

# 目 录

1 策略路由 .....	1-1
1.1 策略路由简介 .....	1-1
1.1.1 报文的转发流程 .....	1-1
1.1.2 策略路由类型 .....	1-1
1.1.3 策略简介 .....	1-1
1.1.4 策略路由与 Track 联动 .....	1-2
1.1.5 策略路由配置限制和指导 .....	1-2
1.2 策略路由配置任务简介 .....	1-2
1.3 配置策略 .....	1-3
1.3.1 创建策略节点 .....	1-3
1.3.2 配置策略节点的匹配规则 .....	1-3
1.3.3 配置策略节点的动作 .....	1-3
1.4 应用策略 .....	1-5
1.4.1 对本地报文应用策略 .....	1-5
1.4.2 对接口转发的报文应用策略 .....	1-6
1.5 开启策略路由日志信息功能 .....	1-6
1.6 策略路由显示和维护 .....	1-7
1.7 策略路由典型配置举例 .....	1-7
1.7.1 基于报文协议类型的本地策略路由配置举例 .....	1-7
1.7.2 基于报文协议类型的转发策略路由配置举例 .....	1-9
1.7.3 基于报文源地址的转发策略路由配置举例 .....	1-10

# 1 策略路由

## 1.1 策略路由简介

与单纯依照 IP 报文的目的地址查找路由表进行转发不同，策略路由是一种依据用户制定的策略进行路由转发的机制。策略路由可以对于满足一定条件（ACL 规则）的报文，执行指定的操作（设置报文的下一跳、出接口和缺省下一跳等）。

### 1.1.1 报文的转发流程

报文到达后，其后续的转发流程如下：

- 首先根据配置的策略路由转发。
- 若找不到匹配的节点，或虽然找到了匹配的节点但指导报文转发失败时，根据路由表中除缺省路由之外的路由来转发报文。
- 若转发失败，则根据策略路由中配置的缺省下一跳指导报文转发。
- 若转发失败，则再根据缺省路由来转发报文。

### 1.1.2 策略路由类型

根据作用对象的不同，策略路由可分为以下三种类型：

- 本地策略路由：对设备本身产生的报文（比如本地发出的 ping 报文）起作用，指导其发送。
- 转发策略路由：对接口接收的报文起作用，指导其转发。

### 1.1.3 策略简介

策略用来定义报文的匹配规则，以及对报文执行的操作。策略由节点组成。

一个策略可以包含一个或者多个节点。节点的构成如下：

- 每个节点由节点编号来标识。节点编号越小节点的优先级越高，优先级高的节点优先被执行。
- 每个节点的具体内容由 **if-match** 子句和 **apply** 子句来指定。**if-match** 子句定义该节点的匹配规则，**apply** 子句定义该节点的动作。
- 每个节点对报文的处理方式由匹配模式决定。匹配模式分为 **permit**（允许）和 **deny**（拒绝）两种。

应用策略后，系统将根据策略中定义的匹配规则和操作，对报文进行处理：系统按照优先级从高到低的顺序依次匹配各节点，如果报文满足这个节点的匹配规则，就执行该节点的动作；如果报文不满足这个节点的匹配规则，就继续匹配下一个节点；如果报文不能满足策略中任何一个节点的匹配规则，则根据路由表来转发报文。

#### 1. if-match 子句关系

目前，策略路由只提供了一种 **if-match** 子句：**if-match acl**，用于设置 ACL 的匹配规则。在一个节点中只能配置一条 **if-match** 子句。

## 2. apply 子句关系

同一个节点中可以配置多条 **apply** 子句，但配置的多条 **apply** 子句不一定会都会执行。多条 **apply** 子句之间的关系请参见“[1.3.3 配置策略节点的动作](#)”。

## 3. 节点的匹配模式与节点的 if-match 子句、apply 子句的关系

一个节点的匹配模式与这个节点的 **if-match** 子句、**apply** 子句的关系如[表 1-1](#)所示。

表1-1 节点的匹配模式、if-match 子句、apply 子句三者之间的关系

是否满足所有 if-match 子句	节点匹配模式	
	permit（允许模式）	deny（拒绝模式）
是	<ul style="list-style-type: none"><li>如果节点配置了 <b>apply</b> 子句，则执行此节点 <b>apply</b> 子句，不再匹配下一节点</li><li>如果节点未配置 <b>apply</b> 子句，则不会执行任何动作，且不再匹配下一节点，报文将根据路由表来进行转发</li></ul>	不执行此节点 <b>apply</b> 子句，不再匹配下一节点，报文将根据路由表来进行转发
否	不执行此节点 <b>apply</b> 子句，继续匹配下一节点	不执行此节点 <b>apply</b> 子句，继续匹配下一节点



