101/24
Device C	XGE1/0/1	192.168.20.102/24			
	XGE1/0/2	192.168.30.102/24			

5.2 配置思路

- 由于需要两端设备均支持BFD，才能够使用控制报文方式，本例中Device B不支持BFD，在 Device A 上配置的 BFD 功能仅能使用 echo 报文方式。
- echo 报文方式下必须配置 echo 报文的源 IP 地址。IP 地址可以任意指定，不需要与实际接口地址对应。建议不要将 echo 报文的源 IP 地址配置为属于该设备任何一个接口所在网段，避免对端发送大量的 ICMP 重定向报文造成网络拥塞。

5.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

5.4 配置步骤

5.4.1 配置各接口的 IP 地址

(1) 配置 Device A 各接口的 IP 地址

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 192.168.10.101 24
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 请参考以上方法配置图 2 中其它接口的 IP 地址，配置步骤这里省略

5.4.2 配置静态路由

(1) 配置 Device A

配置 Device A 到 192.168.50.0/24 网段的静态路由，Device A 到 Device B 的流量优先走 Device A –> L2 Switch–> Device B 链路，当此链路发生故障时，流量切换到 Device A –> Device C–> Device B 链路上。

```
[DeviceA] ip route-static 192.168.50.0 24 gigabitethernet 1/0/1 192.168.10.102 bfd
echo-packet
[DeviceA] ip route-static 192.168.50.0 24 gigabitethernet 1/0/2 192.168.20.102
preference 65
```

(2) 配置 Device B

配置 Device B 到 192.168.40.0/24 网段的静态路由，Device B 到 Device A 的流量优先走 Device B –> L2 Switch–> Device A 链路，当此链路发生故障时，流量切换到 Device B –> Device C–> Device A 链路上。

```
[DeviceB] ip route-static 192.168.40.0 24 gigabitethernet 1/0/1 192.168.10.101
[DeviceB] ip route-static 192.168.40.0 24 gigabitethernet 1/0/2 192.168.30.102
preference 65
```

(3) 配置 Device C

配置 Device C 到 192.168.40.0/24 和 192.168.50.0/24 网段的静态路由。

```
[DeviceC] ip route-static 192.168.40.0 24 gigabitethernet 1/0/1 192.168.20.101
[DeviceC] ip route-static 192.168.50.0 24 gigabitethernet 1/0/2 192.168.30.101
```

5.4.3 配置 Device A 的 BFD 功能

静态路由支持的 BFD 会话方式为 echo 报文方式，该方式下必须配置 BFD echo 报文的源 IP 地址。IP 地址可以任意指定，不需要与实际接口地址对应。建议不要将 BFD echo 报文的源 IP 地址配置为属于该设备任何一个接口所在网段。

```
[DeviceA] bfd echo-source-ip 10.10.10.10
```

配置接口接收 BFD echo 报文的最小时间间隔为 100ms，单跳 BFD 检测时间倍数为 3。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] bfd min-echo-receive-interval 100
[DeviceA-GigabitEthernet1/0/1] bfd detect-multiplier 3
[DeviceA-GigabitEthernet1/0/1] quit
```

5.5 验证配置

(1) Device A 和 Device B 设备及之间的链路均正常工作时

在 Device A 查看静态路由信息。

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

Summary Count : 2

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

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
192.168.50.0/24     Static 60   0            192.168.10.102  XGE1/0/1

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

以上显示信息表示 Device A 经过 L2 Switch 到达 Device B。

查看 BFD 会话。

```
[DeviceA] display bfd session

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

 IPv4 Session Working Under Echo Mode:

 LD/RD          SourceAddr      DestAddr        State    Holdtime    Interface
67              192.168.10.101  192.168.10.102  Up       300ms       XGE1/0/1
```

以上显示信息表示 BFD 会话已经创建。

(2) Device B 与 L2 Switch 之间的链路出现故障时

查看静态路由。

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

Summary Count : 1

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

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
192.168.50.0/24     Static 65   0            192.168.20.102  XGE1/0/2

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

以上显示信息表示 Device A 经过 Device C 到达 Device B。

5.6 配置文件

- Device A：

```
#
 bfd echo-source-ip 10.10.10.10
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.10.101 255.255.255.0
 bfd min-echo-receive-interval 100
 bfd detect-multiplier 3
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 192.168.20.101 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 192.168.40.101 255.255.255.0
#
 ip route-static 192.168.50.0 24 GigabitEthernet1/0/1 192.168.10.102 bfd echo-packet
 ip route-static 192.168.50.0 24 GigabitEthernet1/0/2 192.168.20.102 preference 65
#
```

- Device B：

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.10.102 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 192.168.30.101 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 192.168.50.101 255.255.255.0
#
 ip route-static 192.168.40.0 24 GigabitEthernet1/0/1 192.168.10.101
 ip route-static 192.168.40.0 24 GigabitEthernet1/0/2 192.168.30.102 preference 65
#
```

- Device C：

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.20.102 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 192.168.30.102 255.255.255.0
#
 ip route-static 192.168.40.0 24 GigabitEthernet1/0/1 192.168.20.101
```

```
 ip route-static 192.168.50.0 24 GigabitEthernet1/0/2 192.168.30.101
#
```

6 RIP 与 BFD 联动配置举例

6.1 组网需求

如图 3 所示，某公司通过一台二层交换机作为中继将两个相距较远的部门连接。Device A、Device B、Device C 上运行 RIP，建立 RIP 邻居关系，保证网络层相互可达。

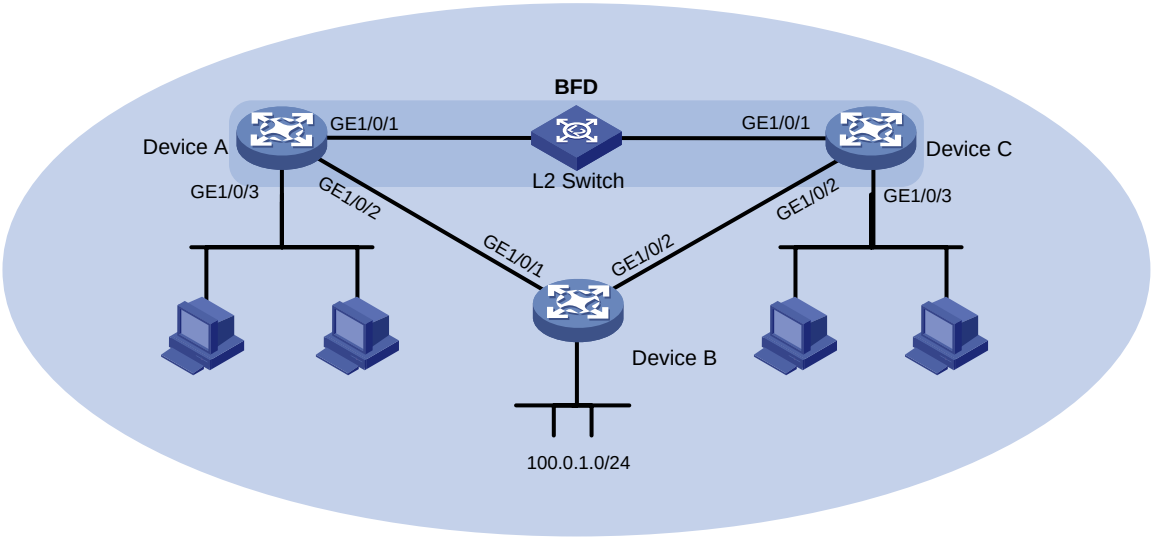
公司希望在 Device A 上使用 RIP 与 BFD 联动技术，实现当 Device C 与二层交换机之间的链路出现故障（如链路 down）时，BFD 能够快速感知并通告 RIP 协议。

已知 Device C 不支持 BFD 功能，公司希望使用 RIP 与 BFD 联动技术，采用 BFD echo 报文方式实现当 Device A 或 Device C 与二层交换机之间的链路出现故障时，BFD 能够快速感知并通告 RIP 协议。

现要求通过在 Device A 和 Device C 上配置 RIP 与 BFD 联动功能，实现：

- 监测通过 L2 Switch 通信的链路；
- 当链路出现故障时设备能够快速感知并通告 RIP 协议，快速切换到 Device B 链路进行通信。

图3 RIP 与 BFD 联动配置组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	XGE1/0/1	10.1.0.101/24	Device B	XGE1/0/1	192.168.0.102/24
	XGE1/0/2	192.168.0.101/24		XGE1/0/2	13.1.1.101/24
	XGE1/0/3	120.1.1.1/24			
Device C	XGE1/0/1	10.1.0.102/24			
	XGE1/0/2	13.1.1.102/24			
	XGE1/0/3	121.1.1.1/24			

6.2 配置思路

- 由于需要两端设备均支持 BFD，才能够使用控制报文方式，本例中 Device C 不支持 BFD，在 Device A 上配置的 BFD 功能仅能使用 echo 报文方式。

- echo 报文方式下必须配置 echo 报文的源 IP 地址。IP 地址可以任意指定，不需要与实际接口地址对应。建议不要将 echo 报文的源 IP 地址配置为属于该设备任何一个接口所在网段，避免对端发送大量的 ICMP 重定向报文造成网络拥塞。

6.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

6.4 配置步骤

6.4.1 配置各接口的 IP 地址

(1) 配置 Device A 各接口的 IP 地址

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 10.1.0.101 24
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 请参考以上方法配置图 3 中其它接口的 IP 地址，配置步骤这里省略

6.4.2 配置 RIP 基本功能

(1) 配置 Device A

配置 Device A 的 RIP 基本功能，引入直连路由，并使能 RIP 的 BFD 功能。

```
<DeviceA> system-view
[DeviceA] rip 1
[DeviceA-rip-1] version 2
[DeviceA-rip-1] undo summary
[DeviceA-rip-1] network 10.1.0.0
[DeviceA-rip-1] network 192.168.0.0
[DeviceA-rip-1] import-route direct
[DeviceA-rip-1] quit
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] rip bfd enable
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 配置 Device B

配置 Device B 的 RIP 基本功能，引入直连路由。

```
<DeviceB> system-view
[DeviceB] rip 1
[DeviceB-rip-1] version 2
[DeviceB-rip-1] undo summary
[DeviceB-rip-1] network 192.168.0.0
[DeviceB-rip-1] network 13.1.1.0
[DeviceB-rip-1] import-route direct
[DeviceB-rip-1] quit
```

(3) 配置 Device C

配置 Device C 的 RIP 基本功能，引入直连路由。

```
<DeviceC> system-view
```

```
[DeviceC] rip 1
[DeviceC-rip-1] version 2
[DeviceC-rip-1] undo summary
[DeviceC-rip-1] network 10.1.0.0
[DeviceC-rip-1] network 13.1.1.0
[DeviceC-rip-1] import-route direct
[DeviceC-rip-1] quit
```

6.4.3 配置 Device A 的 BFD 参数

RIP 支持的 BFD 会话方式为 echo 报文方式，该方式下必须配置 BFD echo 报文的源 IP 地址。IP 地址可以任意指定，不需要与实际接口地址对应。建议不要将 BFD echo 报文的源 IP 地址配置为属于该设备任何一个接口所在网段。

```
[DeviceA] bfd echo-source-ip 11.11.11.11
```

配置接口接收 BFD echo 报文的最小时间间隔为 100ms，单跳 BFD 检测时间倍数为 3。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] bfd min-echo-receive-interval 100
[DeviceA-GigabitEthernet1/0/1] bfd detect-multiplier 3
[DeviceA-GigabitEthernet1/0/1] quit
```

6.5 验证配置

查看 Device A 上 BFD 会话信息，显示 BFD 会话已被创建，且状态为 Up。

```
[DeviceA] display bfd session verbose
 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 Session Working Under Echo Mode:
       Local Discr: 2049
         Source IP: 10.1.0.101          Destination IP: 10.1.0.102
    Session State: Up                        Interface: GigabitEthernet1/0/1
         Hold Time: 300ms                Act Tx Inter: 100ms
      Min Rx Inter: 100ms                Detect Inter: 300ms
          Rx Count: 464                      Tx Count: 465
      Connect Type: Direct             Running Up for: 00:00:46
       Detect Mode: Async                          Slot: 0
          Protocol: RIP
         Diag Info: No Diagnostic
```

查看 Device A 上学到的路由 121.1.1.0/24，可以看到 Device A 经过 L2 Switch 到达 Device C。

```
<DeviceA> display ip routing-table 121.1.1.0 24 verbose

Summary Count : 1

Destination: 121.1.1.0/24
   Protocol: RIP             Process ID: 1
  SubProtID: 0x1                    Age: 04h20m37s
       Cost: 1              Preference: 100
        Tag: 0                    State: Active Adv
```

```
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NBRID: 0x26000002          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 10.1.0.102
      Flags: 0x1008c        OrigNextHop: 10.1.0.102
      Label: NULL           RealNextHop: 10.1.0.102
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid        BkInterface: N/A
```

当 Device C 和二层交换机之间的链路发生故障，BFD 快速检测到链路发生变化并立刻通告 RIP。

```
%Oct  9 18:42:17:650 2017 Device A BFD/5/BFD_CHANGE_FSM: -MDC=1;Sess[10.1.0.101/10.1.0.102,
LD/RD:2049/2049, Interface: GigabitEthernet1/0/1, SessType:Echo, LinkType:INET] , Sta: UP->
DOWN, Diag:1
```

查看 Device A 上学到的路由 121.1.1.0/24，可以看到 Device A 经过 Device B 到达 Device C。

```
<DeviceA> display ip routing-table 121.1.1.0 24 verbose

Summary Count : 1

Destination: 121.1.1.0/24
   Protocol: RIP              Process ID: 2
  SubProtID: 0x1                    Age: 04h20m37s
       Cost: 2               Preference: 100
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NBRID: 0x26000002         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 192.168.0.102
      Flags: 0x1008c       OrigNextHop: 192.168.0.102
      Label: NULL          RealNextHop: 192.168.0.102
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid         Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid       BkInterface: N/A
```

6.6 配置文件

- Device A：

```
#
 bfd echo-source-ip 11.11.11.11
#
rip 1
 undo summary
 version 2
 network 10.0.0.0
network 192.168.0.0
 import-route direct
#
interface GigabitEthernet1/0/1
 port link-mode route
```

```
 ip address 10.1.0.101 255.255.255.0
bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 192.168.0.101 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 120.1.1.1 255.255.255.0
#
```

- Device B：

```
#
rip 1
 undo summary
 version 2
 network 192.168.0.0
network 13.1.1.0
 import-route direct
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.0.102 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 13.1.1.101 255.255.255.0
#
```

- Device C：

```
#
rip 1
 undo summary
 version 2
 network 10.1.0.0
network 13.1.1.0
 import-route direct
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.0.102 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 13.1.1.102 255.255.255.0
#
interface GigabitEthernet1/0/3
```

```
 port link-mode route
 ip address 121.1.1.1 255.255.255.0
#
```

7 OSPF 与 BFD 联动配置举例

7.1 组网需求

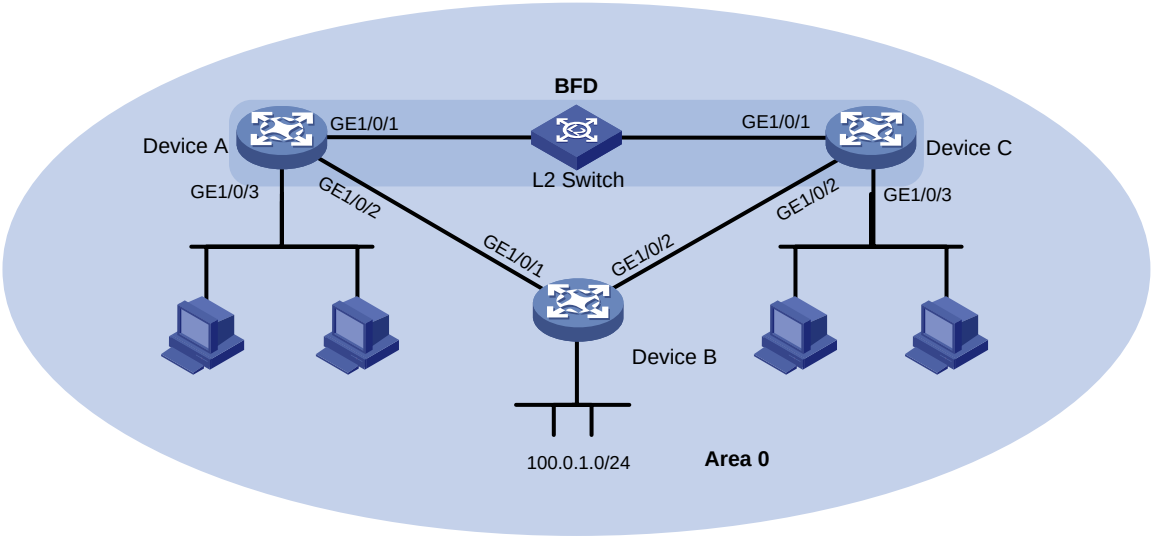
如图 4 所示，某公司通过一台二层交换机作为中继将两个相距较远的部门连接。Device A、Device B、Device C 上运行 OSPF，建立 OSPF 邻居关系，保证网络层相互可达。

已知 Device A 和 Device C 都支持 BFD 功能，要求使用 OSPF 与 BFD 联动技术，采用 BFD 控制报文方式实现当 Device A 或 Device C 与二层交换机之间的链路出现故障（如链路 down）时，BFD 能够快速感知并通告 OSPF 协议。

现要求通过在 Device A 和 Device C 上配置 OSPF 与 BFD 联动功能，实现：

- 监测通过 L2 Switch 通信的链路；
- 当链路出现故障时设备能够快速感知并通告 OSPF 协议，快速切换到 Device B 链路进行通信。

图4 OSPF 与 BFD 联动配置组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	XGE1/0/1	10.1.0.101/24	Device B	XGE1/0/1	192.168.0.102/24
	XGE1/0/2	192.168.0.101/24		XGE1/0/2	13.1.1.101/24
	XGE1/0/3	120.1.1.1/24			
Device C	XGE1/0/1	10.1.0.102/24			
	XGE1/0/2	13.1.1.102/24			
	XGE1/0/3	121.1.1.1/24			

7.2 配置思路

Device A 和 Device C 都支持 BFD，可以使用 BFD 控制报文方式，通信双方至少要有一方运行在主动模式才能成功建立起 BFD 会话。

7.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

7.4 配置步骤

7.4.1 配置各接口的 IP 地址

(1) 配置 Device A 各接口的 IP 地址

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 10.1.0.101 24
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 请参考以上方法配置图 4 中其它接口的 IP 地址，配置步骤这里省略

7.4.2 配置 OSPF 基本功能

(1) 配置 Device A

配置 Device A 的 OSPF 基本功能，并使能 OSPF 的 BFD 功能。

```
[DeviceA] ospf
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 120.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] quit
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ospf bfd enable
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 配置 Device B

配置 Device B 的 OSPF 基本功能。

```
[DeviceB] ospf
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

(3) 配置 Device C

配置 Device C 的 OSPF 基本功能，并使能 OSPF 的 BFD 功能。

```
[DeviceC] ospf
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 121.1.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] quit
[DeviceC-ospf-1] quit
```

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ospf bfd enable
[DeviceC-GigabitEthernet1/0/1] quit
```

7.4.3 配置 BFD 功能

(1) 配置 Device A

配置 BFD 会话建立前的运行模式为主动模式（缺省为主动模式）。

```
[DeviceA] bfd session init-mode active
```

配置发送和接收单跳 BFD 控制报文的最小时间间隔都为 100ms，单跳 BFD 检测时间倍数为 3。

```
 [DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] bfd min-transmit-interval 100
[DeviceA-GigabitEthernet1/0/1] bfd min-receive-interval 100
[DeviceA-GigabitEthernet1/0/1] bfd detect-multiplier 3
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 配置 Device C

配置 BFD 会话建立前的运行模式为主动模式（缺省为主动模式）。

```
[DeviceC] bfd session init-mode active
```

配置发送和接收单跳 BFD 控制报文的最小时间间隔都为 100ms，单跳 BFD 检测时间倍数为 3。

```
 [DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] bfd min-transmit-interval 100
[DeviceC-GigabitEthernet1/0/1] bfd min-receive-interval 100
[DeviceC-GigabitEthernet1/0/1] bfd detect-multiplier 3
[DeviceC-GigabitEthernet1/0/1] quit
```

7.5 验证配置

检查 Device A 连接的主机 host A（120.1.1.2）到 Device C 连接的主机 host C（121.1.1.2）是否可达。

```
<host A> ping 121.1.1.2
PING 121.1.1.2 (121.1.1.2): 56 data bytes
56 bytes from 121.1.1.2: seq=0 ttl=128 time=22.43 ms
56 bytes from 121.1.1.2: seq=1 ttl=128 time=7.17 ms
56 bytes from 121.1.1.2: seq=2 ttl=128 time=8.91 ms
56 bytes from 121.1.1.2: seq=3 ttl=128 time=7.45 ms
56 bytes from 121.1.1.2: seq=4 ttl=128 time=9.11 ms

--- 121.1.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.17/11.01/22.43 ms
```

查看 Device A 上 OSPF 邻居信息，显示 Device A 和 Device C 已建立 OSPF 邻居关系。

```
[DeviceA] display ospf peer verbose

          OSPF Process 1 with Router ID 2.2.2.2
```

```
                Neighbors

 Area 0.0.0.0 interface 10.1.0.101(GigabitEthernet1/0/1)'s neighbors
 Router ID: 1.1.1.1          Address: 10.1.0.102       GR State: Normal
   State: Full  Mode: Nbr is Slave  Priority: 1
   DR: 10.1.0.101  BDR: 10.1.0.102  MTU: 0
   Options is 0x42 (-|O|-|-|-|E|-)
   Dead timer due in 39  sec
   Neighbor is up for 00:09:01
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 5
   BFD status: Enabled(Control mode)
```

BFD 会话已被创建，且状态为 UP。

```
[DeviceA] display bfd session verbose

 Total session number: 1   Up session number: 1   Init mode: Active

 IPv4 session working under Ctrl mode:
     Local Discr: 10                  Remote Discr: 1
       Source IP: 10.1.0.101        Destination IP: 10.1.0.102
   Session State: Up                     Interface: GigabitEthernet1/0/1
 Min Trans Inter: 100ms            Act Trans Inter: 100ms
  Min Recv Inter: 100ms           Act Detect Inter: 300ms
          Rx Count: 3971                   Tx Count: 3776
      Connect Type: Direct             Running Up for: 00:06:52
         Hold Time: 300ms                   Auth mode: None
       Detect Mode: Async                        Slot: 0
        Protocol: OSPF
       Diag Info: No Diagnostic

[DeviceC] display bfd session verbose
 Total session number: 1   Up session number: 1   Init mode: Active

 IPv4 session working under Ctrl mode:
     Local Discr: 1                   Remote Discr: 10
       Source IP: 10.1.0.102        Destination IP: 10.1.0.101
   Session State: Up                     Interface: GigabitEthernet1/0/1
 Min Trans Inter: 100ms            Act Trans Inter: 100ms
  Min Recv Inter: 100ms           Act Detect Inter: 300ms
Min Trans Inter: 100ms             Act Trans Inter: 100ms
  Min Recv Inter: 100ms           Act Detect Inter: 100ms
          Rx Count: 3                      Tx Count: 3
      Connect Type: Direct             Running Up for: 00:06:52
         Hold Time: 300ms                   Auth mode: None
       Detect Mode: Async                        Slot: 0
        Protocol: OSPF
       Diag Info: No Diagnostic
```

在 Device A 上查看 121.1.1.0/24 的路由信息，可以看出 Device A 和 Device C 是通过 L2 Switch 进行通信的。

```
<DeviceA> display ip routing-table 121.1.1.0 verbose

Summary Count : 1

Destination: 120.1.1.0/24
   Protocol: OSPF            Process ID: 1
  SubProtID: 0x1                   Age: 04h20m37s
       Cost: 1               Preference: 10
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NBRID: 0x26000002         LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 10.1.0.102
      Label: NULL           RealNextHop: 10.1.0.102
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid        BkInterface: N/A
```

当 Device C 和二层交换机之间的链路状态变为 Down，BFD 快速检测到链路发生变化立刻通告 OSPF。

```
%Apr  2 11:34:26:880 2017 DeviceA BFD/5/BFD_CHANGE_FSM:
Sess[10.1.0.101/10.1.0.102,1026/1026
,GigabitEthernet1/0/1,Ctrl] , Sta: UP-> DOWN, Diag: 5
%Apr  2 11:34:27:011 2017 DeviceA OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 10.1.0.102
GigabitEthernet1/0/1) from Full to Down.
```

查看 121.1.1.0/24 的路由信息，可以看出 Device A 和 Device C 已经切换到 Device B 进行通信。

```
<Device A> display ip routing-table 121.1.1.0 verbose

Summary Count : 1

Destination: 121.1.1.0/24
   Protocol: OSPF            Process ID: 1
  SubProtID: 0x1                   Age: 04h20m37s
       Cost: 2               Preference: 10
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NBRID: 0x26000002         LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 192.168.0.102
      Label: NULL           RealNextHop: 192.168.0.102
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid        BkInterface: N/A
```

7.6 配置文件

- Device A：

```
#
ospf 1
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 120.1.1.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.0.101 255.255.255.0
 ospf bfd enable
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 192.168.0.101 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 120.1.1.1 255.255.255.0
#
```

- Device B：

```
#
ospf 1
 area 0.0.0.0
  network 13.1.1.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.0.102 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 13.1.1.101 255.255.255.0
#
```

- Device C：

```
#
ospf 1
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 13.1.1.0 0.0.0.255
```

```
  network 121.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.0.102 255.255.255.0
 ospf bfd enable
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
#
interface GigabitEthernet1/0/2
 port link-mode route
ip address 13.1.1.102 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode route
ip address 121.1.1.1 255.255.255.0
#
```

8 IS-IS 与 BFD 联动配置举例

8.1 组网需求

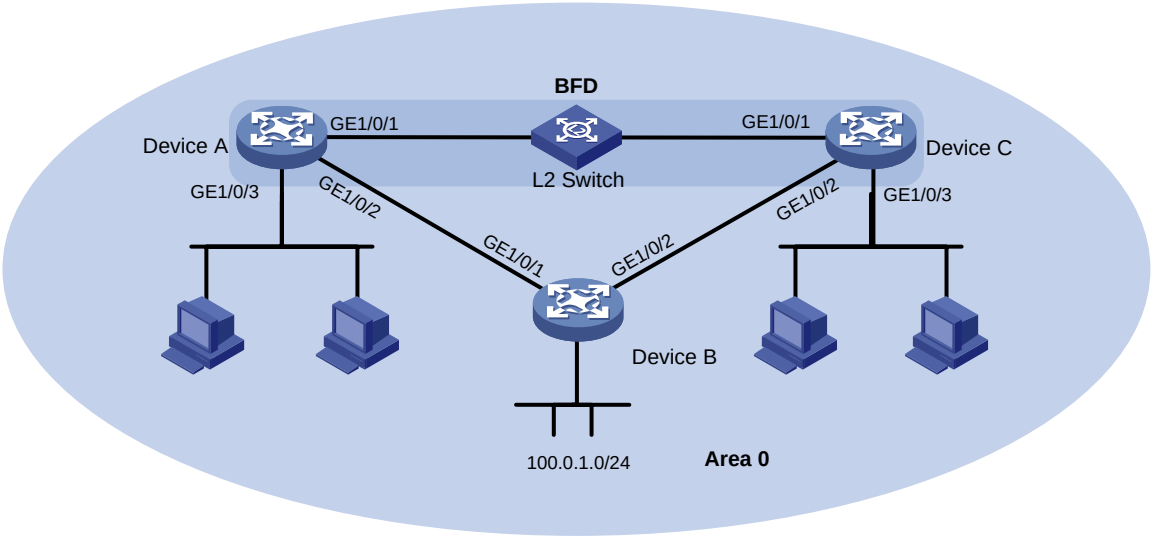
如图 5 所示，某公司通过一台二层交换机作为中继将两个相距较远的部门连接。Device A、Device B、Device C 上运行 IS-IS，建立 IS-IS 邻居关系，保证网络层相互可达。

已知 Device A 和 Device C 都支持 BFD 功能，公司希望使用 IS-IS 与 BFD 联动技术，采用 BFD 控制报文方式实现当 Device A 或 Device C 与二层交换机之间的链路出现故障（如链路 down）时，BFD 能够快速感知并通告 IS-IS 协议。

现要求通过在 Device A 和 Device C 上配置 IS-IS 与 BFD 联动功能，实现：

- 监测通过 L2 Switch 通信的链路；
- 当链路出现故障时设备能够快速感知并通告 IS-IS 协议，快速切换到 Device B 链路进行通信。

图5 IS-IS 与 BFD 联动配置组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	XGE1/0/1	10.1.0.101/24	Device B	XGE1/0/1	192.168.0.102/24
	XGE1/0/2	192.168.0.101/24		XGE1/0/2	13.1.1.101/24
	XGE1/0/3	120.1.1.1/24			
Device C	XGE1/0/1	10.1.0.102/24			
	XGE1/0/2	13.1.1.102/24			
	XGE1/0/3	121.1.1.1/24			

8.2 配置思路

Device A 和 Device C 都支持 BFD，可以使用 BFD 控制报文方式，通信双方至少要有一方运行在主动模式才能成功建立起 BFD 会话。

8.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

8.4 配置步骤

8.4.1 配置各接口的 IP 地址

(1) 配置 Device A 各接口的 IP 地址

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 10.1.0.101 24
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 请参考以上方法配置图 5 中其它接口的 IP 地址，配置步骤这里省略

8.4.2 配置 IS-IS 基本功能

(1) 配置 Device A

配置 Device A 的 IS-IS 基本功能，并使能 IS-IS 的 BFD 功能。

```
[DeviceA] isis
[DeviceA-isis-1] network-entity 10.0000.0000.0001.00
[DeviceA-isis-1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] isis enable
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] isis enable
[DeviceA-GigabitEthernet1/0/1] isis bfd enable
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 配置 Device B

配置 Device B 的 IS-IS 基本功能。

```
[DeviceB] isis
[DeviceB-isis-1] network-entity 10.0000.0000.0003.00
[DeviceB-isis-1] quit
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] isis enable
[DeviceB-GigabitEthernet1/1/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] isis enable
[DeviceB-GigabitEthernet1/0/2] quit
```

(3) 配置 Device C

配置 Device C 的 IS-IS 基本功能，并使能 IS-IS 的 BFD 功能。

```
[DeviceC] isis
[DeviceC-isis-1] network-entity 10.0000.0000.0002.00
[DeviceC-isis-1] quit
 [DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] isis enable
[DeviceC-GigabitEthernet1/0/1] isis bfd enable
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] isis enable
[DeviceC-GigabitEthernet1/0/2] quit
```

8.4.3 配置 BFD 功能

(1) 配置 Device A

配置 BFD 会话建立前的运行模式为主动模式（缺省为主动模式）。

```
[DeviceA] bfd session init-mode active
```

配置发送和接收单跳 BFD 控制报文的最小时间间隔都为 100ms，单跳 BFD 检测时间倍数为 3。

```
 [DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] bfd min-transmit-interval 100
[DeviceA-GigabitEthernet1/0/1] bfd min-receive-interval 100
[DeviceA-GigabitEthernet1/0/1] bfd detect-multiplier 3
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 配置 Device C

配置 BFD 会话建立前的运行模式为主动模式（缺省为主动模式）。

```
[DeviceC] bfd session init-mode active
```

配置发送和接收单跳 BFD 控制报文的最小时间间隔都为 100ms，单跳 BFD 检测时间倍数为 3。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] bfd min-transmit-interval 100
[DeviceC-GigabitEthernet1/0/1] bfd min-receive-interval 100
[DeviceC-GigabitEthernet1/0/1] bfd detect-multiplier 3
[DeviceC-GigabitEthernet1/0/1] quit
```

8.5 验证配置

查看 Device A 上 IS-IS 邻居信息，显示 Device A 和 Device C 已建立 IS-IS 邻居关系。

```
[DeviceA] display isis peer verbose

                        Peer information for IS-IS(1)
                        ------------------------------

 System ID: 0000.0000.0002
 Interface: GigabitEthernet1/0/1     Circuit Id:  0000.0000.0002.01
 State: Up    HoldTime: 6s         Type: L1(L1L2)     PRI: 64
 Area address(es): 00
 Peer IP address(es): 10.1.0.102
 Peer local circuit ID: 1
 Peer circuit SNPA address: ce9d-d91d-d100
 Uptime: 00:01:19
 Adj protocol:  IPv4
 Graceful Restart capable
   Restarting signal: No
   Suppress adjacency advertisement: No
 Local topology:
   0
 Remote topology:
   0
```

查看 Device A 和 Device C 上 BFD 会话信息，显示 BFD 会话已被创建，且状态为 Up。

```
[DeviceA] display bfd session verbose
 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 Session Working Under Ctrl Mode:
      Local Discr: 2049                Remote Discr: 2049
        Source IP: 10.1.0.101         Destination IP: 10.1.0.102
    Session State: Up                      Interface: GigabitEthernet1/0/1
     Min Tx Inter: 100ms                 Act Tx Inter: 100ms
     Min Rx Inter: 100ms                 Detect Inter: 300ms
         Rx Count: 3                        Tx Count: 3
     Connect Type: Direct              Running Up for: 00:06:09
        Hold Time: 300ms                    Auth mode: None
```

```
       Detect Mode: Async                       Slot: 0
          Protocol: ISIS_BR_L1/ISIS_BR_L2
         Diag Info: No Diagnostic
[DeviceC] display bfd session verbose
 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 Session Working Under Ctrl Mode:
       Local Discr: 2049                Remote Discr: 2049
         Source IP: 10.1.0.102        Destination IP: 10.1.0.101
    Session State: Up                      Interface: GigabitEthernet1/0/1
      Min Tx Inter: 100ms               Act Tx Inter: 100ms
      Min Rx Inter: 100ms               Detect Inter: 300ms
          Rx Count: 3                       Tx Count: 3
      Connect Type: Direct            Running Up for: 00:07:10
         Hold Time: 300ms                   Auth mode: None
       Detect Mode: Async                       Slot: 0
          Protocol: ISIS_BR_L1/ISIS_BR_L2
         Diag Info: No Diagnostic
```

在 Device A 上查看 121.1.1.0/24 的路由信息，可以看出 Device A 和 Device C 是通过 L2 Switch 进行通信的。

```
<DeviceA> display ip routing-table 121.1.1.0 verbose

Summary Count : 1

Destination: 121.1.1.0/24
   Protocol: isis            Process ID: 1
  SubProtID: 0x1                   Age: 04h20m37s
       Cost: 20              Preference: 15
        Tag: 0                    State: Active Adv
  OrigTblID: 0x2               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NBRID: 0x26000002         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 10.1.0.102
      Label: NULL           RealNextHop: 10.1.0.102
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid        BkInterface: N/A
```

当 Device C 和二层交换机之间的链路 Down 了，BFD 快速检测到链路发生变化并立刻通告 IS-IS。

```
%Oct  9 16:11:24:163 2017 DeviceC BFD/5/BFD_CHANGE_FSM: -MDC=1; Sess[10.1.0.102/10.1.0.101,
LD/RD:2049/2049, Interface: GigabitEthernet1/0/1, SessType:Ctrl, LinkType:INET] , S
ta: UP-> DOWN, Diag: 1
%Oct  9 16:11:24:164 2017 DeviceC ISIS/5/ISIS_NBR_CHG: -MDC=1; IS-IS 1, Level-1 adj
acency 0000.0000.0001 (GigabitEthernet1/0/1), state change to: DOWN.
%Oct  9 16:11:24:164 2017 DeviceC ISIS/5/ISIS_NBR_CHG: -MDC=1; IS-IS 1, Level-2 adj
acency 0000.0000.0001 (GigabitEthernet1/0/1), state change to: DOWN.
```

查看 121.1.1.0/24 的路由信息，可以看出 Device A 和 Device C 已经切换到 Device B 进行通信。

```
<Device A> display ip routing-table 121.1.1.0 verbose
```

```
Summary Count : 1

Destination: 121.1.1.0/24
   Protocol: OSPF            Process ID: 1
  SubProtID: 0x1                   Age: 04h20m37s
       Cost: 21              Preference: 10
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NBRID: 0x26000002         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 192.168.0.102
      Label: NULL           RealNextHop: 192.168.0.102
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid        BkInterface: N/A
```

8.6 配置文件

- Device A：

```
#
isis 1
 network-entity 10.0000.0000.0001.00
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.0.101 255.255.255.0
isis enable 1
 isis bfd enable
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 192.168.0.101 255.255.255.0
 isis enable 1
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 120.1.1.1 255.255.255.0
#
```

- Device B：

```
#
isis 1
 network-entity 10.0000.0000.0003.00
#
```

```
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.0.102 255.255.255.0
isis enable 1
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 13.1.1.101 255.255.255.0
isis enable 1
#
```

- Device C：

```
#
isis 1
 network-entity 10.0000.0000.0002.00
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.0.102 255.255.255.0
isis enable 1
 isis bfd enable
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
#
interface GigabitEthernet1/0/2
 port link-mode route
ip address 13.1.1.102 255.255.255.0
 isis enable 1
#
interface GigabitEthernet1/0/3
 port link-mode route
ip address 121.1.1.1 255.255.255.0
#
```

9 BGP 与 BFD 联动配置举例

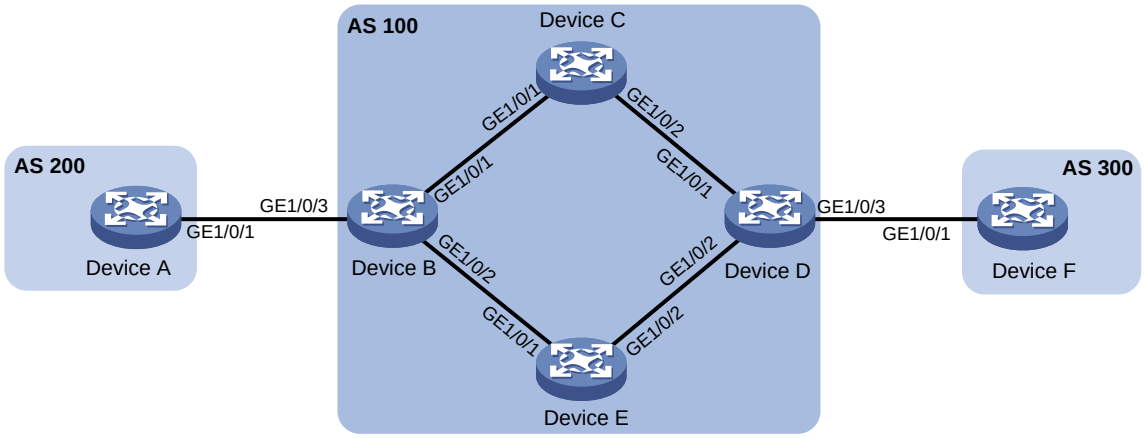
9.1 组网需求

如图 6 所示，某公司的两个部门相距较远，Device A 和 Device F 分别作为这两个部门的出口设备，现通过部署 BGP，使两个部门可以进行业务通信。已知 Device B 和 Device D 都支持 BFD 功能，公司希望使用 BGP 与 BFD 联动技术，采用 BFD 控制报文方式检测 AS 200 与 AS 300 之间通信的主链路状态，实现当 Device B 或 Device D 之间的链路出现故障（如链路 down）时，BFD 能够快速感知并通告 BGP 协议。具体要求如下：

- 在 AS 100 内使用 OSPF 作为 IGP；
- 配置 Device B<－>Device C<－>Device D 链路作为主链路，负责转发 Device A 和 Device F 之间的流量，并采用 BFD 控制报文的方式检测主链路；

- 当主链路发生故障时，BFD 能够快速检测并通告 BGP 协议，使得迅速切换到 Device B<—>Device E<—>Device D 这条路径进行通信。

图6 BGP 与 BFD 联动配置组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	XGE1/0/1	120.1.0.1/24	Device D	XGE1/0/1	10.2.0.101/24
Device B	XGE1/0/1	10.1.0.101/24		XGE1/0/2	13.1.1.101/24
	XGE1/0/2	192.168.0.101/24		XGE1/0/3	120.2.0.2/24
	XGE1/0/3	120.1.0.2/24	Device E	XGE1/0/1	192.168.0.102/24
Device C	XGE1/0/1	10.1.0.102/24		XGE1/0/2	13.1.1.102/24
	XGE1/0/2	10.2.0.102/24	Device F	XGE1/0/1	120.2.0.1/24

9.2 配置思路

- Device B 和 Device D 都支持 BFD，可以使用 BFD 控制报文方式，通信双方至少要有一方运行在主动模式才能成功建立起 BFD 会话。
- 为了使 Device B<—>Device C<—>Device D 成为主链路，需要通过路由策略配置其路由开销低于链路 Device B<—>Device E<—>Device D 的路由开销。

9.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

9.4 配置步骤

9.4.1 配置各接口的 IP 地址

(1) 配置 Device A 各接口的 IP 地址

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
[DeviceA-GigabitEthernet1/0/1] ip address 120.1.0.1 24
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 请参考以上方法配置图 6 中其它接口的 IP 地址，配置步骤这里省略

9.4.2 在 AS 100 内配置 OSPF 功能，保证设备间路由可达

(1) 配置 Device B

```
[DeviceB] ospf
[DeviceB-ospf-1] import-route direct
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

(2) 配置 Device C

```
[DeviceC] ospf
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 10.2.0.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] quit
[DeviceC-ospf-1] quit
```

(3) 配置 Device D

```
[DeviceD] ospf
[DeviceD-ospf-1] import-route direct
[DeviceD-ospf-1] area 0
[DeviceD-ospf-1-area-0.0.0.0] network 10.2.0.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] quit
[DeviceD-ospf-1] quit
```

(4) 配置 Device E

```
[DeviceE] ospf
[DeviceE-ospf-1] area 0
[DeviceE-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] quit
[DeviceE-ospf-1] quit
```

9.4.3 配置 BGP 功能

(1) 配置 Device A

启动 BGP，指定本地 AS 号为 200。

```
[DeviceA] bgp 200
[DeviceA-bgp] router id 1.1.1.1
```

配置 Device A 和 Device B 建立 EBGP 连接。

```
[DeviceA-bgp] peer 120.1.0.2 as-number 100
```

创建 BGP IPv4 单播地址族，并进入 BGP IPv4 单播地址族视图。

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

在 BGP IPv4 单播地址族视图下，将本地路由表中到达 120.1.0.0/24 网段的路由添加到 BGP 路由表中。

```
[DeviceA-bgp-ipv4] network 120.1.0.0 255.255.255.0
```

使能 Device A 与对等体 120.1.0.2 交换 IPv4 单播路由信息的能力。

```
[DeviceA-bgp-ipv4] peer 120.1.0.2 enable
[DeviceA-bgp-ipv4] quit
```

(2) 配置 Device B

启动 BGP，指定本地 AS 号为 100。

```
[DeviceB] bgp 100
[DeviceB-bgp] router id 2.2.2.2
```

配置 Device B 和 Device A 建立 EBGP 连接。

```
[DeviceB-bgp] peer 120.1.0.1 as-number 200
```

配置 Device B 和 Device D 建立 IBGP 连接。

```
[DeviceB-bgp] peer 10.2.0.101 as-number 100
[DeviceB-bgp] peer 13.1.1.101 as-number 100
```

创建 BGP IPv4 单播地址族，并进入 BGP IPv4 单播地址族视图。

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

使能 Device B 与对等体 10.2.0.101 交换 IPv4 单播路由信息的能力。

```
[DeviceB-bgp-ipv4] peer 10.2.0.101 enable
```

在 BGP IPv4 单播地址族视图下，配置向对等体 10.2.0.101 发布 BGP 路由时，将下一跳属性修改为自身的地址。

```
[DeviceB-bgp-ipv4] peer 10.2.0.101 next-hop-local
```

使能 Device B 与对等体 13.1.1.101 交换 IPv4 单播路由信息的能力。

```
[DeviceB-bgp-ipv4] peer 13.1.1.101 enable
```

在 BGP IPv4 单播地址族视图下，配置向对等体 13.1.1.101 发布 BGP 路由时，将下一跳属性修改为自身的地址。

```
[DeviceB-bgp-ipv4] peer 13.1.1.101 next-hop-local
```

使能 Device B 与对等体 120.1.0.1 交换 IPv4 单播路由信息的能力。

```
[DeviceB-bgp-ipv4] peer 120.1.0.1 enable
[DeviceB-bgp-ipv4] quit
```

(3) 配置 Device D

启动 BGP，指定本地 AS 号为 100。

```
[DeviceD] bgp 100
[DeviceD-bgp] router id 4.4.4.4
```

配置 Device D 和 Device B 建立 IBGP 连接。

```
[DeviceD-bgp] peer 10.1.0.101 as-number 100
[DeviceD-bgp] peer 192.168.0.101 as-number 100
```

配置 Device D 和 Device F 建立 EBGP 连接。

```
[DeviceD-bgp] peer 120.2.0.1 as-number 300
```

创建 BGP IPv4 单播地址族，并进入 BGP IPv4 单播地址族视图。

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

使能 Device D 与对等体 10.1.0.101 交换 IPv4 单播路由信息的能力。

```
[DeviceD-bgp-ipv4] peer 10.1.0.101 enable
```

在 BGP IPv4 单播地址族视图下，配置向对等体 10.1.0.101 发布 BGP 路由时，将下一跳属性修改为自身的地址。

```
[DeviceD-bgp-ipv4] peer 10.1.0.101 next-hop-local
```

使能 Device D 与对等体 192.168.0.101 交换 IPv4 单播路由信息的能力。

```
[DeviceD-bgp-ipv4] peer 192.168.0.101 enable
```

在 BGP IPv4 单播地址族视图下，配置向对等体 192.168.0.101 发布 BGP 路由时，将下一跳属性修改为自身的地址。

```
[DeviceD-bgp-ipv4] peer 192.168.0.101 next-hop-local
```

使能 Device D 与对等体 120.2.0.1 交换 IPv4 单播路由信息的能力。

```
[DeviceD-bgp-ipv4] peer 120.2.0.1 enable
[DeviceD-bgp-ipv4] quit
```

(4) 配置 Device F

#启动 BGP，指定本地 AS 号为 300。

```
[DeviceF] bgp 300
[DeviceF-bgp] router id 6.6.6.6
```

配置 Device F 和 Device D 建立 EBGP 连接。

```
[DeviceF-bgp] peer 120.2.0.2 as-number 100
```

创建 BGP IPv4 单播地址族，并进入 BGP IPv4 单播地址族视图。

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

在 BGP IPv4 单播地址族视图下，将本地路由表中到达 120.2.0.0/24 网段的路由添加到 BGP 路由表中。

```
[DeviceF-bgp-ipv4] network 120.2.0.0 255.255.255.0
```

使能 Device F 与对等体 120.2.0.2 交换 IPv4 单播路由信息的能力。

```
[DeviceF-bgp-ipv4] peer 120.2.0.2 enable
[DeviceF-bgp-ipv4] quit
```

9.4.4 配置路由策略

(1) 配置 Device B

创建 ACL 2000，允许源 IP 地址为 120.1.0.0/24 的报文通过。

```
[DeviceB] acl basic 2000
[DeviceB-acl-ipv4-basic-2000] rule permit source 120.1.0.0 0.0.0.255
[DeviceB-acl-ipv4-basic-2000] quit
```

配置向对等体 10.2.0.101 发布的路由设置本地优先级为 200，并配置 IBGP 路由优先级为 100。

```
[DeviceB] route-policy local-pre permit node 10
[DeviceB-route-policy-local-pre] if-match ip address acl 2000
[DeviceB-route-policy-local-pre] apply local-preference 200
[DeviceB-route-policy-local-pre] quit
[DeviceB] bgp 100
[DeviceB-bgp] address-family ipv4 unicast
[DeviceB-bgp-ipv4] peer 10.2.0.101 route-policy local-pre export
[DeviceB-bgp-ipv4] preference 255 100 130
[DeviceB-bgp-ipv4] quit
```

(2) 配置 Device D

创建 ACL 2000，允许源 IP 地址为 120.2.0.0/24 的报文通过。

```
[DeviceD] acl basic 2000
[DeviceD-acl-ipv4-basic-2000] rule permit source 120.2.0.0 0.0.0.255
```

```
[DeviceD-acl-ipv4-basic-2000] quit
```

配置向对等体 10.1.0.101 发布的路由设置本地优先级为 200，并配置 IBGP 路由优先级为 100。

```
[DeviceD] route-policy local-pre permit node 10
[DeviceD-route-policy-local-pre] if-match ip address acl 2000
[DeviceD-route-policy-local-pre] apply local-preference 200
[DeviceD-route-policy-local-pre] quit
[DeviceD] bgp 100
[DeviceD-bgp] address-family ipv4 unicast
[DeviceD-bgp-ipv4] peer 10.1.0.101 route-policy local-pre export
[DeviceD-bgp-ipv4] preference 255 100 130
[DeviceD-bgp-ipv4] quit
```

9.4.5 配置 BFD 功能

(1) 配置 Device B

```
[DeviceB] bgp 100
[DeviceB-bgp] peer 10.2.0.101 bfd
[DeviceB-bgp] quit
```

(2) 配置 Device D

```
[DeviceD] bgp 100
[DeviceD-bgp] peer 10.1.0.101 bfd
[DeviceD-bgp] quit
```

9.5 验证配置

从 Device A 上 ping Device F 的 IP 地址，可以互通。

```
[DeviceA] ping 120.2.0.1
Ping 120.2.0.1 (120.2.0.1): 56 data bytes, press CTRL_C to break
56 bytes from 120.2.0.1: icmp_seq=0 ttl=252 time=1.189 ms
56 bytes from 120.2.0.1: icmp_seq=1 ttl=252 time=1.095 ms
56 bytes from 120.2.0.1: icmp_seq=2 ttl=252 time=1.086 ms
56 bytes from 120.2.0.1: icmp_seq=3 ttl=252 time=1.097 ms
56 bytes from 120.2.0.1: icmp_seq=4 ttl=252 time=1.089 ms

--- Ping statistics for 120.2.0.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.086/1.111/1.189/0.039 ms
```

在 Device B 上通过命令 **display bgp peer** 查看 BGP 对等体信息，可以看到 Device B 与 Device D 建立 IBGP 连接，Device B 与 Device A 建立 EBGP 连接，且均处于 Established 状态。

```
[DeviceB] display bgp peer ipv4

 BGP local router ID: 2.2.2.2
 Local AS number: 100
 Total number of peers: 3                 Peers in established state: 3

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State
```

```
  10.2.0.101              100        6        4    0       1 00:00:56 Established
  13.1.1.101              100        6        5    0       1 00:00:56 Established
  120.1.0.1               200        6        5    0       1 00:00:56 Established
```

查看 Device B 上 BFD 会话信息，显示 BFD 会话已被创建，且状态为 Up。

```
[DeviceB] display bfd session verbose
 Total Session Num: 1     Up Session Num: 0     Init Mode: Active

 IPv4 Session Working Under Ctrl Mode:
       Local Discr: 2049                 Remote Discr: 0
         Source IP: 10.1.0.101         Destination IP: 10.2.0.101
     Session State: UP                      Interface: N/A
      Min Tx Inter: 1000ms                Act Tx Inter: 1000ms
      Min Rx Inter: 1000ms                Detect Inter: 5000ms
          Rx Count: 0                         Tx Count: 910
      Connect Type: Indirect            Running Up for: 00:00:00
         Hold Time: 0ms                       Auth mode: None
       Detect Mode: Async                          Slot: 0
          Protocol: BGP
         Diag Info: No Diagnostic
```

在 Device B 上查看 120.2.0.0/24 的路由信息，可以看出 Device B 通过 Device B<—>Device C<—>Device D 这条路径与 120.2.0.0/24 网段通信。

```
[DeviceB] display ip routing-table 120.2.0.0 24 verbose

Summary Count : 3

Destination: 120.2.0.0/24
   Protocol: BGP             Process ID: 0
  SubProtID: 0x1                    Age: 00h24m48s
       Cost: 0               Preference: 100
        Tag: 0                     State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 300
      NibID: 0x15000001         LastAs: 300
     AttrID: 0x1              Neighbor: 10.2.0.101
      Flags: 0x10060        OrigNextHop: 10.2.0.101
      Label: NULL           RealNextHop: 10.1.0.102
    BkLabel: NULL             BkNextHop: N/A
Tunnel ID: Invalid          Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid        BkInterface: N/A

Destination: 120.2.0.0/24
   Protocol: OSPF            Process ID: 1
  SubProtID: 0x8                    Age: 00h26m19s
       Cost: 1               Preference: 150
        Tag: 1                     State: Inactive Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
```

```
      NibID: 0x13000005          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x41           OrigNextHop: 10.1.0.102
      Label: NULL           RealNextHop: 10.1.0.102
    BkLabel: NULL             BkNextHop: N/A
Tunnel ID: Invalid          Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid        BkInterface: N/A

Destination: 120.2.0.0/24
   Protocol: OSPF            Process ID: 1
  SubProtID: 0x8                    Age: 00h26m19s
       Cost: 1               Preference: 150
        Tag: 1                    State: Inactive Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NibID: 0x13000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x41           OrigNextHop: 192.168.0.102
      Label: NULL           RealNextHop: 192.168.0.102
    BkLabel: NULL             BkNextHop: N/A
Tunnel ID: Invalid          Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid        BkInterface: N/A
```

在 Device B<—>Device C<—>Device D 链路发生故障后，从 Device A 上 ping Device F 的 IP 地址，可以互通。

```
<DeviceA> ping 120.2.0.1
Ping 120.1.0.1 (120.2.0.1): 56 data bytes, press CTRL_C to break
56 bytes from 120.2.0.1: icmp_seq=0 ttl=252 time=0.680 ms
56 bytes from 120.2.0.1: icmp_seq=1 ttl=252 time=0.295 ms
56 bytes from 120.2.0.1: icmp_seq=2 ttl=252 time=0.423 ms
56 bytes from 120.2.0.1: icmp_seq=3 ttl=252 time=0.464 ms
56 bytes from 120.2.0.1: icmp_seq=4 ttl=252 time=0.445 ms

--- Ping statistics for 120.2.0.1 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.295/0.461/0.680/0.124 ms
```

在 Device B 上查看 120.2.0.0/24 的路由信息，可以看出 Device B 通过 Device B<—>Device E<—>Device D 这条路径与 120.2.0.0/24 网段通信。

```
<DeviceB> display ip routing-table 120.2.0.0 24 verbose

Summary Count : 2

Destination: 120.2.0.0/24
   Protocol: BGP             Process ID: 0
  SubProtID: 0x1                    Age: 00h00m18s
       Cost: 0               Preference: 100
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 300
```

```
      NibID: 0x15000001          LastAs: 300
     AttrID: 0x1               Neighbor: 10.2.0.101
      Flags: 0x10060        OrigNextHop: 10.2.0.101
      Label: NULL           RealNextHop: 192.168.0.102
    BkLabel: NULL             BkNextHop: N/A
Tunnel ID: Invalid          Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid        BkInterface: N/A

Destination: 120.2.0.0/24
   Protocol: OSPF            Process ID: 1
  SubProtID: 0x8                    Age: 00h00m18s
       Cost: 1               Preference: 150
        Tag: 1                     State: Inactive Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NibID: 0x13000001         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x41           OrigNextHop: 192.168.0.102
      Label: NULL           RealNextHop: 192.168.0.102
    BkLabel: NULL             BkNextHop: N/A
Tunnel ID: Invalid          Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid        BkInterface: N/A
```

9.6 配置文件

- Device A：

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 120.1.0.1 255.255.255.0
#
bgp 200
 router id 1.1.1.1
 peer 120.1.0.2 as-number 200
 #
 address-family ipv4 unicast
  network 120.1.0.0 255.255.255.0
  peer 120.1.0.2 enable
#
```

- Device B：

```
#
ospf 1
import-route direct
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
interface GigabitEthernet1/0/1
```

```
 port link-mode route
 ip address 10.1.0.101 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 192.168.0.101 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 120.1.0.2 255.255.255.0
#
bgp 100
 router id 2.2.2.2
 peer 10.2.0.101 as-number 100
 peer 10.2.0.101 bfd
 peer 13.1.1.101 as-number 100
 peer 120.1.0.1 as-number 200
#
 address-family ipv4 unicast
  preference 255 100 130
  peer 10.2.0.101 enable
  peer 10.2.0.101 next-hop-local
  peer 10.2.0.101 route-policy local-pre export
  peer 13.1.1.101 enable
  peer 13.1.1.101 next-hop-local
  peer 120.1.0.1 enable
#
route-policy local-pre permit node 10
 if-match ip address acl 2000
 apply local-preference 200
#
acl basic 2000
 rule 0 permit source 120.1.0.0 0.0.0.255
#
```

- Device C：

```
#
ospf 1
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 10.2.0.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.0.102 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.2.0.102 255.255.255.0
```

```
#
```

- Device D

```
#
ospf 1
 import-route direct
 area 0.0.0.0
  network 10.2.0.0 0.0.0.255
  network 13.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.2.0.101 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 13.1.1.101 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 120.1.0.2 255.255.255.0
#
bgp 100
 router id 4.4.4.4
 peer 10.1.0.101 as-number 100
 peer 10.1.0.101 bfd
 peer 120.2.0.1 as-number 300
 peer 192.168.0.101 as-number 100
#
 address-family ipv4 unicast
  preference 255 100 130
  peer 10.1.0.101 enable
  peer 10.1.0.101 next-hop-local
  peer 10.1.0.101 route-policy local-pre export
  peer 192.168.0.101 enable
  peer 192.168.0.101 next-hop-local
  peer 120.2.0.1 enable
#
acl basic 2000
 rule 0 permit source 120.2.0.0 0.0.0.255
#
```

- Device E：

```
#
ospf 1
 area 0.0.0.0
  network 13.1.1.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
interface GigabitEthernet1/0/1
```

```
 port link-mode route
 ip address 192.168.0.102 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 13.1.1.102 255.255.255.0
#
```

- Device F：

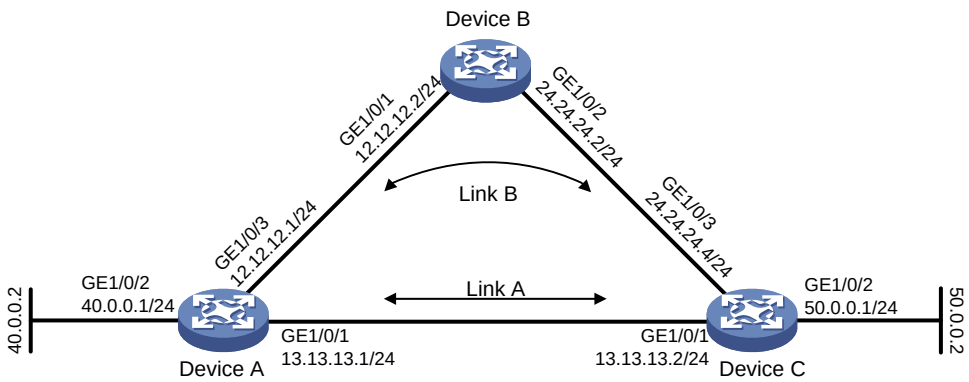
```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 120.2.0.1 255.255.255.0
#
bgp 300
 router id 6.6.6.6
 peer 120.2.0.2 as-number 100
 #
 address-family ipv4 unicast
  network 120.2.0.0 255.255.255.0
  peer 120.2.0.2 enable
#
```

10 策略路由与 BFD 联动配置举例

10.1 组网需求

某公司内部网络如图 7 所示，从 Device A 到 Device C 有两条转发路径：Link A 和 Link B。下一跳分别为 Device B 和 Device C。Link A 为直连链路，Link B 为非直连链路。已知 Device C 不支持 BFD 功能，公司希望使用策略路由与 BFD 联动技术，实现源 IP 为 40.0.0.2 的报文优先选择 Link B，当 Device A 和 Device B 的链路出现故障（如链路 down）时，Device A 能快速感知，并将流量切换到 Link A 的链路上。

图7 策略路由与 BFD 联动配置组网图



10.2 配置思路

- 由于需要两端设备均支持 BFD，才能够使用控制报文方式，本例中 Device C 不支持 BFD，在 Device A 上配置的 BFD 功能仅能使用 echo 报文方式。
- echo 报文方式下必须配置 echo 报文的源 IP 地址。IP 地址可以任意指定，不需要与实际接口地址对应。建议不要将 echo 报文的源 IP 地址配置为属于该设备任何一个接口所在网段，避免对端发送大量的 ICMP 重定向报文造成网络拥塞。

10.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

10.4 配置步骤

10.4.1 配置各接口的 IP 地址

(1) 配置 Device A 各接口的 IP 地址

```
<DeviceA> system-view
[DeviceA] interface GigabitEthernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] ip address 40.0.0.1 24
[DeviceA-GigabitEthernet1/0/2] quit
```

(2) 请参考以上方法配置图 7 中其它接口的 IP 地址，配置步骤这里省略

10.4.2 配置静态路由

(1) 配置 Device A

配置 Device A 到 Device C 50.0.0.0 网段的静态路由。

```
[DeviceA] ip route-static 50.0.0.0 24 gigabitEthernet 1/0/1 13.13.13.2
```

(2) 配置 Device B

配置 Device B 到 Device C 50.0.0.0 网段的静态路由。

```
[DeviceB] ip route-static 50.0.0.0 24 gigabitEthernet 1/0/2 24.24.24.4
```

10.4.3 配置 Device A 上的路由策略

配置匹配源 IP 地址为 40.0.0.2 的 IP 报文的 ACL 规则。

```
[DeviceA] acl advanced 3010
[DeviceA-acl-ipv4-adv-3010] rule 0 permit ip source 40.0.0.2 0
[DeviceA-acl-ipv4-adv-3010] quit
```

配置策略路由 aaa，使满足 ACL 规则报文的下一跳为 12.12.12.2，并与 track 11 绑定。

```
[DeviceA] policy-based-route aaa permit node 5
[DeviceA-pbr-aaa-5] if-match acl 3010
[DeviceA-pbr-aaa-5] apply next-hop 12.12.12.2 track 11
[DeviceA-pbr-aaa-5] quit
```

在接口上应用路由策略 aaa。

```
[DeviceA] interface gigabitEthernet 1/0/2
```

```
[DeviceA-GigabitEthernet1/0/2] ip policy-based-route aaa
[DeviceA-GigabitEthernet1/0/2] quit
```

10.4.4 配置 BFD 功能，并创建和 BFD 会话关联的 Track 项 11，检测 Device B 是否可达

(1) 配置 Device A

策略路由支持的 BFD 会话方式为 echo 报文方式，该方式下必须配置 BFD echo 报文的源 IP 地址。IP 地址可以任意指定，不需要与实际接口地址对应。建议不要将 BFD echo 报文的源 IP 地址配置为属于该设备任何一个接口所在网段。

```
[DeviceA] bfd echo-source-ip 3.3.3.3
```

配置发送和接收单跳 BFD 控制报文的最小时间间隔都为 100ms，单跳 BFD 检测时间倍数为 3。

```
[DeviceA] interface gigabitEthernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] bfd min-echo-receive-interval 100
[DeviceA-GigabitEthernet1/0/3] bfd detect-multiplier 3
[DeviceA-GigabitEthernet1/0/3] quit
[DeviceA] track 11 bfd echo interface GigabitEthernet 1/0/3 remote ip 12.12.12.2 local
ip 12.12.12.1
```

10.5 验证配置

查看 Device A 上源地址为 40.0.0.0 网段的流量，可以看到该网段当前流量优先从 GigabitEthernet1/0/3 接口（即 Link B）转发出去。

```
<DeviceA> reset counters interface
<DeviceA> display counters outbound interface
Interface         Total (pkts)   Broadcast (pkts)   Multicast (pkts)  Err (pkts)
XGE1/0/1                     0                  0                  0           0
XGE1/0/2                     0                  0                  0           0
XGE1/0/3                585414                  0                  0           0
XGE1/0/4                     0                  0                  0           0
XGE1/0/5                     0                  0                  0           0
XGE1/0/6                     0                  0                  0           0
```

查看 BFD 会话信息，显示 BFD 会话已被创建，且状态为 Up。

```
[DeviceA] display bfd session verbose
 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 Session Working Under Echo Mode:
       Local Discr: 2049
         Source IP: 12.12.12.1         Destination IP: 12.12.12.2
     Session State: Up                      Interface: GigabitEthernet1/0/3
      Min Tx Inter: 100ms                 Act Tx Inter: 100ms
      Min Rx Inter: 100ms                 Detect Inter: 300ms
          Rx Count: 128234                    Tx Count: 371950
      Connect Type: Direct              Running Up for: 00:01:04
       Detect Mode: Async                 Chassis/Slot: 1/0
          Protocol: TRACK
         Diag Info: No Diagnostic
```

当 Device A 和 Device B 间链路故障后，BFD 会话 Down。

```
%Dec 10 16:39:46:210 2017 DeviceA BFD/5/BFD_CHANGE_FSM: -MDC=1; Sess[12.12.12.1/
12.12.12.2, LD/RD:2049/2049, Interface: GigabitEthernet1/0/3, SessType:Echo,
LinkType:INET] , S
ta: UP-> DOWN, Diag: 1
%Dec 10 16:39:47:342 2017 DeviceA IFNET/3/PHY_UPDOWN: -MDC=1; GigabitEtherne
T1/0/3 link status is down.
%Dec 10 16:39:47:343 2017 DeviceA IFNET/5/LINK_UPDOWN: -MDC=1; Line protocol on
the interface GigabitEthernet1/0/3 is down.
%Dec 10 16:39:47:343 2017 DeviceA IFNET/3/PHY_UPDOWN: -MDC=1; GigabitEthernet1/0/3
link status is down.
```

清除流量后重新查看 Device A 上源地址为 40.0.0.0 网段的流量，可以看到当前流量从 GigabitEthernet1/0/1 接口（即 Link A）转发出去。

```
<DeviceA> reset counters interface
<DeviceA> display counters outbound interface
Interface         Total (pkts)   Broadcast (pkts)   Multicast (pkts)  Err (pkts)
XGE1/0/1               863764                  0                  0           0
XGE1/0/2                    0                  0                  0           0
XGE1/0/3                    0                  0                  0           0
XGE1/0/4                    0                  0                  0           0
XGE1/0/5                    0                  0                  0           0
XGE1/0/6                    0                  0                  0           0
```

10.6 配置文件

- Device A

```
#
 bfd echo-source-ip 3.3.3.3
#
policy-based-route aaa permit node 5
 if-match acl 3010
 apply next-hop 12.12.12.2 track 11
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 13.13.13.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 40.0.0.1 255.255.255.0
 ip policy-based-route aaa
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 12.12.12.1 255.255.255.0
 bfd min-echo-receive-interval 10
 bfd detect-multiplier 3
#
```

```
ip route-static 50.0.0.0 24 GigabitEthernet1/0/1 13.13.13.2
#
 ip local policy-based-route aaa
#
acl advanced 3010
 rule 0 permit ip source 40.0.0.2 0
#
 track 11 bfd echo interface GigabitEthernet1/0/3 remote ip 12.12.12.2 local ip 12.
12.12.1
#
```

- Device B

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 12.12.12.2 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 24.24.24.2 255.255.255.0
#
ip route-static 50.0.0.0 24 GigabitEthernet1/0/2 24.24.24.4
```

- Device C

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 13.13.13.2 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 50.0.0.1 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 24.24.24.4 255.255.255.0
#
```

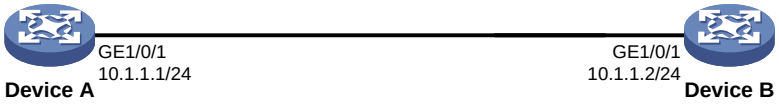
11 BFD 单跳检测三层链路配置举例

11.1 组网需求

如图 8 所示，Device A 和 Device B 通过三层以太网接口 GigabitEthernet1/0/1 相互连接。

现要求实现以下需求：在 Device A 和 Device B 上配置 BFD 检测三层接口功能，当 Device A 与 Device B 之间出现故障时，BFD 能够快速发现并将接口置为 Down 状态，使上层协议快速感知，确保数据流量不再从该三层接口上转发。

图8 BFD 单跳检测三层链路配置组网图



11.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

11.3 配置步骤

11.3.1 配置 Device A

Device A 各接口的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 10.1.1.1 24
[DeviceA-GigabitEthernet1/0/1] quit
```

配置 BFD。

```
[DeviceA] bfd session init-mode active
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] bfd min-transmit-interval 100
[DeviceA-GigabitEthernet1/0/1] bfd min-receive-interval 100
[DeviceA-GigabitEthernet1/0/1] bfd detect-multiplier 3
[DeviceA-GigabitEthernet1/0/1] bfd detect-interface source-ip 10.1.1.1
[DeviceA-GigabitEthernet1/0/1] quit
```

11.3.2 配置 Device B

Device B 各接口的 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 10.1.1.2 24
[DeviceB-GigabitEthernet1/0/1] quit
```

配置 BFD。

```
[DeviceB] bfd session init-mode active
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] bfd min-transmit-interval 100
[DeviceB-GigabitEthernet1/0/1] bfd min-receive-interval 100
[DeviceB-GigabitEthernet1/0/1] bfd detect-multiplier 3
[DeviceB-GigabitEthernet1/0/1] bfd detect-interface source-ip 10.1.1.2
[DeviceB-GigabitEthernet1/0/1] quit
```

11.4 验证配置

(1) Device A 和 Device B 设备及之间的链路均正常工作时

查看 Device A 的 BFD 会话。

```
<DeviceA> display bfd session verbose
 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 Session Working Under Ctrl Mode:
       Local Discr: 1537                Remote Discr: 1537
         Source IP: 10.1.1.1          Destination IP: 224.0.0.184
     Session State: Up                     Interface: GigabitEthernet1/0/1
      Min Tx Inter: 100ms               Act Tx Inter: 100ms
      Min Rx Inter: 100ms               Detect Inter: 300ms
          Rx Count: 280                      Tx Count: 367
      Connect Type: Direct            Running Up for: 00:00:28
         Hold Time: 276ms                   Auth mode: None
       Detect Mode: Async                        Slot: 1
          Protocol: Interface
         Diag Info: No Diagnostic
```

查看 Device B 的 BFD 会话。

```
<DeviceB> display bfd session verbose
 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 Session Working Under Ctrl Mode:
       Local Discr: 1537                Remote Discr: 1537
         Source IP: 10.1.1.2          Destination IP: 224.0.0.184
     Session State: Up                     Interface: GigabitEthernet1/0/1
      Min Tx Inter: 100ms               Act Tx Inter: 100ms
      Min Rx Inter: 100ms               Detect Inter: 300ms
          Rx Count: 143                      Tx Count: 145
      Connect Type: Direct            Running Up for: 00:00:14
         Hold Time: 251ms                   Auth mode: None
       Detect Mode: Async                        Slot: 0
          Protocol: Interface
         Diag Info: No Diagnostic
```

以上显示信息表示 Device A 和 Device B 用 BFD 协议检测本设备 GigabitEthernet1/0/1 接口及链路状态，报文目的地址固定为 224.0.0.184。

(2) Device A 的 GigabitEthernet1/0/1 或 Device A 与 Device B 之间的链路 Down 时

```
<DeviceB> %Dec 19 11:25:47:528 2017 DeviceB BFD/5/BFD_CHANG
E_FSM: -MDC=1; Sess[10.1.1.2/224.0.0.184, LD/RD:1540/1540, Interface:GE1/0/1, Se
ssType:Ctrl, LinkType:INET], Sta: UP->DOWN, Diag: 1
%Dec 19 11:25:47:530 2017 DeviceB IFNET/5/LINK_UPDOWN: -MDC=1; Line protocol on
the interface GigabitEthernet1/0/1 is down.
%Dec 19 11:25:49:162 2017 DeviceB IFNET/3/PHY_UPDOWN: -MDC=1; GigabitEthernet3/0
/1 link status is down.
```

查看 Device B 的 BFD 会话。

```
<DeviceB> display bfd session verbose
 Total Session Num: 1     Up Session Num: 0     Init Mode: Active

 IPv4 Session Working Under Ctrl Mode:
       Local Discr: 1537                 Remote Discr: 0
         Source IP: 10.1.1.2          Destination IP: 224.0.0.184
     Session State: Down                    Interface: GigabitEthernet1/0/1
      Min Tx Inter: 100ms                 Act Tx Inter: 100ms
      Min Rx Inter: 100ms                 Detect Inter: 300ms
          Rx Count: 3123                       Tx Count: 3133
      Connect Type: Direct              Running Up for: 00:00:00
         Hold Time: 0ms                       Auth mode: None
       Detect Mode: Async                          Slot: 0
          Protocol: Interface
         Diag Info: Control Detection Time Expired
```

以上显示信息表示当 Device B 上 BFD 协议监视的端口或与此端口相连的链路 down 时，立即将 BFD 状态置为 Down，并通知端口模块将端口的链路层状态置为 Down，以便上层协议及时发现，不再将流量从此接口上通过。

11.5 配置文件

- Device A：

```
#
 bfd session init-mode active
#
interface GigabitEthernet1/0/1
 port link-mode route
ip address 10.1.1.1 255.255.255.0
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
 bfd detect-interface source-ip 10.1.1.1
#
```

- Device B：

```
#
 bfd session init-mode active
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.2 255.255.255.0
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
 bfd detect-interface source-ip 10.1.1.2
#
```

12 BFD 检测三层静态聚合组配置举例

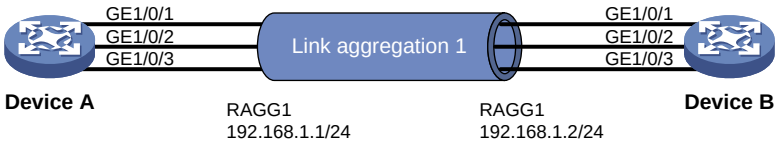
12.1 组网需求

如图 9 所示，Device A 和 Device B 通过三层以太网接口 GigabitEthernet1/0/1～GigabitEthernet1/0/3 相互连接。

现要求实现以下需求：

- 在 Device A 和 Device B 上分别配置三层静态链路聚合组，将这些接口加入聚合组。
- 在静态链路聚合组的每个成员接口上分别配置 BFD 功能，当成员接口或成员链路出现故障（如链路 Down）时，BFD 能够快速发现并知会三层静态链路聚合组，使聚合组的数据流量不再从该成员接口上转发。

图9 BFD 检测三层静态聚合组成员接口配置组网图



12.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

12.3 配置注意事项

- 聚合链路的两端应配置相同的聚合模式。
- 建议不要将镜像反射端口加入聚合组。
- 配置了下列功能的端口将不能加入三层聚合组：AC 与交叉连接关联（请参见“MPLS 配置指导”中的“MPLS L2VPN”）以及 AC 与 VSI 关联（请参见“MPLS 配置指导”中的“VPLS”）。

12.4 配置步骤

12.4.1 配置 Device A

创建三层聚合接口 1，并为该接口配置 IP 地址和子网掩码。

```
<DeviceA> system-view
[DeviceA] interface route-aggregation 1
[DeviceA-Route-Aggregation1] ip address 192.168.1.1 24
[DeviceA-Route-Aggregation1] quit
```

分别将接口 GigabitEthernet1/0/1 至 GigabitEthernet1/0/3 加入到聚合组 1 中。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/1] quit
```

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/3] quit
```

配置 BFD。

```
[DeviceA] bfd session init-mode active
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] bfd min-transmit-interval 100
[DeviceA-GigabitEthernet1/0/1] bfd min-receive-interval 100
[DeviceA-GigabitEthernet1/0/1] bfd detect-multiplier 3
[DeviceA-GigabitEthernet1/0/1] bfd detect-interface source-ip 1.1.1.1
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] bfd min-transmit-interval 100
[DeviceA-GigabitEthernet1/0/2] bfd min-receive-interval 100
[DeviceA-GigabitEthernet1/0/2] bfd detect-multiplier 3
[DeviceA-GigabitEthernet1/0/2] bfd detect-interface source-ip 1.1.1.2
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] bfd min-transmit-interval 100
[DeviceA-GigabitEthernet1/0/3] bfd min-receive-interval 100
[DeviceA-GigabitEthernet1/0/3] bfd detect-multiplier 3
[DeviceA-GigabitEthernet1/0/3] bfd detect-interface source-ip 1.1.1.3
[DeviceA-GigabitEthernet1/0/3] quit
```

12.4.2 配置 Device B

创建三层聚合接口 1，并为该接口配置 IP 地址和子网掩码。

```
<DeviceB> system-view
[DeviceB] interface route-aggregation 1
[DeviceB-Route-Aggregation1] ip address 192.168.1.2 24
[DeviceB-Route-Aggregation1] quit
```

分别将接口 GigabitEthernet1/0/1 至 GigabitEthernet1/0/3 加入到聚合组 1 中。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-aggregation group 1
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-aggregation group 1
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-aggregation group 1
[DeviceB-GigabitEthernet1/0/3] quit
```

配置 BFD。

```
[DeviceB] bfd session init-mode active
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] bfd min-transmit-interval 100
```

```
[DeviceB-GigabitEthernet1/0/1] bfd min-receive-interval 100
[DeviceB-GigabitEthernet1/0/1] bfd detect-multiplier 3
[DeviceB-GigabitEthernet1/0/1] bfd detect-interface source-ip 2.1.1.1
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] bfd min-transmit-interval 100
[DeviceB-GigabitEthernet1/0/2] bfd min-receive-interval 100
[DeviceB-GigabitEthernet1/0/2] bfd detect-multiplier 3
[DeviceB-GigabitEthernet1/0/2] bfd detect-interface source-ip 2.1.1.2
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] bfd min-transmit-interval 100
[DeviceB-GigabitEthernet1/0/3] bfd min-receive-interval 100
[DeviceB-GigabitEthernet1/0/3] bfd detect-multiplier 3
[DeviceB-GigabitEthernet1/0/3] bfd detect-interface source-ip 2.1.1.3
[DeviceB-GigabitEthernet1/0/3] quit
```

12.5 验证配置

(1) Device A 和 Device B 设备及之间的链路均正常工作时

查看 Device A 的 BFD 会话。

```
<DeviceA> display bfd session verbose
 Total Session Num: 3     Up Session Num: 3     Init Mode: Passive

 IPv4 Session Working Under Ctrl Mode:
       Local Discr: 1538                Remote Discr: 1538
         Source IP: 1.1.1.3           Destination IP: 224.0.0.184
     Session State: Up                     Interface: GigabitEthernet1/0/3
      Min Tx Inter: 100ms                Act Tx Inter: 100ms
      Min Rx Inter: 100ms                Detect Inter: 300ms
          Rx Count: 892                      Tx Count: 890
      Connect Type: Direct             Running Up for: 00:01:29
         Hold Time: 299ms                    Auth mode: None
       Detect Mode: Async                         Slot: 1
          Protocol: Interface
         Diag Info: No Diagnostic

       Local Discr: 1539                Remote Discr: 1539
         Source IP: 1.1.1.2           Destination IP: 224.0.0.184
     Session State: Up                     Interface: GigabitEthernet1/0/2
      Min Tx Inter: 100ms                Act Tx Inter: 100ms
      Min Rx Inter: 100ms                Detect Inter: 300ms
          Rx Count: 599                      Tx Count: 598
      Connect Type: Direct             Running Up for: 00:01:00
         Hold Time: 290ms                    Auth mode: None
       Detect Mode: Async                         Slot: 1
          Protocol: Interface
         Diag Info: No Diagnostic
```

```
      Local Discr: 1540                Remote Discr: 1540
        Source IP: 1.1.1.1           Destination IP: 224.0.0.184
    Session State: Up                      Interface: GigabitEthernet1/0/1
     Min Tx Inter: 100ms               Act Tx Inter: 100ms
     Min Rx Inter: 100ms               Detect Inter: 300ms
         Rx Count: 443                      Tx Count: 442
     Connect Type: Direct            Running Up for: 00:00:44
        Hold Time: 282ms                    Auth mode: None
      Detect Mode: Async                         Slot: 1
         Protocol: Interface
        Diag Info: No Diagnostic
```

查看 Device B 的 BFD 会话。

```
<DeviceB> display bfd session verbose
Total Session Num: 3     Up Session Num: 3     Init Mode: Active

 IPv4 Session Working Under Ctrl Mode:
      Local Discr: 1538                Remote Discr: 1538
        Source IP: 2.1.1.3           Destination IP: 224.0.0.184
    Session State: Up                      Interface: GigabitEthernet1/0/3
     Min Tx Inter: 100ms               Act Tx Inter: 100ms
     Min Rx Inter: 100ms               Detect Inter: 300ms
         Rx Count: 2626                     Tx Count: 2829
     Connect Type: Direct            Running Up for: 00:04:22
        Hold Time: 297ms                    Auth mode: None
      Detect Mode: Async                         Slot: 0
         Protocol: Interface
        Diag Info: No Diagnostic

      Local Discr: 1539                Remote Discr: 1539
        Source IP: 2.1.1.2           Destination IP: 224.0.0.184
    Session State: Up                      Interface: GigabitEthernet1/0/2
     Min Tx Inter: 100ms               Act Tx Inter: 100ms
     Min Rx Inter: 100ms               Detect Inter: 300ms
         Rx Count: 2333                     Tx Count: 2543
     Connect Type: Direct            Running Up for: 00:03:53
        Hold Time: 296ms                    Auth mode: None
      Detect Mode: Async                         Slot: 0
         Protocol: Interface
        Diag Info: No Diagnostic

      Local Discr: 1540                Remote Discr: 1540
        Source IP: 2.1.1.1           Destination IP: 224.0.0.184
    Session State: Up                      Interface: GigabitEthernet1/0/1
     Min Tx Inter: 100ms               Act Tx Inter: 100ms
     Min Rx Inter: 100ms               Detect Inter: 300ms
         Rx Count: 2786                     Tx Count: 2789
     Connect Type: Direct            Running Up for: 00:03:37
```

```
  Hold Time: 297ms                  Auth mode: None
Detect Mode: Async                       Slot: 0
  Protocol: Interface
  Diag Info: No Diagnostic
```

以上显示信息表示 Device A 和 Device B 用 BFD 协议检测本设备 GigabitEthernet1/0/1、GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 接口及链路状态，报文目的地址固定为 224.0.0.184。

查看 Device A 接口上的数据流量。

```
<DeviceA> display counters inbound interface
Interface         Total (pkts)   Broadcast (pkts)   Multicast (pkts)  Err (pkts)
GE1/0/1                  12691                 21              12398           0
GE1/0/2                  11551                  0              11551           0
GE1/0/3                  11837                  0              11837           0
```

查看 Device B 接口上的数据流量。

```
<DeviceB> display counters inbound interface
Interface         Total (pkts)   Broadcast (pkts)   Multicast (pkts)  Err (pkts)
GE1/0/1                  11330                 16              11028           0
GE1/0/2                  10386                  0              10386           0
GE1/0/3                  10853                  0              10853           0
```

以上显示信息表示 Device A 和 Device B 上静态聚合组 1 中各端口都能正常转发流量。

查看 Device B 上所有聚合组的详细信息。

```
<DeviceB>display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status  Priority Oper-Key
--------------------------------------------------------------------------------
  GE1/0/1          S       32768    1
  GE1/0/2          S       32768    1
  GE1/0/3          S       32768    1
```

以上显示信息表示静态聚合组中，GigabitEthernet1/0/1～GigabitEthernet1/0/3 都是选中状态，流量会从这些接口上通过。

(2) Device A 的 GigabitEthernet1/0/1 端口故障或 Device A 与 DeviceB 之间的链路 Down 时

```
<DeviceB>%Dec 19 11:25:47:528 2017 DeviceB BFD/5/BFD_CHANG
E_FSM: -MDC=1; Sess[2.1.1.1/224.0.0.184, LD/RD:1540/1540, Interface:GE1/0/1, Se
ssType:Ctrl, LinkType:INET], Sta: UP->DOWN, Diag: 1
%Dec 19 11:25:47:530 2017 DeviceB IFNET/5/LINK_UPDOWN: -MDC=1; Line protocol on
the interface GigabitEthernet1/0/1 is down.
%Dec 19 11:25:47:533 2017 DeviceB LAGG/6/LAGG_INACTIVE_PHYSTATE: -MDC=1; Member
port GE1/0/1 of aggregation group RAGG1 changed to the inactive state, because
```

```
the physical state of the port is down.
%Dec 19 11:25:49:162 2017 DeviceB IFNET/3/PHY_UPDOWN: -MDC=1; GigabitEthernet3/0
/1 link status is down.
```

查看 Device B 的 BFD 会话。

```
<DeviceB> display bfd session verbose
 Total Session Num: 3     Up Session Num: 2     Init Mode: Active

 IPv4 Session Working Under Ctrl Mode:
       Local Discr: 1538                Remote Discr: 1538
         Source IP: 2.1.1.3           Destination IP: 224.0.0.184
     Session State: Up                     Interface: GigabitEthernet1/0/3
      Min Tx Inter: 100ms                Act Tx Inter: 100ms
      Min Rx Inter: 100ms                Detect Inter: 300ms
          Rx Count: 20987                    Tx Count: 21191
      Connect Type: Direct             Running Up for: 00:34:59
         Hold Time: 246ms                    Auth mode: None
       Detect Mode: Async                         Slot: 0
          Protocol: Interface
         Diag Info: No Diagnostic

       Local Discr: 1539                Remote Discr: 1539
         Source IP: 2.1.1.2           Destination IP: 224.0.0.184
     Session State: Up                     Interface: GigabitEthernet1/0/2
      Min Tx Inter: 100ms                Act Tx Inter: 100ms
      Min Rx Inter: 100ms                Detect Inter: 300ms
          Rx Count: 20694                    Tx Count: 20905
      Connect Type: Direct             Running Up for: 00:34:30
         Hold Time: 244ms                    Auth mode: None
       Detect Mode: Async                         Slot: 0
          Protocol: Interface
         Diag Info: No Diagnostic

       Local Discr: 1540                Remote Discr: 0
         Source IP: 2.1.1.1           Destination IP: 224.0.0.184
     Session State: Down                   Interface: GigabitEthernet1/0/1
      Min Tx Inter: 100ms                Act Tx Inter: 100ms
      Min Rx Inter: 100ms                Detect Inter: 300ms
          Rx Count: 16323                    Tx Count: 16816
      Connect Type: Direct             Running Up for: 00:00:00
         Hold Time: 0ms                      Auth mode: None
       Detect Mode: Async                         Slot: 0
          Protocol: Interface
         Diag Info: Control Detection Time Expired
```

查看 Device B 接口上的数据流量。

```
<DeviceB> reset counters interface
<DeviceB> display counters inbound interface
Interface         Total (pkts)   Broadcast (pkts)   Multicast (pkts)  Err (pkts)
GE1/0/1                      0                  0                  0           0
```

```
GE1/0/2                   185                 0                   5           0
GE1/0/3                   185                 0                   5           0
```

查看 Device B 上所有聚合组的详细信息。

```
<DeviceB>display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status  Priority Oper-Key
--------------------------------------------------------------------------------
  GE1/0/1          U       32768    1
  GE1/0/2          S       32768    1
  GE1/0/3          S       32768    1
```

以上显示信息表示当 Device B 上 BFD 协议监视到 Device A 的 GigabitEthernet1/0/1 端口 down 时，立即将 BFD 状态置为 Down，并通知端口模块将端口的链路层状态置为 Down。静态聚合组中，GigabitEthernet1/0/1 不再是选中状态，流量不会再从此接口上通过。

12.6 配置文件

- Device A：

```
#
interface Route-Aggregation1
  ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
 bfd detect-interface source-ip 1.1.1.1
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-mode route
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
 bfd detect-interface source-ip 1.1.1.2
 port link-aggregation group 1
#
interface GigabitEthernet1/0/3
 port link-mode route
```

```
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
 bfd detect-interface source-ip 1.1.1.3
 port link-aggregation group 1
#
```

- Device B：

```
#
interface Route-Aggregation1
  ip address 192.168.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
 bfd detect-interface source-ip 2.1.1.1
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-mode route
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
 bfd detect-interface source-ip 2.1.1.2
 port link-aggregation group 1
#
interface GigabitEthernet1/0/3
 port link-mode route
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
 bfd detect-interface source-ip 2.1.1.3
 port link-aggregation group 1
#
```

13 相关资料

- H3C SR6600 SR6600-X 路由器 可靠性配置指导-R7607
- H3C SR6600 SR6600-X 路由器 可靠性命令参考-R7607
- H3C SR6600 SR6600-X 路由器 二层技术-以太网交换配置指导-R7607
- H3C SR6600 SR6600-X 路由器 二层技术-以太网交换命令参考-R7607
- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由配置指导-R7607
- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由命令参考-R7607
- H3C SR6600 SR6600-X 路由器 MPLS 配置指导-R7607
- H3C SR6600 SR6600-X 路由器 MPLS 命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

BGP 基础配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1

2 配置前提 1

3 IPv4 BGP 基础配置举例 1

3.1 组网需求 1

3.2 配置思路 1

3.3 使用版本 1

3.4 配置注意事项 2

3.5 配置步骤 2

3.5.1 配置各接口的 IP 地址 2

3.5.2 配置 IBGP 连接 2

3.5.3 配置 EBGP 连接 3

3.5.4 配置 Router B 发布本地网段路由 5

3.6 验证配置 5

3.7 配置文件 6

4 BGP 与 IGP 交互配置举例 7

4.1 组网需求 7

4.2 配置思路 8

4.3 使用版本 8

4.4 配置注意事项 8

4.5 配置步骤 8

4.5.1 配置各接口的 IP 地址 8

4.5.2 配置 OSPF 8

4.5.3 配置 EBGP 连接 9

4.5.4 配置 BGP 与 IGP 交互 9

4.6 验证配置 10

4.7 配置文件 12

5 相关资料 13

1 简介

本文档介绍了 BGP 的基础配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

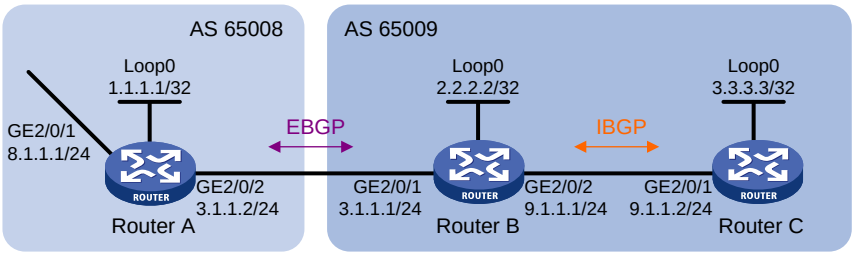
本文档假设您已了解 BGP 特性。

3 IPv4 BGP 基础配置举例

3.1 组网需求

随着 A 公司的不断发展，其网络规模也不断扩大，导致其设备运行的 IGP 协议不堪重负，为了解决这一问题，公司管理者决定在设备上运行一些 BGP 的基础配置。如图 1 所示，所有路由器均运行 BGP 协议。要求 Router A 和 Router B 之间建立 EBGP 连接，Router B 和 Router C 之间建立 IBGP 连接，使得 Router C 能够访问 Router A 直连的 8.1.1.0/24 网段。

图1 BGP 基础配置组网图



3.2 配置思路

- 在 AS 65009 内部，保证 Router B 到 Router C 的 LoopBack 接口路由可达，Router C 到 Router B 的 LoopBack 接口路由可达，这样两个 IBGP 对等体才能建立 TCP 连接，本案例使用 OSPF 协议实现。
- 由于设备缺省情况下 BGP 不发布任何本地的网段路由，为了使 Router C 能够访问 Router A 直连的 8.1.1.0/24 网段，将 8.1.1.0/24 网段宣告进 Router A 的 BGP 进程中，将 3.1.1.0/24 网段和 9.1.1.0/24 网段宣告进 Router B 的 BGP 进程中。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置注意事项

- 为了防止端口状态不稳定引起路由震荡，本举例使用 LoopBack 接口来创建 IBGP 对等体。
- 使用 LoopBack 接口创建 IBGP 对等体时，因为 LoopBack 接口不是两对等体实际连接的接口，所以，必须使用 **peer connect-interface** 命令将 LoopBack 接口配置为 BGP 连接的源接口。
- EBGP 邻居关系的两台路由器，处于不同的 AS 域，对端的 LoopBack 接口一般路由不可达，所以一般使用直连地址建立 EBGP 邻居。

3.5 配置步骤

3.5.1 配置各接口的 IP 地址

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface GigabitEthernet 2/0/1
[RouterA-GigabitEthernet2/0/1] ip address 8.1.1.1 24
```

请参考以上方法配置其它相关接口的 IP 地址，配置步骤这里省略。

3.5.2 配置 IBGP 连接

1. Router B 的配置

```
<RouterB> system-view
[RouterB] bgp 65009
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 3.3.3.3 as-number 65009
[RouterB-bgp] peer 3.3.3.3 connect-interface Loopback 0
[RouterB-bgp] address-family ipv4 unicast
[RouterB-bgp-ipv4] peer 3.3.3.3 enable
[RouterB-bgp-ipv4] quit
[RouterB-bgp] quit
[RouterB] ospf 1
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

2. Router C 的配置

```
<RouterC> system-view
[RouterC] bgp 65009
[RouterC-bgp] router-id 3.3.3.3
[RouterC-bgp] peer 2.2.2.2 as-number 65009
[RouterC-bgp] peer 2.2.2.2 connect-interface Loopback 0
[RouterC-bgp] address-family ipv4 unicast
[RouterC-bgp-ipv4] peer 2.2.2.2 enable
```

```
[RouterC-bgp-ipv4] quit
[RouterC-bgp] quit
[RouterC] ospf 1
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[RouterC-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

查看 Router C 的 BGP 对等体的连接状态。

```
[RouterC] display bgp peer ipv4

 BGP local router ID : 3.3.3.3
 Local AS number : 65009
 Total number of peers : 1                 Peers in established state : 1

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  2.2.2.2              65009        2        2    0       0 00:00:13 Established
```

以上显示信息表明 Router B 和 Router C 之间的 IBGP 连接已经建立。

3.5.3 配置 EBGP 连接

1. Router A 的配置

```
<RouterA> system-view
[RouterA] bgp 65008
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 3.1.1.1 as-number 65009
[RouterA-bgp] address-family ipv4 unicast
[RouterA-bgp-ipv4] peer 3.1.1.1 enable
[RouterA-bgp-ipv4] network 8.1.1.0 24
[RouterA-bgp-ipv4] quit
[RouterA-bgp] quit
```

2. Router B 的配置

```
[RouterB] bgp 65009
[RouterB-bgp] peer 3.1.1.2 as-number 65008
[RouterB-bgp] address-family ipv4 unicast
[RouterB-bgp-ipv4] peer 3.1.1.2 enable
[RouterB-bgp-ipv4] quit
[RouterB-bgp] quit
```

查看 Router B 的 BGP 对等体的连接状态。

```
[RouterB] display bgp peer ipv4

 BGP local router ID : 2.2.2.2
 Local AS number : 65009
 Total number of peers : 2                 Peers in established state : 2
```

```
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  3.3.3.3              65009        4        4    0       0 00:02:49 Established
  3.1.1.2              65008        2        2    0       0 00:00:05 Established
```

可以看出，Router B 与 Router C、Router B 与 Router A 之间的 BGP 连接均已建立。

查看 Router A 的 BGP 路由表。

```
[RouterA] display bgp routing-table ipv4

 Total number of routes: 1

 BGP local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >  8.1.1.0/24         8.1.1.1         0                     32768   i
```

查看 Router B 的 BGP 路由表。

```
[RouterB] display bgp routing-table ipv4

 Total number of routes: 1

 BGP local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >e 8.1.1.0/24         3.1.1.2         0                     0       65008i
```

查看 Router C 的 BGP 路由表。

```
[RouterC] display bgp routing-table ipv4

 Total number of routes: 1

 BGP local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

   i 8.1.1.0/24         3.1.1.2         0          100        0       65008i
```

从路由表可以看出，Router A 没有学到 AS 65009 内部的任何路由，Router C 虽然学到了 AS 65008 中的 8.1.1.0 的路由，但因为下一跳 3.1.1.2 不可达，所以也不是有效路由。

3.5.4 配置 Router B 发布本地网段路由

在 Router B 上配置 BGP 发布本地网段路由，以便 Router A 能够获取到网段 9.1.1.0/24 的路由，Router C 能够获取到网段 3.1.1.0/24 的路由。

```
[RouterB] bgp 65009
[RouterB-bgp] address-family ipv4 unicast
[RouterB-bgp-ipv4] network 3.1.1.0 24
[RouterB-bgp-ipv4] network 9.1.1.0 24
[RouterB-bgp-ipv4] quit
[RouterB-bgp] quit
```

查看 Router A 的 BGP 路由表。

```
[RouterA] display bgp routing-table ipv4

 Total number of routes: 3

 BGP local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >e 3.1.1.0/24         3.1.1.1         0                     0       65009?
* >  8.1.1.0/24         8.1.1.1         0                     32768   i
* >e 9.1.1.0/24         3.1.1.1         0                     0       65009i
```

以上显示信息表明，在 Router B 上发布本地网段路由后，Router A 新增了到达 9.1.1.0/24 的路由。

查看 Router C 的 BGP 路由表。

```
[RouterC] display bgp routing-table ipv4

 Total number of routes: 3

 BGP local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >i 3.1.1.0/24         2.2.2.2         0          100        0       ?
* >i 8.1.1.0/24         3.1.1.2         0          100        0       65008i
* >i 9.1.1.0/24         2.2.2.2         0          100        0       i
```

以上显示信息表明，到 8.1.1.0 的路由变为有效路由，下一跳为 Router A 的地址。

3.6 验证配置

使用 Ping 进行验证。

```
[RouterC] ping 8.1.1.1
Ping 8.1.1.1 (8.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 8.1.1.1: icmp_seq=0 ttl=254 time=10.000 ms
56 bytes from 8.1.1.1: icmp_seq=1 ttl=254 time=4.000 ms
56 bytes from 8.1.1.1: icmp_seq=2 ttl=254 time=4.000 ms
56 bytes from 8.1.1.1: icmp_seq=3 ttl=254 time=3.000 ms
56 bytes from 8.1.1.1: icmp_seq=4 ttl=254 time=3.000 ms

--- Ping statistics for 8.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 3.000/4.800/10.000/2.638 ms
```

以上信息表明 Router C 能够访问 Router A 直连的 8.1.1.0/24 网段。

3.7 配置文件

- Router A

```
#
interface Loopback0
ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet 2/0/1
 ip address 8.1.1.1 255.255.255.0
#
interface GigabitEthernet 2/0/2
 ip address 3.1.1.2 255.255.255.0
#
bgp 65008
router-id 1.1.1.1
peer 3.1.1.1 as-number 65009
#
address-family ipv4 unicast
network 8.1.1.0 255.255.255.0
peer 3.1.1.1 enable
#
```

- Router B

```
#
interface Loopback0
ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet 2/0/1
ip address 3.1.1.1 255.255.255.0
#
interface GigabitEthernet 2/0/2
ip address 9.1.1.1 255.255.255.0
#
bgp 65009
router-id 2.2.2.2
```

```
peer 3.1.1.2 as-number 65008
peer 3.3.3.3 as-number 65009
peer 3.3.3.3 connect-interface Loopback0
#
address-family ipv4 unicast
network 3.1.1.0 24
network 9.1.1.0 24
peer 3.1.1.2 enable
peer 3.3.3.3 enable
#
ospf 1
area 0.0.0.0
network 2.2.2.2 0.0.0.0
network 9.1.1.0 0.0.0.255
#
```

- Router C

```
#
interface Loopback0
ip address 3.3.3.3 255.255.255.255
#
interface GigabitEthernet 2/0/1
ip address 9.1.1.2 255.255.255.0
#
bgp 65009
router-id 3.3.3.3
peer 2.2.2.2 as-number 65009
peer 2.2.2.2 connect-interface Loopback0
#
address-family ipv4 unicast
peer 2.2.2.2 enable
#
ospf 1
area 0.0.0.0
network 3.3.3.3 0.0.0.0
network 9.1.1.0 0.0.0.255
#
```

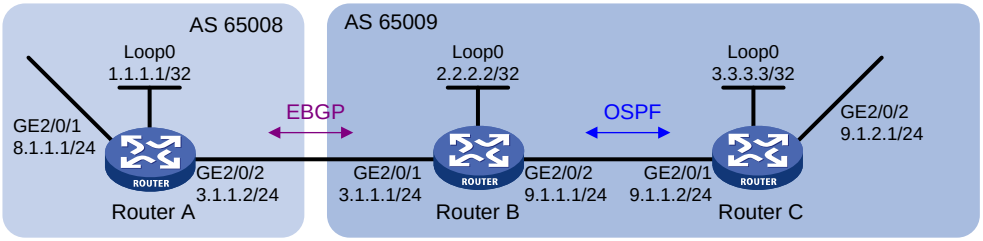
4 BGP 与 IGP 交互配置举例

4.1 组网需求

公司 A 的所有设备在 AS 65008 内，公司 B 的所有设备在 AS 65009 内，AS 65008 和 AS 65009 通过设备 Router A 和 Router B 相连。公司 A 的研发部门所在网段为 8.1.1.0/24，公司 B 的研发部门所在网段为 9.1.2.0/24。

由于市场需求，现在两个公司决定联合开发一款新型产品，这就需要两个公司的研发部门可以互相通信，实现网段 9.1.2.0/24 与网段 8.1.1.0/24 的互通，同时需要确保两个公司的其它网段不能相互通信。

图2 BGP 与 IGP 交互配置组网图



4.2 配置思路

在 Router B 上将 BGP 和 OSPF 路由互相引入，使得 Router A 可以访问 9.1.2.0/24 网段，Router C 可以访问 8.1.1.0/24 网段。

4.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.4 配置注意事项

EBGP 邻居关系的两台路由器，处于不同的 AS 域，对端的 LoopBack 接口一般路由不可达，所以一般使用直连地址建立 EBGP 邻居。

4.5 配置步骤

4.5.1 配置各接口的 IP 地址

#配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface GigabitEthernet 2/0/1
[RouterA-GigabitEthernet2/0/1] ip address 8.1.1.1 255.255.255.0
```

#请参考以上方法配置其它相关接口的 IP 地址，配置步骤这里省略。

4.5.2 配置 OSPF

在 AS 65009 内配置 OSPF，使得 Router B 能获取到到 9.1.2.0/24 网段的路由。

1. Router B 的配置

```
<RouterB> system-view
[RouterB] ospf 1
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
```

```
[RouterB-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

2. Router C 的配置

```
<RouterC> system-view
[RouterC] ospf 1
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 9.1.2.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

4.5.3 配置 EBGP 连接

配置 EBGP 连接，并在 Router A 上将 8.1.1.0/24 网段通告到 BGP 路由表中，以便 Router B 获取到网段 8.1.1.0/24 的路由。

1. Router A 的配置

```
<RouterA> system-view
[RouterA] bgp 65008
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 3.1.1.1 as-number 65009
[RouterA-bgp] address-family ipv4 unicast
[RouterA-bgp-ipv4] peer 3.1.1.1 enable
[RouterA-bgp-ipv4] network 8.1.1.0 24
[RouterA-bgp-ipv4] quit
[RouterA-bgp] quit
```

2. Router B 的配置

```
[RouterB] bgp 65009
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 3.1.1.2 as-number 65008
[RouterB-bgp] address-family ipv4 unicast
[RouterB-bgp-ipv4] peer 3.1.1.2 enable
```

4.5.4 配置 BGP 与 IGP 交互

在 Router B 上配置 BGP 和 OSPF 互相引入路由。

```
[RouterB-bgp-ipv4] import-route ospf 1
[RouterB-bgp-ipv4] quit
[RouterB-bgp] quit
[RouterB] ospf 1
[RouterB-ospf-1] import-route bgp
[RouterB-ospf-1] quit
```

查看 Router A 的 BGP 路由表。

```
[RouterA] display bgp routing-table ipv4

 Total number of routes: 3
```

```
 BGP local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >  8.1.1.0/24         8.1.1.1         0                     32768   i
* >e 9.1.2.0/24         3.1.1.1         1                     0       65009?
```

查看 RouterC 的 OSPF 路由表。

```
[RouterC] display ospf routing

          OSPF Process 1 with Router ID 3.3.3.3
                  Routing Tables

 Routing for Network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 9.1.1.0/24         1        Transit 9.1.1.2         3.3.3.3         0.0.0.0
 9.1.2.0/24         1        Stub    9.1.2.1         192.168.0.63    0.0.0.0
 2.2.2.2/32         1        Stub    9.1.1.1         2.2.2.2         0.0.0.0

 Routing for ASEs
 Destination        Cost     Type    Tag         NextHop         AdvRouter
 8.1.1.0/24         1        Type2   1           9.1.1.1         2.2.2.2

 Total Nets: 3
 Intra Area: 2  Inter Area: 0  ASE: 1  NSSA: 0
```

从 Router A 的 BGP 路由表和 Router C 的 OSPF 路由表可以看出，Router B 上的 BGP 和 OSPF 已经互相引入。

4.6 验证配置

在 Router A 上使用源地址 8.1.1.1Ping 目标地址 9.1.2.1 进行验证。

```
[RouterA] ping -a 8.1.1.1 9.1.2.1
Ping 9.1.2.1 (9.1.2.1) from 8.1.1.1: 56 data bytes, press CTRL_C to break
56 bytes from 9.1.2.1: icmp_seq=0 ttl=254 time=10.000 ms
56 bytes from 9.1.2.1: icmp_seq=1 ttl=254 time=12.000 ms
56 bytes from 9.1.2.1: icmp_seq=2 ttl=254 time=2.000 ms
56 bytes from 9.1.2.1: icmp_seq=3 ttl=254 time=7.000 ms
56 bytes from 9.1.2.1: icmp_seq=4 ttl=254 time=9.000 ms

--- Ping statistics for 9.1.2.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 2.000/8.000/12.000/3.406 ms
```

在 Router C 上使用源地址 9.1.2.1Ping 目标地址 8.1.1.1 进行验证。

```
[RouterC] ping -a 9.1.2.1 8.1.1.1
```

```
Ping 8.1.1.1 (8.1.1.1) from 9.1.2.1: 56 data bytes, press CTRL_C to break
56 bytes from 8.1.1.1: icmp_seq=0 ttl=254 time=9.000 ms
56 bytes from 8.1.1.1: icmp_seq=1 ttl=254 time=4.000 ms
56 bytes from 8.1.1.1: icmp_seq=2 ttl=254 time=3.000 ms
56 bytes from 8.1.1.1: icmp_seq=3 ttl=254 time=3.000 ms
56 bytes from 8.1.1.1: icmp_seq=4 ttl=254 time=3.000 ms

--- Ping statistics for 8.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 3.000/4.400/9.000/2.332 ms
```

上述显示信息说明网段 9.1.2.0/24 与网段 8.1.1.0/24 能实现互通。

在 Router A 上使用源地址 8.1.2.1 分别 Ping 目标地址 9.1.2.1 和 9.1.3.1 进行验证。

```
[RouterA] ping –a 8.1.2。1 9.1.2.1
Ping 9.1.2.1 (9.1.2.1) from 8.1.2.1: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping statistics for 9.1.2.1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss

[RouterA] ping –a 8.1.2.1 9.1.3.1
Ping 9.1.3.1 (9.1.3.1) from 8.1.2.1: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping statistics for 9.1.3.1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

在 Router C 上使用源地址 9.1.3.1 分别 Ping 目标地址 8.1.1.1 和 8.1.2.1 进行验证。

```
[RouterC] ping –a 9.1.3.1 8.1.1.1
Ping 8.1.1.1 (8.1.1.1) from 9.1.3.1: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping statistics for 8.1.1.1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss

[RouterC] ping –a 9.1.3.1 8.1.2.1
Ping 8.1.2.1 (8.1.2.1) from 9.1.3.1: 56 data bytes, press CTRL_C to break
```

```
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping statistics for 8.1.2.1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

上述信息说明两个自治区域之间只有网段 9.1.2.0/24 与网段 8.1.1.0/24 能实现互通，其他网段之间是无法互通的。

4.7 配置文件

- Router A

```
#
interface Loopback0
ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet 2/0/1
ip address 8.1.1.1 255.255.255.0
#
interface GigabitEthernet 2/0/2
ip address 3.1.1.2 255.255.255.0
#
bgp 65008
router-id 1.1.1.1
peer 3.1.1.1 as-number 65009
#
address-family ipv4 unicast
network 8.1.1.0 255.255.255.0
peer 3.1.1.1 enable
#
```

- Router B

```
#
interface Loopback0
ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet 2/0/1
ip address 3.1.1.1 255.255.255.0
#
interface GigabitEthernet 2/0/2
ip address 9.1.1.1 255.255.255.0
#
bgp 65009
router-id 2.2.2.2
peer 3.1.1.2 as-number 65008
#
```

```
address-family ipv4 unicast
import-route ospf 1
peer 3.1.1.2 enable
#
ospf 1
import-route bgp
area 0.0.0.0
network 2.2.2.2 0.0.0.0
network 9.1.1.0 0.0.0.255
#
```

- Router C

```
#
interface Loopback0
ip address 3.3.3.3 255.255.255.255
#
interface GigabitEthernet 2/0/1
ip address 9.1.1.2 255.255.255.0
#
interface GigabitEthernet 2/0/2
ip address 9.1.2.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 9.1.1.0 0.0.0.255
network 9.1.2.0 0.0.0.255
#
```

5 相关资料

- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由配置指导-R7607
- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

BGP 路由属性控制路由选择配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1

2 配置前提 1

3 通过 AS-Path 属性控制路由选择配置举例 1

3.1 组网需求 1

3.2 配置思路 2

3.3 使用版本 2

3.4 配置步骤 2

3.4.1 配置各接口的 IP 地址 2

3.4.2 配置路由策略 5

3.5 验证配置 5

3.6 配置文件 6

4 通过 MED 属性控制路由选择配置举例 9

4.1 组网需求 9

4.2 配置思路 10

4.3 使用版本 10

4.4 配置步骤 10

4.4.1 基础配置 10

4.4.2 配置路由策略 12

4.5 验证配置 12

4.6 配置文件 12

5 相关资料 14

1 简介

本文档介绍使用通过 BGP 路由属性控制路由选择的配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 BGP 特性和路由策略特性。

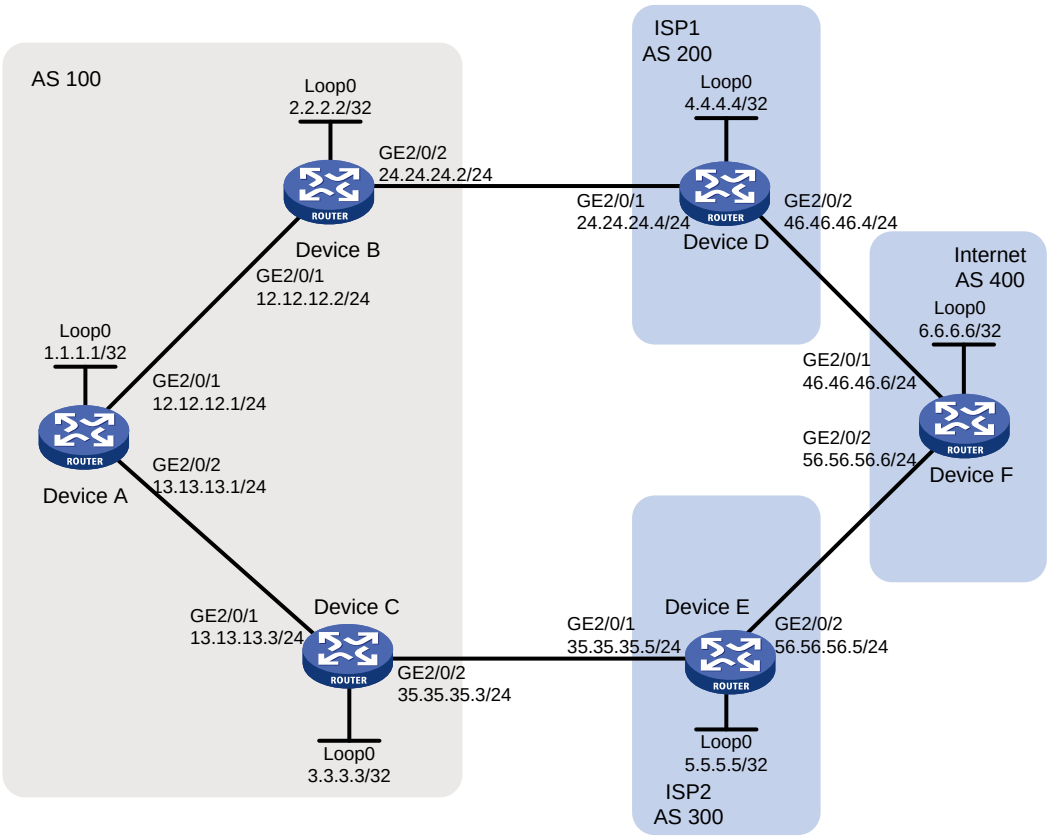
3 通过 AS-Path 属性控制路由选择配置举例

3.1 组网需求

如图 1 所示，所有设备均运行 BGP 协议。AS 100 和 AS 400 之间有两条路径可以通信，这两条路径分别经过 AS 200 和 AS 300。现要求通过配置路由策略，实现：

- AS 100 内的设备访问 AS 200 始发的路由时，优先选择从 Device D 转发；
- AS 100 内的设备访问 AS 300 始发的路由时，优先选择从 Device E 转发；
- AS 100 内的设备访问 AS 400 始发的路由时，优先选择从 Device D 转发。

图1 AS-Path 属性控制路由选择配置组网图



3.2 配置思路

- 为了使 AS 100 内的设备能够根据路由的始发 AS 号来选择优先转发路径，需要在 AS 100 的边缘设备上为特定 AS 始发的路由提高优先级，并将该路由扩散至 AS 100 内部：
  - 在 Device B 上配置路由策略，将从 AS 200 或 AS 400 始发的路由的本地优先级设置为 300；
  - 在 Device C 上配置路由策略，将从 AS 300 始发的路由的本地优先级设置为 200。
- 使用 AS 路径过滤列表来匹配由指定 AS 始发的路由。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置步骤

3.4.1 配置各接口的 IP 地址

配置 Device A 的接口 GigabitEthernet2/0/1 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface GigabitEthernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 12.12.12.1 24
```

```
[DeviceA-GigabitEthernet2/0/1] quit
```
请参考以上方法配置其它相关接口的 IP 地址，配置步骤这里省略。

配置 BGP 连接

在 Device A 上创建本地 AS 号为 100 的 BGP 实例，指定对等体 12.12.12.2 和 13.13.13.3。
```
[DeviceA] bgp 100
[DeviceA-bgp] router-id 1.1.1.1
[DeviceA-bgp] peer 12.12.12.2 as-number 100
[DeviceA-bgp] peer 13.13.13.3 as-number 100
[DeviceA-bgp] address-family ipv4 unicast
[DeviceA-bgp-ipv4] peer 12.12.12.2 enable
[DeviceA-bgp-ipv4] peer 13.13.13.3 enable
[DeviceA-bgp-ipv4] quit
[DeviceA-bgp] quit
```
在 Device B 上创建本地 AS 号为 100 的 BGP 实例，,指定对等体 12.12.12.1 和 24.24.24.4，并引入直连路由。
```
[DeviceB] bgp 100
[DeviceB-bgp] router-id 2.2.2.2
[DeviceB-bgp] peer 12.12.12.1 as-number 100
[DeviceB-bgp] peer 24.24.24.4 as-number 200
[DeviceB-bgp] address-family ipv4 unicast
[DeviceB-bgp-ipv4] peer 12.12.12.1 enable
[DeviceB-bgp-ipv4] peer 24.24.24.4 enable
[DeviceB-bgp-ipv4] import-route direct
[DeviceB-bgp-ipv4] quit
[DeviceB-bgp] quit
```
在 Device C 上创建本地 AS 号为 100 的 BGP 实例，指定对等体 13.13.13.1 和 35.35.35.5，并引入直连路由。
```
[DeviceC] bgp 100
[DeviceC-bgp] router-id 3.3.3.3
[DeviceC-bgp] peer 13.13.13.1 as-number 100
[DeviceC-bgp] peer 35.35.35.5 as-number 300
[DeviceC-bgp] address-family ipv4 unicast
[DeviceC-bgp-ipv4] peer 13.13.13.1 enable
[DeviceC-bgp-ipv4] peer 35.35.35.5 enable
[DeviceC-bgp-ipv4] import-route direct
[DeviceC-bgp-ipv4] quit
[DeviceC-bgp] quit
```
在 Device D 上创建本地 AS 号为 200 的 BGP 实例，指定对等体 24.24.24.2 和 46.46.46.6，并发布路由 4.4.4.4/32。
```
[DeviceD] bgp 200
[DeviceD-bgp] router-id 4.4.4.4
[DeviceD-bgp] peer 24.24.24.2 as-number 100
[DeviceD-bgp] peer 46.46.46.6 as-number 400
[DeviceD-bgp] address-family ipv4 unicast
[DeviceD-bgp-ipv4] peer 24.24.24.2 enable
[DeviceD-bgp-ipv4] peer 46.46.46.6 enable
```

```
[DeviceD-bgp-ipv4] network 4.4.4.4 32
[DeviceD-bgp-ipv4] quit
[DeviceD-bgp] quit
```

在 Device E 上创建本地 AS 号为 300 的 BGP 实例，指定对等体 35.35.35.3 和 56.56.56.6，并发布路由 5.5.5.5/32。

```
[DeviceE] bgp 300
[DeviceE-bgp] router-id 5.5.5.5
[DeviceE-bgp] peer 35.35.35.3 as-number 100
[DeviceE-bgp] peer 56.56.56.6 as-number 400
[DeviceE-bgp] address-family ipv4 unicast
[DeviceE-bgp-ipv4] peer 35.35.35.3 enable
[DeviceE-bgp-ipv4] peer 56.56.56.6 enable
[DeviceE-bgp-ipv4] network 5.5.5.5 32
[DeviceE-bgp-ipv4] quit
[DeviceE-bgp] quit
```

