IP Routing: Protocol-Independent Configuration Guide, Cisco IOS Release 15E

First Published: August 26, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

PBR Recursive Next Hop

The PBR Recursive Next Hop feature enhances route maps to enable configuration of a recursive next-hop IP address that is used by policy-based routing (PBR). The recursive next-hop IP address is installed in the routing table and can be a subnet that is not directly connected. If the recursive next-hop IP address is not available, packets are routed using a default route.

Because Cisco Express Forwarding (CEF) or process switching provides the infrastructure, the benefit of this feature is the CEF loadsharing.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for PBR Recursive Next Hop

If there are multiple equal-cost routes to the subnet that have been configured by the **set next-hop recursive** command, load balancing will occur only if all the adjacencies to the routes are resolved. If any of the adjacencies have not been resolved, load balancing will not occur and only one of the routes whose adjacency is resolved will be used. If none of the adjacencies are resolved, then the packets will be processed, resulting in the resolution of at least one of the adjacencies, leading to the programming of the adjacency in the hardware. Policy based routing relies on routing protocols or other means to resolve all adjacencies and as a result, load balancing occurs.

PBR Recursive Next Hope for IPv6 does not support load sharing.

Information About PBR Recursive Next-Hop

PBR Recursive Next Hop Overview

The PBR Recursive Next Hop feature enhances route maps to enable configuration of a recursive next-hop IP address that is used by policy-based routing (PBR). The recursive next-hop IP address is installed in the routing table and can be a subnet that is not directly connected. If the recursive next-hop IP address is not available, packets are routed using a default route.

PBR Recursive Next Hop for IPv6 also supports non-directly connected next hop. The recursive next hop specified can be a host address or a subnet address. The routing table is looked up to get the next hop based on the longest match of addresses. Only one such recursive next hop is supported per route map entry.

How to Configure PBR Recursive Next Hop

Setting the Recursive Next-Hop IP Address

The infrastructure provided by CEF or process switching performs the recursion to the next-hop IP address. The configuration sequence, which affects routing, is as follows:

1. Next-hop
2. Next-hop recursive
3. Interface
4. Default next-hop
5. Default interface

If both a next-hop address and a recursive next-hop IP address are present in the same route-map entry, the next hop is used. If the next hop is not available, the recursive next hop is used. If the recursive next hop is not available and no other IP address is present, the packet is routed using the default routing table; it is not dropped. If the packet is supposed to be dropped, use the **set ip next-hop**command with the **recursive** keyword, followed by a **set interface null0** configuration.

Perform this task to set the IP address for the recursive next-hop router.

Before You Begin

If loadsharing is required, CEF loadsharing should be configured for per-packet or per-destination loadsharing. Loadbalancing should be done over all equal-cost routes to the subnet that has been configured by the **set ip next-hop recursive**command.

This functionality should be available in centralized and distributed systems.

Note Only one recursive next-hop IP address is supported per route-map entry.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} *source*[*source-wildcard*] [**log**]
4. **route-map** *map-tag*
5. Do one of the following:
   - **set ip next-hop** *ip-address*
   - **set ipv6 next-hop** *ip-address*
6. Do one of the following:
   - **set ip next-hop** {*ip-address* [*...ip-address*] | **recursive** *ip-address*}
   - **set ipv6 next-hop** {*ipv6-address* [*...ipv6-address*] | **recursive** *ipv6-address*}
7. Do one of the following:
   - **match ip address** *access-list-number*
   - **match ipv6 address** {**prefix-list** *prefix-list-name* |*access-list-name*}
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**access-list** *access-list-number* {**deny** | **permit**} *source*[*source-wildcard*] [**log**] **Example:** `Router(config)# access-list 101 permit 10.60.0.0 0.0.255.255`	Configures an access list. The example configuration permits any source IP address that falls within the 10.60.0.0. 0.0.255.255 subnet.
Step 4	**route-map** *map-tag* **Example:** `Router(config)# route-map abccomp`	Enables policy routing and enters route-map configuration mode.

Step 5	Do one of the following:
	• **set ip next-hop** *ip-address*
	• **set ipv6 next-hop** *ip-address*
	
	Example:
	
	`Router(config-route-map)# set ip next-hop 10.10.1.1`
	
	Example:
	`Router(config-route-map)# set ipv6 next-hop 2001:DB8:2003:1::95`
		Sets a next-hop router IPv4 or IPv6 address.
		