说明

如果一个节点中未配置任何 **if-match** 子句，则认为所有报文都满足该节点的匹配规则，按照“报文满足所有 **if-match** 子句”的情况进行后续处理。

### 1.1.4 策略路由与 Track 联动

策略路由通过与 **Track** 联动，增强了应用的灵活性和对网络环境变化的动态感知能力。

策略路由可以在配置报文的下一跳、出接口、缺省下一跳时与 **Track** 项关联，根据 **Track** 项的状态来动态地决定策略的可用性。策略路由配置仅在关联的 **Track** 项状态为 **Positive** 或 **NotReady** 时生效。关于策略路由与 **Track** 联动的详细介绍和相关配置，请参见“可靠性配置指导”中的“**Track**”。

### 1.1.5 策略路由配置限制和指导

设备收到某些目的为本设备的 **IP** 报文后，如果策略路由匹配该报文，会在报文中先按策略节点动作处理。

## 1.2 策略路由配置任务简介

策略路由配置任务如下：

- (1) [配置策略](#)
  - a. [创建策略节点](#)
  - b. [配置策略节点的匹配规则](#)
  - c. [配置策略节点的动作](#)
- (2) [应用策略](#)

请选择以下至少一项任务进行配置：

- [对本地报文应用策略](#)
- [对接口转发的报文应用策略](#)
- (3) [\(可选\) 开启策略路由日志信息功能](#)

## 1.3 配置策略

### 1.3.1 创建策略节点

- (1) 进入系统视图。

```
system-view
```

- (2) 创建策略节点，并进入策略节点视图。

```
policy-based-route policy-name [ deny | permit ] node node-number
```

### 1.3.2 配置策略节点的匹配规则

#### 1. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入策略节点视图。

```
policy-based-route policy-name [ deny | permit ] node node-number
```

- (3) 设置 ACL 匹配规则。

```
if-match acl { acl-number | name acl-name }
```

缺省情况下，未设置 ACL 匹配规则。

策略路由不支持匹配二层信息的 ACL 匹配规则。

### 1.3.3 配置策略节点的动作

#### 1. 功能简介

影响报文转发路径的 **apply** 子句有四条，优先级从高到低依次为：

- (1) **apply access-vpn vpn-instance**
- (2) **apply next-hop**
- (3) **apply output-interface**
- (4) **apply default-next-hop**

**apply** 子句的含义、执行优先情况和详细说明如[表 1-2](#)所示。

表1-2 **apply** 子句的含义以及执行优先情况等说明

子句	含义	执行优先情况/详细说明
<b>apply precedence</b>	设置IP报文的IP优先级	只要配置了该子句，该子句就一定会执行

子句	含义	执行优先情况/详细说明
<b>apply access-vpn vpn-instance</b>	设置报文在指定VPN实例中进行转发	报文如果匹配了其中一个VPN实例下的转发表，报文将在该VPN实例中进行转发 SPC类单板、CSPC类单板（CSPC-GE16XP4L-E、CSPC-GE24L-E和CSPC-GP24GE8XP2L-E单板除外）和CMPE-1104单板不支持本命令。
<b>apply next-hop</b> 和 <b>apply output-interface</b>	设置报文的下一跳、出接口	当两条子句同时配置并且都有效时，系统只会执行 <b>apply next-hop</b> 子句 SPC类单板、CSPC类单板（CSPC-GE16XP4L-E、CSPC-GE24L-E和CSPC-GP24GE8XP2L-E单板除外）和CMPE-1104单板不支持 <b>apply output-interface</b> 本命令。
<b>apply default-next-hop</b>	设置报文的缺省下一跳	执行缺省下一跳的前提是：在策略中未配置下一跳，或者配置的下一跳无效，并且在路由表中未找到与报文目的IP地址匹配的路由表项 SPC类单板、CSPC类单板（CSPC-GE16XP4L-E、CSPC-GE24L-E和CSPC-GP24GE8XP2L-E单板除外）和CMPE-1104单板不支持本命令。



