



Implementing Policy-Based Routing for IPv6

First Published: March 1, 2004
Last Updated: July 25, 2005

This module describes policy-based routing (PBR) for IPv6. 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 using several attributes and to specify the next hop or 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 feature information and caveats, see 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 for Implementing Policy-Based Routing for IPv6](#)” section on [page 12](#).

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

Contents

- [Prerequisites for Implementing Policy-Based Routing for IPv6, page 2](#)
- [Restrictions for Implementing Policy-Based Routing for IPv6, page 2](#)
- [Information About Implementing Policy-Based Routing for IPv6, page 2](#)
- [How to Implement Policy-Based Routing for IPv6, page 4](#)
- [Configuration Examples for Implementing Policy-Based Routing for IPv6, page 9](#)
- [Additional References, page 10](#)
- [Feature Information for Implementing Policy-Based Routing for IPv6, page 12](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2004–2009 Cisco Systems, Inc. All rights reserved.

Prerequisites for Implementing Policy-Based Routing for IPv6

- This module assumes that you are familiar with IPv6 addressing and basic configuration. Refer to [Implementing IPv6 Addressing and Basic Connectivity](#) for more information.
- This module assumes that you are familiar with IPv4. Refer to the publications referenced in the “[Related Documents](#)” section for IPv4 configuration and command reference information, as needed.

Restrictions for Implementing Policy-Based Routing for IPv6

Distributed Cisco Express Forwarding is supported on the Cisco 7500 series routers only.

Information About Implementing Policy-Based Routing for IPv6

To configure PBR for IPv6 for Cisco IOS software, you should understand the following concepts:

- [Policy-Based Routing Overview, page 2](#)
- [How Policy-Based Routing Works, page 3](#)
- [When to Use Policy-Based Routing, page 4](#)

Policy-Based Routing Overview

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. To this end, 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. 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 process, Cisco Express Forwarding, and distributed Cisco Express Forwarding forwarding paths.

You can set up PBR as a way to route packets based on configured policies. For example, you can implement routing policies to allow or deny paths based on the identity of a particular end system, an application protocol, or the size of packets.

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.

Policies can be based on IPv6 address, port numbers, protocols, or size of packets. For a simple policy, you can use any one of these descriptors; for a complex policy, you can use all of them.

PBR allows you to classify and mark packets at the edge of the network. PBR marks a packet by setting its precedence value. The precedence value can be used directly by routers 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 PBR enabled are passed through enhanced packet filters known as 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, then the router 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, then 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 the normal forwarding channels and destination-based routing is performed.

You specify PBR on the interface that receives the packet, not on the interface from which the packet is sent.

Packet Matching

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 (using a prefix list or a standard or extended access list [ACL])
- Destination IPv6 address (standard or extended ACL)
- Protocol (extended ACL)
- Source port and destination port (extended ACL)
- Differentiated services code point (DSCP) (extended ACL)
- Flow-label (extended ACL)
- Fragment (extended ACL)

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

Match statements are evaluated first by the criteria specified in the **match ipv6 address** command and then by 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 then 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

PBR for IPv6 packet forwarding is controlled 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 of the set statements in turn. PBR evaluates each set statement by itself, 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 path set. 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 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 Cisco IOS **show** commands.

When to Use Policy-Based Routing

You might use PBR 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 versus batch traffic
- Routing based on dedicated links

Some applications or traffic can benefit from 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 Implement Policy-Based Routing for IPv6

The tasks in the following sections explain how to implement policy-based routing for IPv6:

- [Enabling PBR on an Interface, page 4](#)
- [Enabling Local PBR for IPv6, page 7](#)
- [Enabling Cisco Express Forwarding-Switched PBR for IPv6, page 7](#)
- [Troubleshooting PBR for IPv6, page 8](#)

Enabling PBR on an Interface

To enable PBR for IPv6, you must create a route map that specifies the packet match criteria and desired policy-route action. Then you 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.