		Note Set this IPv4/IPv6 address separately from the next-hop recursive router configuration.

Step 6	Do one of the following:
	• **set ip next-hop** {*ip-address* [*...ip-address*] | **recursive** *ip-address*}
	• **set ipv6 next-hop** {*ipv6-address* [*...ipv6-address*] | **recursive** *ipv6-address*}
	
	Example:
	
	`Router(config-route-map)# set ip next-hop recursive 10.20.3.3`
	
	Example:
	`Router(config-route-map)# set ipv6 next-hop recursive 2001:DB8:2003:2::95`
		Sets a recursive next-hop IPv4/IPv6 address.
		
		Note This configuration does not ensure that packets get routed using the recursive IP address if an intermediate IP address is a shorter route to the destination.

Step 7	Do one of the following: • **match ip address** *access-list-number*	Sets an access list to be matched.

	Command or Action	Purpose

	• **match ipv6 address** {**prefix-list** *prefix-list-name* |*access-list-name*}
	
	Example:
	`Router(config-route-map)# match ip address 101`
	
	Example:
	`Router(config-route-map)# match ipv6 address kmd`	

Step 8	**end** **Example:** `Router(config-route-map)# end`	Exits route-map configuration mode and returns to privileged EXEC mode.

Verifying the Recursive Next-Hop Configuration

To verify the recursive next-hop configuration, perform the following steps.

SUMMARY STEPS

1. **show running-config | begin abccomp**
2. **show route-map** *map-name*

DETAILED STEPS

Step 1 **show running-config | begin abccomp**

Use this command to verify the IPv4/IPv6 addresses for a next-hop and recursive next-hop IPv4/IPv6 address as listed in the following examples:

Example:

```
Router# show running-config | begin abccomp
route-map abccomp permit 10
 match ip address 101 ! Defines the match criteria for an access list.
 set ip next-hop recursive 10.3.3.3 ! If the match criteria are met, the recursive IP  address is
set.
 set ip next-hop 10.1.1.1 10.2.2.2 10.4.4.4

Router# show running-config | begin abccomp
route-map abccomp permit 10
 match ip address kmd! Defines the match criteria for an access list.
 set ipv6 next-hop recursive 2001:DB8:3000:1 ! If the match criteria are met, the recursive IPv6
```

```
address is set.
 set ipv6 next-hop 2001:DB8:3000:1 2001:DB8:4000:1 2001:DB8:5000:1
```

Step 2 **show route-map** *map-name*

Use this command to display the route maps, for example:

Example:

```
Router# show route-map abccomp
route-map abccomp, permit, sequence 10
 Match clauses:
  ip address (access-lists): 101
 Set clauses:
  ip next-hop recursive 10.3.3.3
  ip next-hop 10.1.1.1 10.2.2.2 10.4.4.4
 Policy routing matches: 0 packets, 0 bytes

Router# show route-map abccomp
route-map abccomp, permit, sequence 10
 Match clauses:
  ipv6 address (access-lists): kmd
 Set clauses:
  ipv6 next-hop recursive 2001:DB8:3000:1
  ipv6 next-hop 2001:DB8:3000:1 2001:DB8:4000:1 2001:DB8:5000:1
 Policy routing matches: 0 packets, 0 bytes
```

Configuration Examples for PBR Recursive Next Hop

Example: Recursive Next-Hop IP Address

The following example shows the configuration of IP address 10.3.3.3 as the recursive next-hop router:

```
route-map abccomp
 set ip next-hop 10.1.1.1
 set ip next-hop 10.2.2.2
 set ip next-hop recursive 10.3.3.3
 set ip next-hop 10.4.4.4
```

The following example shows the configuration of IPv6 address 2001:DB8:2003:1::95 as the recursive next-hop router:

```
route-map abccomp
 set ipv6 next-hop 2001:DB8:2003:1::95
 set ipv6 next-hop 2001:DB8:2004:3::96
 set ipv6 next-hop recursive 2001:DB8:2005:2::95
 set ipv6 next-hop 2001:DB8:2006:1::95
```