在 Device F 上创建本地 AS 号为 400 的 BGP 实例，指定对等体 46.46.46.4 和 56.56.56.5，并发布路由 6.6.6.6/32。

```
[DeviceF] bgp 400
[DeviceF-bgp] router-id 6.6.6.6
[DeviceF-bgp] peer 46.46.46.4 as-number 200
[DeviceF-bgp] peer 56.56.56.5 as-number 300
[DeviceF-bgp] address-family ipv4 unicast
[DeviceF-bgp-ipv4] peer 46.46.46.4  enable
[DeviceF-bgp-ipv4] peer 56.56.56.5 enable
[DeviceF-bgp-ipv4] network 6.6.6.6 32
[DeviceF-bgp-ipv4] quit
[DeviceF-bgp] quit
```

完成以上配置后，在 Device A 上查看 BGP 路由表，可以看到 Device D、Device E 和 Device F 发布的路由及其 AS-Path 属性。

```
[DeviceA] display bgp routing-table ipv4

Total number of routes: 12

 BGP local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >i 2.2.2.2/32         12.12.12.2      0          100        0       ?
* >i 3.3.3.3/32         13.13.13.3      0          100        0       ?
* >i 4.4.4.4/32         24.24.24.4      0          100        0       200i
*  i                    35.35.35.5                 100        0       300 400
                                                                      200i
* >i 5.5.5.5/32         35.35.35.5      0          100        0       300i
*  i                    24.24.24.4                 100        0       200 400
```

```
                                                                    300i
* >i 6.6.6.6/32          24.24.24.4                100        0       200 400i
*  i                     35.35.35.5                100        0       300 400i
* >i 12.12.12.0/24       12.12.12.2       0        100        0       ?
* >i 13.13.13.0/24       13.13.13.3       0        100        0       ?
* >i 24.24.24.0/24       12.12.12.2       0        100        0       ?
* >i 35.35.35.0/24       13.13.13.3       0        100        0       ?
```

3.4.2 配置路由策略

在 Device B 上创建路由策略 aspath，将 AS-Path 以 200 或 400 结尾的路由的本地优先级设置为 300。

```
[DeviceB] ip as-path 1 permit 200$
[DeviceB] ip as-path 1 permit 400$
[DeviceB] route-policy aspath permit node 10
[DeviceB-route-policy-aspath-10] if-match as-path 1
[DeviceB-route-policy-aspath-10] apply local-preference 300
[DeviceB-route-policy-aspath-10] quit
```

在 Device B 上配置对从对等体 24.24.24.4 接收的路由应用路由策略 aspath。

```
[DeviceB] bgp 100
[DeviceB-bgp] address-family ipv4
[DeviceB-bgp-ipv4] peer 24.24.24.4 route-policy aspath import
```

在 Device C 上创建路由策略 aspath，将 AS-Path 以 300 结尾的路由的本地优先级设置为 200。

```
[DeviceC] ip as-path 1 permit 300$
[DeviceC] route-policy aspath permit node 20
[DeviceC-route-policy-aspath-20] if-match as-path 1
[DeviceC-route-policy-aspath-20] apply local-preference 200
[DeviceC-route-policy-aspath-20] quit
```

在 Device C 上配置对从对等体 35.35.35.5 接收的路由应用路由策略 aspath。

```
[DeviceC] bgp 100
[DeviceC-bgp] address-family ipv4
[DeviceC-bgp-ipv4] peer 35.35.35.5 route-policy aspath import
```

3.5 验证配置

在 Device A 上再次查看 BGP 路由表，可以看到路由的本地优先级发生了变化，从 AS 200 和 AS 400 始发的路由的本地优先级变为 300，从 AS 300 始发的路由的本地优先级变为 200。

```
[DeviceA] display bgp routing-table ipv4

Total number of routes: 11

 BGP local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
```

```
* >i 2.2.2.2/32         12.12.12.2      0          100        0       ?
* >i 3.3.3.3/32         13.13.13.3      0          100        0       ?
* >i 4.4.4.4/32         24.24.24.4      0          300        0       200i
* >i 5.5.5.5/32         35.35.35.5      0          200        0       300i
* >i 6.6.6.6/32         24.24.24.4                 300        0       200 400i
* >i 12.12.12.0/24      12.12.12.2      0          100        0       ?
* >i 13.13.13.0/24      13.13.13.3      0          100        0       ?
* >i 24.24.24.0/24      12.12.12.2      0          100        0       ?
* >i 35.35.35.0/24      13.13.13.3      0          100        0       ?
```

从 Device A 查看到达 6.6.6.6 的报文所经过的路径。可以看出，报文通过 Device D 转发。

```
[DeviceA] tracert 6.6.6.6
traceroute to 6.6.6.6 (6.6.6.6), 30 hops at most, 52 bytes each packet, press CT
RL_C to break
 1  12.12.12.2 (12.12.12.2)  2.417 ms  1.887 ms  1.773 ms
 2  24.24.24.4 (24.24.24.4)  4.057 ms  2.293 ms  2.739 ms
 3  6.6.6.6 (6.6.6.6)  5.145 ms  4.205 ms  4.402 ms
```

3.6 配置文件

- Device A：

```
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 12.12.12.1 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 13.13.13.1 255.255.255.0
#
bgp 100
 router-id 1.1.1.1
 peer 12.12.12.2 as-number 100
 peer 13.13.13.3 as-number 100
 #
 address-family ipv4 unicast
  peer 12.12.12.2 enable
  peer 13.13.13.3 enable
#
```

- Device B ：

```
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet2/0/1
```

```
 port link-mode route
 ip address 12.12.12.2 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 24.24.24.2 255.255.255.0
#
bgp 100
 router-id 2.2.2.2
 peer 12.12.12.1 as-number 100
 peer 24.24.24.4 as-number 200
 #
 address-family ipv4 unicast
  import-route direct
  peer 12.12.12.1 enable
  peer 24.24.24.4 enable
  peer 24.24.24.4 route-policy aspath import
#
route-policy aspath permit node 10
 if-match as-path 1
 apply local-preference 300
#
 ip as-path 1 permit 200$
 ip as-path 1 permit 400$
#
```

- Device C：

```
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 13.13.13.3 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 35.35.35.3 255.255.255.0
#
bgp 100
 router-id 3.3.3.3
 peer 13.13.13.1 as-number 100
 peer 35.35.35.5 as-number 300
 #
 address-family ipv4 unicast
  import-route direct
  peer 13.13.13.1 enable
  peer 35.35.35.5 enable
  peer 35.35.35.5 route-policy aspath import
```

```
#
route-policy aspath permit node 20
 if-match as-path 1
 apply local-preference 200
#
 ip as-path 1 permit 300$
#
```

- Device D：

```
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface GigabitEthernet2/1/1
 port link-mode route
 ip address 24.24.24.4 255.255.255.0
#
interface GigabitEthernet2/1/2
 port link-mode route
 ip address 46.46.46.4 255.255.255.0
#
bgp 200
 router-id 4.4.4.4
 peer 24.24.24.2 as-number 100
 peer 46.46.46.6 as-number 400
 #
 address-family ipv4 unicast
  network 4.4.4.4 255.255.255.255
  peer 24.24.24.2 enable
  peer 46.46.46.6 enable
#
```

- Device E：

```
#
interface LoopBack0
 ip address 5.5.5.5 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 35.35.35.5 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 56.56.56.5 255.255.255.0
#
bgp 300
 router-id 5.5.5.5
 peer 35.35.35.3 as-number 100
 peer 56.56.56.6 as-number 400
 #
```

```
 address-family ipv4 unicast
  network 5.5.5.5 255.255.255.255
  peer 35.35.35.3 enable
  peer 56.56.56.6 enable
#
```

- Device F：

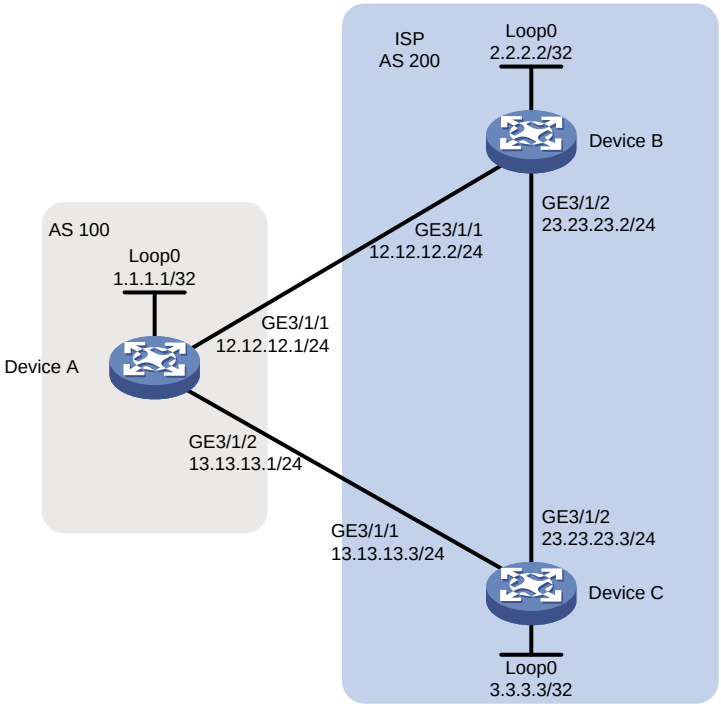
```
#
interface LoopBack0
 ip address 6.6.6.6 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 combo enable copper
 ip address 46.46.46.6 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 combo enable copper
 ip address 56.56.56.6 255.255.255.0
#
bgp 400
 router-id 6.6.6.6
 peer 46.46.46.4 as-number 200
 peer 56.56.56.5 as-number 300
 #
 address-family ipv4 unicast
  network 6.6.6.6 255.255.255.255
  peer 46.46.46.4 enable
  peer 56.56.56.5 enable
#
```

4 通过 MED 属性控制路由选择配置举例

4.1 组网需求

如图 2 所示，所有设备均运行 BGP 协议。Device A 与 Device B、Device C 之间运行 EBGP，Device B、Device C 之间运行 IBGP。由于 Device B 的 Router ID 小于 Device C 的 Router ID，所以当 AS 100 访问 AS 200 时，流量优先选择从 Device B 转发。现要求通过配置路由策略，实现 AS 100 访问 AS 200 的流量优先选择通过 Device C 转发。

图2 MED 属性控制路由选择配置组网图



4.2 配置思路

为了实现 AS 100 访问 AS 200 的流量优先选择通过 Device C 转发，需要通过路由策略修改 Device B 发送给 Device A 的 MED 值，使其大于缺省 MED 值 0。

4.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.4 配置步骤

4.4.1 基础配置

配置 Device A 的接口 GigabitEthernet2/0/1 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface GigabitEthernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 12.12.12.1 24
[DeviceA-GigabitEthernet2/0/1] quit
```

请参考以上方法配置其它相关接口的 IP 地址，配置步骤这里省略。

#请参考以上方法配置其它相关接口的 IP 地址，配置步骤这里省略。

在 Device A 上创建本地 AS 号为 100 的 BGP 实例，指定对等体 12.12.12.2 和 13.13.13.3。

```
[DeviceA] bgp 100
[DeviceA-bgp] router-id 1.1.1.1
[DeviceA-bgp] peer 12.12.12.2 as-number 200
```

```
[DeviceA-bgp] peer 13.13.13.3 as-number 200
[DeviceA-bgp] address-family ipv4 unicast
[DeviceA-bgp-ipv4] peer 12.12.12.2 enable
[DeviceA-bgp-ipv4] peer 13.13.13.3 enable
[DeviceA-bgp-ipv4] quit
[DeviceA-bgp] quit
```

在 Device B 上创建本地 AS 号为 200 的 BGP 实例，指定对等体 12.12.12.1 和 3.3.3.3。

```
[DeviceB] bgp 200
[DeviceB-bgp] router-id 2.2.2.2
[DeviceB-bgp] peer 12.12.12.1 as-number 100
[DeviceB-bgp] peer 3.3.3.3 as-number 200
[DeviceB-bgp] peer 3.3.3.3 connect-interface LoopBack0
[DeviceB-bgp] address-family ipv4 unicast
[DeviceB-bgp-ipv4] peer 12.12.12.1 enable
[DeviceB-bgp-ipv4] peer 3.3.3.3 enable
[DeviceB-bgp-ipv4] network 23.23.23.0 24
[DeviceB-bgp-ipv4] quit
[DeviceB-bgp] quit
```

在 Device B 上配置目的地址为 3.3.3.3/32 的静态路由，以保证对等体 3.3.3.3 可达。

```
[DeviceB] ip route-static 3.3.3.3 32 23.23.23.3
```

在 Device C 上创建本地 AS 号为 200 的 BGP 实例，指定对等体 13.13.13.1 和 2.2.2.2。

```
[DeviceC] bgp 200
[DeviceC-bgp] router-id 3.3.3.3
[DeviceC-bgp] peer 13.13.13.1 as-number 100
[DeviceC-bgp] peer 2.2.2.2 as-number 200
[DeviceC-bgp] peer 2.2.2.2 connect-interface LoopBack0
[DeviceC-bgp] address-family ipv4 unicast
[DeviceC-bgp-ipv4] peer 13.13.13.1 enable
[DeviceC-bgp-ipv4] peer 2.2.2.2 enable
[DeviceC-bgp-ipv4] network 23.23.23.0 24
[DeviceC-bgp-ipv4] quit
[DeviceC-bgp] quit
```

在 Device C 上配置目的地址为 2.2.2.2/32 的静态路由，以保证对等体 2.2.2.2 可达。

```
[DeviceC] ip route-static 2.2.2.2 32 23.23.23.2
```

完成以上配置后，在 Device A 上查看 BGP 路由表，可以看到前往 23.23.23.0/24 网段的两条有效路由，其中下一跳为 12.12.12.2 的路由为最优路由，这是由于 Device B 的 Router ID 较小。

```
[DeviceA] display bgp routing-table ipv4

 Total number of routes: 2

 BGP local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
```

```
* >e 23.23.23.0/24      12.12.12.2      0                    0       200i
*  e                    13.13.13.3      0                    0       200i
```

4.4.2 配置路由策略

在 Device B 上创建路由策略 10，将 cost 修改为 100。

```
[DeviceB] route-policy 10 permit node 10
[DeviceB-route-policy-10-10] apply cost 100
[DeviceB-route-policy-10-10] quit
```

在 Device B 上配置对向对等体 12.12.12.1 发送的路由应用路由策略 10，即修改 Device B 发送给 Device A 的 MED 值为 100。

```
[DeviceB] bgp 200
[DeviceB-bgp] address-family ipv4 unicast
[DeviceB-bgp-ipv4] peer 12.12.12.1 route-policy 10 export
[DeviceB-bgp-ipv4] quit
[DeviceB-bgp] quit
```

4.5 验证配置

查看 Device A 的 BGP 路由表，可以看到下一跳为 12.12.12.2 的路由的 MED 值变为 100，下一跳为 13.13.13.3 的路由成为了最优路由。

```
[DeviceA] display bgp routing-table ipv4

 Total number of routes: 2

 BGP local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >e 23.23.23.0/24      13.13.13.3      0                     0       200i
*  e                    12.12.12.2      100                   0       200i
```

4.6 配置文件

- Device A：

```
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 12.12.12.1 255.255.255.0
#
interface GigabitEthernet2/0/2
```

```
 port link-mode route
 ip address 13.13.13.1 255.255.255.0
#
bgp 100
 router-id 1.1.1.1
 peer 12.12.12.2 as-number 200
 peer 13.13.13.3 as-number 200
 #
 address-family ipv4 unicast
  peer 12.12.12.2 enable
  peer 13.13.13.3 enable
#
```

- Device B：

```
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 12.12.12.2 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 23.23.23.2 255.255.255.0
#
bgp 200
 router-id 2.2.2.2
 peer 3.3.3.3 as-number 200
 peer 3.3.3.3 connect-interface LoopBack0
 peer 12.12.12.1 as-number 100
 #
 address-family ipv4 unicast
  network 23.23.23.0 255.255.255.0
  peer 3.3.3.3 enable
  peer 12.12.12.1 enable
  peer 12.12.12.1 route-policy 10 export
#
route-policy 10 permit node 10
 apply cost 100
#
 ip route-static 3.3.3.3 32 23.23.23.3
#
```

- Device B：

```
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface GigabitEthernet2/0/1
```

```
 port link-mode route
 ip address 13.13.13.3 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 23.23.23.3 255.255.255.0
#
bgp 200
 router-id 3.3.3.3
 peer 2.2.2.2 as-number 200
 peer 2.2.2.2 connect-interface LoopBack0
 peer 13.13.13.1 as-number 100
 #
 address-family ipv4 unicast
  network 23.23.23.0 255.255.255.0
  peer 2.2.2.2 enable
  peer 13.13.13.1 enable
#
 ip route-static 2.2.2.2 32 23.23.23.2
#
```

5 相关资料

- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由配置指导-R7607
- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

CPOS 接口配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 CPOS 汇聚 E1 典型配置举例 1
3.1 组网需求 1
3.2 使用版本 1
3.3 配置注意事项 1
3.4 配置步骤 2
3.5 验证配置 2
3.6 配置文件 5
4 相关资料 5

1 简介

本文档介绍了使用 CPOS 汇聚 E1 的配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

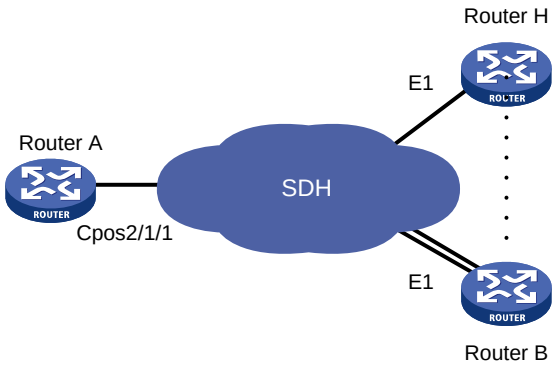
本文假设您已了解 CPOS、E1、MP 特性。

3 CPOS 汇聚 E1 典型配置举例

3.1 组网需求

Router A 中心节点下属有 B～H 七个分支节点，每个分支节点设备通过 E1 链路上行连接到 Router A；Router A 通过 CPOS 接口汇聚上行的链路。最近，由于 Router B 上的接入用户增多，导致带宽需求增加，一条 E1 链路满足不了需求，因此添加了一条 E1 链路。要求用 MP-group 接口的方式，对这两条 E1 链路进行捆绑。

图1 CPOS 汇聚 E1 配置组网图



3.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.3 配置注意事项

设备与 SONET/SDH 设备相连时，由于 SONET/SDH 网络的时钟精度高于设备内部时钟源的精度，所以在本举例中请确保在 SONET/SDH 设备上已经配置主时钟模式。

3.4 配置步骤

(1) 配置 Router A

设置 CPOS 接口的 E1 通道工作在非成帧模式。

```
<RouterA> system-view
[RouterA] controller cpos 2/1/1
[RouterA-Cpos2/1/1] e1 1 unframed
[RouterA-Cpos2/1/1] e1 2 unframed
[RouterA-Cpos2/1/1] quit
```

创建 MP-group 接口，配置相应的 IP 地址。

```
[RouterA] interface mp-group 2/1/1
[RouterA-Mp-group2/1/1] ip address 10.1.1.1 24
[RouterA-Mp-group2/1/1] quit
```

为与 Router B 的两条 E1 链路配置逻辑串口 Serial2/1/1/1:0 和 Serial2/1/1/2:0。

```
[RouterA] interface serial2/1/1/1:0
[RouterA-Serial2/1/1/1:0] ppp mp mp-group 2/1/1
[RouterA-Serial2/1/1/1:0] quit
[RouterA] interface serial2/1/1/2:0
[RouterA-Serial2/1/1/2:0] ppp mp mp-group 2/1/1
[RouterA-Serial2/1/1/2:0] quit
```

(2) 配置 Router B

进入 CE1 接口 E1 2/1/1 的视图，并配置此接口工作在 E1 方式。

```
<RouterB> system-view
[RouterB] controller e1 2/1/1
[RouterB-E1 2/1/1] using e1
[RouterB-E1 2/1/1] quit
```

进入 CE1 接口 E1 2/1/2 的视图，并配置此接口工作在 E1 方式。

```
[RouterB] controller e1 2/1/2
[RouterB-E1 2/1/2] using e1
[RouterB-E1 2/1/2] quit
```

创建 MP-group 接口。

```
[RouterB] interface mp-group 2/1/1
[RouterB-Mp-group2/1/1] ip address 10.1.1.2 24
[RouterB-Mp-group2/1/1] quit
```

为两条 E1 链路配置逻辑串口 Serial2/1/1:0 和 Serial2/1/2:0。

```
[RouterB] interface serial2/1/1:0
[RouterB-Serial2/1/1:0] ppp mp mp-group 2/1/1
[RouterB-Serial2/1/1:0] quit
[RouterB] interface serial2/1/2:0
[RouterB-Serial2/1/2:0] ppp mp mp-group 2/1/1
[RouterB-Serial2/1/2:0] quit
```

3.5 验证配置

(1) 检查 Router A 与 Router B 的 MP-group 接口是否可以互相正常通信。

检查 Router A 上的 MP-group 接口。

```
[RouterA] ping 10.1.1.2
Ping 10.1.1.2 (10.1.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 10.1.1.2: icmp_seq=0 ttl=255 time=32.998 ms
56 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=27.632 ms
56 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=34.517 ms
56 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=45.058 ms
56 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=35.121 ms

--- Ping statistics for 10.1.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 27.632/35.065/45.058/5.651 ms
```

检查 Router B 上的 MP-group 接口。

```
[RouterB] ping 10.1.1.1
Ping 10.1.1.1 (10.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 10.1.1.1: icmp_seq=0 ttl=255 time=27.877 ms
56 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=27.616 ms
56 bytes from 10.1.1.1: icmp_seq=2 ttl=255 time=42.308 ms
56 bytes from 10.1.1.1: icmp_seq=3 ttl=255 time=36.238 ms
56 bytes from 10.1.1.1: icmp_seq=4 ttl=255 time=71.639 ms

--- Ping statistics for 10.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 27.616/41.136/71.639/16.214 ms
```

(2) 检查 Router A 和 Router B 的 MP-group 接口的详细信息，查看 MP-group 接口状态。

检查 Router A 的 MP-group 接口的详细信息。

```
[RouterA] display interface mp-group 2/1/1
MP-group2/1/1
Current state: UP
Line protocol state: UP
Description: MP-group2/1/1 Interface
Bandwidth: 1024kbps
Maximum Transmit Unit: 1500
Hold timer: 10 seconds, retry times: 5
Internet Address is 10.1.1.1/24 (primary)
Link layer protocol: PPP
LCP: opened, MP: opened, IPCP: opened, OSICP: opened, MPLSCP: opened, IPv6CP: op
ened
Physical: MP, baudrate: 1024000 bps
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last link flapping: Never
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
```

```
Output: 0 packets, 0 bytes, 0 drops
```

检查 Router B 的 MP-group 接口的详细信息。

```
[RouterB] display interface mp-group 2/1/1
MP-group2/1/1
Current state: UP
Line protocol state: UP
Description: MP-group2/1/1 Interface
Bandwidth: 1024kbps
Maximum Transmit Unit: 1500
Hold timer: 10 seconds, retry times: 5
Internet Address is 10.1.1.2/24 (primary)
Link layer protocol: PPP
LCP: opened, MP: opened, IPCP: opened, OSICP: opened, MPLSCP: opened, IPv6CP: opened
Physical: MP, baudrate: 1024000 bps
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last link flapping: Never
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

以上信息表明，Router A 与 Router B 的 MP-group 接口都为 UP，可以正常通信。

(3) 检查 Router A 和 Router B 的 MP 的详细信息，验证 MP-group 1 的 MP 配置是否正确。

检查 Router A 的 MP 的详细信息。

```
[RouterA] display ppp mp interface mp-group 2/1/1
Template: MP-group2/1/1
max-bind: 16, fragment: enabled, min-fragment: 128
  Master link: MP-group2/1/1, Active members: 2, Bundle Multilink
  Peer's endPoint descriptor: MP-group2/1/1
  Sequence format: long (rcv)/long (sent)
  Bundle Up Time: 2017/07/25  09:16:07:745
  0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved
  Sequence: 0 (rcv)/0 (sent)
  Active member channels: 16 members
        Serial2/1/1/1:0           Up-Time:2017/07/25  09:16:07:747
        Serial2/1/1/2:0           Up-Time:2017/07/25  09:16:07:746
```

检查 Router B 的 MP 的详细信息。

```
[RouterB] display ppp mp interface mp-group 2/1/1
Template: MP-group2/1/1
max-bind: 16, fragment: enabled, min-fragment: 128
  Master link: MP-group2/1/1, Active members: 2, Bundle Multilink
  Peer's endPoint descriptor: MP-group2/1/1
  Sequence format: long (rcv)/long (sent)
  Bundle Up Time: 2017/07/25  09:16:07:745
  0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved
```

```
  Sequence: 0 (rcv)/0 (sent)
  Active member channels: 16 members
        Serial2/1/1:0              Up-Time:2017/07/25  09:16:07:747
        Serial2/1/2:0              Up-Time:2017/07/25  09:16:07:746
```

以上信息表明，Router A 与 Router B 的 MP-group 1 的 MP 配置正确，可以正常通信。

3.6 配置文件

- Router A：

```
#
controller cpos 2/1/1
 e1 1 unframed
 e1 2 unframed
#
interface mp-group 2/1/1
 ip address 10.1.1.1 24
#
interface serial2/1/1/1:0
 ppp mp mp-group 2/1/1
#
interface serial2/1/1/2:0
 ppp mp mp-group 2/1/1
#
```

- Router B：

```
#
controller e1 2/1/1
 using e1
#
controller e1 2/1/2
 using e1
#
interface mp-group 2/1/1
 ip address 10.1.1.2 24
#
interface serial2/1/1:0
 ppp mp mp-group 2/1/1
#
interface serial2/1/2:0
 ppp mp mp-group 2/1/1
#
```

4 相关资料

- H3C SR6600 SR6600-X 路由器 接口管理配置指导-R7607
- H3C SR6600 SR6600-X 路由器 接口管理配置指导-R7607
- H3C SR6600 SR6600-X 路由器 二层技术-广域网接入配置指导-R7607
- H3C SR6600 SR6600-X 路由器 二层技术-广域网接入命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

EAA 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1

2 配置前提 1

3 EAA Tcl 监控策略典型配置举例 1

3.1 组网需求 1

3.2 使用版本 1

3.3 配置步骤 1

3.3.1 编辑 Tcl 脚本 1

3.3.2 Device 的配置 2

3.4 验证配置 2

3.5 配置文件 4

4 EAA CLI 监控策略典型配置举例 4

4.1 组网需求 4

4.2 使用版本 5

4.3 配置注意事项 5

4.4 配置步骤 5

4.5 验证配置 6

4.6 配置文件 7

5 相关资料 8

1 简介

本文档介绍使用 EAA 的典型配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 EAA 特性，对于同一需求，Tcl 和 CLI 监控策略的实现效果是一致的，用户可以根据习惯选择任意一种策略。

3 EAA Tcl 监控策略典型配置举例

3.1 组网需求

为设备配置 Tcl 监控策略，当检测接口 GigabitEthernet2/0/0 入流量值大于等于 500Mbps 时，执行如下操作：

- 生成流量超范围的日志。
- 显示当前 cpu 状态，并保存至文件。
- 显示接口 GigabitEthernet2/0/0 状态，并保存至文件。

如果后续入流量大于等于 200Mbps 时会再次启动监控，当再次检测到接口入流量大于 500Mbps 时，执行上述操作。

3.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.3 配置步骤

3.3.1 编辑 Tcl 脚本

使用写字板编辑文件 test.tcl，如下：

定义监控事件，监控接口为 GigabitEthernet2/0/0，关注入方向流量，当入流量大于等于 500Mbps 时，执行动作；再次开启轮询的条件为接口流量大于等于 200Mbps。

```
::comware::rtm::event_register interface gigabitethernet2/0/0 monitor-obj rcv-bps start-op ge start-val 500000000 restart-op ge restart-val 200000000 user-role network-admin
```

当监控事件发生时执行动作为：发送优先级为 1、设备号为 local1、信息为 GE2/0/0 input rate exceeded 500000000bps 的日志。

```
::comware::rtm::action syslog priority 1 facility local1 msg "GE2/0/0 input rate exceeded
500000000bps"
```

当监控事件发生时执行动作为：执行 **display cpu-usage** 命令，显示 CPU 利用率的统计信息，并将信息保存在文件 ge0_info.txt 中。

```
display cpu-usage >> ge0_info.txt
```

当监控事件发生时执行动作为：执行 **display interface gigabitethernet 2/0/0** 命令，显示 GigabitEthernet2/0/0 当前的运行状态和相关信息，并将信息保存在文件 ge0_info.txt 中。

```
display interface gigabitethernet2/0/0 >> ge0_info.txt
```

3.3.2 Device 的配置

配置接口 GigabitEthernet2/0/0 的 IP 地址。

```
<Device> system-view
[Device] interface gigabitethernet 2/0/0
[Device-GigabitEthernet2/0/0] ip address 192.168.100.66 255.255.255.0
[Device-GigabitEthernet2/0/0] quit
[Device] quit
```

通过 TFTP 将 test.tcl 下载到设备上。

```
<Device> tftp 192.168.100.14 get test.tcl
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   189  100   189    0     0   7900      0 --:--:-- --:--:-- --:--:-- 12600
```

创建并启用 Tcl 监控策略，并将其和 Tcl 脚本 test.tcl 绑定。

```
<Device> system-view
[Device] rtm tcl-policy test test.tcl
[Device] quit
```

3.4 验证配置

通过 **display rtm policy registered** 命令可以看到存在策略名为 test，策略类型为 Tcl 的策略。

```
<Device> display rtm policy registered
Total number: 1
Type  Event             TimeRegistered       PolicyName
TCL   INTERFACE         Oct 22 14:06:20 2017 test
```

当检测到接口 GigabitEthernet2/0/0 入流量值大于等于 500Mbps 时，查看设备中所有的文件及文件夹信息，存在 ge0_info.txt。

```
<Device> dir
Directory of cfa0:
   0 -rw-        3227 Nov 19 2017 17:28:36   1.cfg
   1 -rw-        2296 Apr 26 2017 18:55:08   5660_data.ak
   2 -rw-        2304 Apr 26 2017 18:54:56   5660_security.ak
   3 -rw-        2298 Apr 26 2017 18:55:16   5660_voice.ak
   4 -rw-        3227 Nov 19 2017 17:15:19   STARTUP110.CFG
   5 drw-           - Mar 10 2017 04:10:10   diagfile
   6 -rw-         567 Jul 17 2017 14:25:00   dsakey
```

```
   7 -rw-         223 Jul 17 2017 14:25:00   ecdsakey
   8 -rw-         278 Jul 17 2017 14:25:00   ge0_info.txt
   9 -rw-         735 Jul 17 2017 14:25:00   hostkey
  10 -rw-         492 Nov 18 2017 16:40:50   ifindex.dat
  11 -rw-         276 Apr 23 2017 19:00:00   lauth.dat
  12 drw-           - Jul 17 2017 11:26:34   license
  13 drw-           - Apr 24 2017 12:39:38   logfile
  14 -rw-    18839552 Nov 14 2017 16:42:12   msr56-cmw710-boot-r000706.bin
  15 -rw-     1150976 Nov 14 2017 16:43:00   msr56-cmw710-data-r000706.bin
  16 -rw-    47470592 Nov 14 2017 16:42:24   msr56-cmw710-system-r000706.bin
  17 -rw-     2975744 Nov 14 2017 16:42:56   msr56-cmw710-voice-r000706.bin
  18 -rw-    70445056 Nov 14 2017 17:41:08   msr56.ipe
  19 -rw-    70445056 Nov 14 2017 16:40:00   msr56NN.ipe
  20 drw-           - Aug 21 2017 16:23:10   pkey
  21 -rw-         189 Nov 19 2017 17:49:34   test.tcl
  22 drw-           - Mar 10 2017 04:10:10   seclog
  23 -rw-         591 Jul 17 2017 14:25:00   serverkey
  24 -rw-        3227 Nov 18 2017 16:40:50   startup.cfg

507492 KB total (298412 KB free)
```

使用 TFTP 方式，将 ge0_info.txt 文件复制到 TFTP 服务器上。

```
<Device> tftp 192.168.100.14 put ge0_info.txt
```

查看 ge0_info.txt 文件，显示包含当前 CPU 和接口 GigabitEthernet2/0/0 状态。

```
Slot 1 CPU 0 CPU usage:
       5% in last 5 seconds
       5% in last 1 minute
       6% in last 5 minutes

Slot 2 CPU 0 CPU usage:
       1% in last 5 seconds
       1% in last 1 minute
       1% in last 5 minutes

GigabitEthernet2/0/0
Current state: UP
Line protocol state: UP
Description: GigabitEthernet2/0/0 Interface
Bandwidth: 1000000kbps
Maximum Transmit Unit: 1500
Internet Address is 192.168.100.66/24 Primary
IP Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 4431-9255-f3fc
IPv6 Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 4431-9255-f3fc
Media type is twisted pair
Port hardware type is 1000_BASE_T
Port priority: 0
1000Mbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
```

```
The Maximum Frame Length is 9216
Last clearing of counters: Never
 Peak value of input: 108106680 bytes/sec, at 2017-10-15 14:14:30
 Peak value of output: 20 bytes/sec, at 2017-10-15 13:24:25
 Last 300 seconds input:  1028465 packets/sec 65821768 bytes/sec 69%
 Last 300 seconds output:  0 packets/sec 9 bytes/sec 0%
 Input (total):  9585460958 packets, 759947089836 bytes
          9585460803 unicasts, 3 broadcasts, 9 multicasts, 0 pauses
 Input (normal):  9585460815 packets, - bytes
          9585460803 unicasts, 3 broadcasts, 9 multicasts, 0 pauses
 Input:  1 input errors, 0 runts, 0 giants, 0 throttles
          1 CRC, 0 frame, - overruns, 0 aborts
          - ignored, - parity errors
 Output (total): 313 packets, 94288 bytes
          0 unicasts, 0 broadcasts, 313 multicasts, 0 pauses
 Output (normal): 313 packets, - bytes
          0 unicasts, 0 broadcasts, 313 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          0 lost carrier, - no carrier
```

3.5 配置文件

- test.tcl 脚本文本：

```
::comware::rtm::event_register interface gigabitethernet2/0/0 monitor-obj rcv-bps start-op ge start-val 500000000 restart-op ge restart-val 200000000 user-role network-admin
::comware::rtm::action syslog priority 1 facility local1 msg "GE2/0/0 input rate exceeded 500000000bps"
display cpu-usage >> ge0_info.txt
display interface gigabitethernet2/0/0 >> ge0_info.txt
```

- Device：

```
#
interface GigabitEthernet2/0/0
 port link-mode route
 ip address 192.168.100.66 255.255.255.0
#
rtm tcl-policy test test.tcl
#
```

4 EAA CLI 监控策略典型配置举例

4.1 组网需求

为设备配置 Tcl 监控策略，当检测接口 GigabitEthernet2/0/0 入流量值大于等于 500Mbps 时，执行如下操作：

- 生成流量超范围的日志。

- 显示当前 cpu 状态，并保存至文件。
- 显示接口 GigabitEthernet2/0/0 状态，并保存至文件。

如果后续入流量大于等于 200Mbps 时会再次启动监控，当再次检测到接口入流量大于 500Mbps 时，执行上述操作。

4.2 使用版本

本举例是在 R7607 上进行配置和验证的。

4.3 配置注意事项

- 同一个策略下，只能配置一个触发事件和运行时间。当多次执行 **event** 或者 **running-time** 命令时，则最近配置并且 **commit** 的生效。
- 如果新配置的动作的编号和已有动作的编号相同，则执行 **commit** 命令后最近配置生效。
- 给 CLI 监控策略配置事件、动作、用户角色和运行时间后，必须执行 **commit** 命令，该策略才会启用，该策略下的配置才会生效。

4.4 配置步骤

配置接口 GigabitEthernet2/0/0 的 IP 地址。

```
<Device> system-view
[Device] interface gigabitethernet 2/0/0
[Device-GigabitEthernet2/0/0] ip address 192.168.100.66 255.255.255.0
[Device-GigabitEthernet2/0/0] quit
```

创建 CLI 策略 1。

```
[Device] rtm cli-policy 1
```

配置监控事件，监控接口为 GigabitEthernet2/0/0，当入流量大于等于 500Mbps 时执行动作；再次开启轮询的条件为接口流量大于等于 200Mbps。

```
[Device-rtm-1] event interface gigabitEthernet 2/0/0 monitor-obj rcv-bps start-op ge
start-val 500000000 restart-op ge restart-val 200000000
```

当事件发生时，发送优先级为 1、日志记录工具为 local1、信息为 GE2/0/0 input rate exceeded 500000000bps 的日志。

```
[Device-rtm-1] action 1 syslog priority 1 facility local1 msg "GE2/0/0 input rate exceeded
500000000bps"
```

当事件发生时，执行 **display cpu-usage** 命令，显示 CPU 利用率的统计信息，并将信息保存在文件 ge0_info.txt 中。

```
[Device-rtm-1] action 2 cli display cpu-usage >> ge0_info.txt
```

当事件发生时，执行 **display interface gigabitetherne 2/0/0** 命令，显示 GigabitEthernet2/0/0 当前的运行状态和相关信息，并将信息保存在文件 ge0_info.txt 中。

```
[Device-rtm-1] action 3 cli display interface gigabitethernet 2/0/0 >> ge0_info.txt
```

配置策略运行时间为 30s。

```
[Device-rtm-1] running-time 30
```

配置执行 CLI 监控策略 1 时使用的用户角色为 network-admin。

```
[Device-rtm-1] user-role network-admin
```

启用 CLI 监控策略 1。

```
[Device-rtm-1] commit
[Device-rtm-1] quit
```

4.5 验证配置

通过 **display rtm policy registered** 命令查看，可以看到策略名为 1，策略类型为 CLI 的策略。

```
<Device> display rtm policy registered
Total number: 1
Type  Event      TimeRegistered        PolicyName
CLI   INTERFACE  May 04 00:12:40 2017  1
```

当检测到接口 GigabitEthernet2/0/0 入流量值大于等于 500Mbps 时，查看设备中所有的文件及文件夹信息，存在 ge0_info.txt。

```
<Device> dir
Directory of cfa0:
   0 -rw-        3227 Nov 19 2017 17:28:36   1.cfg
   1 -rw-        2296 Apr 26 2017 18:55:08   5660_data.ak
   2 -rw-        2304 Apr 26 2017 18:54:56   5660_security.ak
   3 -rw-        2298 Apr 26 2017 18:55:16   5660_voice.ak
   4 -rw-        3227 Nov 19 2017 17:15:19   STARTUP110.CFG
   5 drw-           - Mar 10 2017 04:10:10   diagfile
   6 -rw-         567 Jul 17 2017 14:25:00   dsakey
   7 -rw-         223 Jul 17 2017 14:25:00   ecdsakey
   8 -rw-         278 Jul 17 2017 14:25:00   ge0_info.txt
   9 -rw-         735 Jul 17 2017 14:25:00   hostkey
  10 -rw-         492 Nov 18 2017 16:40:50   ifindex.dat
  11 -rw-         276 Apr 23 2017 19:00:00   lauth.dat
  12 drw-           - Jul 17 2017 11:26:34   license
  13 drw-           - Apr 24 2017 12:39:38   logfile
  14 -rw-    18839552 Nov 14 2017 16:42:12   msr56-cmw710-boot-r000706.bin
  15 -rw-     1150976 Nov 14 2017 16:43:00   msr56-cmw710-data-r000706.bin
  16 -rw-    47470592 Nov 14 2017 16:42:24   msr56-cmw710-system-r000706.bin
  17 -rw-     2975744 Nov 14 2017 16:42:56   msr56-cmw710-voice-r000706.bin
  18 -rw-    70445056 Nov 14 2017 17:41:08   msr56.ipe
  19 -rw-    70445056 Nov 14 2017 16:40:00   msr56NN.ipe
  20 drw-           - Aug 21 2017 16:23:10   pkey
  21 -rw-         189 Nov 19 2017 17:49:34   test.tcl
  22 drw-           - Mar 10 2017 04:10:10   seclog
  23 -rw-         591 Jul 17 2017 14:25:00   serverkey
  24 -rw-        3227 Nov 18 2017 16:40:50   startup.cfg

507492 KB total (298412 KB free)
```

使用 TFTP 方式，将 ge0_info.txt 文件复制到 TFTP 服务器上。

```
<Device> tftp 192.168.100.14 put ge0_info.txt
```

查看 ge0_info.txt 文件，显示包含当前 CPU 和接口 GigabitEthernet2/0/0 状态。

```
Slot 1 CPU 0 CPU usage:
```

```
        5% in last 5 seconds
        5% in last 1 minute
        6% in last 5 minutes

Slot 2 CPU 0 CPU usage:
        1% in last 5 seconds
        1% in last 1 minute
        1% in last 5 minutes

GigabitEthernet2/0/0
Current state: UP
Line protocol state: UP
Description: GigabitEthernet2/0/0 Interface
Bandwidth: 1000000kbps
Maximum Transmit Unit: 1500
Internet Address is 192.168.100.66/24 Primary
IP Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 4431-9255-f3fc
IPv6 Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 4431-9255-f3fc
Media type is twisted pair
Port hardware type is 1000_BASE_T
Port priority: 0
1000Mbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
The Maximum Frame Length is 9216
Last clearing of counters: Never
 Peak value of input: 108106680 bytes/sec, at 2017-10-15 14:14:30
 Peak value of output: 20 bytes/sec, at 2017-10-15 13:24:25
 Last 300 seconds input:  1028465 packets/sec 65821768 bytes/sec 69%
 Last 300 seconds output:  0 packets/sec 9 bytes/sec 0%
 Input (total):  9585460958 packets, 759947089836 bytes
          9585460803 unicasts, 3 broadcasts, 9 multicasts, 0 pauses
 Input (normal):  9585460815 packets, - bytes
          9585460803 unicasts, 3 broadcasts, 9 multicasts, 0 pauses
 Input:  1 input errors, 0 runts, 0 giants, 0 throttles
          1 CRC, 0 frame, - overruns, 0 aborts
          - ignored, - parity errors
 Output (total): 313 packets, 94288 bytes
          0 unicasts, 0 broadcasts, 313 multicasts, 0 pauses
 Output (normal): 313 packets, - bytes
          0 unicasts, 0 broadcasts, 313 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          0 lost carrier, - no carrier
```

4.6 配置文件

```
#
```

```
interface GigabitEthernet2/0/0
 port link-mode route
 ip address 192.168.100.66 255.255.255.0
#
rtm cli-policy 1
 event interface GigabitEthernet2/0/0 monitor-obj rcv-bps start-op ge start-val 500000000
restart-op ge restart-val 200000000
 action 1 syslog priority 1 facility local1 msg "GE2/0/0 input rate exceeded 500000000bps"
 action 2 cli display cpu-usage >> ge0_info.txt
 action 3 cli display interface gigabitethernet 2/0/0 >> ge0_info.txt
 running-time 30
 user-role network-admin
#
```

5 相关资料

- H3C SR6600 SR6600-X 路由器 网络管理和监控配置指导-R7607
- H3C SR6600 SR6600-X 路由器 网络管理和监控命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

GRE 和 OSPF 结合使用配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 配置举例 1
3.1 组网需求 1
3.2 使用版本 2
3.3 配置步骤 2
3.3.1 配置准备 2
3.3.2 配置 Device A 2
3.3.3 配置 Device B 3
3.3.4 配置 Device C 3
3.4 验证配置 4
3.5 配置文件 5
4 相关资料 6

1 简介

本文档介绍了 GRE 隧道和 OSPF 相结合使用的典型配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文假设您已了解 GRE 隧道和 OSPF 的相关特性。

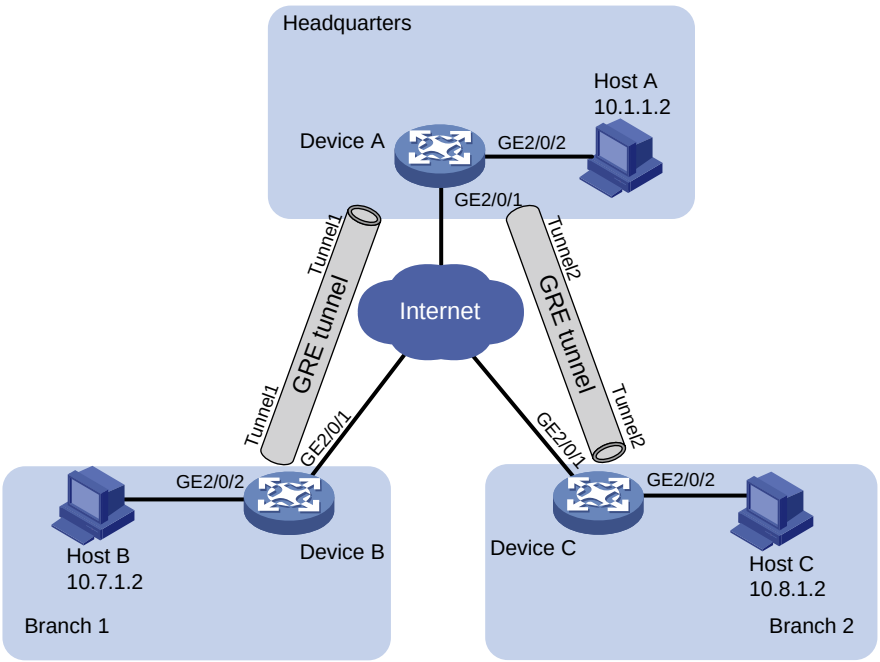
3 配置举例

3.1 组网需求

如图 1 所示，Device A 为某机构总部网关，Device B 和 Device C 为分支网关，运营商为各网关分配了公网 IP 地址，并保证网关之间可以通信，要求：

- 总部和分支之间建立 GRE 隧道，通过隧道使各总部、分支机构可以实现互访；
- 配置 OSPF 协议使网关上存在通过 Tunnel 接口到达目的地址的路由表项。

图1 GRE 和 OSPF 结合使用典型配置举例组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	GE2/0/1	191.2.1.1/24	Device B	GE2/0/1	191.3.1.1/24
	GE2/0/2	10.1.1.1/24		GE2/0/2	10.7.1.1/24
	Tunnel 1	10.5.1.1/24		Tunnel 1	10.5.1.2/24
	Tunnel 2	10.6.1.1/24			

设备	接口	IP地址	设备	接口	IP地址
Device C	GE2/0/1	191.4.1.1/24			
	GE2/0/2	10.8.1.1/24			
	Tunnel 2	10.6.1.2/24			

3.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.3 配置步骤

3.3.1 配置准备

配置网关设备之间的 IPv4 路由协议，确保设备之间 IPv4 报文能够正常交互，具体配置过程略。

3.3.2 配置 Device A

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 191.2.1.1 255.255.255.0
[DeviceA-GigabitEthernet2/0/1] quit
```

请参考以上方法配置上图中 Device A 其它接口的 IP 地址，配置步骤这里省略。

创建 Tunnel1 接口，并指定隧道模式为 GRE over IPv4 隧道。

```
[DeviceA] interface tunnel 1 mode gre
```

配置 Tunnel1 接口的 IP 地址。

```
[DeviceA-Tunnel1] ip address 10.5.1.1 24
```

配置 Tunnel1 接口的源接口为 GigabitEthernet 2/0/1。

```
[DeviceA-Tunnel1] source GigabitEthernet 2/0/1
```

配置 Tunnel1 接口的目的端地址。

```
[DeviceA-Tunnel1] destination 191.3.1.1
[DeviceA-Tunnel1] quit
```

创建 Tunnel2 接口，并指定隧道模式为 GRE over IPv4 隧道。

```
[DeviceA] interface tunnel 2 mode gre
```

配置 Tunnel2 接口的 IP 地址。

```
[DeviceA-Tunnel2] ip address 10.6.1.1 24
```

配置 Tunnel2 接口的源接口为 GigabitEthernet 2/0/1。

```
[DeviceA-Tunnel2] source GigabitEthernet 2/0/1
```

配置 Tunnel2 接口的目的端地址。

```
[DeviceA-Tunnel2] destination 191.4.1.1
[DeviceA-Tunnel2] quit
```

启动 OSPF，并配置其 Router ID 为 10.6.1.1。

```
[DeviceA] router id 10.6.1.1
[DeviceA] ospf 1
[DeviceA-ospf-1] area 0
```

```
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 10.5.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 10.6.1.0 0.0.0.255
```

3.3.3 配置 Device B

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] ip address 191.3.1.1 255.255.255.0
[DeviceB-GigabitEthernet2/0/1] quit
```

请参考以上方法配置上图中 Device B 其它接口的 IP 地址，配置步骤这里省略。

创建 Tunnel1 接口，并指定隧道模式为 GRE over IPv4 隧道。

```
[DeviceB] interface tunnel 1 mode gre
```

配置 Tunnel1 接口的 IP 地址。

```
[DeviceB-Tunnel1] ip address 10.5.1.2 24
```

配置 Tunnel1 接口的源接口为 GigabitEthernet 2/0/1。

```
[DeviceB-Tunnel1] source GigabitEthernet 2/0/1
```

配置 Tunnel1 接口的目的端地址。

```
[DeviceB-Tunnel1] destination 191.2.1.1
[DeviceB-Tunnel1] quit
```

启动 OSPF，并配置其 Router ID 为 10.7.1.1。

```
[DeviceB] router id 10.7.1.1
[DeviceB] ospf 1
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 10.7.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 10.5.1.0 0.0.0.255
```

3.3.4 配置 Device C

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<DeviceC> system-view
[DeviceC] interface gigabitethernet 2/0/1
[DeviceC-GigabitEthernet2/0/1] ip address 191.4.1.1 255.255.255.0
[DeviceC-GigabitEthernet2/0/1] quit
```

请参考以上方法配置上图中 Device C 其它接口的 IP 地址，配置步骤这里省略。

创建 Tunnel2 接口，并指定隧道模式为 GRE over IPv4 隧道。

```
[DeviceC] interface tunnel 2 mode gre
```

配置 Tunnel2 接口的 IP 地址。

```
[DeviceC-Tunnel2] ip address 10.6.1.2 24
```

配置 Tunnel1 接口的源接口为 GigabitEthernet 2/0/1。

```
[DeviceC-Tunnel2] source GigabitEthernet 2/0/1
```

配置 Tunnel2 接口的目的端地址。

```
[DeviceC-Tunnel2] destination 191.2.1.1
[DeviceC-Tunnel2] quit
```

启动 OSPF，并配置其 Router ID 为 10.8.1.1。

```
[DeviceC] router id 10.8.1.1
[DeviceC] ospf 1
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] network 10.8.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 10.6.1.0 0.0.0.255
```

3.4 验证配置

(1) 从 Host A 可以 ping 通 Host B。

```
C:\> ping 10.7.1.2

Pinging 10.7.1.2 with 32 bytes of data:

Reply from 10.7.1.2: bytes=32 time=19ms TTL=253
Reply from 10.7.1.2: bytes=32 time<1ms TTL=253
Reply from 10.7.1.2: bytes=32 time<1ms TTL=253
Reply from 10.7.1.2: bytes=32 time<1ms TTL=253

Ping statistics for 10.7.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 （0% loss），
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 19ms, Average = 4ms
```

(2) 从 Host A 可以 ping 通 Host C。

```
C:\> ping 10.8.1.2

Pinging 10.8.1.2 with 32 bytes of data:

Reply from 10.8.1.2: bytes=32 time=18ms TTL=253
Reply from 10.8.1.2: bytes=32 time<1ms TTL=253
Reply from 10.8.1.2: bytes=32 time<1ms TTL=253
Reply from 10.8.1.2: bytes=32 time<1ms TTL=253

Ping statistics for 10.8.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 （0% loss），
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 19ms, Average = 4ms
```

(3) 从 Host B 可以 ping 通 Host C。

```
C:\> ping 10.8.1.2

Pinging 10.8.1.2 with 32 bytes of data:

Reply from 10.8.1.2: bytes=32 time=20ms TTL=251
Reply from 10.8.1.2: bytes=32 time<1ms TTL=251
Reply from 10.8.1.2: bytes=32 time<1ms TTL=251
Reply from 10.8.1.2: bytes=32 time<1ms TTL=251
```

```
Ping statistics for 10.8.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 （0% loss），
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 19ms, Average = 4ms
```

3.5 配置文件

- Device A

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 191.2.1.1 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
#
interface Tunnel1 mode gre
 source GigabitEthernet2/0/1
 destination 191.3.1.1
 ip address 10.5.1.1 255.255.255.0
#
interface Tunnel2 mode gre
 source GigabitEthernet2/0/1
 destination 191.4.1.1
 ip address 10.6.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 10.5.1.0 0.0.0.255
network 10.6.1.0 0.0.0.255
#
```

- Device B

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 191.3.1.1 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.7.1.1 255.255.255.0
#
interface Tunnel1 mode gre
 source GigabitEthernet2/0/1
 destination 191.2.1.1
 ip address 10.5.1.2 255.255.255.0
```

```
#
ospf 1
 area 0.0.0.0
network 10.7.1.0 0.0.0.255
network 10.5.1.0 0.0.0.255
#
```

- Device C

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 191.4.1.1 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.8.1.1 255.255.255.0
#
interface Tunnel2 mode gre
 source GigabitEthernet2/0/1
 destination 191.2.1.1
 ip address 10.6.1.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
network 10.8.1.0 0.0.0.255
network 10.6.1.0 0.0.0.255
#
```

4 相关资料

- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由配置指导-R7607
- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由命令参考-R7607
- H3C SR6600 SR6600-X 路由器 三层技术-IP 业务配置指导-R7607
- H3C SR6600 SR6600-X 路由器 三层技术-IP 业务命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

HoVPN 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 配置举例 2
3.1 组网需求 2
3.2 配置思路 2
3.3 使用版本 2
3.4 配置注意事项 2
3.5 配置步骤 3
3.6 验证配置 9
3.7 配置文件 10
4 相关资料 15

1 简介

本文档介绍 MPLS HoVPN 的典型配置举例。

在 MPLS L3VPN 网络中，PE 设备起到了最为关键的作用，不仅需要负责 VPN 用户的接入，同时也负责 VPN 路由的管理和维护，以及私网报文的转发工作。这就对 PE 设备的性能有了非常高的要求，从而导致网络的扩展性受到限制。

HoVPN（Hierarchy of VPN，分层 VPN）将 PE 设备的功能分布到多台设备，多台设备承担不同的角色，并形成层次结构，共同完成一个 PE 的功能。HoVPN 对不同角色的设备的性能要求也不相同，从而使网络具备了良好的可扩展性。

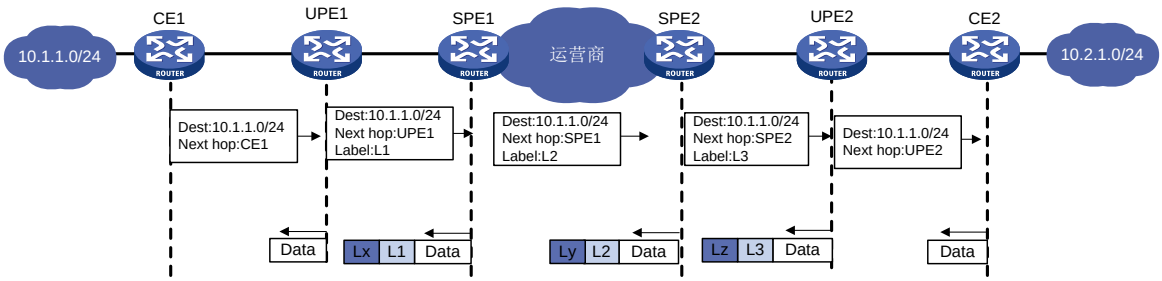
在 HoVPN 组网下，直接连结用户的设备称为 UPE（Underlayer PE or User-end PE，下层 PE 或用户侧 PE）；连结 UPE 并位于网络内部的设备称为 SPE（Superstratum PE or Service Provider-end PE，上层 PE 或运营商侧 PE）。UPE 与 SPE 构成分层式 PE，共同完成传统上一个 PE 的功能。

SPE 与 UPE 的分工是：

- UPE 主要完成用户接入功能。UPE 维护其直接相连的 VPN Site 的路由，但不维护 VPN 中其它远程 Site 的路由或仅维护它们的聚合路由；UPE 为其直接相连的 Site 的路由分配内层标签，并通过 MP-BGP 随 VPN 路由发布此标签给 SPE。
- SPE 主要完成 VPN 路由的管理和发布。SPE 维护其通过 UPE 连接的 VPN 所有路由，包括本地和远程 Site 的路由，SPE 将路由信息发布给 UPE，并携带标签。SPE 发布的路由信息可以是 VPN 实例的缺省路由（或聚合路由），也可以是通过路由策略的路由信息。通过后者可以实现对同一 VPN 下不同站点之间互访的控制。

如图 1 所示，UPE 与连接用户的 CE 设备相连，并与运营商内部的 SPE 设备相连，图中为路由和标签交换过程，其中，Lx 和 Lz 为 UPE 与 SPE 之间的公网的标签，Ly 为运营商骨干网的公网的标签。

图1 HoVPN 组网路由和标签交换图



2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 HoVPN 特性。

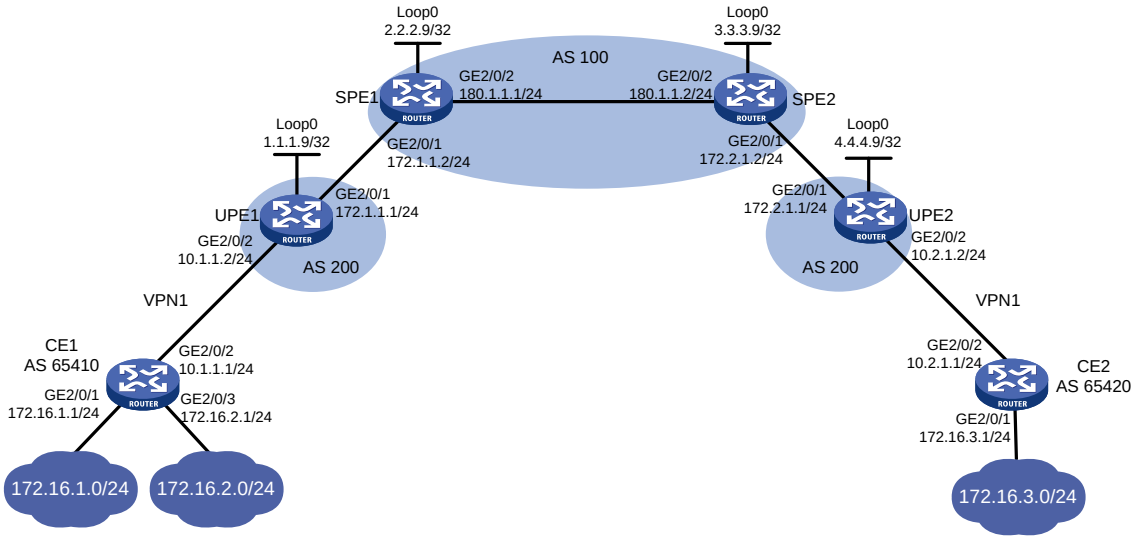
3 配置举例

3.1 组网需求

如图 2 所示，SPE 设备处于 AS100 中，UPE 设备处于 AS200 中，SPE 为运营商骨干网设备，UPE 为连接用户端 CE 的设备。UPE1 和 UPE2 分别连接属于 VPN1 的 CE1 和 CE2。CE1 连接两个网段，分别为：172.16.1.0/24 和 172.16.2.0/24；CE2 下连 172.16.3.0/24 网段。

现要求在用户网络中部署 HoVPN 服务，并通过配置路由策略，限制不同 CE 下连网段之间的互相访问权限，使得 CE1 的 172.16.1.0/24 和 CE2 的 172.16.3.0/24 可以相互访问，CE1 的 172.16.2.0/24 和 CE2 的 172.16.3.0/24 不能相互访问。

图2 HoVPN 典型配置举例组网图



3.2 配置思路

此案例配置主要分为两部分：

- 在网络中配置 HoVPN 服务。
- 在 SPE 设备上配置路由策略，使得 SPE2 仅发布 CE1 的私网路由 172.16.1.0/24 给 UPE2。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置注意事项

- 只有在 SPE 设备上配置了路由策略，并允许向 UPE 设备发布路由时，SPE 设备才会向 UPE 设备发布路由，即，在 HoVPN 组网中，路由策略为必选配置。

- 配置 SPE 与 UPE 之间建立 EBGP 对等体并发布标签时，仅使能与对等体交换标签的能力并不能进行标签的发布，还需配置路由策略才可为对等体发布标签。
- 由于在配置接口与 VPN 实例绑定后，接口上的 IP 地址等配置会清除，因此先配置接口与 VPN 实例的绑定关系，再进行其他配置。

3.5 配置步骤

1. 在 SPE 设备上使能 MPLS 和 MPLS LDP 功能，并配置 OSPF 作为 IGP 协议

(1) 配置 SPE1

配置 MPLS 基本能力和 MPLS LDP 能力，建立 LDP LSP。

```
<SPE1> system-view
[SPE1] interface loopback 0
[SPE1-LoopBack0] ip address 2.2.2.9 32
[SPE1-LoopBack0] quit
[SPE1] mpls lsr-id 2.2.2.9
[SPE1] mpls ldp
[SPE1-ldp] quit
[SPE1] interface gigabitethernet2/0/1
[SPE1-GigabitEthernet2/0/1] ip address 172.1.1.2 24
[SPE1-GigabitEthernet2/0/1] mpls enable
[SPE1-GigabitEthernet2/0/1] quit
[SPE1] interface gigabitethernet2/0/2
[SPE1-GigabitEthernet2/0/2] ip address 180.1.1.1 24
[SPE1-GigabitEthernet2/0/2] mpls enable
[SPE1-GigabitEthernet2/0/2] mpls ldp enable
[SPE1-GigabitEthernet2/0/2] quit
```

配置 OSPF 作为 IGP 协议。

```
[SPE1] ospf
[SPE1-ospf-1] area 0
[SPE1-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[SPE1-ospf-1-area-0.0.0.0] network 180.1.1.0 0.0.0.255
[SPE1-ospf-1-area-0.0.0.0] quit
[SPE1-ospf-1] quit
```

(2) 配置 SPE2

配置 MPLS 基本能力和 MPLS LDP 能力，建立 LDP LSP。

```
<SPE2> system-view
[SPE2] interface loopback 0
[SPE2-LoopBack0] ip address 3.3.3.9 32
[SPE2-LoopBack0] quit
[SPE2] mpls lsr-id 3.3.3.9
[SPE2] mpls ldp
[SPE2-ldp] quit
[SPE2] interface gigabitethernet2/0/2
[SPE2-GigabitEthernet2/0/2] ip address 180.1.1.2 24
[SPE2-GigabitEthernet2/0/2] mpls enable
[SPE2-GigabitEthernet2/0/2] mpls ldp enable
```

```
[SPE2-GigabitEthernet2/0/2] quit
[SPE2] interface gigabitethernet2/0/1
[SPE2-GigabitEthernet2/0/1] ip address 172.2.1.2 24
[SPE2-GigabitEthernet2/0/1] mpls enable
[SPE2-GigabitEthernet2/0/1] quit
```

配置 OSPF 作为 IGP 协议。

```
[SPE2] ospf
[SPE2-ospf-1] area 0
[SPE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[SPE2-ospf-1-area-0.0.0.0] network 180.1.1.0 0.0.0.255
[SPE2-ospf-1-area-0.0.0.0] quit
[SPE2-ospf-1] quit
```

配置完成后，在 SPE 设备上执行 **display mpls ldp peer** 命令可以看到 LDP 会话建立成功，LDP 会话状态为 Operational；执行 **display ospf peer** 命令可以看到 OSPF 邻居关系已建立，状态为 FULL。

2. 配置 SPE 之间建立 MP-IBGP 对等体，交换 VPNv4 路由

配置 SPE 1 与 SPE 2 建立 MP-IBGP 对等体，交换 VPNv4 路由。

```
[SPE1] bgp 100
[SPE1-bgp] peer 3.3.3.9 as-number 100
[SPE1-bgp] peer 3.3.3.9 connect-interface loopback 0
[SPE1-bgp] address-family vpnv4
[SPE1-bgp-vpnv4] peer 3.3.3.9 enable
[SPE1-bgp-vpnv4] quit
[SPE1-bgp] quit
```

配置 SPE 2 与 SPE 1 建立 MP-IBGP 对等体，交换 VPNv4 路由。

```
[SPE2] bgp 100
[SPE2-bgp] peer 2.2.2.9 as-number 100
[SPE2-bgp] peer 2.2.2.9 connect-interface loopback 0
[SPE2-bgp] address-family vpnv4
[SPE2-bgp-vpnv4] peer 2.2.2.9 enable
[SPE2-bgp-vpnv4] quit
[SPE2-bgp] quit
```

配置完成后，在 SPE1 和 SPE2 上执行 **display bgp peer vpnv4** 命令可以看到 BGP 对等体关系已建立，并达到 Established 状态。

3. 在 UPE 设备上使能 MPLS 功能

(1) 配置 UPE1

配置 MPLS 基本能力。

```
<UPE1> system-view
[UPE1] interface loopback 0
[UPE1-LoopBack0] ip address 1.1.1.9 32
[UPE1-LoopBack0] quit
[UPE1] mpls lsr-id 1.1.1.9
[UPE1] interface gigabitethernet2/0/1
[UPE1-GigabitEthernet2/0/1] ip address 172.1.1.1 24
[UPE1-GigabitEthernet2/0/1] mpls enable
```

```
[UPE1-GigabitEthernet2/0/1] quit
```

(2) 配置 UPE2

配置 MPLS 基本能力。

```
<UPE2> system-view
[UPE2] interface loopback 0
[UPE2-Loopback0] ip address 4.4.4.9 32
[UPE2-Loopback0] quit
[UPE2] mpls lsr-id 4.4.4.9
[UPE2] interface gigabitethernet2/0/1
[UPE2-GigabitEthernet2/0/1] ip address 172.2.1.1 24
[UPE2-GigabitEthernet2/0/1] mpls enable
[UPE2-GigabitEthernet2/0/1] quit
```

4. 配置 SPE 与 UPE 建立 EBGP 对等体，并交换带标签的路由，建立 BGP LSP

(1) 配置 SPE1

```
[SPE1] bgp 100
[SPE1-bgp] peer 172.1.1.1 as-number 200
[SPE1-bgp] address-family ipv4
[SPE1-bgp-ipv4] peer 172.1.1.1 enable
[SPE1-bgp-ipv4] peer 172.1.1.1 label-route-capability
[SPE1-bgp-ipv4] peer 172.1.1.1 route-policy policy1 export
[SPE1-bgp-ipv4] network 2.2.2.9 255.255.255.255
[SPE1-bgp-ipv4] quit
[SPE1-bgp] quit
```

配置路由策略，为路由分配标签。

```
[SPE1] route-policy policy1 permit node 0
[SPE1-route-policy-policy1-0] apply mpls-label
[SPE1-route-policy-policy1-0] quit
```

(2) 配置 UPE1

```
[UPE1] bgp 200
[UPE1-bgp] peer 172.1.1.2 as-number 100
[UPE1-bgp] address-family ipv4
[UPE1-bgp-ipv4] peer 172.1.1.2 enable
[UPE1-bgp-ipv4] peer 172.1.1.2 label-route-capability
[UPE1-bgp-ipv4] peer 172.1.1.2 route-policy policy1 export
[UPE1-bgp-ipv4] network 1.1.1.9 255.255.255.255
[UPE1-bgp-ipv4] quit
[UPE1-bgp] quit
```

配置路由策略，为路由分配标签。

```
[UPE1] route-policy policy1 permit node 0
[UPE1-route-policy-policy1-0] apply mpls-label
[UPE1-route-policy-policy1-0] quit
```

(3) 配置 SPE2

```
[SPE2] bgp 100
[SPE2-bgp] peer 172.2.1.1 as-number 200
[SPE2-bgp] address-family ipv4
[SPE2-bgp-ipv4] peer 172.2.1.1 enable
```

```
[SPE2-bgp-ipv4] peer 172.2.1.1 label-route-capability
[SPE2-bgp-ipv4] peer 172.2.1.1 route-policy policy1 export
[SPE2-bgp-ipv4] network 3.3.3.9 255.255.255.255
[SPE2-bgp-ipv4] quit
[SPE2-bgp] quit
[SPE2] route-policy policy1 permit node 0
[SPE2-route-policy-policy1-0] apply mpls-label
[SPE2-route-policy-policy1-0] quit
```

(4) 配置 UPE2

```
[UPE2] bgp 200
[UPE2-bgp] peer 172.2.1.2 as-number 100
[UPE2-bgp] address-family ipv4
[UPE2-bgp-ipv4] peer 172.2.1.2 enable
[UPE2-bgp-ipv4] peer 172.2.1.2 label-route-capability
[UPE2-bgp-ipv4] peer 172.2.1.2 route-policy policy1 export
[UPE2-bgp-ipv4] network 4.4.4.9 255.255.255.255
[UPE2-bgp-ipv4] quit
[UPE2-bgp] quit
# 配置路由策略，为路由分配标签。
[UPE2] route-policy policy1 permit node 0
[UPE2-route-policy-policy1-0] apply mpls-label
[UPE2-route-policy-policy1-0] quit
```

配置完成后，在各设备上执行 **display mpls lsp** 命令可以看到已在 SPE 与 UPE 之间建立 BGP LSP。

5. 配置 SPE 与 UPE 建立 MP-EBGP 对等体，使能 HoVPN 服务

(1) 配置 UPE1

配置 UPE 1 与 SPE 1 建立 MP-EBGP 对等体。

```
[UPE1] bgp 200
[UPE1-bgp] peer 2.2.2.9 as-number 100
[UPE1-bgp] peer 2.2.2.9 connect-interface loopback 0
[UPE1-bgp] address-family vpnv4
[UPE1-bgp-vpnv4] peer 2.2.2.9 enable
```

配置 UPE1 接受 AS_PATH 属性中已包含本地 AS 号的路由，以接收位于相同 AS 的 UPE2 的路由。

```
[UPE1-bgp-vpnv4] peer 2.2.2.9 allow-as-loop
[UPE1-bgp-vpnv4] quit
```

(2) 配置 SPE1

配置 VPN 实例 vpn1。

```
[SPE1] ip vpn-instance vpn1
[SPE1-vpn-instance-vpn1] route-distinguisher 100:1
[SPE1-vpn-instance-vpn1] vpn-target 100:1 both
[SPE1-vpn-instance-vpn1] quit
```

配置 SPE 1 与 UPE 1 建立 MP-EBGP 对等体，指定 UPE 1，并引入 VPN 路由。

```
[SPE1] bgp 100
[SPE1-bgp] peer 1.1.1.9 as-number 200
```

```
[SPE1-bgp] peer 1.1.1.9 connect-interface loopback 0
[SPE1-bgp] address-family vpnv4
[SPE1-bgp-vpnv4] peer 1.1.1.9 enable
[SPE1-bgp-vpnv4] peer 1.1.1.9 upe
[SPE1-bgp-vpnv4] quit
[SPE1-bgp] ip vpn-instance vpn1
[SPE1-bgp-vpn1] quit
[SPE1-bgp] quit
```

(3) 配置 UPE2

配置 UPE 2 与 SPE 2 建立 MP-EBGP 对等体。

```
[UPE2] bgp 200
[UPE2-bgp] peer 3.3.3.9 as-number 100
[UPE2-bgp] peer 3.3.3.9 connect-interface loopback 0
[UPE2-bgp] address-family vpnv4
[UPE2-bgp-vpnv4] peer 3.3.3.9 enable
```

配置 UPE2 接受 AS_PATH 属性中已包含本地 AS 号的路由，以接收位于相同 AS 的 UPE2 的路由。

```
[UPE2-bgp-vpnv4] peer 3.3.3.9 allow-as-loop
[UPE2-bgp-vpnv4] quit
```

(4) 配置 SPE2

配置 VPN 实例 vpn1。

```
[SPE2] ip vpn-instance vpn1
[SPE2-vpn-instance-vpn1] route-distinguisher 100:1
[SPE2-vpn-instance-vpn1] vpn-target 100:1 both
[SPE2-vpn-instance-vpn1] quit
```

配置 SPE 2 与 UPE 2 建立 MP-EBGP 对等体，指定 UPE 2，并引入 VPN 路由。

```
[SPE2] bgp 100
[SPE2-bgp] peer 4.4.4.9 as-number 200
[SPE2-bgp] peer 4.4.4.9 connect-interface loopback 0
[SPE2-bgp] address-family vpnv4
[SPE2-bgp-vpnv4] peer 4.4.4.9 enable
[SPE2-bgp-vpnv4] peer 4.4.4.9 upe
[SPE2-bgp-vpnv4] quit
[SPE2-bgp] ip vpn-instance vpn1
[SPE2-bgp-vpn1] quit
[SPE2-bgp] quit
```

配置完成后，在 SPE 和 UPE 设备上执行 **`display bgp peer vpnv4`** 命令可以看到相互之间的 BGP 对等体关系已建立，并达到 Established 状态。

6. 配置 UPE 接入 CE

(1) 配置 UPE1

配置 VPN 实例 vpn1，将 CE 1 接入 UPE 1。

```
[UPE1] ip vpn-instance vpn1
[UPE1-vpn-instance-vpn1] route-distinguisher 100:1
[UPE1-vpn-instance-vpn1] vpn-target 100:1 both
[UPE1-vpn-instance-vpn1] quit
```

```
[UPE1] interface gigabitethernet2/0/2
[UPE1-Gigabitethernet2/0/2] ip binding vpn-instance vpn1
[UPE1-Gigabitethernet2/0/2] ip address 10.1.1.2 24
[UPE1-Gigabitethernet2/0/2] quit
```

配置 UPE 1 与 CE 1 建立 EBGP 对等体，并引入 VPN 路由。

```
[UPE1] bgp 200
[UPE1-bgp] ip vpn-instance vpn1
[UPE1-bgp-vpn1] peer 10.1.1.1 as-number 65410
[UPE1-bgp-vpn1] address-family ipv4 unicast
[UPE1-bgp-ipv4-vpn1] peer 10.1.1.1 enable
[UPE1-bgp-ipv4-vpn1] import-route direct
[UPE1-bgp-ipv4-vpn1] quit
[UPE1-bgp-vpn1] quit
```

(2) 配置 CE1

配置 CE1 与 UPE1 建立 EBGP 对等体，并引入直连路由。

```
<CE1> system-view
[CE1] interface gigabitethernet2/0/2
[CE1-GigabitEthernet2/0/2] ip address 10.1.1.1 255.255.255.0
[CE1-GigabitEthernet2/0/2] quit
[CE1] bgp 65410
[CE1-bgp] peer 10.1.1.2 as-number 200
[CE1-bgp] address-family ipv4 unicast
[CE1-bgp-ipv4] peer 10.1.1.2 enable
[CE1-bgp-ipv4] import-route direct
[CE1-bgp-ipv4] quit
[CE1-bgp] quit
```

(3) 配置 UPE2

配置 VPN 实例 vpn1，将 CE 2 接入 UPE 2。

```
[UPE2] ip vpn-instance vpn1
[UPE2-vpn-instance-vpn1] route-distinguisher 100:1
[UPE2-vpn-instance-vpn1] vpn-target 100:1 both
[UPE2-vpn-instance-vpn1] quit
[UPE2] interface gigabitethernet2/0/2
[UPE2-GigabitEthernet2/0/2] ip binding vpn-instance vpn1
[UPE2-GigabitEthernet2/0/2] ip address 10.2.1.2 24
[UPE2-GigabitEthernet2/0/2] quit
```

配置 UPE 2 与 CE 2 建立 EBGP 对等体，并引入 VPN 路由。

```
[UPE2] bgp 200
[UPE2-bgp] ip vpn-instance vpn1
[UPE2-bgp-vpn1] peer 10.2.1.1 as-number 65420
[UPE2-bgp-vpn1] address-family ipv4 unicast
[UPE2-bgp-ipv4-vpn1] peer 10.2.1.1 enable
[UPE2-bgp-ipv4-vpn1] import-route direct
[UPE2-bgp-ipv4-vpn1] quit
[UPE2-bgp-vpn1] quit
```

(4) 配置 CE2

配置 CE2 与 UPE2 建立 EBGP 对等体，并引入直连路由。

```
<CE2> system-view
[CE2] interface gigabitethernet2/0/2
[CE2-GigabitEthernet2/0/2] ip address 10.2.1.1 255.255.255.0
[CE2-GigabitEthernet2/0/2] quit
[CE2] bgp 65420
[CE2-bgp] peer 10.2.1.2 as-number 200
[CE2-bgp] address-family ipv4 unicast
[CE2-bgp-ipv4] peer 10.2.1.2 enable
[CE2-bgp-ipv4] import-route direct
[CE2-bgp-ipv4] quit
[CE2-bgp] quit
```

配置完成后，在 UPE 和 CE 设备上执行 **display bgp peer ipv4** 命令可以看到相互之间的 BGP 对等体关系已建立，并达到 Established 状态。

7. 在 SPE 设备上配置路由策略，控制 VPN 之间路由的传播

(1) 配置 SPE1

配置 SPE 1 向 UPE 1 发送通过策略的路由信息，允许 CE 2 的路由发送给 UPE 1。

```
[SPE1] ip prefix-list list1 index 10 permit 172.16.3.0 24
[SPE1] route-policy policy2 permit node 0
[SPE1-route-policy-policy2-0] if-match ip address prefix-list list1
[SPE1-route-policy-policy2-0] quit
[SPE1] bgp 100
[SPE1-bgp] address-family vpnv4
[SPE1-bgp-vpnv4] peer 1.1.1.9 upe route-policy policy2 export
```

(2) 配置 SPE2

配置 SPE 2 向 UPE 2 发送通过策略的路由信息，允许 CE 1 的私网路由 172.16.1.0/24 发送给 UPE 2。

```
[SPE2] ip prefix-list list1 index 10 permit 172.16.1.0 24
[SPE2] route-policy policy2 permit node 0
[SPE2-route-policy-policy2-0] if-match ip address prefix-list list1
[SPE2-route-policy-policy2-0] quit
[SPE2] bgp 100
[SPE2-bgp] address-family vpnv4
[SPE2-bgp-vpnv4] peer 4.4.4.9 upe route-policy policy2 export
```

3.6 验证配置

配置完成后，可以看到 CE1 已经学习到 CE2 下连网段 172.16.3.0/24，如下：

```
[CE1] display ip routing-table

Destinations : 25        Routes : 25

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
172.16.1.0/24       Direct 0    0            172.16.1.1      GE2/0/1
172.16.1.0/32       Direct 0    0            172.16.1.1      GE2/0/1
172.16.1.1/32       Direct 0    0            127.0.0.1       InLoop0
```

```
172.16.1.255/32     Direct 0    0           172.16.1.1      GE2/0/1
172.16.2.0/24       Direct 0    0           172.16.2.1      GE2/0/3
172.16.2.0/32       Direct 0    0           172.16.2.1      GE2/0/3
172.16.2.1/32       Direct 0    0           127.0.0.1       InLoop0
172.16.2.255/32     Direct 0    0           172.16.2.1      GE2/0/3
172.16.3.0/24       BGP    255  0           10.1.1.2        GE2/0/2
```

CE2 已经学习到 CE1 的下连网段 172.16.1.0/24，但并未学习到 CE1 的下连网段 172.16.2.0/24。如下：

```
<CE2> display ip routing-table

Destinations : 21        Routes : 21

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
172.16.1.0/24       BGP    255  0            10.2.1.2        GE2/0/2
172.16.3.0/24       Direct 0    0           172.16.3.1      GE2/0/1
172.16.3.0/32       Direct 0    0           172.16.3.1      GE2/0/1
172.16.3.1/32       Direct 0    0           127.0.0.1       InLoop0
172.16.3.255/32     Direct 0    0           172.16.3.1      GE2/0/1
```

CE1 的下连网段 172.16.1.0/24 可与 CE2 的下连网段 172.16.3.0/24 互通；CE1 的下连网段 172.16.2.0/24 不能与 CE2 的下连网段 172.16.3.0/24 互通。

3.7 配置文件

- CE1：

```
#
 interface GigabitEthernet2/0/1
 ip address 172.16.1.1 255.255.255.0
#
 interface GigabitEthernet2/0/2
 ip address 10.1.1.1 255.255.255.0
#
 interface GigabitEthernet2/0/1
 ip address 172.16.2.1 255.255.255.0
#
 bgp 65410
 peer 10.1.1.2 as-number 200
#
 address-family ipv4 unicast
 import-route direct
 peer 10.1.1.2 enable
#
```

- CE2：

```
#
 interface GigabitEthernet2/0/1
 ip address 172.16.3.1 255.255.255.0
#
 interface GigabitEthernet2/0/2
```

```
 ip address 10.2.1.1 255.255.255.0
#
 bgp 65420
 peer 10.2.1.2 as-number 200
 #
 address-family ipv4 unicast
 import-route direct
 peer 10.2.1.2 enable
#
```

- UPE1：

```
#
 ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
 mpls lsr-id 1.1.1.9
#
 interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
 interface GigabitEthernet2/0/1
 ip address 172.1.1.1 255.255.255.0
 mpls enable
#
 interface GigabitEthernet2/0/2
 ip binding vpn-instance vpn1
 ip address 10.1.1.2 255.255.255.0
#
 bgp 200
 peer 2.2.2.9 as-number 100
 peer 2.2.2.9 connect-interface LoopBack0
 peer 172.1.1.2 as-number 100
 #
 address-family ipv4 unicast
 import-route direct
 network 1.1.1.9 255.255.255.255
 network 172.1.1.0 255.255.255.0
 peer 172.1.1.2 enable
 peer 172.1.1.2 route-policy hope export
 peer 172.1.1.2 label-route-capability
#
 address-family vpnv4
 peer 2.2.2.9 enable
 peer 2.2.2.9 allow-as-loop 1
#
 ip vpn-instance vpn1
 peer 10.1.1.1 as-number 65410
```

```
#
 address-family ipv4 unicast
 import-route direct
 peer 10.1.1.1 enable
#
 route-policy hope permit node 0
 apply mpls-label
#
```

- SPE1：

```
#
 ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
 ospf 1
 area 0.0.0.0
 network 2.2.2.9 0.0.0.0
 network 180.1.1.0 0.0.0.255
#
 mpls lsr-id 2.2.2.9
#
 mpls ldp
#
 interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
 interface GigabitEthernet2/0/1
 ip address 172.1.1.2 255.255.255.0
 mpls enable
#
 interface GigabitEthernet2/0/2
 ip address 180.1.1.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
 bgp 100
 peer 1.1.1.9 as-number 200
 peer 1.1.1.9 connect-interface LoopBack0
 peer 3.3.3.9 as-number 100
 peer 3.3.3.9 connect-interface LoopBack0
 peer 172.1.1.1 as-number 200
#
 address-family ipv4 unicast
 network 2.2.2.9 255.255.255.255
 peer 172.1.1.1 enable
 peer 172.1.1.1 route-policy policy1 export
 peer 172.1.1.1 label-route-capability
```

```
#
 address-family vpnv4
 peer 1.1.1.9 enable
 peer 1.1.1.9 upe
 peer 1.1.1.9 upe route-policy policy2 export
 peer 3.3.3.9 enable
#
 ip vpn-instance vpn1
#
 route-policy policy1 permit node 0
 apply mpls-label
#
 route-policy policy2 permit node 0
 if-match ip address prefix-list list1
#
 ip prefix-list list1 index 10 permit 172.16.3.0 24
#
```

- UPE2：

```
#
 ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
 mpls lsr-id 4.4.4.9
#
 interface LoopBack0
 ip address 4.4.4.9 255.255.255.255
#
 interface GigabitEthernet2/0/1
 ip address 172.2.1.1 255.255.255.0
 mpls enable
#
 interface GigabitEthernet2/0/2
 ip binding vpn-instance vpn1
 ip address 10.2.1.2 255.255.255.0
#
 bgp 200
 peer 3.3.3.9 as-number 100
 peer 3.3.3.9 connect-interface LoopBack0
 peer 172.2.1.2 as-number 100
#
 address-family ipv4 unicast
 network 4.4.4.9 255.255.255.255
 peer 172.2.1.2 enable
 peer 172.2.1.2 route-policy hope export
 peer 172.2.1.2 label-route-capability
#
```

```
 address-family vpnv4
 peer 3.3.3.9 enable
 peer 3.3.3.9 allow-as-loop 1
#
 ip vpn-instance vpn1
 peer 10.2.1.1 as-number 65420
#
 address-family ipv4 unicast
 import-route direct
 peer 10.2.1.1 enable
#
 route-policy hope permit node 0
 apply mpls-label
#
```

- SPE2：

```
#
 ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
 ospf 1
 area 0.0.0.0
 network 3.3.3.9 0.0.0.0
 network 180.1.1.0 0.0.0.255
#
 mpls lsr-id 3.3.3.9
#
 mpls ldp
#
 interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
 interface GigabitEthernet2/0/1
 ip address 172.2.1.2 255.255.255.0
 mpls enable
#
 interface GigabitEthernet2/0/2
 ip address 180.1.1.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
 bgp 100
 router-id 3.3.3.9
 peer 2.2.2.9 as-number 100
 peer 2.2.2.9 connect-interface LoopBack0
 peer 4.4.4.9 as-number 200
 peer 4.4.4.9 connect-interface LoopBack0
```

```
 peer 172.2.1.1 as-number 200
#
 address-family ipv4 unicast
 network 3.3.3.9 255.255.255.255
 peer 172.2.1.1 enable
 peer 172.2.1.1 route-policy policy1 export
 peer 172.2.1.1 label-route-capability
#
 address-family vpnv4
 peer 2.2.2.9 enable
 peer 4.4.4.9 enable
 peer 4.4.4.9 upe
 peer 4.4.4.9 upe route-policy policy2 export
#
 ip vpn-instance vpn1
#
 route-policy policy1 permit node 0
 apply mpls-label
#
 route-policy policy2 permit node 0
 if-match ip address prefix-list list1
#
 ip prefix-list list1 index 10 permit 172.16.1.0 24
#
```

4 相关资料

- H3C SR6600 SR6600-X 路由器 MPLS 配置指导-R7607
- H3C SR6600 SR6600-X 路由器 MPLS 命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

IGMP 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1

2 配置前提 1

3 IGMP 基本功能配置举例 1

3.1 组网需求 1

3.2 配置思路 2

3.3 使用版本 2

3.4 配置注意事项 2

3.5 配置步骤 2

3.6 验证配置 3

3.7 配置文件 4

4 IGMP 静态加入组播组配置举例 5

4.1 组网需求 5

4.2 配置思路 6

4.3 使用版本 6

4.4 配置注意事项 6

4.5 配置步骤 6

4.6 验证配置 8

4.7 配置文件 9

5 IGMP SSM Mapping 典型配置举例 10

5.1 组网需求 10

5.2 使用版本 10

5.3 配置步骤 11

5.4 验证配置 12

5.5 配置文件 13

6 IGMP Proxying 典型配置举例 15

6.1 组网需求 15

6.2 配置思路 15

6.3 使用版本 15

6.4 配置注意事项 15

6.5 配置步骤 16

6.6 验证配置 16

6.7 配置文件 17

7 参考资料 ····· 18

1 简介

IGMP（Internet Group Management Protocol，互联网组管理协议）用于在三层设备和其直连网段中的用户主机之间建立和维护组播组成员关系。本文介绍了 IGMP 的典型配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 IGMP 特性。

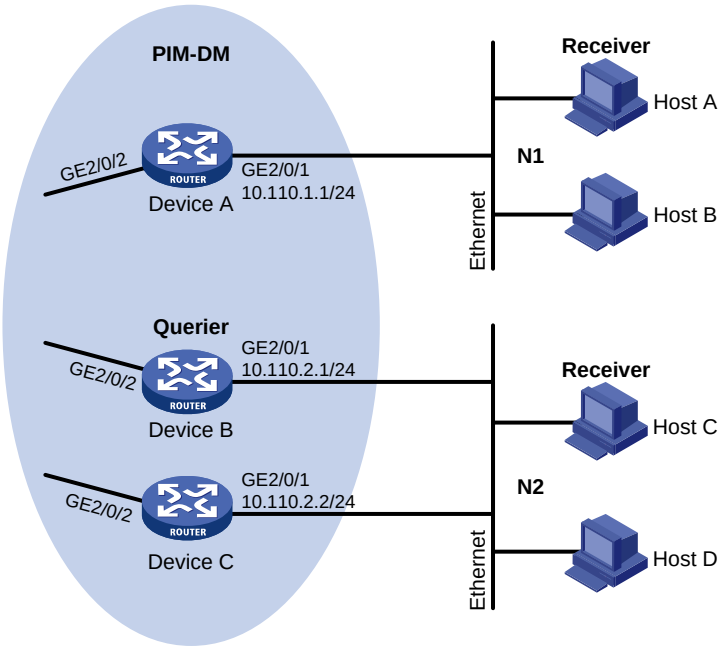
3 IGMP 基本功能配置举例

3.1 组网需求

如图 1 所示，网络中运行 OSPF 和 PIM，接收者通过组播方式接收视频点播信息，不同组织的接收者组成末梢网络 N1 和 N2，Host A 和 Host C 分别为 N1 和 N2 中的组播信息接收者。Router A 与 N1 之间运行 IGMPv2，Router A 为 IGMP 查询器；Router B、Router C 与 N2 之间也分别运行 IGMPv2，且由于 Router B 的接口 IP 地址较小，因此由其充当 IGMP 查询器。现要求：

- 对网络 N1 内的接收者所能加入的组播组没有限制；
- 控制网络 N2 内的接收者只能加入组播组 224.1.1.1。

图1 IGMP 基本功能配置组网图



3.2 配置思路

- 因共享网段 N2 内有多台 IGMP 路由器，为实现本组网需求，需要在该共享网段内的所有 IGMP 路由器上都配置相同的 IGMP 组播组过滤器。
- 为实现 IGMP 组播组过滤器控制主机加入组播组的范围，需要为其创建基本 ACL，并在该 ACL 规则中指定允许主机加入的组播组范围。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置注意事项

由于不同版本 IGMP 协议的报文结构与种类不同，因此需要为同一网段上的所有路由器配置相同版本的 IGMP，否则 IGMP 将不能正常运行。

3.5 配置步骤

(1) 配置 PIM-DM 域内各路由器的 IP 地址、单播路由协议和组播路由协议

配置 PIM-DM 域内路由器上各接口的 IP 地址和子网掩码，具体配置过程略。

配置 PIM-DM 域内的各路由器之间采用 OSPF 协议进行互连，确保 PIM-DM 域内部在网络层互通，并在各路由器上配置 PIM-DM 协议，以建立组播路由转发表项，实现组播数据可以从组播源到达接收者，具体配置过程略。

(2) 配置 Router A

在 Router A 上使能 IP 组播路由，在接口 GigabitEthernet2/0/2 上使能 PIM-DM，并在主机侧接口 GigabitEthernet2/0/1 上使能 IGMP。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] igmp enable
[RouterA-GigabitEthernet2/0/1] quit
[RouterA] interface gigabitethernet 2/0/2
[RouterA-GigabitEthernet2/0/2] pim dm
[RouterA-GigabitEthernet2/0/2] quit
```

(3) 配置 Router B

在 Router B 上使能 IP 组播路由，在接口 GigabitEthernet2/0/2 上使能 PIM-DM，并在主机侧接口 GigabitEthernet2/0/1 上使能 IGMP 及配置组播组过滤器，以在 Router B 上限制用户网络 N2 内的主机只能加入组播组 224.1.1.1。

```
<RouterB> system-view
[RouterB] acl basic 2001
[RouterB-acl-ipv4-basic-2001] rule permit source 224.1.1.1 0
[RouterB-acl-ipv4-basic-2001] quit
[RouterB] multicast routing
```

```
[RouterB-mrib] quit
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] igmp enable
[RouterB-GigabitEthernet2/0/1] igmp group-policy 2001
[RouterB-GigabitEthernet2/0/1] quit
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] pim dm
[RouterB-GigabitEthernet2/0/2] quit
```

(4) 配置 Router C

在 Router C 上使能 IP 组播路由，在接口 GigabitEthernet2/0/2 上使能 PIM-DM，并在主机侧接口 GigabitEthernet2/0/1 上使能 IGMP 及配置组播组过滤器，以在 Router C 上限制用户网络 N2 内的主机只能加入组播组 224.1.1.1。

```
<RouterC> system-view
[RouterC] acl basic 2001
[RouterC-acl-ipv4-basic-2001] rule permit source 224.1.1.1 0
[RouterC-acl-ipv4-basic-2001] quit
[RouterC] multicast routing
[RouterC-mrib] quit
[RouterC] interface gigabitethernet 2/0/1
[RouterC-GigabitEthernet2/0/1] igmp enable
[RouterC-GigabitEthernet2/0/1] igmp group-policy 2001
[RouterC-GigabitEthernet2/0/1] quit
[RouterC] interface gigabitethernet 2/0/2
[RouterC-GigabitEthernet2/0/2] pim dm
[RouterC-GigabitEthernet2/0/2] quit
```

3.6 验证配置

(1) 配置完成后，用户网络 N1 内的组播接收者 Host A（地址为 10.110.1.10）分别发送组播组地址为 224.1.1.1 和 224.1.1.2 的 IGMP 成员关系报告报文，通过 **display igmp group** 命令查看 Router A 上 IGMP 组播组信息，验证配置效果。

查看 Router A 上 IGMP 组播组信息。

```
[RouterA] display igmp group
IGMP groups in total: 2.
GigabitEthernet2/0/1(10.110.1.1):
  IGMP groups reported in total: 2
  Group address   Last reporter   Uptime      Expires
   224.1.1.1       10.110.1.10     00:02:04    00:01:15
   224.1.1.2       10.110.1.10     00:02:00    00:01:19
```

Host A 发送了组播组地址为 224.1.1.1 和 224.1.1.2 的 IGMP 成员关系报告报文，因 Router A 上没有对加入的组播组做限制，用户网络 N1 内的组播接收者可以加入组播组 224.1.1.1 和 224.1.1.2。

(2) 配置完成后，用户网络 N2 内的组播接收者 Host C（地址为 10.110.2.10）分别发送组播组地址为 224.1.1.1 和 224.1.1.2 的 IGMP 成员关系报告报文，通过 display igmp group 命令查看 Router B 和 Router C 上 IGMP 组播组信息，验证配置效果。

查看 Router B 上 IGMP 组播组信息。

```
[RouterB] display igmp group
IGMP groups in total: 1.
GigabitEthernet2/0/1(10.110.2.1):
  IGMP groups reported in total: 1
  Group address   Last reporter   Uptime      Expires
   224.1.1.1       10.110.2.10     00:02:04    00:01:15
```

查看 Router C 上 IGMP 组播组信息。

```
[RouterC] display igmp group
IGMP groups in total: 1..
GigabitEthernet2/0/1(10.110.2.2):
  IGMP groups reported in total: 1
   Group address   Last reporter   Uptime      Expires
   224.1.1.1       10.110.2.10     00:02:04    00:01:15
```

Host C 发送了组播组地址为 224.1.1.1 和 224.1.1.2 的 IGMP 成员关系报告报文，而 Router B 和 Router C 上只有组播组 224.1.1.1 的 IGMP 组播组信息，由此可见在 Router B 和 Router C 上配置的 IGMP 组播组过滤器已生效，用户网络 N2 内的组播接收者只能加入组播组 224.1.1.1。

3.7 配置文件

- Router A：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 igmp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 pim dm
#
multicast routing
#
```

- Router B：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 igmp enable
 igmp group-policy 2001
#
interface GigabitEthernet2/0/2
 port link-mode route
 pim dm
#
multicast routing
#
acl basic 2001
 rule 0 permit source 224.1.1.1 0
```

```
#
```

- Router C：

```
#
interface GigabitEthernet2/0/2
 port link-mode route
 pim dm
#
interface GigabitEthernet2/0/1
 port link-mode route
 igmp enable
 igmp group-policy 2001
#
multicast routing
#
acl basic 2001
 rule 0 permit source 224.1.1.1 0
#
```

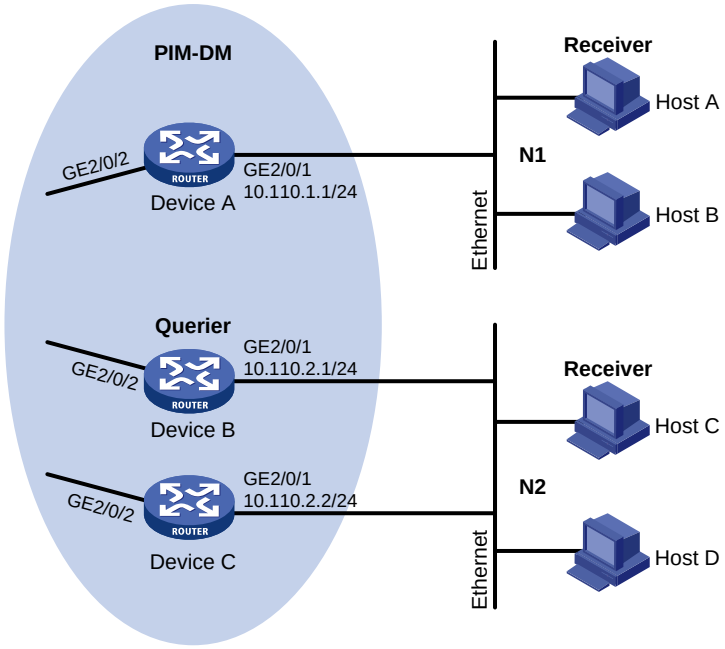
4 IGMP 静态加入组播组配置举例

4.1 组网需求

如 3.1 图 1 所示，网络中运行 OSPF 和 PIM，接收者通过组播方式接收视频点播信息，不同组织的接收者组成末梢网络 N1 和 N2，Host A 和 Host C 分别为 N1 和 N2 中的组播信息接收者。Router A 与 N1 之间运行 IGMPv2，Router A 为 IGMP 查询器；Router B、Router C 与 N2 之间也分别运行 IGMPv2，且由于 Router B 的接口 IP 地址较小，因此由其充当 IGMP 查询器。现要求：

- 对网络 N1 内的接收者所能加入的组播组没有限制，但 Host A 希望长期稳定地接收组播组 224.1.1.2 的数据；
- 控制网络 N2 内的接收者只能加入组播组 224.1.1.1。

图2 IGMP 静态加入组播组配置组网图



4.2 配置思路

- 为使 Host A 可以稳定的接收 224.1.1.2 的数据，可以通过在连接 Host A 的 Router A 接口上配置静态加入组播组来实现该需求。
- 为实现 IGMP 组播组过滤器控制主机加入组播组的范围，需要为其创建基本 ACL，并在该 ACL 规则中指定允许主机加入的组播组范围。
- 因共享网段 N2 内有多台 IGMP 路由器，为实现本组网需求，需要在该共享网段内的所有 IGMP 路由器上都配置相同的 IGMP 组播组过滤器。

4.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.4 配置注意事项

由于不同版本 IGMP 协议的报文结构与种类不同，因此需要为同一网段上的所有路由器配置相同版本的 IGMP，否则 IGMP 将不能正常运行。

4.5 配置步骤

(1) 配置 PIM-DM 域内各路由器的 IP 地址、单播路由协议和组播路由协议

配置 PIM-DM 域内路由器上各接口的 IP 地址和子网掩码，具体配置过程略。

配置 PIM-DM 域内的各路由器之间采用 OSPF 协议进行互连，确保 PIM-DM 域内部在网络层互通，以用来建立组播路由转发表项，实现组播数据可以从组播源到达接收者，具体配置过程略。

(2) 配置 Router A

在 Router A 上使能 IP 组播路由，并在接口 GigabitEthernet2/0/2 上使能 PIM-DM。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 2/0/2
[RouterA-GigabitEthernet2/0/2] pim dm
[RouterA-GigabitEthernet2/0/2] quit
```

在主机侧接口 GigabitEthernet2/0/1 上使能 IGMP，并配置该接口静态加入组播组 224.1.1.2。

```
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] igmp enable
[RouterA-GigabitEthernet2/0/1] igmp static-group 224.1.1.2
[RouterA-GigabitEthernet2/0/1] quit
```

(3) 配置 Router B

在 Router B 上使能 IP 组播路由，并在接口 GigabitEthernet2/0/2 上使能 PIM-DM。

```
<RouterB> system-view
[RouterB] multicast routing
[RouterB-mrib] quit
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] pim dm
[RouterB-GigabitEthernet2/0/2] quit
```

配置 ACL 2001 用于组播过滤器。

```
[RouterB] acl basic 2001
[RouterB-acl-ipv4-basic-2001] rule permit source 224.1.1.1 0
[RouterB-acl-ipv4-basic-2001] quit
```

在主机侧接口 GigabitEthernet2/0/1 上使能 IGMP 及配置组播组过滤器，以在 Router B 上限制用户网络 N2 内的主机只能加入组播组 224.1.1.1。

```
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] igmp enable
[RouterB-GigabitEthernet2/0/1] igmp group-policy 2001
[RouterB-GigabitEthernet2/0/1] quit
```

(4) 配置 Router C

在 Router C 上使能 IP 组播路由，并在接口 GigabitEthernet2/0/2 上使能 PIM-DM。

```
<RouterC> system-view
[RouterC] multicast routing
[RouterC-mrib] quit
[RouterC] interface gigabitethernet 2/0/2
[RouterC-GigabitEthernet2/0/2] pim dm
[RouterC-GigabitEthernet2/0/2] quit
```

配置 ACL 2001 用于组播过滤器。

```
[RouterC] acl basic 2001
```

```
[RouterC-acl-ipv4-basic-2001] rule permit source 224.1.1.1 0
[RouterC-acl-ipv4-basic-2001] quit
```

在主机侧接口 GigabitEthernet2/0/1 上使能 IGMP 及配置组播组过滤器，以在 Router C 上限制用户网络 N2 内的主机只能加入组播组 224.1.1.1

```
[RouterC] interface gigabitethernet 2/0/1
[RouterC-GigabitEthernet2/0/1] igmp enable
[RouterC-GigabitEthernet2/0/1] igmp group-policy 2001
[RouterC-GigabitEthernet2/0/1] quit
```

4.6 验证配置

(1) 配置完成后，用户网络 N1 内的组播接收者 Host A（地址为 10.110.1.10）分别发送组播组地址为 224.1.1.1 和 224.1.1.2 的 IGMP 成员关系报告报文，通过 **display igmp group** 命令查看 Router A 上 IGMP 组播组信息，验证配置效果。

查看 Router A 上动态加入的 IGMP 组播组信息。

```
[RouterA] display igmp group
IGMP groups in total: 2.
GigabitEthernet2/0/1(10.110.1.1):
  IGMP groups reported in total: 2
  Group address   Last reporter   Uptime      Expires
   224.1.1.1       10.110.1.10     00:02:04    00:01:15
   224.1.1.2       10.110.1.10     00:02:00    00:01:19
```

显示 Router A 上静态加入的 IGMP 组播组信息。

```
[RouterA] display igmp group static
 Entries in total: 1
   Group address   Source address  Interface           Expires
   224.1.1.2       0.0.0.0         GE2/0/1             Never
```

Host A 发送了组播组地址为 224.1.1.1 和 224.1.1.2 的 IGMP 成员关系报告报文，因 Router A 上没有对加入的组播组做限制，用户网络 N1 内的组播接收者可以加入组播组 224.1.1.1 和 224.1.1.2，且 N1 内的组播接收者可以长期稳定的接收组播组 224.1.1.2 的数据。

(2) 配置完成后，用户网络 N2 内的组播接收者 Host C（地址为 10.110.2.10）分别发送组播组地址为 224.1.1.1 和 224.1.1.2 的 IGMP 成员关系报告报文，通过 **display igmp group** 命令查看 Router B 和 Router C 上 IGMP 组播组信息，验证配置效果。

查看 Router B 上动态加入的 IGMP 组播组信息。

```
[RouterB] display igmp group
IGMP groups in total: 1.
GigabitEthernet2/0/1(10.110.2.1):
  IGMP groups reported in total: 1
  Group address   Last reporter   Uptime      Expires
   224.1.1.1       10.110.2.10     00:02:04    00:01:15
```

查看 Router C 上动态加入的 IGMP 组播组信息。

```
[RouterC] display igmp group
IGMP groups in total: 1..
GigabitEthernet2/0/1(10.110.2.2):
  IGMP groups reported in total: 1
```

```
  Group address   Last reporter   Uptime      Expires
  224.1.1.1       10.110.2.10     00:02:04    00:01:15
```

Host C 发送了组播组地址为 224.1.1.1 和 224.1.1.2 的 IGMP 成员关系报告报文，而 Router B 和 Router C 上只有组播组 224.1.1.1 的 IGMP 组播组信息，由此可见在 Router B 和 Router C 上配置的 IGMP 组播组过滤器已生效，用户网络 N2 内的组播接收者只能加入组播组 224.1.1.1。

4.7 配置文件

- Router A：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.110.1.1 255.255.255.0
 igmp enable
 igmp static-group 224.1.1.2
#
interface GigabitEthernet2/0/2
 port link-mode route
 pim dm
#
multicast routing
#
```

- Router B：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.110.2.1 255.255.255.0
 igmp enable
 igmp group-policy 2001
#
interface GigabitEthernet2/0/2
 port link-mode route
 pim dm
#
multicast routing
#
acl basic 2001
 rule 0 permit source 224.1.1.1 0
#
```

- Router C：

```
#
interface GigabitEthernet2/0/2
 port link-mode route
 pim dm
#
interface GigabitEthernet2/0/1
```

```
 port link-mode route
 ip address 10.110.2.2 255.255.255.0
 igmp enable
 igmp group-policy 2001
#
multicast routing
#
acl basic 2001
 rule 0 permit source 224.1.1.1 0
#
```

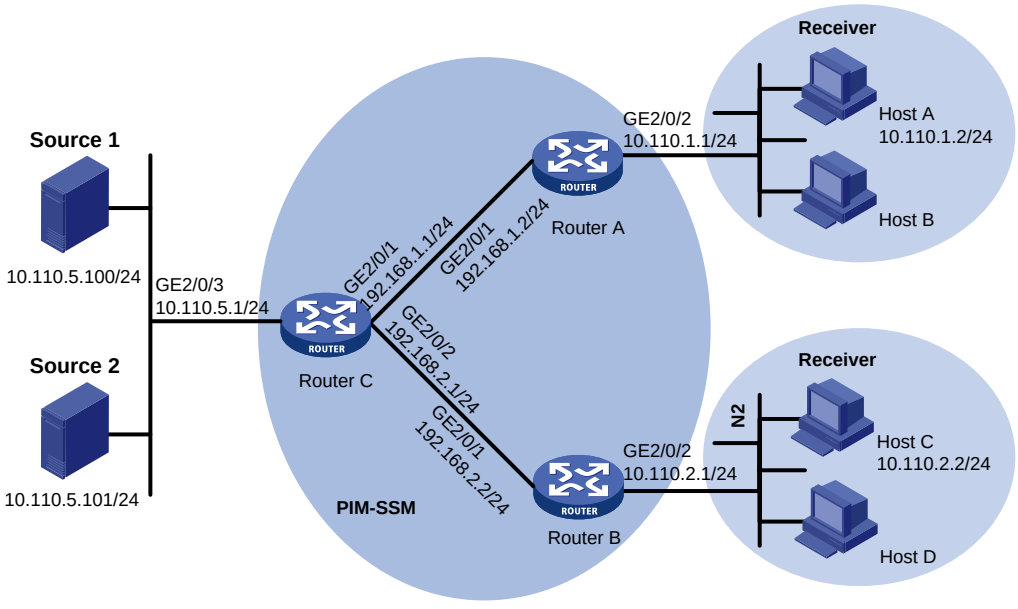
5 IGMP SSM Mapping 典型配置举例

5.1 组网需求

如图 3 所示，PIM-SSM 网络所服务的 SSM 组播组范围为 232.1.1.0/24，PIM-SSM 网络内连接用户网络 N1 和 N2 的边界路由器上均运行 IGMPv3 功能，而用户网络 N1、N2 内的主机 Host A 和 Host C 上只能运行 IGMPv1 或 IGMPv2，且不能升级至 IGMPv3；其他主机运行 IGMPv3。

现要求：通过在 IGMP 路由器上配置 IGMP SSM Mapping 功能，使 PIM-SSM 网络能够为用户网络 N1 内的接收者提供 SSM 组播服务，实现用户网络 N1 中的接收者只接收来自 Source 1 的组播报文。用户网络 N2 中的接收者只接收来自 Source 2 的组播报文。

图3 IGMP SSM Mapping 功能配置组网图



5.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

5.3 配置步骤

(1) 配置 IP 地址和单播路由协议

请按照 5.1 图 3 配置各接口的 IP 地址和子网掩码，具体配置过程略。

配置 PIM-SSM 网络内的各路由器之间采用 OSPF 协议进行互连，具体配置过程略。

(2) 使能 IP 组播路由，并使能 PIM-SM

在 Router A 上使能 IP 组播路由，在接口上使能 PIM-SM。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] pim sm
[RouterA-GigabitEthernet2/0/1] quit
```

Router B 的配置与 Router A 相似，配置过程略。

在 Router C 上使能 IP 组播路由，在各接口上使能 PIM-SM。

```
<RouterC> system-view
[RouterC] multicast routing
[RouterC-mrib] quit
[RouterC] interface gigabitethernet 2/0/1
[RouterC-GigabitEthernet2/0/1] pim sm
[RouterC-GigabitEthernet2/0/1] quit
[RouterC] interface gigabitethernet2/0/2
[RouterC-GigabitEthernet2/0/2] pim sm
[RouterC-GigabitEthernet2/0/2] quit
[RouterC] interface gigabitethernet2/0/3
[RouterC-GigabitEthernet2/0/3] pim sm
[RouterC-GigabitEthernet2/0/3] quit
```

(3) 配置 C-BSR 和 C-RP

在 Router C 上配置 C-BSR 和 C-RP 的位置。

```
[RouterC] pim
[RouterC-pim] c-bsr 192.168.1.1
[RouterC-pim] c-rp 192.168.1.1
[RouterC-pim] quit
```

(4) 在连接网络 N1 和 N2 的接口上使能 IGMPv3 功能

在 Router A 的接口 GigabitEthernet2/0/2 上使能 IGMPv3。

```
[RouterA] interface gigabitethernet 2/0/2
[RouterA-GigabitEthernet2/0/2] igmp enable
[RouterA-GigabitEthernet2/0/2] igmp version 3
[RouterA-GigabitEthernet2/0/2] quit
```

Router B 的配置与 Router A 相似，配置过程略。

(5) 配置 SSM 组播组的地址范围

在 Router A 上配置 SSM 组播组地址范围为 232.1.1.0/24。

```
[RouterA] acl basic 2000
[RouterA-acl-ipv4-basic-2000] rule permit source 232.1.1.0 0.0.0.255
[RouterA-acl-ipv4-basic-2000] quit
```

```
[RouterA] pim
[RouterA-pim] ssm-policy 2000
[RouterA-pim] quit
```

Router B 和 Router C 的配置与 Router A 相同，配置过程略。

(6) 使能 IGMP SSM Mapping 功能，并配置 IGMP SSM Mapping 规则

在 Router A 上配置 IGMP SSM Mapping 规则，满足 N1 网络内组播报文接收者只接收来自组播源 Source 1 的组播数据的要求。

```
[RouterA] igmp
[RouterA-igmp] ssm-mapping 10.110.5.100 2000
[RouterA-igmp] quit
```

#在 Router B 上配置 IGMP SSM Mapping 规则，满足 N2 网络内组播报文接收者只接收来自组播源 Source 2 的组播数据的要求。

```
[RouterB] igmp
[RouterB-igmp] ssm-mapping 10.110.5.101 2000
[RouterB-igmp] quit
```

5.4 验证配置

配置完成后，Host A 和 Host C 都发送组播组地址为 232.1.1.1 的 IGMPv2 加入报文，在 Router A 和 Router B 上通过相关命令查看配置效果。

(1) Router A 上的显示信息

查看 Router A 上组播组 232.1.1.1 的 IGMP SSM Mapping 规则。

```
[RouterA] display igmp ssm-mapping 232.1.1.1
 Group: 232.1.1.1
 Source list:
        10.110.5.100
```

查看 Router A 上的 PIM 路由表信息。

```
[RouterA] display pim routing-table
Total 0 (*, G) entry; 1 (S, G) entry

(10.110.5.100, 232.1.1.1)
     Protocol: pim-ssm, Flag:
     UpTime: 00:00:47
     Upstream interface: GigabitEthernet2/0/1
         Upstream neighbor: 192.168.1.1
         RPF prime neighbor: 192.168.1.1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/0/2
             Protocol: igmp, UpTime: 00:00:47, Expires: -
```

(2) Router B 上的显示信息

查看 Router B 上组播组 232.1.1.1 的 IGMP SSM Mapping 规则。

```
[RouterB] display igmp ssm-mapping 232.1.1.1
 Group: 232.1.1.1
 Source list:
```

```
        10.110.5.101
```

查看 Router B 上的 PIM 路由表信息。

```
[RouterB] display pim routing-table
Total 0 (*, G) entry; 1 (S, G) entry

(10.110.5.101, 232.1.1.1)
     Protocol: pim-ssm, Flag:
     UpTime: 00:00:47
     Upstream interface: GigabitEthernet2/0/1
         Upstream neighbor: 192.168.2.1
         RPF prime neighbor: 192.168.2.1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/0/2
             Protocol: igmp, UpTime: 00:00:47, Expires: -
```

通过显示信息可知，在 Router A 和 Router B 上配置了 IGMP SSM Mapping 功能后，Router A 将接收者主机发来的 IGMPv2 成员关系报告报文中所包含的（0.0.0.0，232.1.1.1）信息映射为（10.110.5.100，232.1.1.1）信息，Router B 将接收者主机发来的 IGMPv2 成员关系报告报文中所包含的（0.0.0.0，232.1.1.1）信息映射为（10.110.5.101，232.1.1.1）信息，从而使接收者 Host A 只接收来自 Source 1 的组播报文，使接收者 Host C 只接收来自 Source 2 的组播报文。

5.5 配置文件

- RouterA：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 pim sm
#
interface GigabitEthernet2/0/2
 port link-mode route
 igmp enable
 igmp version 3
#
multicast routing
#
pim
 ssm-policy 2000
#
igmp
 ssm-mapping 10.110.5.100 2000
#
acl basic 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#
```

- Router B：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 pim sm
#
interface GigabitEthernet2/0/2
 port link-mode route
 igmp enable
 igmp version 3
#
multicast routing
#
pim
 ssm-policy 2000
#
igmp
 ssm-mapping 10.110.5.100 2000
#
acl basic 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#
```

- Router C：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 pim sm
#
interface GigabitEthernet2/0/2
 port link-mode route
 pim sm
#
interface GigabitEthernet2/0/3
 port link-mode route
 pim sm
#
multicast routing
#
pim
 c-bsr 192.168.1.1
 c-rp 192.168.1.1
#
```

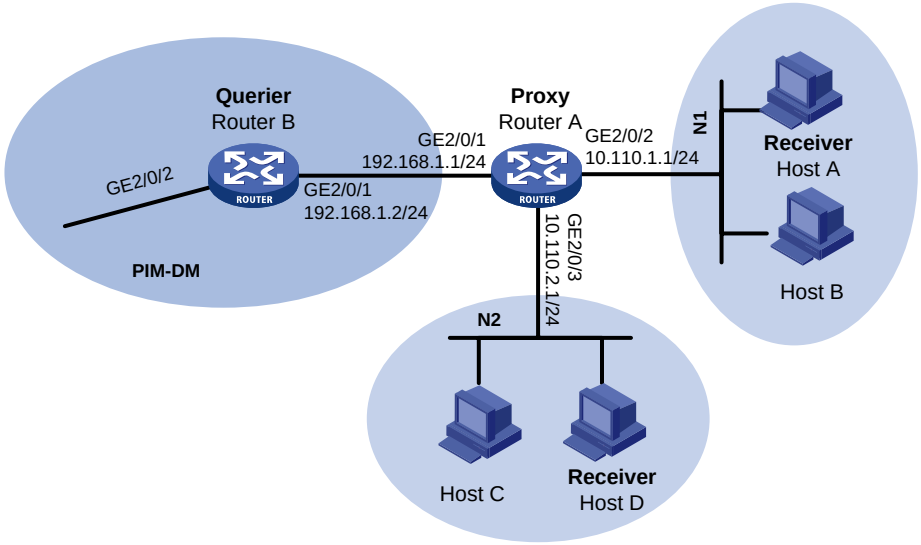
6 IGMP Proxying 典型配置举例

6.1 组网需求

如图 4 所示，用户网络 N1 和 N2 通过路由器 Router A 与 PIM-DM 域内的 IGMP 查询器 Router B 相连。

现要求通过在路由器 Router A 上配置 IGMP Proxying 功能，使其在不运行 PIM-DM 的情况下实现用户网络 N1、N2 内的接收者可以接收到通过 PIM-DM 域转发过来的组播数据报文。

图4 IGMP Proxying 功能配置组网图



6.2 配置思路

为实现本组网需求，需要在 IGMP 代理设备的上行接口上运行 IGMP Proxying 功能，上游设备将视 IGMP 代理设备为主机，而在其下行接口上运行 IGMP 协议，下游设备视 IGMP 代理设备为 IGMP 路由器。

