
Contents

1 Configuring PBR.....	1
1.1 Introduction.....	1
1.1.1 Overview.....	1
1.1.2 Principles.....	1
1.2 Configuration Task Summary.....	4
1.3 Configuring Basic Functions of PBR.....	4
1.3.1 Overview.....	4
1.3.2 Restrictions and Guidelines.....	4
1.3.3 Configuration Tasks.....	4
1.3.4 Applying PBR to an Interface.....	5
1.3.5 Applying PBR to a Local Device.....	5
1.4 Configuring Redundant Backup or Load Balancing.....	6
1.4.1 Overview.....	6
1.4.2 Restrictions and Guidelines.....	6
1.4.3 Procedure.....	7
1.5 Configuring Source-Address-Based PBR.....	7
1.5.1 Overview.....	7
1.5.2 Restrictions and Guidelines.....	7
1.5.3 Procedure.....	8
1.6 Monitoring.....	8

- 1.7 Configuration Examples..... 10
 - 1.7.1 Configuring PBR to Implement Multi-Exit High Availability..... 10
 - 1.7.2 Selecting an Output Link based on Source Addresses of Packets..... 14

1 Configuring PBR

1.1 Introduction

1.1.1 Overview

You can apply a route map containing policies to interfaces and devices to implement Policy-Based Routing (PBR).

Similar to static routing, PBR is manually configured and does not automatically update with network changes. It is effective only for packets from local interfaces and devices. PBR is more flexible than static and dynamic routing. Static and dynamic routing forwards packets only based on destination addresses. PBR forwards packets based on the source IP address, destination IP address, packet length, and ingress port.

1.1.2 Principles

1. PBR-Procedure

To implement PBR, perform the following steps:

- (1) Define a policy: Use the route map to define matching rules for traffic characteristics and set processing actions.
- (2) Apply the policy: Apply the policy to interfaces or local devices.

2. Packet Processing Flow

After the device identifies packets, it processes packets as follows:

- (1) Identify the source of traffic to determine the traffic is forwarded or is local, and check whether any policy is applied.
- (2) Forward the packets based on the defined policy.
- (3) If no next hop is matched or the next hop is unreachable, forward the packets based on the routing table.
- (4) If the routing table does not contain any route to the destination address, discard the packets.

3. Definition of a Policy

A policy is a "**match...**, **set...**" statement, which indicates that "if certain conditions are matched, you can perform some processing actions"

 Note

For details about the policies, see *Configuring Routing Policies*.

- Executing a policy

A route map contains multiple policies. Each policy has a sequence number. A smaller sequence number means a higher priority. You can execute policies by sequence number. Once the matching condition of a policy is met, the processing action of this policy is performed and the route map exits. If no matching condition of any policy is met, no processing is performed.

Policies support two working modes:

- permit: When the matching condition of a policy is met, perform the processing action of this policy and exit the route map.
- deny: When the matching condition of a policy is met, do not perform the processing action of this policy, but exit the route map.
- Matching conditions of policies

The matching condition of a policy may contain zero, one, or more match rules.

- If the matching condition contains 0 matching rule, no packet is matched.
- If the matching condition contains one or more match rules, the matching condition is met only when all the rules are matched.

In the route map mode, run the **match** command to set matching rules. One **match** command corresponds to one matching rule.

- Processing action for a policy

The processing action of a policy contains 0, 1 or more set rules.

- If the processing action contains 0 set rule, no processing action is performed and the route map directly exits.
- If the processing action contains one or more set rules, all processing actions are performed and then the route map exits.

▲ Caution

If set rules have different priorities, only the set rule with the highest priority takes effect.

4. Application of a Policy

Apply a route map including policies to interfaces or devices to implement PBR.

- If a route map is applied to an interface, packets received by the interface are routed based on the policy.
The PBR is often used to control user packets received by a device. It is effective only for forwarded packets, but not for locally initiated packets.
- If a route map is applied to a device, locally initiated packets are routed based on the policy.
The PBR is often used to control protocol packets exchanged between devices (such as ping packets sent locally). It is effective only for locally initiated packets, but not for forwarded packets.

5. Enhanced Reliability of PBR

- Redundant backup or load balancing

You can set multiple next hops in a policy. Either redundant backup or load balancing can be implemented among multiple next hops. Redundant backup is implemented by default.