#### 说明

策略路由通过查询 FIB 表是否存在下一跳或缺省下一跳地址对应的条目，判断设置报文转发下一跳或缺省下一跳地址是否可用。策略路由周期性检查 FIB 表，如果在此周期内设备到下一跳的路径发生变化，策略路由无法及时刷新导致通信发生短暂中断。

## 2. 配置限制和指导

在设置报文转发的下一跳时，对于配置接口出方向策略路由，仅支持直连下一跳，且仅支持一个下一跳。

## 3. 配置修改报文字段类动作

- (1) 进入系统视图。

```
system-view
```

- (2) 进入策略节点视图。

```
policy-based-route policy-name [ deny | permit ] node node-number
```

- (3) 设置 IP 报文的 IP 优先级。

```
apply precedence { type | value }
```

缺省情况下，未设置 IP 报文的优先级。

## 4. 配置指导报文转发类动作

- (1) 进入系统视图。

```
system-view
```

- (2) 进入策略节点视图。

```
policy-based-route policy-name [ deny | permit ] node node-number
```

(3) 配置动作。

- 设置报文在指定 VPN 实例中进行转发。

```
apply access-vpn vpn-instance vpn-instance-name
```

SPC 类单板、CSPC 类单板（CSPC-GE16XP4L-E、CSPC-GE24L-E 和 CSPC-GP24GE8XP2L-E 单板除外）和 CMPE-1104 单板不支持本命令。

缺省情况下，未设置报文在指定 VPN 实例中进行转发。

- 设置报文转发的下一跳。

```
apply next-hop [ vpn-instance vpn-instance-name ] { ip-address [ direct ] [ track track-entry-number ] }&<1-2>
```

缺省情况下，未设置报文转发的下一跳。

用户通过一次或多次配置本命令可以同时配置多个下一跳，这些下一跳起到主备的作用。

- 设置指导报文转发的出接口。

```
apply output-interface { interface-type interface-number [ track track-entry-number ] }
```

SPC 类单板、CSPC 类单板（CSPC-GE16XP4L-E、CSPC-GE24L-E 和 CSPC-GP24GE8XP2L-E 单板除外）和 CMPE-1104 单板不支持本命令。

缺省情况下，未设置指导报文转发的出接口。

- 设置指导报文转发的缺省下一跳。

```
apply default-next-hop [ vpn-instance vpn-instance-name ] { ip-address [ direct ] [ track track-entry-number ] }&<1-2>
```

SPC 类单板、CSPC 类单板（CSPC-GE16XP4L-E、CSPC-GE24L-E 和 CSPC-GP24GE8XP2L-E 单板除外）和 CMPE-1104 单板不支持本命令。

缺省情况下，未设置指导报文转发的缺省下一跳。

用户通过一次或多次配置本命令可以同时配置多个缺省下一跳，这些缺省下一跳起到主备的作用。

## 1.4 应用策略

### 1.4.1 对本地报文应用策略

#### 1. 功能简介

通过本配置，可以将已经配置的策略应用到本地，指导设备本身产生报文的发送。应用策略时，该策略必须已经存在，否则配置将失败。

#### 2. 配置限制和指导

- 对本地报文只能应用一个策略。应用新的策略前必须删除本地原来已经应用的策略。
- 若无特殊需求，建议用户不要对本地报文应用策略。否则，有可能会对本地报文的发送造成不必要的影响（如 ping、telnet 服务的失效）。

#### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

(2) 对本地报文应用策略。

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

缺省情况下，未对本地报文应用策略。

## 1.4.2 对接口转发的报文应用策略

### 1. 功能简介

通过本配置，可以将已经配置的策略应用到接口，指导接口接收的所有报文的转发。应用策略时，该策略必须已经存在，否则配置将失败。

### 2. 配置限制和指导

- 对接口转发的报文应用策略时，一个接口只能应用一个策略。应用新的策略前必须删除接口上原来已经应用的策略。
- 一个策略可以同时被多个接口应用。
- 在 VLAN 接口上应用策略指导接口接收的所有报文的转发时，仅对普通 VLAN 的流量生效，对 Super VLAN 的流量不生效。有关 VLAN 的详细介绍和具体配置过程，请参见“二层技术-以太网交换配置指导”中的“VLAN 配置”。

