Contents

Policy-based routing commands

apply default-next-hop

Use **apply default-next-hop** to set default next hops.

Use **undo apply default-next-hop** to remove default next hops.

Syntax

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

undo apply default-next-hop [[**vpn-instance** *vpn-instance-name*] *ip-address*&<1-2>]

Default

No default next hop is set.

Views

Policy node view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. The specified VPN must already exist.

ip-address: Specifies the IP address of the default next hop. If you do not specify the **vpn-instance** *vpn-instance-name* option, the default next hop belongs to the public network.

direct: Specifies a directly connected default next hop.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

&<1-2>: Indicates that the argument before it can be entered up to two times.

Usage guidelines

You can specify multiple default next hops for backup in one command line or by executing this command multiple times.

With a default next hop specified, the **undo apply default-next-hop** command removes the default next hop.

Without any default next hop specified, the **undo apply default-next-hop** command removes all default next hops.

Examples

Set a directly-connected default next hop of 1.1.1.1.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply default-next-hop 1.1.1.1 direct
```

apply fail-action-drop next-hop

Use **apply fail-action-drop next-hop** to set the action that drops matching packets when all next hops on a policy node are invalid.

Use **undo apply fail-action-drop next-hop** to restore the default.

Syntax

apply fail-action-drop next-hop

undo apply fail-action-drop next-hop

Default

The drop action is not configured. The matching packets are forwarded based on the typical packet forwarding process if all next hops on the policy node are invalid.

Views

Policy node view

Predefined user roles

network-admin

Usage guidelines

By default, the device uses the typical packet forwarding process to route matching packets when all next hops on the policy node are unavailable. To drop the matching packets when all next hops on the policy node are unavailable, use this command. This command is typically used in scenarios that require strict routing paths.

If no next hops are specified on the policy node, this command drops all packets that match the node.

This command does not apply to software-forwarded packets.

Examples

Set next hop 1.1.1.1 on policy node 10 and configure the policy node to drop matching packets when the next hop is invalid.

```
<Sysname> system-view
[Sysname] policy-based-route policy1 permit node 10
[Sysname-pbr-policy1-10] apply next-hop 1.1.1.1
[Sysname-pbr-policy1-10] apply fail-action-drop next-hop
```

apply next-hop

Use **apply next-hop** to set next hops.

Use **undo apply next-hop** to remove next hops.

Syntax

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

undo apply next-hop [[**vpn-instance** *vpn-instance-name*] *ip-address*&<1-2>]

Default

No next hop is set.

Views

Policy node view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. The specified VPN instance must already exist.

ip-address: Specifies the IP address of the next hop. If you do not specify the **vpn-instance** *vpn-instance-name* option, the next hop belongs to the public network.

direct: Specifies that the next hop must be directly connected to take effect.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

&<1-2>: Indicates that the argument before it can be entered up to two times.

Usage guidelines

You can specify multiple next hops for backup in one command line or by executing this command multiple times.

With a next hop specified, the **undo apply next-hop** command removes the next hop.

Without any next hop specified, the **undo apply next-hop** command removes all next hops.

Examples

Set a directly-connected next hop of 1.1.1.1.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply next-hop 1.1.1.1 direct
```

apply precedence

Use **apply precedence** to set a precedence for IP packets.

Use **undo apply precedence** to restore the default.

Syntax

apply precedence { *type* | *value* }

undo apply precedence

Default

No precedence is set for IP packets.

Views

Policy node view

Predefined user roles

network-admin

Parameters

type: Specifies the precedence type for IP packets.

value: Specifies the precedence for IP packets. Eight precedence values (0 to 7) are available. Each precedence value corresponds to a precedence type, as shown in Table 1. You can set either a precedence value or a precedence type for IP packets.

Table 1 IP precedences and corresponding types

Precedence value	Precedence type
0	routine
1	priority
2	immediate
3	flash
4	flash-override

