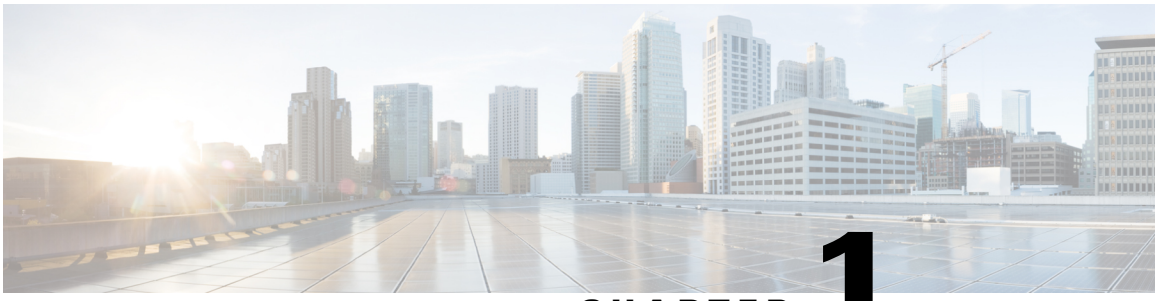
Performance Routing Configuration Guide, Cisco IOS Release 15S

First Published: November 29, 2012

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

Configuring Basic Performance Routing

Performance Routing (PfR) provides additional intelligence to classic routing technologies to track the performance of, or verify the quality of, a path between two devices over a Wide Area Networking (WAN) infrastructure to determine the best egress or ingress path for application traffic.

Cisco Performance Routing complements classic IP routing technologies by adding intelligence to select best paths to meet application performance requirements. The first phase of Performance Routing technology intelligently optimizes application performance over enterprise WANs and to and from the Internet. This technology will evolve to help enable application performance optimization throughout the enterprise network through an end-to-end, performance-aware network.

This document contains an introduction to the basic concepts and tasks required to implement Performance Routing using Cisco IOS Software.

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 Table at the end of this document.

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 Configuring Basic Performance Routing

Only border router functionality is included in the Cisco IOS XE Release 3.1S and 3.2S images; no master controller configuration is available. The master controller that communicates with the Cisco ASR 1000 series router being used as a border router in the Cisco IOS XE Release 3.1S and 3.2S images must be a router running Cisco IOS Release 15.0(1)M, or a later 15.0M release.

Note In Cisco IOS XE Release 3.3S, and later releases, master controller configuration is supported.

Information About Performance Routing

Performance Routing Overview

Performance Routing (PfR) is an advanced Cisco technology to allow businesses to complement classic routing technologies with additional serviceability parameters to select the best egress or ingress path. It complements these classic routing technologies with additional intelligence. PfR can select an egress or ingress WAN interface based upon parameters like reachability, delay, cost, jitter, MOS score, or it can use interface parameters like load, throughput and monetary cost. Classic routing (for example, EIGRP, OSPF, RIPv2, and BGP) generally focuses upon creating a loop-free topology based upon the shortest or least cost path.

PfR gains additional intelligence using measurement instrumentation. It uses interface statistics, Cisco IP SLA for active monitoring, and NetFlow for passive monitoring. No prior knowledge or experience of IP SLA or NetFlow is required, PfR automatically enables these technologies without any manual configuration.

Cisco Performance Routing selects an egress or ingress WAN path based on parameters that affect application performance, including reachability, delay, cost, jitter, and Mean Opinion Score (MOS). This technology can reduce network costs by facilitating more efficient load balancing and by increasing application performance without WAN upgrades.

PfR is an integrated Cisco IOS solution that allows you to monitor IP traffic flows and then define policies and rules based on traffic class performance, link load distribution, link bandwidth monetary cost, and traffic type. PfR provides active and passive monitoring systems, dynamic failure detection, and automatic path correction. Deploying PfR enables intelligent load distribution and optimal route selection in an enterprise network.

Performance Routing Versus Optimized Edge Routing

Cisco Performance Routing takes advantage of the vast intelligence embedded in Cisco IOS Software to determine the optimal path based upon network and application policies. Cisco Performance Routing is an evolution of the Cisco IOS Optimized Edge Routing (OER) technology with a much broader scope. OER was originally designed to provide route control on a per destination prefix basis, but Performance Routing has expanded capabilities that facilitate intelligent route control on a per application basis. The expanded capabilities provide additional flexibility and more granular application optimization than OER.

Performance Routing Versus Classic Routing Technologies

PfR was developed to identify and control network performance issues that traditional IP routing cannot address. In traditional IP routing, each peer device communicates its view of reachability to a prefix destination with some concept of a cost related to reaching the metric. The best path route to a prefix destination is usually determined using the least cost metric, and this route is entered into the routing information base (RIB) for the device. As a result, any route introduced into the RIB is treated as the best path to control traffic destined for the prefix destination. The cost metric is configured to reflect a statically engineered view of the network, for example, the cost metric is a reflection of either a user preference for a path or a preference for a higher bandwidth interface (inferred from the type of interface). The cost metric does not reflect the state of the network or the state of the performance of traffic traveling on that network at that time. Traditional IP routed networks are therefore adaptive to physical state changes in the network (for example, interfaces going down) but not to performance changes (degradation or improvement) in the network. Occasionally, degradation in traffic can be inferred from either the degradation in performance of the routing device or the loss of session connectivity, but these traffic degradation symptoms are not a direct measure of the performance of the traffic and cannot be used to influence decisions about best-path routing.

To address performance issues for traffic within a network, PfR manages traffic classes. Traffic classes are defined as subsets of the traffic on the network, and a subset may represent the traffic associated with an application, for example. The performance of each traffic class is measured and compared against configured or default metrics defined in an PfR policy. PfR monitors the traffic class performance and selects the best entrance or exit for the traffic class. If the subsequent traffic class performance does not conform to the policy, PfR selects another entrance or exit for the traffic class.

Basic Performance Routing Deployment

PfR is configured on Cisco routers using Cisco IOS command-line interface (CLI) configurations. Performance Routing comprises two components: the Master Controller (MC) and the Border Router (BR). A PfR deployment requires one MC and one or more BRs. Communication between the MC and the BR is protected by key-chain authentication. Depending on your Performance Routing deployment scenario and scaling requirements, the MC may be deployed on a dedicated router or may be deployed along with the BR on the same physical router.

A PfR-managed network must have at least two egress interfaces that can carry outbound traffic and can be configured as external interfaces, see the figure below. These interfaces should connect to an ISP or WAN link (Frame-Relay, ATM) at the network edge. The router must also have one interface (reachable by the internal network) that can be configured as an internal interface for passive monitoring. There are three interface configurations required to deploy PfR: external interfaces, internal interfaces, and local interfaces.

PfR Border Router

The BR component resides within the data plane of the edge router with one or more exit links to an ISP or other participating network. The BR uses NetFlow to passively gather throughput and TCP performance information. The BR also sources all IP service-level agreement (SLA) probes used for explicit application performance monitoring. The BR is where all policy decisions and changes to routing in the network are enforced. The BR participates in prefix monitoring and route optimization by reporting prefix and exit link measurements to the master controller and then by enforcing policy changes received from the master controller. The BR enforces policy changes by injecting a preferred route to alter routing in the network. A BR process can be enabled on the same router as a master controller process.

For more details about the Border router only functionality in Cisco IOS XE Releases 2, 3.1S and 3.2S, see the "Performance Routing Border Router Only Functionality" module. In Cisco IOS XE Release 3.3S, and later releases, master controller configuration is supported.

PfR Master Controller

The MC is a single router that acts as the central processor and database for the Performance Routing system. The MC component does not reside in the forwarding plane and, when deployed in a standalone fashion, has no view of routing information contained within the BR. The master controller maintains communication and authenticates the sessions with the BRs. The role of the MC is to gather information from the BR or BRs to determine whether or not traffic classes are in or out of policy, and to instruct the BRs how to ensure that traffic classes remain in policy using route injection or dynamic PBR injection.

In Cisco IOS XE Release 2, 3.1S and 3.2S, PfR supports the ASR 1000 series router as a border router only and the master controller must be running a Cisco IOS Release 15.0(1)M image. In Cisco IOS XE Release 3.3S, and later releases, master controller configuration is supported.

PfR Component Version

When new PfR functionality is introduced that changes the API between the MC and the BR, the version number for the Performance Routing components, master controller and border router, is incremented. The version number of the master controller must be equal or higher to the version number for the border routers.The version numbers for both the master controller and the border routers are displayed using the **show pfr master** command. In the following partial output, the MC version is shown in the first paragraph and the BR versions are shown in the last column of the information for the border routers.

```
Router# show pfr master
OER state: ENABLED and ACTIVE
 Conn Status: SUCCESS, PORT: 7777
  Version: 2.0
  Number of Border routers: 2
  Number of Exits: 2
.
.
.
Border           Status   UP/DOWN             AuthFail  Version
1.1.1.2          ACTIVE   UP       00:18:57          0  2.0
1.1.1.1          ACTIVE   UP       00:18:58          0  2.0
.
.
.
```

The version numbers are not updated at each Cisco IOS software release for a specific release train, but if the Cisco IOS software image is the same release on the devices configured as a master controller and all the border routers, then the versions will be compatible.

Key Chain Authentication for PfR

Communication between the master controller and the border router is protected by key-chain authentication. The authentication key must be configured on both the master controller and the border router before communication can be established. The key-chain configuration is defined in global configuration mode on both the master controller and the border router before key-chain authentication is enabled for master controller-to-border router communication. For more information about key management, see the "Managing

Authentication Keys" section of the Configuring IP Routing Protocol-Independent Features chapter in the *Cisco IOS IP Routing: Protocol Independent Configuration Guide*.

PfR-Managed Network Interfaces

A PfR-managed network must have at least two egress interfaces that can carry outbound traffic and that can be configured as external interfaces. These interfaces should connect to an ISP or WAN link at the network edge. The router must also have one interface (reachable by the internal network) that can be configured as an internal interface for passive monitoring. There are three interface configurations required to deploy PfR:

- *External interfaces* are configured as PfR-managed exit links to forward traffic. The physical external interface is enabled on the border router. The external interface is configured as a PfR external interface on the master controller. The master controller actively monitors prefix and exit link performance on these interfaces. Each border router must have at least one external interface, and a minimum of two external interfaces are required in an PfR-managed network.
- *Internal interfaces* are used only for passive performance monitoring with NetFlow. No explicit NetFlow configuration is required. The internal interface is an active border router interface that connects to the internal network. The internal interface is configured as an PfR-internal interface on the master controller. At least one internal interface must be configured on each border router.
- *Local interfaces* are used only for master controller and border router communication. A single interface must be configured as a local interface on each border router. The local interface is identified as the source interface for communication with the master controller.

The following interface types can be configured as external and internal interfaces:

- ATM
- Channelized Interface (T3/STM1 down to T1)
- Fast Ethernet
- Gigabit Ethernet
- 10 Gigabit Ethernet
- Packet-over-SONET (POS)
- Serial
- Tunnel (not supported with NAT in Cisco IOS XE Releases 2, 3.1S, and later releases)
- VLAN (QinQ is not supported)

The following interface types can be configured as local interfaces:

- ATM
- Fast Ethernet
- Gigabit Ethernet
- 10 Gigabit Ethernet
- Packet-over-SONET (POS)
- Serial

- Tunnel (not supported with NAT in Cisco IOS XE Releases 2, 3.1S, and later releases)
- VLAN (QinQ is not supported)

Performance Routing DMVPN mGre Support

- PfR does not support split tunneling.
- PfR supports hub-to-spoke links only. Spoke-to-spoke links are not supported.
- PfR is supported on DMVPN Multipoint GRE (mGRE) deployments. Any multipoint interface deployment that has multiple next hops for the same destination IP address is not supported (for example, Ethernet).

PfR Network Performance Loop

Every traditional routing protocol creates a feedback loop among devices to create a routing topology. Performance Routing infrastructure includes a performance routing protocol that is communicated in a client-server messaging mode. The routing protocol employed by PfR runs between a network controller called a master controller and performance-aware devices called border routers. This performance routing protocol creates a network performance loop in which the network profiles which traffic classes have to be optimized, measures and monitors the performance metrics of the identified traffic classes, applies policies to the traffic classes, and routes the identified traffic classes based on the best performance path. The diagram below shows the five PfR phases: profile, measure, apply policy, enforce, and verify.

Figure 1: PfR Network Performance Loop

To understand how PfR operates in a network, you should understand and implement the five PfR phases. The PfR performance loop starts with the profile phase followed by the measure, apply policy, control, and verify phases. The flow continues after the verify phase back to the profile phase to update the traffic classes and cycle through the process.

Profile Phase

In medium to large networks there are hundreds of thousands of routes in the RIB to which a device is trying to route traffic. Because performance routing is a means of preferring some traffic over another, a subset of

the total routes in the RIB has to be selected to optimize for performance routing. PfR profiles traffic in one of two ways, automatic learning or manual configuration.

- Automatic Learning—The device profiles the traffic that has to be performance routed (optimized) by learning the flows that pass through the device and by selecting those flows that have the highest delay or the highest throughput.
- Manual configuration—In addition to, or instead of learning, you can configure a class of traffic to performance route.

Measure Phase

After profiling traffic classes that are to be performance routed, PfR measures the performance metrics of these individual traffic classes. There are two mechanisms--passive monitoring and active monitoring--to measure performance metrics, and one or both could be deployed in the network to accomplish this task. Monitoring is the act of measuring at periodic intervals.

Passive monitoring is the act of measuring the performance metrics of the traffic flow as the flow is traversing the device in the data path. Passive monitoring uses NetFlow functionality and cannot be employed for measuring performance metrics for some traffic classes, and there are some hardware or software limitations.

Active monitoring consists of generating synthetic traffic using IP Service Level Agreements (SLAs) to emulate the traffic class that is being monitored. The synthetic traffic is measured instead of the actual traffic class. The results of the synthetic traffic monitoring are applied to performance route the traffic class represented by the synthetic traffic.

Both passive and active monitoring modes can be applied to the traffic classes. The passive monitoring phase may detect traffic class performance that does not conform to an PfR policy, and then active monitoring can be applied to that traffic class to find the best alternate performance path, if available.

Support for NetFlow or IP SLAs configuration is enabled automatically.

Apply Policy Phase

After collecting the performance metrics of the class of traffic to be optimized, PfR compares the results with a set of configured low and high thresholds for each metric configured as a policy. When a metric, and consequently a policy, goes out of bounds, it is an Out-of-Policy (OOP) event. The results are compared on a relative basis--a deviation from the observed mean--or on a threshold basis--the lower or upper bounds of a value--or a combination of both.

There are two types of policies that can be defined in PfR: traffic class policies and link policies. Traffic class policies are defined for prefixes or for applications. Link policies are defined for exit or entrance links at the network edge. Both types of PfR policies define the criteria for determining an OOP event. The policies are applied on a global basis in which a set of policies is applied to all traffic classes, or on a more targeted basis in which a set of policies is applied to a selected (filtered) list of traffic classes.

With multiple policies, many performance metric parameters, and different ways of assigning these policies to traffic classes, a method of resolving policy conflicts was created. The default arbitration method uses a default priority level given to each performance metric variable and each policy. Different priority levels can be configured to override the default arbitration for all policies, or a selected set of policies.

Enforce Phase

In the PfR enforce phase (also called the control phase) of the performance loop, the traffic is controlled to enhance the performance of the network. The technique used to control the traffic depends on the class of traffic. For traffic classes that are defined using a prefix only, the prefix reachability information used in traditional routing can be manipulated. Protocols such as Border Gateway Protocol (BGP) or RIP are used to announce or remove the prefix reachability information by introducing or deleting a route and its appropriate cost metrics.

For traffic classes that are defined by an application in which a prefix and additional packet matching criteria are specified, PfR cannot employ traditional routing protocols because routing protocols communicate the reachability of the prefix only and the control becomes device specific and not network specific. This device specific control is implemented by PfR using policy-based routing (PBR) functionality. If the traffic in this scenario has to be routed out to a different device, the remote border router should be a single hop away or a tunnel interface that makes the remote border router look like a single hop.

Verify Phase

During the PfR enforce phase if a traffic class is OOP, then PfR introduces controls to influence (optimize) the flow of the traffic for the traffic class that is OOP. A static route and a BGP route are examples of controls introduced by PfR into the network. After the controls are introduced, PfR will verify that the optimized traffic is flowing through the preferred exit or entrance links at the network edge. If the traffic class remains OOP, PfR will drop the controls that were introduced to optimize the traffic for the OOP traffic class and cycle through the network performance loop.

PfR and the Enterprise Network

Enterprise networks use multiple Internet Service Provider (ISP) or WAN connections at the network edge for reliability and load distribution. Existing reliability mechanisms depend on link state or route removal on the border router to select the best exit link for a prefix or set of prefixes. Multiple connections protect enterprise networks from catastrophic failures but do not protect the network from brownouts, or soft failures, that occur because of network congestion. Existing mechanisms can respond to catastrophic failures at the first indication of a problem. However, blackouts and brownouts can go undetected and often require the network operator to take action to resolve the problem. When a packet is transmitted between external networks (nationally or globally), the packet spends the vast majority of its life cycle on the WAN segments of the network. Optimizing WAN route selection in the enterprise network provides the end-user with the greatest performance improvement, even better than LAN speed improvements in the local network.

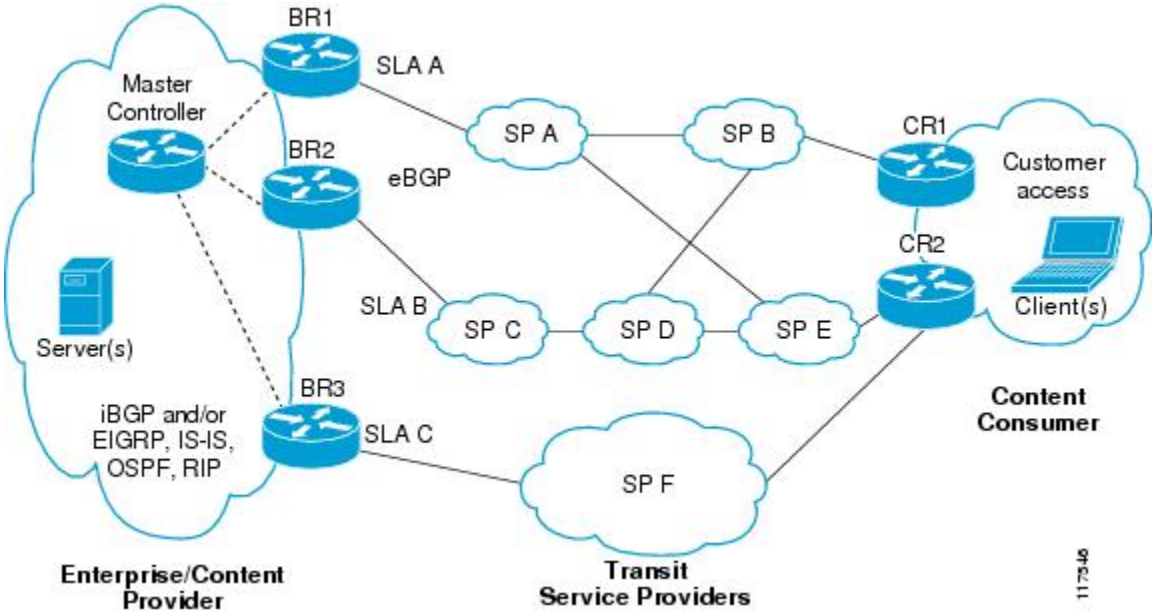
Although many of the examples used to describe PfR deployment show ISPs as the network with which the edge devices communicate, there are other solutions. The network edge can be defined as any logical separation in a network: can be another part of the network such as a data center network within the same location, as well as WAN and ISP connections. The network, or part of the network, connected to the original network edge devices must have a separate autonomous system number when communicating using BGP.

PfR is implemented as an integrated part of Cisco core routing functionality. Deploying PfR enables intelligent network traffic load distribution and dynamic failure detection for data paths at the network edge. While other routing mechanisms can provide both load distribution and failure mitigation, only PfR can make routing adjustments based on criteria other than static routing metrics, such as response time, packet loss, path availability, and traffic load distribution. Deploying PfR allows you to optimize network performance and link load utilization while minimizing bandwidth costs and reducing operational expenses.

Typical Topology on Which PfR is Deployed

The figure below shows a typical PfR-managed enterprise network of a content provider. The enterprise network has three exit interfaces that are used to deliver content to customer access networks. The content provider has a separate service level agreement (SLA) with a different ISP for each exit link. The customer access network has two edge routers that connect to the Internet. Traffic is carried between the enterprise network and the customer access network over six service provider (SP) networks.

Figure 2: A Typical PfR Deployment



PfR monitors and controls outbound traffic on the three border routers (BRs). PfR measures the packet response time and path availability from the egress interfaces on BR1, BR2 and BR3. Changes to exit link performance on the border routers are detected on a per-prefix basis. If the performance of a prefix falls below default or user-defined policy parameters, routing is altered locally in the enterprise network to optimize performance and to route around failure conditions that occur outside of the enterprise network. For example, an interface failure or network misconfiguration in the SP D network can cause outbound traffic that is carried over the BR2 exit interface to become congested or fail to reach the customer access network. Traditional routing mechanisms cannot anticipate or resolve these types of problems without intervention by the network operator. PfR can detect failure conditions and automatically alter routing inside of the network to compensate.

Note In Cisco IOS XE Releases 2, 3.1S and 3.2S, PfR supports the ASR 1000 series router as a border router only and the master controller must be running a Cisco IOS Release 15.0M image for version compatibility. In Cisco IOS XE Release 3.3S, and later releases, master controller configuration is supported.

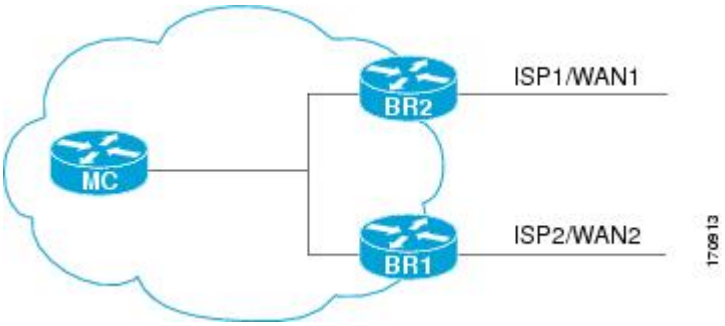
How to Configure Basic Performance Routing

Setting Up the PfR Master Controller

Perform this task to set up the PfR master controller to manage an PfR-managed network. This task must be performed on the router designated as the PfR master controller. For an example network configuration of a master router and two border routers, see the figure below. Communication is first established between the master controller and the border routers with key-chain authentication being configured to protect the communication session between the master controller and the border routers. Internal and external border router interfaces are also specified.

Note In Cisco IOS XE Release 3.1S, and later releases, PfR supports the ASR 1000 series router as a border router only and the master controller must be running a Cisco IOS Release 15.0M image. In Cisco IOS XE Release 3.3S, and later releases, master controller configuration is supported.

Figure 3: Master Controller and Border Router Diagram



To disable a master controller and completely remove the process configuration from the running configuration, use the **no pfr master**command in global configuration mode.

To temporarily disable a master controller, use the **shutdown** command in PfR master controller configuration mode. Entering the **shutdown** command stops an active master controller process but does not remove any configuration parameters. The **shutdown** command is displayed in the running configuration file when enabled.

Before You Begin

Interfaces must be defined and reachable by the master controller and the border routers before a PfR-managed network can be configured.

To set up a PfR-managed network, you must configure routing protocol peering or redistribution between border routers and peer routers in order for PfR to control routing.

Tip We recommend that the master controller be physically close to the border routers to minimize communication response time in PfR-managed networks. If traffic is to be routed between border routers, the border routers also should be physically close each other to minimize the number of hops.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. Repeat Step 3 through Step 7.
8. Repeat Step 3 through Step 7 with appropriate changes to configure key chain authentication for each border router.
9. **pfr master**
10. **logging**
11. **border** *ip-address* [**key-chain** *key-chain-name*]
12. **interface** *type number* **external**
13. **exit**
14. **interface** *type number* **internal**
15. **exit**
16. Repeat Step 11 through Step 15 with appropriate changes to establish communication with each border router.
17. **keepalive** *timer*
18. **end**
19. **show running-config**

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	**key chain** *name-of-chain* **Example:** `Router(config)# key chain border1_PFR`	Enables key-chain authentication and enters key-chain configuration mode. • Key-chain authentication protects the communication session between the master controller and the border router. The key ID and key string must match in order for communication to be established. • In this example, a key chain is created for use with border router 1.
Step 4	**key** *key-id* **Example:** `Router(config-keychain)# key 1`	Identifies an authentication key on a key chain. • The key ID must match the key ID configured on the border router.
Step 5	**key-string** *text* **Example:** `Router(config-keychain-key)# key-string b1`	Specifies the authentication string for the key and enters key-chain key configuration mode. • The authentication string must match the authentication string configured on the border router. • Any encryption level can be configured. • In this example, a key string is created for use with border router 1.
Step 6	**exit** **Example:** `Router(config-keychain-key)# exit`	Exits key-chain key configuration mode and returns to key-chain configuration mode.
Step 7	Repeat Step 3 through Step 7.	Exits key-chain configuration mode and returns to global configuration mode.
Step 8	Repeat Step 3 through Step 7 with appropriate changes to configure key chain authentication for each border router.	--
Step 9	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure a router as a master controller. • A master controller and border router process can be enabled on the same router (for example, in a network that has a single router with two exit links to different service providers).
Step 10	**logging** **Example:** `Router(config-pfr-mc)# logging`	Enables syslog messages for a master controller or border router process. • The notice level of syslog messages is enabled by default.

	Command or Action	Purpose
Step 11	**border** *ip-address* [**key-chain** *key-chain-name*] **Example:** `Router(config-pfr-mc)# border 10.1.1.2 key-chain border1_PFR`	Enters PfR-managed border router configuration mode to establish communication with a border router. • An IP address is configured to identify the border router. • At least one border router must be specified to create an PfR-managed network. A maximum of ten border routers can be controlled by a single master controller. • The value for the *key-chain-name* argument must match the key-chain name configured in Step 3. **Note** The **key-chain** keyword and *key-chain-name* argument must be entered when a border router is initially configured. However, this keyword is optional when reconfiguring an existing border router.
Step 12	**interface** *type number* **external** **Example:** `Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/0 external`	Configures a border router interface as an PfR-managed external interface. • External interfaces are used to forward traffic and for active monitoring. • A minimum of two external border router interfaces are required in an PfR-managed network. At least one external interface must be configured on each border router. A maximum of 20 external interfaces can be controlled by single master controller. **Tip** Configuring an interface as an PfR-managed external interface on a router enters PfR border exit interface configuration mode. In this mode, you can configure maximum link utilization or cost-based optimization for the interface. **Note** Entering the **interface** command without the **external** or **internal** keyword places the router in global configuration mode and not PfR border exit configuration mode. The **no** form of this command should be applied carefully so that active interfaces are not removed from the router configuration.
Step 13	**exit** **Example:** `Router(config-pfr-mc-br-if)# exit`	Exits PfR-managed border exit interface configuration mode and returns to PfR-managed border router configuration mode.
Step 14	**interface** *type number* **internal** **Example:** `Router(config-pfr-mc-br)# interface GigabitEthernet 1/0/0 internal`	Configures a border router interface as an PfR controlled internal interface. • Internal interfaces are used for passive monitoring only. Internal interfaces do not forward traffic. • At least one internal interface must be configured on each border router.
Step 15	**exit** **Example:** `Router(config-pfr-mc-br)# exit`	Exits PfR-managed border router configuration mode and returns to PfR master controller configuration mode.

	Command or Action	Purpose
Step 16	Repeat Step 11 through Step 15 with appropriate changes to establish communication with each border router.	--
Step 17	**keepalive** *timer* **Example:** `Router(config-pfr-mc)# keepalive 10`	(Optional) Configures the length of time that an PfR master controller will maintain connectivity with an PfR border router after no keepalive packets have been received. • The example sets the keepalive timer to 10 seconds. The default keepalive timer is 60 seconds.
Step 18	**end** **Example:** `Router(config-pfr-mc-learn)# end`	Exits PfR Top Talker and Top Delay learning configuration mode and returns to privileged EXEC mode.
Step 19	**show running-config** **Example:** `Router# show running-config`	(Optional) Displays the running configuration to verify the configuration entered in this task.

Setting Up a PFR Border Router

Perform this task to set up a PfR border router. This task must be performed at each border router in your PfR-managed network. Communication is first established between the border router and the master controller with key-chain authentication being configured to protect the communication session between the border router and the master controller. A local interface is configured as the source for communication with the master controller, and external interfaces are configured as PfR-managed exit links.

To disable a border router and completely remove the process configuration from the running configuration, use the **no pfr border** command in global configuration mode.

To temporarily disable a border router process, use the **shutdown** command in PfR border router configuration mode. Entering the **shutdown** command stops an active border router process but does not remove any configuration parameters. The **shutdown** command is displayed in the running configuration file when enabled.

Before You Begin

- Perform the task, Setting Up the PfR Master Controller, to set up the master controller and define the interfaces and establish communication with the border routers.
- Each border router must have at least one external interface that is either used to connect to an ISP or is used as an external WAN link. A minimum of two external interfaces are required in a PfR-managed network.
- Each border router must have at least one internal interface. Internal interfaces are used for only passive performance monitoring with NetFlow. Internal interfaces are not used to forward traffic.

- Each border router must have at least one local interface. Local interfaces are used only for master controller and border router communication. A single interface must be configured as a local interface on each border router.

Tip For Cisco IOS XE Release 3.1S and 3.2S, PfR supports the ASR 1000 series router as a border router only; the master controller cannot be enabled on an ASR 1000 series router. In Cisco IOS XE Release 3.3S, and later releases, master controller configuration is supported.

Tip We recommend that the border routers be physically close to one another to minimize the number of hops. The master controller also should be physically close to the border routers to minimize communication response time in PfR-managed networks.

Note

- Internet exchange points where a border router can communicate with several service providers over the same broadcast media are not supported.
- When two or more border routers are deployed in a PfR-managed network, the next hop to an external network on each border router, as installed in the RIB, cannot be an IP address from the same subnet.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. Repeat Step 6
8. **pfr border**
9. **local** *type number*
10. **master** *ip-address* **key-chain** *key-chain-name*
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**key chain** *name-of-chain* **Example:** `Router(config)# key chain border1_PFR`	Enables key-chain authentication and enters key-chain configuration mode. • Key-chain authentication protects the communication session between both the master controller and the border router. The key ID and key string must match in order for communication to be established.
Step 4	**key** *key-id* **Example:** `Router(config-keychain)# key 1`	Identifies an authentication key on a key chain and enters key-chain key configuration mode. • The key ID must match the key ID configured on the master controller.
Step 5	**key-string** *text* **Example:** `Router(config-keychain-key)# key-string b1`	Specifies the authentication string for the key. • The authentication string must match the authentication string configured on the master controller. • Any level of encryption can be configured.
Step 6	**exit** **Example:** `Router(config-keychain-key)# exit`	Exits key-chain key configuration mode and returns to key-chain configuration mode.
Step 7	Repeat Step 6 **Example:** `Router(config-keychain)# exit`	Exits key-chain configuration mode and returns to global configuration mode.
Step 8	**pfr border** **Example:** `Router(config)# pfr border`	Enters PfR border router configuration mode to configure a router as a border router. • The border router must be in the forwarding path and contain at least one external and internal interface.
Step 9	**local** *type number* **Example:** `Router(config-pfr-br)# local GigabitEthernet 0/0/0`	Identifies a local interface on a PfR border router as the source for communication with an PfR master controller. • A local interface must be defined.

	Command or Action	Purpose
Step 10	**master** *ip-address* **key-chain** *key-chain-name* **Example:** `Router(config-pfr-br)# master 10.1.1.1 key-chain border1_PFR`	Enters PfR-managed border router configuration mode to establish communication with a master controller. • An IP address is used to identify the master controller. • The value for the key-chain-name argument must match the key-chain name configured in Step 3.
Step 11	**end** **Example:** `Router(config-pfr-br)# end`	Exits PfR Top Talker and Top Delay learning configuration mode and returns to privileged EXEC mode.

What to Do Next

If your network is configured to use only static routing, no additional configuration is required. The PfR-managed network should be operational, as long as valid static routes that point to external interfaces on the border routers are configured.

Otherwise, routing protocol peering or static redistribution must be configured between the border routers and other routers in the PfR-managed network.

Configuration Examples for Configuring Basic Performance Routing

Configuring the PfR Master Controller Example

The following configuration example, starting in global configuration mode, shows the minimum configuration required to configure a master controller process to manage the internal network. A key-chain configuration named PFR is defined in global configuration mode.

Note This configuration is performed on a master controller. Only border router functionality is included in Cisco IOS XE Release 3.1S and 3.2S; no master controller configuration is available. The master controller that communicates with the Cisco ASR 1000 series router being used as a border router must be a router running Cisco IOS Release 15.0(1)M, or a later 15.0M release. In Cisco IOS XE Release 3.3S, and later releases, master controller configuration is supported.

```
Router(config)# key chain PFR
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string KEYSTRING2
Router(config-keychain-key)# end
```

The master controller is configured to communicate with the 10.100.1.1 and 10.200.2.2 border routers. The keepalive interval is set to 10 seconds. Route control mode is enabled. Internal and external PfR-controlled border router interfaces are defined.

```
Router(config)# pfr master
Router(config-pfr-mc)# keepalive 10
Router(config-pfr-mc)# logging
Router(config-pfr-mc)# border 10.100.1.1 key-chain PFR
Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/0 external
Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/1 internal
Router(config-pfr-mc-br)# exit
Router(config-pfr-mc)# border 10.200.2.2 key-chain PFR
Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/0 external
Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/1 internal
Router(config-pfr-mc)# exit
```

Configuring a PfR Border Router Example

The following configuration example, starting in global configuration mode, shows the minimum required configuration to enable a border router. The key-chain configuration is defined in global configuration mode.

```
Router(config)# key chain PFR
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string KEYSTRING2
Router(config-keychain-key)# end
```