Additional References for PBR Recursive Next Hop

Related Documents

Related Topic	Document Title
Cisco IOS master command list, all releases	Cisco IOS Master Command List, All Releases
IP routing protocol-independent commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS IP Routing: Protocol-Independent Command Reference
Performing basic system management	*Basic System Management Configuration Guide*
Changing the maximum number of paths	"BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN" module in the *BGP Configuration Guide*
BGP route map configuration tasks and configuration examples.	"Connecting to a Service Provider Using External BGP" module in the *BGP Configuration Guide*
BGP communities and route maps.	"BGP Cost Community" module in the *BGP Configuration Guide*
IPv6 Policy-Based Routing	"IPv6 Policy-Based Routing " module in the *IP Routing: Protocol-Independent Configuration Guide*

RFCs

RFC	Title
RFC 791	*Internet Protocol*
RFC 1219	*Variable-Length Subnet Masks*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for PBR Recursive Next Hop

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for PBR Recursive Next Hop

Feature Name	Releases	Feature Information
PBR Recursive Next Hop	15.2(2)E	The PBR Recursive Next Hop feature enhances route maps to enable configuration of a recursive next-hop IP address that is used by policy-based routing (PBR). In Cisco IOS Release 15.2(2)E, this feature was supported on the following platforms: • Catalyst 3750-X Series Switches • Catalyst 2960-S Series Switches • Catalyst 2960-X Series Switches • Catalyst 2960-XR Series Switches No new commands were introduced or modified.

CHAPTER 2

IPv6 Policy-Based Routing

Policy-based routing (PBR) in both IPv6 and IPv4 allows a user to manually configure how received packets should be routed. PBR allows the user to identify packets by using several attributes and to specify the next hop or the output interface to which the packet should be sent. PBR also provides a basic packet-marking capability.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IPv6 Policy-Based Routing

Policy-Based Routing Overview

Policy-based routing (PBR) gives you a flexible means of routing packets by allowing you to configure a defined policy for traffic flows, which lessens reliance on routes derived from routing protocols. Therefore, PBR gives you more control over routing by extending and complementing the existing mechanisms provided by routing protocols. PBR allows you to set the IPv6 precedence. For a simple policy, you can use any one of these tasks; for a complex policy, you can use all of them. It also allows you to specify a path for certain traffic, such as priority traffic over a high-cost link.

PBR for IPv6 may be applied to both forwarded and originated IPv6 packets. For forwarded packets, PBR for IPv6 will be implemented as an IPv6 input interface feature, supported in the following forwarding paths:

- Process
- Cisco Express Forwarding (formerly known as CEF)
- Distributed Cisco Express Forwarding

Policies can be based on the IPv6 address, port numbers, protocols, or packet size.

PBR allows you to perform the following tasks:

- Classify traffic based on extended access list criteria. Access lists, then, establish the match criteria.
- Set IPv6 precedence bits, giving the network the ability to enable differentiated classes of service.
- Route packets to specific traffic-engineered paths; you might need to route them to allow a specific quality of service (QoS) through the network.

PBR allows you to classify and mark packets at the edge of the network. PBR marks a packet by setting precedence value. The precedence value can be used directly by devices in the network core to apply the appropriate QoS to a packet, which keeps packet classification at your network edge.

How Policy-Based Routing Works

All packets received on an interface with policy-based routing (PBR) enabled are passed through enhanced packet filters called route maps. The route maps used by PBR dictate the policy, determining where to forward packets.

Route maps are composed of statements. The route map statements can be marked as permit or deny, and they are interpreted in the following ways:

- If a packet matches all match statements for a route map that is marked as permit, the device attempts to policy route the packet using the set statements. Otherwise, the packet is forwarded normally.
- If the packet matches any match statements for a route map that is marked as deny, the packet is not subject to PBR and is forwarded normally.
- If the statement is marked as permit and the packets do not match any route map statements, the packets are sent back through normal forwarding channels and destination-based routing is performed.

You must configure policy-based routing (PBR) on the interface that receives the packet, and not on the interface from which the packet is sent.