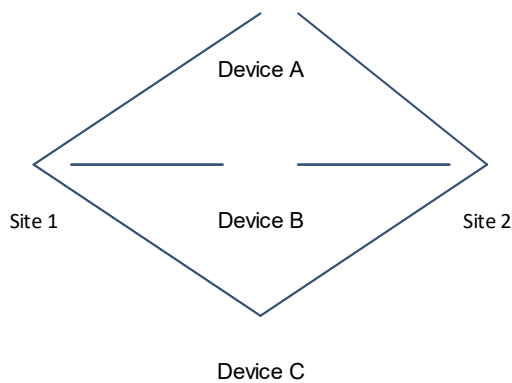
- Redundant backup

As shown in [Figure 1-1](#), the configuration sequence of the next hop from Site 1 to Site 2 is as follows: Device A > Device B > Device C, and the first accessible next hop takes effect. When the currently effective next hop (Device A) is faulty, the traffic automatically switches to the next accessible next hop (Device B). When Device A becomes accessible again, the traffic automatically switches back to Device A.

A new next hop stays at the end of the sequence. If the original sequence is Device A > Device B > Device C, and if Device A is added after it is deleted, the current sequence becomes Device B > Device C > Device A.

If no next hop is accessible, packets are discarded.

Figure 1-1 Redundant backup function



- Load balancing

When multiple accessible next hops take effect concurrently, the Weighted Cost Multiple Path (WCMP) and Equal Cost Multiple Path (ECMP) are supported. After an accessible next hop fails, traffic will be balanced among the other accessible next hops.

- Correlation with BFD

Correlation between PBR and BFD helps the PBR to better perceive network environment changes. When BFD finds the current next hop unaccessible, the BFD immediately notifies the PBR of switching the traffic to another accessible next hop (to implement redundant backup) or all the other accessible next hops (to implement load balancing).

- Correlation with Track

Correlation between PBR and Track helps the PBR to better perceive network environment changes. When Track finds the current next hop inaccessible, the Track immediately notifies the PBR of switching the traffic to another accessible next hop (to implement redundant backup) or all the other accessible next hops (to implement load balancing).

6. Source-address-based PBR

If the source-address-based PBR is generated, you do not need to configure a route map.

- If only the source IPv4 address or source IPv6 address of packets forwarded by the interface needs to be matched, you can run the command of the source-address-based PBR. This command is more simply configured than that of interface-based PBR.
- If the source-address-based PBR is applied to a specified interface, packets received on this interface are routed according to the source addresses.

The PBR is often used to control user packets received by a device. It is effective only for forwarded packets, but not for locally initiated packets.

Note

The source-address-based PBR has a lower priority than the interface-based PBR. If the source-address-based PBR and the interface-based PBR are applied to the same interface, only the interface-based PBR takes effect.

1.2 Configuration Task Summary

The PBR configuration includes the following tasks:

- (1) [Configuring Basic Functions of PBR](#)
 - [Applying PBR to an Interface](#)
 - [Applying PBR to a Local Device](#)
- (2) (Optional) [Configuring Redundant Backup or Load Balancing](#)
- (3) (Optional) [Configuring Source-Address-Based PBR](#)

1.3 Configuring Basic Functions of PBR

1.3.1 Overview

This section describes how to perform personalized routing management of user data streams by preparing flexible policies.

1.3.2 Restrictions and Guidelines

- A route map must be used when PBR is configured. Therefore, you must configure a route map on a device.
- If an ACL is used when the route map is configured, you must configure the ACL on the device.

- If the route map used in PBR does not exist, the PBR does not take effect.

1.3.3 Configuration Tasks

The configuration of PBR basic functions includes the following tasks:

- [Applying PBR to an Interface](#)
- [Applying PBR to a Local Device](#)

1.3.4 Applying PBR to an Interface

1. Overview

This section describes how to apply PBR to an interface to implement personalized routing management on user data streams passing a device.

2. Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Enter the interface configuration mode.

interface *interface-type interface-number*

- (4) Apply PBR to IPv4 packets received by an interface.

ip policy route-map *route-map-name*

By default, no PBR is configured on an interface.

- (5) Apply PBR to IPv6 packets received by an interface.

ipv6 policy route-map *route-map-name*

By default, no IPv6 PBR is configured on an interface.

1.3.5 Applying PBR to a Local Device

1. Overview

This section describes how to apply PBR to a local device to implement personalized management on packets initiated by the local device. A device has only one IPv4 PBR and one IPv6 PBR.

