目 录

1 IP单播策略路由配置

1.1 IP单播策略路由简介

IP 单播策略路由功能可以用来对 IP 单播报文进行策略路由。

1.1.1 策略路由简介

策略路由（policy-based-route）是一种依据用户制定的策略进行路由选择的机制。与单纯依照 IP 报文的目的地址查找路由表进行转发不同，策略路由基于到达报文的源地址、长度等信息灵活地进行路由选择。对于满足一定条件（报文长度或 ACL 规则）的报文，将执行一定的操作（设置转发报文的 VPN 实例、设置报文的优先级、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），以指导报文的转发。

根据作用对象的不同，策略路由可分为本地策略路由和接口策略路由：

- 本地策略路由：对本地产生的报文（比如本地发出的 ping 报文）进行策略路由，它只对本地产生的报文起作用，对转发的报文不起作用。
- 接口策略路由：对到达该接口的报文进行策略路由，它只对转发的报文起作用，对本地产生的报文不起作用。

对于一般转发和安全等方面的使用需求，大多数情况下使用的是接口策略路由。

一般来讲，策略路由的优先级要高于普通路由，即报文先按照策略路由进行转发。如果无法匹配所有的策略路由条件，不能按照策略路由进行转发，再按照普通路由进行转发。但对于配置了缺省出接口（下一跳）的情况，则是先进行普通路由的转发，如果无法匹配，再进行策略路由转发。

1.1.2 策略简介

一个策略用来引入一条路由，对 IP 报文转发进行路由选择。

一个策略可以包含一个或多个节点。

1. 节点

- 每个节点由 *node-number* 来指定。*node-number* 的值越小优先级越高，优先级高的节点优先被执行。
- 每个节点的具体内容由 **if-match** 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** 和 **deny** 两种。

2. if-match子句

IP 单播策略路由提供了三种 **if-match** 子句，分别为 **if-match packet-length**、**if-match reverse-input-interface** 和 **if-match acl**。

在一个节点中，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** 子句才算通过该节点的过滤。

3. apply子句

IP 单播策略路由提供了七种 **apply** 子句，分别为：**apply access-vpn vpn-instance**、**apply ip-precedence** 、 **apply output-interface** 、 **apply ip-address next-hop** 、 **apply default output-interface**、**apply ip-address default next-hop**、**apply fail-action continue**。

同一个节点中的各**apply**子句的执行优先级情况如 表 1-1所示。

表1-1 同一个节点中的各 apply 子句的执行优先级情况

子句	含义	执行优先情况
apply ip-df zero	将报文 IP 首部的 DF 标志置为 0	只要配置了该子句，该子句就一定会执行。
apply access-vpn vpn-instance	配置转发报文的 VPN 实例	只要配置了该子句，就不会执行除了 **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	配置报文的优先级	在公网转发中，即在未配置 **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**	配置策略路由出接口和下一跳	**apply output-interface** 命令的优先级高于 **apply ip-address next-hop**。当两条命令同时配置并且都有效时，系统只会执行 **apply output-interface** 命令。
apply default output-interface 和 **apply ip-address default next-hop**	配置策略路由缺省出接口和下一跳	**apply default output-interface** 命令的优先级高于 **apply ip-address default next-hop**。当两条命令同时配置并且都有效时，系统只会执行 **apply default output-interface** 命令。 执行缺省出接口和下一跳命令的前提是，在策略路由中报文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，并且报文目的 IP 地址在路由表中没有查到相应的路由，这时才会使用策略路由配置的缺省下一跳或者出接口。
apply fail-action continue	配置当前节点处理失败后继续进行下一节点的处理	• 如果仅配置了 **apply fail-action continue** 子句，则会进行下一节点的处理。 • 如果仅配置了 **apply fail-action continue** 子句和 **apply ip-precedence** 子句，则会进行下一节点的处理。 • 如果在配置了 **apply fail-action continue** 子句时，还配置了 **apply ip-address next-hop**、**apply output-interface**、**apply ip-address default next-hop** 、 **apply default output-interface** 这四个子句中的一个或多个（无论是否配置了 **apply ip-precedence** 子句），当配置的子句（除了 **apply fail-action continue** 子句和 **apply ip-precedence** 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。 • 如果配置了 **apply fail-action continue** 子句的节点是策略的最后一个节点，则报文将按正常转发流程处理。