Packet Matching

Policy-based routing (PBR) for IPv6 will match packets using the **match ipv6 address** command in the associated PBR route map. Packet match criteria are those criteria supported by IPv6 access lists, as follows:

- Input interface

- Source IPv6 address (standard or extended access control list [ACL])
- Destination IPv6 address (standard or extended ACL)
- Protocol (extended ACL)
- Source port and destination port (extended ACL)
- DSCP (extended ACL)
- Flow-label (extended ACL)
- Fragment (extended ACL)

Packets may also be matched by length using the **match length** command in the PBR route map.

Match statements are evaluated first by the criteria specified in the **match ipv6 address** command and then by the criteria specified in the **match length** command. Therefore, if both an ACL and a length statement are used, a packet will first be subject to an ACL match. Only packets that pass the ACL match will be subject to the length match. Finally, only packets that pass both the ACL and the length statement will be policy routed.

Packet Forwarding Using Set Statements

Policy-based routing (PBR) for IPv6 packet forwarding is controlled by using a number of set statements in the PBR route map. These set statements are evaluated individually in the order shown, and PBR will attempt to forward the packet using each of the set statements in turn. PBR evaluates each set statement individually, without reference to any prior or subsequent set statement.

You may set multiple forwarding statements in the PBR for IPv6 route map. The following set statements may be specified:

- IPv6 next hop. The next hop to which the packet should be sent. The next hop must be present in the Routing Information Base (RIB), it must be directly connected, and it must be a global IPv6 address. If the next hop is invalid, the set statement is ignored.
- Output interface. A packet is forwarded out of a specified interface. An entry for the packet destination address must exist in the IPv6 RIB, and the specified output interface must be in the set path. If the interface is invalid, the statement is ignored.
- Default IPv6 next hop. The next hop to which the packet should be sent. It must be a global IPv6 address. This set statement is used only when there is no explicit entry for the packet destination in the IPv6 RIB.
- Default output interface. The packet is forwarded out of a specified interface. This set statement is used only when there is no explicit entry for the packet destination in the IPv6 RIB.

Note The order in which PBR evaluates the set statements is the order in which they are listed above. This order may differ from the order in which route-map set statements are listed by **show** commands.

When to Use Policy-Based Routing

Policy-based routing (PBR) can be used if you want certain packets to be routed some way other than the obvious shortest path. For example, PBR can be used to provide the following functionality:

- Equal access
- Protocol-sensitive routing
- Source-sensitive routing
- Routing based on interactive traffic versus batch traffic
- Routing based on dedicated links

Some applications or traffic can benefit from Quality of Service (QoS)-specific routing; for example, you could transfer stock records to a corporate office on a higher-bandwidth, higher-cost link for a short time while sending routine application data such as e-mail over a lower-bandwidth, lower-cost link.

How to Enable IPv6 Policy-Based Routing

Enabling PBR on an Interface

To enable PBR for IPv6, create a route map that specifies the packet match criteria and the desired policy-route action. Then, associate the route map on the required interface. All packets arriving on the specified interface that match the match clauses will be subject to PBR.

Depending on your release, IPv6 PBR allows users to override normal destination IPv6 address-based routing and forwarding results. VPN routing and forwarding (VRF) allows multiple routing instances in Cisco software. The PBR feature is VRF-aware, which means that it works under multiple routing instances, beyond the default or global routing table.

In PBR, the **set vrf** command decouples the VRF and interface association and allows the selection of a VRF based on ACL-based classification using existing PBR or route-map configurations. PBR, through the **set vrf** command, provides a single device with multiple routing tables and the ability to select routes based on ACL classification. The device classifies packets based on ACL, selects a routing table, looks up the destination address, and then routes the packet.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
4. Enter one of the following commands:
    - **match length** *minimum-length maximum-length*
    - **match ipv6 address** {**prefix-list** *prefix-list-name* | *access-list-name*}
5. Enter one of the following commands:
    - **set ipv6 precedence** *precedence-value*
    - **set ipv6 next-hop** *global-ipv6-address* [*global-ipv6-address...*]
    - **set interface** *type number* [*...type number*]
    - **set ipv6 default next-hop** *global-ipv6-address* [*global-ipv6-address...*]
    - **set default interface** *type number* [*...type number*]
    - **set vrf** *vrf-name*
6. **exit**
7. **interface** *type number*
8. **ipv6 policy route-map** *route-map-name*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **Example:** `Device(config)# route-map rip-to-ospf permit`	Enters route-map configuration mode and defines conditions for redistributing routes from one routing protocol into another or enables policy routing.
Step 4	Enter one of the following commands:	Specifies the match criteria.