6.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

6.4 配置注意事项

- 在设备上开启 IGMP 代理功能时，须先使能 IP 组播路由。
- 一个接口上如果同时使能 IGMP 代理功能和 IGMP 协议，IGMP 协议将不会生效。在已使能 IGMP 代理功能的接口上配置其它 IGMP 命令时，只有 **igmp version** 命令会生效。
- 如果在一台设备上同时使能 IGMP 代理功能和组播路由协议（如 PIM 和 MSDP），组播路由协议将不会生效。

6.5 配置步骤

(1) 配置 IP 地址

请按照 6.1 图 4 配置各接口的 IP 地址和子网掩码，具体配置过程略。

配置 PIM-DM 网络内的各路由器之间采用 OSPF 协议进行互连，具体配置过程略。

(2) 配置 Router A

在 Router A 上使能 IP 组播路由，并在朝向 Router B 侧的接口 GigabitEthernet2/0/1 上使能 IGMP 代理功能。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] igmp proxy enable
[RouterA-GigabitEthernet2/0/1] quit
```

在 Router A 上朝向用户侧的接口 GigabitEthernet2/0/2 和 GigabitEthernet2/0/3 上使能 IGMP。

```
[RouterA] interface gigabitethernet 2/0/2
[RouterA-GigabitEthernet2/0/2] igmp enable
[RouterA-GigabitEthernet2/0/2] quit
[RouterA] interface gigabitethernet 2/0/3
[RouterA-GigabitEthernet2/0/3] igmp enable
[RouterA-GigabitEthernet2/0/3] quit
```

(3) 配置 Router B

在 Router B 上使能 IP 组播路由，并在接口 GigabitEthernet2/0/2 上使能 PIM-DM。

```
<RouterB> system-view
[RouterB] multicast routing
[RouterB-mrib]quit
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] pim dm
[RouterB-GigabitEthernet2/0/2] quit
```

#在 Router B 上朝向用户侧的接口 GigabitEthernet2/0/1 上使能 IGMP。

```
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] igmp enable
[RouterB-GigabitEthernet2/0/1] quit
```

6.6 验证配置

配置完成后，用户网络 N1 内的组播接收者 Host A 发送组播组地址为 224.1.1.1 的 IGMP 成员关系报告报文，通过 **display igmp group** 命令查看 Router A 和 Router B 上 IGMP 组播组信息，检验配置效果：

查看 Router A 的 GigabitEthernet2/0/2 接口上 IGMP 组播组信息。

```
[RouterA] display igmp group interface GigabitEthernet2/0/2
GigabitEthernet2/0/2(10.110.1.1):
  IGMP groups reported in total: 1
   Group address   Last reporter   Uptime      Expires
```

```
   224.1.1.1       10.110.1.10     00:02:04    00:01:15
```

查看 Router A 上 IGMP 代理记录的所有组播组信息。

```
[RouterA] display igmp proxy group
IGMP proxy group records in total: 1
 GigabitEthernet2/0/1(192.168.1.1):
  IGMP proxy group records in total: 1
   Group address      Member state      Expires
   224.1.1.1          Delay            00:00:02
```

通过显示信息可知，Router A 的 GigabitEthernet2/0/2 接口接收到主机的 IGMP 成员关系报告报文后，建立并维护该组播组成员关系，对于下面的主机而言，Router A 的下行接口执行 IGMP 协议的路由器行为。

查看 Router B 的 GigabitEthernet2/0/1 接口上 IGMP 组播组信息。

```
[RouterB] display igmp group interface GigabitEthernet2/0/1
GigabitEthernet2/0/1(192.168.1.2):
  IGMP groups reported in total: 1
   Group address   Last reporter   Uptime      Expires
   224.1.1.1       192.168.1.1      00:02:04    00:01:15
```

通过显示信息可知，Router B 的 GigabitEthernet2/0/1 接口接收到 IGMP Proxying 设备的 IGMP 成员关系报告报文后，建立并维护该组播组成员关系。由此可见，对于上游查询器 Router B 而言，Router A 的上行接口执行 IGMP 协议的主机行为。

6.7 配置文件

- Router A：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 igmp proxy enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 igmp enable
#
interface GigabitEthernet2/0/3
 port link-mode route
 igmp enable
#
multicast routing
#
```

- Router B：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 igmp enable
#
interface GigabitEthernet2/0/2
```

```
 port link-mode route
 pim dm
#
multicast routing
#
```

7 参考资料

- H3C SR6600 SR6600-X 路由器 IP 组播配置指导-R7607
- H3C SR6600 SR6600-X 路由器 IP 组播命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

IPsec 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1

2 配置前提 1

3 使用 iNode 客户端基于证书认证的 L2TP over IPsec 功能配置举例 1

3.1 组网需求 1

3.2 配置思路 2

3.3 使用版本 2

3.4 配置步骤 2

3.4.1 Device 的配置 2

3.4.2 Host 的配置 4

3.5 验证配置 11

3.6 配置文件 15

4 IPsec over GRE 的典型配置举例 16

4.1 组网需求 16

4.2 配置思路 16

4.3 使用版本 17

4.4 配置步骤 17

4.4.1 Device A 的配置 17

4.4.2 Device B 的配置 18

4.5 验证配置 19

4.6 配置文件 21

5 GRE over IPsec 的典型配置举例 22

5.1 组网需求 22

5.2 配置思路 23

5.3 使用版本 23

5.4 配置步骤 23

5.4.1 Device A 的配置 23

5.4.2 Device B 的配置 24

5.5 验证配置 25

5.6 配置文件 27

6 IPsec 同流双隧道的典型配置举例 29

6.1 组网需求 29

6.2 使用版本 29
6.3 配置步骤 29
6.3.1 Device A 的配置 29
6.3.2 Device B 的配置 30
6.4 验证配置 32
6.5 配置文件 33
7 相关资料 35

1 简介

本文档介绍 IPsec 的典型配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 IPsec 特性。

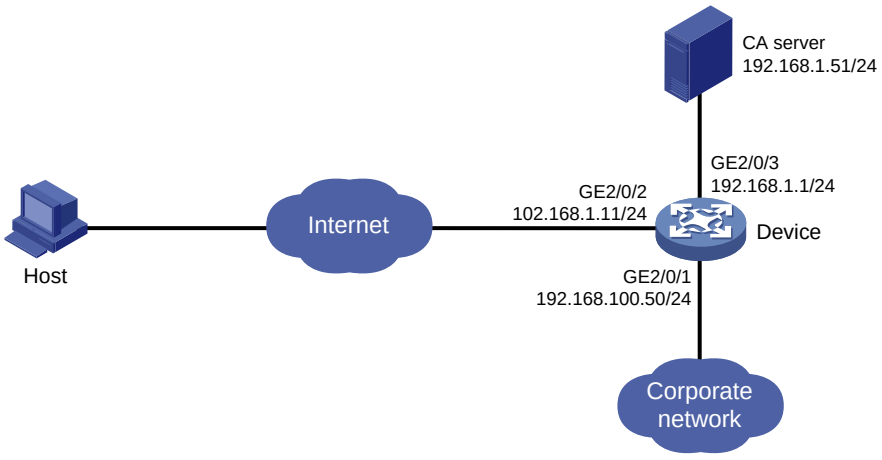
3 使用 iNode 客户端基于证书认证的 L2TP over IPsec 功能配置举例

3.1 组网需求

如图 1 所示，PPP 用户 Host 与 Device 建立 L2TP 隧道，Windows server 2003 作为 CA Server 服务器，要求：

- 通过 L2TP 隧道访问 Corporate network。
- 用 IPsec 对 L2TP 隧道进行数据加密。
- 采用 RSA 证书认证方式建立 IPsec 隧道。

图1 基于证书认证的 L2TP over IPsec 配置组网图



3.2 配置思路

由于使用证书认证方式建立 IPsec 隧道，所以需要在 ike profile 中配置 local-identity 为 dn，指定总从本端证书中的主题字段取得本端身份。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置步骤

3.4.1 Device 的配置

(1) 配置各接口 IP 地址

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<Device> system-view
[Device] interface gigabitethernet 2/0/1
[Device-GigabitEthernet2/0/1] ip address 192.168.100.50 24
[Device-GigabitEthernet2/0/1] quit
```

配置接口 GigabitEthernet2/0/2 的 IP 地址。

```
[Device] interface gigabitethernet 2/0/2
[Device-GigabitEthernet2/0/2] ip address 102.168.1.11 24
[Device-GigabitEthernet2/0/2] quit
```

配置接口 GigabitEthernet2/0/3 的 IP 地址。

```
[Device] interface gigabitethernet 2/0/3
[Device-GigabitEthernet2/0/3] ip address 192.168.1.1 24
[Device-GigabitEthernet2/0/3] quit
```

(2) 配置 L2TP

创建本地 PPP 用户 l2tpuser，设置密码为 hello。

```
[Device] local-user l2tpuser class network
[Device-luser-network-l2tpuser] password simple hello
[Device-luser-network-l2tpuser] service-type ppp
[Device-luser-network-l2tpuser] quit
# 配置 ISP 域 system 对 PPP 用户采用本地验证。
[Device] domain system
[Device-isp-system] authentication ppp local
[Device-isp-system] quit
```

启用 L2TP 服务。

```
[Device] l2tp enable
```

创建接口 Virtual-Template0，配置接口的 IP 地址为 172.16.0.1/24。

```
[Device] interface virtual-template 0
[Device-Virtual-Template0] ip address 172.16.0.1 255.255.255.0
# 配置 PPP 认证方式为 PAP。
[Device-Virtual-Template0] ppp authentication-mode pap
```

配置为 PPP 用户分配的 IP 地址为 172.16.0.2。

```
[Device-Virtual-Template0] remote address 172.16.0.2
[Device-Virtual-Template0] quit
```

创建 LNS 模式的 L2TP 组 1。

```
[Device] l2tp-group 1 mode lns
```

配置 LNS 侧本端名称为 lns。

```
[Device-l2tp1] tunnel name lns
```

关闭 L2TP 隧道验证功能。

```
[Device-l2tp1] undo tunnel authentication
```

指定接收呼叫的虚拟模板接口为 VT0。

```
[Device-l2tp1] allow l2tp virtual-template 0
[Device-l2tp1] quit
```

(3) 配置 PKI 证书

配置 PKI 实体 security。

```
[Device] pki entity security
[Device-pki-entity-security] common-name device
[Device-pki-entity-security] quit
```

新建 PKI 域。

```
[Device] pki domain headgate
[Device-pki-domain-headgate] ca identifier LYQ
[Device-pki-domain-headgate] certificate request url
http://192.168.1.51/certsrv/mscep/mscep.dll
[Device-pki-domain-headgate] certificate request from ra
[Device-pki-domain-headgate] certificate request entity security
[Device-pki-domain-headgate] undo crl check enable
[Device-pki-domain-headgate] public-key rsa general name abc length 1024
[Device-pki-domain-headgate] quit
```

生成 RSA 算法的本地密钥对。

```
[Device] public-key local create rsa name abc
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512,it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.
Create the key pair successfully.
```

获取 CA 证书并下载至本地。

```
[Device] pki retrieve-certificate domain headgate ca
The trusted CA's finger print is:
    MD5  fingerprint:8649 7A4B EAD5 42CF 5031 4C99 BFS3 2A99
    SHA1 fingerprint:61A9 6034 181E 6502 12FA 5A5F BA12 0EA0 5187 031C
Is the finger print correct?(Y/N):y
Retrieved the certificates successfully.
```

手工申请本地证书。

```
[Device] pki request-certificate domain headgate
```

```
Start to request general certificate ...
Certificate requested successfully.
```

(4) 配置 IPsec 隧道

创建 IKE 安全提议。

```
[Device] ike proposal 1
[Device-ike-proposal-1] authentication-method rsa-signature
[Device-ike-proposal-1] encryption-algorithm 3des-cbc
[Device-ike-proposal-1] dh group2
[Device-ike-proposal-1] quit
```

配置 IPsec 安全提议。

```
[Device] ipsec transform-set tran1
[Device-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[Device-ipsec-transform-set-tran1] esp encryption-algorithm 3des
[Device-ipsec-transform-set-tran1] quit
```

配置 IKE profile。

```
[Device] ike profile profile1
[Device-ike-profile-profile1] local-identity dn
[Device-ike-profile-profile1] certificate domain headgate
[Device-ike-profile-profile1] proposal 1
[Device-ike-profile-profile1] match remote certificate device
[Device-ike-profile-profile1] quit
```

在采用数字签名认证时，指定总从本端证书中的主题字段取得本端身份。

```
[Device]ike signature-identity from-certificate
```

创建一条 IPsec 安全策略模板，名称为 template1，序列号为 1。

```
[Device] ipsec policy-template template1 1
[Device-ipsec-policy-template-template1-1] transform-set tran1
[Device-ipsec-policy-template-template1-1] ike-profile profile1
[Device-ipsec-policy-template-template1-1] quit
```

引用 IPsec 安全策略模板创建一条 IPsec 安全策略，名称为 policy1，顺序号为 1。

[Device] ipsec policy policy1 1 isakmp template template1

在接口上应用 IPsec 安全策略。

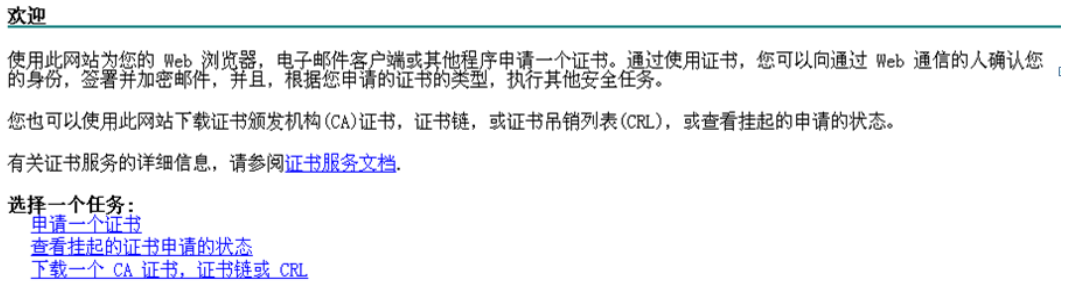
```
[Device] interface gigabitethernet 2/0/2
[Device-GigabitEthernet2/0/2] ipsec apply policy policy1
[Device-GigabitEthernet2/0/2] quit
```

3.4.2 Host 的配置

- 从证书服务器上申请客户端证书

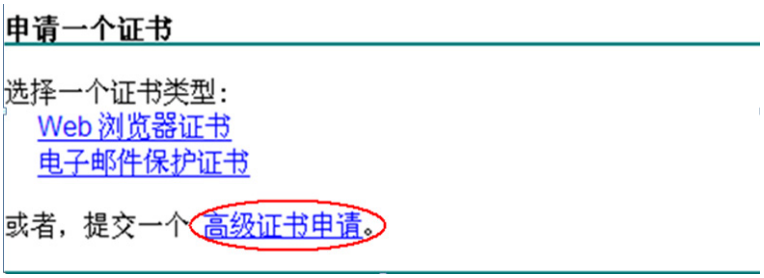
登录到证书服务器：http://192.168.1.51/certsrv，点击“申请一个证书”。

图2 进入申请证书页面



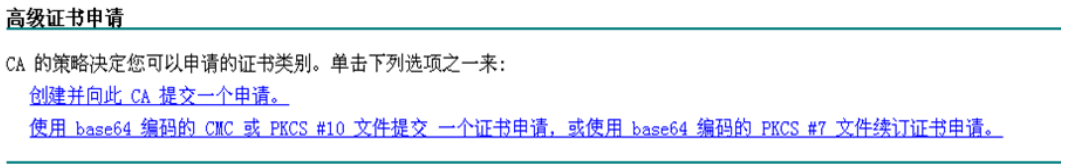
点击“高级证书申请”。

图3 高级证书申请



选择第一项：创建并向此 CA 提交一个申请。

图4 创建并向 CA 提交一个申请



填写相关信息。

a. 需要的证书类型，选择“客户端身份验证证书”；

b. 密钥选项的配置，勾选“标记密钥为可导出”前的复选框。

点击<提交>，弹出一提示框 ：在对话框中选择“是”。

点击安装此证书。

图5 安装证书

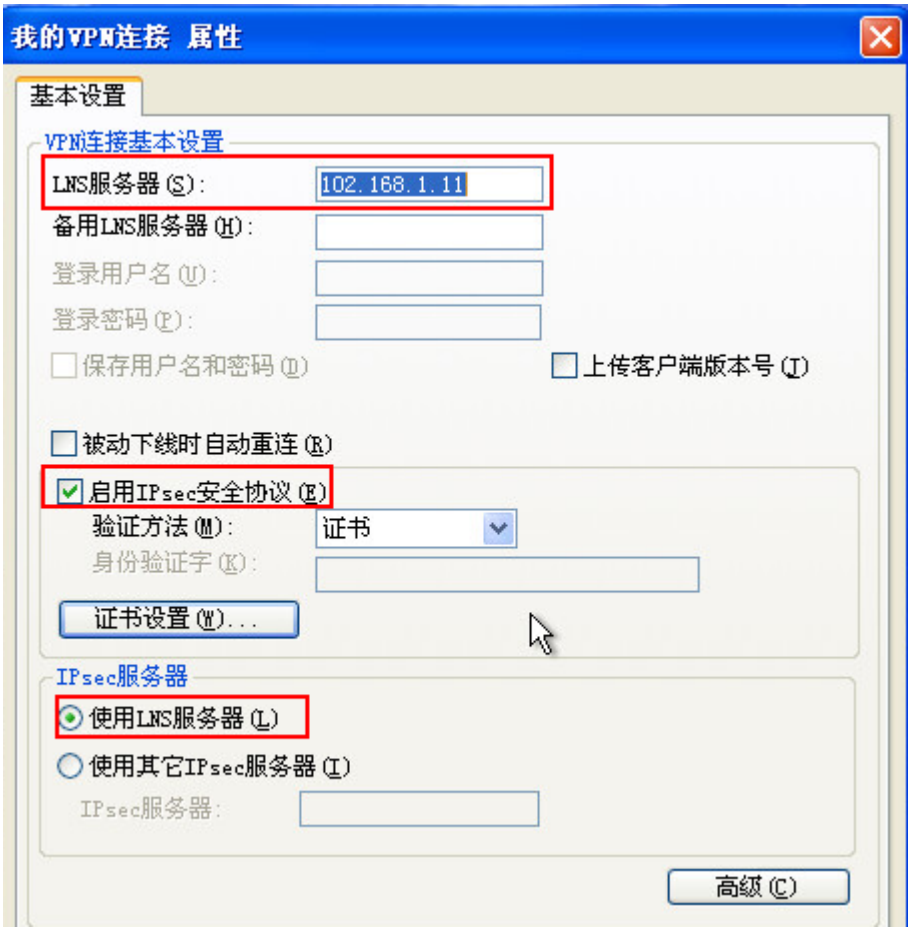
- iNode 客户端的配置（使用 iNode 版本为：iNode PC 5.2(E0409)）

  # 打开 L2TP VPN 连接，并单击“属性...(Y)”。

  图6 打开 L2TP 连接

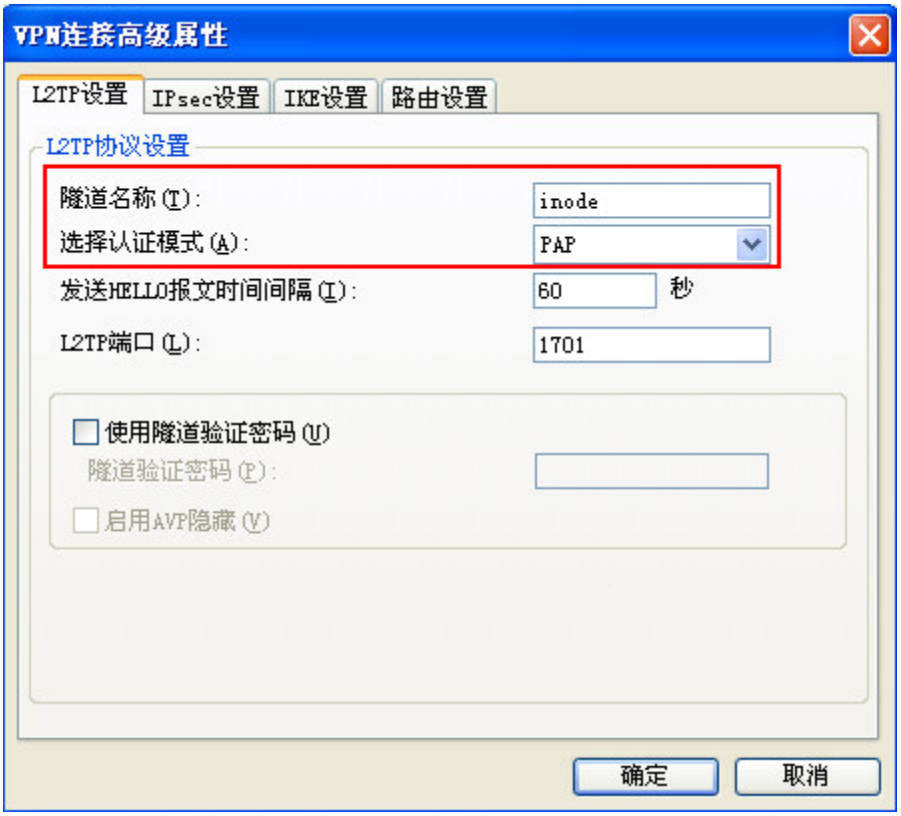
  # 输入 LNS 服务器的地址，并启用 IPsec 安全协议，验证证方法选择证书认证。

图7 基本配置



单击<高级(C)>按钮，进入“L2TP 设置”页签，设置 L2TP 参数如下图所示。

图8 L2TP 设置

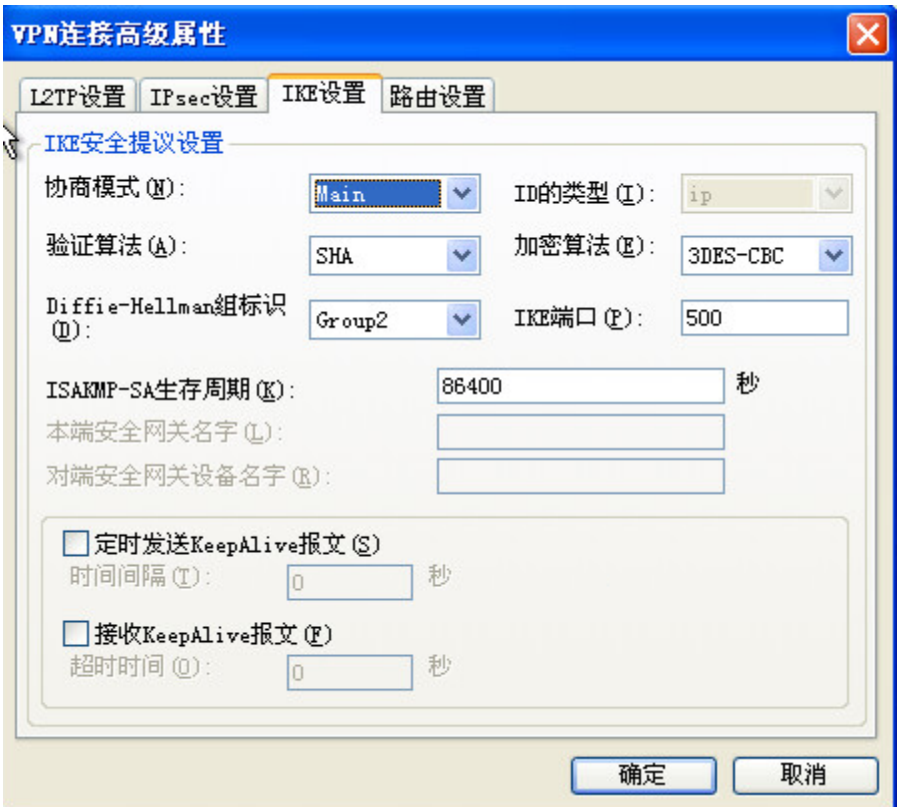


单击“IPsec 设置”页签，配置 IPsec 参数。

图9 IPsec 参数设置

单击“IKE 设置”页签，配置 IKE 参数。

图10 IKE 参数设置



单击“路由设置”页签，添加访问 Corporate network 的路由。

图11 路由设置

完成上述配置后，单击<确定>按钮，回到 L2TP 连接页面。

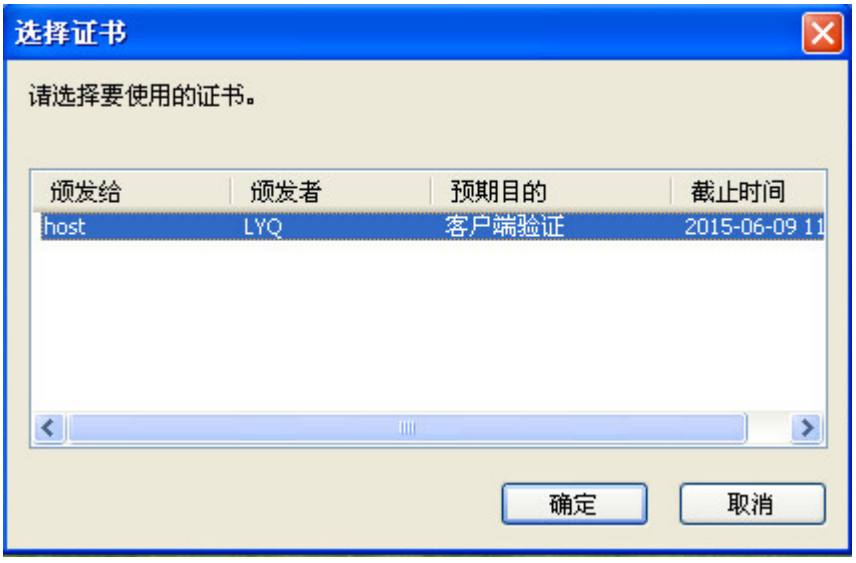
3.5 验证配置

在 L2TP 连接对话框中，输入用户名“l2tpuser”和密码“hello”，单击<连接>按钮。

图12 连接 L2TP

在弹出的对话框中选择申请好的证书，单击<确定>按钮。

图13 证书选择



通过下图可以看到 L2TP 连接成功。

图14 连接成功

图15 连接成功

在 Device 上使用 **display ike sa** 命令，可以看到 IPsec 隧道第一阶段的 SA 正常建立。

```
<Device> display ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
    10              102.168.1.1           RD           IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
```

在 Device 上使用 **display ipsec sa** 命令可以看到 IPsec SA 的建立情况。

```
<Device> display ipsec sa
-------------------------------
Interface: GigabitEthernet2/0/2
-------------------------------

  -----------------------------
  IPsec policy: policy1
  Sequence number: 1
  Mode: template
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect forward secrecy:
    Path MTU: 1443
    Tunnel:
        local  address: 102.168.1.11
        remote address: 102.168.1.1
    Flow:
    sour addr: 102.168.1.11/255.255.255.255  port: 1701  protocol: udp
    dest addr: 102.168.1.1/255.255.255.255  port: 0  protocol: udp

    [Inbound ESP SAs]
      SPI: 2187699078 (0x8265a386)
      Transform set:  ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843197/3294
      Max received sequence-number: 51
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active

    [Outbound ESP SAs]
      SPI: 3433374591 (0xcca5237f)
      Transform set:  ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843197/3294
      Max sent sequence-number: 52
      UDP encapsulation used for NAT traversal: N
      Status: Active
```

3.6 配置文件

```
#
interface Virtual-Template0
 ppp authentication-mode pap
 remote address 172.16.0.2
 ip address 172.16.0.1 255.255.255.0
#
interface GigabitEthernet2/0/1
 ip address 192.168.100.50 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 102.168.1.11 255.255.255.0
 ipsec apply policy policy1
#
interface GigabitEthernet2/0/3
 ip address 192.168.1.1 255.255.255.0
#
domain system
 authentication ppp local
#
local-user l2tpuser class network
 password cipher $c$3$nl46fURLtkCkcbdnB6irTXma+E6u0c+h
 service-type ppp
 authorization-attribute user-role network-operator
#
pki domain headgate
 ca identifier LYQ
 certificate request url http://192.168.1.51/certsrv/mscep/mscep.dll
 certificate request from ra
 certificate request entity security
 public-key rsa general name abc
 undo crl check enable
#
pki entity security
 common-name host
#
ipsec transform-set tran1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#
ipsec policy-template template1 1
 transform-set tran1
 ike-profile profile1
#
ipsec policy policy1 1 isakmp template template1
#
l2tp-group 1 mode lns
```

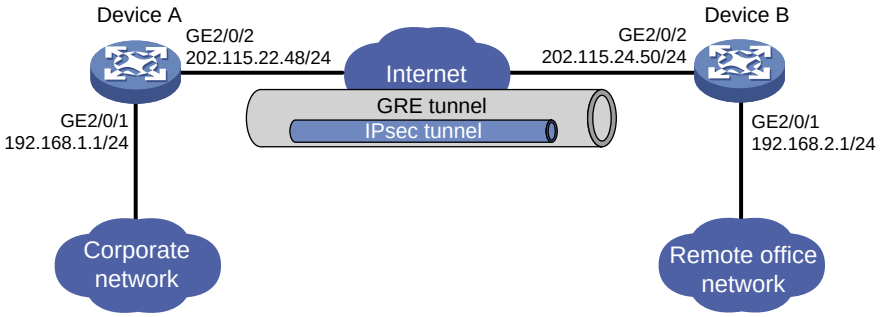
```
 allow l2tp virtual-template 0
 undo tunnel authentication
 tunnel name lns
#
 l2tp enable
#
ike signature-identity from-certificate
#
ike profile profile1
 certificate domain headgate
 local-identity dn
 match remote certificate device
 proposal 1
#
ike proposal 1
 authentication-method rsa-signature
 encryption-algorithm 3des-cbc
 dh group2
#
```

4 IPsec over GRE 的典型配置举例

4.1 组网需求

如图 16 所示，企业远程办公网络通过 IPsec VPN 接入企业总部，要求：通过 GRE 隧道传输两网络之间的 IPsec 加密数据。

图16 IPsec over GRE 组网图



4.2 配置思路

- 为了对数据先进行 IPsec 处理，再进行 GRE 封装，访问控制列表需匹配数据的原始范围，并且要将 IPsec 应用到 GRE 隧道接口上。
- 为了对网络间传输的数据先进行 IPsec 封装，再进行 GRE 封装，需要配置 IPsec 隧道的对端 IP 地址为 GRE 隧道的接口地址。

4.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.4 配置步骤

4.4.1 Device A 的配置

(1) 配置各接口 IP 地址。

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 192.168.1.1 255.255.255.0
[DeviceA-GigabitEthernet2/0/1] tcp mss 1350
[DeviceA-GigabitEthernet2/0/1] quit
```

配置接口 GigabitEthernet2/0/2 的 IP 地址。

```
[DeviceA] interface gigabitethernet 2/0/2
[DeviceA-GigabitEthernet2/0/2] ip address 202.115.22.48 255.255.255.0
[DeviceA-GigabitEthernet2/0/2] quit
```

(2) 配置 GRE 隧道。

创建 Tunnel0 接口，并指定隧道模式为 GRE over IPv4 隧道。

```
[DeviceA] interface tunnel 0 mode gre
```

配置 Tunnel0 接口的 IP 地址为 10.1.1.1/24。

```
[DeviceA-Tunnel0] ip address 10.1.1.1 255.255.255.0
```

配置 Tunnel0 接口的源端地址为 202.115.22.48/24（Device A 的 GigabitEthernet2/0/2 的 IP 地址）。

```
[DeviceA-Tunnel0] source 202.115.22.48
```

配置 Tunnel0 接口的目的端地址为 202.115.24.50/24（Device B 的 GigabitEthernet2/0/2 的 IP 地址）。

```
[DeviceA-Tunnel0] destination 202.115.24.50
[DeviceA-Tunnel0] quit
```

配置从 Device A 经过 Tunnel0 接口到 Remote office network 的静态路由。

```
[DeviceA] ip route-static 192.168.2.1 255.255.255.0 tunnel 0
```

(3) 配置 IPsec VPN。

配置 IKE keychain。

```
[DeviceA] ike keychain keychain1
[DeviceA-ike-keychain-keychain1] pre-shared-key address 10.1.1.2 255.255.255.0 key
simple 123
[DeviceA-ike-keychain-keychain1] quit
```

创建 ACL3000，定义需要 IPsec 保护的数据流。

```
[DeviceA] acl advanced 3000
[DeviceA-acl-ipv4-adv-3000] rule 0 permit ip source 192.168.1.0 0.0.0.255 destination
192.168.2.0 0.0.0.255
[DeviceA-acl-ipv4-adv-3000] quit
```

配置 IPsec 安全提议。

```
[DeviceA] ipsec transform-set tran1
[DeviceA-ipsec-transform-set-tran1] esp encryption-algorithm des
[DeviceA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceA-ipsec-transform-set-tran1] quit
```

创建一条 IKE 协商方式的 IPsec 安全策略，名称为 policy1，序列号为 1。

```
[DeviceA] ipsec policy policy1 1 isakmp
[DeviceA-ipsec-policy-isakmp-policy1-1] security acl 3000
[DeviceA-ipsec-policy-isakmp-policy1-1] remote-address 10.1.1.2
[DeviceA-ipsec-policy-isakmp-policy1-1] transform-set tran1
[DeviceA-ipsec-policy-isakmp-policy1-1] quit
```

在 GRE 隧道接口上应用安全策略。

```
[DeviceA] interface tunnel 0
[DeviceA-Tunnel0] ipsec apply policy policy1
[DeviceA-Tunnel0] quit
```

4.4.2 Device B 的配置

(1) 配置各接口 IP 地址。

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<DevoceB> system-view
[DeviceB] interface gigabitethernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] ip address 192.168.2.1 255.255.255.0
[DeviceB-GigabitEthernet2/0/1] tcp mss 1350
[DeviceB-GigabitEthernet2/0/1] quit
```

配置接口 GigabitEthernet2/0/2 的 IP 地址。

```
[DeviceB] interface gigabitethernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] ip address 202.115.24.50 255.255.255.0
[DeviceB-GigabitEthernet2/0/2] quit
```

(2) 配置 GRE 隧道。

创建 Tunnel0 接口，并指定隧道模式为 GRE over IPv4 隧道。

```
[DeviceB] interface tunnel 0 mode gre
```

配置 Tunnel0 接口的 IP 地址为 10.1.1.2/24。

```
[DeviceB-Tunnel0] ip address 10.1.1.2 255.255.255.0
```

配置 Tunnel0 接口的源端地址为 202.115.24.50/24（Device B 的 GigabitEthernet2/0/2 的 IP 地址）。

```
[DeviceB-Tunnel0] source 202.115.24.50
```

配置 Tunnel0 接口的目的端地址为 202.115.22.48/24（Device A 的 GigabitEthernet2/0/2 的 IP 地址）。

```
[DeviceB-Tunnel0] destination 202.115.22.48
[DeviceB-Tunnel0] quit
```

配置从 DeviceB 经过 Tunnel0 接口到 Corporate network 的静态路由。

```
[DeviceB] ip route-static 192.168.1.1 255.255.255.0 tunnel 0
```

(3) 配置 IPsec VPN。

配置 IKE keychain。

```
[DeviceB] ike keychain keychain1
```

```
[DeviceB-ike-keychain-keychain1] pre-shared-key address 10.1.1.1 255.255.255.0 key
simple 123
[DeviceB-ike-keychain-keychain1] quit
```

创建 ACL3000，定义需要 IPsec 保护的数据流。

```
[DeviceB] acl advanced 3000
[DeviceB-acl-ipv4-adv-3000] rule 0 permit ip source 192.168.2.0 0.0.0.255 destination
192.168.1.0 0.0.0.255
[DeviceB-acl-ipv4-adv-3000] quit
```

配置 IPsec 安全提议。

```
[DeviceB] ipsec transform-set tran1
[DeviceB-ipsec-transform-set-tran1] esp encryption-algorithm des
[DeviceB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceB-ipsec-transform-set-tran1] quit
```

创建一条 IKE 协商方式的 IPsec 安全策略，名称为 policy1，序列号为 1。

```
[DeviceB] ipsec policy policy1 1 isakmp
[DeviceB-ipsec-policy-isakmp-policy1-1] security acl 3000
[DeviceB-ipsec-policy-isakmp-policy1-1] remote-address 10.1.1.1
[DeviceB-ipsec-policy-isakmp-policy1-1] transform-set tran1
[DeviceB-ipsec-policy-isakmp-policy1-1] quit
```

在 GRE 隧道接口上应用安全策略。

```
[DeviceB] interface tunnel 0
[DeviceB-Tunnel0] ipsec apply policy policy1
[DeviceB-Tunnel0] quit
```

4.5 验证配置

以 Corporate network 的主机 192.168.1.2 向 Remote office network 的主机 192.168.2.2 发起通信为例，从 192.168.1.2 ping 192.168.2.2，会触发 IPsec 协商，建立 IPsec 隧道，在成功建立 IPsec 隧道后，可以 ping 通。

```
C:\Users\corporatenetwork>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.2.2: bytes=32 time=2ms TTL=254
Reply from 192.168.2.2: bytes=32 time=2ms TTL=254
Reply from 192.168.2.2: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

在 Device A 上使用 **display ike sa** 命令，可以看到第一阶段的 SA 正常建立。

```
<DeviceA> display ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
    1               10.1.1.2              RD           IPSEC
Flags:
```

```
RD--READY RL--REPLACED FD-FADING
```

在 Device A 上使用 **display ipsec sa** 命令可以看到 IPsec SA 的建立情况。

```
<DeviceA> display ipsec sa
------------------------------
Interface: Tunnel0
------------------------------

  ----------------------------
  IPsec policy: policy1
  Sequence number: 1
  Mode: isakmp
  ----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect forward secrecy:
    Path MTU: 1419
    Tunnel:
        local  address: 10.1.1.1
        remote address: 10.1.1.2
    Flow:
    sour addr: 192.168.1.1/255.255.255.255  port: 0  protocol: ip
    dest addr: 192.168.2.1/255.255.255.255  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 3128557135 (0xba79fe4f)
      Transform set:  ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3550
      Max received sequence-number: 3
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active

    [Outbound ESP SAs]
      SPI: 2643166978 (0x9d8b8702)
      Transform set:  ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3550
      Max sent sequence-number: 3
      UDP encapsulation used for NAT traversal: N
      Status: Active
```

在 Device A 上通过命令 display interface tunnel 0 可以查看经过 GRE 隧道传输的流量情况。

```
<DeviceA> display interface tunnel 0
Tunnel0
Current state: UP
Line protocol state: UP
Description: Tunnel0 Interface
```

```
Bandwidth: 64kbps
Maximum Transmit Unit: 1476
Internet Address is 10.1.1.1/24 Primary
Tunnel source 202.115.22.48, destination 202.115.24.50
Tunnel keepalive disabled
Tunnel TTL 255
Tunnel protocol/transport GRE/IP
    GRE key disabled
    Checksumming of GRE packets disabled
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 40 packets, 3300 bytes, 0 drops
Output: 41 packets, 3464 bytes, 0 drops
```

从 Remote office network 的主机向 Corporate network 的主机发起通信验证方法相同，此不赘述。

4.6 配置文件

- Device A：

```
#
interface GigabitEthernet2/0/1
 ip address 192.168.1.1 255.255.255.0
 tcp mss 1350
#
interface GigabitEthernet2/0/2
 ip address 202.115.22.48 255.255.255.0
#
interface Tunnel0 mode gre
 ip address 10.1.1.1 255.255.255.0
 source 202.115.22.48
 destination 202.115.24.50
 ipsec apply policy policy1
#
ip route-static 192.168.2.0 24 Tunnel0
#
acl advanced 3000
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
#
ipsec transform-set tran1
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec policy policy1 1 isakmp
 transform-set tran1
 security acl 3000
```

```
 remote-address 10.1.1.2
#
ike keychain keychain1
 pre-shared-key address 10.1.1.2 255.255.255.0 key cipher $c$3$n6jdlYtuR+K6mijQ8
qp4hMMjV/iteA==
#
```

- Devoce B

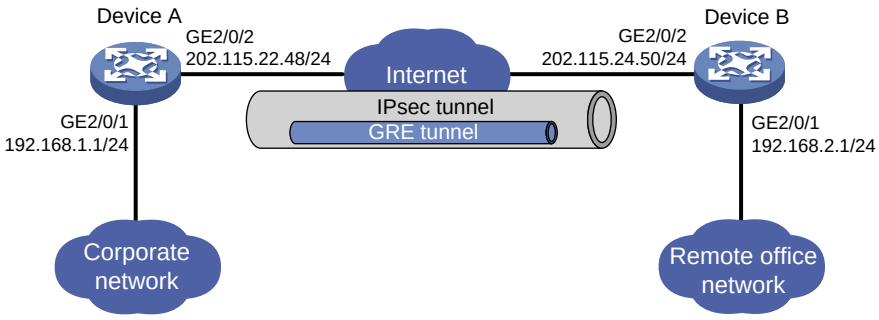
```
#
interface GigabitEthernet2/0/1
 ip address 192.168.2.1 255.255.255.0
 tcp mss 1350
#
interface GigabitEthernet2/0/2
 ip address 202.115.22.50 255.255.255.0
#
interface Tunnel0 mode gre
 ip address 10.1.1.2 255.255.255.0
 source 202.115.24.50
 destination 202.115.22.48
 ipsec apply policy policy1
#
ip route-static 192.168.1.1 24 Tunnel0
#
acl advanced 3000
 rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
ipsec transform-set tran1
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec policy policy1 1 isakmp
 transform-set tran1
 security acl 3000
 remote-address 10.1.1.1
#
ike keychain keychain1
 pre-shared-key address 10.1.1.1 255.255.255.0 key cipher $c$3$n6jdlYtuR+K6mijQ8
qp4hMMjV/iteA==
#
```

5 GRE over IPsec 的典型配置举例

5.1 组网需求

如图 17所示，企业远程办公网络通过 GRE 隧道与企业总部传输数据，要求：对通过 GRE 隧道的数据进行 IPsec 加密处理。

图17 GRE over IPsec 组网图



5.2 配置思路

- 为了对经 GRE 封装的数据进行 IPsec 加密，将 IPsec 策略应用在物理接口上，访问控制列表源和目的地址为物理接口地址。
- 为了使 IPsec 保护整个 GRE 隧道，本端和对端应用 IPsec 策略的接口分别为 GRE 隧道的源和目的接口。

5.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

5.4 配置步骤

5.4.1 Device A 的配置

(1) 配置各接口 IP 地址。

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 192.168.1.1 255.255.255.0
[DeviceA-GigabitEthernet2/0/1] quit
```

配置接口 GigabitEthernet2/0/2 的 IP 地址。

```
[DeviceA] interface gigabitethernet 2/0/2
[DeviceA-GigabitEthernet2/0/2] ip address 202.115.22.48 255.255.255.0
[DeviceA-GigabitEthernet2/0/2] quit
```

(2) 配置 GRE 隧道。

创建 Tunnel0 接口，并指定隧道模式为 GRE over IPv4 隧道。

```
[DeviceA] interface tunnel 0 mode gre
```

配置 Tunnel0 接口的 IP 地址为 10.1.1.1/24。

```
[DeviceA-Tunnel0] ip address 10.1.1.1 255.255.255.0
```

配置 Tunnel0 接口的源端地址为 202.115.22.48/24（Device A 的 GigabitEthernet2/0/2 的 IP 地址）。

```
[DeviceA-Tunnel0] source 202.115.22.48
```

配置 Tunnel0 接口的目的端地址为 202.115.24.50/24（Device B 的 GigabitEthernet2/0/2 的 IP 地址）。

```
[DeviceA-Tunnel0] destination 202.115.24.50
[DeviceA-Tunnel0] quit
```

配置从 Device A 经过 Tunnel0 接口到 Remote office network 的静态路由。

```
[DeviceA] ip route-static 192.168.2.1 255.255.255.0 tunnel 0
```

(3) 配置 IPsec VPN。

配置 IKE keychain。

```
[DeviceA] ike keychain keychain1
[DeviceA-ike-keychain-keychain1] pre-shared-key address 202.115.24.50 255.255.255.0
key simple 123
[DeviceA-ike-keychain-keychain1] quit
```

创建 ACL3000，定义需要 IPsec 保护的数据流。

```
[DeviceA] acl advanced 3000
[DeviceA-acl-ipv4-adv-3000] rule 0 permit gre source 202.115.22.48 0 destination
202.115.24.50 0
[DeviceA-acl-ipv4-adv-3000] quit
```

配置 IPsec 安全提议。

```
[DeviceA] ipsec transform-set tran1
[DeviceA-ipsec-transform-set-tran1] esp encryption-algorithm des
[DeviceA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceA-ipsec-transform-set-tran1] quit
```

创建一条 IKE 协商方式的 IPsec 安全策略，名称为 policy1，序列号为 1。

```
[DeviceA] ipsec policy policy1 1 isakmp
[DeviceA-ipsec-policy-isakmp-policy1-1] security acl 3000
[DeviceA-ipsec-policy-isakmp-policy1-1] remote-address 202.115.24.50
[DeviceA-ipsec-policy-isakmp-policy1-1] transform-set tran1
[DeviceA-ipsec-policy-isakmp-policy1-1] quit
```

在接口 GigabitEthernet2/0/2 上应用安全策略。

```
[DeviceA] interface gigabitethernet 2/0/2
[DeviceA-GigabitEthernet2/0/2] ipsec apply policy policy1
[DeviceA-GigabitEthernet2/0/2] quit
```

5.4.2 Device B 的配置

(1) 配置各接口 IP 地址

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] ip address 192.168.2.1 255.255.255.0
[DeviceB-GigabitEthernet2/0/1] quit
```

配置接口 GigabitEthernet2/0/2 的 IP 地址。

```
[DeviceB] interface gigabitethernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] ip address 202.115.24.50 255.255.255.0
[DeviceB-GigabitEthernet2/0/2] quit
```

(2) 配置 GRE 隧道。

创建 Tunnel0 接口，并指定隧道模式为 GRE over IPv4 隧道。

```
[DeviceB] interface tunnel 0 mode gre
```

配置 Tunnel0 接口的 IP 地址为 10.1.1.2/24。

```
[DeviceB-Tunnel0] ip address 10.1.1.2 255.255.255.0
```

配置 Tunnel0 接口的源端地址为 202.115.24.50/24（Device B 的 GigabitEthernet2/0/2 的 IP 地址）。

```
[DeviceB-Tunnel0] source 202.115.24.50
```

配置 Tunnel0 接口的目的端地址为 202.115.22.48/24（Device A 的 GigabitEthernet2/0/2 的 IP 地址）。

```
[DeviceB-Tunnel0] destination 202.115.22.48
[DeviceB-Tunnel0] quit
```

配置从 DeviceB 经过 Tunnel0 接口到 Corporate network 的静态路由。

```
[DeviceB] ip route-static 192.168.1.1 255.255.255.0 tunnel 0
```

(3) 配置 IPsec VPN

配置 IKE keychain。

```
[DeviceB] ike keychain keychain1
[DeviceB-ike-keychain-keychain1] pre-shared-key address 202.115.22.48 255.255.255.0
key simple 123
[DeviceB-ike-keychain-keychain1] quit
```

创建 ACL3000，定义需要 IPsec 保护的数据流。

```
[DeviceB] acl advanced 3000
[DeviceB-acl-ipv4-adv-3000] rule 0 permit gre source 202.115.24.50 0 destination
202.115.22.48 0
[DeviceB-acl-ipv4-adv-3000] quit
```

配置 IPsec 安全提议。

```
[DeviceB] ipsec transform-set tran1
[DeviceB-ipsec-transform-set-tran1] esp encryption-algorithm des
[DeviceB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceB-ipsec-transform-set-tran1] quit
```

创建一条 IKE 协商方式的 IPsec 安全策略，名称为 policy1，序列号为 1。

```
[DeviceB] ipsec policy policy1 1 isakmp
[DeviceB-ipsec-policy-isakmp-policy1-1] security acl 3000
[DeviceB-ipsec-policy-isakmp-policy1-1] remote-address 202.115.22.48
[DeviceB-ipsec-policy-isakmp-policy1-1] transform-set tran1
[DeviceB-ipsec-policy-isakmp-policy1-1] quit
```

在接口 GigabitEthernet2/0/2 上应用安全策略。

```
[DeviceB] interface gigabitethernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] ipsec apply policy policy1
[DeviceB-GigabitEthernet2/0/2] quit
```

5.5 验证配置

以 Corporate network 的主机 192.168.1.2 向 Remote office network 的主机 192.168.2.2 发起通信为例，从 192.168.1.2 ping 192.168.2.2，会触发 IPsec 协商，建立 IPsec 隧道，在成功建立 IPsec 隧道后，可以 ping 通。

```
C:\Users\corporatenetwork> ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.2.2: bytes=32 time=2ms TTL=254
Reply from 192.168.2.2: bytes=32 time=2ms TTL=254
Reply from 192.168.2.2: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

在 Device A 上使用 **display ike sa** 命令，可以看到第一阶段的 SA 正常建立。

```
<DeviceA> display ike sa
    Connection-ID   Remote                Flag         DOI
-------------------------------------------------------------------
    2               202.115.22.49         RD           IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
```

在 Device A 上使用 **display ipsec sa** 命令可以看到 IPsec SA 的建立情况。

```
<DeviceA> display ipsec sa
------------------------------
Interface: GigabitEthernet2/0/2
------------------------------

  ----------------------------
  IPsec policy: policy1
  Sequence number: 1
  Mode: isakmp
  ----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect forward secrecy:
    Path MTU: 1443
    Tunnel:
        local  address: 202.115.22.48
        remote address: 202.115.24.50
    Flow:
    sour addr: 202.115.22.48/255.255.255.255  port: 0  protocol: gre
    dest addr: 202.115.24.50/255.255.255.255  port: 0  protocol: gre

    [Inbound ESP SAs]
      SPI: 2130348402 (0x7efa8972)
      Transform set:  ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3573
      Max received sequence-number: 3
      Anti-replay check enable: Y
```

```
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: Active

  [Outbound ESP SAs]
    SPI: 2811839266 (0xa7994322)
    Transform set:  ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3573
    Max sent sequence-number: 3
    UDP encapsulation used for NAT traversal: N
    Status: Active
```

在 Device A 上通过命令 display interface tunnel 0 可以查看经过 GRE 隧道传输的流量情况。

```
<DeviceA> display interface tunnel 0
Tunnel0
Current state: UP
Line protocol state: UP
Description: Tunnel0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1476
Internet Address is 10.1.1.1/24 Primary
Tunnel source 202.115.22.48, destination 202.115.24.50
Tunnel keepalive disabled
Tunnel TTL 255
Tunnel protocol/transport GRE/IP
    GRE key disabled
    Checksumming of GRE packets disabled
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 43 packets, 3480 bytes, 0 drops
Output: 45 packets, 3740 bytes, 2 drops
```

从 Remote office network 的主机向 Corporate network 的主机发起通信验证方法相同，此不赘述。

5.6 配置文件

- Device A：

```
#
interface GigabitEthernet2/0/1
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 202.115.22.48 255.255.255.0
ipsec apply policy policy1
#
```

```
interface Tunnel0 mode gre
 ip address 10.1.1.1 255.255.255.0
 source 202.115.22.48
 destination 202.115.24.50
#
ip route-static 192.168.2.0 24 Tunnel0
#
acl advanced 3000
 rule 0 permit gre source 202.115.22.48 0 destination 202.115.24.50 0
#
ipsec transform-set tran1
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec policy policy1 1 isakmp
 transform-set tran1
 security acl 3000
 remote-address 202.115.24.50
#
ike keychain keychain1
 pre-shared-key address 202.115.24.50 255.255.255.0 key cipher $c$3$n6jdlYtuR+K6mijQ8
qp4hMMjV/iteA==
#
```

- Devoce B

```
#
interface GigabitEthernet2/0/1
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 202.115.24.50 255.255.255.0
ipsec apply policy policy1
#
interface Tunnel0 mode gre
 ip address 10.1.1.2 255.255.255.0
 source 202.115.24.50
 destination 202.115.22.48
#
ip route-static 192.168.1.1 24 Tunnel0
#
acl advanced 3000
 rule 0 permit ip source 202.115.24.50 0 destination 202.115.22.48 0
#
ipsec transform-set tran1
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec policy policy1 1 isakmp
 transform-set tran1
```

```
 security acl 3000
 remote-address 202.115.22.48
#
ike keychain keychain1
 pre-shared-key address 202.115.22.48 255.255.255.0 key cipher $c$3$n6jdlYtuR+K6mijQ8
qp4hMMjV/iteA==
#
```

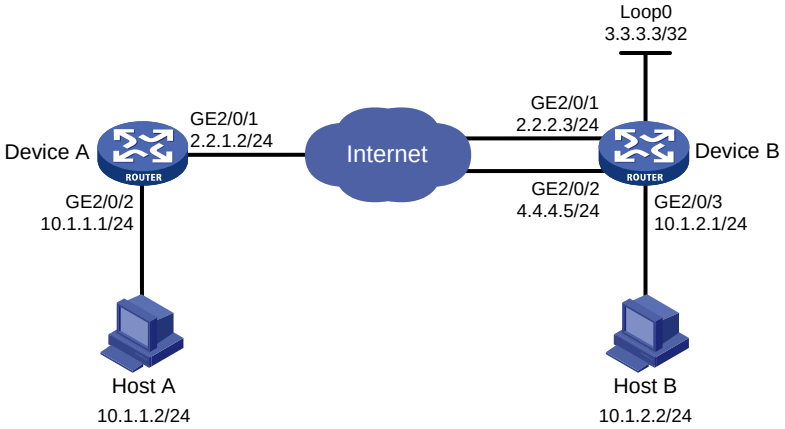
6 IPsec 同流双隧道的典型配置举例

6.1 组网需求

如图 18 所示组网，要求：

- 在 Device A 和 Device B 之间建立 IPsec 隧道，对 Host A 所在的子网（10.1.1.0/24）与 Host B 所在的子网（10.1.2.0/24）之间的数据流进行安全保护。
- Device B 上通过两条链路接入互联网，在这两条链路上配置相同的 IPsec 隧道形成备份。
- 使用 IKE 自动协商方式建立 SA，安全协议采用 ESP 协议，加密算法采用 DES，认证算法采用 SHA1-HMAC-96。
- 在 Device B 上配置共享源接口安全策略，实现数据流量在不同接口间平滑切换。

图18 IPsec 同流双隧道组网图



6.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

6.3 配置步骤

6.3.1 Device A 的配置

(1) 配置各接口 IP 地址

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 2.2.1.2 255.255.255.0
[DeviceA-GigabitEthernet2/0/1] quit
```

配置接口 GigabitEthernet2/0/2 的 IP 地址。

```
[DeviceA] interface gigabitethernet 2/0/2
[DeviceA-GigabitEthernet2/0/2] ip address 10.1.1.1 255.255.255.0
[DeviceA-GigabitEthernet2/0/2] quit
```

配置访问 10.1.2.0 网段的静态路由。

```
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 2.2.2.3
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 4.4.4.5
```

配置到 Device B 上 Loopback0 接口的静态路由。

```
[DeviceA] ip route-static 3.3.3.3 255.255.255.255 2.2.2.3
[DeviceA] ip route-static 3.3.3.3 255.255.255.255 4.4.4.5
```

(2) 配置 IPsec VPN

配置 IKE keychain。

```
[DeviceA] ike keychain keychain1
[DeviceA-ike-keychain-keychain1] pre-shared-key address 3.3.3.3 255.255.255.255 key
simple 123
[DeviceA-ike-keychain-keychain1] quit
```

创建 ACL3000，定义需要 IPsec 保护的数据流。

```
[DeviceA] acl advanced 3000
[DeviceA-acl-ipv4-adv-3000] rule 0 permit ip source 10.1.1.0 0.0.0.255 destination
10.1.2.0 0.0.0.255
[DeviceA-acl-ipv4-adv-3000] quit
```

配置 IPsec 安全提议。

```
[DeviceA] ipsec transform-set tran1
[DeviceA-ipsec-transform-set-tran1] esp encryption-algorithm des
[DeviceA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceA-ipsec-transform-set-tran1] quit
```

创建一条 IKE 协商方式的 IPsec 安全策略，名称为 policy1，序列号为 1。

```
[DeviceA] ipsec policy policy1 1 isakmp
[DeviceA-ipsec-policy-isakmp-policy1-1] security acl 3000
[DeviceA-ipsec-policy-isakmp-policy1-1] remote-address 3.3.3.3
[DeviceA-ipsec-policy-isakmp-policy1-1] transform-set tran1
[DeviceA-ipsec-policy-isakmp-policy1-1] quit
```

在接口 GigabitEthernet2/0/1 上应用安全策略。

```
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ipsec apply policy policy1
[DeviceA-GigabitEthernet2/0/1] quit
```

6.3.2 Device B 的配置

(1) 配置各接口 IP 地址

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<DeviceB> system-view
```

```
[DeviceB] interface gigabitethernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] ip address 2.2.2.3 255.255.255.0
[DeviceB-GigabitEthernet2/0/1] quit
```

配置接口 GigabitEthernet2/0/2 的 IP 地址。

```
[DeviceB] interface gigabitethernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] ip address 4.4.4.5 255.255.255.0
[DeviceB-GigabitEthernet2/0/2] quit
```

配置接口 GigabitEthernet2/0/3 的 IP 地址。

```
[DeviceB] interface gigabitethernet 2/0/3
[DeviceB-GigabitEthernet2/0/3] ip address 10.1.2.1 255.255.255.0
[DeviceB-GigabitEthernet2/0/3] quit
```

配置接口 Loopback 0 的 IP 地址。

```
[DeviceB] interface loopback 0
[DeviceB-LoopBack0] ip address 3.3.3.3 255.255.255.0
[DeviceB-LoopBack0] quit
```

配置访问 10.1.1.0 网段的静态路由。

```
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 gigabitethernet 2/0/1 2.2.1.2
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 gigabitethernet 2/0/2 2.2.1.2
```

(2) 配置 IPsec VPN

配置 IKE keychain。

```
[DeviceB] ike keychain keychain1
[DeviceB-ike-keychain-keychain1] pre-shared-key address 2.2.1.2 255.255.255.0 key
simple 123
[DeviceB-ike-keychain-keychain1] quit
```

创建 ACL3000，定义需要 IPsec 保护的数据流。

```
[DeviceB] acl advanced 3000
[DeviceB-acl-ipv4-adv-3000] rule 0 permit ip source 10.1.2.0 0.0.0.255 destination
10.1.1.0 0.0.0.255
[DeviceB-acl-ipv4-adv-3000] quit
```

配置 IPsec 安全提议。

```
[DeviceB] ipsec transform-set tran1
[DeviceB-ipsec-transform-set-tran1] esp encryption-algorithm des
[DeviceB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceB-ipsec-transform-set-tran1] quit
```

创建一条 IKE 协商方式的 IPsec 安全策略，名称为 policy1，序列号为 1。

```
[DeviceB] ipsec policy policy1 1 isakmp
[DeviceB-ipsec-policy-isakmp-policy1-1] security acl 3000
[DeviceB-ipsec-policy-isakmp-policy1-1] remote-address 2.2.1.2
[DeviceB-ipsec-policy-isakmp-policy1-1] transform-set tran1
[Device-ipsec-policy-isakmp-policy1-1] quit
```

在接口 GigabitEthernet2/0/1 上应用安全策略。

```
[DeviceB] interface gigabitethernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] ipsec apply policy policy1
[DeviceB-GigabitEthernet2/0/1] quit
```

在接口 GigabitEthernet2/0/2 上应用安全策略。

```
[DeviceB] interface gigabitethernet 2/0/2
```

```
[DeviceB-GigabitEthernet2/0/2] ipsec apply policy policy1
[DeviceB-GigabitEthernet2/0/2] quit
```

配置 IPsec 安全策略 policy1 为共享源接口安全策略，共享源接口为 Loopback0。

```
[DeviceB] ipsec policy policy1 local-address loopback 0
```

6.4 验证配置

从 Host A ping Host B，会触发 IPsec 协商，建立 IPsec 隧道，在成功建立 IPsec 隧道后，可以 ping 通。

```
C:\Users\hosta>ping 10.1.2.2

Pinging 10.1.2.2 with 32 bytes of data:
Request timed out.
Reply from 10.1.2.2: bytes=32 time=3ms TTL=126
Reply from 10.1.2.2: bytes=32 time=1ms TTL=126
Reply from 10.1.2.2: bytes=32 time=5ms TTL=126

Ping statistics for 10.1.2.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 3ms
```

在 Device A 上使用 **display ike sa** 命令，可以看到第一阶段的 SA 正常建立。

```
[DeviceA] display ike sa
    Connection-ID   Remote                Flag         DOI
-------------------------------------------------------------------
    9               3.3.3.3               RD           IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
```

在 Device A 上使用 **display ipsec sa** 命令可以看到 IPsec SA 的建立情况。

```
[DeviceA] display ipsec sa
------------------------------
Interface: GigabitEthernet2/0/1
------------------------------

  ----------------------------
  IPsec policy: policy1
  Sequence number: 1
  Mode: isakmp
  ----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect forward secrecy:
    Path MTU: 1443
    Tunnel:
        local  address: 2.2.1.2
        remote address: 3.3.3.3
    Flow:
```

```
sour addr: 10.1.1.0/255.255.255.0  port: 0  protocol: ip
dest addr: 10.1.2.0/255.255.255.0  port: 0  protocol: ip

[Inbound ESP SAs]
  SPI: 1851852454 (0x6e6106a6)
  Transform set:  ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
  SA duration (kilobytes/sec): 1843200/3600
  SA remaining duration (kilobytes/sec): 1843199/3035
  Max received sequence-number: 3
  Anti-replay check enable: Y
  Anti-replay window size: 64
  UDP encapsulation used for NAT traversal: N
  Status: Active

[Outbound ESP SAs]
  SPI: 718692851 (0x2ad661f3)
  Transform set:  ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
  SA duration (kilobytes/sec): 1843200/3600
  SA remaining duration (kilobytes/sec): 1843199/3035
  Max sent sequence-number: 3
  UDP encapsulation used for NAT traversal: N
  Status: Active
```

从 Host B 向 Host A 发起通信验证方法相同，此不赘述。

当 Device B 侧的 GigabitEthernet2/0/1 接口所在链路中断时，上述 IPsec 隧道依然存在，用户业务数据继续被保护不会中断。

6.5 配置文件

- Device A：

```
#
interface GigabitEthernet2/0/1
 ip address 2.2.1.2 255.255.255.0
ipsec apply policy policy1
#
interface GigabitEthernet2/0/2
 ip address 10.1.1.1 255.255.255.0
#
ip route-static 3.3.3.3 32 2.2.2.3
ip route-static 3.3.3.3 32 4.4.4.5
ip route-static 10.1.2.0 24 2.2.2.3
ip route-static 10.1.2.0 24 4.4.4.5
#
acl advanced 3000
 rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec transform-set tran1
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
```

```
#
ipsec policy policy1 1 isakmp
 transform-set tran1
 security acl 3000
 remote-address 3.3.3.3
#
ike keychain keychain1
 pre-shared-key address 3.3.3.3 255.255.255.255 key cipher $c$3$n6jdlYtuR+K6mijQ8
qp4hMMjV/iteA==
#
```

- Device B：

```
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.0
#
interface GigabitEthernet2/0/1
 ip address 2.2.2.3 255.255.255.0
ipsec apply policy policy1
#
interface GigabitEthernet2/0/2
 ip address 4.4.4.5 255.255.255.0
ipsec apply policy policy1
#
interface GigabitEthernet2/0/3
 ip address 10.1.2.1 255.255.255.0
#
ip route-static 10.1.1.0 24 GigabitEthernet2/0/1 2.2.1.2
ip route-static 10.1.1.0 24 GigabitEthernet2/0/2 2.2.1.2
#
acl advanced 3000
 rule 0 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec transform-set tran1
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec policy policy1 1 isakmp
 transform-set tran1
 security acl 3000
 remote-address 2.2.1.2
#
ipsec policy policy1 local-address LoopBack0
#
ike keychain keychain1
 pre-shared-key address 2.2.1.2 255.255.255.0 key cipher $c$3$n6jdlYtuR+K6mijQ8
qp4hMMjV/iteA==
#
```

7 相关资料

- H3C SR6600 SR6600-X 路由器 安全配置指导-R7607
- H3C SR6600 SR6600-X 路由器 安全命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

IPv6 IS-IS 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 配置举例 1
3.1 组网需求 1
3.2 配置思路 2
3.3 使用版本 2
3.4 配置步骤 2
3.4.1 Router A 的配置 2
3.4.2 Router B 的配置 3
3.4.3 Router C 的配置 3
3.4.4 Router D 的配置 4
3.4.5 Router E 的配置 5
3.5 验证配置 5
3.6 配置文件 7
4 相关资料 9

1 简介

本文档介绍 IPv6 IS-IS 配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 IPv6 IS-IS 特性。

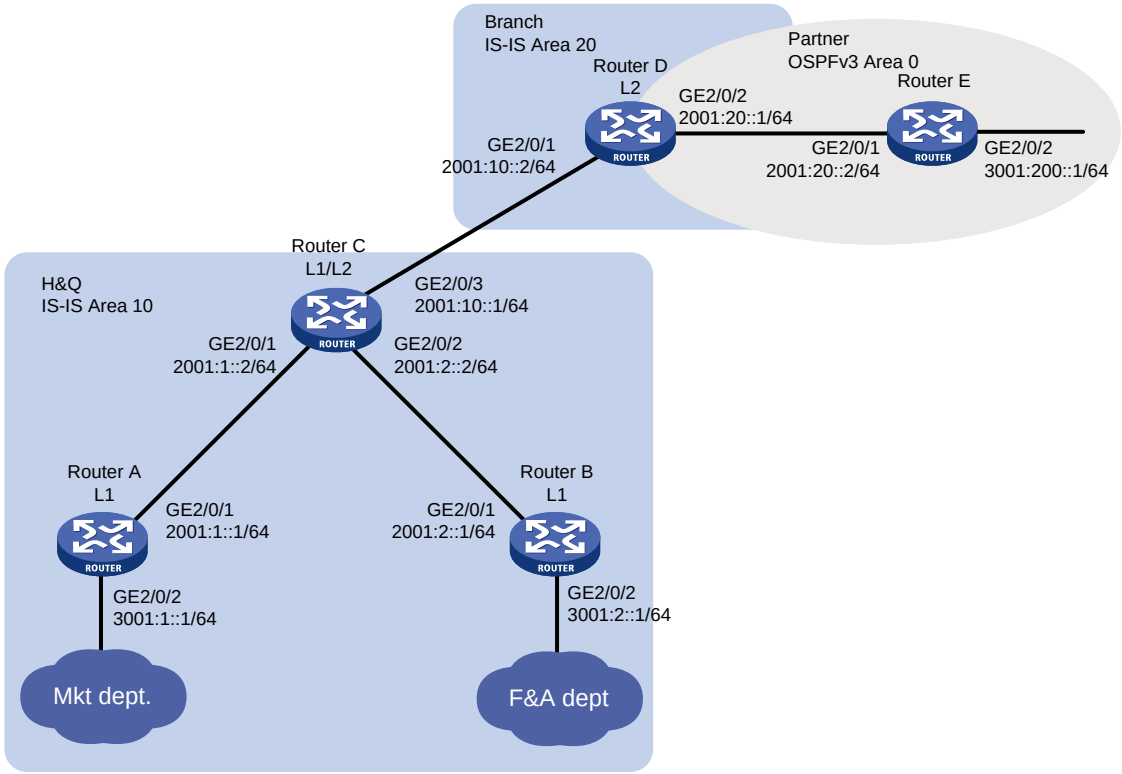
3 配置举例

3.1 组网需求

如图 1 所示，某公司总部和分部使用 IPv6 IS-IS 路由协议进行互联。公司总部内为市场部（Mkt dept.）和财务部（F&A dept.）设置了独立的网络。该公司的合作伙伴使用的是 OSPFv3 路由协议。现要求：

- Router A 和 Router B 性能相对较低，尽量使其处理较少的数据信息。
- 公司总部内市场部和财务部可以通信；并通过配置路由渗透功能，实现总部与分部间，市场部与分部可以正常通信，财务部与分部无法通信，且分部无法查看到财务部的路由信息。
- 将合作伙伴的 OSPFv3 路由引入公司分部的网络中，并保证市场部与合作伙伴可以通信。

图1 IPv6 IS-IS 配置组网图



3.2 配置思路

- 为了降低 Router A 和 Router B 运行压力，将其部署为 Level-1 路由器，仅处理公司总部 area 10 区域内的数据信息。
- 为了使公司总部内财务部和公司分部不能相互通信，且公司分部无法查看财务部的路由，需要通过在 Router C 上配置 IS-IS 路由渗透并引用地址前缀列表来实现 Level-1 区域只将 3001:1::/64 网段的路由信息向 Level-2 发布。
- 为了实现公司总部内市场部与合作伙伴的网络互通，需要在 Router D 的 IPv6 IS-IS 进程中引入 OSPFv3 路由，并在 OSPFv3 进程中引入 IPv6 IS-IS 路由。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置步骤

3.4.1 Router A 的配置

配置接口 GigabitEthernet 2/0/1 的 IPv6 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/0/1
```

```
[RouterA-GigabitEthernet2/0/1] ipv6 address 2001:1::1 64
[RouterA-GigabitEthernet2/0/1] quit
```

请参考以上方法配置图 1 中 Router A 的其它接口的 IPv6 地址，具体配置过程略。

配置 IPv6 IS-IS 基本功能。

```
[RouterA] isis 1
[RouterA-isis-1] is-level level-1
[RouterA-isis-1] network-entity 10.3001.0001.0001.00
[RouterA-isis-1] address-family ipv6 unicast
[RouterA-isis-1-ipv6] quit
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] isis ipv6 enable 1
[RouterA-GigabitEthernet2/0/1] quit
[RouterA] interface gigabitethernet 2/0/2
[RouterA-GigabitEthernet2/0/2] isis ipv6 enable 1
[RouterA-GigabitEthernet2/0/2] quit
```

3.4.2 Router B 的配置

配置接口 GigabitEthernet 2/0/1 的 IPv6 地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] ipv6 address 2001:2::1 64
[RouterB-GigabitEthernet2/0/1] quit
```

请参考以上方法配置图 1 中 Router B 的其它接口的 IPv6 地址，具体配置过程略。

配置 IPv6 IS-IS 基本功能。

```
[RouterB] isis 1
[RouterB-isis-1] is-level level-1
[RouterB-isis-1] network-entity 10.3001.0002.0001.00
[RouterB-isis-1] address-family ipv6 unicast
[RouterB-isis-1-ipv6] quit
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] isis ipv6 enable 1
[RouterB-GigabitEthernet2/0/1] quit
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] isis ipv6 enable 1
[RouterB-GigabitEthernet2/0/2] quit
```

3.4.3 Router C 的配置

配置接口 GigabitEthernet 2/0/1 的 IPv6 地址。

```
<RouterC> system-view
[RouterC] interface gigabitethernet 2/0/1
[RouterC-GigabitEthernet2/0/1] ipv6 address 2001:1::2 64
[RouterC-GigabitEthernet2/0/1] quit
```

请参考以上方法配置图 1 中 Router C 的其它接口的 IPv6 地址，具体配置过程略。

配置 IPv6 IS-IS 基本功能。

```
[RouterC] isis 1
[RouterC-isis-1] network-entity 10.2001.0010.0001.00
[RouterC-isis-1] address-family ipv6 unicast
[RouterC-isis-1-ipv6] quit
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 2/0/1
[RouterC-GigabitEthernet2/0/1] isis ipv6 enable 1
[RouterC-GigabitEthernet2/0/1] quit
[RouterC] interface gigabitethernet 2/0/2
[RouterC-GigabitEthernet2/0/2] isis ipv6 enable 1
[RouterC-GigabitEthernet2/0/2] quit
[RouterC] interface gigabitethernet 2/0/3
[RouterC-GigabitEthernet2/0/3] isis ipv6 enable 1
[RouterC-GigabitEthernet2/0/3] quit
```

配置 IPv6 IS-IS 路由渗透，并引用名为 1 的地址前缀列表，实现 Level-1 区域只将 3001:1::/64 网段的路由信息向 Level-2 发布。

```
[RouterC] ipv6 prefix-list 1 permit 3001:1:: 64
[RouterC] isis 1
[RouterC-isis-1] address-family ipv6
[RouterC-isis-1-ipv6] import-route isisv6 level-1 into level-2 filter-policy prefix-list 1
[RouterC-isis-1-ipv6] quit
[RouterC-isis-1] quit
```

3.4.4 Router D 的配置

配置接口 GigabitEthernet 2/0/1 的 IPv6 地址。

```
<RouterD> system-view
[RouterD] interface gigabitethernet 2/0/1
[RouterD-GigabitEthernet2/0/1] ipv6 address 2001:10::2 64
[RouterD-GigabitEthernet2/0/1] quit
```

请参考以上方法配置图 1 中 Router D 的其它接口的 IPv6 地址，具体配置过程略。

配置 IPv6 IS-IS 基本功能。

```
[RouterD] isis 1
[RouterD-isis-1] is-level level-2
[RouterD-isis-1] network-entity 20.2001.0020.0001.00
[RouterD-isis-1] address-family ipv6 unicast
[RouterD-isis-1-ipv6] quit
[RouterD-isis-1] quit
[RouterD] interface gigabitethernet 2/0/1
[RouterD-GigabitEthernet2/0/1] isis ipv6 enable 1
[RouterD-GigabitEthernet2/0/1] quit
[RouterD] interface gigabitethernet 2/0/2
[RouterD-GigabitEthernet2/0/2] isis ipv6 enable 1
[RouterD-GigabitEthernet2/0/2] quit
```

配置 OSPFv3 基本功能。

```
[RouterD] ospfv3
```

```
[RouterD-ospfv3-1] router-id 4.4.4.4
[RouterD-ospfv3-1] quit
[RouterD] interface gigabitethernet 2/0/2
[RouterD–GigabitEthernet2/0/2] ospfv3 1 area 0
[RouterD–GigabitEthernet2/0/2] quit
```

配置 IPv6 IS-IS 进程引入 OSPFv3 进程的路由和直连路由。

```
[RouterD] isis 1
[RouterD-isis-1] address-family ipv6
[RouterD-isis-1-ipv6] import-route ospfv3
[RouterD-isis-1-ipv6] import-route direct
[RouterD-isis-1-ipv6] quit
[RouterD-isis-1] quit
```

配置 OSPFv3 进程引入 IPv6 IS-IS 进程的路由和直连路由。

```
[RouterD] ospfv3 1
[RouterD-ospfv3-1] import-route isisv6 1
[RouterD-ospfv3-1] import-route direct
```

3.4.5 Router E 的配置

配置接口 GigabitEthernet 2/0/1 的 IPv6 地址。

```
<RouterE> system-view
[RouterE] interface gigabitethernet 2/0/1
[RouterE-GigabitEthernet2/0/1] ipv6 address 2001:20::2 64
[RouterE-GigabitEthernet2/0/1] quit
```

请参考以上方法配置图 1 中 Router E 的其它接口的 IPv6 地址，具体配置过程略。

配置 OSPFv3 基本功能。

```
[RouterE] ospfv3
[RouterE-ospfv3-1] router-id 5.5.5.5
[RouterE-ospfv3-1] quit
[RouterE] interface gigabitethernet 2/0/1
[RouterE–GigabitEthernet2/0/1] ospfv3 1 area 0
[RouterE–GigabitEthernet2/0/1] quit
[RouterE] interface gigabitethernet 2/0/2
[RouterE–GigabitEthernet2/0/2] ospfv3 1 area 0
[RouterE–GigabitEthernet2/0/2] quit
```

3.5 验证配置

(1) 在 Router D 上查看 IPv6 IS-IS 路由表，可以查看到市场部（3001:1::/64）的路由，无法查看到财务部（3001:2::/64）的路由，说明公司分部只能与市场部通信。

```
[RouterD] display isis route ipv6

                      Route information for IS-IS(1)
                      ------------------------------

                      Level-2 IPv6 Forwarding Table
                      -----------------------------
```

```
Destination : 2001:10::                                 PrefixLen: 64
Flag        : D/L/-                                     Cost     : 10
Next Hop    : Direct                                    Interface: GE2/0/1

Destination : 2001:1::                                  PrefixLen: 64
Flag        : R/-/-                                     Cost     : 20
Next Hop    : FE80::7625:8AFF:FE02:4D13                 Interface: GE2/0/1

Destination : 2001:2::                                  PrefixLen: 64
Flag        : R/-/-                                     Cost     : 20
Next Hop    : FE80::7625:8AFF:FE02:4D13                 Interface: GE2/0/1

Destination : 3001:1::                                  PrefixLen: 64
Flag        : R/-/-                                     Cost     : 30
Next Hop    : FE80::7625:8AFF:FE02:4D13                 Interface: GE2/0/1

     Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
```

(2) 在 Router C 上查看 IPv6 IS-IS 路由表，可以看到 3001:200::1/64 的路由，并且 Router A 可以 ping 通 3001:200::1，说明本公司与合作伙伴可以正常通信。

查看 Router C 上的 IPv6 IS-IS 路由表。

```
[RouterC] display isis route ipv6 level-2

                        Route information for IS-IS(1)
                        ------------------------------

                        Level-2 IPv6 Forwarding Table
                        ------------------------------

Destination : 2001:10::                                 PrefixLen: 64
Flag        : D/L/-                                     Cost     : 10
Next Hop    : Direct                                    Interface: GE2/0/3

Destination : 2001:1::                                  PrefixLen: 64
Flag        : D/L/-                                     Cost     : 10
Next Hop    : Direct                                    Interface: GE2/0/1


Destination : 2001:2::                                  PrefixLen: 64
Flag        : D/L/-                                     Cost     : 10
Next Hop    : Direct                                    Interface: GE2/0/2

Destination : 2001:20::                                 PrefixLen: 64
Flag        : R/L/-                                     Cost     : 20
Next Hop    : FE80::BAAF:67FF:FE30:3304                 Interface: GE2/0/3

Destination : 3001:200::                                PrefixLen: 64
Flag        : R/-/-                                     Cost     : 20
```

```
 Next Hop    : FE80::BAAF:67FF:FE30:3304              Interface: GE2/0/3

      Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
```

从 Router A 的 GE2/0/2 接口 ping 3001:200::1。

```
[RouterA] ping ipv6 –a 3001:1::1 3001:200::1
Ping6(56 data bytes) 2001:10::1 --> 3001:200::1, press CTRL_C to break
56 bytes from 3001:200::1, icmp_seq=0 hlim=61 time=7.230 ms
56 bytes from 3001:200::1, icmp_seq=1 hlim=61 time=3.449 ms
56 bytes from 3001:200::1, icmp_seq=2 hlim=61 time=2.779 ms
56 bytes from 3001:200::1, icmp_seq=3 hlim=61 time=2.652 ms
56 bytes from 3001:200::1, icmp_seq=4 hlim=61 time=2.558 ms

--- Ping6 statistics for 3001:200::1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 2.558/3.734/7.230/1.776 ms
```

3.6 配置文件

- Router A：

```
#
isis 1
 is-level level-1
 network-entity 10.3001.0001.0001.00
 #
 address-family ipv6 unicast
#
interface GigabitEthernet2/0/1
 isis ipv6 enable 1
 ipv6 address 2001:1::1/64
#
interface GigabitEthernet2/0/2
 isis ipv6 enable 1
 ipv6 address 3001:1::1/64
#
```

- Router B：

```
#
isis 1
 is-level level-1
 network-entity 10.3001.0002.0001.00
 #
 address-family ipv6 unicast
#
interface GigabitEthernet2/0/1
 isis ipv6 enable 1
 ipv6 address 2001:2::1/64
#
interface GigabitEthernet2/0/2
 isis ipv6 enable 1
```

```
 ipv6 address 3001:2::1/64
#
```

- Router C：

```
#
isis 1
 network-entity 10.2001.0010.0001.00
 #
 address-family ipv6 unicast
  import-route isisv6 level-1 into level-2 filter-policy prefix-list 1
#
interface GigabitEthernet2/0/1
 isis ipv6 enable 1
 ipv6 address 2001:1::2/64
#
interface GigabitEthernet2/0/2
 isis ipv6 enable 1
 ipv6 address 2001:2::2/64
#
interface GigabitEthernet2/0/3
 isis ipv6 enable 1
 ipv6 address 2001:10::1/64
#
 ipv6 prefix-list 1 index 10 permit 3001:1:: 64
#
```

- Router D：

```
#
isis 1
 is-level level-2
 network-entity 20.2001.0020.0001.00
 #
 address-family ipv6 unicast
  import-route direct
  import-route ospfv3 1
#
ospfv3 1
 router-id 4.4.4.4
 area 0.0.0.0
 import-route direct
 import-route isisv6 1
#
interface GigabitEthernet2/0/1
 isis ipv6 enable 1
 ipv6 address 2001:10::2/64
#
interface GigabitEthernet2/0/2
 ospfv3 1 area 0.0.0.0
 ipv6 address 2001:20::1/64
#
```

- Router E：

```
#
ospfv3 1
 router-id 5.5.5.5
 area 0.0.0.0
#
interface GigabitEthernet2/0/1
 ospfv3 1 area 0
 ipv6 address 2001:20::2/64
#
interface GigabitEthernet2/0/2
 ospfv3 1 area 0
 ipv6 address 3001:200::1/64
#
```

4 相关资料

- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由配置指导-R7607
- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

IPv6 over IPv4 GRE 隧道配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 配置举例 1
3.1 组网需求 1
3.2 配置思路 1
3.3 使用版本 2
3.4 配置注意事项 2
3.5 配置步骤 2
3.5.1 配置 Device A 2
3.5.2 配置 Device B 3
3.5.3 配置 Device C 3
3.6 验证配置 3
3.7 配置文件 4
4 相关资料 5

1 简介

本文档介绍了 IPv6 over IPv4 GRE 隧道的典型配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文假设您已了解 IPv6 over IPv4 GRE 隧道的相关特性。

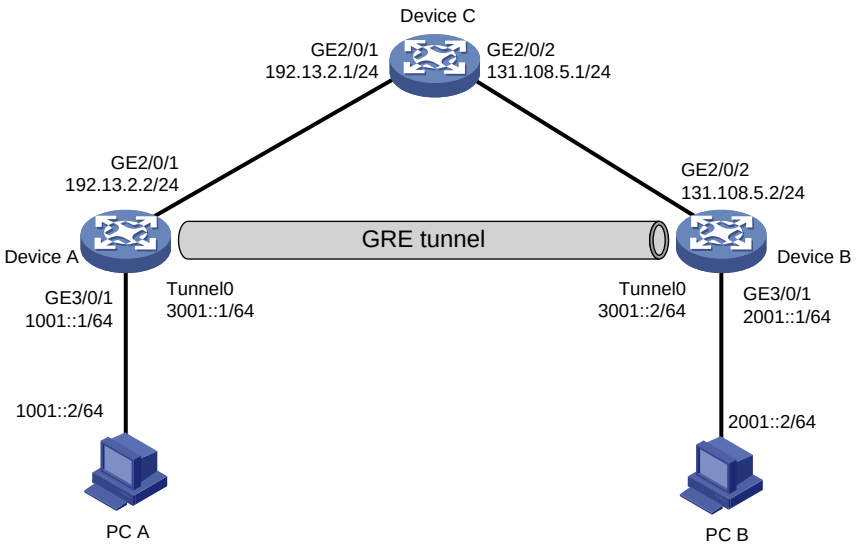
3 配置举例

3.1 组网需求

如图 1 所示，Device A、Device B、Device C 之间通过 IPv4 网络互连。Device A 和 Device B 分别连接 IPv6 主机 PC A 和 PC B。

要求通过在边界的双栈设备（Device A、Device B）之间建立 GRE 隧道，实现两台 IPv6 主机 PC A 和 PC B 的通信。

图1 IPv6 over IPv4 GRE 隧道配置组网图



3.2 配置思路

- 为实现两台 IPv6 主机 PC A 和 PC B 的通信，需要将 GRE 隧道模式为 GRE over IPv4，隧道接口配置为 IPv6 地址；

- 为了使 PC A 发往 PC B 的报文经由 GRE 隧道进行转发，需要在边界设备 Device A 上建立 Tunnel 转发的路由表项：目的地址是未进行 GRE 封装的报文的目的地址（即 PC B 的 IPv6 地址），下一跳是 GRE 隧道对端 Device B 的 Tunnel 接口地址或者直接指定出接口为 GRE 隧道接口。该路由表项可以通过配置静态路由来建立，也可以在 Tunnel 接口上和与 PC A 相连的三层接口上分别使能动态路由协议，由动态路由协议来建立。本例中选择配置静态路由方式。同理，Device B 上也需进行相应配置；
- 对于 GRE 隧道，必须确保隧道源端和目的端之间 IPv4 路由可达，因此需要在 Device A 和 Device B 上分别配置到对端的静态路由。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置注意事项

Tunnel 两端必须都配置隧道的源端地址和目的端地址，且本端配置的源端地址应该与对端配置的目的端地址相同、本端配置的目的端地址应该与对端配置的源端地址相同。

3.5 配置步骤

3.5.1 配置 Device A

配置接口 GigabitEthernet2/0/1 的 IPv6 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ipv6 address 1001::1 64
[DeviceA-GigabitEthernet2/0/1] quit
```

请参考以上方法配置上图中 Device A 其它接口的 IP 地址，配置步骤这里省略。

创建隧道接口 Tunnel0，并指定隧道模式为 GRE over IPv4 隧道。

```
[DeviceA] interface tunnel 0 mode gre
```

配置 Tunnel0 接口的 IPv6 地址。

```
[DeviceA-Tunnel0] ipv6 address 3001::1 64
```

配置 Tunnel0 接口的源端地址。

```
[DeviceA-Tunnel0] source 192.13.2.2
```

配置 Tunnel0 接口的目的端地址。

```
[DeviceA-Tunnel0] destination 131.108.5.2
[DeviceA-Tunnel0] quit
```

配置从 Device A 经过 Tunnel0 接口到 PC B 的静态路由。

```
[DeviceA] ipv6 route-static 2001:: 64 tunnel 0
```

配置从 DeviceA 到达隧道目的端的静态路由。

```
[DeviceA] ip route-static 131.108.5.2 255.255.255.0 192.13.2.1
```

3.5.2 配置 Device B

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] ipv6 address 2001::1 64
[DeviceB-GigabitEthernet2/0/1] quit
```

请参考以上方法配置上图中 Device B 其它接口的 IP 地址，配置步骤这里省略。

创建隧道接口 Tunnel0，并指定隧道模式为 GRE over IPv4 隧道。

```
[DeviceB] interface tunnel 0 mode gre
```

配置 Tunnel0 接口的 IPv6 地址。

```
[DeviceB-Tunnel0] ipv6 address 3001::2 64
```

配置 Tunnel0 接口的源端地址。

```
[DeviceB-Tunnel0] source 131.108.5.2
```

配置 Tunnel0 接口的目的端地址。

```
[DeviceB-Tunnel0] destination 192.13.2.2
[DeviceB-Tunnel0] quit
```

配置从 DeviceB 经过 Tunnel0 接口到 PC A 的静态路由。

```
[DeviceB] ipv6 route-static 1001:: 64 Tunnel 0
```

配置 DeviceB 到达隧道目的端的静态路由。

```
[DeviceB] ip route-static 192.13.2.2 255.255.255.0 131.108.5.1
```

3.5.3 配置 Device C

配置接口 GigabitEthernet2/1/1 的 IP 地址。

```
<DeviceC> system-view
[DeviceC] interface gigabitethernet 2/0/1
[DeviceC-GigabitEthernet2/0/1] ip address 192.13.2.1 24
[DeviceC-GigabitEthernet2/0/1] quit
```

配置接口 GigabitEthernet2/1/2 的 IP 地址。

```
[DeviceC] interface gigabitethernet 2/0/2
[DeviceC-GigabitEthernet2/0/2] ip address 131.108.5.1 24
[DeviceC-GigabitEthernet2/0/2] quit
```

3.6 验证配置

PCA 和 PCB 之间可以互相 Ping 通。

```
C:\>ping6 2001::2

Pinging 2001::2
from 1001::1 with 32 bytes of data:

Reply from 2001::2: bytes=32 time<1ms
Reply from 2001::2: bytes=32 time<1ms
Reply from 2001::2: bytes=32 time<1ms
Reply from 2001::2: bytes=32 time<1ms
```

```
Ping statistics for 2001::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

3.7 配置文件

- Device A：

```
#
interface GigabitEthernet2/1/1
 port link-mode route
 ip address 192.13.2.2 255.255.255.0
#
interface GigabitEthernet2/0/1
 port link-mode route
 ipv6 address 1001::1/64
#
interface Tunnel0 mode gre
 ipv6 address 3001::1/64
 source 192.13.2.2
 destination 131.108.5.2
#
 ip route-static 131.108.5.2 255.255.255.0 192.13.2.1
#
 ipv6 route-static 2001:: 64 Tunnel 0
#
```

- Device B：

```
#
interface GigabitEthernet2/1/2
 port link-mode route
 ip address 131.108.5.2 255.255.255.0
#
interface GigabitEthernet2/0/1
 port link-mode route
 ipv6 address 2001::1/64
#
interface Tunnel0 mode gre
 ipv6 address 3001::2/64
 source 131.108.5.2
 destination 192.13.2.2
#
ip route-static 192.13.2.2 255.255.255.0 131.108.5.1
#
ipv6 route-static 1001:: 64 Tunnel 0
#
```

- Device C：

```
#
```

```
interface GigabitEthernet2/1/1
 port link-mode route
 ip address 192.13.2.1 255.255.255.0
#
interface GigabitEthernet2/1/2
 port link-mode route
 ip address 131.108.5.1 255.255.255.0
#
```

4 相关资料

- H3C SR6600 SR6600-X 路由器 三层技术-IP 业务配置指导-R7607
- H3C SR6600 SR6600-X 路由器 三层技术-IP 业务命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

IS-IS 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 配置举例 1
3.1 组网需求 1
3.2 配置思路 2
3.3 使用版本 2
3.4 配置注意事项 2
3.5 配置步骤 3
3.5.1 Router A 的配置 3
3.5.2 Router B 的配置 3
3.5.3 Router C 的配置 3
3.5.4 Router D 的配置 4
3.5.5 Router E 的配置 5
3.6 验证配置 5
3.7 配置文件 8
4 相关资料 9

1 简介

本文档介绍 IS-IS 配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 IS-IS 特性。

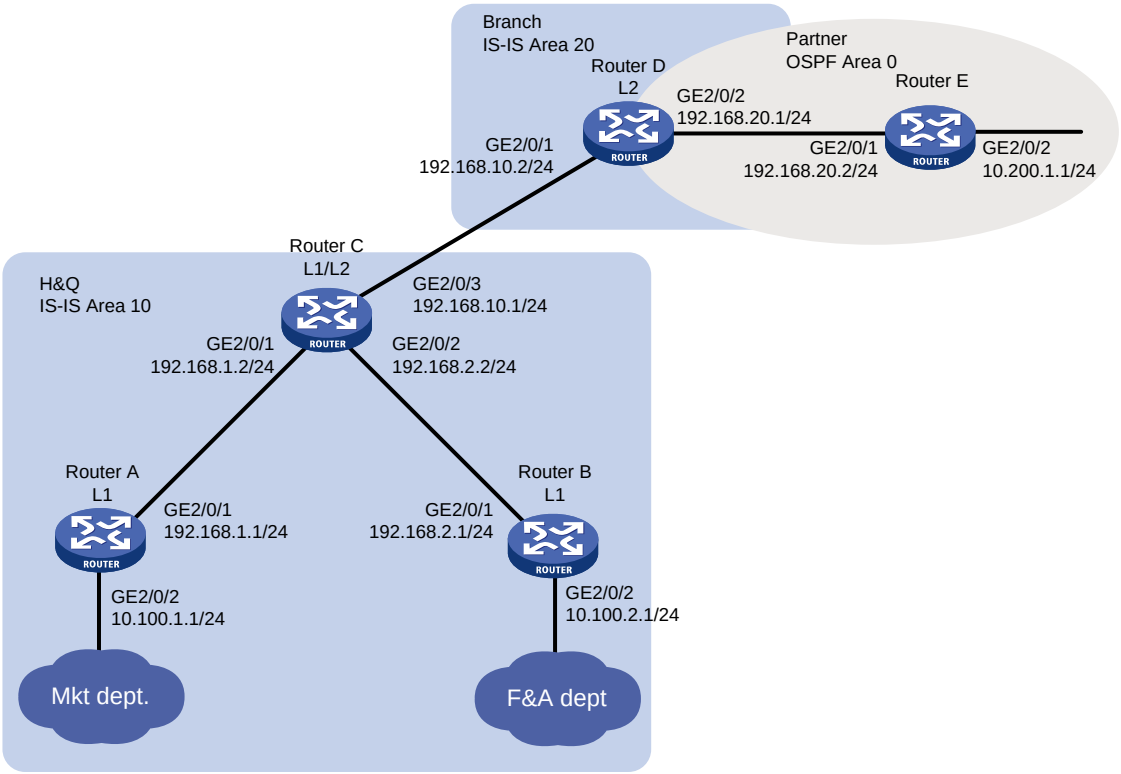
3 配置举例

3.1 组网需求

如图 1 所示，某公司总部和分部使用 IS-IS 路由协议进行互联。公司总部内为市场部（Mkt dept.）和财务部（F&A dept.）设置了独立的网络。该公司的合作伙伴使用的是 OSPF 路由协议。现要求：

- Router A 和 Router B 性能相对较低，尽量使其处理较少的数据信息。
- 公司总部内市场部和财务部可以通信；并通过配置路由渗透功能，实现总部与分部间，市场部与分部可以正常通信，财务部与分部无法通信，且分部无法查看到财务部的路由信息。
- 将合作伙伴的 OSPF 路由引入公司分部的网络中，并保证市场部与合作伙伴可以通信。
- 当总部的网关设备 Router C IS-IS 协议进程重启时，原有的通信不中断。

图1 IS-IS 配置组网图



3.2 配置思路

- 为了降低 Router A 和 Router B 运行压力，将其部署为 Level-1 路由器，仅处理公司总部 area 10 区域内的数据信息。
- 为了使公司总部内财务部和公司分部不能相互通信，且公司分部无法查看财务部的路由，需要通过在 Router C 上配置 IS-IS 路由渗透并引用地址前缀列表来实现 Level-1 区域只将 10.100.1.0/24 网段的路由信息向 Level-2 发布。
- 为了实现公司总部内市场部与合作伙伴的网络互通，需要在 Router D 的 IS-IS 进程中引入 OSPF 进程的路由，并在 OSPF 进程中引入 IS-IS 进程的路由。
- 为了保证 Router C IS-IS 协议进程重启时，原有的通信不中断，需要在 Router C 上使能 IS-IS 协议的 GR（Graceful Restart，平滑重启）能力。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置注意事项

在设备平滑重启过程中，请勿变更拓扑，否则可能导致路由黑洞。

3.5 配置步骤

3.5.1 Router A 的配置

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] ip address 192.168.1.1 24
[RouterA-GigabitEthernet2/0/1] quit
```

请参考以上方法配置图 1 中 Router A 的其它接口的 IP 地址，具体配置过程略。

配置 IS-IS 基本功能。

```
[RouterA] isis 1
[RouterA-isis-1] is-level level-1
[RouterA-isis-1] network-entity 10.1921.6800.1001.00
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 2/0/1
[RouterA–GigabitEthernet2/0/1] isis enable 1
[RouterA–GigabitEthernet2/0/1] quit
[RouterA] interface gigabitethernet 2/0/2
[RouterA–GigabitEthernet2/0/2] isis enable 1
[RouterA–GigabitEthernet2/0/2] quit
```

3.5.2 Router B 的配置

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] ip address 192.168.2.1 24
[RouterB-GigabitEthernet2/0/1] quit
```

请参考以上方法配置图 1 中 Router B 的其它接口的 IP 地址，具体配置过程略。

配置 IS-IS 基本功能。

```
[RouterB] isis 1
[RouterB-isis-1] is-level level-1
[RouterB-isis-1] network-entity 10.1921.6800.2001.00
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 2/0/1
[RouterB–GigabitEthernet2/0/1] isis enable 1
[RouterB–GigabitEthernet2/0/1] quit
[RouterB] interface gigabitethernet 2/0/2
[RouterB–GigabitEthernet2/0/2] isis enable 1
[RouterB–GigabitEthernet2/0/2] quit
```

3.5.3 Router C 的配置

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<RouterC> system-view
[RouterC] interface gigabitethernet 2/0/1
```

```
[RouterC-GigabitEthernet2/0/1] ip address 192.168.1.2 24
[RouterC-GigabitEthernet2/0/1] quit
```

请参考以上方法配置图 1 中 Router C 的其它接口的 IP 地址，具体配置过程略。

配置 IS-IS 基本功能。

```
[RouterC] isis 1
[RouterC-isis-1] network-entity 10.1921.6801.0001.00
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 2/0/1
[RouterC–GigabitEthernet2/0/1] isis enable 1
[RouterC–GigabitEthernet2/0/1] quit
[RouterC] interface gigabitethernet 2/0/2
[RouterC–GigabitEthernet2/0/2] isis enable 1
[RouterC–GigabitEthernet2/0/2] quit
[RouterC] interface gigabitethernet 2/0/3
[RouterC–GigabitEthernet2/0/3] isis enable 1
[RouterC–GigabitEthernet2/0/3] quit
```

配置 IS-IS 路由渗透，并引用名为 1 的地址前缀列表，实现 Level-1 区域只将 10.100.1.0/24 网段的路由信息向 Level-2 发布。

```
[RouterC] ip prefix-list 1 permit 10.100.1.0 24
[RouterC] isis 1
[RouterC-isis-1] address-family ipv4
[RouterC-isis-1-ipv4] import-route isis level-1 into level-2 filter-policy prefix-list 1
[RouterC-isis-1-ipv4] quit
[RouterC-isis-1] import-route isis level-1 into level-2 filter-policy prefix-list 1
```

使能 IS-IS 协议的 GR 能力。

```
[RouterC -isis-1] graceful-restart
[RouterC -isis-1] quit
```

3.5.4 Router D 的配置

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<RouterD> system-view
[RouterD] interface gigabitethernet 2/0/1
[RouterD-GigabitEthernet2/0/1] ip address 192.168.10.2 24
[RouterD-GigabitEthernet2/0/1] quit
```

请参考以上方法配置图 1 中 Router D 的其它接口的 IP 地址，具体配置过程略。

配置 IS-IS 基本功能。

```
[RouterD] isis 1
[RouterD-isis-1] is-level level-2
[RouterD-isis-1] network-entity 20.1921.6802.0001.00
[RouterD-isis-1] quit
[RouterD] interface gigabitethernet 2/0/1
[RouterD–GigabitEthernet2/0/1] isis enable 1
[RouterD–GigabitEthernet2/0/1] quit
[RouterD] interface gigabitethernet 2/0/2
[RouterD–GigabitEthernet2/0/2] isis enable 1
[RouterD–GigabitEthernet2/0/2] quit
```

配置 OSPF 基本功能。

```
[RouterD] ospf
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] quit
[RouterD-ospf-1] quit
```

配置 IS-IS 进程引入 OSPF 进程的路由和直连路由。

```
[RouterD] isis 1
[RouterD-isis-1] address-family ipv4
[RouterD-isis-1-ipv4] import-route ospf
[RouterD-isis-1-ipv4] import-route direct
[RouterD-isis-1-ipv4] quit
[RouterD-isis-1] quit
```

配置 OSPF 进程引入 IS-IS 进程的路由和直连路由。

```
[RouterD] ospf 1
[RouterD-ospf-1] import-route isis 1
[RouterD-ospf-1] import-route direct
```

3.5.5 Router E 的配置

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<RouterE> system-view
[RouterE] interface gigabitethernet 2/0/1
[RouterE-GigabitEthernet2/0/1] ip address 192.168.20.2 24
[RouterE-GigabitEthernet2/0/1] quit
```

请参考以上方法配置图 1 中 Router E 的其它接口的 IP 地址，具体配置过程略。

配置 OSPF 基本功能。

```
[RouterE] ospf
[RouterE-ospf-1] area 0
[RouterE-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[RouterE-ospf-1-area-0.0.0.0] network 10.200.1.0 0.0.0.255
[RouterE-ospf-1-area-0.0.0.0] quit
[RouterE-ospf-1] quit
```

3.6 验证配置

(1) 在 Router D 上查看 IS-IS 路由表，可以查看到市场部（10.100.1.0/24）的路由，无法查看到财务部（10.100.2.0/24）的路由，说明公司分部只能与市场部通信。

```
[RouterD] display isis route

                          Route information for IS-IS(1)
                          ------------------------------

                          Level-2 IPv4 Forwarding Table
                          ------------------------------

 IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
```

```
------------------------------------------------------------------------------
 192.168.10.0/24      10         NULL    GE2/0/1         Direct          D/L/-
 192.168.1.0/24       20         NULL    GE2/0/1         192.168.10.1    R/-/-
 10.100.1.0/24        30         NULL    GE2/0/1         192.168.10.1    R/-/-
 192.168.2.0/24       20         NULL    GE2/0/1         192.168.10.1    R/-/-

      Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
```

(2) 在 Router C 上查看 IS-IS 路由表，可以看到 10.200.1.0/24 的路由，并且 Router A 可以 ping 通 10.200.1.1，说明本公司与合作伙伴可以正常通信。

查看 Router C 上的 IS-IS 路由表。

```
[RouterC] display isis route

                         Route information for IS-IS(1)
                         ------------------------------

                         Level-1 IPv4 Forwarding Table
                         ------------------------------

 IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
------------------------------------------------------------------------------
 192.168.10.0/24      10         NULL    GE2/0/3         Direct          D/L/-
 192.168.1.0/24       10         NULL    GE2/0/1         Direct          D/L/-
 10.100.1.0/24        20         NULL    GE2/0/1         192.168.1.1     R/L/-
 10.100.2.0/24        20         NULL    GE2/0/2         192.168.2.1     R/-/-
 192.168.2.0/24       10         NULL    GE2/0/2         Direct          D/L/-

      Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

                         Level-2 IPv4 Forwarding Table
                         ------------------------------

 IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
------------------------------------------------------------------------------
 192.168.10.0/24      10         NULL    GE2/0/3         Direct          D/L/-
 10.200.1.0/24        10         0       GE2/0/3         192.168.10.2    R/-/-
 192.168.20.0/24      10         0       GE2/0/3         192.168.10.2    R/-/-
 192.168.1.0/24       10         NULL    GE2/0/1         Direct          D/L/-
 192.168.2.0/24       10         NULL    GE2/0/2         Direct          D/L/-

      Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
```

从 Router A 的 GE2/0/2 接口 ping 10.200.1.1。

```
[RouterA] ping –a 10.1.1.1 10.200.1.1
Ping 10.200.1.1 (10.200.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 10.200.1.1: icmp_seq=0 ttl=252 time=1.862 ms
56 bytes from 10.200.1.1: icmp_seq=1 ttl=252 time=2.969 ms
56 bytes from 10.200.1.1: icmp_seq=2 ttl=252 time=1.402 ms
56 bytes from 10.200.1.1: icmp_seq=3 ttl=252 time=1.324 ms
```

```
56 bytes from 10.200.1.1: icmp_seq=4 ttl=252 time=1.510 ms

--- Ping statistics for 10.200.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.324/1.813/2.969/0.606 ms
```

(3) 在 Router A 上持续 ping Router B，期间在 Router C 上重启 IS-IS 进程，查看 Router C 的 IS-IS 协议重启时，通信是否中断。并使用 **display isis graceful-restart status** 命令，可查看 Router C 上 IS-IS 协议的 GR 状态。

在 Router A 上持续 ping Router B。

```
[RouterA] ping -c 10000 10.100.2.1
Ping 10.100.2.1 (10.100.2.1): 56 data bytes, press CTRL_C to break
56 bytes from 10.100.2.1: icmp_seq=0 ttl=254 time=1.185 ms
56 bytes from 10.100.2.1: icmp_seq=1 ttl=254 time=1.087 ms
……
```

重启 Router C 的 IS-IS 进程。

```
[RouterC] reset isis all graceful-restart
Reset IS-IS process? [Y/N] :y
```

在 Router A 上查看到 IS-IS 协议重启时通信未发生中断。

```
[RouterA] ping -c 10000 10.100.2.1
Ping 10.100.2.1 (10.100.2.1): 56 data bytes, press CTRL_C to break
56 bytes from 10.100.2.1: icmp_seq=0 ttl=254 time=1.185 ms
56 bytes from 10.100.2.1: icmp_seq=1 ttl=254 time=1.087 ms
56 bytes from 10.100.2.1: icmp_seq=2 ttl=254 time=1.672 ms
56 bytes from 10.100.2.1: icmp_seq=3 ttl=254 time=1.751 ms
56 bytes from 10.100.2.1: icmp_seq=4 ttl=254 time=1.816 ms
56 bytes from 10.100.2.1: icmp_seq=5 ttl=254 time=1.814 ms
```

查看 Router C 上 IS-IS 协议的 GR 状态。

```
[RouterC] display isis graceful-restart status

                        Restart information for IS-IS(1)
                        --------------------------------
Restart status: COMPLETE
Restart phase: Finish
Restart t1: 3, count 10; Restart t2: 60; Restart t3: 300
SA Bit: supported

                          Level-1 restart information
                          ---------------------------
Total number of interfaces: 3
Number of waiting LSPs: 0

                          Level-2 restart information
                          ---------------------------
Total number of interfaces: 3
Number of waiting LSPs: 0
```

3.7 配置文件

- Router A：

```
#
 isis 1
 is-level level-1
 network-entity 10.1921.6800.1001.00
#
 interface GigabitEthernet2/0/1
 ip address 192.168.1.1 255.255.255.0
 isis enable 1
#
 interface GigabitEthernet2/0/2
 ip address 10.100.1.1 255.255.255.0
 isis enable 1
#
```

- Router B：

```
#
 isis 1
 is-level level-1
 network-entity 10.1921.6800.2001.00
#
 interface GigabitEthernet2/0/1
 ip address 192.168.2.1 255.255.255.0
 isis enable 1
#
 interface GigabitEthernet2/0/2
 ip address 10.100.2.1 255.255.255.0
 isis enable 1
#
```

- Router C：

```
#
 isis 1
 graceful-restart
 network-entity 10.1921.6801.0001.00
 #
 address-family ipv4 unicast
 import-route isis level-1 into level-2 filter-policy prefix-list 1
#
 interface GigabitEthernet2/0/1
 ip address 192.168.1.2 255.255.255.0
 isis enable 1
#
 interface GigabitEthernet2/0/2
 ip address 192.168.2.2 255.255.255.0
 isis enable 1
#
```

```
 interface GigabitEthernet2/0/3
 ip address 192.168.10.1 255.255.255.0
 isis enable 1
#
 ip prefix-list 1 index 10 permit 10.100.1.0 24
#
```

- Router D：

```
#
 isis 1
 is-level level-2
 network-entity 20.1921.6802.0001.00
#
 address-family ipv4 unicast
 import-route direct
 import-route ospf 1
#
 ospf 1
 import-route direct
 import-route isis 1
 area 0.0.0.0
 network 192.168.20.0 0.0.0.255
#
 interface GigabitEthernet2/0/1
 ip address 192.168.10.2 255.255.255.0
 isis enable 1
#
 interface GigabitEthernet2/0/2
 ip address 192.168.20.1 255.255.255.0
#
```

- Router E：

```
#
 ospf 1
 area 0.0.0.0
 network 10.200.1.0 0.0.0.255
 network 192.168.20.0 0.0.0.255
#
 interface GigabitEthernet2/0/1
 ip address 192.168.20.2 255.255.255.0
#
 interface GigabitEthernet2/0/2
 ip address 10.200.1.1 255.255.255.0
#
```

4 相关资料

- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由配置指导-R7607
- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

IS-IS 路由聚合配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
1 IS-IS 路由聚合配置举例 1
1.1 组网需求 1
1.2 配置思路 2
1.3 使用版本 2
1.4 配置步骤 2
1.4.1 配置各接口的 IP 地址 2
1.4.2 配置 IS-IS 基本功能 3
1.4.3 在 Device A 上配置 IS-IS 路由聚合 4
1.5 验证配置 4
1.6 配置文件 4
2 相关资料 6

1 简介

本文档介绍 IS-IS 路由聚合配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

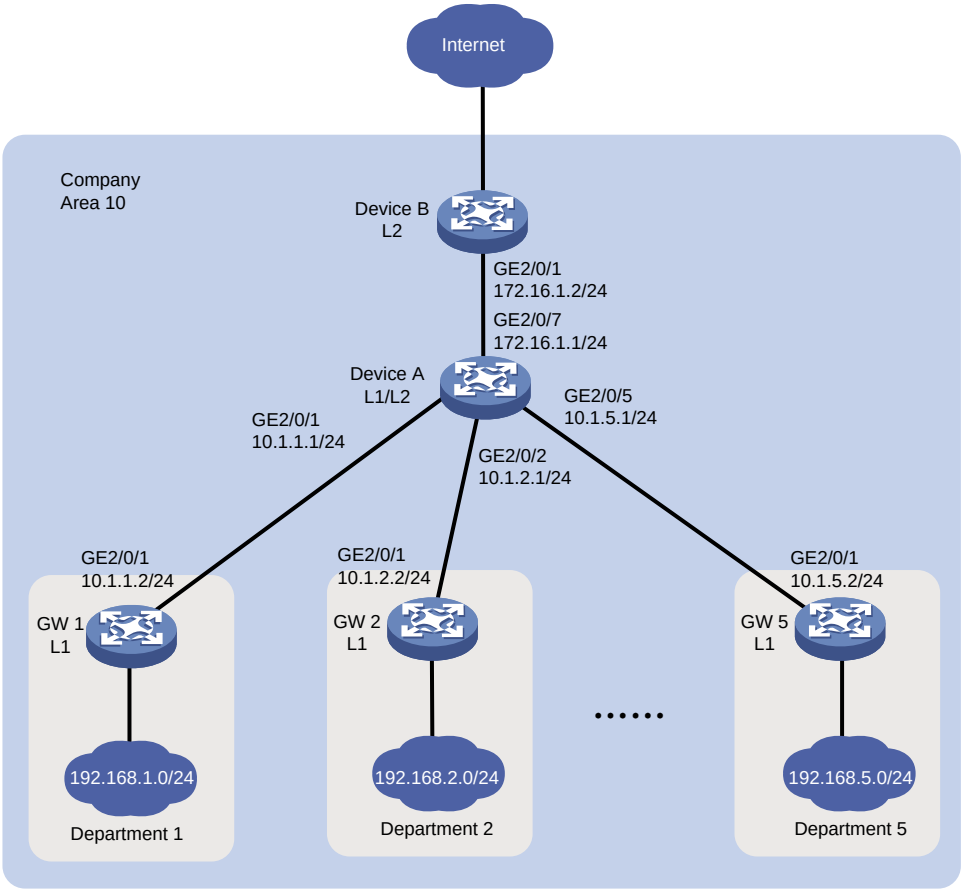
本文档假设您已了解 IS-IS 路由聚合特性。

1 IS-IS 路由聚合配置举例

1.1 组网需求

如图 1 所示，某公司内部 5 个部门使用 IS-IS 协议接入公司骨干网。公司为每个部门分配一个 C 类地址段。为了降低 Device B 设备的系统资源消耗，现要求通过在 Device A 上配置 IS-IS 路由聚合，减少 Device B 设备上的路由表项。

图1 IS-IS 路由聚合配置组网图



1.2 配置思路

- 由于路由器只对本地生成的 LSP 中的路由进行聚合，所以需要在 Device A 上配置路由聚合。
- 为了减小路由黑洞，所以可以将路由聚合为 192.168.0.0/21。

1.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

1.4 配置步骤

1.4.1 配置各接口的 IP 地址

配置 Device A 接口 GigabitEthernet 2/0/7 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 2/0/7
[DeviceA-GigabitEthernet2/0/7] ip address 172.16.1.2 24
[DeviceA-GigabitEthernet2/0/7] quit
```

请参考以上方法配置图 1 中其它设备的接口 IP 地址，具体配置过程略。

1.4.2 配置 IS-IS 基本功能

1. Device A 的配置

使能 IS-IS 进程，并配置 Device A 工作在 Level-1-2。

```
[DeviceA] isis 1
[DeviceA-isis-1] network-entity 10.0000.0000.0001.00
[DeviceA-isis-1] is-level level-1-2
[DeviceA-isis-1] quit
```

在所有接口使能 IS-IS 进程，此处仅以 GigabitEthernet 2/0/1 为例。

```
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] isis enable 1
[DeviceA-GigabitEthernet2/0/1] quit
```

2. Device B 的配置

使能 IS-IS 进程，并配置 Device B 工作在 Level-2。

```
[DeviceB] isis 1
[DeviceB-isis-1] network-entity 10.0000.0000.0002.00
[DeviceB-isis-1] is-level level-2
[DeviceB-isis-1] quit
```

在 GigabitEthernet 2/0/1 接口使能使能 IS-IS 进程。

```
[DeviceB] interface gigabitethernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] isis enable 1
[DeviceB-GigabitEthernet2/0/1] quit
```

3. GW 的配置

使能 IS-IS 进程，并配置 GW 1 工作在 Level-1。

```
[GW1] isis 1
[GW1-isis-1] network-entity 10.0001.0001.0001.00
[GW1-isis-1] is-level level-1
[GW1-isis-1] quit
```

在 GigabitEthernet 2/0/1 接口使能使能 IS-IS 进程。

```
[GW1] interface gigabitethernet 2/0/1
[GW1-GigabitEthernet2/0/1] isis enable 1
[GW1-GigabitEthernet2/0/1] quit
```

请参考以上方法配置其他 GW，具体配置过程略。

4. 查看 Device B 上的 IS-IS 路由信息

完成以上配置后，在 Device B 上查看 IS-IS 路由信息，可以查看到每个公司所在网段的路由。

```
[DeviceB] display isis route

                        Route information for IS-IS(1)
                        ------------------------------

                        Level-2 IPv4 Forwarding Table
                        -----------------------------

 IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
```

```
------------------------------------------------------------------------------
192.168.1.0/24      30         NULL    GE2/0/1         172.16.1.1      R/-/-
10.1.1.0/24         20         NULL    GE2/0/1         172.16.1.1      R/-/-
192.168.2.0/24      30         NULL    GE2/0/1         172.16.1.1      R/-/-
10.1.2.0/24         20         NULL    GE2/0/1         172.16.1.1      R/-/-
192.168.3.0/24      30         NULL    GE2/0/1         172.16.1.1      R/-/-
10.1.3.0/24         20         NULL    GE2/0/1         172.16.1.1      R/-/-
192.168.4.0/24      30         NULL    GE2/0/1         172.16.1.1      R/-/-
10.1.4.0/24         20         NULL    GE2/0/1         172.16.1.1      R/-/-
192.168.5.0/24      30         NULL    GE2/0/1         172.16.1.1      R/-/-
10.1.5.0/24         20         NULL    GE2/0/1         172.16.1.1      R/-/-
172.16.1.0/24       10         NULL    GE2/0/1         Direct          D/L/-

      Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
```

1.4.3 在 Device A 上配置 IS-IS 路由聚合

```
[DeviceA] isis 1
[DeviceA-isis-1] address-family ipv4
[DeviceA-isis-1-ipv4] summary 192.168.0.0 21
```

1.5 验证配置

在 Device B 上查看 IS-IS 路由信息，可以看到各部门的网段已被聚合为 192.168.0.0/21。

```
[DeviceB]display isis route

                         Route information for IS-IS(1)
                         ------------------------------

                         Level-2 IPv4 Forwarding Table
                         ------------------------------

 IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
------------------------------------------------------------------------------
 10.1.1.0/24          20         NULL    GE2/0/1         172.16.1.1      R/-/-
 10.1.2.0/24          20         NULL    GE2/0/1         172.16.1.1      R/-/-
 10.1.3.0/24          20         NULL    GE2/0/1         172.16.1.1      R/-/-
 10.1.4.0/24          20         NULL    GE2/0/1         172.16.1.1      R/-/-
 10.1.5.0/24          20         NULL    GE2/0/1         172.16.1.1      R/-/-
 172.16.1.0/24        10         NULL    GE2/0/1         Direct          D/L/-
 192.168.0.0/21       30         NULL    GE2/0/1         172.16.1.1      R/-/-

      Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
```

1.6 配置文件

- Device A：

```
#
```

```
isis 1
 network-entity 10.0000.0000.0001.00
 #
 address-family ipv4
 summary 192.168.0.0 255.255.248.0
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.1.2.1 255.255.255.0
 isis enable 1
#
interface GigabitEthernet2/0/3
 port link-mode route
 ip address 10.1.3.1 255.255.255.0
 isis enable 1
#
interface GigabitEthernet2/0/4
 port link-mode route
 ip address 10.1.4.1 255.255.255.0
 isis enable 1
#
interface GigabitEthernet2/0/5
 port link-mode route
 ip address 10.1.5.1 255.255.255.0
 isis enable 1
#
interface GigabitEthernet2/0/7
 port link-mode route
 ip address 172.16.1.1 255.255.255.0
 isis enable 1
#
```

- Device B：

```
#
isis 1
 is-level level-2
 network-entity 10.0000.0000.0002.00
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 172.16.1.2 255.255.255.0
 isis enable 1
#
```

- GW 1：

