

目 录

1 策略路由	1-1
1.1 策略路由简介	1-1
1.1.1 策略简介	1-1
1.1.2 策略路由与Track联动	1-3
1.2 策略路由配置任务简介	1-3
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	1-4
1.3.3 配置策略节点的动作	1-4
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 策略路由显示和维护	1-6
1.6 策略路由典型配置举例	1-7
1.6.1 基于报文协议类型的本地策略路由配置举例	1-7
1.6.2 基于报文协议类型的转发策略路由配置举例	1-8
1.6.3 基于报文长度的转发策略路由配置举例	1-10
1.6.4 基于反向入接口的转发策略路由配置举例	1-13
1.6.5 SR6600/SR6600-X工作在网关模式时VLAN接口策略路由配置举例	1-14

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。策略路由可以基于报文的源地址、长度等信息灵活地控制报文的发送：对于满足一定条件（报文长度、ACL 规则等）的报文，将执行指定的操作（设置报文的出接口和下一跳、设置报文的缺省出接口和下一跳等）。

报文到达后，系统首先根据策略路由转发，若没有配置策略路由或配置了策略路由但找不到匹配的表项时，再根据路由表来转发报文。

根据作用对象的不同，策略路由可分为本地策略路由和转发策略路由：

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

1.1.1 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

策略路由提供了三种 **if-match** 子句，作用如下：

- **if-match acl**：设置 ACL 匹配规则。
- **if-match packet-length**：设置 IP 报文长度匹配规则。
- **if-match reverse-input-interface**：设置反向入接口匹配规则。如果进入接口的响应报文所对应的请求报文的入接口与用户配置的接口一致，则认为报文满足该 **if-match** 子句。

在一个节点中可以配置多条 **if-match** 子句，同一类型的 **if-match** 子句最多只能有一条。同一个节点中的各 **if-match** 子句之间是“与”的关系，即报文必须满足该节点的所有 **if-match** 子句才算满足这个节点的匹配规则。

2. apply子句

策略路由提供了九种**apply**子句，同一个节点中可以配置多条**apply**子句，但配置的多条**apply**子句不一定会执行。**apply**子句的含义以及执行优先情况等说明如 [表 1-1](#) 所示。

表1-1 **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
apply ip-df zero	将IP报文头中的DF（Don't Fragment，不分片）标志置为0，表示允许对该报文进行分片	只要配置了该子句，该子句就一定会执行
apply access-vpn vpn-instance	设置报文在指定VPN实例中进行转发	只要配置了该子句，就不会执行除 apply ip-df zero 之外的其他 apply 子句 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，如果对于所有配置的VPN实例，报文都未能匹配其下的转发表，该报文将被丢弃
apply ip-precedence	设置IP报文优先级	在未配置 apply access-vpn vpn-instance 的情况下，只要配置了该子句，该子句就一定会执行
apply output-interface 和 apply ip-address next-hop	设置报文的出接口、下一跳	apply ip-address next-hop 命令的优先级高于 apply output-interface 。当两条命令同时配置并且都有效时，系统只会执行 apply ip-address next-hop 命令
apply default output-interface 和 apply ip-address default next-hop	设置报文的缺省出接口、缺省下一跳	apply ip-address default next-hop 命令的优先级高于 apply default output-interface 。当两条命令同时配置并且都有效时，系统只会执行 apply ip-address default next-hop 命令。 执行缺省出接口和下一跳的前提是，在策略中没有配置出接口或者下一跳，或者配置的出接口和下一跳无效，并且在路由表中没有找到与报文目的IP地址匹配的非缺省路由表项
apply fail-action continue	设置当前节点处理失败后继续进行下一节点的处理	如果当前节点中没有配置报文的出接口、下一跳、缺省出接口、缺省下一跳这四个子句，或者配置了这四个子句中的一个或多个，但配置的子句都失效（出接口down或者下一跳不可达）时，会进行下一节点的处理

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 1-2](#) 所示。

表1-2 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	执行此节点 apply 子句	不执行此节点 apply 子句，不再匹配下一节点，报文将根据路由表来进行转发
否	不执行此节点 apply 子句，继续匹配下一节点	不执行此节点 apply 子句，继续匹配下一节点