	Command or Action	Purpose

	• **match length** *minimum-length maximum-length*
	• **match ipv6 address** {**prefix-list** *prefix-list-name* | *access-list-name*}
	
	Example:
	`Device(config-route-map)# match length 3 200`
	`Device(config-route-map)# match ipv6 address marketing`
		• You can specify any or all of the following:
		  • Match the Level 3 length of the packet.
		  • Match a specified IPv6 access list.
		  • If you do not specify a **match** command, the route map applies to all packets.

Step 5	Enter one of the following commands:
	• **set ipv6 precedence** *precedence-value*
	• **set ipv6 next-hop** *global-ipv6-address* [*global-ipv6-address...*]
	• **set interface** *type number* [*...type number*]
	• **set ipv6 default next-hop** *global-ipv6-address* [*global-ipv6-address...*]
	• **set default interface** *type number* [*...type number*]
	• **set vrf** *vrf-name*
	
	Example:
	`Device(config-route-map)# set ipv6 precedence 1`
	`Device(config-route-map)# set ipv6 next-hop 2001:DB8:2003:1::95`
	`Device(config-route-map)# set interface serial 0/0`
	`Device(config-route-map)# set ipv6 default next-hop 2001:DB8:2003:1::95`
	`Device(config-route-map)# set default interface ethernet 0`
	`Device(config-route-map)# set vrf vrfname`
		Specifies the action or actions to be taken on the packets that match the criteria.
		• You can specify any or all of the following actions:
		  • Set the precedence value in the IPv6 header.
		  • Set the next hop for the packet (the next hop must be an adjacent device).
		  • Set output interface for the packet.
		  • Set the next hop for the packet, if there is no explicit route for this destination.
		  • Set the output interface for the packet, if there is no explicit route for this destination.
		  • Set VRF instance selection within a route map for a policy-based routing VRF selection.

Step 6	**exit** **Example:** `Device(config-route-map)# exit`	Returns to global configuration mode.
Step 7	**interface** *type number* **Example:** `Device(config)# interface FastEthernet 1/0`	Specifies an interface type and number and enters interface configuration mode.

	Command or Action	Purpose
Step 8	**ipv6 policy route-map** *route-map-name* **Example:** `Device(config-if)# ipv6 policy-route-map interactive`	Identifies a route map to be used for IPv6 PBR on an interface.
Step 9	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Enabling Local PBR for IPv6

Packets that are generated by the device are not normally policy routed. Perform this task to enable local IPv6 policy-based routing (PBR) for such packets, indicating which route map the device should use.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 local policy route-map** *route-map-name*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ipv6 local policy route-map** *route-map-name* **Example:** `Device(config)# ipv6 local policy route-map pbr-src-90`	Configures IPv6 PBR for packets generated by the device.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Verifying the Configuration and Operation of PBR for IPv6

SUMMARY STEPS

1. **enable**
2. **show ipv6 policy**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ipv6 policy** **Example:** `Device# show ipv6 policy`	Displays IPv6 policy routing packet activity.

Troubleshooting PBR for IPv6

Policy routing analyzes various parts of the packet and then routes the packet based on certain user-defined attributes in the packet.

SUMMARY STEPS

1. **enable**
2. **show route-map** [*map-name* | **dynamic** [*dynamic-map-name* | **application** [*application-name*]] | **all**] [**detailed**]
3. **debug ipv6 policy** [*access-list-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show route-map** [*map-name* | **dynamic** [*dynamic-map-name* | **application** [*application-name*]] | **all**] [**detailed**] **Example:** `Device# show route-map`	Displays all route maps configured or only the one specified.
Step 3	**debug ipv6 policy** [*access-list-name*] **Example:** `Device# debug ipv6 policy`	Enables debugging of the IPv6 policy routing packet activity.