```
#
isis 1
 is-level level-1
 network-entity 10.0001.0001.0001.00
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 192.168.1.1 255.255.255.0
 isis enable 1
#
```

其余 GW 设备的配置请参考 GW 1，此处省略。

2 相关资料

- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由配置指导-R7607
- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

MPLS 基础配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 静态 LSP 配置举例 1
3.1 组网需求 1
3.2 配置思路 2
3.3 使用版本 2
3.4 配置注意事项 2
3.5 配置步骤 2
3.6 验证配置 4
3.7 配置文件 5
4 利用 LDP 动态建立 LSP 配置举例 6
4.1 组网需求 6
4.2 配置思路 7
4.3 使用版本 7
4.4 配置步骤 7
4.5 验证配置 12
4.6 配置文件 13
5 相关资料 17

1 简介

本文档介绍通过静态方式和 LDP（Label Distribution Protocol，标签分发协议）方式建立 LSP 的基本过程。

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

LDP 协议是 MPLS 的一种信令协议，负责划分 FEC、通告 FEC—标签绑定、建立维护 LSP 等。通过 LDP 建立 LSP 消耗资源比较多，但动态建立的 LSP 能根据网络拓扑变化动态调整。因此，LDP 方式建立 LSP 适用于拓扑结构复杂并且不太稳定的大中型网络。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

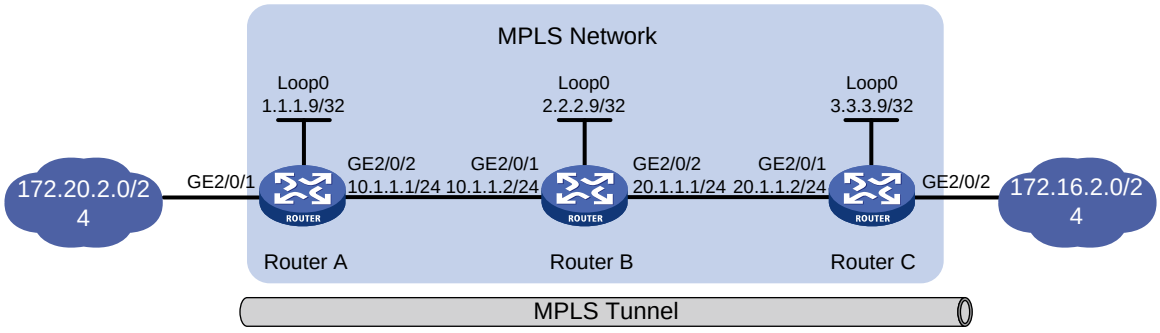
本文档假设您已了解静态 MPLS 特性。

3 静态 LSP 配置举例

3.1 组网需求

如图 1 所示，运营商网络运行 MPLS，Router A 和 Router C 作为 MPLS 的边缘设备，现要求在 172.20.2.0/24 网段和 172.16.2.0/24 网段间，通过配置静态 LSP 隧道，使这两个网段中互访的报文能够通过 LSP 在 MPLS 网络中进行传输。

图1 配置静态 LSP 组网图



3.2 配置思路

- 为了使设备能够按正确的路径转发 MPLS 报文，需要在手工配置 LSP 的标签时，确保上游 LSR 出标签的值就是下游 LSR 入标签的值。
- LSP 是一种单向通道，为了实现数据的双向正常传输，需要在数据传输的两个方向上分别配置一条静态 LSP，并指定各自的入节点、中间节点和出节点。
- 在静态 LSP 环境中，只需要 Ingress 节点上存在到达 FEC 目的地址的路由即可，Transit 和 Egress 节点上无需存在到达 FEC 目的地址的路由，因此本例中使用简单的静态路由即可完成路由配置。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置注意事项

- 通过静态路由配置路由信息时，如果静态路由指定的是出接口，则静态 LSP 必须指定相同的出接口；如果静态路由指定的是下一跳，则静态 LSP 必须指定相同的下一跳。
- 配置 Ingress 和 Transit 时，本地的公网地址不能被指定为下一跳。
- 由于 MPLS 功能会在原有报文上封装一层或多层标签，因此建议用户在使能某接口的 MPLS 功能后，将该接口的 jumboframe 帧功能开启，并根据实际应用和标签嵌套层数配置相应的帧长，避免某些报文因超长而被丢弃。

3.5 配置步骤

(1) 配置各接口的 IP 地址

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

(2) 配置静态路由，使两条 LSP 的 Ingress 节点上存在到达 FEC 目的地址的路由。

配置 Router A。

```
<RouterA> system-view
[RouterA] ip route-static 172.16.2.1 24 10.1.1.2
```

配置 Router C。

```
<RouterC> system-view
[RouterC] ip route-static 172.20.2.1 24 20.1.1.1
```

配置完成后，在 Ingress 设备上执行 **display ip routing-table** 命令，可以看到静态路由已生效。以 Router A 为例：

```
[RouterA] display ip routing-table

Destinations : 18        Routes : 18

Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/32          Direct  0   0           127.0.0.1       InLoop0
1.1.1.9/32          Direct  0   0           127.0.0.1       InLoop0
```

```
10.1.1.0/24        Direct  0   0           10.1.1.1        GE2/0/2
10.1.1.0/32        Direct  0   0           10.1.1.1        GE2/0/2
10.1.1.1/32        Direct  0   0           127.0.0.1       InLoop0
10.1.1.255/32      Direct  0   0           10.1.1.1        GE2/0/2
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
172.16.2.0/24      Static  60  0           10.1.1.2        GE2/0/2
172.20.2.0/24      Direct  0   0           172.20.2.1      GE2/0/1
172.20.2.0/32      Direct  0   0           172.20.2.1      GE2/0/1
172.20.2.1/32      Direct  0   0           127.0.0.1       InLoop0
172.20.2.255/32    Direct  0   0           172.20.2.1      GE2/0/1
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

(3) 使能 MPLS 功能

配置 Router A。

```
[RouterA] mpls lsr-id 1.1.1.9
[RouterA] interface gigabitethernet 2/0/2
[RouterA-GigabitEthernet2/0/2] mpls enable
[RouterA-GigabitEthernet2/0/2] quit
```

配置 Router B。

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

配置 Router C。

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

(4) 创建从 Router A 到 Router C 的静态 LSP

为 Ingress 节点 Router A 配置一条到目的地址 172.16.2.1/24 的静态 LSP，LSP 的名称为 AtoC，下一跳地址为 10.1.1.2，出标签为 30。

```
[RouterA] static-lsp ingress AtoC destination 172.16.2.1 24 nexthop 10.1.1.2 out-label 30
```

为 Transit 节点 Router B 配置一条名为 AtoC 的静态 LSP，入标签为 30，下一跳地址为 20.1.1.2，出标签为 50。

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

为 Egress 节点 Router C 上配置一条名为 AtoC 的静态 LSP，入标签为 50。

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

(5) 创建从 Router C 到 Router A 的静态 LSP

为 Ingress 节点 Router C 配置一条到目的地址 172.20.2.1/24 的静态 LSP，LSP 的名称为 CtoA，下一跳地址为 20.1.1.1，出标签为 40。

```
[RouterC] static-lsp ingress CtoA destination 172.20.2.1 24 nexthop 20.1.1.1 out-label 40
```

为 Transit 节点 Router B 配置一条名为 CtoA 的静态 LSP，入标签为 40，下一跳地址为 10.1.1.1，出标签为 70。

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

为 Egress 节点 Router A 配置一条名为 CtoA 的静态 LSP，入标签为 70。

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

3.6 验证配置

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

```
[RouterA] display mpls static-lsp
Total: 2
Name            FEC               In/Out Label Nexthop/Out Interface    State
AtoC            172.16.2.0/24     NULL/30      10.1.1.2                 Up
CtoA            -/-               70/NULL      -                        Up
```

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

```
[RouterA] ping mpls -a 172.20.2.1 ipv4 172.16.2.0 24
MPLS ping FEC 172.16.2.0/24 with 100 bytes of data:
100 bytes from 20.1.1.2: Sequence=1 time=3 ms
100 bytes from 20.1.1.2: Sequence=2 time=2 ms
100 bytes from 20.1.1.2: Sequence=3 time=2 ms
100 bytes from 20.1.1.2: Sequence=4 time=2 ms
100 bytes from 20.1.1.2: Sequence=5 time=27 ms

--- Ping statistics for FEC 172.16.2.0/24 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
Round-trip min/avg/max = 2/7/27 ms
```

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

```
[RouterC] ping mpls -a 172.16.2.1 ipv4 172.20.2.0 24
MPLS ping FEC 172.20.2.0/24 with 100 bytes of data:
100 bytes from 10.1.1.1: Sequence=1 time=3 ms
100 bytes from 10.1.1.1: Sequence=2 time=2 ms
100 bytes from 10.1.1.1: Sequence=3 time=2 ms
100 bytes from 10.1.1.1: Sequence=4 time=2 ms
100 bytes from 10.1.1.1: Sequence=5 time=27 ms

--- Ping statistics for FEC 172.20.2.0/24 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
Round-trip min/avg/max = 2/7/27 ms
```

3.7 配置文件

- Router A：

```
#
 mpls lsr-id 1.1.1.9
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
ip address 172.20.2.1 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
ip address 10.1.1.1 255.255.255.0
 mpls enable
#
 ip route-static 172.16.2.0 24 10.1.1.2
#
 static-lsp ingress AtoC destination 172.16.2.0 24 nexthop 10.1.1.2 out-label 30
 static-lsp egress CtoA in-label 70
```

- Router B：

```
#
 mpls lsr-id 2.2.2.9
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
ip address 10.1.1.2 255.255.255.0
 mpls enable
#
interface GigabitEthernet2/0/2
 port link-mode route
ip address 20.1.1.1 255.255.255.0
 mpls enable
#
 static-lsp transit AtoC in-label 30 nexthop 20.1.1.2 out-label 50
 static-lsp transit CtoA in-label 40 nexthop 10.1.1.1 out-label 70
```

- Router C：

```
#
 mpls lsr-id 3.3.3.9
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
```

```
#
interface GigabitEthernet2/0/1
 port link-mode route
ip address 20.1.1.2 255.255.255.0
 mpls enable
#
interface GigabitEthernet2/0/2
 port link-mode route
ip address 172.16.2.1 255.255.255.0
#
 ip route-static 172.20.2.1 255.255.255.0 20.1.1.1
#
 static-lsp ingress CtoA destination 172.20.2.0 24 nexthop 20.1.1.1 out-label 40
 static-lsp egress AtoC in-label 50
#
```

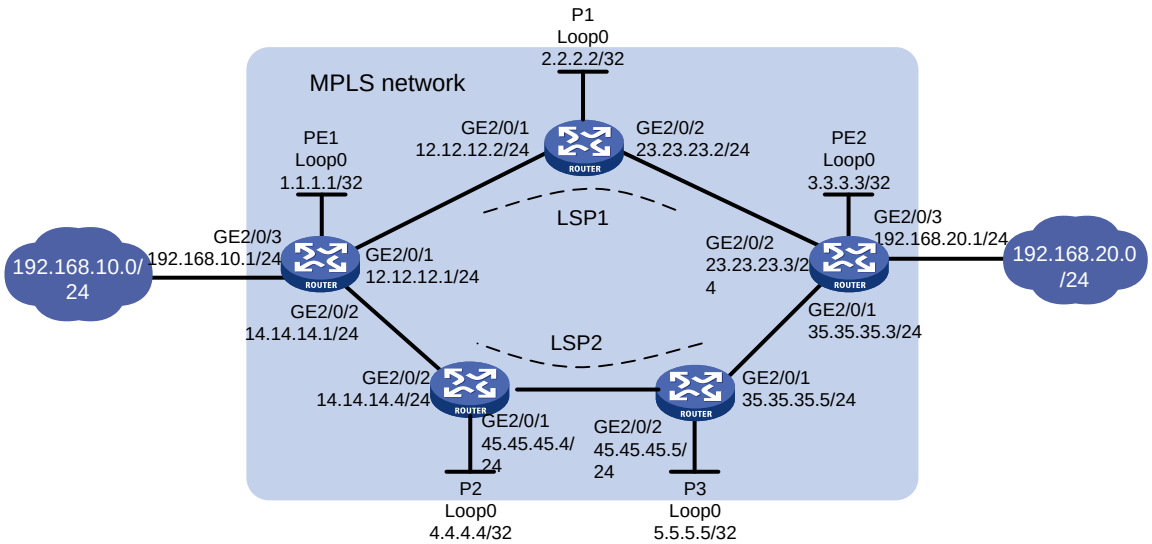
4 利用 LDP 动态建立 LSP 配置举例

4.1 组网需求

如图 2 所示，在运营商网络的 MPLS 区域中，PE 1 和 PE 2 之间有两条路由可达，现要求：

- 在 MPLS 网络中配置 LDP 协议，动态建立 LSP，使 192.168.10.0/24 网段与 192.168.20.0/24 网段之间转发的报文沿建立的 LSP 转发。
- 缺省情况下，报文通过 LSP 1 路径传输；当 P 1 故障时，报文通过 LSP 2 路径传输。
- 所有设备上只允许目的地址为 1.1.1.1/32、2.2.2.2/32、3.3.3.3/32、4.4.4.4/32、5.5.5.5/32、192.168.10.0/24 和 192.168.20.0/24 的路由表项触发 LDP 建立 LSP，其他路由表项不能触发 LDP 建立 LSP，以避免建立的 LSP 数量过多，影响设备性能。

图2 动态 LSP 配置组网图



4.2 配置思路

- 为了通过 LDP 动态创建 LSP，需要配置路由协议，使得各设备间路由可达，本例中使用 OSPF 路由协议。
- 为了实现缺省情况下报文通过 LSP 1 路径传输，并且当 P 1 故障时，报文通过 LSP 2 路径传输，需要配置 192.168.10.0/24 和 192.168.20.0/24 之间的主路由为 LSP 1，备份路由为 LSP 2（本例通过配置 OSPF 路由协议来实现：使能 OSPF 协议后，会自动计算出 LSP 1 路径的开销小于 LSP 2，所以走 LSP 1）。
- 为了只允许目的地址为 1.1.1.1/32、2.2.2.2/32、3.3.3.3/32、4.4.4.4/32、5.5.5.5/32、192.168.10.0/24 和 192.168.20.0/24 的路由表项触发 LDP 建立 LSP，需要配置 LSP 触发策略。

4.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.4 配置步骤

(1) 配置各接口的 IP 地址

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

(2) 配置 OSPF，以保证各路由器之间路由可达

配置 PE 1。

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 14.14.14.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 192.168.10.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

配置 P 1。

```
[P1] ospf
[P1-ospf-1] area 0
[P1-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[P1-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0] quit
[P1-ospf-1] quit
```

配置 P 2。

```
[P2] ospf
[P2-ospf-1] area 0
[P2-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[P2-ospf-1-area-0.0.0.0] network 14.14.14.0 0.0.0.255
[P2-ospf-1-area-0.0.0.0] network 45.45.45.0 0.0.0.255
```

```
[P2-ospf-1-area-0.0.0.0] quit
[P2-ospf-1] quit
```

配置 P 3。

```
[P3] ospf
[P3-ospf-1] area 0
[P3-ospf-1-area-0.0.0.0] network 5.5.5.5 0.0.0.0
[P3-ospf-1-area-0.0.0.0] network 45.45.45.0 0.0.0.255
[P3-ospf-1-area-0.0.0.0] network 35.35.35.0 0.0.0.255
[P3-ospf-1-area-0.0.0.0] quit
[P3-ospf-1] quit
```

配置 PE2。

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 35.35.35.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

配置完成后，在各路由器上执行 **display ospf routing** 命令，可以看到相互之间都学到了到对方的路由。以 PE1 为例：

```
[PE1] display ospf routing

       OSPF Process 1 with Router ID 1.1.1.1
                  Routing Table

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 45.45.45.0/24      2        Transit 14.14.14.4      5.5.5.5         0.0.0.0
 35.35.35.0/24      3        Transit 14.14.14.4      5.5.5.5         0.0.0.0
 35.35.35.0/24      3        Transit 12.12.12.2      5.5.5.5         0.0.0.0
 192.168.10.0/24    1        Stub    192.168.10.1    1.1.1.1         0.0.0.0
 5.5.5.5/32         2        Stub    14.14.14.4      5.5.5.5         0.0.0.0
 14.14.14.0/24      1        Transit 14.14.14.1      4.4.4.4         0.0.0.0
 23.23.23.0/24      2        Transit 12.12.12.2      3.3.3.3         0.0.0.0
 4.4.4.4/32         1        Stub    14.14.14.4      4.4.4.4         0.0.0.0
 3.3.3.3/32         2        Stub    12.12.12.2      3.3.3.3         0.0.0.0
 12.12.12.0/24      1        Transit 12.12.12.1      2.2.2.2         0.0.0.0
 2.2.2.2/32         1        Stub    12.12.12.2      2.2.2.2         0.0.0.0
 1.1.1.1/32         0        Stub    1.1.1.1         1.1.1.1         0.0.0.0
 192.168.20.0/24    3        Stub    12.12.12.2      3.3.3.3         0.0.0.0
```

PE 1 和 P 1、P 2，P 2、P 3 和 PE 2 之间应建立起 OSPF 邻居关系，执行 **display ospf peer verbose** 命令可以看到邻居达到 FULL 状态。以 PE 1 为例：

```
[PE1] display ospf peer verbose
          OSPF Process 1 with Router ID 1.1.1.1
                  Neighbors
```

```
 Area 0.0.0.0 interface 14.14.14.1(GigabitEthernet2/0/2)'s neighbors
 Router ID: 4.4.4.4          Address: 14.14.14.4       GR state: Normal
   State: Full  Mode: Nbr is master  Priority: 1
   DR: 14.14.14.4  BDR: 14.14.14.1  MTU: 0
   Options is 0x42 (-|O|-|-|-|-|E|-)
   Dead timer due in 40  sec
   Neighbor is up for 00:03:30
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled

                 Neighbors

 Area 0.0.0.0 interface 12.12.12.1(GigabitEthernet2/0/1)'s neighbors
 Router ID: 2.2.2.2          Address: 12.12.12.2       GR state: Normal
   State: Full  Mode: Nbr is master  Priority: 1
   DR: 12.12.12.2  BDR: 12.12.12.1  MTU: 0
   Options is 0x42 (-|O|-|-|-|-|E|-)
   Dead timer due in 36  sec
   Neighbor is up for 00:03:24
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled

 Last Neighbor Down Event:
 Router ID: 4.4.4.4
 Local Address: 14.14.14.1
 Remote Address: 14.14.14.4
 Time: May 14 09:07:19 2017
 Reason: Reset ospf command was performed
```

(3) 配置 MPLS 基本能力，并使能 LDP

配置 PE 1。

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] interface gigabitethernet 2/0/1
[PE1-GigabitEthernet2/0/1] mpls enable
[PE1-GigabitEthernet2/0/1] mpls ldp enable
[PE1-GigabitEthernet2/0/1] quit
[PE1] interface gigabitethernet 2/0/2
[PE1-GigabitEthernet2/0/2] mpls enable
[PE1-GigabitEthernet2/0/2] mpls ldp enable
[PE1-GigabitEthernet2/0/2] quit
```

配置 P 1。

```
[P1] mpls lsr-id 2.2.2.2
[P1] mpls ldp
```

```
[P1-ldp] quit
[P1] interface gigabitethernet 2/0/1
[P1-GigabitEthernet2/0/1] mpls enable
[P1-GigabitEthernet2/0/1] mpls ldp enable
[P1-GigabitEthernet2/0/1] quit
[P1] interface gigabitethernet 2/0/2
[P1-GigabitEthernet2/0/2] mpls enable
[P1-GigabitEthernet2/0/2] mpls ldp enable
[P1-GigabitEthernet2/0/2] quit
```

配置 P 2。

```
[P2] mpls lsr-id 4.4.4.4
[P2] mpls ldp
[P2-ldp] quit
[P2] interface gigabitethernet 2/0/1
[P2-GigabitEthernet2/0/1] mpls enable
[P2-GigabitEthernet2/0/1] mpls ldp enable
[P2-GigabitEthernet2/0/1] quit
[P2] interface gigabitethernet 2/0/2
[P2-GigabitEthernet2/0/2] mpls enable
[P2-GigabitEthernet2/0/2] mpls ldp enable
[P2-GigabitEthernet2/0/2] quit
```

配置 P 3。

```
[P3] mpls lsr-id 5.5.5.5
[P3] mpls ldp
[P3-ldp] quit
[P3] interface gigabitethernet 2/0/1
[P3-GigabitEthernet2/0/1] mpls enable
[P3-GigabitEthernet2/0/1] mpls ldp enable
[P3-GigabitEthernet2/0/1] quit
[P3] interface gigabitethernet 2/0/2
[P3-GigabitEthernet2/0/2] mpls enable
[P3-GigabitEthernet2/0/2] mpls ldp enable
[P3-GigabitEthernet2/0/2] quit
```

配置 PE2。

```
[PE2] mpls lsr-id 3.3.3.3
[PE2] mpls ldp
[PE2-ldp] quit
[PE2] interface gigabitethernet 2/0/1
[PE2-GigabitEthernet2/0/1] mpls enable
[PE2-GigabitEthernet2/0/1] mpls ldp enable
[PE2-GigabitEthernet2/0/1] quit
[PE2] interface gigabitethernet 2/0/2
[PE2-GigabitEthernet2/0/2] mpls enable
[PE2-GigabitEthernet2/0/2] mpls ldp enable
[PE2-GigabitEthernet2/0/2] quit
```

完成上述配置后，PE 1 和 P 1、P 2，P 2、P 3 和 PE 2 之间的本地 LDP 会话建立成功。

在各设备上执行 **display mpls ldp peer** 命令，可以看到 LDP 的对等体情况。以 PE1 为例：

```
[PE1] display mpls ldp peer
Total number of peers: 2
Peer LDP ID             State         Role     GR   MD5  KA Sent/Rcvd
2.2.2.2:0               Operational   Passive  Off  Off  55/55
4.4.4.4:0               Operational   Passive  Off  Off  6/6
```

(4) 配置LSP的触发策略，为目的地址为1.1.1.1/32、2.2.2.2/32、3.3.3.3/32、4.4.4.4/32、5.5.5.5/32、192.168.10.0/24 和 192.168.20.0/24 的路由表项建立 LSP

在PE 1上创建IP地址前缀列表PE1，并配置只有通过该列表过滤的路由表项能够触发LDP建立 LSP。

```
[PE1] ip prefix-list PE1 index 10 permit 1.1.1.1 32
[PE1] ip prefix-list PE1 index 20 permit 2.2.2.2 32
[PE1] ip prefix-list PE1 index 30 permit 3.3.3.3 32
[PE1] ip prefix-list PE1 index 40 permit 4.4.4.4 32
[PE1] ip prefix-list PE1 index 50 permit 5.5.5.5 32
[PE1] ip prefix-list PE1 index 60 permit 192.168.10.0 24
[PE1] ip prefix-list PE1 index 70 permit 192.168.20.0 24
[PE1] mpls ldp
[PE1-ldp] lsp-trigger prefix-list PE1
[PE1-ldp] quit
```

在 P 1 上创建 IP 地址前缀列表 P1，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[P1] ip prefix-list P1 index 10 permit 1.1.1.1 32
[P1] ip prefix-list P1 index 20 permit 2.2.2.2 32
[P1] ip prefix-list P1 index 30 permit 3.3.3.3 32
[P1] ip prefix-list P1 index 40 permit 4.4.4.4 32
[P1] ip prefix-list P1 index 50 permit 5.5.5.5 32
[P1] ip prefix-list P1 index 60 permit 192.168.10.0 24
[P1] ip prefix-list P1 index 70 permit 192.168.20.0 24
[P1] mpls ldp
[P1-ldp] lsp-trigger prefix-list P1
[P1-ldp] quit
```

在 P 2 上创建 IP 地址前缀列表 P2，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[P2] ip prefix-list P2 index 10 permit 1.1.1.1 32
[P2] ip prefix-list P2 index 20 permit 2.2.2.2 32
[P2] ip prefix-list P2 index 30 permit 3.3.3.3 32
[P2] ip prefix-list P2 index 40 permit 4.4.4.4 32
[P2] ip prefix-list P2 index 50 permit 5.5.5.5 32
[P2] ip prefix-list P2 index 60 permit 192.168.10.0 24
[P2] ip prefix-list P2 index 70 permit 192.168.20.0 24
[P2] mpls ldp
[P2-ldp] lsp-trigger prefix-list P2
[P2-ldp] quit
```

在 P 3 上创建 IP 地址前缀列表 P3，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[P3] ip prefix-list P3 index 10 permit 1.1.1.1 32
[P3] ip prefix-list P3 index 20 permit 2.2.2.2 32
[P3] ip prefix-list P3 index 30 permit 3.3.3.3 32
[P3] ip prefix-list P3 index 40 permit 4.4.4.4 32
[P3] ip prefix-list P3 index 50 permit 5.5.5.5 32
[P3] ip prefix-list P3 index 60 permit 192.168.10.0 24
[P3] ip prefix-list P3 index 70 permit 192.168.20.0 24
[P3] mpls ldp
[P3-ldp] lsp-trigger prefix-list P3
[P3-ldp] quit
```

在 PE 2 上创建 IP 地址前缀列表 PE 2，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[PE2] ip prefix-list PE2 index 10 permit 1.1.1.1 32
[PE2] ip prefix-list PE2 index 20 permit 2.2.2.2 32
[PE2] ip prefix-list PE2 index 30 permit 3.3.3.3 32
[PE2] ip prefix-list PE2 index 40 permit 4.4.4.4 32
[PE2] ip prefix-list PE2 index 50 permit 5.5.5.5 32
[PE2] ip prefix-list PE2 index 60 permit 192.168.10.0 24
[PE2] ip prefix-list PE2 index 70 permit 192.168.20.0 24
[PE2] mpls ldp
[PE2-ldp] lsp-trigger prefix-list PE2
[PE2-ldp] quit
```

4.5 验证配置

配置完成后，在 PE 1 上执行 **display mpls ldp lsp** 命令，查看 LDP LSP 的建立情况，可以看到去往 192.168.20.0/24 网段的 LSP 缺省下一跳指向 P 1。

```
[PE1] display mpls ldp lsp
Status Flags: * - stale, L - liberal
Statistics:
  FECs: 7      Ingress LSPs: 5     Transit LSPs: 5     Egress LSPs: 2

FEC                In/Out Label    Nexthop         OutInterface
1.1.1.1/32         3/-
                   -/1151(L)
                   -/1151(L)
2.2.2.2/32         -/3             12.12.12.2      GE2/0/1
                   1151/3          12.12.12.2      GE2/0/1
                   -/1150(L)
3.3.3.3/32         -/1150          12.12.12.2      GE2/0/1
                   1150/1150       12.12.12.2      GE2/0/1
                   -/1148(L)
4.4.4.4/32         -/1149(L)
                   -/3             14.14.14.4      GE2/0/2
                   1149/3          14.14.14.4      GE2/0/2
```

```
5.5.5.5/32          -/1148(L)
                    -/1149          14.14.14.4      GE2/0/2
                    1148/1149       14.14.14.4      GE2/0/2
192.168.10.0/24     1147/-
192.168.20.0/24     -/1147          12.12.12.2      GE2/0/1
                    1146/1147       12.12.12.2      GE2/0/1
                    -/1147(L)
```

当 P 1 故障时，在 PE 1 上执行 **display mpls ldp lsp** 命令，查看 LDP LSP 的变化，可以看到去往 192.168.20.0/24 网段的 LSP 下一跳指向 P 2。

```
[PE1] display mpls ldp lsp
Status Flags: * - stale, L - liberal
Statistics:
  FECs: 7      Ingress LSPs: 5     Transit LSPs: 5     Egress LSPs: 2

FEC                 In/Out Label    Nexthop         OutInterface
1.1.1.1/32          3/-
                    -/1150(L)
2.2.2.2/32          -/1149          14.14.14.4      GE2/0/2
                    1150/1149       14.14.14.4      GE2/0/2
3.3.3.3/32          -/1148          14.14.14.4      GE2/0/2
                    1147/1148       14.14.14.4      GE2/0/2
4.4.4.4/32          -/3             14.14.14.4      GE2/0/2
                    1149/3          14.14.14.4      GE2/0/2
5.5.5.5/32          -/1151          14.14.14.4      GE2/0/2
                    1148/1151       14.14.14.4      GE2/0/2
192.168.10.0/24     1151/-
                    -/1146(L)
192.168.20.0/24     -/1147          14.14.14.4      GE2/0/2
                    1146/1147       14.14.14.4      GE2/0/2
```

使用 MPLS ping 检测 MPLS LSP 的有效性和可达性。

```
[PE1] ping mpls -a 192.168.10.1 ipv4 192.168.20.0 24
MPLS ping FEC 192.168.20.0/24 with 100 bytes of data:
100 bytes from 23.23.23.3: Sequence=1 time=2 ms
100 bytes from 23.23.23.3: Sequence=2 time=2 ms
100 bytes from 23.23.23.3: Sequence=3 time=2 ms
100 bytes from 23.23.23.3: Sequence=4 time=2 ms
100 bytes from 23.23.23.3: Sequence=5 time=2 ms

--- Ping statistics for FEC 192.168.20.0/24 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
Round-trip min/avg/max = 2/2/2 ms
```

4.6 配置文件

- PE1：

```
#
ospf 1
```

```
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 12.12.12.0 0.0.0.255
  network 14.14.14.0 0.0.0.255
  network 192.168.10.0 0.0.0.255
#
 mpls lsr-id 1.1.1.1
#
mpls ldp
 lsp-trigger prefix-list PE1
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
ip address 12.12.12.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
ip address 14.14.14.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet2/0/3
 port link-mode route
ip address 192.168.10.1 255.255.255.0
#
 ip prefix-list PE1 index 10 permit 1.1.1.1 32
 ip prefix-list PE1 index 20 permit 2.2.2.2 32
 ip prefix-list PE1 index 30 permit 3.3.3.3 32
 ip prefix-list PE1 index 40 permit 4.4.4.4 32
 ip prefix-list PE1 index 50 permit 5.5.5.5 32
 ip prefix-list PE1 index 60 permit 192.168.10.0 24
 ip prefix-list PE1 index 70 permit 192.168.20.0 24
```

- P 1：

```
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 12.12.12.0 0.0.0.255
  network 23.23.23.0 0.0.0.255
#
 mpls lsr-id 2.2.2.2
#
mpls ldp
```

```
 lsp-trigger prefix-list P1
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
ip address 12.12.12.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
ip address 23.23.23.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
 ip prefix-list P1 index 10 permit 1.1.1.1 32
 ip prefix-list P1 index 20 permit 2.2.2.2 32
 ip prefix-list P1 index 30 permit 3.3.3.3 32
 ip prefix-list P1 index 40 permit 4.4.4.4 32
 ip prefix-list P1 index 50 permit 5.5.5.5 32
 ip prefix-list P1 index 60 permit 192.168.10.0 24
 ip prefix-list P1 index 70 permit 192.168.20.0 24
#
```

- P 2：

```
#
ospf 1
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 14.14.14.0 0.0.0.255
  network 45.45.45.0 0.0.0.255
#
 mpls lsr-id 4.4.4.4
#
mpls ldp
 lsp-trigger prefix-list P2
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
ip address 45.45.45.4 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet2/0/2
```

```
port link-mode route
 ip address 14.14.14.4 255.255.255.0
 mpls enable
 mpls ldp enable
#
 ip prefix-list P2 index 10 permit 1.1.1.1 32
 ip prefix-list P2 index 20 permit 2.2.2.2 32
 ip prefix-list P2 index 30 permit 3.3.3.3 32
 ip prefix-list P2 index 40 permit 4.4.4.4 32
 ip prefix-list P2 index 50 permit 5.5.5.5 32
 ip prefix-list P2 index 60 permit 192.168.10.0 24
 ip prefix-list P2 index 70 permit 192.168.20.0 24
#
```

- P 3：

```
#
ospf 1
 area 0.0.0.0
  network 5.5.5.5 0.0.0.0
  network 35.35.35.0 0.0.0.255
  network 45.45.45.0 0.0.0.255
#
 mpls lsr-id 5.5.5.5
#
mpls ldp
 lsp-trigger prefix-list P3
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
ip address 35.35.35.5 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet2/0/1
 port link-mode route
ip address 45.45.45.5 255.255.255.0
 mpls enable
 mpls ldp enable
#
 ip prefix-list P3 index 10 permit 1.1.1.1 32
 ip prefix-list P3 index 20 permit 2.2.2.2 32
 ip prefix-list P3 index 30 permit 3.3.3.3 32
 ip prefix-list P3 index 40 permit 4.4.4.4 32
 ip prefix-list P3 index 50 permit 5.5.5.5 32
 ip prefix-list P3 index 60 permit 192.168.10.0 24
 ip prefix-list P3 index 70 permit 192.168.20.0 24
```

```
#
```

- PE2：

```
#
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 23.23.23.0 0.0.0.255
  network 33.0.0.0 0.0.0.255
  network 192.168.20.0 0.0.0.255
#
 mpls lsr-id 3.3.3.3
#
mpls ldp
 lsp-trigger prefix-list PE2
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
ip address 35.35.35.3 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
ip address 23.23.23.3 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet2/0/3
 port link-mode route
ip address 192.168.20.1 255.255.255.0
#
 ip prefix-list PE2 index 10 permit 1.1.1.1 32
 ip prefix-list PE2 index 20 permit 2.2.2.2 32
 ip prefix-list PE2 index 30 permit 3.3.3.3 32
 ip prefix-list PE2 index 40 permit 4.4.4.4 32
 ip prefix-list PE2 index 50 permit 5.5.5.5 32
 ip prefix-list PE2 index 60 permit 192.168.10.0 24
 ip prefix-list PE2 index 70 permit 192.168.20.0 24
#
```

5 相关资料

- H3C SR6600 SR6600-X 路由器 MPLS 配置指导-R7607
- H3C SR6600 SR6600-X 路由器 MPLS 命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

MPLS L3VPN 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 配置举例 1
3.1 组网需求 1
3.2 配置思路 2
3.3 使用版本 2
3.4 配置注意事项 2
3.5 配置步骤 2
3.6 验证配置 10
3.7 配置文件 10
4 相关资料 14

1 简介

本文介绍了通过 MPLS L3VPN 技术提供 VPN 服务的典型配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

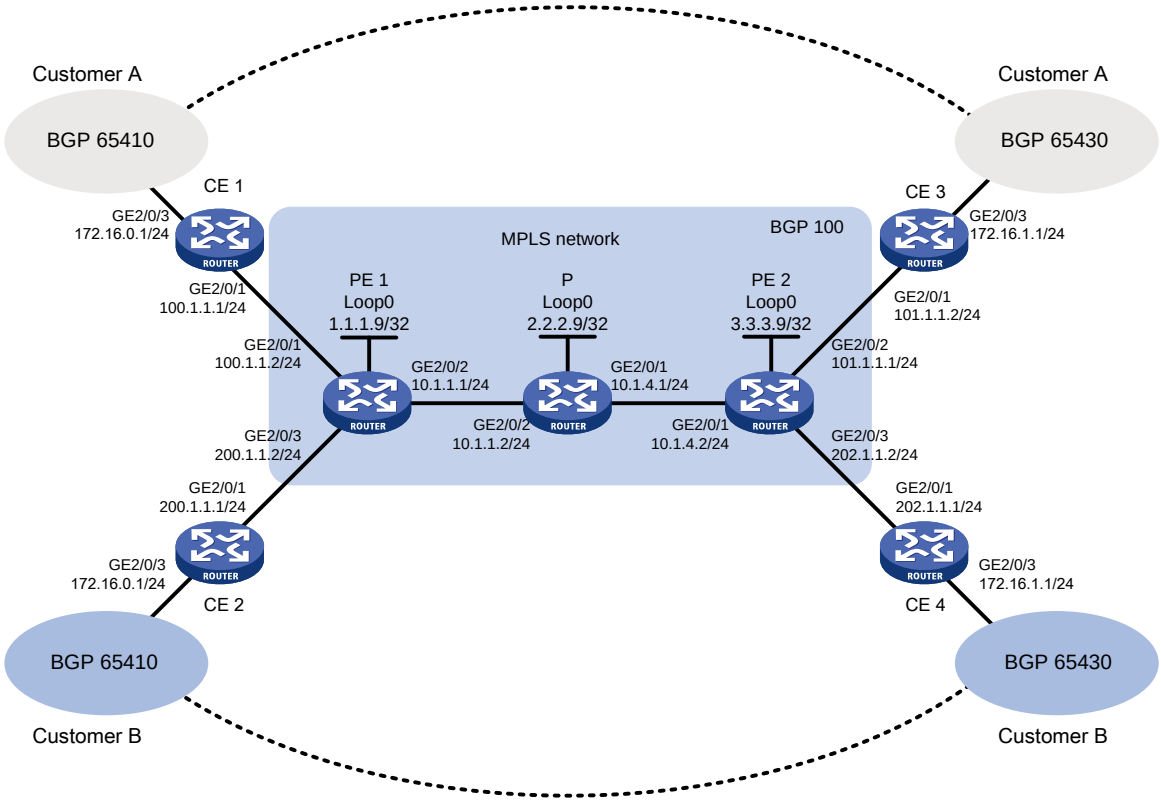
本文档假设您已了解 MPLS L3VPN 特性。

3 配置举例

3.1 组网需求

如图 1 所示，Customer A 和 Customer B 分别有位于两地的分支机构，现要求通过 MPLS L3VPN 技术，实现用户分支机构间路由信息的正常交互，且用户数据可以通过 VPN 方式在各站点间安全传输，不会发送至私网 IP 地址相同的其它用户站点中。

图1 MPLS L3VPN 基本组网图



3.2 配置思路

- 为了使报文能够通过 MPLS 网络传输，需要在 MPLS 骨干网络中配置 IGP 路由协议，并利用 LDP 分发公网标签，作为 VPN 报文的外层标签。
- 为区分不同用户的路由信息，需要在 PE 上分别创建两个 VPN 实例，并为 VPN 实例配置 RD 和 RT，在各实例内通过 BGP 分别引入不同用户的私网路由。
- 在 PE 设备之间配置 MP-BGP 协议并建立对等体，用于传输 VPN 的私网路由信息并分发内层标签，即私网标签。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置注意事项

由于在配置接口与 VPN 实例绑定后，接口上的 IP 地址等配置会清除，因此先配置接口与 VPN 实例的绑定关系，再进行其他配置。

3.5 配置步骤

1. 在 MPLS 骨干网上配置 IGP 协议（本例为 OSPF 协议），实现骨干网 PE 和 P 的互通

(1) 配置 PE 1

配置骨干网接口以及环回口地址。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.9 32
[PE1-LoopBack0] quit
[PE1] interface gigabitethernet 2/0/2
[PE1-GigabitEthernet2/0/2] ip address 10.1.1.1 24
[PE1-GigabitEthernet2/0/2] quit
```

配置 OSPF 协议发布骨干网侧路由。

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

(2) 配置 P

配置骨干网接口以及环回口地址。

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 2.2.2.9 32
[P-LoopBack0] quit
[P] interface gigabitethernet 2/0/2
[P-GigabitEthernet2/0/2] ip address 10.1.1.2 24
```

```
[P-GigabitEthernet2/0/2] quit
[P] interface gigabitethernet 2/0/1
[P-GigabitEthernet2/0/1] ip address 10.1.4.1 24
[P-GigabitEthernet2/0/1] quit
```

配置 OSPF 协议发布骨干网侧路由。

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.1.4.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

(3) 配置 PE 2

配置骨干网接口以及环回口地址。

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 3.3.3.9 32
[PE2-LoopBack0] quit
[PE2] interface gigabitethernet 2/0/1
[PE2-GigabitEthernet2/0/1] ip address 10.1.4.2 24
[PE2-GigabitEthernet2/0/1] quit
```

配置 OSPF 协议发布骨干网侧路由。

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 10.1.4.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

配置完成后，PE 1、P、PE 2 之间应能建立 OSPF 邻居，执行 **display ospf peer** 命令可以看到邻居达到 Full 状态。执行 **display ip routing-table** 命令可以看到 PE 之间学习到对方的 Loopback 路由。

以 PE 1 为例：

```
[PE1] display ospf peer verbose

          OSPF Process 1 with Router ID 1.1.1.9
                  Neighbors

 Area 0.0.0.0 interface 10.1.1.1(GE2/0/2)'s neighbors
 Router ID: 2.2.2.9          Address: 10.1.1.2        GR State: Normal
   State: Full  Mode: Nbr is Master  Priority: 1
   DR: 10.1.1.2  BDR: 10.1.1.1  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 38  sec
   Neighbor is up for 17:30:25
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled
```

```
[PE1] display ip routing-table protocol ospf

Summary Count : 5

OSPF Routing table Status : <Active>
Summary Count : 3

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
2.2.2.9/32          OSPF    10   1            10.1.1.2        GE2/0/2
3.3.3.9/32          OSPF    10   2            10.1.1.2        GE2/0/2
10.1.4.0/24         OSPF    10   2            10.1.1.2        GE2/0/2


OSPF Routing table Status : <Inactive>
Summary Count : 2

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
1.1.1.9/32          OSPF    10   0            0.0.0.0         Loop0
10.1.1.0/24         OSPF    10   1            0.0.0.0        GE2/0/2
```

2. 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP

(1) 配置 PE 1

```
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] interface gigabitethernet 2/0/2
[PE1-GigabitEthernet2/0/2] mpls enable
[PE1-GigabitEthernet2/0/2] mpls ldp enable
[PE1-GigabitEthernet2/0/2] quit
```

(2) 配置 P

```
[P] mpls lsr-id 2.2.2.9
[P] mpls ldp
[P-ldp] quit
[P] interface gigabitethernet 2/0/2
[P-GigabitEthernet2/0/2] mpls enable
[P-GigabitEthernet2/0/2] mpls ldp enable
[P-GigabitEthernet2/0/2] quit
[P] interface gigabitethernet 2/0/1
[P-GigabitEthernet2/0/1] mpls enable
[P-GigabitEthernet2/0/1] mpls ldp enable
[P-GigabitEthernet2/0/1] quit
```

(3) 配置 PE 2

```
[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls ldp
[PE2-ldp] quit
[PE2] interface gigabitethernet 2/0/1
[PE2-GigabitEthernet2/0/1] mpls enable
```

```
[PE2-GigabitEthernet2/0/1] mpls ldp enable
[PE2-GigabitEthernet2/0/1] quit
```

上述配置完成后，PE 1、P、PE 2 之间应能建立 LDP 会话，执行 **display mpls ldp peer** 命令可以看到 LDP 会话的状态为 Operational。执行 **display mpls ldp lsp** 命令，可以看到 LDP LSP 的建立情况。

以 PE 1 为例：

```
[PE1] display mpls ldp peer
Total number of peers: 1
Peer LDP ID             State         Role     GR   MD5  KA Sent/Rcvd
2.2.2.9:0               Operational   Passive  Off  Off  5/5
[PE1] display mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup
FECs: 4            Ingress: 1          Transit: 1      Egress: 3

FEC                In/Out Label        Nexthop         OutInterface
1.1.1.9/32         3/-
                   -/1151(L)
2.2.2.9/32         -/3                 10.1.1.2        GE2/0/2
                   1151/3              10.1.1.2        GE2/0/2
3.3.3.9/32         -/1150              10.1.1.2        GE2/0/2
                   1150/1150           10.1.1.2        GE2/0/2
```

3. 在 PE 设备上配置 VPN 实例，将 CE 接入 PE

(1) 配置 PE 1

在 PE 1 上为 Customer A 创建 VPN 实例，名为“customerA”。

```
[PE1] ip vpn-instance customerA
```

为该实例配置 RD 为 100:1，用于形成 VPNv4 路由，以便区分不同用户相同网段的路由。

```
[PE1-vpn-instance-customerA] route-distinguisher 100:1
```

为该 VPN 实例配置 VPN Target 属性，其中接收路由的属性为 111:1，发布路由的属性为 222:1。（此处为表示接收和发送属性的含义，取值有所不同，为便于管理，用户可以将接收和发送的属性配置为相同的值）

```
[PE1-vpn-instance-customerA] vpn-target 111:1 import-extcommunity
[PE1-vpn-instance-customerA] vpn-target 222:1 export-extcommunity
[PE1-vpn-instance-customerA] quit
```

按同样方式为 Customer B 创建 VPN 实例，名为“customerB”，并为其配置 RD 为 200:1，接收和发送的 VPN Target 属性分别为 333:1 和 444:1。

```
[PE1] ip vpn-instance customerB
[PE1-vpn-instance-customerB] route-distinguisher 200:1
[PE1-vpn-instance-customerB] vpn-target 333:1 import-extcommunity
[PE1-vpn-instance-customerB] vpn-target 444:1 export-extcommunity
[PE1-vpn-instance-customerB] quit
```

配置 GigabitEthernet 2/0/1 与 VPN 实例 customerA 进行绑定。

```
[PE1] interface gigabitethernet 2/0/1
[PE1-GigabitEthernet2/0/1] ip binding vpn-instance customerA
[PE1-GigabitEthernet2/0/1] ip address 100.1.1.2 24
[PE1-GigabitEthernet2/0/1] quit
```

配置 GigabitEthernet 2/0/3 与 VPN 实例 customerB 进行绑定。

```
[PE1] interface gigabitethernet 2/0/3
[PE1-GigabitEthernet2/0/3] ip binding vpn-instance customerB
[PE1-GigabitEthernet2/0/3] ip address 200.1.1.2 24
[PE1-GigabitEthernet2/0/3] quit
```

(2) 配置 PE 2

在 PE 2 上为 Customer A 创建 VPN 实例，名为“customerA”。

```
[PE2] ip vpn-instance customerA
```

为该 VPN 实例配置 RD，为便于识别，建议与 PE 1 上为该实例配置的 RD 保持一致。

```
[PE2-vpn-instance-customerA] route-distinguisher 100:1
```

为该 VPN 实例配置 VPN Target，需要注意的是接收和发送的属性要分别与 PE 1 上配置的发送和接收的属性保持一致。

```
[PE2-vpn-instance-customerA] vpn-target 222:1 import-extcommunity
[PE2-vpn-instance-customerA] vpn-target 111:1 export-extcommunity
[PE2-vpn-instance-customerA] quit
```

按同样方式配置 VPN 实例“customerB”，并配置相应的 RD 和 VPN Target。

```
[PE2] ip vpn-instance customerB
[PE2-vpn-instance-customerB] route-distinguisher 200:1
[PE2-vpn-instance-customerB] vpn-target 444:1 import-extcommunity
[PE2-vpn-instance-customerB] vpn-target 333:1 export-extcommunity
[PE2-vpn-instance-customerB] quit
```

分别将 GigabitEthernet2/0/2 和 GigabitEthernet2/0/3 与 customerA 和 customerB 实例进行绑定。

```
[PE2] interface gigabitethernet 2/0/2
[PE2-GigabitEthernet2/0/2] ip binding vpn-instance customerA
[PE2-GigabitEthernet2/0/2] ip address 101.1.1.1 24
[PE2-GigabitEthernet2/0/2] quit
[PE2] interface gigabitethernet 2/0/3
[PE2-GigabitEthernet2/0/3] ip binding vpn-instance customerB
[PE2-GigabitEthernet2/0/3] ip address 202.1.1.2 24
[PE2-GigabitEthernet2/0/3] quit
```

(3) 配置 CE

按图 1 配置各 CE 的接口 IP 地址，配置过程略。

配置完成后，在 PE 设备上执行 **display ip vpn-instance** 命令可以看到 VPN 实例的配置情况。各 PE 能 ping 通自己接入的 CE。

以 PE 1 和 CE 1 为例：

```
[PE1] display ip vpn-instance
  Total VPN-Instances configured : 2
  VPN-Instance Name               RD                     Create time
  customerA                       100:1                  2017/03/22 13:20:08
  customerB                       200:1                  2017/03/22 13:20:20
[PE1] ping -vpn-instance customerA 100.1.1.1
Ping 10.1.1.1 (100.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 100.1.1.1: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 100.1.1.1: icmp_seq=1 ttl=255 time=2.000 ms
```

```
56 bytes from 100.1.1.1: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 100.1.1.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 100.1.1.1: icmp_seq=4 ttl=255 time=0.000 ms

--- Ping statistics for 10.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.800/2.000/0.748 ms
```

4. 在 PE 与 CE 之间建立 EBGP 对等体，引入 VPN 路由

(1) 配置 PE 1

在 PE 1 上创建 BGP 进程 100。

```
[PE1] bgp 100
```

将 CE 1 指定为对等体，并将 PE 1 的直连路由引入到 BGP-VPN 实例路由表中。

```
[PE1-bgp] ip vpn-instance customerA
[PE1-bgp-customerA] peer 100.1.1.1 as-number 65410
[PE1-bgp-customerA] address-family ipv4 unicast
[PE1-bgp-ipv4-customerA] peer 100.1.1.1 enable
[PE1-bgp-ipv4-customerA] import-route direct
[PE1-bgp-ipv4-customerA] quit
[PE1-bgp-customerA] quit
```

将 CE 2 指定为对等体，并将 PE 1 的直连路由引入到 BGP-VPN 实例路由表中。

```
[PE1-bgp] ip vpn-instance customerB
[PE1-bgp-customerB] peer 200.1.1.1 as-number 65410
[PE1-bgp-customerB] address-family ipv4 unicast
[PE1-bgp-ipv4-customerB] peer 200.1.1.1 enable
[PE1-bgp-ipv4-customerB] import-route direct
[PE1-bgp-ipv4-customerB] quit
[PE1-bgp-customerB] quit
[PE1-bgp] quit
```

(2) 配置 PE 2

在 PE 2 上创建 BGP 进程 100。

```
[PE2] bgp 100
```

将 CE 3 指定为对等体，并将 PE 2 的直连路由引入到 BGP-VPN 实例路由表中。

```
[PE2-bgp] ip vpn-instance customerA
[PE2-bgp-customerA] peer 101.1.1.2 as-number 65430
[PE2-bgp-customerA] address-family ipv4 unicast
[PE2-bgp-ipv4-customerA] peer 101.1.1.2 enable
[PE2-bgp-ipv4-customerA] import-route direct
[PE2-bgp-ipv4-customerA] quit
[PE2-bgp-customerA] quit
```

将 CE 4 指定为对等体，并将 PE 2 的直连路由引入到 BGP-VPN 实例路由表中。

```
[PE2-bgp] ip vpn-instance customerB
[PE2-bgp-customerB] peer 202.1.1.1 as-number 65430
[PE2-bgp-customerB] address-family ipv4 unicast
[PE2-bgp-ipv4-customerB] peer 202.1.1.1 enable
[PE2-bgp-ipv4-customerB] import-route direct
[PE2-bgp-ipv4-customerB] quit
```

```
[PE2-bgp-customerB] quit
[PE2-bgp] quit
```

(3) 配置 CE1

CE 1 上创建 BGP 进程 65410，并指定 PE 1 为对等体，对等体自治系统号为 100。

```
<CE1> system-view
[CE1] bgp 65410
[CE1-bgp] peer 100.1.1.2 as-number 100
```

使能 CE1 与对等体 100.1.1.2 交换 IPv4 单播路由信息的能力。

```
[CE1-bgp] address-family ipv4 unicast
[CE1-bgp-ipv4] peer 100.1.1.2 enable
```

将 CE 1 上连接站点的直连接口路由引入 EBGP。

```
[CE1-bgp-ipv4] import-route direct
[CE1-bgp-ipv4] quit
[CE1-bgp] quit
```

(4) 配置 CE2

CE 2 上创建 BGP 进程 65410，并指定 PE 1 为对等体，对等体自治系统号为 100。

```
<CE2> system-view
[CE2] bgp 65410
[CE2-bgp] peer 200.1.1.2 as-number 100
```

使能 CE2 与对等体 200.1.1.2 交换 IPv4 单播路由信息的能力。

```
[CE2-bgp] address-family ipv4 unicast
[CE2-bgp-ipv4] peer 200.1.1.2 enable
```

将 CE 2 上连接站点的直连接口路由引入 EBGP。

```
[CE2-bgp-ipv4] import-route direct
[CE2-bgp-ipv4] quit
[CE2-bgp] quit
```

(5) 配置 CE3

CE 3 上创建 BGP 进程 65430，并指定 PE 2 为对等体，对等体自治系统号为 100。

```
<CE3> system-view
[CE3] bgp 65430
[CE3-bgp] peer 101.1.1.1 as-number 100
```

使能 CE3 与对等体 101.1.1.1 交换 IPv4 单播路由信息的能力。

```
[CE3-bgp] address-family ipv4 unicast
[CE3-bgp-ipv4] peer 101.1.1.1 enable
```

将 CE 3 上连接站点的直连接口路由引入 EBGP。

```
[CE3-bgp-ipv4] import-route direct
[CE3-bgp-ipv4] quit
[CE3-bgp] quit
```

(6) 配置 CE4

CE4 上创建 BGP 进程 65430，并指定 PE 2 为对等体，对等体自治系统号为 100。

```
<CE4> system-view
[CE4] bgp 65430
[CE4-bgp] peer 202.1.1.2 as-number 100
```

使能 CE4 与对等体 202.1.1.2 交换 IPv4 单播路由信息的能力。

```
[CE4-bgp] address-family ipv4 unicast
[CE4-bgp-ipv4] peer 202.1.1.2 enable
```

将 CE 4 上连接站点的直连接口路由引入 EBGP。

```
[CE4-bgp-ipv4] import-route direct
[CE4-bgp-ipv4] quit
[CE4-bgp] quit
```

配置完成后，在 PE 设备上执行 **display bgp peer ipv4 vpn-instance** 命令，可以看到 PE 与 CE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

以 PE 1 与 CE 1 的对等体关系为例：

```
[PE1] display bgp peer ipv4 vpn-instance customerA
 BGP local router ID: 1.1.1.9
 Local AS number: 100
 Total number of peers: 1                 Peers in established state: 1

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  100.1.1.1            65410        4        4    0       2 13:35:25 Established
```

5. 在 PE 之间建立 MP-IBGP 对等体

(1) 配置 PE 1

在 PE 1 上配置 PE 2 为 BGP 对等体，并指定连接时使用的接口为 Loopback0 接口。

```
[PE1] bgp 100
[PE1-bgp] peer 3.3.3.9 as-number 100
[PE1-bgp] peer 3.3.3.9 connect-interface loopback 0
```

进入 BGP-VPNv4 地址族视图，指定 PE 2 为对等体。

```
[PE1-bgp] address-family vpnv4
[PE1-bgp-vpnv4] peer 3.3.3.9 enable
[PE1-bgp-vpnv4] quit
[PE1-bgp] quit
```

(2) 配置 PE 2

在 PE 2 上配置 PE 1 为 BGP 对等体，并指定连接时使用的接口为 Loopback0 接口。

```
[PE2] bgp 100
[PE2-bgp] peer 1.1.1.9 as-number 100
[PE2-bgp] peer 1.1.1.9 connect-interface loopback 0
```

进入 BGP-VPNv4 地址族视图，指定 PE 1 为对等体。

```
[PE2-bgp] address-family vpnv4
[PE2-bgp-vpnv4] peer 1.1.1.9 enable
[PE2-bgp-vpnv4] quit
[PE2-bgp] quit
```

配置完成后，在 PE 设备上执行 **display bgp peer vpnv4** 命令，可以看到 PE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

```
[PE1] display bgp peer vpnv4

 BGP local router ID: 1.1.1.9
 Local AS number: 100
 Total number of peers: 1                 Peers in established state: 1
```

```
Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

3.3.3.9                100        8        8    0       0 00:00:08 Established
```

3.6 验证配置

在 PE 设备上执行 **display ip routing-table vpn-instance** 命令，可以看到去往对端 CE 的路由。

以 PE 1 上的 customerA 为例：

```
[PE1] display ip routing-table vpn-instance customerA

Destinations : 13        Routes : 13

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
100.1.1.0/24        Direct 0    0            100.1.1.2       GE2/0/1
100.1.1.0/32        Direct 0    0            100.1.1.2       GE2/0/1
100.1.1.2/32        Direct 0    0            127.0.0.1       InLoop0
100.1.1.255/32      Direct 0    0            100.1.1.2       GE2/0/1
101.1.1.0/24        BGP    255  0            3.3.3.9         GE2/0/2
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

同一 VPN 的 CE 能够相互 Ping 通，不同 VPN 的 CE 不能相互 Ping 通。

例如：CE1 能够 Ping 通 CE 3（101.1.1.2），但不能 Ping 通 CE 4（202.1.1.1）。

3.7 配置文件

- PE 1：

```
#
ip vpn-instance customerA
 route-distinguisher 100:1
 vpn-target 111:1 import-extcommunity
 vpn-target 222:1 export-extcommunity
#
ip vpn-instance customerB
 route-distinguisher 200:1
 vpn-target 333:1 import-extcommunity
 vpn-target 444:1 export-extcommunity
#
ospf 1
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
```

```
  network 10.1.1.0 0.0.0.255
#
 mpls lsr-id 1.1.1.9
#
mpls ldp
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip binding vpn-instance customerA
 ip address 100.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet2/0/3
 port link-mode route
 ip binding vpn-instance customerB
 ip address 200.1.1.2 255.255.255.0
#
bgp 100
peer 3.3.3.9 as-number 100
 peer 3.3.3.9 connect-interface LoopBack0
#
 address-family vpnv4
  peer 3.3.3.9 enable
#
ip vpn-instance customerA
  peer 100.1.1.1 as-number 65410
 #
address-family ipv4 unicast
  import-route direct
  peer 100.1.1.1 enable
#
ip vpn-instance customerB
  peer 200.1.1.1 as-number 65410
 #
 address-family ipv4 unicast
  import-route direct
  peer 200.1.1.1 enable
#
```

- P：

```
#
```

```
ospf 1
 area 0.0.0.0
  network 2.2.2.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.4.0 0.0.0.255
#
 mpls lsr-id 2.2.2.9
#
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.1.4.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.1.1.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
```

- PE 2：

```
#
ip vpn-instance customerA
 route-distinguisher 100:1
 vpn-target 111:1 export-extcommunity
 vpn-target 222:1 import-extcommunity
#
ip vpn-instance customerB
 route-distinguisher 200:1
 vpn-target 333:1 export-extcommunity
 vpn-target 444:1 import-extcommunity
#
ospf 1
 area 0.0.0.0
  network 10.1.4.0 0.0.0.255
  network 3.3.3.9 0.0.0.0
#
 mpls lsr-id 3.3.3.9
#
mpls ldp
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
```

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.1.4.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip binding vpn-instance customerA
 ip address 101.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/3
 port link-mode route
 ip binding vpn-instance customerB
 ip address 202.1.1.2 255.255.255.0
#
bgp 100
peer 1.1.1.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack0
 #
address-family vpnv4
  peer 1.1.1.9 enable
#
ip vpn-instance customerA
  peer 101.1.1.2 as-number 65430
#
 address-family ipv4 unicast
  import-route direct
peer 101.1.1.2 enable
 #
ip vpn-instance customerB
  peer 202.1.1.1 as-number 65430
  #
 address-family ipv4 unicast
  import-route direct
peer 202.1.1.1 enable
 #
```

- CE 1：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 100.1.1.1 255.255.255.0
#
bgp 65410
 peer 100.1.1.2 as-number 100
#
address-family ipv4 unicast
```

```
  import-route direct
  peer 100.1.1.2 enable
#
```

- CE 2：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 200.1.1.1 255.255.255.0
#
bgp 65410
peer 200.1.1.2 as-number 100
#
address-family ipv4 unicast
  import-route direct
  peer 200.1.1.2 enable
#
```

- CE 3：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 101.1.1.2 255.255.255.0
#
bgp 65430
 peer 101.1.1.1 as-number 100
#
address-family ipv4 unicast
  import-route direct
  peer 101.1.1.1 enable
#
```

- CE 4：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 202.1.1.1 255.255.255.0
#
bgp 65430
peer 202.1.1.2 as-number 100
#
address-family ipv4 unicast
  import-route direct
  peer 202.1.1.2 enable
#
```

4 相关资料

- H3C SR6600 SR6600-X 路由器 MPLS 配置指导-R7607
- H3C SR6600 SR6600-X 路由器 MPLS 命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

MPLS OAM 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 BFD 检测 LSP 典型配置举例 1
3.1 组网需求 1
3.2 使用版本 2
3.3 配置步骤 2
3.4 验证配置 6
3.5 配置文件 7
4 BFD 检测 MPLS TE 典型配置举例 11
4.1 组网需求 11
4.2 使用版本 11
4.3 配置注意事项 11
4.4 配置步骤 12
4.5 验证配置 14
4.6 配置文件 17
5 相关资料 21

1 简介

本文档介绍 MPLS OAM 配置举例。

MPLS OAM（Operations, Administration and Maintenance，操作、管理和维护）功能为 MPLS 网络提供了数据平面连通性检测、数据平面与控制平面一致性校验、故障点定位等多种错误管理（Fault Management）工具。MPLS OAM 利用这些错误管理工具对 LSP、MPLS TE 隧道和 MPLS PW 进行检测和故障定位，降低了 MPLS 网络的管理和维护的复杂度，提高了 MPLS 网络的可用性。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 MPLS OAM 特性。

3 BFD 检测 LSP 典型配置举例

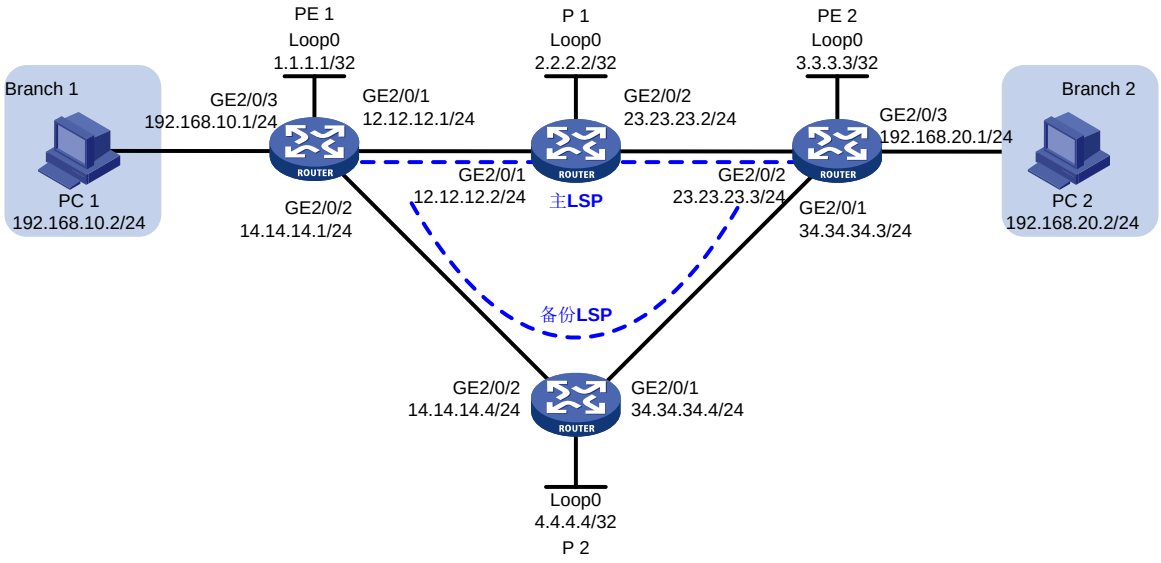
3.1 组网需求

如图 1 所示，某公司有两个位于不同的地理位置的分支机构通过运营商的 MPLS 骨干网互联，两个分支机构之间需要进行实时业务的同步传输。该公司要求运营商提供高可靠性的服务，以保证实时业务的不间断性。

为满足该用户需求，可通过在 MPLS 骨干网中部署 LDP FRR 服务来提供主备两条 LSP 链路，并配置 LDP 与 BFD 联动技术提高主备链路的切换速度，具体实现如下：

- 正常情况下，使用主 LSP 链路转发 PE 1 和 PE 2 之间的流量。
- 使用 BFD 对主链路进行监测，当主链路发生故障时，BFD 能够快速感知并通告 LDP 协议，使得 PE 1 和 PE 2 之间的流量迅速切换到备 LSP 链路进行转发。

图1 BFD 检测 LSP 配置组网图



3.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.3 配置步骤

(1) 配置各接口的 IP 地址

配置 PE 1 接口 GigabitEthernet 2/0/1 的 IP 地址。

```
<PE1> system-view
[PE1] interface gigabitethernet 2/0/1
[PE1-GigabitEthernet2/0/1] ip address 12.12.12.1 24
[PE1-GigabitEthernet2/0/1] quit
```

请参考以上方法配置图 1 中其它接口（包括 LoopBack 接口）的 IP 地址，配置步骤这里省略。

(2) 在 MPLS 骨干网内配置 OSPF，以保证各路由器之间路由可达，并使能 OSPF 快速重路由功能。

配置 PE 1。

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 14.14.14.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 192.168.10.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] fast-reroute lfa
[PE1-ospf-1] quit
```

配置 P 1。

```
[P1] ospf
[P1-ospf-1] area 0
[P1-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[P1-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0] quit
[P1-ospf-1] quit
```

配置 PE 2。

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 34.34.34..0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] fast-reroute lfa
[PE2-ospf-1] quit
```

配置 P 2。

```
[P2] ospf
[P2-ospf-1] area 0
[P2-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[P2-ospf-1-area-0.0.0.0] network 14.14.14.0 0.0.0.255
[P2-ospf-1-area-0.0.0.0] network 34.34.34.0 0.0.0.255
[P2-ospf-1-area-0.0.0.0] quit
[P2-ospf-1] quit
```

调整 P 2 上 GigabitEthernet2/0/1 和 GigabitEthernet2/0/2 的 OSPF cost 值，使备份 LSP 路径上的 OSPF 开销值大于主 LSP 路径。

```
[P2] interface gigabitethernet 2/0/1
[P2-GigabitEthernet2/0/1] ospf cost 10
[P2-GigabitEthernet2/0/1] quit
[P2] interface gigabitethernet 2/0/2
[P2-GigabitEthernet2/0/2] ospf cost 10
[P2-GigabitEthernet2/0/2] quit
```

(3) 配置 MPLS 基本能力，并使能 LDP

配置 PE 1。

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] interface gigabitethernet 2/0/1
[PE1-GigabitEthernet2/0/1] mpls enable
[PE1-GigabitEthernet2/0/1] mpls ldp enable
[PE1-GigabitEthernet2/0/1] quit
[PE1] interface gigabitethernet 2/0/2
[PE1-GigabitEthernet2/0/2] mpls enable
[PE1-GigabitEthernet2/0/2] mpls ldp enable
[PE1-GigabitEthernet2/0/2] quit
```

配置 P 1。

```
[P1] mpls lsr-id 2.2.2.2
[P1] mpls ldp
[P1-ldp] quit
[P1] interface gigabitethernet 2/0/1
[P1-GigabitEthernet2/0/1] mpls enable
[P1-GigabitEthernet2/0/1] mpls ldp enable
[P1-GigabitEthernet2/0/1] quit
[P1] interface gigabitethernet 2/0/2
[P1-GigabitEthernet2/0/2] mpls enable
[P1-GigabitEthernet2/0/2] mpls ldp enable
[P1-GigabitEthernet2/0/2] quit
```

配置 PE 2。

```
[PE2] mpls lsr-id 3.3.3.3
[PE2] mpls ldp
[PE2-ldp] quit
[PE2] interface gigabitethernet 2/1/1
[PE2-GigabitEthernet2/1/1] mpls enable
[PE2-GigabitEthernet2/1/1] mpls ldp enable
[PE2-GigabitEthernet2/1/1] quit
[PE2] interface gigabitethernet 2/1/2
[PE2-GigabitEthernet2/1/2] mpls enable
[PE2-GigabitEthernet2/1/2] mpls ldp enable
[PE2-GigabitEthernet2/1/2] quit
```

配置 P 2。

```
[P2] mpls lsr-id 4.4.4.4
[P2] mpls ldp
[P2-ldp] quit
[P2] interface gigabitethernet 2/0/1
[P2-GigabitEthernet2/0/1] mpls enable
[P2-GigabitEthernet2/0/1] mpls ldp enable
[P2-GigabitEthernet2/0/1] quit
[P2] interface gigabitethernet 2/0/2
[P2-GigabitEthernet2/0/2] mpls enable
[P2-GigabitEthernet2/0/2] mpls ldp enable
[P2-GigabitEthernet2/0/2] quit
```

完成上述配置后，在各设备上可以看到 LDP 会话的状态为 operational，会话建立成功。以 PE1 为例：

```
[PE1] display mpls ldp peer
Total number of peers: 2
Peer LDP ID             State         Role     GR   MD5  KA Sent/Rcvd
2.2.2.2:0               Operational   Passive  Off  Off  55/55
4.4.4.4:0               Operational   Passive  Off  Off  6/6
```

(4) 配置 LSP 的触发策略，为目的地址为 192.168.10.0/24、192.168.20.0/24、1.1.1.1/32 和 3.3.3.3/32 的路由表项建立 LSP

在 PE 1 上创建 IP 地址前缀列表 PE1，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[PE1] ip prefix-list PE1 index 10 permit 192.168.10.0 24
```

```
[PE1] ip prefix-list PE1 index 20 permit 192.168.20.0 24
[PE1] ip prefix-list PE1 index 30 permit 1.1.1.1 32
[PE1] ip prefix-list PE1 index 40 permit 3.3.3.3 32
[PE1] mpls ldp
[PE1-ldp] lsp-trigger prefix-list PE1
[PE1-ldp] quit
```

在 P 1 上创建 IP 地址前缀列表 P1，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[P1] ip prefix-list P1 index 10 permit 192.168.10.0 24
[P1] ip prefix-list P1 index 20 permit 192.168.20.0 24
[P1] ip prefix-list P1 index 30 permit 1.1.1.1 32
[P1] ip prefix-list P1 index 40 permit 3.3.3.3 32
[P1] mpls ldp
[P1-ldp] lsp-trigger prefix-list P1
[P1-ldp] quit
```

在 PE 2 上创建 IP 地址前缀列表 PE 2，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[PE2] ip prefix-list PE2 index 10 permit 192.168.10.0 24
[PE2] ip prefix-list PE2 index 20 permit 192.168.20.0 24
[PE2] ip prefix-list PE2 index 30 permit 1.1.1.1 32
[PE2] ip prefix-list PE2 index 40 permit 3.3.3.3 32
[PE2] mpls ldp
[PE2-ldp] lsp-trigger prefix-list PE2
[PE2-ldp] quit
```

在 P 2 上创建 IP 地址前缀列表 P2，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[P2] ip prefix-list P2 index 10 permit 192.168.10.0 24
[P2] ip prefix-list P2 index 20 permit 192.168.20.0 24
[P2] ip prefix-list P2 index 30 permit 1.1.1.1 32
[P2] ip prefix-list P2 index 40 permit 3.3.3.3 32
[P2] mpls ldp
[P2-ldp] lsp-trigger prefix-list P2
[P2-ldp] quit
```

配置完成后，在 PE 1 上执行 **display mpls ldp lsp** 命令，查看 LDP LSP 的建立情况，可以看到去往 192.168.20.0/24 网段的 LSP 建立完成。

```
[PE1] display mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup
Statistics:
  FECs: 4      Ingress LSPs: 4     Transit LSPs: 4     Egress LSPs: 2

FEC                In/Out Label        Nexthop         OutInterface
1.1.1.1/32         3/-
                   -/1151(L)
                   -/1279(L)
3.3.3.3/32         -/1150              12.12.12.2      GE2/0/1
                   1150/1150           12.12.12.2      GE2/0/1
                   -/1150(B)           12.12.12.2      GE2/0/2
```

```
                    1150/1150(B)        12.12.12.2      GE2/0/2
192.168.10.0/24     1141/-
                    -/1141(L)
                    -/1141(L)
192.168.20.0/24     -/1133              12.12.12.2      GE2/0/1
                    1133/1133           12.12.12.2      GE2/0/1
                    -/1133(B)           14.14.14.4      GE2/0/2
                    1133/1133(B)        14.14.14.4      GE2/0/2
```

(5) 使能 MPLS 与 BFD 联动功能，并配置通过 BFD 检测 LSP 的连通性

配置 PE 1。

```
[PE1] mpls bfd enable
[PE1] mpls bfd 3.3.3.3 32
```

配置 PE 2。

```
[PE2] mpls bfd enable
[PE2] mpls bfd 1.1.1.1 32
```

3.4 验证配置

(1) 配置完成后，在设备 PE 1 和 PE 2 上执行 **display mpls bfd** 命令，可以看到检测 LSP 的 BFD 会话的建立情况。以 PE 1 为例。

```
[PE1] display mpls bfd
 Total number of sessions: 2, 2 up, 0 down, 0 init

 FEC Type: LSP
 FEC Info:
   Destination: 1.1.1.1
   Mask Length: 32
 NHLFE ID: -
 Local Discr: 1026                  Remote Discr: 514
 Source IP: 1.1.1.1                 Destination IP: 3.3.3.3
 Session State: Up                  Session Role: Active
 Template Name: -

 FEC Type: LSP
 FEC Info:
   Destination: 3.3.3.3
   Mask Length: 32
 NHLFE ID: 1028
 Local Discr: 1025                  Remote Discr: -
 Source IP: 1.1.1.1                 Destination IP: 127.0.0.1
 Session State: Up                  Session Role: Passive
 Template Name: -
```

(2) 在 PE 1 上使用 **tracert mpls ipv4** 命令查看到当前所使用的路径是主 LSP。（使用 Tracert 功能需要在中间设备上开启 ICMP 超时报文发送功能，在目的端开启 ICMP 目的不可达报文发送功能）

```
<PE1> tracert mpls -a 192.168.10.1 ipv4 192.168.20.0 24
MPLS trace route FEC 192.168.20.0/24
```

```
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   12.12.12.2/[1141]
  1     12.12.12.2         2 ms    Transit   23.23.23.3/[1141]
  2     23.23.23.3         2 ms    Egress
```

(3) 在 PE 1 上持续 ping PE 2，期间将 P 1 的 GigabitEthernet2/0/1 接口 **shutdown**，查看通信是否中断。

#在 PE 1 上持续 ping PE 2，

```
<PE1> ping -c 100000 -a 192.168.10.1 192.168.20.1
Ping 192.168.20.1 (192.168.20.1) from 192.168.10.1: 56 data bytes, press CTRL_C
to break
56 bytes from 192.168.20.1: icmp_seq=0 ttl=254 time=2.576 ms
56 bytes from 192.168.20.1: icmp_seq=1 ttl=254 time=1.996 ms
...
```

关闭 P 1 的 GigabitEthernet2/0/1 接口。

```
[P1] interface gigabitethernet2/0/1
[P1-GigabitEthernet2/0/1] shut
```

#在 PE1 上查看到通讯断开后迅速恢复。

```
<PE1> ping -c 100000 -a 192.168.10.1 192.168.20.1
Ping 192.168.20.1 (192.168.20.1) from 192.168.10.1: 56 data bytes, press CTRL_C
to break
56 bytes from 192.168.20.1: icmp_seq=0 ttl=254 time=2.576 ms
56 bytes from 192.168.20.1: icmp_seq=1 ttl=254 time=1.996 ms
...
56 bytes from 192.168.20.1: icmp_seq=7 ttl=254 time=2.214 ms
Request time out
56 bytes from 192.168.20.1: icmp_seq=9 ttl=254 time=2.659 ms
56 bytes from 192.168.20.1: icmp_seq=10 ttl=254 time=5.049 ms
56 bytes from 192.168.20.1: icmp_seq=11 ttl=254 time=2.098 ms
56 bytes from 192.168.20.1: icmp_seq=12 ttl=254 time=2.225 ms
56 bytes from 192.168.20.1: icmp_seq=13 ttl=254 time=2.187 ms

--- Ping statistics for 192.168.20.1 ---
14 packets transmitted, 13 packets received, 7.1% packet loss
round-trip min/avg/max/std-dev = 1.990/2.455/5.049/0.772 ms
```

(4) 查看链路是否发生切换。

在 PE 1 上使用 **tracert mpls ipv4** 命令查看到当前路径是备份 LSP。

```
<PE1> tracert mpls -a 192.168.10.1 ipv4 192.168.20.0 24
MPLS trace route FEC 192.168.20.0/24
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   14.14.14.4/[1133]
  1     14.14.14.4         2 ms    Transit   34.34.34.3/[1141]
  2     34.34.34.3         2 ms    Egress
```

3.5 配置文件

- PE 1

```
#
ospf 1
 fast-reroute lfa
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 12.12.12.0 0.0.0.255
  network 14.14.14.0 0.0.0.255
  network 192.168.10.0 0.0.0.255
#
 mpls lsr-id 1.1.1.1
#
mpls ldp
 lsp-trigger prefix-list PE1
#
 mpls bfd enable
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 12.12.12.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 14.14.14.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
 ip prefix-list PE1 index 10 permit 192.168.10.0 24
 ip prefix-list PE1 index 20 permit 192.168.20.0 24
 ip prefix-list PE1 index 30 permit 1.1.1.1 32
 ip prefix-list PE1 index 40 permit 3.3.3.3 32
#
 mpls bfd 3.3.3.3 32
#
```

- PE 2

```
#
ospf 1
 fast-reroute lfa
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 23.23.23.0 0.0.0.255
  network 34.34.34.0 0.0.0.255
  network 192.168.20.0 0.0.0.255
#
```

```
 mpls lsr-id 3.3.3.3
#
mpls ldp
 lsp-trigger prefix-list PE2
#
 mpls bfd enable
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 34.34.34.3 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 23.23.23.3 255.255.255.0
 mpls enable
 mpls ldp enable
#
 ip prefix-list PE2 index 10 permit 192.168.10.0 24
 ip prefix-list PE2 index 20 permit 192.168.20.0 24
 ip prefix-list PE2 index 30 permit 1.1.1.1 32
 ip prefix-list PE2 index 40 permit 3.3.3.3 32
#
 mpls bfd 1.1.1.1 32
#
```

- P 1

```
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 12.12.12.0 0.0.0.255
  network 23.23.23.0 0.0.0.255
#
 mpls lsr-id 2.2.2.2
#
mpls ldp
 lsp-trigger prefix-list P1
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 12.12.12.2 255.255.255.0
```

```
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 23.23.23.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
 ip prefix-list P1 index 10 permit 192.168.10.0 24
 ip prefix-list P1 index 20 permit 192.168.20.0 24
 ip prefix-list P1 index 30 permit 1.1.1.1 32
 ip prefix-list P1 index 40 permit 3.3.3.3 32
#
```

- P 2

```
#
ospf 1
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 14.14.14.0 0.0.0.255
  network 34.34.34.0 0.0.0.255
#
 mpls lsr-id 4.4.4.4
#
mpls ldp
 lsp-trigger prefix-list P2
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 34.34.34.4 255.255.255.0
 ospf cost 10
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 14.14.14.4 255.255.255.0
 ospf cost 10
 mpls enable
 mpls ldp enable
#
 ip prefix-list P2 index 10 permit 192.168.10.0 24
 ip prefix-list P2 index 20 permit 192.168.20.0 24
 ip prefix-list P2 index 30 permit 1.1.1.1 32
 ip prefix-list P2 index 40 permit 3.3.3.3 32
```

#

4 BFD 检测 MPLS TE 典型配置举例

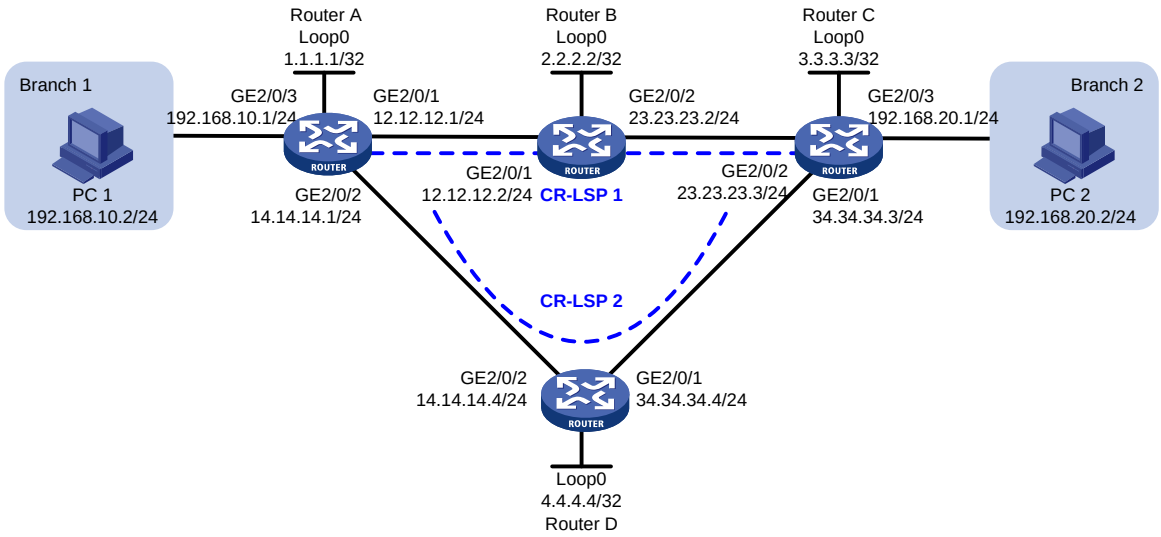
4.1 组网需求

如图 2 所示，某公司有两个位于不同的地理位置的分支机构通过 MPLS TE 隧道实现互联，两个分支机构之间需要进行实时业务的同步传输。该公司要求运营商提供高可靠性的服务，以保证实时业务的不间断性。

为满足该用户需求，可通过部署 CRLSP 备份服务来提供主备两条 CRLSP 链路，并使用 BFD 检测 MPLS TE 技术提高主备 CR-LSP 的切换速度，具体实现如下：

- 正常情况下，使用 CR-LSP 1 作为主 CR-LSP，负责转发 Router A 和 Router C 之间的流量。
- 使用 BFD 对主 CR-LSP 进行监测，当主 CR-LSP 发生故障时，BFD 能够快速感知并通告 RSVP 协议，使得 Router A 和 Router C 之间的流量迅速切换到 CR-LSP 2 进行转发。

图2 BFD 检测 MPLS TE 配置组网图



4.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.3 配置注意事项

- OSPF TE 使用 Opaque Type 10 LSA 携带链路的 TE 属性信息，因此，配置 OSPF TE 时必须先使能 OSPF 的 Opaque 能力。有关 OSPF Opaque 能力的介绍请参见“三层技术-IP 路由配置指导”中的“OSPF”。
- 由于 MPLS TE 无法在 OSPF 虚连接上预留资源和分配标签，即 MPLS TE 无法通过 OSPF 虚连接建立 CRLSP 隧道。因此，配置 OSPF TE 时，OSPF 路由域内不能存在虚连接。

4.4 配置步骤

(1) 配置各接口的 IP 地址

配置 Router A 接口 GigabitEthernet 2/0/1 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] ip address 12.12.12.1 24
[RouterA-GigabitEthernet2/0/1] quit
```

请参考以上方法配置图 2 中其它接口（包括 LoopBack 接口）的 IP 地址，配置步骤这里省略。

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

配置 Router A。

```
[RouterA] mpls lsr-id 1.1.1.1
[RouterA] mpls te
[RouterA-te] quit
[RouterA] rsvp
[RouterA-rsvp] quit
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] mpls enable
[RouterA-GigabitEthernet2/0/1] mpls te enable
[RouterA-GigabitEthernet2/0/1] rsvp enable
[RouterA-GigabitEthernet2/0/1] quit
[RouterA] interface gigabitethernet 2/0/2
[RouterA-GigabitEthernet2/0/2] mpls enable
[RouterA-GigabitEthernet2/0/2] mpls te enable
[RouterA-GigabitEthernet2/0/2] rsvp enable
[RouterA-GigabitEthernet2/0/2] quit
```

Router B、Router C 和 Router D 的配置与 Router A 相似，此处不再赘述，具体请参见配置文件。

(3) 在 MPLS 骨干网内配置 OSPF，以保证各路由器之间路由可达，并使能 OSPF 的 Opaque LSA 发布接收能力，在 OSPF 区域 0 使能 MPLS TE 能力

配置 Router A。

```
[RouterA] ospf
[RouterA-ospf-1] opaque-capability enable
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] mpls te enable
[RouterA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[RouterA-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 14.14.14.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 192.168.10.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

配置 Router B。

```
[RouterB] ospf
[RouterB-ospf-1] opaque-capability enable
```

```
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] mpls te enable
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

配置 Router C。

```
[RouterC] ospf
[RouterC-ospf-1] opaque-capability enable
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] mpls te enable
[RouterC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[RouterC-ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 34.34.34..0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

配置 Router D。

```
[RouterD] ospf
[RouterD-ospf-1] opaque-capability enable
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] mpls te enable
[RouterD-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[RouterD-ospf-1-area-0.0.0.0] network 14.14.14.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] network 34.34.34.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] quit
[RouterD-ospf-1] quit
```

(4) 配置 MPLS TE 隧道

在 Router A 上配置 MPLS TE 隧道 Tunnel3：目的地址为 Router C 的 LSR ID（3.3.3.3）；采用 RSVP-TE 信令协议建立 MPLS TE 隧道；隧道支持 CRLSP 热备份功能。

```
[RouterA] interface tunnel 3 mode mpls-te
[RouterA-Tunnel3] ip address 9.1.1.1 255.255.255.0
[RouterA-Tunnel3] destination 3.3.3.3
[RouterA-Tunnel3] mpls te signaling rsvp-te
[RouterA-Tunnel3] mpls te backup hot-standby
[RouterA-Tunnel3] quit
```

#创建隧道的显式路径，设置 CR-LSP 1 优先级为 1，作为主 CR-LSP，CR-LSP 2 优先级为 2，作为备份 CR-LSP。

```
[RouterA] explicit-path cr-lsp1
[RouterA-explicit-path-cr-lsp1] nexthop 12.12.12.2
[RouterA-explicit-path-cr-lsp1] quit
[RouterA]explicit-path cr-lsp2
[RouterA-explicit-path-cr-lsp2] nexthop 14.14.14.4
[RouterA-explicit-path-cr-lsp2]quit
[RouterA] interface tunnel 3
[RouterA-Tunnel3] mpls te path preference 1 explicit-path cr-lsp1
```

```
[RouterA-Tunnel3] mpls te path preference 2 explicit-path cr-lsp2
[RouterA-Tunnel3] quit
```

在 Router C 上配置 MPLS TE 隧道 Tunnel3：目的地址为 Router A 的 LSR ID（1.1.1.1）；采用 RSVP-TE 信令协议建立 MPLS TE 隧道；隧道支持 CRLSP 热备份功能。

```
[RouterC] interface tunnel 3 mode mpls-te
[RouterC-Tunnel3] ip address 9.3.3.3 255.255.255.0
[RouterC-Tunnel3] destination 1.1.1.1
[RouterC-Tunnel3] mpls te signaling rsvp-te
[RouterC-Tunnel3] mpls te backup hot-standby
[RouterC-Tunnel3] quit
```

#创建隧道的显式路径，设置 CR-LSP 1 优先级为 1，作为主 CR-LSP，CR-LSP 2 优先级为 2，作为备份 CR-LSP。

```
[RouterC] explicit-path cr-lsp1
[RouterC-explicit-path-cr-lsp1] nexthop 23.23.23.2
[RouterC-explicit-path-cr-lsp1] quit
[RouterC]explicit-path cr-lsp2
[RouterC-explicit-path-cr-lsp2] nexthop 34.34.34.4
[RouterC-explicit-path-cr-lsp2]quit
[RouterC] interface tunnel 3
[RouterC-Tunnel3] mpls te path preference 1 explicit-path cr-lsp1
[RouterC-Tunnel3] mpls te path preference 2 explicit-path cr-lsp2
[RouterC-Tunnel3] quit
```

(5) 配置静态路由使流量沿 MPLS TE 隧道转发

在 Router A 上配置静态路由，使得到达网络 192.168.20.0/24 的流量通过 MPLS TE 隧道接口 Tunnel3 转发。

```
[RouterA] ip route-static 192.168.20.0 24 tunnel 3 preference 1
```

在 Router C 上配置静态路由，使得到达网络 192.168.10.0/24 的流量通过 MPLS TE 隧道接口 Tunnel3 转发。

```
[RouterC] ip route-static 192.168.10.0 24 tunnel 3 preference 1
```

(6) 使能 MPLS 与 BFD 联动功能，并配置通过 BFD 检测 TE 隧道的连通性

配置 Router A。

```
[RouterA] mpls bfd enable
[RouterA] interface tunnel 3
[RouterA-Tunnel3] mpls bfd
[RouterA-Tunnel3] quit
```

配置 Router C。

```
[RouterC] mpls bfd enable
[RouterC] interface tunnel 3
[RouterC-Tunnel3] mpls bfd
[RouterC-Tunnel3] quit
```

4.5 验证配置

(1) 配置完成后，查看 MPLS TE 隧道是否成功建立。

#在 Router A 和 Router C 上执行 **display interface tunnel** 命令，可以看到 Tunnel3 的状态为 up，以 Router A 为例。

```
<RouterA> display interface tunnel
Tunnel3
Current state: UP
Line protocol state: UP
Description: Tunnel3 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1496
Internet Address is 9.1.1.1/24 Primary
Tunnel source unknown, destination 3.3.3.3
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

(2) 在 Router A 上使用 **tracert mpls te** 命令查看到当前路径是 CR-LSP1。（使用 Tracert 功能需要在中间设备上开启 ICMP 超时报文发送功能，在目的端开启 ICMP 目的不可达报文发送功能）

```
<RouterA> tracert mpls te Tunnel 3
MPLS trace route TE tunnel Tunnel3
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   12.12.12.2/[1140]
  1     12.12.12.2         30 ms   Transit   23.23.23.3/[3]
  2     23.23.23.3         2 ms    Egress
```

(3) 使用 **display mpls bfd** 查看到 2 条 MPLS TE 隧道的 BFD 检测信息，分别检测主 CR-LSP 和备份 CR-LSP 的状态，其中检测主 CR-LSP 的 BFD 状态为 UP，以 Router A 为例。

```
<RouterA> display mpls bfd te tunnel 3
 Total number of sessions: 2, 1 up, 1 down, 0 init

 FEC Type: TE Tunnel
 FEC Info:
   Send Addr: 1.1.1.1
   End  Addr: 3.3.3.3
   Tunnel ID: 3
   LSP ID   : 1150
 NHLFE ID: 1045
 Local Discr: 1026                  Remote Discr: -
 Source IP: 1.1.1.1                 Destination IP: 127.0.0.2
 Session State: Down                Session Role: Passive
 Template Name: -

 FEC Type: TE Tunnel
 FEC Info:
   Send Addr: 1.1.1.1
```

```
  End  Addr: 3.3.3.3
  Tunnel ID: 3
  LSP ID   : 1151
NHLFE ID: 1047
Local Discr: 1027                    Remote Discr: 515
Source IP: 1.1.1.1                   Destination IP: 127.0.0.1
Session State: Up                    Session Role: Passive
Template Name: -
```

(4) 在 Router A 上持续 ping Router C，期间将 Router B 的 GigabitEthernet2/0/1 接口 **shutdown**，查看通信是否中断。

#在 Router A 上持续 ping Router C，

```
<RouterA> ping -c 10000 -a 192.168.10.1 192.168.20.1
Ping 192.168.20.1 (192.168.20.1) from 192.168.10.1: 56 data bytes, press CTRL_C
to break
56 bytes from 192.168.20.1: icmp_seq=0 ttl=254 time=3.443 ms
56 bytes from 192.168.20.1: icmp_seq=1 ttl=254 time=2.835 ms
...
```

关闭 Router B 的 GigabitEthernet2/0/1 接口。

```
[RouterB] interface gigabitethernet2/0/1
[RouterB-GigabitEthernet2/0/1] shutdown
```

#在 Router A 上查看到通讯断开后迅速恢复。

```
<RouterA> ping -c 10000 -a 192.168.10.1 192.168.20.1
Ping 192.168.20.1 (192.168.20.1) from 192.168.10.1: 56 data bytes, press CTRL_C
to break
56 bytes from 192.168.20.1: icmp_seq=0 ttl=254 time=3.443 ms
56 bytes from 192.168.20.1: icmp_seq=1 ttl=254 time=2.835 ms
...
56 bytes from 192.168.20.1: icmp_seq=22 ttl=254 time=3.503 ms
Request time out
56 bytes from 192.168.20.1: icmp_seq=24 ttl=254 time=2.434 ms
56 bytes from 192.168.20.1: icmp_seq=25 ttl=254 time=3.196 ms
56 bytes from 192.168.20.1: icmp_seq=26 ttl=254 time=3.592 ms
56 bytes from 192.168.20.1: icmp_seq=27 ttl=254 time=2.305 ms
56 bytes from 192.168.20.1: icmp_seq=28 ttl=254 time=2.139 ms

--- Ping statistics for 192.168.20.1 ---
29 packets transmitted, 28 packets received, 3.4% packet loss
round-trip min/avg/max/std-dev = 2.076/2.701/3.921/0.609 ms
```

(5) 查看链路是否发生切换。

在 Router A 上使用 **tracert mpls te** 命令查看到当前路径是 CR-LSP2。

```
<RouterA> tracert mpls te Tunnel 3
MPLS trace route TE tunnel Tunnel3
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   14.14.14.4/[1142]
  1     14.14.14.4         198 ms  Transit   34.34.34.3/[3]
  2     34.34.34.3         7 ms    Egress
```

使用 **display mpls bfd** 查看到 MPLS TE 隧道 CR-LSP2 的 BFD 检测信息，以 Router A 为例。

```
<RouterA> display mpls bfd te tunnel 3
 Total number of sessions: 1, 1 up, 0 down, 0 init

 FEC Type: TE Tunnel
 FEC Info:
   Send Addr: 1.1.1.1
   End  Addr: 3.3.3.3
   Tunnel ID: 3
   LSP ID   : 1151
 NHLFE ID: 1047
 Local Discr: 1027                  Remote Discr: 515
 Source IP: 1.1.1.1                 Destination IP: 127.0.0.1
 Session State: Up                  Session Role: Passive
 Template Name: -
```

4.6 配置文件

- Router A：

```
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 12.12.12.0 0.0.0.255
  network 14.14.14.0 0.0.0.255
  network 192.168.10.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 1.1.1.1
#
mpls te
#
explicit-path cr-lsp1
 nexthop index 1 12.12.12.2 include strict
#
explicit-path cr-lsp2
 nexthop index 1 14.14.14.4 include strict
#
rsvp
#
 mpls bfd enable
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
```

```
 ip address 12.12.12.1 255.255.255.0
 mpls enable
 mpls te enable
 rsvp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 14.14.14.1 255.255.255.0
 mpls enable
 mpls te enable
 rsvp enable
#
interface GigabitEthernet2/0/3
 port link-mode route
 ip address 192.168.10.1 255.255.255.0
#
interface Tunnel3 mode mpls-te
 ip address 9.1.1.1 255.255.255.0
 mpls te path preference 1 explicit-path cr-lsp1
 mpls te path preference 2 explicit-path cr-lsp2
 mpls te backup hot-standby
 mpls bfd
 destination 3.3.3.3
#
 ip route-static 192.168.20.0 24 Tunnel3 preference 1
#
```

- Router B：

```
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 12.12.12.0 0.0.0.255
  network 23.23.23.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 2.2.2.2
#
mpls te
#
rsvp
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 12.12.12.2 255.255.255.0
 mpls enable
```

```
 mpls te enable
 rsvp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 23.23.23.2 255.255.255.0
 mpls enable
 mpls te enable
 rsvp enable
#
```

- Router C：

```
#
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 23.23.23.0 0.0.0.255
  network 34.34.34.0 0.0.0.255
  network 192.168.20.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 3.3.3.3
#
mpls te
#
explicit-path cr-lsp1
 nexthop index 1 23.23.23.2 include strict
#
explicit-path cr-lsp2
 nexthop index 1 34.34.34.4 include strict
#
rsvp
#
 mpls bfd enable
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 34.34.34.3 255.255.255.0
 mpls enable
 mpls te enable
 rsvp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 23.23.23.3 255.255.255.0
 mpls enable
```

```
 mpls te enable
 rsvp enable
#
interface GigabitEthernet2/0/3
 port link-mode route
 ip address 192.168.20.1 255.255.255.0
#
interface Tunnel3 mode mpls-te
 ip address 9.3.3.3 255.255.255.0
 mpls te path preference 1 explicit-path cr-lsp1
 mpls te path preference 2 explicit-path cr-lsp2
 mpls te backup hot-standby
 mpls bfd
 destination 1.1.1.1
#
 ip route-static 192.168.10.0 24 Tunnel3 preference 1
#
```

- Router D：

```
#
ospf 1
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 14.14.14.0 0.0.0.255
  network 34.34.34.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 4.4.4.4
#
mpls te
#
rsvp
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 34.34.34.4 255.255.255.0
 mpls enable
 mpls te enable
 rsvp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 14.14.14.4 255.255.255.0
 mpls enable
 mpls te enable
 rsvp enable
```

#

5 相关资料

- H3C SR6600 SR6600-X 路由器 MPLS 配置指导-R7607
- H3C SR6600 SR6600-X 路由器 MPLS 命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

MPLS TE 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 2
3 使用 RSVP-TE 配置 MPLS TE 隧道典型配置举例 3
3.1 组网需求 3
3.2 配置思路 3
3.3 使用版本 3
3.4 配置注意事项 4
3.5 配置步骤 4
3.6 验证配置 9
3.7 配置文件 13
4 MPLS TE FRR 典型配置举例 16
4.1 组网需求 16
4.2 配置思路 17
4.3 使用版本 17
4.4 配置注意事项 17
4.5 配置步骤 18
4.6 验证配置 26
4.7 配置文件 30
5 相关资料 34

1 简介

MPLS TE（Traffic Engineering，流量工程）结合了 MPLS 技术与流量工程，通过建立沿着指定路径的 LSP 隧道进行资源预留（这种 LSP 也称为 CRLSP，即基于约束路由的 LSP），使网络流量绕开拥塞节点，达到平衡网络流量的目的。

1. 使用 RSVP-TE 建立 CRLSP

MPLS TE 可以通过静态和动态两种方式建立 CRLSP：

- 静态方式是指：在流量经过的每一跳设备上（包括 Ingress、Transit 和 Egress）分别手工指定入标签、出标签、流量所需的带宽等信息，从而建立满足约束条件的 CRLSP。静态方式的优点是配置简单，缺点是不能根据网络的变化动态调整建立的 CRLSP；
- 动态方式是指：根据链路状态信息计算出路径后，通过标签分发协议（如 RSVP-TE）通告标签，并在经过的节点上为流量预留所需的带宽资源，从而建立满足约束条件的 CRLSP。该方式的优点是能根据网络的变化动态调整建立的 CRLSP，且支持 CRLSP 备份、快速重路由等功能，缺点是配置复杂。

本文着重介绍通过 RSVP-TE 动态建立 CRLSP，从而建立 MPLS TE 隧道的典型配置举例。

2. MPLS TE FRR

MPLS TE 中有两种网络保护技术，分别是 FRR 和 CRLSP 备份：

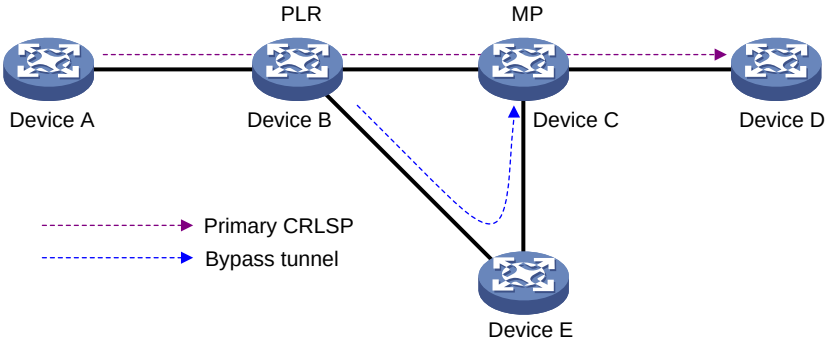
- FRR（Fast Reroute，快速重路由）是 MPLS TE 中实现网络局部保护的技术。开启隧道的 FRR 功能后，当主 CRLSP 上的某条链路或某个节点失效时，流量会被切换到 Bypass 隧道上。同时，隧道的 Ingress 节点尝试建立新的 CRLSP。新的 CRLSP 建立成功后，流量将切换到新的 CRLSP。FRR 的切换速度可以达到 50ms，能够最大程度减少网络故障时数据的丢失。
- CRLSP 备份是指通过备份 CRLSP 对主 CRLSP 进行保护。当 Ingress 节点感知到主 CRLSP 不可用时，将流量切换到备份 CRLSP 上，当主 CRLSP 路径恢复后再将流量切换回来，以实现对主 CRLSP 的备份保护。

FRR 和 CRLSP 备份的不同之处在于：CRLSP 备份是一种端到端的路径保护，对整条 CRLSP 提供保护，而 FRR 则是一种局部保护措施，只能保护 CRLSP 中的某条链路或某个节点。并且，FRR 是一种快速响应的临时性保护措施，对于切换时间有严格要求，CRLSP 备份则没有时间要求。在实际应用中是配置 FRR 还是 CRLSP 备份，可以根据上述两种技术的特点来进行选择。本文将介绍 FRR 的典型应用。

根据保护的对象不同，FRR 分为两类：

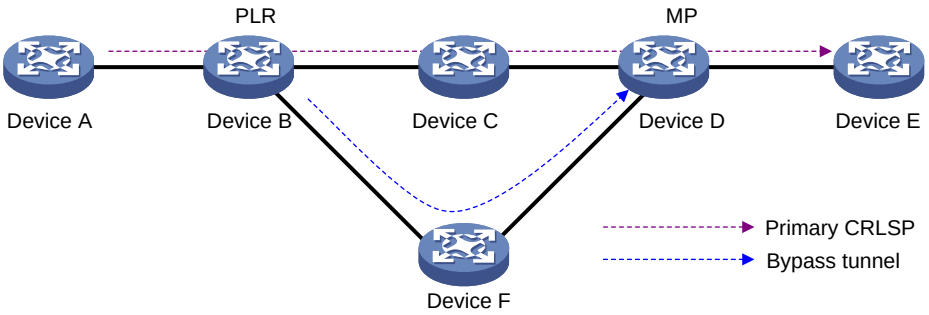
- 链路保护：又称为 Next-hop（NHOP）保护。PLR（Point of Local Repair，本地修复节点）和 MP（Merge Point，汇聚点）之间有直接链路连接，主 CRLSP 经过这条链路。当这条链路失效时，流量可以切换到 Bypass 隧道上。如图 1 所示，主 CRLSP 是 Device A→Device B→Device C→Device D，Bypass 隧道是 Device B→Device E→Device C。

图1 FRR 链路保护示意图



- 节点保护：又称为 Next-next-hop（NNHOP）保护。PLR 和 MP 之间通过一台设备连接，主 CRLSP 经过这台设备。当这台设备失效时，流量可以切换到 Bypass 隧道上。如图 2 所示，主 CRLSP 是 Device A→Device B→Device C→Device D→Device E，Bypass 隧道是 Device B→Device F→Device D，Device C 是被保护的设备。

图2 FRR 节点保护技术示意图



本文着重介绍链路保护的 MPLS TE FRR 典型配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 MPLS TE 特性。

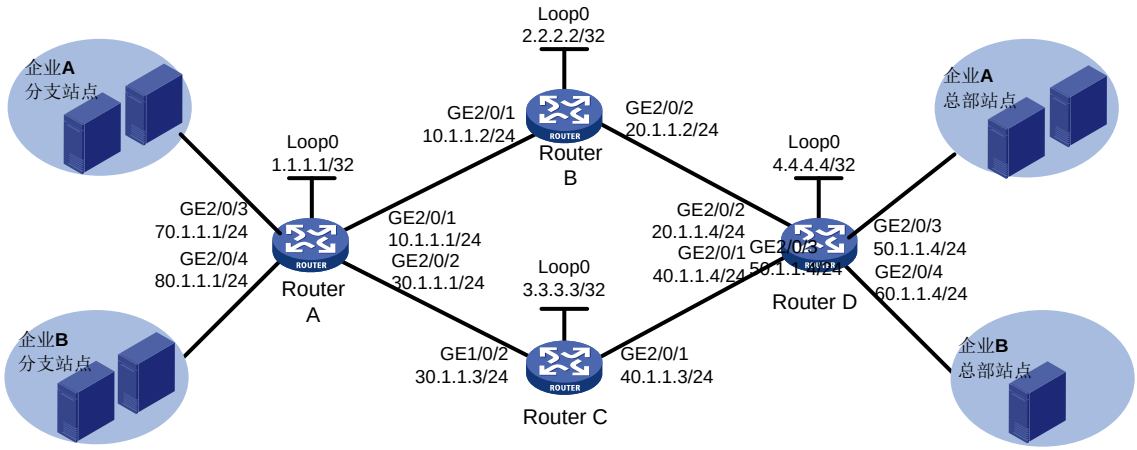
3 使用 RSVP-TE 配置 MPLS TE 隧道典型配置举例

3.1 组网需求

企业 A 和企业 B 分别有总部和分支机构两个站点，均通过运营商的 MPLS 网络进行互联。两企业的分支机构均有重要数据，需要穿越 MPLS 网络备份到总部服务器上。企业 A 的数据流量的最大带宽为 20000kbps，企业 B 的数据流量的最大带宽为 30000kbps。

在如图 3 所示的网络环境中，每条链路的最大带宽为 50000kbps，最大可预留带宽为 40000kbps，可通过部署 RSVP-TE 服务，自动为两个用户分别建立满足其带宽需求的 MPLS TE 隧道。

图3 使用 RSVP-TE 配置 MPLS TE 隧道典型配置举例组网图



3.2 配置思路

- 为了使用 RSVP-TE 配置 MPLS TE 隧道，需要在骨干网的设备上配置 MPLS、MPLS TE 和 RSVP-TE 功能。
- 为了满足两个企业用户同时在运营商 MPLS 网络中传输数据，并且拥有足够的隧道带宽，需要在 MPLS TE 隧道的 Ingress 节点上为两个用户分别创建 Tunnel 接口，并指定隧道带宽。
- 为了保证每条链路具有足够的带宽和最大可预留带宽，需要在 MPLS TE 隧道经过的各个接口上配置链路的 MPLS TE 属性，指定链路最大带宽和最大可预留带宽。
- 为了在各个节点上生成 TEDB，从而计算出到达某个节点的符合约束条件的最短路径，需要在骨干网中配置 OSPF 支持 MPLS TE，以便各个节点通过 OSPF 路由协议发布链路的 MPLS TE 相关属性。
- 为了实现使用 RSVP-TE 分发 MPLS TE 标签并建立 CRLSP，需要在 MPLS TE 隧道的 Ingress 节点上配置通过 RSVP-TE 自动建立 CRLSP。
- 为了使流量沿着 MPLS TE 隧道转发，需要在 MPLS TE 隧道的 Ingress 节点上配置静态路由，将流量引入 MPLS TE 隧道。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置注意事项

在采用 RSVP-TE 动态建立 CRLSP 时，必须配置 IGP 的 TE 扩展（目前支持 OSPF TE 和 ISIS TE），否则，不能形成 TEDB（TE DataBase，流量工程数据库）。在不配置 IGP 的 TE 扩展时计算出的路径是由 IGP 路由得到的，而不是 CSPF（Constraint-based Shortest Path First，基于约束的最短路径优先）计算出来的。

3.5 配置步骤

(1) 配置各接口的 IP 地址

按照图 3 配置各接口的 IP 地址和掩码，包括 LoopBack 接口，具体配置过程略。

(2) 配置 OSPF 协议，以保证各路由器之间路由可达

配置 Router A。

```
<RouterA> system-view
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[RouterA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

配置 Router B。

```
<RouterB> system-view
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

配置 Router C。

```
<RouterC> system-view
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[RouterC-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

配置 Router D。

```
<RouterD> system-view
[RouterD] ospf
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[RouterD-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
```

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

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

```
[RouterA] display ip routing-table

Destinations : 21        Routes : 21

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
1.1.1.1/32         Direct  0   0           127.0.0.1       InLoop0
2.2.2.2/32         O_INTRA 10  1           10.1.1.2        GE2/0/1
3.3.3.3/32         O_INTRA 10  1           30.1.1.3        GE2/0/2
4.4.4.4/32         O_INTRA 10  2           10.1.1.2        GE2/0/1
10.1.1.0/24        Direct  0   0           10.1.1.1        GE2/0/1
10.1.1.0/32        Direct  0   0           10.1.1.1        GE2/0/1
10.1.1.1/32        Direct  0   0           127.0.0.1       InLoop0
10.1.1.255/32      Direct  0   0           10.1.1.1        GE2/0/1
20.1.1.0/24        O_INTRA 10  2           10.1.1.2        GE2/0/1
30.1.1.0/24        Direct  0   0           30.1.1.1        GE2/0/2
30.1.1.0/32        Direct  0   0           30.1.1.1        GE2/0/2
30.1.1.1/32        Direct  0   0           127.0.0.1       InLoop0
30.1.1.255/32      Direct  0   0           30.1.1.1        GE2/0/2
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

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

配置 Router A。

```
[RouterA] mpls lsr-id 1.1.1.1
[RouterA] mpls te
[RouterA-te] quit
[RouterA] rsvp
[RouterA-rsvp] quit
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] mpls enable
[RouterA-GigabitEthernet2/0/1] mpls te enable
[RouterA-GigabitEthernet2/0/1] rsvp enable
[RouterA-GigabitEthernet2/0/1] quit
[RouterA] interface gigabitethernet 2/0/2
[RouterA-GigabitEthernet2/0/2] mpls enable
[RouterA-GigabitEthernet2/0/2] mpls te enable
[RouterA-GigabitEthernet2/0/2] rsvp enable
[RouterA-GigabitEthernet2/0/2] quit
```

配置 Router B。

```
[RouterB] mpls lsr-id 2.2.2.2
[RouterB] mpls te
[RouterB-te] quit
[RouterB] rsvp
[RouterB-rsvp] quit
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] mpls enable
[RouterB-GigabitEthernet2/0/1] mpls te enable
[RouterB-GigabitEthernet2/0/1] rsvp enable
[RouterB-GigabitEthernet2/0/1] quit
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] mpls enable
[RouterB-GigabitEthernet2/0/2] mpls te enable
[RouterB-GigabitEthernet2/0/2] rsvp enable
[RouterB-GigabitEthernet2/0/2] quit
```

配置 Router C。

```
[RouterC] mpls lsr-id 3.3.3.3
[RouterC] mpls te
[RouterC-te] quit
[RouterC] rsvp
[RouterC-rsvp] quit
[RouterC] interface gigabitethernet 2/0/1
[RouterC-GigabitEthernet2/0/1] mpls enable
[RouterC-GigabitEthernet2/0/1] mpls te enable
[RouterC-GigabitEthernet2/0/1] rsvp enable
[RouterC-GigabitEthernet2/0/1] quit
[RouterC] interface gigabitethernet 2/0/2
[RouterC-GigabitEthernet2/0/2] mpls enable
[RouterC-GigabitEthernet2/0/2] mpls te enable
[RouterC-GigabitEthernet2/0/2] rsvp enable
[RouterC-GigabitEthernet2/0/2] quit
```

配置 Router D。

```
[RouterD] mpls lsr-id 4.4.4.4
[RouterD] mpls te
[RouterD-te] quit
[RouterD] rsvp
[RouterD-rsvp] quit
[RouterD] interface gigabitethernet 2/0/1
[RouterD-GigabitEthernet2/0/1] mpls enable
[RouterD-GigabitEthernet2/0/1] mpls te enable
[RouterD-GigabitEthernet2/0/1] rsvp enable
[RouterD-GigabitEthernet2/0/1] quit
[RouterD] interface gigabitethernet 2/0/2
[RouterD-GigabitEthernet2/0/2] mpls enable
[RouterD-GigabitEthernet2/0/2] mpls te enable
[RouterD-GigabitEthernet2/0/2] rsvp enable
[RouterD-GigabitEthernet2/0/2] quit
```

(4) 配置链路的 MPLS TE 属性

在 Router A 上配置链路的最大带宽和最大可预留带宽。

```
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] mpls te max-link-bandwidth 50000
[RouterA-GigabitEthernet2/0/1] mpls te max-reservable-bandwidth 40000
[RouterA-GigabitEthernet2/0/1] quit
[RouterA] interface gigabitethernet 2/0/2
[RouterA-GigabitEthernet2/0/2] mpls te max-link-bandwidth 50000
[RouterA-GigabitEthernet2/0/2] mpls te max-reservable-bandwidth 40000
[RouterA-GigabitEthernet2/0/2] quit
```

在 Router B 上配置链路的最大带宽和最大可预留带宽。

```
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] mpls te max-link-bandwidth 50000
[RouterB-GigabitEthernet2/0/1] mpls te max-reservable-bandwidth 40000
[RouterB-GigabitEthernet2/0/1] quit
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] mpls te max-link-bandwidth 50000
[RouterB-GigabitEthernet2/0/2] mpls te max-reservable-bandwidth 40000
[RouterB-GigabitEthernet2/0/2] quit
```

在 Router C 上配置链路的最大带宽和最大可预留带宽。

```
[RouterC] interface gigabitethernet 2/0/1
[RouterC-GigabitEthernet2/0/1] mpls te max-link-bandwidth 50000
[RouterC-GigabitEthernet2/0/1] mpls te max-reservable-bandwidth 40000
[RouterC-GigabitEthernet2/0/1] quit
[RouterC] interface gigabitethernet 2/0/2
[RouterC-GigabitEthernet2/0/2] mpls te max-link-bandwidth 50000
[RouterC-GigabitEthernet2/0/2] mpls te max-reservable-bandwidth 40000
[RouterC-GigabitEthernet2/0/2] quit
```

在 Router D 上配置链路的最大带宽和最大可预留带宽。

```
[RouterD] interface gigabitethernet 2/0/1
[RouterD-GigabitEthernet2/0/1] mpls te max-link-bandwidth 50000
[RouterD-GigabitEthernet2/0/1] mpls te max-reservable-bandwidth 40000
[RouterD-GigabitEthernet2/0/1] quit
[RouterD] interface gigabitethernet 2/0/2
[RouterD-GigabitEthernet2/0/2] mpls te max-link-bandwidth 50000
[RouterD-GigabitEthernet2/0/2] mpls te max-reservable-bandwidth 40000
[RouterD-GigabitEthernet2/0/2] quit
```

(5) 配置 OSPF TE，发布链路的 MPLS TE 属性

在 Router A 上使能 OSPF 的 Opaque LSA 发布接收能力（缺省情况下处于开启状态），并在 OSPF 区域 0 内使能 MPLS TE 能力。

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

在 Router B 上使能 OSPF 的 Opaque LSA 发布接收能力（缺省情况下处于开启状态），并在 OSPF 区域 0 内使能 MPLS TE 能力。

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

在 Router C 上使能 OSPF 的 Opaque LSA 发布接收能力（缺省情况下处于开启状态），并在 OSPF 区域 0 内使能 MPLS TE 能力。

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

在 Router D 上使能 OSPF 的 Opaque LSA 发布接收能力（缺省情况下处于开启状态），并在 OSPF 区域 0 内使能 MPLS TE 能力。

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

(6) 配置 MPLS TE 隧道

在 Router A 上配置 MPLS TE 隧道 Tunnel1，用于传输企业 A 的数据：目的地址为 Router D 的 LSR ID（4.4.4.4）；采用 RSVP-TE 信令协议建立 MPLS TE 隧道；隧道所需的带宽为 20000kbps；开启路由记录功能。

```
[RouterA] interface tunnel 1 mode mpls-te
[RouterA-Tunnel1] ip address 7.1.1.1 255.255.255.0
[RouterA-Tunnel1] destination 4.4.4.4
[RouterA-Tunnel1] mpls te signaling rsvp-te
[RouterA-Tunnel1] mpls te bandwidth 20000
[RouterA-Tunnel1] mpls te record-route
[RouterA-Tunnel1] quit
```

在 Router A 上配置 MPLS TE 隧道 Tunnel2，用于传输企业 B 的数据：目的地址为 Router D 的 LSR ID（4.4.4.4）；采用 RSVP-TE 信令协议建立 MPLS TE 隧道；隧道所需的带宽为 30000kbps；开启路由记录功能。

```
[RouterA] interface tunnel 2 mode mpls-te
[RouterA-Tunnel2] ip address 8.1.1.1 255.255.255.0
[RouterA-Tunnel2] destination 4.4.4.4
[RouterA-Tunnel2] mpls te signaling rsvp-te
[RouterA-Tunnel2] mpls te bandwidth 30000
[RouterA-Tunnel2] mpls te record-route
[RouterA-Tunnel2] quit
```

(7) 配置静态路由使流量沿 MPLS TE 隧道转发

在 Router A 上配置静态路由，使得到达网络 50.1.1.0/24 的流量通过 MPLS TE 隧道接口 Tunnel1 转发。

```
[RouterA] ip route-static 50.1.1.0 24 tunnel 1 preference 1
```

在 Router A 上配置静态路由，使得到达网络 60.1.1.0/24 的流量通过 MPLS TE 隧道接口 Tunnel2 转发。

```
[RouterA] ip route-static 60.1.1.0 24 tunnel 2 preference 1
```

3.6 验证配置

配置完成后，在 Router A 上执行 **display interface tunnel** 命令可以看到 2 个隧道接口的状态为 UP。

```
[RouterA] display interface tunnel
Tunnel1
Current state: UP
Line protocol state: UP
Description: Tunnel1 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 64000
Internet Address is 7.1.1.1/24 Primary
Tunnel source unknown, destination 4.4.4.4
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops

Tunnel2
Current state: UP
Line protocol state: UP
Description: Tunnel2 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 64000
Internet Address is 8.1.1.1/24 Primary
Tunnel source unknown, destination 4.4.4.4
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
```

```
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

在 Router A 上执行 **display mpls te tunnel-interface** 命令可以看到 2 条隧道的详细信息。