2. Procedure

- (1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Apply PBR to IPv4 packets initiated by the local device.

ip local policy route-map *route-map-name*

By default, no IPv4 PBR is applied to the local device.

(4) Apply PBR to IPv6 packets initiated by the local device.

ipv6 local policy route-map *route-map-name*

By default, no IPv6 PBR is applied to the local device.

1.4 Configuring Redundant Backup or Load Balancing

1.4.1 Overview

Multiple next hops in the mutual backup mode can enhance the network reliability.

Load balancing mode among multiple next hops can expand the network bandwidth.

1.4.2 Restrictions and Guidelines

- If redundant backup is selected, the first next hop takes effect based on the configuration sequence.
- If load balancing is selected, all next hops take effect at the same time and share traffic by weight.
- This configuration applies to all PBRs configured on a device.
- The basic functions of PBR must be configured.
- Redundant backup and load balancing are effective only for the next hops set by the following **set** commands, and only among multiple next hops set by the same **set** command.

Table 1-1 set commands for configuring the next hop

Command	Description
set ip next-hop	Configures the next hop of IPv4 packets. This command carries the weight parameter to set the weight of the WCMP. The default value is 1.
set ip default next-hop	Configures the default next hop of IPv4 packets. This command carries the weight parameter to set the weight of the WCMP. The default value is 1.

Command	Description
set ipv6 next-hop	Configures the next hop of IPv6 packets. This command carries the weight parameter to set the weight of the WCMP. The default value is 1 .
set ipv6 default next-hop	Configures the default next hop of IPv6 packets. This command carries the weight parameter to set the weight of the WCMP. The default value is 1 .
set ip next-hop recursive	Configures the recursive next hop of IPv4 packets. Only one command is configured for a route map, and packets can recur to multiple next hops (up to 32 next hops) of a static or dynamic ECMP route. The redundant backup or load balancing mode for recurring to multiple next hops is also determined by the ip policy { redundancy load-balance } command.
set ipv6 next-hop recursive	Configures the recursive next hop of IPv6 packets. Only one command is configured for a route map, and packets can recur to multiple next hops (up to 32 next hops) of a static or dynamic ECMP route. The redundant backup or load balancing mode for recurring to multiple next hops is also determined by the ipv6 policy { redundancy load-balance } command.

1.4.3 Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Configure an IPv4 PBR to implement redundant backup or load balancing among multiple next hops.

ip policy { redundancy | load-balance }

By default, multiple next hops of the PBR adopt the redundant backup mode.

- (4) Configure an IPv6 PBR to implement redundant backup or load balancing among multiple next hops.

ipv6 policy { redundancy | load-balance }

By default, multiple next hops of the IPv6 PBR adopt the redundant backup mode.

1.5 Configuring Source-Address-Based PBR

1.5.1 Overview

This section describes how to perform personalized routing management for IPv4 or IPv6 addresses of user data streams by preparing flexible policies.

1.5.2 Restrictions and Guidelines

- Source-address-based PBR has a higher priority than interface-based PBR. When they are applied to an interface at the same time, interface-based PBR takes effect whereas source-address-based PBR does not take effect.
- The global configuration takes effect on the input interface of specified user data streams.
- You can specify multiple source-address-based PBRs for the same interface. The sequence numbers of source-address-based PBRs must be different. A smaller sequence number indicates a higher priority of the source-address-based PBR.

If the sequence number is the same, the priorities of next hop types are as follows:

next-hop *ip-address* > **default next-hop** *ip-address*

1.5.3 Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Configure an **IPv6** PBR to implement redundant backup or load balancing among multiple next hops.

```
ip policy-source in-interface interface-type interface-number sequence { source-address mask | source-address/mask } { [ default ] next-hop [ ipv4-address [ weight ] ]&<1-4> | [ default ] interface { out-interface-type out-interface-number } &<1-4> }
```

By default, no source-address-based PBR takes effect on an interface.

- (4) Apply a source-address-based PBR for IPv6 packets received by an interface.

```
ipv6 policy-source in-interface interface-type interface-number sequence source-address/prefix-length { [ default ] next-hop [ ipv6-address [ weight ] ]&<1-4> | [ default ] interface out-interface-type&<1-4> }
```

By default, no source-address-based IPv6 PBR takes effect on an interface.