Precedence value	Precedence type
5	critical
6	internet
7	network

Examples

Set the precedence to 5 (critical) for IP packets.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply precedence critical
```

apply service-chain

Use **apply service-chain** to set the service chain information.

Use **undo apply service-chain** to restore the default.

Syntax

apply service-chain path-id *service-path-id* [**path-index** *service-path-index*]

undo apply service-chain

Default

No service chain information is set.

Views

Policy node view

Predefined user roles

network-admin

Parameters

path-id *service-path-id*: Specifies a service chain by its path ID in the range of 1 to 8388606. The path ID uniquely identifies a service chain.

path-index *service-path-index*: Specifies the path index of the node to which you are sending the matching packets. The value range for path indexes is 1 to 255. Specify this option if the destination node might receive packets from different nodes in the service chain. If the destination node receives packets only from the device, you do not need to specify this option.

Usage guidelines

For the **apply service-chain** clause to take effect, make sure you have specified a reachable next hop in the **apply next-hop** clause.

Examples

Set service chain path ID 1 and node index 10.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 5
[Sysname-pbr-aa-5] apply service-chain path-id 1 path-index 10
```

display ip policy-based-route

Use **display ip policy-based-route** to display PBR policy information.

Syntax

display ip policy-based-route [**policy** *policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy *policy-name*: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a policy, this command displays information for all PBR policies.

Examples

Display all policy information.

```
<Sysname> display ip policy-based-route
Policy name: aaa
  node 1 permit:
    if-match acl 2000
    apply next-hop 1.1.1.1
```

Table 2 Command output

Field	Description
node 1 permit	The match mode of Node 1 is **permit**.
if-match acl	Compares packets with the ACL.
apply next-hop	Specifies a next hop for permitted packets.

Related commands

policy-based-route

display ip policy-based-route egress interface

Use **display ip policy-based-route egress interface** to display the outbound PBR configuration and statistics for a VXLAN tunnel interface.

Syntax

display ip policy-based-route egress interface *interface-type interface-number* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies a VXLAN tunnel interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for the specified VXLAN tunnel interface on the master device.

Examples

Display the outbound PBR configuration and statistics for Tunnel 1.

```
<Sysname> display ip policy-based-route egress interface tunnel 1
Policy based routing information for interface Tunnel1:
Policy name: aaa
  node 0 deny:
  Matched: 0
  node 1 permit:
    if-match acl 3999
  Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 2.2.2.2
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1.1.1.1
    apply output-interface Ten-GigabitEthernet1/0/2 track 1
    apply output-interface Ten-GigabitEthernet1/0/3 track 2
  Matched: 0
Total matched: 0
```

Table 3 Command output

Field	Description
Policy based routing information for interface *xxxx*(failed)	Outbound PBR configuration and statistics for the VXLAN tunnel interface. This field displays **failed** in brackets if none of the nodes in the policy has been successfully issued to the driver. The **failed** status will persist even after the policy is successfully issued. To clear the **failed** status, you must remove the policy from the interface and then apply it on the interface again. **NOTE:** The **failed** status is available on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
node 0 deny(not support) node 2 permit(no resource)	Match mode of the node: **permit** or **deny**. If a node fails to be issued to the driver, the command displays the cause in brackets, which include: • **not support**—The device does not support the match criteria configured on the node. • **no resource**—No sufficient resources (for example, ACLs) are available for the node. **NOTE:** The cause is available only on a per-slot basis. To obtain this

Field	Description
	information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
if-match acl	Compares packets with the ACL.
apply next-hop	Specifies a next hop for permitted packets.
apply output-interface *xxxx* track 1 (down)	Specifies an output interface and its associated track entry for permitted packets. This field displays the interface status in brackets. • **down**—The interface is down at the network layer. • **inactive**—The card that hosts the interface is not in position.
Matched: 0 (no statistics resource)	Number of successful matches on the node. If the device does not have sufficient resources to count matches, this field displays **no statistics resource** in brackets. **NOTE:** The statistics collection failure cause is available only on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
Total matched	Total number of successful matches on all nodes.

Related commands

reset ip policy-based-route statistics

display ip policy-based-route interface

Use **display ip policy-based-route interface** to display interface PBR configuration and statistics.

Syntax

display ip policy-based-route interface *interface-type interface-number* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information on the master device.

Examples

Display PBR configuration and statistics on VLAN-interface 2.

```
<Sysname> display ip policy-based-route interface vlan-interface 2
Policy based routing information for interface Vlan-interface2:
Policy name: aaa
  node 0 deny:
  Matched: 0
  node 1 permit:
    if-match acl 3999
  Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 2.2.2.2
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1.1.1.1
  Matched: 0
Total matched: 0
<Sysname> display ip policy-based-route interface vlan-interface 2
Policy based routing information for interface Vlan-interface2:
Policy name: aaa
  node 0 deny:
  Matched: 0
  node 1 permit:
    if-match acl 3999
  Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 2.2.2.2
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1.1.1.1
  Matched: 0
Total matched: 0
```

Table 4 Command output

Field	Description
Policy based routing information for interface *XXXX*(failed)	PBR configuration and statistics on the interface. This field displays **failed** in brackets if none of the nodes in the policy has been successfully issued to the driver. The **failed** status will persist even after the policy is successfully issued. To clear the **failed** status, you must remove the policy from the interface and then apply it on the interface again. **NOTE:** The **failed** status is available on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command.