```
[RouterA] display mpls te tunnel-interface
Tunnel Name            : Tunnel 1
Tunnel State           : Up (Main CRLSP up, Shared-resource CRLSP down)
Tunnel Attributes      :
  LSP ID               : 46362           Tunnel ID            : 1
  Admin State          : Normal
  Ingress LSR ID       : 1.1.1.1         Egress LSR ID        : 4.4.4.4
  Signaling            : RSVP-TE         Static CRLSP Name    : -
  Resv Style           : SE
  Tunnel mode          : -
  Reverse-LSP name     : -
  Reverse-LSP LSR ID   : -               Reverse-LSP Tunnel ID: -
  Class Type           : CT0             Tunnel Bandwidth     : 20000 kbps
  Reserved Bandwidth   : 20000 kbps
  Setup Priority       : 7               Holding Priority     : 7
  Affinity Attr/Mask   : 0/0
  Explicit Path        : -
  Backup Explicit Path : -
  Metric Type          : TE
  Record Route         : Enabled         Record Label         : Disabled
  FRR Flag             : Disabled        Bandwidth Protection : Disabled
  Backup Bandwidth Flag: Disabled        Backup Bandwidth Type: -
  Backup Bandwidth     : -
  Bypass Tunnel        : No              Auto Created         : No
  Route Pinning        : Disabled
  Retry Limit          : 3               Retry Interval       : 2 sec
  Reoptimization       : Disabled        Reoptimization Freq  : -
  Backup Type          : None            Backup LSP ID        : -
  Auto Bandwidth       : Disabled        Auto Bandwidth Freq  : -
  Min Bandwidth        : -               Max Bandwidth        : -
  Collected Bandwidth  : -

Tunnel Name            : Tunnel 2
Tunnel State           : Up (Main CRLSP up, Shared-resource CRLSP down)
Tunnel Attributes      :
  LSP ID               : 46362           Tunnel ID            : 2
  Admin State          : Normal
  Ingress LSR ID       : 1.1.1.1         Egress LSR ID        : 4.4.4.4
  Signaling            : RSVP-TE         Static CRLSP Name    : -
  Resv Style           : SE
  Tunnel mode          : -
  Reverse-LSP name     : -
  Reverse-LSP LSR ID   : -               Reverse-LSP Tunnel ID: -
  Class Type           : CT0             Tunnel Bandwidth     : 30000 kbps
```

```
  Reserved Bandwidth   : 30000 kbps
  Setup Priority       : 7              Holding Priority     : 7
  Affinity Attr/Mask   : 0/0
  Explicit Path        : -
  Backup Explicit Path : -
  Metric Type          : TE
  Record Route         : Enabled        Record Label         : Disabled
  FRR Flag             : Disabled       Bandwidth Protection : Disabled
  Backup Bandwidth Flag: Disabled       Backup Bandwidth Type: -
  Backup Bandwidth     : -
  Bypass Tunnel        : No             Auto Created         : No
  Route Pinning        : Disabled
  Retry Limit          : 3              Retry Interval       : 2 sec
  Reoptimization       : Disabled       Reoptimization Freq  : -
  Backup Type          : None           Backup LSP ID        : -
  Auto Bandwidth       : Disabled       Auto Bandwidth Freq  : -
  Min Bandwidth        : -              Max Bandwidth        : -
  Collected Bandwidth  : -
```

在 Router A 上执行 **display ip routing-table** 命令，可以看到路由表中有以 Tunnel1 和 Tunnel2 为出接口的静态路由信息。

```
[RouterA] display ip routing-table

Destinations : 30        Routes : 30

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
1.1.1.1/32         Direct  0   0           127.0.0.1       InLoop0
2.2.2.2/32         O_INTRA 10  1           10.1.1.2        GE2/0/1
3.3.3.3/32         O_INTRA 10  1           30.1.1.3        GE2/0/2
4.4.4.4/32         O_INTRA 10  2           10.1.1.2        GE2/0/1
7.1.1.0/24         Direct  0   0           7.1.1.1         Tun1
7.1.1.0/32         Direct  0   0           7.1.1.1         Tun1
7.1.1.1/32         Direct  0   0           127.0.0.1       InLoop0
7.1.1.255/32       Direct  0   0           7.1.1.1         Tun1
8.1.1.0/24         Direct  0   0           8.1.1.1         Tun2
8.1.1.0/32         Direct  0   0           8.1.1.1         Tun2
8.1.1.1/32         Direct  0   0           127.0.0.1       InLoop0
8.1.1.255/32       Direct  0   0           8.1.1.1         Tun2
10.1.1.0/24        Direct  0   0           10.1.1.1        GE2/0/1
10.1.1.0/32        Direct  0   0           10.1.1.1        GE2/0/1
10.1.1.1/32        Direct  0   0           127.0.0.1       InLoop0
10.1.1.255/32      Direct  0   0           10.1.1.1        GE2/0/1
50.1.1.0/24        Static  1   0           0.0.0.0         Tun1
30.1.1.0/24        Direct  0   0           30.1.1.1        GE2/0/2
30.1.1.0/32        Direct  0   0           30.1.1.1        GE2/0/2
30.1.1.1/32        Direct  0   0           127.0.0.1       InLoop0
30.1.1.255/32      Direct  0   0           30.1.1.1        GE2/0/2
60.1.1.0/24        Static  1   0           0.0.0.0         Tun2
```

```
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

在 Router A 上执行 **display rsvp lsp verbose** 命令，可以看到 Tunnel 1 的 CRLSP 使用了 Router A—Router B—Router D 的路径；Tunnel 2 的 CRLSP 使用了 Router A—Router C—Router D 的路径。

```
[RouterA] display rsvp lsp verbose
Tunnel name: RouterA_t1
Destination: 4.4.4.4                    Source: 1.1.1.1
Tunnel ID: 1                            LSP ID: 46362
LSR type: Ingress                       Direction: Unidirectional
Setup priority: 7                       Holding priority: 7
In-Label: -                             Out-Label: 1150
In-Interface: -                         Out-Interface: GE2/0/1
Nexthop: 10.1.1.2                       Exclude-any: 0
Include-Any: 0                          Include-all: 0
Mean rate (CIR): 20000 kbps             Mean burst size (CBS): 1000.00 bytes
Path MTU: 1500                          Class type: CT0
RRO number: 6
  10.1.1.1/32        Flag: 0x00 (No FRR)
  10.1.1.2/32        Flag: 0x40 (No FRR/In-Int)
  2.2.2.2/32         Flag: 0x20 (No FRR/Node-ID)
  20.1.1.2/32        Flag: 0x00 (No FRR)
  20.1.1.4/32        Flag: 0x40 (No FRR/In-Int)
  4.4.4.4/32         Flag: 0x20 (No FRR/Node-ID)
Fast Reroute protection: None

Tunnel name: RouterA_t2
Destination: 4.4.4.4                    Source: 1.1.1.1
Tunnel ID: 2                            LSP ID: 46362
LSR type: Ingress                       Direction: Unidirectional
Setup priority: 7                       Holding priority: 7
In-Label: -                             Out-Label: 1150
In-Interface: -                         Out-Interface: GE2/0/2
Nexthop: 30.1.1.3                       Exclude-any: 0
Include-Any: 0                          Include-all: 0
Mean rate (CIR): 30000 kbps             Mean burst size (CBS): 1000.00 bytes
Path MTU: 1500                          Class type: CT0
RRO number: 6
  30.1.1.1/32        Flag: 0x00 (No FRR)
  30.1.1.3/32        Flag: 0x40 (No FRR/In-Int)
  3.3.3.3/32         Flag: 0x20 (No FRR/Node-ID)
  40.1.1.3/32        Flag: 0x00 (No FRR)
  40.1.1.4/32        Flag: 0x40 (No FRR/In-Int)
```

```
  4.4.4.4/32          Flag: 0x20 (No FRR/Node-ID)
Fast Reroute protection: None
```

经过验证，可以看到通过部署 RSVP-TE 服务，自动为两个用户分别建立了两条 CRLSP：经过 Router A—Router B—Router D 的带宽为 20000kbps 的 CRLSP 和经过 Router A—Router C—Router D 的带宽为 30000kbps 的 CRLSP。

3.7 配置文件

- Router A

```
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 30.1.1.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 1.1.1.1
#
mpls te
#
rsvp
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 30.1.1.1 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface Tunnel1 mode mpls-te
 ip address 7.1.1.1 255.255.255.0
 mpls te bandwidth ct0 20000
 mpls te record-route
```

```
 destination 4.4.4.4
#
interface Tunnel2 mode mpls-te
 ip address 8.1.1.1 255.255.255.0
 mpls te bandwidth ct0 30000
 mpls te record-route
 destination 4.4.4.4
#
 ip route-static 50.1.1.0 24 Tunnel1 preference 1
 ip route-static 60.1.1.0 24 Tunnel2 preference 1
#
```

- Router B

```
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 2.2.2.2
#
mpls te
#
rsvp
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.1.1.2 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 20.1.1.2 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
```

- Router C

```
#
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 30.1.1.0 0.0.0.255
  network 40.1.1.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 3.3.3.3
#
mpls te
#
rsvp
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.0
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 40.1.1.3 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 30.1.1.3 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
```

- Router D

```
#
ospf 1
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 40.1.1.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 4.4.4.4
#
mpls te
#
```

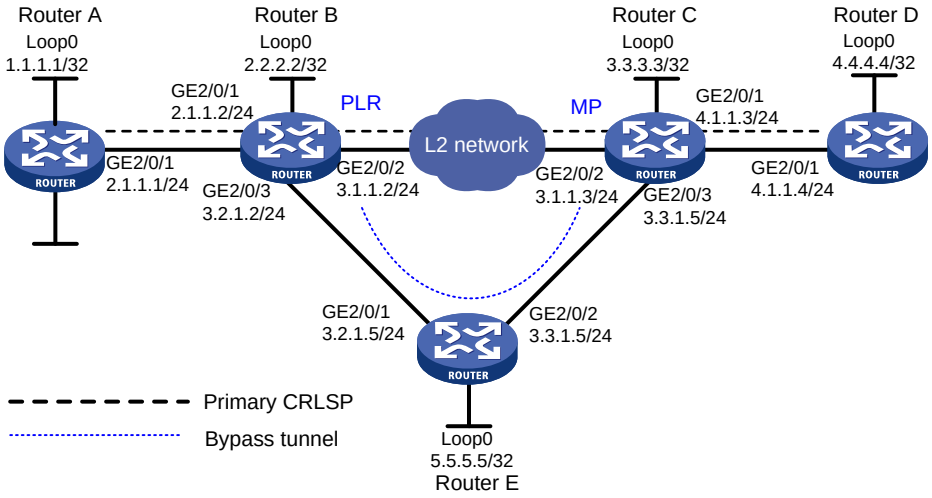
```
rsvp
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 40.1.1.4 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 20.1.1.4 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
```

4 MPLS TE FRR 典型配置举例

4.1 组网需求

如图 4 所示，Router A->Router B->Router C->Router D 之间建立了一条 CRLSP，承载着某公司的语音业务。由于 Router B 和 Router C 两台路由器相隔较远，中间连有多台二层交换机，链路不太稳定，可能会发生故障，现要求使用 MPLS TE FRR 功能对 Router B->Router C 这段链路进行保护，当链路出现故障时，能快速切换到 Bypass CRLSP（Router A->Router B->Router E->Router C->Router D）。(假设 Primary 隧道和 Bypass 隧道的所需带宽均为 30000kbps；每条链路的最大带宽为 50000kbps，最大可预留带宽为 40000kbps)

图4 MPLS TE FRR 典型配置举例组网图



4.2 配置思路

- 为建立主备 CRLSP，需要在各 Router 上使能 MPLS、MPLS TE 和 RSVP-TE 基本能力。
- 由于组网需求中已经明确主 CRLSP 的路径和 Bypass CRLSP 的路径，需要通过显式路径的方式指定 MPLS TE 的主 CRLSP 和 Bypass CRLSP。
- 为实现被保护的主 CRLSP 链路发生故障后，PLR 能快速感知到，需要在主 CRLSP 保护链路两端的节点上（Router B 和 Router C）配置 BFD 联动 RSVP-TE，使 BFD 能够快速检测并通告 RSVP-TE 协议，以便将流量快速切换到 Bypass 隧道。
- 为实现当 BFD 检测到被保护链路故障后，主 CRLSP 上的流量能快速切换到 Bypass CRLSP，需在主 CRLSP 的 Ingress 节点上使能 MPLS TE FRR 功能。
- 为了保证主 CRLSP 链路故障时，MPLS TE 能在多条 Bypass 隧道可能同时并存的情况下，选择出最优的 Bypass 隧道，需要在 PLR 节点上配置 FRR 的 Bypass 隧道的优选时间间隔为 5 秒（缺省为 300 秒）。

4.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.4 配置注意事项

- 只有使用 RSVP-TE 信令协议建立的 MPLS TE 隧道支持 FRR 功能。
- 不要在同一个接口同时配置快速重路由功能和 RSVP 认证功能。
- 由于 FRR 使用的 Bypass 隧道需要预先建立，占用额外的带宽，因此，在网络带宽余量不多的情况下，应该只对关键的接口或链路进行快速重路由保护。
- 用户在配置时应保证 Bypass 隧道的带宽不小于被保护的所有主 CRLSP 所需带宽之和，否则可能导致部分主 CRLSP 不能被 Bypass 隧道保护。

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

4.5 配置步骤

(1) 配置各接口的 IP 地址

按照图 4 配置各接口的 IP 地址和掩码，包括 LoopBack 接口，具体配置过程略。

(2) 配置 OSPF 协议，以保证各路由器之间路由可达

配置 Router A。

```
<RouterA> system-view
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[RouterA-ospf-1-area-0.0.0.0] network 2.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

配置 Router B。

```
<RouterB> system-view
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 2.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 3.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 3.2.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

配置 Router C。

```
<RouterC> system-view
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[RouterC-ospf-1-area-0.0.0.0] network 3.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 3.3.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 4.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

配置 Router D。

```
<RouterD> system-view
[RouterD] ospf
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[RouterD-ospf-1-area-0.0.0.0] network 4.1.1.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] quit
[RouterD-ospf-1] quit
```

配置 Router E。

```
<RouterE> system-view
[RouterE] ospf
[RouterE-ospf-1] area 0
[RouterE-ospf-1-area-0.0.0.0] network 5.5.5.5 0.0.0.0
[RouterE-ospf-1-area-0.0.0.0] network 3.2.1.0 0.0.0.255
[RouterE-ospf-1-area-0.0.0.0] network 3.3.1.0 0.0.0.255
[RouterE-ospf-1-area-0.0.0.0] quit
[RouterE-ospf-1] quit
```

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

```
[RouterA] display ip routing-table

Destinations : 19        Routes : 19

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
1.1.1.1/32         Direct  0   0           127.0.0.1       InLoop0
2.1.1.0/24         Direct  0   0           2.1.1.1         GE2/0/1
2.1.1.0/32         Direct  0   0           2.1.1.1         GE2/0/1
2.1.1.1/32         Direct  0   0           127.0.0.1       InLoop0
2.1.1.255/32       Direct  0   0           2.1.1.1         GE2/0/1
2.2.2.2/32         O_INTRA 10  1           2.1.1.2         GE2/0/1
3.1.1.0/24         O_INTRA 10  2           2.1.1.2         GE2/0/1
3.2.1.0/24         O_INTRA 10  2           2.1.1.2         GE2/0/1
3.3.1.0/24         O_INTRA 10  3           2.1.1.2         GE2/0/1
3.3.3.3/32         O_INTRA 10  2           2.1.1.2         GE2/0/1
5.5.5.5/32         O_INTRA 10  2           2.1.1.2         GE2/0/1
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

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

配置 Router A。

```
[RouterA] mpls lsr-id 1.1.1.1
```

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

配置 Router B。

```
[RouterB] mpls lsr-id 2.2.2.2
[RouterB] mpls te
[RouterB-te] quit
[RouterB] rsvp
[RouterB-rsvp] quit
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] mpls enable
[RouterB-GigabitEthernet2/0/1] mpls te enable
[RouterB-GigabitEthernet2/0/1] rsvp enable
[RouterB-GigabitEthernet2/0/1] quit
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] mpls enable
[RouterB-GigabitEthernet2/0/2] mpls te enable
[RouterB-GigabitEthernet2/0/2] rsvp enable
[RouterB-GigabitEthernet2/0/2] rsvp bfd enable
[RouterB-GigabitEthernet2/0/2] quit
[RouterB] interface gigabitethernet 2/0/3
[RouterB-GigabitEthernet2/0/3] mpls enable
[RouterB-GigabitEthernet2/0/3] mpls te enable
[RouterB-GigabitEthernet2/0/3] rsvp enable
[RouterB-GigabitEthernet2/0/3] quit
```

配置 Router C。

```
[RouterC] mpls lsr-id 3.3.3.3
[RouterC] mpls te
[RouterC-te] quit
[RouterC] rsvp
[RouterC-rsvp] quit
[RouterC] interface gigabitethernet 2/0/1
[RouterC-GigabitEthernet2/0/1] mpls enable
[RouterC-GigabitEthernet2/0/1] mpls te enable
[RouterC-GigabitEthernet2/0/1] rsvp enable
[RouterC-GigabitEthernet2/0/1] quit
[RouterC] interface gigabitethernet 2/0/2
[RouterC-GigabitEthernet2/0/2] mpls enable
[RouterC-GigabitEthernet2/0/2] mpls te enable
[RouterC-GigabitEthernet2/0/2] rsvp enable
[RouterC-GigabitEthernet2/0/2] rsvp bfd enable
[RouterC-GigabitEthernet2/0/2] quit
```

```
[RouterC] interface gigabitethernet 2/0/3
[RouterC-GigabitEthernet2/0/3] mpls enable
[RouterC-GigabitEthernet2/0/3] mpls te enable
[RouterC-GigabitEthernet2/0/3] rsvp enable
[RouterC-GigabitEthernet2/0/3] quit
```

配置 Router D。

```
[RouterD] mpls lsr-id 4.4.4.4
[RouterD] mpls te
[RouterD-te] quit
[RouterD] rsvp
[RouterD-rsvp] quit
[RouterD] interface gigabitethernet 2/0/1
[RouterD-GigabitEthernet2/0/1] mpls enable
[RouterD-GigabitEthernet2/0/1] mpls te enable
[RouterD-GigabitEthernet2/0/1] rsvp enable
[RouterD-GigabitEthernet2/0/1] quit
```

配置 Router E。

```
[RouterE] mpls lsr-id 5.5.5.5
[RouterE] mpls te
[RouterE-te] quit
[RouterE] rsvp
[RouterE-rsvp] quit
[RouterE] interface gigabitethernet 2/0/1
[RouterE-GigabitEthernet2/0/1] mpls enable
[RouterE-GigabitEthernet2/0/1] mpls te enable
[RouterE-GigabitEthernet2/0/1] rsvp enable
[RouterE-GigabitEthernet2/0/1] quit
[RouterE] interface gigabitethernet 2/0/2
[RouterE-GigabitEthernet2/0/2] mpls enable
[RouterE-GigabitEthernet2/0/2] mpls te enable
[RouterE-GigabitEthernet2/0/2] rsvp enable
[RouterE-GigabitEthernet2/0/2] quit
```

(4) 配置链路的 MPLS TE 属性

在 Router A 上配置链路的最大带宽和最大可预留带宽。

```
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] mpls te max-link-bandwidth 50000
[RouterA-GigabitEthernet2/0/1] mpls te max-reservable-bandwidth 40000
[RouterA-GigabitEthernet2/0/1] quit
```

在 Router B 上配置链路的最大带宽和最大可预留带宽。

```
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] mpls te max-link-bandwidth 50000
[RouterB-GigabitEthernet2/0/1] mpls te max-reservable-bandwidth 40000
[RouterB-GigabitEthernet2/0/1] quit
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] mpls te max-link-bandwidth 50000
[RouterB-GigabitEthernet2/0/2] mpls te max-reservable-bandwidth 40000
[RouterB-GigabitEthernet2/0/2] quit
```

```
[RouterB] interface gigabitethernet 2/0/3
[RouterB-GigabitEthernet2/0/3] mpls te max-link-bandwidth 50000
[RouterB-GigabitEthernet2/0/3] mpls te max-reservable-bandwidth 40000
[RouterB-GigabitEthernet2/0/3] quit
```

在 Router C 上配置链路的最大带宽和最大可预留带宽。

```
[RouterC] interface gigabitethernet 2/0/1
[RouterC-GigabitEthernet2/0/1] mpls te max-link-bandwidth 50000
[RouterC-GigabitEthernet2/0/1] mpls te max-reservable-bandwidth 40000
[RouterC-GigabitEthernet2/0/1] quit
[RouterC] interface gigabitethernet 2/0/2
[RouterC-GigabitEthernet2/0/2] mpls te max-link-bandwidth 50000
[RouterC-GigabitEthernet2/0/2] mpls te max-reservable-bandwidth 40000
[RouterC-GigabitEthernet2/0/2] quit
[RouterC] interface gigabitethernet 2/0/3
[RouterC-GigabitEthernet2/0/3] mpls te max-link-bandwidth 50000
[RouterC-GigabitEthernet2/0/3] mpls te max-reservable-bandwidth 40000
[RouterC-GigabitEthernet2/0/3] quit
```

在 Router D 上配置链路的最大带宽和最大可预留带宽。

```
[RouterD] interface gigabitethernet 2/0/1
[RouterD-GigabitEthernet2/0/1] mpls te max-link-bandwidth 50000
[RouterD-GigabitEthernet2/0/1] mpls te max-reservable-bandwidth 40000
[RouterD-GigabitEthernet2/0/1] quit
```

在 Router E 上配置链路的最大带宽和最大可预留带宽。

```
[RouterE] interface gigabitethernet 2/0/1
[RouterE-GigabitEthernet2/0/1] mpls te max-link-bandwidth 50000
[RouterE-GigabitEthernet2/0/1] mpls te max-reservable-bandwidth 40000
[RouterE-GigabitEthernet2/0/1] quit
[RouterE] interface gigabitethernet 2/0/2
[RouterE-GigabitEthernet2/0/2] mpls te max-link-bandwidth 50000
[RouterE-GigabitEthernet2/0/2] mpls te max-reservable-bandwidth 40000
[RouterE-GigabitEthernet2/0/2] quit
```

(5) 配置 OSPF TE，发布链路的 MPLS TE 属性

Router A 上使能 OSPF 的 Opaque LSA 发布接收能力（缺省情况下处于开启状态），并在 OSPF 区域 0 内使能 MPLS TE 能力。

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

Router B 上使能 OSPF 的 Opaque LSA 发布接收能力（缺省情况下处于开启状态），并在 OSPF 区域 0 内使能 MPLS TE 能力。

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

```
[RouterB-ospf-1] quit
```

Router C 上使能 OSPF 的 Opaque LSA 发布接收能力（缺省情况下处于开启状态），并在 OSPF 区域 0 内使能 MPLS TE 能力。

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

Router D 上使能 OSPF 的 Opaque LSA 发布接收能力（缺省情况下处于开启状态），并在 OSPF 区域 0 内使能 MPLS TE 能力。

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

Router E 上使能 OSPF 的 Opaque LSA 发布接收能力（缺省情况下处于开启状态），并在 OSPF 区域 0 内使能 MPLS TE 能力。

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

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

配置主 CRLSP 的显式路径，缺省采用严格下一跳方式。

```
[RouterA] explicit-path pri-path
[RouterA-explicit-path-pri-path] nexthop 2.1.1.2
[RouterA-explicit-path-pri-path] nexthop 3.1.1.3
[RouterA-explicit-path-pri-path] nexthop 4.1.1.4
[RouterA-explicit-path-pri-path] nexthop 4.4.4.4
[RouterA-explicit-path-pri-path] quit
```

配置主 CRLSP 的 MPLS TE 隧道 Tunnel4：目的地址为 Router D 的 LSR ID（4.4.4.4）；采用 RSVP-TE 信令协议建立 MPLS TE 隧道；隧道所需带宽为 30000kbps；隧道引用显式路径 pri-path。

```
[RouterA] interface tunnel4 mode mpls-te
[RouterA-Tunnel4] ip address 10.1.1.1 255.255.255.0
[RouterA-Tunnel4] destination 4.4.4.4
[RouterA-Tunnel4] mpls te signaling rsvp-te
[RouterA-Tunnel4] mpls te bandwidth 30000
[RouterA-Tunnel4] mpls te path preference 1 explicit-path pri-path
```

开启 MPLS TE 隧道的 FRR 功能。

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

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

```
[RouterA] display interface tunnel
Tunnel4
Current state: UP
Line protocol state: UP
Description: Tunnel4 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 64000
Internet Address is 10.1.1.1/24 Primary
Tunnel source unknown, destination 4.4.4.4
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

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

```
[RouterA] display mpls te tunnel-interface
Tunnel Name            : Tunnel 4
Tunnel State           : Up (Main CRLSP up, Shared-resource CRLSP down)
Tunnel Attributes      :
  LSP ID               : 37325           Tunnel ID            : 4
  Admin State          : Normal
  Ingress LSR ID       : 1.1.1.1         Egress LSR ID        : 4.4.4.4
  Signaling            : RSVP-TE         Static CRLSP Name    : -
  Resv Style           : SE
  Tunnel mode          : -
  Reverse-LSP name     : -
  Reverse-LSP LSR ID   : -               Reverse-LSP Tunnel ID: -
  Class Type           : CT0             Tunnel Bandwidth     : 30000 kbps
  Reserved Bandwidth   : 30000 kbps
  Setup Priority       : 7               Holding Priority     : 7
  Affinity Attr/Mask   : 0/0
  Explicit Path        : pri-path
  Backup Explicit Path : -
  Metric Type          : TE
  Record Route         : Enabled         Record Label         : Enabled
  FRR Flag             : Enabled         Bandwidth Protection : Disabled
  Backup Bandwidth Flag: Disabled        Backup Bandwidth Type: -
  Backup Bandwidth     : -
  Bypass Tunnel        : No              Auto Created         : No
  Route Pinning        : Disabled
```

```
  Retry Limit          : 3               Retry Interval       : 2 sec
  Reoptimization       : Disabled        Reoptimization Freq  : -
  Backup Type          : None            Backup LSP ID        : -
  Auto Bandwidth       : Disabled        Auto Bandwidth Freq  : -
  Min Bandwidth        : -               Max Bandwidth        : -
  Collected Bandwidth  : -
```

(7) 在作为 PLR 的 Router B 上配置 Bypass 隧道

配置 Bypass 隧道的显式路径。

```
[RouterB] explicit-path by-path
[RouterB-explicit-path-by-path] nexthop 3.2.1.5
[RouterB-explicit-path-by-path] nexthop 3.3.1.3
[RouterB-explicit-path-by-path] nexthop 3.3.3.3
[RouterB-explicit-path-by-path] quit
```

配置 Bypass 隧道 Tunnel5：目的地址为 Router C 的 LSR ID（3.3.3.3）；采用 RSVP-TE 信令协议建立 MPLS TE 隧道；隧道所需带宽为 30000kbps；隧道引用显式路径 by-path。

```
[RouterB] interface tunnel 5 mode mpls-te
[RouterB-Tunnel5] ip address 11.1.1.1 255.255.255.0
[RouterB-Tunnel5] destination 3.3.3.3
[RouterB-Tunnel5] mpls te signaling rsvp-te
[RouterA-Tunnel5] mpls te backup bandwidth 30000
[RouterB-Tunnel5] mpls te path preference 1 explicit-path by-path
```

将 Bypass 隧道绑定到被保护的接口。

```
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] mpls te fast-reroute bypass-tunnel tunnel 5
[RouterB-GigabitEthernet2/0/2] quit
```

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

```
[RouterB] display interface tunnel
Tunnel5
Current state: UP
Line protocol state: DOWN
Description: Tunnel5 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 64000
Internet Address is 11.1.1.1/24 Primary
Tunnel source unknown, destination 3.3.3.3
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

(8) 配置静态路由使流量沿 MPLS TE 隧道转发

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

```
[Router A] ip route-static 4.1.1.0 24 tunnel 4 preference 1
```

4.6 验证配置

在所有设备上执行 **display mpls lsp** 命令，可以看到 LSP 表项。在 Router B 上存在两条 LSP，通过 Bypass 隧道保护主 CRLSP。

```
[RouterA] display mpls lsp
FEC                         Proto    In/Out Label    Interface/Out NHLFE
1.1.1.1/4/37325             RSVP     -/1150          GE2/0/1
2.1.1.2                     Local    -/-             GE2/0/1
Tunnel4                     Local    -/-             NHLFE1026
[RouterB] display mpls lsp
FEC                         Proto    In/Out Label    Interface/Out NHLFE
1.1.1.1/4/37325             RSVP     1150/1147       GE2/0/2
Backup                               1150/1147       Tun5
2.2.2.2/5/18928             RSVP     -/1149          GE2/0/3
3.1.1.3                     Local    -/-             GE2/0/2
3.2.1.5                     Local    -/-             GE2/0/3
Tunnel5                     Local    -/-             NHLFE1027
[RouterC] display mpls lsp
FEC                         Proto    In/Out Label    Interface/Out NHLFE
1.1.1.1/4/37325             RSVP     1147/3          GE2/0/1
2.2.2.2/5/18928             RSVP     3/-             -
4.1.1.4                     Local    -/-             GE2/0/1
```

在 PLR 上 **shutdown** 被保护的出接口 GigabitEthernet2/0/2。

```
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] shutdown
[RouterB-GigabitEthernet2/0/2] quit
```

在 Router A 上执行 **display interface tunnel 4** 命令查看主 CRLSP 的状态，可以看到 Tunnel 接口仍然处于 UP 状态。

```
[RouterA] display interface tunnel 4
Tunnel4
Current state: UP
Line protocol state: UP
Description: Tunnel4 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 64000
Internet Address is 10.1.1.1/24 Primary
Tunnel source unknown, destination 4.4.4.4
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
```

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

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

```
[RouterA] display mpls te tunnel-interface
Tunnel Name            : Tunnel 4
Tunnel State           : Up (Main CRLSP up, Shared-resource CRLSP being set up)
Tunnel Attributes      :
  LSP ID               : 37325           Tunnel ID            : 4
  Admin State          : Normal
  Ingress LSR ID       : 1.1.1.1         Egress LSR ID        : 4.4.4.4
  Signaling            : RSVP-TE         Static CRLSP Name    : -
  Resv Style           : SE
  Tunnel mode          : -
  Reverse-LSP name     : -
  Reverse-LSP LSR ID   : -               Reverse-LSP Tunnel ID: -
  Class Type           : CT0             Tunnel Bandwidth     : 30000 kbps
  Reserved Bandwidth   : 30000 kbps
  Setup Priority       : 7               Holding Priority     : 7
  Affinity Attr/Mask   : 0/0
  Explicit Path        : pri-path
  Backup Explicit Path : -
  Metric Type          : TE
  Record Route         : Enabled         Record Label         : Enabled
  FRR Flag             : Enabled         Bandwidth Protection : Disabled
  Backup Bandwidth Flag: Disabled        Backup Bandwidth Type: -
  Backup Bandwidth     : -
  Bypass Tunnel        : No              Auto Created         : No
  Route Pinning        : Disabled
  Retry Limit          : 3               Retry Interval       : 2 sec
  Reoptimization       : Disabled        Reoptimization Freq  : -
  Backup Type          : None            Backup LSP ID        : -
  Auto Bandwidth       : Disabled        Auto Bandwidth Freq  : -
  Min Bandwidth        : -               Max Bandwidth        : -
  Collected Bandwidth  : -
```

在 Router B 上执行 **display mpls lsp** 命令，可以看到 Bypass 隧道被使用。

```
[RouterB] display mpls lsp
FEC                       Proto    In/Out Label    Interface/Out NHLFE
1.1.1.1/4/37325           RSVP     1150/1147       Tun5
2.2.2.2/5/18928           RSVP     -/1149          GE2/0/3
3.2.1.5                   Local    -/-             GE2/0/3
Tunnel5                   Local    -/-             NHLFE1027
```

在 PLR 上配置在多条旁路隧道中进行优选的时间间隔为 5 秒。

```
[RouterB] mpls te
[RouterB-te] fast-reroute timer 5
```

```
[RouterB-te] quit
```

在 PLR 上 **undo shutdown** 被保护的出接口 GigabitEthernet2/0/2。

```
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] undo shutdown
[RouterB-GigabitEthernet2/0/2] quit
```

在 Router A 上执行 **display interface tunnel 4** 命令查看主 CRLSP 的状态，可以看到 Tunnel 接口处于 up 状态。

```
[RouterA] display interface tunnel 4
Tunnel4
Current state: UP
Line protocol state: UP
Description: Tunnel4 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 64000
Internet Address is 10.1.1.1/24 Primary
Tunnel source unknown, destination 4.4.4.4
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

等待约 5 秒钟后，在 Router B 上执行 **display mpls lsp verbose** 命令，可以看到 Tunnel5 仍绑定到出接口 GigabitEthernet2/0/2，但未被使用。

```
[RouterB] display mpls lsp verbose
Destination  : 4.4.4.4
FEC          : 1.1.1.1/4/53319
Protocol     : RSVP
LSR Type     : Transit
Service      : -
In-Label     : 1150
Path ID      : 0x540000003.1
State        : Active
Out-Label    : 1150
Nexthop      : 3.1.1.3
Out-Interface: GE2/0/2
BkLabel      : 1150
BkInterface  : Tun5

Destination  : 3.3.3.3
FEC          : 2.2.2.2/5/16429
Protocol     : RSVP
LSR Type     : Ingress
```

```
Service      : -
NHLFE ID     : 1025
State        : Active
Out-Label    : 1151
Nexthop      : 3.2.1.5
Out-Interface: GE2/0/3

Destination  : 3.1.1.3
FEC          : 3.1.1.3
Protocol     : Local
LSR Type     : Ingress
Service      : -
NHLFE ID     : 1027
State        : Active
Nexthop      : 3.1.1.3
Out-Interface: GE2/0/2

Destination  : 3.2.1.5
FEC          : 3.2.1.5
Protocol     : Local
LSR Type     : Ingress
Service      : -
NHLFE ID     : 1024
State        : Active
Nexthop      : 3.2.1.5
Out-Interface: GE2/0/3

Destination  : 3.3.3.3
FEC          : Tunnel5
Protocol     : Local
LSR Type     : Ingress
Service      : -
NHLFE ID     : 268435461
State        : Active
Out-Interface: NHLFE1025
```

在 Router A 上执行 **display ip routing-table** 命令，可以看到路由表中有以 Tunnel4 为出接口的静态路由信息。

```
[RouterA] display ip routing-table
Destinations : 25        Routes : 25

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
1.1.1.1/32         Direct  0   0           127.0.0.1       InLoop0
2.1.1.0/24         Direct  0   0           2.1.1.1         GE2/0/1
2.1.1.0/32         Direct  0   0           2.1.1.1         GE2/0/1
2.1.1.1/32         Direct  0   0           127.0.0.1       InLoop0
2.1.1.255/32       Direct  0   0           2.1.1.1         GE2/0/1
2.2.2.2/32         O_INTRA 10  1           2.1.1.2         GE2/0/1
```

```
3.1.1.0/24          O_INTRA 10  2           2.1.1.2         GE2/0/1
3.2.1.0/24          O_INTRA 10  2           2.1.1.2         GE2/0/1
3.3.1.0/24          O_INTRA 10  3           2.1.1.2         GE2/0/1
3.3.3.3/32          O_INTRA 10  2           2.1.1.2         GE2/0/1
4.1.1.0/24          Static  1   0           0.0.0.0         Tun4
4.4.4.4/32          O_INTRA 10  3           2.1.1.2         GE2/0/1
5.5.5.5/32          O_INTRA 10  2           2.1.1.2         GE2/0/1
10.1.1.0/24         Direct  0   0           10.1.1.1        Tun4
10.1.1.0/32         Direct  0   0           10.1.1.1        Tun4
10.1.1.1/32         Direct  0   0           127.0.0.1       InLoop0
10.1.1.255/32       Direct  0   0           10.1.1.1        Tun4
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
```

4.7 配置文件

- Router A

```
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 2.1.1.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 1.1.1.1
#
mpls te
#
explicit-path pri-path
 nexthop index 1 2.1.1.2 include strict
 nexthop index 101 3.1.1.3 include strict
 nexthop index 201 4.1.1.4 include strict
 nexthop index 301 4.4.4.4 include strict
#
rsvp
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 2.1.1.1 255.255.255.0
 mpls enable
```

```
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface Tunnel4 mode mpls-te
 ip address 10.1.1.1 255.255.255.0
 mpls te bandwidth ct0 30000
 mpls te path preference 1 explicit-path pri-path
 mpls te fast-reroute
 destination 4.4.4.4
#
ip route-static 4.1.1.0 24 Tunnel4 preference 1
#
```

- Router B

```
#
ospf 1
 area 0.0.0.0
  network 2.1.1.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
  network 3.1.1.0 0.0.0.255
  network 3.2.1.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 2.2.2.2
#
mpls te
  fast-reroute timer 5
#
explicit-path by-path
 nexthop index 1 3.2.1.5 include strict
 nexthop index 101 3.3.1.3 include strict
 nexthop index 201 3.3.3.3 include strict
#
rsvp
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 2.1.1.2 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
```

```
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 3.1.1.2 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 mpls te fast-reroute bypass-tunnel Tunnel5
 rsvp enable
 rsvp bfd enable
#
interface GigabitEthernet2/0/3
 port link-mode route
 ip address 3.2.1.2 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface Tunnel5 mode mpls-te
 ip address 11.1.1.1 255.255.255.0
 mpls te backup bandwidth ct0 30000
 mpls te path preference 1 explicit-path by-path
 destination 3.3.3.3
#
```

- Router C

```
#
ospf 1
 area 0.0.0.0
  network 3.1.1.0 0.0.0.255
  network 3.3.1.0 0.0.0.255
  network 3.3.3.3 0.0.0.0
  network 4.1.1.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 3.3.3.3
#
mpls te
#
rsvp
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 4.1.1.3 255.255.255.0
```

```
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 3.1.1.3 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
 rsvp bfd enable
#
interface GigabitEthernet2/0/3
 port link-mode route
 ip address 3.3.1.3 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
```

- Router D

```
#
ospf 1
 area 0.0.0.0
  network 4.1.1.0 0.0.0.255
  network 4.4.4.4 0.0.0.0
  mpls te enable
#
 mpls lsr-id 4.4.4.4
#
mpls te
#
rsvp
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 4.1.1.4 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
```

```
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
```

- Router E

```
#
ospf 1
 area 0.0.0.0
  network 3.2.1.0 0.0.0.255
  network 3.3.1.0 0.0.0.255
  network 5.5.5.5 0.0.0.0
  mpls te enable
#
 mpls lsr-id 5.5.5.5
#
mpls te
#
rsvp
#
interface LoopBack0
 ip address 5.5.5.5 255.255.255.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 3.2.1.5 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 3.3.1.5 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
```

5 相关资料

- H3C SR6600 SR6600-X 路由器 MPLS 配置指导-R7607
- H3C SR6600 SR6600-X 路由器 MPLS 命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

NAT 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 配置举例 1
3.1 组网需求 1
3.2 配置思路 2
3.3 使用版本 2
3.4 配置步骤 2
3.5 验证配置 3
3.6 配置文件 5
4 相关资料 5

1 简介

本文介绍 NAT 配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 NAT 特性。

3 配置举例

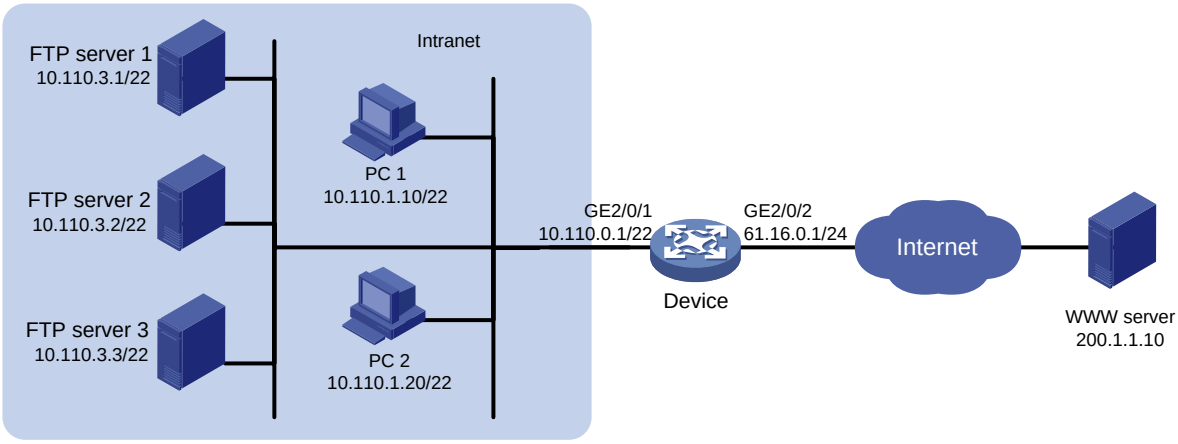
3.1 组网需求

如图 1 所示，某公司内网地址是 10.110.0.0/22，向运营商申请的公网地址是 61.16.0.1～61.16.0.3。公司内网用户使用 10.110.0.0～10.110.2.255 地址段内 IP 地址；公司内网目前共有 3 台 FTP 服务器可以同时提供服务，服务器使用 10.110.3.1～10.110.3.3 的 IP 地址。

要求实现如下功能：

- 内网用户经过地址转换后使用 61.16.0.2～61.16.0.3 公网地址访问 Internet；
- 外网主机和内网主机都可以通过 61.16.0.1 访问内网中的 FTP 服务器；
- 3 台 FTP 服务器提供服务时进行负载分担，但不允许主动访问外网。

图1 负载分担内部服务器配置组网图



3.2 配置思路

- 为了实现 10.110.0.0～10.110.2.255 可以转换成 61.16.0.2～61.16.0.3 公网地址访问 Internet，需要定义 ACL 规则，实现只对内网匹配指定的 ACL 规则的报文在 Device 的 GigabitEthernet2/0/2 出方向上进行动态地址转换。
- 为了保证 3 台 FTP 服务器同时提供服务，需要配置 NAT 内部服务器组，并采用负载分担方式。
- 为了实现内网用户也可以使用 61.16.0.1 地址访问 FTP 服务器，需要在 Device 的 GigabitEthernet2/0/1 上使能 NAT hairpin 功能。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置步骤

1. 配置接口 IP 地址

配置接口 GigabitEthernet 2/0/1 和 GigabitEthernet 2/0/2 的 IP 地址。

```
<Device> system-view
[Device] interface gigabitethernet 2/0/1
[Device-GigabitEthernet2/0/1] ip address 10.110.0.1 255.255.252.0
[Device-GigabitEthernet2/0/1] quit
[Device] interface gigabitethernet 2/0/2
[Device-GigabitEthernet2/0/2] ip address 61.16.0.1 255.255.255.0
[Device-GigabitEthernet2/0/2] quit
```

2. 配置内网用户访问外网

配置地址组 0，包含两个外网地址 61.16.0.2 和 61.16.0.3。

```
[Device] nat address-group 0
[Device-nat-address-group-0] address 61.16.0.2 61.16.0.3
[Device-nat-address-group-0] quit
```

配置 ACL 2000，仅允许对内部网络中 10.110.0.0～10.110.2.255 网段的用户报文进行地址转换。

```
[Device] acl basic 2000
[Device-acl-ipv4-basic-2000] rule permit source 10.110.0.0 0.0.1.255
[Device-acl-ipv4-basic-2000] rule permit source 10.110.2.0 0.0.0.255
[Device-acl-ipv4-basic-2000] quit
```

在接口 GigabitEthernet2/0/2 上配置出方向动态地址转换，允许使用地址组 0 中的地址对匹配 ACL 2000 的报文进行源地址转换，并在转换过程中使用端口信息。

```
[Device] interface gigabitethernet 2/0/2
[Device-GigabitEthernet2/0/2] nat outbound 2000 address-group 0
[Device-GigabitEthernet2/0/2] quit
```

3. 配置 FTP 服务器同时提供服务

配置内部服务器组 0 及其成员 10.110.3.1、10.110.3.2 和 10.110.3.3。

```
[Device] nat server-group 0
[Device-nat-server-group-0] inside ip 10.110.3.1 port 21
[Device-nat-server-group-0] inside ip 10.110.3.2 port 21
```

```
[Device-nat-server-group-0] inside ip 10.110.3.3 port 21
[Device-nat-server-group-0] quit
```

在接口 Gigabitethernet2/0/2 上配置负载分担内部服务器，引用内部服务器组 0，该组内的主机共同提供 FTP 服务。

```
[Device] interface gigabitethernet 2/0/2
[Device-GigabitEthernet2/0/2] nat server protocol tcp global 61.16.0.1 ftp inside
server-group 0
```

在接口 GigabitEthernet2/0/1 上使能 NAT hairpin 功能。

```
[Device] interface gigabitethernet 2/0/1
[Device-GigabitEthernet2/0/1] nat hairpin enable
```

3.5 验证配置

当 PC 1 访问 WWW server 时，可以看到生成的 NAT 会话信息。

```
[Device] display nat session verbose
Initiator:
  Source      IP/port: 10.110.1.10/1024
  Destination IP/port: 200.1.1.10/80
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: UDP(17)
Responder:
  Source      IP/port: 200.1.1.10/80
  Destination IP/port: 61.16.0.2/1025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: UDP(17)
State: UDP_READY
Application: HTTP
Start time: 2017-07-08 13:30:47  TTL: 60s
Interface(in) : GigabitEthernet2/0/1
Interface(out): GigabitEthernet2/0/2
Initiator->Responder:     21946552 packets 2414120720 bytes
Responder->Initiator:       650389 packets   71542790 bytes

Total sessions found: 1
```

当有两个外网用户（61.16.0.10、61.16.0.11）同时请求 FTP 服务时，可以查看到建立了 2 条 NAT 会话，并且 FTP server 1 和 FTP server 2 分别为这两个用户提供 FTP 服务。

```
[Device] display nat session verbose
Initiator:
  Source      IP/port: 61.16.0.11/1024
  Destination IP/port: 61.16.0.1/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
Responder:
  Source      IP/port: 10.110.3.1/21
```

```
  Destination IP/port: 61.16.0.11/1024
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
State: TCP_ESTABLISHED
Application: FTP
Start time: 2017-07-08 14:11:41  TTL: 3600s
Interface(in) : GigabitEthernet2/0/2
Interface(out): GigabitEthernet2/0/1
Initiator->Responder:       598098 packets   65790780 bytes
Responder->Initiator:            0 packets          0 bytes

Initiator:
  Source      IP/port: 61.16.0.10/1024
  Destination IP/port: 61.16.0.1/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
Responder:
  Source      IP/port: 10.110.3.2/21
  Destination IP/port: 61.16.0.10/1024
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
State: TCP_ESTABLISHED
Application: FTP
Start time: 2017-07-08 14:12:00  TTL: 3600s
Interface(in) : GigabitEthernet2/0/2
Interface(out): GigabitEthernet2/0/1
Initiator->Responder:        74783 packets    8226130 bytes
Responder->Initiator:            0 packets          0 bytes

Total sessions found: 2
```

当 PC 1 通过 61.16.0.1 地址访问 FTP 服务器时，可以查看到建立的 NAT 会话。

```
[Device] display nat session verbose
Initiator:
  Source      IP/port: 10.110.1.10/1024
  Destination IP/port: 61.16.0.1/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
Responder:
  Source      IP/port: 10.110.3.1/21
  Destination IP/port: 61.16.0.2/1025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
State: TCP_ESTABLISHED
```

```
Application: FTP
Start time: 2017-07-08 14:24:15  TTL: 3600s
Interface(in) : GigabitEthernet2/0/1
Interface(out): GigabitEthernet2/0/1
Initiator->Responder:       209716 packets   23068760 bytes
Responder->Initiator:            0 packets          0 bytes

Total sessions found: 1
```

3.6 配置文件

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.110.0.1 255.255.252.0
 qos apply policy 1 inbound
 nat hairpin enable
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 61.16.0.1 255.255.255.0
 nat outbound 2000 address-group 0
 nat server protocol tcp global 61.16.0.1 21 inside server-group 0
#
acl basic 2000
 rule 0 permit source 10.110.0.0 0.0.1.255
 rule 5 permit source 10.110.2.0 0.0.0.255
#
acl basic 2001
 rule 0 permit source 10.110.0.0 0.0.1.255
 rule 5 permit source 10.110.2.0 0.0.0.255
#
nat address-group 0
 address 61.16.0.2 61.16.0.3
#
nat server-group 0
 inside ip 10.110.3.1 port 21
 inside ip 10.110.3.2 port 21
 inside ip 10.110.3.3 port 21
#
```

4 相关资料

- H3C SR6600 SR6600-X 路由器 三层技术-IP 业务配置指导-R7607
- H3C SR6600 SR6600-X 路由器三层技术-IP 业务配置指导-R7607

H3C SR6600/SR6600-X 系列路由器

NetStream 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 IPv4 NetStream 典型配置举例 1
3.1 组网需求 1
3.2 使用版本 2
3.3 配置注意事项 2
3.4 配置步骤 2
3.4.1 Gateway 的配置 2
3.4.2 服务器的配置 2
3.5 验证配置 4
3.6 配置文件 5
4 IPv6 NetStream 典型配置举例 5
4.1 组网需求 5
4.2 使用版本 6
4.3 配置注意事项 6
4.4 配置步骤 6
4.4.1 Gateway 的配置 6
4.4.2 服务器的配置 7
4.5 验证配置 9
4.6 配置文件 9
5 相关资料 10

1 简介

本章介绍了 IPv4 NetStream 典型配置举例和 IPv6 NetStream 典型配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

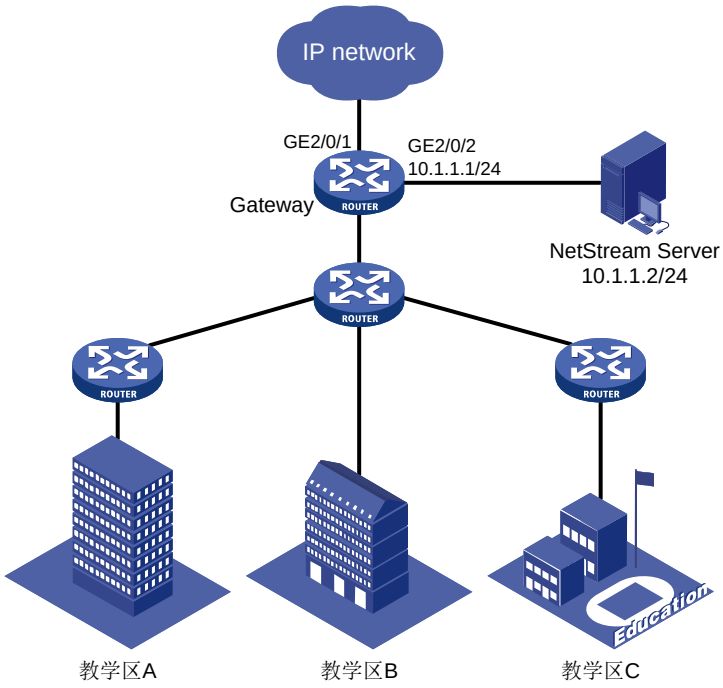
本文档假设您已了解 Netstream 特性。

3 IPv4 NetStream 典型配置举例

3.1 组网需求

如图 1 所示，某校园被划分为三个教学区，在 Gateway 上配置 IPv4 NetStream，以实现对内网用户的上网流量和行为进行监控。

图1 IPv4 NetStream 典型配置组网图



3.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.3 配置注意事项

- 设备输出统计报文的目的 UDP 端口号与 NetStream 服务器的 UDP 端口号必须保持一致。
- 本配置举例中，Netstream 服务器以 IMC PLAT 7.0 (E0202)为例进行介绍。

3.4 配置步骤

3.4.1 Gateway 的配置

在 Gateway 的出、入方向启用 NetStream 统计功能。

```
<Gateway> system-view
[Gateway] interface gigabitethernet 2/0/1
[Gateway-GigabitEthernet2/0/1] ip netstream inbound
[Gateway-GigabitEthernet2/0/1] ip netstream outbound
[Gateway-GigabitEthernet2/0/1] quit
```

配置 GE2/0/2 作为 NetStream 统计输出报文的源接口。

```
[Gateway] interface gigabitethernet 2/0/2
[Gateway-GigabitEthernet2/0/2] ip address 10.1.1.1 255.255.255.0
[Gateway-GigabitEthernet2/0/2] quit
[Gateway] ip netstream export source interface gigabitethernet 2/0/2
```

配置普通流统计信息输出的目的地址和 UDP 端口号。

```
[Gateway] ip netstream export host 10.1.1.2 5000
```

3.4.2 服务器的配置

增加设备

- 登录 iMC，选择“业务”页签，在左导航树中选择[流量分析与审计/配置管理]，进入配置管理页面；
- 在“网络流量分析与审计快速配置向导”区域点击“设备管理”链接，进入设备列表页面；
- 单击<增加>按钮增加设备，如图 2 所示。

图2 增加设备

下发服务器配置

- 选择“业务”页签，在左导航树中选择[流量分析与审计/配置管理]，进入配置管理页面；
- 点击“服务器管理”链接，进入服务器列表页面；
- 点击 NTA/UBA 服务器对应的“修改”图标，进入服务器配置页面；
- 配置相应的服务器参数，如图 3 所示，单击<下发>按钮下发服务器配置。

图3 下发服务器配置

增加流量分析任务

NTA 支持增加多种流量分析任务，这里以接口流量分析任务为例，配置步骤如下：

- 择“业务”页签，在左导航树中选择[流量分析与审计/配置管理]，进入配置管理页面；
- 点击“流量分析任务管理”链接，进入流量分析任务管理页面；
- 在流量分析任务列表中，单击<增加>按钮，进入任务类型选择页面；

- 选择“接口”任务类型，单击<下一步>按钮，进入增加流量分析任务参数配置页面；
- 配置相应的基本信息和接口信息后，单击<确定>按钮，增加任务成功，如图 4 所示。

图4 增加流量分析任务

3.5 验证配置

在完成上述配置后，查看 NetStream 统计输出报文的信息。

```
[Gateway] display ip netstream export
IP export information:
  Flow source interface                          : GigabitEthernet2/0/2
  Flow destination VPN instance                  : Not specified
  Flow destination IP address (UDP)              : 10.1.1.2 (5000)
  Version 5 exported flow number                 : 8
  Version 5 exported UDP datagram number (failed) : 8 (0)
  Version 9 exported flow number                 : 0
  Version 9 exported UDP datagram number (failed) : 0 (0)
```

在 Netstream 服务器上可以查看接口任务 Interface 的流量信息

选择“业务”页签，在左导航树中选择[流量分析与审计/接口流量分析任务]，进入接口流量分析汇总页面，查看流量信息有两种方法：

- 在汇总页面下方的“汇总列表”区域，点击任务名称“域，点击任务名称汇总链接，进入 Interface 流量分析页面；
- 将鼠标移至左导航树中“接口流量分析任务”链接右侧的快捷菜单图标上，在弹出的快捷菜单中点击“接右侧的快捷菜单图标链接，进入 Interface 流量分析页面。如图 5 所示。

图5 Interface 流量分析

3.6 配置文件

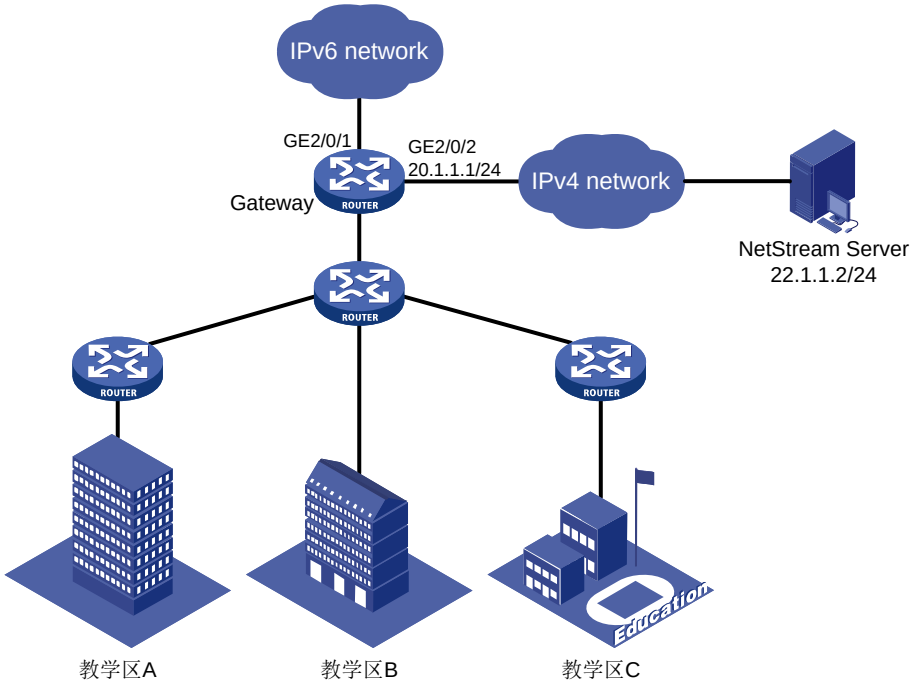
```
#
interface GigabitEthernet2/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/1
 ip netstream inbound
 ip netstream outbound
#
 ip netstream export host 10.1.1.2 5000
 ip netstream export source interface GigabitEthernet2/0/2
#
```

4 IPv6 NetStream 典型配置举例

4.1 组网需求

如图 6 所示，某校园要建设 IPv6 网络，现要求在 Gateway 上配置 IPv6 NetStream，以实现对内网用户的上网流量和行为进行监控。

图6 IPv6 NetStream 典型组网图



4.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.3 配置注意事项

- 设备输出统计报文的目的 UDP 端口号与 NetStream 服务器的 UDP 端口号必须保持一致。
- 本配置举例中，Netstream 服务器以 IMC PLAT 7.0 (E0202)为例进行介绍。

4.4 配置步骤

4.4.1 Gateway 的配置

配置服务器的 IP 地址为 22.1.1.2/24，并确保服务器与 Gateway 之间路由可达。（配置步骤略）

配置 GigabitEthernet2/0/1，在出、入方向启动 IPv6 NetStream 统计。

```
<Gateway> system-view
[Gateway] interface GigabitEthernet 2/0/1
[Gateway-GigabitEthernet2/0/1] ipv6 netstream inbound
[Gateway-GigabitEthernet2/0/1] ipv6 netstream outbound
[Gateway-GigabitEthernet2/0/1] quit
```

在 GE2/0/2 上配置 IP 地址。

```
[Gateway] interface gigabitethernet 2/0/2
[Gateway-GigabitEthernet2/0/2] ip address 20.1.1.1 255.255.255.0
[Gateway-GigabitEthernet2/0/2] quit
```

配置 IPv6 NetStream 聚合统计信息输出的源接口

```
[Gateway] ipv6 netstream export source interface GigabitEthernet 2/0/2
```

配置 IPv6 NetStream 普通流统计信息输出的目的地址和 UDP 端口号。

```
[Gateway] ipv6 netstream export host 22.1.1.2 5000
```

4.4.2 服务器的配置

增加设备

- 登录 iMC，选择“业务”页签，在左导航树中选择[流量分析与审计/配置管理]，进入配置管理页面；
- 在“网络流量分析与审计快速配置向导”区域点击“设备管理”链接，进入设备列表页面；
- 单击<增加>按钮增加设备，如图 7 所示。

图7 增加设备

下发服务器配置

- 选择“业务”页签，在左导航树中选择[流量分析与审计/配置管理]，进入配置管理页面；
- 点击“服务器管理”链接，进入服务器列表页面；
- 点击 NTA/UBA 服务器对应的“修改”图标，进入服务器配置页面；
- 配置相应的服务器参数，如图 8 所示，单击<下发>按钮下发服务器配置。

图8 下发服务器配置

增加流量分析任务

NTA 支持增加多种流量分析任务，这里以接口流量分析任务为例，配置步骤如下：

- 择“业务”页签，在左导航树中选择[流量分析与审计/配置管理]，进入配置管理页面；
- 点击“流量分析任务管理”链接，进入流量分析任务管理页面；
- 在流量分析任务列表中，单击<增加>按钮，进入任务类型选择页面；
- 选择“接口”任务类型，单击<下一步>按钮，进入增加流量分析任务参数配置页面；
- 配置相应的基本信息和接口信息后，单击<确定>按钮，增加任务成功，如 3.4.2 图 4 所示。

图9 增加流量分析任务

4.5 验证配置

在完成上述配置后，查看 IPv6 NetStream 统计输出报文的信息。

```
[Gateway] display ipv6 netstream export
IPv6 export information:
  Flow source interface                          : GigabitEthernet2/0/2
  Flow destination VPN instance                  : Not specified
  Flow destination IP address (UDP)              : 22.1.1.2 (5000)
  Version 9 exported flow number                 : 0
  Version 9 exported UDP datagram number (failed) : 0 (0)
```

在 Netstream 服务器上可以查看接口任务 Interface 的流量信息

选择“业务”页签，在左导航树中选择[流量分析与审计/接口流量分析任务]，进入接口流量分析汇总页面，查看流量信息有两种方法：

- 在汇总页面下方的“汇总列表”区域，点击任务名称“Interface”链接，进入 Interface 流量分析页面；
- 将鼠标移至左导航树中“接口流量分析任务”链接右侧的快捷菜单图标上，在弹出的快捷菜单中点击“Interface”链接，进入 Interface 流量分析页面。如图 10 所示。

图10 Interface 流量分析

4.6 配置文件

```
#
interface GigabitEthernet2/0/2
 ip address 20.1.1.1 255.255.255.0
```

```
#
interface GigabitEthernet2/0/1
 ipv6 netstream inbound
 ipv6 netstream outbound
#
 ipv6 netstream export host 22.1.1.2 5000
 ipv6 netstream export source interface GigabitEthernet2/0/2
```

5 相关资料

- H3C SR6600 SR6600-X 路由器 网络管理和监控配置指导-R7607
- H3C SR6600 SR6600-X 路由器 网络管理和监控命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

NQA 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 0

2 配置前提 0

3 使用限制 0

4 ICMP-echo 测试典型配置指导 0

4.1 组网需求 0

4.2 使用版本 1

4.3 配置注意事项 1

4.4 配置步骤 1

4.5 验证配置 1

4.6 配置文件 2

5 DHCP 测试典型配置指导 2

5.1 组网需求 2

5.2 使用版本 3

5.3 配置注意事项 3

5.4 配置步骤 3

5.5 验证配置 3

5.6 配置文件 4

6 DNS 测试典型配置指导 4

6.1 组网需求 4

6.2 使用版本 4

6.3 配置注意事项 4

6.4 配置步骤 5

6.5 验证配置 5

6.6 配置文件 5

7 FTP 测试典型配置指导 6

7.1 组网需求 6

7.2 使用版本 6

7.3 配置注意事项 6

7.4 配置步骤 6

7.5 验证配置 7

7.6 配置文件 7

8 HTTP 测试典型配置指导 ····· 8
8.1 组网需求 ····· 8
8.2 使用版本 ····· 8
8.3 配置注意事项 ····· 8
8.4 配置步骤 ····· 8
8.5 验证配置 ····· 9
8.6 配置文件 ····· 9
9 相关资料 ····· 9

1 简介

本文档介绍了 NQA（Network Quality Analyzer，网络质量分析）特性的典型配置举例。

NQA 通过发送测试报文，对网络性能、网络提供的服务及服务质量进行分析，并为用户提供网络性能和服务质量的参数，如时延抖动、TCP 连接时延、FTP 连接时延和文件传输速率等。利用 NQA 的测试结果，用户可以及时了解网络的性能状况，针对不同的网络性能进行相应处理并对网络故障进行诊断和定位。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文假设您已了解 NQA 特性。

3 使用限制

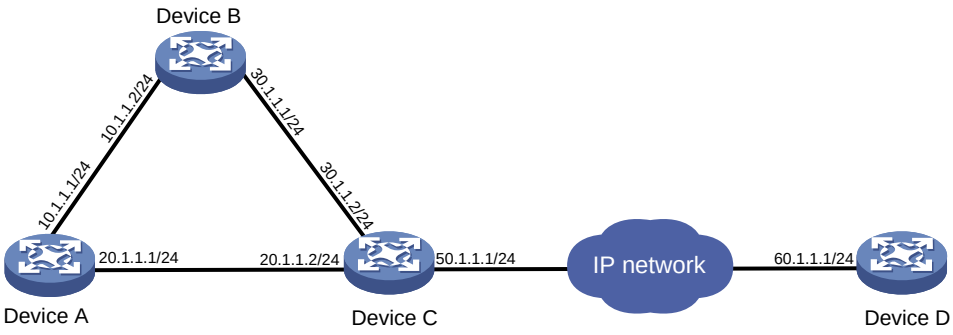
ICMP-echo 测试不支持在 IPv6 网络中使用，如果要测试 IPv6 网络中目的主机的可达性，可以使用 **ping ipv6** 命令；

4 ICMP-echo 测试典型配置指导

4.1 组网需求

当前网络如图 1 所示，Device A 到 Device D 有两条链路，其中经过 Device B 的是一条次优的备份链路。现要求配置 ICMP-echo 测试方案，使用户可以根据实际需要随时调用该测试方案测试 Device A 发送的报文经过指定的下一跳（Device B）是否可以到达 Device D，以及报文的往返时间。

图1 ICMP-echo 测试组网图



4.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.3 配置注意事项

- 进行 NQA 测试之前，请确保各设备之间路由可达。
- 测试组开始测试后就不能再进入该测试组视图和测试类型视图进行配置修改，测试结束后才可以进入该测试组视图和测试类型视图。

4.4 配置步骤

创建 ICMP-echo 类型的 NQA 测试组（管理员为 admin，操作标签为 test），并配置测试操作的目的地址为 60.1.1.1。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type icmp-echo
[DeviceA-nqa-admin-test-icmp-echo] destination ip 60.1.1.1
```

配置下一跳地址为 10.1.1.2，以便测试报文经过指定的下一跳设备（Device B）到达目的端，而不是通过 Device C 到达目的端。

```
[DeviceA-nqa-admin-test-icmp-echo] next-hop 10.1.1.2
```

配置可选参数：一次 NQA 测试中探测的次数为 10，探测的超时时间为 500 毫秒，测试组连续两次测试开始时间的时间间隔为 5000 毫秒。

```
[DeviceA-nqa-admin-test-icmp-echo] probe count 10
[DeviceA-nqa-admin-test-icmp-echo] probe timeout 500
[DeviceA-nqa-admin-test-icmp-echo] frequency 5000
```

开启 NQA 历史记录保存功能，并配置一个测试组中能够保存的最大历史记录个数为 10。

```
[DeviceA-nqa-admin-test-icmp-echo] history-record enable
[DeviceA-nqa-admin-test-icmp-echo] history-record number 10
[DeviceA-nqa-admin-test-icmp-echo] quit
```

4.5 验证配置

启动 ICMP-echo 测试方案进行测试。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

测试执行一段时间后，停止 ICMP-echo 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

以上配置完成后，显示 ICMP-echo 测试中最后一次测试的结果。

```
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 10              Receive response times: 10
    Min/Max/Average round trip time: 2/5/3
    Square-Sum of round trip time: 96
    Last succeeded probe time: 2017-03-23 15:00:01.2
  Extended results:
```

```
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

显示 ICMP-echo 测试的历史记录。

```
[DeviceA] display nqa history admin test
NQA entry (admin admin, tag test) history records:
  Index      Response     Status           Time
  370        3            Succeeded        2017-03-23 15:00:01.2
  369        3            Succeeded        2017-03-23 15:00:01.2
  368        3            Succeeded        2017-03-23 15:00:01.2
  367        5            Succeeded        2017-03-23 15:00:01.2
  366        3            Succeeded        2017-03-23 15:00:01.2
  365        3            Succeeded        2017-03-23 15:00:01.2
  364        3            Succeeded        2017-03-23 15:00:01.1
  363        2            Succeeded        2017-03-23 15:00:01.1
  362        3            Succeeded        2017-03-23 15:00:01.1
  361        2            Succeeded        2017-03-23 15:00:01.1
```

以上显示信息表示，Device A 发送的报文可以通过 Device B 到达 Device D；测试过程中未发生丢包；报文的最小、最大、平均往返时间分别为 2 毫秒、5 毫秒和 3 毫秒。

4.6 配置文件

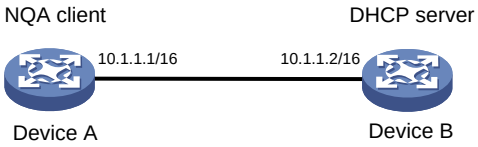
```
#
nqa entry admin test
 type icmp-echo
  destination ip 60.1.1.1
  frequency 5000
  history-record enable
  history-record number 10
  next-hop 10.1.1.2
  probe count 10
  probe timeout 500
#
```

5 DHCP 测试典型配置指导

5.1 组网需求

当前网络如图 2 所示，现要求配置 DHCP 测试方案，使用户可以根据实际需要随时调用该测试方案测试 Device A 是否可以从 DHCP 服务器 Device B 申请到 IP 地址以及申请到 IP 地址所需的时间。

图2 DHCP 测试组网图



5.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

5.3 配置注意事项

- 进行 NQA 测试之前，请确保各设备之间路由可达。
- 测试组开始测试后就不能再进入该测试组视图和测试类型视图进行配置修改，测试结束后才可以进入该测试组视图和测试类型视图。
- 在进行 DHCP 测试之前，需要完成 DHCP 服务器的配置。

5.4 配置步骤

创建 DHCP 类型的 NQA 测试组。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type dhcp
```

指定进行 DHCP 测试的目的地址为 10.1.1.2。

```
[DeviceA-nqa-admin-test-dhcp] destination ip 10.1.1.2
```

开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test-dhcp] history-record enable
[DeviceA-nqa-admin-test-dhcp] quit
```

5.5 验证配置

启动 DHCP 测试方案进行测试。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

测试执行一段时间后，停止 DHCP 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

以上配置完成后，显示 DHCP 测试中最后一次测试的结果。

```
[DeviceA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 624/624/624
      Square-Sum of round trip time: 389376
      Last succeeded probe time: 2017-03-24 09:56:03.2
    Extend results:
```

```
    Packet lost in test: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

显示 DHCP 测试的历史记录。

```
[DeviceA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          624          Succeeded        2017-03-24 09:56:03.2
```

以上显示信息表示，Router A 可以从 DHCP 服务器获取 IP 地址，获取 IP 地址所需的时间为 624 毫秒。

5.6 配置文件

```
#
nqa entry admin test
 type dhcp
  destination ip 10.1.1.2
  history-record enable
#
```

6 DNS 测试典型配置指导

6.1 组网需求

当前网络如图 3 所示，现要求配置 DNS 测试方案，使用户可以根据实际需要随时调用该测试方案测试 Device A 是否可以通过指定的 DNS 服务器将域名 host.com 解析为 IP 地址，以及域名解析所需的时间。

图3 DNS 测试组网图

6.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

6.3 配置注意事项

- 进行 NQA 测试之前，请确保各设备之间路由可达。
- 测试组开始测试后就不能再进入该测试组视图和测试类型视图进行配置修改，测试结束后才可以进入该测试组视图和测试类型视图。

6.4 配置步骤

创建 DNS 类型的 NQA 测试组。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type dns
```

配置 DNS 服务器的 IP 地址为 10.2.2.2，要解析的域名为 host.com。

```
[DeviceA-nqa-admin-test-dns] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-dns] resolve-target host.com
```

开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test-dns] history-record enable
[DeviceA-nqa-admin-test-dns] quit
```

6.5 验证配置

启动 DNS 测试方案进行测试。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

测试执行一段时间后，停止 DNS 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

以上配置完成后，显示 DNS 测试中最后一次测试的结果。

```
[DeviceA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 62/62/62
      Square-Sum of round trip time: 3844
      Last succeeded probe time: 2017-03-24 10:49:37.3
    Extended results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
```

显示 DNS 测试的历史记录。

```
[DeviceA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          62           Succeeded        2017-03-24 10:49:37.3
```

以上显示信息表示，Device A 可以通过指定的 DNS 服务器将域名 host.com 解析为 IP 地址，域名解析所需的时间为 62 毫秒。

6.6 配置文件

```
#
nqa entry admin test
 type dns
  destination ip 10.2.2.2
  history-record enable
```

```
  resolve-target host.com
#
```

7 FTP 测试典型配置指导

7.1 组网需求

当前网络如图 4 所示，登录 FTP 服务器的用户名为 admin，密码为 systemtest，现要求配置 FTP 测试方案，使用户可以根据实际需要随时调用该测试方案测试 Device A 是否可以与指定的 FTP 服务器 Device B 建立连接，以及与 FTP 服务器之间传送文件的时间，从而判断 FTP 服务器的连通性及性能。

图4 FTP 测试组网图

7.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

7.3 配置注意事项

- 进行 NQA 测试之前，请确保各设备之间路由可达。
- 测试组开始测试后就不能再进入该测试组视图和测试类型视图进行配置修改，测试结束后才可以进入该测试组视图和测试类型视图。
- 进行 **put** 操作时，通过 **filename** 命令指定的文件在 NQA 客户端对应存储介质中必须存在，否则将导致测试失败。
- 进行 FTP 测试时，建议选用较小的测试文件并将 NQA 探测超时时间调大，如果测试文件太大或探测超时时间太小，可能会导致探测超时。

7.4 配置步骤

创建 FTP 类型的 NQA 测试组。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type ftp
```

配置测试操作的目的地址为 FTP 服务器的 IP 地址 10.2.2.2。

```
[DeviceA-nqa-admin-test-ftp] url ftp://10.2.2.2
```

配置探测报文的源 IP 地址为 10.1.1.1。

```
[DeviceA-nqa-admin-test-ftp] source ip 10.1.1.1
```

配置 FTP 操作类型。

```
[DeviceA-nqa-admin-test-ftp] operation put
```

配置客户端传送文件的文件名。

```
[DeviceA-nqa-admin-test-ftp] filename config.txt
```

配置登录 FTP 服务器的用户名和密码。

```
[DeviceA-nqa-admin-test-ftp] username admin
[DeviceA-nqa-admin-test-ftp] password simple systemtest
```

开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test-ftp] history-record enable
[DeviceA-nqa-admin-test-ftp] quit
```

7.5 验证配置

启动 FTP 测试方案进行测试。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

测试执行一段时间后，停止 FTP 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

以上配置完成后，显示 FTP 测试中最后一次测试的结果。

```
[DeviceA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 173/173/173
      Square-Sum of round trip time: 29929
      Last succeeded probe time: 2017-03-25 10:07:28.6
    Extend results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
```

显示 FTP 测试的历史记录。

```
[DeviceA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1           173          Succeeded        2017-03-25 10:07:28.6
```

以上显示信息表示，Device A 可以和指定的 FTP 服务器 Device B 建立连接，向 FTP 服务器上传一个文件的时间是 173 毫秒。

7.6 配置文件

```
#
nqa entry admin test
 type ftp
  filename config.txt
  history-record enable
```

```
  operation put
  password cipher $c$3$BP255atzDilAfIPwfh+RMHqmP5LTiKWpVf/hpBs=
  source ip 10.1.1.1
  url ftp://10.2.2.2
  username admin
#
```

8 HTTP 测试典型配置指导

8.1 组网需求

当前网络如图 5 所示，现要求配置 HTTP 测试方案，使用户可以根据实际需要随时调用该测试方案测试 Device A 是否可以与指定的 HTTP 服务器建立连接，以及访问 HTTP 服务器网页 index.htm 所需的时间，从而判断 HTTP 服务器的连通性及性能。

图5 HTTP 测试组网图

8.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

8.3 配置注意事项

- 进行 NQA 测试之前，请确保各设备之间路由可达。
- 测试组开始测试后就不能再进入该测试组视图和测试类型视图进行配置修改，测试结束后才可以进入该测试组视图和测试类型视图。

8.4 配置步骤

创建 HTTP 类型的 NQA 测试组。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type http
```

配置 HTTP 测试服务器的 IP 地址为 10.2.2.2，访问的网址为/index.htm。

```
[DeviceA-nqa-admin-test-http] url http://10.2.2.2/index.htm
```

开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test-http] history-record enable
[DeviceA-nqa-admin-test-http] quit
```

至此，已完成 HTTP 测试方案配置。

8.5 验证配置

启动 HTTP 测试方案进行测试。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

测试执行一段时间后，停止 HTTP 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

以上配置完成后，显示 HTTP 测试中一次测试的结果。

```
[DeviceA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 64/64/64
      Square-Sum of round trip time: 4096
      Last succeeded probe time: 2017-03-25 11:12:47.9
    Extend results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
```

显示 HTTP 测试的历史记录。

```
[DeviceA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          64           Succeeded        2017-03-25 11:12:47.9
```

以上显示信息表示，Device A 可以和指定的 HTTP 服务器 Device B 建立连接，从 HTTP 服务器获取数据的时间为 64 毫秒。

8.6 配置文件

```
#
nqa entry admin test
 type http
  history-record enable
  url http://10.2.2.2/index.htm
#
```

9 相关资料

- H3C SR6600 SR6600-X 路由器 网络管理和监控配置指导-R0106
- H3C SR6600 SR6600-X 路由器 网络管理和监控命令参考-R0106

H3C SR6600/SR6600-X 系列路由器

NTP 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 0
2 配置前提 0
3 NTP 服务器/客户端模式典型配置举例 0
3.1 组网需求 0
3.2 使用版本 0
3.3 配置步骤 1
3.3.1 Device A 的配置 1
3.3.2 Device B 的配置 1
3.3.3 Device C 的配置 1
3.4 验证配置 1
3.5 配置文件 2
4 NTP 广播模式典型配置举例 2
4.1 组网需求 2
4.2 使用版本 3
4.3 配置步骤 3
4.3.1 Device A 的配置 3
4.3.2 Device B 的配置 3
4.4 验证配置 4
4.5 配置文件 4
5 NTP 组播模式典型配置举例 5
5.1 组网需求 5
5.2 使用版本 5
5.3 配置步骤 5
5.3.1 Device C 的配置 5
5.3.2 Device D 的配置 6
5.3.3 Device B 的配置 6
5.3.4 Device A 的配置 6
5.4 验证配置 7
5.5 配置文件 7
6 带身份验证的 NTP 客户端/服务器模式典型配置举例 8
6.1 组网需求 8
6.2 使用版本 9

6.3 配置步骤 9
6.3.1 Device A 的配置 9
6.3.2 Device B 的配置 9
6.3.3 Device C 的配置 9
6.4 验证配置 10
6.5 配置文件 10
7 SNTP 典型配置举例 11
7.1 组网需求 11
7.2 使用版本 12
7.3 配置步骤 12
7.3.1 Device A 的配置 12
7.3.2 Device B 的配置 12
7.3.3 Device C 的配置 12
7.4 验证配置 13
7.5 配置文件 13
8 相关资料 13

1 简介

本章介绍了与 NTP 有关的各种典型配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

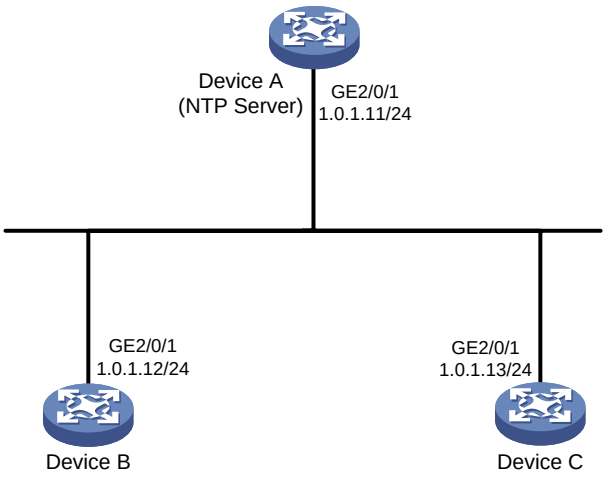
本文档假设您已了解 NTP 特性。

3 NTP 服务器/客户端模式典型配置举例

3.1 组网需求

如图 1 所示，网络中有一台时间服务器 Device A，为网络中的其它设备提供精确的时间服务，为保证网络中的所有设备能保持一致、统一的时钟，现要求配置 NTP 服务器/客户端模式，使所有设备能从时间服务器 Device A 上获得时钟同步。

图1 配置 NTP 服务器/客户端模式组网图



3.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.3 配置步骤

3.3.1 Device A 的配置

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 1.0.1.11 24
[DeviceA-GigabitEthernet2/0/1] quit
```

开启 NTP 功能。

```
[DeviceA] ntp-service enable
```

设置本地时钟作为参考时钟，层数为 2。

```
[DeviceA] ntp-service refclock-master 2
```

3.3.2 Device B 的配置

配置接口的 IP 地址，配置步骤这里省略。

开启 NTP 功能。

```
<DeviceB> system-view
[DeviceB] ntp-service enable
```

设置 NTP Server 为 Device B 的时间服务器。

```
[DeviceB] ntp-service unicast-server 1.0.1.11
```

3.3.3 Device C 的配置

配置接口的 IP 地址，配置步骤这里省略。

开启 NTP 功能。

```
<DeviceC> system-view
[DeviceC] ntp-service enable
```

设置 NTP Server 为 Device C 的时间服务器。

```
[DeviceC] ntp-service unicast-server 1.0.1.11
```

3.4 验证配置

以上配置完成后，Device B 和 Device C 向 Device A 进行时间同步。以 Device B 为例，查看 NTP 的运行状态。

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 1.0.1.11
 Local mode: client
 Reference clock ID: 1.0.1.11
 Leap indicator: 00
 Clock jitter: 0.003479 s
 Stability: 0.000 pps
 Clock precision: 2^-16
```

```
 Root delay: 1.95313 ms
 Root dispersion: 28.38135 ms
 Reference time: d5ed8cd5.577006ea  Wed, Sep 25 2017 16:24:53.341
```

此时 Device B 已经与 Device A 同步，层数比 Device A 的层数大 1，为 3。

查看 Device B 的 NTP 会话信息，可以看到 Device B 与 Device A 建立了连接。

```
[DeviceB] display ntp-service sessions
        source          reference       stra reach poll  now offset  delay disper
********************************************************************************
[12345]1.0.1.11        127.127.1.0        2   255   64   38 -10.22 1.9531 3.3416
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

3.5 配置文件

- Device A：

```
#
interface GigabitEthernet2/0/1
 ip address 1.0.1.11 255.255.255.0
#
 ntp-service enable
 ntp-service refclock-master 2
#
```

- Device B：

```
#
interface GigabitEthernet2/0/1
 ip address 1.0.1.12 255.255.255.0
#
 ntp-service enable
 ntp-service unicast-server 1.0.1.11
#
```

- Device C：

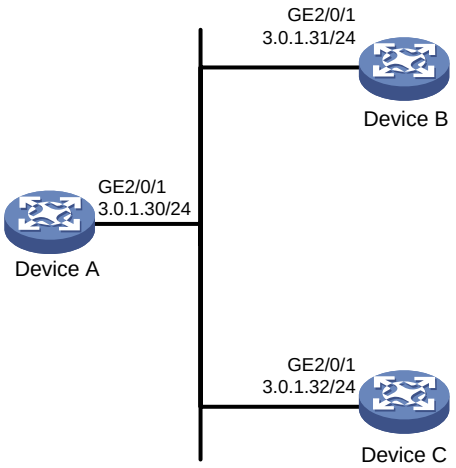
```
#
interface GigabitEthernet2/0/1
 ip address 1.0.1.13 255.255.255.0
#
 ntp-service enable
 ntp-service unicast-server 1.0.1.11
#
```

4 NTP 广播模式典型配置举例

4.1 组网需求

如图 2 所示，网络中设备较多，所有设备都位于同一个网段（3.0.1.0/24）中，为了便于管理，现要求通过配置 NTP 广播模式，使网络中的设备拥有一致，统一的时间。

图2 NTP 广播模式配置组网图



4.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.3 配置步骤

4.3.1 Device A 的配置

开启 NTP 功能。

```
<DeviceA> system-view
[DeviceA] ntp-service enable
```

设置本地时钟作为参考时钟，层数为 2。

```
[DeviceA] ntp-service refclock-master 2
```

配置接口的 IP 地址。

```
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 3.0.1.30 24
```

配置 Device A 为广播服务器，向网络中发送 NTP 广播报文。

```
[DeviceA-GigabitEthernet2/0/1] ntp-service broadcast-server
[DeviceA-GigabitEthernet2/0/1] quit
```

4.3.2 Device B 的配置

配置接口的 IP 地址，配置步骤这里省略。

开启 NTP 功能。

```
<DeviceB> system-view
[DeviceB] ntp-service enable
```

设置为广播客户端，从 GigabitEthernet2/0/1 监听广播消息。

```
[DeviceB] interface gigabitethernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] ntp-service broadcast-client
```

说明

Device C 的配置与 Device B 相同，此处不再赘述。

4.4 验证配置

以 Device B 为例，查看 NTP 的运行状态。

```
[DeviceA-GigabitEthernet2/0/1] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3.0.1.30
 Local mode: bclient
 Reference clock ID: 3.0.1.30
 Leap indicator: 00
 Clock jitter: 0.000061 s
 Stability: 0.000 pps
 Clock precision: 2^-16
 Root delay: 0.00000 ms
 Root dispersion: 7951.43127 ms
 Reference time: d5ee8d88.2faabed0  Thu, Sep 26 2017 10:40:08.186
```

此时 Device B 已经与 Device A 同步，层数比 Device A 的层数大 1，为 3。

查看 Device B 的 NTP 会话信息，可以看到 Device B 与 Device A 建立了连接。

```
[DeviceA-GigabitEthernet2/0/1] display ntp-service sessions
      source          reference       stra reach poll  now offset  delay disper
**************************************************************************
 [1234]3.0.1.30        127.127.1.0        2   254   64   82 -2.190 0.0000 7937.5
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

4.5 配置文件

- Device A：

```
#
interface GigabitEthernet2/0/1
 ip address 3.0.1.30 255.255.255.0
 ntp-service broadcast-server
#
 ntp-service enable
 ntp-service refclock-master 2
#
```

- Device B：

```
#
interface GigabitEthernet2/0/1
 ip address 3.0.1.31 255.255.255.0
 ntp-service broadcast-client
```

```
#
 ntp-service enable
#
```

- Device C：

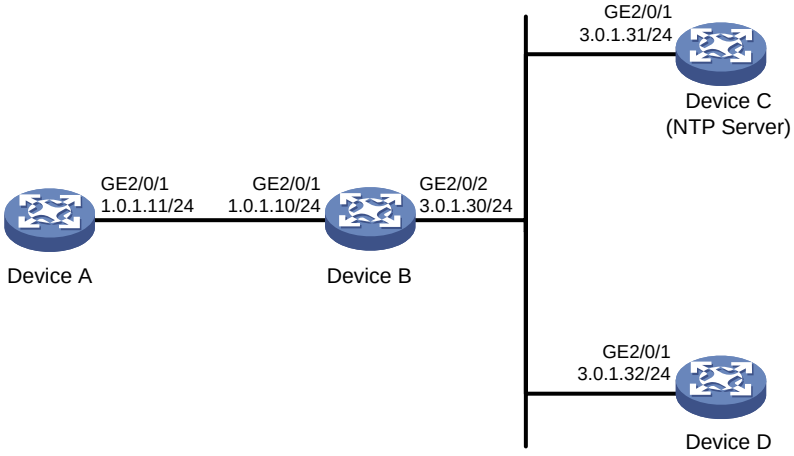
```
#
interface GigabitEthernet2/0/1
 ip address 3.0.1.32 255.255.255.0
 ntp-service broadcast-client
#
 ntp-service enable
#
```

5 NTP 组播模式典型配置举例

5.1 组网需求

如图 3 所示，网络中有一台时间服务器 Device C，网络中设备较多，而且这些设备分布在不同网段中，为了便于管理，现要求配置 NTP 组播模式，使网络中的设备拥有统一，一致的时间。

图3 配置 NTP 组播模式组网图



5.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

5.3 配置步骤

5.3.1 Device C 的配置

开启 NTP 功能。

```
<DeviceC> system-view
[DeviceC] ntp-service enable
```

设置本地时钟作为参考时钟，层数为 2。

```
[DeviceC] ntp-service refclock-master 2
```
配置接口 GigabitEthernet2/0/1 的 IP 地址。
```
[DeviceC] interface gigabitethernet 2/0/1
[DeviceC-GigabitEthernet2/0/1] ip address 3.0.1.31 24
```
设置 Device C 为组播服务器，从接口 GigabitEthernet2/0/1 发送组播报文。
```
[DeviceC-GigabitEthernet2/0/1] ntp-service multicast-server
```

5.3.2 Device D 的配置

开启 NTP 功能。
```
<DeviceD> system-view
[DeviceD] ntp-service enable
```
配置接口 GigabitEthernet2/0/1 的 IP 地址。
```
[DeviceD] interface gigabitethernet 2/0/1
[DeviceD-GigabitEthernet2/0/1] ip address 3.0.1.32 24
```
设置 Device D 为组播客户端，从接口 GigabitEthernet2/0/1 监听组播报文。
```
[DeviceD-GigabitEthernet2/0/1] ntp-service multicast-client
```

5.3.3 Device B 的配置

配置接口的 IP 地址，配置步骤这里省略。

开启 NTP 功能。
```
<DeviceB> system-view
[DeviceB] ntp-service enable
```
设置 Device B 为组播客户端，从接口 GigabitEthernet2/0/2 监听组播报文。
```
[DeviceB] interface gigabitethernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] ntp-service multicast-client
[DeviceB-GigabitEthernet2/0/2] quit
```
由于 Device A 与 Device C 不在同一网段，所以 Device B 上需要配置组播功能，否则 Device A 收不到 Device C 发出的组播报文。

配置组播功能。
```
[DeviceB] multicast routing
[DeviceB] interface gigabitethernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] pim dm
[DeviceB-GigabitEthernet2/0/2] quit
[DeviceB] interface gigabitethernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] ip address 1.0.1.10 24
[DeviceB-GigabitEthernet2/0/1] igmp enable
[DeviceB-GigabitEthernet2/0/1] igmp static-group 224.0.1.1
[DeviceB-GigabitEthernet2/0/1] quit
```

5.3.4 Device A 的配置

开启 NTP 功能。
```
<DeviceA> system-view
[DeviceA] ntp-service enable
```

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 1.0.1.11 24
```

设置 Device A 为组播客户端，从接口 GigabitEthernet2/0/1 监听组播报文。

```
[DeviceA-GigabitEthernet2/0/1] ntp-service multicast-client
```

5.4 验证配置

以 Device A 为例，查看 NTP 的运行状态。

```
[DeviceA-GigabitEthernet2/0/1] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3.0.1.31
 Local mode: bclient
 Reference clock ID: 3.0.1.31
 Leap indicator: 00
 Clock jitter: 0.000061 s
 Stability: 0.000 pps
 Clock precision: 2^-16
 Root delay: 1.69373 ms
 Root dispersion: 1950.18005 ms
 Reference time: d5ee9b15.2f3a684d  Thu, Sep 26 2017 11:37:57.184
```

此时 Device A 已经与 Device C 同步，层数比 Device C 的层数大 1，为 3。

5.5 配置文件

- Device A：

```
#
 ntp-service enable
#
interface  GigabitEthernet2/0/1
 ip address 1.0.1.11 255.255.255.0
 ntp-service multicast-client
#
```

- Device B：

```
#
ntp-service enable
#
multicast routing
#
interface GigabitEthernet2/0/2
 ip address 3.0.1.30 255.255.255.0
 pim dm
 ntp-service multicast-client
#
interface GigabitEthernet2/0/1
 ip address 1.0.1.10 255.255.255.0
```

```
 igmp enable
 igmp static-group 224.0.1.1
#
```

- Device C：

```
#
 ntp-service enable
ntp-service refclock-master 2
#
interface GigabitEthernet2/0/1
 ip address 3.0.1.31 255.255.255.0
 ntp-service multicast-server
#
```

- Device D：

```
#
 ntp-service enable
#
interface GigabitEthernet2/0/1
 ip address 3.0.1.32 255.255.255.0
 ntp-service multicast-client
#
```

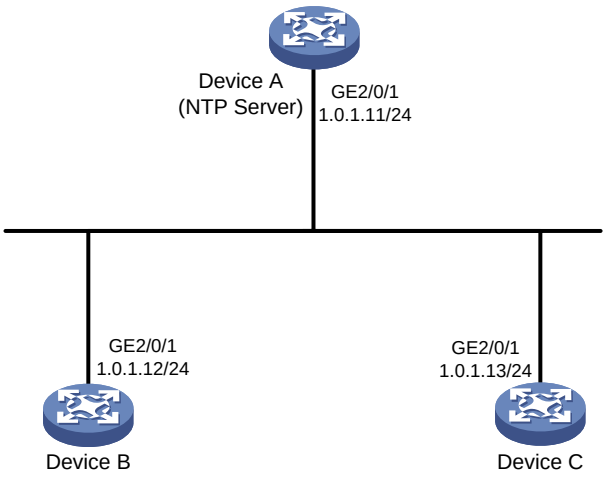
6 带身份验证的 NTP 客户端/服务器模式典型配置举例

6.1 组网需求

网络中有一台时间服务器 Device A，为网络中的其它设备提供精确的时间服务，为保证网络中的所有设备能保持一致、统一的时钟，现要求：

- 配置 NTP 服务器/客户端模式，使所有设备能从时间服务器 Device A 上获得时钟同步。
- 设备在获得时钟同步前，需要通过 Device A 的 NTP 验证。

图4 带身份验证的 NTP 客户端/服务器模式典型配置举例组网图



6.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

6.3 配置步骤

6.3.1 Device A 的配置

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 1.0.1.11 24
[DeviceA-GigabitEthernet2/0/1] quit
```

开启 NTP 服务。

```
[DeviceA] ntp-service enable
```

设置本地时钟作为参考时钟，层数为 2。

```
[DeviceA] ntp-service refclock-master 2
```

在 Device A 上启动 NTP 验证功能。

```
[DeviceA] ntp-service authentication enable
```

创建编号为 42 的 NTP 验证密钥，密钥值为 aNiceKey，以明文形式输入。

```
[DeviceA] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
```

配置编号为 42 的密钥为可信密钥。

```
[DeviceA] ntp-service reliable authentication-keyid 42
```

6.3.2 Device B 的配置

配置接口的 IP 地址，配置步骤这里省略。

开启 NTP 服务。

```
<DeviceB> system-view
[DeviceB] ntp-service enable
```

在 Device B 上启动 NTP 验证功能。

```
[DeviceB] ntp-service authentication enable
```

创建编号为 42 的 NTP 验证密钥，密钥值为 aNiceKey，以明文形式输入。

```
[DeviceB] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
```

配置编号为 42 的密钥为可信密钥。

```
[DeviceB] ntp-service reliable authentication-keyid 42
```

设置 Device A 为 Device B 的 NTP 服务器，并将该服务器与编号为 42 的密钥关联。

```
[DeviceB] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

以上配置将使得 Device B 与 Device A 进行时间同步。

6.3.3 Device C 的配置

配置接口的 IP 地址，配置步骤这里省略。

开启 NTP 服务。

```
<DeviceC> system-view
[DeviceC] ntp-service enable
```
在 Device C 上启动 NTP 验证功能。
```
[DeviceC] ntp-service authentication enable
```
创建编号为 42 的 NTP 验证密钥，密钥值为 aNiceKey，以明文形式输入。
```
[DeviceC] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
```
配置编号为 42 的密钥为可信密钥。
```
[DeviceC] ntp-service reliable authentication-keyid 42
```
设置 Device A 为 Device C 的 NTP 服务器，并将该服务器与编号为 42 的密钥关联。
```
[DeviceC] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```
以上配置将使得 Device C 与 Device A 进行时间同步。

6.4 验证配置

完成上述配置后，Device B、DeviceC 可以与 Device A 的时间同步。同步后查看 Device B 的状态。可以看出，Device B 已经与 Device A 同步，层数比 Device A 的层数大 1，为 3。
```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 1.0.1.11
 Local mode: client
 Reference clock ID: 1.0.1.11
 Leap indicator: 00
 Clock jitter: 0.005096 s
 Stability: 0.000 pps
 Clock precision: 2^-16
 Root delay: 0.00655 ms
 Root dispersion: 1.15869 ms
 Reference time: d0c62687.ab1bba7d  Mon, Sep 30 2017 16:06:26.764
```
查看 Device B 的 NTP 服务的所有 IPv4 会话信息，可以看到 Device B 与 Device A 建立了会话。
```
[DeviceB] display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**************************************************************************
 [1245]1.0.1.11        127.127.1.0        2     1   64  519   -0.0 0.0065    0.0
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions : 1
```

6.5 配置文件

- Device A：

```
#
interface GigabitEthernet2/0/1
 ip address 1.0.1.11 255.255.255.0
#
 ntp-service enable
 ntp-service authentication enable
```

```
 ntp-service authentication-keyid 42 authentication-mode md5 cipher
$c$3$4j3SKCgQWBK3Un41B9U0JXzJX9i7IuNoSqi
 ntp-service reliable authentication-keyid 42
 ntp-service refclock-master 2
#
```

- Device B：

```
#
interface GigabitEthernet2/0/1
 ip address 1.0.1.12 255.255.255.0
#
 ntp-service enable
 ntp-service authentication enable
 ntp-service authentication-keyid 42 authentication-mode md5 cipher
$c$3$22eIc8l796cpudZqiaAZ2SLzIfrgzFTVYn8X
 ntp-service reliable authentication-keyid 42
 ntp-service unicast-server 1.0.1.11 authentication-keyid 42
#
```

- Device C：

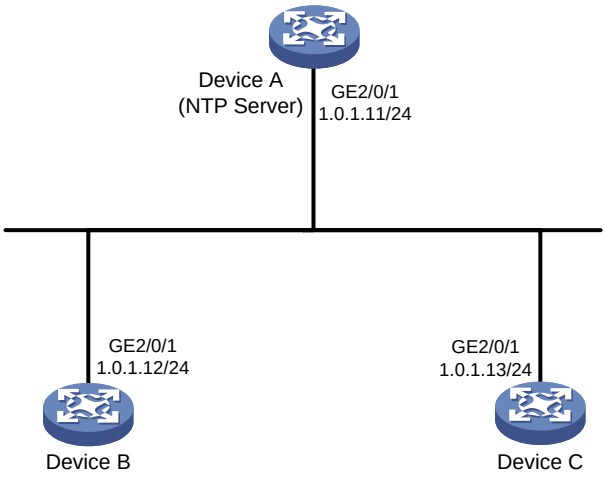
```
#
interface GigabitEthernet2/0/1
 ip address 1.0.1.13 255.255.255.0
#
 ntp-service enable
 ntp-service authentication enable
 ntp-service authentication-keyid 42 authentication-mode md5 cipher
$c$3$XJzVmJ1TJbWyYAXpPXxF7JiEOZag8CehibM8
 ntp-service reliable authentication-keyid 42
 ntp-service unicast-server 1.0.1.11 authentication-keyid 42
#
```

7 SNTP 典型配置举例

7.1 组网需求

如图 5 所示，网络中有一台时间服务器 Device A，为网络中的其它网络设备提供精确的时间服务，为保证网络中的所有设备能保持一致、统一的时钟，现要求配置所有网络设备为 SNTP 客户端，使所有设备能从时间服务器 Device A 上获得时钟同步。

图5 SNTP 典型配置举例组网图



7.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

7.3 配置步骤

7.3.1 Device A 的配置

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1 ip address 1.0.1.11 24
```

开启 NTP 功能。

```
[DeviceA] ntp-service enable
```

设置本地时钟作为参考时钟，层数为 2。

```
[DeviceA] ntp-service refclock-master 2
```

7.3.2 Device B 的配置

配置接口的 IP 地址，配置步骤这里省略。

开启 SNTP 功能。

```
<DeviceB> system-view
[DeviceB] sntp enable
```

设置 Device A 为 Device B 的时间服务器。

```
[DeviceB] sntp unicast-server 1.0.1.11
```

7.3.3 Device C 的配置

配置接口的 IP 地址，配置步骤这里省略。

开启 SNTP 功能。

```
<DeviceC> system-view
[DeviceC] sntp enable
```

设置 Device A 为 Device C 的时间服务器。

```
[DeviceC] sntp unicast-server 1.0.1.11
```

7.4 验证配置

以上配置完成后，Device B 和 Device C 向 Device A 进行时间同步。以 Device B 为例，查看 Device B 的 NTP 会话信息，可以看到 Device B 与 Device A 建立了连接。

```
[DeviceB] display sntp sessions
SNTP server     Stratum   Version    Last receive time
1.0.1.11        2         4          Thu, Sep 26 2017 17:25:09.121 (Synced)
```

7.5 配置文件

- Device A：

```
#
interface GigabitEthernet2/0/1
 ip address 1.0.1.11 255.255.255.0
#
 ntp-service enable
 ntp-service refclock-master 2
#
```

- Device B：

```
#
interface GigabitEthernet2/0/1
 ip address 1.0.1.12 255.255.255.0
#
 sntp enable
 sntp unicast-server 1.0.1.11
#
```

- Device C：

```
#
interface GigabitEthernet2/0/1
 ip address 1.0.1.13 255.255.255.0
#
 sntp enable
 sntp unicast-server 1.0.1.11
#
```

8 相关资料

- H3C SR6600 SR6600-X 路由器 网络管理和监控配置指导-R0106
- H3C SR6600 SR6600-X 路由器 网络管理和监控命令参考-R0106

H3C SR6600/SR6600-X 系列路由器

OSPF 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介……1
2 配置前提……1
3 OSPF 路由信息过滤配置举例……1
3.1 组网需求……1
3.2 使用版本……2
3.3 配置注意事项……2
3.4 配置步骤……2
3.4.1 配置各接口的 IP 地址……2
3.4.2 配置 OSPF 网络的基本功能……2
3.4.3 配置 RIP 网络的基本功能……3
3.4.4 将 RIP 路由和 OSPF 路由互相引入……4
3.4.5 配置 OSPF 的路由过滤功能……5
3.5 验证配置……5
3.6 配置文件……8
4 相关资料……10

1 简介

本文档介绍了 OSPF 路由信息过滤的配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 OSPF 路由信息过滤的特性。

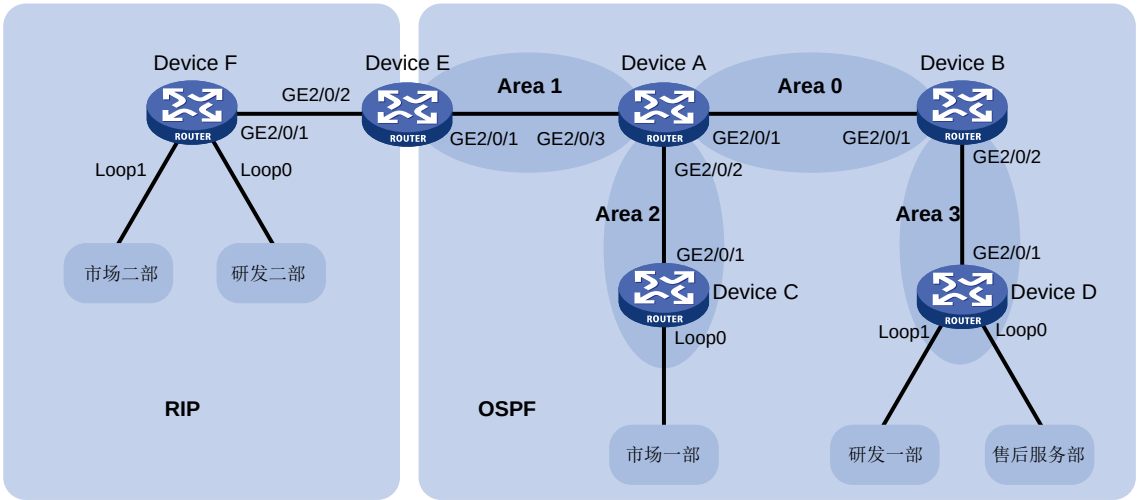
3 OSPF 路由信息过滤配置举例

3.1 组网需求

如图 1 所示，公司 A 使用 OSPF 路由协议实现公司设备全网互通，后来公司 A 扩张兼并了公司 B，要求将公司 B 采用的 RIP 路由协议与公司 A 的 OSPF 协议互相引入，使得各个部门可以实现互通。Device A 和 Device B 作为公司核心设备负责各个部门间的通信。由于业务需要，现要求通过下列措施控制并调整网络中的路由信息：

- 在 Device E 上对引入的路由信息进行过滤，使得研发二部所在网段无法被引入到 OSPF 内。
- 在 Device C 上使用路由信息的过滤功能，使得市场一部所在网段无法访问研发一部。
- 在 Device D 上使用路由信息的过滤功能，使得研发一部和售后服务部所在网段无法访问市场二部。

图1 OSPF 路由信息过滤组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	GE2/0/1	10.1.1.1/24	Device B	GE2/0/1	10.1.1.2/24
	GE2/0/2	10.2.1.1/24		GE2/0/2	10.3.1.1/24

设备	接口	IP地址	设备	接口	IP地址
	GE2/0/3	10.4.1.1/24			
Device C	GE2/0/1	10.2.1.2/24	Device D	GE2/0/1	10.3.1.2/24
	Loop0	192.168.3.1/24 （市场一部所在网段）		Loop0	192.168.1.1/24 （售后服务部所在网段）
				Loop1	192.168.2.1/24 （研发一部所在网段）
Device E	GE2/0/1	10.4.1.2/24	Device F	GE2/0/1	10.5.1.2/24
	GE2/0/2	10.5.1.1/24		Loop0	192.168.4.1/24 （研发二部所在网段）
				Loop1	192.168.5.1/24 （市场二部所在网段）

3.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.3 配置注意事项

- 路由信息过滤功能中对于引入外部路由信息时采用 **export** 关键字进行过滤，该参数只能在 ASBR 上生效。
- 路由信息过滤功能只是对路由表中相关路由信息过滤，并不是过滤掉 OSPF 中通告的 LSA。
- 由于路由通信是双向的，使用路由信息过滤功能将某一目的网段过滤后，该路由器下联的其它网段无法访问这个目的网段的设备，这个目的网段的设备也不能访问源地址网段的设备。
- 使用路由信息过滤功能配合 ACL 使用时，必须将最后一条规则设置为允许所有源地址通过才能避免将所有网段路由全部过滤掉。

3.4 配置步骤

3.4.1 配置各接口的 IP 地址

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface GigabitEthernet 2/0/1
[Device A-GigabitEthernet2/0/1] ip address 10.1.1.1 24
```

请参考以上方法配置其它相关接口的 IP 地址，配置步骤这里省略。

3.4.2 配置 OSPF 网络的基本功能

在 Device A 上使能指定网段的 OSPF 路由功能。

```
<DeviceA> system-view
[DeviceA] ospf
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] area 2
[DeviceA-ospf-1-area-0.0.0.2] network 10.2.1.0 0.0.0.255
```

```
[DeviceA-ospf-1-area-0.0.0.2] quit
[DeviceA-ospf-1] area 1
[DeviceA-ospf-1-area-0.0.0.1] network 10.4.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.1] quit
[DeviceA-ospf-1] quit
```

在 Device B 上使能指定网段的 OSPF 路由功能。

```
<DeviceB> system-view
[DeviceB] ospf
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] area 3
[DeviceB-ospf-1-area-0.0.0.3] network 10.3.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.3] quit
[DeviceB-ospf-1] quit
```

在 Device C 上使能指定网段的 OSPF 路由功能。

```
<DeviceC> system-view
[DeviceC] ospf
[DeviceC-ospf-1] area 2
[DeviceC-ospf-1-area-0.0.0.2] network 10.2.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.2] network 192.168.3.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.2] quit
[DeviceC-ospf-1] quit
```

在 Device D 上使能指定网段的 OSPF 路由功能。

```
<DeviceD> system-view
[DeviceD] ospf
[DeviceD-ospf-1] area 3
[DeviceD-ospf-1-area-0.0.0.3] network 10.3.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.3] network 192.168.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.3] network 192.168.2.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.3] quit
[DeviceD-ospf-1] quit
```

在 Device E 上使能指定网段的 OSPF 路由功能。

```
<DeviceE> system-view
[DeviceE] ospf
[DeviceE-ospf-1] area 1
[DeviceE-ospf-1-area-0.0.0.1] network 10.4.1.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.1] quit
[DeviceE-ospf-1] quit
```

3.4.3 配置 RIP 网络的基本功能

在 Device E 上使能指定网段的 RIP 功能。

```
<DeviceE> system-view
[DeviceE] rip
[DeviceE-rip-1] version 2
[DeviceE-rip-1] undo summary
```

```
[DeviceE-rip-1] network 10.5.1.0 0.0.0.255
[DeviceE-rip-1] quit
```

在 Device F 上使能指定网段的 RIP 功能。

```
<DeviceF> system-view
[DeviceF] rip
[DeviceF-rip-1] version 2
[DeviceF-rip-1] undo summary
[DeviceF-rip-1] network 10.5.1.0 0.0.0.255
[DeviceF-rip-1] network 192.168.4.0 0.0.0.255
[DeviceF-rip-1] network 192.168.5.0 0.0.0.255
[DeviceF-rip-1] quit
```

3.4.4 将 RIP 路由和 OSPF 路由互相引入

在 Device E 上将直连路由和 OSPF 路由引入到 RIP 网络中。

```
<DeviceE> system-view
[DeviceE] rip
[DeviceE-rip-1] import-route direct
[DeviceE-rip-1] import-route ospf
[DeviceE-rip-1] quit
```

在 Device E 上将直连路由和 RIP 路由引入到 OSPF 网络中。

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

查看 Device E 的路由表信息。

```
[Device E]display ip routing-table

Destinations : 24        Routes : 24

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         O_INTER 10   2            10.4.1.1        GE2/0/1
10.2.1.0/24         O_INTER 10   2            10.4.1.1        GE2/0/1
10.3.1.0/24         O_INTER 10   3            10.4.1.1        GE2/0/1
10.4.1.0/24         O_INTER 0    0            10.4.1.2        GE2/0/1
10.4.1.0/32         Direct  0    0            10.4.1.2        GE2/0/1
10.4.1.2/32         Direct  0    0            127.0.0.1       InLoop0
10.4.1.255/32       Direct  0    0            10.4.1.2        GE2/0/1
10.5.1.0/24         Direct  0    0            10.5.1.1        GE2/0/2
10.5.1.0/32         Direct  0    0            10.5.1.1        GE2/0/2
10.5.1.1/32         Direct  0    0            127.0.0.1       InLoop0
10.5.1.255/32       Direct  0    0            10.5.1.1        GE2/0/2
127.0.0.0/8         Direct  0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct  0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct  0    0            127.0.0.1       InLoop0
192.168.1.1/32      O_INTER 10   3            10.4.1.1        GE2/0/1
```

```
192.168.2.1/32      O_INTER 10   3            10.4.1.1        GE2/0/1
192.168.3.1/32      O_INTER 10   2            10.4.1.1        GE2/0/1
192.168.4.0/24      RIP     100  1            10.5.1.2        GE2/0/2
192.168.5.0/24      RIP     100  1            10.5.1.2        GE2/0/2
224.0.0.0/4         Direct  0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct  0    0            0.0.0.0         NULL0
255.255.255.255/32 Direct  0    0            127.0.0.1       InLoop0
```

以上显示信息表明 Device E 拥有路由域内所有网段路由，然后依次查看其他所有设备的路由表信息，路由域内所有的网段均可互通。

3.4.5 配置 OSPF 的路由过滤功能

在 Device C 上创建基本 ACL 并匹配需要拒绝访问的目的网段 192.168.2.0/24。

```
<DeviceC> system-view
[DeviceC] acl basic 2000
[DeviceC-acl-ipv4-basic-2000] rule 0 deny source 192.168.2.0 0.0.0.255
[DeviceC-acl-ipv4-basic-2000] rule permit source any
[DeviceC-acl-ipv4-basic-2000] quit
```

在 Device C 上通过指定访问控制列表 ACL 2000 来对要加入到路由表的路由信息进行过滤。

```
[DeviceC] ospf
[DeviceC-ospf-1] filter-policy 2000 import
[DeviceC-ospf-1] quit
```

在 Device D 上创建基本 ACL 并匹配需要拒绝访问的目的网段 192.168.5.0/24。

```
<DeviceD> system-view
[DeviceD] acl basic 2000
[DeviceD-acl-ipv4-basic-2000] rule 0 deny source 192.168.5.0 0.0.0.255
[DeviceD-acl-ipv4-basic-2000] rule permit source any
[DeviceD-acl-ipv4-basic-2000] quit
```

在 Device D 上通过指定访问控制列表 ACL 2000 来对要加入到路由表的路由信息进行过滤。

```
[DeviceD] ospf
[DeviceD-ospf-1] filter-policy 2000 import
[DeviceD-ospf-1] quit
```

在 Device E 上创建基本 ACL 并匹配需要拒绝访问的目的网段 192.168.4.0/24。

```
<DeviceE> system-view
[DeviceE] acl basic 2000
[DeviceE-acl-ipv4-basic-2000] rule 0 deny source 192.168.4.0 0.0.0.255
[DeviceE-acl-ipv4-basic-2000] rule permit source any
[DeviceE-acl-ipv4-basic-2000] quit
```

在 Device E 上通过指定访问控制列表 ACL 2000 来对引入 OSPF 的 RIP 路由信息进行过滤。

```
[DeviceE] ospf
[DeviceE-ospf-1] filter-policy 2000 export rip 1
[DeviceE-ospf-1] quit
```

3.5 验证配置

查看 Device C 的路由表信息。

```
[DeviceC] display ip routing-table

Destinations : 22        Routes : 22

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         O_INTER 10  2           10.2.1.1        GE2/0/1
10.2.1.0/24         Direct  0   0           10.2.1.2        GE2/0/1
10.2.1.0/32         Direct  0   0           10.2.1.2        GE2/0/1
10.2.1.2/32         Direct  0   0           127.0.0.1       GE2/0/1
10.2.1.255/32       Direct  0   0           10.2.1.2        GE2/0/1
10.3.1.0/24         O_INTER 10  3           10.2.1.1        GE2/0/1
10.4.1.0/24         O_INTER 10  2           10.2.1.1        GE2/0/1
10.5.1.0/24         O_ASE2  150 1           10.2.1.1        GE2/0/1
127.0.0.0/8         Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
192.168.1.1/32      O_INTER 10  3           10.2.1.1        GE2/0/1
192.168.3.0/24      Direct  0   0           192.168.3.1     Loop0
192.168.3.0/32      Direct  0   0           192.168.3.1     Loop0
192.168.3.1/32      Direct  0   0           127.0.0.1       InLoop0
192.168.3.255/32    Direct  0   0           192.168.3.1     Loop0
192.168.5.0/24      O_ASE2  150 1           10.2.1.1        GE2/0/1
224.0.0.0/4         Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24        Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

以上显示信息表明 Device C 的路由表中已经没有 192.168.2.0/24 网段的路由信息了。

在 Device C 上使用源地址 192.168.3.1Ping 目标地址 192.168.2.1 进行验证。

```
[DeviceC] ping -a 192.168.3.1 192.168.2.1
Ping 192.168.2.1 (192.168.2.1) from 192.168.3.1: 56 data bytes, press CTRL_C to
break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping statistics for 192.168.2.1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

以上信息表明 Device C 通过过滤路由表中 192.168.2.0/24 网段的路由信息，使得市场一部所在网段无法访问研发一部所在网段。

查看 Device D 的路由表信息。

```
[DeviceD] display ip routing-table

Destinations : 25        Routes : 25
```

```
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         O_INTER 10  2           10.3.1.1        GE2/0/1
10.2.1.0/24         O_INTER 10  3           10.3.1.1        GE2/0/1
10.3.1.0/24         Direct  0   0           10.3.1.2        GE2/0/1
10.3.1.0/32         Direct  0   0           10.3.1.2        GE2/0/1
10.3.1.2/32         Direct  0   0           127.0.0.1       InLoop0
10.3.1.255/32       Direct  0   0           10.3.1.2        GE2/0/1
10.4.1.0/24         O_INTER 10  3           10.3.1.1        GE2/0/1
10.5.1.0/24         O_ASE2  150 1           10.3.1.1        GE2/0/1
127.0.0.0/8         Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
192.168.1.0/24      Direct  0   0           192.168.1.1     Loop0
192.168.1.0/32      Direct  0   0           192.168.1.1     Loop0
192.168.1.1/32      Direct  0   0           127.0.0.1       InLoop0
192.168.1.255/32    Direct  0   0           192.168.1.1     Loop0
192.168.2.0/24      Direct  0   0           192.168.2.1     Loop1
192.168.2.0/32      Direct  0   0           192.168.2.1     Loop1
192.168.2.1 /32     Direct  0   0           127.0.0.1       InLoop0
192.168.2.255/32    Direct  0   0           192.168.2.1     Loop1
192.168.3.1/32      O_INTER 10  3           10.3.1.1        GE2/0/1
224.0.0.0/4         Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24        Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

以上显示信息表明 Device D 的路由表中已经没有 192.168.5.0/24 网段的路由信息了。

在 Device D 上使用源地址 192.168.1.1Ping 目标地址 192.168.5.1 进行验证。

```
[DeviceD] ping -a 192.168.1.1 192.168.5.1
Ping 192.168.5.1 (192.168.5.1) from 192.168.1.1: 56 data bytes, press CTRL_C to
break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping statistics for 192.168.5.1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

在 Device D 上使用源地址 192.168.2.1Ping 目标地址 192.168.5.1 进行验证。

```
[DeviceD] ping -a 192.168.2.1 192.168.5.1
Ping 192.168.5.1 (192.168.5.1) from 192.168.2.1: 56 data bytes, press CTRL_C to
break
Request time out
Request time out
Request time out
Request time out
Request time out
```

```
--- Ping statistics for 192.168.5.1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

以上信息表明 Device D 通过过滤路由表中 192.168.5.0/24 网段的路由信息，使得研发一部和售后服务部所在网段无法访问市场二部所在网段。

综合 Device C 和 Device D 的路由表信息，发现路由表中均没有 192.168.4.0/24 网段路由信息，说明设备已经将引入 OSPF 的 RIP 路由中研发二部所在网段过滤掉。

