

密级：D

# RSR系列路由器 策略路由(PBR)功能初阶培训



# 目录 Contents

- **PBR作用及原理介绍**
- **PBR的典型应用及配置**

# 策略路由(PBR)作用及原理介绍

- **策略路由的作用**

策略路由 ( PBR : Policy-Based Routing ) 提供了一种比基于目的地址进行路由转发更加灵活的数据包路由转发机制：策略路由可以根据 IP/IPv6 报文源地址、目的地址、端口、报文长度等内容来决定报文转发的下一跳路由器

- **策略路由的原理**

路由器在转发数据报文的时，根据报文的目的地址查询路由表来获取报文转发的出口；策略路由则是在路由器执行路由查找之前，对于满足策略路由设定的条件，则按照策略路由定义的出口来执行转发。

策略路由使用路由图 ( route-map ) 来定义

策略路由比常规路由表 ( 包括直连路由 ) 更优先

# 策略路由(PBR)作用及原理介绍

- **route-map**

策略路由 ( PBR : Policy-Based Routing ) 通过route-map功能来实现  
示例如下

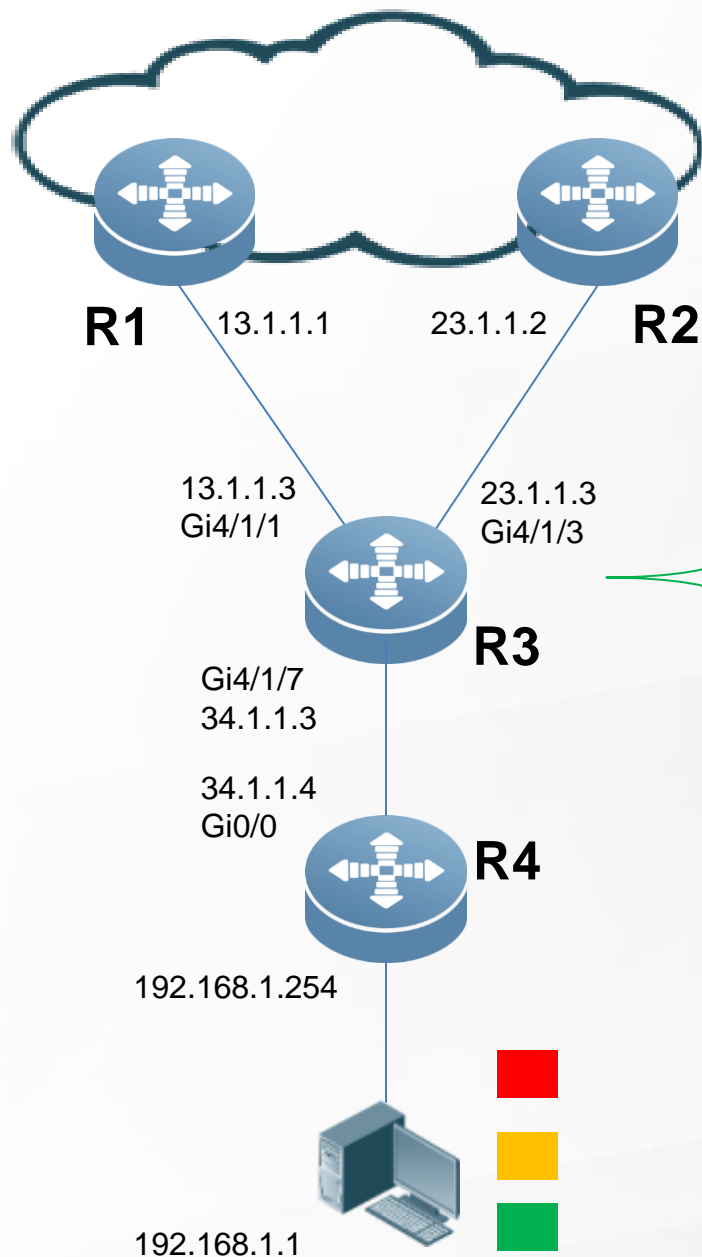
```
route-map pbr permit 10      //定义route-map名为pbr
match ip address 100         //match语句定义的匹配条件
set ip next-hop 13.1.1.1     //set语句定义的是满足match语句定义的条件下载文转发的下一跳地址

interface GigabitEthernet 4/1/7
ip policy route-map pbr      //在接口上应用，PBR作用于接口的in方向
```