说明

- 如果一个节点中没有配置任何 **if-match** 子句，则认为所有报文都满足该节点的匹配规则。
- 如果一个 **permit** 模式的节点没有配置 **apply** 子句，当报文满足此节点的所有 **if-match** 子句时，将不会执行任何动作，且不再继续匹配下一节点，报文将根据路由表来进行转发。
- 如果一个节点没有配置任何 **if-match** 子句和 **apply** 子句，则所有报文都满足该节点的匹配规则，但不会执行任何动作，且不再继续匹配下一节点，报文将根据路由表来进行转发。

1.1.2 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出接口、缺省出接口、下一跳、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 **Invalid** 时生效。



说明

关于策略路由与 **Track** 联动的详细介绍和相关配置请参见“可靠性配置指导”中的“**Track**”。

1.2 策略路由配置任务简介

表1-3 策略路由配置任务简介

配置任务		说明	详细配置
配置策略	创建策略节点	必选	1.3.1
	配置策略节点的匹配规则		1.3.2
	配置策略节点的动作		1.3.3
应用策略	对本地报文应用策略	必选	1.4.1
	对接口转发的报文应用策略	用户可根据实际情况进行选择	1.4.2

1.3 配置策略

1.3.1 创建策略节点

表1-4 创建策略节点

操作	命令	说明
进入系统视图	system-view	-
创建策略节点，并进入策略节点视图	policy-based-route <i>policy-name</i> [deny permit] node <i>node-number</i>	必选

1.3.2 配置策略节点的匹配规则

表1-5 配置策略节点的匹配规则

操作	命令	说明
进入系统视图	system-view	-
进入策略节点视图	policy-based-route <i>policy-name</i> [deny permit] node <i>node-number</i>	-
设置ACL匹配规则	if-match acl <i>acl-number</i>	可选
设置IP报文长度匹配规则	if-match packet-length <i>min-len max-len</i>	可选
设置反向入接口匹配规则	if-match reverse-input-interface <i>interface-type interface-number</i>	可选



说明

- **if-match** 子句中使用 ACL 时，如果 ACL 规则的动作作为 **permit**，则该子句可以用来匹配报文；如果使用的 ACL 不存在或者 ACL 规则的动作作为 **deny**，则所有报文都不能满足该子句。
- **if-match reverse-input-interface** 子句是根据会话查找响应报文所对应的请求报文的入接口的，如果系统没有配置相关业务，不能生成会话，则所有报文都不能满足该子句。

1.3.3 配置策略节点的动作

表1-6 配置策略节点的动作

操作	命令	说明
进入系统视图	system-view	-
进入策略节点视图	policy-based-route <i>policy-name</i> [deny permit] node <i>node-number</i>	-
将IP报文头中的DF标志置为0，表示允许对该报文进行分片	apply ip-df zero	可选
设置报文在指定VPN实例进行转发	apply access-vpn <i>vpn-instance vpn-instance-name</i> <1-6>	可选
设置报文的优先级	apply ip-precedence <i>value</i>	可选
设置报文的出接口	apply output-interface <i>interface-type interface-number</i> [track <i>track-entry-number</i>] [<i>interface-type interface-number</i> [track <i>track-entry-number</i>]]	可选 用户可以同时配置两个出接口，这两个出接口同时有效，可以起到负载均衡的作用 对于非P2P接口（广播类型的接口和NBMA类型的接口），比如以太网接口，由于有多个可能的下一跳，可能会造成报文转发不成功的现象

操作	命令	说明
设置报文的下一跳IP地址	apply ip-address next-hop <i>ip-address</i> [direct] [track <i>track-entry-number</i>] [<i>ip-address</i> [direct] [track <i>track-entry-number</i>]]	可选 用户可以同时配置两个下一跳，这两个下一跳同时有效，可以起到负载均衡的作用
设置两个下一跳地址通过主备方式转发报文	apply ip-address next-hop standby	可选 缺省情况下两个下一跳同时有效，可以起到负载均衡的作用
设置报文缺省出接口	apply default output-interface <i>interface-type interface-number</i> [track <i>track-entry-number</i>] [<i>interface-type interface-number</i> [track <i>track-entry-number</i>]]	可选 用户可以同时配置两个缺省出接口，这两个出接口同时有效，可以起到负载均衡的作用
设置报文缺省下一跳	apply ip-address default next-hop <i>ip-address</i> [direct] [track <i>track-entry-number</i>] [<i>ip-address</i> [direct] [track <i>track-entry-number</i>]]	可选 用户可以同时配置两个缺省下一跳，这两个下一跳同时有效，可以起到负载均衡的作用
设置两个缺省下一跳地址通过主备方式转发报文	apply ip-address default next-hop standby	可选 缺省情况下两个缺省下一跳同时有效，可以起到负载均衡的作用
设置当前节点处理失败后继续进行下一节点的处理	apply fail-action continue	可选 本命令仅在策略节点的匹配模式为 permit 时生效