Field	Description
	• For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
node 0 deny(not support) node 2 permit(no resource)	Match mode of the node, **permit** or **deny**. If a node fails to be issued to the driver, the command displays the cause in brackets, which include: • **not support**—The device does not support the match criteria configured on the node. • **no resource**—No sufficient resources (for example, ACLs) are available for the node. **NOTE:** The cause is available only on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
if-match acl	Compares packets with the ACL.
apply next-hop	Specifies a next hop for permitted packets.
Matched: 0 (no statistics resource)	Number of successful matches on the node. If the device does not have sufficient resources to count matches, this field displays **no statistics resource** in brackets. **NOTE:** The statistics collection failure cause is available only on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
Total matched	Total number of successful matches on all nodes.

Related commands

reset ip policy-based-route statistics

display ip policy-based-route local

Use **display ip policy-based-route local** to display local PBR configuration and statistics.

Syntax

display ip policy-based-route local [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays local PBR configuration and statistics for the master device.

Examples

Display local PBR configuration and statistics.

```
<Sysname> display ip policy-based-route local
Policy based routing information for local:
Policy name: aaa
  node 0 deny:
  Matched: 0
  node 1 permit:
    if-match acl 3999
  Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 2.2.2.2
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1.1.1.1
  Matched: 0
Total matched: 0
```

Table 5 Command output

Field	Description
Policy based routing information for local	Local PBR configuration and statistics.
node 0 deny/node 2 permit	Match mode of the node: permit or deny.
if-match acl	Compares packets with the ACL.
apply next-hop	Specifies a next hop for permitted packets.
Matched: 0	Number of successful matches on the node.
Total matched	Total number of successful matches on all nodes.

Related commands

reset ip policy-based-route statistics

display ip policy-based-route setup

Use **display ip policy-based-route setup** to display PBR configuration.

Syntax

display ip policy-based-route setup

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display PBR configuration.

```
<Sysname> display ip policy-based-route setup
Policy name             Type     Interface
pr01                    Forward  Vlan-interface2
aaa                     Egress   Tunnel1
aaa                     Local    N/A
```

Table 6 Command output

Field	Description
Type	Type of the PBR: • **Forward**—Interface PBR. • **Egress**—Outbound PBR. • **Local**—Local PBR.
Interface	Interface where the policy is applied.

Related commands

ip policy-based-route

if-match acl

Use **if-match acl** to set an ACL match criterion.

Use **undo if-match acl** to restore the default.

Syntax

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

undo if-match acl

Default

No ACL match criterion is set.

Views

Policy node view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number in the range of 2000 to 2999 for a basic ACL, and in the range of 3000 to 3999 for an advanced ACL.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters starting with letter *a* to *z* or *A* to *Z*. The ACL name cannot be **all**.

Examples

Configure Node 11 of policy **aa** to permit the packets matching ACL 2011.

```
<Sysname> system-view
```

```
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] if-match acl 2011
```

Configure Node 11 of policy **aa** to permit the packets matching ACL **aaa**.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] if-match acl name aaa
```

if-match service-chain

Use **if-match service-chain** to set a service chain match criterion.

Use **undo if-match service-chain** to restore the default.

Syntax

if-match service-chain { **path-id** *service-path-id* [**path-index** *service-path-index*] }&<1-2>

undo if-match service-chain [**path-id** *service-path-id*]&<1-2>]

Default

No service chain match criteria are set.

Views

Policy node view

Predefined user roles

network-admin

Parameters

path-id *service-path-id*: Specifies a service chain by its path ID in the range of 1 to 8388606. The path ID uniquely identifies a service chain.

path-index *service-path-index*: Specifies a node in the service chain by its index to match packets sent from that node. The value range for path indexes is 1 to 255. Specify this option if the device might receive packets from different nodes in the service chain. If only one node in the service chain sends packets to the device, you do not need to specify this option.

&<1-2>: Indicates that the argument before it can be entered up to two times

Examples

Set a service chain match criterion to match packets with service chain path ID 1 and node index 10.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 5
[Sysname-pbr-aa-5] apply service-chain path-id 1 path-index 10
```

if-match vxlan-id

Use **if-match vxlan-id** to set a VXLAN match criterion

Use **undo if-match vxlan-id** to restore the default.