The key-chain PFR is applied to protect communication. An interface is identified to the master controller as the local interface (source) for PfR communication.

```
Router(config)# pfr border
Router(config-pfr-br)# local GigabitEthernet 1/0/0
Router(config-pfr-br)# master 192.168.1.1 key-chain PFR
Router(config-pfr-br)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco IOS PfR commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS Performance Routing Command Reference
Basic PfR configuration for Cisco IOS XE releases	“Configuring Basic Performance Routing” module
Information about configuration for the border router only functionality for Cisco IOS XE Releases 3.1 and 3.2	“Performance Routing Border Router Only Functionality” module
Concepts required to understand the Performance Routing operational phases for Cisco IOS XE releases	“Understanding Performance Routing” module

Related Topic	Document Title
Advanced PfR configuration for Cisco IOS XE releases	"Configuring Advanced Performance Routing" module
IP SLAs overview	"Cisco IOS IP SLAs Overview" module
PfR home page with links to PfR-related content on our DocWiki collaborative environment	PfR:Home

MIBs

MIB	MIBs Link
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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

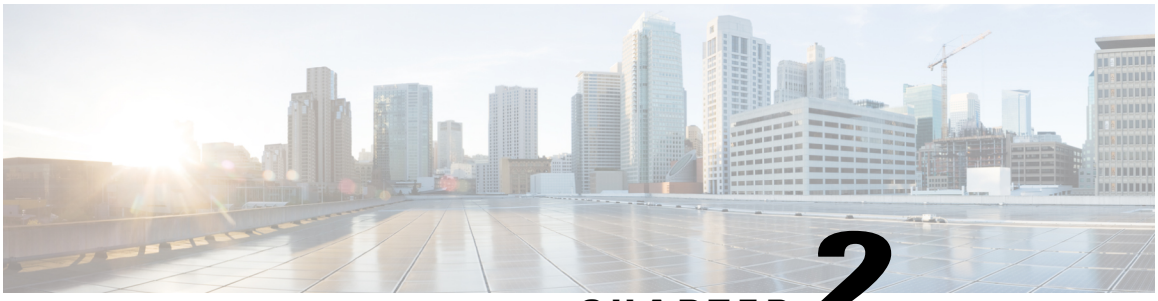
Feature Information for Configuring Basic Performance Routing

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 1: Feature Information for Configuring Basic Performance Routing

Feature Name	Releases	Feature Information
Optimized Edge Routing	Cisco IOS XE Release 2.6.1, Cisco IOS XE Release 3.1S	OER was introduced on the Cisco ASR 1000 series routers. Performance Routing is an extension of OER. PfR syntax was introduced in Cisco IOS XE Release 3.1S. The following commands were introduced or modified: pfr, show pfr master. **Note** Only border router functionality is included in the Cisco IOS XE Release 2.6.1 and Cisco IOS XE Release 3.1S releases; no master controller configuration is available. The master controller that communicates with the Cisco ASR 1000 series routers being used as a border router must be a router running Cisco IOS Release 15.0(1)M.
PfR Master Controller support for ASR 1000	Cisco IOS XE Release 3.3S	In Cisco IOS XE Release 3.3S and later releases, master controller functionality is supported.



CHAPTER 2

Understanding Performance Routing

This module describes how Performance Routing (PfR) operates to help you understand how to implement the technology in your network. After configuration, the PfR technology runs through a series of phases that start with profiling traffic classes, measuring the traffic classes, apply policies to the traffic classes, controlling the traffic classes to meet the policy conditions, and finally verifying the result of the traffic class optimization.

Note The PfR configuration modules refer to the PfR syntax introduced in Cisco IOS Release 15.1(2)T. If you are running Cisco IOS Release 15.1(1)T, or an earlier release, or any 12.2SR or 12.2SX image, you need to consult the Optimized Edge Routing Configuration Guide to help you locate all the Optimized Edge Routing documentation.

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 Table at the end of this document.

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.

Prerequisites for Understanding Performance Routing

- The PfR configuration modules refer to the PfR syntax introduced in Cisco IOS Release 15.1(2)T. If you are running Cisco IOS Release 15.1(1)T, or an earlier release, or any 12.2SR or 12.2SX image, you need to consult the Optimized Edge Routing Configuration Guide.
- Before understanding the PfR phases, you need to understand an overview of how PfR works and how to set up basic PfR network components. See the "Configuring Basic Performance Routing" module for more details.
- Cisco Express Forwarding (CEF) must be enabled on all participating devices. No other switching path is supported, even if otherwise supported by policy-based routing (PBR).

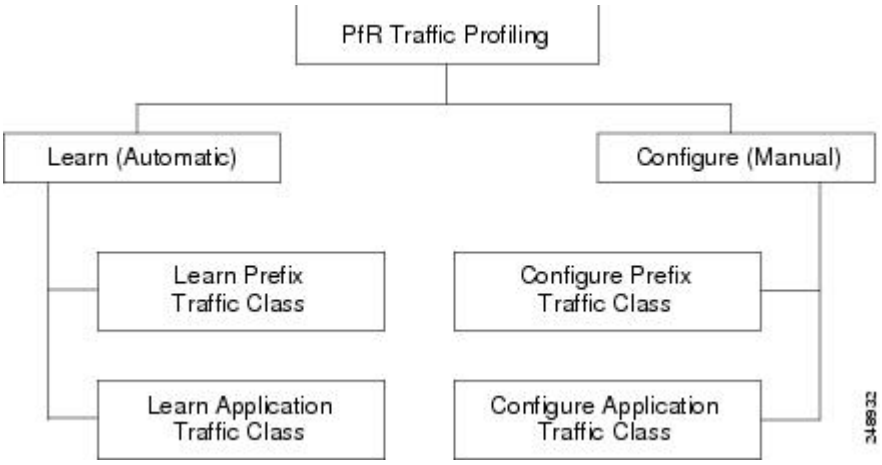
Information About Understanding Performance Routing

Profile Phase Concepts

Traffic Class Profiling Overview

Before optimizing traffic, PfR has to determine the traffic classes from the traffic flowing through the border routers. To optimize traffic routing, subsets of the total traffic must be identified, and these traffic subsets are named traffic classes. The list of traffic classes entries is named a Monitored Traffic Class (MTC) list. The entries in the MTC list can be profiled either by automatically learning the traffic flowing through the device or by manually configuring the traffic classes. Learned and configured traffic classes can both exist in the MTC list at the same time. The PfR profile phase includes both the learn mechanism and the configure mechanism. The overall structure of the PfR traffic class profile process and its component parts can be seen in the figure below.

Figure 4: PfR Traffic Class Profiling Process



The ultimate objective of this phase is to select a subset of traffic flowing through the network. This subset of traffic--the traffic classes in the MTC list--represents the classes of traffic that need to be routed based on the best performance path available.

Automatic Traffic Class Learning

PfR can automatically learn the traffic classes while monitoring the traffic flow through border routers. Although the goal is to optimize a subset of the traffic, you may not know all the exact parameters of this traffic and PfR provides a method to automatically learn the traffic and create traffic classes by populating the MTC list. Several features have been added to PfR since the original release to add functionality to the automatic traffic class learning process.

Within the automatic traffic class learning process there are now three components. One component describes the automatic learning of prefix-based traffic classes, the second component describes automatic learning of application-based traffic classes, and the third component describes the use of learn lists to categorize both prefix-based and application-based traffic classes. These three components are described in the following sections:

Prefix Traffic Class Learning Using PfR

The PfR master controller can be configured, using NetFlow Top Talker functionality, to automatically learn prefixes based on the highest outbound throughput or the highest delay time. Throughput learning measures prefixes that generate the highest outbound traffic volume. Throughput prefixes are sorted from highest to lowest. Delay learning measures prefixes with the highest round-trip response time (RTT) to optimize these highest delay prefixes to try to reduce the RTT for these prefixes. Delay prefixes are sorted from the highest to the lowest delay time.

PfR can automatically learn two types of prefixes:

- outside prefix--An outside prefix is defined as a public IP prefix assigned outside the company. Outside prefixes are received from other networks.
- inside prefix--An inside prefix is defined as a public IP prefix assigned to a company. An inside prefix is a prefix configured within the company network.

In the BGP Inbound Optimization feature the ability to learn inside prefixes was introduced. Using BGP, PfR can select inside prefixes to support best entrance selection for traffic that originates from prefixes outside an autonomous system destined for prefixes inside the autonomous system. In prior releases, only outside prefixes were supported. For more details about inside prefix PfR support, see the BGP Inbound Optimization Using Performance Routing module.

Automatic prefix learning is configured in PfR Top Talker and Top Delay learning configuration mode. The **learn** (PfR) command is used to enter this mode from PfR master controller configuration mode. When automatic prefix learning is enabled, prefixes and their delay or throughput characteristics are measured on the border routers. Performance measurements for the prefix-based traffic classes are reported to the master controller where the learned prefixes are stored in the MTC list.

Prefixes are learned on the border routers through monitoring the traffic flow using the embedded NetFlow capability. All incoming and outgoing traffic flows are monitored. The top 100 flows are learned by default, but the master controller can be configured to learn up to 2500 flows for each learn cycle.

The master controller can be configured to aggregate learned prefixes based on type; BGP or non-BGP (static). Prefixes can be aggregated based on the prefix length. Traffic flows are aggregated using a /24 prefix length

by default. Prefix aggregation can be configured to include any subset or superset of the network, from single host route (/32) to a major network address range. For each aggregated prefix, up to five host addresses are selected to use as active probe targets. Prefix aggregation is configured with the **aggregation-type**(PfR) command in PfR Top Talker and Delay learning configuration mode.

Application Traffic Class Learning Using PfR

PfR can learn Layer 3 prefixes, and Layer 4 options such as protocol or port numbers can be added as filters to the prefix-based traffic class. The protocol and port numbers can be used to identify specific application traffic classes; protocol and port number parameters are monitored only within the context of a prefix and are not sent to the master controller database (MTC list). The prefix that carries the specific traffic is then monitored by the master controller. PfR application traffic class learning also supports Differentiated Services Code Point (DSCP) values in addition to protocol and port numbers, and these Layer 4 options are entered in the MTC list.

DSCP Value, Port, and Protocol Learning by PfR

PfR has the ability to filter and aggregate application traffic by DSCP value, port number or protocol. Traffic classes can be defined by a combination of keys comprising of protocol, port numbers, and DSCP values. The ability to filter out traffic that is not required, and the ability to aggregate the traffic in which you are interested, was introduced. Information such as protocol, port number, and DSCP value is now sent to the master controller database in addition to the prefix information. The new functionality allows PfR to both actively and passively monitor application traffic. Using new CLI and access lists, PfR can be configured to automatically learn application traffic classes.

Learn List Configuration Mode

PfR supports a learn list configuration mode to simplify the learning of traffic classes. Learn lists are a way to categorize learned traffic classes. In each learn list, different criteria including prefixes, application definitions, filters, and aggregation parameters for learning traffic classes can be configured. A traffic class is automatically learned by PfR based on each learn list criteria, and each learn list is configured with a sequence number. The sequence number determines the order in which learn list criteria are applied. Learn lists allow different PfR policies to be applied to each learn list; in previous releases, the traffic classes could not be divided, and an PfR policy was applied to all the learned traffic classes.

Learn list configuration mode uses **traffic-class** commands to simplify the learning of traffic classes. Four types of traffic classes--to be automatically learned--can be profiled:

- Traffic classes based on destination prefixes
- Traffic classes representing custom application definitions using access lists
- Traffic classes based on a static application mapping name with optional prefix lists to define destination prefixes
- Traffic classes based on a NBAR application mapping name with optional prefix lists to define destination prefixes

Only one type of **traffic-class** command can be specified per learn list, and the **throughput** (PfR) and **delay** (PfR) commands are also mutually exclusive within a learn list.

Static Application Mapping Using PfR

The static application mapping feature introduced the ability to define an application using a keyword to simplify the configuration of application-based traffic classes. PfR uses well-known applications with fixed ports, and more than one application may be configured at the same time. For more details about static application mapping, see the Static Application Mapping Using Performance Routing feature.

PfR Application Mapping Using NBAR

PfR supports the ability to profile an application-based traffic class using NBAR. Network-Based Application Recognition (NBAR) is a classification engine that recognizes and classifies a wide variety of protocols and applications, including web-based and other difficult-to-classify applications and protocols that use dynamic TCP/UDP port assignments. PfR uses NBAR to recognize and classify a protocol or application, and the resulting traffic classes are added to the PfR application database to be passively and actively monitored. For more details about PfR application mapping using NBAR, see the Performance Routing with NBAR/CCE Application Recognition feature.

Manual Traffic Class Configuration

PfR can be manually configured to create traffic classes for monitoring and subsequent optimizing. Automatic learning generally uses a default prefix length of /24 but manual configuration allows exact prefixes to be defined. Within the manual traffic class configuration process there are two components-- manually configuring prefix-based traffic classes and manually configuring application-based traffic classes, both of which are described in the following sections:

Prefix Traffic Class Configuration Using PfR

A prefix or range of prefixes can be selected for PfR monitoring by configuring an IP prefix list. The IP prefix list is then imported into the MTC list by configuring a match clause in a PfR map. A PfR map is similar to an IP route map. IP prefix lists are configured with the **ip prefix-list** command and PfR maps are configured with the **pfr-map** command in global configuration mode.

The prefix list syntax operates in a slightly different way with PfR than in regular routing. The **ge** keyword is not used and the **le** keyword is used by PfR to specify only an inclusive prefix. A prefix list can also be used to specify an exact prefix.

A master controller can monitor and control an exact prefix of any length including the default route. If an exact prefix is specified, PfR monitors only the exact prefix.

A master controller can monitor and control an inclusive prefix using the**le** keyword and the *le-value* argument set to 32. PfR monitors the configured prefix and any more specific prefixes (for example, configuring the 10.0.0.0/8 le 32 prefix would include the 10.1.0.0/16 and the 10.1.1.0/24 prefixes) over the same exit and records the information in the routing information base (RIB).

Note Use the inclusive prefix option with caution in a typical PfR deployment because of the potential increase in the amount of prefixes being monitored and recorded.

An IP prefix list with a deny statement can be used to configure the master controller to exclude a prefix or prefix length for learned traffic classes. Deny prefix list sequences should be applied in the lowest PfR map sequences for best performance. The master controller can also be configured to tell border routers to filter out uninteresting traffic using an access list.

Note IP prefix lists with deny statements can be applied only to learned traffic classes.

Two types of prefix can be manually configured for PfR monitoring using an IP prefix list:

- outside prefix--An outside prefix is defined as a public IP prefix assigned outside the company. Outside prefixes are received from other networks.
- inside prefix--An inside prefix is defined as a public IP prefix assigned to a company. An inside prefix is a prefix configured within the company network.

In the BGP Inbound Optimization feature the ability to manually configure inside prefixes was introduced. Using BGP, PfR can be configured to select inside prefixes to support best entrance selection for traffic that originates from prefixes outside an autonomous system destined for prefixes inside the autonomous system. In prior releases, only outside prefixes were supported.

For more details about inside prefix PfR support, see the BGP Inbound Optimization Using Performance Routing module.

Application Traffic Class Configuration Using PfR

PfR supports the manual configuration of Layer 3 prefixes during the PfR profile phase. Application-aware routing for policy-based routing (PBR) is also supported. Application-aware routing allows the selection of traffic for specific applications based on values in the IP packet header, other than the Layer 3 destination address through a named extended IP access control list (ACL). Only named extended ACLs are supported. The extended ACL is configured with a permit statement and then referenced in a PfR map. The protocol and port numbers can be used to identify specific application traffic classes, but protocol and port number parameters are monitored only within the context of a prefix, and are not sent to the MTC list. Only the prefix that carries the specific application traffic is profiled by the master controller. With application-aware routing support, active monitoring of application traffic was supported. Passive monitoring of application traffic is also supported. Application traffic classes can be defined using DSCP values as well as protocol and port numbers. DSCP values, port numbers, and protocols in addition to prefixes, are all now stored in the MTC list.

Learn list configuration mode uses **match traffic-class** commands under PfR map configuration mode to simplify the configuration of traffic classes. Four types of traffic classes--to be manually configured--can be profiled:

- Traffic classes based on destination prefixes
- Traffic classes representing custom application definitions using access lists
- Traffic classes based on a static application mapping name and a prefix list to define destination prefixes
- Traffic classes based on NBAR application mapping name and a prefix list to define destination prefixes

Only one type of **match traffic-class** command can be specified per PfR map.

For a series of well-known applications, static ports have been defined and each application can be defined by entering a keyword. For more details about static application mapping, see the Static Application Mapping Using Performance Routing feature.

PfR supports the ability to profile an application-based traffic class using NBAR. NBAR is a classification engine that recognizes and classifies a wide variety of protocols and applications, including web-based and other difficult-to-classify applications and protocols that use dynamic TCP/UDP port assignments. PfR uses

NBAR to recognize and classify a protocol or application, and the resulting traffic classes are added to the PfR application database to be passively and actively monitored. For more details about PfR application mapping using NBAR, see the Performance Routing with NBAR/CCE Application Recognition feature.

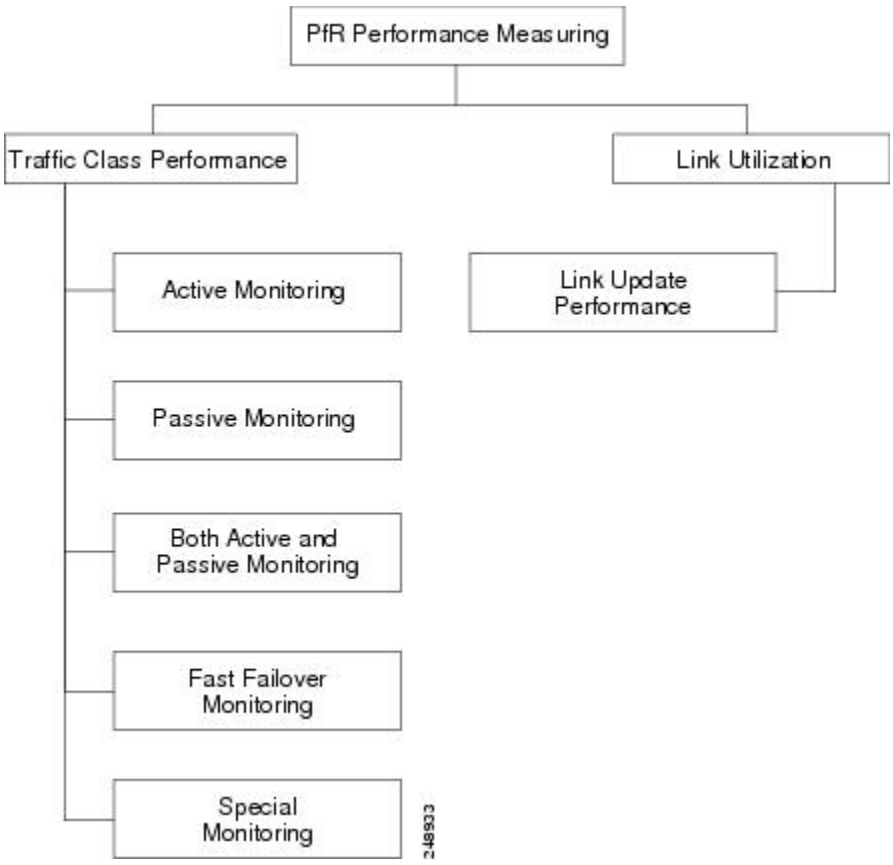
Measure Phase Concepts

Traffic Class Performance Measurement Overview

The PfR measure phase is the second step in the PfR performance loop and it follows the PfR profile phase where the traffic class entries fill the Monitored Traffic Class (MTC) list. The MTC list is now full of traffic class entries and PfR must measure the performance metrics of these traffic class entries. Monitoring is defined here as the act of measurement performed periodically over a set interval of time where the measurements are compared against a threshold. PfR measures the performance of traffic classes using active and passive monitoring techniques but it also measures, by default, the utilization of links. The master controller can be configured to monitor learned and configured traffic classes. The border routers collect passive monitoring and active monitoring statistics and then transmit this information to the master controller. The PfR measure phase is complete when each traffic class entry in the MTC list has associated performance metric measurements.

The overall structure of the PfR measure phase and its component parts can be seen in the figure below.

Figure 5: PfR Performance Measuring Process



PfR measures the performance of both traffic classes and links, but before monitoring a traffic class or link PfR checks the state of the traffic class or link. PfR uses a policy decision point (PDP) that operates according to a traffic class state transition diagram.

After determining the state of the traffic class or link, PfR may initiate one of the following performance measuring processes.

Traffic Class Performance Measurement Techniques

PfR uses three methods of traffic class performance measurement:

- Passive monitoring--measuring the performance metrics of traffic class entries while the traffic is flowing through the device using NetFlow functionality.
- Active monitoring--creating a stream of synthetic traffic replicating a traffic class as closely as possible and measuring the performance metrics of the synthetic traffic. The results of the performance metrics of the synthetic traffic are applied to the traffic class in the MTC list. Active monitoring uses integrated IP Service Level Agreements (IP SLAs) functionality.
- Both active and passive monitoring--combining both active and passive monitoring in order to generate a more complete picture of traffic flows within the network.

Fast failover monitoring mode is another variation of the combined active and passive monitoring modes. In fast failover monitoring mode, all exits are continuously probed using active monitoring and passive monitoring. When fast failover monitoring mode is enabled, the probe frequency can be set to a lower frequency than for other monitoring modes, to allow a faster failover capability.

No explicit NetFlow or IP SLAs configuration is required and support for NetFlow and IP SLAs is enabled automatically. You can use both active and passive monitoring methods for a traffic class.

After the master controller is defined and PfR functionality is enabled, the master controller uses both passive and active monitoring by default. All traffic classes are passively monitored using integrated NetFlow functionality. Out-of-policy traffic classes are actively monitored using IP SLA functionality. You can configure the master controller to use only passive monitoring, active monitoring, both passive and active monitoring, or fast failover monitoring. The main differences between the different modes can be seen in the table below.

Table 2: Mode Comparison Table

Comparison Parameter	Active Mode	Passive Mode	Combined Mode	Fast Failover Mode
Active/IP SLA	Yes	No	Yes	Yes
Passive/NetFlow	No	Yes	Yes	Yes
Monitoring of Alternate Paths	On Demand	On Demand	On Demand	Continuous
Best Failover Time	10 seconds	~ 1 minute	~ 1.1 minute	3 seconds
Support for Round Trip Delay	Yes	Yes	Yes	Yes

Comparison Parameter	Active Mode	Passive Mode	Combined Mode	Fast Failover Mode
Support for Loss	Only with Jitter probe	Only for TCP traffic	Only for TCP traffic	Only for TCP traffic and Jitter probe
Support for Reachability	Yes	Only for TCP traffic	Only for TCP traffic	Yes
Support for Jitter	Yes	No	No	Yes
Support for MOS	Yes	No	No	Yes

Passive Monitoring

Cisco IOS PfR uses NetFlow, an integrated technology in Cisco IOS software, to collect and aggregate passive monitoring statistics on a per traffic class basis. Passive monitoring is enabled along with active monitoring by default when an PfR managed network is created. Passive monitoring can also be enabled explicitly using the **mode monitor passive** command. Netflow is a flow-based monitoring and accounting system, and NetFlow support is enabled by default on the border routers when passive monitoring is enabled.

Passive monitoring uses only existing traffic; additional traffic is not generated. Border routers collect and report passive monitoring statistics to the master controller approximately once per minute. If traffic does not go over an external interface of a border router, no data is reported to the master controller. Threshold comparison is done at the master controller. Passive monitoring supports traffic classes defined by prefix, port, protocol, and DSCP value.

PfR uses passive monitoring to measure the following metrics for all the traffic classes:

- Delay--PfR measures the average delay of TCP flows for a given prefix. Delay is the measurement of the round-trip response time (RTT) between the transmission of a TCP synchronization message and receipt of the TCP acknowledgement.
- Packet loss--PfR measures packet loss by tracking TCP sequence numbers for each TCP flow. PfR estimates packet loss by tracking the highest TCP sequence number. If a subsequent packet is received with a lower sequence number, PfR increments the packet loss counter. Packet loss is measured in packets per million.
- Reachability--PfR measures reachability by tracking TCP synchronization messages that have been sent repeatedly without receiving a TCP acknowledgement.
- Throughput--PfR measures throughput by measuring the total number of bytes and packets for each traffic class for a given interval of time.

Note Although all traffic classes are monitored, delay, loss, and reachability information is captured only for TCP traffic flows. Throughput statistics are captured for all non-TCP traffic flows.

DSCP values, port numbers, and protocols in addition to prefixes, are all sent from border routers to the master controller. Passive monitoring statistics are gathered and stored in a prefix history buffer that can hold a minimum of 60 minutes of information depending on whether the traffic flow is continuous. PfR uses this

information to determine if the prefix is in-policy based on the default or user-defined policies. No alternative path analysis is performed as the traffic for a traffic class is flowing through one transit device in the network. If the traffic class goes OOP and only passive monitoring mode is enabled, the traffic class is moved to another point and the measurement repeated until a good or best exit is found. If the traffic class goes OOP and both passive and active monitoring modes are enabled, active probing is executed on all the exits and a best or good exit is selected.

Active Monitoring

If PfR passive monitoring techniques create too much overhead on a network device, or the performance metrics of a traffic class cannot be measured using the PfR passive monitoring mode, then PfR active monitoring techniques are performed. Active monitoring involves creating a stream of synthetic traffic that replicates a traffic class as closely as possible. The performance metrics of the synthetic traffic are measured and the results are applied to the traffic class entry in the MTC list. Active monitoring supports traffic classes defined by prefix, port, protocol, and DSCP value.

PfR uses active monitoring to measure the following metrics for all the traffic classes:

- Delay--PfR measures the average delay of TCP, UDP, and ICMP flows for a given prefix. Delay is the measurement of the round-trip response time (RTT) between the transmission of a TCP synchronization message and receipt of the TCP acknowledgement.
- Reachability--PfR measures reachability by tracking TCP synchronization messages that have been sent repeatedly without receiving a TCP acknowledgement.
- Jitter--Jitter means interpacket delay variance. PfR measures jitter by sending multiple packets to a target address and a specified target port number, and measuring the delay interval between packets arriving at the destination.
- MOS--Mean Opinion Score (MOS) is a standards-based method of measuring voice quality. Standards bodies like the ITU have derived two important recommendations: P.800 (MOS) and P.861 (Perceptual Speech Quality Measurement [PSQM]). P.800 is concerned with defining a method to derive a Mean Opinion Score of voice quality. MOS scores range between 1 representing the worst voice quality, and 5 representing the best voice quality. A MOS of 4 is considered "toll-quality" voice.

The creation of synthetic traffic in Cisco network devices is activated through the use of Cisco IOS IP SLA probes. PfR is integrated with IP SLAs functionality such that PfR will use IP SLA probes to actively monitor a traffic class. When active monitoring is enabled, the master controller commands the border routers to send active probes to set of target IP addresses. The border sends probe packets to no more than five target host addresses per traffic class, and transmits the probe results to the master controller for analysis.

Active probe monitoring periods are defined as short-term which consists of the last 5 probe results, and long-term which consists of the last 60 probe results.

IP SLA Active Probe Types Used by PfR

IP SLAs are an embedded feature set in Cisco IOS software and they allow you to analyze IP service levels for IP applications and services, to increase productivity, to lower operational costs, and to reduce occurrences of network congestion or outages. IP SLAs use active traffic monitoring--the generation of traffic in a continuous, reliable, and predictable manner--for measuring network performance. The accuracy of measured data is enhanced by enabling the IP SLAs Responder, available in Cisco routers, on the destination device. For more details about IP SLAs, see the IP SLAs Configuration Guide.

The following types of active probes can be configured:

- ICMP Echo--A ping is sent to the target address. PfR uses ICMP Echo probes, by default, when an active probe is automatically generated. Configuring an ICMP echo probe does not require knowledgeable cooperation from the target device. However, repeated probing could trigger an Intrusion Detection System (IDS) alarm in the target network. If an IDS is configured in a target network that is not under your control, we recommend that you notify the administrator of this target network.
- Jitter--A jitter probe is sent to the target address. A target port number must be specified. A remote responder must be enabled on the target device, regardless of the configured port number. Loss policy is supported for active monitoring if the jitter probe is used.
- TCP Connection--A TCP connection probe is sent to the target address. A target port number must be specified. A remote responder must be enabled if TCP messages are configured to use a port number other than TCP port number 23, which is well-known.
- UDP Echo--A UDP echo probe is sent to the target address. A target port number must be specified. A remote responder must be enabled on the target device, regardless of which port number is configured.

PfR marks the probe packets with the DSCP value by default if the monitored traffic classes have the DSCP field set to a nonzero value.

Creation of Active Probe for a Traffic Class

To create an active probe for a traffic class, a probe type has to be discovered, and a probe target assigned to the traffic class. To discover a probe type, PfR uses one of the following methods:

- Learned probe--Active probes are automatically generated when a traffic class is learned using the NetFlow TopTalker Learn mechanism. Five targets are learned for each traffic class and, by default, the active probe is set as an ICMP echo probe.
- Configured probe--Active probes can also be configured on the master controller by specifying the probe type, target address and port if needed. Configured traffic classes can be configured to use any of the IP SLA active probes.

To assign a probe target for a traffic class, PfR uses one of the following methods:

- Longest match--By default, PfR assigns a probe target to the traffic class with the longest matching prefix in the MTC list. This is referred to as a default probe assignment.
- Forced assignment--An IP SLA probe can be configured using a PfR map and the results of the probe are assigned to specific traffic classes associated with the PfR map. This specific assignment of active probe results is called a forced target probe assignment.

The active probe is sourced from the border router and transmitted through an external interface (the external interface may, or may not, be the preferred route for an optimized prefix). When creating an active probe through an external interface for a specified target, the target should be reachable through the external interface. To test the reachability of the specified target, PfR performs a route lookup in the BGP and static routing tables for the specified target and external interface. Protocol Independent Route Optimization (PIRO) introduced the ability of PfR to search for a parent route--an exact matching route, or a less specific route--in any IP Routing Information Base (RIB). The BGP routing table is searched first, followed by the static routing table, and finally the RIB.

In active monitoring mode, the probes are activated from all the border routers to find the best performance path for the specific traffic class. The active probes for that traffic class are not activated again unless the traffic class goes OOP.

By default, the frequency of an active probe used by PfR is set to 60 seconds. The frequency of an active probe can be increased for each policy by configuring a lower time-interval between two probes. Increased probe frequency can reduce the response time and, for voice traffic, provide a better approximation of the MOS-low count percentage.

PfR Active Probe Source Address

PfR supports the ability to configure an active probe source address. By default, active probes use the source IP address of the PfR external interface that transmits the probe. The active probe source address feature is configured on the border router. When this command is configured, the primary IP address of the specified interface is used as the active probe source. The active probe source interface IP address must be unique to ensure that the probe reply is routed back to the specified source interface. If the interface is not configured with an IP address, the active probe will not be generated. If the IP address is changed after the interface has been configured as an active probe source, active probing is stopped, and then restarted with the new IP address. If the IP address is removed after the interface has been configured as an active probe source, active probing is stopped and not restarted until a valid primary IP address is configured.

PfR Voice Traffic Optimization Using Active Probes

PfR supports outbound optimization of voice traffic using active probes on the basis of voice metrics such as delay, reachability, jitter, and Mean Opinion Score (MOS).

For more details about optimizing voice traffic, see the "PfR Voice Traffic Optimization Using Active Probes" module.

Combined Monitoring

Cisco IOS PfR can also be configured to combine both active and passive monitoring in order to generate a more complete picture of traffic flows within the network. There are some scenarios in which you may want to combine both PfR monitoring modes.

One example scenario is when you want to learn traffic classes and then monitor them passively, but you also want to determine the alternate path performance metrics in order to control the traffic classes. The alternate path performance metrics, in the absence of the actual traffic flowing through the alternate path in the network, can be measured using the active probes. PfR automates this process by learning traffic classes at five targets and probing through all the alternate paths using active probes.

Fast Failover Monitoring

Fast monitoring sets the active probes to continuously monitor all the exits (probe-all), and passive monitoring is enabled too. Fast failover monitoring can be used with all types of active probes: ICMP echo, Jitter, TCP connection, and UDP echo. When the **mode monitor fast** command is enabled, the probe frequency can be set to a lower frequency than for other monitoring modes, to allow a faster failover ability. Under fast monitoring with a lower probe frequency, route changes can be performed within 3 seconds of an out-of-policy situation. When an exit becomes OOP under fast monitoring, the select best exit is operational and the routes from the OOP exit are moved to the best in-policy exit. Fast monitoring is a very aggressive mode that incurs a lot of overhead with the continuous probing. We recommend that you use fast monitoring only for performance sensitive traffic. For example, a voice call is very sensitive to any performance problems or congested links, but the ability to detect and reroute the call within a few seconds can demonstrate the value of using fast monitoring mode.

Note In fast monitoring mode, probe targets are learned as well as learned prefixes. To avoid triggering large numbers of probes in the network, use fast monitoring mode only for real time applications and critical applications with performance sensitive traffic.

Special Monitoring

The PfR Border Router Only feature introduced the ability to run PfR on some hardware platforms that do not support the master controller functions but do allow these platforms to operate as border routers with limited functionality. The master controller that communicates with the Cisco Catalyst 6500 series switch or a Cisco 7600 series router being used as a border router must be a router running Cisco IOS Release 12.4(6)T or a later release.

A special monitoring mode was introduced, mode monitor special, as an alternate syntax to mode monitor both for the hardware platforms that do not support the master controller functions. The special mode is set globally and cannot be configured using the command-line interface (CLI). On hardware platforms that do not support the master controller functions, PfR cannot determine performance characteristics such as delay, loss, or reachability from passive monitoring of TCP flows; PfR can only measure passive throughput. Throughput-based load balancing is still supported and active probing is enabled to accommodate the passive monitoring limitations and this allows active IP SLA measurements. The master controller automatically detects the limited capabilities of the Cisco Catalyst 6500 series switch or a Cisco 7600 series router and downgrades other border routers to capture only the throughput statistics for traffic classes. By ignoring other types of statistics, the master controller is presented with a uniform view of the border router functionality.

Note The output from the **show oer master prefix** command lists an # next to the prefix with mode monitor special.

Link Utilization Measurement Techniques

Link Utilization Threshold

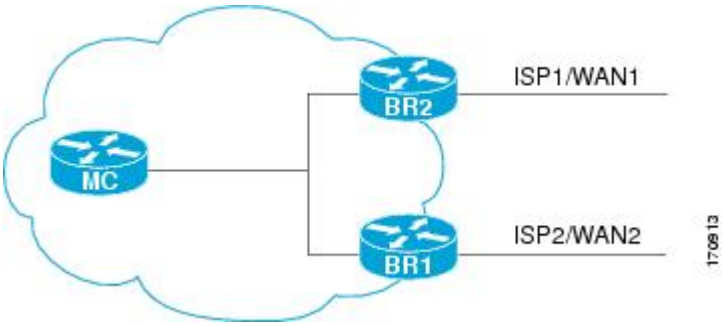
After an external interface is configured for a border router, PfR automatically monitors the utilization of the external link (an external link is an interface on a border router that typically links to a WAN). Every 20 seconds, by default, the border router reports the link utilization to the master controller. Both egress (transmitted) and ingress (received) traffic utilization values are reported to the master controller. If the exit or entrance link utilization is above the default threshold of 75-percent, the exit or entrance link is in an OOP state and PfR starts the monitoring process to find an alternative link for the traffic class. The link utilization threshold can be manually configured either as an absolute value in kilobytes per second (kbps) or as a percentage.

Link Utilization Range

PfR can also be configured to calculate the range of utilization over all the links. Both egress (transmitted) and ingress (received) traffic utilization values are reported to the master controller. In the diagram below

there are two border routers with exits links to the Internet through two ISPs. The master controller determines which link on one of the border routers--either BR1 or BR2 in the diagram below--is used by a traffic class.

Figure 6: PfR network diagram



PfR range functionality attempts to keep the exit or entrance links within a utilization range, relative to each other to ensure that the traffic load is distributed. The range is specified as a percentage and is configured on the master controller to apply to all the exit or entrance links on border routers managed by the master controller. For example, if the range is specified as 25-percent, and the utilization of the exit link at BR1 (in the diagram above) is 70-percent, then if the utilization of the exit link at BR2 (in the diagram above) falls to 40-percent, the percentage range between the two exit links will be more than 25-percent and PfR will attempt to move some traffic classes to use the exit link at BR1 to even the traffic load. If BR1 (in the diagram above) is being configured as an entrance link, the link utilization range calculations work in the same way as for an exit link, except that the utilization values are for received traffic, not transmitted traffic.

Note If you are configuring link grouping, configure the **no max-range-utilization** command because using a link utilization range is not compatible with using a preferred or fallback set of exit links configured for link grouping. With CSCtr33991, this requirement is removed and PfR can perform load balancing within a PfR link group.

Apply Policy Phase Concepts

Apply Policy Phase Overview

The PfR apply policy phase is the third step in the PfR performance loop following after the profile phase that identifies the traffic classes, and the measure phase where each traffic class entry in the MTC list is monitored to determine performance metric measurements. The apply policy phase compares the measured performance metrics against well-known or configured thresholds to determine if the traffic is meeting specified levels of service, or if some action is required. If the performance metric does not conform to the threshold, a decision is made by PfR to move the traffic class or exit into another state.

An PfR policy is a rule that defines an objective and contains the following attributes:

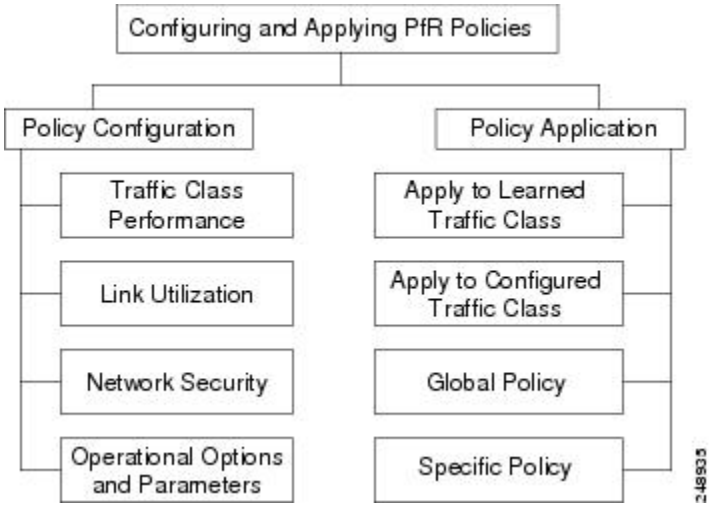
- A scope.
- An action.

- A triggering event or condition.

For example, a policy can be configured to maintain a delay of less than or equal to 100 milliseconds for packets sent to a specific traffic class entry. The scope is the network traffic sent to the specific traffic class entry, the action is a routing table change, and the triggering event is a measured delay of greater than 100 milliseconds for this traffic. The action may be not be executed until PfR is configured to control the traffic in the PfR control phase. By default, PfR runs in an observe mode during the profile, measure, and apply policy phases.

In the PfR apply policy phase you can configure and apply policies. Different types of PfR policies can be configured--see the figure below--and specific PfR parameters and options can be included within a policy. In this document, a parameter is a configurable element that can be fine-tuned, and an option is a configurable element that is either enabled or disabled. After an PfR policy is configured, the policy can be applied to learned traffic classes or configured traffic classes. PfR policies can be applied globally--to all the traffic classes--or to just a specific set of traffic classes.

Figure 7: PfR Apply Policy Phase Structure



In the figure above you can see that there are three types of PfR policies plus some operational options and parameters that can be configured. Use the following links to review more information about each policy type, parameter, or option:

After an PfR policy is configured, you can see from the figure above that a policy can be applied to learned traffic classes or configured traffic classes on a global basis for all traffic classes or for a specific set of traffic classes.

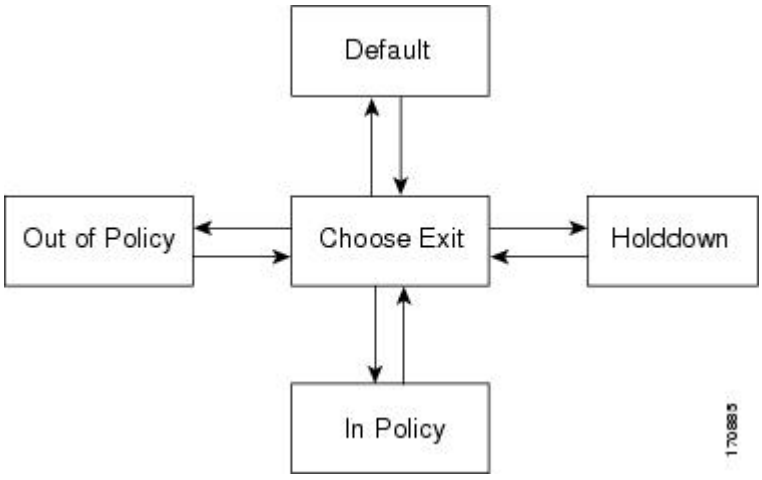
When configuring multiple policy parameters for traffic classes, it is possible to have multiple overlapping policies. To resolve the potential conflict of which policy to run, PfR uses its resolve function: a flexible mechanism that allows you to set the priority for most of the policy types.

PfR Policy Decision Point

When running an PfR policy that compares the traffic class performance metrics with default or configured thresholds, a traffic class may change state. PfR uses a policy decision point (PDP) that operates according to the traffic class state transition diagram shown in the figure below. The state transition diagram below contains the following states:

- Default--A traffic class is placed in the default state when it is not under PfR control. Traffic classes are placed in the default state when they are initially added to the central policy database, the MTC. A traffic class will transition into and out of the default state depending on performance measurements, timers, and policy configuration.
- Choose Exit--This is a temporary state in which the PDP compares the current state of the traffic class against its policy settings and chooses the optimal exit for the traffic class. PfR will try to keep a traffic class flowing through its current exit but, as in the default state, performance measurements, timers, and policy configurations can cause the master controller to place a traffic class in this state for the duration of the exit link selection process. The traffic class remains in the choose exit state until it is moved to the new exit.
- Holddown--A traffic class is placed in the holddown state when the master controller requests a border router to forward the traffic class to be monitored using probes. Measurements are collected for the selected traffic class until the holddown timer expires unless the exit used by this traffic class is declared unreachable. If the exit is unreachable, the traffic class transitions back to the choose exit state.

Figure 8: PfR Traffic Class State Transition Diagram



- In-Policy--After performance measurements are compared against default or user-defined policy settings and an exit selection is made, the traffic class enters an in-policy state. When a traffic class is in the in-policy state, the traffic class is forwarded through an exit that satisfies the default or user-defined settings. The master controller continues to monitor the traffic class, but no action is taken until the periodic timer expires, or an out-of-policy message is received from a measurement collector, when the traffic class transitions back to the choose exit state.

Note When observe mode is running, a prefix goes into an in-policy state only if the exit selected for that prefix is the current exit.

- Out-of-Policy (OOP)--A traffic class is placed in this state when there are no exits through which to forward the traffic class that conform to default or user-defined policies. While the traffic class is in this state, the backoff timer controls exiting from this state. Each time the traffic class enters this state, the amount of time the traffic class spends in this state increases. The timer is reset for a traffic class when

the traffic class enters an in-policy state. If all exit links are out-of-policy, the master controller may select the best available exit.

Traffic Class Performance Policies

PfR traffic class performance policies are a set of rules that govern performance characteristics for traffic classes that can be network addresses (prefixes) or application criteria such as protocol, port number, or DSCP value. Network addresses can refer to individual endpoints within a network (e.g. 10.1.1.1/32) or to entire subnets (e.g. 10.0.0.0/8). The major performance characteristics that can be managed within an PfR policy are:

With the exception of reachability, none of these performance characteristics can be managed within the constructs of conventional routing protocol metrics. Cisco PfR extends the concept of reachability (beyond ensuring that a particular route exists in the routing table) by automatically verifying that the destination can be reached through the indicated path. Using Cisco PfR provides the network administrator with a new and powerful toolset for managing the flow of traffic.

Reachability

Reachability is specified as the relative percentage or the absolute maximum number of unreachable hosts, based on flows per million (fpm), that PfR will permit from a traffic class entry. If the absolute number or relative percentage of unreachable hosts is greater than the user-defined or the default value, PfR determines that the traffic class entry is out-of-policy and searches for an alternate exit link.

To configure parameters for reachability, use the **unreachable** (PfR) command. This command has two keywords, **relative** and **threshold**. The **relative** keyword is used to configure the relative percentage of unreachable hosts. The relative unreachable host percentage is based on a comparison of short-term and long-term measurements. The short-term measurement reflects the percentage of hosts that are unreachable within a 5-minute period. The long-term measurement reflects the percentage of unreachable hosts within a 60-minute period. The following formula is used to calculate this value:

Relative percentage of unreachable hosts = ((short-term percentage - long-term percentage) / long-term percentage) * 100

The master controller measures the difference between these two values as a percentage. If the percentage exceeds the user-defined or default value, the traffic class entry is determined to be out-of-policy. For example, if 10 hosts are unreachable during the long-term measurement and 12 hosts are unreachable during short-term measurement, the relative percentage of unreachable hosts is 20 percent.

The **threshold** keyword is used to configure the absolute maximum number of unreachable hosts. The maximum value is based on the actual number of hosts that are unreachable based on fpm.

Delay

Delay (also referred as latency) is defined as the delay between when the packet was sent from the source device and when it arrived at a destination device. Delay can be measured as one-way delay or round-trip delay. The largest contributor to latency is caused by network transmission delay.

PfR supports defining delay performance characteristics with respect to voice traffic. Round-trip delay affects the dynamics of conversation and is used in Mean Opinion Score (MOS) calculations. One-way delay is used for diagnosing network problems. A caller may notice a delay of 200 milliseconds and try to speak just as the other person is replying because of packet delay. The telephone industry standard specified in ITU-T G.114 recommends the maximum desired one-way delay be no more than 150 milliseconds. Beyond a one-way

delay of 150 milliseconds, voice quality is affected. With a round-trip delay of 300 milliseconds or more, users may experience annoying talk-over effects.

Packet Loss

Packet loss can occur due an interface failing, a packet being routed to the wrong destination, or congestion in the network.

Packet loss for voice traffic leads to the degradation of service in which a caller hears the voice sound with breaks. Although average packet loss is low, voice quality may be affected by a short series of lost packets.

Jitter

PfR supports defining jitter performance characteristics. Jitter means interpacket delay variance. When multiple packets are sent consecutively from source to destination, for example, 10 ms apart, and if the network is behaving ideally, the destination should be receiving them 10 ms apart. But if there are delays in the network (like queuing, arriving through alternate routes, and so on) the arrival delay between packets might be greater than or less than 10 ms. Using this example, a positive jitter value indicates that the packets arrived more than 10 ms apart. If the packets arrive 12 ms apart, then positive jitter is 2 ms; if the packets arrive 8 ms apart, then negative jitter is 2 ms. For delay-sensitive networks like VoIP, both positive and negative jitter values are undesirable; a jitter value of 0 is ideal.

Mean Opinion Score (MOS)

PfR supports defining MOS performance characteristics. With all the factors affecting voice quality, many people ask how voice quality can be measured. Standards bodies like the ITU have derived two important recommendations: P.800 (MOS) and P.861 (Perceptual Speech Quality Measurement [PSQM]). P.800 is concerned with defining a method to derive a Mean Opinion Score of voice quality. MOS scores range between 1 representing the worst voice quality, and 5 representing the best voice quality. A MOS of 4 is considered "toll-quality" voice.

Jitter and MOS performance characteristic can be configured in an PfR policy as well as delay and packet loss to determine the quality of a phone call over an IP network.

PfR Link Policies

PfR link policies are a set of rules that are applied against PfR-managed external link (an external link is an interface on a border router on the network edge). Link policies define the desired performance characteristics of the links. Instead of defining the performance of an individual traffic class entry that uses the link (as in traffic class performance policies), link policies are concerned with the performance of the link as a whole. Link policies can be applied to exit (egress) links and entrance (ingress) links. The following performance characteristics are managed by link policies:

- Traffic Load (Utilization)
- Range
- Cost

Traffic Load

A traffic load (also referred to as utilization) policy consists of an upper threshold on the amount of traffic that a specific link can carry. Cisco IOS PfR supports per traffic class load distribution. Every 20 seconds, by default, the border router reports the link utilization to the master controller, after an external interface is

configured for a border router. Exit link and entrance link traffic load thresholds can be configured as an PfR policy. If the exit or entrance link utilization is above the configured threshold, or the default threshold of 75-percent, the exit or entrance link is in an OOP state and PfR starts the monitoring process to find an alternative link for the traffic class. The link utilization threshold can be manually configured either as an absolute value in kilobits per second (kbps) or as a percentage. A load utilization policy for an individual interface is configured on the master controller under the border router configuration.

Tip When configuring load distribution, we recommend that you set the interface load calculation on external interfaces to 30-second intervals with the **load-interval** (PfR) interface configuration command. The default calculation interval is 300 seconds. The load calculation is configured under interface configuration mode on the border router. This configuration is not required, but it is recommended to allow Cisco IOS PfR to respond as quickly as possible to load distribution issues.

Range

A range policy is defined to maintain all links within a certain utilization range, relative to each other in order to ensure that the traffic load is distributed. For example, if a network has multiple exit links, and there is no financial reason to choose one link over another, the optimal choice is to provide an even load distribution across all links. The load-sharing provided by traditional routing protocols is not always evenly distributed, because the load-sharing is flow-based rather than performance- or policy-based. Cisco PfR range functionality allows you to configure PfR to maintain the traffic utilization on a set of links within a certain percentage range of each other. If the difference between the links becomes too great, PfR will attempt to bring the link back to an in-policy state by distributing traffic classes among the available links. The master controller sets the maximum range utilization to 20 percent for all PfR-managed links by default, but the utilization range can be configured using a maximum percentage value. Exit link and entrance link utilization ranges can be configured as a PfR policy.

Note If you are configuring link grouping, configure the **no max-range-utilization** command because using a link utilization range is not compatible with using a preferred or fallback set of exit links configured for link grouping. With CSCtr33991, this requirement is removed and PfR can perform load balancing within a PfR link group.

Cost

Cost-based optimization allow you to configure policies based on the monetary cost (ISP service level agreements [SLAs]) of each exit link in your network. To implement PfR cost-based optimization the PfR master controller is configured to send traffic over exit links that provide the most cost-effective bandwidth utilization, while still maintaining the desired performance characteristics.

Cost Based Optimization can be applied to links that are billed using a fixed or tiered billing method and load balancing based on cost can also be achieved. For more configuration details, see the “Configuring Performance Routing Cost Policies” module.

PfR Link Grouping

In the Performance Routing - Link Groups feature, the ability to define a group of exit links as a preferred set of links, or a fallback set of links for PfR to use when optimizing traffic classes specified in an PfR policy,

was introduced. PfR currently selects the best link for a traffic class based on the preferences specified in a policy and the traffic class performance--using parameters such as reachability, delay, loss, jitter or MOS--on a path out of the specified link. Bandwidth utilization, cost, and the range of links can also be considered in selecting the best link. Link grouping introduces a method of specifying preferred links for one or more traffic classes in an PfR policy so that the traffic classes are routed through the best link from a list of preferred links, referred to as the primary link group. A fallback link group can also be specified in case there are no links in the primary group that satisfy the specified policy and performance requirements. If no primary group links are available, the traffic classes are routed through the best link from the fallback group. To identify the best exit, PfR probes links from both the primary and fallback groups.

Note If you are configuring link grouping, configure the **no max-range-utilization** command because using a link utilization range is not compatible with using a preferred or fallback set of exit links configured for link grouping. With CSCtr33991, this requirement is removed and PfR can perform load balancing within a PfR link group.

For more details about PfR link grouping, see the “Performance Routing Link Groups” module.

PfR Network Security Policies

The ability to configure network security policies either to prevent unauthorized use of the network or to mitigate attacks inside and outside the network is provided by PfR. You can configure PfR to use black hole or sinkhole routing techniques to limit the impact of attacks against your network. Black hole routing refers to the process of forwarding packets to a null interface, meaning that the packets are dropped into a "black hole." Sinkhole routing directs packets to a next hop where the packets can be stored, analyzed, or dropped. Another term for sinkhole routing is honey-pot routing.

PfR Policy Operational Options and Parameters

In addition to the specific types of PfR policies, there are some PfR policy operational parameters or options that can be configured. The operational parameters are timers and the operational options consist of different operational modes. For more details, see the following sections:

PfR Timers Parameters

Three types of timers can be configured as PfR policy operational parameters:

Backoff Timer

The backoff timer is used to adjust the transition period that the master controller holds an out-of-policy traffic class entry. The master controller waits for the transition period before making an attempt to find an in-policy exit. A minimum, a maximum, and an optional step timer value can be configured.

Holddown Timer

The holddown timer is used to configure the traffic class entry route dampening timer to set the minimum period of time that a new exit must be used before an alternate exit can be selected. To prevent the traffic class entry from flapping because of rapid state changes, the master controller does not move the traffic class entry to a different exit even if it goes out-of-policy during the holddown timer period. PfR does not implement policy changes while a traffic class entry is in the holddown state. A traffic class entry will remain in a

holddown state for the default or configured time period. When the holddown timer expires, PfR will select the best exit based on performance and policy configuration. However, an immediate route change will be triggered if the current exit for a traffic class entry becomes unreachable.

Periodic Timer

The periodic timer is used to find a better path for a traffic class entry, even if the traffic class entry is in-policy on the current exit. When the periodic timer expires, the master controller evaluates current exit links for the traffic class entry and, if a better exit exists based on the current measurements and priorities, the traffic class entry is moved to a new in-policy exit link.

When adjusting PfR timers note that a newly configured timer setting will immediately replace the existing setting if the value of the new setting is less than the time remaining. If the value is greater than the time remaining, the new setting will be applied when the existing timer expires or is reset.

Note Overly aggressive timer settings can keep an exit link or traffic class entry in an out-of-policy state.

PfR Mode Options

Three types of mode options can be configured as PfR policy operational options:

Mode Monitor

The mode monitor option enables the configuration of PfR monitoring settings. Monitoring is defined here as the act of measurement performed periodically over a set interval of time where the measurements are compared against a threshold. PfR measures the performance of traffic classes using active and passive monitoring techniques but it also measures, by default, the utilization of exit links.

Mode Route

The mode route option specifies one of three PfR route control policy settings. Mode route control enables PfR to control routes automatically, mode route metric specifies PfR route protocol-related settings, and mode route observe offers route control advice, but does not take any action. Observe mode monitoring is enabled by default when PfR is enabled. In observe mode, the master controller monitors traffic classes and exit links based on default and user-defined policies and then reports the status of the network and the decisions that should be made but does not implement any changes. Observe mode is used to verify the effect of PfR features before PfR is actively deployed on your network.

If you have different routing protocols operating on your PfR border routers (for example, BGP on one border router and EIGRP on another) you must configure the **protocol** and **pbr** keywords with the mode route command to allow destination-only traffic classes to be controlled using dynamic PBR. Entering the **no mode route protocol pbr** command will initially set the destination-only traffic classes to be uncontrolled and PfR then reverts to the default behavior using a single protocol to control the traffic class in the following order; BGP, EIGRP, static, and PBR.

Mode Select-Exit

The mode select-exit option enables the exit selection settings. The definition of an in-policy traffic class entry is that the measured performance metrics do not exceed a default or configured threshold while the traffic class entry is on the current path. In this situation, PfR does not search for an alternate exit link because the current network path keeps the traffic class entry in-policy. This type of configuration would be activated

by using the **mode select-exit good** command which is the default if the **mode** (PfR) command is not specified. There are other deployment scenarios, where PfR selects the best performance path. This type of configuration can be activated by using the **mode select-exit best** command. In this type of situation, PfR measures alternate path performance metrics while the traffic class entry is in-policy on the current path. PfR moves the current path if a better performance path is found. After the first selection of the best path, however, PfR does not initiate another search unless the periodic timer is configured. When the periodic timer expires, the master controller evaluates current exit links for the traffic class entry and, if a better exit exists based on the current measurements and priorities, the traffic class entry is moved to a new in-policy exit link. Use the periodic timer with the **mode select-exit best** command if you have a deployment scenario where you need PfR to select the best performance path at any given time.

There is one further use of the mode select-exit option. If PfR does not find an in-policy exit for a traffic class entry when the **mode select-exit good** command is operational, PfR transitions the traffic class entry to an uncontrolled state. If PfR does not find an in-policy exit for a traffic class entry when the **mode select-exit best** command is operational, PfR selects the best of the OOP exit links for the traffic class entry.

PfR Policy Application

PfR policies can be applied to learned or configured traffic classes. PfR policies can be applied on a global basis when the policy is configured directly under PfR master controller configuration mode. All traffic classes inherit global policies. If, however, you want to apply a policy to a subset of the traffic classes, then a specific policy can be configured. A specific PfR policy applies only to the specific traffic classes that match a prefix list or access list. Specific policies inherit global policies unless the same policy is overwritten by the specific policy. PfR policies can apply to prefixes alone, or PfR policies can apply to traffic classes that define an application traffic class and may include prefixes, protocols, port numbers, and DSCP values. To apply specific policies to learned or configured traffic classes, PfR map configuration is used.

PfR Map Configuration for PfR Policies

A PfR map may appear to be similar to a route map but there are significant differences. A PfR map is designed to select learned or configured traffic classes using a match clause and then to apply PfR policy configurations using a set clause. The PfR map can be optionally configured with a sequence number like a route map, but only the PfR map with the lowest sequence number is evaluated. The operation of a PfR map differs from a route map at this point. There are two important distinctions:

- Only a single match clause may be configured for each sequence. An error message will be displayed on the console if you attempt to configure multiple match clauses for a single PfR map sequence.
- A PfR map is not configured with permit or deny statements. However, a permit or deny sequence can be configured for an IP traffic flow by configuring a permit or deny statement in an IP prefix list and then applying the prefix list to the PfR map.

Note Match precedence priority is not supported in PfR maps.

The PfR map applies the configuration of the set clause after a successful match occurs. A PfR set clause can be used to set policy parameters such as the backoff timer, packet delay, holddown timer, packet loss, mode settings, periodic timer, resolve settings, unreachable hosts, and traceroute reporting.

Policies applied by an PfR map take effect immediately. The PfR map configuration can be viewed in the output of the **show running-config** command. PfR policy configuration can be viewed in the output of the

show pfr master policy command. These policies are applied only to traffic classes that match or pass through the PfR map.

Policy Rules Configuration to Apply an PfR Policy

The **policy-rules** (PfR) command allows you to select a PfR map using a sequence number and apply the configuration under PfR master controller configuration mode, providing an improved method to switch between predefined PfR maps. Only one PfR map is used at a time for policy configuration, but many PfR maps can be defined.

Priority Resolution for Multiple PfR Policies

When configuring multiple policy criteria for a single traffic class entry, or a set of traffic classes, it is possible to have multiple overlapping policies. To resolve the potential conflict of which policy to run, PfR uses its resolve function: a flexible mechanism that allows you to set the priority for a PfR policy. Each policy is assigned a unique value, and the policy with the lowest value is selected as the highest priority policy. By default, PfR assigns the highest priority to delay policies, followed by utilization policies. Assigning a priority value to any policy will override the default settings. To configure the policy conflict resolution, use the **resolve** (PfR) command in PfR master controller configuration mode, or the **set resolve** (PfR) command in PfR map configuration mode.

Variance Setting for PfR Policy Conflict Resolution

When configuring PfR resolve settings, you can also set an allowable variance for the defined policy. Variance configures the average delay, as a percentage, that all traffic classes for one exit, or the specific policy traffic classes for an exit, can vary from the defined policy value and still be considered equivalent. For example, if the delay on the best exit link (best exit in terms of delay) for a traffic class entry is 80 milliseconds (ms) and a 10 percent variance is configured, then any other exit links with a delay between 80 and 88 ms for the same traffic class entry are considered equivalent to the best exit link.

To illustrate how variance is used by PfR consider three exit links with the following performance values for delay and jitter for a traffic class entry:

- Exit A--Delay is 80 ms, jitter is 3ms
- Exit B--Delay is 85 ms, jitter is 1ms
- Exit C--Delay is 100 ms, jitter is 5ms

The following PfR policy conflict resolution is configured and applied to the traffic class entry:

```
delay priority 1 variance 10
jitter priority 2 variance 10
```

PfR determines the best exit by looking at the policy with the lowest priority value, which in this example is the delay policy. Exit A has the lowest delay value, but Exit B has a delay value of 85 which is within a 10-percent variance of the delay value at Exit A. Exit A and Exit B can therefore be considered equal in terms of delay values. Exit C is now eliminated because the delay values are too high. The next priority policy is jitter, and Exit B has the lowest jitter value. PfR will select Exit B as the only best exit for the traffic class entry because Exit A has a jitter value that is not within 10-percent variance of the Exit B jitter value.

Note Variance cannot be configured for cost or range policies.

Enforce Phase Concepts

PfR Enforce Phase Overview

After profiling the traffic classes during the PfR learn phase, measuring the performance metrics of the traffic classes during the measure phase, and using network policies to map the measured performance metrics of traffic class entries in the Monitored Traffic Class (MTC) list against well-known or configured thresholds to determine if the traffic is meeting specified levels of service in the policy phase, the next step in the PfR performance loop is the PfR enforce phase.

PfR, by default, operates in an observation mode and the documentation for the PfR learn, measure, and apply policy phases assumes that PfR is in the observe mode. In observe mode, the master controller monitors traffic classes and exit links based on default and user-defined policies and then reports the status of the network including out-of-policy (OOP) events and the decisions that should be made, but does not implement any changes. The PfR enforce phase operates in control mode, not observe mode, and control mode must be explicitly configured using the **mode route control** command. In control mode, the master controller coordinates information from the borders routers in the same way as observe mode, but commands are sent back to the border routers to alter routing in the PfR managed network to implement the policy decisions.

PfR initiates route changes when one of the following occurs:

- A traffic class goes OOP.
- An exit link goes OOP.
- The periodic timer expires and the select exit mode is configured as select best mode.

During the PfR enforce phase, the master controller continues to monitor in-policy traffic classes that conform to the desired performance characteristics, to ensure that they remain in-policy. Changes are only implemented for OOP traffic classes and exits in order to bring them in-policy. To achieve the desired level of performance in your network, you must be aware of the configuration options that can affect the policy decisions made by the master controller.

Another configuration issue to consider when deploying PfR is that if aggressive delay or loss policies are defined, and the exit links are also seriously over-subscribed, it is possible that PfR will find it impossible to bring a traffic class in-policy. In this case, the master controller will either choose the link that most closely conforms to the performance policy, even though the traffic class still remains OOP, or it will remove the prefix from PfR control. PfR is designed to allow you to make the best use of available bandwidth, but it does not solve the problem of over-subscribed bandwidth.

After PfR control mode is enabled, and configuration options are considered, the next step is to review the traffic class control techniques employed by PfR.

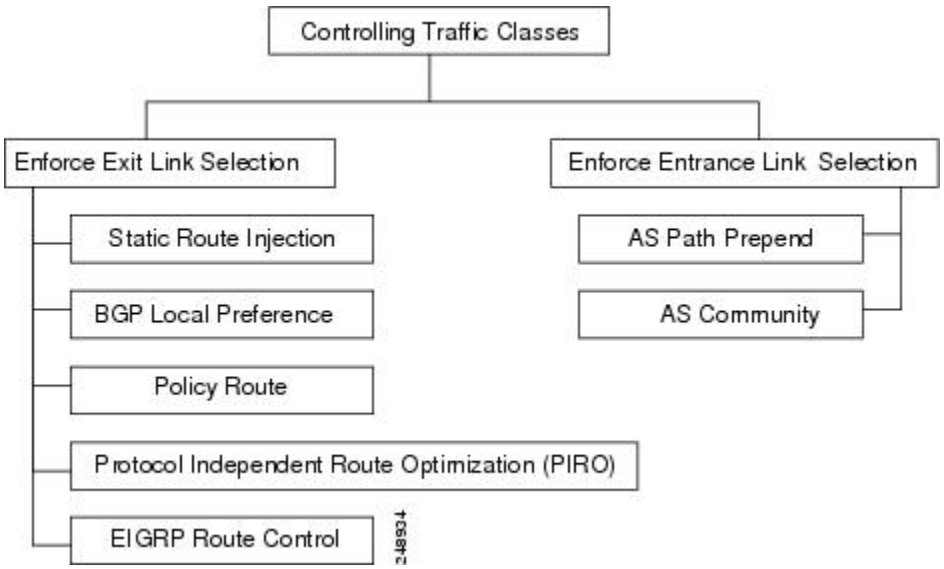
PfR Traffic Class Control Techniques

After the PfR master controller has determined that it needs to take some action involving an OOP traffic class or exit link, there are a number of techniques that can be used to alter the routing metrics, alter BGP attributes, or introduce policy-based routing using a route map to influence traffic to use a different link. If the traffic associated with the traffic class is defined only by a prefix then a traditional routing control mechanism such as introducing a BGP route or a static route can be deployed. This control is network wide after redistribution because a prefix introduced into the routing protocol with a better metric will attract traffic for that prefix towards a border router. If the traffic associated with the traffic class is defined by a prefix and

other matching criteria for the packet (application traffic, for example), then traditional routing cannot be employed to control the application traffic. In this situation, the control becomes device specific and not network specific. This device specific control is implemented by PfR using policy-based routing (PBR) functionality. If the traffic in this scenario has to be routed out to a different device, the remote border router should be a single hop away or a tunnel interface that makes the remote border router look like a single hop.

The figure below shows the various traffic class control techniques grouped by exit or entrance link selection.

Figure 9: Controlling Traffic Class Techniques



PfR Exit Link Selection Control Techniques

Before introducing the exit link selection control techniques you need to understand one principle about load balancing with Performance Routing as it applies to exit selection. PfR does not treat a more specific route as a parent route unless you configure the more specific route as a default route.

When searching for a parent route, the software tries to find the most specific route that includes the specified prefix and verifies that it points to the expected exit. If there are two or more static routes that are more specific, each route is inspected for the expected exit. If the expected exit is found, the probe is created.

In the configuration where:

```
ip route 10.4.0.0 255.255.0.0 172.17.40.2
ip route 0.0.0.0 0.0.0.0 serial 6/0
```

Probes for prefix 10.4.1.0/24 and target 10.4.1.1 will not be created over the exit using serial interface 6/0 because the most specific route inclusive of 10.4.1.1 is the exit to 172.17.40.2. If you are looking to load balance the traffic over both exits, the answer is to create a default route of the more specific route. For example:

```
ip route 10.4.0.0 255.255.0.0 172.17.40.2
ip route 10.4.0.0 255.255.0.0 serial 6/0
```

Or

```
ip route 0.0.0.0 0.0.0.0 serial 6/0
ip route 0.0.0.0 0.0.0.0 172.17.40.2
```

In the modified configuration, two probes are created, one for the exit to 172.17.40.2 and one for the exit using serial interface 6/0.

To enforce an exit link selection, PfR offers the following methods:

Static Route Injection

A PfR master controller can enforce the use of a particular border router as the preferred exit link for a traffic class by injecting temporary static routes. These static routes exist only in the memory of the router, and are intentionally not saved to the permanent configuration. There are a few different methods that the master controller can use to inject static routes on the border routers. Existing static routes can be overwritten with new static routes, which have a better routing metric. If a default route, or even a less specific route, exists on the border router, the master controller can add a specific static route for the monitored traffic classes, which will be preferred to the existing default route. Finally, the master controller can also use something known as split prefixes.

A split prefix refers to the addition of a more specific route, which will be preferred over a less specific route. For example, if the border router already has a route of 10.10.10.0/24, adding a static route of 10.10.10.128/25 will also cause the addresses 10.10.10.129-10.10.10.254 to be forwarded using the newly injected route. If PfR has been configured to monitor a subset of a larger network, it will add an appropriate route to the existing routing table. PfR can use split prefixes to redirect subsets of an existing prefix to a more optimal exit link, and can use split prefixes for both internal BGP (iBGP) and static routes.

PfR will never inject a route where one does not already exist in the routing protocol table. Before injecting a route of a particular type, PfR will verify that a route exists in the BGP or static table that includes the prefix and points to the exit link. This route may be a default route.

BGP Control Techniques

PfR uses two BGP techniques to enforce the best exit path; injecting a BGP route, or modifying the BGP local preference attribute.

If the traffic associated with the traffic class is defined only by a prefix, the master controller can instruct a border router to inject a BGP route into the BGP table to influence traffic to use a different link. All PfR injected routes remain local to an autonomous system, and these injected routes are never shared with external BGP peers. As a safeguard to ensure this behavior, when PfR injects a BGP route, it will set the no-export community on it. This is done automatically, and does not require any user configuration. However, because these routes now have a special marking, some extra configuration is required to allow the information to be shared with internal BGP peers. For each iBGP peer, the send community configuration must be specified. Although the border routers know about the best exit for the injected route, it may also be necessary to redistribute this information further into the network.

PfR also uses BGP local preference to control traffic classes. BGP local preference (Local_Pref) is a discretionary attribute applied to a BGP prefix to specify the degree of preference for that route during route selection. The Local_Pref is a value applied to a BGP prefix, and a higher Local_Pref value causes a route to be preferred over an equivalent route. The master controller instructs one of the border routers to apply the Local_Pref attribute to a prefix or set of prefixes associated with a traffic class. The border router then shares the Local_Pref value with all of its internal BGP peers. Local_Pref is a locally significant value within an autonomous system, but it is never shared with external BGP peers. Once the iBGP reconvergence is complete, the router with the highest Local_Pref for the prefix will become the exit link from the network.

Note If a local preference value of 5000 or higher has been configured for default BGP routing, you should configure a higher BGP local preference value in PfR using the **mode** (PfR) command.

EIGRP Route Control

The PfR EIGRP mGRE DMVPN Hub-and-Spoke Support feature introduced PfR route control for EIGRP. When enabled, a parent route check is performed in the EIGRP database for controlling PfR prefixes/routes in addition to the existing BGP and static route databases. For more details, see the "Using Performance Routing to Control EIGRP Routes with mGRE DMVPN Hub-and-Spoke Support" module.

Policy-Based Routing Control

PfR can control application traffic using policy-based routing. Application traffic traveling through a particular PfR border router can be identified by matching traffic defined in a PfR map as part of a PfR policy. The **match ip address** (PfR) command was enhanced to support extended ACLs. The extended ACL is referenced in an PfR map, and a single match clause can be configured for each PfR map sequence. Set clauses are configured to apply independent PfR policies to the matched traffic, which is a subset of a monitored prefix. The PfR policy is applied to all border routers to enforce policy routing for the application. Matched traffic is policy routed through the PfR external interface that conforms to policy parameters.

DSCP values, as well as prefixes, port numbers, and protocols, can all be used to identify and control application traffic. DSCP values, protocols, and port numbers are sent by the border routers to the master controller for inclusion in the MTC list.

Protocol Independent Route Optimization (PIRO)

PIRO was introduced to extend the ability of PfR to identify and control traffic classes. Prior to PIRO, PfR optimizes paths for traffic classes that have a parent route--an exact matching route, or a less specific route--in BGP or static route databases. PIRO enables PfR to search the IP Routing Information Base (RIB) for a parent route allowing PfR to be deployed in any IP-routed environment including Interior Gateway Protocols (IGPs) such as OSPF and IS-IS.

For more details, see the "PfR Protocol Independent Route Optimization" module.

PfR Entrance Link Selection Control Techniques

The PfR BGP inbound optimization feature introduced the ability to influence inbound traffic. A network advertises reachability of its inside prefixes to the Internet using eBGP advertisements to its ISPs. If the same prefix is advertised to more than one ISP, then the network is multihoming. PfR BGP inbound optimization works best with multihomed networks, but it can also be used with a network that has multiple connections to the same ISP. To implement BGP inbound optimization, PfR manipulates eBGP advertisements to influence the best entrance selection for traffic bound for inside prefixes. The benefit of implementing the best entrance selection is limited to a network that has more than one ISP connection.

For more details about PfR entrance link selection control techniques, see the "BGP Inbound Optimization Using Performance Routing" module.

Verify Phase Concepts

Verify Phase Overview

The last phase of the PfR performance loop is to verify that the actions taken during the PfR control phase control actually change the flow of traffic and that the performance of the traffic class or link does move to an in-policy state. PfR uses NetFlow to automatically verify the route control. The master controller expects

a Netflow update for the traffic class from the new link interface and ignores Netflow updates from the previous path. If a Netflow update does not appear after two minutes, the master controller moves the traffic class into the default state. A traffic class is placed in the default state when it is not under PfR control.

In addition to the NetFlow verification used by PfR, there are two other methods you can use to verify that PfR has initiated changes in the network:

- Syslog report--The logging command can be configured to notify you of all the main PfR state changes, and a syslog report can be run to confirm that PfR changes have occurred. The master controller is expecting bidirectional traffic, and a syslog report delimited for the specified prefix associated with the traffic class can confirm this.
- PfR show commands--PfR show commands can be used to verify that network changes have occurred and that traffic classes are in-policy. Use the **show pfr master prefix** command to display the status of monitored prefixes. The output from this command includes information about the current exit interface, prefix delay, egress and ingress interface bandwidth, and path information sourced from a specified border router. Use the **show pfr border routes** command to display information about PfR controlled routes on a border router. This command can display information about BGP or static routes.

Where To Go Next

To access configuration tasks and configuration examples that implement the concepts contained in this module, see the "Configuring Advanced Performance Routing" module. For details about other Performance Routing modules and features, see the "Related Documents" section.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco PfR commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples	Cisco IOS Performance Routing Command Reference
Basic PfR configuration	"Configuring Basic Performance Routing" module
Concepts required to understand the Performance Routing operational phases	"Understanding Performance Routing" module
Advanced PfR configuration	"Configuring Advanced Performance Routing" module
IP SLAs overview	*IP SLAs Configuration Guide*
PfR home page with links to PfR-related content on our DocWiki collaborative environment	PfR:Home

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 Understanding Performance 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 3: Feature Information for Understanding Performance Routing

Feature Name	Releases	Feature Configuration Information
Port and Protocol Based Prefix Learning	12.3(11)T 12.2(33)SRB	Port and protocol based prefix learning allows you to configure a master controller to learn prefixes based on the protocol type and TCP or UDP port number. The **protocol** (PfR) command was introduced by this feature.
expire command[1]	12.3(14)T 12.2(33)SRB	The **expire after** (PfR) command is used to set an expiration period for learned prefixes. By default, the master controller removes inactive prefixes from the central policy database as memory is needed. This command allows you to refine this behavior by setting a time or session based limit. The time based limit is configured in minutes. The session based limit is configured for the number of monitor periods (or sessions).

Feature Name	Releases	Feature Configuration Information
OER Active Probe Source Address	12.4(2)T 12.2(33)SRB	The OER Active Probe Source Address feature allows you to configure a specific exit interface on the border router as the source for active probes. The **active-probe address source** (PfR) command was introduced by this feature.
OER Application-Aware Routing: PBR	12.4(2)T 12.2(33)SRB	The OER Application-Aware Routing: PBR feature introduces the capability to optimize IP traffic based on the type of application that is carried by the monitored prefix. Independent policy configuration is applied to the subset (application) of traffic. The following commands were introduced or modified by this feature: **debug pfr border pbr**, **debug pfr master prefix**, **match ip address (PfR)**, **show pfr master active-probes**, and **show pfr master appl**.

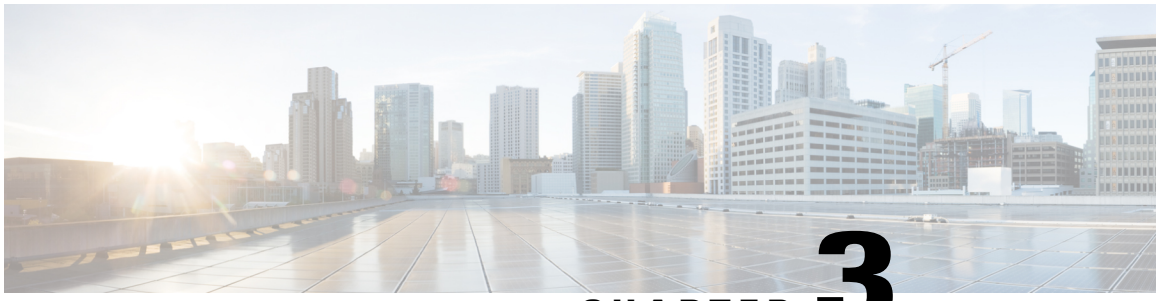
Feature Name	Releases	Feature Configuration Information
OER DSCP Monitoring	12.4(9)T 12.2(33)SRB	OER DSCP Monitoring introduced automatic learning of traffic classes based on protocol, port numbers, and DSCP value. Traffic classes can be defined by a combination of keys comprising of protocol, port numbers, and DSCP values, with the ability to filter out traffic that is not required, and the ability to aggregate the traffic in which you are interested. Layer 4 information such as protocol, port number, and DSCP information is now sent to the master controller database in addition to the Layer 3 prefix information. The new functionality allows PfR to both actively and passively monitor application traffic. The following commands were introduced or modified by this feature: **show pfr border passive applications**, **show pfr border passive cache**, **show pfr border passive learn**, **show pfr master appl**, **traffic-class aggregation** (PfR), **traffic-class filter** (PfR), and **traffic-class keys** (PfR).

Feature Name	Releases	Feature Configuration Information
OER Border Router Only Functionality	12.2(33)SXH 12.2(33)SRB	Border Router Only Functionality was introduced in Cisco IOS Release 12.2(33)SXH and in Cisco IOS Release 12.2(33)SRB. Due to hardware limitations, only border router functionality is available for the Cisco Catalyst 6500 series switch and Cisco 7600 series router; no master controller configuration is available. The master controller that communicates with the Cisco Catalyst 6500 series switch or Cisco 7600 series router being used as a border router must be a router running Cisco IOS Release 12.4(6)T or a later release. The PfR master controller software has been modified to handle the limited functionality and the border routers can capture throughput statistics only for a traffic class compared to the delay, loss, unreachability, and throughput statistics collected by routers and switches without the hardware limitation. A master controller automatically detects the limited capabilities and downgrades other border routers to capture only the throughput statistics for traffic classes. By ignoring other types of statistics, the master controller is presented with a uniform view of the border router functionality. The following command was introduced or modified by this feature: **show pfr border passive cache**.

Feature Name	Releases	Feature Configuration Information
OER Support for Policy-Rules Configuration	12.3(11)T 12.2(33)SRB	The OER Support for Policy-Rules Configuration feature introduced the capability to select a PfR map and apply the configuration under PfR master controller configuration mode, providing an improved method to switch between predefined PfR maps. The following commands were introduced or modified by this feature: **policy-rules** (PfR).
Support for Fast Failover Monitoring[2]	12.4(15)T	Fast Failover Monitoring introduced the ability to configure a fast monitoring mode. In fast failover monitoring mode, all exits are continuously probed using active monitoring and passive monitoring. The probe frequency can be set to a lower frequency in fast failover monitoring mode than for other monitoring modes, to allow a faster failover capability. Fast failover monitoring can be used with all types of active probes: ICMP echo, jitter, TCP connection, and UDP echo. The following commands were modified by this feature: **mode (PfR)**, **set mode** (PfR).

1 This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.

2 This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.



CHAPTER 3

Configuring Advanced Performance Routing

After configuring the Performance Routing (PfR) master controller and border routers (see the “Configuring Basic Performance Routing” module), additional configuration is required to activate the full optimization capabilities of PfR. Tasks and configuration examples that represent each of the PfR phases are documented here to help you learn how to configure and verify some of the advanced options for each PfR phase.

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 Table at the end of this document.

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.

Prerequisites for Configuring Advanced Performance Routing

- Before configuring the tasks in this module, you must configure a master controller and at least two border routers using the "Configuring Basic Performance Routing" module.

- Before configuring the tasks in this module, you must be familiar with the concepts contained in the "Understanding Performance Routing" module.
- Either routing protocol peering must be established on your network or static routing must be configured before route control mode is enabled.

If you have configured internal Border Gateway Protocol (iBGP) on the border routers, BGP peering must be either established and consistently applied throughout your network or redistributed into an Interior Gateway Protocol (IGP). The following IGPs are supported: Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), or Routing Information Protocol (RIP).

If an IGP is deployed in your network, static route redistribution must be configured with the **redistribute** command unless iBGP is configured. IGP or static routing should also be applied consistently throughout a PfR-managed network; the border router should have a consistent view of the network.

Caution Caution must be applied when redistributing PfR static routes into an IGP. The routes injected by PfR may be more specific than routes in the IGP, and it will appear as if the PfR border router is originating these routes. To avoid routing loops, the redistributed PfR static routes should never be advertised over a WAN by a PfR border router or any other router. Route filtering and stub network configuration can be used to prevent advertising the PfR static routes. If the PfR static routes are redistributed to routers terminating the PfR external interfaces, routing loops may occur.

Information About Advanced Performance Routing

To configure advanced PfR, you should understand the following concepts:

Performance Routing Overview

Performance Routing (PfR) is an advanced Cisco technology to allow businesses to complement classic routing technologies with additional serviceability parameters to select the best egress or ingress path. It complements these classic routing technologies with additional intelligence. PfR can select an egress or ingress WAN interface based upon parameters like reachability, delay, cost, jitter, MOS score, or it can use interface parameters like load, throughput and monetary cost. Classic routing (for example, EIGRP, OSPF, RIPv2, and BGP) generally focuses upon creating a loop-free topology based upon the shortest or least cost path.

PfR gains additional intelligence using measurement instrumentation. It uses interface statistics, Cisco IP SLA for active monitoring, and NetFlow for passive monitoring. No prior knowledge or experience of IP SLA or NetFlow is required, PfR automatically enables these technologies without any manual configuration.

Cisco Performance Routing selects an egress or ingress WAN path based on parameters that affect application performance, including reachability, delay, cost, jitter, and Mean Opinion Score (MOS). This technology can reduce network costs by facilitating more efficient load balancing and by increasing application performance without WAN upgrades.

PfR is an integrated Cisco IOS solution that allows you to monitor IP traffic flows and then define policies and rules based on traffic class performance, link load distribution, link bandwidth monetary cost, and traffic type. PfR provides active and passive monitoring systems, dynamic failure detection, and automatic path correction. Deploying PfR enables intelligent load distribution and optimal route selection in an enterprise network.

Advanced Performance Routing Deployment

Advanced PfR is configured on Cisco routers using Cisco IOS command-line interface (CLI) configurations. The PfR infrastructure includes a performance routing protocol that is communicated in a client-server messaging mode. The routing protocol employed by PfR runs between a network controller called a master controller and performance-aware devices called border routers. This performance routing protocol creates a network performance loop in which the network profiles which traffic classes have to be optimized, measures and monitors the performance metrics of the identified traffic classes, applies policies to the traffic classes, and routes the identified traffic classes based on the best performance path.

The PfR performance loop starts with the profile phase followed by the measure, apply policy, control, and verify phases. The flow continues after the verify phase back to the profile phase to update the traffic classes and cycle through the process.

Advanced PfR requires configuring tasks to address each of the following PfR Phases:

Profile Phase

In medium to large networks there are hundreds of thousands of routes in the RIB to which a device is trying to route traffic. Because performance routing is a means of preferring some traffic over another, a subset of the total routes in the RIB has to be selected to optimize for performance routing. PfR profiles traffic in one of two ways, automatic learning or manual configuration.

- Automatic Learning—The device profiles the traffic that has to be performance routed (optimized) by learning the flows that pass through the device and by selecting those flows that have the highest delay or the highest throughput.
- Manual configuration—In addition to, or instead of learning, you can configure a class of traffic to performance route.

Measure Phase

After profiling traffic classes that are to be performance routed, PfR measures the performance metrics of these individual traffic classes. There are two mechanisms--passive monitoring and active monitoring--to measure performance metrics, and one or both could be deployed in the network to accomplish this task. Monitoring is the act of measuring at periodic intervals.

Passive monitoring is the act of measuring the performance metrics of the traffic flow as the flow is traversing the device in the data path. Passive monitoring uses NetFlow functionality and cannot be employed for measuring performance metrics for some traffic classes, and there are some hardware or software limitations.

Active monitoring consists of generating synthetic traffic using IP Service Level Agreements (SLAs) to emulate the traffic class that is being monitored. The synthetic traffic is measured instead of the actual traffic class. The results of the synthetic traffic monitoring are applied to performance route the traffic class represented by the synthetic traffic.

Both passive and active monitoring modes can be applied to the traffic classes. The passive monitoring phase may detect traffic class performance that does not conform to an PfR policy, and then active monitoring can be applied to that traffic class to find the best alternate performance path, if available.

Support for NetFlow or IP SLAs configuration is enabled automatically.

Apply Policy Phase

After collecting the performance metrics of the class of traffic to be optimized, PfR compares the results with a set of configured low and high thresholds for each metric configured as a policy. When a metric, and consequently a policy, goes out of bounds, it is an Out-of-Policy (OOP) event. The results are compared on a relative basis--a deviation from the observed mean--or on a threshold basis--the lower or upper bounds of a value--or a combination of both.

There are two types of policies that can be defined in PfR: traffic class policies and link policies. Traffic class policies are defined for prefixes or for applications. Link policies are defined for exit or entrance links at the network edge. Both types of PfR policies define the criteria for determining an OOP event. The policies are applied on a global basis in which a set of policies is applied to all traffic classes, or on a more targeted basis in which a set of policies is applied to a selected (filtered) list of traffic classes.

With multiple policies, many performance metric parameters, and different ways of assigning these policies to traffic classes, a method of resolving policy conflicts was created. The default arbitration method uses a default priority level given to each performance metric variable and each policy. Different priority levels can be configured to override the default arbitration for all policies, or a selected set of policies.

Enforce Phase

In the PfR enforce phase (also called the control phase) of the performance loop, the traffic is controlled to enhance the performance of the network. The technique used to control the traffic depends on the class of traffic. For traffic classes that are defined using a prefix only, the prefix reachability information used in traditional routing can be manipulated. Protocols such as Border Gateway Protocol (BGP) or RIP are used to announce or remove the prefix reachability information by introducing or deleting a route and its appropriate cost metrics.

For traffic classes that are defined by an application in which a prefix and additional packet matching criteria are specified, PfR cannot employ traditional routing protocols because routing protocols communicate the reachability of the prefix only and the control becomes device specific and not network specific. This device specific control is implemented by PfR using policy-based routing (PBR) functionality. If the traffic in this scenario has to be routed out to a different device, the remote border router should be a single hop away or a tunnel interface that makes the remote border router look like a single hop.

Verify Phase

During the PfR enforce phase if a traffic class is OOP, then PfR introduces controls to influence (optimize) the flow of the traffic for the traffic class that is OOP. A static route and a BGP route are examples of controls introduced by PfR into the network. After the controls are introduced, PfR will verify that the optimized traffic is flowing through the preferred exit or entrance links at the network edge. If the traffic class remains OOP, PfR will drop the controls that were introduced to optimize the traffic for the OOP traffic class and cycle through the network performance loop.

PfR Active Probing Target Reachability

The active probe is sourced from the border router and transmitted through an external interface (the external interface may or may not be the preferred route for an optimized prefix). When creating an active probe through an external interface for a specified target, the target should be reachable through the external interface.

To test the reachability of the specified target, PfR performs a route lookup in the BGP and static routing tables for the specified target and external interface.

ICMP Echo Probes

Configuring an ICMP echo probe does not require knowledgeable cooperation from the target device. However, repeated probing could trigger an IDS alarm in the target network. If an IDS is configured in a target network that is not under your administrative control, we recommend that you notify the target network administration entity.

The following defaults are applied when active monitoring is enabled:

- The border router collects up to five host addresses from the traffic class for active probing when a traffic class is learned or aggregated.
- Active probes are sent once per minute.
- ICMP probes are used to actively monitor learned traffic classes.

Jitter

Jitter means interpacket delay variance. When multiple packets are sent consecutively from source to destination, for example, 10 ms apart, and if the network is behaving ideally, the destination should be receiving them 10 ms apart. But if there are delays in the network (like queuing, arriving through alternate routes, and so on) the arrival delay between packets might be greater than or less than 10 ms. Using this example, a positive jitter value indicates that the packets arrived more than 10 ms apart. If the packets arrive 12 ms apart, then positive jitter is 2 ms; if the packets arrive 8 ms apart, then negative jitter is 2 ms. For delay-sensitive networks like VoIP, positive jitter values are undesirable, and a jitter value of 0 is ideal.

MOS

Mean Opinion Score (MOS) is a quantitative quality metric for voice traffic that can be measured using PfR active probes. With all the factors affecting voice quality, many people ask how voice quality can be measured. Standards bodies like the ITU have derived two important recommendations: P.800 (MOS) and P.861 (Perceptual Speech Quality Measurement [PSQM]). P.800 is concerned with defining a method to derive a Mean Opinion Score of voice quality. MOS scores range between 1 representing the worst voice quality, and 5 representing the best voice quality. A MOS of 4 is considered "toll-quality" voice.

How to Configure Advanced Performance Routing

This section contains the following tasks:

Profiling Phase Tasks

The following tasks show how to configure elements of the PfR profiling phase:

Defining a Learn List for Automatically Learned Application Traffic Classes Using an Access List

Perform this task at the master controller to define a learn list that will contain traffic classes that are automatically learned by PfR using an access list to create customized application traffic classes. In this task, an access list is created that defines custom application traffic classes. Every entry in the access list defines one application. A learn list is then defined, the access list is applied, and an aggregation method is configured. Using the **count** (PfR) command, 50 traffic classes can be learned during one learning session for the learn list named LEARN_USER_DEFINED_TC, with a maximum specified number of 90 traffic classes for this learn list. The master controller is configured to learn the top prefixes based on highest delay for the filtered traffic and the resulting traffic classes are added to the PfR application database.

A learn list is activated using a PfR map and the last few steps in this task demonstrate how to configure a PfR map to activate the learn list defined in this task and create the custom traffic class.

For an example of defining a learn list for automatically learned prefix-based traffic classes using a prefix list, see the "Example: Defining a Learn List for Automatically Learned Prefix-Based Traffic Classes" section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list** {**standard** | **extended**} *access-list-name*
4. [*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**dscp** *dscp-value*]
5. Repeat Step 4 for more access list entries, as required.
6. **exit**
7. **pfr master**
8. **learn**
9. **list seq** *number* **refname** *refname*
10. **count** *number* **max** *max-number*
11. **traffic-class access-list** *access-list-name* [**filter** *prefix-list-name*]
12. **aggregation-type** {**bgp non-bgp prefix-length**} *prefix-mask*
13. **delay**
14. **exit**
15. Repeat Step 14 twice to return to global configuration mode.
16. **pfr-map** *map-name sequence-number*
17. **match traffic-class access-list** *access-list-name*
18. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip access-list** {**standard** | **extended**} *access-list-name* **Example:** `Router(config)# ip access-list extended USER_DEFINED_TC`	Defines an IP access list by name. • PfR supports only named access lists. • The example creates an extended IP access list named USER_DEFINED_TC.
Step 4	[*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**dscp** *dscp-value*] **Example:** `Router(config-ext-nacl)# permit tcp any any 500`	Sets conditions to allow a packet to pass a named IP access list. • The example is configured to identify all TCP traffic from any destination or source and from destination port number of 500. This specific TCP traffic is to be optimized. **Note** Only the syntax applicable to this task is shown. For more details, see the *Cisco IOS IP Application Services Command Reference*.
Step 5	Repeat Step 4 for more access list entries, as required.	--
Step 6	**exit** **Example:** `Router(config-ext-nacl)# exit`	(Optional) Exits extended access list configuration mode and returns to global configuration mode.
Step 7	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure a Cisco router as a master controller and to configure master controller policy and timer settings.
Step 8	**learn** **Example:** `Router(config-pfr-mc)# learn`	Enters PfR Top Talker and Top Delay learning configuration mode to automatically learn traffic classes.
Step 9	**list seq** *number* **refname** *refname*	Creates an PfR learn list and enters learn list configuration mode.

	Command or Action	Purpose
	Example: `Router(config-pfr-mc-learn)# list seq 10 refname LEARN_USER_DEFINED_TC`	• Use the **seq** keyword and *number* argument to specify a sequence number used to determine the order in which learn list criteria is applied. • Use the **refname** keyword and *refname* argument to specify a reference name for the learn list. • The example creates a learn list named LEARN_USER_DEFINED_TC.
Step 10	**count** *number* **max** *max-number* **Example:** `Router(config-pfr-mc-learn-list)# count 50 max 90`	Sets the number of traffic classes to be learned during an PfR learn session. • Use the *number* argument to specify a number of traffic classes to be learned for the specified learn list during a learn session. • Use the **max** keyword and *max-number* argument to specify a maximum number of traffic classes to be learned for the specified learn list during all learning sessions. • The example specifies 50 traffic classes to be learned per learning session for the learn list named LEARN_USER_DEFINED_TC, and a maximum of 90 traffic classes in total for this learn list.
Step 11	**traffic-class access-list** *access-list-name* [**filter** *prefix-list-name*] **Example:** `Router(config-pfr-mc-learn-list)# traffic-class access-list USER_DEFINED_TC`	Defines a PfR traffic class using an access list. • Use the *access-list-name* argument to specify an access list that contains criteria for defining the traffic classes. • The example uses the access list named USER_DEFINED_TC to create the traffic classes.
Step 12	**aggregation-type** {**bgp non-bgp prefix-length**} *prefix-mask* **Example:** `Router(config-pfr-mc-learn-list)# aggregation-type prefix-length 24`	(Optional) Configures a master controller to aggregate learned prefixes based on traffic flow type. • The **bgp** keyword configures prefix aggregation based on entries in the BGP routing table. This keyword is used if BGP peering is enabled in the network. • The **non-bgp** keyword configures learned prefix aggregation based on static routes. Entries in the BGP routing table are ignored when this keyword is entered. • The **prefix-length** keyword configures aggregation based on the specified prefix length. The range of values that can be configured for this argument is a prefix mask from 1 to 32. • If this command is not specified, the default aggregation is performed based on a /24 prefix length. • The example configures prefix length aggregation based on a /24 prefix length.

	Command or Action	Purpose
Step 13	**delay** **Example:** `Router(config-pfr-mc-learn-list)# delay`	Enables prefix learning based on the highest delay time. • *Top Delay* prefixes are sorted from the highest to lowest delay time. • The example configures prefix learning based on the highest delay. **Note** To configure automatic PfR learning within a learn list you can specify either the **delay** (PfR) command or the **throughput** (PfR) command, but they are mutually exclusive in learn list configuration mode.
Step 14	**exit** **Example:** `Router(config-pfr-mc-learn-list)# exit`	(Optional) Exits learn list configuration mode and returns to global configuration mode.
Step 15	Repeat Step 14 twice to return to global configuration mode.	--
Step 16	**pfr-map** *map-name sequence-number* **Example:** `Router(config)# pfr-map ACCESS_MAP 10`	Enters PfR map configuration mode to configure a PfR map. • Only one match clause can be configured for each PfR map sequence. • Permit sequences are first defined in an IP access list and then applied with the **match traffic-class access-list** command in Step 17. • The example creates a PfR map named ACCESS_MAP.
Step 17	**match traffic-class access -list** *access-list-name* **Example:** `Router(config-pfr-map)# match traffic-class access-list USER_DEFINED_TC`	Manually configures an access list as match criteria used to create traffic classes using a PfR map. • The example defines a traffic class using the destination address defined in the IP access list named USER_DEFINED_TC.
Step 18	**end** **Example:** `Router(config-pfr-mc-learn-list)# end`	Exits learn list configuration mode, and returns to privileged EXEC mode.

Manually Selecting Prefix-Based Traffic Classes Using a Prefix List

Perform this task on the master controller to manually select traffic classes based only on destination prefixes. Use this task when you know the destination prefixes that you want to select for the traffic classes. An IP prefix list is created to define the destination prefixes and using a PfR map, the traffic classes are profiled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*}
4. Repeat Step 3 for more prefix list entries, as required.
5. **pfr-map** *map-name sequence-number*
6. **match traffic-class prefix-list** *prefix-list-name*
7. **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.
Step 3	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} **Example:** `Router(config)# ip prefix-list PREFIX_TC permit 172.16.1.0/24`	Creates a prefix list to specify destination prefix-based traffic classes. • The example creates a prefix list named PREFIX_TC that specifies a destination prefix of 172.16.1.0/24 to be selected for a traffic class.
Step 4	Repeat Step 3 for more prefix list entries, as required.	--
Step 5	**pfr-map** *map-name sequence-number* **Example:** `Router(config)# pfr-map PREFIX_MAP 10`	Enters PfR map configuration mode to configure a PfR map. • Only one match clause can be configured for each PfR map sequence. • Permit sequences are first defined in an IP prefix list and then applied with the **match traffic-class prefix-list** command in Step 6. • The example creates a PfR map named PREFIX_MAP.

	Command or Action	Purpose
Step 6	**match traffic-class prefix-list** *prefix-list-name* **Example:** `Router(config-pfr-map)# match traffic-class prefix-list PREFIX_TC`	Manually configures a prefix list as match criteria used to create traffic classes using a PfR map. • The example defines a traffic class using the destination address defined in the IP prefix list named PREFIX_TC.
Step 7	**end** **Example:** `Router(config-pfr-map)# end`	(Optional) Exits PfR map configuration mode and returns to privileged EXEC mode.

Displaying and Resetting Traffic Class and Learn List Information

Perform this task to display traffic class and learn list information and optionally, to reset some traffic class information. These commands can be entered on a master controller after learn lists are configured and traffic classes are automatically learned, or when traffic classes are manually configured using a PfR map. The commands can be entered in any order and all the commands are optional.

SUMMARY STEPS

1. **enable**
2. **show pfr master traffic-class** [**access-list** *access-list-name*| **application** *application-name*[*prefix*] | **inside** | **learned**[**delay** | **inside** | **list** *list-name*| **throughput**] | **prefix** *prefix*| **prefix-list** *prefix-list-name*] [**active**| **passive**| **status**] [**detail**]
3. **show pfr master learn list** [*list-name*]
4. **clear pfr master traffic-class** [**access-list** *access-list-name*| **application** *application-name*[*prefix*]| **inside** | **learned**[**delay** | **inside** | **list** *list-name*| **throughput**]| **prefix** *prefix*| **prefix-list** *prefix-list-name*]

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 2 **show pfr master traffic-class** [**access-list** *access-list-name*| **application** *application-name*[*prefix*] | **inside** | **learned**[**delay** | **inside** | **list** *list-name*| **throughput**] | **prefix** *prefix*| **prefix-list** *prefix-list-name*] [**active**| **passive**| **status**] [**detail**]
This command is used to display information about traffic classes learned or manually configured under PfR learn list configuration mode.

Example:

```
Router# show pfr master traffic-class

OER Prefix Statistics:
 Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
 P - Percentage below threshold, Jit - Jitter (ms),
 MOS - Mean Opinion Score
 Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
 E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
 U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
 # - Prefix monitor mode is Special, & - Blackholed Prefix
 % - Force Next-Hop, ^ - Prefix is denied

DstPrefix           Appl_ID Dscp Prot     SrcPort     DstPort SrcPrefix
          Flags             State     Time            CurrBR  CurrI/F Protocol
         PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos      EBw      IBw
         ActSDly  ActLDly   ActSUn   ActLUn  ActSJit  ActPMOS
-------------------------------------------------------------------------------
10.1.1.0/24               N defa    N           N           N N
               #          OOPOLICY       32         10.11.1.3  Gi0/0/0      BGP
               N        N         N        N        N        N        N      IBwN
             130      134         0        0        N        N
```

Step 3 **show pfr master learn list** [*list-name*]

This command is used to display one or all of the configured PfR learn lists. In this example, the information about two learn lists is displayed.

Example:

```
Router# show pfr master learn list

Learn-List LIST1 10
   Configuration:
    Application: ftp
    Aggregation-type: bgp
    Learn type: thruput
    Policies assigned: 8 10
   Stats:
    Application Count: 0
    Application Learned:
 Learn-List LIST2 20
   Configuration:
    Application: telnet
    Aggregation-type: prefix-length 24
    Learn type: thruput
    Policies assigned: 5 20
   Stats:
    Application Count: 2
    Application Learned:
     Appl Prefix 10.1.5.0/24 telnet
     Appl Prefix 10.1.5.16/28 telnet
```

Step 4 **clear pfr master traffic-class** [**access-list** *access-list-name*| **application** *application-name*[*prefix*]| **inside** | **learned**[**delay** | **inside** | **list** *list-name*| **throughput**]| **prefix** *prefix*| **prefix-list** *prefix-list-name*]

This command is used to clear PfR controlled traffic classes from the master controller database. The following example clears traffic classes defined by the Telnet application and the 10.1.1.0/24 prefix:

Example:

```
Router# clear pfr master traffic-class application telnet 10.1.1.0/24
```

Measuring Phase Tasks

The following tasks show how to configure elements of the PfR measure phase:

Modifying the PfR Link Utilization for Outbound Traffic

Perform this task at the master controller to modify the PfR exit (outbound) link utilization threshold. After an external interface has been configured for a border router, PfR automatically monitors the utilization of external links on a border router every 20 seconds. The utilization is reported back to the master controller and, if the utilization exceeds 75 percent, PfR selects another exit link for traffic classes on that link. An absolute value in kilobytes per second (kbps), or a percentage, can be specified.

For more details about the configuration of measuring inbound traffic, see the "BGP Inbound Optimization Using Performance Routing" module.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **border** *ip-address* [**key-chain** *key-chain-name*]
5. **interface** *type number* **external**
6. **max-xmit-utilization** {**absolute** *kbps* | **percentage** *value*
7. **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.
Step 3	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure a router as a master controller and to configure global operations and policies.

	Command or Action	Purpose
Step 4	**border** *ip-address* [**key-chain** *key-chain-name*] **Example:** `Router(config-pfr-mc)# border 10.1.1.2`	Enters PfR-managed border router configuration mode to establish communication with a border router. • An IP address is configured to identify the border router. • At least one border router must be specified to create a PfR-managed network. A maximum of ten border routers can be controlled by a single master controller. **Note** The **key-chain** keyword and *key-chain-name* argument must be entered when a border router is initially configured. However, this keyword is optional when reconfiguring an existing border router.
Step 5	**interface** *type number* **external** **Example:** `Router(config-pfr-mc-br)# interface Ethernet 1/0 external`	Configures a border router interface as a PfR-managed external interface and enters PfR border exit interface configuration mode. • External interfaces are used to forward traffic and for active monitoring. • A minimum of two external border router interfaces are required in a PfR-managed network. At least one external interface must be configured on each border router. A maximum of 20 external interfaces can be controlled by single master controller. **Note** Entering the **interface** (PfR) command without the **external** or**internal** keyword places the router in global configuration mode and not PfR border exit configuration mode. The **no** form of this command should be applied carefully so that active interfaces are not removed from the router configuration.
Step 6	**max-xmit-utilization** {**absolute** *kbps* | **percentage** *value* **Example:** `Router(config-pfr-mc-br-if)# max-xmit-utilization absolute 500000`	Configures the maximum utilization on a single PfR managed exit link. • Use the **absolute** keyword and *kbps* argument to specify the absolute maximum utilization on a PfR managed exit link in kbps. • Use the **percentage** keyword and *value* argument to specify percentage utilization of an exit link.
Step 7	**end** **Example:** `Router(config-pfr-mc-br-if)# end`	Exits PfR border exit interface configuration mode and returns to privileged EXEC mode.

Modifying the PfR Exit Link Utilization Range

Perform this task at the master controller to modify the maximum exit link utilization range threshold over all the border routers. By default, PfR automatically monitors the utilization of external links on a border router every 20 seconds, and the border router reports the utilization to the master controller. If the utilization

range between all the exit links exceeds 20 percent, the master controller tries to equalize the traffic load by moving some traffic classes to another exit link. The maximum utilization range is configured as a percentage.

PfR uses the maximum utilization range to determine if exit links are in-policy. PfR will equalize outbound traffic across all exit links by moving traffic classes from overutilized or out-of-policy exits to in-policy exits.

Note If you are configuring link grouping, configure the **no max-range-utilization** command because using a link utilization range is not compatible with using a preferred or fallback set of exit links configured for link grouping. With CSCtr33991, this requirement is removed and PfR can perform load balancing within a PfR link group.

For more details about the configuration of measuring inbound traffic, see the "BGP Inbound Optimization Using Performance Routing" module.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **max-range-utilization percent** *maximum*
5. **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.
Step 3	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure a router as a master controller and to configure global operations and policies.
Step 4	**max-range-utilization percent** *maximum* **Example:** `Router(config-pfr-mc)# max-range-utilization percent 25`	Sets the maximum utilization range for all PfR-managed exit link.s. • Use the **percent** keyword and *maximum* argument to specify the maximum utilization range between all the exit links. • In this example, the utilization range between all the exit links on the border routers must be within 25 percent.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-pfr-mc)# end`	Exits PfR master controller configuration mode and returns to privileged EXEC mode.

Configuring and Verifying PfR Passive Monitoring

PfR enables passive monitoring by default when a PfR managed network is created, but there are times when passive monitoring is disabled. Use this task to configure passive monitoring and then verify that the passive monitoring is being performed. Perform the first five steps on a master controller and then move to a border router to display passive measurement information collected by NetFlow for monitored prefixes or application traffic flows. The **show** commands are entered on a border router through which the application traffic is flowing. The **show** commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **mode monitor** {**active** | **both**| **fast**| **passive**}
5. **end**
6. Move to one of the border routers.
7. **enable**
8. **show pfr border passive cache** {**learned**[**application**| **traffic-class**]}
9. **show pfr border passive prefixes**

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 2 **configure terminal**
Enters global configuration mode.

Example:

```
Router# configure terminal
```

Step 3 **pfr master**
Enters PfR master controller configuration mode to configure a router as a master controller and to configure global operations and policies.

Example:

```
Router(config)# pfr master
```

Step 4 **mode monitor** {**active** | **both**| **fast**| **passive**}
Configures route monitoring or route control on a PfR master controller. The **monitor** keyword is used to configure active monitoring, passive monitoring, or both active and passive monitoring. Passive monitoring is enabled when either the **both** or **passive** keywords are specified. In this example, passive monitoring is enabled.

Example:

```
Router(config-pfr-mc)# mode monitor passive
```

Step 5 **end**
Exits PfR master controller configuration mode and returns to privileged EXEC mode.

Example:

```
Router(config-pfr-mc)# end
```

Step 6 Move to one of the border routers.

Step 7 **enable**
Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 8 **show pfr border passive cache** {**learned**[**application**| **traffic-class**]}
This command is used to display real-time passive measurement information collected by NetFlow from the border router for PfR monitored prefixes and traffic flows. The following example uses the learned and application keywords to display measurement information about monitored application traffic classes that have been learned by PfR. In this example for voice traffic, the voice application traffic is identified by the User Datagram Protocol (UDP) protocol, a DSCP value of ef, and port numbers in the range from 3000 to 4000.

Example:

```
Router# show pfr border passive cache learned application
OER Learn Cache:
    State is enabled
    Measurement type: throughput, Duration: 2 min
    Aggregation type: prefix-length, Prefix length: 24
    4096 oer-flows per chunk,
    8 chunks allocated, 32 max chunks,
    5 allocated records, 32763 free records, 4588032 bytes allocated
```

```
Prefix          Mask     Pkts  B/Pk  Delay Samples   Active
Prot  Dscp  SrcPort          DstPort
Host1           Host2          Host3          Host4          Host5
dport1          dport2         dport3         dport4         dport5
10.1.3.0         /24     873     28      0      0      13.3
17      ef [1, 65535]        [3000, 4000]
10.1.3.1        0.0.0.0        0.0.0.0        0.0.0.0        0.0.0.0
3500             0              0              0              0
10.1.1.0         /24    7674     28      0      0      13.4
17      ef [1, 65535]        [3000, 4000]
10.1.1.1        0.0.0.0        0.0.0.0        0.0.0.0        0.0.0.0
3600             0              0              0              0
```

Step 9 **show pfr border passive prefixes**

This command is used to display passive measurement information collected by NetFlow for PfR monitored prefixes and traffic flows. The following output shows the prefix that is being passively monitored by NetFlow for the border router on which the **show pfr border passive prefixes** command was run:

Example:

```
Router# show pfr border passive prefixes
OER Passive monitored prefixes:
Prefix          Mask   Match Type
10.1.5.0        /24     exact
```

Configuring PfR Active Probing Using the Longest Match Target Assignment

Perform this task at the master controller to configure active probing using the longest match target assignment. Active monitoring is enabled with the **mode monitor active**or**mode monitor both** commands, and the type of active probe is specified using the **active-probe** (PfR) command. Active probes are configured with a specific host or target address and the active probes are sourced on the border router. The active probe source external interface may, or may not, be the preferred route for an optimized prefix. In this example, both active and passive monitoring are enabled and the target IP address of 10.1.5.1 is to be actively monitored using Internet Control Message Protocol (ICMP) echo (ping) messages. This task does not require an IP SLA responder to be enabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **mode monitor** {**active** | **both** | **passive**}
5. **active-probe** {**echo** *ip-address* | **tcp-conn** *ip-address* **target-port** *number* | **udp-echo** *ip-address* **target-port** *number*}
6. **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.
Step 3	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure a router as a master controller and to configure global operations and policies.
Step 4	**mode monitor** {**active** | **both** | **passive**} **Example:** `Router(config-pfr-mc)# mode monitor both`	Configures route monitoring on a PfR master controller. • The **monitor** keyword is used to configure active and/or passive monitoring. • The example enables both active and passive monitoring.
Step 5	**active-probe** {**echo** *ip-address* | **tcp-conn** *ip-address* **target-port** *number* | **udp-echo** *ip-address* **target-port** *number*} **Example:** `Router(config-pfr-mc)# active-probe echo 10.1.5.1`	Configures an active probe for a target prefix. • Active probing measures delay and jitter of the target prefix more accurately than is possible with only passive monitoring. • Active probing requires you to configure a specific host or target address. • Active probes are sourced from a PfR managed external interfaces. This external interface may or may not be the preferred route for an optimized prefix. • A remote responder with the corresponding port number must be configured on the target device when configuring UDP echo probe or when configuring a TCP connection probe that is configured with a port number other than 23. The remote responder is configured with the **ip sla monitor responder** global configuration command.
Step 6	**end** **Example:** `Router(config-pfr-mc)# end`	Exits PfR master controller configuration mode and returns to privileged EXEC mode.

Configuring PfR Voice Probes with a Forced Target Assignment

Perform this task to enable active monitoring using PfR jitter probes. In this example, the traffic to be monitored is voice traffic, which is identified using an access list. The active voice probes are assigned a forced target for PfR instead of the usual longest match assigned target. This task also demonstrates how to modify the PfR probe frequency.

Before configuring the PfR jitter probe on the source device, the IP SLAs Responder must be enabled on the target device (the operational target). The IP SLAs Responder is available only on Cisco IOS software-based devices. Start this task at the network device that runs the IP SLAs Responder.

Note The device that runs the IP SLAs Responder does not have to be configured for PfR.

Before You Begin

Before configuring this task, an access list must be defined. For an example access list and more details about configuring voice traffic using active probes, see the "PfR Voice Traffic Optimization Using Active Probes" solution module.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla monitor responder**
4. **exit**
5. Move to the network device that is the PfR master controller.
6. **enable**
7. **configure terminal**
8. **pfr master**
9. **mode monitor** {**active** | **both** | **passive**}
10. **exit**
11. **pfr-map** *map-name sequence-number*
12. **match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*}
13. **set active-probe** *probe-type ip-address* [**target-port** *number*] [**codec** *codec-name*] [**dscp** *value*]
14. **set probe frequency** *seconds*
15. **set jitter threshold** *maximum*
16. **set mos** {**threshold** *minimum* **percent** *percent*}
17. **set delay** {**relative** *percentage* | **threshold** *maximum*}
18. **end**
19. **show pfr master active-probes** [**appl**| **forced**]

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.
Step 3	**ip sla monitor responder** **Example:** `Router(config)# ip sla monitor responder`	Enables the IP SLAs Responder.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	Move to the network device that is the PfR master controller.	--
Step 6	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 7	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 8	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure a router as a master controller and to configure global operations and policies.
Step 9	**mode monitor** {**active** | **both** | **passive**}	Configures route monitoring on a PfR master controller.

	Command or Action	Purpose
	Example: `Router(config-pfr-mc)# mode monitor active`	• The **monitor** keyword is used to configure active and/or passive monitoring. • The example enables active monitoring.
Step 10	**exit** **Example:** `Router(config-pfr-mc)# exit`	Exits PfR master controller configuration mode and returns to global configuration.
Step 11	**pfr-map** *map-name sequence-number* **Example:** `Router(config)# pfr-map TARGET_MAP 10`	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes. • Only one match clause can be configured for each PfR map sequence. • Deny sequences are first defined in an IP prefix list and then applied with the **match ip address** (PfR) command in Step 12. • The example creates a PfR map named TARGET_MAP.
Step 12	**match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*} **Example:** `Router(config-pfr-map)# match ip address access-list VOICE_ACCESS_LIST`	References an extended IP access list or IP prefix as match criteria in a PfR map. • The example configures the IP access list named VOICE_ACCESS_LIST as match criteria in a PfR map.
Step 13	**set active-probe** *probe-type ip-address* [**target-port** *number*] [**codec** *codec-name*] [**dscp** *value*] **Example:** `Router(config-pfr-map)# set active-probe jitter 10.20.22.1 target-port 2000 codec g729a`	Creates a set clause entry to assign a target prefix for an active probe. • Use the *probe-type* argument to specify one of four probe types: echo, jitter, tcp-conn, or udp-echo. • The *ip-address*argument to specify the target IP address of a prefix to be monitored using the specified type of probe. • The **target-port** keyword and *number* argument are used to specify the destination port number for the active probe. • The **codec** keyword and *codec-name* argument are used only with the jitter probe type. Specifies the codec value used for Mean Opinion Score (MOS) calculation. The codec values must be one of the following: g711alaw, g711ulaw, or g729a. • The example creates a set clause entry to specify the target IP address of a prefix and a specific port number to actively monitor using jitter.
Step 14	**set probe frequency** *seconds*	Creates a set clause entry to set the frequency of the PfR active probe.

	Command or Action	Purpose
	Example: `Router(config-pfr-map)# set probe frequency 10`	• The *seconds* argument is used to set the time, in seconds, between the active probe monitoring of the specified IP prefixes. • The example creates a set clause to set the active probe frequency to 10 seconds.
Step 15	**set jitter threshold** *maximum* **Example:** `Router(config-pfr-map)# set jitter threshold 20`	Creates a set clause entry to configure the jitter threshold value. • The **threshold** keyword is used to configure the maximum jitter value, in milliseconds. • The example creates a set clause that sets the jitter threshold value to 20 for traffic that is matched in the same PfR map sequence.
Step 16	**set mos** {**threshold** *minimum* **percent** *percent*} **Example:** `Router(config-pfr-map)# set mos threshold 4.0 percent 30`	Creates a set clause entry to configure the MOS threshold and percentage values used to decide whether an alternate exit is be selected. • The **threshold** keyword is used to configure the minimum MOS value. • The **percent** keyword is used to configure the percentage of MOS values that are below the MOS threshold. • PfR calculates the percentage of MOS values below the MOS threshold that are recorded in a five-minute period. If the percentage value exceeds the configured percent value or the default value, the master controller searches for alternate exit links. • The example creates a set clause that sets the threshold MOS value to 4.0 and the percent value to 30 percent for traffic that is matched in the same PfR map sequence.
Step 17	**set delay** {**relative** *percentage* | **threshold** *maximum*} **Example:** `Router(config-pfr-map)# set delay threshold 100`	Creates a set clause entry to configure the delay threshold. • The delay threshold can be configured as a relative percentage or as an absolute value for match criteria. • The **relative** keyword is used to configure a relative delay percentage. The relative delay percentage is based on a comparison of short-term and long-term measurements. • The **threshold** keyword is used to configure the absolute maximum delay period in milliseconds. • The example creates a set clause that sets the absolute maximum delay threshold to 100 milliseconds for traffic that is matched in the same PfR map sequence.
Step 18	**end** **Example:** `Router(config-pfr-map)# end`	Exits PfR map configuration mode and enters privileged EXEC mode.

	Command or Action	Purpose
Step 19	**show pfr master active-probes** [**appl**| **forced**] **Example:** `Router# show pfr master active-probes forced`	Displays connection and status information about active probes on a PfR master controller. • The output from this command displays the active probe type and destination, the border router that is the source of the active probe, the target prefixes that are used for active probing, and whether the probe was learned or configured. • The **appl** keyword is used to filter the output to display information about applications optimized by the master controller. • The **forced** keyword is used to show any forced targets that are assigned. • The example displays connection and status information about the active probes generated for voice traffic configured with a forced target assignment.

Examples

This example shows output from the **show pfr master active-probes forced** command. The output is filtered to display only connection and status information about the active probes generated for voice traffic configured with a forced target assignment.

```
Router# show pfr master active-probes forced
OER Master Controller active-probes
Border   = Border Router running this Probe
Policy   = Forced target is configure under this policy
Type     = Probe Type
Target   = Target Address
TPort    = Target Port
N - Not applicable
The following Forced Probes are running:
Border          State    Policy            Type     Target          TPort
10.20.20.2     ACTIVE    40                jitter   10.20.22.1      3050
10.20.21.3     ACTIVE    40                jitter   10.20.22.4      3050
```

Configuring PfR Voice Probes for Fast Failover

Perform this task to enable fast monitoring using PfR jitter probes. In fast failover monitoring mode, all exits are continuously probed using active monitoring and passive monitoring. The probe frequency can be set to a lower frequency in fast failover monitoring mode than for other monitoring modes, to allow a faster failover capability. Fast failover monitoring can be used with all types of active probes: ICMP echo, jitter, TCP connection, and UDP echo.

Fast failover monitoring is designed for traffic classes that are very sensitive to performance issues or congested links, and voice traffic is very sensitive to any dropped links. In this example, the fast failover monitoring mode is enabled and the voice traffic to be monitored is identified using an IP prefix list. To reduce some of the overhead that fast failover monitoring produces, the active voice probes are assigned a forced target for PfR. The PfR probe frequency is set to 2 seconds. In the examples section after the task table, the **show pfr master prefix** command is used to show the policy configuration for the prefix specified in the task steps and some logging output is displayed to show that fast failover is configured.

Note In fast monitoring mode, probe targets are learned as well as learned prefixes. To avoid triggering large numbers of probes in the network, use fast monitoring mode only for real time applications and critical applications with performance sensitive traffic.

Before configuring the PfR jitter probe on the source device, the IP SLAs Responder must be enabled on the target device (the operational target). The IP SLAs Responder is available only on Cisco IOS software-based devices. Start this task at the network device that runs the IP SLAs Responder.

Note The device that runs the IP SLAs Responder does not have to be configured for PfR.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla monitor responder**
4. **exit**
5. Move to the network device that is the PfR master controller.
6. **enable**
7. **configure terminal**
8. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length*| **permit** *network/length*}
9. Repeat Step 4 for more prefix list entries, as required.
10. **pfr-map** *map-name sequence-number*
11. **match traffic-class prefix-list** *prefix-list-name*
12. **set mode monitor** {**active** | **both**| **fast**| **passive**}
13. **set jitter threshold** *maximum*
14. **set mos** {**threshold** *minimum* **percent** *percent*}
15. **set delay** {**relative** *percentage* | **threshold** *maximum*}
16. **set active-probe** *probe-type ip-address* [**target-port** *number*] [**codec** *codec-name*] [**dscp** *value*]
17. **set probe frequency** *seconds*
18. **end**
19. **show pfr master prefix** [*prefix*[**detail**| **policy**| **traceroute**[*exit-id*| *border-address*| **current**]]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla monitor responder** **Example:** `Router(config)# ip sla monitor responder`	Enables the IP SLAs Responder.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	Move to the network device that is the PfR master controller.	--
Step 6	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 7	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 8	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length*| **permit** *network/length*} **Example:** `Router(config)# ip prefix-list VOICE_FAIL_LIST permit 10.1.0.0/24`	Creates an IP prefix list. • The IP prefix list specified here is used in a PfR map to specify the destination IP addresses for a traffic class. • The example creates an IP prefix list named VOICE_FAIL_LIST for PfR to profile the prefix, 10.1.0.0/24.
Step 9	Repeat Step 4 for more prefix list entries, as required.	—
Step 10	**pfr-map** *map-name sequence-number* **Example:** `Router(config)# pfr-map FAST_FAIL_MAP 10`	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes. • Only one match clause can be configured for each PfR map sequence. • The example creates a PfR map named FAST_FAIL_MAP.

	Command or Action	Purpose
Step 11	**match traffic-class prefix-list** *prefix-list-name* **Example:** `Router(config-pfr-map)# match traffic-class prefix-list VOICE_FAIL_LIST`	References an IP prefix list as traffic class match criteria in a PfR map. • The example configures the IP prefix list named VOICE_FAIL_LIST as match criteria in a PfR map.
Step 12	**set mode monitor** {**active** | **both**| **fast**| **passive**} **Example:** `Router(config-pfr-map)# set mode monitor fast`	Creates a set clause entry to configure route monitoring on a PfR master controller. • The **monitor** keyword is used to configure active and/or passive monitoring. • The **fast** keyword is used to configure fast failover monitoring mode where continuous active monitoring is enabled as well as passive monitoring. • The example enables fast failover monitoring.
Step 13	**set jitter threshold** *maximum* **Example:** `Router(config-pfr-map)# set jitter threshold 12`	Creates a set clause entry to configure the jitter threshold value. • The **threshold** keyword is used to configure the maximum jitter value, in milliseconds. • The example creates a set clause that sets the jitter threshold value to 12 for traffic that is matched in the same PfR map sequence.
Step 14	**set mos** {**threshold** *minimum* **percent** *percent*} **Example:** `Router(config-pfr-map)# set mos threshold 3.6 percent 30`	Creates a set clause entry to configure the MOS threshold and percentage values used to decide whether an alternate exit is be selected. • The **threshold** keyword is used to configure the minimum MOS value. • The **percent** keyword is used to configure the percentage of MOS values that are below the MOS threshold. • PfR calculates the percentage of MOS values below the MOS threshold that are recorded in a five-minute period. If the percentage value exceeds the configured percent value or the default value, the master controller searches for alternate exit links. • The example creates a set clause that sets the threshold MOS value to 3.6 and the percent value to 30 percent for traffic that is matched in the same PfR map sequence.
Step 15	**set delay** {**relative** *percentage* | **threshold** *maximum*}	Creates a set clause entry to configure the delay threshold. • The delay threshold can be configured as a relative percentage or as an absolute value for match criteria.

	Command or Action	Purpose
	Example: `Router(config-pfr-map)# set delay relative 50`	• The **relative** keyword is used to configure a relative delay percentage. The relative delay percentage is based on a comparison of short-term and long-term measurements. • The **threshold** keyword is used to configure the absolute maximum delay period in milliseconds. • The example creates a set clause that sets the relative delay percentage to 50 percent for traffic that is matched in the same PfR map sequence.
Step 16	**set active-probe** *probe-type ip-address* [**target-port** *number*] [**codec** *codec-name*] [**dscp** *value*] **Example:** `Router(config-pfr-map)# set active-probe jitter 10.120.120.1 target-port 20 codec g729a`	Creates a set clause entry to assign a target prefix for an active probe. • Use the *probe-type* argument to specify one four probe types: echo, jitter, tcp-conn, or udp-echo. • The *ip-address*argument to specify the target IP address of a prefix to be monitored using the specified type of probe. • The **target-port** keyword and *number* argument are used to specify the destination port number for the active probe. • The **codec** keyword and *codec-name* argument are used only with the jitter probe type. Specifies the codec value used for Mean Opinion Score (MOS) calculation. The codec values must be one of the following: g711alaw, g711ulaw, or g729a. • The example creates a set clause entry to specify the target IP address of a prefix and a specific port number to actively monitor using jitter.
Step 17	**set probe frequency** *seconds* **Example:** `Router(config-pfr-map)# set probe frequency 2`	Creates a set clause entry to set the frequency of the PfR active probe. • The *seconds* argument is used to set the time, in seconds, between the active probe monitoring of the specified IP prefixes. • The example creates a set clause to set the active probe frequency to 2 seconds. **Note** A probe frequency of less than 4 seconds is possible here because the fast failover monitoring mode has been enabled in Step 12.
Step 18	**end** **Example:** `Router(config-pfr-map)# end`	Exits PfR map configuration mode and enters privileged EXEC mode.
Step 19	**show pfr master prefix** [*prefix*[**detail**| **policy**| **traceroute**[*exit-id*| *border-address*| **current**]]]	(Optional) Displays the status of monitored prefixes. • The *prefix*argument is entered as an IP address and bit length mask.

	Command or Action	Purpose
	Example: `Router# show pfr master prefix 10.1.1.0/24 policy`	• The **policy**keyword is used to display policy information for the specified prefix. • The example displays policy information for the prefix, 10.1.1.0/24.

Examples

This example shows output from the **show pfr master prefix**command when a prefix is specified with the policy keyword to display the policy configured for the prefix 10.1.1.0/24. Note that the mode monitor is set to fast, which automatically sets the select-exit to best, and allows the probe frequency to be set at 2.

```
Router# show pfr master prefix 10.1.1.0/24 policy
* Overrides Default Policy Setting
pfr-map MAP 10
  sequence no. 8444249301975040, provider id 1, provider priority 30
    host priority 0, policy priority 10, Session id 0
  match ip prefix-lists: VOICE_FAIL_LIST
  backoff 90 90 90
  delay relative 50
  holddown 90
  periodic 0
 *probe frequency 2
  mode route control
 *mode monitor fast
 *mode select-exit best
  loss relative 10
 *jitter threshold 12
  mos threshold 3.60 percent 30
  unreachable relative 50
  next-hop not set
  forwarding interface not set
  resolve jitter priority 1 variance 10
  resolve utilization priority 12 variance 20

  Forced Assigned Target List:
   active-probe jitter 10.120.120.1 target-port 20 codec g729a
```

Configuring the Source Address of an Active Probe

Perform this task on a border router to specify the source interface for active probing. The active probe source interface is configured on the border router with the **active-probe address source** ((PfR) in PfR border router configuration mode. The active probe source interface IP address must be unique to ensure that the probe reply is routed back to the specified source interface.

The following is default behavior:

- The source IP address is used from the default PfR external interface that transmits the active probe when this command is not enabled or if the **no** form is entered.
- If the interface is not configured with an IP address, the active probe will not be generated.
- If the IP address is changed after the interface has been configured as an active probe source, active probing is stopped, and then restarted with the new IP address.

- If the IP address is removed after the interface has been configured as an active probe source, active probing is stopped and not restarted until a valid primary IP address is configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr border**
4. **active-probe address source interface** *type number*
5. **end**
6. **show pfr border active-probes**

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.
Step 3	**pfr border** **Example:** `Router(config)# pfr border`	Enters PfR border router configuration mode to configure a router as a border router.
Step 4	**active-probe address source interface** *type number* **Example:** `Router(config-pfr-br)# active-probe address source interface FastEthernet 0/0`	Configures an interface on a border router as the active-probe source. • The example configures interface FastEthernet 0/0 as the source interface.
Step 5	**end** **Example:** `Router(config-pfr-br)# end`	Exits PfR border router configuration mode and enters privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show pfr border active-probes** **Example:** `Router# show pfr border active-probes`	Displays connection and status information about active probes on a PfR border router. • Use this command to verify the configured source IP address.

Apply Policy Phase Tasks

The following tasks show how to configure elements of the PfR apply policy phase:

Configuring and Applying a PfR Policy to Learned Traffic Classes

Perform this task at the master controller to configure and apply a PfR policy to learned traffic classes. After configuring the router as a PfR master controller using the **pfr master** command, most of the commands in this task are all optional. Each step configures a performance policy that applies to learned traffic classes on a global basis. In this example, PfR is configured to select the first in-policy exit.

In this task some PfR timers are modified. When adjusting PfR timers note that a newly configured timer setting will immediately replace the existing setting if the value of the new setting is less than the time remaining. If the value is greater than the time remaining, the new setting will be applied when the existing timer expires or is reset.

Note Overly aggressive timer settings can keep an exit link or traffic class entry in an out-of-policy state.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **backoff** *min-timer max-timer* [*step-timer*]
5. **delay** {**relative** *percentage* | **threshold** *maximum*}
6. **holddown** *timer*
7. **loss** {**relative** *average* | **threshold** *maximum*}
8. **periodic** *timer*
9. **unreachable** {**relative** *average* | **threshold** *maximum*}
10. **mode select-exit** {**best** | **good**}}
11. **end**
12. **show pfr master policy** [*sequence-number*|*policy-name* | **default**]

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.
Step 3	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode.
Step 4	**backoff** *min-timer max-timer* [*step-timer*] **Example:** `Router(config-pfr-mc)# backoff 400 4000 400`	(Optional) Sets the backoff timer to adjust the time period for policy decisions. • The *min-timer* argument is used to set the minimum transition period in seconds. • The *max-timer* argument is used to set the maximum length of time PfR holds an out-of-policy traffic class entry when there are no links that meet the policy requirements of the traffic class entry. • The *step-timer* argument allows you to optionally configure PfR to add time each time the minimum timer expires until the maximum time limit has been reached.
Step 5	**delay** {**relative** *percentage* | **threshold** *maximum*} **Example:** `Router(config-pfr-mc)# delay relative 80`	(Optional) Sets the delay threshold as a relative percentage or as an absolute value. • The **relative** keyword is used to configure a relative delay percentage. The relative delay percentage is based on a comparison of short-term and long-term measurements. • The **threshold**keyword is used to configure the absolute maximum delay period in milliseconds. • If the configured delay threshold is exceeded, then the prefix is out-of-policy. • The example sets a delay threshold of 80 percent based on a relative average.
Step 6	**holddown** *timer* **Example:** `Router(config-pfr-mc)# holddown 600`	(Optional) Configures the traffic class entry route dampening timer to set the minimum period of time that a new exit must be used before an alternate exit can be selected. • PfR does not implement route changes while a traffic class entry is in the holddown state.

	Command or Action	Purpose
		• When the holddown timer expires, PfR will select the best exit based on performance and policy configuration. • PfR starts the process of finding an alternate path if the current exit for a traffic class entry becomes unreachable. • The example sets the traffic class entry route dampening timer to 600 seconds.
Step 7	**loss** {**relative** *average* | **threshold** *maximum*} **Example:** `Router(config-pfr-mc)# loss relative 20`	(Optional) Sets the relative or maximum packet loss limit that PfR will permit for a traffic class entry. • The **relative** keyword sets a relative percentage of packet loss based on a comparison of short-term and long-term packet loss percentages. • The **threshold** keyword sets the absolute packet loss based on packets per million. • The example configures the master controller to search for a new exit link when the relative percentage of packet loss is equal to or greater than 20 percent.
Step 8	**periodic** *timer* **Example:** `Router(config-pfr-mc)# periodic 300`	(Optional) Configures PfR to periodically select the best exit link when the periodic timer expires. • When this command is enabled, the master controller will periodically evaluate and then make policy decisions for traffic classes. • The example sets the periodic timer to 300 seconds. When the timer expires, PfR will select either the best exit or the first in-policy exit. **Note** The **mode select-exit** command is used to determine if PfR selects the first in-policy exit or the best available exit when this timer expires.
Step 9	**unreachable** {**relative** *average* | **threshold** *maximum*} **Example:** `Router(config-pfr-mc)# unreachable relative 10`	(Optional) Sets the maximum number of unreachable hosts. • This command is used to specify the relative percentage or the absolute maximum number of unreachable hosts, based on flows per million (fpm), that PfR will permit for a traffic class entry. If the absolute number or relative percentage of unreachable hosts is greater than the user-defined or the default value, PfR determines that the traffic class entry is OOP and searches for an alternate exit link. • The **relative** keyword is used to configure the relative percentage of unreachable hosts. The relative unreachable host percentage is based on a comparison of short-term and long-term measurements. • The **threshold** keyword is used to configure the absolute maximum number of unreachable hosts based on fpm. • The example configures PfR to search for a new exit link for a traffic class entry when the relative percentage of unreachable hosts is equal to or greater than 10 percent.
Step 10	**mode select-exit** {**best** | **good**}}	Enables the exit link selection based on performance or policy.

	Command or Action	Purpose
	Example: `Router(config-pfr-mc)# mode select-exit good`	• The **select-exit** keyword is used to configure the master controller to select either the best available exit when the **best**keyword is entered or the first in-policy exit when the **good** keyword is entered.
Step 11	**end** **Example:** `Router(config-pfr-mc)# end`	Exits PfR master controller configuration mode and enters privileged EXEC mode.
Step 12	**show pfr master policy** [*sequence-number*|*policy-name* | **default**] **Example:** `Router# show pfr master policy`	Displays policy settings on a PfR master controller. • The output of this command displays default policies and, optionally, policies configured with a PfR map. • The *sequence-number* argument is used to display policy settings for the specified PfR map sequence. • The *policy-name* argument is used to display policy settings for the specified PfR policy map name. • The**default**keyword is used to display only the default policy settings. • The example displays the default policy settings and policy settings updated by the configuration in this task.

Examples

This example shows output from the **show pfr master policy** command. Default policy settings are displayed except where the configuration in this task has overwritten specific policy settings.

```
Router# show pfr master policy
Default Policy Settings:
  backoff 400 4000 400
  delay relative 80
  holddown 600
  periodic 300
  probe frequency 56
  mode route observe
  mode monitor both
  mode select-exit good
  loss relative 20
  unreachable relative 10
  resolve delay priority 11 variance 20
  resolve utilization priority 12 variance 20
 *tag 0
```

Preventing PfR Optimization of Learned Prefixes

Perform this task at the master controller to configure and apply a PfR policy to prevent PfR from attempting to optimize specified learned prefixes. This task is useful when you know a few prefixes that you want to

exclude from the PfR optimization, but these prefixes will be learned automatically by PfR. In this task, an IP prefix list is configured with two entries for different prefixes that are not to be optimized. A PfR map is configured with two entries in a sequence that will prevent PfR from optimizing the prefixes specified in the prefix list, although the prefixes may be learned. If the sequence numbers of the PfR map entries are reversed, PfR will learn and attempt to optimize the prefixes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network / length*| **permit** *network / length*}
4. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network / length*| **permit** *network / length*}
5. **pfr-map** *map-name sequence-number*
6. **match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*}
7. **exit**
8. **pfr-map** *map-name sequence-number*
9. **match pfr learn** {**delay**| **inside**| **throughput**}
10. **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.
Step 3	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network / length*| **permit** *network / length*} **Example:** `Router(config)# ip prefix-list DENY_LIST deny 10.1.1.0/24`	Creates an IP prefix list. • IP prefix lists are used to manually deny or permit prefixes for monitoring by the master controller. • The prefixes specified in the IP prefix list are imported into the PfR map with the **match ip address** (PfR) command. • The example creates an IP prefix list with an entry that denies prefixes only from the 10.1.1.0/24 subnet.
Step 4	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network / length*| **permit** *network / length*}	Creates an IP prefix list. • IP prefix lists are used to manually deny or permit prefixes for monitoring by the master controller.

	Command or Action	Purpose
	Example: `Router(config)# ip prefix-list DENY_LIST deny 172.20.1.0/24`	• The prefixes specified in the IP prefix list are imported into the PfR map with the **match ip address** (PfR) command. • The example creates an IP prefix entry that denies prefixes only from the 172.20.1.0/24 subnet.
Step 5	**pfr-map** *map-name sequence-number* **Example:** `Router(config)# pfr-map DENY_MAP 10`	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes. • Only one match clause can be configured for each PfR map sequence. • Deny sequences are first defined in an IP prefix list and then applied with the **match ip address** (PfR) command in Step 6. • The example creates a PfR map named DENY_MAP with a sequence number of 10.
Step 6	**match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*} **Example:** `Router(config-pfr-map)# match ip address prefix-list DENY_LIST`	References an extended IP access list or IP prefix list as match criteria in a PfR map. • The example configures the prefix list named DENY_LIST as match criteria in a PfR map.
Step 7	**exit** **Example:** `Router(config-pfr-map)# exit`	Exits PfR map configuration mode and returns to global configuration mode.
Step 8	**pfr-map** *map-name sequence-number* **Example:** `Router(config)# pfr-map DENY_MAP 20`	Enters a PfR map entry. • Only one match clause can be configured for each PfR map sequence. • Deny sequences are first defined in an IP prefix list and then applied with the **match ip address** (PfR) command in Step 9. • The example creates a PfR map entry for the PfR map named DENY_MAP with a sequence number of 20.
Step 9	**match pfr learn** {**delay**| **inside**| **throughput**} **Example:** `Router(config-pfr-map)# match pfr learn throughput`	Creates a match clause entry in a PfR map to match PfR learned prefixes. • PfR can be configured to learn traffic classes that are inside prefixes or prefixes based on highest delay, or highest outbound throughput. • The example creates a match clause entry that matches traffic classes that are learned on the basis of the highest throughput.

	Command or Action	Purpose
Step 10	**end** **Example:** `Router(config-pfr-map)# end`	(Optional) Exits PfR map configuration mode and returns to privileged EXEC mode.

Configuring Policy Rules for PfR Maps

Perform this task to select a PfR map and apply the configuration under PfR master controller configuration mode. The **policy-rules** (PfR) command provides an improved method to switch between predefined PfR maps.

Before You Begin

At least one PfR map must be configured before you can enable policy-rule support.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **policy-rules** *map-name*
5. **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.
Step 3	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure global prefix and exit link policies.

	Command or Action	Purpose
Step 4	**policy-rules** *map-name* **Example:** `Router(config-pfr-mc)# policy-rules TARGET_MAP`	Applies a configuration from a PfR map to a master controller configuration in PfR master controller configuration mode. • Reentering this command with a new PfR map name will immediately overwrite the previous configuration. This behavior is designed to allow you to quickly select and switch between predefined PfR maps. • The example applies the configuration from the PfR map named TARGET_MAP.
Step 5	**end** **Example:** `Router(config-pfr-mc)# end`	Exits PfR master controller configuration mode and enters privileged EXEC mode.

Configuring Multiple PfR Policy Conflict Resolution

Perform this task to use the PfR resolve function to assign a priority to a PfR policy to avoid any conflict over which policy to run first. Each policy is assigned a unique value, and the policy with the highest value is selected as the highest priority. By default, a delay policy has the highest priority and a traffic load (utilization) policy has the second highest priority. Assigning a priority value to any policy will override default settings.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **resolve** {**cost priority** *value*| **delay priority** *value* **variance** *percentage* | **loss priority** *value* **variance** *percentage* | **range priority** *value* | **utilization priority** *value* **variance** *percentage*}
5. Repeat Step 4 to assign a priority for each required PfR policy.
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode.
Step 4	**resolve** {**cost priority** *value*| **delay priority** *value* **variance** *percentage* | **loss priority** *value* **variance** *percentage* | **range priority** *value* | **utilization priority** *value* **variance** *percentage*} **Example:** `Router(config-pfr-mc)# resolve loss priority 2 variance 10`	Sets policy priority or resolves policy conflicts. • This command is used to set priority when multiple policies are configured for the same prefix. When this command is configured, the policy with the highest priority will be selected to determine the policy decision. • The **priority** keyword is used to specify the priority value. Setting the number 1 assigns the highest priority to a policy. Setting the number 10 assigns the lowest priority. • Each policy must be assigned a different priority number. • The **variance** keyword is used to set an allowable variance for a user-defined policy. This keyword configures the allowable percentage that an exit link or prefix can vary from the user-defined policy value and still be considered equivalent. • The example sets the priority for loss policies to 2 with a 10 percent variance. **Note** Variance cannot be configured for range or cost policies.
Step 5	Repeat Step 4 to assign a priority for each required PfR policy.	--
Step 6	**end** **Example:** `Router(config-pfr-mc)# end`	Exits PfR master controller configuration mode, and enters privileged EXEC mode.

Configuring Black Hole Routing Using a PfR Map

Perform this task to configure a PfR map to filter packets to be forwarded to a null interface, meaning that the packets are discarded in a “black hole.” The prefix list is configured after an IP prefix is identified as the

source of the attack on the network. Some protocols such as BGP allow the redistribution of black hole routes, but other protocols do not.

This optional task can help prevent and mitigate attacks on your network.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length*| **permit** *network/length*}
4. **pfr-map** *map-name sequence-number*
5. **match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*}
6. **set interface null0**
7. **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.
Step 3	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length*| **permit** *network/length*} **Example:** `Router(config)# ip prefix-list BLACK_HOLE_LIST seq 10 permit 10.20.21.0/24`	Creates an IP prefix list. • IP prefix lists are used to manually select prefixes for monitoring by the PfR master controller. • A master controller can monitor and control an exact prefix of any length including the default route. If an exact prefix is specified, PfR monitors only the exact prefix. • The prefixes specified in the IP prefix list are imported into a PfR map using the **match ip address** (PfR) command. • The example creates an IP prefix list named BLACK_HOLE_LIST that permits prefixes from the 10.20.21.0/24 subnet.
Step 4	**pfr-map** *map-name sequence-number* **Example:** `Router(config)# pfr-map BLACK_HOLE_MAP 10`	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes. • Only one match clause can be configured for each PfR map sequence.

	Command or Action	Purpose
		• Deny sequences are first defined in an IP prefix list and then applied with the **match ip address** (PfR) command in the previous step. • The example creates a PfR map named BLACK_HOLE_MAP.
Step 5	**match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*} **Example:** `Router(config-pfr-map)# match ip address prefix-list BLACK_HOLE_LIST`	References an extended IP access list or IP prefix as match criteria in a PfR map. • The example configures the IP prefix list named BLACK_HOLE_LIST as match criteria in a PfR map.
Step 6	**set interface null0** **Example:** `Router(config-pfr-map)# set interface null0`	Creates a set clause entry to forward packets to the null interface, meaning that they are discarded. • The example creates a set clause entry to specify that the packets matching the prefix list, BLACK_HOLE_LIST, are discarded.
Step 7	**end** **Example:** `Router(config-pfr-map)# end`	(Optional) Exits PfR map configuration mode and returns to privileged EXEC mode.

Configuring Sinkhole Routing Using a PfR Map

Perform this task to configure a PfR map to filter packets to be forwarded to a next hop. The next hop is a router where the packets can be stored, analyzed, or discarded (the sinkhole analogy). The prefix list is configured after an IP prefix is identified as the source of an attack on the network.

This optional task can help prevent and mitigate attacks on your network

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length*| **permit** *network/length*}
4. **pfr-map** *map-name sequence-number*
5. **match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*}
6. **set next-hop** *ip-address*
7. **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.
Step 3	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length*| **permit** *network/length*} **Example:** `Router(config)# ip prefix-list SINKHOLE_LIST seq 10 permit 10.20.21.0/24`	Creates an IP prefix list. • IP prefix lists are used to manually select prefixes for monitoring by the PfR master controller. • A master controller can monitor and control an exact prefix of any length including the default route. If an exact prefix is specified, PfR monitors only the exact prefix. • The prefixes specified in the IP prefix list are imported into a PfR map using the **match ip address** (PfR) command. • The example creates an IP prefix list named SINKHOLE_LIST that permits prefixes from the 10.20.21.0/24 subnet.
Step 4	**pfr-map** *map-name sequence-number* **Example:** `Router(config-pfr-mc)# pfr-map SINKHOLE_MAP 10`	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes. • Only one match clause can be configured for each PfR map sequence. • Deny sequences are first defined in an IP prefix list and then applied with the **match ip address** (PfR) command in the previous step. • The example creates a PfR map named SINKHOLE_MAP.
Step 5	**match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*} **Example:** `Router(config-pfr-map)# match ip address prefix-list SINKHOLE_LIST`	References an extended IP access list or IP prefix as match criteria in a PfR map. • The example configures the IP prefix list named SINKHOLE_LIST as match criteria in a PfR map.

	Command or Action	Purpose
Step 6	**set next-hop** *ip-address* **Example:** `Router(config-pfr-map)# set next-hop 10.20.21.6`	Creates a set clause entry specifying that packets are forwarded to the next hop. • The example creates a set clause entry to specify that the packets matching the prefix list, SINKHOLE_LIST, are forwarded to the next hop at 10.20.21.6.
Step 7	**end** **Example:** `Router(config)# end`	(Optional) Exits PfR map configuration mode and returns to privileged EXEC mode.

Enforce Phase Tasks

The following tasks show how to configure elements of the PfR configure and apply policy phase:

Controlling Application Traffic

Perform this task on a master controller to control application traffic. This task shows how to use policy-based routing (PBR) to allow PfR to control specified application traffic classes. Use application-aware policy routing to configure application traffic that can be filtered with a permit statement in an extended IP access list.

Application traffic such as Telnet traffic is delay sensitive and long TCP delays can make Telnet sessions difficult to use. In this task, an extended IP access list is configured to permit Telnet traffic. A PfR map is configured with an extended access list that references a match clause to match Telnet traffic that is sourced from the 192.168.1.0/24 network. PfR route control is enabled and a delay policy is configured to ensure that Telnet traffic is sent out through exit links with a response time that is equal to, or less than, 30 milliseconds. The configuration is verified with the **show pfr master appl** command.

Note

- Border routers must be single-hop peers.
- Only named extended IP access lists are supported
- Application traffic optimization is supported in PfR only over CEF switching paths

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list** {**standard** | **extended**} *access-list-name*}
4. [*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* [**option** *option-name*][**precedence** *precedence*][**tos** *tos*] [**ttl** *operator value*] [**log**][**time-range** *time-range-name*][**fragments**]
5. **exit**
6. **pfr-map** *map-name sequence-number*
7. **match ip address** {*access-list name*| *prefix-list name*}
8. **set mode route control**
9. set delay {**relative** *percentage* | **threshold** *maximum*}
10. **set resolve** {**cost priority** *value* | **delay priority** *value* **variance** *percentage* | **loss priority** *value* **variance** *percentage* | **range priority** *value* | **utilization priority** *value* **variance** *percentage*}
11. **end**
12. **show pfr master appl** [**access-list** *name*] [**detail**] | [**tcp** | **udp**] [*protocol-number*] [*min-port max-port*] [**dst** | **src**] [**detail** | **policy**]

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.
Step 3	**ip access-list** {**standard**	**extended**} *access-list-name*} **Example:** `Router(config)# ip access-list extended TELNET_ACL`	Creates an extended access list and enters extended access list configuration mode. • Only named access lists are supported.
Step 4	[*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* [**option** *option-name*][**precedence** *precedence*][**tos** *tos*] [**ttl** *operator value*] [**log**][**time-range** *time-range-name*][**fragments**]	Defines the extended access list. • Any protocol, port, or other IP packet header value can be specified. • The example permits Telnet traffic that is sourced from the 192.168.1.0/24 network.

	Command or Action	Purpose
	Example: `Router(config-ext-nacl)# permit tcp 192.168.1.0 0.0.0.255 any eq telnet`	
Step 5	**exit** **Example:** `Router(config-ext-nacl)# exit`	Exits extended access list configuration mode, and returns to global configuration mode.
Step 6	**pfr-map** *map-name sequence-number* **Example:** `Router(config# pfr-map BLUE`	Enters PfR map configuration mode to configure a PfR map.
Step 7	**match ip address** {*access-list name*| *prefix-list name*} **Example:** `Router(config-pfr-map)# match ip address access-list TELNET`	References an extended IP access list or IP prefix as match criteria in a PfR map. • An extended IP access list is used to filter a subset of traffic from the monitored prefix.
Step 8	**set mode route control** **Example:** `Router(config-pfr-map)# set mode route control`	Creates a set clause entry to configure route control for matched traffic. • In control mode, the master controller analyzes monitored prefixes and implements changes based on policy parameters. • In this example, a set clause that enables PfR control mode is created.
Step 9	set delay {**relative** *percentage* | **threshold** *maximum*} **Example:** `Router(config-pfr-map)# set delay threshold 30`	(Optional) Configures a PfR map to configure PfR to set the delay threshold. • This example configures a delay policy. However, other policies could be configured. • The delay threshold is set to 30 milliseconds for Telnet traffic.
Step 10	**set resolve** {**cost priority** *value* | **delay priority** *value* **variance** *percentage* | **loss priority** *value* **variance** *percentage* | **range priority** *value* | **utilization priority** *value* **variance** *percentage*}	(Optional) Configures a PfR map to set policy priority for overlapping policies. • The resolve policy configures delay policies to have the highest priority with a 20 percent variance.

	Command or Action	Purpose
	Example: `Router(config-pfr-map)# set resolve delay priority 1 variance 20`	
Step 11	**end** **Example:** `Router(config-pfr-map)# end`	Exits PfR map configuration mode and returns to privileged EXEC mode.
Step 12	**show pfr master appl** [**access-list** *name*] [**detail**] | [**tcp** | **udp**] [*protocol-number*] [*min-port max-port*] [**dst** | **src**] [**detail** | **policy**] **Example:** `Router# show pfr master appl tcp 23 23 dst policy`	(Optional) Displays information about applications monitored and controlled by a PfR master controller.

Examples

The following example output from the **show pfr master appl** command shows TCP application traffic filtered based on port 23 (Telnet):