1.4 应用策略

1.4.1 对本地报文应用策略

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。

对本地报文只能应用一个策略。多次配置命令，生效的是最新的配置。

若无特殊需求，建议用户不要对本地报文应用策略。

表1-7 对本地报文应用策略

操作	命令	说明
进入系统视图	system-view	-
对本地报文应用策略	ip local policy-based-route <i>policy-name</i>	必选 缺省情况下，对本地报文没有应用策略



说明

如果配置时策略不存在，命令可以配置成功但不生效，当策略创建后，该配置才真正生效。

1.4.2 对接口转发的报文应用策略

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。

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。多次配置命令，生效的是最新的配置。一个策略可以同时被多个接口应用。。

表1-8 配置接口策略路由

操作	命令	说明
进入系统视图	system-view	-
进入接口视图	interface <i>interface-type</i> <i>interface-number</i>	-
对接口转发的报文应用策略	ip policy-based-route <i>policy-name</i>	必选 缺省情况下，对接口转发的报文没有应用策略



说明

- 如果配置时策略不存在，命令可以配置成功但不生效，当策略创建后，该配置才真正生效。
- SR6600/SR6600-X 工作在网关模式，并且配置了 SAP 板时，当在 VLAN 接口上应用策略路由时，需要使用 **redirect** 命令在相应的 VLAN 下配置流量重定向动作。流量重定向的配置请参见“ACL 和 QoS 配置指导”中的“流量重定向配置”。

1.5 策略路由显示和维护

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

在用户视图下，用户可以执行 **reset** 命令清除策略路由的统计信息。

表1-9 策略路由显示和维护

操作	命令
显示已经配置的策略	display policy-based-route [<i>policy-name</i>] [[{ begin exclude include } <i>regular-expression</i>]]
显示本地策略路由和转发策略路由的应用情况	display ip policy-based-route [[{ begin exclude include } <i>regular-expression</i>]]
显示已经应用的策略路由的设置情况（非IRF模式）	display ip policy-based-route setup { <i>policy-name</i> interface <i>interface-type</i> <i>interface-number</i> [slot <i>slot-number</i>] local [slot <i>slot-number</i>] } [[{ begin exclude include } <i>regular-expression</i>]]
显示已经应用的策略路由的设置情况（IRF模式）	display ip policy-based-route setup { <i>policy-name</i> interface <i>interface-type</i> <i>interface-number</i> [chassis <i>chassis-number</i> slot <i>slot-number</i>] local [chassis <i>chassis-number</i> slot <i>slot-number</i>] } [[{ begin exclude include } <i>regular-expression</i>]]

操作	命令
显示策略路由的统计信息（非IRF模式）	display ip policy-based-route statistics { interface <i>interface-type interface-number</i> local } [slot <i>slot-number</i>] [[{ begin exclude include } <i>regular-expression</i>]
显示策略路由的统计信息（IRF模式）	display ip policy-based-route statistics { interface <i>interface-type interface-number</i> local } [chassis <i>chassis-number</i> slot <i>slot-number</i>] [[{ begin exclude include } <i>regular-expression</i>]
清除策略路由的统计信息	reset policy-based-route statistics [<i>policy-name</i>]

1.6 策略路由典型配置举例

1.6.1 基于报文协议类型的本地策略路由配置举例

1. 组网需求

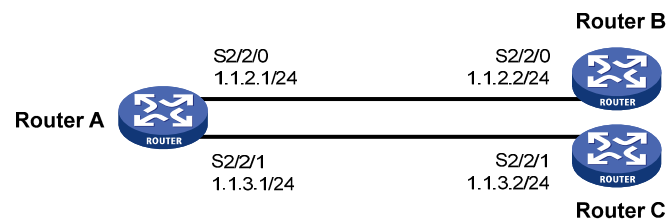
通过策略路由控制 Router A 产生的报文：

- 所有 TCP 报文均通过串口 Serial2/2/0 发送；
- 其它报文仍然按照查找路由表的方式进行转发。

其中，Router A 分别与 Router B 和 Router C 直连。

2. 组网图

图1-1 基于报文协议类型的策略路由的配置举例组网图



3. 配置步骤

(1) 配置 Router A

定义访问控制列表 ACL 3101，用来匹配 TCP 报文。

```

<RouterA> system-view
[RouterA] acl number 3101
[RouterA-acl-adv-3101] rule permit tcp
[RouterA-acl-adv-3101] quit
  