4. 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

节点匹配模式 / 是否满足 **if-match** 子句	**permit**（允许模式）	**deny**（拒绝模式）
报文满足此节点的所有 **if-match** 子句	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，报文按正常转发流程处理
报文不满足此节点的 **if-match** 子句	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

同一个策略中的各节点之间是“或”的关系，即只要报文通过一个节点的过滤，就意味着通过该策略的过滤；如果报文不能通过一个策略中任何一个节点的过滤，则认为没有通过该策略的过滤，报文将按正常转发流程处理。

1.1.3 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策略路由对网络环境的动态感知能力。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，通过 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 配置IP单播策略路由

1.2.1 配置策略

表1-3 配置策略

操作	命令	说明
进入系统视图	**system-view**	-
创建策略或一个策略节点，并进入策略路由视图	**policy-based-route** *policy-name* [**deny** | **permit**] **node** *node-number*	必选
设置 IP 报文长度匹配条件	**if-match packet-length** *min-len max-len*	可选
设置反向入接口匹配条件	**if-match reverse-input-interface** *interface-type interface-number*	可选
设置 ACL 匹配条件	**if-match acl** *acl-number*	可选
设置报文在指定 VPN 实例进行转发	**apply access-vpn vpn-instance** *vpn-instance-name*&<1-6>	可选
设置报文的优先级	**apply ip-precedence** *value*	可选

操作	命令	说明
设置报文的出接口	**apply output-interface** *interface-type interface-number* [**track** *track-entry-number*] [*interface-type interface-number* [**track** *track-entry-number*]]	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，可以起到负载分担的作用 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
设置报文的下一跳	**apply ip-address next-hop** *ip-address* [**direct**] [**track** *track-entry-number*] [*ip-address* [**direct**] [**track** *track-entry-number*]] [**standby**]	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，可以起到负载分担的作用，如果配置 standby 关键字，则表示两个下一跳之间采用主备方式
设置报文缺省出接口	**apply default output-interface** *interface-type interface-number* [**track** *track-entry-number*] [*interface-type interface-number* [**track** *track-entry-number*]]	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，可以起到负载分担的作用
设置报文缺省下一跳	**apply ip-address default next-hop** *ip-address* [**direct**] [**track** *track-entry-number*] [*ip-address* [**track** *track-entry-number*]] [**standby**]	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，可以起到负载分担的作用，如果配置 standby 关键字，则表示两个下一跳之间采用主备方式
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

说明

- 如果 **if-match** 子句中使用了 ACL，将忽略 ACL 规则的 **permit/deny** 动作，只使用 ACL 中的分类域来匹配报文。如果使用的 ACL 不存在，则不匹配任何报文。
- **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能够生成会话，则所有报文都不匹配该子句。
- 当使用 **if-match reverse-input-interface** *interface-type interface-number* 命令配置接口后，若接口所在接口卡被拔出或该接口被删除的情况下，则显示信息中策略节点上 `if-match reverse-input-interface` 后配置的接口会消失，此时，任何报文都不能被该策略路由节点匹配。
- **apply ip-address next-hop** 命令可以配置两个下一跳，可以通过一次配置两个下一跳参数进行，也可以通过两条配置命令完成。当用户希望修改其中一个时，只需要继续执行 **apply ip-address next-hop** 命令，系统就会将最早配置的下一跳（一次配置两个下一跳参数的情况下为命令行输入的第二个参数值）替换；如果先前配置的两个下一跳都需要修改，则直接在 **apply ip-address next-hop** 命令后配置两个参数即可。命令 **apply output-interface**、**apply default output-interface** 和 **apply ip-address default next-hop** 的情况与 **apply ip-address next-hop** 相同，不再赘述。
- 在点对点的情况下，报文的下一跳即是对端地址，此时可以仅指定出接口，采用命令 **apply output-interface** *interface-type interface-number* [**track** *track-entry-number*] [*interface-type interface-number* [**track** *track-entry-number*]]；对于非点对点的情况，如果指定出接口，还需要知道下一跳。当指定 DHCP 客户端接口（该接口通过 DHCP 方式获取地址）为出接口，由于不是点对点应用，且不知道下一跳，就可以通过命令 **apply output-interface** *interface-type interface-number* **ip-address next-hop dhcpc**，将报文下一跳指定为通过 DHCP 学到的网关地址，通过这种方式来更改报文的下一跳。