```
Router# show pfr master appl tcp 23 23 dst policy

Prefix              Appl Prot       Port                 Port Type       Policy
-------------------------------------------------------------------------------
10.1.1.0/24         tcp             [23, 23]             src             10
```

Verify Phase Task

The following task shows how to configure elements of the PfR verify phase:

Manually Verifying the PfR Route Enforce Changes

PfR automatically verifies route enforce changes in the network using NetFlow output. PfR monitors the NetFlow messages and uncontrols a traffic class if a message does not appear to verify the route enforce change. Perform the steps in this optional task if you want to manually verify that the traffic control implemented by the PfR enforce phase actually changes the traffic flow, and brings the OOP event to be in-policy. All the steps are optional and are not in any order. The information from these steps can verify that a specific prefix associated with a traffic class has been moved to another exit or entrance link interface, or that it is being controlled by PfR. The first three commands are entered at the master controller, the last two commands are entered at a border router. For more details about other PfR show commands, see the Cisco IOS Performance Routing Command Reference.

SUMMARY STEPS

1. **enable**
2. **show logging** [**slot** *slot-number* | **summary**]
3. **show pfr master prefix** *prefix* [**detail**]
4. Move to a border router to enter the next step.
5. **enable**
6. **show pfr border routes** {**bgp** | **cce** | **eigrp** [**parent**] | **rwatch** | **static**}

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 2 **show logging** [**slot** *slot-number* | **summary**]

This command is used to display the state of system logging (syslog) and the contents of the standard system logging buffer. Using optional delimiters, this example shows the logging buffer with PfR messages for the prefix 10.1.1.0 that is OOP and has a route change.

Note With CStx06699, PfR syslog levels are added to minimize the number of messages displayed, and a syslog notice is added to display when 30 percent of the traffic classes are out-of-policy.

Example:

```
Router# show logging | I 10.1.1.0
*Apr 26 22:58:20.919: %OER_MC-5-NOTICE: Discovered Exit for prefix 10.1.1.0/24, BR
10.10.10.1, I/f Et9/0
*Apr 26 23:03:14.987: %OER_MC-5-NOTICE: Route changed 10.1.1.0/24, BR 10.10.10.1, I/f
Se12/0, Reason Delay, OOP Reason Timer Expired
*Apr 26 23:09:18.911: %OER_MC-5-NOTICE: Passive REL Loss OOP 10.1.1.0/24, loss 133, BR
10.10.10.1, I/f Se12/0, relative loss 23, prev BR Unknown I/f Unknown
*Apr 26 23:10:51.123: %OER_MC-5-NOTICE: Route changed 10.1.1.0/24, BR 10.10.10.1, I/f
Et9/0, Reason Delay, OOP Reason Loss
```

Step 3 **show pfr master prefix** *prefix* [**detail**]

This command is used to display the status of monitored prefixes. The output from this command includes information about the source border router, current exit interface, prefix delay, and egress and ingress interface bandwidth. In this example, the output is filtered for the prefix 10.1.1.0 and shows that the prefix is currently in a holddown state. Only syntax relevant to this task, is shown in this step.

Example:

```
Router# show pfr master prefix 10.1.1.0
Prefix          State   Time Curr BR     CurrI/F     Protocol
           PasSDly PasLDly  PasSUn  PasLUn PasSLos PasLLos
           ActSDly ActLDly  ActSUn  ActLUn   EBw   IBw
------------------------------------------------------------------------------
10.1.1.0/24   HOLDDOWN  42 10.10.10.1   Et9/0      STATIC
```

```
                16      16       0       0       0       0
                 U       U       0       0      55       2
```

Step 4 Move to a border router to enter the next step.
The next command is entered on a border router, not the master controller.

Step 5 **enable**
Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 6 **show pfr border routes** {**bgp** | **cce** | **eigrp** [**parent**] | **rwatch** | **static**}
This command is entered on a border router. This command is used to display information about PfR controlled routes on a border router. In this example, the output shows that prefix 10.1.1.0 is being controlled by PfR.

Example:

```
Router# show pfr border routes bgp
OER BR 10.10.10.1 ACTIVE, MC 10.10.10.3 UP/DOWN: UP 00:10:08,
   Auth Failures: 0
   Conn Status: SUCCESS, PORT: 3949
BGP table version is 12, local router ID is 10.10.10.1
Status codes: s suppressed, d damped, h history, * valid, > best, I - internal,
              r RIB-failure, S Stale
Origin codes: I - IGP, e - EGP, ? - incomplete
OER Flags: C - Controlled, X - Excluded, E - Exact, N - Non-exact, I - Injected
    Network          Next Hop        OER    LocPrf Weight Path
*> 10.1.1.0/24     10.40.40.2         CE          0 400 600 I
```

Configuration Examples for Advanced Performance Routing

Profile Phase Tasks Examples

Example Defining a Learn List for Automatically Learned Prefix-Based Traffic Classes

The following example configured on the master controller, defines a learn list that will contain traffic classes that are automatically learned based only on a prefix list. In this example, there are three branch offices and the goal is to optimize all the traffic going to branch offices A and B using one policy (Policy1), and to optimize traffic going to branch office C using a different policy (Policy2).

Branch A is defined as any prefix that matches 10.1.0.0./16, Branch B is defined as any prefix that matches 10.2.0.0./16, and Branch C is defined as any prefix that matches 10.3.0.0./16.

This task configures prefix learning based on the highest outbound throughput.

```
ip prefix-list BRANCH_A_B permit seq 10 10.1.0.0/16
ip prefix-list BRANCH_A_B permit seq 20 10.2.0.0/16
ip prefix-list BRANCH_C permit seq 30 10.3.0.0/16
```

```
pfr master
 learn
 list seq 10 refname LEARN_BRANCH_A_B
 traffic-class prefix-list BRANCH_A_B
 throughput
 exit
 exit
 learn
 list seq 20 refname LEARN_BRANCH_C
 traffic-class prefix-list BRANCH_C
 throughput
 exit
 exit
pfr-map POLICY1 10
 match learn list LEARN_BRANCH_A_B
 exit
pfr-map POLICY2 10
 match learn list LEARN_BRANCH_C
 end
```

Example Defining a Learn List for Automatically Learned Application Traffic Classes Using an Access List

The following example creates an access list that defines custom application traffic classes. In this example, the custom application consists of four criteria:

- Any TCP traffic on destination port 500
- Any TCP traffic on ports in the range from 700 to 750
- Any UDP traffic on source port 400
- Any IP packet marked with a DSCP bit of ef

The goal is to optimize the custom application traffic using a learn list that is referenced in a PfR policy named POLICY_CUSTOM_APP. This task configures traffic class learning based on the highest outbound throughput.

```
ip access-list extended USER_DEFINED_TC
 permit tcp any any 500
 permit tcp any any range 700 750
 permit udp any eq 400 any
 permit ip any any dscp ef
 exit
pfr master
 learn
  list seq 10 refname CUSTOM_APPLICATION_TC
  traffic-class access-list USER_DEFINED_TC
  aggregation-type prefix-length 24
  throughput
  exit
 exit
pfr-map POLICY_CUSTOM_APP 10
 match learn list CUSTOM_APPLICATION_TC
 end
```

Example Manually Selecting Prefix-Based Traffic Classes Using a Prefix List

The following example configured on the master controller, manually selects traffic classes based only on destination prefixes. Use this task when you know the destination prefixes that you want to select for the

traffic classes. An IP prefix list is created to define the destination prefixes and using a PfR map, the traffic classes are profiled.

```
ip prefix-list PREFIX_TC permit 10.1.1.0/24
ip prefix-list PREFIX_TC permit 10.1.2.0/24
ip prefix-list PREFIX_TC permit 172.16.1.0/24
pfr-map PREFIX_MAP 10
 match traffic-class prefix-list PREFIX_TC
```

Example Manually Selecting Application Traffic Classes Using an Access List

The following example configured on the master controller, manually selects traffic classes using an access list. Each access list entry is a traffic class that must include a destination prefix and may include other optional parameters.

```
ip access-list extended ACCESS_TC
 permit tcp any 10.1.1.0 0.0.0.255 eq 500
 permit tcp any 172.17.1.0 0.0.255.255 eq 500
 permit tcp any 172.17.1.0 0.0.255.255 range 700 750
 permit tcp 192.168.1.1 0.0.0.0 10.1.2.0 0.0.0.255 eq 800any any dscp ef
 exit
pfr-map ACCESS_MAP 10
 match traffic-class access-list ACCESS_TC
```

Measure Phase Tasks Examples

Example Modifying the PfR Link Utilization for Outbound Traffic

The following example shows how to modify the PfR exit link utilization threshold. In this example, the exit utilization is set to 80 percent. If the utilization for this exit link exceeds 80 percent, PfR selects another exit link for traffic classes that were using this exit link.

```
Router(config)# pfr master
Router(config-pfr-mc)# border 10.1.4.1
Router(config-pfr-mc-br)# interface Ethernet 1/0 external
Router(config-pfr-mc-br-if)# max-xmit-utilization percentage 80
Router(config-pfr-mc-br-if)# end
```

Example Modifying the PfR Exit Link Utilization Range

The following example shows how to modify the PfR exit utilization range. In this example, the exit utilization range for all exit links is set to 10 percent. PfR uses the maximum utilization range to determine if exit links are in-policy. PfR will equalize outbound traffic across all exit links by moving prefixes from overutilized or out-of-policy exits to in-policy exits.

```
Router(config)# pfr master
Router(config-pfr-mc)# max-range-utilization percentage 10
Router(config-pfr-mc)# end
```

Example TCP Probe for Longest Match Target Assignment

The following example shows how to configure active probing using the TCP probe with the longest match target assignment. The IP SLAs Responder must first be enabled on the target device, and this device does

not have to be configured for PfR. A border router can be used as the target device. The second configuration is performed at the master controller.

Target Device

```
Router> enable
Router# configure terminal
Router(config)# ip sla monitor responder type tcpConnect port 49152
Router(config)# exit
```

Master Controller

```
Router(config)# pfr master
Router(config-pfr-mc)# mode monitor active
Router(config-pfr-mc)# active-probe tcp-conn 10.4.4.44 target-port 49152
```

UDP Probe for Forced Target Assignment Example

The following example shows how to configure active probing with a forced target assignment and a configured probe frequency of 20 seconds. This example requires an IP SLAs Responder to be enabled on the target device.

Target Device

```
Router> enable
Router# configure terminal
Router(config)# ip sla monitor responder type udpEcho port 1001
Router(config)# exit
```

Master Controller

```
Router(config)# pfr master

Router(config-pfr-mc)# mode monitor active
Router(config-pfr-mc)# exit

Router(config)# pfr-map FORCED_MAP 10

Router(config-pfr-map)# match ip address access-list FORCED_LIST
Router(config-pfr-map)# set active-probe udp-echo 10.5.5.57 target-port 1001
Router(config-pfr-map)# set probe frequency 20
Router(config-pfr-map)# end
```

Example Configuring PfR Voice Probes for Fast Failover

The following example, starting in global configuration mode, shows how quickly a new exit can be selected when fast failover is configured.

Note Fast monitoring is a very aggressive mode that incurs a lot of overhead with the continuous probing. We recommend that you use fast monitoring only for performance sensitive traffic.

The first output shows the configuration at the master controller of three border routers. Route control mode is enabled.

```
Router# show run | sec pfr master
pfr master
 policy-rules MAP
 port 7777
 logging
 !
 border 10.3.3.3 key-chain key1
  interface Ethernet9/0 external
  interface Ethernet8/0 internal
 !
 border 10.3.3.4 key-chain key2
  interface Ethernet5/0 external
  interface Ethernet8/0 internal
 !
 border 10.4.4.2 key-chain key3
  interface Ethernet2/0 external
  interface Ethernet8/0 internal
 backoff 90 90
 mode route control
 resolve jitter priority 1 variance 10
 no resolve delay
!
```

To verify the basic configuration and show the status of the border routers, the **show pfr master** command is run:

```
Router# show pfr master
OER state: ENABLED and ACTIVE
  Conn Status: SUCCESS, PORT: 7777
  Version: 2.1
  Number of Border routers: 3
  Number of Exits: 3
  Number of monitored prefixes: 1 (max 5000)
  Max prefixes: total 5000 learn 2500
  Prefix count: total 1, learn 0, cfg 1

Border          Status   UP/DOWN             AuthFail  Version
10.4.4.2        ACTIVE   UP       17:00:32          0  2.1
10.3.3.4        ACTIVE   UP       17:00:35          0  2.1
10.3.3.3        ACTIVE   UP       17:00:38          0  2.1

Global Settings:
  max-range-utilization percent 20 recv 20
  mode route metric bgp local-pref 5000
  mode route metric static tag 5000
  trace probe delay 1000
  logging

Default Policy Settings:
  backoff 90 90 90
  delay relative 50
  holddown 90
  periodic 0
  probe frequency 56
  mode route control
  mode monitor both
  mode select-exit good
  loss relative 10
  jitter threshold 20
  mos threshold 3.60 percent 30
  unreachable relative 50
  resolve jitter priority 1 variance 10
  resolve utilization priority 12 variance 20

Learn Settings:
  current state : DISABLED
  time remaining in current state : 0 seconds
  no throughput
```

```
  no delay
  no inside bgp
  no protocol
  monitor-period 5
  periodic-interval 120
  aggregation-type prefix-length 24
  prefixes 100
  expire after time 720
```

Fast failover is now configured for active voice probes and the probe frequency is set to 2 seconds using a PfR map. The fast failover monitoring mode is enabled and the voice traffic to be monitored is identified using an IP prefix list to specify the 10.1.1.0/24 prefix. To reduce some of the overhead that fast failover monitoring produces, the active voice probes are assigned a forced target for PfR.

```
Router# show run | sec pfr-map
pfr-map MAP 10
 match traffic-class prefix-list VOICE_FAIL_LIST
 set mode select-exit best
 set mode monitor fast
 set jitter threshold 12
 set active-probe jitter 120.120.120.1 target-port 20 codec g729a
 set probe frequency 2
```

The following output from the **show pfr master prefix**command when a prefix is specified with the policy keyword shows the policy configured for the prefix 10.1.1.0/24. Note that the mode monitor is set to fast, which automatically sets the select-exit to best, and allows the probe frequency to be set at 2.

```
Router# show pfr master prefix 10.1.1.0/24 policy
* Overrides Default Policy Setting
pfr-map MAP 10
  sequence no. 8444249301975040, provider id 1, provider priority 30
    host priority 0, policy priority 10, Session id 0
  match ip prefix-lists: VOICE_FAIL_LIST
  backoff 90 90 90
  delay relative 50
  holddown 90
  periodic 0
 *probe frequency 2
  mode route control
 *mode monitor fast
 *mode select-exit best
  loss relative 10
 *jitter threshold 12
  mos threshold 3.60 percent 30
  unreachable relative 50
  next-hop not set
  forwarding interface not set
  resolve jitter priority 1 variance 10
  resolve utilization priority 12 variance 20

  Forced Assigned Target List:
   active-probe jitter 10.120.120.1 target-port 20 codec g729a
```

After the master controller is configured for fast failover as shown in this task, and a traffic class goes out of policy, the logging output below shows that the traffic class represented by prefix 10.1.1.0/24 is routed by PfR through a new border router exit at interface 10.3.3.4 within 3 seconds. From the logging output, it appears that the traffic class moved to an out-of-policy state due to the jitter threshold being exceeded.

```
May  2 10:55:27.355: %OER_MC-5-NOTICE: Active ABS Jitter OOP Prefix 10.1.1.0/24,
jitter 15, BR 10.4.4.2, i/f Et2/0
May  2 10:55:27.367: %OER_MC-5-NOTICE: Route changed Prefix 10.1.1.0/24, BR 10.3.3.4,
i/f Et5/0, Reason Jitter, OOP Reason Jitter
```

Example Configuring the Source Address of an Active Probe

The following example, starting in global configuration mode, configures FastEthernet 0/0 as the active-probe source interface.

```
Router(config)# pfr border
Router(config-pfr-br)# active-probe address source interface FastEthernet 0/0
```

Apply Policy Phase Tasks Examples

Example Configuring and Applying a PfR Policy to Learned Traffic Classes

The following example uses learned traffic classes and overwrites many of the default policy settings and configures the master controller to move traffic classes to the best available exit link when any of the configured or default policy settings exceed their thresholds:

```
enable
configure terminal
pfr master
 backoff 200 2000 200
 delay threshold 2000
 holddown 400
 loss threshold 1500
 periodic 180
 unreachable threshold 1000
 mode select-exit best
 end
```

Example Configuring and Applying a PfR Policy to Configured Traffic Classes

The following example uses traffic classes filtered by a prefix list and an access list and overwrites some of the default policy settings. The policies are configured using two PfR maps that apply to different traffic classes that represent voice traffic. The master controller is configured to move traffic classes to the first in-policy exit link when any of the configured or default policy settings exceed their thresholds.

```
enable
configure terminal
ip prefix-list CONFIG_TRAFFIC_CLASS seq 10 permit 10.1.5.0/24
ip access-list extended VOICE_TRAFFIC_CLASS
 permit udp any range 16384 32767 10.1.5.0 0.0.0.15 range 16384 32767 dscp ef
 exit
pfr-map CONFIG_MAP 10
 match ip address prefix-list CONFIG_TRAFFIC_CLASS
 set backoff 100 1000 100
 set delay threshold 1000
 set loss relative 25
 set periodic 360
 set unreachable relative 20
 exit
pfr-map VOICE_MAP 10
 match ip address access-list VOICE_TRAFFIC_CLASS
 set active-probe jitter 10.1.5.1 target-port 2000 codec g729a
 set probe-frequency 20
 set jitter threshold 30
 set mos threshold 4.0 percent 25
 set mode select-exit good
 end
```

Example Preventing PfR Optimization of Learned Prefixes

The following example shows how to configure PfR to prevent specified prefixes being optimized. In this example, an IP prefix list is created with two entries for different prefixes that are not to be optimized. A PfR map is configured with two entries in a sequence that will prevent PfR from optimizing the prefixes specified in the prefix list, although the prefixes may be learned. If the sequence numbers of the PfR map entries are reversed, PfR will learn and attempt to optimize the prefixes.

```
enable
configure terminal
ip prefix-list DENY_PREFIX deny 172.17.10.0/24
ip prefix-list DENY_PREFIX deny 172.19.10.0/24
pfr-map DENY_PREFIX_MAP 10
 match ip address prefix-list DENY_PREFIX
 exit
pfr-map DENY_PREFIX_MAP 20
 match pfr learn throughput
 end
```

Example Configuring Policy Rules for PfR Maps

The following example shows how to configure the **policy-rules** (PfR) command to apply the PfR map configuration named BLUE under PfR master controller mode:

```
enable
configure terminal
pfr-map BLUE 10
 match pfr learn delay
 set loss relative 90
 exit
pfr master
 policy-rules BLUE
 exit
```

Example Configuring Multiple PfR Policy Conflict Resolution

The following example configures a PfR resolve policy that sets delay to the highest priority, followed by loss, and then utilization. The delay policy is configured to allow a 20 percent variance, the loss policy is configured to allow a 30 percent variance, and the utilization policy is configured to allow a 10 percent variance.

```
enable
configure terminal
pfr master
 resolve delay priority 1 variance 20
 resolve loss priority 2 variance 30
 resolve utilization priority 3 variance 10
 end
```

Example Configuring an Exit Link Load Balancing PfR Policy

The following example configures a PfR load balancing policy for traffic class flows over the border router exit links. This example task is performed at the master controller and configures an exit link utilization range and an exit link utilization threshold with policy priorities set for utilization and range policies. Performance

policies, delay and loss, are disabled. PfR uses both the utilization and range thresholds to load balance the traffic flow over the exit links.

```
enable
configure terminal
pfr master
 max-range-utilization percentage 25
 mode select-exit best
 resolve range priority 1
 resolve utilization priority 2 variance 15
 no resolve delay
 no resolve loss
 border 10.1.4.1
 interface Ethernet 1/0 external
 max-xmit-utilization absolute 10000
 exit
 exit
 border 10.1.2.1
 interface Ethernet 1/0 external
 max-xmit-utilization absolute 10000
 end
```

Example Configuring Black Hole Routing Using a PfR Map

The following example creates a PfR map named BLACK_HOLE_MAP that matches traffic defined in the IP prefix list named PREFIX_BLACK_HOLE. The PfR map filters packets to be forwarded to a null interface, meaning that the packets are discarded in a “black hole.” The prefix list is configured after an IP prefix is identified as the source of the attack on the network.

```
enable
configure terminal
ip prefix-list PREFIX_BLACK_HOLE seq 10 permit 10.1.5.0/24
pfr-map BLACK_HOLE_MAP 10
 match ip address prefix-list PREFIX_BLACK_HOLE
 set interface null0
 end
```

Example Configuring Sinkhole Routing Using a PfR Map

The following example creates a PfR map named SINK_HOLE_MAP that matches traffic defined in the IP prefix list named PREFIX_SINK_HOLE. The PfR map filters packets to be forwarded to a next hop. The next hop is a router where the packets can be stored, analyzed, or discarded (the sinkhole analogy). The prefix list is configured after an IP prefix is identified as the source of an attack on the network.

```
enable
configure terminal
ip prefix-list PREFIX_SINK_HOLE seq 10 permit 10.1.5.0/24
pfr-map SINK_HOLE_MAP 10
 match ip address prefix-list PREFIX_SINK_HOLE
 set next-hop 10.1.1.3
 end
```

Enforce Phase Tasks Examples

Example Setting a Tag Value for Injected PfR Static Routes

The following example shows how to set a tag value for an injected static route to allow the routes to be uniquely identified. A static route may be injected by PfR to control the traffic defined by a traffic class when it goes out-of-policy. By default, PfR uses a tag value of 5000 for injected static routes. In this task, the PfR route control mode is configured globally with the **mode** (PfR) command in PfR master controller configuration mode and any injected static routes will be tagged with a value of 15000.

```
Router(config)# pfr master
Router(config-pfr-mc)# mode route control

Router(config-pfr-mc)# mode route metric static tag 15000
Router(config-pfr-mc)# end
```

Example Setting a BGP Local Preference Value for PfR Controlled BGP Routes

The following example shows how to set a BGP local preference attribute value. PfR uses the BGP Local_Pref value to influence the BGP best path selection on internal BGP (iBGP) neighbors as a method of enforcing exit link selection. By default, PfR uses a Local_Pref value of 5000. In this task, route control is enabled for traffic matching a prefix list and the BGP local preference value of 60000 is set.

```
Router(config)# pfr-map BLUE 10
Router(config-pfr-map)# match ip address prefix-list BLUE
Router(config-pfr-map)# set mode route control
Router(config-pfr-map)# set mode route metric bgp local-pref 60000
Router(config-pfr-map)# end
```

Example Controlling Application Traffic

The following example shows how to use policy-based routing (PBR) to allow PfR to control specified application traffic classes. Application traffic such as Telnet traffic is delay sensitive. Long TCP delays can make Telnet sessions difficult to use. This example is configured on a master controller and matches Telnet traffic sourced from the 192.168.1.0/24 network and applies a policy to ensure it is sent out through exit links with that have a response time that is equal to or less than 30 milliseconds:

```
Router(config)# ip access-list extended TELNET
Router(config-ext-nacl)# permit tcp 192.168.1.0 0.0.0.255 any eq telnet
Router(config-ext-nacl)# exit

Router(config)# pfr-map SENSITIVE
Router(config-route-map)# match ip address access-list TELNET
Router(config-route-map)# set mode route control
Router(config-route-map)# set delay threshold 30
Router(config-route-map)# set resolve delay priority 1 variance 20
Router(config-route-map)# end
```

The following example shows TCP application traffic filtered based on port 23 (Telnet):

```
Router# show pfr master appl tcp 23 23 dst policy

Prefix              Appl Prot       Port                 Port Type       Policy
-------------------------------------------------------------------------------
10.1.1.0/24        tcp             [23, 23]             src             10
```

Verify Phase Task Example

Example Manually Verifying the PfR Route Control Changes

The following examples show how to manually verify that the traffic control implemented by the PfR enforce phase actually changes the traffic flow and brings the OOP event to be in-policy. On the master controller the **show logging** command is used to display the state of system logging (syslog) and the contents of the standard system logging buffer. Using optional delimiters, the logging buffer can be displayed with PfR messages for a specific prefix. The **show pfr master prefix** command displays the status of monitored prefixes. On the border router, the **show pfr border routes** command displays information about PfR controlled BGP or static routes on the border router. For example output of these commands, see the "Manually Verifying the PfR Route Enforce Changes" section.

Master Controller

```
Router# show logging | i 10.1.1.0
Router# show pfr master
prefix 10.1.1.0
Router# end
```

Border Router