```

定义 5 号节点，使 TCP 报文被发往串口 Serial2/2/0。

```

[RouterA] policy-based-route aaa permit node 5
[RouterA-pbr-aaa-5] if-match acl 3101
[RouterA-pbr-aaa-5] apply output-interface serial 2/2/0
[RouterA-pbr-aaa-5] quit
  
```

在 Router A 上应用本地策略路由。


```
[RouterA] ip local policy-based-route aaa
# 配置 Serial 接口的 IP 地址。
[RouterA] interface serial 2/2/0
[RouterA-Serial2/2/0] ip address 1.1.2.1 255.255.255.0
[RouterA-Serial2/2/0] quit
[RouterA] interface serial 2/2/1
[RouterA-Serial2/2/1] ip address 1.1.3.1 255.255.255.0
```

(2) 配置 Router B

配置 Serial 接口的 IP 地址。

```
<RouterB> system-view
[RouterB] interface serial 2/2/0
[RouterB-Serial2/2/0] ip address 1.1.2.2 255.255.255.0
[RouterB-Serial2/2/0] quit
```

(3) 配置 Router C

配置 Serial 接口的 IP 地址。

```
<RouterC> system-view
[RouterC] interface serial 2/2/1
[RouterC-Serial2/2/1] ip address 1.1.3.2 255.255.255.0
[RouterC-Serial2/2/1] quit
```

(4) 验证配置结果

从 Router A 上 Telnet Router B (1.1.2.2/24)，结果成功。

从 Router A 上 Telnet 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 报文均从串口 Serial2/2/0 发送，串口 Serial2/2/1 不发送 TCP 报文，但可以发送非 TCP 报文，策略路由设置成功。

1.6.2 基于报文协议类型的转发策略路由配置举例

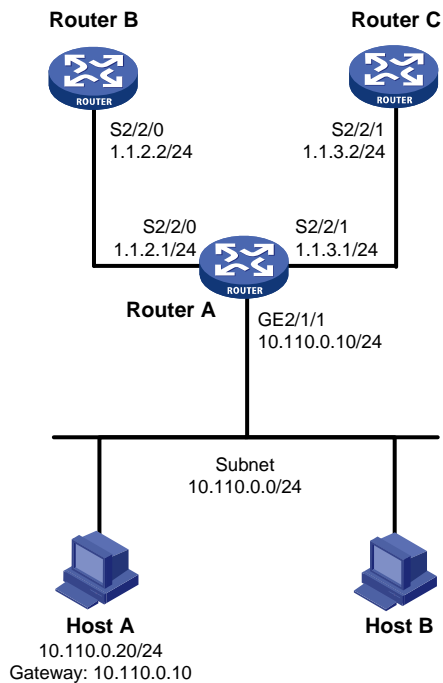
1. 组网需求

通过策略路由控制从 Router A 的以太网接口 GigabitEthernet2/1/1 接收的报文：

- 所有 TCP 报文均通过串口 Serial2/2/0 发送；
- 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

(1) 配置 Router A

定义访问控制列表 ACL 3101，用来匹配 TCP 报文。

```
<RouterA> system-view
[RouterA] acl number 3101
[RouterA-acl-adv-3101] rule permit tcp
[RouterA-acl-adv-3101] quit
```

定义 5 号节点，使 TCP 报文被发往串口 Serial2/2/0。

```
[RouterA] policy-based-route aaa permit node 5
[RouterA-pbr-aaa-5] if-match acl 3101
[RouterA-pbr-aaa-5] apply output-interface serial 2/2/0
[RouterA-pbr-aaa-5] quit
```

在以太网接口 GigabitEthernet2/1/1 上应用转发策略路由，处理此接口接收的报文。

```
[RouterA] interface GigabitEthernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 10.110.0.10 255.255.255.0
[RouterA-GigabitEthernet2/1/1] ip policy-based-route aaa
[RouterA-GigabitEthernet2/1/1] quit
```

配置 Serial 接口的 IP 地址。

```
[RouterA] interface serial 2/2/0
[RouterA-Serial2/2/0] ip address 1.1.2.1 255.255.255.0
[RouterA-Serial2/2/0] quit
[RouterA] interface serial 2/2/1
[RouterA-Serial2/2/1] ip address 1.1.3.1 255.255.255.0
```