从Gi4/1/7接口进来的报文，如果满足ACL 100的定义，则直接从下一跳地址为13.1.1.1的接口转发出去；否则，通过查询路由表，决定转发报文的出接口

route-map可以定义多条条目，报文从上之下依次匹配，一旦命中则直接执行对应的set动作，若匹配至最后一条route-map条目，仍然未命中(或者未指定set动作)，则查询路由表，确定转发报文的出接口

# 策略路由(PBR)作用及原理介绍



```
access-list 100 permit ip host 192.168.1.1 host 11.11.11.11
access-list 101 permit ip host 192.168.1.1 host 22.22.22.22
```

```
route-map pbr permit 10
match ip address 100
set ip next-hop 13.1.1.1
route-map pbr permit 20
match ip address 101
set ip next-hop 23.1.1.2
```

```
interface GigabitEthernet 4/1/7
ip policy route-map pbr
```

```
ip route 0.0.0.0 0.0.0.0 13.1.1.1
ip route 0.0.0.0 0.0.0.0 23.1.1.2 100
```

# 部署策略路由(PBR)的几个注意点

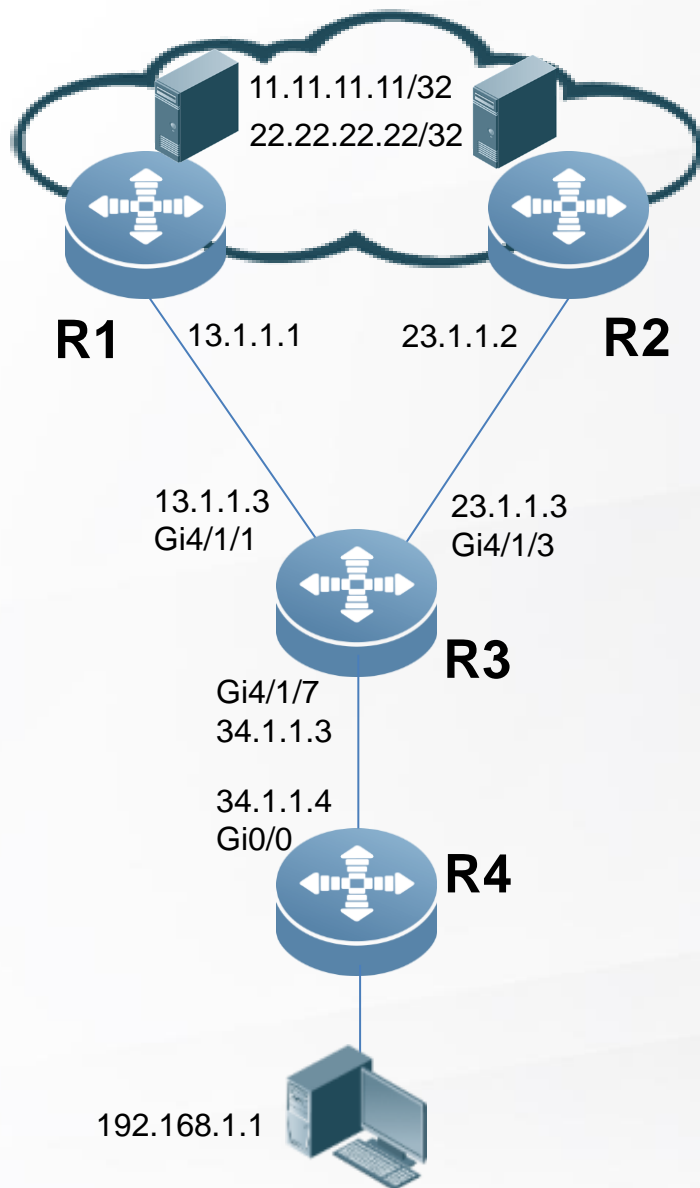
- **1、指定下一跳的地址是set ip next-hop而不是set next-hop**  
set next-hop为bgp路由的属性而非设置下一跳
- **2、下一跳地址的设定默认是无状态的**
  - 1) 意味着下一跳地址不可达且本地接口up的情况下，pbr会将对应的报文丢弃  
(解决办法为配置探测协议联动PBR，并指定备用的下一跳)
  - 2) 如果对应下一跳地址的本地接口down，则匹配该语句的报文将直接查路由表进行数据转发
- **3、对于一个match语句可以指定多个下一跳，默认是冗余备份关系**
  - 1) 冗余备份的优先顺序按照配置顺序而定  
冗余切换的条件如下：
    - A) 若未配置和探测协议联动的话，配置靠前的下一跳地址对应的本地接口down
    - B) 配置了探测协议和pbr联动的话，以探测协议状态切换为down为切换条件
  - 2) 可修订为负载模式（命令为ip policy load-balance），**但推荐使用冗余模式**
- **4、route-map语句若采用deny则表示该语句命中的报文直接查路由表**  
route-map pbrtest deny 10  
match ip address 100 -----ACL100命中的报文直接查询路由表进行转发