Configuration Examples for IPv6 Policy-Based Routing

Example: Enabling PBR on an Interface

In the following example, a route map named pbr-dest-1 is created and configured. The route map specifies the packet match criteria and the desired policy-route action. PBR is then enabled on Ethernet interface 0/0.

```
ipv6 access-list match-dest-1
  permit ipv6 any 2001:DB8:2001:1760::/32
route-map pbr-dest-1 permit 10
  match ipv6 address match-dest-1
  set interface serial 0/0
interface Ethernet0/0
  ipv6 policy route-map interactive
```

Example: Enabling Local PBR for IPv6

In the following example, packets with a destination IPv6 address that match the IPv6 address range allowed by access list pbr-src-90 are sent to the device at IPv6 address 2001:DB8:2003:1::95:

```
ipv6 access-list src-90
  permit ipv6 host 2001:DB8:2003::90 2001:DB8:2001:1000::/64
route-map pbr-src-90 permit 10
  match ipv6 address src-90
  set ipv6 next-hop 2001:DB8:2003:1::95
ipv6 local policy route-map pbr-src-90
```

Example: Verifying IPv6 PBR Configuration

The following sample output from the **show ipv6 policy** command displays the IPv6 PBR configuration enabled on interface Ethernet interface 0/0:

```
Device# show ipv6 policy

Interface                  Routemap
Ethernet0/0                src-1
```