3.6 配置文件

- Device A：

```
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
 area 0.0.0.1
network 10.4.1.0 0.0.0.255
area 0.0.0.2
  network 10.2.1.0 0.0.0.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.2.1.1 255.255.255.0
#
interface GigabitEthernet2/0/3
 port link-mode route
 ip address 10.4.1.1 255.255.255.0
#
```

- Device B ：

```
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
 area 0.0.0.3
  network 10.3.1.0 0.0.0.255
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.3.1.1 255.255.255.0
```

```
#
```

- Device C：

```
#
ospf 1
 filter-policy 2000 import
 area 0.0.0.2
  network 10.2.1.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
interface LoopBack0
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.2.1.2 255.255.255.0
#
acl basic 2000
 rule 0 deny source 192.168.2.0 0.0.0.255
rule 5 permit
#
```

- Device D：

```
#
ospf 1
 filter-policy 2000 import
 area 0.0.0.3
  network 10.3.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
interface LoopBack0
 ip address 192.168.1.1 255.255.255.0
#
interface LoopBack1
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.3.1.2 255.255.255.0
#
acl basic 2000
 rule 0 deny source 192.168.5.0 0.0.0.255
rule 5 permit
#
```

- Device E：

```
#
ospf 1
 import-route direct
 import-route rip 1
```

```
 filter-policy 2000 export rip 1
 area 0.0.0.1
  network 10.4.1.0 0.0.0.255
#
rip 1
 undo summary
 version 2
 network 10.5.1.0 0.0.0.255
 import-route direct
 import-route ospf 1
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.4.1.2 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.5.1.1 255.255.255.0
#
acl basic 2000
 rule 0 deny source 192.168.4.0 0.0.0.255
rule 5 permit
#
```

- Device F：

```
#
rip 1
 undo summary
 version 2
 network 10.5.1.0 0.0.0.255
 network 192.168.4.0
 network 192.168.5.0
#
interface LoopBack0
 ip address 192.168.4.1 255.255.255.0
#
interface LoopBack1
 ip address 192.168.5.1 255.255.255.0
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.5.1.2 255.255.255.0
#
```

4 相关资料

- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由配置指导-R7607
- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

OSPFv3 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 OSPFv3 路由信息过滤配置举例 1
3.1 组网需求 1
3.2 使用版本 2
3.3 配置注意事项 2
3.4 配置步骤 2
3.4.1 配置各接口的 IP 地址 2
3.4.2 配置 OSPFv3 网络的基本功能 2
3.4.3 配置 RIPng 网络的基本功能 4
3.4.4 将 RIPng 路由和 OSPFv3 路由互相引入 4
3.4.5 配置 OSPFv3 的路由过滤功能 6
3.5 验证配置 7
3.6 配置文件 10
4 相关资料 12

1 简介

本文档介绍了 OSPFv3 路由信息过滤的配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 OSPFv3 路由信息过滤的特性。

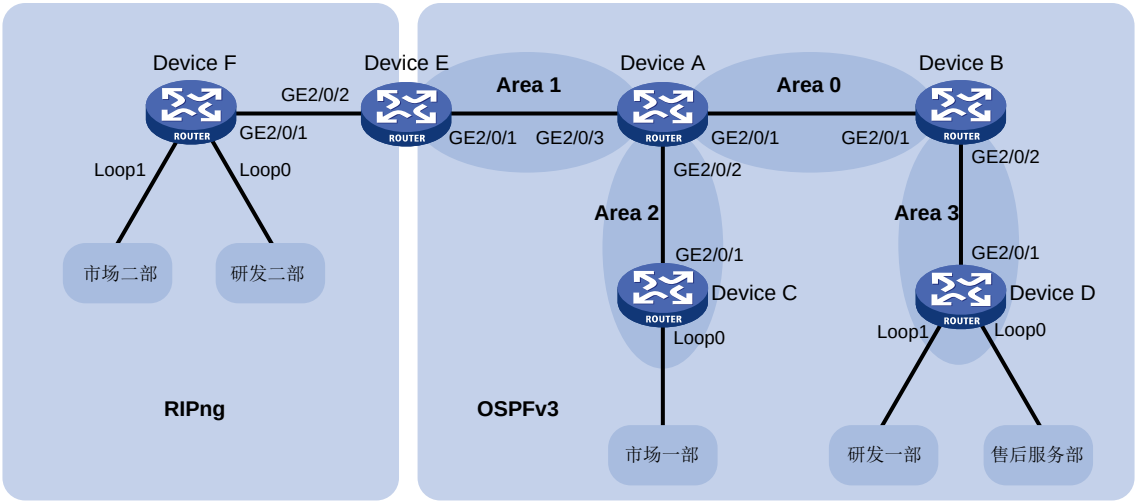
3 OSPFv3 路由信息过滤配置举例

3.1 组网需求

如图 1 所示，公司 A 使用 OSPFv3 路由协议实现公司设备全网互通，后来公司 A 扩张兼并了公司 B，要求将公司 B 采用的 RIPng 路由协议与公司 A 的 OSPFv3 协议互相引入，使得各个部门可以实现互通。Device A 和 Device B 作为公司核心设备负责各个部门间的通信。由于业务需要，现要求通过下列措施控制并调整网络中的路由信息：

- 在 Device E 上对引入的路由信息进行过滤，使得研发二部所在网段无法被引入到 OSPFv3 内。
- 在 Device C 上使用路由信息的过滤功能，使得市场一部所在网段无法访问研发一部。
- 在 Device D 上使用路由信息的过滤功能，使得研发一部和售后服务部所在网段无法访问市场二部。

图1 OSPFv3 路由信息过滤组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	GE2/0/1	1::1/64	Device B	GE2/0/1	1::2/64
	GE2/0/2	2::1/64		GE2/0/2	3::1/64

设备	接口	IP地址	设备	接口	IP地址
	GE2/0/3	4::1/64			
Device C	GE2/0/1	2::2/64	Device D	GE2/0/1	3::2/64
	Loop0	13::1/64 （市场一部所在网段）		Loop0	11::1/64 （售后服务部所在网段）
				Loop1	12::1/64 （研发一部所在网段）
Device E	GE2/0/1	4::2/64	Device F	GE2/0/1	5::2/64
	GE2/0/2	5::1/64		Loop0	14::1/64 （研发二部所在网段）
				Loop1	15::1/64 （市场二部所在网段）

3.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.3 配置注意事项

- 路由信息过滤功能中对于引入外部路由信息时采用 **export** 关键字进行过滤，该参数只能在 ASBR 上生效。
- 路由信息过滤功能只是对路由表中相关路由信息过滤，并不是过滤掉 OSPFv3 中通告的 LSA。
- 由于路由通信是双向的，使用路由信息过滤功能将某一目的网段过滤后，该路由器下联的其它网段无法访问这个目的网段的设备，这个目的网段的设备也不能访问源地址网段的设备。
- 使用路由信息过滤功能配合 ACL 使用时，必须将最后一条规则设置为允许所有源地址通过才能避免将所有网段路由被全部过滤掉。
- 配置 OSPFv3 时必须手工指定 Router ID。

3.4 配置步骤

3.4.1 配置各接口的 IP 地址

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface GigabitEthernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ipv6 address 1::1 64
```

请参考以上方法配置其它相关接口的 IP 地址，配置步骤这里省略。

3.4.2 配置 OSPFv3 网络的基本功能

创建 OSPFv3 进程，并在 Device A 的接口上使能 OSPFv3 路由功能。

```
<DeviceA> system-view
[DeviceA] ospfv3
[DeviceA-ospfv3-1] router-id 6.6.6.6
[DeviceA-ospfv3-1] quit
[DeviceA] interface GigabitEthernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ospfv3 1 area 0
```

```
[DeviceA-GigabitEthernet2/0/1]quit
[DeviceA] interface GigabitEthernet 2/0/2
[DeviceA-GigabitEthernet2/0/2] ospfv3 1 area 2
[DeviceA-GigabitEthernet2/0/2]quit
[DeviceA] interface GigabitEthernet 2/0/3
[DeviceA-GigabitEthernet2/0/3] ospfv3 1 area 1
[DeviceA-GigabitEthernet2/0/3]quit
```

创建 OSPFv3 进程，并在 Device B 的接口上使能 OSPFv3 路由功能。

```
<DeviceB> system-view
[DeviceB] ospfv3
[DeviceB-ospfv3-1] router-id 5.5.5.5
[DeviceB-ospfv3-1] quit
[DeviceB] interface GigabitEthernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] ospfv3 1 area 0
[DeviceB-GigabitEthernet2/0/1]quit
[DeviceB] interface GigabitEthernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] ospfv3 1 area 3
[DeviceB-GigabitEthernet2/0/2]quit
```

创建 OSPFv3 进程，并在 Device C 的接口上使能 OSPFv3 路由功能。

```
<DeviceC> system-view
[DeviceC] ospfv3
[DeviceC-ospfv3-1] router-id 4.4.4.4
[DeviceC-ospfv3-1] quit
[DeviceC] interface GigabitEthernet 2/0/1
[DeviceC-GigabitEthernet2/0/1] ospfv3 1 area 2
[DeviceC-GigabitEthernet2/0/1]quit
[DeviceC]interface LoopBack 0
[DeviceC-LoopBack0] ospfv3 1 area 2
[DeviceC-LoopBack0] quit
```

创建 OSPFv3 进程，并在 Device D 的接口上使能 OSPFv3 路由功能。

```
<DeviceD> system-view
[DeviceD] ospfv3
[DeviceD-ospfv3-1] router-id 3.3.3.3
[DeviceD-ospfv3-1] quit
[DeviceD] interface GigabitEthernet 2/0/1
[DeviceD-GigabitEthernet2/0/1] ospfv3 1 area 3
[DeviceD-GigabitEthernet2/0/1]quit
[DeviceD]interface LoopBack 0
[DeviceD-LoopBack0] ospfv3 1 area 3
[DeviceD-LoopBack0] quit
[DeviceD]interface LoopBack 1
[DeviceD-LoopBack1] ospfv3 1 area 3
[DeviceD-LoopBack1] quit
```

创建 OSPFv3 进程，并在 Device E 的接口上使能 OSPFv3 路由功能。

```
<DeviceE> system-view
[DeviceE] ospfv3
[DeviceE-ospfv3-1] router-id 2.2.2.2
```

```
[DeviceE-ospfv3-1] quit
[DeviceE] interface GigabitEthernet 2/0/1
[DeviceE-GigabitEthernet2/0/1] ospfv3 1 area 1
[DeviceE-GigabitEthernet2/0/1]quit
```

3.4.3 配置 RIPng 网络的基本功能

创建 RIPng 进程，并在 Device E 的接口上使能 RIPng 路由功能。

```
<DeviceE> system-view
[DeviceE] ripng
[DeviceE-ripng-1] quit
[DeviceE] interface GigabitEthernet 2/0/2
[DeviceE-GigabitEthernet2/0/2] ripng 1 enable
[DeviceE-GigabitEthernet2/0/2] quit
```

创建 RIPng 进程，并在 Device F 的接口上使能 RIPng 路由功能。

```
<DeviceF> system-view
[DeviceF] ripng
[DeviceF-ripng-1] quit
[DeviceF] interface GigabitEthernet 2/0/1
[DeviceF-GigabitEthernet2/0/1] ripng 1 enable
[DeviceF-GigabitEthernet2/0/1]quit
[DeviceF]interface LoopBack 0
[DeviceF-LoopBack0]ripng 1 enable
[DeviceF-LoopBack0] quit
[DeviceF]interface LoopBack 1
[DeviceF-LoopBack1]ripng 1 enable
[DeviceF-LoopBack1] quit
```

3.4.4 将 RIPng 路由和 OSPFv3 路由互相引入

在 Device E 上将直连路由和 OSPFv3 路由引入到 RIPng 网络中。

```
<DeviceE> system-view
[DeviceE] ripng
[DeviceE-ripng-1] import-route direct
[DeviceE-ripng-1] import-route ospfv3
[DeviceE-ripng-1] quit
```

在 Device E 上将直连路由和 RIPng 路由引入到 OSPFv3 网络中。

```
[DeviceE] ospfv3
[DeviceE-ospfv3-1] import-route direct
[DeviceE-ospfv3-1] import-route ripng
[DeviceE-ospfv3-1] quit
```

查看 Device E 的路由表信息。

```
[Device E]display ipv6 routing-table

Destinations : 15        Routes : 15

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
```

```
Interface  : InLoop0                                Cost      : 0

Destination: 1::/64                                 Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:124D               Preference: 10
Interface  : GE2/0/1                               Cost      : 2

Destination: 2::/64                                 Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:124D               Preference: 10
Interface  : GE2/0/1                               Cost      : 2

Destination: 3::/64                                 Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:124D               Preference: 10
Interface  : GE2/0/1                               Cost      : 3

Destination: 4::/64                                 Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : GE2/0/1                               Cost      : 0

Destination: 4::2/128                               Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: 5::/64                                 Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : GE2/0/2                               Cost      : 0

Destination: 5::1/128                               Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: 11::1/128                              Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:124D               Preference: 10
Interface  : GE2/0/1                               Cost      : 3

Destination: 12::1/128                              Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:124D               Preference: 10
Interface  : GE2/0/1                               Cost      : 3

Destination: 13::1/128                              Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:124D               Preference: 10
Interface  : GE2/0/1                               Cost      : 2

Destination: 14::/64                                Protocol  : RIPng
NextHop    : FE80::2E0:FCFF:FE11:19B5               Preference: 100
Interface  : GE2/0/2                               Cost      : 1

Destination: 15::/64                                Protocol  : RIPng
NextHop    : FE80::2E0:FCFF:FE11:19B5               Preference: 100
```

```
Interface  : GE2/0/2                                  Cost      : 1

Destination: FE80::/10                                Protocol  : Direct
NextHop    : ::                                       Preference: 0
Interface  : InLoop0                                  Cost      : 0

Destination: FF00::/8                                 Protocol  : Direct
NextHop    : ::                                       Preference: 0
Interface  : NULL0
```

以上显示信息表明 Device E 拥有路由域内所有网段路由，然后依次查看其他所有设备的路由表信息，路由域内所有的网段均可互通。

3.4.5 配置 OSPFv3 的路由过滤功能

在 Device C 上创建基本 IPv6 ACL 并匹配需要拒绝访问的目的网段 12::1/64。

```
<DeviceC> system-view
[DeviceC] acl ipv6 basic 2000
[DeviceC-acl-ipv6-basic-2000] rule 0 deny source 12::1 64
[DeviceC-acl-ipv6-basic-2000] rule permit source any
[DeviceC-acl-ipv6-basic-2000] quit
```

在 Device C 上通过指定访问控制列表 IPv6 ACL 2000 来对要加入到路由表的路由信息进行过滤。

```
[DeviceC] ospfv3
[DeviceC-ospfv3-1] filter-policy 2000 import
[DeviceC-ospfv3-1] quit
```

在 Device D 上创建基本 IPv6 ACL 并匹配需要拒绝访问的目的网段 15::1/64。

```
<DeviceD> system-view
[DeviceD] acl ipv6 basic 2000
[DeviceD-acl-ipv6-basic-2000] rule 0 deny source 15::1 64
[DeviceD-acl-ipv6-basic-2000] rule permit source any
[DeviceD-acl-ipv6-basic-2000] quit
```

在 Device D 上通过指定访问控制列表 IPv6 ACL 2000 来对要加入到路由表的路由信息进行过滤。

```
[DeviceD] ospfv3
[DeviceD-ospfv3-1] filter-policy 2000 import
[DeviceD-ospfv3-1] quit
```

在 Device E 上创建基本 IPv6 ACL 并匹配需要拒绝访问的目的网段 14::1/64。

```
<DeviceE> system-view
[DeviceE] acl ipv6 basic 2000
[DeviceE-acl-ipv6-basic-2000] rule 0 deny source 14::1 64
[DeviceE-acl-ipv6-basic-2000] rule permit source any
[DeviceE-acl-ipv6-basic-2000] quit
```

在 Device E 上通过指定访问控制列表 IPv6 ACL 2000 来对引入 OSPFv3 的 RIPng 路由信息进行过滤。

```
[DeviceE] ospfv3
[DeviceE-ospfv3-1] filter-policy 2000 export ripng 1
[DeviceE-ospfv3-1] quit
```

3.5 验证配置

查看 Device C 的路由表信息。

```
[DeviceC]display ipv6 routing-table

Destinations : 13        Routes : 13

Destination: ::1/128                                 Protocol  : Direct
NextHop    : ::1                                     Preference: 0
Interface  : InLoop0                                 Cost      : 0

Destination: 1::/64                                  Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:1245                Preference: 10
Interface  : GE2/0/1                                Cost      : 2

Destination: 2::/64                                  Protocol  : Direct
NextHop    : ::                                      Preference: 0
Interface  : GE2/0/1                                Cost      : 0

Destination: 2::2/128                                Protocol  : Direct
NextHop    : ::1                                     Preference: 0
Interface  : InLoop0                                 Cost      : 0

Destination: 3::/64                                  Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:1245                Preference: 10
Interface  : GE2/0/1                                Cost      : 3

Destination: 4::/64                                  Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:1245                Preference: 10
Interface  : GE2/0/1                                Cost      : 2

Destination: 5::/64                                  Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:1245                Preference: 150
Interface  : GE2/0/1                                Cost      : 1

Destination: 11::1/128                               Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:1245                Preference: 10
Interface  : GE2/0/1                                Cost      : 3

Destination: 13::/64                                 Protocol  : Direct
NextHop    : ::                                      Preference: 0
Interface  : Loop0                                   Cost      : 0

Destination: 13::1/128                               Protocol  : Direct
NextHop    : ::1                                     Preference: 0
Interface  : InLoop0                                 Cost      : 0

Destination: 15::/64                                 Protocol  : OSPFv3
```

```
NextHop    : FE80::2E0:FCFF:FE58:1245                  Preference: 150
Interface  : GE2/0/1                                   Cost      : 1

Destination: FE80::/10                                 Protocol  : Direct
NextHop    : ::                                        Preference: 0
Interface  : InLoop0                                   Cost      : 0

Destination: FF00::/8                                  Protocol  : Direct
NextHop    : ::                                        Preference: 0
Interface  : NULL0
```

以上显示信息表明 Device C 的路由表中已经没有 12::/64 网段的路由信息了。

在 Device C 上使用源地址 13::1 Ping 目标地址 12::1 进行验证。

```
[DeviceC] ping ipv6 -a 13::1 12::1
Ping6(56 data bytes) 13::1 --> 12::1, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping6 statistics for 12::1 ---
5 packets transmitted, 0 packets received, 100.0% packet loss
```

以上信息表明 Device C 通过过滤路由表中 12::/64 网段的路由信息，使得市场一部所在网段无法访问研发一部所在网段。

查看 Device D 的路由表信息。

```
[DeviceD]display ipv6 routing-table

Destinations : 14        Routes : 14

Destination: ::1/128                                   Protocol  : Direct
NextHop    : ::1                                       Preference: 0
Interface  : InLoop0                                   Cost      : 0

Destination: 1::/64                                    Protocol  : OSPFv3
NextHop    : FE80::2A0:FCFF:FE00:5815                  Preference: 10
Interface  : GE2/0/1                                   Cost      : 2

Destination: 2::/64                                    Protocol  : OSPFv3
NextHop    : FE80::2A0:FCFF:FE00:5815                  Preference: 10
Interface  : GE2/0/1                                   Cost      : 3

Destination: 3::/64                                    Protocol  : Direct
NextHop    : ::                                        Preference: 0
Interface  : GE2/0/1                                   Cost      : 0

Destination: 3::3/128                                  Protocol  : Direct
NextHop    : ::1                                       Preference: 0
```

```
Interface  : InLoop0                                    Cost      : 0

Destination: 4::/64                                     Protocol  : OSPFv3
NextHop    : FE80::2A0:FCFF:FE00:5815                   Preference: 10
Interface  : GE2/0/1                                   Cost      : 3

Destination: 5::/64                                     Protocol  : OSPFv3
NextHop    : FE80::2A0:FCFF:FE00:5815                   Preference: 150
Interface  : GE2/0/1                                   Cost      : 1

Destination: 11::/64                                    Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : Loop0                                      Cost      : 0

Destination: 11::1/128                                  Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 12::/64                                    Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : Loop1                                      Cost      : 0

Destination: 12::1/128                                  Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 13::1/128                                  Protocol  : OSPFv3
NextHop    : FE80::2A0:FCFF:FE00:5815                   Preference: 10
Interface  : GE2/0/1                                   Cost      : 3

Destination: FE80::/10                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0

Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0
```

以上显示信息表明 Device D 的路由表中已经没有 15::/64 网段的路由信息了。

在 Device D 上使用源地址 11::1 Ping 目标地址 15::1 进行验证。

```
[DeviceD] ping ipv6 -a 11::1 15::1
Ping6(56 data bytes) 11::1 --> 15::1, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping6 statistics for 15::1 ---
```

```
5 packets transmitted, 0 packets received, 100.0% packet loss
```

在 Device D 上使用源地址 12::1 Ping 目标地址 15::1 进行验证。

```
[DeviceD] ping ipv6 -a 12::1 15::1
Ping6(56 data bytes) 12::1 --> 15::1, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping6 statistics for 15::1 ---
5 packets transmitted, 0 packets received, 100.0% packet loss
```

以上信息表明 Device D 通过过滤路由表中 15::/64 网段的路由信息，使得研发一部和售后服务部所在网段无法访问市场二部所在网段。

综合 Device C 和 Device D 的路由表信息，发现路由表中均没有 14::/64 网段路由信息，说明设备已经将引入 OSPFv3 的 RIPng 路由中研发二部所在网段过滤掉。

3.6 配置文件

- Device A：

```
#
ospfv3 1
 router-id 6.6.6.6
 area 0.0.0.0
 area 0.0.0.1
 area 0.0.0.2
#
interface GigabitEthernet2/0/1
 ospfv3 1 area 0.0.0.0
 ipv6 address 1::1/64
#
interface GigabitEthernet2/0/2
 ospfv3 1 area 0.0.0.2
 ipv6 address 2::1/64
#
interface GigabitEthernet2/0/3
 ospfv3 1 area 0.0.0.1
 ipv6 address 4::1/64
#
```

- Device B ：

```
#
ospfv3 1
 router-id 5.5.5.5
 area 0.0.0.0
 area 0.0.0.3
#
interface GigabitEthernet2/0/1
```

```
 ospfv3 1 area 0.0.0.0
 ipv6 address 1::2/64
#
interface GigabitEthernet2/0/2
 ospfv3 1 area 0.0.0.3
 ipv6 address 3::1/64
#
```

- Device C：

```
#
ospfv3 1
 router-id 4.4.4.4
 filter-policy 2000 import
 area 0.0.0.2
#
interface LoopBack0
 ospfv3 1 area 0.0.0.2
 ipv6 address 13::1/64
#
interface GigabitEthernet2/0/1
 ospfv3 1 area 0.0.0.2
 ipv6 address 2::2/64
#
acl ipv6 basic 2000
 rule 0 deny source 12::/64
 rule 5 permit
#
```

- Device D：

```
#
ospfv3 1
 router-id 3.3.3.3
 filter-policy 2000 import
 area 0.0.0.3
#
interface LoopBack0
 ospfv3 1 area 0.0.0.3
 ipv6 address 11::1/64
#
interface LoopBack1
 ospfv3 1 area 0.0.0.3
 ipv6 address 12::1/64
#
interface GigabitEthernet2/0/1
 ospfv3 1 area 0.0.0.3
 ipv6 address 3::2/64
#
acl ipv6 basic 2000
 rule 0 deny source 15::/64
 rule 5 permit
```

```
#
```

- Device E：

```
#
ospfv3 1
 router-id 2.2.2.2
 import-route direct
import-route ripng 1
 filter-policy 2000 export ripng 1
 area 0.0.0.1
#
ripng 1
 import-route direct
 import-route ospfv3 1
#
interface GigabitEthernet2/0/1
 ospfv3 1 area 0.0.0.1
 ipv6 address 4::2/64
#
interface GigabitEthernet2/0/2
 ipv6 address 5::1/64
 ripng 1 enable
#
acl ipv6 basic 2000
 rule 0 deny source 14::/64
 rule 5 permit
#
```

- Device F：

```
#
ripng 1
#
interface LoopBack0
 ipv6 address 14::1/64
 ripng 1 enable
#
interface LoopBack1
 ipv6 address 15::1/64
 ripng 1 enable
#
interface GigabitEthernet2/0/1
 ipv6 address 5::2/64
 ripng 1 enable
#
```

4 相关资料

- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由配置指导-R7607
- H3C SR6600 SR6600-X 路由器 三层技术-IP 路由命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

Portal 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1

2 配置前提 1

3 可跨三层 Portal 认证配置举例 1

3.1 组网需求 1

3.2 配置思路 2

3.3 使用版本 2

3.4 配置注意事项 2

3.5 配置步骤 3

3.5.1 RADIUS/Portal server 的配置 3

3.5.2 Device A 的配置 8

3.5.3 Device B 的配置 8

3.6 验证配置 9

3.7 配置文件 11

4 可跨三层 Portal 认证方式扩展功能配置举例 12

4.1 组网需求 12

4.2 配置思路 13

4.3 使用版本 13

4.4 配置注意事项 13

4.5 配置步骤 14

4.5.1 Device A 的配置 14

4.5.2 Device B 的配置 14

4.6 验证配置 16

4.7 配置文件 17

5 直接 Portal 认证配置举例 18

5.1 组网需求 18

5.2 配置思路 19

5.3 使用版本 19

5.4 配置注意事项 19

5.5 配置步骤 20

5.5.1 Device 的配置 20

5.5.2 验证配置 21

5.6 配置文件 22

6 相关资料 ·····23

1 简介

本文档介绍了可跨三层 Portal 认证和直接 Portal 认证的典型配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文假设您已了解 Portal 特性。

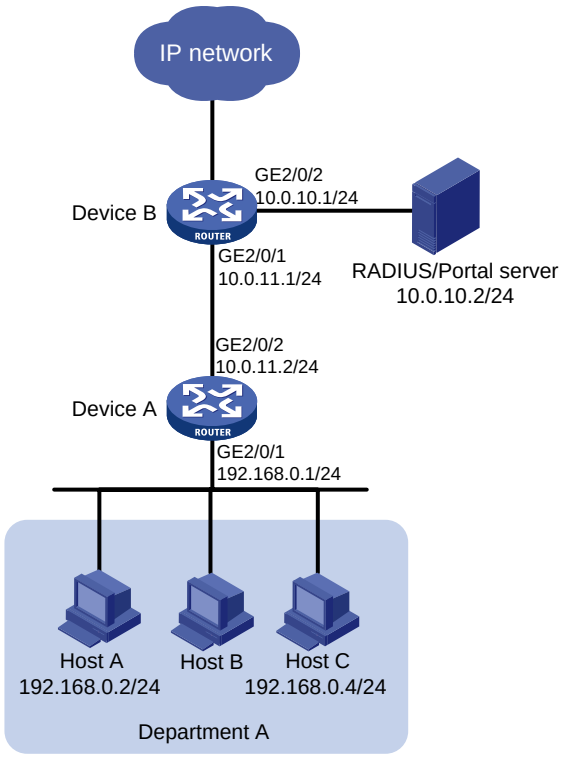
3 可跨三层 Portal 认证配置举例

3.1 组网需求

如图 1 所示，Device B 支持 Portal 认证功能，Host A、Host B 和 Host C 通过 Device A 接入到 Device B，要求：

- 采用一台 Portal 服务器承担 Portal 认证服务器和 Portal Web 服务器的职责。
- 配置 Device B 采用可跨三层 Portal 认证。
- 用户在通过 Portal 认证前，只能访问 Portal Web 服务器。用户通过认证后，可以访问非受限互联网资源。
- 采用 RADIUS 服务器对 Portal 用户接入进行认证/授权和计费。
- 配置发送给 Portal 认证服务器的 Portal 报文的 BAS-IP 属性。
- 使能 RADIUS session control 功能来监听并接收 RADIUS 服务器发送的 session control 报文。

图1 可跨三层 Portal 认证配置组网图



3.2 配置思路

- 为了对 Department A 的网络访问进行 Portal 认证，需要在 Device B 上配置 Portal 服务器并且使能 Portal 认证。
- 为了实现通过 RADIUS 来对 Portal 用户进行认证/授权和计费，需要在 Device B 上配置 RADIUS 方案并指定相应的认证/授权服务器和计费服务器，并将其应用于 Portal 用户所属的认证域。
- 配置系统缺省的 ISP 域，所有接入用户共用此缺省域的认证/授权和计费方法，若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方法。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置注意事项

目前仅支持使用 RADIUS 服务器对 Portal 用户进行认证/授权和计费，同时服务器需要配置路由，可以访问认证端口及用户 IP 地址所在网段。

3.5 配置步骤

3.5.1 RADIUS/Portal server 的配置

说明

下面以 iMC 为例(使用 iMC 版本为：iMC PLAT 7.0 (E0202)、iMC EIA 7.0 (E0202))，说明 RADIUS server 和 Portal server 的基本配置。

增加接入设备

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击<增加>按钮，进入增加接入设备页面。

- 设置与 Device B 交互报文时的认证共享密钥为“expert”；
- 设置认证及计费的端口号分别为“1812”和“1813”；
- 选择业务类型为“LAN 接入业务”；
- 选择接入设备类型为“H3C（General）”；
- 选择或手工增加接入设备，添加 IP 地址为 10.0.10.1 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

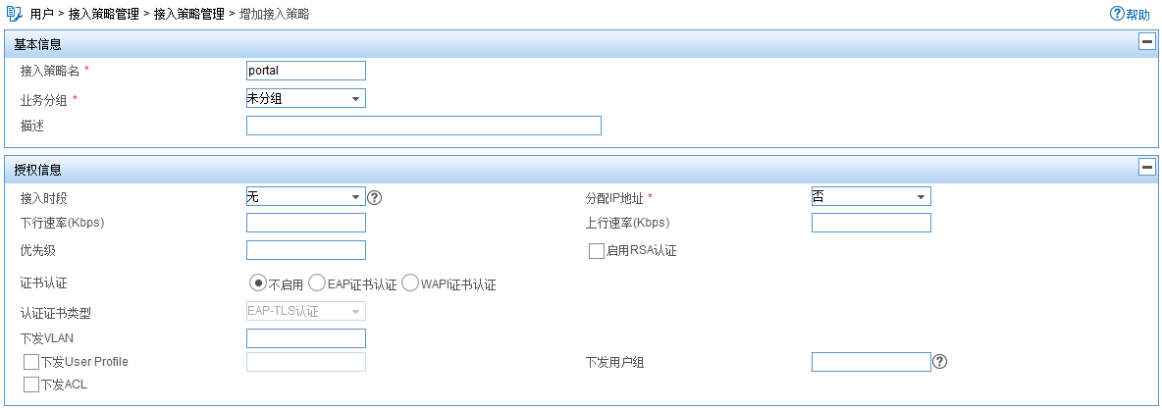
图2 增加接入设备

增加接入策略

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，单击<增加>按钮，进入“增加接入策略”页面。

- 接入策略名填写 portal（该名称可以自定义)。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

图3 增加接入策略



增加服务配置

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，进入服务器配置管理页面，在该页面中单击<增加>按钮，进入增加服务配置页面。

- 输入服务名为“Portal-auth”（该名称可以自定义）。
- 缺省接入策略选择“portal”，即上一步配置的接入策略名。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

图4 增加服务配置

增加接入用户

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入接入用户列表页面，在该页面中单击<增加>按钮，进入增加接入用户页面。

- 单击<增加用户>按钮，手工增加用户姓名为“hello”（可自定义），证件号码为 111111（可自定义）；
- 其它参数采用缺省值，并单击<确定>按钮完成操作；

图5 接入用户配置

- 输入帐号名“portal”和密码；
- 选择该用户所关联的接入服务为“Portal-auth”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图6 增加接入用户

配置 Portal 主页

选择“用户”页签，单击导航树中的[接入策略管理/Portal 服务管理/服务器配置]菜单项，进入服务器配置页面，配置 Portal 主页，采用默认配置即可，并单击<确定>按钮完成操作。

图7 Portal 服务器配置页面

配置 Portal 认证的地址组范围

单击导航树中的[接入策略管理/Portal 服务管理/IP 地址组配置]菜单项，进入“IP 地址组配置”页面，在该页面中单击<增加>按钮，进入“增加 IP 地址组配置”页面。

- 输入 IP 地址组名为“Portal_user”；
- 输入起始地址为“192.168.0.0”、终止地址为“192.168.0.255”。用户主机 IP 地址必须包含在该 IP 地址组范围内；
- 其他采用默认配置；
- 单击<确定>按钮完成操作。

图8 增加 IP 地址组配置页面

增加 Portal 接入设备信息

单击导航树中的[接入策略管理/Portal 服务管理/设备配置]菜单项，进入“设备配置”页面，在该页面中单击<增加>按钮，进入“增加设备信息”页面。

- 输入设备名为“NAS”；

- 输入 IP 地址为“10.0.11.1”，该地址为与接入用户相连的设备接口 IP 地址；
- 输入密钥为“portal”，该密钥与接入设备 Device B 上的配置保持一致；
- 选择组网方式为“三层”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图9 增加设备信息配置页面

配置端口组信息

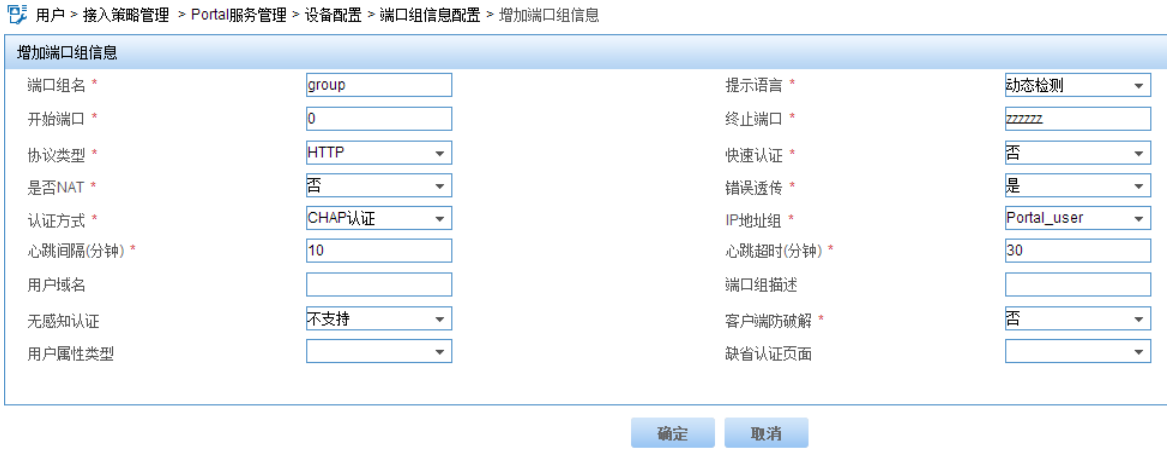
返回[接入策略管理/Portal 服务管理/设备配置]菜单项，单击<端口组信息管理>按钮，进入“端口组信息配置”页面。

图10 设备信息列表

在“端口组信息配置”页面中单击<增加>按钮，进入“增加端口组信息”页面。

- 输入端口组名为“group”；
- 选择 IP 地址组为“Portal_user”，用户接入网络时使用的 IP 地址必须属于所选的 IP 地址组；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图11 增加端口组信息配置页面



3.5.2 Device A 的配置

配置接口 GigabitEthernet2/0/1 和 GigabitEthernet2/0/2 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 192.168.0.1 24
[DeviceA-GigabitEthernet2/0/1] quit
[DeviceA] interface gigabitethernet 2/0/2
[DeviceA-GigabitEthernet2/0/2] ip address 10.0.11.2 24
[DeviceA-GigabitEthernet2/0/2] quit
```

配置到 10.0.10.0/24 网段的静态路由，下一跳为 10.0.11.1。

```
[DeviceA] ip route-static 10.0.10.0 255.255.255.0 10.0.11.1
```

3.5.3 Device B 的配置

配置接口 GigabitEthernet2/0/1 和 GigabitEthernet2/0/2 的 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] ip address 10.0.11.1 24
[DeviceB-GigabitEthernet2/0/1] quit
[DeviceB] interface gigabitethernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] ip address 10.0.10.1 24
[DeviceB-GigabitEthernet2/0/2] quit
```

配置 Portal 认证服务器：名称为 newpt，IP 地址为 10.0.10.2，密钥为明文 portal，监听 Portal 报文的端口为 50100（设备缺省端口号）。

```
[DeviceB] portal server newpt
[DeviceB-portal-server-newpt] ip 10.0.10.2 key simple portal
[DeviceB-portal-server-newpt] port 50100
[DeviceB-portal-server-newpt] quit
```

配置 Portal Web 服务器的 URL 为 http://10.0.10.2:8080/portal。（Portal Web 服务器的 URL 请与实际环境中的 Portal Web 服务器配置保持一致，此处仅为示例）

```
[DeviceB] portal web-server newpt
[DeviceB-portal-websvr-newpt] url http://10.0.10.2:8080/portal
[DeviceB-portal-websvr-newpt] quit
```

在与 Device A 相连的接口上使能可跨三层方式的 Portal 认证。

```
[DeviceB] interface gigabitethernet2/0/1
[DeviceB-GigabitEthernet2/0/1] portal enable method layer3
```

在与 Device A 相连的接口上设置发送给 Portal 报文中的 BAS-IP 属性值为 10.0.11.1。

```
[DeviceB-GigabitEthernet2/0/1] portal bas-ip 10.0.11.1
```

在与 Device A 相连的接口上引用 Portal Web 服务器 newpt。

```
[DeviceB-GigabitEthernet2/0/1] portal apply web-server newpt
[DeviceB-GigabitEthernet2/0/1] quit
```

创建名字为 imc 的 RADIUS 方案并进入该方案视图。

```
[DeviceB] radius scheme imc
```

配置 RADIUS 方案主认证/计费服务器及其通信密钥。

```
[DeviceB-radius-imc] primary authentication 10.0.10.2
[DeviceB-radius-imc] primary accounting 10.0.10.2
[DeviceB-radius-imc] key authentication simple expert
[DeviceB-radius-imc] key accounting simple expert
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[DeviceB-radius-imc] user-name-format without-domain
[DeviceB-radius-imc] quit
```

配置名为 portal.com 的认证域。

```
[DeviceB] domain portal.com
```

配置 ISP 域的 AAA 方法。

```
[DeviceB-isp-portal.com] authentication portal radius-scheme imc
[DeviceB-isp-portal.com] authorization portal radius-scheme imc
[DeviceB-isp-portal.com] accounting portal radius-scheme imc
[DeviceB-isp-portal.com] quit
```

配置系统缺省的 ISP 域 portal.com，所有接入用户共用此缺省域的认证/授权和计费方法，若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方法。

```
[DeviceB] domain default enable portal.com
```

配置到 Department A 的静态路由。

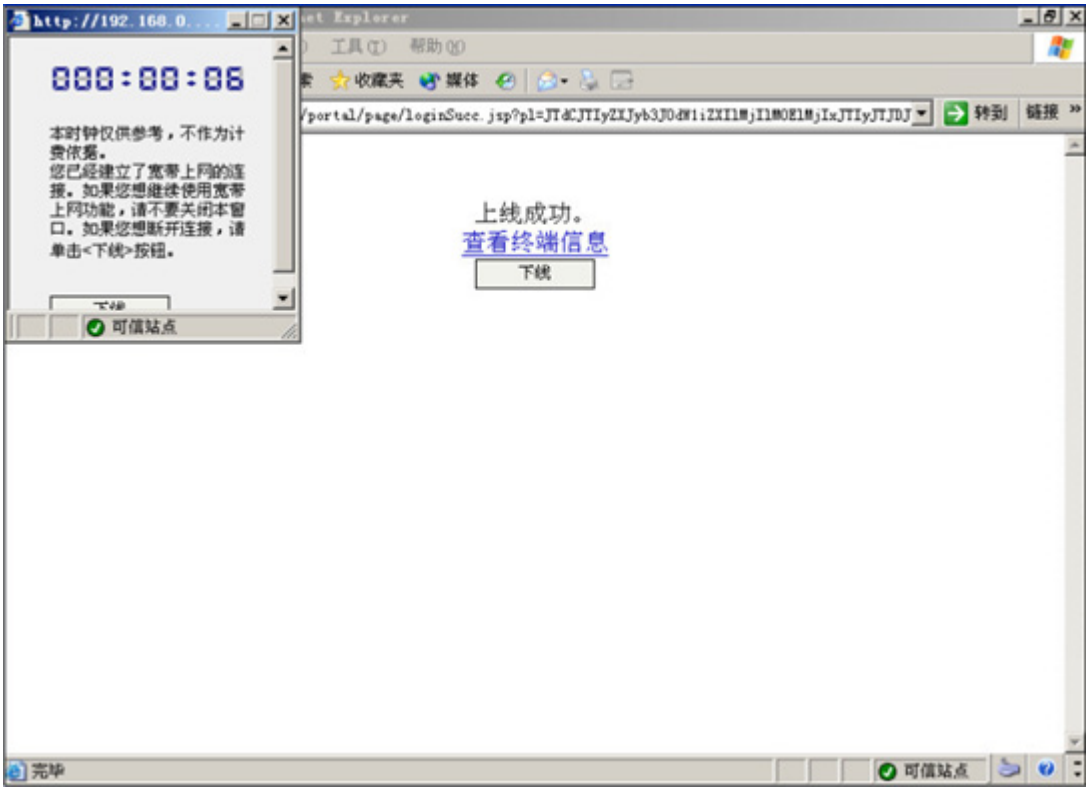
```
[DeviceB] ip route-static 192.168.0.0 255.255.255.0 10.0.11.2
```

3.6 验证配置

用户既可以使用 H3C 的 iNode 客户端，也可以通过网页方式进行 Portal 认证。本例用网页方式进行 Portal 认证。用户在通过认证前，任何 Web 访问请求都会被重定向到认证页面 http://10.0.10.2:8080/portal，且发起的 Web 访问请求均被重定向到该认证页面，如图 12。当用户通过认证后，跳转到图 13 界面。

图12 Portal 认证页面

图13 Portal 用户认证成功页面



认证通过后，可通过执行以下显示命令查看 Device B 上生成的 Portal 在线用户信息。

```
[DeviceB] display portal user interface gigabitethernet 2/0/1
```

```
Total portal users: 1
Username: portal
  Portal server: newpt
  State: Online
  VPN instance: --
  Authorization ACL: None
  VPN instance: --
  MAC              IP               Vlan   Interface
   --------------------------------------------------------------------------
  0000-0000-0000   192.168.0.2       --     GigabitEthernet2/0/1
```

3.7 配置文件

- Device A：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.0.11.2 255.255.255.0
#
ip route-static 10.0.10.0 24 10.0.11.1
#
```

- Device B：

```
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.0.10.1 255.255.255.0
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.0.11.1 255.255.255.0
 portal enable method layer3
 portal bas-ip 10.0.11.1
 portal apply web-server newpt
#
ip route-static 192.168.0.0 24 10.0.11.2
#
radius session-control enable
#
radius scheme imc
primary authentication 10.0.10.2
primary accounting 10.0.10.2
key authentication cipher $c$3$M30nGDQxiOCAxe2AJ9yEZdk8kjoWag==
key accounting cipher $c$3$M23dGDQxiOCAxe2BJ9yEZdk8kjoWag==
user-name-format without-domain
```

```
#
domain portal.com
 authentication portal radius-scheme imc
 authorization portal radius-scheme imc
accounting portal radius-scheme imc
#
domain default enable portal.com
#
portal web-server newpt
 url http://10.0.10.2:8080/portal
#
portal server newpt
 ip 10.0.10.2 key cipher $c$3$r0VxoIiBrpzju9h2akP4TxyknX8VTuYKfA==
#
```

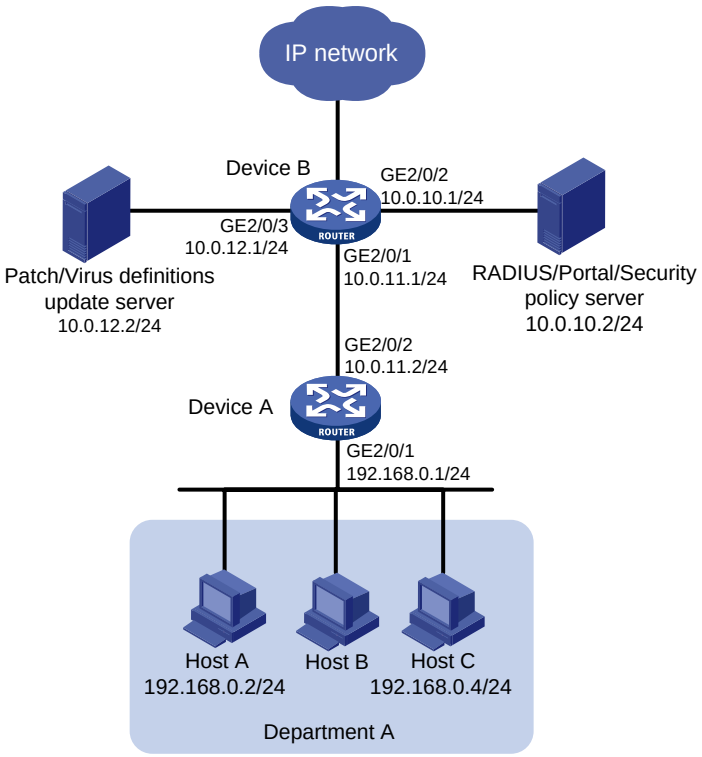
4 可跨三层 Portal 认证方式扩展功能配置举例

4.1 组网需求

如图 14所示，Device B 支持 Portal 认证功能，Host A、Host B 和 Host C 通过 Device A 接入到 Device B，要求：

- 采用一台 Portal 服务器承担 Portal 认证服务器和 Portal Web 服务器的职责。
- 配置 Device B 采用可跨三层 Portal 认证。
- 用户在通过 Portal 认证前，只能访问 Portal Web 服务器。
- 用户通过认证，但没有安装指定版本的防病毒软件，则对用户进行隔离，只允许访问病毒和补丁服务器。
- 用户通过认证，且安装了指定版本的防病毒软件，则通过安全策略检查，可正常访问网络。
- 采用 RADIUS 服务器对用户接入进行认证和授权，并采用安全策略服务器对登录成功的用户进行安全检查。
- 配置发送给 Portal 认证服务器的 Portal 报文的 BAS-IP 属性。
- 使能 RADIUS session control 功能来监听并接收 RADIUS 服务器发送的 session control 报文。

图14 Portal 三层认证扩展功能配置组网图



4.2 配置思路

- 为了对 Department A 的网络访问进行 Portal 认证，需要在 Device B 上配置 Portal 服务器并且使能 Portal 认证，认证通过前，所有客户端只能访问 Portal Web 服务器，用户访问任何网页都被重定向到 Portal Web 服务器主页面。
- 为了实现通过 RADIUS 来进行认证和授权，需要在 Device B 上配置 RADIUS 方案并指定相应的认证和授权服务器，并将其应用于 Portal 用户所属的认证域。
- 为了对登录成功的用户进行安全检查，需要创建 ACL 并制定规则，不符合检查要求的用户，只能访问病毒和补丁服务器，升级病毒库版本满足安全策略要求后，该用户才可访问所有网络资源。
- 配置系统缺省的 ISP 域，所有接入用户共用此缺省域的认证、授权方法，若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方法。

4.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.4 配置注意事项

目前仅支持使用 RADIUS 服务器对 Portal 用户进行认证和授权，同时服务器需要配置路由，可以访问认证端口及用户 IP 地址所在网段。

4.5 配置步骤

说明

- 请保证在 RADIUS 服务器、Portal 服务器上完成相应的配置，具体配置步骤请参见 3.5.1 RADIUS/Portal server 的配置。
- 安全策略服务器上需要将 ACL 3000 和 ACL 3001 分别指定为隔离 ACL 和安全 ACL。

4.5.1 Device A 的配置

配置接口 GigabitEthernet2/0/1 和 GigabitEthernet2/0/2 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 192.168.0.1 24
[DeviceA-GigabitEthernet2/0/1] quit
[DeviceA] interface gigabitethernet2/0/2
[DeviceA-GigabitEthernet2/0/2] ip address 10.0.11.2 24
[DeviceA-GigabitEthernet2/0/2] quit
```

配置到 10.0.10.0/24 网段的静态路由，下一跳为 10.0.11.1。

```
[DeviceA] ip route-static 10.0.10.0 255.255.255.0 10.0.11.1
```

配置到 10.0.12.0/24 网段的静态路由，下一跳为 10.0.11.1。

```
[DeviceA] ip route-static 10.0.12.0 255.255.255.0 10.0.11.1
```

4.5.2 Device B 的配置

配置接口 GigabitEthernet 2/0/1、GigabitEthernet2/0/2 和 GigabitEthernet2/0/3 的 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] ip address 10.0.11.1 24
[DeviceB-GigabitEthernet2/0/1] quit
[DeviceB] interface gigabitethernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] ip address 10.0.10.1 24
[DeviceB-GigabitEthernet2/0/2] quit
[DeviceB] interface gigabitethernet 2/0/3
[DeviceB-GigabitEthernet2/0/3] ip address 10.0.12.1 24
[DeviceB-GigabitEthernet2/0/3] quit
```

配置 Portal 认证服务器：名称为 newpt，IP 地址为 10.0.10.2，密钥为明文 portal，监听 Portal 报文的端口为 50100（设备缺省端口号）。

```
[DeviceB] portal server newpt
[DeviceB-portal-server-newpt] ip 10.0.10.2 key simple portal
[DeviceB-portal-server-newpt] port 50100
[DeviceB-portal-server-newpt] quit
```

配置 Portal Web 服务器的 URL 为 http://10.0.10.2:8080/portal。（Portal Web 服务器的 URL 请与实际环境中的 Portal Web 服务器配置保持一致，此处仅为示例）

```
[DeviceB] portal web-server newpt
[DeviceB-portal-websvr-newpt] url http://10.0.10.2:8080/portal
[DeviceB-portal-websvr-newpt] quit
```
在与 Device A 相连的接口上使能可跨三层方式的 Portal 认证。
```
[DeviceB] interface gigabitethernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] portal enable method layer3
```
在与 Device A 相连的接口上设置发送给 Portal 报文中的 BAS-IP 属性值为 10.0.11.1。
```
[DeviceB–GigabitEthernet2/0/1] portal bas-ip 10.0.11.1
```
在与 Device A 相连的接口上引用 Portal Web 服务器 newpt。
```
[DeviceB–GigabitEthernet2/0/1] portal apply web-server newpt
[DeviceB-GigabitEthernet2/0/1] quit
```
配置到 Department A 的静态路由。
```
[DeviceB] ip route-static 192.168.0.0 255.255.255.0 10.0.11.2
```
创建名字为 imc 的 RADIUS 方案并进入该方案视图。
```
[DeviceB] radius scheme imc
```
配置 RADIUS 方案相关参数，包括 RADIUS 服务器地址，认证密钥等。
```
[DeviceB-radius-imc] primary authentication 10.0.10.2
[DeviceB-radius-imc] primary accounting 10.0.10.2
[DeviceB-radius-imc] key authentication simple expert
[DeviceB-radius-imc] key accounting simple expert
```
配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。
```
[DeviceB-radius-imc] user-name-format without-domain
[DeviceB-radius-imc] quit
```
使能 RADIUS session control 功能。
```
[DeviceB] radius session-control enable
```
配置名为 portal.com 的认证域。
```
[DeviceB] domain portal.com
```
配置 ISP 域的 AAA 方法。
```
[DeviceB-isp-portal.com] authentication portal radius-scheme imc
[DeviceB-isp-portal.com] authorization portal radius-scheme imc
[DeviceB-isp-portal.com] accounting portal radius-scheme imc
[DeviceB-isp-portal.com] quit
```
配置系统缺省的 ISP 域 portal.com，所有接入用户共用此缺省域的认证/授权和计费方法，若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方法。
```
[DeviceB] domain default enable portal.com
```
配置 ACL 3000，只允许访问补丁和病毒服务器。
```
[DeviceB] acl advanced 3000
[DeviceB-acl-ipv4-adv-3000] rule permit ip destination 10.0.12.2 0
[DeviceB-acl-ipv4-adv-3000] rule deny ip destination any
[DeviceB-acl-ipv4-adv-3000] quit
```
配置 ACL 3001，允许所有 IP 地址通过。
```
[DeviceB] acl advanced 3001
[DeviceB-acl-ipv4-adv-3001] rule permit ip destination any
[DeviceB-acl-ipv4-adv-3001] quit
```

4.6 验证配置

用户只能使用 H3C 的 iNode 客户端，进行 Portal 扩展功能认证。用户通过 iNode 客户端，新建 Portal 连接，输入正确的用户名和密码，登录成功。

然后，开始安全检查，安全检查不合格，进入隔离模式，查看设备上 Portal 用户，可看到下发了隔离 ACL 3000。

```
[DeviceB]display portal user all
Total portal users: 1
Username: cc16
  Portal server: newpt
  State: Online
  Authorization ACL: 3000
  VPN instance: --
  MAC             IP                   VLAN    Interface
  0000-0000-0000  192.168.0.2           --      GigabitEthernet2/0/1
```

升级病毒库，版本满足安全策略要求。客户端断开后，重新登录，认证成功后，进行安全检查，客户端提示安全检查合格，设备上查看通过认证的 Portal 用户信息，可见下发了安全 ACL 3001。

```
[DeviceB] display portal user all
Total portal users: 1
Username: portal
```

```
Portal server: newpt
State: Online
Authorization ACL: 3001
VPN instance: --
MAC             IP                    VLAN    Interface
0000-0000-0000  192.168.0.2            --     GigabitEthernet2/0/1
```

4.7 配置文件

- Device A：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.0.11.2 255.255.255.0
#
ip route-static 10.0.10.0 24 10.0.11.1
ip route-static 10.0.12.0 24 10.0.11.1
#
```

- Device B：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.0.11.1 255.255.255.0
portal enable method layer3
portal bas-ip 10.0.11.1
 portal apply web-server newpt
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.0.10.1 255.255.255.0
#
interface GigabitEthernet2/0/3
 port link-mode route
 ip address 10.0.12.1 255.255.255.0
#
ip route-static 192.168.0.0 24 10.0.11.2
#
acl advanced 3000
 rule 0 permit ip destination 10.0.12.2 0
 rule 5 deny ip
#
acl advanced 3001
 rule 0 permit ip
#
```

```
 radius session-control enable
#
radius scheme imc
 primary authentication 10.0.10.2
primary accounting 10.0.10.2
key authentication cipher $c$3$M30nGDQxiOCAxe2AJ9yEZdk8kjoWag==
key accounting cipher $c$3$M23dGDQxiOCAxe2BJ9yEZdk8kjoWag==
 user-name-format without-domain
#
domain portal.com
 authentication portal radius-scheme imc
 authorization portal radius-scheme imc
accounting portal radius-scheme imc
#
 domain default enable portal.com
#
portal web-server newpt
 url http://10.0.10.2:8080/portal
#
portal server newpt
 ip 10.0.10.2 key cipher $c$3$r0VxoIiBrpzju9h2akP4TxyknX8VTuYKfA==
#
```

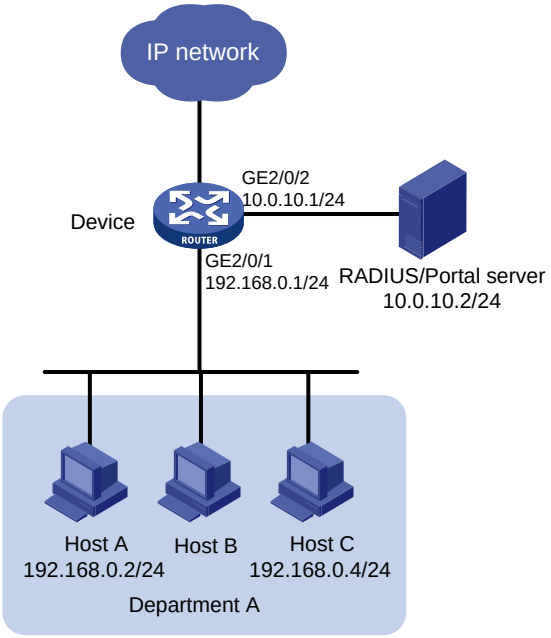
5 直接 Portal 认证配置举例

5.1 组网需求

如图 15 所示，Department A 客户端与接入设备直接相连，采用直接方式的 Portal 认证。

- 采用一台 Portal 服务器承担 Portal 认证服务器和 Portal Web 服务器的职责。
- Department A 下面的用户在通过 Portal 认证前，只能访问 Portal Web 服务器，无法访问内部其它网络或 Internet。用户通过认证后，可以正常访问网络。
- 采用 RADIUS 服务器对 Portal 用户接入进行认证/授权和计费。
- 配置发送给 Portal 认证服务器的 Portal 报文的 BAS-IP 属性。
- 使能 RADIUS session control 功能来监听并接收 RADIUS 服务器发送的 session control 报文。

图15 Portal 特性直接认证配置组网图



5.2 配置思路

- 为了对 Department A 的网络访问进行 Portal 认证，需要在 Device 上配置 Portal 服务器并且使能 Portal 认证。
- 为了实现通过 RADIUS 来对 Portal 用户进行认证/授权和计费，需要在 Device 上配置 RADIUS 方案并指定相应的认证/授权服务器和计费服务器，并将其应用于 Portal 用户所属的认证域。
- 配置系统缺省的 ISP 域，所有接入用户共用此缺省域的认证/授权和计费方法，若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方法。

5.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

5.4 配置注意事项

目前仅支持使用 RADIUS 服务器对 Portal 用户进行认证/授权和计费，同时服务器需要配置路由，可以访问认证端口及用户 IP 地址所在网段。

5.5 配置步骤

说明

请保证在 RADIUS 服务器、Portal 服务器上完成相应的配置，具体配置步骤请参见 3.5.1 RADIUS/Portal server 的配置。其中“增加 Portal 设备”步骤中的选择组网方式改为“直连”，并将 IP 地址改为 192.168.0.1 即可。

5.5.1 Device 的配置

配置接口 GigabitEthernet2/0/1 和 GigabitEthernet2/0/2 的 IP 地址。

```
<Device> system-view
[Device] interface gigabitethernet 2/0/1
[Device-GigabitEthernet2/0/1] ip address 192.168.0.1 24
[Device-GigabitEthernet2/0/1] quit
[Device] interface gigabitethernet 2/0/2
[Device-GigabitEthernet2/0/2] ip address 10.0.10.1 24
[Device-GigabitEthernet2/0/2] quit
```

配置 Portal 认证服务器：名称为 newpt，IP 地址为 10.0.10.2，密钥为明文 portal，监听 Portal 报文的端口为 50100（设备缺省端口号）。

```
[Device] portal server newpt
[Device-portal-server-newpt] ip 10.0.10.2 key simple portal
[Device-portal-server-newpt] port 50100
[Device-portal-server-newpt] quit
```

配置 Portal Web 服务器的 URL 为 http://10.0.10.2:8080/portal。（Portal Web 服务器的 URL 请与实际环境中的 Portal Web 服务器配置保持一致，此处仅为示例）

```
[Device] portal web-server newpt
[Device-portal-websvr-newpt] url http://10.0.10.2:8080/portal
[Device-portal-websvr-newpt] quit
```

在与客户端相连的接口上使能直接方式的 Portal 认证。

```
[Device] interface gigabitethernet2/0/1
[Device-GigabitEthernet2/0/1] portal enable method direct
```

在与客户端相连的接口上设置发送给 Portal 报文中的 BAS-IP 属性值为 192.168.0.1。

```
[Device-GigabitEthernet2/0/1] portal bas-ip 192.168.0.1
```

在与客户端相连的接口上引用 Portal Web 服务器 newpt。

```
[Device-GigabitEthernet2/0/1] portal apply web-server newpt
[Device-GigabitEthernet2/0/1] quit
```

创建名字为 imc 的 RADIUS 方案并进入该方案视图。

```
[Device] radius scheme imc
```

配置 RADIUS 方案主认证服务器及其通信密钥。

```
[Device-radius-imc] primary authentication 10.0.10.2
[Device-radius-imc] primary accounting 10.0.10.2
[Device-radius-imc] key authentication simple expert
[Device-radius-imc] key accounting simple expert
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[Device-radius-imc] user-name-format without-domain
[Device-radius-imc] quit
```

使能 RADIUS session control 功能。

```
[Device] radius session-control enable
```

配置名为 portal.com 的认证域。

```
[Device] domain portal.com
```

配置 ISP 域的 AAA 方法。

```
[Device-isp-portal.com] authentication portal radius-scheme imc
[Device-isp-portal.com] authorization portal radius-scheme imc
[Device-isp-portal.com] accounting portal radius-scheme imc
[Device-isp-portal.com] quit
```

配置系统缺省的 ISP 域 portal.com，所有接入用户共用此缺省域的认证、授权方法，若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方法。

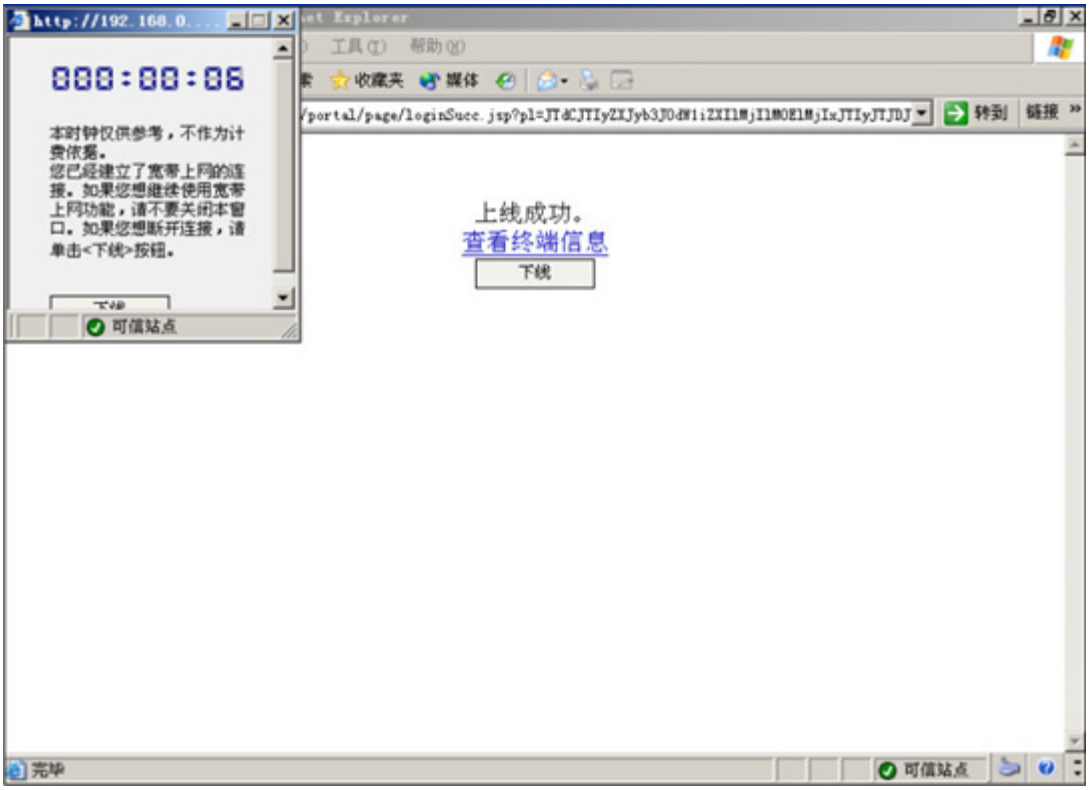
```
[Device] domain default enable portal.com
```

5.5.2 验证配置

用户既可以使用 H3C 的 iNode 客户端，也可以通过网页方式进行 Portal 认证。本例用网页方式进行 Portal 认证。用户在通过认证前，只能访问认证页面 http://10.0.10.2:8080/portal，且发起的 Web 访问请求均被重定向到该认证页面，如图 16。当用户通过认证后，跳转到图 17 界面。

图16 Portal 认证页面

图17 认证成功页面



认证通过后，可通过执行以下显示命令查看 Device 上生成的 Portal 在线用户信息。

```
[DeviceB] display portal user interface gigabitethernet 2/0/1
Total portal users: 1
Username: portal
  Portal server: newpt
  State: Online
  VPN instance: --
  Authorization ACL: None
  VPN instance: --
  MAC              IP               Vlan   Interface
   --------------------------------------------------------------------------
  0015-e9a6-7cfe   192.168.0.2       --     GigabitEthernet2/0/1
```

5.6 配置文件

```
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.0.10.1 255.255.255.0
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 192.168.0.1 255.255.255.0
 portal enable method direct
```

```
 portal bas-ip 192.168.0.1
 portal apply web-server newpt
#
 radius session-control enable
#
radius scheme imc
 primary authentication 10.0.10.2
 primary accounting 10.0.10.2
 key authentication cipher $c$3$M30nGDQxiOCAxe2AJ9yEZdk8kjoWag==
 key accounting cipher $c$3$M23dGDQxiOCAxe2BJ9yEZdk8kjoWag==
 user-name-format without-domain
#
domain portal.com
 authentication portal radius-scheme imc
 authorization portal radius-scheme imc
accounting portal radius-scheme imc
#
domain default enable portal.com
#
portal web-server newpt
 url http://10.0.10.2:8080/portal
#
portal server newpt
 ip 10.0.10.2 key cipher $c$3$r0VxoIiBrpzju9h2akP4TxyknX8VTuYKfA==
#
```

6 相关资料

- H3C SR6600 SR6600-X 路由器 安全配置指导-R7607
- H3C SR6600 SR6600-X 路由器 安全命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

POS 接口配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1

2 配置前提 1

3 POS 接口使用 PPP 协议光纤直连配置举例 1

3.1 组网需求 1

3.2 配置思路 2

3.3 使用版本 2

3.4 配置注意事项 2

3.5 配置步骤 2

3.5.1 Router A 的配置 2

3.5.2 Router B 的配置 3

3.5.3 Router C 的配置 3

3.6 验证配置 4

3.7 配置文件 5

4 POS 接口使用 HDLC 协议光纤直连配置举例 6

4.1 组网需求 6

4.2 使用版本 6

4.3 配置注意事项 6

4.4 配置步骤 7

4.4.1 Router A 的配置 7

4.4.2 Router B 的配置 7

4.5 验证配置 8

4.6 配置文件 8

5 POS 接口经帧中继网互连配置举例 9

5.1 组网需求 9

5.2 使用版本 9

5.3 配置步骤 9

5.3.1 Router A 的配置 9

5.3.2 Router B 的配置 10

5.3.3 Router C 的配置 10

5.4 验证配置 11

5.5 配置文件 12

6 相关资料 ·····13

1 简介

本文档介绍了使用 POS 接口的配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文假设您已了解 POS、FR、SDH、SONET、PPP 协议和 HDLC 特性。

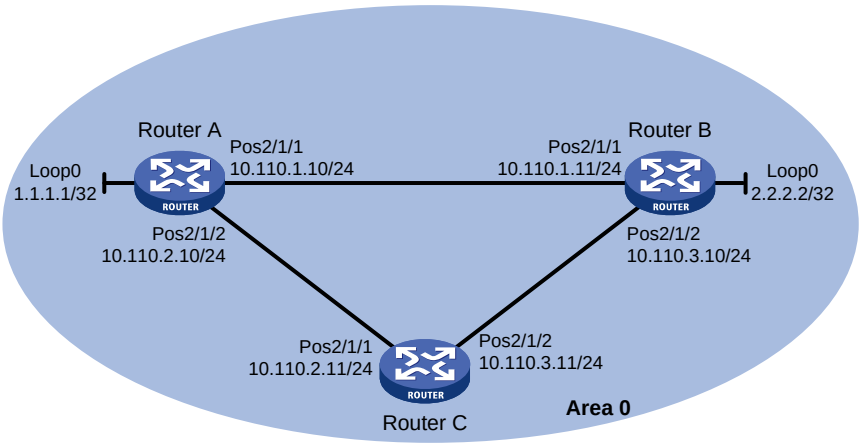
3 POS 接口使用 PPP 协议光纤直连配置举例

3.1 组网需求

分别用一对（接收、发送）单模光纤直接连接路由器 Router A 和 Router B、Router A 和 Router C 以及 Router B 和 Router C 的 POS 接口，通过 PPP 互连。每台设备上使用 OSPF 协议与其他两台设备互相连通。实现以下需求：

- 当 Router A 和 Router B 链路完整时，从 Router A 到 Router B 的流量转发路径为 Router A—>Router B。
- 当 Router A 收到对端 Router B 发送的 MS-RDI 信号后，不立即关闭 POS 接口，在 100ms 内 MS-RDI 信号仍未结束，则自动将接口的物理状态设置为 down。
- 当 Router A 的 POS2/1/1 端口 down 后，从 Router A 到 Router B 的流量转发路径为 Router A—>Router C—>Router B。

图1 POS 接口使用 PPP 协议光纤直连配置组网图



3.2 配置思路

- 为了实现收到对端发送的 MS-RDI 信号后，会自动将接口的物理状态设置为 down，需要配置当前接口的告警联动动作。并且设备收到对端发送的 MS-RDI 信号时，认为发生了 RDI 告警。
- 为了实现当收到对端发送的 MS-RDI 信号后，不立即关闭 POS 接口，在 100ms 内 MS-RDI 信号仍未结束才自动将接口的物理状态设置为 down，需要配置接口物理连接状态抑制时间为 100ms。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置注意事项

当两台路由器的 POS 接口直接相连时，应配置一端使用主时钟模式，另一端使用从时钟模式。

3.5 配置步骤

3.5.1 Router A 的配置

(1) 配置 Router A 接口

配置 POS2/1/1 接口的 IP 地址，链路类型采用 PPP。

```
<RouterA> system-view
[RouterA] interface pos 2/1/1
[RouterA-Pos2/1/1] ip address 10.110.1.10 255.255.255.0
[RouterA-Pos2/1/1] link-protocol ppp
```

配置 POS2/1/1 接口时钟模式为主时钟模式。

```
[RouterA-Pos2/1/1] clock master
```

配置当 POS2/1/1 接口检测到 RDI 告警时，自动将接口的物理状态设置为 down。

```
[RouterA-Pos2/1/1] alarm-detect rdi action link-down
```

设置 POS 接口物理连接状态抑制时间为 100 毫秒，即在 POS 接口发生 up 或 down 的时候，需要经过 100 毫秒后，接口状态才能变为 up 或 down。

```
[RouterA-Pos2/1/1] link-delay msec 100
[RouterA-Pos2/1/1] quit
```

配置 POS2/1/2 接口的 IP 地址，链路类型采用 PPP。

```
[RouterA] interface pos 2/1/2
[RouterA-Pos2/1/2] ip address 10.110.2.10 255.255.255.0
[RouterA-Pos2/1/2] link-protocol ppp
```

配置 POS2/1/2 接口时钟模式为主时钟模式。

```
[RouterA-Pos2/1/2] clock master
[RouterA-Pos2/1/2] quit
```

(2) 配置 OSPF

```
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.110.1.0 0.0.0.255
```

```
[RouterA-ospf-1-area-0.0.0.0] network 10.110.2.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

3.5.2 Router B 的配置

(1) 配置 Router B 的接口

配置 POS2/1/1 接口的 IP 地址，链路类型采用 PPP，时钟模式采用缺省的从时钟模式。

```
<RouterB> system-view
[RouterB] interface pos 2/1/1
[RouterB-Pos2/1/1] ip address 10.110.1.11 255.255.255.0
[RouterB-Pos2/1/1] link-protocol ppp
[RouterB-Pos2/1/1] quit
```

配置 POS2/1/2 接口的 IP 地址，链路类型采用 PPP，时钟模式采用缺省的从时钟模式。

```
[RouterB] interface pos 2/1/2
[RouterB-Pos2/1/2] ip address 10.110.3.10 255.255.255.0
[RouterB-Pos2/1/2] link-protocol ppp
[RouterB-Pos2/1/2] quit
```

(2) 配置 OSPF

```
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 10.110.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 10.110.3.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

3.5.3 Router C 的配置

(1) 配置 Router C 的接口

配置 POS2/1/1 接口的 IP 地址，链路类型采用 PPP，时钟模式采用缺省的从时钟模式。

```
<RouterC> system-view
[RouterC] interface pos 2/1/1
[RouterC-Pos2/1/1] ip address 10.110.2.11 255.255.255.0
[RouterC-Pos2/1/1] link-protocol ppp
[RouterC-Pos2/1/1] quit
```

配置 POS2/1/1 接口的 IP 地址，链路类型采用 PPP。

```
[RouterC] interface pos 2/1/2
[RouterC-Pos2/1/2] ip address 10.110.3.11 255.255.255.0
[RouterC-Pos2/1/2] link-protocol ppp
```

配置 POS2/1/2 接口时钟模式为主时钟模式。

```
[RouterA-Pos2/1/2] clock master
[RouterC-Pos2/1/2] quit
```

(2) 配置 OSPF

```
[RouterC] ospf
[RouterC-ospf-1] area 0
```

```
[RouterC-ospf-1-area-0.0.0.0] network 10.110.2.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 10.110.3.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

3.6 验证配置

完成以上配置后，在 Router A 上查看 2.2.2.2/32 的路由信息，可以看出 Router A 和 Router B 是通过直连链路进行通信的。

```
<RouterA> display ip routing-table 2.2.2.2 verbose

Summary Count : 1

Destination: 2.2.2.2/32
   Protocol: OSPF             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
      NBRID: 0x26000002          LastAs: 0
     AttrID: 0xffffffff         Neighbor: 0.0.0.0
      Flags: 0x1008c         OrigNextHop: 10.110.1.11
      Label: NULL            RealNextHop: 10.110.1.11
    BkLabel: NULL              BkNextHop: N/A
  Tunnel ID: Invalid           Interface: Pos2/1/1
BkTunnel ID: Invalid         BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A
```

当 Router A 的 POS2/1/1 端口在 100 毫秒内持续收到 RDI 告警后，改端口状态变成 Down。

```
<RouterA> display interface pos 2/1/1 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link   Protocol    Primary IP         Description
Pos2/1/1             DOWN   DOWN        --
```

当 Router A 的 POS2/1/1 端口 down 时，查看 2.2.2.2/32 的路由信息，可以看出 Router A 和 Router B 已经切换到 Router C 进行通信。

```
<RouterA> display ip routing-table 2.2.2.2 verbose

Summary Count : 1

Destination: 2.2.2.2/32
   Protocol: OSPF             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
      NBRID: 0x26000002          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c         OrigNextHop: 10.110.2.11
      Label: NULL            RealNextHop: 10.110.2.11
    BkLabel: NULL              BkNextHop: N/A
  Tunnel ID: Invalid           Interface: Pos2/1/2
BkTunnel ID: Invalid         BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A
```

3.7 配置文件

- Router A：

```
#
interface Pos2/1/1
 link-protocol ppp
 clock master
 ip address 10.110.1.10 255.255.255.0
 alarm-detect rdi action link-down
 link-delay msec 100
#
interface Pos2/1/2
 link-protocol ppp
 clock master
 ip address 10.110.1.10 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.110.1.0 0.0.0.255
  network 10.110.2.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
#
```

- Router B：

```
#
interface Pos2/1/1
 link-protocol ppp
 ip address 10.110.1.11 255.255.255.0
#
interface Pos2/1/2
 link-protocol ppp
 ip address 10.110.3.10 255.255.255.0
#
ospf 1
 area 0.0.0.0
```

```
  network 10.110.1.0 0.0.0.255
  network 10.110.3.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
#
```

- Router C：

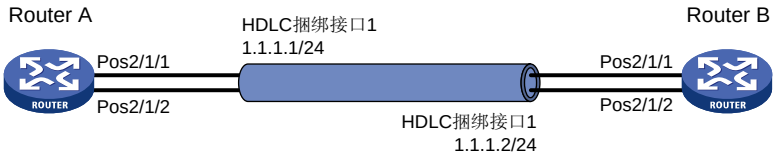
```
#
interface Pos2/1/1
 link-protocol ppp
ip address 10.110.1.10 255.255.255.0
#
interface Pos2/1/2
 link-protocol ppp
clock master
 ip address 10.110.1.10 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 10.110.3.0 0.0.0.255
#
```

4 POS 接口使用 HDLC 协议光纤直连配置举例

4.1 组网需求

为了增加 Router A 和 Router B 之间的链路带宽，并提高连接可靠性，在设备之间建立 HDLC 捆绑的逻辑链路。

图2 POS 接口使用 HDLC 协议光纤直连配置举例组网图



4.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.3 配置注意事项

- 只有物理 POS 接口可以加入 HDLC 捆绑。
- 一个接口只能加入一个 HDLC 捆绑，如果需要加入其他 HDLC 捆绑，必须先退出原来的 HDLC 捆绑。
- 加入 HDLC 捆绑的接口封装的链路层协议必须为 HDLC。接口加入 HDLC 捆绑之后不允许修改链路层协议。

- 当两台路由器的 POS 接口直接相连时，应配置一端使用主时钟模式，另一端使用从时钟模式；

4.4 配置步骤

4.4.1 Router A 的配置

创建 HDLC 捆绑接口 1，并配置 IP 地址。

```
<RouterA> system-view
[RouterA] interface hdlc-bundle 1
[RouterA-HDLC-bundle1] ip address 1.1.1.1 24
[RouterA-HDLC-bundle1] quit
```

配置 POS2/1/1 接口的时钟模式采用主时钟模式，链路类型采用 HDLC。

```
[RouterA] interface pos 2/1/1
[RouterA-Pos2/1/1] clock master
[RouterA-Pos2/1/1] link-protocol hdlc
```

配置 POS2/1/1 接口加入到 HDLC 捆绑 1。

```
[RouterA-Pos2/1/1] bundle id 1
[RouterA-Pos2/1/1] quit
```

配置 POS2/1/2 接口的时钟模式采用主时钟模式，链路类型采用 HDLC。

```
[RouterA] interface pos 2/1/2
[RouterA-Pos2/1/2] clock master
[RouterA-Pos2/1/2] link-protocol hdlc
```

配置 POS2/1/2 接口加入到 HDLC 捆绑 1。

```
[RouterA-Pos2/1/2] bundle id 1
[RouterA-Pos2/1/2] quit
```

4.4.2 Router B 的配置

创建 HDLC 捆绑接口 1，并配置 IP 地址。

```
<RouterB> system-view
[RouterB] interface hdlc-bundle 1
[RouterB-HDLC-bundle1] ip address 1.1.1.2 24
[RouterB-HDLC-bundle1] quit
```

配置 POS2/1/1 接口的链路类型为 HDLC，时钟模式采用缺省的从时钟模式。

```
[RouterB] interface pos 2/1/1
[RouterB-Pos2/1/1] link-protocol hdlc
```

配置 POS2/1/1 接口加入到 HDLC 捆绑 1。

```
[RouterB-Pos2/1/1] bundle id 1
[RouterB-Pos2/1/1] quit
```

配置 POS2/1/2 接口的链路类型为 HDLC，时钟模式采用缺省的从时钟模式。

```
[RouterB] interface pos 2/1/2
[RouterB-Pos2/1/2] link-protocol hdlc
```

配置 POS2/1/2 接口加入到 HDLC 捆绑 1。

```
[RouterB-Pos2/1/2] bundle id 1
[RouterB-Pos2/1/2] quit
```

4.5 验证配置

Router A 和 Router B 的 HDLC 捆绑接口能够互相 Ping 通。

```
[RouterA] ping –a 1.1.1.1 1.1.1.2
Ping 1.1.1.2 (1.1.1.2) from 1.1.1.1: 56 data bytes, press CTRL_C to break
56 bytes from 1.1.1.2: icmp_seq=0 ttl=255 time=0.000 ms
56 bytes from 1.1.1.2: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 1.1.1.2: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 1.1.1.2: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 1.1.1.2: icmp_seq=4 ttl=255 time=0.000 ms

--- Ping statistics for 1.1.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.000/0.000/0.000 ms
```

在 Router A 或 Router B 上执行 **`display bundle hdlc-bundle`** 命令，可以看到 HDLC 捆绑接口 1 的捆绑信息。以 Router A 的显示为例。

```
[RouterA] display bundle hdlc-bundle 1 slot 2
Bundle: HDLC-bundle1, slot 2
  Selected members: 2, Total bandwidth: 1244160 kbps
  Member              State               Bandwidth(kbps)     Priority
  Pos2/1/1            Selected            622080              32768
  Pos2/1/2            Selected            622080              32768
```

上述信息表明，POS2/1/1 和 POS2/1/2 都处于选中状态，可以进行流量的负载分担；HDLC 捆绑的带宽为 1244160 kbps，是两个 POS 接口的带宽之和；当其中一个 POS 接口出现故障（如 Router A 的 POS2/1/1 端口 down）时，流量可以通过另一个 POS 接口发送，提高了链路的连接可靠性。

4.6 配置文件

- Router A：

```
#
interface pos 2/1/1
 link-protocol hdlc
 clock master
 bundle id 1
#
interface pos 2/1/2
 link-protocol hdlc
 clock master
 bundle id 1
#
interface hdlc-bundle 1
 ip address 1.1.1.1 24
#
```

- Router B：

```
#
interface pos 2/1/1
```

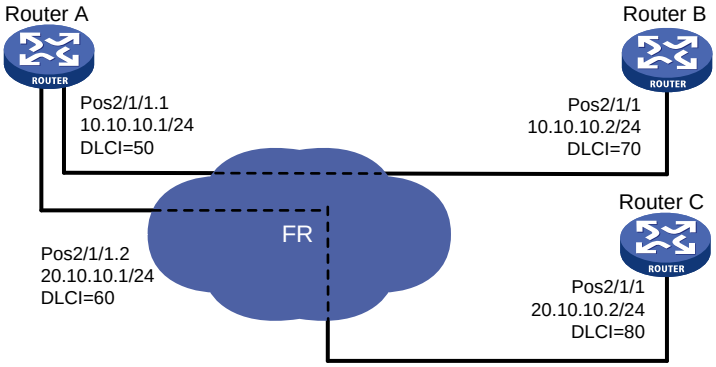
```
 link-protocol hdlc
 bundle id 1
#
interface pos 2/1/2
 link-protocol hdlc
 bundle id 1
#
interface hdlc-bundle 1
 ip address 1.1.1.2 24
#
```

5 POS 接口经帧中继网互连配置举例

5.1 组网需求

- 设备（Router A、Router B、Router C）使用 POS 接口通过公用帧中继网络互连，且作为用户设备，工作在帧中继的 DTE 方式。
- Router A 利用帧中继子接口连接处于不同网段的 Router B 和 Router C，使 Router A 分别与 Rouer B 和 Router C 通信。

图3 POS 接口使用 HDLC 协议光纤直连配置举例组网图



5.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

5.3 配置步骤

5.3.1 Router A 的配置

配置 POS2/1/1 接口的链路类型为 FR。

```
<RouterA> system-view
[RouterA] interface pos 2/1/1
[RouterA-Pos2/1/1] link-protocol fr
```

配置帧中继接口 POS2/1/1 类型为 DTE。

```
[RouterA-Pos2/1/1] fr interface-type dte
[RouterA-Pos2/1/1] quit
```
创建 POS2/1/1 接口的子接口 1，并为其配置 IP 地址。
```
[RouterA] interface pos 2/1/1.1
[RouterA-Pos2/1/1.1] ip address 10.10.10.1 255.255.255.0
```
为帧中继接口 POS2/1/1.1 创建一条 DLCI 为 50 的虚电路。
```
[RouterA-Pos2/1/1.1] fr dlci 50
[RouterA-Pos2/1/1.1-fr-dlci-50] quit
```
接口 POS2/1/1.1 连接的对端路由器的 IP 地址为 10.10.10.2，在本地 POS2/1/1.1 接口上有一条 DLCI 为 50 的虚电路连接到该路由器。
```
[RouterA-Pos2/1/1.1] fr map ip 10.10.10.2 50
[RouterA-Pos2/1/1.1] quit
```
创建 POS2/1/1 接口的子接口 2，并为其配置 IP 地址。
```
[RouterA] interface pos 2/1/1.2
[RouterA-Pos2/1/1.2] ip address 20.10.10.1 255.255.255.0
```
为帧中继接口 POS2/1/1.2 创建一条 DLCI 为 60 的虚电路。
```
[RouterA-Pos2/1/1.2] fr dlci 60
[RouterA-Pos2/1/1.2-fr-dlci-60] quit
```
接口 POS2/1/1.2 连接的对端路由器的 IP 地址为 20.10.10.2，在本地 POS2/1/1.2 接口上有一条 DLCI 为 60 的虚电路连接到该路由器。
```
[RouterA-Pos2/1/1.2] fr map ip 20.10.10.2 60
[RouterA-Pos2/1/1.2] quit
```

5.3.2 Router B 的配置

配置 POS2/1/1 接口的链路类型为 FR。
```
<RouterB> system-view
[RouterB] interface pos 2/1/1
[RouterB-Pos2/1/1] link-protocol fr
```
配置帧中继接口 POS2/1/1 类型为 DTE。
```
[RouterB-Pos2/1/1] fr interface-type dte
```
配置 POS2/1/1 接口的 IP 地址为 10.10.10.2/24。
```
[RouterB-Pos2/1/1] ip address 10.10.10.2 255.255.255.0
```
为帧中继接口 POS2/1/1 创建一条 DLCI 为 70 的虚电路。
```
[RouterB-Pos2/1/1] fr dlci 70
[RouterB-Pos2/1/1-fr-dlci-70] quit
```
接口 POS2/1/1 连接的对端路由器的 IP 地址为 10.10.10.1，在本地 POS 2/1/1 接口上有一条 DLCI 为 70 的虚电路连接到该路由器。
```
[RouterB-Pos2/1/1] fr map ip 10.10.10.1 70
[RouterB-Pos2/1/1] quit
```

5.3.3 Router C 的配置

配置 POS2/1/1 接口的链路类型为 FR。
```
<RouterC> system-view
```

```
[RouterC] interface pos 2/1/1
[RouterC-Pos2/1/1] link-protocol fr
```
配置帧中继接口 POS 2/1/1 类型为 DTE。
```
[RouterC-Pos2/1/1] fr interface-type dte
```
配置 POS2/1/1 接口的 IP 地址为 20.10.10.2/24。
```
[RouterC-Pos2/1/1] ip address 20.10.10.2 255.255.255.0
```
为帧中继接口 POS2/1/1 创建一条 DLCI 为 80 的虚电路。
```
[RouterC-Pos2/1/1] fr dlci 80
[RouterC-Pos2/1/1-fr-dlci-70] quit
```
接口 POS2/1/1 连接的对端路由器的 IP 地址为 20.10.10.1，在本地 POS2/1/1 接口上有一条 DLCI 为 80 的虚电路连接到该路由器。
```
[RouterC-Pos2/1/1] fr map ip 20.10.10.1 80
[RouterC-Pos2/1/1] quit
```

5.4 验证配置

在 Router A 上通过 **`display fr pvc`** 命令可以查看接口 POS2/1/1 的 PVC 信息，发现 PVC 的状态为 Active。
```
[RouterA] display fr pvc
PVC information for interface Pos2/1/1 (DTE, physical UP)
  DLCI: 50, Type: Dynamic, Pos2/1/1.1
    Encapsulation: IETF
    Creation time: 2017/02/19 14:34:42, Status: Active
    Input: 2 packets, 60 bytes, 0 dropped
    Output: 2 packets, 60 bytes, 0 dropped
  DLCI: 60, Type: Dynamic, Pos2/1/1.2
    Encapsulation: IETF
    Creation time: 2017/02/19 15:03:35, Status: Active
    Input: 2 packets, 60 bytes, 0 dropped
    Output: 2 packets, 60 bytes, 0 dropped
```
在 Router A 上通过 **`display fr map`** 命令可以查看帧中继地址映射表。
```
[RouterA] display fr map
Map information for interface Pos2/1/1 (DTE)
  DLCI: 50, IP 10.10.10.2, Pos2/1/1.1
    Creation time: 2017/02/19 14:34:42, Status: Active
  DLCI: 60, IP 20.10.10.2, Pos2/1/1.2
    Creation time: 2017/02/19 15:03:35, Status: Active
```
Router A 和 Router B 可以互相 ping 通对方。
```
[RouterB] ping 10.10.10.1
Ping 10.10.10.1 (10.10.10.1): 56 data bytes, press CTRL_C to break
56 bytes from 10.10.10.1: icmp_seq=0 ttl=255 time=76.007 ms
56 bytes from 10.10.10.1: icmp_seq=1 ttl=255 time=8.790 ms
56 bytes from 10.10.10.1: icmp_seq=2 ttl=255 time=1.630 ms
56 bytes from 10.10.10.1: icmp_seq=3 ttl=255 time=0.841 ms
56 bytes from 10.10.10.1: icmp_seq=4 ttl=255 time=1.012 ms
```

```
--- Ping statistics for 10.10.10.1 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.841/17.656/76.007/29.326 ms
```

Router A 和 Router C 可以互相 ping 通对方。

```
[RouterC] ping 20.10.10.1
Ping 20.10.10.1 (20.10.10.1): 56 data bytes, press CTRL_C to break
56 bytes from 20.10.10.1: icmp_seq=0 ttl=255 time=10.007 ms
56 bytes from 20.10.10.1: icmp_seq=1 ttl=255 time=8.790 ms
56 bytes from 20.10.10.1: icmp_seq=2 ttl=255 time=1.630 ms
56 bytes from 20.10.10.1: icmp_seq=3 ttl=255 time=0.841 ms
56 bytes from 20.10.10.1: icmp_seq=4 ttl=255 time=1.012 ms

--- Ping statistics for 20.10.10.1 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.841/17.656/76.007/29.326 ms
```

5.5 配置文件

- Router A：

```
#
interface Pos2/1/1
 link-protocol fr
 fr interface-type dte
#
interface Pos2/1/1.1
 link-protocol fr
 ip address 10.10.10.1 255.255.255.0
 fr map ip 10.10.10.2 50
  fr dlci 50
#
interface Pos2/1/1.2
 link-protocol fr
 ip address 20.10.10.1 255.255.255.0
 fr map ip 20.10.10.2 50
  fr dlci 60
```

- Router B：

```
#
interface Pos2/1/1
 link-protocol fr
 fr interface-type dte
 ip address 10.10.10.2 255.255.255.0
 fr map ip 10.10.10.1 70
  fr dlci 70
#
```

- Router C：

```
#
interface Pos2/1/1
```

```
 link-protocol fr
 fr interface-type dte
 ip address 20.10.10.2 255.255.255.0
 fr map ip 20.10.10.1 80
  fr dlci 80
#
```

6 相关资料

- H3C SR6600 SR6600-X 路由器 接口管理配置指导-R7607
- H3C SR6600 SR6600-X 路由器 接口管理命令参考-R7607
- H3C SR6600 SR6600-X 路由器 二层技术-广域网接入配置指导-R7607
- H3C SR6600 SR6600-X 路由器 二层技术-广域网接入命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

PPP 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目　录

1 特性简介 ····· 0
2 配置前提 ····· 0
3 MP+CHAP 配置举例 ····· 0
3.1 组网需求 ····· 0
3.2 使用版本 ····· 0
3.3 配置注意事项 ····· 0
3.4 配置步骤 ····· 0
3.4.1 配置 Device A ····· 0
3.4.2 配置 Device B ····· 1
3.5 验证配置 ····· 2
3.6 配置文件 ····· 3
4 PPPoE Server 通过远端 DHCP 服务器为用户分配 IP 地址配置举例 ····· 4
4.1 组网需求 ····· 4
4.2 使用版本 ····· 4
4.3 配置注意事项 ····· 4
4.4 配置步骤 ····· 5
4.5 配置文件 ····· 13
5 相关资料 ····· 14

1 特性简介

本文档介绍 PPP 协议相关的典型配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

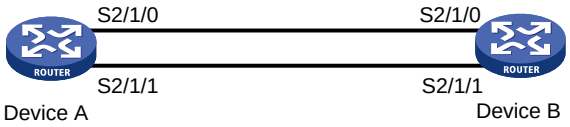
本文档假设您已了解了 PPP、MP、PPPoE、DHCP 协议。

3 MP+CHAP 配置举例

3.1 组网需求

如图 1 所示，设备 Device A 和 Device B 的 Serial2/1/0 和 Serial2/1/1 分别对应连接，使用 MP-Group 的方式建立 MP 链路，每个 PPP 链路使用 CHAP 进行认证。

图1 终端描述符捆绑 MP 组网图



3.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.3 配置注意事项

- 配置采用 CHAP 认证时两端的用户名和密码必须一致。
- Serial 接口配置完成之后，需要执行 **undo shutdown** 命令开启接口。
- 创建 PPP 用户需要在 **local-user** 命令的 **class** 关键字后面选择 **network** 参数。

3.4 配置步骤

3.4.1 配置 Device A

(1) 为 Device B 创建本地用户，设置本地用户的服务类型为 PPP。

```
<DeviceA> system-view
```

```
[DeviceA] local-user userb class network
[DeviceA-luser-network-userb] password simple hello
[DeviceA-luser-network-userb] service-type ppp
[DeviceA-luser-network-userb] quit
```

(2) 配置串口 Serial2/1/0，通过缺省的 ISP 域 system 对 Rotuer B 进行 CHAP 认证。

```
[DeviceA] interface serial 2/1/0
[DeviceA-Serial2/1/0] link-protocol ppp
[DeviceA-Serial2/1/0] ppp authentication-mode chap domain system
[DeviceA-Serial2/1/0] quit
```

(3) 配置串口 Serial2/1/1，通过缺省的 ISP 域 system 对 Rotuer B 进行 CHAP 认证。

```
[DeviceA] interface serial 2/1/1
[DeviceA-Serial2/1/1] link-protocol ppp
[DeviceA-Serial2/1/1] ppp authentication-mode chap domain system
[DeviceA-Serial2/1/1] quit
```

(4) 在系统缺省的 ISP 域 system 下，配置 PPP 用户使用本地认证方案。

```
[DeviceA] domain system
[DeviceA-isp-system] authentication ppp local
```

(5) 创建 MP-group 接口，配置相应的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface mp-group 2/0/0
[DeviceA-MP-group2/0/0] ip address 1.1.1.1 24
[DeviceA-MP-group2/0/0] quit
```

(6) 配置串口 Serial2/1/0 加入 MP-Group 3/0/1 并开启接口。

```
[DeviceA] interface serial 2/1/0
[DeviceA-Serial2/1/0] ppp mp mp-group 2/0/0
[DeviceA-Serial2/1/0] shutdown
[DeviceA-Serial2/1/0] undo shutdown
[DeviceA-Serial2/1/0] quit
```

(7) 配置串口 Serial2/1/1 加入 MP-Group 3/0/1 并开启接口。

```
[DeviceA] interface serial 2/1/1
[DeviceA-Serial2/1/1] ppp mp mp-group 2/0/0
[DeviceA-Serial2/1/1] shutdown
[DeviceA-Serial2/1/1] undo shutdown
[DeviceA-Serial2/1/1] quit
```

3.4.2 配置 Device B

(1) 配置串口 Serial2/1/0，封装的链路层协议为 PPP，并配置采用 CHAP 认证时 Device B 的用户名和设置缺省的 CHAP 认证密码。

```
<DeviceB> system-view
[DeviceB] interface serial 2/1/0
[DeviceB-Serial2/1/0] link-protocol ppp
[DeviceB-Serial2/1/0] ppp chap user userb
[DeviceB-Serial2/1/0] ppp chap password simple hello
[DeviceB-Serial2/1/0] quit
```

(2) 配置串口 Serial2/1/1，封装的链路层协议为 PPP，并配置采用 CHAP 认证时 Device B 的用户名和设置缺省的 CHAP 认证密码。

```
[DeviceB] interface serial 2/1/1
[DeviceB-Serial2/1/1] link-protocol ppp
[DeviceB-Serial2/1/1] ppp chap user userb
[DeviceB-Serial2/1/1] ppp chap password simple hello
[DeviceB-Serial2/1/1] quit
```

(3) 创建 MP-group 接口，配置相应的 IP 地址。

```
[DeviceB] interface mp-group 2/0/0
[DeviceB-MP-group2/0/0] ip address 1.1.1.2 24
[DeviceB-MP-group2/0/0] quit
```

(4) 配置串口 Serial2/1/0 加入 MP-Group 3/0/1 并开启接口。

```
[DeviceB] interface serial 2/1/0
[DeviceB-Serial2/1/0] link-protocol ppp
[DeviceB-Serial2/1/0] ppp mp mp-group 2/0/0
[DeviceB-Serial2/1/0] shutdown
[DeviceB-Serial2/1/0] undo shutdown
[DeviceB-Serial2/1/0] quit
```

(5) 配置串口 Serial2/1/1 加入 MP-Group 3/0/1 并开启接口。

```
[DeviceB] interface serial 2/1/1
[DeviceB-Serial2/1/1] link-protocol ppp
[DeviceB-Serial2/1/1] ppp mp mp-group 2/0/0
[DeviceB-Serial2/1/1] shutdown
[DeviceB-Serial2/1/1] undo shutdown
[DeviceB-Serial2/1/1] quit
```

3.5 验证配置

(1) 在 Device A 上查看 MP 的相关信息。

```
[DeviceA] display ppp mp
Template: MP-group2/0/0
max-bind: 16, fragment: enabled, min-fragment: 128
  Master link: MP-group2/0/0, Active members: 2, Bundle Multilink
  Peer's endPoint descriptor: MP-group2/0/0
  Sequence format: long (rcv)/long (sent)
  Bundle Up Time: 2017/07/22  16:51:40:835
  0 lost fragments, 5 reordered, 0 unassigned, 0 interleaved
  Sequence: 4 (rcv)/5 (sent)
  Active member channels: 2 members
       Serial2/1/0              Up-Time:2017/07/22  16:51:40:836
       Serial2/1/1              Up-Time:2017/07/22  16:51:53:542
```

(2) 在 Device A 上查看 MP-group2/0/0 接口的相关信息。

```
[DeviceA] display interface mp-group 2/0/0
MP-group2/0/0
Current state: UP
Line protocol state: UP
Description: MP-group2/0/0 Interface
```

```
Bandwidth: 128kbps
Maximum Transmit Unit: 1500
Hold timer: 10 seconds
Internet Address is 1.1.1.1/24 Primary
Link layer protocol: PPP
LCP: opened, MP: opened, IPCP: opened
Physical: MP, baudrate: 128000 bps
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 1 bytes/sec, 8 bits/sec, 0 packets/sec
Last 300 seconds output rate: 1 bytes/sec, 8 bits/sec, 0 packets/sec
Input: 8 packets, 466 bytes, 0 drops
Output: 8 packets, 456 bytes, 0 drops
```

(3) 在 DeviceA 上 ping 对端 IP 地址。

```
[DeviceA] ping 1.1.1.2
Ping 1.1.1.2 (1.1.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.1.2: icmp_seq=0 ttl=255 time=25.749 ms
56 bytes from 1.1.1.2: icmp_seq=1 ttl=255 time=25.751 ms
56 bytes from 1.1.1.2: icmp_seq=2 ttl=255 time=25.521 ms
56 bytes from 1.1.1.2: icmp_seq=3 ttl=255 time=25.512 ms
56 bytes from 1.1.1.2: icmp_seq=4 ttl=255 time=25.599 ms
--- Ping statistics for 1.1.1.2 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 25.512/25.626/25.751/0.105 ms
<DeviceA>%Jul 22 17:08:22:460 2017 DeviceA PING/6/PING_STATISTICS: Ping statisti
cs for 1.1.1.2: 5 packets transmitted, 5 packets received, 0.0% packet loss, rou
nd-trip min/avg/max/std-dev = 25.512/25.626/25.751/0.105 ms.
```

3.6 配置文件

- Device A：

```
#
interface Serial2/1/0
 ppp authentication-mode chap domain system
 ppp mp MP-group2/0/0
#
interface Serial2/1/1
 ppp authentication-mode chap domain system
 ppp mp MP-group2/0/0
#
interface MP-group2/0/0
 ip address 1.1.1.1 255.255.255.0
#
local-user 123 class network
 password cipher $c$3$5ulb/vg58eiBIm5EnilnsZ2cS2Cmwg==
 service-type ppp
```

```
 authorization-attribute user-role network-operator
#
```

- Device B：

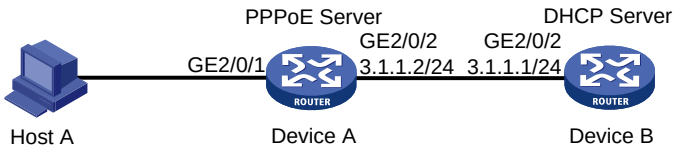
```
#
interface Serial2/1/0
 ppp chap password cipher $c$3$4kD4T3bLZ/lngijhEKIS70/oTbNSkw==
 ppp chap user 123
 ppp mp MP-group2/0/0
#
interface Serial2/1/1
 ppp chap password cipher $c$3$mVlcV3W+YQBgmxKePKpZV9tTcaFhXg==
 ppp chap user 123
 ppp mp MP-group2/0/0
#
interface MP-group2/0/0
 ip address 1.1.1.2 255.255.255.0
#
```

4 PPPoE Server 通过远端 DHCP 服务器为用户分配 IP 地址配置举例

4.1 组网需求

如图 2 所示，某小区通过 PPPoE 方式拨号上网，小区用户的主机 Host A 通过 PPPoE 方式拨号到 Device A 上，Device A 作为小区的 PPPoE Server 为用户提供接入控制和 CHAP 认证服务，并且通过 Device B 为主机分配 IP 地址。

图2 PPPoE Server 配置组网图



4.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.3 配置注意事项

- 配置采用 CHAP 认证时两端的用户名和密码必须一致。
- 创建 PPP 用户需要在 **local-user** 命令的 **class** 关键字后面选择 **network** 参数。

4.4 配置步骤

1. 配置 Device A

(1) 配置 GigabitEthernet2/0/1 接口 IP 地址为 10.1.1.1，GigabitEthernet2/0/2 接口 IP 地址为 3.1.1.2。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 10.1.1.1 24
[DeviceA-GigabitEthernet2/0/1] quit
[DeviceA] interface gigabitethernet 2/0/2
[DeviceA-GigabitEthernet2/0/2] ip address 3.1.1.2 24
[DeviceA-GigabitEthernet2/0/2] quit
```

(2) 配置虚拟模板接口 10 的参数，采用 CHAP 认证对端，使用 DHCP 地址池 pool1 为用户分配 IP 地址，配置本端的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface virtual-template 10
[DeviceA-Virtual-Template10] ppp authentication-mode chap domain system
[DeviceA-Virtual-Template10] ip address 1.1.1.1 32
[DeviceA-Virtual-Template10] quit
```

(3) 在 GigabitEthernet2/0/1 接口上启用 PPPoE Server 协议，将该以太网接口与虚拟模板接口 10 绑定。

```
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] pppoe-server bind virtual-template 10
[DeviceA-GigabitEthernet2/0/1] quit
```

(4) 启用 DHCP 服务。

```
[DeviceA] dhcp enable
```

(5) 启用 DHCP 中继的用户地址表项记录功能。

```
[DeviceA] dhcp relay client-information record
```

(6) 创建中继地址池 pool1，指定匹配该地址池的 DHCPv4 客户端所在的网段地址，并指定中继地址池对应的 DHCP 服务器地址。

```
[DeviceA] dhcp server ip-pool pool1
[DeviceA-dhcp-pool-pool1] gateway-list 2.2.2.2 export-route
[DeviceA-dhcp-pool-pool1] remote-server 3.1.1.1
[DeviceA-dhcp-pool-pool1] quit
```

(7) 配置与 DHCP 服务器连接的 GigabitEthernet2/0/2 接口的 IP 地址。

```
[DeviceA] interface gigabitethernet 2/0/2
[DeviceA-GigabitEthernet2/0/2] ip address 3.1.1.2 24
[DeviceA-GigabitEthernet2/0/2] quit
```

(8) 配置 PPPoE 用户。

```
[DeviceA] local-user user1 class network
[DeviceA-luser-network-user1] password simple pass1
[DeviceA-luser-network-user1] service-type ppp
[DeviceA-luser-network-user1] quit
# 在系统缺省的 ISP 域 system 下，配置域用户使用本地认证方案。
[DeviceA] domain system
```

```
[DeviceA-isp-system] authentication ppp local
[DeviceA-isp-system] authorization-attribute ip-pool pool1
[DeviceA-isp-system] quit
```

2. 配置 Device B

(1) 配置 GigabitEthernet2/0/2 接口 IP 地址为 3.1.1.1。

```
<DeviceA> system-view
 [DeviceA] interface gigabitethernet 2/0/2
[DeviceA-GigabitEthernet2/0/2] ip address 3.1.1.1 24
[DeviceA-GigabitEthernet2/0/2] quit
```

(2) 启用 DHCP 服务。

```
<DeviceB> system-view
[DeviceB] dhcp enable
```

(3) 创建 DHCP 地址池 pool1，配置为 DHCP 客户端分配的 IP 地址网段和网关地址。

```
[DeviceB] dhcp server ip-pool pool1
[DeviceB-dhcp-pool-pool1] network 2.2.2.0 24
[DeviceB-dhcp-pool-pool1] gateway-list 2.2.2.1
[DeviceB-dhcp-pool-pool1] quit
```

(4) 配置与 PPPoE Server 连接的 GigabitEthernet2/0/2 接口的 IP 地址。

```
[DeviceB] interface gigabitethernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] ip address 3.1.1.1 24
[DeviceB-GigabitEthernet2/0/2] quit
```

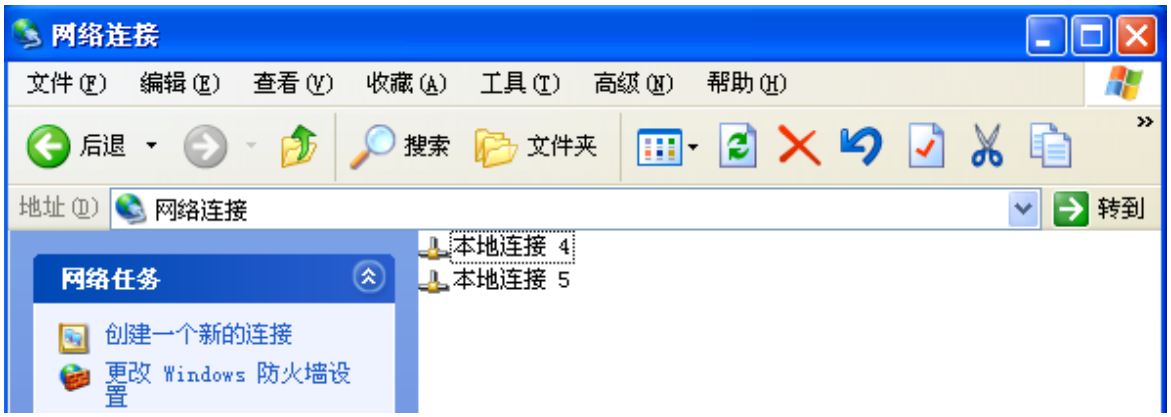
(5) 配置到 PPPoE Server 的静态路由。

```
[DeviceB] ip route-static 2.2.2.0 24 3.1.1.2
```

3. 4. 验证配置

(1) 鼠标右键单击“网上邻居”，选择属性，进入网络连接界面。

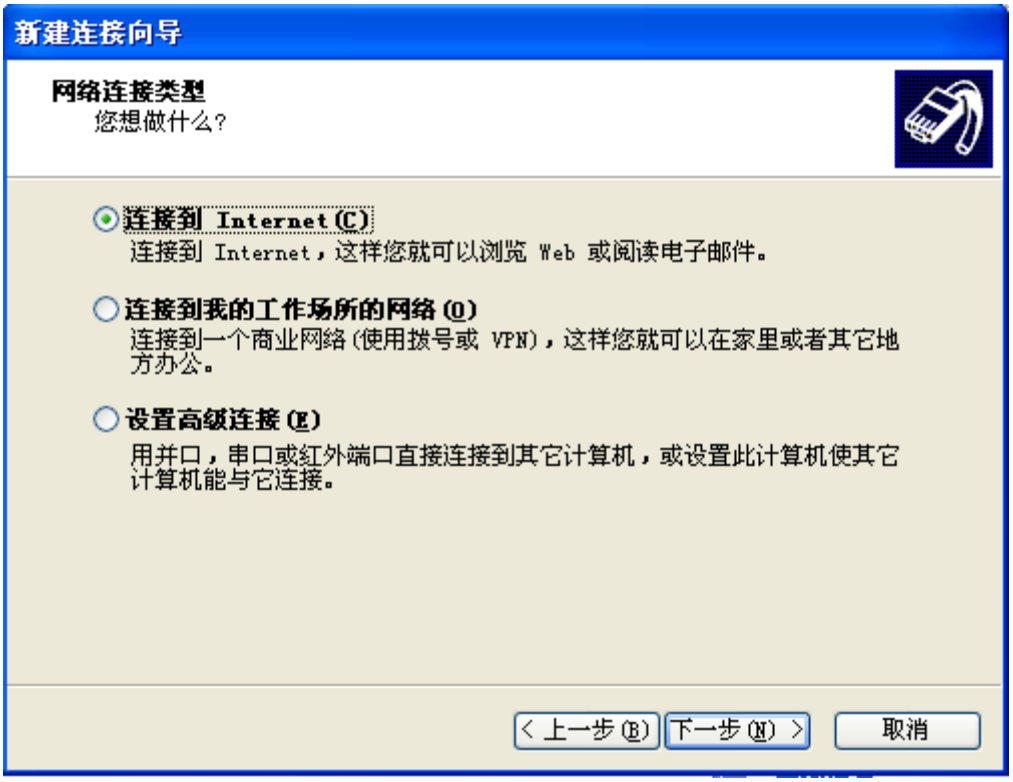
图3 网络连接界面



(2) 选择“创建一个新的连接”，进入新建连接向导界面，单击<下一步>按钮。

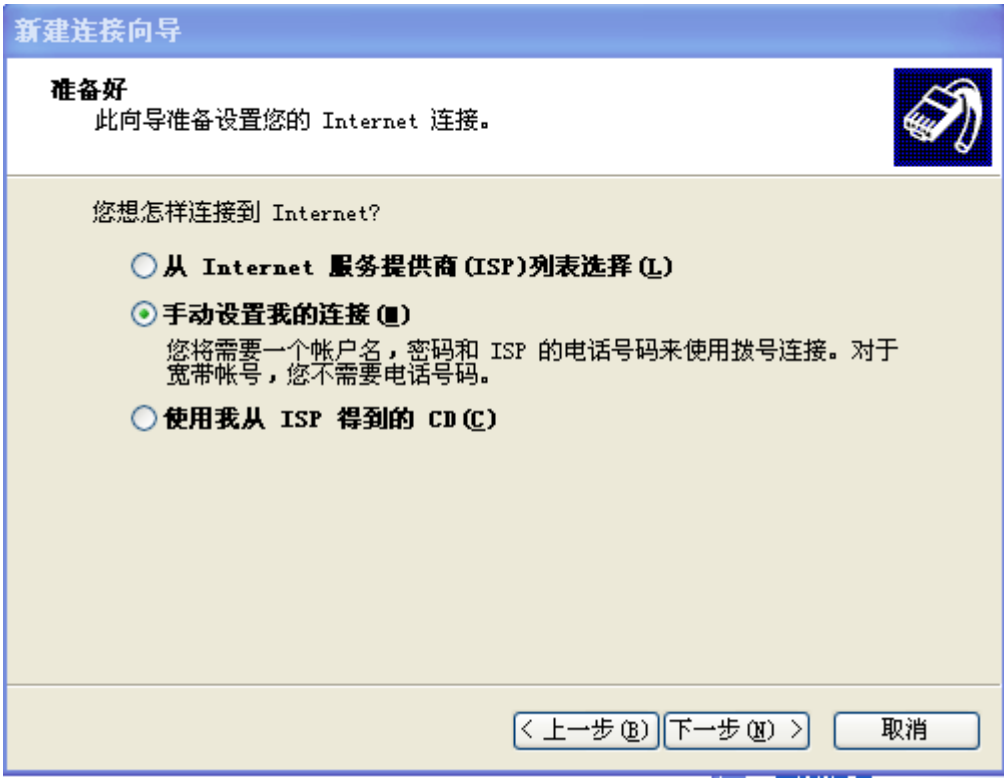
(3) 选择“连接到 Internet（C）”选项，单击<下一步>按钮。

图4 选择网络连接类型界面



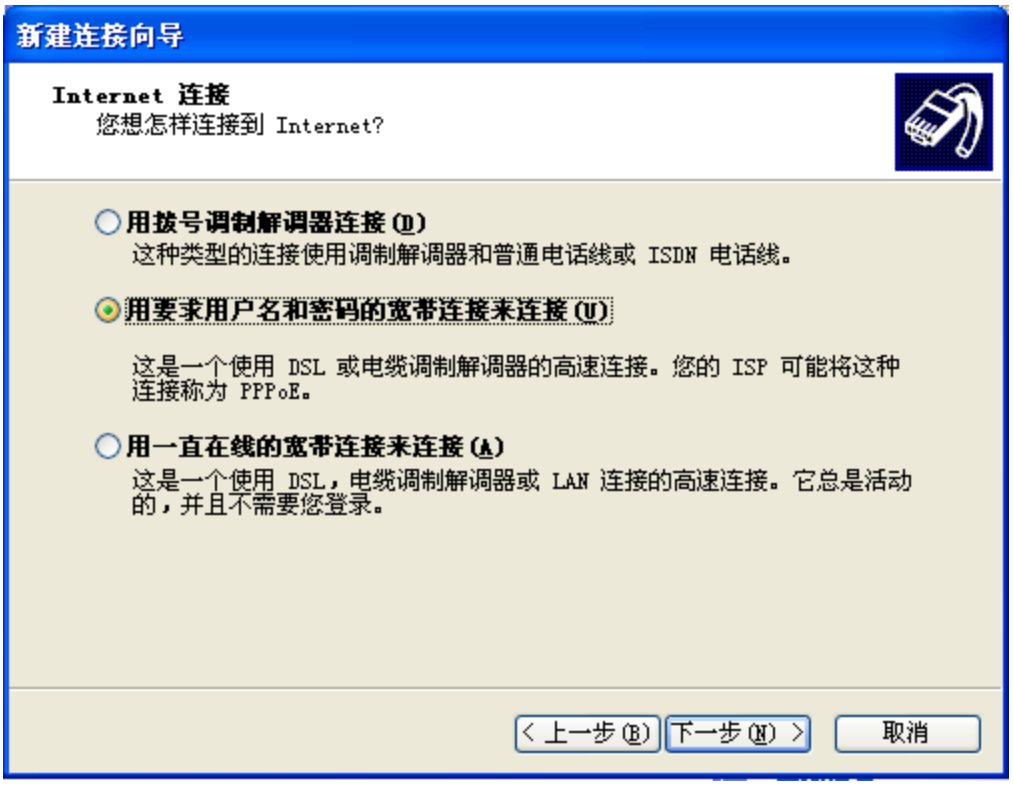
(4) 选择“手动设置我的连接”，单击<下一步>按钮。

图5 准备好界面



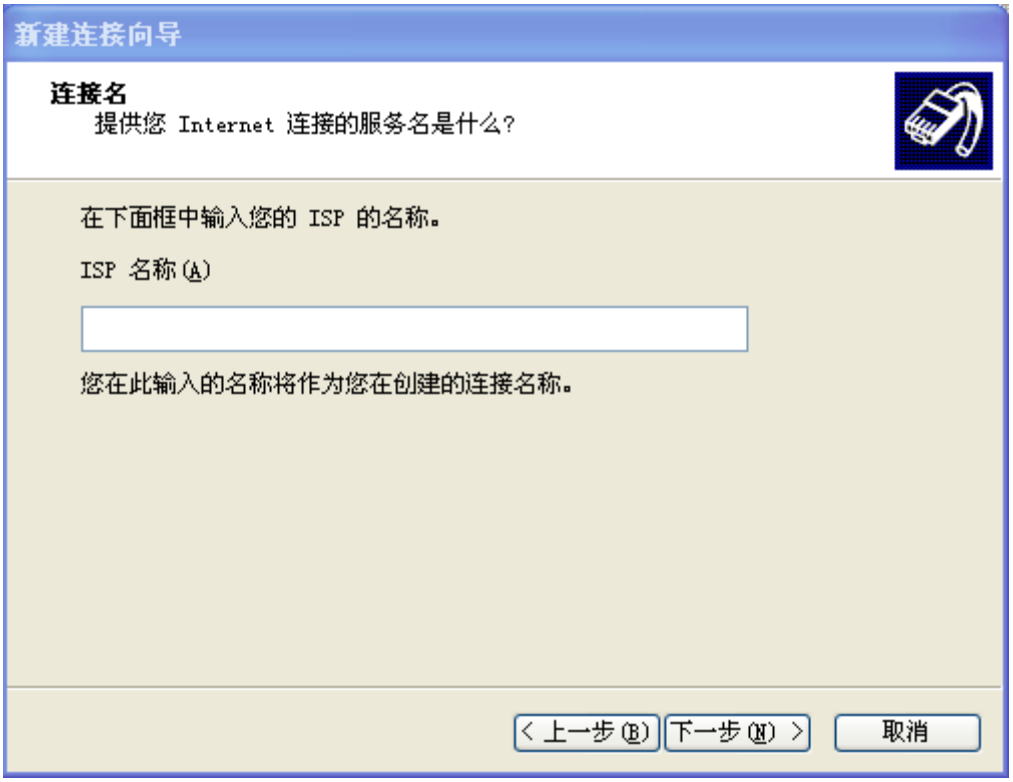
(5) 选择“用要求用户名和密码的宽带连接来连接”，单击<下一步>按钮。

图6 Internet 连接界面



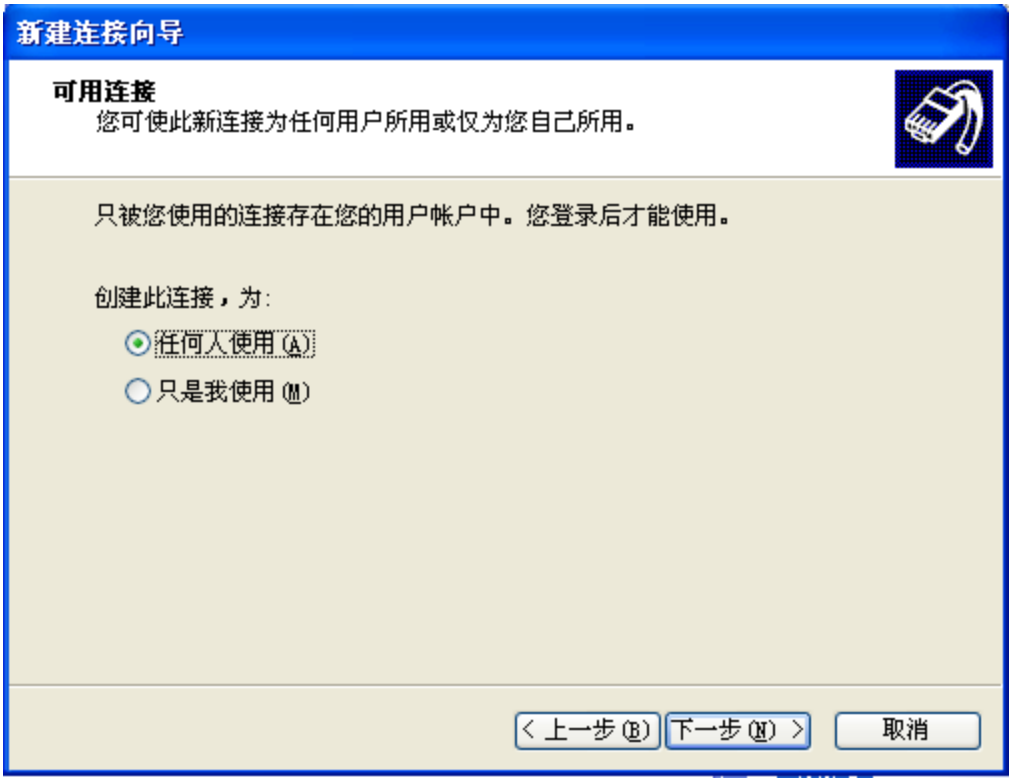
(6) 输入一个 ISP 名称，单击<下一步>按钮。或者直接单击<下一步>按钮跳过。