(2) 配置 Router B

配置到网段 10.110.0.0/24 的静态路由。

```
<RouterB> system-view
[RouterB] ip route-static 10.110.0.0 24 1.1.2.1
```

配置 Serial 接口的 IP 地址。

```
[RouterB] interface serial 2/2/0
[RouterB-Serial2/2/0] ip address 1.1.2.2 255.255.255.0
```

(3) 配置 Router C

配置到网段 10.110.0.0/24 的静态路由。

```
<RouterC> system-view
[RouterC] ip route-static 10.110.0.0 24 1.1.3.1
```

配置 Serial 接口的 IP 地址。

```
[RouterC] interface serial 2/2/1
[RouterC-Serial2/2/1] ip address 1.1.3.2 255.255.255.0
```

(4) 验证配置结果

将 Host A 的 IP 地址配置为 10.110.0.20/24，网关地址配置为 10.110.0.10。

从 Host A 上 Telnet Router B，结果成功。

从 Host A 上 Telnet 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 GigabitEthernet2/1/1 接收的 TCP 报文均从串口 Serial2/2/0 转发，串口 Serial2/2/1 不转发 TCP 报文，但可以转发非 TCP 报文，策略路由设置成功。

1.6.3 基于报文长度的转发策略路由配置举例

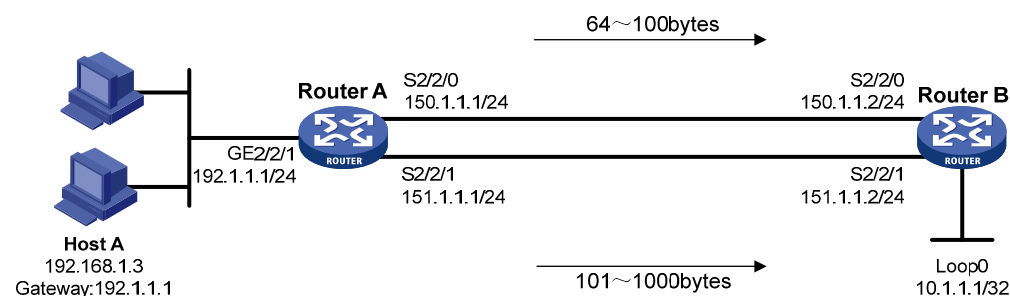
1. 组网需求

通过策略路由控制从 Router A 的以太网接口 GigabitEthernet2/1/1 接收的报文：

- 长度为 64~100 字节的报文以 150.1.1.2/24 作为下一跳 IP 地址；
- 长度为 101~1000 字节的报文以 151.1.1.2/24 作为下一跳 IP 地址；
- 所有其它长度的报文都按照查找路由表的方式转发。

2. 组网图

图1-3 基于报文长度的转发策略路由的配置举例组网图



3. 配置步骤

(1) 配置 Router A

配置动态路由协议 RIP。

```
<RouterA> system-view
[RouterA] rip
[RouterA-rip-1] network 192.1.1.0
[RouterA-rip-1] network 150.1.0.0
[RouterA-rip-1] network 151.1.0.0
[RouterA-rip-1] quit
```

配置策略 lab1，将长度为 64~100 字节的报文转发到下一跳 150.1.1.2，而将长度为 101~1000 字节的报文转发到下一跳 151.1.1.2。

```
[RouterA] policy-based-route lab1 permit node 10
[RouterA-pbr-lab1-10] if-match packet-length 64 100
[RouterA-pbr-lab1-10] apply ip-address next-hop 150.1.1.2
[RouterA-pbr-lab1-10] quit
[RouterA] policy-based-route lab1 permit node 20
[RouterA-pbr-lab1-20] if-match packet-length 101 1000
[RouterA-pbr-lab1-20] apply ip-address next-hop 151.1.1.2
[RouterA-pbr-lab1-20] quit
```

在以太网接口 GigabitEthernet2/1/1 上应用定义的策略 lab1，处理此接口接收的报文。

```
[RouterA] interface GigabitEthernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 192.1.1.1 255.255.255.0
[RouterA-GigabitEthernet2/1/1] ip policy-based-route lab1
[RouterA-GigabitEthernet2/1/1] quit
```

配置 Serial 接口的 IP 地址。

```
[RouterA] interface serial 2/2/0
[RouterA-Serial2/2/0] ip address 150.1.1.1 255.255.255.0
[RouterA-Serial2/2/0] quit
[RouterA] interface serial 2/2/1
[RouterA-Serial2/2/1] ip address 151.1.1.1 255.255.255.0
[RouterA-Serial2/2/1] return
```