Syntax

if-match vxlan-id *vxlan-id*

undo if-match vxlan-id

Default

No VXLAN match criterion is set.

Views

Policy node view

Predefined user roles

network-admin

Parameters

vxlan-id: Specifies a VXLAN ID in the range of 0 to 16777215.

Examples

Configure Node 11 of policy **aaa** to permit packets with the VXLAN ID 1000.

```
<Sysname> system-view
[Sysname] policy-based-route aaa permit node 11
[Sysname-pbr-aaa-11] if-match vxlan-id 1000
```

ip local policy-based-route

Use **ip local policy-based-route** to specify a policy for local PBR.

Use **undo ip local policy-based-route** to restore the default.

Syntax

ip local policy-based-route *policy-name*

undo ip local policy-based-route

Default

No policy is referenced for local PBR.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. The specified policy must already exist.

Usage guidelines

Local PBR guides the forwarding of locally generated packets, such as ICMP packets generated by using the **ping** command.

Local PBR might affect local services, such as ping and Telnet. When you use local PBR, make sure you fully understand its impact on local services of the device.

You can specify only one policy for local PBR and must make sure the specified policy already exists.

Before you apply a new policy, you must first remove the current policy.

Examples

Configure local PBR based on policy **aaa**.

```
<Sysname> system-view
[Sysname] ip local policy-based-route aaa
```

Related commands

display ip policy-based-route setup

policy-based-route

ip policy-based-route

Use **ip policy-based-route** to specify a policy for interface PBR on an interface.

Use **undo ip policy-based-route** to restore the default.

Syntax

ip policy-based-route *policy-name*

undo ip policy-based-route

Default

No policy is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. The specified policy must already exist.

Usage guidelines

You can apply only one policy to an interface. Before you apply a new policy, you must first remove the current policy from the interface.

Examples

Apply policy **aaa** to VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip policy-based-route aaa
```

Related commands

display ip policy-based-route setup

policy-based-route

ip policy-based-route egress

Use **ip policy-based-route egress** to specify a policy for outbound PBR on a VXLAN tunnel interface.

Use **undo ip policy-based-route egress** to restore the default.

Syntax

ip policy-based-route *policy-name* **egress**

undo ip policy-based-route egress

Default

No policy is specified for outbound PBR on a VXLAN tunnel interface.

Views

VXLAN tunnel interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. The specified policy must already exist.

Examples

Apply policy **aaa** to Tunnel 1.

```
<Sysname> system-view
[Sysname] interface Tunnel 1 mode vxlan
[Sysname-Tunnel1] ip policy-based-route aaa egress
```

policy-based-route

Use **policy-based-route** to create a policy node and enter its view, or enter the view of an existing policy node.

Use **undo policy-based-route** to delete a policy or policy node.

Syntax

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

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

Default

No policy nodes exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters.

deny: Specifies the match mode for the policy node as **deny**.

permit: Specifies the match mode for the policy node as **permit** (default mode).

node *node-number*: Specifies a policy node by its number. A smaller number has a higher priority. The value range for the *node-number* argument is 0 to 255.

Usage guidelines

A policy that has been applied to an interface or locally cannot be deleted. To delete it, you must first cancel the application.

- If a policy node is specified, the **undo policy-based-route** command deletes the specified policy node.
- If a match mode is specified, the command deletes all nodes configured with the match mode.
- If no policy node or match mode is specified, the command deletes the whole policy.

Examples

Create permit-mode of Node 10 for policy **policy1** and enter its view.

```
<Sysname> system-view
[Sysname] policy-based-route policy1 permit node 10
[Sysname-pbr-policy1-10]
```

Related commands

display ip policy-based-route

reset ip policy-based-route statistics

Use **reset ip policy-based-route statistics** to clear PBR statistics.

Syntax

reset ip policy-based-route statistics [**policy** *policy-name*]

Views

User view

Predefined user roles

network-admin

Parameters

policy *policy-name*: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a policy, this command clears PBR statistics for all policies.

Examples

Clear all PBR statistics.

```
<Sysname> reset ip policy-based-route statistics
```

Related commands

display ip policy-based-route egress interface

display ip policy-based-route interface

display ip policy-based-route local