注意

- 如果某一节点不配置 **if-match** 子句，则所有报文都会通过该节点的过滤，根据 **permit/deny** 执行相应的操作。
- 如果某一 **permit** 模式的节点不配置 **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，报文按正常转发流程处理。
- 如果某一节点没有配置任何 **if-match** 子句和 **apply** 子句，则所有报文都会通过该节点的过滤，但不会执行任何动作，且不再继续匹配下一节点，报文按正常转发流程处理。

1.2.2 配置本地策略路由

在应用本地策略路由时，只能引用一个策略。

表1-4 配置本地策略路由

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
应用本地策略路由	**ip local policy-based-route** *policy-name*	必选 缺省情况下，没有应用本地策略路由

1.2.3 配置接口策略路由

在应用接口策略路由时，一个接口只能引用一个策略。

表1-5 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** *interface-type interface-number*	-
应用接口策略路由	**ip policy-based-route** *policy-name*	必选 缺省情况下，没有应用接口策略路由

说明

SR6600 工作在网关模式，并且配置了 SAP 高密以太网板时，当在 VLAN 接口上应用策略路由时，需要先使用 **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”。

1.3 IP单播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 IP 单播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** 命令重置策略路由的统计信息。

表1-6 IP 单播策略路由显示和维护

操作	命令
显示系统和接口应用的所有策略路由的信息	**display ip policy-based-route** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示系统的策略路由的设置情况	**display ip policy-based-route setup** { **interface** *interface-type interface-number* | **local** | *policy-name* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示策略路由的统计信息	**display ip policy-based-route statistics** { **interface** *interface-type interface-number* | **local** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示已经配置的策略路由	**display policy-based-route** [*policy-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

操作	命令
重置策略路由的统计信息	**reset policy-based-route statistics** [*policy-name*]

说明

- 如果只添加一个节点而没有配置任何 **if-match** 子句和 **apply** 子句，则所有报文都匹配，但不执行动作，不再继续往下匹配。策略路由的统计数字不会改变。
- 如果添加一个节点，只配置 **if-match** 子句，没有配置 **apply** 子句，则进行匹配，但不执行动作，不再继续往下匹配。策略路由的统计数字不会改变。
- 如果添加一个节点，没有配置 **if-match** 子句，只配置 **apply** 子句，则所有报文都匹配，根据 **permit/deny** 执行相应的操作。策略路由的统计数字将改变。
- 当配置节点的匹配模式为 **deny** 时，如果报文满足该节点的所有 **if-match** 子句，不执行节点的 **apply** 子句，也不再继续往下匹配，数据包将走正常路由表转发，因此没有 **deny** 的调试信息以及相应的统计信息。

1.4 IP单播策略路由典型配置举例

1.4.1 基于报文协议类型的本地策略路由配置举例

1. 组网需求

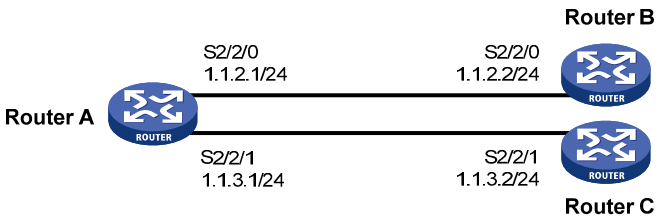
通过策略路由控制从 Router A 发出的报文：

- 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。Router B 与 Router C 路由不可达。