(2) 配置 Router B

配置动态路由协议 RIP。

```
<RouterB> system-view
[RouterB] rip
[RouterB-rip-1] network 10.0.0.0
[RouterB-rip-1] network 150.1.0.0
[RouterB-rip-1] network 151.1.0.0
```

配置 Serial 接口的 IP 地址。

```
[RouterB] interface serial 2/2/0
[RouterB-Serial2/2/0] ip address 150.1.1.2 255.255.255.0
[RouterB-Serial2/2/0] quit
[RouterB] interface serial 2/2/1
[RouterB-Serial2/2/1] ip address 151.1.1.2 255.255.255.0
[RouterB-Serial2/2/1] quit
```

配置 Loopback 接口的 IP 地址。

```
[RouterB] interface loopback 0  
[RouterB-LoopBack0] ip address 10.1.1.1 32
```

(3) 验证配置结果

在 Router A 上用 **debugging ip policy-based-route** 命令监视策略路由。

```
<RouterA> debugging ip policy-based-route  
<RouterA> terminal debugging  
<RouterA> terminal monitor
```

从 Host A 上 Ping Router B 的 Loopback0，并将报文数据字段长度设为 80 字节。

```
C:\>ping -l 80 10.1.1.1
```

Pinging 10.1.1.1 with 80 bytes of data:

```
Reply from 10.1.1.1: bytes=80 time<lms TTL=255  
Reply from 10.1.1.1: bytes=80 time<lms TTL=255  
Reply from 10.1.1.1: bytes=80 time<lms TTL=255  
Reply from 10.1.1.1: bytes=80 time<lms TTL=255
```

Ping statistics for 10.1.1.1:

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

从 Router A 上显示的策略路由调试信息如下:

```
<RouterA>  
*Jun  7 12:04:33:519 2009 RouterA PBR/7/POLICY-ROUTING: IP policy based routing  
success : POLICY_ROUTE_MAP : lab1, Node : 10, next-hop : 150.1.1.2  
*Jun  7 12:04:34:518 2009 RouterA PBR/7/POLICY-ROUTING: IP policy based routing  
success : POLICY_ROUTE_MAP : lab1, Node : 10, next-hop : 150.1.1.2  
*Jun  7 12:04:35:518 2009 RouterA PBR/7/POLICY-ROUTING: IP policy based routing  
success : POLICY_ROUTE_MAP : lab1, Node : 10, next-hop : 150.1.1.2  
*Jun  7 12:04:36:518 2009 RouterA PBR/7/POLICY-ROUTING: IP policy based routing  
success : POLICY_ROUTE_MAP : lab1, Node : 10, next-hop : 150.1.1.2
```

以上策略路由信息显示，Router A 在接收到报文后，根据策略路由确定的下一跳为 150.1.1.2，也就是说将报文从接口 Serial2/2/0 转发出去。

从 Host A 上 Ping Router B 的 Loopback0，并将报文数据字段长度设为 200 字节。

```
C:\>ping -l 200 10.1.1.1
```

Pinging 10.1.1.1 with 200 bytes of data:

```
Reply from 10.1.1.1: bytes=200 time<lms TTL=255  
Reply from 10.1.1.1: bytes=200 time<lms TTL=255  
Reply from 10.1.1.1: bytes=200 time<lms TTL=255  
Reply from 10.1.1.1: bytes=200 time<lms TTL=255
```

Ping statistics for 10.1.1.1:

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

从 Router A 上显示的策略路由调试信息如下:

```
<RouterA>
*Jun  7 12:06:47:631 2009 RouterA PBR/7/POLICY-ROUTING: IP policy based routing
success : POLICY_ROUTE_MAP : lab1, Node : 20, next-hop : 151.1.1.2
*Jun  7 12:06:48:630 2009 RouterA PBR/7/POLICY-ROUTING: IP policy based routing
success : POLICY_ROUTE_MAP : lab1, Node : 20, next-hop : 151.1.1.2
*Jun  7 12:06:49:627 2009 RouterA PBR/7/POLICY-ROUTING: IP policy based routing
success : POLICY_ROUTE_MAP : lab1, Node : 20, next-hop : 151.1.1.2
*Jun  7 12:06:50:627 2009 RouterA PBR/7/POLICY-ROUTING: IP policy based routing
success : POLICY_ROUTE_MAP : lab1, Node : 20, next-hop : 151.1.1.2
```