Example: Verifying Route-Map Information

The following sample output from the **show route-map** command displays specific route-map information, such as a count of policy matches:

```
Device# show route-map

route-map bill, permit, sequence 10
  Match clauses:
  Set clauses:
  Policy routing matches:0 packets, 0 bytes
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Policy-Based Routing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for IPv6 Policy-Based Routing

Feature Name	Releases	Feature Information
IPv6 Policy-Based Routing	15.2(2)E	Policy-based routing for IPv6 allows a user to manually configure how received packets should be routed. In Cisco IOS Release 15.2(2)E, this feature was supported on the following platform: • Catalyst 2960-X Series Switches The following commands were introduced or modified: **debug fm ipv6 pbr**, **debug ipv6 policy**, **ipv6 local policy route-map**, **ipv6 policy route-map**, **match ipv6 address**, **match length**, **route-map**, **set default interface**, **set interface**, **set ipv6 default next-hop**, **set ipv6 next-hop (PBR)**, **set ipv6 precedence**, **set vrf**, **show fm ipv6 pbr all**, **show fm ipv6 pbr interface**, **show ipv6 policy**, and **show route-map**.

CHAPTER 3

PBR Support for Multiple Tracking Options

The PBR Support for Multiple Tracking Options feature extends the capabilities of object tracking using Cisco Discovery Protocol (CDP) to allow the policy-based routing (PBR) process to verify object availability by using additional methods. The verification method can be an Internet Control Message Protocol (ICMP) ping, a User Datagram Protocol (UDP) ping, or an HTTP GET request.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About PBR Support for Multiple Tracking Options

Object Tracking

Object tracking is an independent process that monitors objects such as the following:

- State of the line protocol of an interface

- Existence of an entry in the routing table
- Results of a Service Assurance Agent (SAA) operation, such as a ping

Clients such as Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), Gateway Load Balancing Protocol (GLBP), and (with this feature) PBR can register their interest in specific, tracked objects and then take action when the state of the objects changes.

PBR Support for Multiple Tracking Options Feature Design

The PBR Support for Multiple Tracking Options feature gives PBR access to all the objects that are available through the tracking process. The tracking process provides the ability to track individual objects--such as ICMP ping reachability, routing adjacency, an application running on a remote device, a route in the Routing Information Base (RIB)--or to track the state of an interface line protocol.

Object tracking functions in the following manner. PBR will inform the tracking process that a certain object should be tracked. The tracking process will in turn notify PBR when the state of that object changes.

How to Configure PBR Support for Multiple Tracking Options

The tasks in this section are divided according to the Cisco IOS release that you are running because Cisco IOS Release 12.3(14)T introduced new syntax for IP Service Level Agreements (SLAs). To use this feature, you must be running Cisco IOS Release 12.3(4)T, 12.2(25)S, or a later release. This section contains the following tasks:

Configuring PBR Support for Multiple Tracking Options

Perform this task to configure PBR support for multiple tracking options. In this task, a route map is created and configured to verify the reachability of the tracked object.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla monitor** *operation-number*
4. **type echo protocol ipIcmpEcho** {*destination-ip-address*| *destination-hostname*}[**source-ipaddr** {*ip-address*| *hostname*} | **source-interface** *interface-name*]
5. **exit**
6. **ip sla monitor schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh* **:** *mm*[**:** *ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh* **:** *mm* **:** *ss*}] [**ageout** *seconds*] [**recurring**]
7. **track** *object-number* **rtr** *entry-number* [**reachability**| **state**]
8. **delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
9. **exit**
10. **interface** *type number*
11. **ip address** *ip-address mask* [**secondary**]
12. **ip policy route-map** *map-tag*
13. **exit**
14. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
15. **set ip next-hop verify-availability** [*next-hop-address sequence* **track** *object*]
16. **end**
17. **show track** *object-number*
18. **show route-map** [*map-name*| **all**| **dynamic**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip sla monitor** *operation-number* **Example:** `Device(config)# ip sla monitor 1`	Starts a Cisco IOS IP Service Level Agreement (SLA) operation configuration and enters IP SLA monitor configuration mode.

	Command or Action	Purpose
Step 4	**type echo protocol ipIcmpEcho** {*destination-ip-address*| *destination-hostname*}[**source-ipaddr** {*ip-address*| *hostname*} | **source-interface** *interface-name*] **Example:** `Device(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1`	Configures an IP SLA Internet Control Message Protocol (ICMP) echo probe operation.
Step 5	**exit** **Example:** `Device(config-sla-monitor)# exit`	Exits IP SLA monitor configuration mode and returns the device to global configuration mode.
Step 6	**ip sla monitor schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh* **:** *mm*[**:** *ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh* **:** *mm* **:** *ss*}] [**ageout** *seconds*] [**recurring**] **Example:** `Device(config)# ip sla monitor schedule 1 life forever start-time now`	Configures the scheduling parameters for a single Cisco IOS IP SLA operation. • In this example, the time parameters for the IP SLA operation are configured.
Step 7	**track** *object-number* **rtr** *entry-number* [**reachability**| **state**] **Example:** `Device(config)# track 123 rtr 1 reachability`	Tracks the reachability of a Response Time Reporter (RTR) object and enters tracking configuration mode.
Step 8	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*} **Example:** `Device(config-track)# delay up 60 down 30`	(Optional) Specifies a period of time, in seconds, to delay communicating state changes of a tracked object.
Step 9	**exit** **Example:** `Device(config-track)# exit`	Exits tracking configuration mode and returns the device to global configuration mode.
Step 10	**interface** *type number* **Example:** `Device(config)# interface serial 2/0`	Specifies an interface type and number and enters interface configuration mode.

	Command or Action	Purpose
Step 11	**ip address** *ip-address mask* [**secondary**] **Example:** `Device(config-if)# ip address 192.168.1.1 255.255.255.0`	Specifies a primary or secondary IP address for an interface. • See the "Configuring IPv4 Addresses" chapter of the *Cisco IOS IP Addressing Services Configuration Guide* for information on configuring IPv4 addresses. • In this example, the IP address of the incoming interface is specified. This is the interface on which policy routing is to be enabled.
Step 12	**ip policy route-map** *map-tag* **Example:** `Device(config-if)# ip policy route-map alpha`	Enables policy routing and identifies a route map to be used for policy routing.
Step 13	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns the device to global configuration mode.
Step 14	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **Example:** `Device(config)# route-map alpha`	Specifies a route map and enters route-map configuration mode.
Step 15	**set ip next-hop verify-availability** [*next-hop-address sequence* **track** *object*] **Example:** `Device(config-route-map)# set ip next-hop verify-availability 10.1.1.1 10 track 123`	Configures the route map to verify the reachability of the tracked object. • In this example, the policy is configured to forward packets received on serial interface 2/0 to 10.1.1.1 if that device is reachable.
Step 16	**end** **Example:** `Device(config-route-map)# end`	Exits route-map configuration mode and returns the device to privileged EXEC mode.
Step 17	**show track** *object-number* **Example:** `Device# show track 123`	(Optional) Displays tracking information. • Use this command to verify the configuration. See the display output in the "Examples" section of this task.
Step 18	**show route-map** [*map-name*| **all**| **dynamic**]	(Optional) Displays route map information.

	Command or Action	Purpose
	Example: `Device# show route-map alpha`	• In this example, information about the route map named alpha is displayed. See the display output in the "Examples" section of this task.

Examples

The following output from the **show track** command shows that the tracked object 123 is reachable.