# 目录 Contents

- PBR作用及原理介绍
- **PBR的典型应用及配置**

# PBR的典型应用及配置

## 一、拓扑



## 二、需求

- 1、出口路由器为R3，申请了2根MSTP专线作为出口
- 2、要求内网一台主机 ( 192.168.1.1 ) 在访问11.11.11.11/32服务器时优先选择走R1，如果R1宕机或者线路异常，再选择走R2
- 3、同一台主机在访问22.22.22.22/32服务器优先走R2，在R2宕机或者对应线路故障时，再选择走R1
- 4、访问其他服务器则根据实际路由选择即可



# PBR的典型应用及配置

## 三、功能部署

### 1) 基本配置

```
interface GigabitEthernet 4/1/1
 ip address 13.1.1.3 255.255.255.0
interface GigabitEthernet 4/1/3
 ip address 23.1.1.3 255.255.255.0
interface GigabitEthernet 4/1/7
 ip address 34.1.1.3 255.255.255.0
```

### 2) 定义要进行策略路由的流量

```
ip access-list extended 100
 10 permit ip host 192.168.1.1 host 11.11.11.11 //定义pc访问服务器11.11.11.11的流量
ip access-list extended 101
 10 permit ip host 192.168.1.1 host 22.22.22.22 //定义pc访问服务器22.22.22.22的流量
```

# PBR的典型应用及配置

## 三、功能部署(续)

### 2) 探测协议选择track，定义探测内容

```
ip rns 1
```

```
icmp-echo 13.1.1.1 source-ipaddr 13.1.1.3 out-interface GigabitEthernet 4/1/1 next-hop 13.1.1.1
```

```
timeout 1000
```

```
frequency 2000
```

//定义rns 1，探测地址13.1.1.1的连通性；探测报文源地址为13.1.1.3，从接口gi4/1/1接口发出，2s探测一次，超时时间为1s

```
track 1 rns 1
```

//定义track 1关联rns 1

# PBR的典型应用及配置

## 三、功能部署(续)

### 2) 探测协议选择track，定义探测内容（续）

```
ip rns 2
```

```
icmp-echo 23.1.1.2 source-ipaddr 23.1.1.3 out-interface GigabitEthernet 4/1/3 next-hop 23.1.1.2
```

```
timeout 1000
```

```
frequency 2000
```

//定义rns 2，探测地址23.1.1.2的连通性；探测报文源地址为23.1.1.3，从接口gi4/1/3接口发出，2s探测一次，超时时间为1s

```
track 2 rns 2
```

//定义track 2关联rns 2

# PBR的典型应用及配置

## 三、功能部署(续)

### 3) 定义策略路由规则 ( route-map )

```
route-map pbr permit 10      //定义名为pbr的route-map的第一条规则
match ip address 100         //匹配ACL100定义的流量
set ip next-hop verify-availability 13.1.1.1 track 1 //设置下一跳为13.1.1.1并和track1的状态绑定
set ip next-hop 23.1.1.2     //备用下一跳为23.1.1.2在13.1.1.1不可达的时候启用

route-map pbr permit 20      //定义名为pbr的route-map的第二条规则
match ip address 101         //匹配ACL101定义的流量
set ip next-hop verify-availability 23.1.1.2 track 2 //设置下一跳为23.1.1.2并和track2的状态绑定
set ip next-hop 13.1.1.1     //备用下一跳为13.1.1.1在23.1.1.2不可达的时候启用
```

尾部有一条隐藏的deny any的语句，意味着不被上面2条规则命中的流量通过查询路由表进行转发

# PBR的典型应用及配置

## 三、功能部署(续)

### 4) 策略路由应用

```
interface GigabitEthernet 4/1/7  
ip policy route-map pbr
```

### 5) 部署浮动静态路由

```
ip route 0.0.0.0 0.0.0.0 13.1.1.1 track 1 //主用路由从出口至R1的线路走，并和track1联动  
ip route 0.0.0.0 0.0.0.0 23.1.1.2 100 //备用路由从出口至R2的线路走  
ip route 192.168.1.0 255.255.255.0 34.1.1.4 //到内网PC的的路由
```