图7 连接名界面



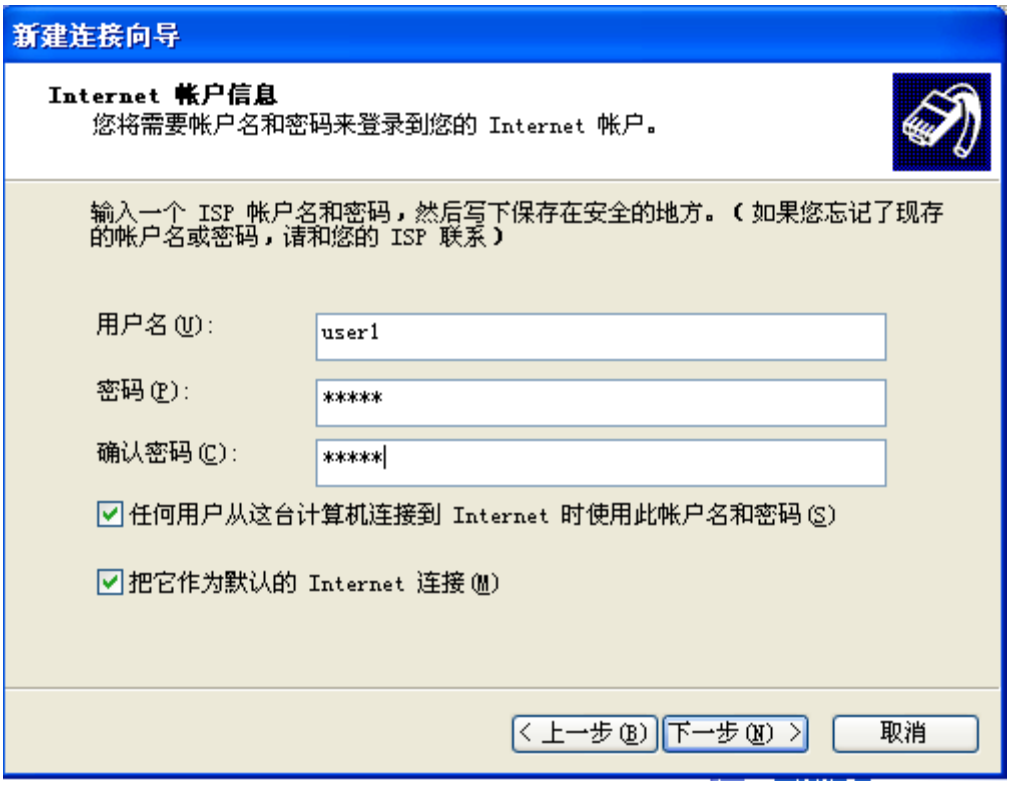
(7) 选择“任何人使用”，单击<下一步>按钮。

图8 可用连接界面



(8) 输入用户名和密码，分别为 user1 和 pass1。单击<下一步>按钮。

图9 Internet 账户信息界面



(9) 单击<完成>按钮，出下如下界面，单击<连接>按钮。

图10 宽带连接界面

(10) 再次双击网络连接里的宽带连接，显示如下图，表示已连接成功。

图11 连接成功界面

当 Host 使用用户名 user1、密码 pass1，通过 PPPoE 接入 Device A 后，Device B 通过 DHCPv4 协议为 Host 分配一个 IP 地址。

显示 DHCP 中继 Device A 的用户地址表项信息。

```
[DeviceA] display dhcp relay client-information
Total number of client-information items: 1
Total number of dynamic items: 1
Total number of temporary items: 0
IP address      MAC address     Type       Interface          VPN name
2.2.2.1         3408-0499-b48c  Dynamic    VA0                N/A
```

显示 DHCP 服务器 Device B 的 DHCP 地址绑定信息。

```
[DeviceA] display dhcp server ip-in-use
IP address      Client identifier/    Lease expiration     Type
                Hardware address
2.2.2.1         0033-3430-382e-3034-  Jul 24 16:28:57 2017  Auto(C)
                3939-2e62-3438-632d-
                5641-30
```

4.5 配置文件

- Device A：

```
#
 dhcp enable
 dhcp relay client-information record
#
dhcp server ip-pool pool1
 gateway-list 2.2.2.10 2.2.2.20 export-route
 remote-server 3.1.1.1
#
interface Virtual-Template10
 ppp authentication-mode chap domain system
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/1
 port link-mode route
 pppoe-server bind virtual-template 10
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 3.1.1.2 255.255.255.0
#
domain system
 authorization-attribute ip-pool pool1
 authentication ppp local
#
local-user user1 class network
 password cipher $c$3$rgL97ckhgtCEhbMs1yy7lxMp2yVuIOk8
 service-type ppp
 authorization-attribute user-role network-operator
```

- Device B：

```
#
 dhcp enable
#
dhcp server ip-pool pool1
#
dhcp server ip-pool pool1
 gateway-list 2.2.2.1
 network 2.2.2.0 mask 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 3.1.1.1 255.255.255.0
#
ip route-static 2.2.2.0 24 3.1.1.2
#
```

5 相关资料

- H3C SR6600 SR6600-X 路由器 二层技术-广域网接入配置指导-R0106

- H3C SR6600 SR6600-X 路由器 二层技术-广域网接入命令参考-R0106

H3C SR6600/SR6600-X 系列路由器

RBAC 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 配置用户具有特定特性中读写类型命令的执行权限举例 1
3.1 组网需求 1
3.2 配置思路 1
3.3 使用版本 1
3.4 配置注意事项 2
3.5 配置步骤 2
3.6 验证配置 3
3.7 配置文件 5
4 配置用户具有切换用户角色权限举例 5
4.1 组网需求 5
4.2 配置思路 6
4.3 使用版本 6
4.4 配置注意事项 6
4.5 配置步骤 6
4.6 验证配置 8
4.7 配置文件 11
5 相关资料 11

1 简介

本文介绍了如何通过 RBAC（Role Based Access Control，基于角色的访问控制）来对登录用户的权限进行控制的典型配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 RBAC 的特性。

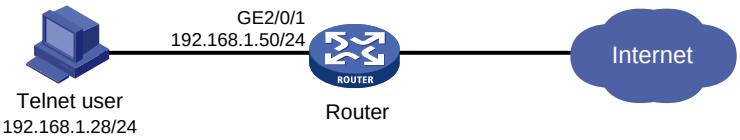
3 配置用户具有特定特性中读写类型命令的执行权限举例

3.1 组网需求

如图 1 所示，为了加强用户登录的安全性，采用本地 AAA 认证对登录设备的 Telnet 用户进行认证。使得 Telnet 用户具有如下权限：

- 允许执行特性 ospf 相关的所有读写类型命令。
- 允许执行特性 filesystem 相关的所有读写类型命令。

图1 特定特性中读写类型命令的执行权限配置组网图



3.2 配置思路

- 为了使 Telnet 用户能够具备以上权限，需要创建 Telnet 本地用户和用户角色 role1，并对 Telnet 用户授予用户角色 role1。
- 通过配置用户角色规则，限定 Telnet 用户可以执行特性特性 ospf 和 filesystem 相关的读写类型命令。
- 为了确保 Telnet 用户仅使用授权的用户角色 role1，需要删除用户具有的缺省用户角色。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置注意事项

- 一个 ISP 域被配置为缺省的 ISP 域后将不能够被删除，必须首先使用命令 **undo domain default enable** 将其修改为非缺省 ISP 域，然后才可以被删除。
- 一个用户角色中允许创建多条规则，各规则以创建时指定的编号为唯一标识，被授权该角色的用户可以执行的命令为这些规则定义的可执行命令的并集。若这些规则定义的权限内容有冲突，则规则编号大的有效。例如，规则 1 允许执行命令 A，规则 2 允许执行命令 B，规则 3 禁止执行命令 A，则最终规则 2 和规则 3 生效，即禁止执行命令 A，允许执行命令 B。

3.5 配置步骤

(1) 配置接口

为接口 GigabitEthernet2/0/1 配置 IP 地址。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] ip address 192.168.1.50 24
[Sysname-GigabitEthernet2/0/1] quit
```

(2) 配置 Telnet 用户登录设备的认证方式

开启设备的 Telnet 服务器功能。

```
[Sysname] telnet server enable
```

在编号为 0～63 的 VTY 用户线下，配置 Telnet 用户登录采用 AAA 认证方式。

```
[Sysname] line vty 0 63
[Sysname-line-vty0-63] authentication-mode scheme
[Sysname-line-vty0-63] quit
```

(3) 配置 ISP 域 bbb 的 AAA 方法

创建 ISP 域 bbb，为 login 用户配置的 AAA 方法为本地认证、本地授权。

```
[Sysname] domain bbb
[Sysname-isp-bbb] authentication login local
[Sysname-isp-bbb] authorization login local
[Sysname-isp-bbb] quit
```

(4) 配置设备管理类本地用户 telnetuser 的密码和服务类型。

创建设备管理类本地用户 telnetuser。

```
[Sysname] local-user telnetuser class manage
```

配置用户的密码是明文的 123456TESTplat&!。

```
[Sysname-luser-manage-telnetuser] password simple 123456TESTplat&!
```

指定用户的服务类型是 Telnet。

```
[Sysname-luser-manage-telnetuser] service-type telnet
[Sysname-luser-manage-telnetuser] quit
```

(5) 创建用户角色 role1，并配置用户角色规则

创建用户角色 role1，进入用户角色视图。

```
[Sysname] role name role1
```

配置用户角色规则 1，允许用户执行特性 ospf 中所有读写类型的命令。

```
[Sysname-role-role1] rule 1 permit read write feature ospf
```

配置用户角色规则 2，允许用户执行特性 filesystem 中所有读写类型的命令。

```
[Sysname-role-role1] rule 2 permit read write feature filesystem
[Sysname-role-role1] quit
```

(6) 为本地用户配置授权用户角色

进入设备管理类本地用户 telnetuser 视图。

```
[Sysname] local-user telnetuser class manage
```

指定用户 telnetuser 的授权角色为 role1。

```
[Sysname-luser-manage-telnetuser] authorization-attribute user-role role1
```

为保证用户仅使用授权的用户角色 role1，删除用户 telnetuser 具有的缺省用户角色 network-operator。

```
[Sysname-luser-manage-telnetuser] undo authorization-attribute user-role
network-operator
[Sysname-luser-manage-telnetuser] quit
```

3.6 验证配置

(1) 查看用户角色信息

通过 **display role** 命令查看显示用户角色 role1 的信息。

```
<Sysname> display role name role1
Role: role1
  Description:
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  1       permit RW-   feature       ospf
  2       permit RW-   feature       filesystem
  R:Read W:Write X:Execute
```

(2) 用户登录设备

用户向设备发起 Telnet 连接，在 Telnet 客户端按照提示输入用户名 telnetuser@bbb 及正确的密码后，成功登录设备。

```
C:\Documents and Settings\user> telnet 192.168.1.50

******************************************************************************
* Copyright (c) 2004-2017 Hangzhou H3C Tech. Co., Ltd. All rights reserved.  *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: telnetuser@bbb
Password:
<Sysname>
```

(3) 验证用户权限

Telnet 用户成功登录设备后，可通过如下步骤验证用户的权限：

- 可执行特性 ospf 中所有写类型的命令。（以配置 OSPF 为例）

```
[Sysname] ospf 1
[Sysname-ospf-1] area 0
[Sysname-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
```

- 可执行特性 ospf 相关的读类型命令。

```
[Sysname] show ospf

          OSPF Process 1 with Router ID 192.168.1.50
                  OSPF Protocol Information

 RouterID: 192.168.1.50   Router type:
 Route tag: 0
 Multi-VPN-Instance is not enabled
 Ext-community type: Domain ID 0x5, Route Type 0x306, Router ID 0x107
 Domain ID: 0.0.0.0
 Opaque capable
 ISPF is enabled
 SPF-schedule-interval: 5 50 200
 LSA generation interval: 5 50 200
 LSA arrival interval: 1000
 Transmit pacing: Interval: 20 Count: 3
 Default ASE parameters: Metric: 1 Tag: 1 Type: 2
 Route preference: 10
 ASE route preference: 150
 SPF calculation count: 0
 RFC 1583 compatible
 Fast-reroute: Remote-lfa Disabled
   Maximum-cost: 4294967295
 Node-Protecing Preference: 40
 Lowest-cost Preference: 20
 Graceful restart interval: 120
 SNMP trap rate limit interval: 10  Count: 7
 Area count: 0   NSSA area count: 0
 ExChange/Loading neighbors: 0
 MPLS segment routing: Disabled
   Segment routing adjacency   : Disabled
   Effective SRGB              : 16000  24000
   Segment routing local block : 15000  15999
   Segment routing tunnel count: 0
```

- 可执行特性 filesystem 相关的所有读写类型命令。（以配置设备发送 FTP 报文的源 IP 地址为 192.168.0.60 为例）

```
[Sysname-a] ftp client source ip 192.168.0.60
[Sysname-a] quit
```

- 不能执行特性 filesystem 相关的执行类型命令。（以进入 FTP 视图为例）

```
<Sysname-a> ftp
Permission denied.
```

通过显示信息可以确认配置生效。

3.7 配置文件

```
#
 telnet server enable
#
interface GigabitEthernet2/0/1
 ip address 192.168.1.50 24
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
domain bbb
 authentication login local
 authorization login local
#
role name role1
 rule 1 permit read write feature ospf
 rule 2 permit read write feature filesystem
#
local-user telnetuser class manage
 password hash $h$6$kZw1rKFsAY4lhgUz$+teVLy8gmKN4Mr00VWgXQTB8ai94gKHlrys5OkytGf4
kT+nz5X1ZGASjc282CYAR6A1upH2jbmRoTcfDzZ9Gmw==
 service-type telnet
 authorization-attribute user-role role1
#
```

4 配置用户具有切换用户角色权限举例

4.1 组网需求

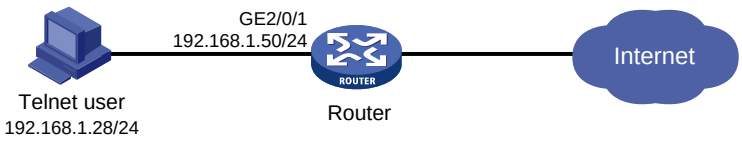
如图 2 所示，为了加强用户登录的安全性，采用本地 AAA 认证对登录设备的 Telnet 用户进行认证。登录设备的 Telnet 用户能够进行用户角色的切换，即在不下线的情况下，临时改变自身对系统的操作权限。当前 Telnet 用户被授权为用户角色 role1，用户角色 role1 具有如下权限：

- 允许执行系统预定义特性组 L3 相关的所有命令。
- 允许执行所有以 **display** 开头的命令。
- 允许执行所有以 **super** 开头的命令。
- 具有所有接口、VLAN 和 VPN 实例资源的操作权限。

现要求，Telnet 用户能够被切换到用户角色 role2 和 network-operator，其中用户角色 role2 具有如下权限：

- 允许执行系统预定义特性组 L2 相关的所有命令。
- 具有所有接口、VLAN 和 VPN 实例资源的操作权限。

图2 切换用户角色权限配置组网图



4.2 配置思路

- 缺省情况下，用户角色切换的认证方式为 local。在本例中 Telnet 用户登录设备的认证方式为本地 AAA 认证，因此，配置用户角色切换时的认证方式为 local。
- 为了使 Telnet 用户 telnetuser 能够进行切换用户角色，需要创建本地用户角色 role1 和 role2，并配置相应的配置用户角色规则和资源控制策略。
- 为了保证操作的安全性，Telnet 用户将用户角色切换到不同的用户角色时，需要配置相应切换密码。

4.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.4 配置注意事项

- 一个 ISP 域被配置为缺省的 ISP 域后将不能够被删除，必须首先使用命令 **undo domain default enable** 将其修改为非缺省 ISP 域，然后才可以被删除。
- 一个用户角色中允许创建多条规则，各规则以创建时指定的编号为唯一标识，被授权该角色的用户可以执行的命令为这些规则定义的可执行命令的并集。若这些规则定义的权限内容有冲突，则规则编号大的有效。例如，规则 1 允许执行命令 A，规则 2 允许执行命令 B，规则 3 禁止执行命令 A，则最终规则 2 和规则 3 生效，即禁止执行命令 A，允许执行命令 B。
- 切换后的用户角色只对当前登录生效，用户重新登录后，又会恢复到原有用户角色。

4.5 配置步骤

(1) 配置接口

为接口 GigabitEthernet2/0/1 配置 IP 地址。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] ip address 192.168.1.50 24
[Sysname-GigabitEthernet2/0/1] quit
```

(2) 配置 Telnet 用户登录设备的认证方式

开启设备的 Telnet 服务器功能。

```
[Sysname] telnet server enable
```

在编号为 0～63 的 VTY 用户线下，配置 Telnet 用户登录采用 AAA 认证方式。

```
[Sysname] line vty 0 63
```

```
[Sysname-line-vty0-63] authentication-mode scheme
[Sysname-line-vty0-63] quit
```

(3) 配置 ISP 域 bbb 的 AAA 方法

创建 ISP 域 bbb，为 login 用户配置的 AAA 方法为本地认证、本地授权。

```
[Sysname] domain bbb
[Sysname-isp-bbb] authentication login local
[Sysname-isp-bbb] authorization login local
[Sysname-isp-bbb] quit
```

(4) 配置设备管理类本地用户 telnetuser 的密码和服务类型

创建设备管理类本地用户 telnetuser。

```
[Sysname] local-user telnetuser class manage
```

配置用户的密码是明文的 123456TESTplat&!。

```
[Sysname-luser-manage-telnetuser] password simple 123456TESTplat&!
```

指定用户的服务类型是 Telnet。

```
[Sysname-luser-manage-telnetuser] service-type telnet
[Sysname-luser-manage-telnetuser] quit
```

(5) 创建用户角色 role1，并配置用户角色规则

创建用户角色 role1，进入用户角色视图。

```
[Sysname] role name role1
```

配置用户角色规则 1，允许用户执行预定义特性组 L3 相关的所有命令。

```
[Sysname-role-role1] rule 1 permit execute read write feature-group L3
```

配置用户角色规则 2，允许用户执行所有以 **display** 开头的命令。

```
[Sysname-role-role1] rule 2 permit command display *
```

配置用户角色规则 3，允许用户执行所有以 **super** 开头的命令。

```
[Sysname-role-role1] rule 3 permit command super *
[Sysname-role-role1] quit
```

(6) 创建用户角色 role2，并配置用户角色规则

创建用户角色 role2，进入用户角色视图。

```
[Sysname] role name role2
```

配置用户角色规则 1，允许用户执行预定义特性组 L2 相关的所有命令。

```
[Sysname-role-role2] rule 1 permit execute read write feature-group L2
[Sysname-role-role2] quit
```

(7) 为本地用户配置授权用户角色

进入设备管理类本地用户 telnetuser 视图。

```
[Sysname] local-user telnetuser class manage
```

指定用户 telnetuser 的授权角色为 role1。

```
[Sysname-luser-manage-telnetuser] authorization-attribute user-role role1
```

为保证用户仅使用授权的用户角色 role1，删除用户 telnetuser 具有的缺省用户角色 network-operator。

```
[Sysname-luser-manage-telnetuser] undo authorization-attribute user-role
network-operator
[Sysname-luser-manage-telnetuser] quit
```

(8) 配置用户角色切换的方式及切换密码

配置 Telnet 用户切换用户角色时采用 **local** 认证方式（系统缺省值为 **local**）。

```
[Sysname] super authentication-mode local
```

配置 Telnet 用户将用户角色切换到 role2 时使用的密码为明文密码 123456TESTplat&!。

```
[Sysname] super password role role2 simple 123456TESTplat&!
```

配置 Telnet 用户将用户角色切换到 network-operator 时使用的密码为明文密码 987654TESTplat&!。

```
[Sysname] super password role network-operator simple 987654TESTplat&!
```

4.6 验证配置

(1) 查看用户角色和特性组信息

通过 **display role** 命令查看用户角色 role1、role2 和 network-operator 的信息。

显示用户角色 role1 的信息。

```
<Sysname> display role name role1
Role: role1
  Description:
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  1       permit RWX   feature-group L3
  2       permit       command       display *
  3       permit       command       super *
  R:Read W:Write X:Execute
```

显示用户角色 role2 的信息。

```
<Sysname> display role name role2
Role: role2
  Description:
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  1       permit RWX   feature-group L2
  R:Read W:Write X:Execute
```

显示用户角色 network-operator 的信息。

```
[Sysname] display role name network-operator
Role: network-operator
  Description: Predefined network operator role has access to all read commands
on the Sysname
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
```

```
----------------------------------------------------------------------
Rule    Perm   Type  Scope         Entity
----------------------------------------------------------------------
sys-1   permit       command       display *
sys-2   permit       command       xml
sys-3   deny         command       display history-command all
sys-4   deny         command       display exception *
sys-5   deny         command       display cpu-usage configuration
                                   *
sys-6   deny         command       display kernel exception *
sys-7   deny         command       display kernel deadloop *
sys-8   deny         command       display kernel starvation *
sys-9   deny         command       display kernel reboot *
sys-10  deny         command       display memory trace *
sys-11  deny         command       display kernel memory *
sys-12  permit       command       system-view ; local-user *
sys-13  permit       command       system-view ; switchto mdc *
sys-14  permit R--   xml-element   -
sys-15  deny         command       display security-logfile summary
sys-16  deny         command       system-view ; info-center securi
                                   ty-logfile directory *
sys-17  deny         command       security-logfile save
R:Read W:Write X:Execute
```

通过 **display role feature-group** 命令查看特性组 L2 和 L3 中包括的特性信息，此处不详细介绍。

(2) 用户登录设备

用户向设备发起 Telnet 连接，在 Telnet 客户端按照提示输入用户名 telnetuser@bbb 及正确的密码后，成功登录设备。

```
C:\Documents and Settings\user> telnet 192.168.1.50

******************************************************************************
* Copyright (c) 2004-2017 Hangzhou H3C Tech. Co., Ltd. All rights reserved.  *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: telnetuser@bbb
Password:
<Sysname>
```

(3) 验证切换用户角色前的用户权限

Telnet 用户成功登录设备后，可通过如下步骤验证用户的权限：

- 可执行特性组 L3 中特性相关的所有命令。（以创建 VPN 实例 vpn1 为例）

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
```

- 可执行所有以 **display** 开头的命令。（以显示系统当前日期和时间为例）

```
<Sysname> display clock
```

```
09:31:56 UTC Wed 01/01/2017
<Sysname>
```

(4) 验证切换用户角色

Telnet 用户成功登录设备后，可通过如下步骤验证用户的权限：

a. 在用户视图下使用 **super** 命令切换到用户角色 role2。

```
<Sysname> super role2
Password:
User privilege role is role2, and only those commands that authorized to the rol
e can be used.
<Sysname>
```

b. 切换到用户角色 role2 后，可执行特性组 L2 中特性相关的所有命令。（以创建 VLAN 10 为例）

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] quit
[Sysname] quit
```

c. 切换到用户角色 role2 后，不能执行非特性组 L2 中特性相关的命令。（以切换到用户角色 network-operator 为例）

```
<Sysname> super network-operator
Permission denied.
```

d. 切换到用户角色 role2 后，不能执行以 **display** 开头的命令。（以显示系统当前日期和时间为例）

```
<Sysname> display clock
Permission denied.
```

e. Telnet 用户重新登录设备后，才能执行所有以 **super** 开头的命令。（以切换到用户角色 network-operator 并输入相应的切换密码为例）

```
C:\Documents and Settings\user> telnet 192.168.1.50

******************************************************************************
* Copyright (c) 2004-2017 Hangzhou H3C Tech. Co., Ltd. All rights reserved.  *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: telnetuser@bbb
Password:
<Sysname>
<Sysname> super network-operator
Password:
User privilege role is network-operator, and only those commands that authorized
 to the role can be used.
<Sysname>
```

通过显示信息可以确认配置生效。

4.7 配置文件

```
#
 telnet server enable
#
interface GigabitEthernet2/0/1
 ip address 192.168.1.50 24
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
 super password role role2 hash $h$6$D0kjHFktkktzgR5g$e673xFnIcKytCj6EDAw+pvwgh3
/ung3WNWHnrUTnXT862B+s7PaLfKTdil8ef71RBOvuJvPAZHjiLjrMPyWHQw==
 super password role network-operator hash $h$6$3s5KMmscn9hJ6gPx$IcxbNjUc8u4yxwR
m87b/Jki8BoPAxw/s5bEcPQjQj/cbbXwTVcnQGL91WOd7ssO2rX/wKzfyzAO5VhBTn9Q4zQ==
#
domain bbb
 authentication login local
 authorization login local
#
role name role1
 rule 1 permit read write execute feature-group L3
 rule 2 permit command display *
 rule 3 permit command super *
#
role name role2
 rule 1 permit read write execute feature-group L2
#
 local-user telnetuser class manage
 password hash $h$6$kZw1rKFsAY4lhgUz$+teVLy8gmKN4Mr00VWgXQTB8ai94gKHlrys5OkytGf4
kT+nz5X1ZGASjc282CYAR6A1upH2jbmRoTcfDzZ9Gmw==
 service-type telnet
 authorization-attribute user-role role1
#
```

5 相关资料

- H3C SR6600 SR6600-X 路由器 基础配置配置指导-R7607
- H3C SR6600 SR6600-X 路由器 基础配置命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

Sampler 结合 IPv4 NetStream 使用配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1
2 配置前提 1
3 配置举例 1
3.1 组网需求 1
3.2 使用版本 1
3.3 配置步骤 2
3.4 验证配置 2
3.4.2 配置文件 4
4 相关资料 4

1 简介

本文档介绍通过 Sampler 结合 IPv4 NetStream 使用的典型配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 Sampler 特性和 IPv4 NetStream 特性。

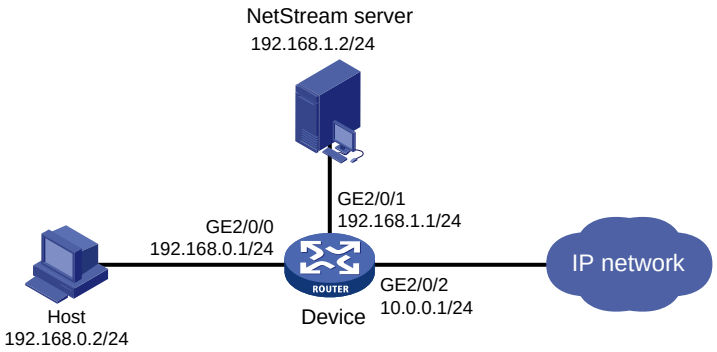
3 配置举例

3.1 组网需求

如图 1 所示，路由器作为局域网内主机访问外网的网关，现要求通过 NetStream 功能使用采样器对路由器上 GigabitEthernet2/0/0 出方向和 GigabitEthernet2/0/2 入方向的流量进行统计，再将统计的信息输出到 Netstream 服务器上。具体应用需求如下：

- 在接口 GigabitEthernet2/0/2 的入方向上配置固定采样，每 100 个报文中抽取一个报文进行 NetStream 统计。
- 在接口 GigabitEthernet2/0/0 的出方向上配置随机采样，每 200 个报文中抽取一个报文进行 NetStream 统计。

图1 Sampler 结合 IPv4 NetStream 使用配置组网图



3.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.3 配置步骤

(1) 创建 Sampler 采样器。

创建一个名为 samplerin 的采样器，采用固定采样方式，设置采样率为 100，即 100 个报文中抽取第一个报文。

```
<Device> system-view
[Device] sampler samplerin mode fixed packet-interval 100
```

创建一个名为 samplerout 的采样器，采用随机采样方式，设置采样率为 200，即 200 个报文中抽取任意一个报文。

```
[Device] sampler samplerout mode random packet-interval 200
```

(2) 使能路由器 NetStream 功能。

配置 GigabitEthernet2/0/2 IP 地址，在此接口的入方向开启 NetStream 功能，使用 samplerin 采样器对该接口的流量进行采样。

```
[Device] interface gigabitethernet 2/0/2
[Device-GigabitEthernet2/0/2] ip address 10.0.0.1 24
[Device-GigabitEthernet2/0/2] ip netstream inbound
[Device-GigabitEthernet2/0/2] ip netstream inbound sampler samplerin
[Device-GigabitEthernet2/0/2] quit
```

配置 GigabitEthernet2/0/0 IP 地址，在此接口的出方向开启 NetStream 功能，使用 samplerout 采样器对该接口的流量进行采样。

```
[Device] interface gigabitethernet 2/0/0
[Device-GigabitEthernet2/0/0] ip address 192.168.0.1 24
[Device-GigabitEthernet2/0/0] ip netstream outbound
[Device-GigabitEthernet2/0/0] ip netstream outbound sampler samplerout
[Device-GigabitEthernet2/0/0] quit
```

配置 GigabitEthernet2/0/1 IP 地址。

```
[Device] interface gigabitethernet 2/0/1
[Device-GigabitEthernet2/0/1] ip address 192.168.1.1 24
[Device-GigabitEthernet2/0/1] quit
```

配置 NetStream 普通流统计信息输出的目的地址为 192.168.1.2 和目的 UDP 端口号为 5000。

```
[Device] ip netstream export host 192.168.1.2 5000
```

3.4 验证配置

(1) 通过 **display sampler** 查看采样器的配置信息。

```
[Device] display sampler
 Sampler name: samplerin
  Mode: fixed;  Packet-interval: 100;  IsNpower : N
 Sampler name: samplerout
  Mode: random;  Packet-interval: 200;  IsNpower : N
```

(2) 路由器运行一段时间后，查看 NetStream 普通流的统计信息。

通过 **display ip netstream cache** 命令来查看 NetStream 流缓存区的配置和状态信息。

```
[Device] display ip netstream cache
IP NetStream cache information:
  Active flow timeout              : 30 min
  Inactive flow timeout            : 30 sec
  Max number of entries            : 10000
  IP active flow entries           : 1
  MPLS active flow entries         : 0
  L2 active flow entries           : 0
  IPL2 active flow entries         : 0
  IP flow entries counted          : 7
  MPLS flow entries counted        : 0
  L2 flow entries counted          : 0
  IPL2 flow entries counted        : 0
  Last statistics resetting time   : Never

IP packet size distribution (157 packets in total):

 1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
 .000 .929 .031 .006 .000 .006 .000 .000 .000 .000 .025 .000 .000 .000 .000

  512  544  576 1024 1536 2048 2560 3072 3584 4096 4608 >4608
 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

 Protocol          Total  Packets    Flows  Packets Active(sec) Idle(sec)
                   Flows  /sec       /sec   /flow   /flow       /flow
--------------------------------------------------------------------------------
 TCP-other             3        0        0       26           7        30
 ICMP                  1        0        0        1           0        30
 UDP-BOOTP             1        0        0        4          15        30
 TCP-Telnet            2        0        0       35          24        30

Type DstIP(Port)            SrcIP(Port)            Pro ToS If(Direct)  Pkts
     DstMAC(VLAN)           SrcMAC(VLAN)
     TopLblType(IP/MASK)    Lbl-Exp-S-List
--------------------------------------------------------------------------------
IP   192.168.0.1(23)       192.168.0.2(56839)      6   0   GE2/0/0(I)    1
```

通过 **display ip netstream export** 命令来查看 NetStream 统计输出报文的信息。

```
[Device] display ip netstream export
IP export information:
  Flow source interface                          : Not specified
  Flow destination VPN instance                  : Not specified
  Flow destination IP address (UDP)              : 192.168.1.2 (5000)
  Version 5 exported flows number                : 0
  Version 5 exported UDP datagrams number (failed): 0 (0)
  Version 9 exported flows number                : 8
  Version 9 exported UDP datagrams number (failed): 6 (6)
```

3.4.2 配置文件

```
#
 sampler samplerout mode random packet-interval 200
 sampler samplerin mode fixed packet-interval 100
#
 ip netstream export host 192.168.1.2 5000
#
interface GigabitEthernet2/0/0
 port link-mode route
 ip address 192.168.0.1 255.255.255.0
 ip netstream outbound
 ip netstream outbound sampler samplerout
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.0.0.1 255.255.255.0
 ip netstream inbound
 ip netstream inbound sampler samplerin
#
```

4 相关资料

- H3C SR6600 SR6600-X 路由器 网络管理和监控配置指导-R7607
- H3C SR6600 SR6600-X 路由器 网络管理和监控命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

SNMP 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1

2 配置前提 1

3 SNMPv1/SNMPv2c 配置举例 1

3.1 组网需求 1

3.2 使用版本 1

3.3 配置注意事项 1

3.4 配置步骤 2

3.4.1 设备的配置 2

3.4.2 NMS 的配置 2

3.5 验证配置 3

3.6 配置文件 5

4 SNMPv3 配置举例 5

4.1 组网需求 5

4.2 使用版本 5

4.3 配置注意事项 6

4.4 配置步骤 6

4.4.1 设备的配置 6

4.4.2 NMS 的配置 6

4.4.3 验证配置 8

4.5 配置文件 10

5 相关资料 10

1 简介

本文档介绍了 SNMP 功能典型配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

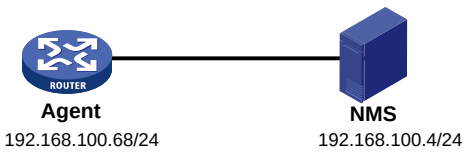
本文档假设您已了解 SNMP 特性。

3 SNMPv1/SNMPv2c 配置举例

3.1 组网需求

如图 1 所示，服务器作为 NMS 通过 SNMPv1/SNMPv2c 协议对设备进行配置文件备份，并且当设备出现故障时能够主动向 NMS 发送告警信息。

图1 SNMPv1/v2c 功能典型配置组网图



3.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.3 配置注意事项

- SNMPv2c 与 SNMPv1 配置方法完全一致，本举例中以配置 SNMPv2c 为例进行介绍。
- 用户在设备和 NMS 上配置的 SNMP 版本号和团体字必须一致，否则，NMS 无法对设备进行管理和维护。
- 不同厂商的 NMS 软件配置方法不同，本配置举例中，以 IMC PLAT 7.0 (E0202)为例进行介绍。

3.4 配置步骤

3.4.1 设备的配置

设置 Agent 使用的 SNMP 版本为 v2c、只读团体名为 readtest，读写团体名为 writetest。

```
<Agent> system-view
[Agent] snmp-agent sys-info version v2c
[Agent] snmp-agent community read readtest
[Agent] snmp-agent community write writetest
```

设置设备的联系人和位置信息，以方便维护。

```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```

设置允许向 NMS 发送告警信息，使用的团体名为 readtest。

```
[Agent] snmp-agent trap enable
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname
readtest
```

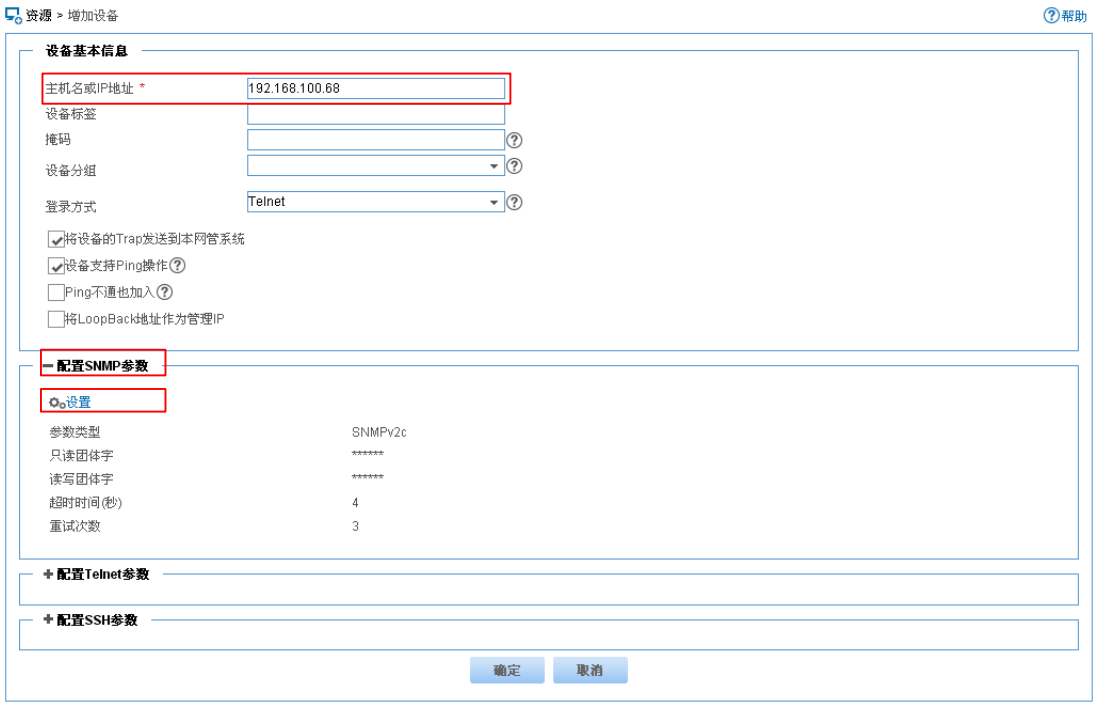
3.4.2 NMS 的配置

增加设备

登录进入 IMC 管理平台，选择“资源”页签，单击导航树中的[增加设备]菜单项，进入增加设备配置页面。

- 设置设备的主机名或 IP 地址为“192.168.100.68”；
- 其它参数采用缺省值。

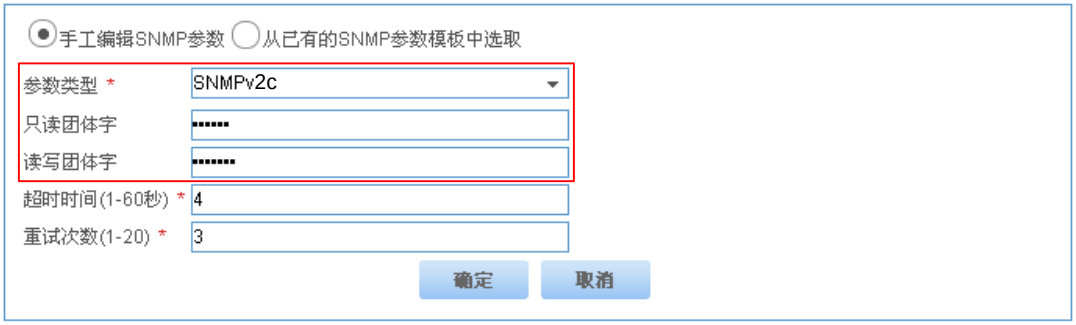
图2 增加设备配置页面



在该页面中单击“配置 SNMP 参数”按钮，展开配置 SNMP 参数页面，单击“设置”，在弹出的对话框中设置如下内容。

- 设置参数类型为“SNMPv2c”；
- 设置只读团体字为“readtest”；
- 设置读写团体字为“writetest”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图3 SNMP 参数设置页面



在“增加设备”页面单击<确定>按钮，iMC 返回增加设备成功信息。

图4 增加设备成功页面

增加设备成功后，用户即可通过 iMC（NMS）对设备进行配置、管理和维护。不同 NMS 管理软件配置不同，关于 NMS 的详细配置，具体请参考 NMS 的相关手册。

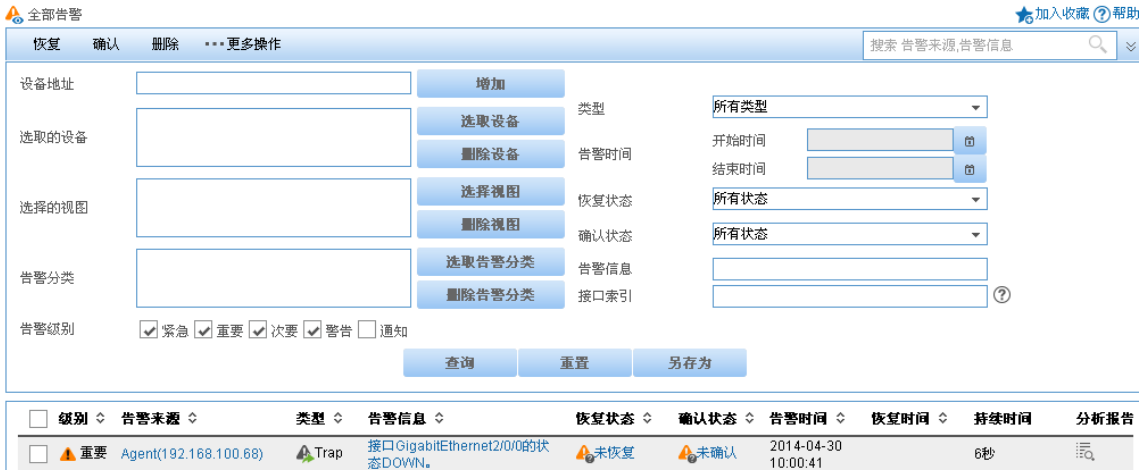
3.5 验证配置

(1) Agent 向 NMS 发送 Trap 信息

完成以上配置之后，在设备上的某个空闲接口执行 **shutdown** 或 **undo shutdown** 操作，设备会向 NMS 发送接口状态改变的 Trap。

在“告警>告警浏览>全部告警”页面中可以查看上述 Trap 信息。

图5 全部告警视图页面



(2) 在 NMS 上备份 Agent 配置文件

在“资源>设备视图”页签点击“Agent”，进入如图 6 页面，点击右侧的“备份配置文件”。

图6 备份配置文件

操作成功后会显示如下页面。

图7 备份配置文件成功

3.6 配置文件

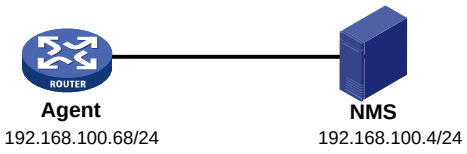
```
#
 snmp-agent
 snmp-agent community write writetest
 snmp-agent community read readtest
 snmp-agent sys-info contact Mr.Wang-Tel:3306
 snmp-agent sys-info location telephone-closet,3rd-floor
 snmp-agent sys-info version v2c
 snmp-agent trap enable arp
 snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname readtest
#
```

4 SNMPv3 配置举例

4.1 组网需求

如图 8 所示，服务器作为 NMS 通过 SNMPv3 协议对设备进行配置文件备份，提供更高的安全性，并且当设备出现故障时能够主动向 NMS 发送告警信息。

图8 SNMPv3 功能典型配置组网图



4.2 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.3 配置注意事项

- 用户需要分别对设备和 NMS 配置 SNMP 功能，设备与 NMS 的 SNMP 配置必须一致，否则，NMS 无法对设备进行管理和维护。
- 不同厂商的 NMS 软件配置方法不同，本配置举例中，以 IMC PLAT 7.0 (E0202)为例进行介绍。
- SNMPv3 接收 Trap 报文的目的主机的安全参数要使用设备已配置的 v3 用户，且安全模型要一致。

4.4 配置步骤

4.4.1 设备的配置

设置 Agent 使用的 SNMP 版本为 v3。

```
<Agent> system-view
[Agent] snmp-agent sys-info version v3
```

创建 MIB 视图，名字为 mibtest，包含 mib-2 子树（OID 为“1.3.6.1”）所有对象。

```
[Agent] snmp-agent sys-info version v1
[Agent] snmp-agent mib-view included mibtest 1.3.6.1
```

创建 SNMPv3 组 managev3group，并配置与该组绑定的 SNMPv3 用户与 NMS 建立连接时，均进行认证和加密，NMS 可以对设备进行读写的视图均为 mibtest。

```
[Agent] snmp-agent group v3 managev3group privacy read-view mibtest write-view mibtest
notify-view mibtest
```

设置 SNMPv3 用户名为 managev3user，认证算法为 SHA-1，认证密码为 123456TESTauth&!，加密算法为 AES，加密密码是 123456TESTencr&!。

```
[Agent] snmp-agent usm-user v3 managev3user managev3group simple authentication-mode sha
123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

开启 SNMP 告警功能。

```
[Agent] snmp-agent trap enable
```

设置接收 SNMP 告警信息的目的主机 IP 地址，即 NMS 的 IP 地址，配置安全认证参数为 managev3user。

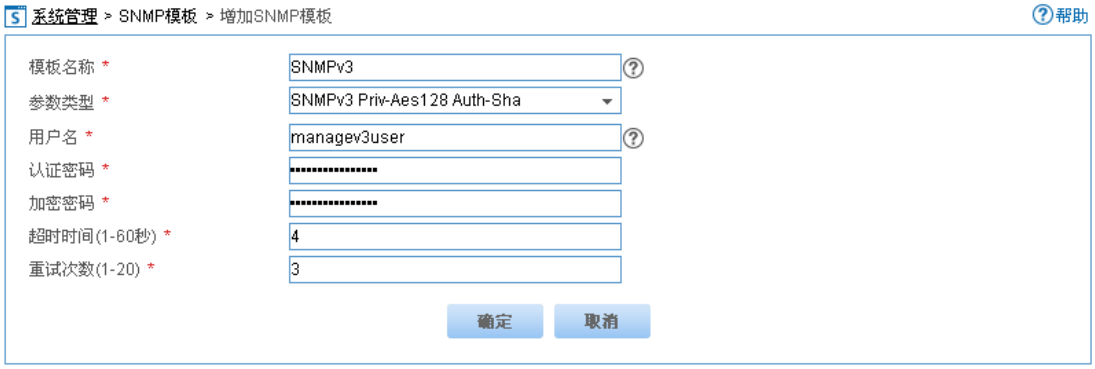
```
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname
managev3user v3 privacy
```

4.4.2 NMS 的配置

登录 iMC，选择“系统管理”页签，单击导航树中的[资源管理/SNMP 模板]菜单项，进入 SNMP 模板配置页面，在该页面中单击<增加>按钮，进入增加 SNMP 模板配置页面。

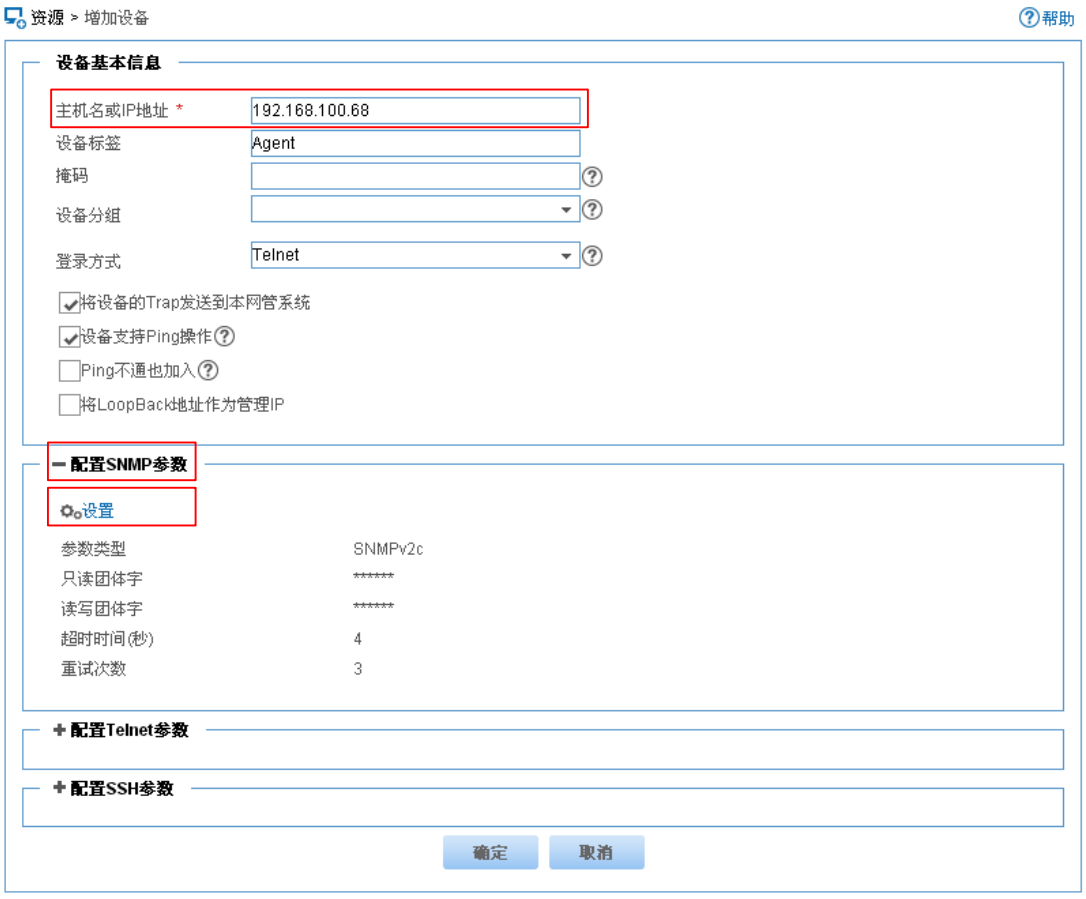
- 配置 SNMP 模板的名称为 SNMPv3。
- 选择参数类型为 SNMPv3 Priv-Aes128 Auth-Sha。
- 配置 SNMP 用户名为 managev3user。
- 认证密码为 123456TESTauth&!。
- 加密密码为 123456TESTencr&!。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图9 增加 SNMP 模板页面



选择“资源”页签，单击导航树中的[资源管理/增加设备]菜单项，进入增加设备配置页面，在该页面中输入设备的主机名或 IP 地址，并点击<配置 SNMP 参数/设置>链接。

图10 增加设备页面

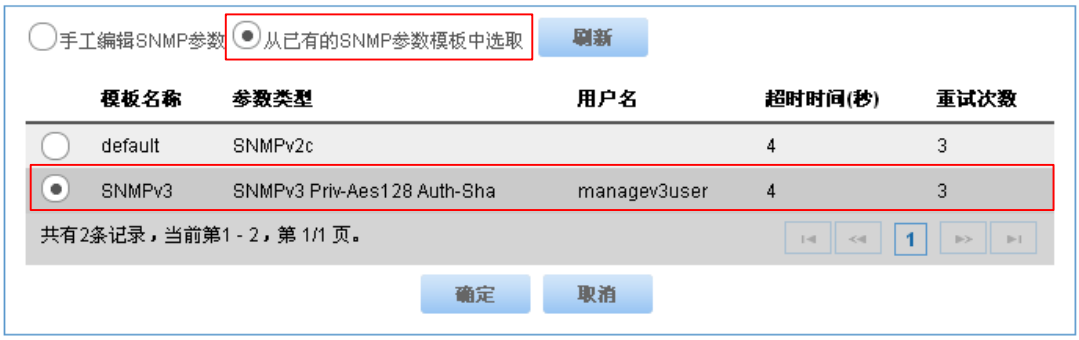


进入 SNMP 参数设置页面配置 SNMP 参数

- 选择“从已有的 SNMP 参数模板中选取”。
- 选择名称为“SNMPv3”的 SNMP 模板。

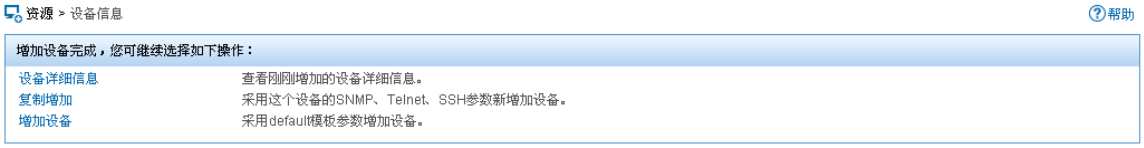
- 单击<确定>按钮完成操作，返回到“增加设备”页面。

图11 SNMP 参数设置页面



在“增加设备”页面单击<确定>按钮，iMC 返回增加设备成功信息。

图12 增加设备成功页面



增加设备成功后，用户即可通过 iMC（NMS）对设备进行配置、管理和维护。不同 NMS 管理软件配置不同，关于 NMS 的详细配置，具体请参考 NMS 的相关手册。

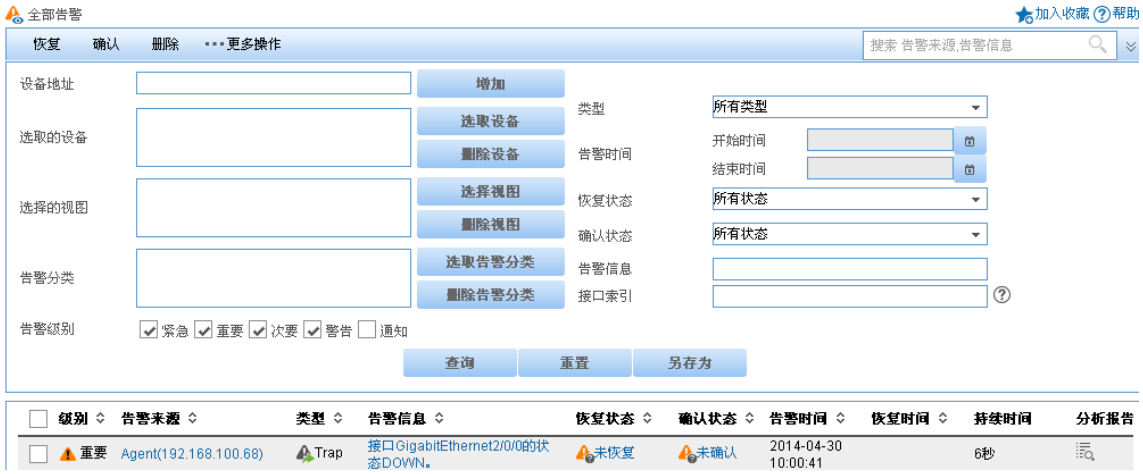
4.4.3 验证配置

(1) Agent 向 NMS 发送 Trap 信息

完成以上配置之后，在设备上的某个空闲接口执行 **shutdown** 或 **undo shutdown** 操作，设备会向 NMS 发送接口状态改变的 Trap。

在“告警>告警浏览>全部告警”页面中可以查看上述 Trap 信息。

图13 全部告警视图页面



(2) 在 NMS 上备份 Agent 配置文件

在“资源>设备视图”页签点击“Agent”，进入如下页面，点击右侧的“备份配置文件”。

图14 备份配置文件

操作成功后会显示如下页面。

图15 备份配置文件成功

4.5 配置文件

```
#
 snmp-agent sys-info version v3
 snmp-agent group v3 managev3group privacy read-view mibtest write-view mibtest notify-view
mibtest
 snmp-agent mib-view included mibtest internet
 snmp-agent trap enable arp
 snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname
managev3user v3 privacy
 snmp-agent usm-user v3 managev3user managev3group cipher authentication-mode sha
$c$3$5JaJZ6gNXlyNRq2FR2ELDT3QQH1exwJRWdYYq7eLfcBewuM5ncM= privacy-mode aes128
$c$3$+bbXZS4+PnsLDyr16OogzBckaLzR6XMDwZQuLBU8RM+dpw==
#
```

5 相关资料

- H3C SR6600 SR6600-X 路由器 网络管理和监控配置指导-R7607
- H3C SR6600 SR6600-X 路由器 网络管理和监控命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

SSH 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 配置前提 ····· 1

2 使用限制 ····· 1

3 设备作为 Stelnet 服务器配置举例（password 认证） ····· 1

3.1 组网需求 ····· 1

3.2 配置思路 ····· 1

3.3 使用版本 ····· 2

3.4 配置步骤 ····· 2

3.5 验证配置 ····· 3

3.6 配置文件 ····· 4

4 设备作为 Stelnet 服务器配置举例（publickey 认证） ····· 5

4.1 组网需求 ····· 5

4.2 配置思路 ····· 5

4.3 使用版本 ····· 6

4.4 配置注意事项 ····· 6

4.5 配置步骤 ····· 6

4.5.1 配置 Host 作为 Stelnet 客户端 ····· 6

4.5.2 配置 Device 作为 FTP 服务器 ····· 8

4.5.3 配置 FTP 客户端上传公钥文件 ····· 8

4.5.4 配置 Device 作为 Stelnet 服务器 ····· 9

4.6 验证配置 ····· 10

4.7 配置文件 ····· 12

5 设备作为 Stelnet 客户端配置举例（password 认证） ····· 13

5.1 组网需求 ····· 13

5.2 配置思路 ····· 13

5.3 使用版本 ····· 14

5.4 配置步骤 ····· 14

5.4.1 Stelnet 服务器的配置 ····· 14

5.4.2 Stelnet 客户端的配置 ····· 15

5.5 验证配置 ····· 16

5.6 配置文件 ····· 16

6 设备作为 SFTP 客户端配置举例（password-publickey 认证） ····· 17

6.1 组网需求 ····· 17

6.2 配置思路 17
6.3 使用版本 18
6.4 配置注意事项 18
6.5 配置步骤 18
6.5.1 SFTP 客户端的配置 18
6.5.2 配置 DeviceB 作为 FTP 服务器 19
6.5.3 配置客户端 DeviceA 上传公钥文件 19
6.5.4 配置 Device B 作为 SFTP 服务器 19
6.6 验证配置 20
6.7 配置文件 22
7 SCP 文件传输配置举例（password 认证） 23
7.1 组网需求 23
7.2 配置思路 23
7.3 使用版本 23
7.4 配置步骤 24
7.4.1 配置 RADIUS 服务器 24
7.4.2 配置 Device B 25
7.4.3 配置 Device A 26
7.5 验证配置 26
7.6 配置文件 26
8 相关资料 27

1 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文假设您已了解 SSH 特性。

2 使用限制

举例中的设备运行于非 FIPS 模式下。若设备运行于 FIPS 模式下：

- 支持的密钥对的模数只能为 2048 比特，因此相关的配置和显示信息也有所变化，请以设备的实际情况为准。
- 设备作为服务器仅支持 RSA 密钥对，请不要生成 DSA 密钥对。

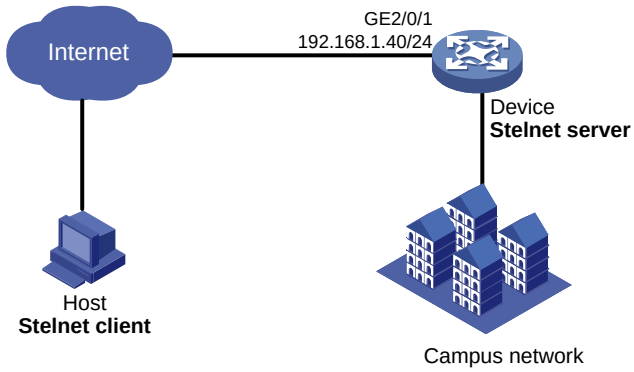
3 设备作为 Stelnet 服务器配置举例（password 认证）

3.1 组网需求

如图 1 所示，网络管理员需要通过 Internet 远程登录到校园网的网关设备（Device）上对其进行相关配置。为了提高对 Device 进行管理的安全性，可将 Device 配置为 Stelnet 服务器，并在 Host 上运行 Stelnet 客户端软件，在二者之间建立 SSH 连接。要求：

- Device 通过 SSH 的 password 认证方式对客户端进行认证，认证过程在 Device 本地完成；
- 网络管理员 Host 的登录用户名为 client001，密码为 aabbcc，登录设备后可以正常使用所有命令。

图1 设备作为 Stelnet 服务器配置组网图



3.2 配置思路

- 为了使 SSH 的版本协商和算法协商过程正常运行，且为了保证客户端对连接的服务器的认证正常进行，请在服务器端生成 RSA、DSA 密钥对。

- 为了采用本地认证的方式认证用户，需要在本地服务器 Device 上创建相应的本地用户，并在本地用户视图下配置密码。
- Stelnet 客户端通过 VTY 用户线访问设备。因此，需要配置登录用户线的认证方式为 scheme 方式。
- 为了使 Stelnet 用户登录设备后能正常使用所有命令，将用户角色设置为 network-admin，缺省情况下本地用户的用户角色为 network-operator。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置步骤

生成 RSA 密钥对。

```
<Device> system-view
[Device] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[Device] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

使能 SSH 服务器功能。

```
[Device] ssh server enable
```

配置接口 GigabitEthernet2/0/1 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
[Device] interface GigabitEthernet 2/0/1
[Device-GigabitEthernet2/0/1] ip address 192.168.1.40 255.255.255.0
[Device-GigabitEthernet2/0/1] quit
```

设置 Stelnet 客户端登录用户界面的认证方式为 scheme。

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

创建本地用户 client001，并设置用户密码、服务类型和用户角色。

```
[Device] local-user client001 class manage
New local user added.
```

```
[Device-luser-manage-client001] password simple aabbcc
[Device-luser-manage-client001] service-type ssh
[Device-luser-manage-client001] authorization-attribute user-role network-admin
[Device-luser-manage-client001] quit
```

3.5 验证配置

说明

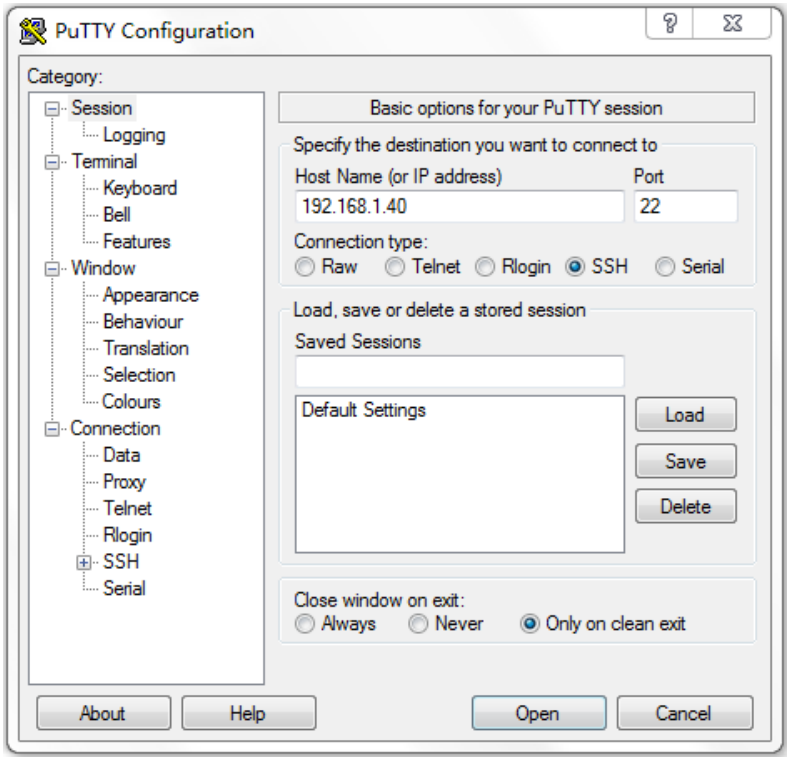
Stelnet客户端软件有很多，例如PuTTY、OpenSSH等。本文中仅以客户端软件PuTTY0.60为例，说明 Stelnet 客户端的配置方法。

安装 PuTTY0.60 软件。

打开 PuTTY.exe 程序，点击“Session”功能区，出现如图 2 所示的客户端配置界面。

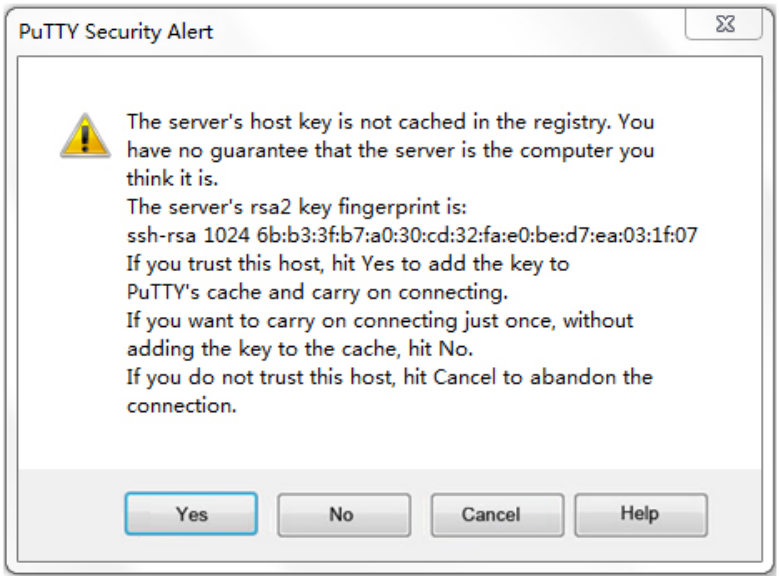
- 在“Host Name（or IP address）”文本框中输入 Stelnet 服务器的 IP 地址为 192.168.1.40。
- 在“Port”文本框中输入 SSH 协议端口号 22。
- 在“Connection type”区域选择 SSH 协议。

图2 Stelnet 客户端配置界面



在图 2 界面中，单击<Open>按钮。弹出“PuTTY Security Alert”对话框。

图3 Stelnet 客户端登录界面（一）



单击“是（Y）”按钮，并输入用户名“client001”和密码“aabbcc”，即可成功登录设备使用所有命令。

```
login as: client001
client001@192.168.1.40's password:

******************************************************************************
* Copyright (c) 2004-2021 Hangzhou H3C Tech. Co., Ltd. All rights reserved.  *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Device>
```

3.6 配置文件

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 192.168.1.40 255.255.255.0
#
line vty 0 63
 authentication-mode scheme
#
ssh server enable
#
local-user client001 class manage
 password                                                                    hash
$h$6$CqMnWdX6LIW/hz2Z$4+0Pumk+A98VlGVgqN3n/mEi7hJka9fEZpRZIpSNi9bcBEXhpvIqaYTvIVBf7ZUNGn
ovFsqW7nYxjoToRDvYBg==
 service-type ssh
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
```

#

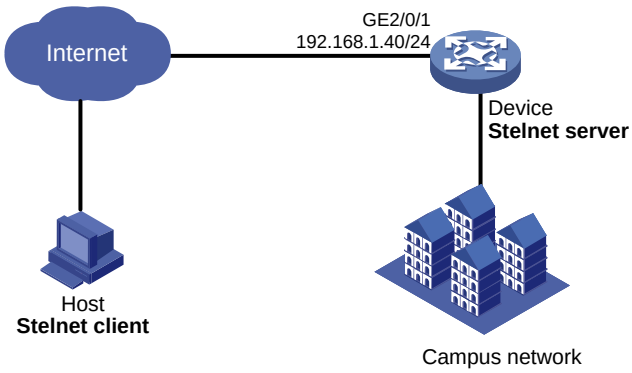
4 设备作为 Stelnet 服务器配置举例（publickey 认证）

4.1 组网需求

如图 4 所示，网络管理员需要通过 Internet 远程登录到校园网的网关设备（Device）上对其进行相关配置。为了提高对 Device 进行管理的安全性和认证强度，将 Device 配置为 Stelnet 服务器，要求：

- Device 通过 publickey 认证方式对 Stelnet 客户端进行认证，使用的公钥算法为 RSA。
- 网络管理员 Host 的登录用户名为 client001，登录设备后可以正常使用所有命令。
- 服务器端通过从公钥文件中导入的方式来配置客户端的公钥。

图4 设备作为 Stelnet 服务器配置组网图



4.2 配置思路

- 在服务器的配置过程中需要指定客户端的公钥信息，因此需要首先完成客户端密钥对的配置，再进行服务器的配置。
- 服务器在采用 publickey 方式验证客户端身份时，首先要比较客户端发送的 Stelnet 用户名、主机公钥是否与本地配置的 SSH 用户名以及相应的客户端主机公钥一致，在确认用户名和客户端主机公钥正确后，再利用数字签名对客户端进行验证，而该签名是客户端利用主机公钥对应的私钥计算出的。因此，需要在服务器端配置客户端的 RSA 主机公钥，并在客户端为该 SSH 用户指定与主机公钥对应的 RSA 主机私钥。
- 如果 SSH 服务器采用 publickey 方式认证客户端，必须在服务器上创建相应的 SSH 用户，以及同名的本地用户（用于下发授权属性：工作目录、用户角色）。
- Stelnet 客户端通过 VTY 用户线访问设备。因此，需要配置登录用户线的认证方式为 scheme 方式。
- 为了使 Stelnet 用户登录设备后要能正常使用所有命令，将用户的用户角色设置为 network-admin，缺省情况下本地用户的用户角色为 network-operator。

4.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.4 配置注意事项

- FIPS 模式下，设备作为 SSH 服务器不支持 publickey 认证方式。
- 虽然一个客户端只会采用 RSA、DSA 公钥算法中的一种来认证服务器，但是由于不同客户端支持的公钥算法不同，为了确保客户端能够成功登录服务器，请在服务器上同时生成 RSA、DSA 密钥对。

4.5 配置步骤

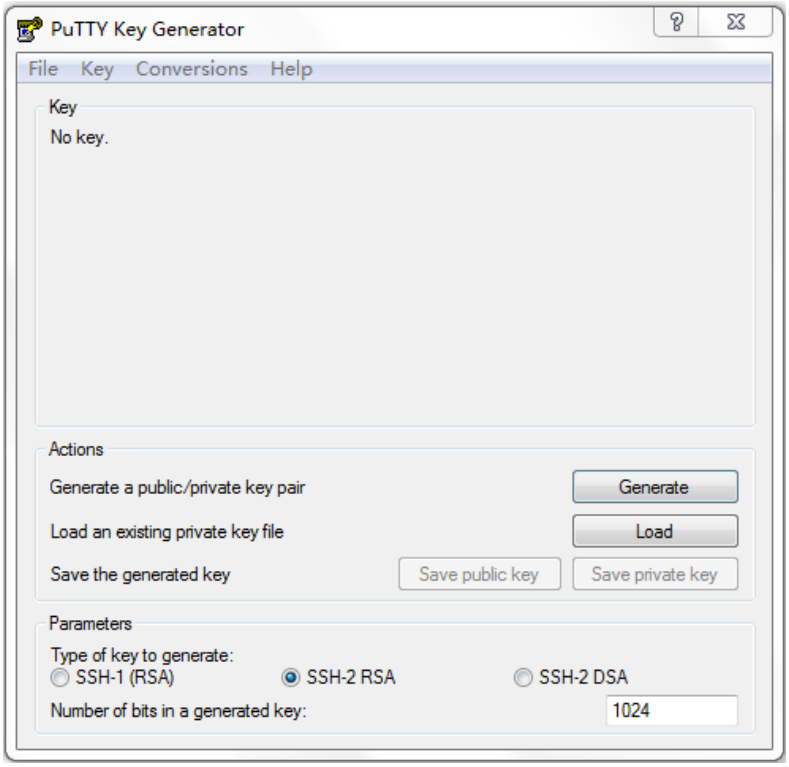
4.5.1 配置 Host 作为 Stelnet 客户端

说明

客户端软件有很多，例如 PuTTY、OpenSSH 等。本文中仅以客户端软件 PuTTY0.60 为例，说明 Stelnet 客户端的配置方法。

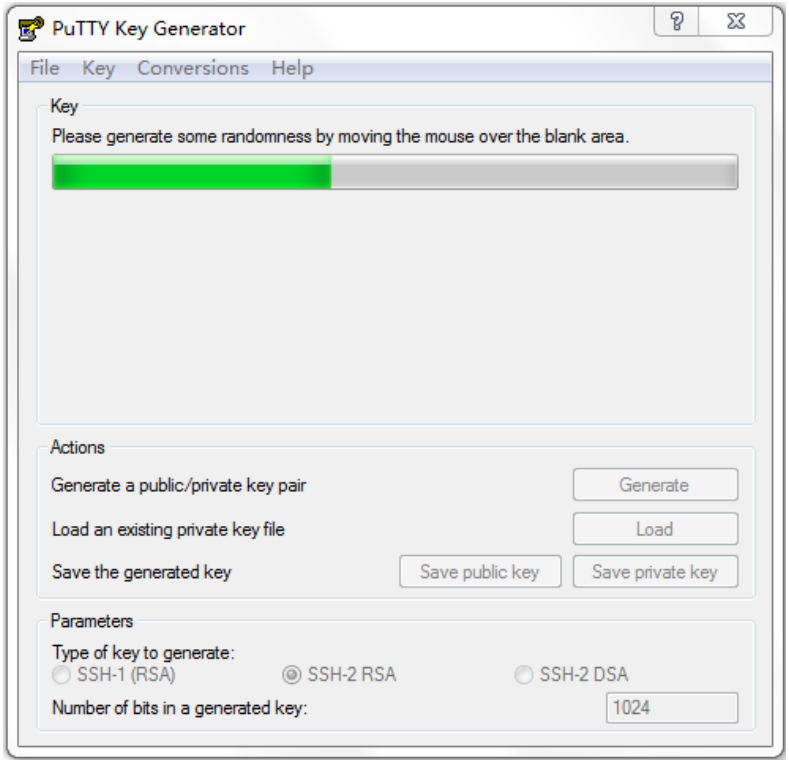
在客户端运行 PuTTYGen.exe，在参数栏中选择“SSH-2 RSA”，点击<Generate>，产生客户端密钥对。

图5 生成客户端密钥（1）



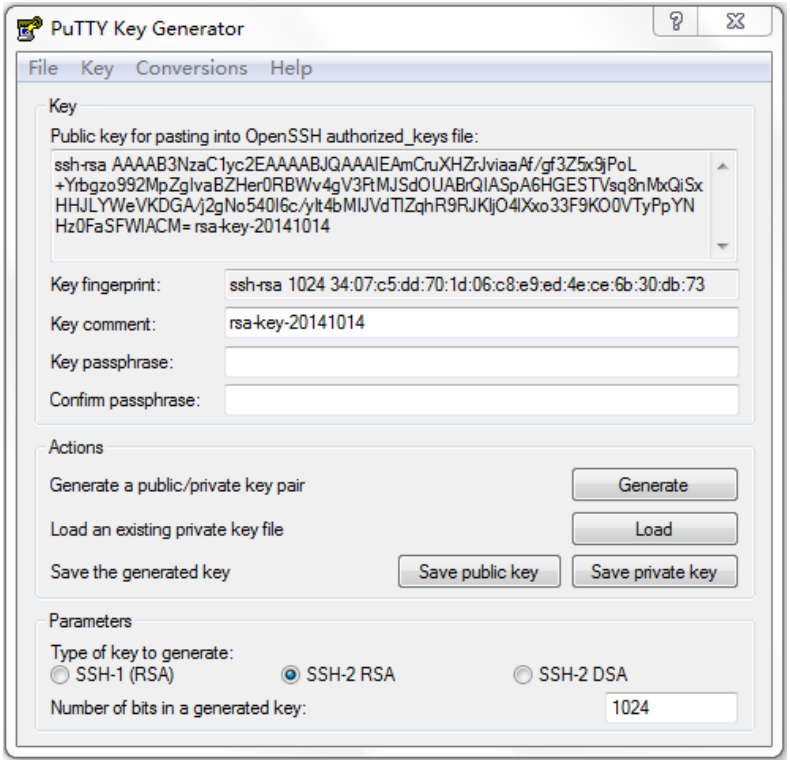
在产生密钥对的过程中需不停地移动鼠标，鼠标移动仅限于图 6 蓝色框中除绿色标记进程条外的地方，否则进程条会停止显示，密钥对将停止产生。

图6 生成客户端密钥（2）



密钥对产生后，点击<Save public key>，输入存储公钥的文件名 key.pub，点击<保存>按钮将公钥文件保存在 D 盘。

图7 生成客户端密钥（3）



点击<Save private key>存储私钥，选择保存的路径（例如 D:\），并输入私钥文件名为 private.ppk，点击保存。

4.5.2 配置 Device 作为 FTP 服务器

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<Device> system-view
[Device] interface GigabitEthernet 2/0/1
[Device-GigabitEthernet2/0/1] ip address 192.168.1.40 255.255.255.0
[Device-GigabitEthernet2/0/1] quit
```

在 Device 上创建一个 ftp 类型的本地用户，并设置密码为明文 ftp，服务类型为 FTP，用户角色为 network-admin，工作目录为 flash:/。

```
[Device] local-user ftp class manage
New local user added.
[Device-luser-manage-ftp] password simple ftp
[Device-luser-manage-ftp] authorization-attribute user-role network-admin
[Device-luser-manage-ftp] authorization-attribute work-directory flash:/
[Device-luser-manage-ftp] service-type ftp
[Device-luser-manage-ftp] quit
```

开启 Device 的 FTP 服务器功能。

```
[Device] ftp server enable
[Device] quit
```

4.5.3 配置 FTP 客户端上传公钥文件

Host 通过 FTP 登录并上传公钥文件 key.pub 到 Device。

```
<DeviceA>ftp 192.168.1.40
Press CTRL+C to abort.
Connected to 192.168.1.40 (192.168.1.40).
220 FTP service ready.
User (192.168.1.56:(none)): ftp
331 Password required for ftp.
Password:
230 User logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put flash:/key.pub
227 Entering Passive Mode (192,168,1,40,41,116)
150 Accepted data connection
226 File successfully transferred
301 bytes sent in 0.000 seconds (1.05 Mbytes/s)
ftp> quit
221-Goodbye. You uploaded 1 and downloaded 0 kbytes.
221 Logout.
```

4.5.4 配置 Device 作为 Stelnet 服务器

生成 RSA 密钥对。

```
[Device] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[Device] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

使能 SSH 服务器功能。

```
[Device] ssh server enable
```

设置 Stelnet 客户端登录用户界面的认证方式为 scheme。

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

从文件 key.pub 中导入客户端的公钥，并命名为 devicekey。

```
[Device] public-key peer devicekey import sshkey key.pub
```

设置 SSH 用户 client001 的认证方式为 publickey，并指定公钥为 devicekey。

```
[Device] ssh user client001 service-type stelnet authentication-type publickey assign publickey devicekey
```

创建本地用户 client001，并设置服务类型为 SSH，用户角色为 network-admin。

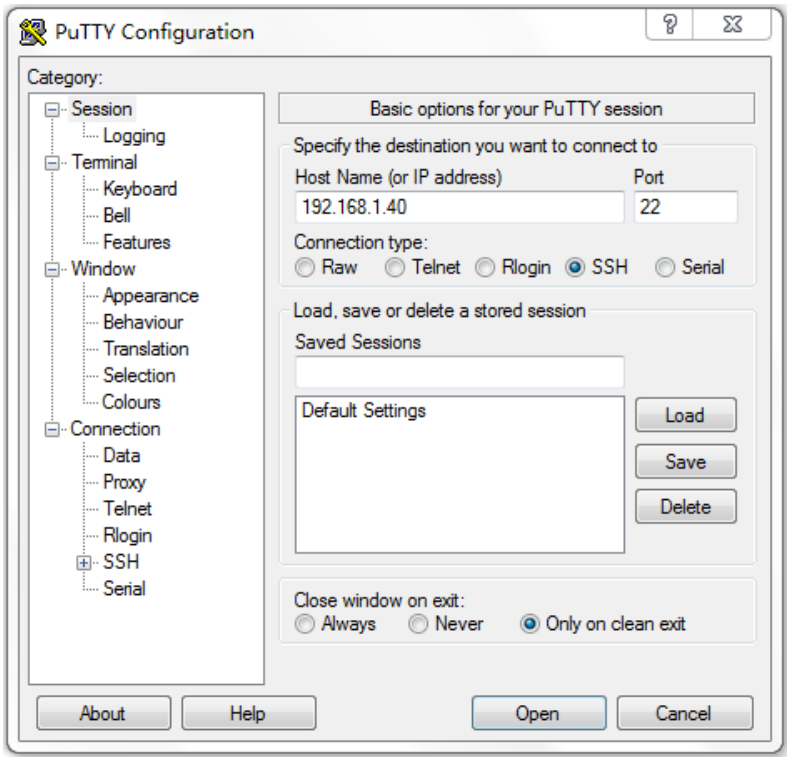
```
[Device] local-user client001 class manage
New local user added.
[Device-luser-manage-client001] service-type ssh
[Device-luser-manage-client001] authorization-attribute user-role network-admin
[Device-luser-manage-client001] quit
```

4.6 验证配置

客户端打开 PuTTY.exe 程序，点击“Session”功能区，出现如图 8 所示的客户端配置界面。

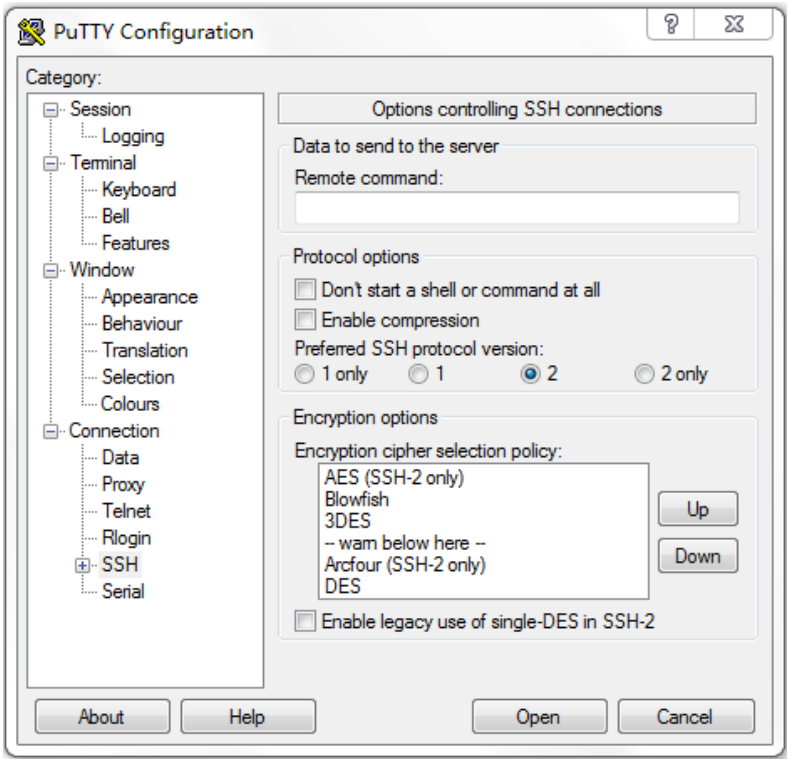
- 在“Host Name（or IP address）”文本框中输入 Stelnet 服务器的 IP 地址为 192.168.1.40。
- 在“Port”文本框中输入 SSH 协议端口号 22。
- 在“Connection type”区域选择 SSH 协议。

图8 Stelnet 客户端配置界面（1）



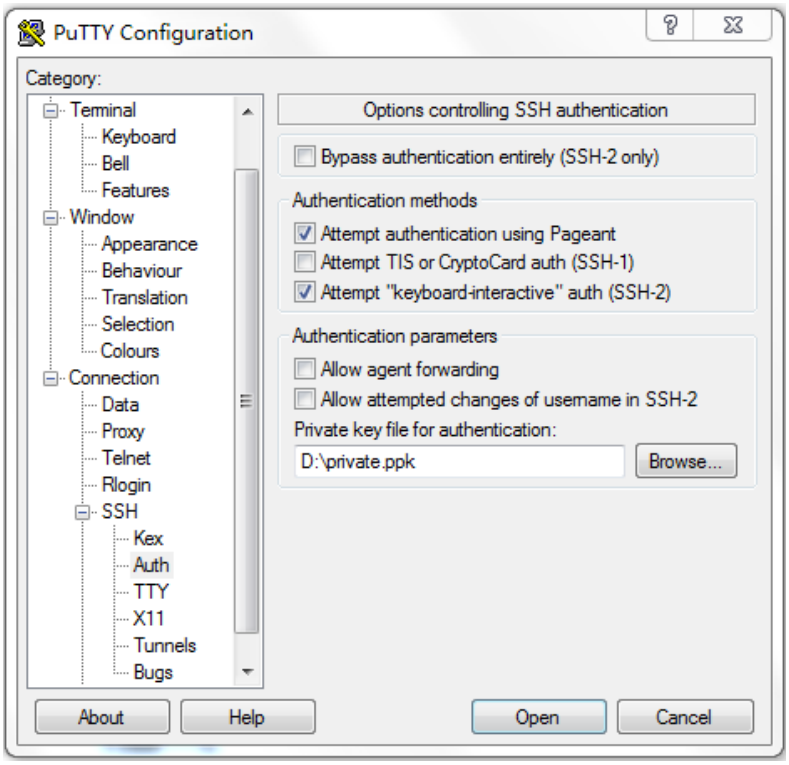
单击左侧导航栏“Connection->SSH”，出现如图 9 的界面。选择“Preferred SSH protocol version”为“2”。

图9 Stelnet 客户端配置界面（2）



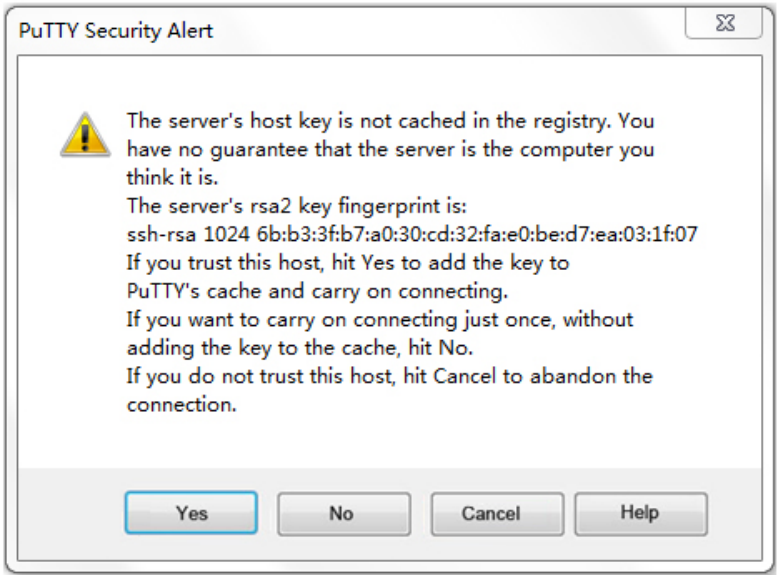
单击左侧导航栏“Connection->SSH”下面的“Auth”（认证），出现如图 10 的界面。单击<Browse…>按钮，弹出文件选择窗口。选择与配置到服务器端的公钥对应的私钥文件 private.ppk。

图10 Stelnet 客户端配置界面（3）



单击<Open>按钮。弹出“PuTTY Security Alert”对话框。

图11 Stelnet 客户端登录界面（一）



单击“是（Y）”按钮，按提示输入用户名 client001，即可进入 Device 的配置界面，用户角色为 network-admin。

```
login as: client001
Authenticating with public key ”rsa-key-20170726”

******************************************************************************
* Copyright (c) 2004-2021 Hangzhou H3C Tech. Co., Ltd. All rights reserved.  *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Device>
```

4.7 配置文件

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 192.168.1.40 255.255.255.0
#
line vty 0 63
 authentication-mode scheme
#
ssh server enable
ssh user client001 service-type stelnet authentication-type publickey assign publickey devicekey
#
local-user client001 class manage
 service-type ssh
 authorization-attribute user-role network-operator
```

```
 authorization-attribute user-role network-admin
#
public-key peer Devicekey
 public-key-code begin
30819D300D06092A864886F70D010101050003818B0030818702818100A2DBC1FD76A837BEF5D322598442D6
753B2E8F7ADD6D6209C80843B206B309078AFE2416CB4FAD496A6627243EAD766D57AEA70B901B4B4566D9A6
51B133BAE34E9B9F04E542D64D0E9814D7E3CBCDBCAF28FF21EE4EADAE6DF52001944A40414DFF280FF043B1
4838288BE7F9438DC71ABBC2C28BF78F34ADF3D1C912579A19020175
 public-key-code end
 peer-public-key end
#
local-user ftp
 password simple $c$3$sg9WgqO1w8vnAv2FKGTOYgFJm3nn2w==
 authorization-attribute work-directory flash:/
 authorization-attribute user-role network-operator
 service-type ftp
#
ftp server enable
#
```

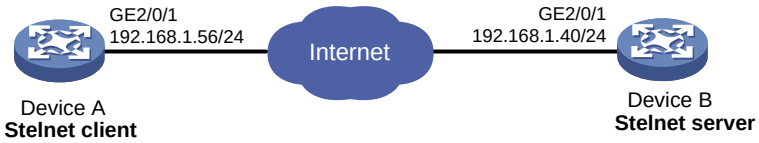
5 设备作为 Stelnet 客户端配置举例（password 认证）

5.1 组网需求

如图 12 所示，Device A 作为 Stelnet 客户端，采用 SSH 协议远程登录到 Device B 上。要求：

- Device B 采用本地认证的方式认证用户，Stelnet 服务器采用的认证方式为 password 认证。
- 登录用户名为 client001，密码为 aabbcc，用户登录设备后可以正常使用所有命令。
- 为提高安全性，需要以 Stelnet 客户端保存的主机公钥来验证 Stelnet 服务器，Stelnet 客户端只信任通过验证的 Stelnet 服务器并继续访问该服务器。

图12 设备作为 Stelnet 客户端配置组网图



5.2 配置思路

- 为了使 SSH 的版本协商和算法协商过程正常运行，且为了保证客户端对连接的服务器的认证正常进行，请在服务器端生成 RSA、DSA 密钥对。
- Stelnet 客户端通过 VTY 用户线访问设备。因此，需要配置登录用户线的认证方式为 scheme 方式。
- 为了采用本地认证的方式认证用户，需要在 Stelnet 服务器上创建相应的本地用户，并在本地用户视图下配置密码。

- 为了使 Stelnet 用户登录设备后能正常使用所有命令，将用户的用户角色设置为 network-admin，缺省情况下本地用户的用户角色为 network-operator。
- 因为需要以 Stelnet 客户端保存的主机公钥来验证 Stelnet 服务器，所以需要先将 Stelnet 服务器主机公钥配置在 Stelnet 客户端上。

5.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

5.4 配置步骤

5.4.1 Stelnet 服务器的配置

生成 RSA 密钥对。

```
<DeviceB> system-view
[DeviceB] public-key modulus create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[DeviceB] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

使能 SSH 服务器功能。

```
[DeviceB] ssh server enable
```

配置接口 GigabitEthernet2/0/1 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
[DeviceB] interface GigabitEthernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] ip address 192.168.1.40 255.255.255.0
[DeviceB-GigabitEthernet2/0/1] quit
```

设置 Stelnet 客户端登录用户界面的认证方式为 scheme。

```
[DeviceB] line vty 0 63
[DeviceB-line-vty0-63] authentication-mode scheme
[DeviceB-line-vty0-63] quit
```

创建本地用户 client001，并设置密码为明文 aabbcc，服务类型为 SSH，用户角色为 network-admin。

```
[DeviceB]local-user client001 class manage
New local user added.
[DeviceB-luser-manage-client001] password simple aabbcc
```

```
[DeviceB-luser-manage-client001]service-type ssh
[DeviceB-luser-manage-client001] authorization-attribute user-role network-admin
[DeviceB-luser-manage-client001]quit
```

显示服务器端 DSA 公钥内容。

```
[DeviceB] display public-key local dsa public

=====================================================
Key name: dsakey (default)
Key type: DSA
Time when key pair created: 11:02:10 2017/08/07
Key code:

   308201B73082017C06072A8648CE3804013082017F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF03818400028180077F06B3E343CAE9988F4BE3F76FACBAB565
   AB73D4BA295C52BA92428B1F2DA1E6DD652413DD3AFE0C5A4FCF365100CBE34CECA55A2C30
   A2A9FF7E899628557E39CE8FC615F53193A7E200B4B1CB21E3F1091D595716D229DDED6872
   061F9B4B08301ADC81F7EC1501FFB863C0009536596CCB508596C3325892DC6D8C5C35B5
```

5.4.2 Stelnet 客户端的配置

配置接口 GigabitEthernet2/0/1 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
[DeviceA] interface GigabitEthernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 192.168.1.56 255.255.255.0
[DeviceA-GigabitEthernet2/0/1] quit
```

指定服务器端的主机公钥名称为 key1，并进入公钥视图。

```
[DeviceA] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
```

在客户端配置服务器端的主机公钥(由于客户端缺省采用 DSA 主机公钥认证服务器，因此这里输入的是在服务器端通过 **display public-key local dsa public** 命令显示公钥内容。)

```
[DeviceA-pkey-public-key-key1]
   308201B73082017C06072A8648CE3804013082017F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF03818400028180077F06B3E343CAE9988F4BE3F76FACBAB565
   AB73D4BA295C52BA92428B1F2DA1E6DD652413DD3AFE0C5A4FCF365100CBE34CECA55A2C30
   A2A9FF7E899628557E39CE8FC615F53193A7E200B4B1CB21E3F1091D595716D229DDED6872
```

```
   061F9B4B08301ADC81F7EC1501FFB863C0009536596CCB508596C3325892DC6D8C5C35B5
```

退出公钥视图，并保存用户输入的公钥。

```
[DeviceA-pkey-public-key-key1] peer-public-key end
[DeviceA] return
```

5.5 验证配置

建立到服务器 192.168.1.40 的 SSH 连接，并指定服务器端的主机公钥 key1。输入正确的用户名和密码之后，即可成功登录到 Device B 上，用户角色为 network-admin。

```
<DeviceA> ssh2 192.168.1.40 public-key key1
login as: client001
client001@192.168.1.40's password:

******************************************************************************
* Copyright (c) 2004-2021 Hangzhou H3C Tech. Co., Ltd. All rights reserved.  *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************


<DeviceB>
```

5.6 配置文件

- DeviceA

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 192.168.1.56 255.255.255.0
#
public-key peer key1
public-key-code begin
308201B73082017C06072A8648CE3804013082017F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF03818400028180077F06B3E343CAE9988F4BE3F76FACBAB565
   AB73D4BA295C52BA92428B1F2DA1E6DD652413DD3AFE0C5A4FCF365100CBE34CECA55A2C30
   A2A9FF7E899628557E39CE8FC615F53193A7E200B4B1CB21E3F1091D595716D229DDED6872
   061F9B4B08301ADC81F7EC1501FFB863C0009536596CCB508596C3325892DC6D8C5C35B5
public-key-code end
peer-public-key end
#
```

- DeviceB

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 192.168.1.40 255.255.255.0
#
line vty 0 63
 authentication-mode scheme
#
ssh server enable
#
local-user client001
 password simple $c$3$o71Exx1XIKs9gJoxqSodHGl1uT9rlZEd4w==
 authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin
 service-type ssh
#
```

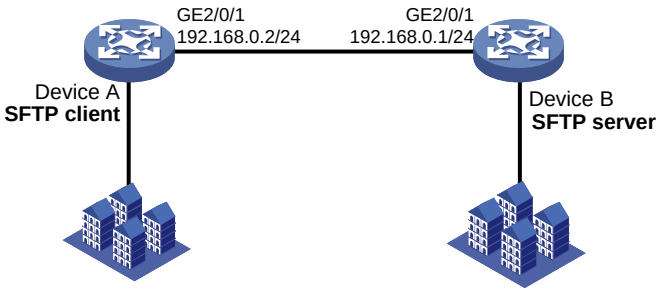
6 设备作为 SFTP 客户端配置举例（password-publickey 认证）

6.1 组网需求

如图 13 所示，Device A 和 Device B 之间建立 SSH 连接，Device A 作为 SFTP 客户端登录到 Device B，进行文件管理和文件传送等操作。要求：

- 为了保证高安全性和认证强度，要求 Device B 通过 password-publickey 认证方式对客户端进行认证，公钥算法为 RSA。
- 登录用户名为 client001，密码为 aabbcc，用户登录设备后可以正常使用所有命令。
- 服务器端通过从公钥文件中导入的方式来配置客户端的公钥。

图13 设备作为 SFTP 客户端配置组网图



6.2 配置思路

- 为了采用本地认证认证用户，需在本地 SFTP 服务器 DeviceB 上创建相应的本地用户，并在本地用户视图下配置密码。

- 服务器在采用 publickey 方式验证客户端身份时，首先要比较客户端发送的 SSH 用户名、主机公钥是否与本地配置的 SSH 用户名以及相应的客户端主机公钥一致，在确认用户名和客户端主机公钥正确后，再对客户端发送的数字签名进行验证，而该签名是客户端利用主机公钥对应的私钥计算出的。因此，需要在服务器端配置客户端的 RSA 主机公钥，并在客户端为该 SSH 用户指定与主机公钥对应的 RSA 主机私钥（在向服务器发起连接时通过 identity-key 关键字指定公钥算法来实现）。
- 如果 SSH 服务器采用 publickey 方式认证客户端，必须在 SFTP 服务器上创建相应的 SSH 用户，以及同名的本地用户（用于下发授权属性：工作目录、用户角色）。
- 在服务器的配置过程中需要指定客户端的公钥信息，因此需要首先完成客户端密钥对的配置，再进行服务器的配置。
- 因为 SFTP 用户登录设备后要能正常使用所有命令，所以将用户的用户角色设置为 network-admin，缺省情况下本地用户的用户角色为 network-operator。

6.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

6.4 配置注意事项

- FIPS 模式下，设备作为 SSH 服务器不支持 publickey 认证方式。
- 虽然一个客户端只会采用 RSA、DSA 公钥算法中的一种来认证服务器，但是由于不同客户端支持的公钥算法不同，为了确保客户端能够成功登录服务器，建议在服务器上同时生成 RSA、DSA 密钥对。

6.5 配置步骤

6.5.1 SFTP 客户端的配置

配置接口 GigabitEthernet2/0/1 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
<DeviceA> system-view
[DeviceA] interface GigabitEthernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 192.168.0.2 255.255.255.0
[DeviceA-GigabitEthernet2/0/1] quit
```

生成 RSA 密钥对。

```
[DeviceA] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.
Create the key pair successfully.
```

将生成的 RSA 主机公钥导出到指定文件 key.pub 中。

```
[DeviceA] public-key local export rsa ssh2 key.pub
[DeviceA] quit
```

6.5.2 配置 DeviceB 作为 FTP 服务器

配置接口 GigabitEthernet2/0/1 的 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface GigabitEthernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] ip address 192.168.0.1 255.255.255.0
[DeviceB-GigabitEthernet2/0/1] quit
```

在 Device 上创建一个 ftp 类型的本地用户，并设置密码为明文 ftp，服务类型为 FTP，用户角色为 network-admin，工作目录为 flash:/。

```
[DeviceB] local-user ftp class manage
New local user added.
[DeviceB-luser-manage-ftp] password simple ftp
[DeviceB-luser-manage-ftp] authorization-attribute user-role network-admin
[DeviceB-luser-manage-ftp] authorization-attribute work-directory flash:/
[DeviceB-luser-manage-ftp] service-type ftp
[DeviceB-luser-manage-ftp] quit
```

开启 Device 的 FTP 服务器功能。

```
[DeviceB] ftp server enable
[DeviceB] quit
```

6.5.3 配置客户端 DeviceA 上传公钥文件

DeviceA 通过 FTP 登录并上传 flash:/路径下的公钥文件 key.pub 到 Device。

```
<DeviceA>ftp 192.168.0.1
Press CTRL+C to abort.
Connected to 192.168.0.1 (192.168.0.1).
220 FTP service ready.
User (192.168.0.2:(none)): ftp
331 Password required for ftp.
Password:
230 User logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put flash:/key.pub
227 Entering Passive Mode (192,168,0,1,41,116)
150 Accepted data connection
226 File successfully transferred
301 bytes sent in 0.000 seconds (1.05 Mbytes/s)
ftp> quit
221-Goodbye. You uploaded 1 and downloaded 0 kbytes.
221 Logout.
```

6.5.4 配置 Device B 作为 SFTP 服务器

生成 RSA 密钥对。

```
<DeviceB> system-view
[DeviceB] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
```

```
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[DeviceB] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

启动 SFTP 服务器。

```
[DeviceB] sftp server enable
```

从文件 key.pub 中导入远端的公钥，并命名为 devicekey。

```
[DeviceB] public-key peer devicekey import sshkey key.pub
```

设置 SSH 用户 client001 的服务类型为 SFTP，认证方式为 password-publickey，并指定公钥为 devicekey。

```
[DeviceB] ssh user client001 service-type sftp authentication-type password-publickey assign
publickey devicekey
```

创建设备管理类本地用户 client001，并设置密码为明文 aabbcc，服务类型为 SSH，用户角色为 network-admin，工作目录为 flash:/。

```
[DeviceB] local-user client001 class manage
New local user added.
[DeviceB-luser-manage-client001] password simple aabbcc
[DeviceB-luser-manage-client001] service-type ssh
[DeviceB-luser-manage-client001] authorization-attribute user-role network-admin
work-directory flash:/
[DeviceB-luser-manage-client001] quit
```

6.6 验证配置

与远程 SFTP 服务器建立连接。

```
<DeviceA >sftp 192.168.0.1 identity-key rsa
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
client001@192.168.0.1's password:
```

输入用户密码 aabbcc 后进入 SFTP 客户端视图。

```
sftp>
```

显示服务器的当前目录，删除文件 z，并检查此文件是否删除成功。

```
sftp> dir -l
-rwxrwxrwx    1 1        1             1759 Aug 23 06:52 config.cfg
-rw-rw----    1 1        1              301 Aug  7 16:52 key.pub
-rwxrwxrwx    1 1        1                0 Sep 01 06:22 new
-rwxrwxrwx    1 1        1              225 Sep 01 06:55 pub
-rwxrwxrwx    1 1        1              225 Aug 24 08:01 pubkey2
-rwxrwxrwx    1 1        1                0 Sep 01 08:00 z
sftp> delete z
Removing /z
sftp> dir -l
-rwxrwxrwx    1 1        1             1759 Aug 23 06:52 config.cfg
-rw-rw----    1 1        1              301 Aug  7 16:52 key.pub
-rwxrwxrwx    1 1        1                0 Sep 01 06:22 new
-rwxrwxrwx    1 1        1              225 Sep 01 06:55 pub
-rwxrwxrwx    1 1        1              225 Aug 24 08:01 pubkey2
```

新增目录 new1，并检查新目录是否创建成功。

```
sftp> mkdir new1
sftp> dir -l
-rwxrwxrwx    1 1        1             1759 Aug 23 06:52 config.cfg
-rw-rw----    1 1        1              301 Aug  7 16:52 key.pub
-rwxrwxrwx    1 1        1                0 Sep 01 06:22 new
drwxrwxrwx    1 1        1                0 Sep 02 06:30 new1
-rwxrwxrwx    1 1        1              225 Sep 01 06:55 pub
-rwxrwxrwx    1 1        1              225 Aug 24 08:01 pubkey2
```

将目录名 new1 更名为 new2，并查看是否更名成功。

```
sftp> rename new1 new2
sftp> dir -l
-rwxrwxrwx    1 1        1             1759 Aug 23 06:52 config.cfg
-rw-rw----    1 1        1              301 Aug  7 16:52 key.pub
-rwxrwxrwx    1 1        1                0 Sep 01 06:22 new
drwxrwxrwx    1 1        1                0 Sep 02 06:33 new2
-rwxrwxrwx    1 1        1              225 Sep 01 06:55 pub
-rwxrwxrwx    1 1        1              225 Aug 24 08:01 pubkey2
```

从服务器上下载文件 pubkey2 到本地，并更名为 public。

```
sftp> get pubkey2 public
Fetching /pubkey2 to public
/public                                       100%  301     0.3KB/s   00:00
```

将本地文件 public 上传到服务器上，并查看上传是否成功。

```
sftp> put public
Uploading public to /public
public                                        100%  301     0.3KB/s   00:00
sftp> dir -l
-rwxrwxrwx    1 1        1             1759 Aug 23 06:52 config.cfg
-rw-rw----    1 1        1              301 Aug  7 16:52 key.pub
-rwxrwxrwx    1 1        1                0 Sep 01 06:22 new
drwxrwxrwx    1 1        1                0 Sep 02 06:33 new2
-rwxrwxrwx    1 1        1              225 Sep 01 06:55 pub
```

```
-rwxrwxrwx    1 1        1              225 Aug 24 08:01 pubkey2
-rwxrwxrwx    1 1        1              301 Jul 30 16:21 public
sftp>
```

退出 SFTP 客户端视图。

```
sftp> quit
<DeviceA>
```

6.7 配置文件

- DeviceA

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 192.168.0.2 255.255.255.0
#
```

- DeviceB

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 192.168.0.1 255.255.255.0
#
sftp server enable
ssh user client001 service-type sftp authentication-type password-publickey assign
publickey devicekey
#
local-user client001 class manage
 service-type ssh
 password simple $c$3$o71Exx1XIKs9gJoxqSodHGl1uT9rlZEd4w==
 authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin
#
ftp server enable
#
 local-user ftp class manage
  password simple ftp
  service-type ftp
  authorization-attribute user-role network-admin
  authorization-attribute user-role network-operator
#
public-key peer devicekey
 public-key-code begin
30819F300D06092A864886F70D010101050003818D00308189
1BD316C0DBB9009503E78F31947B651F9950E9A6E9E256E1E
 public-key-code end
 peer-public-key end
#
```

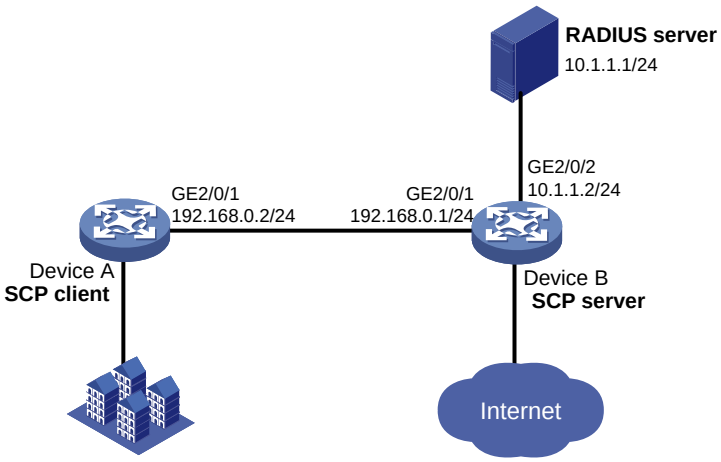
7 SCP 文件传输配置举例（password 认证）

7.1 组网需求

如图 14 所示，Device A 作为 SCP 客户端，Device B 作为 SCP 服务器。要求：

- 采用 password 认证方式对 SCP 客户端进行远程认证，用户能够通过 Device A 安全地登录到 Device B 上。
- 采用 RADIUS 服务器对登录 Device B 的 SCP 用户 Device A 进行认证和授权，登录用户名为 hello@bbb，密码为 aabbcc，Device A 登录 Device B 后可以正常使用所有命令；
- Device B 向 RADIUS 服务器发送的用户名带域名。

图14 SCP 文件传输配置组网图



7.2 配置思路

- 为了使 SSH 的版本协商和算法协商过程正常运行，且为了保证客户端对连接的服务器的认证正常进行，请在服务器端生成 RSA、DSA 密钥对。
- 采用 RADIUS 服务器对登录 Device B 的 SCP 用户 Device A 进行认证，需要在 RADIUS 服务器上添加用户名和密码。
- 为保证 RADIUS 客户端和 RADIUS 服务器之间信息交互的安全性，且为了防止用户密码在不安全的网络上传递时被窃取，需要在 Device B 和 RADIUS 服务器上设置相同的共享密钥。
- 为了使 Device A 登录 Device B 后可以正常使用所有命令，在 RADIUS 服务器上设置用户角色为 network-admin。
- 为了实现通过 RADIUS 来进行认证和授权，需要在 Device B 上配置 RADIUS 方案指定相应的认证和授权服务器，并配置认证 SSH 用户的 ISP 域。

7.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

7.4 配置步骤

7.4.1 配置 RADIUS 服务器

说明

本文以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.0(E0102)、iMC EIA 7.0(E0201)），说明该例中 RADIUS 服务器的基本配置。

1. 增加接入设备

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击“增加”按钮，进入增加接入设备页面。

- 设置认证及计费的端口号分别为“1812”（RADIUS 服务器的认证端口为 UDP 端口 1812）和“1813”（RADIUS 服务器的计费端口为 UDP 端口 1813）；
- 选择业务类型为“设备管理业务”；
- 选择接入设备类型为“H3C(General)”；
- 设置与 Device 交互报文时使用的认证和授权共享密钥为“expert”；
- 选择或手工增加接入设备，添加 IP 地址为 10.1.1.2 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图15 增加接入设备

2. 增加设备管理用户

选择“用户”页签，单击导航树中的[接入用户管理视图/设备管理用户]菜单项，进入设备管理用户列表页面，在该页面中单击<增加>按钮，进入增加设备管理用户页面。

- 输入用户名“hello@bbb”和密码“aabbcc”。
- 选择服务类型为“SSH”。
- 输入用户角色名“network-admin”
- 添加所管理设备的 IP 地址，IP 地址范围为“10.1.1.0～10.1.1.255”。
- 单击<确定>按钮完成操作。

图16 增加设备管理用户

7.4.2 配置 Device B

生成 RSA 密钥对。

```
<DeviceB> system-view
[DeviceB] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[DeviceB] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

配置接口 GigabitEthernet2/0/1 的 IP 地址，客户端将通过该地址连接 SCP 服务器。

```
[DeviceB] interface GigabitEthernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] ip address 192.168.0.1 255.255.255.0
[DeviceB-GigabitEthernet2/0/1] quit
```

配置接口 GigabitEthernet2/0/2 的 IP 地址。

```
[DeviceB] interface GigabitEthernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] ip address 10.1.1.2 255.255.255.0
```

```
[DeviceB-GigabitEthernet2/0/2] quit
```
使能 SSH 服务器功能。
```
[DeviceB] ssh server enable
```
创建 RADIUS 方案 rad。
```
[DeviceB] radius scheme rad
```
配置主认证服务器的 IP 地址为 10.1.1.1，认证端口号为 1812。
```
[DeviceB-radius-rad] primary authentication 10.1.1.1 1812
```
配置主计费服务器的 IP 地址为 10.1.1.1，计费端口号为 1813。
```
[DeviceB-radius-rad] primary accounting 10.1.1.1 1813
```
配置与认证和计费服务器交互报文时的共享密钥为明文 expert。
```
[DeviceB-radius-rad] key authentication simple expert
[DeviceB-radius-rad] key accounting simple expert
```
配置向 RADIUS 服务器发送的用户名要携带域名。
```
[DeviceB-radius-rad] user-name-format with-domain
[DeviceB-radius-rad] quit
```
创建 ISP 域 bbb，为 login 用户配置 AAA 认证方法为 RADIUS 认证、授权和计费。
```
[DeviceB] domain bbb
[DeviceB-isp-bbb] authentication login radius-scheme rad
[DeviceB-isp-bbb] authorization login radius-scheme rad
[DeviceB-isp-bbb] accounting login radius-scheme rad
[DeviceB-isp-bbb] quit
```

7.4.3 配置 Device A

配置接口 GigabitEthernet2/0/1 的 IP 地址。
```
<DeviceA> system-view
[DeviceA] interface GigabitEthernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 192.168.0.2 255.255.255.0
[DeviceA-GigabitEthernet2/0/1] quit
[DeviceA] quit
```

7.5 验证配置

与远程 SCP 服务器建立连接，并下载远端的 remote.bin 文件，下载到本地后更名为 local.bin。
```
<DeviceA> scp 192.168.0.1 get remote.bin local.bin
Username: hello@bbb
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
hello@bbb@192.168.0.1's password:
remote.bin                    100% 8275KB 318.3KB/s   00:26.
```

7.6 配置文件

- DeviceA：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 192.168.0.2 255.255.255.0
#
```

- DeviceB：

```
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet2/0/2
 port link-mode route
 ip address 10.1.1.2 255.255.255.0
#
ssh server enable
#
radius scheme rad
 primary authentication 10.1.1.1
 primary accounting 10.1.1.1
 key authentication cipher $c$3$63G7LzIQElGq4aFGTiYQafU+loQxS/cbLg==
 key accounting cipher $c$3$tUIVlyGISJ5X/yiTFWrmh8nyjBIF+1LFzQ==
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
 accounting login radius-scheme rad
#
```

8 相关资料

- H3C SR6600 SR6600-X 路由器 安全配置指导-R7607
- H3C SR6600 SR6600-X 路由器 安全命令参考-R7607

H3C SR6600/SR6600-X 系列路由器

VRRP 配置举例

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1

2 配置前提 1

3 IPv4 VRRP 单备份组配置举例 1

3.1 组网需求 1

3.2 配置思路 2

3.3 使用版本 2

3.4 配置注意事项 2

3.5 配置步骤 2

3.6 验证配置 3

3.7 配置文件 5

4 IPv4 VRRP 多备份组配置举例 5

4.1 组网需求 5

4.2 配置思路 6

4.3 使用版本 6

4.4 配置注意事项 6

4.5 配置步骤 7

4.6 验证配置 8

4.7 配置文件 11

5 IPv4 VRRP 负载均衡模式配置举例 12

5.1 组网需求 12

5.2 配置思路 13

5.3 使用版本 13

5.4 配置注意事项 13

5.5 配置步骤 14

5.5.1 Device A 的配置 14

5.5.2 Device B 的配置 15

5.5.3 Device C 的配置 15

5.5.4 验证配置 16

5.5.5 配置文件 22

6 IPv4 VRRP with IPsec 配置举例 23

6.1 组网需求 23

6.2 配置思路 24

6.3 使用版本 24
6.4 配置注意事项 24
6.5 配置步骤 24
6.5.1 Device A 的配置 24
6.5.2 Device B 的配置 26
6.5.3 Device C 的配置 27
6.6 验证配置 29
6.7 配置文件 32
7 IPv6 VRRP 单备份组配置举例 35
7.1 组网需求 35
7.2 配置思路 35
7.3 使用版本 36
7.4 配置注意事项 36
7.5 配置步骤 36
7.6 验证配置 37
7.7 配置文件 39
8 IPv6 VRRP 多备份组配置举例 40
8.1 组网需求 40
8.2 配置思路 41
8.3 使用版本 41
8.4 配置注意事项 41
8.5 配置步骤 42
8.6 验证配置 43
8.7 配置文件 47
9 IPv6 VRRP 负载均衡模式配置举例 48
9.1 组网需求 48
9.2 配置思路 49
9.3 使用版本 49
9.4 配置注意事项 49
9.5 配置步骤 50
9.5.1 Device A 的配置 50
9.5.2 Device B 的配置 51
9.5.3 Device C 的配置 51
9.5.4 验证配置 52
9.5.5 配置文件 58

10 相关资料 ·····59

1 简介

本文档介绍 VRRP 的配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 VRRP 特性。

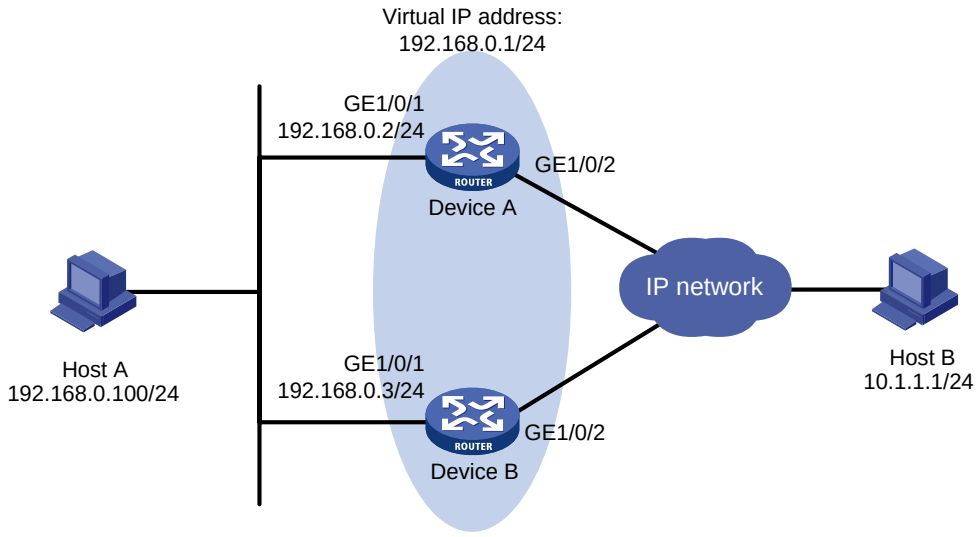
3 IPv4 VRRP 单备份组配置举例

3.1 组网需求

如图 1 所示，Host A 所在网络的出口处部署了两台网关设备。现要求使用 VRRP 主备备份功能，将这两台设备组成一台虚拟路由器，作为 Host A 的缺省网关。具体应用需求如下：

