



## Service Redirection in VXLAN Fabrics

---

This chapter contains the following sections:

- [Service Redirection in VXLAN EVPN Fabrics, on page 1](#)
- [Guidelines and Limitations for Policy-Based Redirect, on page 1](#)
- [Enabling the Policy-Based Redirect Feature, on page 2](#)
- [Configuring a Route Policy, on page 3](#)
- [Verifying the Policy-Based Redirect Configuration, on page 4](#)
- [Configuration Example for Policy-Based Redirect, on page 4](#)

## Service Redirection in VXLAN EVPN Fabrics

Today, insertion of service appliances (also referred to as service nodes or service endpoints) such as firewalls, load-balancers, etc are needed to secure and optimize applications within a data center. This section describes the Layer 4-Layer 7 service insertion and redirection features offered on VXLAN EVPN fabrics that provides sophisticated mechanisms to onboard and selectively redirect traffic to these services.

## Guidelines and Limitations for Policy-Based Redirect

The following guidelines and limitations apply to PBR over VXLAN.

- The following platforms support PBR over VXLAN:
  - Cisco Nexus 9332C and 9364C switches
  - Cisco Nexus 9300-EX switches
  - Cisco Nexus 9300-FX/FX2/FX3 switches
  - Cisco Nexus 9300-GX switches
  - Cisco Nexus 9300-GX2 switches
  - Cisco Nexus 9504 and 9508 switches with -EX/FX line cards
- Beginning with Cisco NX-OS Release 10.2(3)F, the VXLAN PBR feature is supported with VXLANv6 on all TOR switches.

- PBR over VXLAN doesn't support the following features: VTEP ECMP, and the **load-share** keyword in the **set {ip | ipv6} next-hop ip-address** command.

## Enabling the Policy-Based Redirect Feature

To configure basic PBR, in cases where the advanced (and recommended) ePBR functions are not deployed, see the following sections:

- [Enabling the Policy-Based Redirect Feature, on page 2](#)
- [Configuring a Route Policy, on page 3](#)
- [Verifying the Policy-Based Redirect Configuration, on page 4](#)
- [Configuration Example for Policy-Based Redirect, on page 4](#)

### Before you begin

Enable the policy-based redirect feature before you can configure a route policy.

### SUMMARY STEPS

1. **configure terminal**
2. **[no] feature pbr**
3. (Optional) **show feature**
4. (Optional) **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>[no] feature pbr</b> <b>Example:</b> switch(config)# <b>feature pbr</b>	Enables the policy-based routing feature.
<b>Step 3</b>	(Optional) <b>show feature</b> <b>Example:</b> switch(config)# <b>show feature</b>	Displays enabled and disabled features.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config)# <b>copy running-config startup-config</b>	Saves this configuration change.

# Configuring a Route Policy

You can use route maps in policy-based routing to assign routing policies to the inbound interface. Cisco NX-OS routes the packets when it finds a next hop and an interface.



**Note** The switch has a RAACL TCAM region by default for IPv4 traffic.

## Before you begin

Configure the RAACL TCAM region (using TCAM carving) before you apply the policy-based routing policy. For instructions, see the “Configuring ACL TCAM Region Sizes” section in the [Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.2\(x\)](#).

## SUMMARY STEPS

1. **configure terminal**
2. **interface** *type slot/port*
3. **{ip | ipv6} policy route-map** *map-name*
4. **route-map** *map-name* [**permit** | **deny**] [*seq*]
5. **match {ip | ipv6} address access-list-name** *name* [*name...*]
6. **set ip next-hop** *address1*
7. **set ipv6 next-hop** *address1*
8. (Optional) **set interface null0**
9. (Optional) **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>interface</b> <i>type slot/port</i> <b>Example:</b> switch(config)# <b>interface ethernet 1/2</b>	Enters interface configuration mode.
Step 3	<b>{ip   ipv6} policy route-map</b> <i>map-name</i> <b>Example:</b> switch(config-inf)# <b>ip policy route-map Testmap</b>	Assigns a route map for IPv4 or IPv6 policy-based routing to the interface.
Step 4	<b>route-map</b> <i>map-name</i> [ <b>permit</b>   <b>deny</b> ] [ <i>seq</i> ] <b>Example:</b> switch(config-inf)# <b>route-map Testmap</b>	Creates a route map or enters route-map configuration mode for an existing route map. Use <i>seq</i> to order the entries in a route map.