This task enables PBR on an interface.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	route-map <i>map-tag</i> [permit deny] [<i>sequence-number</i>] Example: Router(config)# route-map rip-to-ospf permit	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing. <ul style="list-style-type: none"> • Use the route-map command to enter route-map configuration mode.

Command or Action	Purpose
<p>Step 4</p> <pre>match length <i>minimum-length maximum-length</i> or match ipv6 address {<i>prefix-list</i> <i>prefix-list-name</i> <i>access-list-name</i>}</pre> <p>Example: Router(config-route-map)# match length 3 200 or Router(config-route-map)# match ipv6 address marketing </p>	<p>Specifies the match criteria.</p> <ul style="list-style-type: none"> • You can specify any or all of the following: <ul style="list-style-type: none"> – Matches the Level 3 length of the packet. – Matches a specified IPv6 access list. – If you do not specify a match command, the route map applies to all packets.
<p>Step 5</p> <pre>set ipv6 precedence <i>precedence-value</i> or set ipv6 next-hop <i>global-ipv6-address</i> [<i>global-ipv6-address...</i>] or set interface <i>type number</i> [...<i>type number</i>] or set ipv6 default next-hop <i>global-ipv6-address</i> [<i>global-ipv6-address...</i>] or set default interface <i>type number</i> [...<i>type</i> <i>number</i>]</pre> <p>Example: Router(config-route-map)# set ipv6 precedence 1 or Router(config-route-map)# set ipv6 next-hop 2001:0db8:2003:1::95 or Router(config-route-map)# set interface ethernet 0 or Router(config-route-map)# set ipv6 default next-hop 2001:0db8:2003:1::95 or Router(config-route-map)# set default interface ethernet 0 </p>	<p>Specifies the action or actions to take on the packets that match the criteria.</p> <ul style="list-style-type: none"> • You can specify any or all of the following: <ul style="list-style-type: none"> – Sets precedence value in the IPv6 header. – Sets next hop to which to route the packet (the next hop must be adjacent). – Sets output interface for the packet. – Sets next hop to which to route the packet, if there is no explicit route for this destination. – Sets output interface for the packet, if there is no explicit route for this destination.
<p>Step 6</p> <pre>exit</pre> <p>Example: Router(config-route-map)# exit </p>	<p>Returns the router to global configuration mode.</p>

	Command or Action	Purpose
Step 7	<code>interface type number</code> Example: Router(config)# interface FastEthernet 1/0	Specifies an interface type and number, and places the router in interface configuration mode.
Step 8	<code>ipv6 policy route-map route-map-name</code> Example: Router(config-if)# ipv6 policy-route-map interactive	Identifies a route map to use for IPv6 PBR on an interface.

Enabling Local PBR for IPv6

Packets that are generated by the router are not normally policy routed. This task enables local PBR for IPv6 for such packets, indicating which route map the router should use.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ipv6 local policy route-map route-map-name`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.
Step 3	<code>ipv6 local policy route-map route-map-name</code> Example: Router(config)# ipv6 local policy route-map pbr-src-90	Configures PBR for IPv6 for packets generated by the router.

Enabling Cisco Express Forwarding-Switched PBR for IPv6

Beginning in Cisco IOS Release 12.3(7)T, PBR for IPv6 is supported in the Cisco Express Forwarding switching path. Cisco Express Forwarding-switched PBR is the optimal way to perform PBR on a router.

No special configuration is required to enable Cisco Express Forwarding-switched PBR for IPv6. It is on by default as soon as you enable Cisco Express Forwarding and PBR on the router.

Verifying Configuration and Operation of PBR for IPv6

This task explains how to display information to verify 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: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show ipv6 policy Example: Router# show ipv6 policy	Displays IPv6 policy routing packet activity.