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 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。
```
<RouterA> telnet 1.1.2.2
Trying 1.1.2.2 ...
Press CTRL+K to abort
Connected to 1.1.2.2 ...
******************************************************************************
* Copyright (c) 2004-2009 Hangzhou H3C Tech. Co., Ltd. All rights reserved.  *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************
```
从 Router A 上 Telnet Router C（1.1.3.2/24），结果失败。
```
<RouterA> telnet 1.1.3.2
Trying 1.1.3.2 ...
Press CTRL+K to abort
Can't connect to the remote host!
```
从 Router A 上 ping Router C（1.1.3.2/24），结果成功。
```
<RouterA> ping 1.1.3.2
  PING 1.1.3.2: 56  data bytes, press CTRL_C to break
    Reply from 1.1.3.2: bytes=56 Sequence=1 ttl=255 time=2 ms
```

```
  Reply from 1.1.3.2: bytes=56 Sequence=2 ttl=255 time=1 ms
  Reply from 1.1.3.2: bytes=56 Sequence=3 ttl=255 time=1 ms
  Reply from 1.1.3.2: bytes=56 Sequence=4 ttl=255 time=1 ms
  Reply from 1.1.3.2: bytes=56 Sequence=5 ttl=255 time=1 ms

--- 1.1.3.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/1/2 ms
```

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 发出的 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。

1.4.2 基于报文协议类型的接口策略路由配置举例

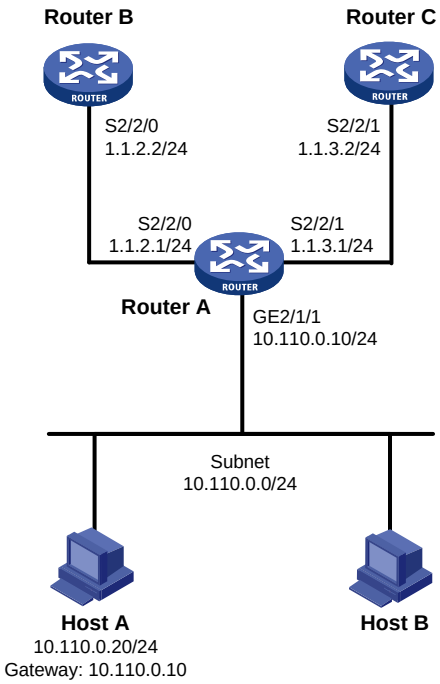
1. 组网需求

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策略路由的配置举例组网图



3. 配置步骤

说明

本例中采用静态路由保证各设备之间路由可达。

(1) 配置 Router A

定义访问控制列表，ACL 3101 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 上应用接口策略路由，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
[RouterB-Serial2/2/0] quit
```

(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
[RouterC-Serial2/2/1] quit
```

(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 与 Router A 直连的 Router B（**telnet** 1.1.2.2），结果成功。

从 Host A 上 Telnet 与 Router A 直连的 Router C（**telnet** 1.1.3.2），结果失败。

从 Host A 上 ping 与 Router A 直连的 Router C（**ping** 1.1.3.2），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。

1.4.3 基于报文长度的接口策略路由配置举例

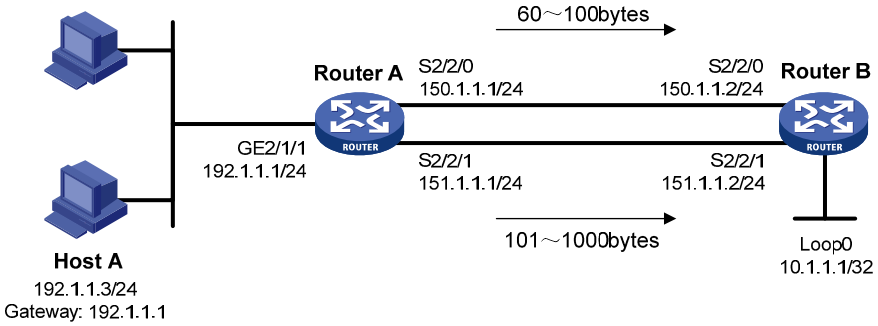
1. 组网需求

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 基于报文长度的策略路由的配置举例组网图



3. 配置步骤

说明

本例中采用动态路由协议 RIP 保证各设备之间路由可达。

(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] quit
```

(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
```