以上策略路由信息显示, Router A 在接收到报文后, 根据策略路由确定的下一跳为 151.1.1.2, 也就是说将报文从接口 Serial2/2/1 转发出去。

1.6.4 基于反向入接口的转发策略路由配置举例

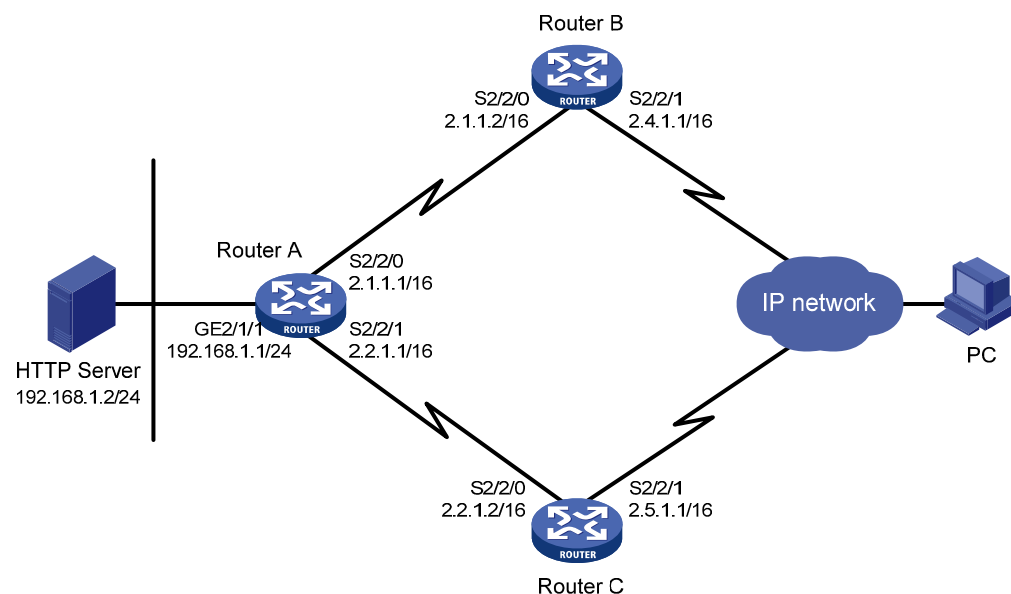
1. 组网需求

网关设备 Router A 通过两个接口 (Serial2/2/0 和 Serial2/2/1) 和公网连接。用户 PC 从公网访问内网的 HTTP 服务器, 假设 PC 请求报文从 Router A 接口 Serial2/2/0 进入, 通过网关设备转发, 从 Router A 的私网接口 GigabitEthernet2/1/1 进入内网访问 HTTP 服务器。

要求: 从私网返回的响应报文从 Router A 的接口 GigabitEthernet2/1/1 进入, 经 Router A 转发时, 能够从原来请求报文的入接口 Serial2/2/0 进入公网, 返回用户 PC。

2. 组网图

图1-4 基于反向入接口的转发策略路由配置举例组网图



3. 配置步骤

配置 Router A 各接口 IP 地址, 并保证 Router A 与公网连通 (略)。

在接口 Serial2/2/0 上配置 NAT 的内部服务器功能，将 HTTP 服务器的 IP 地址 192.168.1.2/24 映射为 2.1.1.100/16（和 Router A 的接口 Serial2/2/0 的 IP 地址在同一网段）。

```
<RouterA> system-view
[RouterA] interface serial 2/2/0
[RouterA-Serial2/2/0] nat server protocol tcp global 2.1.1.100 www inside 192.168.1.2 www
[RouterA-Serial2/2/0] quit
```

在接口 Serial2/2/1 上配置 NAT 的内部服务器功能，将 HTTP 服务器的 IP 地址 192.168.1.2/24 映射为 2.2.1.100/16（和 Router A 的接口 Serial2/2/1 的 IP 地址在同一网段）。

```
[RouterA] interface serial 2/2/1
[RouterA-Serial2/2/1] nat server protocol tcp global 2.2.1.100 www inside 192.168.1.2 www
[RouterA-Serial2/2/1] quit
```

定义 10 号节点，使匹配反向入接口 Serial2/2/0 的报文的下一跳地址为 2.1.1.2/16。

```
[RouterA] policy-based-route test permit node 10
[RouterA-pbr-test-10] if-match reverse-input-interface serial 2/2/0
[RouterA-pbr-test-10] apply ip-address next-hop 2.1.1.2
[RouterA-pbr-test-10] quit
```