# PBR的典型应用及配置

## 四、功能验证

### 1) PC访问11.11.11.11服务器

```
2014e_r4#ping 11.11.11.11 source 192.168.1.1
```

```
Sending 5, 100-byte ICMP Echoes to 11.11.11.11, timeout is 2 seconds:
```

```
< press Ctrl+C to break >
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/10/10 ms
```

```
2014e_r4#traceroute 11.11.11.11 source 192.168.1.1
```

```
< press Ctrl+C to break >
```

```
Tracing the route to 11.11.11.11
```

```
1  34.1.1.3 0 msec 10 msec 0 msec
```

```
2  13.1.1.1 0 msec 10 msec 10 msec
```

```
3  11.11.11.11 0 msec 10 msec 10 msec
```

```
2014e_r4#
```

# PBR的典型应用及配置

## 四、功能验证

### 2) PC访问22.22.22.22服务器

2014e\_r4#ping 22.22.22.22 source 192.168.1.1

Sending 5, 100-byte ICMP Echoes to 22.22.22.22, timeout is 2 seconds:

< press Ctrl+C to break >

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/10 ms

2014e\_r4#tra 22.22.22.22 source 192.168.1.1

< press Ctrl+C to break >

Tracing the route to 22.22.22.22

1 34.1.1.3 0 msec 0 msec 0 msec

2 23.1.1.2 0 msec 0 msec 0 msec

3 22.22.22.22 0 msec 10 msec 0 msec

2014e\_r4#

# PBR的典型应用及配置

## 四、功能验证

### 3) 出口至R1线路故障，PC访问11.11.11.11服务器

```
2014e_r4#ping 11.11.11.11 source 192.168.1.1
```

```
Sending 5, 100-byte ICMP Echoes to 11.11.11.11, timeout is 2 seconds:
```

```
< press Ctrl+C to break >
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/10/10 ms
```

```
2014e_r4#traceroute 11.11.11.11 source 192.168.1.1
```

```
< press Ctrl+C to break >
```

```
Tracing the route to 11.11.11.11
```

```
1  34.1.1.3 0 msec 10 msec 0 msec
```

```
2  23.1.1.2 0 msec 0 msec 0 msec
```

```
3  11.11.11.11 0 msec 10 msec 10 msec
```

```
2014e_r4#
```



# PBR的典型应用及配置

## 四、功能验证

### 4) 恢复出口至R1的线路，中断出口至R2的线路，PC访问22.22.22.22服务器

```
2014e_r4#ping 22.22.22.22 source 192.168.1.1
```

```
Sending 5, 100-byte ICMP Echoes to 22.22.22.22, timeout is 2 seconds:
```

```
< press Ctrl+C to break >
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/10 ms
```

```
2014e_r4#tra 22.22.22.22 source 192.168.1.1
```

```
< press Ctrl+C to break >
```

```
Tracing the route to 22.22.22.22
```

```
1  34.1.1.3 0 msec 0 msec 0 msec
```

```
2  13.1.1.1 0 msec 10 msec 10 msec
```

```
3  22.22.22.22 0 msec 10 msec 0 msec
```

```
2014e_r4#
```

# 部署总结

1. 策略路由使用的route-map尾部默认的deny any的规则使得未配精确匹配的报文通过查询路由表的方式进行转发，**而不是丢弃**
2. 下一跳接口对应的本地接口down后，对应规则命中的报文会通过查询路由表进行转发
3. 若中间链路导致下一跳不可达，而本地接口处于up的情况下，对应规则命中的报文仍然会从对应接口转发出去，导致连通性异常
4. 为解决3中提到的问题，会使用探测协议（track/bfd）来和pbr关联用于探测下一跳的可达性；但需注意：**此时必须配置备用下一跳**
5. 鉴于当前mstp专线的普及，3中的问题是一个常见问题，因此部署PBR建议都要和探测协议联动，探测协议推荐使用track，只需本端配置，对端只需要允许ping即可。
6. 策略路由针对策略部署接口入向的流量生效，对设备本地发出的流量无效（要对本地发出的流量执行策略路由，可通过Ruijie(config)# ip local policy route-map *name*来实现，这里不再详述，感兴趣的可以查阅设备对应的配置手册进一步了解）

# THANKS

锐捷网络股份有限公司

地址：北京海淀区复兴路29号中意鹏奥大厦东塔A座11层 邮编：100036

Office Tel: 010-51715999 Fax: 010-51413399

[www.ruijie.com.cn](http://www.ruijie.com.cn)