	Command or Action	Purpose
<b>Step 5</b>	<b>match {ip   ipv6} address access-list-name name [name...]</b> <b>Example:</b> switch(config-route-map) # <b>match ip address access-list-name ACL1</b>	Matches an IPv4 or IPv6 address against one or more IPv4 or IPv6 access control lists (ACLs). This command is used for policy-based routing and is ignored by route filtering or redistribution.
<b>Step 6</b>	<b>set ip next-hop address1</b> <b>Example:</b> switch(config-route-map) # <b>set ip next-hop 192.0.2.1</b>	Sets the IPv4 next-hop address for policy-based routing.
<b>Step 7</b>	<b>set ipv6 next-hop address1</b> <b>Example:</b> switch(config-route-map) # <b>set ipv6 next-hop 2001:0DB8::1</b>	Sets the IPv6 next-hop address for policy-based routing.
<b>Step 8</b>	(Optional) <b>set interface null0</b> <b>Example:</b> switch(config-route-map) # <b>set interface null0</b>	Sets the interface that is used for routing. Use the <b>null0</b> interface to drop packets.
<b>Step 9</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config-route-map) # <b>copy running-config startup-config</b>	Saves this configuration change.

## Verifying the Policy-Based Redirect Configuration

To display the policy-based redirect configuration information, perform one of the following tasks:

Command	Purpose
<b>show [ip   ipv6] policy [name]</b>	Displays information about an IPv4 or IPv6 policy.
<b>show route-map [name] pbr-statistics</b>	Displays policy statistics.

Use the **route-map map-name pbr-statistics** command to enable policy statistics. Use the **clear route-map map-name pbr-statistics** command to clear these policy statistics.

## Configuration Example for Policy-Based Redirect

Perform the following configuration on all tenant VTEPs, excluding the service VTEP.

```
feature pbr

ipv6 access-list IPV6_App_group_1
10 permit ipv6 any 2001:10:1:1::0/64

ip access-list IPV4_App_group_1
10 permit ip any 10.1.1.0/24
```

```

ipv6 access-list IPV6_App_group_2
10 permit ipv6 any 2001:20:1:1::0/64

ip access-list IPV4_App_group_2
10 permit ip any 20.1.1.0/24

route-map IPV6_PBR_Appgroup1 permit 10
  match ipv6 address IPV6_App_group_2
  set ipv6 next-hop 2001:100:1:1::20 (next hop is that of the firewall)

route-map IPV4_PBR_Appgroup1 permit 10
  match ip address IPV4_App_group_2
  set ip next-hop 10.100.1.20 (next hop is that of the firewall)

route-map IPV6_PBR_Appgroup2 permit 10
  match ipv6 address IPV6_App_group1
  set ipv6 next-hop 2001:100:1:1::20 (next hop is that of the firewall)

route-map IPV4_PBR_Appgroup2 permit 10
  match ip address IPV4_App_group_1
  set ip next-hop 10.100.1.20 (next hop is that of the firewall)

```

```

interface Vlan10
! tenant SVI appgroup 1
vrf member appgroup
  ip address 10.1.1.1/24
  no ip redirect
  ipv6 address 2001:10:1:1::1/64
  no ipv6 redirects
  fabric forwarding mode anycast-gateway
ip policy route-map IPV4_PBR_Appgroup1
ipv6 policy route-map IPV6_PBR_Appgroup1
interface Vlan20
! tenant SVI appgroup 2
vrf member appgroup
  ip address 20.1.1.1/24
  no ip redirect
  ipv6 address 2001:20:1:1::1/64
  no ipv6 redirects
  fabric forwarding mode anycast-gateway
ip policy route-map IPV4_PBR_Appgroup2
ipv6 policy route-map IPV6_PBR_Appgroup2

```

On the service VTEP, the PBR policy is applied on the tenant VRF SVI. This ensures the traffic post decapsulation will be redirected to firewall.  
feature pbr

```

ipv6 access-list IPV6_App_group_1
10 permit ipv6 any 2001:10:1:1::0/64

ip access-list IPV4_App_group_1
10 permit ip any 10.1.1.0/24

ipv6 access-list IPV6_App_group_2
10 permit ipv6 any 2001:20:1:1::0/64

ip access-list IPV4_App_group_2
10 permit ip any 20.1.1.0/24

route-map IPV6_PBR_Appgroup1 permit 10
  match ipv6 address IPV6_App_group_2
  set ipv6 next-hop 2001:100:1:1::20 (next hop is that of the firewall)

```

```
route-map IPV6_PBR_Appgroup permit 20
  match ipv6 address IPV6_App_group1
  set ipv6 next-hop 2001:100:1:1::20 (next hop is that of the firewall)

route-map IPV4_PBR_Appgroup permit 10
  match ip address IPV4_App_group_2
  set ip next-hop 10.100.1.20 (next hop is that of the firewall)

route-map IPV4_PBR_Appgroup permit 20
  match ip address IPV4_App_group_1
  set ip next-hop 10.100.1.20 (next hop is that of the firewall)

interface vlan1000
!L3VNI SVI for Tenant VRF
vrf member appgroup
ip forward
ipv6 forward
ipv6 ipv6 address use-link-local-only
ip policy route-map IPV4_PBR_Appgroup
ipv6 policy route-map IPV6_PBR_Appgroup
```