在以太网接口 GigabitEthernet2/1/1 上应用策略 test。

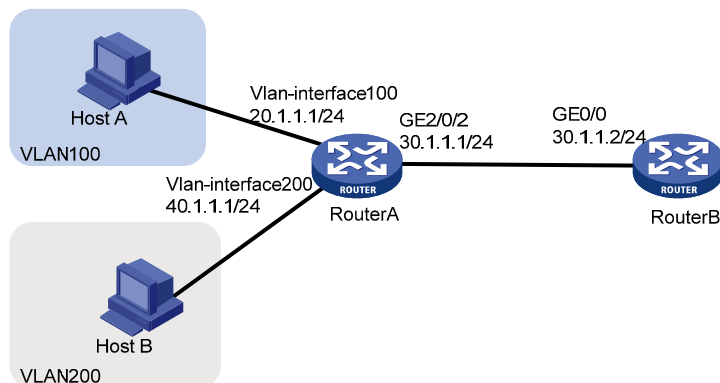
```
[RouterA] interface GigabitEthernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip policy-based-route test
```

1.6.5 SR6600/SR6600-X工作在网关模式时VLAN接口策略路由配置举例

1. 组网需求

Router A 工作在网关模式，并且配置了 SAP 板。Router A 与 Router B 相连。在 Router A 上划分 VLAN100 和 VLAN200，Host A 属于 VLAN100，Host B 属于 VLAN200。VLAN100 和 VLAN200 路由可达，通过策略路由控制 VLAN200 到 VLAN100 的报文通过 GigabitEthernet2/0/2 转发。

2. 组网图



3. 配置步骤

配置 RouterA 工作在网关模式，并将 RouterA 上与 VLAN100 和 VLAN200 相连的以太网接口 GigabitEthernet2/0/0 和 GigabitEthernet2/0/1 切换为二层模式。

```
<RouterA> system-view
[RouterA] gateway-mode
```

```
[RouterA] interface gigabitethernet2/0/0
[RouterA-gigabitethernet2/0/0] port link-mode bridge
[RouterA-gigabitethernet2/0/0] quit
[RouterA] interface gigabitethernet2/0/1
[RouterA-gigabitethernet2/0/1] port link-mode bridge
[RouterA-gigabitethernet2/0/1] quit
```

在 Router A 上创建两个 VLAN，分别为 VLAN100 和 VLAN200，将 GigabitEthernet 2/0/0 加入到 VLAN100，将 GigabitEthernet2/0/1 加入到 VLAN200。

```
[RouterA] vlan 100
[RouterA-vlan100] quit
[RouterA] vlan 200
[RouterA-vlan200] quit
[RouterA] interface gigabitethernet2/0/0
[RouterA-gigabitethernet2/0/0] port access vlan 100
[RouterA-gigabitethernet2/0/0] quit
[RouterA] interface gigabitethernet2/0/1
[RouterA-gigabitethernet2/0/1] port access vlan 200
[RouterA-gigabitethernet2/0/1] quit
```

定义高级访问控制列表

```
[RouterA] acl number 3000
[Route A-acl-adv-3000]rule permit ip
[Route A-acl-adv-3000] quit
```

定义 1 号节点，使 IP 报文的下一跳地址为 30.1.1.2

```
[Route A] policy-based-route aaa node 1
[Route A-pbr-aaa-1] if-match acl 3000
[Route A-pbr-aaa-1] apply ip-address next-hop 30.1.1.2
[Route A-pbr-aaa-1] quit
```

在 VLAN200 上应用接口策略路由

```
[Route A] interface Vlan-interface 200
[Route A-Vlan-interface200] ip policy-based-route aaa
[Route A-Vlan-interface200] quit
```

配置 QoS 重定向下一跳和策略路由下一跳保持一致

```
[Route A] traffic classifier aaa
[Route A-classifier-aaa] if-match acl 3000
[Route A-classifier-aaa] quit
[Route A] traffic behavior aaa
[Route A-behavior-aaa] redirect next-hop 30.1.1.2
[Route A-behavior-aaa] quit
[Route A] qos policy 1
[Route A-qospolicy-1] classifier aaa behavior aaa
[Route A-qospolicy-1] quit
[Route A] qos vlan-policy 1 vlan 200 inbound
```