### 3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入接口视图。

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

(3) 对接口转发的报文应用策略。

```
ip policy-based-route policy-name [ share-mode ]
```

缺省情况下，未对接口转发的报文应用策略。

## 1.5 开启策略路由日志信息功能

### 1. 功能简介

策略路由日志是为了满足管理员审计需求。设备生成策略路由日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

### 2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 开启策略路由日志信息功能。

```
ip policy-based-route-log enable
```

缺省情况下，策略路由日志信息功能处于关闭状态。

## 1.6 策略路由显示和维护

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

在用户视图下执行 **reset** 命令可以清除策略路由的统计信息。

表1-3 策略路由显示和维护

操作	命令
显示已经配置的策略	<code>display ip policy-based-route [ policy policy-name ]</code>
显示已经应用的策略路由信息	<code>display ip policy-based-route setup</code>
显示本地策略路由的配置信息和统计信息（独立运行模式）	<code>display ip policy-based-route local [ slot slot-number ]</code>
显示本地策略路由的配置信息和统计信息（IRF模式）	<code>display ip policy-based-route local [ chassis chassis-number slot slot-number ]</code>
显示接口下转发策略路由的配置信息和统计信息（独立运行模式）	<code>display ip policy-based-route interface interface-type interface-number [ slot slot-number ]</code>
显示接口下转发策略路由的配置信息和统计信息（IRF模式）	<code>display ip policy-based-route interface interface-type interface-number [ chassis chassis-number slot slot-number ]</code>
清除策略路由的统计信息	<code>reset ip policy-based-route statistics [ policy policy-name ]</code>

## 1.7 策略路由典型配置举例

### 1.7.1 基于报文协议类型的本地策略路由配置举例

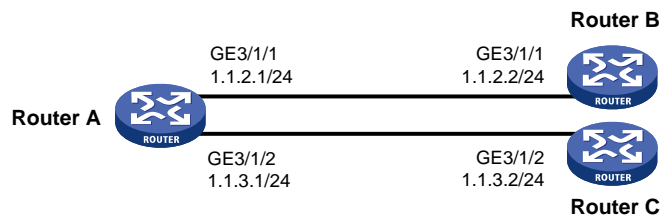
#### 1. 组网需求

Router A 分别与 Router B 和 Router C 直连（保证 Router B 和 Router C 之间路由完全不可达）。通过策略路由控制 Router A 产生的报文：

- 指定所有 TCP 报文的下一跳为 1.1.2.2；
- 其它报文仍然按照查找路由表的方式进行转发。

#### 2. 组网图

图1-1 基于报文协议类型的本地策略路由的配置举例组网图





### 3. 配置步骤

#### (1) 配置 Router A

# 配置 GigabitEthernet 接口的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 3/1/1
[RouterA-GigabitEthernet3/1/1] ip address 1.1.2.1 24
[RouterA-GigabitEthernet3/1/1] quit
[RouterA] interface gigabitethernet 3/1/2
[RouterA-GigabitEthernet3/1/2] ip address 1.1.3.1 24
[RouterA-GigabitEthernet3/1/2] quit
```

# 定义访问控制列表 ACL 3101，用来匹配 TCP 报文。

```
[RouterA] acl advanced 3101
[RouterA-acl-ipv4-adv-3101] rule permit tcp
[RouterA-acl-ipv4-adv-3101] quit
```

# 定义 5 号节点，指定所有 TCP 报文的下一跳为 1.1.2.2。

```
[RouterA] policy-based-route aaa permit node 5
[RouterA-pbr-aaa-5] if-match acl 3101
[RouterA-pbr-aaa-5] apply next-hop 1.1.2.2
[RouterA-pbr-aaa-5] quit
```

# 在 Router A 上应用本地策略路由。

```
[RouterA] ip local policy-based-route aaa
```

#### (2) 配置 Router B

# 配置 GigabitEthernet 接口的 IP 地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 3/1/1
[RouterB-GigabitEthernet3/1/1] ip address 1.1.2.2 24
```

#### (3) 配置 Router C

# 配置 GigabitEthernet 接口的 IP 地址。

```
<RouterC> system-view
[RouterC] interface gigabitethernet 3/1/2
[RouterC-GigabitEthernet3/1/2] ip address 1.1.3.2 24
```