```
Router# show pfr border routes static
Router# show pfr border routes bgp
Router# end
```

Where to Go Next

For more detailed concepts, see the “Understanding Performance Routing” module.

For information about other Performance Routing features or general conceptual material, see the documents in the “Related Documents” section.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco PfR commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples	Cisco IOS Performance Routing Command Reference
Basic PfR configuration	"Configuring Basic Performance Routing" module

Related Topic	Document Title
Concepts required to understand the Performance Routing operational phases	"Understanding Performance Routing" module
Advanced PfR configuration	"Configuring Advanced Performance Routing" module
IP SLAs overview	*IP SLAs Configuration Guide*
PfR home page with links to PfR-related content on our DocWiki collaborative environment	PfR:Home

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 Configuring Advanced Performance 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 4: Feature Information for Configuring Advanced Performance Routing

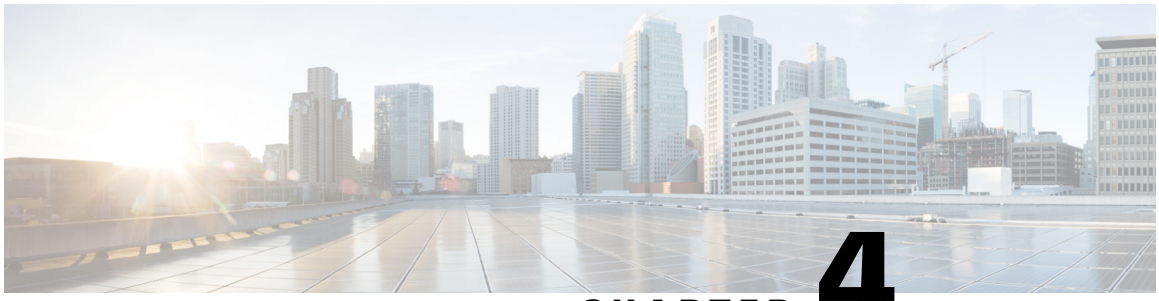
Feature Name	Releases	Feature Information
Optimized Edge Routing	12.3(8)T 12.2(33)SRB	OER was introduced. Performance Routing is an extension of OER.

Feature Name	Releases	Feature Information
OER Support for Policy-Rules Configuration	12.3(11)T 12.2(33)SRB	The OER Support for Policy-Rules Configuration feature introduced the capability to select a PfR map and apply the configuration under PfR master controller configuration mode, providing an improved method to switch between predefined PfR maps. The following commands were introduced or modified by this feature: **policy-rules**(PfR).
expire after command[3]	12.3(14)T 12.2(33)SRB	The**expire after** (PfR) command is used to set an expiration period for learned prefixes. By default, the master controller removes inactive prefixes from the central policy database as memory is needed. This command allows you to refine this behavior by setting a time or session based limit. The time based limit is configured in minutes. The session based limit is configured for the number of monitor periods (or sessions).
OER Active Probe Source Address	12.4(2)T 12.2(33)SRB	The OER Active Probe Source Address feature allows you to configure a specific exit interface on the border router as the source for active probes. The **active-probe address source** (PfR) command was introduced by this feature.

Feature Name	Releases	Feature Information
OER Application-Aware Routing: PBR	12.4(2)T 12.2(33)SRB	The OER Application-Aware Routing: PBR feature introduces the capability to optimize IP traffic based on the type of application that is carried by the monitored prefix. Independent policy configuration is applied to the subset (application) of traffic. The following commands were introduced or modified by this feature: **debug pfr border pbr**, **debug pfr master prefix**, **match ip address (PfR)**,**show pfr master active-probes**, and **show pfr master appl**.
OER DSCP Monitoring	12.4(9)T 12.2(33)SRB	OER DSCP Monitoring introduced automatic learning of traffic classes based on protocol, port numbers, and DSCP value. Traffic classes can be defined by a combination of keys comprising of protocol, port numbers, and DSCP values, with the ability to filter out traffic that is not required, and the ability to aggregate the traffic in which you are interested. Layer 4 information such as protocol, port number, and DSCP information is now sent to the master controller database in addition to the Layer 3 prefix information. The new functionality allows PfR to both actively and passively monitor application traffic. The following commands were introduced or modified by this feature: **show pfr border passive applications**,**show pfr border passive cache**, **show pfr border passive learn**, **show pfr master appl**, **traffic-class aggr egation (PfR)**, **traffic-class filter (PfR)**, and **traffic-class key s (PfR)**.

Feature Name	Releases	Feature Information
Performance Routing - Link Groups	12.4(15)T	The Performance Routing - Link Groups feature introduces the ability to define a group of exit links as a preferred set of links, or a fallback set of links for PfR to use when optimizing traffic classes specified in a PfR policy. The following commands were introduced or modified by this feature: **link-group (PfR)**, **set link-group (PfR)**, and **show pfr master link-group**.
Support for Fast Failover Monitoring[4]	12.4(15)T	Fast Failover Monitoring introduced the ability to configure a fast monitoring mode. In fast failover monitoring mode, all exits are continuously probed using active monitoring and passive monitoring. The probe frequency can be set to a lower frequency in fast failover monitoring mode than for other monitoring modes, to allow a faster failover capability. Fast failover monitoring can be used with all types of active probes: ICMP echo, jitter, TCP connection, and UDP echo. The following commands were modified by this feature: **mode (PfR)**, **set mode (PfR)**.

3 This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.
4 This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.



CHAPTER 4

BGP Inbound Optimization Using Performance Routing

The PfR BGP Inbound Optimization feature introduced support for the best entrance selection for traffic that originates from prefixes outside an autonomous system destined for prefixes inside the autonomous system. External BGP (eBGP) advertisements from an autonomous system to an Internet service provider (ISP) can influence the entrance path for traffic entering the network. PfR uses eBGP advertisements to manipulate the best entrance selection.

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 Table at the end of this document.

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 BGP Inbound Optimization Using Performance Routing

BGP Inbound Optimization

The PfR BGP Inbound Optimization feature introduced the ability to support inside prefixes. Using BGP, PfR can select inside prefixes to support best entrance selection for traffic that originates from prefixes outside an autonomous system destined for prefixes inside the autonomous system. Company networks advertise the inside prefixes over the Internet using an Internet service provider (ISP) and receive advertisements for outside prefixes from an ISP.

BGP inbound optimization provides the ability to manually configure or automatically learn inside prefixes. The resulting prefixes can be monitored using link utilization threshold or link utilization range techniques. Link policies defining traffic load or range performance characteristics can be applied against PfR-managed entrance links. BGP inbound optimization provides the ability to influence inbound traffic by manipulating eBGP advertisements to influence the best entrance selection for traffic bound for inside prefixes.

Note Although PfR can learn an inside prefix, PfR will not try to control an inside prefix unless there is an exact match in the BGP routing information base (RIB) because PfR does not advertise a new prefix to the Internet.

Prefix Traffic Class Learning Using PfR

The PfR master controller can be configured, using NetFlow Top Talker functionality, to automatically learn prefixes based on the highest outbound throughput or the highest delay time. Throughput learning measures prefixes that generate the highest outbound traffic volume. Throughput prefixes are sorted from highest to lowest. Delay learning measures prefixes with the highest round-trip response time (RTT) to optimize these highest delay prefixes to try to reduce the RTT for these prefixes. Delay prefixes are sorted from the highest to the lowest delay time.

PfR can automatically learn two types of prefixes:

- outside prefix--An outside prefix is defined as a public IP prefix assigned outside the company. Outside prefixes are received from other networks.
- inside prefix--An inside prefix is defined as a public IP prefix assigned to a company. An inside prefix is a prefix configured within the company network. The maximum number of inside prefixes that can be learned in a monitoring period is 30.

The PfR BGP Inbound Optimization feature introduced the ability to learn inside prefixes. Using BGP, PfR can select inside prefixes to support best entrance selection for traffic that originates from prefixes outside an autonomous system destined for prefixes inside the autonomous system. Company networks advertise the inside prefixes over the Internet using an Internet service provider (ISP) and receive advertisements for outside prefixes from an ISP.

PfR Link Utilization Measurement

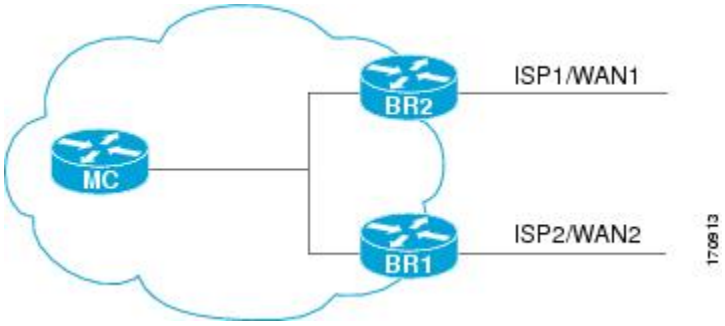
Link Utilization Threshold

After an external interface is configured for a border router, PfR automatically monitors the utilization of the external link (an external link is an interface on a border router that typically links to a WAN). Every 20 seconds, by default, the border router reports the link utilization to the master controller. Both egress (transmitted) and ingress (received) traffic utilization values are reported to the master controller. If the exit or entrance link utilization is above the default threshold of 75 percent, the exit or entrance link is in an OOP state and PfR starts the monitoring process to find an alternative link for the traffic class. The link utilization threshold can be manually configured either as an absolute value in kilobytes per second (kbps) or as a percentage.

Link Utilization Range

PfR can also be configured to calculate the range of utilization over all the links. Both egress (transmitted) and ingress (received) traffic utilization values are reported to the master controller. In the figure below there are two border routers with exits links to the Internet through two ISPs. The master controller determines which link on one of the border routers--either BR1 or BR2 in the figure below--is used by a traffic class.

Figure 10: PfR network diagram



PfR range functionality attempts to keep the exit or entrance links within a utilization range, relative to each other to ensure that the traffic load is distributed. The range is specified as a percentage and is configured on the master controller to apply to all the exit or entrance links on border routers managed by the master controller. For example, if the range is specified as 25 percent, and the utilization of the exit link at BR1 (in the figure above) is 70 percent, then if the utilization of the exit link at BR2 (in the figure above) falls to 40 percent, the percentage range between the two exit links will be more than 25 percent and PfR will attempt to move some traffic classes to use the exit link at BR1 to even the traffic load. If BR1 (in the figure above) is being configured as an entrance link, the link utilization range calculations work in the same way as for an exit link, except that the utilization values are for received traffic, not transmitted traffic.

PfR Link Policies

PfR link policies are a set of rules that are applied against PfR-managed external links (an external link is an interface on a border router on the network edge). Link policies define the desired performance characteristics of the links. Instead of defining the performance of an individual traffic class entry that uses the link (as in traffic class performance policies), link policies are concerned with the performance of the link as a whole.

The BGP Inbound Optimization feature introduced support for selected entrance (ingress) link policies.

The following performance characteristics are managed by link policies:

- Traffic Load (Utilization)
- Range
- Cost—Cost policies are not supported by the BGP Inbound Optimization feature. For more details about cost policies, see the "Configuring Performance Routing Cost Policies" module.

Traffic Load

A traffic load (also referred to as utilization) policy consists of an upper threshold on the amount of traffic that a specific link can carry. Cisco IOS PfR supports per traffic class load distribution. Every 20 seconds, by default, the border router reports the link utilization to the master controller, after an external interface is configured for a border router. Both exit link and entrance link traffic load thresholds can be configured as an PfR policy. If the exit or entrance link utilization is above the configured threshold, or the default threshold of 75-percent, the exit or entrance link is in an OOP state and PfR starts the monitoring process to find an alternative link for the traffic class. The link utilization threshold can be manually configured either as an absolute value in kilobytes per second (kbps) or as a percentage. A load utilization policy for an individual interface is configured on the master controller under the border router configuration.

Tip When configuring load distribution, we recommend that you set the interface load calculation on external interfaces to 30-second intervals with the **load-interval** interface configuration command. The default calculation interval is 300 seconds. The load calculation is configured under interface configuration mode on the border router. This configuration is not required, but it is recommended to allow Cisco IOS PfR to respond as quickly as possible to load distribution issues.

Range

A range policy is defined to maintain all links within a certain utilization range, relative to each other in order to ensure that the traffic load is distributed. For example, if a network has multiple exit links, and there is no financial reason to choose one link over another, the optimal choice is to provide an even load distribution across all links. The load-sharing provided by traditional routing protocols is not always evenly distributed, because the load-sharing is flow-based rather than performance- or policy-based. Cisco IOS PfR range functionality allows you to configure PfR to maintain the traffic utilization on a set of links within a certain percentage range of each other. If the difference between the links becomes too great, PfR will attempt to bring the link back to an in-policy state by distributing traffic classes among the available links. The master controller sets the maximum range utilization to 20-percent for all PfR-managed links by default, but the utilization range can be configured using a maximum percentage value. Both exit link and entrance link utilization ranges can be configured as a PfR policy.

Note If you are configuring link grouping, configure the **no max-range-utilization** command because using a link utilization range is not compatible with using a preferred or fallback set of exit links configured for link grouping. With CSCtr33991, this requirement is removed and PfR can perform load balancing within a PfR link group.

PfR Entrance Link Selection Control Techniques

The PfR BGP inbound optimization feature introduced the ability to influence inbound traffic. A network advertises reachability of its inside prefixes to the Internet using eBGP advertisements to its ISPs. If the same prefix is advertised to more than one ISP, then the network is multihoming. PfR BGP inbound optimization works best with multihomed networks, but it can also be used with a network that has multiple connections to the same ISP. To implement BGP inbound optimization, PfR manipulates eBGP advertisements to influence the best entrance selection for traffic bound for inside prefixes. The benefit of implementing the best entrance selection is limited to a network that has more than one ISP connection.

To enforce an entrance link selection, PfR offers the following methods:

BGP Autonomous System Number Prepend

When an entrance link goes out-of-policy (OOP) due to delay, or in images prior to Cisco IOS Releases 15.2(1)T1 and 15.1(2)S, and PfR selects a best entrance for an inside prefix, extra autonomous system hops are prepended one at a time (up to a maximum of six) to the inside prefix BGP advertisement over the other entrances. In Cisco IOS Releases 15.2(1)T1, 15.1(2)S, and later releases, when an entrance link goes out-of-policy (OOP) due to unreachable or loss reasons, and PfR selects a best entrance for an inside prefix, six extra autonomous system hops are prepended immediately to the inside prefix BGP advertisement over the other entrances. The extra autonomous system hops on the other entrances increase the probability that the best entrance will be used for the inside prefix. When the entrance link is OOP due to unreachable or loss reasons, six extra autonomous system hops are added immediately to allow the software to quickly move the traffic away from the old entrance link. This is the default method PfR uses to control an inside prefix, and no user configuration is required.

BGP Autonomous System Number Community Prepend

When an entrance link goes out-of-policy (OOP) due to delay, or in images prior to Cisco IOS Releases 15.2(1)T1 and 15.1(2)S, and PfR selects a best entrance for an inside prefix, a BGP prepend community is attached one at a time (up to a maximum of six) to the inside prefix BGP advertisement from the network to another autonomous system such as an ISP. In Cisco IOS Releases 15.2(1)T1, 15.1(2)S, and later releases, when an entrance link goes out-of-policy (OOP) due to unreachable or loss reasons, and PfR selects a best entrance for an inside prefix, six BGP prepend communities are attached to the inside prefix BGP advertisement. The BGP prepend community will increase the number of autonomous system hops in the advertisement of the inside prefix from the ISP to its peers. Autonomous system prepend BGP community is the preferred method to be used for PfR BGP inbound optimization because there is no risk of the local ISP filtering the extra autonomous system hops. There are some issues, for example, not all ISPs support the BGP prepend community, ISP policies may ignore or modify the autonomous system hops, and a transit ISP may filter the autonomous system path. If you use this method of inbound optimization and a change is made to an autonomous system, you must issue an outbound reconfiguration using the **clear ip bgp** command.

PfR Map Operation for Inside Prefixes

The operation of a PfR map is similar to the operation of a route-map. A PfR map is configured to select an IP prefix list or PfR learn policy using a match clause and then to apply PfR policy configurations using a set clause. The PfR map is configured with a sequence number like a route-map, and the PfR map with the lowest sequence number is evaluated first.

The BGP Inbound Optimization feature introduced the **inside** keyword to the **match ip address** (PfR) command to identify inside prefixes. Inbound BGP only supports the passive mode which results in some configuration

restrictions when using a PfR map. The following commands are not supported in a PfR map for inbound BGP; **set active-probe**, **set interface**, **set mode monitor**, **set mode verify bidirectional**, **set mos threshold**, **set nexthop**, **set periodic**, **set probe frequency**, and **set traceroute reporting**.

Note Match precedence priority is not supported in PfR maps.

How to Configure BGP Inbound Optimization Using Performance Routing

Configuring PfR to Automatically Learn Traffic Classes Using Inside Prefixes

Perform this task at a PfR master controller to configure PfR to automatically learn inside prefixes to be used as traffic classes. The traffic classes are entered in the MTC list. This task introduces the **inside bgp** (PfR) command used in PfR Top Talker and Top Delay configuration mode. This task configures automatic prefix learning of the inside prefixes (prefixes within the network). Optional configuration parameters such as learning period timers, maximum number of prefixes, and an expiration time for MTC list entries are also shown.

Before You Begin

Before configuring this task, BGP peering for internal and external BGP neighbors must be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **learn**
5. **inside bgp**
6. **monitor-period** *minutes*
7. **periodic-interval** *minutes*
8. **prefixes** *number*
9. **expire after session** *number* | **time** *minutes*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure a router as a master controller and to configure global operations and policies.
Step 4	**learn** **Example:** `Router(config-pfr-mc)# learn`	Enters PfR Top Talker and Top Delay learning configuration mode to configure prefix learning policies and timers.
Step 5	**inside bgp** **Example:** `Router(config-pfr-mc-learn)# inside bgp`	Learns prefixes inside the network.
Step 6	**monitor-period** *minutes* **Example:** `Router(config-pfr-mc-learn)# monitor-period 10`	(Optional) Sets the time period that a PfR master controller learns traffic flows. • The default learning period is 5 minutes. • The length of time between monitoring periods is configured with the **periodic-interval** command. • The number of prefixes that are learned is configured with the **prefixes** command. • The example sets the length of each monitoring period to 10 minutes.
Step 7	**periodic-interval** *minutes* **Example:** `Router(config-pfr-mc-learn)# periodic-interval 20`	(Optional) Sets the time interval between prefix learning periods. • By default, the interval between prefix learning periods is 120 minutes. • The example sets the time interval between monitoring periods to 20 minutes.
Step 8	**prefixes** *number* **Example:** `Router(config-pfr-mc-learn)# prefixes 30`	(Optional) Sets the number of prefixes that the master controller will learn during the monitoring period. • By default, the top 100 traffic flows are learned. • The example configures a master controller to learn 30 prefixes during each monitoring period.

	Command or Action	Purpose
		Note The maximum number of inside prefixes that can be learned in a monitoring period is 30.
Step 9	**expire after session** *number* | **time** *minutes* **Example:** `Router(config-pfr-mc-learn)# expire after session 100`	(Optional) Sets the length of time that learned prefixes are kept in the central policy database. • The **session** keyword configures learned prefixes to be removed after the specified number of monitoring periods have occurred. • The **time** keyword configures learned prefixes to be removed after the specified time period. The time value is entered in minutes. • The example configures learned prefixes to be removed after 100 monitoring periods.
Step 10	**end** **Example:** `Router(config-pfr-mc-learn)# end`	Exits PfR Top Talker and Top Delay learning configuration mode, and enters privileged EXEC mode.

Manually Selecting Inside Prefixes for PfR Monitoring

The PfR BGP inbound optimization feature introduced the ability to manually select inside prefixes to support best entrance selection for traffic that originates from prefixes outside an autonomous system destined for prefixes inside the autonomous system. Perform this task to manually select inside prefixes for PfR monitoring by creating an IP prefix list to define the inside prefix or prefix range. The prefix list is then imported into the Monitored Traffic Class (MTC) list by configuring a match clause in a PfR map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*]{**deny** *network/length* | **permit** *network/length*}
4. **pfr-map map-name** *sequence-number*
5. **match ip address prefix-list** *name* [**inside**]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip prefix-list** *list-name* [**seq** *seq-value*]{**deny** *network/length* | **permit** *network/length*} **Example:** `Router(config)# ip prefix-list INSIDE_PREFIXES seq 20 permit 192.168.1.0/24`	Creates a prefix list to manually select prefixes for monitoring. • A master controller can monitor and control an exact prefix of any length including the default route. The master controller acts only on the configured prefix. • The example creates an IP prefix list for PfR to monitor and control the exact prefix, 192.168.1.0/24
Step 4	**pfr-map map-name** *sequence-number* **Example:** `Router(config)# pfr-map INSIDE_MAP 10`	Enters PfR map configuration mode to create or configure a PfR map. • PfR map operation is similar to that of route maps. • Only a single match clause can be configured for each PfR map sequence. • Common and deny sequences should be applied to lowest PfR map sequence for best performance. • The example creates a PfR map named INSIDE_MAP.
Step 5	**match ip address prefix-list** *name* [**inside**] **Example:** `Router(config-pfr-map)# match ip address prefix-list INSIDE_PREFIXES inside`	Creates a prefix list match clause entry in a PfR map to apply PfR policies. • This command supports IP prefix lists only. • Use the **inside** keyword to identify inside prefixes. • The example creates a match clause to use the prefix list INSIDE_PREFIXES to specify that inside prefixes must be matched.
Step 6	**end** **Example:** `Router(config-pfr-map)# end`	Exits PfR map configuration mode and returns to privileged EXEC mode.

Modifying the PfR Link Utilization for Inbound Traffic

The BGP Inbound Optimization feature introduced the ability to report inbound traffic utilization to the master controller. Perform this task at the master controller to modify the PfR entrance (inbound) link utilization threshold. After an external interface has been configured for a border router, PfR automatically monitors the utilization of entrance links on a border router every 20 seconds. The utilization is reported back to the master controller and, if the utilization exceeds 75 percent, PfR selects another entrance link for traffic classes on that link. An absolute value in kilobytes per second (kbps), or a percentage, can be specified.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **border** *ip-address* [**key-chain** *key-chain-name*]
5. **interface** *type number* **external**
6. **maximum utilization receive** {**absolute** *kbps* | **percent** *percentage*}
7. **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.
Step 3	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure a router as a master controller and to configure global operations and policies.
Step 4	**border** *ip-address* [**key-chain** *key-chain-name*] **Example:** `Router(config-pfr-mc)# border 10.1.1.2`	Enters PfR-managed border router configuration mode to establish communication with a border router. • An IP address is configured to identify the border router. • At least one border router must be specified to create an PfR-managed network. A maximum of ten border routers can be controlled by a single master controller.

	Command or Action	Purpose
		Note The **key-chain** keyword and *key-chain-name* argument must be entered when a border router is initially configured. However, this keyword is optional when reconfiguring an existing border router.
Step 5	**interface** *type number* **external** **Example:** `Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/0 external`	Configures a border router interface as an PfR-managed external interface and enters PfR border exit interface configuration mode. • External interfaces are used to forward traffic and for active monitoring. • A minimum of two external border router interfaces are required in a PfR-managed network. At least one external interface must be configured on each border router. A maximum of 20 external interfaces can be controlled by single master controller. **Note** Entering the **interface** command without the **external** or**internal** keyword places the router in global configuration mode and not PfR border exit configuration mode. The **no** form of this command should be applied carefully so that active interfaces are not removed from the router configuration.
Step 6	**maximum utilization receive** {**absolute** *kbps* | **percent** *percentage*} **Example:** `Router(config-pfr-mc-br-if)# maximum utilization receive percent 90`	Sets the maximum receive utilization threshold for the configured PfR-managed link interface. • Use the **absolute** keyword and *kbps* argument to specify the absolute threshold value, in kilobytes per second (kbps), of the throughput for all the entrance links. • Use the **percent** keyword and *percentage* argument to specify the maximum utilization threshold as a percentage of bandwidth received by all the entrance links. • In this example, the maximum utilization threshold of inbound traffic on this entrance link on the border router must be 90 percent, or less.
Step 7	**end** **Example:** `Router(config-pfr-mc-br-if)# end`	Exits PfR border exit interface configuration mode and returns to privileged EXEC mode.

Modifying the PfR Entrance Link Utilization Range

Perform this task at the master controller to modify the maximum entrance link utilization range over all the border routers. By default, PfR automatically monitors the utilization of external links on a border router every 20 seconds, and the border router reports the utilization to the master controller. The BGP Inbound Optimization feature introduced the ability to report inbound traffic utilization to the master controller, and to specify a link utilization range for entrance links.

In this task, if the utilization range between all the entrance links exceeds 20 percent, the master controller tries to equalize the traffic load by moving some traffic classes to another entrance link. The maximum utilization range is configured as a percentage.

PfR uses the maximum utilization range to determine if links are in-policy. In this task, PfR will equalize inbound traffic across all entrance links by moving traffic classes from overutilized or out-of-policy exits to in-policy exits.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **max range receive percent** *percentage*
5. **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.
Step 3	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure a router as a master controller and to configure global operations and policies.
Step 4	**max range receive percent** *percentage* **Example:** `Router(config-pfr-mc)# max range receive percent 20`	Specifies the upper limit of the receive utilization range between all the entrance links on the border routers. • The **percent** keyword and *percentage* argument are used to specify the range percentage. • In this example, the receive utilization range between all the entrance links on the border routers must be within 20 percent.
Step 5	**end** **Example:** `Router(config-pfr-mc)# end`	Exits PfR master controller configuration mode and returns to privileged EXEC mode.

Configuring and Applying a PfR Policy to Learned Inside Prefixes

Perform this task to apply a policy to learned inside prefix traffic class entries from the MTC list at the master controller. Support for optimizing inside prefixes was introduced in the BGP Inbound Optimization feature. The policy is configured using a PfR map and contains some set clauses.

Inbound BGP only supports the passive mode which results in some configuration restrictions when using a PfR map. The following commands are not supported in a PfR map for inbound BGP; **set active-probe**, **set interface**, **set mode monitor**, **set mode verify bidirectional**, **set mos threshold**, **set nexthop**, **set periodic**, **set probe frequency**, and **set traceroute reporting**.

Note Policies applied in an PfR map do not override global policy configurations.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr-map** *map-name sequence-number*
4. **match pfr learn inside**
5. **set delay** {**relative** *percentage* | **threshold** *maximum*}
6. **set loss** {**relative** *average* | **threshold** *maximum*}
7. **set unreachable** {**relative** *average* | **threshold** *maximum*}
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.
Step 3	**pfr-map** *map-name sequence-number*	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.

	Command or Action	Purpose
	Example: `Router(config)# pfr-map INSIDE_LEARN 10`	• Only one match clause can be configured for each PfR map sequence. • Deny sequences are first defined in an IP prefix list and then applied with a **match**command. • The example creates an PfR map named INSIDE_LEARN.
Step 4	**match pfr learn inside** **Example:** `Router(config-pfr-map)# match pfr learn inside`	Creates a match clause entry in an PfR map to match PfR learned prefixes. • Prefixes can be configured to learn prefixes that are inside prefixes or prefixes based on lowest delay, or highest outbound throughput. • Only a single match clause can be configured for each PfR map sequence. • The example creates a match clause entry that matches traffic learned using inside prefixes.
Step 5	**set delay** {**relative** *percentage* | **threshold** *maximum*} **Example:** `Router(config-pfr-map)# set delay threshold 2000`	Creates a set clause entry to configure the delay threshold. • The delay threshold can be configured as a relative percentage or as an absolute value for match criteria. • The **relative** keyword is used to configure a relative delay percentage. The relative delay percentage is based on a comparison of short-term and long-term measurements. • The **threshold** keyword is used to configure the absolute maximum delay period in milliseconds. • The example creates a set clause that sets the absolute maximum delay threshold to 2000 milliseconds for traffic that is matched in the same PfR map sequence.
Step 6	**set loss** {**relative** *average* | **threshold** *maximum*} **Example:** `Router(config-pfr-map)# set loss relative 20`	Creates a set clause entry to configure the relative or maximum packet loss limit that the master controller will permit for an exit link. • This command is used to configure a PfR map to configure the relative percentage or maximum number of packets that PfR will permit to be lost during transmission on an exit link. If packet loss is greater than the user-defined or the default value, the master controller determines that the exit link is out-of-policy. • The **relative** keyword is used to configure the relative packet loss percentage. The relative packet loss percentage is based on a comparison of short-term and long-term packet loss. • The**threshold**keyword is used to configure the absolute maximum packet loss. The maximum value is based on the actual number of packets per million that have been lost. • The example creates a set clause that configures the relative percentage of acceptable packet loss to less than 20 percent for traffic that is matched in the same PfR map sequence.

	Command or Action	Purpose
Step 7	**set unreachable** {**relative** *average* | **threshold** *maximum*} **Example:** `Router(config-pfr-map)# set unreachable relative 10`	Creates a set clause entry to configure the maximum number of unreachable hosts. • This command is used to specify the relative percentage or the absolute maximum number of unreachable hosts, based on flows per million (fpm), that PfR will permit for a traffic class entry. If the absolute number or relative percentage of unreachable hosts is greater than the user-defined or the default value, PfR determines that the traffic class entry is OOP and searches for an alternate exit link. • The **relative** keyword is used to configure the relative percentage of unreachable hosts. The relative unreachable host percentage is based on a comparison of short-term and long-term measurements. • The**threshold**keyword is used to configure the absolute maximum number of unreachable hosts based on fpm. • The example creates a set clause entry that configures the master controller to search for a new exit link for a traffic class entry when the relative percentage of unreachable hosts is equal to or greater than 10 percent for traffic learned based on highest delay.
Step 8	**end** **Example:** `Router(config-pfr-map)# end`	(Optional) Exits PfR map configuration mode and returns to privileged EXEC mode.

Configuring and Applying a PfR Policy to Configured Inside Prefixes

Perform this task to apply a policy to configured inside prefix traffic class entries from the MTC list at the master controller. Support for optimizing inside prefixes was introduced in the BGP Inbound Optimization feature. The policies are configured using a PfR map. This task contains prefix list configuration with different criteria in the set clauses.

Note Policies applied in a PfR map do not override global policy configurations.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr-map map-name** *sequence-number*
4. **match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name* [**inside**]
5. **set delay** {**relative** *percentage* | **threshold** *maximum*}
6. **set loss** {**relative** *average* | **threshold** *maximum*}
7. **set unreachable** {**relative** *average* | **threshold** *maximum*}
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.
Step 3	**pfr-map map-name** *sequence-number* **Example:** `Router(config)# pfr-map INSIDE_CONFIGURE 10`	Enters PfR map configuration mode to create or configure a PfR map. • PfR map operation is similar to that of route maps. • Only a single match clause can be configured for each PfR map sequence. • Permit and deny sequences should be applied to lowest pfr-map sequence for best performance. • The example creates an PfR map named INSIDE_CONFIGURE.
Step 4	**match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name* [**inside**] **Example:** `Router(config-pfr-map)# match ip address prefix-list INSIDE_PREFIXES inside`	References an extended IP access list or IP prefix list as match criteria in a PfR map. • Use the**inside** keyword to specify inside prefixes to support PfR BGP inbound optimization that supports best entrance selection for traffic that originates from prefixes outside an autonomous system destined for prefixes inside the autonomous system. • The example creates a match clause entry using the prefix list INSIDE_PREFIXES that specifies inside prefixes.
Step 5	**set delay** {**relative** *percentage*	**threshold** *maximum*}	Creates a set clause entry to configure the delay threshold. • The delay threshold can be configured as a relative percentage or as an absolute value for match criteria.

	Command or Action	Purpose
	Example: `Router(config-pfr-map)# set delay threshold 2000`	• The **relative** keyword is used to configure a relative delay percentage. The relative delay percentage is based on a comparison of short-term and long-term measurements. • The **threshold** keyword is used to configure the absolute maximum delay period in milliseconds. • The example creates a set clause that sets the absolute maximum delay threshold to 2000 milliseconds for traffic that is matched in the same PfR map sequence.
Step 6	**set loss** {**relative** *average* | **threshold** *maximum*} **Example:** `Router(config-pfr-map)# set loss relative 20`	Creates a set clause entry to configure the relative or maximum packet loss limit that the master controller will permit for an exit link. • This command is used to configure a PfR map to configure the relative percentage or maximum number of packets that PfR will permit to be lost during transmission on an exit link. If packet loss is greater than the user-defined or the default value, the master controller determines that the exit link is out-of-policy. • The **relative** keyword is used to configure the relative packet loss percentage. The relative packet loss percentage is based on a comparison of short-term and long-term packet loss. • The**threshold**keyword is used to configure the absolute maximum packet loss. The maximum value is based on the actual number of packets per million that have been lost. • The example creates a set clause that configures the relative percentage of acceptable packet loss to less than 20 percent for traffic that is matched in the same PfR map sequence.
Step 7	**set unreachable** {**relative** *average* | **threshold** *maximum*} **Example:** `Router(config-pfr-map)# set unreachable relative 10`	Creates a set clause entry to configure the maximum number of unreachable hosts. • This command is used to specify the relative percentage or the absolute maximum number of unreachable hosts, based on flows per million (fpm), that PfR will permit for a traffic class entry. If the absolute number or relative percentage of unreachable hosts is greater than the user-defined or the default value, PfR determines that the traffic class entry is OOP and searches for an alternate exit link. • The **relative** keyword is used to configure the relative percentage of unreachable hosts. The relative unreachable host percentage is based on a comparison of short-term and long-term measurements. • The**threshold**keyword is used to configure the absolute maximum number of unreachable hosts based on fpm. • The example creates a set clause entry that configures the master controller to search for a new exit link for a traffic class entry when the relative percentage of unreachable hosts is equal to or greater than 10 percent for traffic learned based on highest delay.

	Command or Action	Purpose
Step 8	**end** **Example:** `Router(config-pfr-map)# end`	Exits PfR map configuration mode and returns to privileged EXEC mode.

Configuration Examples for BGP Inbound Optimization Using Performance Routing

Example Configuring PfR to Automatically Learn Traffic Classes Using Inside Prefixes

The following example shows how to configure PfR to automatically learn prefixes inside the network:

```
Router> enable
Router#
configure terminal
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# inside bgp
Router(config-pfr-mc-learn)# monitor-period 10
Router(config-pfr-mc-learn)# periodic-interval 20

Router(config-pfr-mc-learn)# prefixes 30
Router(config-pfr-mc-learn)# end
```

Example Manually Selecting Inside Prefixes for PfR Monitoring

The following example shows how to manually configure PfR to learn prefixes inside the network using a PfR map:

```
Router> enable
Router# configure terminal
Router(config)# ip prefix-list INSIDE_PREFIXES seq 20 permit 192.168.1.0/24
Router(config)# pfr-map INSIDE_MAP 10
Router(config-pfr-map)# match ip address prefix-list INSIDE_PREFIXES inside
Router(config-pfr-map)# end
```

Example Modifying the PfR Link Utilization for Inbound Traffic

The following example shows how to modify the PfR entrance link utilization threshold. In this example, the entrance utilization is set to 65 percent. If the utilization for this exit link exceeds 65 percent, PfR selects another entrance link for traffic classes that were using this entrance link.

```
Router(config)# pfr master
Router(config-pfr-mc)# border 10.1.2.1
Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/0 external
Router(config-pfr-mc-br-if)# maximum receive utilization percentage 65
Router(config-pfr-mc-br-if)# end
```

Example Modifying the PfR Entrance Link Utilization Range

The following example shows how to modify the PfR entrance utilization range. In this example, the entrance utilization range for all entrance links is set to 15 percent.PfR uses the maximum utilization range to determine if entrance links are in-policy. PfR will equalize inbound traffic across all entrance links by moving prefixes from overutilized or out-of-policy exits to in-policy exits.

```
Router(config)# pfr master
Router(config-pfr-mc)# max range receive percent 15
Router(config-pfr-mc)# end
```

Example Configuring and Applying a PfR Policy to Learned Inside Prefixes

The following example shows how to apply a PfR policy to learned inside prefixes:

```
enable
configure terminal
pfr-map INSIDE_LEARN 10
 match pfr learn inside
 set delay threshold 2000
 set loss relative 20
 set unreachable relative 90
 end
```

Example Configuring and Applying a PfR Policy to Configured Inside Prefixes

The following example shows how to create a PfR map named INSIDE_CONFIGURE and apply a PfR policy to manually configured inside prefixes:

```
enable
configure terminal
 pfr-map INSIDE_CONFIGURE 10
 match ip address prefix-list INSIDE_PREFIXES inside
 set delay threshold 2000
 set loss relative 20
 set unreachable relative 80
 end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco PfR commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples	Cisco IOS Performance Routing Command Reference
Basic PfR configuration	"Configuring Basic Performance Routing" module
Concepts required to understand the Performance Routing operational phases	"Understanding Performance Routing" module
Advanced PfR configuration	"Configuring Advanced Performance Routing" module
IP SLAs overview	*IP SLAs Configuration Guide*
PfR home page with links to PfR-related content on our DocWiki collaborative environment	PfR:Home

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 BGP Inbound Optimization Using Performance Routing

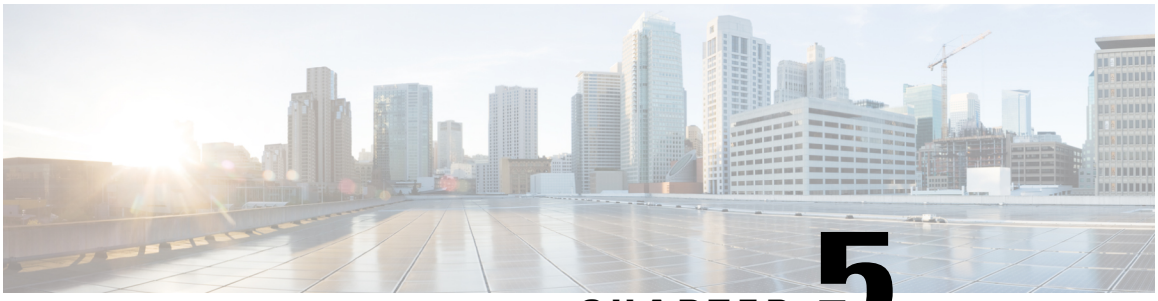
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train 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 5: Feature Information for BGP Inbound Optimization Using Performance Routing

Feature Name	Releases	Feature Information
OER BGP Inbound Optimization	12.4(9)T 12.2(33)SRB	PfR BGP inbound optimization supports best entrance selection for traffic that originates from prefixes outside an autonomous system destined for prefixes inside the autonomous system. External BGP (eBGP) advertisements from an autonomous system to an Internet service provider (ISP) can influence the entrance path for traffic entering the network. PfR uses eBGP advertisements to manipulate the best entrance selection. The following commands were introduced or modified by this feature: **clear pfr master prefix**, **downgrade bgp (PfR)**, **inside bgp (PfR)**, **match ip address (PfR)**, **match pfr learn**, **max range receive (PfR)**, **maximum utilization receive (PfR)**, **show pfr master prefix**.
expire after command[5]	12.3(14)T 12.2(33)SRB	The**expire after (PfR)**command is used to set an expiration period for learned prefixes. By default, the master controller removes inactive prefixes from the central policy database as memory is needed. This command allows you to refine this behavior by setting a time or session based limit. The time based limit is configured in minutes. The session based limit is configured for the number of monitor periods (or sessions).

5 This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.



CHAPTER 5

Configuring Performance Routing Cost Policies

This module describes how to configure and apply Cisco IOS Performance Routing (PfR) cost policies. A PfR policy can be configured to optimize traffic based on the monetary cost of the exit links. The PfR Cost Based Optimization feature provides financial benefits by directing traffic to lower cost links, while at the same time honoring other configured policies such as delay, loss, and utilization. Cost Based Optimization can be applied to links that are billed using a fixed or tiered billing method. Load balancing based on cost can also be achieved.

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 Table at the end of this document.

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.

Prerequisites for Performance Routing Cost Policies

Before implementing PfR cost policies, you need to understand an overview of how PfR works and how to set up PfR network components. See the “Understanding Performance Routing,” “Configuring Basic Performance Routing,” and “Configuring Advanced Performance Routing,” modules for more details.

Information About Performance Routing Cost Policies

To configure and apply PfR policies, you should understand the following concepts:

Overview of PfR Link Policies

PfR link policies are a set of rules that are applied against PfR-managed external links (an external link is an interface on a border router on the network edge). Link policies define the desired performance characteristics of the links. Instead of defining the performance of an individual traffic class entry that uses the link (as in traffic class performance policies), link policies are concerned with the performance of the link as a whole. Link policies are applied both to exit (egress) links and entrance (ingress) links. The following link policy types describe the different performance characteristics that can be managed using link policies:

Traffic Load (Utilization) Policy

A traffic load (also referred to as utilization) policy consists of an upper threshold on the amount of traffic that a specific link can carry. Cisco IOS PfR supports per traffic class load distribution. Every 20 seconds, by default, the border router reports the link utilization to the master controller, after an external interface is configured for a border router. Both exit link traffic and entrance link traffic load thresholds can be configured as a PfR policy. If the exit or entrance link utilization is above the configured threshold, or the default threshold of 75-percent, the exit or entrance link is in an out-of-policy (OOP) state and PfR starts the monitoring process to find an alternative link for the traffic class. The link utilization threshold can be manually configured either as an absolute value in kilobytes per second (kbps) or as a percentage. A load utilization policy for an individual interface is configured on the master controller under the border router configuration.

Tip When configuring load distribution, we recommend that you set the interface load calculation on external interfaces to 30-second intervals with the **load-interval** interface configuration command. The default calculation interval is 300 seconds. The load calculation is configured under interface configuration mode on the border router. This configuration is not required, but it is recommended to allow Cisco IOS PfR to respond as quickly as possible to load distribution issues.

A traffic load policy describes an upper limit for the traffic to be carried on a single link. For more details about configuring a traffic load policy, see the Configuring an Exit Link Load Balancing PfR Policy: Example configuration example in the "Configuring Advanced Performance Routing" module.

Range Policy

A range policy is defined to maintain all links within a certain utilization range, relative to each other in order to ensure that the traffic load is distributed. For example, if a network has multiple exit links, and there is no financial reason to choose one link over another, the optimal choice is to provide an even load distribution across all links. The load-sharing provided by traditional routing protocols is not always evenly distributed, because the load-sharing is flow-based rather than performance- or policy-based. Cisco PfR range functionality allows you to configure PfR to maintain the traffic utilization on a set of links within a certain percentage range of each other. If the difference between the links becomes too great, PfR will attempt to bring the link back to an in-policy state by distributing traffic classes among the available links. The master controller sets the maximum range utilization to 20 percent for all PfR-managed links by default, but the utilization range can be configured using a maximum percentage value.

Both exit link and entrance link utilization ranges can be configured as a PfR policy.

Note When configuring a range policy remember that 80 percent utilization of a serial link is very different from 80 percent utilization of a GigabitEthernet link.

A range policy describes a method of load-balancing the traffic over multiple links. For more details about configuring a range policy, see the Configuring an Exit Link Load Balancing PfR Policy: Example configuration example in the Configuring Advanced Performance Routing module.

Cost Policy

PfR support for cost-based optimization was introduced in Cisco IOS Release 12.3(14)T, 12.2(33)SRB, and later releases. Cost-based optimization allows you to configure policies based on the monetary cost (ISP service level agreements [SLAs]) of each exit link in your network. To implement PfR cost-based optimization the PfR master controller is configured to send traffic over exit links that provide the most cost-effective bandwidth utilization, while still maintaining the desired performance characteristics. A cost policy describes a method of load-balancing the traffic over multiple links.

In response to changing business practices, in Cisco IOS Release 12.4(15)T9 and later releases, the calculation of the Momentary Target Link Utilization (MTLU) algorithm is modified to allow for more efficient bandwidth utilization while minimizing the link cost.

To understand how cost-based optimization works, review the following sections:

Cost Policy Billing Models

PfR cost-based optimization supports two methods of billing: fixed-rate billing or tier-based billing.

Fixed-rate billing is used when the ISP bills one flat rate for a link regardless of bandwidth usage. If fixed-rate billing only is configured on the exit links, all exits are considered equal with regard to cost-optimization and other policy parameters (such as delay, loss, and utilization) are used to determine if the prefix or exit link is in-policy.

Tier-based billing is used when the ISP bills at a tiered rate based on the percentage of exit link utilization. Each cost tier is configured separately with an associated monetary cost and a percentage of bandwidth utilization that activates the tier is defined. The lowest cost tier for an exit using tier-based billing is charged each month regardless of the bandwidth actually utilized. An allowance is made for bursting in the algorithm

used to determine the tier-based billing. In this situation, bursting is defined as short periods of high bandwidth usage that would be expensive under fixed-rate billing.

A fixed-rate billing is a set monthly fee regardless of utilization. Tier-based billing also incurs at least the lowest-tier cost per month, but the final monthly tier-based billing charge is determined by the cost assigned to the tier that matches the sustained monthly utilization.

Link Utilization Rollup Calculations

The first step in determining the billing fee for each exit link per month is to calculate the link utilization rollup values. Link utilization rollup values are the averages of the link utilization readings taken at regular intervals (sampling period) from the ingress and egress interfaces at the border routers for a given rollup period. For example, if a sampling period was set to 60 minutes, and the rollup was set at 1440 minutes (24 hours), we would have 24 ingress and 24 egress link utilization samples used for calculating the link utilization rollup. An average is taken for each set of ingress and egress samples from that rollup period to get a link utilization rollup value for the ingress and egress links.

Monthly Sustained Utilization Calculation

After the link utilization rollup calculation is performed, the monthly sustained utilization is calculated, The specific details of tier-based billing models vary by ISP. However, most ISPs use some variation of the following algorithm to calculate what an enterprise should pay in a tiered billing plan:

- Gather periodic measurements of egress and ingress traffic carried on the enterprise connection to the ISP network and aggregate the measurements to generate a rollup value for a rollup period.
- Calculate one or more rollup values per billing period.
- Rank the rollup values for the billing period into a stack from the largest value to the smallest.
- Discard the top default 5 percent (an absolute or percentage value can be configured, but 5 percent is the default) of the rollup values from the stack to accommodate bursting. In this situation, bursting is defined as any bandwidth above the sustained monthly utilization. The remaining rollup values are known as the 95th percentile high if the default 5% is discarded.
- After the rollups with the highest utilization values (the top 5 percent in this case) are removed, apply the highest remaining rollup value in the stack, referred to as the sustained Monthly Target Link Utilization (MTLU), to a tiered structure to determine a tier associated with the rollup value.
- Charge the customer based on a set cost associated with the identified tier.

Note A billing policy must be configured and applied to links in order for the master controller to perform cost-based optimization.

The monthly sustained utilization rollup calculations can be configured to use one of the following three techniques:

- Combined
- Separate
- Summed

In the following explanations of the sustained utilization calculation techniques, the discard value is configured as an absolute value of 10. The default discard value is 5 percent.

Using the combined technique, the monthly sustained utilization calculation is based on a combination of the egress and ingress rollup samples on a single sorted stack, the highest 10 rollup values are discarded, and the next highest rollup value is the MTLU.

Using the separate technique, the egress and ingress rollup samples for a link are sorted into separate stacks and the highest 10 rollup values for each stack are discarded. The highest remaining rollup value of the two stacks is selected as the MTLU.

Using the summed technique the egress and ingress rollup samples are added together. The summed values of each rollup sample are placed into one stack, the top 10 rollup values are discarded, leaving the next highest rollup value as the MTLU.

The following table displays an example of how the sustained monthly utilization is calculated using the separate technique. In the table below the rollup values for a 30-day period are displayed in order from the highest bandwidth to the lowest bandwidth for both the egress and ingress rollup values. The top 10 values (shown in italic) are discarded because the master controller has been configured to discard this absolute number of rollups. The next highest rollup value remaining in the two stacks, 62 (shown in bold), is the sustained monthly utilization. The sustained monthly utilization is used to determine the tier at which the customer is billed for bandwidth usage on that link for that billing period.

Table 6: Sustained Monthly Utilization Example Calculation

Egress Rollups	Ingress Rollups	Rollups are Sorted from Highest Bandwidth to Lowest Bandwidth in Billing Period
89	*92*	Discard the top 10 egress and ingress as configured as an absolute value (see numbers in italics).
80	*84*	
71	*82*	
70	*80*	
65	*78*	
65	*75*	
51	*73*	
50	*84*	
49	*82*	
49	*80*	

Egress Rollups	Ingress Rollups	Rollups are Sorted from Highest Bandwidth to Lowest Bandwidth in Billing Period
45	**62**	After the discarded values. the next highest value is 62 and this becomes the **Sustained Monthly Utilization**
42	60	
39	55	
35	53	
34	52	
30	45	
30	43	
30	35	
29	33	
25	31	
20	25	
19	23	
12	21	
10	15	
10	11	
9	10	
8	10	
4	5	
1	1	
0	**0**	

How to Configure Performance Routing Cost Policies

Configuring a Basic PfR Cost-Based Policy

Perform this task to configure basic PfR cost-based optimization. Cost-based optimization is configured on a master controller using the **cost-minimization** command in PfR border exit interface configuration mode (under the external interface configuration). Cost-based optimization supports tiered and fixed billing methods.

In this task, the configuration is performed on the master controller router and it assumes that the border routers are configured. Tier-based billing is configured with three cost tiers and a nickname for the service provider is set to ISP1. The monthly sustained utilization calculation technique is configured to use the sum technique and the last day of the billing cycle is on the 30th day of the month with an offset of 3 hours to allow for a difference in time zones.

The **cost-minimization** command contains many variations of keywords and arguments. Only one of the required keywords and its associated syntax can be configured on one CLI line, but multiple instances of this command can be entered. Only the **fixed** and **tier** keywords are mutually exclusive within the configuration for each border router link. For details about the full syntax, see the *Cisco IOS Performance Routing Command Reference*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **border** *ip-address* [**key-chain** *key-chain-name*]
5. **interface** *type number* **external**
6. **cost-minimization nickname** *name*
7. **cost-minimization calc** {**combined** | **separate** | **sum**}
8. **cost-minimization sampling period** *minutes* [**rollup** *minutes*]
9. **cost-minimization end day-of-month** *day* [**offset** [**-**] *hh:mm*]
10. **cost-minimization** {**fixed fee** *cost*| **tier** *percentage* **fee** *fee*}
11. Repeat Step 9 to configure additional tiers for a tier-based billing cycle.
12. **exit**
13. **interface** *type number* **internal**
14. **exit**
15. Repeat Step 14 to return to PfR master controller configuration mode.
16. Repeat from Step 4 to Step 15 to configure additional cost-based optimization policies for other links, if required.
17. **mode route control**
18. **resolve cost priority** *value*
19. **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.
Step 3	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure global prefix and exit link policies.
Step 4	**border** *ip-address* [**key-chain** *key-chain-name*] **Example:** `Router(config-pfr-mc)# border 10.100.1.1 key-chain PFR_cost`	Enters PfR-managed border router configuration mode to establish communication with a border router. • An IP address is configured to identify the border router. • The value for the *key-chain-name* argument must match the key-chain name configured at the border router identified by the *ip-address* argument. **Note** The **key-chain** keyword and *key-chain-name* argument must be entered when a border router is initially configured. However, this keyword is optional when reconfiguring or adding configuration for this border router.
Step 5	**interface** *type number* **external** **Example:** `Router(config-pfr-mc-br)# interface ethernet 0/0 external`	Enters PfR border exit interface configuration mode to configure a border router interface as an external interface. • At least one external interface must be configured on each border router.
Step 6	**cost-minimization nickname** *name* **Example:** `Router(config-pfr-mc-br-if)# cost-minimization nickname ISP1`	Configures a nickname for a border router interface within a cost-based optimization policy on a master controller. • Use the **nickname** keyword to apply a label that identifies the service provider. • In this example, the label of ISP1 is configured for the service provider.
Step 7	**cost-minimization calc** {**combined** | **separate** | **sum**}	Configures how the cost-minimization fee is calculated.

	Command or Action	Purpose
	Example: `Router(config-pfr-mc-br-if)# cost-minimization calc sum`	• Use the **combined** keyword to configure the master controller to combine ingress and egress samples. • Use the **separate** keyword to configure the master controller to analyze ingress and egress samples separately. • Use the **sum** keyword to configure the master controller to first add ingress and egress samples and then combine the samples. • In this example, cost-minimization fee is calculated using the sum technique.
Step 8	**cost-minimization sampling period** *minutes* [**rollup** *minutes*] **Example:** `Router(config-pfr-mc-br-if)# cost-minimization sampling period 10 rollup 60`	Specifies the sampling period in minutes. • The value that can be entered for the sampling period *minutes* argument is a number from 1 to 1440. • Use the optional **rollup**keyword to specify that samples are rolled up at the interval specified for the *minutes* argument. The value that can be entered for the rollup *minutes* argument is a number from 1 to 1440. The minimum number that can be entered must be equal to or greater than the number that is entered for the sampling period. • In this example, the time interval between sampling is set to 10 minutes. These samples are configured to be rolled up every 60 minutes.
Step 9	**cost-minimization end day-of-month** *day* [**offset** [**-**] *hh:mm*] **Example:** `Router(config-pfr-mc-br-if)# cost-minimization end day-of-month 30 offset 5:00`	Configures the parameters used to configure the last day of the billing cycle. • Use the optional **offset**keyword to adjust the end of the cycle to compensate for a service provider in a different zone from UTC. The optional "**-**" keyword is used to allow for negative hours and minutes to be specified when the time zone is ahead of UTC. • In this example, the last day of the billing cycle is on the 30th day of the month with an offset of 5 hours added to UTC.
Step 10	**cost-minimization** {**fixed fee** *cost*| **tier** *percentage* **fee** *fee*} **Example:** `Router(config-pfr-mc-br-if)# cost-minimization tier 100 fee 1000`	Configures a nonusage-based fixed cost billing cycle or a tier of a tier-based billing cycle. • The **fixed fee** keywords and *cost* argument are used to specify a fixed (nonusage-based) cost associated with an exit link. • The *percentage* argument is used to specify the percentage of capacity utilization for a cost tier. • The **tier fee** keywords and *fee* argument are used to specify the fee associated with this tier. • In this example, the tier-based fee for 100 percent utilization is set to 1000.

	Command or Action	Purpose
		Note The first tier specified must be the 100 percent capacity utilization. Any following tier configurations must be for lesser percentages and lower fees.
Step 11	Repeat Step 9 to configure additional tiers for a tier-based billing cycle.	--
Step 12	**exit** **Example:** `Router(config-pfr-mc-br-if)# exit`	Exits PfR border exit interface configuration mode and returns to PfR-managed border router configuration mode.
Step 13	**interface** *type number* **internal** **Example:** `Router(config-pfr-mc-br)# interface Ethernet 1/0 internal`	Configures a border router interface as a PfR controlled internal interface. • Internal interfaces are used for passive monitoring only. Internal interfaces do not forward traffic. • At least one internal interface must be configured on each border router. **Note** Support to configure a VLAN interface as an internal interface was introduced in Cisco IOS Release 12.3(14)T, and 12.2(33)SRB.
Step 14	**exit** **Example:** `Router(config-pfr-mc-br-if)# exit`	Exits PfR border exit interface configuration mode and returns to PfR-managed border router configuration mode.
Step 15	Repeat Step 14 to return to PfR master controller configuration mode.	--
Step 16	Repeat from Step 4 to Step 15 to configure additional cost-based optimization policies for other links, if required.	--
Step 17	**mode route control** **Example:** `Router(config-pfr-mc)# mode route control`	Configures route control for matched traffic. • In control mode, the master controller analyzes monitored prefixes and implements changes based on policy parameters.
Step 18	**resolve cost priority** *value* **Example:** `Router(config-pfr-mc)# resolve cost priority 1`	Sets policy priority for cost policies. • The resolve policy configures cost policies to have the highest priority. • In this task, only one type of PfR policy is given priority. Be aware that other PfR policies are usually configured and priorities must be carefully reviewed.

	Command or Action	Purpose
Step 19	**end** **Example:** `Router(config-pfr-mc)# end`	Exits PfR master controller configuration mode and returns to privileged EXEC mode.