```
Device# show track 123
Track 123
  Response Time Reporter 1 reachability
  Reachability is Up
    2 changes, last change 00:00:33
  Delay up 60 secs, down 30 secs
  Latest operation return code: OK
  Latest RTT (millisecs) 20
  Tracked by:
    ROUTE-MAP 0
```

The following output from the **show route-map** command shows information about the route map named alpha that was configured in the task.

```
Device# show route-map alpha
route-map alpha, permit, sequence 10
  Match clauses:
  Set clauses:
    ip next-hop verify-availability 10.1.1.1 10 track 123  [up]
  Policy routing matches: 0 packets, 0 bytes
```

Configuration Examples for PBR Support for Multiple Tracking Options

Example: Configuring PBR Support for Multiple Tracking Options

The following example shows how to configure PBR support for multiple tracking options.

The configured policy is that packets received on Ethernet interface 0, should be forwarded to 10.1.1.1 only if that device is reachable (responding to pings). If 10.1.1.1 is not up, then the packets should be forwarded to 10.2.2.2. If 10.2.2.2 is also not reachable, then the policy routing fails and the packets are routed according to the routing table.

Two RTRs are configured to ping the remote devices. The RTRs are then tracked. Policy routing will monitor the state of the tracked RTRs and make forwarding decisions based on their state.

```
! Define and start the RTRs.
ip sla monitor 1
 type echo protocol ipicmpecho 10.1.1.1
ip sla monitor schedule 1 start-time now life forever
!
ip sla monitor 2
```

```
 type echo protocol ipicmpecho 10.2.2.2
ip sla monitor schedule 2 start-time now life forever
!
! Track the RTRs.
track 123 rtr 1 reachability
track 124 rtr 2 reachability
!
! Enable policy routing on the incoming interface.
interface ethernet 0
 ip address 10.4.4.4 255.255.255.0
 ip policy route-map beta
!
! 10.1.1.1 is via this interface.
interface ethernet 1
 ip address 10.1.1.254 255.255.255.0
!
! 10.2.2.2 is via this interface.
interface ethernet 2
 ip address 10.2.2.254 255.255.255.0
!
! Define a route map to set the next-hop depending on the state of the tracked RTRs.
route-map beta
 set ip next-hop verify-availability 10.1.1.1 10 track 123
 set ip next-hop verify-availability 10.2.2.2 20 track 124
```

Additional References

The following sections provide references related to the PBR Support for Multiple Tracking Options feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Object tracking within Cisco IOS software	Configuring Enhanced Object Tracking" chapter of the *Cisco IOS IP Application Services Configuration Guide*
Configuring IP addresses	"Configuring IPv4 Addresses" chapter of the *Cisco IOS IP Addressing Services Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for PBR Support for Multiple Tracking Options

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3: Feature Information for PBR Support for Multiple Tracking Options

Feature Name	Releases	Feature Information
PBR Support for Multiple Tracking Options	15.2(2)E	The PBR Support for Multiple Tracking Options feature extends the capabilities of object tracking using Cisco Discovery Protocol (CDP) to allow the policy-based routing (PBR) process to verify object availability by using additional methods. The verification method can be an Internet Control Message Protocol (ICMP) ping, a User Datagram Protocol (UDP) ping, or an HTTP GET request. In Cisco IOS 15.2(2)E, this feature was supported on the following platforms: • Catalyst 3750-X Series Switches • Catalyst 3560-X Series Switches • Catalyst 3560-C Series Switches • Catalyst 2960 Series Switches • Catalyst 2960-C Series Switches • Catalyst 2960-S Series Switches • Catalyst 2960-X Series Switches • Catalyst 2960-XR Series Switches • Catalyst 2960-Plus Series Switches The following commands were introduced or modified by this feature: **set ip next-hop verify-availability**.