### 4. 验证配置

从 Router A 上通过 Telnet 方式登录 Router B (1.1.2.2/24)，结果成功。

从 Router A 上通过 Telnet 方式登录 Router C (1.1.3.2/24)，结果失败。

从 Router A 上 ping Router C (1.1.3.2/24)，结果成功。

由于 Telnet 使用的是 TCP 协议，ping 使用的是 ICMP 协议，所以由以上结果可证明：Router A 产生的 TCP 报文的下一跳为 1.1.2.2，接口 GigabitEthernet3/1/2 不发送 TCP 报文，但可以发送非 TCP 报文，策略路由设置成功。

## 1.7.2 基于报文协议类型的转发策略路由配置举例

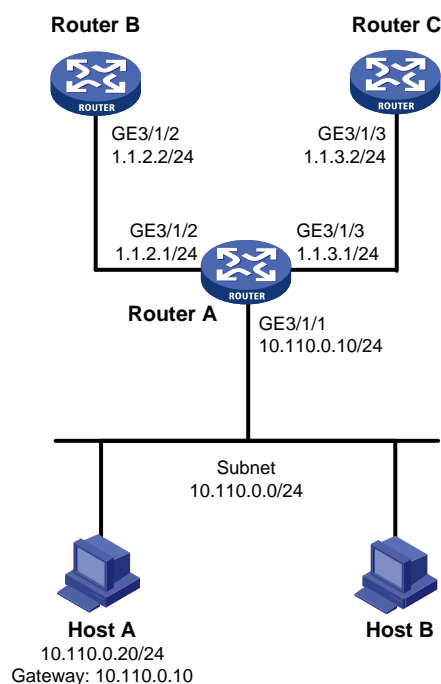
### 1. 组网需求

Router A 分别与 Router B 和 Router C 直连（保证 Router B 和 Router C 之间路由完全不可达）。通过策略路由控制从 Router A 的以太网接口 GigabitEthernet3/1/1 接收的报文：

- 指定所有 TCP 报文的下一跳为 1.1.2.2；
- 其它报文仍然按照查找路由表的方式进行转发。

### 2. 组网图

图1-2 基于报文协议类型的转发策略路由的配置举例组网图



### 3. 配置步骤

配置前请确保 Router B 和 Host A，Router C 和 Host A 之间路由可达。

#### (1) 配置 Router A

# 配置接口 GigabitEthernet3/1/2 和 GigabitEthernet3/1/3 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 3/1/2
[RouterA-GigabitEthernet3/1/2] ip address 1.1.2.1 24
[RouterA-GigabitEthernet3/1/2] quit
[RouterA] interface gigabitethernet 3/1/3
[RouterA-GigabitEthernet3/1/3] ip address 1.1.3.1 24
[RouterA-GigabitEthernet3/1/3] quit
```

# 定义访问控制列表 ACL 3101，用来匹配 TCP 报文。

```
[RouterA] acl advanced 3101
[RouterA-acl-ipv4-adv-3101] rule permit tcp
[RouterA-acl-ipv4-adv-3101] quit
```