1.6 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

You can run the **clear** commands to clear information.

▲ Caution

Running the **clear** commands may lose vital information and thus interrupt services.

You can run the **debug** command to output debugging information.

▲ Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 Monitoring of the PBR

Command	Purpose
show ip policy [<i>route-map-name</i>]	Displays the configurations of the IPv4 PBR.
show ipv6 policy	Displays the configurations of the IPv6 PBR.
show route-map [<i>name</i>]	Displays the configurations of a route map.
show access-list	Displays the configurations of an ACL.
show ip pbr bfd	Displays the correlation between the IPv4 PBR and BFD.
show ipv6 pbr bfd	Displays the correlation between the IPv6 PBR and BFD.
show ip pbr route [interface <i>interface-type</i> <i>interface-number</i> local]	Displays the routing information of the IPv4 PBR.
show ipv6 pbr route [interface <i>interface-type</i> <i>interface-number</i> local]	Displays the routing information of the IPv6 PBR.
show ip pbr route-map <i>rmap-name</i>	Displays a route map used by the IPv4 PBR.
show ipv6 pbr route-map <i>rmap-name</i>	Displays a route map used by the IPv6 PBR.
show ip pbr source-route [interface <i>interface-type</i> <i>interface-number</i>]	Displays the routing information of source-address-based IPv4 PBR.
show ipv6 pbr source-route [interface <i>interface-type</i> <i>interface-number</i>]	Displays the routing information of source-address-based IPv6 PBR.
show ip pbr statistics [interface <i>interface-type</i> <i>interface-number</i> local]	Displays the statistics about the IPv4 PBR.

Command	Purpose
show ipv6 pbr statistics [interface <i>interface-type interface-number</i> local]	Displays the statistics about the IPv6 PBR.
clear ip pbr statistics [interface <i>interface-type interface-number</i> local]	Clears the statistics about packets forwarded by the IPv4 PBR.
clear ipv6 pbr statistics [interface <i>interface-type interface-number</i> local]	Clears the statistics about packets forwarded by the IPv6 PBR.
debug pbr error	Debugs PBR errors.
debug pbr events	Debugs PBR events.
debug pbr ms	Debugs multiple service cards supported by PBR.
debug pbr msg	Debugs PBR message communication.
debug pbr nsm	Debugs interaction between PBR and NSM.
debug pbr packet	Debugs packet forwarding of PBR.
debug pbr restart	Debugs PBR GR.

1.7 Configuration Examples

1.7.1 Configuring PBR to Implement Multi-Exit High Availability

1. Requirements

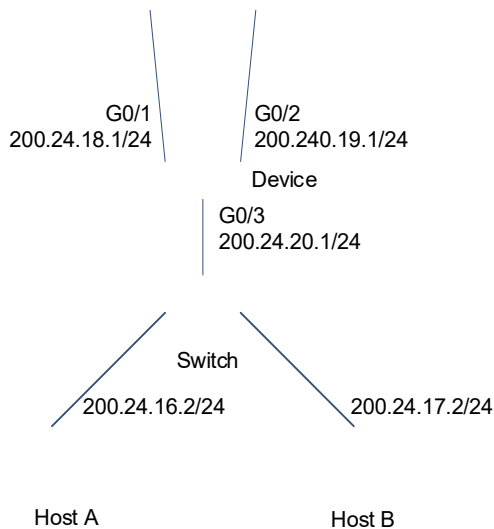
Configure PBR on the devices to achieve the following purposes:

- Packets from Host A (200.24.16.2/24) are sent from GigabitEthernet 0/1 first.
- Packets from Host B (200.24.17.2/24) are sent from GigabitEthernet 0/2 first.

The two output links work in mutual backup mode, and are correlated with Track. Thus, when one link is faulty, traffic is quickly switched over to the other link.

2. Topology

Figure 1-1 PBR topology



3. Notes

- Configure two different ACLs to match packets in the Host A and Host B network segment respectively.
- Configure the route map RM_FOR_PBR: policy 10 is used to ensure that "packets in the Host A network segment are sent from GigabitEthernet 0/1 first"; policy 20 is used to ensure that "packets in the Host B network segment are sent from GigabitEthernet 0/2 first".
- Configure a PBR to implement redundant backup among multiple next hops.
- Configure the track rules and correlation between PBR and Track.
- Configure PBR and apply the route map RM_FOR_PBR to packets received from GigabitEthernet 0/3.