Example:

The following example is just a sample configuration as shown in the task but with the added tiers to complete the tier-based fee configuration. For a more complete example configuration of a basic PfR cost policy that includes both fixed-rate and tier-based billing, see the "Example: Configuring a Basic PfR Cost-Based Policy" section.

```
pfr master
 border 10.100.1.1 key-chain PFR_cost
  interface Ethernet 0/0 external
   cost-minimization nickname ISP1
   cost-minimization calc sum
   cost-minimization sampling period 10 rollup 60
   cost-minimization end day-of-month 30 offset 5:00
   cost-minimization tier 100 fee 1000
   cost-minimization tier 70 fee 700
   cost-minimization tier 50 fee 500
   exit
  interface Ethernet 1/0 internal
  exit
 mode route control
 resolve cost priority 1
 end
```

Using a PfR Cost Policy to Minimize Billing and Load Balance Traffic

While basic PfR cost-based optimization can be useful, many organizations have multiple border router exit links and possibly several different service providers charging different billing rates that increase according to the bandwidth utilized. In this situation, some form of traffic load balancing across the links may be required in addition to the cost minimization policy.

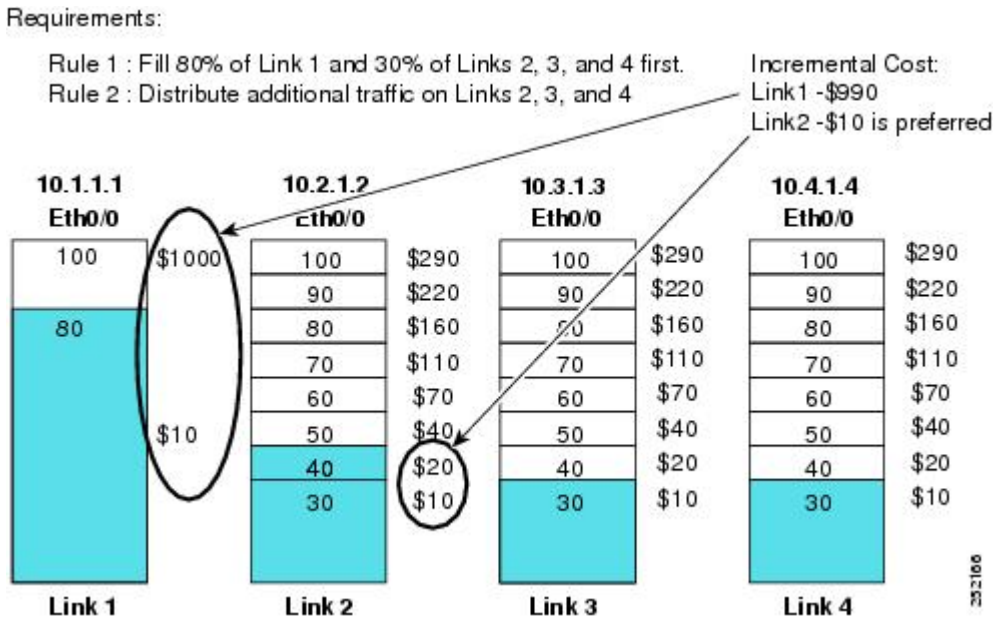
Perform this task on the master controller to configure a Performance Routing cost policy to minimize the monthly billing charge for multiple border router exit links while load balancing traffic across the links. In this scenario, the network has both fixed-rate and tier-based billing, and assuming that the customer is paying a monthly fee for the fixed-rate billing and the pre-paid (lowest cost) tier of tier-based billing, PfR can perform traffic load balancing while optimizing for cost.

The figure below shows an example of how different billing rates can be defined for each link using bandwidth and cost parameters that are defined through service level agreements (SLAs) that are identified as rules in the diagram. The main goal of this task is to minimize the billing charge per exit link and to load balance traffic across the exit links. Although Link 1 may be billed at a fixed-rate and Links 2 through 4 are subject to tier-based billing, all the links are set up as PfR tiers. To accomplish the cost minimization the first rule is to utilize 80 percent of Link 1 and 30 percent of Links 2, 3 and 4, as shown in the figure below. The second rule is to distribute additional traffic across Links 2, 3 and 4 to balance the traffic load. To achieve the traffic load balancing while minimizing cost, the solution is to configure a PfR cost policy using multiple tiers

representing bandwidth percentages that are assigned artificial costs to ensure that the PfR traffic is optimized for cost and load balanced across all the exits. To illustrate the configured tiers, see the figure below.

The steps in this task create a cost policy in which PfR is configured to direct traffic through any of the lowest cost exits first; Link 1 at 10.1.1.1 and the pre-paid tier of the other three exits. When the pre-paid tier bandwidth at each link is fully utilized, the software determines the next lowest incremental cost between the tiers at all the links. The incremental cost of utilizing the next tier at Link 1 is $990. The incremental cost of utilizing the next tier at Link 2 is only $10. PfR forwards traffic to the next lowest cost tier which is the blue bar representing 40 percent of the bandwidth at Link 2, as shown in the figure below. The process continues to use cost to balance the load across Links 2, 3, and 4. This task illustrates how the monthly billing rate per exit link is minimized by utilizing the pre-paid bandwidth at Links 1 though 4 first, and then the traffic is effectively load balanced across Links 2, 3 and 4 by determining the lowest incremental cost between tiers.

Figure 11: Diagram Showing PfR Cost-Minimization Solution to Minimize Billing and Load Balance Traffic



In the following task steps, the exit link 10.1.1.1 is configured as a tier-based link although it is actually charged at a fixed rate. If a fixed rate link is configured as a tier for load balancing, the monthly cost calculation will not reflect the true cost for that link. Using this solution, the artificial costs assigned to the multiple tiers may affect the accuracy of all the monthly cost calculations.

Only some of the configuration steps for this task scenario are shown in the summary and detailed steps, the full configuration for the master controller is displayed in the Examples section shown after the detailed steps table.

Note Disable the range and utilization policy priorities because they may conflict with this application of the cost-minimization feature.

Note Do not configure the **periodic**(PfR) or the **set periodic**(PfR) command with a time interval to avoid system churn as the system tries to select the best exit link at specified intervals. This command is disabled by default.

The **cost-minimization** (PfR) command contains many variations of keywords and arguments. Only one of the required keywords and its associated syntax can be configured on one CLI line, but multiple instances of this command can be entered. Only the **fixed** and **tier** keywords are mutually exclusive within the configuration for each border router link. For details about the full syntax, see the *Cisco IOS Performance Routing Command Reference*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **border** *ip-address* [**key-chain** *key-chain-name*]
5. **interface** *type number* **external**
6. **cost-minimization nickname** *name*
7. **cost-minimization summer-time** *start end* [*offset*]
8. **cost-minimization** {**fixed fee** *cost*| **tier** *percentage* **fee** *fee*}
9. Repeat Step 8 to configure additional tiers for a tier-based billing cycle.
10. **cost-minimization discard** [**daily**] {**absolute** *number*| **percent** *percentage*}
11. **exit**
12. **interface** *type number* **internal**
13. **exit**
14. Repeat Step 13 to return to PfR master controller configuration mode.
15. Repeat from Step 4 to Step 14 to configure additional cost-based optimization policies for other links, if required.
16. **mode route control**
17. **policy-rules** *map-name*
18. **exit**
19. **pfr-map** *map-name sequence-number*
20. **match pfr learn** {**delay**| **inside**| **throughput**}
21. **set resolve cost priority** *value*
22. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure global prefix and exit link policies.
Step 4	**border** *ip-address* [**key-chain** *key-chain-name*] **Example:** `Router(config-pfr-mc)# border 10.1.1.1 key-chain pfr`	Enters PfR-managed border router configuration mode to establish communication with a border router. • An IP address is configured to identify the border router. • The value for the *key-chain-name* argument must match the key-chain name configured at the border router identified by the *ip-address* argument. **Note** The **key-chain** keyword and *key-chain-name* argument must be entered when a border router is initially configured. However, this keyword is optional when reconfiguring or adding configuration for this border router.
Step 5	**interface** *type number* **external** **Example:** `Router(config-pfr-mc-br)# interface ethernet 0/0 external`	Enters PfR border exit interface configuration mode to configure a border router interface as a PfR-managed external interface. • At least one external interface must be configured on each border router. • Configuring an interface as a PfR-managed external interface on a router enters PfR border exit interface configuration mode. In this mode, you can configure maximum link utilization or cost-based optimization for the interface.
Step 6	**cost-minimization nickname** *name* **Example:** `Router(config-pfr-mc-br-if)# cost-minimization nickname 80-percent`	Configures a nickname for a border router interface within a cost-based optimization policy on a master controller. • In this example, the nickname label for the 10.1.1.1 border router link is 80-percent.
Step 7	**cost-minimization summer-time** *start end* [*offset*]	Specifies the start and end dates and times for summer time (daylight savings).

	Command or Action	Purpose
	Example: `Router(config-pfr-mc-br-if)# cost-minimization summer-time 2 Sunday March 02:00 1 Sunday November 02:00 60`	• The *start* and *end* arguments are used to specify the week number, day, month and time in hours and minutes (24 hour clock) that summertime starts and ends. • The *offset* argument allows for an offset in minutes from 1 to 120 to allow for up to two additional hours to be added in the spring and subtracted in the fall. • In this example, summer time is configured to start the second week in March on a Sunday at 2 in the morning plus one hour, and end on Sunday in the first week in November at 2 in the morning minus one hour. **Note** The **summer-time** keyword configuration is only required once for each master controller.
Step 8	**cost-minimization** {**fixed fee** *cost*| **tier** *percentage* **fee** *fee*} **Example:** `Router(config-pfr-mc-br-if)# cost-minimization tier 100 fee 1000`	Configures a nonusage-based fixed cost billing cycle or a tier of a tier-based billing cycle. • The **fixed fee** keywords and *cost* argument are used to specify a fixed (nonusage-based) cost associated with an exit link. • The *percentage* argument is used to specify the percentage of capacity utilization for a cost tier. • The **tier fee** keywords and *fee* argument are used to specify the fee associated with this tier. • In this example, the tier-based fee for 100 percent utilization is set to 1000. **Note** The first tier specified must be the 100 percent capacity utilization. Any following tier configurations must be for lesser percentages and lower fees. When setting up tiers for load balancing, the tiers must be incrementally larger from one tier to the next tier on the same link in order for load balancing to work.
Step 9	Repeat Step 8 to configure additional tiers for a tier-based billing cycle.	--
Step 10	**cost-minimization discard** [**daily**] {**absolute** *number*| **percent** *percentage*} **Example:** `Router(config-pfr-mc-br-if)# cost-minimization discard percent 5`	Configures the number of samples that are removed for bursty link utilization when calculating the sustained monthly utilization value. • The utilization samples are ordered from the highest to the lowest and the number or percentage configured using this command removes the highest number or percentage from the list. • If the optional **daily** keyword is entered, samples are analyzed and discarded on a daily basis. If the **daily** keyword is not entered, by default the samples are analyzed and discarded on a monthly basis. At the end of the billing cycle, monthly sustained usage is calculated by averaging daily sustained utilization.

	Command or Action	Purpose
		• Use the **absolute** keyword to configure a set number of samples to be removed. • Use the **percentage** keyword to configure a percentage number of samples to be removed. • If a sampling rollup is configured, the discard values also applies to the rollup. • In this example, the highest 5 percent of samples are removed when calculating the sustained monthly utilization value.
Step 11	**exit** **Example:** `Router(config-pfr-mc-br-if)# exit`	Exits PfR border exit interface configuration mode and returns to PfR-managed border router configuration mode.
Step 12	**interface** *type number* **internal** **Example:** `Router(config-pfr-mc-br)# interface Ethernet 1/0 internal`	Configures a border router interface as a PfR controlled internal interface. • Internal interfaces are used for passive monitoring only. Internal interfaces do not forward traffic. • At least one internal interface must be configured on each border router.
Step 13	**exit** **Example:** `Router(config-pfr-mc-br-if)# exit`	Exits PfR border exit interface configuration mode and returns to PfR-managed border router configuration mode.
Step 14	Repeat Step 13 to return to PfR master controller configuration mode.	--
Step 15	Repeat from Step 4 to Step 14 to configure additional cost-based optimization policies for other links, if required.	--
Step 16	**mode route control** **Example:** `Router(config-pfr-mc)# mode route control`	Configures route control for matched traffic. • In control mode, the master controller analyzes monitored prefixes and implements changes based on policy parameters.
Step 17	**policy-rules** *map-name* **Example:** `Router(config-pfr-mc)# policy-rules cost_balance`	Applies a configuration from a PfR map to a master controller configuration. • In this example, configuration from a PfR map named cost_balance is applied.

	Command or Action	Purpose
Step 18	**exit** **Example:** `Router(config-pfr-mc)# exit`	Exits PfR master controller configuration mode and returns to global configuration mode.
Step 19	**pfr-map** *map-name sequence-number* **Example:** `Router(config)# pfr-map cost_balance 10`	Enters PfR map configuration mode to configure a PfR map.
Step 20	**match pfr learn** {**delay**| **inside**| **throughput**} **Example:** `Router(config-pfr-map)# match pfr learn throughput`	Creates a match clause entry in a PfR map to match PfR learned prefixes. • Only a single match clause can be configured for each PfR map sequence. • In this example, a match clause entry is created to match traffic classes learned using the highest outbound throughput.
Step 21	**set resolve cost priority** *value* **Example:** `Router(config-pfr-map)# set resolve cost priority 1`	Creates a set clause entry in an PfR map to set policy priority for overlapping policies. • In this example, the resolve policy configures cost policies to have the highest priority. • In this task, only one type of PfR policy is given priority. Be aware that other PfR policies are usually configured and priorities must be carefully reviewed.
Step 22	**end** **Example:** `Router(config-pfr-mc)# end`	Exits PfR master controller configuration mode and returns to privileged EXEC mode.

Example:

The following configuration example is a complete configuration for all the links controlled by the master controller in the figure above the task steps. Note the set resolve cost priority 1 command in the PfR map titled cost_balance that is used to ensure that cost is the first priority for this task. In contrast, the resolve range and resolve utilization commands are disabled to avoid optimization conflicts. For output from associated **show** commands see the "Verifying and Debugging PfR Cost-Minimization Policies" section.

```
pfr master
 logging
 border 10.1.1.1 key-chain pfr
  interface Ethernet1/0 internal
  interface Ethernet0/0 external
   cost-minimization nickname 80-percent
```

```
  cost-minimization summer-time 2 Sunday March 02:00 1 Sunday November 02:00 60
  cost-minimization tier 100 fee 1000
  cost-minimization tier 80 fee 10
  cost-minimization discard percent 5
  exit
 exit
border 10.2.1.2 key-chain pfr
 interface Ethernet1/0 internal
 interface Ethernet0/0 external
  cost-minimization nickname 30-meg
  cost-minimization tier 100 fee 290
  cost-minimization tier 90 fee 220
  cost-minimization tier 80 fee 160
  cost-minimization tier 70 fee 110
  cost-minimization tier 60 fee 70
  cost-minimization tier 50 fee 40
  cost-minimization tier 40 fee 20
  cost-minimization tier 30 fee 10
  cost-minimization discard percent 5
  exit
 exit
border 10.3.1.3 key-chain pfr
 interface Ethernet1/0 internal
 interface Ethernet0/0 external
  cost-minimization nickname 30-meg-2
  cost-minimization tier 100 fee 290
  cost-minimization tier 90 fee 220
  cost-minimization tier 80 fee 160
  cost-minimization tier 70 fee 110
  cost-minimization tier 60 fee 70
  cost-minimization tier 50 fee 40
  cost-minimization tier 40 fee 20
  cost-minimization tier 30 fee 10
  cost-minimization discard percent 5
  exit
 exit
border 10.4.1.4 key-chain pfr
 interface Ethernet1/0 internal
 interface Ethernet0/0 external
  cost-minimization nickname 30-meg-3
  cost-minimization tier 100 fee 290
  cost-minimization tier 90 fee 220
  cost-minimization tier 80 fee 160
  cost-minimization tier 70 fee 110
  cost-minimization tier 60 fee 70
  cost-minimization tier 50 fee 40
  cost-minimization tier 40 fee 20
  cost-minimization tier 30 fee 10
  cost-minimization discard percent 5
  exit
 exit
 learn
  throughput
  periodic-interval 0
  monitor-period 1
  prefixes 2500
  aggregation-type prefix-length 32
  exit
 mode route control
 policy-rules cost_balance
 max-range-utilization percent 100
 exit
pfr-map cost_balance 10
 match pfr learn throughput
 set resolve cost priority 1
 no set resolve range
 no set resolve utilization
 set probe frequency 10
 end
```

Verifying and Debugging PfR Cost-Minimization Policies

Perform this task on a master controller to display information to verify any cost-minimization policies and to help debug any issues. After cost-minimization policies are configured and applied to traffic the **show** command steps allow you to verify that the policy configuration is working as expected. If not, the **debug** command steps can help troubleshoot any issues. The **show** and **debug** commands are all optional and can be entered in any order.

Before You Begin

A cost policy must be configured and applied to PfR traffic before performing any of these steps.

SUMMARY STEPS

1. **enable**
2. **show pfr master cost-minimization** {**border** *ip-address* [*interface*] | **nickname** *name*}
3. **show pfr master cost-minimization billing-history**
4. **debug pfr master cost-minimization** [**detail**]

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 2 **show pfr master cost-minimization** {**border** *ip-address* [*interface*] | **nickname** *name*}
Both the **border** and the **nickname** keywords of the **show pfr master cost-minimization** command display the same cost-minimization information. The keywords and arguments can be used to identify a specified border router by its nickname or by an IP address and, optionally, for a specific interface on the router. Only the syntax applicable to this step is shown. For the full syntax, see the *Cisco IOS Performance Routing Command Reference*.

In this example, the information is displayed about the 10.2.1.2 link from the figure above. Note the number of cost tiers configured for this link. The links at 10.3.1.3 and 10.4.1.4 have the same set of cost tiers to allow more precise load balancing. There is information about the rollup values and parameters set for the discard values shown as an absolute value of 5. For more details about the fields shown in this output, refer to the *Cisco IOS Performance Routing Command Reference*.

Example:

```
Router# show pfr master cost-minimization border 10.2.1.2 GigabitEthernet 3/2/0
pM - per Month, pD - per Day
 ------------------------------------------------------------------------------
  Nickname  : 30-meg           Border: 10.2.1.2         Interface: Gi3/2/0
  Calc type : Separate
  End Date  : 1
  Summer time: Enabled,  2 Sun Mar 02:00 1 Sun Nov 02:00 60
  Fee       : Tier Based
              Tier 1: 100, fee:   290
              Tier 2:  90, fee:   220
```

```
            Tier 3:  80, fee:   160
            Tier 4:  70, fee:   110
            Tier 5:  60, fee:    70
            Tier 6:  50, fee:    40
            Tier 7:  40, fee:    20
            Tier 8:  30, fee:    10
 Period    : Sampling 5, Rollup 5
 Discard   : Type Absolute, Value 5

 Rollup Information:
 Total(pM)       Discard(pM)     Remaining(pM)   Collected(pM)
 8928            5               1460            264

 Current Rollup Information:
   MomentaryTgtUtil:          382 Kbps    CumRxBytes:           747167
  StartingRollupTgt:          400 Kbps    CumTxBytes:          4808628
   CurrentRollupTgt:          400 Kbps    TimeRemain:         00:03:23

 Rollup Utilization (Kbps):
 Egress Utilization Rollups (Descending order)

 1   : 0           2   : 440         3   : 439         4   : 398
 5   : 383         6   : 378         7   : 375         8   : 372
 9   : 371         10  : 371         11  : 370         12  : 370
 13  : 368         14  : 365         15  : 255         16  : 231
 17  : 216         18  : 197         19  : 196         20  : 196
 21  : 195         22  : 194         23  : 191         24  : 190
 25  : 190         26  : 184         27  : 183         28  : 182
 29  : 178         30  : 177         31  : 176         32  : 175
```

Step 3 **show pfr master cost-minimization billing-history**

This command is used to display the billing information for the previous billing period. In this example, the monthly sustained utilization is 62 and the cost is $10,000 for the GigabitEthernet interface 3/0/0 link on border router 10.1.1.1.

Example:

```
Router# show pfr master cost-minimization billing-history

Billing History for the past three months

        ISP2 on 10.4.1.4          Gi4/0/0
  No cost min on 10.2.1.2         Gi3/2/0
        ISP1 on 10.1.1.1          Gi3/0/0
                Mon1                 Mon2                 Mon3
 Nickname     SustUtil       Cost   SustUtil       Cost   SustUtil       Cost
 ----------    ------------------    ------------------   ------------------
    ISP2             0       3000        ---NA---            ---NA---
    ISP1            62      10000        ---NA---            ---NA---

 ----------    ------------------    ------------------   ------------------
 Total Cost                13000                     0                    0
```

Step 4 **debug pfr master cost-minimization** [**detail**]

This command is used to display debugging information for cost-minimization policies. The following example displays detailed cost-minimization policy debug information.

Example:

```
Router# debug pfr master cost-minimization detail

OER Master cost-minimization Detail debugging is on
*May 14 00:38:48.839: OER MC COST: Momentary target utilization for exit 10.2.1.2 i/f
GigabitEthernet3/2/0 nickname ISP1 is 7500 kbps, time_left 52889 secs, cumulative 16 kb,
rollup period 84000 secs, rollup target 6000 kbps, bw_capacity 10000 kbps
*May 14 00:38:48.839: OER MC COST: Cost OOP check for border 10.2.1.2, current util: 0
```

```
target util: 7500 kbps
*May 14 00:39:00.199: OER MC COST: ISP1 calc separate rollup ended at 55 ingress Kbps
*May 14 00:39:00.199: OER MC COST: ISP1 calc separate rollup ended at 55 egress bytes
*May 14 00:39:00.199: OER MC COST: Target utilization for nickname ISP1 set to 6000,
rollups elapsed 4, rollups left 24
*May 14 00:39:00.271: OER MC COST: Momentary target utilization for exit 10.2.1.2 i/f
GigabitEthernet3/2/0 nickname ISP1 is 7500 kbps, time_left 52878 secs, cumulative 0 kb,
rollup period 84000 secs, rollup target 6000 kbps, bw_capacity 10000 kbps
*May 14 00:39:00.271: OER MC COST: Cost OOP check for border 10.2.1.2, current util: 0
target util: 7500 kbps
```

Configuration Examples for Performance Routing Cost Policies

Example Configuring a Basic PfR Cost-Based Policy

The following example shows how to configure cost-based optimization on a master controller. Cost optimization configuration is applied under the external interface configuration. In this example, a policy is configured for multiple exits with a tiered billing cycle for one exit interface on border router 10.2.1.2 and a fixed fee billing cycle for the other exit interface on border router 10.2.1.2 and both exit interfaces on border router 10.3.1.3.

In this scenario, PfR sends traffic first through the fixed-rate exits, serial interface 3/0 at border router 10.2.1.2 and serial interfaces 2/0 and 3/0 at border router 10.3.1.3, because the bandwidth cost is lower for these fixed fee exits than the tier-based exit. When the fixed-rate exits are all fully utilized, the traffic is sent through serial interface 2/0 on border router 10.2.1.2. If the monthly sustained utilization is 40 percent or lower, the billing fee for the month will be $4000. If the monthly sustained utilization is higher then the tier that matches the monthly sustained utilization is charged. In this example, no calculation configuration was entered and the default behavior is triggered; the calculation is performed separately for egress and ingress samples.

This configuration example assumes that the border routers are already configured.

```
pfr master
 no periodic
 resolve cost priority 1
 no resolve delay
 no resolve utilization
 border 10.2.1.2 key-chain key_cost1
  interface Serial12/0 external
   cost-minimization tier 100 fee 10000
   cost-minimization tier 75 fee 8000
   cost-minimization tier 40 fee 4000
   cost-minimization end day-of-month 31
  interface Serial13/0 external
   cost-minimization fixed fee 3000
 border 10.3.1.3 key-chain key_cost2
  interface Serial12/0 external
   cost-minimization fixed fee 3000
  interface Serial13/0 external
   cost-minimization fixed fee 3000
   end
```

Example Using a PfR Cost Policy to Minimize Billing and Load Balance Traffic

The following configuration example shows how to configure cost-minimization policies and balance PfR traffic loads across multiple links. This task is designed to minimize the cost of each link and to precisely control load balancing across multiple border router links. This task controls the load balancing between multiple links by forcing PfR to use the bandwidth of the lowest cost tier first and then use the next lowest cost tiers on all the links.

Keywords in the **show pfr master cost-minimization** command are used to view the utilization of a specific link with the monthly egress and ingress rollup values. After the monthly billing period ends another keyword option for the billing history shows the sustained monthly utilization and link cost.

Border Router 10.1.1.1

```
key chain key1
  key 1
    key-string border1
!
pfr border
  logging
  local GigabitEthernet3/0/0
  master 10.1.1.1 key-chain key1
```

Don't forget to configure all the border routers using a similar configuration but with appropriate changes. Now configure the master controller.

Master Controller

```
key chain key1
  key 1
    key-string border1
 key chain key2
  key 1
    key-string border2
 key chain key3
  key 1
    key-string border3
 pfr master
  logging
  border 10.1.1.1 key-chain key1
   interface GigabitEthernet3/0/0 external
    cost-minimization nickname ISP1
    cost-minimization tier 100 fee 50000
    cost-minimization tier 65 fee 10000
    cost-minimization tier 30 fee 500
    cost-minimization end day-of-month 24
    cost-minimization sampling period 5 rollup 1440
    cost-minimization discard absolute 10
    exit
   interface GigabitEthernet3/0/1 internal
   exit
  border 10.2.1.2 key-chain key2
   interface GigabitEthernet3/2/0 external
   interface GigabitEthernet3/0/0 internal
   exit
  border 10.4.1.4 key-chain key3
   interface GigabitEthernet4/0/0 external
    cost-minimization nickname ISP2
    cost-minimization fixed fee 3000
    cost-minimization end day-of-month 24
    exit
   interface GigabitEthernet4/0/2 internal
   exit
  no max range receive
```

```
  delay threshold 10000
  loss threshold 1000000
  mode route control
  mode monitor passive
  mode select-exit best
  resolve cost priority 1
  active-probe echo 10.1.9.1
  end
```

Now enter the **show pfr master cost-minimization border** command at the master controller to show the configuration and the utilization statistics. The rollup values during the 30-day March through April 24th billing period for the GigabitEthernet interface 3/0/0 on border router 10.1.1.1 are shown in the output:

```
Router# show pfr master cost-minimization border 10.1.1.1
pM - per Month, pD - per Day
 --------------------------------------------------------------------------------
  Nickname  : ISP1             Border: 10.1.1.1          Interface: Gi3/0/0
  Calc type : Separate
  End Date  : 24
  Summer time: Disabled
  Fee       : Tier Based
              Tier 1: 100, fee:      50000
              Tier 2:  65, fee:      10000
              Tier 3:  30, fee:        500
  Period    : Sampling 5, Rollup 1440
  Discard   : Type Absolute, Value 10

  Rollup Information:
  Total(pM)       Discard(pM)     Remaining(pM)   Collected(pM)
  31              10              1               29

  Current Rollup Information:
    MomentaryTgtUtil:           75 Kbps    CumRxBytes:                0
   StartingRollupTgt:           75 Kbps    CumTxBytes:                0
    CurrentRollupTgt:           75 Kbps    TimeRemain:         00:00:51

  Rollup Utilization (Kbps):
  Egress Utilization Rollups (Descending order)

  1   : 0           2   : 89          3   : 80          4   : 71
  5   : 70          6   : 65          7   : 65          8   : 51
  9   : 50          10  : 49          11  : 49          12  : 45
  13  : 42          14  : 39          15  : 35          16  : 34
  17  : 30          18  : 30          19  : 30          20  : 29
  21  : 25          22  : 20          23  : 19          24  : 12
  25  : 10          26  : 10          27  : 9           28  : 8
  29  : 4           30  : 1
  Ingress Utilization Rollups (Descending order)

  1   : 0           2   : 92          3   : 84          4   : 82
  5   : 80          6   : 78          7   : 75          8   : 73
  9   : 72          10  : 70          11  : 63          12  : 62
  13  : 60          14  : 55          15  : 53          16  : 52
  17  : 45          18  : 43          19  : 35          20  : 33
  21  : 31          22  : 25          23  : 23          24  : 21
  25  : 15          26  : 11          27  : 10          28  : 10
  29  : 5           30  : 1
```

If we assume that the March through April 24th billing period is over, we can see the billing for the previous billing period using the **show pfr master cost-minimization billing-history** command. The monthly sustained utilization is 62 and the cost is $10,000 for the GigabitEthernet interface 3/0/0 link on border router 10.1.1.1.

```
Router# show pfr master cost-minimization billing-history
Billing History for the past three months

         ISP2 on 10.4.1.4          Gi4/0/0
  No cost min on 10.2.1.2          Gi3/2/0
         ISP1 on 10.1.1.1          Gi3/0/0
                  Mon1                 Mon2                 Mon3
 Nickname     SustUtil       Cost   SustUtil       Cost   SustUtil       Cost
 ----------    ------------------    ------------------   ------------------
```

```
   ISP2             0       3000        ---NA---             ---NA---
   ISP1            62      10000        ---NA---             ---NA---

----------    ------------------    ------------------   ------------------
Total Cost                13000                     0                    0
```

Where to Go Next

If you want to review more information about PfR, see the documents that are listed under “Related Documents” section.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco PfR commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples	Cisco IOS Performance Routing Command Reference
Basic PfR configuration	"Configuring Basic Performance Routing" module
Concepts required to understand the Performance Routing operational phases	"Understanding Performance Routing" module
Advanced PfR configuration	"Configuring Advanced Performance Routing" module
IP SLAs overview	*IP SLAs Configuration Guide*
PfR home page with links to PfR-related content on our DocWiki collaborative environment	PfR:Home

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

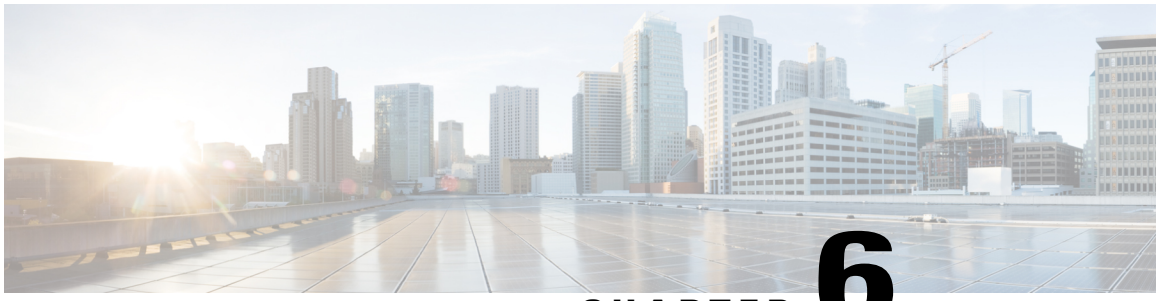
Feature Information for Configuring Performance Routing Cost Policies

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 7: Feature Information for Configuring Performance Routing Cost Policies

Feature Name	Releases	Feature Configuration Information
OER Support for Cost-Based Optimization	12.3(14)T 12.2(33)SRB 12.4(15)T9	The OER Support for Cost-Based Optimization feature introduced the capability to configure exit link policies based monetary cost and the capability to configure traceroute probes to determine prefix characteristics on a hop-by-hop basis. In Cisco IOS Release 12.4(15)T9 and later releases, the calculation of the MTLU algorithm is modified to allow for more efficient bandwidth utilization while minimizing the link cost. The following commands were introduced or modified by this feature: **cost-minimization (PfR)**, **debug pfr master cost-minimization**,**show pfr master cost-minimization**.



CHAPTER 6

Using Performance Routing to Control EIGRP Routes with mGRE DMVPN Hub-and-Spoke Support

The PfR EIGRP mGRE DMVPN Hub-and-Spoke Support feature introduces the ability to inject routes into the EIGRP routing table, which allows Performance Routing (PfR) to control prefixes and applications over EIGRP routes. This feature also adds support for multipoint Generic Routing Encapsulation (mGRE) Dynamic Multipoint Virtual Private Network (DMVPN) deployments that follow a hub-and-spoke network design.

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 Table at the end of this document.

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.

Prerequisites for Using PfR to Control EIGRP Routes

This feature assumes that EIGRP is already configured in your network and that basic PfR functionality is also configured.

Restrictions for Using PfR to Control EIGRP Routes

- PfR does not support split tunneling.
- PfR supports hub-to-spoke links only. Spoke-to-spoke links are not supported. If you are deploying EIGRP in an mGRE DMVPN topology in your network, it must conform to a hub-and-spoke network design.
- PfR is supported on DMVPN Multipoint GRE (mGRE) deployments. Any multipoint interface deployment that has multiple next hops for the same destination IP address is not supported (for example, Ethernet).

Information About Using PfR to Control EIGRP Routes

PfR EIGRP Route Control

The PfR EIGRP mGRE DMVPN Hub-and-Spoke Support feature introduces PfR route control for EIGRP. When enabled, a parent route check is performed in the EIGRP database for controlling PfR prefixes and routes in addition to the existing BGP and static route databases.

PfR can only optimize paths for prefixes, which have an exact matching route or a less specific route (also called as parent route) in the routing protocols. The route being controlled by PfR can be an exact match of the parent route or can be a more specific one. For example, if PfR wants to control 10.1.1.0/24 but the EIGRP routing table has only 10.1.0.0/16 then the parent route is 10.1.0.0/16 and PfR will inject 10.1.1.0/24 in the EIGRP routing table.

If an exact matching parent route in the EIGRP routing table is found, PfR will attempt to install a route on an exit selected by the master controller by influencing the metric. If an exact match parent is not found, then PfR introduces a new route in the EIGRP table that matches the attributes of the parent. If the route installation in the EIGRP table is successful, PfR saves the EIGRP parent and registers for any updates to the parent route. If the parent route is removed, PfR will uncontrol any routes it has installed in the EIGRP table based on this parent route.

PfR monitors traffic performance for prefixes it is controlling either passively using NetFlow or actively using IP SLA probes. Performance statistics such as delay, loss, and reachability are gathered and compared against a set of policies configured for the prefixes. If the traffic performance does not conform to the policies, the prefix is said to be out-of-policy (OOP). PfR tries to find an alternate path when the prefix goes into the OOP state.

While both BGP and static route control are enabled by default, EIGRP route control must be configured. PfR always attempts to control a prefix using BGP first. If BGP route control fails, static route control is tried. When EIGRP route control is enabled, PfR will attempt to control a prefix using BGP first. If no parent route is found, PfR will try to use EIGRP route control. If EIGRP route controls fails, static route control is tried.

To find an alternate path for a prefix, PfR tries to send active probes from all the external interfaces on the border routers to a set of hosts in the destination prefix network. Before an active probe can be sent on an external interface, a parent route lookup is performed in routing protocol tables. When the PfR EIGRP mGRE DMVPN Hub-and-Spoke Support feature is enabled, PfR checks EIGRP routing tables, in addition to BGP and static routing tables, for a parent route, before sending active probes on external interfaces. Active probes are initiated on all the external interfaces that have a parent route in the EIGRP routing table. When the probe activity completes and the timer expires, statistics are sent from the border router to the master controller for policy decision and selection of an optimal exit.

When an exit is selected, a control prefix command is sent to the border router with the selected exit, specifying EIGRP as the protocol to install or modify the route. When the border router receives the command, it checks the EIGRP table to find a parent route. If a parent route is found, PfR will install or modify the route in the EIGRP table and will notify the master controller about the route control status.

If an EIGRP route is successfully installed and advertised into the domain, PfR continues to monitor traffic performance for this prefix and takes further action as mentioned above if the prefix goes OOP.

For more details about the PfR control mode and details about other PfR exit link selection control techniques including BGP, static routes, policy-based routing, and Protocol Independent Route Optimization (PIRO), see the Understanding Performance Routing module and the Performance Routing - Protocol Independent Route Optimization (PIRO) module.

PfR and mGRE Dynamic Multipoint VPN

Performance Routing is supported on mGRE interfaces in Dynamic Multipoint VPN (DMVPN) topologies. DMVPN enables zero-touch deployment of IPsec encrypted VPN networks. Many DMVPN deployments use EIGRP networks, and support was added to PfR to allow DMVPN network deployments to use EIGRP route control within the DMVPN network. In the PfR EIGRP route control implementation, only hub-to-spoke network designs are supported.

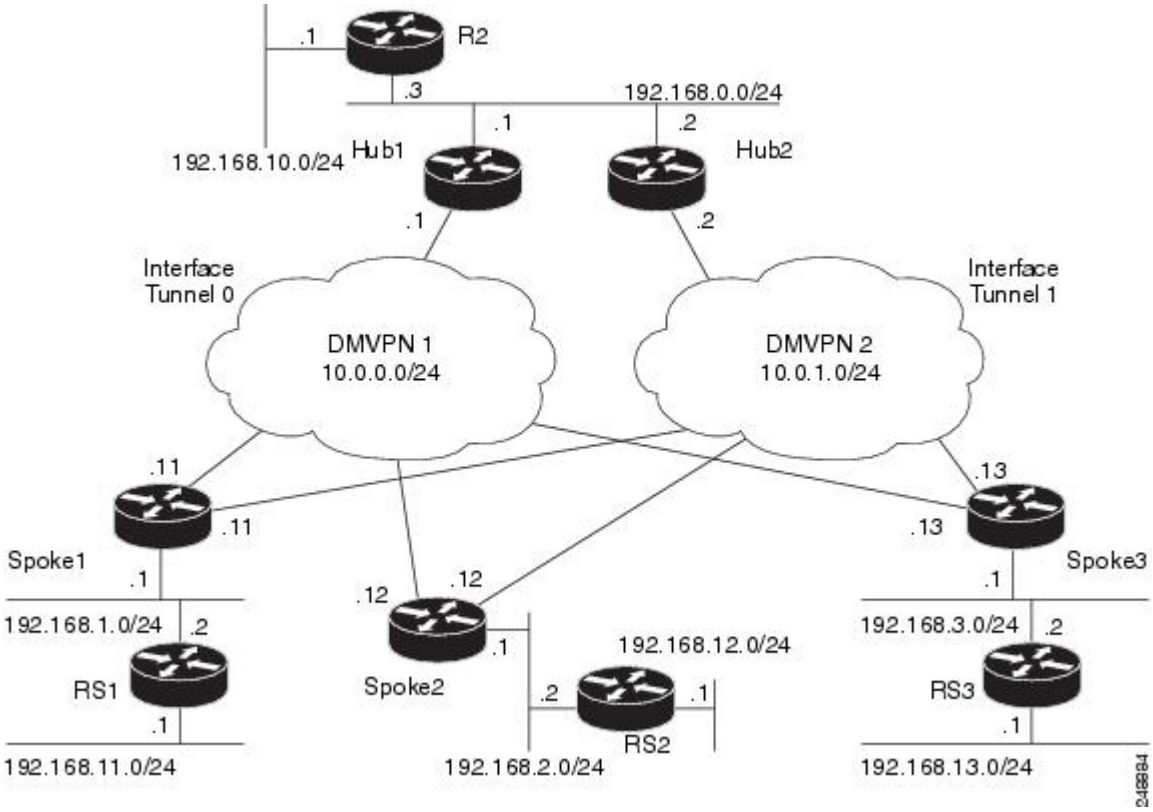
In DMVPN topologies the mGRE interface works as a one-to-many interface and allows the dynamic creation of tunnels for each connected branch.

The figure below shows a typical dual DMVPN topology. The head office (R2) has one hub (hub1) that connects to the remote site spokes using one of the DMVPN networks (DMVPN 1 or DMVPN 2) or the MPLS-GETVPN network.

Remote site 1 (RS1) has spokes 1 and 2 that connect to the hub using the DMVPN1 and DMVPN2 networks. Remote site 2 (RS2) has spoke 3 and connects to the hub using DMVPN1 network only. This means that there is no redundancy at RS2 and any performance optimization is performed between the hub and RS2 only.

Remote site 3 (RS3) has spoke 3 that connects to the hub using the DMVPN2 network and the MPLS-GETVPN network.

Figure 12: PfR Dual DMVPN Topology



When PfR is configured on the network, the system can perform these functions:

- Control and measure the performance of PfR traffic-classes on mGRE interfaces.
- Support load balancing for traffic over multipoint interfaces that are configured as PfR external interfaces. For example, in topologies with two DMVPN clouds PfR can be configured to load balance the traffic across the two tunnel interfaces to ensure that network performance is maintained.
- Reroute traffic from or to a multipoint interface for better performance. For example, PfR policies can be configured to select the best path to a spoke and the best path from the spoke to the hub.
- Provide a back-up connection if the primary connection fails. For example, in a topology with one MPLS-GETVPN and one DMVPN connection, the MPLS-GETVPN could act as a primary connection and PfR could be configured to use the DMVPN connection if the primary connection fails.

The DMVPN topology leverages protocols like multipoint GRE (mGRE) for hub-to-spoke functionality, and for spoke-to-spoke functionality it utilizes the Next Hop Resolution Protocol (NHRP). For more details about configuring mGRE DMVPN networks, see the "Dynamic Multipoint VPN" module in the *Cisco IOS Security Configuration Guide: Secure Connectivity*. For general information about DMVPN, go to http://www.cisco.com/go/dmvpn.

How to Configure PfR to Control EIGRP Routes

Enabling PfR EIGRP Route Control and Setting a Community Value

Perform this task on the master controller to enable EIGRP route control. While both BGP and static route control are enabled by default, EIGRP route control must be enabled using a command-line interface (CLI) command, **mode route metric eigrp**. PfR always attempts to control a prefix using BGP first. If BGP route control fails, static route control is tried. When EIGRP route control is enabled, PfR will attempt to control a prefix using BGP first. If no parent route is found, PfR will try to use EIGRP route control. If EIGRP route controls fails, static route control is tried.

This task can also set an extended community value for an injected EIGRP route to allow the routes to be uniquely identified. An EIGRP route may be injected by PfR to control the traffic defined by a traffic class when it goes out-of-policy (OOP). In this task, the PfR route control mode is configured globally with the **mode route control** command in PfR master controller configuration mode, and any injected EIGRP routes will be tagged with a value of 700.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **mode route control**
5. **mode route metric eigrp tag** *community*
6. **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.
Step 3	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure a router as a master controller and to configure global operations and policies.

	Command or Action	Purpose
Step 4	**mode route control** **Example:** `Router(config-pfr-mc)# mode route control`	Configures the PfR route control mode on a master controller. • The **route**and **control** keywords enable route control mode. In control mode, the master controller analyzes monitored traffic classes and implements changes based on policy parameters.
Step 5	**mode route metric eigrp tag** *community* **Example:** `Router(config-pfr-mc)# mode route metric eigrp tag 7000`	Enables EIGRP route control and sets an EIGRP tag and community number value for injected EIGRP routes. • Use the **tag** keyword to apply a tag to an EIGRP route under PfR control. The*community* argument is a number from 1 to 65535.
Step 6	**end** **Example:** `Router(config-pfr-mc)# end`	Exits PfR master controller configuration mode and returns to privileged EXEC mode.

Disabling PfR EIGRP Route Control

Note When this task is complete, PfR withdraws all the routes that are being controlled using the EIGRP protocol.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **no mode route metric eigrp**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure a router as a master controller and to configure global operations and policies.
Step 4	**no mode route metric eigrp** **Example:** `Router(config-pfr-mc)# no mode route metric eigrp`	Disables EIGRP route control and removes all the routes that are being controlled using the EIGRP protocol.
Step 5	**end** **Example:** `Router(config-pfr-mc)# end`	Exits PfR master controller configuration mode and returns to privileged EXEC mode.

Manually Verifying the PfR EIGRP-Controlled Routes

PfR automatically verifies route control changes in the network using NetFlow output. PfR monitors the NetFlow messages and uncontrols a traffic class if a message does not appear to verify the route control change. Perform the steps in this optional task if you want to manually verify that the traffic control implemented in the PfR control phase actually changes the traffic flow, and brings the OOP event to be in-policy.

All the steps in this task are optional and are not in any order. The information from these steps can verify that a specific prefix associated with a traffic class has been moved to another exit or entrance link interface, or that it is being controlled by PfR. The first two commands are entered at the master controller, the last two commands are entered at a border router.

Only partial command syntax for some of the **show** commands used in this task is displayed. For more details about PfR **show** commands, see the *Cisco IOS Performance Routing Command Reference*.

Before You Begin

This task assumes that you have previously enabled EIGRP route control using PfR.