```
# 定义 5 号节点，指定所有 TCP 报文的下一跳为 1.1.2.2。
[RouterA] policy-based-route aaa permit node 5
[RouterA-pbr-aaa-5] if-match acl 3101
[RouterA-pbr-aaa-5] apply next-hop 1.1.2.2
[RouterA-pbr-aaa-5] quit
# 在以太网接口 GigabitEthernet3/1/1 上应用转发策略路由，处理此接口接收的报文。
[RouterA] interface gigabitethernet 3/1/1
[RouterA-GigabitEthernet3/1/1] ip address 10.110.0.10 24
[RouterA-GigabitEthernet3/1/1] ip policy-based-route aaa
[RouterA-GigabitEthernet3/1/1] quit
```

#### 4. 验证配置

从 Host A 上通过 Telnet 方式登录 Router B，结果成功。

从 Host A 上通过 Telnet 方式登录 Router C，结果失败。

从 Host A 上 ping Router C，结果成功。

由于 Telnet 使用的是 TCP 协议，ping 使用的是 ICMP 协议，所以由以上结果可证明：从 Router A 的以太网接口 GigabitEthernet3/1/1 接收的 TCP 报文的下一跳为 1.1.2.2，接口 GigabitEthernet3/1/3 不转发 TCP 报文，但可以转发非 TCP 报文，策略路由设置成功。

### 1.7.3 基于报文源地址的转发策略路由配置举例

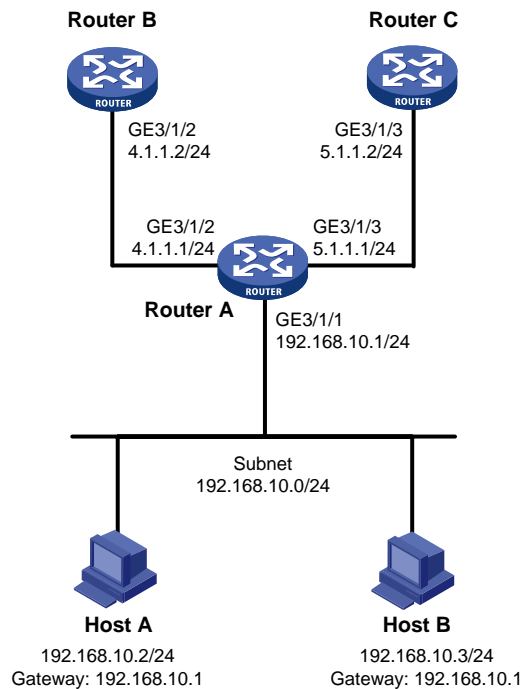
#### 1. 组网需求

Router A 分别与 Router B 和 Router C 直连（保证 Router B 和 Router C 之间路由完全不可达）。通过策略路由控制从 Router A 的以太网接口 GigabitEthernet3/1/1 接收的报文：

- 源地址为 192.168.10.2 的报文以 4.1.1.2/24 作为下一跳 IP 地址；
- 其它源地址的报文以 5.1.1.2/24 作为下一跳 IP 地址。

## 2. 组网图

图1-3 基于报文源地址的转发策略路由的配置举例组网图



## 3. 配置步骤

配置前请确保 Router B 和 Host A/Host B， Router C 和 Host A/Host B 之间路由可达。

### (1) 配置 Router A

# 配置接口 GigabitEthernet3/1/2 和 GigabitEthernet3/1/3 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 3/1/2
[RouterA-GigabitEthernet3/1/2] ip address 4.1.1.1 24
[RouterA-GigabitEthernet3/1/2] quit
[RouterA] interface gigabitethernet 3/1/3
[RouterA-GigabitEthernet3/1/3] ip address 5.1.1.1 24
[RouterA-GigabitEthernet3/1/3] quit
```

# 定义访问控制列表 ACL 2000，用来匹配源地址为 192.168.10.2 的报文。

```
[RouterA] acl basic 2000
[RouterA-acl-ipv4-basic-2000] rule 10 permit source 192.168.10.2 0
[RouterA-acl-ipv4-basic-2000] quit
```

# 定义 0 号节点，指定所有源地址为 192.168.10.2 的报文的下一跳为 4.1.1.2。

```
[RouterA] policy-based-route aaa permit node 0
[RouterA-pbr-aaa-0] if-match acl 2000
[RouterA-pbr-aaa-0] apply next-hop 4.1.1.2
[RouterA-pbr-aaa-0] quit
[RouterA] policy-based-route aaa permit node 1
[RouterA-pbr-aaa-1] apply next-hop 5.1.1.2
[RouterA-pbr-aaa-1] quit
```

# 在以太网接口 **GigabitEthernet3/1/1** 上应用转发策略路由，处理此接口接收的报文。

```
[RouterA] interface gigabitethernet 3/1/1
[RouterA-GigabitEthernet3/1/1] ip address 192.168.10.1 24
[RouterA-GigabitEthernet3/1/1] ip policy-based-route aaa
[RouterA-GigabitEthernet3/1/1] quit
```

#### 4. 验证配置

从 Host A 上 ping Router B，结果成功。

从 Host B 上 ping Router B，结果失败。

从 Host A 上 ping Router C，结果失败。

从 Host B 上 ping Router C，结果成功。

以上结果可证明：从 Router A 的以太网接口 **GigabitEthernet3/1/1** 接收的源地址为 **192.168.10.2** 的报文的下一跳为 **4.1.1.2**，所以 Host A 能 ping 通 Router B，源地址为 **192.168.10.3** 的下一跳 **5.1.1.2**，所以 Host B 能 ping 通 Router C，由此表明策略路由设置成功。