4. Procedure

- (1) Configure the IP addresses of interfaces to implement interworking between networks. (Omitted)
- (2) Configure ACLs for subnets 200.24.16.0/24 and 200.24.17.0/24, respectively.

```

Device> enable
Device# configure terminal
Device(config)# access-list 1 permit 200.24.16.0 0.0.0.255
Device(config)# access-list 2 permit 200.24.17.0 0.0.0.255
    
```

- (3) Configure the track rules.

```

Device(config)# ip rns 1
Device(config-ip-rns)# icmp-echo 200.24.18.1
    
```

```

Device(config-ip-rns)# exit
Device(config)# ip rns schedule 1 start-time now life forever
Device(config)# track 1 rns 1
Device(config)# ip rns 2
Device(config-ip-rns)# icmp-echo 200.24.19.1
Device(config-ip-rns)# exit
Device(config)# ip rns schedule 2 start-time now life forever
Device(config)# track 2 rns 2

```

- (4) Configure the PBR **RM_FOR_PBR**, set the next hop of 200.24.16.0 to **200.24.18.1** and its backup next hop to **200.24.19.1**, and set the next hop of 200.24.17.0 to **200.24.19.1** and its backup next hop to **200.24.18.1**.

```

Device(config)# route-map RM_FOR_PBR 10
Device(config-route-map)# match ip address 1
Device(config-route-map)# set ip next-hop verify-availability 200.24.18.1 track
1
Device(config-route-map)# set ip next-hop verify-availability 200.24.19.1 track
2
Device(config-route-map)# exit
Device(config)# route-map RM_FOR_PBR 20
Device(config-route-map)# match ip address 2
Device(config-route-map)# set ip next-hop verify-availability 200.24.19.1 track
2
Device(config-route-map)# set ip next-hop verify-availability 200.24.18.1 track
1
Device(config-route-map)# exit

```

- (5) Apply the route map **RM_FOR_PBR** to GigabitEthernet 0/3, and enable load balancing.

```

Device(config)# interface GigabitEthernet 0/3
Device(config-if-GigabitEthernet 0/3)# ip policy route-map RM_FOR_PBR
Device(config-if-GigabitEthernet 0/3)# exit
Device(config)# ip policy redundance

```

5. Verification

Check the PBR configurations to verify that the route map is applied to the interface.

```

Device# show ip policy
Balance mode: redundance
Interface                               Route map
GigabitEthernet 0/3                     RM_FOR_PBR
!
```

Check the configurations of the route map to verify the policy rules.

```

Device# show route-map
route-map RM_FOR_PBR, permit, sequence 10

```

```
Match clauses:
  ip address 1
Set clauses:
  ip next-hop 200.24.18.1
  ip next-hop 200.24.19.1
route-map RM_FOR_PBR, permit, sequence 20
Match clauses:
  ip address 2
Set clauses:
  ip next-hop 200.24.19.1
  ip next-hop 200.24.18.1
```

Check the ACL configurations to verify the packet filtering rules.

```
Device# show access-lists
ip access-list standard 1
 10 permit 200.24.16.0 0.0.0.255
 10 permit 200.24.16.0 0.0.0.255
ip access-list standard 2
 10 permit 200.24.17.0 0.0.0.255
```

Check whether the track objects are up.

```
Device#show track
Track 1
  Reliable Network Service 1
  The state is Up
    1 change, current state last: 120 secs
  Delay up 30 secs, down 50 secs
Track 2
  Reliable Network Service 2
  The state is Up
    1 change, current state last: 130 secs
  Delay up 30 secs, down 50 secs
```

6. Configuration Files

Device configuration file

```
!
ip policy redundance
!
access-list 1 permit 200.24.16.0 0.0.0.255
access-list 2 permit 200.24.17.0 0.0.0.255
!
route-map RM_FOR_PBR 10
  match ip address 1
```

```
set ip next-hop verify-availability 200.24.18.1 track 1
set ip next-hop verify-availability 200.24.19.1 track 2
!
route-map RM_FOR_PBR 20
match ip address 2
set ip next-hop verify-availability 200.24.19.1 track 2
set ip next-hop verify-availability 200.24.18.1 track 1
!
ip rns 1
icmp-echo 200.24.18.1
!
ip rns 2
icmp-echo 200.24.19.1
!
ip rns schedule 1 start-time now life forever
ip rns schedule 2 start-time now life forever
!
track 1 rns 1
!
track 2 rns 2
!
interface GigabitEthernet 0/3
ip policy route-map RM_FOR_PBR
!
```

7. Common Errors

- After matching of ACLs and prefix-lists is configured, the corresponding ACLs and prefix lists are not defined.