将 Host A 的 IP 地址配置为 192.1.1.3/24，网关地址配置为 192.1.1.1。

从 Host A 上 Ping Router B 的 Loopback0，并将报文数据字段长度设为 50 字节。

```
C:\>ping -l 50 10.1.1.1

Pinging 10.1.1.1 with 50 bytes of data:

Reply from 10.1.1.1: bytes=50 time<1ms TTL=255
Reply from 10.1.1.1: bytes=50 time<1ms TTL=255
Reply from 10.1.1.1: bytes=50 time<1ms TTL=255
Reply from 10.1.1.1: bytes=50 time<1ms 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_ROUTEMAP : 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_ROUTEMAP : 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_ROUTEMAP : 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_ROUTEMAP : 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<1ms TTL=255
Reply from 10.1.1.1: bytes=200 time<1ms TTL=255
Reply from 10.1.1.1: bytes=200 time<1ms TTL=255
Reply from 10.1.1.1: bytes=200 time<1ms 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_ROUTEMAP : 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_ROUTEMAP : 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_ROUTEMAP : 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_ROUTEMAP : 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。

1.4.4 基于反向入接口的接口策略路由配置举例

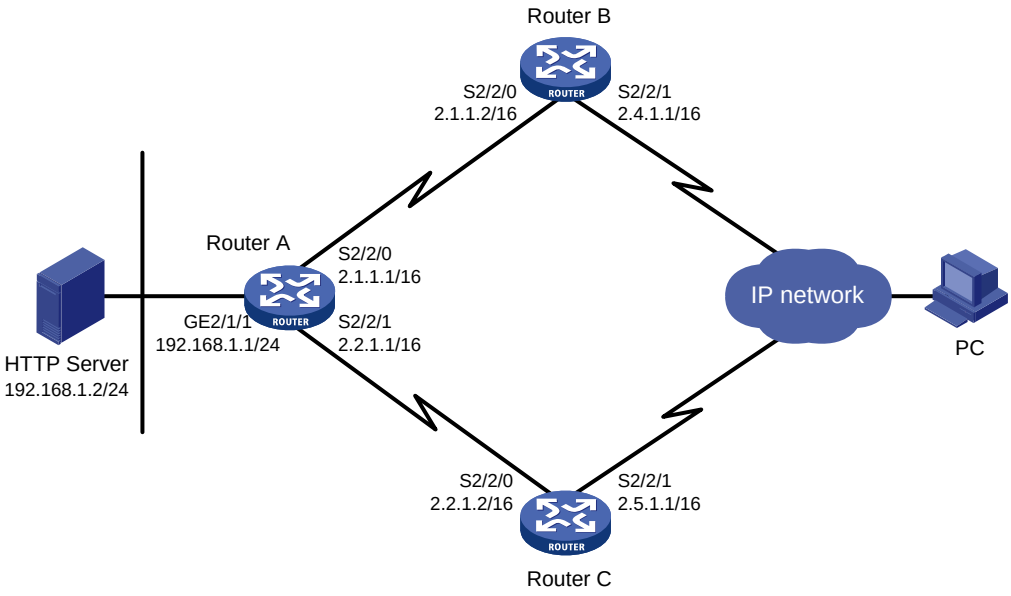
1. 组网需求

网关设备 Router A 通过两个接口（Serail2/2/0 和 Serial2/2/1）和公网连接。用户 PC 从公网访问内网的 HTTP Server 服务，不妨设 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 Server 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 上配置内部服务器功能，将 HTTP Server 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 上配置内部服务器功能，将 HTTP Server 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> system-view
[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。

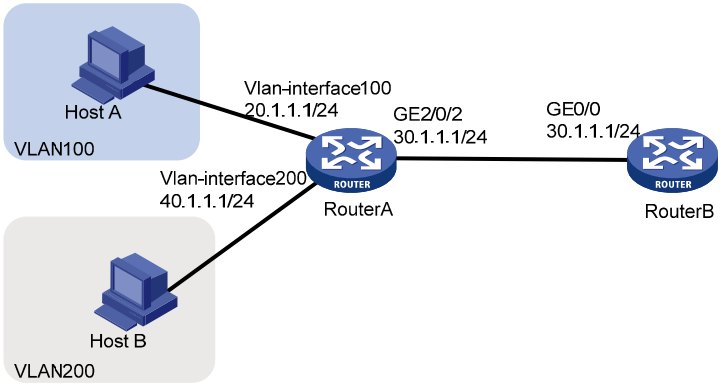
```
[RouterA] interface GigabitEthernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip policy-based-route test
```

1.4.5 SR6600 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 高密以太网板。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] alc 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
```