Troubleshooting PBR for IPv6

Policy routing looks at various parts of the packet and then routes the packet based on certain user-defined attributes in the packet. This task helps you determine what policy routing is following, whether a packet matches the criteria, and if so, the resulting routing information for the packet.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>debug ipv6 policy [<i>access-list-name</i>]</p> <p>Example: Router# debug ipv6 policy</p>	<p>Displays IPv6 policy routing packet activity.</p>
Step 3	<p>show route-map [<i>map-name</i> dynamic [<i>dynamic-map-name</i> application [<i>application-name</i>]] all] [detailed]</p> <p>Example: Router# show route-map</p>	<p>Displays all route maps configured or only the one specified.</p>

Examples

This section provides the following output examples:

- [Sample Output from the show ipv6 policy Command, page 9](#)
- [Sample Output from the show route-map Command, page 9](#)

Sample Output from the show ipv6 policy Command

The **show ipv6 policy** command displays PBR configuration, as shown in the following example:

```
Router# show ipv6 policy

Interface          Routemap
Ethernet0/0       src-1
```

Sample Output from the show route-map Command

The **show route-map** command displays specific route-map information, such as a count of policy matches:

```
Router# show route-map

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

Configuration Examples for Implementing Policy-Based Routing for IPv6

The following sections provide PBR for IPv6 configuration examples:

- [Enabling PBR on an Interface: Example, page 10](#)
- [Enabling Local PBR for IPv6: Example, page 10](#)

Enabling PBR on an Interface: Example

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

```
ipv6 access-list match-dest-1
  permit ipv6 any 2001:0db8:2001:1760::/32

route-map pbr-dest-1 permit 10
  match ipv6 address match-dest-1
  set interface Ethernet 0/0

interface Ethernet0/0
  ipv6 policy-route-map interactive
```

Enabling Local PBR for IPv6: Example

In the following example, packets with a destination IPv6 address matching that allowed by access list pbr-src-90 are sent to the router at IPv6 address 2001:0db8:2003:1::95:

```
ipv6 access-list src-90
  permit ipv6 host 2001:0db8:2003::90 2001:0db8:2001:1000::/64

route-map pbr-src-90 permit 10
  match ipv6 address src-90
  set ipv6 next-hop 2001:0db8:2003:1::95

ipv6 local policy route-map pbr-src-90
```

Additional References

The following sections provide references related to the implementing policy-based routing for IPv6 feature.

Related Documents

Related Topic	Document Title
IPv6 addressing and basic configuration	“Implementing IPv6 Addressing and Basic Connectivity,” Cisco IOS IPv6 Configuration Guide
QoS for IPv6	“Implementing QoS for IPv6,” Cisco IOS IPv6 Configuration Guide
Multicast Border Gateway Protocol (BGP) for IPv6	“Implementing Multiprotocol BGP for IPv6,” Cisco IOS IPv6 Configuration Guide
Access control lists for IPv6	“Implementing Traffic Filters and Firewalls for IPv6 Security,” Cisco IOS IPv6 Configuration Guide
IPv6 supported feature list	“Start Here: Cisco IOS Software Release Specifics for IPv6 Features,” Cisco IOS IPv6 Configuration Guide

Related Topic	Document Title
IPv6 commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS IPv6 Command Reference
IPv4 Quality of Service	“ Quality of Service Overview ,” <i>Cisco IOS Quality of Service Solutions Configuration Guide</i>

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for Implementing Policy-Based Routing for IPv6

Table 17 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.3(7)T or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the [Start Here: Cisco IOS Software Release Specifies for IPv6 Features](#) roadmap.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 17 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 17 Feature Information for Mobile IPv6

Feature Name	Releases	Feature Information
IPv6 routing: IPv6 policy-based routing	12.2(30)S 12.3(7)T 12.4 12.4(2)T	Policy-based routing for IPv6 in Cisco IOS software allows a user to manually configure how received packets should be routed. This entire document describes this feature.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2003–2009 Cisco Systems, Inc. All rights reserved.