1.7.2 Selecting an Output Link based on Source Addresses of Packets

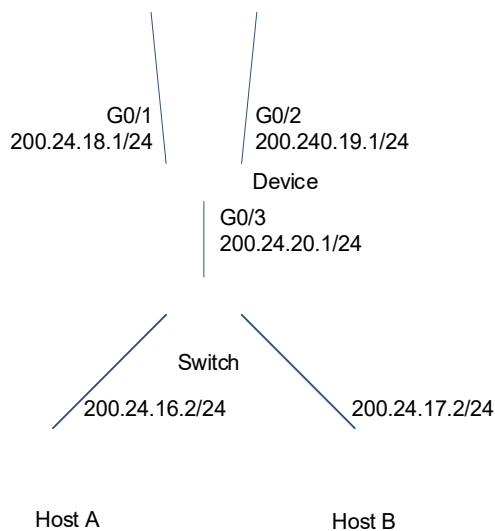
1. Requirements

This LAN has two output interfaces for connecting the Internet. The requirements are as follows:

- Route the Internet access data streams from Host A to GigabitEthernet 0/1.
- Route the Internet access data streams from Host B to GigabitEthernet 0/2.
- If the link on GigabitEthernet 0/1 is disconnected, switch over the data streams from GigabitEthernet 0/1 to GigabitEthernet 0/2. Vice versa.

2. Topology

Figure 1-1 Topology for selecting an output link based on source addresses of packets



3. Notes

- Configure a source-address-based PBR, and set the next hops for packets from the GigabitEthernet 0/3 of Host A to **GigabitEthernet 0/1** and **GigabitEthernet 0/2**. (Note the configuration sequence.)
- Configure a source-address-based PBR, and set the next hops for packets from the GigabitEthernet 0/3 of Host B to **GigabitEthernet 0/2** and **GigabitEthernet 0/1**. (Note the configuration sequence.)
- Configure a PBR to implement redundant backup among multiple next hops. (The default setting is redundant backup.)

4. Procedure

- (1) Configure basic networks, such as the interface IP address.
- (2) Select an output link based on source addresses of packets.

```
Device> enable
Device# configure terminal
Device (config)# ip policy-source in-interface gigabitEthernet 0/3 1
200.24.16.0/24 next-hop 200.24.18.1 200.24.19.1
Device (config)# ip policy-source in-interface gigabitEthernet 0/3 2
200.24.17.0/24 next-hop 200.24.19.1 200.24.18.1
Device (config)# ip policy redundance
```

5. Verification

Check the configurations of the source-address-based IPv4 PBR.

```
Device # show ip pbr source-route
PBR IPv4 Source Route
Interface      : GigabitEthernet 0/3
Sequence      : 1
Source address : 200.24.16.0/24
VRF ID        : 0
Route Flags   :
Route Type    : PBR
Direct        : Permit
Priority       : High
Match_ipaddr  : Exist
Mode          : redundance
Nexthop Count : 2
Nexthop[0]    : 200.24.18.1
Weight[0]     : 1
Ifindex[0]    : 1
Nexthop[1]    : 200.24.19.1
Weight[1]     : 1
Ifindex[1]    : 2

Interface      : GigabitEthernet 0/3
Sequence      : 2
Source address : 200.24.17.0/24
VRF ID        : 0
Route Flags   :
Route Type    : PBR
Direct        : Permit
Priority       : High
Match_ipaddr  : Exist
Mode          : redundance
Nexthop Count : 2
Nexthop[0]    : 200.24.19.1
Weight[0]     : 1
Ifindex[0]    : 2
Nexthop[1]    : 200.24.18.1
Weight[1]     : 1
Ifindex[1]    : 1
```

6. Configuration Files

Device configuration file

```
!  
ip policy-source in-interface gigabitEthernet 0/3 1 200.24.16.0/24 next-hop  
200.24.18.1 200.24.19.1  
ip policy-source in-interface gigabitEthernet 0/3 2 200.24.17.0/24 next-hop  
200.24.19.1 200.24.18.1  
ip policy redundance  
!
```