- 在正常情况下，由 Device A 承担网关功能，转发 Host A 发送至外网的流量；
- 当 Device A 或者 Device A 的上行接口出现故障时，由 Device B 接替 Device A 承担网关功能；
- 当 Device A 或者 Device A 的上行接口故障恢复后，由 Device A 继续承担网关功能。

图1 IPv4 VRRP 单备份组配置组网图



3.2 配置思路

- 为了让 Device A 成为 Master，需要为 Device A 配置较高的优先级；
- 将 VRRP 组的抢占模式和监视上行接口状态功能结合使用，可以使 Master 设备根据上行接口的状态自动调整自身的 VRRP 优先级，从而使 VRRP 组内的角色发生转变，实现主备切换；
- 为了避免 VRRP 备份组中的角色频繁发生变化，可以配置一定的抢占延迟时间。

3.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

3.4 配置注意事项

- 备份组的虚拟 IP 地址不能为全零地址(0.0.0.0)、广播地址(255.255.255.255)、环回地址、非 A/B/C 类地址和其它非法 IP 地址(如 0.0.0.1)。
- IPv4 VRRP 既可以使用 VRRPv2 版本，也可以使用 VRRPv3 版本（缺省情况使用 VRRPv3）。请确保 IPv4 VRRP 备份组中的所有路由器上配置的 IPv4 VRRP 版本一致，否则备份组无法正常工作。
- 建议将备份组的虚拟 IP 地址和备份组中设备下行接口的 IP 地址配置为同一网段，否则可能导致局域网内的主机无法访问外部网络。
- 删除 IP 地址拥有者上的 VRRP 备份组，将导致地址冲突。建议先修改配置了备份组的接口的 IP 地址，再删除该接口上的 VRRP 备份组，以避免地址冲突。
- 对于同一个 VRRP 备份组的成员设备，必须保证虚拟路由器的 IP 地址配置完全一样。
- 用户在配置降低优先级幅度时，需要确保降低后的优先级比备份组内其他设备的优先级要低，确保备份组内有其他设备被选为 Master。

3.5 配置步骤

(1) Device A 的配置

配置接口 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 192.168.0.2 24
```

创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 192.168.0.1。

```
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 virtual-ip 192.168.0.1
```

设置 Device A 在 VRRP 备份组 1 中的优先级为 110，高于 Device B 的优先级 100，以保证 Device A 成为 Master 负责转发流量。

```
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 priority 110
```

设置 Device A 工作在抢占方式，以保证 Device A 故障恢复后，能再次抢占成为 Master，即只要 Device A 正常工作，就由 Device A 负责转发流量。为了避免频繁地进行状态切换，配置抢占延迟时间为 5 秒。

```
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 preempt-mode delay 500
[DeviceA-GigabitEthernet1/0/1] quit
```

创建和上行接口 GigabitEthernet 1/0/2 关联的 Track 项 1。

```
[DeviceA] track 1 interface gigabitethernet 1/0/2
```

配置监视 Track 项 1，Track 项的状态为 Negative 时，Device A 在 VRRP 备份组中的优先级降低的数值为 50。

```
[DeviceA] interface gigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 track 1  priority reduced 50
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) Device B 的配置

配置接口 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 192.168.0.3 24
```

创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 192.168.0.1。

```
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 1 virtual-ip 192.168.0.1
```

设置 Device B 在 VRRP 备份组 1 中的优先级为 100。

```
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 1 priority 100
```

设置 Device B 工作在抢占方式，抢占延迟时间为 5 秒。

```
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 1 preempt-mode delay 500
[DeviceB-GigabitEthernet1/0/1] quit
```

3.6 验证配置

配置完成后，在 Host A 上可以 ping 通 Host B。

通过 **display vrrp verbose** 命令查看配置后的结果，显示 Device A 上 VRRP 备份组 1 的详细信息。

```
[DeviceA] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                    Adver Timer   : 100
     Admin Status   : Up                   State         : Master
     Config Pri     : 110                  Running Pri   : 110
     Preempt Mode   : Yes                  Delay Time    : 500
     Auth Type      : None
     Virtual IP     : 192.168.0.1
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 192.168.0.2
   VRRP Track Information:
     Track Object   : 1                  State : Positive   Pri Reduced : 50
```

通过 **display vrrp verbose** 命令查看配置后的结果，显示 Device B 上 VRRP 备份组 1 的详细信息。

```
[DeviceB] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
```

```
  Interface GigabitEthernet1/0/1
    VRID           : 1                    Adver Timer  : 100
    Admin Status   : Up                   State        : Backup
    Config Pri     : 100                  Running Pri  : 100
    Preempt Mode   : Yes                  Delay Time   : 500
    Become Master  : 412ms left
    Auth Type      : None
    Virtual IP     : 192.168.0.1
    Master IP      : 192.168.0.2
```

以上显示信息表示在 VRRP 备份组 1 中 Device A 为 Master 路由器，Device B 为 Backup 路由器，Host A 发送给 Host B 的报文通过 Device A 转发。

Device A 出现故障后，在 Host A 上仍然可以 ping 通 Host B。

通过 **display vrrp verbose** 命令查看 Device B 上 VRRP 备份组的详细信息，Device A 出现故障后，显示 Device B 上 VRRP 备份组 1 的详细信息。

```
[DeviceB] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                    Adver Timer  : 100
     Admin Status   : Up                   State        : Master
     Config Pri     : 100                  Running Pri  : 100
     Preempt Mode   : Yes                  Delay Time   : 500
     Auth Type      : None
     Virtual IP     : 192.168.0.1
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 192.168.0.3
```

以上显示信息表示 Device A 出现故障后，Device B 成为 Master 路由器，Host A 发送给 Host B 的报文通过 Device B 转发。

Device A 故障恢复后，显示 Device A 上 VRRP 备份组 1 的详细信息。

```
[DeviceA] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                    Adver Timer  : 100
     Admin Status   : Up                   State        : Master
     Config Pri     : 110                  Running Pri  : 110
     Preempt Mode   : Yes                  Delay Time   : 500
     Auth Type      : None
     Virtual IP     : 192.168.0.1
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 192.168.0.2
   VRRP Track Information:
     Track Object   : 1                  State : Positive   Pri Reduced : 50
```

以上显示信息表示 Device A 故障恢复后，Device A 会抢占成为 Master，Host A 发送给 Host B 的报文仍然通过 Device A 转发。

3.7 配置文件

- Device A：

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.0.1
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode delay 500
 vrrp vrid 1 track 1 priority reduced 50
#
 track 1 interface gigabitethernet 1/0/2
#
```

- Device B：

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.0.3 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.0.1
 vrrp vrid 1 priority 100
 vrrp vrid 1 preempt-mode delay 500
#
```

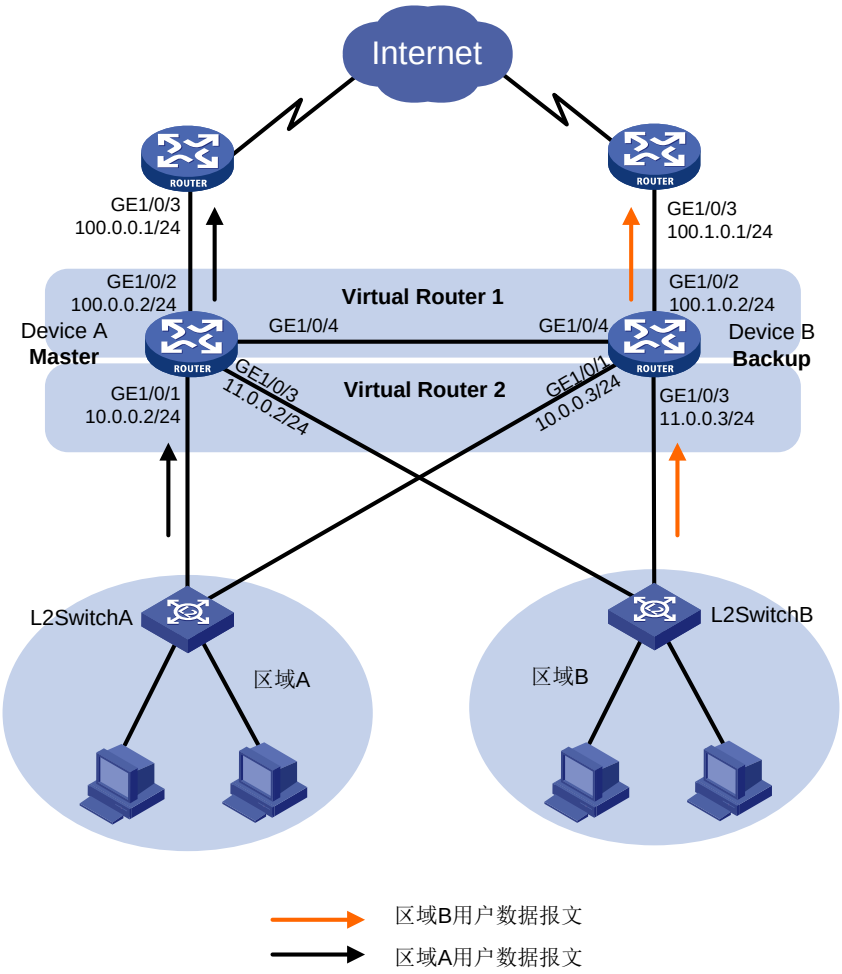
4 IPv4 VRRP 多备份组配置举例

4.1 组网需求

如图 2 所示，某公司为了实现网关设备的冗余备份，以及内网主机流量的负载分担，在内部网络的出口处部署了两台设备，并使用 VRRP 负载分担功能，将这两台设备组成两台虚拟路由器，分别作为区域 A 和区域 B 的缺省网关。具体应用需求如下：

- Device A 是 VRRP 备份组 1 中的 Master 设备，Device B 是 VRRP 备份组 2 中的 Master 设备。在正常情况下，区域 A 的用户通过 Device A 进行数据转发，区域 B 的用户通过 Device B 进行数据转发。
- 当 Device A 或者 Device A 的上行接口发生故障后，Device B 能够迅速承担区域 A 内主机流量的转发任务；Device A 故障恢复后，继续承担 VRRP 备份组 1 的网关功能；
- 当 Device B 或者 Device B 的上行接口故障发生故障后，Device A 能够迅速承担区域 B 内主机流量的转发任务；Device B 故障恢复后，继续承担 VRRP 备份组 2 的网关功能。

图2 IPv4 VRRP 多备份组配置组网图



4.2 配置思路

- 为了让 Device A 和 Device B 分别成为 VRRP 备份组 1 和 VRRP 备份组 2 中的 Master，需要在 VRRP 备份组 1 中为 Device A 配置较高的优先级，在 VRRP 备份组 2 中为 Device B 配置较高的优先级。
- 为了避免 VRRP 备份组中的角色频繁发生变化，可以配置一定的抢占延迟时间。

4.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

4.4 配置注意事项

- VRRP 备份组的虚拟 IP 地址不能为全零地址(0.0.0.0)、广播地址(255.255.255.255)、环回地址、非 A/B/C 类地址和其它非法 IP 地址(如 0.0.0.1)。

- IPv4 VRRP 既可以使用 VRRPv2 版本，也可以使用 VRRPv3 版本（缺省情况使用 VRRPv3）。请确保 IPv4 VRRP 备份组中的所有路由器上配置的 IPv4 VRRP 版本一致，否则 VRRP 备份组无法正常工作。
- 建议将备份组的虚拟 IP 地址和备份组中设备下行接口的 IP 地址配置为同一网段，否则可能导致局域网内的主机无法访问外部网络。
- 删除 IP 地址拥有者上的 VRRP 备份组，将导致地址冲突。建议先修改配置了 VRRP 备份组的接口的 IP 地址，再删除该接口上的 VRRP 备份组，以避免地址冲突。
- 用户在配置降低优先级幅度时，需要确保降低后的优先级比 VRRP 备份组内其他设备的优先级要低，确保 VRRP 备份组内有其他设备被选为 Master 设备。
- 对于同一个 VRRP 备份组的成员设备，如下配置必须保证完全一样：
  - 虚拟路由器的 IP 地址个数
  - 每个备份组虚拟路由器的 IP 地址
  - 定时器间隔时间

4.5 配置步骤

(1) Device A 的配置

配置接口 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 10.0.0.2 24
```

请参考以上方法配置 4.1 图 2 中其它接口的 IP 地址，配置步骤这里省略。

创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 10.0.0.1，并配置 Device A 在 VRRP 备份组 1 中的优先级为 120，高于 Device B 的优先级。

```
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 virtual-ip 10.0.0.1
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 priority 120
[DeviceA-GigabitEthernet1/0/1] quit
```

创建 VRRP 备份组 2，并配置 VRRP 备份组 2 的虚拟 IP 地址为 11.0.0.1。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] vrrp vrid 2 virtual-ip 11.0.0.1
[DeviceA-GigabitEthernet1/0/3] quit
```

设置 Device A 工作在抢占方式，配置抢占延迟时间为 5 秒。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 preempt-mode delay 500
[DeviceA-GigabitEthernet1/0/1] quit
```

创建和上行接口 GigabitEthernet 1/0/2 关联的 Track 项 1。

```
[DeviceA] track 1 interface gigabitethernet 1/0/2
```

配置监视 Track 项 1，Track 项的状态为 Negative 时，Device A 在 VRRP 备份组 1 中的优先级降低的数值为 50。

```
[DeviceA] interface gigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 track 1 priority  reduced 50
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) Device B 的配置

```
<DeviceB> system-view
[DeviceB] interface gigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 10.0.0.3 24
```

请参考以上方法配置 4.1 图 2 中其它接口的 IP 地址，配置步骤省略。

创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 10.0.0.1。

```
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 1 virtual-ip 10.0.0.1
[DeviceB-GigabitEthernet1/0/1] quit
```

创建 VRRP 备份组 2，并配置 VRRP 备份组 2 的虚拟 IP 地址为 11.0.0.1，并配置 Device B 在 VRRP 备份组 2 中的优先级为 120，高于 Device A 的优先级。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] vrrp vrid 2 virtual-ip 11.0.0.1
[DeviceB-GigabitEthernet1/0/3] vrrp vrid 2 priority 120
```

设置 Device B 工作在抢占方式，配置抢占延迟时间为 5 秒。

[DeviceB-GigabitEthernet1/0/3] vrrp vrid 2 preempt-mode delay 500

[DeviceB-GigabitEthernet1/0/3] quit

创建和上行接口 GigabitEthernet 1/0/2 关联的 Track 项 2。

```
[DeviceB] track 2 interface gigabitethernet 1/0/2
```

配置监视 Track 项 2，Track 项的状态为 Negative 时，Device B 在 VRRP 备份组 2 中的优先级降低的数值为 50。

```
[DeviceB] interface gigabitEthernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] vrrp vrid 2 track 2 priority reduced 50
[DeviceB-GigabitEthernet1/0/3] quit
```

4.6 验证配置

(1) 配置完成后，区域 A 和区域 B 中的主机都可以 ping 通外网。

检查区域 A 的主机到目的端 100.0.0.1 是否可达。

```
<host A> ping 100.0.0.1
PING 100.0.0.1 (100.0.0.1): 56 data bytes
56 bytes from 100.0.0.1: seq=0 ttl=128 time=22.43 ms
56 bytes from 100.0.0.1: seq=1 ttl=128 time=7.17 ms
56 bytes from 100.0.0.1: seq=2 ttl=128 time=8.91 ms
56 bytes from 100.0.0.1: seq=3 ttl=128 time=7.45 ms
56 bytes from 100.0.0.1: seq=4 ttl=128 time=9.11 ms

--- 100.0.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.17/11.01/22.43 ms
```

检查区域 B 的主机到目的端 100.1.0.1 是否可达。

```
<host C> ping 100.1.0.1
PING 100.1.0.1 (100.1.0.1): 56 data bytes
56 bytes from 100.1.0.1: seq=0 ttl=128 time=22.43 ms
56 bytes from 100.1.0.1: seq=1 ttl=128 time=7.17 ms
56 bytes from 100.1.0.1: seq=2 ttl=128 time=8.91 ms
56 bytes from 100.1.0.1: seq=3 ttl=128 time=7.45 ms
```

```
56 bytes from 100.1.0.1: seq=4 ttl=128 time=9.11 ms

--- 100.1.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.17/11.01/22.43 ms
```

(2) 通过 **display vrrp verbose** 命令查看配置后的结果。

查看 Device A 上全部 IPv4 VRRP 备份组的详细信息，显示 Device A 在 VRRP 备份组 1 中为 Master 设备，在 VRRP 备份组 2 中为 Backup 设备。

```
[DeviceA] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode       : Standard
 Total number of virtual routers : 2
   Interface GigabitEthernet1/0/1
     VRID           : 1                    Adver Timer  : 100
     Admin Status   : Up                   State        : Master
     Config Pri     : 120                  Running Pri  : 120
     Preempt Mode   : Yes                  Delay Time   : 500
     Auth Type      : None
     Virtual IP     : 10.0.0.1
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 10.0.0.2
   VRRP Track Information:
     Track Object   : 1                  State : Positive   Pri Reduced : 50

   Interface GigabitEthernet1/0/3
     VRID           : 2                    Adver Timer  : 100
     Admin Status   : Up                   State        : Backup
     Config Pri     : 100                  Running Pri  : 100
     Preempt Mode   : Yes                  Delay Time   : 0
     Auth Type      : None
     Become Master  : 3550ms left
     Virtual IP     : 11.0.0.1
     Master IP      : 11.0.0.3
```

查看 Device B 上全部 IPv4 VRRP 备份组的详细信息，显示 Device B 在备份组 1 中为 Backup 设备，在备份组 2 中为 Master 设备。

```
[DeviceB] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode       : Standard
 Total number of virtual routers : 2
   Interface GigabitEthernet1/0/1
     VRID           : 1                    Adver Timer  : 100
     Admin Status   : Up                   State        : Backup
     Config Pri     : 100                  Running Pri  : 100
     Preempt Mode   : Yes                  Delay Time   : 0
     Auth Type      : None
     Become Master  : 3500ms left
     Virtual IP     : 10.0.0.1
```

```
    Master IP       : 10.0.0.2

  Interface GigabitEthernet1/0/3
    VRID            : 2                   Adver Timer  : 100
    Admin Status    : Up                  State        : Master
    Config Pri      : 120                 Running Pri  : 120
    Preempt Mode    : Yes                 Delay Time   : 500
    Auth Type       : None
    Virtual IP      : 11.0.0.1
    Virtual MAC     : 0000-5e00-0102
    Master IP       : 11.0.0.3
  VRRP Track Information:
    Track Object    : 2                   State : Positive   Pri Reduced : 50
```

Device A 出现故障后，通过 **display vrrp verbose** 命令查看 Device B 上备份组的详细信息。可以看到 Device B 抢占为备份组 1 的 Master。

```
[DeviceB] display vrrp verbose
IPv4 Virtual Router Information:
 Running  Mode       : Standard
 Total number of virtual routers : 2
   Interface GigabitEthernet1/0/1
     VRID            : 1                   Adver Timer  : 100
     Admin Status    : Up                  State        : Master
     Config Pri      : 100                 Running Pri  : 100
     Preempt Mode    : Yes                 Delay Time   : 0
     Auth Type       : None
     Virtual IP      : 10.0.0.1
     Virtual MAC     : 0000-5e00-0101
     Master IP       : 10.0.0.3

   Interface GigabitEthernet1/0/3
     VRID            : 2                   Adver Timer  : 100
     Admin Status    : Up                  State        : Master
     Config Pri      : 120                 Running Pri  : 120
     Preempt Mode    : Yes                 Delay Time   : 500
     Auth Type       : None
     Virtual IP      : 11.0.0.1
     Virtual MAC     : 0000-5e00-0102
     Master IP       : 11.0.0.3
   VRRP Track Information:
     Track Object    : 2                   State : Positive   Pri Reduced : 50
```

以上显示信息表示 Device A 出现故障后，区域 A 和区域 B 中的主机仍然可以 ping 通外网。

当 Device A 故障恢复后，显示 Device A 上备份组的详细信息。

```
[DeviceA] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
   Interface GigabitEthernet1/0/1
```

```
    VRID            : 1                 Adver Timer   : 100
    Admin Status    : Up                State         : Master
    Config Pri      : 120               Running Pri   : 120
    Preempt Mode    : Yes               Delay Time    : 500
    Auth Type       : None
    Virtual IP      : 10.0.0.1
    Virtual MAC     : 0000-5e00-0101
    Master IP       : 10.0.0.2
  VRRP Track Information:
    Track Object    : 1                 State : Positive   Pri Reduced : 50

  Interface GigabitEthernet1/0/3
    VRID            : 2                 Adver Timer   : 100
    Admin Status    : Up                State         : Backup
    Config Pri      : 100               Running Pri   : 100
    Preempt Mode    : Yes               Delay Time    : 0
    Become Master   : 3550ms left
    Auth Type       : None
    Virtual IP      : 11.0.0.1
    Master IP       : 11.0.0.3
```

以上显示信息表示当 Device A 故障恢复后，Device A 在 VRRP 备份组 1 中恢复为原来的优先级并抢占成为该备份组的 Master，区域 A 内的主机通过 Device A 与外界通信。

4.7 配置文件

- Device A：

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.0.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.1
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode delay 500
 vrrp vrid 1 track 1 priority reduced 50
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 100.0.0.2 255.255.255.0
 undo stp enable
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 11.0.0.2 255.255.255.0
 vrrp vrid 2 virtual-ip 11.0.0.1
#
 track 1 interface gigabitethernet 1/0/2
#
```

- Device B：

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.0.0.3 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.1
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 100.1.0.2 255.255.255.0
 undo stp enable
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 11.0.0.3 255.255.255.0
 vrrp vrid 2 priority 120
 vrrp vrid 2 preempt-mode delay 500
 vrrp vrid 2 track 2 priority reduced 50
#
 track 2 interface gigabitethernet 1/0/2
#
```

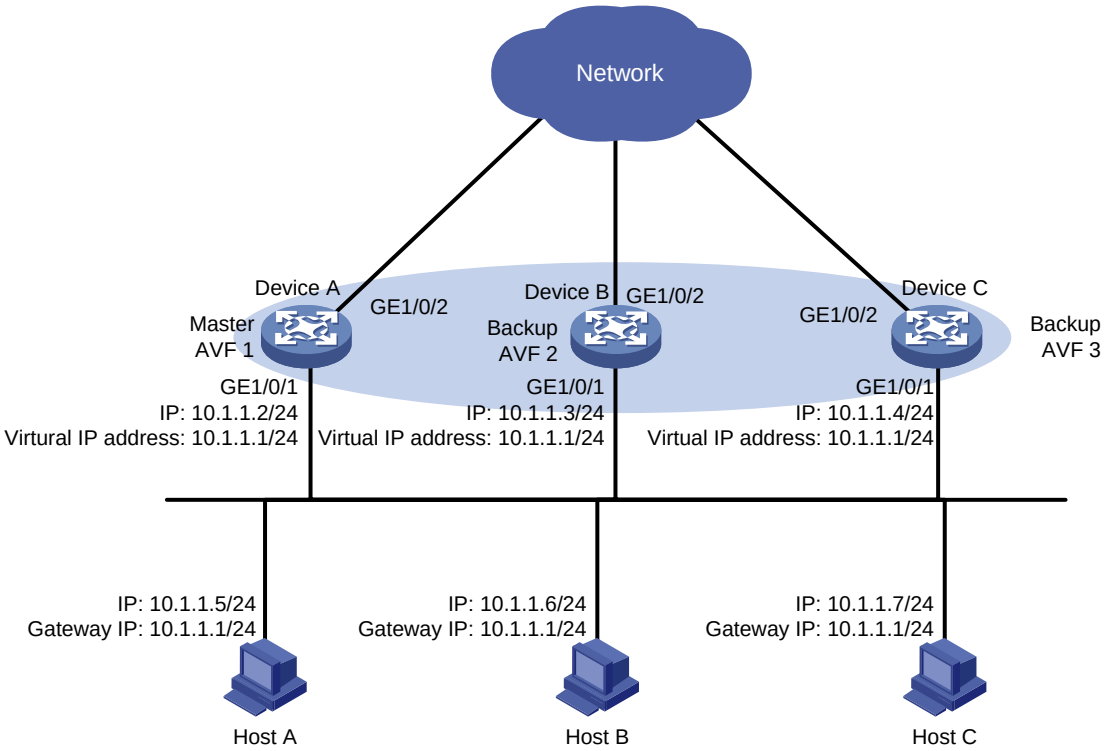
5 IPv4 VRRP 负载均衡模式配置举例

5.1 组网需求

如图 3 所示，Host A、Host B 和 Host C 所在网络的出口处部署了三台设备。现要求使用 VRRP 负载均衡功能，将 Device A、Device B 和 Device C 组成一台虚拟路由器，作为局域网内主机的缺省网关。具体应用需求如下：

- 实现 VRRP 备份组中三台设备都可以转发报文，实现流量负载分担，充分利用网关资源；
- 当 Device A、Device B 或 Device C 自身或其上行接口出现故障时，Host A、Host B 和 Host C 可以通过其他正常运行的设备继续通信，避免通信中断；当 Device A、Device B 或 Device C 故障恢复后，继续承担网关功能。

图3 IPv4 VRRP 负载均衡模式配置组网图



5.2 配置思路

- 为了使 Device A 优先与 Device B 和 Device C 被选举为 VRRP 备份组的 Master 设备，需要为其配置高于 Device B 和 Device C 的优先级；为了使 Device B 优先于 Device C 被选举为 VRRP 备份组的 Master 设备，需要为其配置高于 Device C 的优先级；
- 为了避免由于故障造成 VRRP 备份组中的角色频繁发生变化，可以配置一定的抢占延迟时间；
- 在 Device A、Device B 和 Device C 上配置虚拟转发器通过 Track 项监视上行接口的状态。当上行接口出现故障时，降低该接口所在设备虚拟转发器的权重，以便其他设备接管该设备的转发任务，避免通信中断；
- 为了保证原 Master 设备故障恢复后，能再次抢占成为 Master，需要配置 VRRP 备份组工作在抢占模式。

5.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

5.4 配置注意事项

- 建议将备份组的虚拟 IP 地址和备份组中设备下行接口的 IP 地址配置为同一网段，否则可能导致局域网内的主机无法访问外部网络。
- VRRP 备份组的虚拟 IP 地址不能为全零地址(0.0.0.0)、广播地址(255.255.255.255)、环回地址、非 A/B/C 类地址和其它非法 IP 地址(如 0.0.0.1)。

- IPv4 VRRP 既可以使用 VRRPv2 版本，也可以使用 VRRPv3 版本（缺省情况使用 VRRPv3）。请确保 IPv4 VRRP 备份组中的所有路由器上配置的 IPv4 VRRP 版本一致，否则 VRRP 备份组无法正常工作。
- VRRP 工作在负载均衡模式时，备份组的虚拟 IP 地址和接口的 IP 地址不能相同，否则 VRRP 负载均衡功能将无法正常工作。
- 当监视的上行链路出现故障时，配置的权重降低数额需保证 VF Owner 的权重低于失效下限，即权重降低的数额大于 245，其它的虚拟转发器才能接替 VF Owner 成为 AVF。
- 对于同一个 VRRP 备份组的成员设备，必须保证备份组虚拟路由器的 IP 地址配置完全一样。
- 用户在配置降低权重幅度时，需要确保降低后的优先级比 VRRP 备份组内其他设备的优先级要低，确保 VRRP 备份组内有其他设备被选为 Master。

5.5 配置步骤

5.5.1 Device A 的配置

(1) 配置接口

配置接口。

```
<DeviceA> system-view
[DeviceA] interface gigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 10.1.1.2 24
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 配置 VRRP

配置 VRRP 工作在负载均衡模式。

```
[DeviceA] vrrp mode load-balance
```

创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 10.1.1.1。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 virtual-ip 10.1.1.1
```

配置 Device A 在 VRRP 备份组 1 中的优先级为 120，高于 Device B 的优先级 110 和 Device C 的优先级 100，以保证 Device A 成为 Master。

```
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 priority 120
```

配置 Device A 工作在抢占方式，以保证 Device A 故障恢复后，能再次抢占成为 Master，即只要 Device A 正常工作，Device A 就会成为 Master。为了避免频繁地进行状态切换，配置抢占延迟时间为 5 秒。

```
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 preempt-mode delay 500
[DeviceA-GigabitEthernet1/0/1] quit
```

(3) 配置 Track

创建和 GigabitEthernet1/0/2 关联的 Track 项 1。如果 Track 项的状态为 Negative，则说明 Device A 的上行接口出现故障。

```
[DeviceA] track 1 interface gigabitethernet 1/0/2
```

配置虚拟转发器监视 Track 项 1。Track 项的状态为 Negative 时，降低 Device A 上虚拟转发器的权重，使其低于失效下限 10，即权重降低的数额大于 245，以便其他设备接替 Device A 的转发任务。本例中，配置虚拟转发器权重降低数额为 250。

```
[DeviceA] interface gigabitEthernet 1/0/1
```

```
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 track 1 weight reduced 250
[DeviceA-GigabitEthernet1/0/1] quit
```

5.5.2 Device B 的配置

(1) 配置接口

配置接口。

```
<DeviceB> system-view
[DeviceB] interface gigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 10.1.1.3 24
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitEthernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] quit
```

(2) 配置 VRRP

配置 VRRP 工作在负载均衡模式。

```
[DeviceB] vrrp mode load-balance
```

创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 10.1.1.1。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 1 virtual-ip 10.1.1.1
```

配置 Device B 在 VRRP 备份组 1 中的优先级为 110，高于 Device C 的优先级，以保证 Device A 出现故障时，Device B 成为 Master。

```
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 1 priority 110
```

配置 Device B 工作在抢占方式，抢占延迟时间为 5 秒。

```
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 1 preempt-mode delay 500
[DeviceB-GigabitEthernet1/0/1] quit
```

(3) 配置 Track

创建和 GigabitEthernet1/0/2 关联的 Track 项 1。如果 Track 项的状态为 Negative，则说明 Device B 的上行接口出现故障。

```
[DeviceB] track 1 interface gigabitethernet 1/0/2
```

配置虚拟转发器监视 Track 项 1。Track 项的状态为 Negative 时，降低 Device B 上虚拟转发器的权重，使其低于失效下限 10，即权重降低的数额大于 245，以便其他设备接替 Device B 的转发任务。本例中，配置虚拟转发器权重降低数额为 250。

```
[DeviceB] interface gigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 1 track 1 weight reduced 250
[DeviceB-GigabitEthernet1/0/1] quit
```

5.5.3 Device C 的配置

(1) 配置接口

配置接口。

```
<DeviceC> system-view
[DeviceC] interface gigabitEthernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ip address 10.1.1.4 24
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitEthernet 1/0/2
```

```
[DeviceC-GigabitEthernet1/0/2] quit
```

(2) 配置 VRRP

配置 VRRP 工作在负载均衡模式。

```
[DeviceA] vrrp mode load-balance
```

创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 10.1.1.1。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] vrrp vrid 1 virtual-ip 10.1.1.1
```

配置 Device C 工作在抢占方式，抢占延迟时间为 5 秒。

```
[DeviceC-GigabitEthernet1/0/1] vrrp vrid 1 preempt-mode delay 500
[DeviceC-GigabitEthernet1/0/1] quit
```

(3) 配置 Track

创建和 GigabitEthernet1/0/2 关联的 Track 项 1。如果 Track 项的状态为 Negative，则说明 Device C 的上行接口出现故障。

```
[DeviceC] track 1 interface gigabitethernet 1/0/2
```

配置虚拟转发器监视 Track 项 1。Track 项的状态为 Negative 时，降低 Device C 上虚拟转发器的权重，使其低于失效下限 10，即权重降低的数额大于 245，以便其他设备接替 Device C 的转发任务。本例中，配置虚拟转发器权重降低数额为 250。

```
[DeviceC] interface gigabitEthernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] vrrp vrid 1 track 1 weight reduced 250
[DeviceC-GigabitEthernet1/0/1] quit
```

5.5.4 验证配置

(1) 配置完成后，在 Host A 上可以 ping 通外网，通过 **display vrrp verbose** 命令查看配置后的结果

显示 Device A 上 VRRP 备份组的详细信息。

```
[DeviceA] display vrrp verbose
IPv4 Virtual Device Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                    Adver Timer   : 100
     Admin Status   : Up                   State         : Master
     Config Pri     : 120                  Running Pri   : 120
     Preempt Mode   : Yes                  Delay Time    : 500
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.2 (Local, Master)
                      10.1.1.3 (Backup)
                      10.1.1.4 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Active
     Virtual MAC    : 000f-e2ff-0011 (Owner)
```

```
    Owner ID       : 0000-5e01-1101
    Priority       : 255
    Active         : local
   Forwarder 02
    State          : Listening
    Virtual MAC    : 000f-e2ff-0012 (Learnt)
    Owner ID       : 0000-5e01-1103
    Priority       : 127
    Active         : 10.1.1.3
   Forwarder 03
    State          : Listening
    Virtual MAC    : 000f-e2ff-0013 (Learnt)
    Owner ID       : 0000-5e01-1105
    Priority       : 127
    Active         : 10.1.1.4
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

显示 Device B 上 VRRP 备份组的详细信息。

```
[DeviceB] display vrrp verbose
IPv4 Virtual Device Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                    Adver Timer  : 100
     Admin Status   : Up                   State        : Backup
     Config Pri     : 110                  Running Pri  : 110
     Preempt Mode   : Yes                  Delay Time   : 500
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.3 (Local, Backup)
                      10.1.1.2 (Master)
                      10.1.1.4 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Listening
     Virtual MAC    : 000f-e2ff-0011 (Learnt)
     Owner ID       : 0000-5e01-1101
     Priority       : 127
     Active         : 10.1.1.2
    Forwarder 02
     State          : Active
     Virtual MAC    : 000f-e2ff-0012 (Owner)
     Owner ID       : 0000-5e01-1103
     Priority       : 255
     Active         : local
    Forwarder 03
```

```
    State           : Listening
    Virtual MAC     : 000f-e2ff-0013 (Learnt)
    Owner ID        : 0000-5e01-1105
    Priority        : 127
    Active          : 10.1.1.4
  Forwarder Weight Track Information:
    Track Object    : 1          State : Positive   Weight Reduced : 250
```

显示 Device C 上 VRRP 备份组的详细信息。

```
[DeviceC] display vrrp verbose
IPv4 Virtual Device Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                    Adver Timer  : 100
     Admin Status   : Up                   State        : Backup
     Config Pri     : 100                  Running Pri  : 100
     Preempt Mode   : Yes                  Delay Time   : 500
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.4 (Local, Backup)
                      10.1.1.2 (Master)
                      10.1.1.3 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State           : Listening
     Virtual MAC     : 000f-e2ff-0011 (Learnt)
     Owner ID        : 0000-5e01-1101
     Priority        : 127
     Active          : 10.1.1.2
    Forwarder 02
     State           : Listening
     Virtual MAC     : 000f-e2ff-0012 (Learnt)
     Owner ID        : 0000-5e01-1103
     Priority        : 127
     Active          : 10.1.1.3
    Forwarder 03
     State           : Active
     Virtual MAC     : 000f-e2ff-0013 (Owner)
     Owner ID        : 0000-5e01-1105
     Priority        : 255
     Active          : local
   Forwarder Weight Track Information:
     Track Object    : 1          State : Positive   Weight Reduced : 250
```

以上显示信息表示在 VRRP 备份组 1 中 Device A 为 Master，Device B 和 Device C 为 Backup。Device A、Device B 和 Device C 上各自存在一个 AVF，并存在作为备份的两个 LVF。

(2) Device A 的上行接口（GigabitEthernet1/0/2）出现故障后

显示 Device A 上 VRRP 备份组的详细信息。

```
[DeviceA] display vrrp verbose
IPv4 Virtual Device Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                    Adver Timer  : 100
     Admin Status   : Up                   State        : Master
     Config Pri     : 120                  Running Pri  : 120
     Preempt Mode   : Yes                  Delay Time   : 500
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.2 (Local, Master)
                      10.1.1.3 (Backup)
                      10.1.1.4 (Backup)
   Forwarder Information: 3 Forwarders 0 Active
     Config Weight  : 255
     Running Weight : 5
    Forwarder 01
     State          : Initialize
     Virtual MAC    : 000f-e2ff-0011 (Owner)
     Owner ID       : 0000-5e01-1101
     Priority       : 0
     Active         : 10.1.1.4
    Forwarder 02
     State          : Initialize
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 0
     Active         : 10.1.1.3
    Forwarder 03
     State          : Initialize
     Virtual MAC    : 000f-e2ff-0013 (Learnt)
     Owner ID       : 0000-5e01-1105
     Priority       : 0
     Active         : 10.1.1.4
   Forwarder Weight Track Information:
     Track Object   : 1          State : Negative   Weight Reduced : 250
```

显示 Device C 上 VRRP 备份组的详细信息。

```
[DeviceC] display vrrp verbose
IPv4 Virtual Device Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                    Adver Timer  : 100
     Admin Status   : Up                   State        : Backup
     Config Pri     : 100                  Running Pri  : 100
     Preempt Mode   : Yes                  Delay Time   : 500
```

```
    Auth Type      : None
    Become Master  : 3550ms left
    Virtual IP     : 10.1.1.1
    Member IP List : 10.1.1.4 (Local, Backup)
                     10.1.1.2 (Master)
                     10.1.1.3 (Backup)
  Forwarder Information: 3 Forwarders 2 Active
    Config Weight  : 255
    Running Weight : 255
   Forwarder 01
    State          : Active
    Virtual MAC    : 000f-e2ff-0011 (Take Over)
    Owner ID       : 0000-5e01-1101
    Priority       : 85
    Active         : local
    Redirect Time  : 93 secs
    Time-out Time  : 1293 secs
   Forwarder 02
    State          : Listening
    Virtual MAC    : 000f-e2ff-0012 (Learnt)
    Owner ID       : 0000-5e01-1103
    Priority       : 85
    Active         : 10.1.1.3
   Forwarder 03
    State          : Active
    Virtual MAC    : 000f-e2ff-0013 (Owner)
    Owner ID       : 0000-5e01-1105
    Priority       : 255
    Active         : local
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

以上显示信息表示 Device A 的上行接口出现故障后，Device A 上虚拟转发器的权重降低为 5，低于失效下限。Device A 上所有虚拟转发器的状态均变为 Initialized，不能再用于转发。Device C 成为虚拟 MAC 地址 000f-e2ff-0011 对应虚拟转发器的 AVF，接管 Device A 的转发任务。

Timeout Timer 超时后（约 1800 秒后），查看 Device C 上 VRRP 备份组的详细信息。

```
[DeviceC] display vrrp verbose
IPv4 Virtual Device Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                    Adver Timer  : 100
     Admin Status   : Up                   State        : Backup
     Config Pri     : 100                  Running Pri  : 100
     Preempt Mode   : Yes                  Delay Time   : 500
     Auth Type      : None
     Become Master  : 3550ms left
     Virtual IP     : 10.1.1.1
```

```
  Member IP List : 10.1.1.4 (Local, Backup)
                   10.1.1.2 (Master)
                   10.1.1.3 (Backup)
 Forwarder Information: 2 Forwarders 1 Active
  Config Weight  : 255
  Running Weight : 255
 Forwarder 02
  State          : Listening
  Virtual MAC    : 000f-e2ff-0012 (Learnt)
  Owner ID       : 0000-5e01-1103
  Priority       : 127
  Active         : 10.1.1.3
 Forwarder 03
  State          : Active
  Virtual MAC    : 000f-e2ff-0013 (Owner)
  Owner ID       : 0000-5e01-1105
  Priority       : 255
  Active         : local
 Forwarder Weight Track Information:
  Track Object   : 1          State : Positive   Weight Reduced : 250
```

以上显示信息表示，Timeout Timer 超时后，删除虚拟 MAC 地址 000f-e2ff-0011 对应的虚拟转发器，不再转发目的 MAC 地址为该 MAC 的报文。

(3) Device A 出现故障后

显示 Device B 上 VRRP 备份组的详细信息。

```
[DeviceB] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                    Adver Timer  : 1
     Admin Status   : Up                   State        : Master
     Config Pri     : 110                  Running Pri  : 110
     Preempt Mode   : Yes                  Delay Time   : 500
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.3 (Local, Master)
                      10.1.1.4 (Backup)
   Forwarder Information: 2 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 02
     State          : Active
     Virtual MAC    : 000f-e2ff-0012 (Owner)
     Owner ID       : 0000-5e01-1103
     Priority       : 255
     Active         : local
```

```
    Forwarder 03
      State          : Listening
      Virtual MAC    : 000f-e2ff-0013 (Learnt)
      Owner ID       : 0000-5e01-1105
      Priority       : 127
      Active         : 10.1.1.4
   Forwarder Weight Track Information:
      Track Object   : 1          State : Positive   Weight Reduced : 250
```

以上显示信息表示 Device A 出现故障后，Device B 的优先级高于 Device C，将抢占成为 Master。

5.5.5 配置文件

- Device A：

```
#
 vrrp mode load-balance
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.1
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode delay 500
 vrrp vrid 1 track 1 weight reduced 250
#
interface GigabitEthernet1/0/2
 port link-mode route
#
track 1 interface GigabitEthernet1/0/2
#
```

- Device B：

```
#
 vrrp mode load-balance
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.3 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.1
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode delay 500
 vrrp vrid 1 track 1 weight reduced 250
#
interface GigabitEthernet1/0/2
 port link-mode route
#
track 1 interface GigabitEthernet1/0/2
#
```

- Device C：

```
#
 vrrp mode load-balance
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.4 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.1
 vrrp vrid 1 preempt-mode delay 500
 vrrp vrid 1 track 1 weight reduced 250
#
interface GigabitEthernet1/0/2
 port link-mode route
#
track 1 interface GigabitEthernet1/0/2
#
```

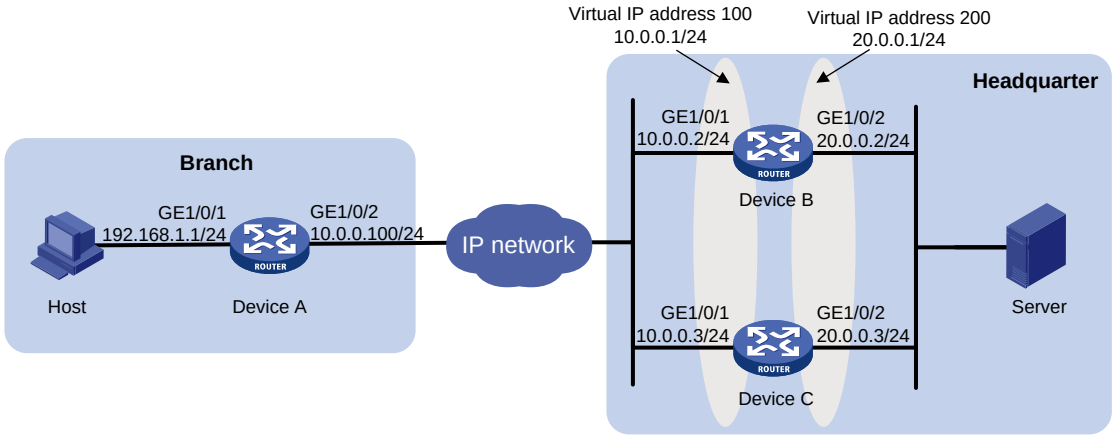
6 IPv4 VRRP with IPsec 配置举例

6.1 组网需求

如图 4 所示，Device A 作为某公司分支机构的网关设备，Device B 和 Device C 是公司总部网关设备。Device B 和 Device C 通过部署 VRRP 协议，实现设备冗余备份，提高可靠性。该分支机构内的主机可以访问公司总部内部服务器的资源。具体应用需求如下：

- 在正常情况下，Device B 作为 Master 负责流量的转发；
- 当 Device B 出现故障时，由 Device C 接替其流量转发任务；
- 要求在 Device A 和公司总部出口网关之间部署 IPsec 隧道，以保证分支机构内网网段 192.168.1.0/24 和总部内网网段 20.0.0.0/24 之间数据的完整性和机密性。

图4 IPv4 VRRP with IPsec 配置组网图



6.2 配置思路

- 由于 IPsec 隧道是点到点建立的，为保护主机与服务器之间数据的安全性，需要 Device A 与 VRRP 备份组 100 中的 Master 建立 IPsec 隧道。
- 为了避免 VRRP 组发生主备切换时造成 IPsec 隧道的中断，可以通过配置 DPD 功能保证 Device A 可以及时的检测到对端路由器的状态，并重新与 VRRP 备份组中的其他路由器进行 IKE 协商。
- 为了让 Device B 成为 Master，需要为 Device B 配置较高的优先级。
- 将 VRRP 组的抢占模式和监视上行接口状态功能结合使用，可以使 Master 设备根据连接总部内网接口 GigabitEthernet 1/0/2 的状态自动调整自身的 VRRP 优先级，从而使 VRRP 组内的角色发生转变，实现主备切换。
- 为了避免 VRRP 备份组中的角色频繁发生变化，可以配置一定的抢占延迟时间。

6.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

6.4 配置注意事项

- VRRP 备份组的虚拟 IP 地址不能为全零地址(0.0.0.0)、广播地址(255.255.255.255)、环回地址、非 A/B/C 类地址和其它非法 IP 地址(如 0.0.0.1)。
- 建议将备份组的虚拟 IP 地址和备份组中设备下行接口的 IP 地址配置为同一网段，否则可能导致局域网内的主机无法访问外部网络。
- IPv4 VRRP 既可以使用 VRRPv2 版本，也可以使用 VRRPv3 版本（缺省情况使用 VRRPv3）。请确保 IPv4 VRRP 备份组中的所有路由器上配置的 IPv4 VRRP 版本一致，否则 VRRP 备份组无法正常工作。
- 删除 IP 地址拥有者上的 VRRP 备份组，将导致地址冲突。建议先修改配置了 VRRP 备份组的接口的 IP 地址，再删除该接口上的 VRRP 备份组，以避免地址冲突。
- IPsec 隧道两端配置的 ACL 的源地址和目的地址必须对称。
- IKE 协商双方配置的预共享密钥必须相同。
- 对于同一个 VRRP 备份组的成员设备，必须保证备份组虚拟路由器的 IP 地址完全一样。
- 用户在配置降低优先级幅度时，需要确保降低后的优先级比 VRRP 备份组内其他设备的优先级要低，确保 VRRP 备份组内有其他设备被选为 Master。

6.5 配置步骤

6.5.1 Device A 的配置

配置接口的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[DeviceA-GigabitEthernet1/0/1] quit
```

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] ip address 10.0.0.100 255.255.255.0
[DeviceA-GigabitEthernet1/0/2] quit
```

配置到 20.0.0.0/24 网段的静态路由。

```
[DeviceA] ip route-static 20.0.0.0 255.255.255.0 10.0.0.1
```

配置 ACL 3000，指定 IPsec 需要保护的数据流。

```
[DeviceA] acl advanced 3000
[DeviceA-acl-ipv4-adv-3000] rule 0 permit ip source 192.168.1.0 0.0.0.255 destination
20.0.0.0 0.0.0.255
[DeviceA-acl-ipv4-adv-3000] quit
```

配置流量触发 IKE DPD 探测间隔时间为 10 秒，重传时间间隔为 5 秒，探测模式为按需探测。

```
[DeviceA] ike dpd interval 10 retry 5 on-demand
```

创建 IKE Keychain，并配置与对端地址为虚拟 IP 地址 10.0.0.1 使用的预共享密钥为明文的 123456。

```
[DeviceA] ike keychain test
[DeviceA-ike-keychain-test] pre-shared-key address 10.0.0.1 key simple 123456
[DeviceA-ike-keychain-test] quit
```

创建 IKE profile，指定采用预共享密钥时使用的 IKE Keychain，并配置使用 IP 地址 10.0.0.100 标识本端身份信息、使用 VRRP 备份组 100 的虚拟 IP 地址 10.0.0.1 来匹配对端身份。

```
[DeviceA] ike profile test
[DeviceA-ike-profile-test] keychain test
[DeviceA-ike-profile-test] local-identity address 10.0.0.100
[DeviceA-ike-profile-test] match remote identity address 10.0.0.1 24
[DeviceA-ike-profile-test] quit
```

创建 IPsec 安全提议 test，安全封装模式、安全协议类型均采用系统缺省值。

```
[DeviceA] ipsec transform-set test
```

配置 ESP 协议采用的加密算法为采用 64 比特的 DES 算法，认证算法为 MD5。

```
[DeviceA-ipsec-transform-set-test] esp encryption-algorithm des-cbc
[DeviceA-ipsec-transform-set-test] esp authentication-algorithm md5
[DeviceA-ipsec-transform-set-test] quit
```

创建 IPsec 安全策略 test、顺序号为 1、采用 IKE 方式协商 IPsec SA 的 IPsec 安全策略，并进入 IPsec 安全策略视图。

```
[DeviceA] ipsec policy test 1 isakmp
```

指定 IPsec 隧道的对端 IP 地址为 10.0.0.1。

```
[DeviceA-ipsec-policy-isakmp-test-1] remote-address 10.0.0.1
```

配置 IPsec 安全策略引用 ACL 3000。

```
[DeviceA-ipsec-policy-isakmp-test-1] security acl 3000
```

配置 IPsec 安全策略引用安全提议 test。

```
[DeviceA-ipsec-policy-isakmp-test-1] transform-set test
```

配置 IPsec 安全策略引用名为 test 的 IKE profile。

```
[DeviceA-ipsec-policy-isakmp-test-1] ike-profile test
[DeviceA-ipsec-policy-isakmp-test-1] quit
```

应用 IPsec 策略。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] ipsec apply policy test
[DeviceA-GigabitEthernet1/0/2] quit
```

6.5.2 Device B 的配置

配置接口的 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 10.0.0.2 255.255.255.0
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip address 20.0.0.2 255.255.255.0
[DeviceB-GigabitEthernet1/0/2] quit
```

配置到 192.168.1.0/24 网段的静态路由。

```
[DeviceB] ip route-static 192.168.1.0 255.255.255.0 10.0.0.100
```

配置 ACL 3000，指定 IPsec 需要保护的数据流。

```
[DeviceB] acl advanced 3000
[DeviceB-acl-ipv4-adv-3000] rule 0 permit ip source 20.0.0.0 0.0.0.255 destination
192.168.0.0 0.0.0.255
[DeviceB-acl-ipv4-adv-3000] quit
```

创建 IKE Keychain，并配置与对端地址为 10.0.0.100 使用的预共享密钥为明文的 123456。

```
[DeviceB] ike keychain test
[DeviceB-ike-keychain-test] pre-shared-key address 10.0.0.100 key simple 123456
[DeviceB-ike-keychain-test] quit
```

创建 IKE profile，指定采用预共享密钥时使用的 IKE Keychain，并配置使用 VRRP 备份组 100 的虚拟 IP 地址 10.0.0.1 标识本端身份信息、使用 DeviceA 的上行接口地址 10.0.0.100 来匹配对端身份。

```
[DeviceB] ike profile test
[DeviceB-ike-profile-test] keychain test
[DeviceB-ike-profile-test] local-identity address 10.0.0.1
[DeviceB-ike-profile-test] match remote identity address 10.0.0.100 24
[DeviceB-ike-profile-test] quit
```

创建 IPsec 安全提议 test，安全封装模式、安全协议类型均采用系统缺省值。

```
[DeviceB] ipsec transform-set test
```

配置 ESP 协议采用的加密算法为采用 64 比特的 DES 算法，认证算法为 MD5。

```
[DeviceB-ipsec-transform-set-test] esp encryption-algorithm des-cbc
[DeviceB-ipsec-transform-set-test] esp authentication-algorithm md5
[DeviceB-ipsec-transform-set-test] quit
```

创建 IPsec 安全策略 test、顺序号为 1、采用 IKE 方式协商 IPsec SA 的 IPsec 安全策略，并进入 IPsec 安全策略视图。

```
[DeviceB] ipsec policy test 1 isakmp
```

指定 IPsec 隧道的对端 IP 地址为 10.0.0.100。

```
[DeviceB-ipsec-policy-isakmp-test-1] remote-address 10.0.0.100
```

配置 IPsec 安全策略引用 ACL 3000。

```
[DeviceB-ipsec-policy-isakmp-test-1] security acl 3000
```

配置 IPsec 安全策略引用安全提议 test。

```
[DeviceB-ipsec-policy-isakmp-test-1] transform-set test
```

配置 IPsec 安全策略引用名为 test 的 IKE profile。

```
[DeviceB-ipsec-policy-isakmp-test-1] ike-profile test
[DeviceB-ipsec-policy-isakmp-test-1] quit
```
应用 IPsec 策略。
```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ipsec apply policy test
[DeviceB-GigabitEthernet1/0/1] quit
```
创建 Track 项 1，监视 GigabitEthernet1/0/2 接口状态。
```
[DeviceB] track 1 interface gigabitethernet 1/0/2
```
创建 VRRP 备份组 100，配置虚拟 IP 地址为 10.0.0.1。
```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 100 virtual-ip 10.0.0.1
```
设备在 VRRP 备份组中的优先级默认为 100，因此配置 Device B 在 VRRP 备份组 100 中的优先级为 150。
```
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 100 priority 150
```
配置监视指定的 Track 项 1，当 Track 项 1 的状态为 Negative 时，Device B 在备份组 100 中的优先级降低 60，使其低于默认值。
```
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 100 track 1 priority reduce 60
[DeviceB-GigabitEthernet1/0/1] quit
```
创建 Track 项 2，监视 GigabitEthernet1/0/1 接口状态。
```
[DeviceB] track 2 interface gigabitethernet 1/0/1
```
创建 VRRP 备份组 200，配置虚拟 IP 地址为 20.0.0.1。
```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] vrrp vrid 200 virtual-ip 20.0.0.1
```
设备在 VRRP 备份组中的优先级默认为 100，因此配置 Device B 在 VRRP 备份组 200 中的优先级为 150。
```
[DeviceB-GigabitEthernet1/0/2] vrrp vrid 200 priority 150
```
配置监视指定的 Track 项 2，当 Track 项 2 的状态为 Negative 时，Device B 在备份组 200 中的优先级降低 60，使其低于默认值。
```
[DeviceB-GigabitEthernet1/0/2] vrrp vrid 200 track 2 priority reduce 60
[DeviceB-GigabitEthernet1/0/2] quit
```

6.5.3 Device C 的配置

配置接口的 IP 地址。
```
<DeviceC> system-view
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ip address 10.0.0.3 255.255.255.0
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] ip address 20.0.0.3 255.255.255.0
[DeviceC-GigabitEthernet1/0/2] quit
```
配置到 192.168.1.0/24 网段的静态路由。
```
[DeviceC] ip route-static 192.168.1.0 255.255.255.0 10.0.0.100
```
配置 ACL 3000，指定 IPsec 需要保护的数据流。
```
[DeviceC] acl advanced 3000
```

```
[DeviceC-acl-ipv4-adv-3000] rule 0 permit ip source 20.0.0.0 0.0.0.255 destination
192.168.0.0 0.0.0.255
[DeviceC-acl-ipv4-adv-3000] quit
```

创建 IKE Keychain，并配置与对端地址为 10.0.0.100 使用的预共享密钥为明文的 123456

```
[DeviceC] ike keychain test
[DeviceC-ike-keychain-test] pre-shared-key address 10.0.0.100 key simple 123456
[DeviceC-ike-keychain-test] quit
```

创建 IKE profile，指定采用预共享密钥时使用的 IKE Keychain，并配置使用 VRRP 备份组 100 的虚拟 IP 地址 10.0.0.1 标识本端身份信息、使用 Device A 的上行接口地址 10.0.0.100 来匹配对端身份。

```
[DeviceC] ike profile test
[DeviceC-ike-profile-test] keychain test
[DeviceC-ike-profile-test] local-identity address 10.0.0.1
[DeviceC-ike-profile-test] match remote identity address 10.0.0.100 24
[DeviceC-ike-profile-test] quit
```

创建 IPsec 安全提议 test，安全封装模式、安全协议类型均采用系统缺省值。

```
[DeviceC] ipsec transform-set test
```

配置 ESP 协议采用的加密算法为采用 64 比特的 DES 算法，认证算法为 MD5。

```
[DeviceC-ipsec-transform-set-test] esp encryption-algorithm des-cbc
[DeviceC-ipsec-transform-set-test] esp authentication-algorithm md5
[DeviceC-ipsec-transform-set-test] quit
```

创建 IPsec 安全策略 test、顺序号为 1、采用 IKE 方式协商 IPsec SA 的 IPsec 安全策略，并进入 IPsec 安全策略视图。

```
[DeviceC] ipsec policy test 1 isakmp
```

指定 IPsec 隧道的对端 IP 地址为 10.0.0.100。

```
[DeviceC-ipsec-policy-isakmp-test-1] remote-address 10.0.0.100
```

配置 IPsec 安全策略引用 ACL 3000。

```
[DeviceC-ipsec-policy-isakmp-test-1] security acl 3000
```

配置 IPsec 安全策略引用安全提议 test。

```
[DeviceC-ipsec-policy-isakmp-test-1] transform-set test
```

配置 IPsec 安全策略引用名为 test 的 IKE profile。

```
[DeviceC-ipsec-policy-isakmp-test-1] ike-profile test
[DeviceC-ipsec-policy-isakmp-test-1] quit
```

应用 IPsec 策略。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ipsec apply policy test
[DeviceC-GigabitEthernet1/0/1] quit
```

创建 VRRP 备份组 100，配置虚拟 IP 地址为 10.0.0.1。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] vrrp vrid 100 virtual-ip 10.0.0.1
[DeviceC-GigabitEthernet1/0/1] quit
```

创建 VRRP 备份组 200，配置虚拟 IP 地址为 20.0.0.1。

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] vrrp vrid 200 virtual-ip 20.0.0.1
[DeviceC-GigabitEthernet1/0/2] quit
```

6.6 验证配置

(1) 在 Device B 和 Device C 上分别查看 VRRP 备份组的信息。可以看到在 VRRP 备份组 100 和 VRRP 备份组 200 中，Master 均为 Device B，Backup 均为 Device C。

在 Device B 上查看 VRRP 备份组信息。

```
[DeviceB] display vrrp verbose
 IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
   Interface GigabitEthernet1/0/1
     VRID           : 100                 Adver Timer  : 100
     Admin Status   : Up                  State        : Master
     Config Pri     : 150                 Running Pri  : 150
     Preempt Mode   : Yes                 Delay Time   : 0
     Auth Type      : None
     Virtual IP     : 10.0.0.1
     Virtual MAC    : 0000-5e00-0164
     Master IP      : 10.0.0.2
   VRRP Track Information:
     Track Object   : 1                   State : Positive   Pri Reduced : 60

   Interface GigabitEthernet1/0/2
     VRID           : 200                 Adver Timer  : 100
     Admin Status   : Up                  State        : Master
     Config Pri     : 150                 Running Pri  : 150
     Preempt Mode   : Yes                 Delay Time   : 0
     Auth Type      : None
     Virtual IP     : 20.0.0.1
     Virtual MAC    : 0000-5e00-0102
     Master IP      : 20.0.0.2
   VRRP Track Information:
     Track Object   : 2                   State : Positive   Pri Reduced : 60
```

在 Device C 上查看 VRRP 备份组信息。

```
[DeviceC] display vrrp verbose
 IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
   Interface GigabitEthernet1/0/1
     VRID           : 100                 Adver Timer  : 100
     Admin Status   : Up                  State        : Backup
     Config Pri     : 100                 Running Pri  : 100
     Preempt Mode   : Yes                 Delay Time   : 0
     Become Master  : 3480ms left
     Auth Type      : None
     Virtual IP     : 10.0.0.1
     Master IP      : 10.0.0.2
```

```
  Interface GigabitEthernet1/0/2
    VRID           : 200                 Adver Timer  : 100
    Admin Status   : Up                  State        : Backup
    Config Pri     : 100                 Running Pri  : 100
    Preempt Mode   : Yes                 Delay Time   : 0
    Become Master  : 2820ms left
    Auth Type      : None
    Virtual IP     : 20.0.0.1
    Master IP      : 20.0.0.2
```

(2) 从分支机构 ping 总部网关的 IP 地址 20.0.0.1，触发 IKE 协商，SA 协商成功后可以 ping 通。

```
<DeviceA> ping -a 192.168.1.1 20.0.0.1
  PING 30.1.1.123: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 20.0.0.1: bytes=56 Sequence=1 ttl=127 time=2 ms
    Reply from 20.0.0.1: bytes=56 Sequence=2 ttl=127 time=1 ms
    Reply from 20.0.0.1: bytes=56 Sequence=3 ttl=127 time=1 ms
    Reply from 20.0.0.1: bytes=56 Sequence=4 ttl=127 time=2 ms

  --- 20.0.0.1 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

(3) 通过 **diplay ike sa** 命令分别在 Device A 和 Device B 上查看到 IKE SA 的建立情况。

在 Device A 上查看 IKE SA 的信息，可以看到 Device A 的 IKE SA 对端地址为 VRRP 备份组的虚拟 IP 地址。

```
[DeviceA] display ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------------
    29              10.0.0.1              RD           IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
```

在 Device B 上查看 IKE SA 的信息，可以看到 Device B 的 IKE SA 对端地址为 Device A 上 GigabitEthernet1/0/2 接口的 IP 地址。

```
[DeviceB] display ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------------
    17              10.0.0.100            RD           IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
```

(4) 通过 **display ipsec sa brief** 命令分别在 Device A 和 Device B 上查看到 IPsec SA 的建立情况，可以看到 IPsec 隧道已成功建立

在 Device A 上查看 IPsec SA 的信息。

```
[DeviceA] display ipsec sa brief
-------------------------------------------------------------------------
Interface/Global    Dst Address       SPI         Protocol    Status
```

```
-----------------------------------------------------------------------
GE1/0/2             10.0.0.1          4051765865  ESP         active
GE1/0/2             10.0.0.100        1860835944  ESP         active
```

在 Device B 上查看 IPsec SA 的信息。

```
[DeviceB] display ipsec sa brief
-----------------------------------------------------------------------
Interface/Global    Dst Address       SPI         Protocol    Status
-----------------------------------------------------------------------
GE1/0/1             10.0.0.100        1860835944  ESP         active
GE1/0/1             10.0.0.1          4051765865  ESP         active
```

(5) 手工关闭 Device B 的 GigabitEthernet1/0/1 接口，Device B 的 VRRP 状态切换到 Backup，Device C 的 VRRP 状态切换到 Master。重新从分支机构 ping 总部的 IP 地址 20.0.0.1，DPD 检测 IKE 对等体无响应，删除本端 SA，重新与 Device C 进行 IKE 协商，建立新的 SA 后，可以 ping 通总部 IP 地址。

在 Device B 上查看当前 VRRP 的状态信息。

```
[DeviceB] display vrrp
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
 Interface          VRID   State       Run     Adver   Auth     Virtual
                                       Pri     Timer   Type        IP
 -----------------------------------------------------------------------
 GE1/0/1            100    Initialize  150     1       None     10.0.0.1
 GE1/0/2            200    Backup      90      1       None     20.0.0.1
```

在 Device C 上查看当前 VRRP 的状态信息，已经从 Backup 状态切换成 Master 状态。

```
[DeviceC] display vrrp
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
 Interface          VRID   State       Run     Adver   Auth     Virtual
                                       Pri     Timer   Type        IP
 -----------------------------------------------------------------------
 GE1/0/1            100    Master      100     1       None     10.0.0.1
 GE1/0/2            200    Master      100     1       None     20.0.0.1
```

从 Device A 上 ping 总部网关 IP 地址 20.0.0.1，可以 ping 通。

```
<DeviceA> ping -a 192.168.1.1 20.0.0.1
  PING 20.0.0.1: 56  data bytes, press CTRL_C to break
    Reply from 20.0.0.1: bytes=56 Sequence=0 ttl=127 time=2 ms
    Reply from 20.0.0.1: bytes=56 Sequence=1 ttl=127 time=1 ms
    Reply from 20.0.0.1: bytes=56 Sequence=2 ttl=127 time=1 ms
    Reply from 20.0.0.1: bytes=56 Sequence=3 ttl=127 time=1 ms
    Reply from 20.0.0.1: bytes=56 Sequence=4 ttl=127 time=2 ms

  --- 20.0.0.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
```

```
    round-trip min/avg/max = 1/1/2 ms
```

通过 **display ike sa** 命令中的标识符 connection-id 字段，可以判断 Device A 上已经重新协商了 SA。

```
[DeviceA] display ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
    30              10.0.0.1              RD           IPSEC

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT RK--REKEY
```

在 Device C 上可以查看到 SA 信息。

```
[DeviceC] display ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
    3               10.0.0.100            RD           IPSEC

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT RK--REKEY
[DeviceC] display ipsec sa brief
 total phase-2 IPv4 SAs: 2
Interface/Global    Dst Address       SPI         Protocol    Status
-------------------------------------------------------------------------
GE1/0/1             10.0.0.100        1235764751  ESP         active
GE1/0/1             10.0.0.1          799485439   ESP         active
```

(6) 当 Device B 的 GE1/0/1 接口重新 UP 时，VRRP 状态切换为 Master，从分支到总部的数据流会重新发送到 Device B 上，通过 DPD 特性，Device A 删除 SA 重新与 Device B 进行 IKE 协商，协商成功后分支到总部的数据流会在新的 IPsec 隧道上得以传输。验证方法与上一个步骤相同，此处省略。

6.7 配置文件

- Device A：

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.0.0.100 255.255.255.0
 ipsec apply policy test
#
ip route-static 20.0.0.0 255.255.255.0 10.0.0.1
#
acl advanced 3000
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 20.0.0.0 0.0.0.255
#
```

```
ipsec transform-set test
 esp encryption-algorithm des-cbc
 esp authentication-algorithm md5
#
ipsec policy test 1 isakmp
 transform-set test
 security acl 3000
 remote-address 10.0.0.1
 ike-profile test
#
 ike dpd interval 10 on-demand
#
ike profile test
 keychain test
 local-identity address 10.0.0.100
 match remote identity address 10.0.0.1 255.255.255.0
#
ike keychain test
 pre-shared-key address 10.0.0.1 255.255.255.255 key cipher
$c$3$VPq7TeKUusm/5GG8rHfZGHQR+Rbrhbk=
#
```

- Device B：

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.0.0.2 255.255.255.0
 vrrp vrid 100 virtual-ip 10.0.0.1
 vrrp vrid 100 priority 150
 vrrp vrid 100 track 1 priority reduce 60
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 20.0.0.2 255.255.255.0
 vrrp vrid 200 virtual-ip 20.0.0.1
 vrrp vrid 200 priority 150
 vrrp vrid 200 track 2 priority reduce 60
 ipsec apply policy test
#
 ip route-static 192.168.1.0 255.255.255.0 10.0.0.100
#
acl advanced 3000
 rule 0 permit ip source 20.0.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
ipsec transform-set test
 esp encryption-algorithm des-cbc
 esp authentication-algorithm md5
#
ipsec policy test 1 isakmp
```

```
 transform-set test
 security acl 3000
 remote-address 10.0.0.100
 ike-profile test
#
ike profile test
 keychain test
 local-identity address 10.0.0.1
 match remote identity address 10.0.0.100 255.255.255.0
#
ike keychain test
 pre-shared-key address 10.0.0.100 255.255.255.255 key cipher
$c$3$VPq7TeKUusm/5GG8rHfZGHQR+Rbrhbk=
#
 track 1 interface gigabitethernet 1/0/2
#
```

- Device C：

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.0.0.3 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 20.0.0.3 255.255.255.0
 ipsec apply policy test
#
ip route-static 192.168.1.0 255.255.255.0 10.0.0.100
#
acl advanced 3000
 rule 0 permit ip source 20.0.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
ipsec transform-set test
 esp encryption-algorithm des-cbc
 esp authentication-algorithm md5
#
ipsec policy test 1 isakmp
 transform-set test
 security acl 3000
 remote-address 10.0.0.100
 ike-profile test
#
ike profile test
 keychain test
 local-identity address 10.0.0.1
 match remote identity address 10.0.0.100 255.255.255.0
#
ike keychain test
```

```
 pre-shared-key address 10.0.0.100 255.255.255.255 key cipher
$c$3$VPq7TeKUusm/5GG8rHfZGHQR+Rbrhbk=
#
```

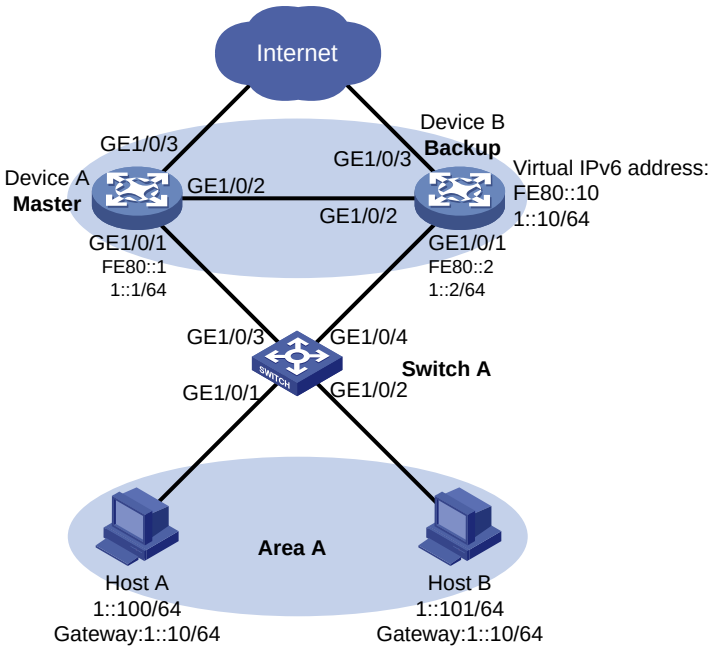
7 IPv6 VRRP 单备份组配置举例

7.1 组网需求

如图 5 所示，Area A 区域的用户（Host A 和 Host B）所在网络的出口处部署了两台网关设备。现要求使用 VRRP 主备备份功能，将这两台设备组成一台虚拟路由器，作为 Area A 区域用户的缺省网关。具体应用需求如下：

- 在正常情况下，由 Device A 承担网关功能，转发 Area A 区域用户发送至外网的流量；
- 当 Device A 或者 Device A 的上行接口出现故障时，由 Device B 接替 Device A 承担网关功能；
- 当 Device A 或者 Device A 的上行接口故障恢复后，由 Device A 继续承担网关功能。

图5 IPv6 VRRP 单备份组配置组网图



7.2 配置思路

- 为了让 Device A 成为 Master，需要为 Device A 配置较高的优先级；
- 将 VRRP 组的抢占模式和监视上行接口状态功能结合使用，可以使 Master 设备根据上行接口的状态自动调整自身的 VRRP 优先级，从而使 VRRP 组内的角色发生转变，实现主备切换；
- 为了避免 VRRP 备份组中的角色频繁发生变化，可以配置一定的抢占延迟时间。

7.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

7.4 配置注意事项

- 建议将备份组的虚拟 IPv6 地址和备份组中设备下行接口的 IPv6 地址配置为同一网段，否则可能导致局域网内的主机无法访问外部网络。
- IPv6 VRRP 既可以使用 VRRPv2 版本，也可以使用 VRRPv3 版本（缺省情况使用 VRRPv3）。请确保 IPv6 VRRP 备份组中的所有路由器上配置的 IPv6 VRRP 版本一致，否则备份组无法正常工作。
- 删除 IP 地址拥有者上的 VRRP 备份组，将导致地址冲突。建议先修改配置了备份组的接口的 IP 地址，再删除该接口上的 VRRP 备份组，以避免地址冲突。
- 对于同一个 VRRP 备份组的成员设备，必须保证虚拟路由器的 IP 地址配置完全一样。
- 用户在配置降低优先级幅度时，需要确保降低后的优先级比备份组内其他设备的优先级要低，确保备份组内有其他设备被选为 Master。

7.5 配置步骤

(1) Device A 的配置

配置接口 IPv6 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ipv6 address fe80::1 link-local
[DeviceA-GigabitEthernet1/0/1] ipv6 address 1::1 64
```

创建 VRRP 备份组 1，并配置备份组 1 的虚拟 IPv6 地址为 FE80::10 和 1::10。

```
[DeviceA-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[DeviceA-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 virtual-ip 1::10
```

配置允许发布 RA 消息，以便 Area A 的主机通过 RA 消息学习到缺省网关地址。

```
[DeviceA-GigabitEthernet1/0/1] undo ipv6 nd ra halt
```

设置 Device A 在 VRRP 备份组 1 中的优先级为 110，高于 Device B 的优先级 100，以保证 Device A 成为 Master 负责转发流量。

```
[DeviceA-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 priority 110
```

设置 Device A 工作在抢占方式，以保证 Device A 故障恢复后，能再次抢占成为 Master，即只要 Device A 正常工作，就由 Device A 负责转发流量。为了避免频繁地进行状态切换，配置抢占延迟时间为 5 秒。

```
[DeviceA-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 preempt-mode delay 500
[DeviceA-GigabitEthernet1/0/1] quit
```

创建和上行接口 GigabitEthernet 1/0/3 关联的 Track 项 1。

```
[DeviceA] track 1 interface gigabitethernet 1/0/3
```

配置监视 Track 项 1，Track 项的状态为 Negative 时，Device A 在 VRRP 备份组中的优先级降低的数值为 50。

```
[DeviceA] interface gigabitEthernet 1/0/1
```

```
[DeviceA-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 track 1 priority reduced 50
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) Device B 的配置

配置接口 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ipv6 address fe80::2 link-local
[DeviceB-GigabitEthernet1/0/1] ipv6 address 1::2 64
```

创建 VRRP 备份组 1，并配置备份组 1 的虚拟 IPv6 地址为 FE80::10 和 1::10。

```
[DeviceB-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[DeviceB-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 virtual-ip 1::10
```

配置允许发布 RA 消息，以便 Area A 的主机通过 RA 消息学习到缺省网关地址。

[DeviceB-GigabitEthernet1/0/1] undo ipv6 nd ra halt

设置 Device B 工作在抢占方式，抢占延迟时间为 5 秒。

```
[DeviceB-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 preempt-mode delay 500
[DeviceB-GigabitEthernet1/0/1] quit
```

7.6 验证配置

配置完成后，Area A 里面的主机可以 ping 通外网。如 Host A 可以 ping 通 IPv6 地址为 30::1 的主机。

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\hostA>ping 30::1

Pinging 30::1 with 32 bytes of data:
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms

Ping statistics for 30::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

通过 **display vrrp ipv6 verbose** 命令查看配置后的结果，显示 Device A 上 IPv6 VRRP 备份组 1 的详细信息。

```
[DeviceA] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running mode      : Standard
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                 Adver Timer   : 100
     Admin Status   : Up                State         : Master
     Config Pri     : 110               Running Pri   : 110
```

```
    Preempt Mode   : Yes                Delay Time   : 500
    Auth Type      : None
    Virtual IP     : FE80::10
                     1::10
    Virtual MAC    : 0000-5e00-0201
    Master IP      : FE80::1
  VRRP Track Information:
    Track Object   : 1                  State : Positive   Pri Reduced : 50
```

通过 **display vrrp ipv6 verbose** 命令查看配置后的结果，显示 Device B 上 IPv6 VRRP 备份组 1 的详细信息。

```
[DeviceB] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                  Adver Timer  : 100
     Admin Status   : Up                 State        : Backup
     Config Pri     : 100                Running Pri  : 100
     Preempt Mode   : Yes                Delay Time   : 500
     Become Master  : 3000ms left
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Master IP      : FE80::1
```

以上显示信息表示在 IPv6 VRRP 备份组 1 中 Device A 为 Master 路由器，Device B 为 Backup 路由器，Area A 的用户发送给外网的报文通过 Device A 转发。

Device A 或 Device A 的上行接口出现故障后，Area A 的用户上仍然可以与外网通信。

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\hostA>ping 30::1

Pinging 30::1 with 32 bytes of data:
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms

Ping statistics for 30::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

通过 **display vrrp ipv6 verbose** 命令查看 Device B 上 IPv6 VRRP 备份组的详细信息，Device A 或 Device A 的上行接口出现故障后，显示 Device B 上 IPv6 VRRP 备份组 1 的详细信息。

```
[DeviceB] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                 Adver Timer   : 100
     Admin Status   : Up                State         : Master
     Config Pri     : 100               Running Pri   : 100
     Preempt Mode   : Yes               Delay Time    : 500
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Virtual MAC    : 0000-5e00-0201
     Master IP      : FE80::2
```

以上显示信息表示 Device A 或 Device A 的上行接口出现故障后，Device B 成为 Master 路由器，Area A 的用户发送给外网的报文通过 Device B 转发。

Device A 或 Device A 的上行接口故障恢复后，显示 Device A 上 VRRP 备份组 1 的详细信息。

```
[DeviceA] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running mode      : Standard
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                 Adver Timer   : 100
     Admin Status   : Up                State         : Master
     Config Pri     : 110               Running Pri   : 110
     Preempt Mode   : Yes               Delay Time    : 500
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Virtual MAC    : 0000-5e00-0201
     Master IP      : FE80::1
   VRRP Track Information:
     Track Object   : 1                 State : Positive   Pri Reduced : 50
```

以上显示信息表示 Device A 故障恢复后，Device A 会抢占成为 Master，Area A 的用户发送给外网的报文仍然通过 Device A 转发。

7.7 配置文件

- Device A：

```
#
 sysname DeviceA
#
interface GigabitEthernet1/0/1
 port link-mode route
ipv6 address fe80::1 link-local
```

```
ipv6 address 1::1/64
 undo ipv6 nd ra halt
 vrrp ipv6 vrid 1 virtual-ip FE80::10 link-local
 vrrp ipv6 vrid 1 virtual-ip 1::10
 vrrp ipv6 vrid 1 priority 110
 vrrp ipv6 vrid 1 preempt-mode delay 500
 vrrp ipv6 vrid 1 track 1 priority reduced 50
#
track 1 interface GigabitEthernet1/0/3
#
```

- Device B：

```
#
 sysname DeviceB
#
interface GigabitEthernet1/0/1
 port link-mode route
ipv6 address fe80::2 link-local
ipv6 address 1::2/64
 undo ipv6 nd ra halt
 vrrp ipv6 vrid 1 virtual-ip FE80::10 link-local
 vrrp ipv6 vrid 1 virtual-ip 1::10
 vrrp ipv6 vrid 1 preempt-mode delay 500
#
```

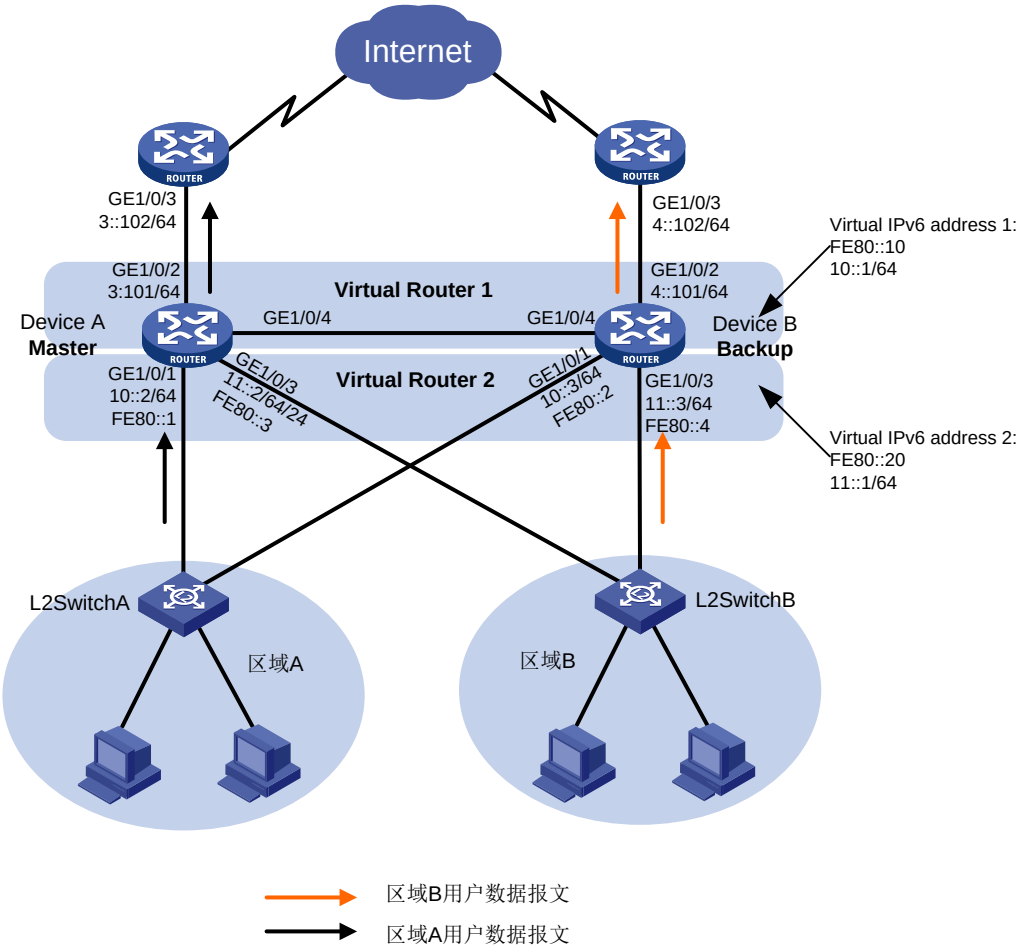
8 IPv6 VRRP 多备份组配置举例

8.1 组网需求

如图 6 所示，某公司为了实现网关设备的冗余备份，以及内网主机流量的负载分担，在内部网络的出口处部署了两台设备，并使用 VRRP 负载分担功能，将这两台设备组成两台虚拟路由器，分别作为区域 A 和区域 B 的缺省网关。具体应用需求如下：

- Device A 是 VRRP 备份组 1 中的 Master 设备，Device B 是 VRRP 备份组 2 中的 Master 设备。在正常情况下，区域 A 的用户通过 Device A 进行数据转发，区域 B 的用户通过 Device B 进行数据转发。
- 当 Device A 或者 Device A 的上行接口发生故障后，Device B 能够迅速承担区域 A 内主机流量的转发任务；Device A 故障恢复后，继续承担 VRRP 备份组 1 的网关功能；
- 当 Device B 或者 Device B 的上行接口故障发生故障后，Device A 能够迅速承担区域 B 内主机流量的转发任务；Device B 故障恢复后，继续承担 VRRP 备份组 2 的网关功能。

图6 IPv6 VRRP 多备份组配置组网图



8.2 配置思路

- 为了让 Device A 和 Device B 分别成为 VRRP 备份组 1 和 VRRP 备份组 2 中的 Master，需要在 VRRP 备份组 1 中为 Device A 配置较高的优先级，在 VRRP 备份组 2 中为 Device B 配置较高的优先级。
- 为了避免 VRRP 备份组中的角色频繁发生变化，可以配置一定的抢占延迟时间。
- 将 VRRP 组的抢占模式和监视上行接口状态功能结合使用，可以使 Master 设备根据上行接口的状态自动调整自身的 VRRP 优先级，从而使 VRRP 组内的角色发生转变，实现主备切换；

8.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

8.4 配置注意事项

- 建议将备份组的虚拟 IPv6 地址和备份组中设备下行接口的 IPv6 地址配置为同一网段，否则可能导致局域网内的主机无法访问外部网络。

- IPv6 VRRP 既可以使用 VRRPv2 版本，也可以使用 VRRPv3 版本（缺省情况使用 VRRPv3）。请确保 IPv6 VRRP 备份组中的所有路由器上配置的 IPv6 VRRP 版本一致，否则 VRRP 备份组无法正常工作。
- 删除 IP 地址拥有者上的 VRRP 备份组，将导致地址冲突。建议先修改配置了 VRRP 备份组的接口的 IPv6 地址，再删除该接口上的 VRRP 备份组，以避免地址冲突。
- 用户在配置降低优先级幅度时，需要确保降低后的优先级比 VRRP 备份组内其他设备的优先级要低，确保 VRRP 备份组内有其他设备被选为 Master 设备。
- 对于同一个 VRRP 备份组的成员设备，如下配置必须保证完全一样：
  - 虚拟路由器的 IP 地址个数
  - 每个备份组虚拟路由器的 IP 地址
  - 定时器间隔时间

8.5 配置步骤

(1) Device A 的配置

配置接口 IPv6 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ipv6 address fe80::1 link-local
[DeviceA-GigabitEthernet1/0/1] ipv6 address 10::2 64
```

请参考以上方法配置 8.1 图 6 中其它接口的 IPv6 地址，配置步骤这里省略。

创建 VRRP 备份组 1，并配置备份组 1 的虚拟 IPv6 地址为 FE80::10 和 10::1，配置抢占延迟时间为 5 秒，并配置 Device A 在 VRRP 备份组 1 中的优先级为 120，高于 Device B 的优先级。

```
[DeviceA-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[DeviceA-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 virtual-ip 10::1
[DeviceA-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 preempt-mode delay 500
[DeviceA-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 priority 120
```

配置允许发布 RA 消息，以便 Area A 内主机通过 RA 消息学习到缺省网关地址。

```
[DeviceA-GigabitEthernet1/0/1] undo ipv6 nd ra halt
[DeviceA-GigabitEthernet1/0/1] quit
```

创建 VRRP 备份组 2，并配置备份组 2 的虚拟 IPv6 地址为 FE80::20 和 11::1，配置抢占延迟时间为 5 秒。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] vrrp ipv6 vrid 2 virtual-ip fe80::20 link-local
[DeviceA-GigabitEthernet1/0/3] vrrp ipv6 vrid 2 virtual-ip 11::1
[DeviceA-GigabitEthernet1/0/3] vrrp ipv6 vrid 2 preempt-mode delay 500
```

配置允许发布 RA 消息，以便 Area B 内主机通过 RA 消息学习到缺省网关地址。

```
[DeviceA-GigabitEthernet1/0/3] undo ipv6 nd ra halt
[DeviceA-GigabitEthernet1/0/3] quit
```

创建和上行接口 GigabitEthernet 1/0/2 关联的 Track 项 1。

```
[DeviceA] track 1 interface gigabitethernet 1/0/2
```

配置监视 Track 项 1，Track 项的状态为 Negative 时，Device A 在 VRRP 备份组 1 中的优先级降低的数值为 50。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 track 1 priority reduced 50
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) Device B 的配置

```
<DeviceB> system-view
[DeviceB] interface gigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ipv6 address fe80::2 link-local
[DeviceB-GigabitEthernet1/0/1] ipv6 address 10::3 64
```

请参考以上方法配置 8.1 图 6 中其它接口的 IP 地址，配置步骤省略。

创建 VRRP 备份组 1，并配置备份组 1 的虚拟 IPv6 地址为 FE80::10 和 10::1。

```
[DeviceB-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[DeviceB-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 virtual-ip 10::1
[DeviceB-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 preempt-mode delay 500
```

配置允许发布 RA 消息，以便 Area A 内主机通过 RA 消息学习到缺省网关地址。

```
[DeviceB-GigabitEthernet1/0/1] undo ipv6 nd ra halt
[DeviceB-GigabitEthernet1/0/1] quit
```

创建 VRRP 备份组 2，并配置备份组 1 的虚拟 IPv6 地址为 FE80::20 和 11::1，并配置 Device B 在 VRRP 备份组 2 中的优先级为 120，高于 Device A 的优先级。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] vrrp ipv6 vrid 2 virtual-ip fe80::20 link-local
[DeviceB-GigabitEthernet1/0/3] vrrp ipv6 vrid 2 virtual-ip 11::1
[DeviceB-GigabitEthernet1/0/3] vrrp ipv6 vrid 2 priority 120
[DeviceA-GigabitEthernet1/0/3] vrrp ipv6 vrid 2 preempt-mode delay 500
```

配置允许发布 RA 消息，以便 Area B 内主机通过 RA 消息学习到缺省网关地址。

```
[DeviceB-GigabitEthernet1/0/3] undo ipv6 nd ra halt
[DeviceB-GigabitEthernet1/0/3] quit
```

创建和上行接口 GigabitEthernet 1/0/2 关联的 Track 项 2。

```
[DeviceB] track 2 interface gigabitethernet 1/0/2
```

配置监视 Track 项 2，Track 项的状态为 Negative 时，Device B 在 VRRP 备份组 2 中的优先级降低的数值为 50。

```
[DeviceB] interface gigabitEthernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] vrrp ipv6 vrid 2 track 2 priority reduced 50
[DeviceB-GigabitEthernet1/0/3] quit
```

8.6 验证配置

(1) 配置完成后，区域 A 和区域 B 中的主机都可以 ping 通外网。

检查区域 A 到外网 IPv6 地址为 30::1 的主机是否可达。

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\areaA>ping 30::1
```

```
Pinging 30::1 with 32 bytes of data:
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms

Ping statistics for 30::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

检查区域 B 到外网 IPv6 地址为 30::1 的主机是否可达。

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\areaB>ping 30::1

Pinging 30::1 with 32 bytes of data:
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms

Ping statistics for 30::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

(2) 通过 **display vrrp ipv6 verbose** 命令查看配置后的结果。

查看 Device A 上全部 IPv6 VRRP 备份组的详细信息，显示 Device A 在 VRRP 备份组 1 中为 Master 设备，在 VRRP 备份组 2 中为 Backup 设备。

```
[DeviceA] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode       : Standard
 Total number of virtual routers : 2
   Interface GigabitEthernet1/0/1
     VRID           : 1                  Adver Timer  : 100
     Admin Status   : Up                 State        : Master
     Config Pri     : 120                Running Pri  : 120
     Preempt Mode   : Yes                Delay Time   : 500
     Auth Type      : None
     Virtual IP     : FE80::10
10::1
     Virtual MAC    : 0000-5e00-0201
     Master IP      : FE80::1
   VRRP Track Information:
     Track Object   : 1                  State : Positive   Pri Reduced : 50

   Interface GigabitEthernet1/0/3
```

```
    VRID            : 2                 Adver Timer  : 100
    Admin Status    : Up                State        : Backup
    Config Pri      : 100               Running Pri  : 100
    Preempt Mode    : Yes               Delay Time   : 500
    Auth Type       : None
    Become Master   : 3550ms left
    Virtual IP      : FE80::20
                      11::1
    Master IP       : FE80::4
```

查看 Device B 上全部 IPv6 VRRP 备份组的详细信息，显示 Device B 在备份组 1 中为 Backup 设备，在备份组 2 中为 Master 设备。

```
[DeviceB] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode       : Standard
 Total number of virtual routers : 2
   Interface GigabitEthernet1/0/1
     VRID            : 1                 Adver Timer  : 100
     Admin Status    : Up                State        : Backup
     Config Pri      : 100               Running Pri  : 100
     Preempt Mode    : Yes               Delay Time   : 500
     Auth Type       : None
     Become Master   : 3500ms left
     Virtual IP      : FE80::10
10::2
     Master IP       : FE80::1

   Interface GigabitEthernet1/0/3
     VRID            : 2                 Adver Timer  : 100
     Admin Status    : Up                State        : Master
     Config Pri      : 120               Running Pri  : 120
     Preempt Mode    : Yes               Delay Time   : 500
     Auth Type       : None
     Virtual IP      : FE80::20
  11::1
     Virtual MAC     : 0000-5e00-0202
     Master IP       : FE80::4
   VRRP Track Information:
     Track Object    : 2                 State : Positive   Pri Reduced : 50
```

Device A 或 Device A 的上行接口出现故障后，通过 **display vrrp ipv6 verbose** 命令查看 Device B 上备份组的详细信息。可以看到 Device B 抢占为备份组 1 的 Master。

```
[DeviceB] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running  Mode       : Standard
 Total number of virtual routers : 2
   Interface GigabitEthernet1/0/1
     VRID            : 1                 Adver Timer  : 100
     Admin Status    : Up                State        : Master
     Config Pri      : 100               Running Pri  : 100
```

```
     Preempt Mode   : Yes                 Delay Time   : 500
     Auth Type      : None
     Virtual IP     : FE80::10
10::2
     Virtual MAC    : 0000-5e00-0101
     Master IP      : FE80::2

  Interface GigabitEthernet1/0/3
     VRID           : 2                   Adver Timer  : 100
     Admin Status   : Up                  State        : Master
     Config Pri     : 120                 Running Pri  : 120
     Preempt Mode   : Yes                 Delay Time   : 500
     Auth Type      : None
     Virtual IP     : FE80::20
  11::1
     Virtual MAC    : 0000-5e00-0202
     Master IP      : FE80::4
   VRRP Track Information:
     Track Object   : 2                   State : Positive   Pri Reduced : 50
```

以上显示信息表示 Device A 或 Device A 的上行接口出现故障后，Device B 设备抢占成为 Master，负责转发用户的业务数据。

当 Device A 或 Device A 的上行接口故障恢复后，显示 Device A 上备份组的详细信息。

```
[DeviceA] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode       : Standard
 Total number of virtual routers : 2
   Interface GigabitEthernet1/0/1
     VRID           : 1                   Adver Timer  : 100
     Admin Status   : Up                  State        : Master
     Config Pri     : 120                 Running Pri  : 120
     Preempt Mode   : Yes                 Delay Time   : 500
     Auth Type      : None
     Virtual IP     : FE80::10
10::1
     Virtual MAC    : 0000-5e00-0201
     Master IP      : FE80::1
   VRRP Track Information:
     Track Object   : 1                   State : Positive   Pri Reduced : 50

   Interface GigabitEthernet1/0/3
     VRID           : 2                   Adver Timer  : 100
     Admin Status   : Up                  State        : Backup
     Config Pri     : 100                 Running Pri  : 100
     Preempt Mode   : Yes                 Delay Time   : 500
     Auth Type      : None
     Become Master  : 3550ms left
     Virtual IP     : FE80::20
                      11::1
```

```
Master IP      : FE80::4
```

以上显示信息表示当 Device A 或 Device A 的上行接口故障恢复后，Device A 在 VRRP 备份组 1 中恢复为原来的优先级并抢占成为该备份组的 Master，区域 A 内的主机通过 Device A 与外界通信。

8.7 配置文件

- Device A：

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ipv6 address fe80::1 link-local
ipv6 address 10::2/64
undo ipv6 nd ra halt
 vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
 vrrp ipv6 vrid 1 virtual-ip 10::1
 vrrp ipv6 vrid 1 priority 120
 vrrp ipv6 vrid 1 preempt-mode delay 500
 vrrp ipv6 vrid 1 track 1 priority reduced 50
#
interface GigabitEthernet1/0/2
 port link-mode route
ipv6 address 3::101/64
#
interface GigabitEthernet1/0/3
 port link-mode route
 ipv6 address fe80::3 link-local
ipv6 address 11::2/64
undo ipv6 nd ra halt
vrrp ipv6 vrid 2 virtual-ip fe80::20 link-local
 vrrp ipv6 vrid 2 virtual-ip 11::1
vrrp ipv6 vrid 2 preempt-mode delay 500
#
 track 1 interface gigabitethernet 1/0/2
#
```

- Device B：

```
#
interface GigabitEthernet1/0/1
 port link-mode route
ipv6 address fe80::2 link-local
ipv6 address 10::3/64
undo ipv6 nd ra halt
 vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
 vrrp ipv6 vrid 1 virtual-ip 10::1
vrrp ipv6 vrid 1 preempt-mode delay 500

#
```

```
interface GigabitEthernet1/0/2
 port link-mode route
 ipv6 address 4::101/64
#
interface GigabitEthernet1/0/3
 port link-mode route
 ipv6 address fe80::4 link-local
ipv6 address 11::3/64
undo ipv6 nd ra halt
vrrp ipv6 vrid 2 virtual-ip fe80::20 link-local
 vrrp ipv6 vrid 2 virtual-ip 11::1
vrrp ipv6 vrid 2 priority 120
vrrp ipv6 vrid 2 preempt-mode delay 500
vrrp ipv6 vrid 2 track 2 priority reduced 50
#
 track 2 interface gigabitethernet 1/0/2
#
```

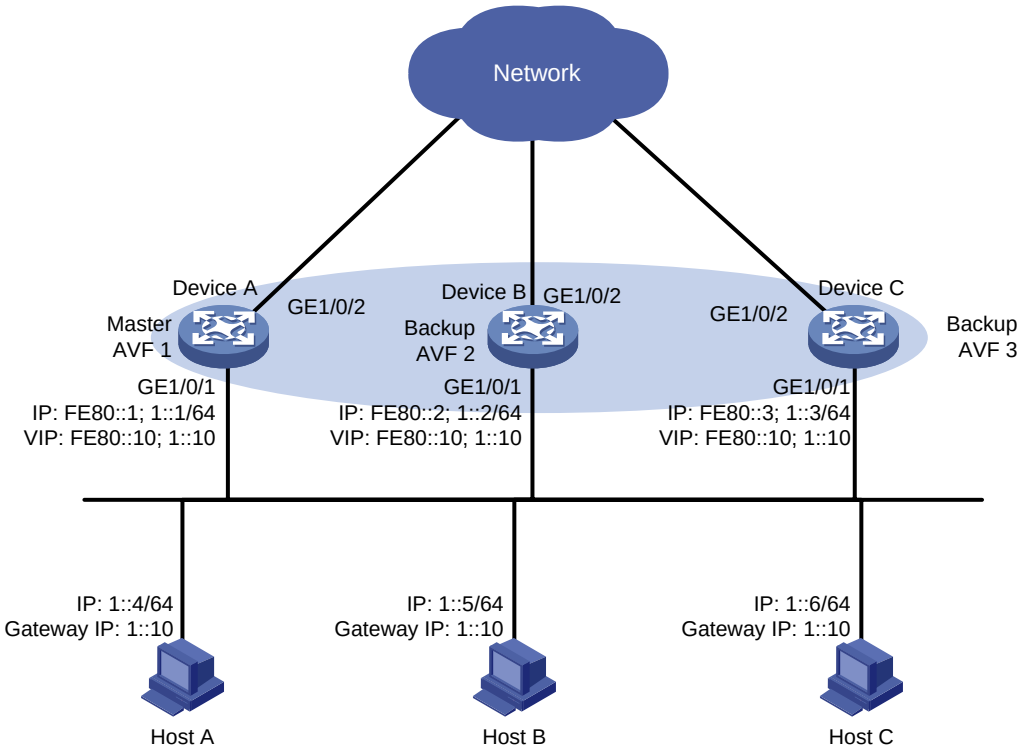
9 IPv6 VRRP 负载均衡模式配置举例

9.1 组网需求

如图 7 所示，Host A、Host B 和 Host C 所在网络的出口处部署了三台设备。现要求使用 VRRP 负载均衡功能，将 Device A、Device B 和 Device C 组成一台虚拟路由器，作为局域网内主机的缺省网关。具体应用需求如下：

- 实现 VRRP 备份组中三台设备都可以转发报文，实现流量负载分担，充分利用网关资源；
- 当 Device A、Device B 或 Device C 自身或其上行接口出现故障时，Host A、Host B 和 Host C 可以通过其他正常运行的设备继续通信，避免通信中断；当 Device A、Device B 或 Device C 故障恢复后，继续承担网关功能。

图7 IPv6 VRRP 负载均衡模式配置组网图



9.2 配置思路

- 为了使 Device A 优先与 Device B 和 Device C 被选举为 VRRP 备份组的 Master 设备，需要为其配置高于 Device B 和 Device C 的优先级；为了使 Device B 优先于 Device C 被选举为 VRRP 备份组的 Master 设备，需要为其配置高于 Device C 的优先级；
- 为了避免由于故障造成 VRRP 备份组中的角色频繁发生变化，可以配置一定的抢占延迟时间；
- 在 Device A、Device B 和 Device C 上配置虚拟转发器通过 Track 项监视上行接口的状态。当上行接口出现故障时，降低该接口所在设备虚拟转发器的权重，以便其他设备接管该设备的转发任务，避免通信中断；
- 为了保证原 Master 设备故障恢复后，能再次抢占成为 Master，需要配置 VRRP 备份组工作在抢占模式。

9.3 使用版本

本举例是在 R8128 版本上进行配置和验证的。

9.4 配置注意事项

- 建议将备份组的虚拟 IPv6 地址和备份组中设备下行接口的 IPv6 地址配置为同一网段，否则可能导致局域网内的主机无法访问外部网络。

- IPv6 VRRP 既可以使用 VRRPv2 版本，也可以使用 VRRPv3 版本（缺省情况使用 VRRPv3）。请确保 IPv6 VRRP 备份组中的所有路由器上配置的 IPv6 VRRP 版本一致，否则 VRRP 备份组无法正常工作。
- VRRP 工作在负载均衡模式时，备份组的虚拟 IPv6 地址和接口的 IPv6 地址不能相同，否则 VRRP 负载均衡功能将无法正常工作。
- 当监视的上行链路出现故障时，配置的权重降低数额需保证 VF Owner 的权重低于失效下限，即权重降低的数额大于 245，其它的虚拟转发器才能接替 VF Owner 成为 AVF。
- 对于同一个 VRRP 备份组的成员设备，必须保证备份组虚拟路由器的 IPv6 地址配置完全一样。
- 用户在配置降低权重幅度时，需要确保降低后的优先级比 VRRP 备份组内其他设备的优先级要低，确保 VRRP 备份组内有其他设备被选为 Master。

9.5 配置步骤

9.5.1 Device A 的配置

(1) 配置接口

配置接口 IPv6 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address ipv6 address fe80::1 link-local
[DeviceA-GigabitEthernet1/0/1] ipv6 address 1::1 64
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 配置 VRRP

配置 VRRP 工作在负载均衡模式。

```
[DeviceA] vrrp ipv6 mode load-balance
```

创建 VRRP 备份组 1，并配置备份组 1 的虚拟 IPv6 地址为 FE80::10 和 1::10。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[DeviceA-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 virtual-ip 1::10
```

配置 Device A 在 VRRP 备份组 1 中的优先级为 120，高于 Device B 的优先级 110 和 Device C 的优先级 100，以保证 Device A 成为 Master。

```
[DeviceA-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 priority 120
```

配置 Device A 工作在抢占方式，配置抢占延迟时间为 5 秒。

```
[DeviceA-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 preempt-mode delay 500
```

配置允许发布 RA 消息，以便 1::/64 网段内主机通过 RA 消息学习到缺省网关地址。

```
[DeviceA-GigabitEthernet1/0/1] undo ipv6 nd ra halt
[DeviceA-GigabitEthernet1/0/1] quit
```

(3) 配置 Track

创建和 GigabitEthernet1/0/2 关联的 Track 项 1。如果 Track 项的状态为 Negative，则说明 Device A 的上行接口出现故障。

```
[DeviceA] track 1 interface gigabitethernet 1/0/2
```

配置虚拟转发器监视 Track 项 1。Track 项的状态为 Negative 时，降低 Device A 上虚拟转发器的权重，使其低于失效下限 10，即权重降低的数额大于 245，以便其他设备接替 Device A 的转发任务。本例中，配置虚拟转发器权重降低数额为 250。

```
[DeviceA] interface gigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 track 1 weight reduced 250
[DeviceA-GigabitEthernet1/0/1] quit
```

9.5.2 Device B 的配置

(1) 配置接口

配置接口 IPv6 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address ipv6 address fe80::2 link-local
[DeviceB-GigabitEthernet1/0/1] ipv6 address 1::2 64
[DeviceB-GigabitEthernet1/0/1] quit
```

(2) 配置 VRRP

配置 VRRP 工作在负载均衡模式。

```
[DeviceB] vrrp ipv6 mode load-balance
```

创建 VRRP 备份组 1，并配置备份组 1 的虚拟 IPv6 地址为 FE80::10 和 1::10。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[DeviceB-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 virtual-ip 1::10
```

配置 Device B 的优先级 110，高于 Device C 的优先级 100，以保证 Device A 出现故障时，Device B 成为 Master。

```
[DeviceB-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 priority 110
```

配置 Device B 工作在抢占方式，配置抢占延迟时间为 5 秒。

```
[DeviceB-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 preempt-mode delay 500
```

配置允许发布 RA 消息，以便 1::/64 网段内主机通过 RA 消息学习到缺省网关地址。

```
[DeviceB-GigabitEthernet1/0/1] undo ipv6 nd ra halt
[DeviceB-GigabitEthernet1/0/1] quit
```

(3) 配置 Track

创建和 GigabitEthernet1/0/2 关联的 Track 项 1。如果 Track 项的状态为 Negative，则说明 Device B 的上行接口出现故障。

```
[DeviceB] track 1 interface gigabitethernet 1/0/2
```

配置虚拟转发器监视 Track 项 1。Track 项的状态为 Negative 时，降低 Device B 上虚拟转发器的权重，使其低于失效下限 10，即权重降低的数额大于 245，以便其他设备接替 Device B 的转发任务。本例中，配置虚拟转发器权重降低数额为 250。

```
[DeviceB] interface gigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 track 1 weight reduced 250
[DeviceB-GigabitEthernet1/0/1] quit
```

9.5.3 Device C 的配置

(1) 配置接口

配置接口 IPv6 地址。

```
<DeviceC> system-view
[DeviceC] interface gigabitEthernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ip address ipv6 address fe80::3 link-local
[DeviceC-GigabitEthernet1/0/1] ipv6 address 1::3 64
[DeviceC-GigabitEthernet1/0/1] quit
```

(2) 配置 VRRP

配置 VRRP 工作在负载均衡模式。

```
[DeviceC] vrrp ipv6 mode load-balance
```

创建 VRRP 备份组 1，并配置备份组 1 的虚拟 IPv6 地址为 FE80::10 和 1::10。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[DeviceC-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 virtual-ip 1::10
```

配置 Device C 工作在抢占方式，配置抢占延迟时间为 5 秒。

```
[DeviceC-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 preempt-mode delay 500
```

配置允许发布 RA 消息，以便 1::/64 网段内主机通过 RA 消息学习到缺省网关地址。

```
[DeviceC-GigabitEthernet1/0/1] undo ipv6 nd ra halt
[DeviceC-GigabitEthernet1/0/1] quit
```

(3) 配置 Track

创建和 GigabitEthernet1/0/2 关联的 Track 项 1。如果 Track 项的状态为 Negative，则说明 Device C 的上行接口出现故障。

```
[DeviceC] track 1 interface gigabitethernet 1/0/2
```

配置虚拟转发器监视 Track 项 1。Track 项的状态为 Negative 时，降低 Device C 上虚拟转发器的权重，使其低于失效下限 10，即权重降低的数额大于 245，以便其他设备接替 Device C 的转发任务。本例中，配置虚拟转发器权重降低数额为 250。

```
[DeviceC] interface gigabitEthernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 track 1 weight reduced 250
[DeviceC-GigabitEthernet1/0/1] quit
```

9.5.4 验证配置

(1) 配置完成后，在 Host A 上可以 ping 通外网，通过 **display vrrp ipv6 verbose** 命令查看配置后的结果

显示 Device A 上 VRRP 备份组的详细信息。

```
[DeviceA] display vrrp ipv6 verbose
IPv6 Virtual Device Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                    Adver Timer  : 100
     Admin Status   : Up                   State        : Master
     Config Pri     : 120                  Running Pri  : 120
     Preempt Mode   : Yes                  Delay Time   : 500
     Auth Type      : None
     Virtual IP     : FE80::10
```

```
1::10
     Member IP List : FE80::1 (Local, Master)
                      FE80::2 (Backup)
                      FE80::3 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Active
     Virtual MAC    : 000f-e2ff-0011 (Owner)
     Owner ID       : 0000-5e01-1101
     Priority       : 255
     Active         : local
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 127
     Active         : FE80::2
    Forwarder 03
     State          : Listening
     Virtual MAC    : 000f-e2ff-0013 (Learnt)
     Owner ID       : 0000-5e01-1105
     Priority       : 127
     Active         : FE80::3
   Forwarder Weight Track Information:
     Track Object   : 1          State : Positive   Weight Reduced : 250
```

显示 Device B 上 VRRP 备份组的详细信息。

```
[DeviceB] display vrrp ipv6 verbose
IPv6 Virtual Device Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                    Adver Timer  : 100
     Admin Status   : Up                   State        : Backup
     Config Pri     : 110                  Running Pri  : 110
     Preempt Mode   : Yes                  Delay Time   : 500
     Auth Type      : None
     Virtual IP     : FE80::10
1::10
     Member IP List : FE80::2 (Local, Backup)
                      FE80::1 (Master)
                      FE80::3 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Listening
```

```
    Virtual MAC    : 000f-e2ff-0011 (Learnt)
    Owner ID       : 0000-5e01-1101
    Priority       : 127
    Active         : FE80::1
  Forwarder 02
    State          : Active
    Virtual MAC    : 000f-e2ff-0012 (Owner)
    Owner ID       : 0000-5e01-1103
    Priority       : 255
    Active         : local
  Forwarder 03
    State          : Listening
    Virtual MAC    : 000f-e2ff-0013 (Learnt)
    Owner ID       : 0000-5e01-1105
    Priority       : 127
    Active         : FE80::3
 Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

显示 Device C 上 VRRP 备份组的详细信息。

```
[DeviceC] display vrrp ipv6 verbose
IPv4 Virtual Device Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                    Adver Timer  : 100
     Admin Status   : Up                   State        : Backup
     Config Pri     : 100                  Running Pri  : 100
     Preempt Mode   : Yes                  Delay Time   : 500
     Auth Type      : None
   Virtual IP     : FE80::10
1::10
     Member IP List : FE80::3 (Local, Backup)
                      FE80::1 (Master)
                      FE80::2 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
   Forwarder 01
     State          : Listening
     Virtual MAC    : 000f-e2ff-0011 (Learnt)
     Owner ID       : 0000-5e01-1101
     Priority       : 127
     Active         : FE80::1
   Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 127
```

```
    Active         : FE80::2
   Forwarder 03
    State          : Active
    Virtual MAC    : 000f-e2ff-0013 (Owner)
    Owner ID       : 0000-5e01-1105
    Priority       : 255
    Active         : local
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

以上显示信息表示在VRRP备份组1中Device A为Master，Device B和Device C为Backup。Device A、Device B和Device C上各自存在一个AVF，并存在作为备份的两个LVF。

(2) Device A的上行接口（GigabitEthernet1/0/2）出现故障后

显示Device A上VRRP备份组的详细信息。

```
[DeviceA] display vrrp ipv6 verbose
IPv6 Virtual Device Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                    Adver Timer  : 100
     Admin Status   : Up                   State        : Master
     Config Pri     : 120                  Running Pri  : 120
     Preempt Mode   : Yes                  Delay Time   : 500
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Member IP List : FE80::1 (Local, Master)
                      FE80::2 (Backup)
                      FE80::3 (Backup)
   Forwarder Information: 3 Forwarders 0 Active
     Config Weight  : 255
     Running Weight : 5
    Forwarder 01
     State          : Initialize
     Virtual MAC    : 000f-e2ff-0011 (Owner)
     Owner ID       : 0000-5e01-1101
     Priority       : 0
     Active         : FE80::3
    Forwarder 02
     State          : Initialize
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 0
     Active         : FE80::2
    Forwarder 03
     State          : Initialize
     Virtual MAC    : 000f-e2ff-0013 (Learnt)
     Owner ID       : 0000-5e01-1105
```

```
    Priority       : 0
    Active         : FE80::3
  Forwarder Weight Track Information:
    Track Object   : 1          State : Negative   Weight Reduced : 250
```

显示 Device C 上 VRRP 备份组的详细信息。

```
[DeviceC] display vrrp ipv6 verbose
IPv6 Virtual Device Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                    Adver Timer  : 100
     Admin Status   : Up                   State        : Backup
     Config Pri     : 100                  Running Pri  : 100
     Preempt Mode   : Yes                  Delay Time   : 500
     Auth Type      : None
     Become Master  : 3550ms left
      Virtual IP     : FE80::10
                       1::10
     Member IP List : FE80::3 (Local, Backup)
                      FE80::1 (Master)
                      FE80::2 (Backup)
   Forwarder Information: 3 Forwarders 2 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Active
     Virtual MAC    : 000f-e2ff-0011 (Take Over)
     Owner ID       : 0000-5e01-1101
     Priority       : 85
     Active         : local
     Redirect Time  : 93 secs
     Time-out Time  : 1293 secs
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 85
     Active         : FE80::2
    Forwarder 03
     State          : Active
     Virtual MAC    : 000f-e2ff-0013 (Owner)
     Owner ID       : 0000-5e01-1105
     Priority       : 255
     Active         : local
   Forwarder Weight Track Information:
     Track Object   : 1          State : Positive   Weight Reduced : 250
```

以上显示信息表示 Device A 的上行接口出现故障后，Device A 上虚拟转发器的权重降低为 5，低于失效下限。Device A 上所有虚拟转发器的状态均变为 Initialized，不能再用于转发。

Device C 成为虚拟 MAC 地址 000f-e2ff-0011 对应虚拟转发器的 AVF，接管 Device A 的转发任务。

Timeout Timer 超时后（约 1800 秒后），查看 Device C 上 VRRP 备份组的详细信息。

```
[DeviceC] display vrrp ipv6 verbose
IPv6 Virtual Device Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                    Adver Timer  : 100
     Admin Status   : Up                   State        : Backup
     Config Pri     : 100                  Running Pri  : 100
     Preempt Mode   : Yes                  Delay Time   : 500
     Auth Type      : None
     Become Master  : 3550ms left
     Virtual IP     : FE80::10
                      1::10
     Member IP List : FE80::3 (Local, Backup)
                      FE80::1 (Master)
                      FE80::2 (Backup)
   Forwarder Information: 2 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 127
     Active         : FE80::2
    Forwarder 03
     State          : Active
     Virtual MAC    : 000f-e2ff-0013 (Owner)
     Owner ID       : 0000-5e01-1105
     Priority       : 255
     Active         : local
   Forwarder Weight Track Information:
     Track Object   : 1          State : Positive   Weight Reduced : 250
```

以上显示信息表示，Timeout Timer 超时后，删除虚拟 MAC 地址 000f-e2ff-0011 对应的虚拟转发器，不再转发目的 MAC 地址为该 MAC 的报文。

(3) Device A 出现故障后

显示 Device B 上 VRRP 备份组的详细信息。

```
[DeviceB] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1                    Adver Timer  : 1
```

```
    Admin Status   : Up                 State         : Master
    Config Pri     : 110                Running Pri   : 110
    Preempt Mode   : Yes                Delay Time    : 500
    Auth Type      : None
    Virtual IP     : FE80::10
                     1::10
    Member IP List : FE80::2 (Local, Master)
                     FE80::3 (Backup)
  Forwarder Information: 2 Forwarders 1 Active
    Config Weight  : 255
    Running Weight : 255
   Forwarder 02
    State          : Active
    Virtual MAC    : 000f-e2ff-0012 (Owner)
    Owner ID       : 0000-5e01-1103
    Priority       : 255
    Active         : local
   Forwarder 03
    State          : Listening
    Virtual MAC    : 000f-e2ff-0013 (Learnt)
    Owner ID       : 0000-5e01-1105
    Priority       : 127
    Active         : FE80::3
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

以上显示信息表示 Device A 出现故障后，Device B 的优先级高于 Device C，将抢占成为 Master。

9.5.5 配置文件

- Device A：

```
#
 vrrp ipv6 mode load-balance
#
interface GigabitEthernet1/0/1
 port link-mode route
 ipv6 address fe80::1 link-local
 ipv6 address 1::1 64
undo ipv6 nd ra halt
 vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
vrrp ipv6 vrid 1 virtual-ip 1::10
 vrrp ipv6 vrid 1 priority 120
vrrp ipv6 vrid 1 preempt-mode delay 500
 vrrp ipv6 vrid 1 track 1 weight reduced 250
#
interface GigabitEthernet1/0/2
 port link-mode route
#
```

```
track 1 interface GigabitEthernet1/0/2
#
```

- Device B：

```
#
 vrrp ipv6 mode load-balance
#
interface GigabitEthernet1/0/1
 port link-mode route
ipv6 address fe80::2 link-local
 ipv6 address 1::2 64
undo ipv6 nd ra halt
 vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
vrrp ipv6 vrid 1 virtual-ip 1::10
 vrrp ipv6 vrid 1 priority 110
vrrp ipv6 vrid 1 preempt-mode delay 500
 vrrp ipv6 vrid 1 track 1 weight reduced 250
#
interface GigabitEthernet1/0/2
 port link-mode route
#
track 1 interface GigabitEthernet1/0/2
#
```

- Device C：

```
#
 vrrp ipv6 mode load-balance
#
interface GigabitEthernet1/0/1
ipv6 address fe80::3 link-local
 ipv6 address 1::3 64
undo ipv6 nd ra halt
 vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
vrrp ipv6 vrid 1 virtual-ip 1::10
vrrp ipv6 vrid 1 preempt-mode delay 500
 vrrp ipv6 vrid 1 track 1 weight reduced 250
#
interface GigabitEthernet1/0/2
 port link-mode route
#
track 1 interface GigabitEthernet1/0/2
#
```

10 相关资料

- H3C SR6600 SR6600-X 路由器 可靠性配置指导-R7607
- H3C SR6600 SR6600-X 路由器 可靠性命令参考-R7607
- H3C SR6600 SR6600-X 路由器 二层技术-以太网交换配置指导-R7607

- H3C SR6600 SR6600-X 路由器 二层技术-以太网交换命令参考-R7607