SUMMARY STEPS

1. **enable**
2. **show pfr master prefix** *prefix* [**detail**]
3. Move to a border router to enter the next step.
4. **enable**
5. **show pfr border routes eigrp** [**parent**]

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 2 **show pfr master prefix** *prefix* [**detail**]

This command is used to display the status of monitored prefixes. The output from this command includes information about the source border router, current exit interface, protocol, prefix delay, and egress and ingress interface bandwidth. In this example, the protocol displayed for the prefix 10.1.0.0/16 is EIGRP, which means that the parent route for the traffic class exists in the EIGRP routing table and EIGRP community values are used to control the prefix. Only syntax relevant to this task is shown in this step.

Example:

```
Router# show pfr master prefix 10.1.0.0

OER Prefix Statistics:
 Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
 P - Percentage below threshold, Jit - Jitter (ms),
 MOS - Mean Opinion Score
 Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
 E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
 U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
 # - Prefix monitor mode is Special, & - Blackholed Prefix
 % - Force Next-Hop, ^ - Prefix is denied
Prefix                  State     Time Curr BR         CurrI/F         Protocol
                     PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos
                     ActSDly  ActLDly   ActSUn   ActLUn      EBw      IBw
                     ActSJit  ActPMOS
------------------------------------------------------------------------------
10.1.0.0/16          DEFAULT*      @69 10.1.1.1        Gi1/22          EIGRP
                           U        U        0        0        0        0
                           U        U        0        0       22        8
                           N        N
```

Step 3 Move to a border router to enter the next step.

The next command is entered on a border router, not the master controller.

Example:

Step 4 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 5 **show pfr border routes eigrp** [**parent**]

This command is entered on a border router. Use this command to display information about EIGRP routes controlled by PfR on a border router. In this example, the output shows that prefix 10.1.2.0/24 is being controlled by PfR. This command is used to show parent route lookup and route changes to existing parent routes when the parent route is identified from the EIGRP routing table.

Example:

```
Router# show pfr border routes eigrp

Flags: C - Controlled by oer, X - Path is excluded from control,
       E - The control is exact, N - The control is non-exact
Flags Network            Parent             Tag
CE    10.1.2.0/24        10.0.0.0/8         5000
```

In this example, the **parent** keyword is used and more details are shown about the parent route lookup.

Example:

```
Router# show pfr border routes eigrp parent

Network            Gateway            Intf       Flags
10.0.0.0/8         10.40.40.2         Gi0/0/2    1
Child Networks
Network            Flag
10.1.2.0/24        6
```

Troubleshooting Tips

If the **show** commands are not displaying output that verifies the EIGRP route control, use the **debug pfr border routes eigrp** command with the optional **detail** keyword for more information. Debugging must be enabled before entering the required commands, and the debug output depends on which commands are subsequently entered.

Configuration Examples for Using PfR to Control EIGRP Routes

Example Enabling PfR EIGRP Route Control and Setting a Community Value

In the following configuration example, PfR route control is enabled first, and then the EIGRP route control is enabled and configured to set an extended community value of 700 to any injected EIGRP routes:

```
pfr master
 mode route control
```

```
mode route metric eigrp tag 700
end
```

Where to Go Next

This module covers PfR EIGRP route control and presumes that you are familiar with the PfR technology. If you want to review more information about PfR, see the documents that are listed under "Related Documents" section.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco PfR commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples	Cisco IOS Performance Routing Command Reference
Basic PfR configuration	"Configuring Basic Performance Routing" module
Advanced PfR configuration	"Configuring Advanced Performance Routing" module
Concepts required to understand the Performance Routing operational phases	"Understanding Performance Routing" module
EIGRP Routing Protocol commands	*Cisco IOS IP Routing: EIGRP Command Reference*
Configuring mGRE DMVPN networks	"Dynamic Multipoint VPN"
General information about the DMVPN technology	http://www.cisco.com/go/dmvpn
PfR home page with links to PfR-related content on our DocWiki collaborative environment	PfR:Home

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/cisco/web/support/index.html

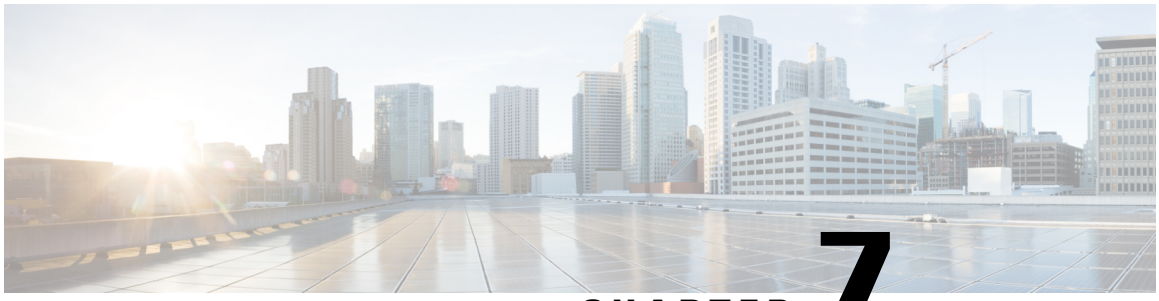
Feature Information for Using PfR to Control EIGRP Routes

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 8: Feature Information for Using PfR to Control EIGRP Routes

Feature Name	Releases	Feature Information
PfR EIGRP mGRE DMVPN Hub-and-Spoke Support	12.2(33)SRE 15.0(1)M 15.0(1)S	The PfR EIGRP feature introduces PfR route control capabilities based on EIGRP by performing a route parent check on the EIGRP database. This feature also adds support for mGRE Dynamic Multipoint VPN (DMVPN) deployments that follow a hub-and-spoke network design. The following commands were introduced or modified: **debug pfr border routes**, **mode (PfR)**, **show pfr border routes**, and **show pfr master prefix**.



CHAPTER 7

Performance Routing Link Groups

The Performance Routing - Link Groups feature introduced the ability to define a group of exit links as a preferred set of links, or a fallback set of links for Performance Routing (PfR) to use when optimizing traffic classes specified in a PfR policy.

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 Table at the end of this document.

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 Performance Routing Link Groups

Performance Routing Link Grouping

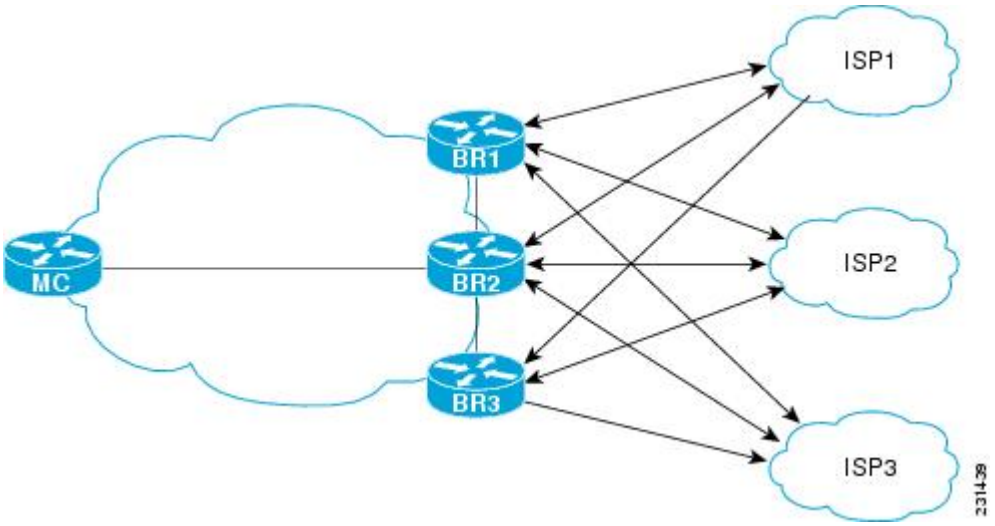
The Performance Routing Link Groups feature introduced the ability to define a group of exit links as a preferred set of links, or a fallback set of links for PfR to use when optimizing traffic classes specified in an PfR policy. PfR currently selects the best link for a traffic class based on the preferences specified in a policy

and the traffic class performance—using parameters such as reachability, delay, loss, jitter or MOS—on a path out of the specified link. Bandwidth utilization, cost, and the range of links can also be considered in selecting the best link. Link grouping introduces a method of specifying preferred links for one or more traffic classes in an PfR policy so that the traffic classes are routed through the best link from a list of preferred links, referred to as the primary link group. A fallback link group can also be specified in case there are no links in the primary group that satisfy the specified policy and performance requirements. If no primary group links are available, the traffic classes are routed through the best link from the fallback group. To identify the best exit, PfR probes links from both the primary and fallback groups.

Primary and fallback link groups can be configured at the master controller and are identified using a unique name. Link groups provide a method of grouping links such as high bandwidth links to be used, for example, by video traffic, by configuring an PfR policy to specify that the best link is to be selected from the link group that consists of only high bandwidth links. The traffic classes specified in a policy can be configured with only one primary link group and one fallback link group. The priority of a link group can vary between policies, a link group might be a primary link group for one policy, and a fallback link group for another policy.

See the figure below for an example of how to implement link grouping. Three link groups, ISP1, ISP2, and ISP3 represent different Internet Service Providers (ISPs) and all three ISPs have links to interfaces on the three border routers shown in the figure below. ISP1 links are the most expensive links, but they have the best Service Level Agreement (SLA) guarantees. ISP3 links are best effort links, and these links are the cheapest links. ISP2 links are not as good as the ISP1 links, but the ISP2 links are more reliable than the ISP3 links. The cost of the ISP2 links is higher than the ISP3 links, but lower than ISP1 links. In this situation, each ISP is created as a link group and associated with an interface on each border router shown in the figure below.

Figure 13: Link Group Diagram



Assuming four types of traffic class, video, voice, FTP, and data, each traffic class can be routed through a border router interface belonging to an appropriate link group. Video and voice traffic classes need the best links so the ISP1 link group is configured as the primary link group, with ISP2 as the fallback group. FTP traffic needs reliable links but the cost might be a factor so ISP2 is assigned as the primary group, and ISP3 is the fallback link group. Note that although ISP1 provides the most reliable links, it may be too expensive for file transfer traffic. For data traffic, ISP3 is a good choice as a primary link group, with ISP2 as the fallback group.

Note If you are configuring link grouping, configure the **no max-range-utilization** command because using a link utilization range is not compatible with using a preferred or fallback set of exit links configured for link grouping. With CSCtr33991, this requirement is removed and PfR can perform load balancing within a PfR link group.

Spillover

Performance routing link groups can be used to support spillover. Spillover is when there are two paths through the network--traffic engineering (TE) tunnels, for example--to the same provider edge (PE) router, but the tunnels take different paths across the network and the traffic is sent through one tunnel until it reaches a traffic load threshold when it spills over to the second tunnel. Using PfR link groups one tunnel is created as a primary link group and the second tunnel is the fallback link group. When the first tunnel goes out of policy, PfR switches to the fallback tunnel link group, which provides the spillover capacity until the traffic load on the first tunnel drops below the threshold. The tunnels must be established before the PfR link groups are configured.

How to Configure Performance Routing Link Groups

Implementing Performance Routing Link Groups

Perform this task on a master controller to set up some performance routing link groups by identifying an exit link on a border router as a member of a link group, and to create a PfR map to specify link groups for traffic classes defined in a PfR policy. In this task, a link group is set up for video traffic and a set of high bandwidth exit links are identified as members of the video link group which is identified as a primary link group. A fallback link group is also specified.

A PfR policy is created using an PfR map where the primary and fall link groups are specified for traffic classes matching the PfR map criteria. PfR probes both the primary and fallback group links and selects the best link in the primary link group for the traffic class specified in this task. If none of the primary links are within policy, PfR selects the bast link from the fallback group. For more details about link groups, see the “Performance Routing Link Grouping” section.

Note If you are configuring link grouping, configure the **no max-range-utilization** command because using a link utilization range is not compatible with using a preferred or fallback set of exit links configured for link grouping. With CSCtr33991, this requirement is removed and PfR can perform load balancing within a PfR link group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **border** *ip-address* [**key-chain** *key-chain-name*]
5. **interface** *type number* **external**
6. **link-group** *link-group-name* [*link-group-name* [*link-group-name*]]
7. **exit**
8. Repeat Step 5 through Step 7 with appropriate changes to set up link groups for all the external interface.
9. **interface** *type number* **internal**
10. **exit**
11. **ip access-list** {**standard** | **extended**} *access-list-name*
12. [*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**dscp** *dscp-value*]
13. Repeat Step 12 for more access list entries, as required.
14. **exit**
15. **pfr-map** *map-name sequence-number*
16. **match traffic-class access-list** *access-list-name*
17. **set link-group** *link-group-name* [**fallback** *link-group-name*]
18. **end**
19. **show pfr master link-group** [*link-group-name*]

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.
Step 3	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure a router as a master controller. • A master controller and border router process can be enabled on the same router (for example, in a network that has a single router with two exit links to different service providers).

	Command or Action	Purpose
Step 4	**border** *ip-address* [**key-chain** *key-chain-name*] **Example:** `Router(config-pfr-mc)# border 192.168.1.2 key-chain border1_PFR`	Enters PfR-managed border router configuration mode to establish communication with a border router. • An IP address is configured to identify the border router. • At least one border router must be specified to create a PfR-managed network. A maximum of ten border routers can be controlled by a single master controller. • The value for the *key-chain-name* argument must match the key-chain name configured when the border router is set up. **Note** The **key-chain** keyword and *key-chain-name* argument must be entered when a border router is initially configured. However, this keyword is optional when reconfiguring an existing border router.
Step 5	**interface** *type number* **external** **Example:** `Router(config-pfr-mc-br)# interface Serial 2/0 external`	Configures a border router interface as a PfR-managed external interface. • External interfaces are used to forward traffic and for active monitoring. • A minimum of two external border router interfaces are required in a PfR-managed network. At least one external interface must be configured on each border router. A maximum of 20 external interfaces can be controlled by single master controller. **Tip** Configuring an interface as a PfR-managed external interface on a router enters PfR border exit interface configuration mode. In this mode, you can configure maximum link utilization or cost-based optimization for the interface. **Note** Entering the **interface** (PfR) command without the **external** or**internal** keyword places the router in global configuration mode and not PfR border exit configuration mode. The **no** form of this command should be applied carefully so that active interfaces are not removed from the router configuration.
Step 6	**link-group** *link-group-name* [*link-group-name* [*link-group-name*]] **Example:** `Router(config-pfr-mc-br-if)# link-group VIDEO`	Configures a PfR border router exit interface as a member of a link group. • Use the *link-group-name* to specify the link group name for the interface. • Up to three link groups can be specified for each interface. • In this example, the Serial 2/0 external interface is configured as a member of the link group named VIDEO. **Note** The **link-group** (PfR) command associates a link group with an interface. Another step, Step 17, uses the **set link-group** (PfR) command to identify the link group as a primary or fallback group for traffic classes defined in a PfR map.
Step 7	**exit** **Example:** `Router(config-pfr-mc-br-if)# exit`	Exits PfR-managed border exit interface configuration mode and returns to PfR-managed border router configuration mode.

	Command or Action	Purpose
Step 8	Repeat Step 5 through Step 7 with appropriate changes to set up link groups for all the external interface.	--
Step 9	**interface** *type number* **internal** **Example:** `Router(config-pfr-mc-br)# interface FastEthernet 0/1 internal`	Configures a border router interface as an PfR controlled internal interface. • Internal interfaces are used for passive monitoring only. Internal interfaces do not forward traffic. • At least one internal interface must be configured on each border router. **Note** Support to configure a VLAN interface as an internal interface was introduced in Cisco IOS Release 12.3(14)T and 12.2(33)SRB.
Step 10	**exit** **Example:** `Router(config-pfr-mc-br)# exit`	Exits PfR-managed border configuration mode and returns to global configuration mode.
Step 11	**ip access-list** {**standard** | **extended**} *access-list-name* **Example:** `Router(config)# ip access-list extended ACCESS_VIDEO`	Defines an IP access list by name and enters extended named access list configuration mode. • PfR supports only named access lists. • The example creates an extended IP access list named ACCESS_VIDEO.
Step 12	[*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**dscp** *dscp-value*] **Example:** `Router(config-ext-nacl)# permit tcp any any 500`	Sets conditions to allow a packet to pass a named IP access list. • The example is configured to identify all TCP traffic from any destination or source and from destination port number of 500. This specific TCP traffic is to be optimized.
Step 13	Repeat Step 12 for more access list entries, as required.	--
Step 14	**exit** **Example:** `Router(config-ext-nacl)# exit`	(Optional) Exits extended named access list configuration mode and returns to global configuration mode.
Step 15	**pfr-map** *map-name sequence-number* **Example:** `Router(config)# pfr-map VIDEO_MAP 10`	Enters PfR map configuration mode to configure a PfR map. • Only one match clause can be configured for each PfR map sequence. • Permit sequences are first defined in an IP prefix list and then applied with the **match ip address** (PfR) command in Step 16 .

	Command or Action	Purpose
		• The example creates n PfR map named VIDEO_MAP.
Step 16	**match traffic-class access-list** *access-list-name* **Example:** `Router(config-pfr-map)# traffic-class access-list ACCESS_VIDEO`	Manually configures an access list as match criteria used to create traffic classes using a PfR map. • Each access list entry must contain a destination prefix and may include other optional parameters. • The example defines a traffic class using the criteria defined in the access list named ACCESS_VIDEO.
Step 17	**set link-group** *link-group-name* [**fallback** *link-group-name*] **Example:** `Router(config-pfr-map)# set link-group video fallback voice`	Specifies a link group for traffic classes defined in a PfR map to create a PfR policy. • Use the *link-group-name* to specify the primary link group name for the policy. • Use the **fallback** keyword to specify the fallback link group name for the policy. • The example specifies the VIDEO link group as the primary link group for the traffic class matching the access list ACCESS_VIDEO. The link group VOICE is specified as the fallback link group.
Step 18	**end** **Example:** `Router(config-pfr-map)# end`	(Optional) Exits PfR map configuration mode and returns to privileged EXEC mode.
Step 19	**show pfr master link-group** [*link-group-name*] **Example:** `Router# show pfr master link-group`	Displays information about configured PfR link groups. • Use the optional *link-group-name* argument to display information for the specified PfR link group. • If the *link-group-name* argument is not specified, information about all PfR link groups is displayed. • The example displays information about all configured link groups.

Example

The example output from the **show pfr master link-group** command displays information about performance routing link groups configured using PfR. In this example, the VIDEO link group is shown with other configured link groups.

```
Router# show pfr master link-group
link group video
  Border          Interface       Exit id
  192.168.1.2     Serial2/0       1
```

```
link group voice
 Border           Interface       Exit id
 192.168.1.2      Serial2/0       1
 192.168.1.2      Serial3/0       2
 192.168.3.2      Serial4/0       4
link group data
 Border           Interface       Exit id
 192.168.3.2      Serial3/0       3
```

Configuration Examples for Performance Routing Link Groups

Example Implementing Performance Routing Link Groups

The following example shows how to implement link groups. In this example, a PfR map named VIDEO_MAP is created to configure PfR to define a traffic class that matches an access list named ACCESS_VIDEO. The traffic class is configured to use a link group named VIDEO as the primary link group, and a fallback group named VOICE. The VIDEO link group may be a set of high bandwidth links that are preferred for video traffic.

```
enable
configure terminal
border 10.1.4.1
 interface serial 2/0 external
  link-group VIDEO
  exit
 interface serial 3/0 external
  link-group VOICE
  exit
 interface Ethernet 1/0 internal
 exit
ip access-list extended ACCESS_VIDEO
 permit tcp any 10.1.1.0 0.0.0.255 eq 500
 permit tcp any 172.17.1.0 0.0.255.255 eq 500
 permit tcp any 172.17.1.0 0.0.255.255 range 700 750
 permit tcp 192.168.1.1 0.0.0.0 10.1.2.0 0.0.0.255 eq 800 any any dscp ef
 exit
pfr-map VIDEO_MAP 10
 match traffic-class access-list ACCESS_VIDEO
 set link-group VIDEO fallback VOICE
 end
```

Where to Go Next

For information about other Performance Routing features or general conceptual material, see the documents in the “Related Documents” section.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
Cisco PfR commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples	Cisco IOS Performance Routing Command Reference
Basic PfR configuration	"Configuring Basic Performance Routing" module
Concepts required to understand the Performance Routing operational phases	"Understanding Performance Routing" module
Advanced PfR configuration	"Configuring Advanced Performance Routing" module
IP SLAs overview	*IP SLAs Configuration Guide*
PfR home page with links to PfR-related content on our DocWiki collaborative environment	PfR:Home

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

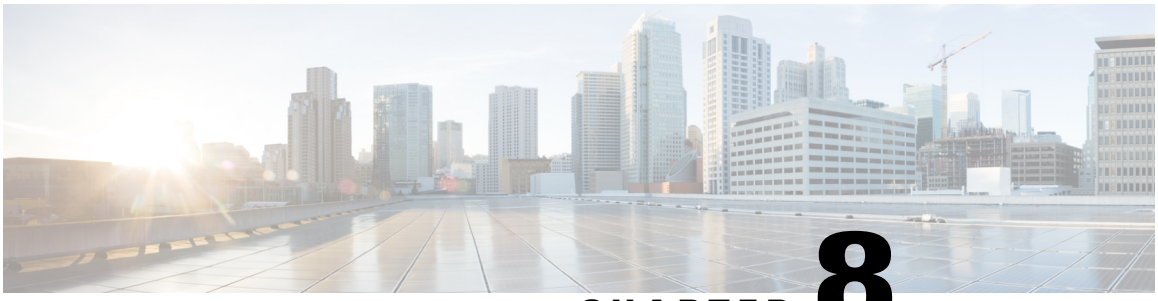
Feature Information for Performance Routing Link Groups

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 9: Feature Information for Performance Routing Link Groups

Feature Name	Releases	Feature Information
Performance Routing - Link Groups	12.4(15)T	The Performance Routing - Link Groups feature introduces the ability to define a group of exit links as a preferred set of links, or a fallback set of links for PfR to use when optimizing traffic classes specified in a PfR policy. The following commands were introduced or modified by this feature: **link-group (PfR)**, **set link-group (PfR)**, and **show pfr master link-group**.



CHAPTER 8

Performance Routing with NAT

Performance Routing (PfR) introduced support for the control of traffic class routing using static routing in networks using NAT with the introduction of a new keyword to an existing NAT command. When PfR and NAT functionality are configured on the same router and PfR controls the routing for a traffic class using static routing, some applications may fail to operate due to dropped packets. This dropping of packets behavior is seen when static routing is used to connect to multiple ISPs from the same router, PfR uses static routing to control the traffic class routing, and one or more of the ISPs use Unicast Reverse Path Forwarding (Unicast RPF) filtering for security reasons.

When the new keyword is configured, new NAT translations are given the source IP address of the interface that PfR has selected for the packet and PfR forces existing flows to be routed through the interface for which the NAT translation was created.

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 Table at the end of this document.

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 Performance Routing with NAT

On Cisco Catalyst 6500 Switch platforms a flow mask conflict has been seen when NAT is configured in a PfR-managed network. Conflicting flow mask requirements can cause traffic to be switched in software. To resolve this conflict, add the following NAT configuration:

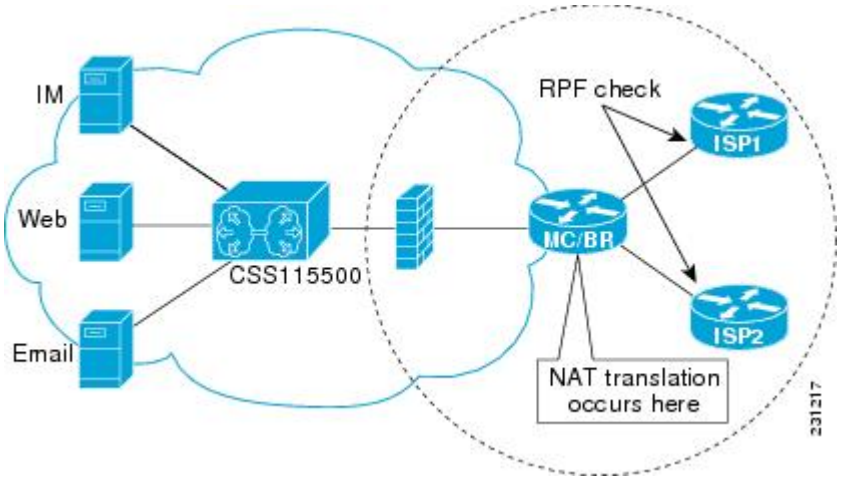
```
mls ip nat netflow-frag-l4-zero
```

Information About Performance Routing with NAT

PfR and NAT

When Cisco IOS PfR and NAT functionality are configured on the same router and PfR controls the routing for a traffic class using static routing, some applications may fail to operate due to dropped packets. This dropping of packets behavior is seen when static routing is used to connect to multiple ISPs from the same router, PfR uses static routing to control the traffic class routing, and one or more of the ISPs use Unicast Reverse Path Forwarding (Unicast RPF) filtering for security reasons. Packets are dropped at the ingress router performing Unicast RPF because PfR changes the route for an outgoing packet for a traffic class from one exit interface to another after the NAT translation from a private IP address to a public IP address is performed. When the packet is transmitted, Unicast RPF filtering at the ingress router (for example, an ISP router) will show a different source IP address from the source IP address pool assigned by NAT, and the packet is dropped. For example, the figure below shows how PfR works with NAT.

Figure 14: PfR with NAT



The NAT translation occurs at the router that is connected to the internal network, and this router can be a border router or a combined master controller and border router. If PfR changes routes to optimize traffic class performance and to perform load balancing, traffic from the border router in the figure above that was routed through the interface to ISP1 may be rerouted through the interface to ISP2 after the traffic performance is measured and policy thresholds are applied. The RPF check occurs at the ISP routers and any packets that

are now routed through ISP2 will fail the RPF check at the ingress router for ISP2 because the IP address of the source interface has changed.

The solution involves a minimal configuration change with a new keyword, **oer**, that has been added to the**ip nat inside source** command. When the**oer** keyword is configured, new NAT translations are given the source IP address of the interface that PfR has selected for the packet and PfR forces existing flows to be routed through the interface for which the NAT translation was created. For example, PfR is configured to manage traffic on a border router with two interfaces, InterfaceA to ISP1 and InterfaceB to ISP2 in the figure above. PfR is first configured to control a traffic class representing Web traffic and the NAT translation for this traffic already exists with the source IP address in the packets set to InterfaceA. PfR measures the traffic performance and determines that InterfaceB is currently the best exit for traffic flows, but PfR does not change the existing flow. When PfR is then configured to learn and measure a traffic class representing e-mail traffic, and the e-mail traffic starts, the NAT translation is done for InterfaceB. The PfR static routing NAT solution is a single box solution and configurations with interfaces on multiple routers using NAT and managed by PfR are not supported. Network configurations using NAT and devices such as PIX firewalls that do not run Cisco IOS software are not supported.

Network Address Translation (NAT)

NAT enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) address in the internal network into legal addresses before packets are forwarded onto another network. NAT can be configured to advertise only one address for the entire network to the outside world. This ability provides additional security, effectively hiding the entire internal network behind that one address.

NAT is also used at the Enterprise edge to allow internal users access to the Internet and to allow Internet access to internal devices such as mail servers.

For more details about NAT, see the “Configuring NAT for IP Address Conservation” chapter of the *Cisco IOS IP Addressing Services Configuration Guide*.

Inside Global Addresses Overloading

You can conserve addresses in the inside global address pool by allowing the router to use one global address for many local addresses. When this overloading is configured, the router maintains enough information from higher-level protocols (for example, TCP or UDP port numbers) to translate the global address back to the correct local address. When multiple local addresses map to one global address, the TCP or UDP port numbers of each inside host distinguish between the local addresses.

How to Configure Performance Routing with NAT

Configuring PfR to Control Traffic with Static Routing in Networks Using NAT

Perform this task to allow PfR to control traffic with static routing in a network using NAT. This task allows PfR to optimize traffic classes while permitting your internal users access to the internet.

When Cisco IOS PfR and NAT functionality are configured on the same router and PfR controls the routing for a traffic class using static routing, some applications may fail to operate due to dropped packets. This

dropping of packets behavior is seen when static routing is used to connect to multiple ISPs from the same router, PfR uses static routing to control the traffic class routing, and one or more of the ISPs use Unicast Reverse Path Forwarding (Unicast RPF) filtering for security reasons.

In this task, the **pfr** keyword is used with the**ip nat inside source** command. When the**pfr** keyword is configured, new NAT translations are given the source IP address of the interface that PfR has selected for the packet and PfR forces existing flows to be routed through the interface where the NAT translation was created. This task uses a single IP address but an IP address pool can also be configured. For a configuration example using an IP address pool, see "Configuring PfR to Control Traffic with Static Routing in Networks Using NAT" section.

Note The PfR static routing NAT solution is a single box solution and configurations with interfaces on multiple routers using NAT and managed by PfR are not supported.

For more details about configuring NAT, see the "Configuring NAT for IP Address Conservation" chapter of the *Cisco IOS IP Addressing Services Configuration Guide*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**permit** | **deny**} *ip-address*mask
4. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
5. **match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*}
6. **match interface** *interface-type interface-number* [*...interface-type interface-number*]
7. **exit**
8. Repeat Step 4 through Step 7 for more route map configurations, as required.
9. **ip nat inside source** {**list** {*access-list-number*| *access-list-name*} | **route-map** *map-name*} {**interface** *type number*| **pool** *name*} [**mapping-id** *map-id* | **overload**| **reversible**| **vrf** *vrf-name*][**pfr**]
10. **interface** *type number*
11. **ip address** *ip-address mask*
12. **ip nat inside**
13. **exit**
14. **interface** *type number*
15. **ip address** *ip-address mask*
16. **ip nat outside**
17. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* {**permit** | **deny**} *ip-address*mask **Example:** `Router(config)# access-list 1 permit 10.1.0.0 0.0.255.255`	Defines a standard access list permitting the IP addresses that are to be translated. • The access list must permit only those addresses that are to be translated. (Remember that there is an implicit "deny all" at the end of each access list.) An access list that is too permissive can lead to unpredictable results.
Step 4	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **Example:** `Router(config)# route-map isp-1 permit 10`	Enters route-map configuration mode to configure a route map. • The example creates a route map named BGP.
Step 5	**match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*} **Example:** `Router(config-route-map)# match ip address access-list 1`	Creates an access list or prefix list match clause entry in a route map to identify traffic to be translated by NAT. • The example references the access list created in Step 3 that specifies the 10.1.0.0 0.0.255.255. prefix as match criteria.
Step 6	**match interface** *interface-type interface-number* [*...interface-type interface-number*] **Example:** `Router(config-route-map)# match interface serial 1/0`	Creates a match clause in a route map to distribute any routes that match out one of the interfaces specified. • The example creates a match clause to distribute routes that pass the match clause in Step 5 through serial interface 1/0.
Step 7	**exit** **Example:** `Router(config-route-map)# exit`	Exits route-map configuration mode and returns to global configuration mode.
Step 8	Repeat Step 4 through Step 7 for more route map configurations, as required.	--

	Command or Action	Purpose
Step 9	**ip nat inside source** {**list** {*access-list-number*| *access-list-name*} | **route-map** *map-name*} {**interface** *type number*| **pool** *name*} [**mapping-id** *map-id* | **overload**| **reversible**| **vrf** *vrf-name*][**pfr**] **Example:** `Router(config)# ip nat inside source interface FastEthernet1/0 overload pfr`	Establishes dynamic source translation with overloading, specifying the interface. • Use the **interface** keyword and type and number arguments to specify an interface. • Use the **pfr** keyword to allow PfR to operate with NAT and control traffic class routing using static routing.
Step 10	**interface** *type number* **Example:** `Router(config)# interface FastEthernet1/0`	Specifies an interface and enters interface configuration mode.
Step 11	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.114.11.8 255.255.255.0`	Sets a primary IP address for the interface.
Step 12	**ip nat inside** **Example:** `Router(config-if)# ip nat inside`	Marks the interface as connected to the inside.
Step 13	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to configuration mode.
Step 14	**interface** *type number* **Example:** `Router(config)# interface ethernet 0`	Specifies a different interface and returns to interface configuration mode.
Step 15	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 172.17.233.208 255.255.255.0`	Sets a primary IP address for the interface.
Step 16	**ip nat outside** **Example:** `Router(config-if)# ip nat outside`	Marks the interface as connected to the outside.

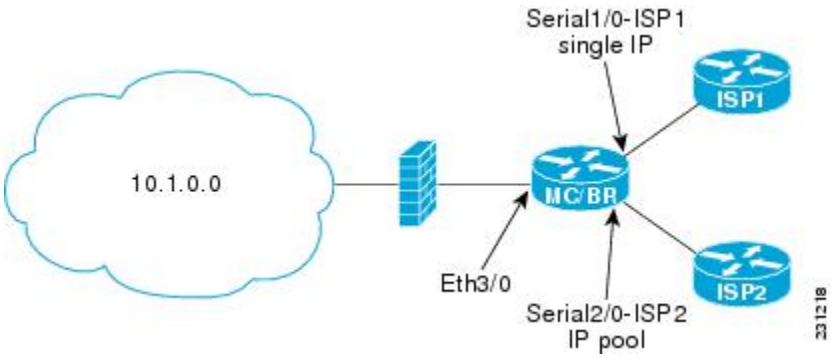
	Command or Action	Purpose
Step 17	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for Performance Routing with NAT

Example Configuring PfR to Control Traffic with Static Routing in Networks Using NAT

The following configuration example configures a master controller to allow PfR to control traffic with static routing in a network using NAT. This example shows how to use a pool of IP addresses for the NAT translation.

Figure 15: PfR and NAT Network Diagram



In the figure above there is a combined master controller and border router that is connected to the Internet through two different ISPs. The configuration below allows PfR to optimize traffic classes while permitting the internal users access to the internet. In this example the traffic classes to be translated using NAT are specified using an access list and a route map. The use of a pool of IP addresses for NAT translation is then configured and the **pfr** keyword is added to the **ip nat inside source** command to configure PfR to keep existing traffic classes flowing through the interface that is the source address that was translated by NAT. New NAT translations can be given the IP address of the interface that PfR has selected for the packet.

Note The PfR static routing NAT solution is a single box solution and configurations with interfaces on multiple routers using NAT and managed by PfR are not supported.

```
Router(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Router(config)# route-map isp-2 permit 10BGP permit 10
```

```
Router(config-route-map)# match ip address access-list 1
Router(config-route-map)# match interface serial 2/0
Router(config-route-map)# exit
Router(config)# ip nat pool ISP2 209.165.201.1 209.165.201.30 prefix-length 27
Router(config)# ip nat inside source route-map isp-2 pool ISP2 pfr
Router(config)# interface FastEthernet 3/0
Router(config-if)# ip address 10.1.11.8 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)# exit

Router(config)# interface serial 1/0
Router(config-if)# ip address 192.168.3.1 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# exit

Router(config)# interface serial 2/0
Router(config-if)# ip address 172.17.233.208 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# end
```

Where to Go Next

For information about other Performance Routing features or general conceptual material, see the documents in the “Related Documents” section.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco PfR commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples	Cisco IOS Performance Routing Command Reference
Basic PfR configuration	“Configuring Basic Performance Routing” module
Advanced PfR configuration	“Configuring Advanced Performance Routing” module
Concepts required to understand the Performance Routing operational phases	“Understanding Performance Routing” module
General information about NAT	“Configuring NAT for IP Address Conservation” module
PfR home page with links to PfR-related content on our DocWiki collaborative environment	PfR:Home

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/cisco/web/support/index.html

Feature Information for Performance Routing with NAT

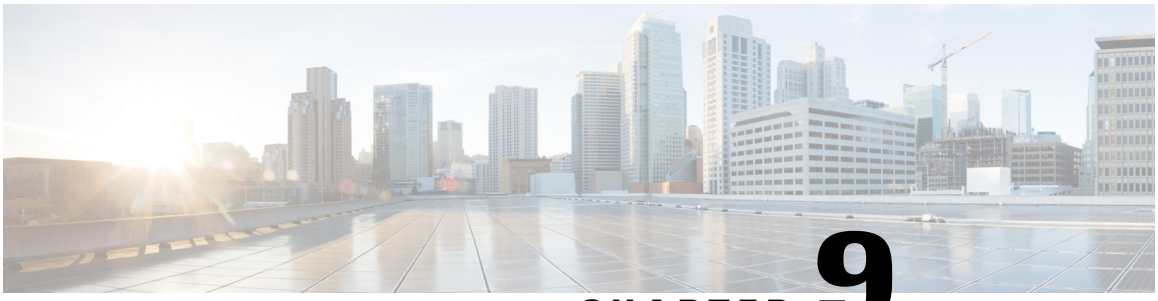
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train 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 10: Feature Information for Performance Routing with NAT

Feature Name	Releases	Feature Information
Support for NAT and Static Routing[6]	12.3(14)T 12.2(33)SRB	Support to allow PfR to control traffic class routing using static routing in networks using NAT. The following command was modified by this feature: **ip nat inside source**.

6 This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.



CHAPTER 9

Performance Routing - Protocol Independent Route Optimization (PIRO)

Protocol Independent Route Optimization (PIRO) introduced the ability of Performance Routing (PfR) to search for a parent route--an exact matching route, or a less specific route--in the IP Routing Information Base (RIB), allowing PfR to be deployed in any IP-routed environment including Interior Gateway Protocols (IGPs) such as OSPF and IS-IS.

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 Table at the end of this document.

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 Performance Routing PIRO

Protocol Independent Route Optimization (PIRO)

The PfR - Protocol Independent Route Optimization (PIRO) feature was introduced to extend the ability of PfR to identify and control traffic classes. Prior to PIRO, PfR optimizes paths for traffic classes that have a parent route--an exact matching route, or a less specific route--in BGP or static route databases. PIRO enables PfR to search the IP Routing Information Base (RIB) for a parent route allowing PfR to be deployed in any IP-routed environment including Interior Gateway Protocols (IGPs) such as OSPF and IS-IS.

The search for a parent route starts in the BGP routing database and, if no parent route is found, the static route database is searched. If a parent route is still not located, the RIB is searched. When a match is found after a parent route search of the RIB, route control is applied to the traffic class using policy-based routing (PBR) where a dynamic route map is created.

After PfR route control mode is enabled, no new customer configuration is required to enable PIRO.

On the master controller the **show pfr master prefix** command will display PIRO routes as “RIB-PBR” in the output.

How to Configure Performance Routing PIRO

Verifying and Debugging Protocol Independent Route Optimization Route Control Changes

After PfR route control mode is enabled, no new customer configuration is required to enable PIRO.Perform the steps in this optional task if you want to debug PIRO routes where the parent route exists in the RIB and is controlled using policy-based routing. All the steps are optional and are not in any order. The information from these steps can verify that a specific prefix associated with a traffic class has been identified using PIRO and that it is being controlled by PfR. The first two CLI commands are entered at the master controller, and the other commands are entered at a border router.

SUMMARY STEPS

1. Start at the master controller.
2. **enable**
3. **show pfr master traffic-class**
4. Move to a border router to enter the next step.
5. **enable**
6. **show ip route**
7. **show route-map dynamic**
8. **show ip access-list dynamic**
9. **debug pfr border routes** {**bgp** | **static** | **piro**[**detail**]}

DETAILED STEPS

Step 1 Start at the master controller.

Step 2 **enable**
Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 3 **show pfr master traffic-class**
This command is used to display information about traffic classes that are monitored and controlled by a PfR master controller. The output from this command includes information about the destination IP address and prefix length for the traffic class, the IP address and the interface of the border router through which the prefix associated with this traffic class is being currently routed, the state of the traffic class, and the protocol. In this example, the protocol displayed for the prefix 10.1.1.0 is RIB-PBR and this means that the parent route for the traffic class exists in the RIB and policy-based routing is being used to control the prefix. Only syntax relevant to this task is shown in this step. You can also use the **show pfr master prefix** command to display similar information.

Example:

```
Router# show pfr master traffic-class

OER Prefix Statistics:
 Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
 P - Percentage below threshold, Jit - Jitter (ms),
 MOS - Mean Opinion Score
 Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
 E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
 U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
 # - Prefix monitor mode is Special, & - Blackholed Prefix
 % - Force Next-Hop, ^ - Prefix is denied
DstPrefix           Appl_ID Dscp Prot     SrcPort     DstPort SrcPrefix
          Flags              State     Time            CurrBR  CurrI/F Protocol
         PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos      EBw      IBw
         ActSDly  ActLDly   ActSUn   ActLUn  ActSJit  ActPMOS  ActSLos  ActLLos
--------------------------------------------------------------------------------
10.1.1.0/24               N defa    N           N           N N
                          INPOLICY        0           10.2.1.2 Gi0/0/1  RIB-PBR
               N        N        N        N        N        N        N        N
               1        1        0        0        N        N        N        N
```

Step 4 Move to a border router to enter the next step.
The next command is entered on a border router, not the master controller.

Step 5 **enable**
Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 6 **show ip route**
Displays the current state of the routing table. Use this command to verify that a parent route exists in the RIB.

Example:

```
Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, GigabitEthernet0/0/1
     192.168.0.0/24 is subnetted, 1 subnets
O       192.168.50.0 [110/20] via 10.10.10.3, 00:20:32, GigabitEthernet0/2/2
     10.0.0.0/8 is variably subnetted, 10 subnets, 4 masks
O       10.1.4.1/32 [110/31] via 10.40.40.2, 00:20:32, GigabitEthernet0/0/2
O       10.1.5.1/32 [110/31] via 10.40.40.2, 00:20:32, GigabitEthernet0/0/2
O       10.1.6.1/32 [110/31] via 10.40.40.2, 00:20:32, GigabitEthernet0/0/2
B       10.1.1.0/24 [20/0] via 10.40.40.2, 00:38:08
     10.1.0.0/24 is subnetted, 1 subnets
O       10.1.1.0 [110/40] via 10.40.40.2, 00:20:33, GigabitEthernet0/0/2
```

Step 7 **show route-map dynamic**

Viewing a dynamic route map is another method of verifying how the route control is being applied for PIRO routes. In the output of this dynamic route map, note the access list named pfr#6. Only syntax relevant to this task is shown in this step.

Example:

```
Router# show route-map dynamic

 route-map OER-04/21/09-21:42:55.543-6-OER, permit, sequence 0, identifier 1755354068
  Match clauses:
    ip address (access-lists): pfr#6
  Set clauses:
    ip next-hop 10.40.40.2
    interface GigatbitEthernet0/0/2
  Policy routing matches: 2314 packets, 138840 bytes
 Current active dynamic routemaps = 1
```

Step 8 **show ip access-list dynamic**

This command displays dynamic IP access lists created on this border router. In the output, a dynamic access list named pfr#6, that permits traffic for the prefix 10.1.1.0 to be routed through this border router, is displayed. The access list, pfr#6, was identified in the **show route-map dynamic** command in the previous step. Only syntax relevant to this task is shown in this step.

Example:

```
Router# show ip access-list dynamic

Extended IP access list pfr#6
    1073741823 permit ip any 10.1.1.0 0.0.0.255 (2243 matches)
```

Step 9 **debug pfr border routes** {**bgp** | **static** | **piro**[**detail**]}

This command is entered on a border router. This command is used to debug parent route lookup and route changes to existing parent routes when the parent route is identified from the RIB. In this example, the detailed debugging information

shows that the parent route for the prefix 10.1.1.0--shown in the output for Step 2--is found in the RIB and a route map is created to control the application. Note that static and BGP route control, and detailed border PBR debugging is also active.

Example:

```
Router# debug pfr border routes piro detail

Apr 21 21:41:25.667: PFR PIRO: Parent lookup found parent 10.1.1.0, mask 24, nexthop
10.40.40.2
Apr 21 21:42:55.539: OER STATIC: No parent found, network 10.1.1.0/24
Apr 21 21:42:55.539: PFR PIRO: Control Route, 10.1.1.0/24, NH 0.0.0.0,
IF GigabitEthernet0/0/2
Apr 21 21:42:55.539: PFR PIRO: Parent lookup found parent 10.1.1.0, mask 24, nexthop
10.40.40.2
Apr 21 21:42:55.539: OER BR PBR(det): control app: 10.1.1.0/24, nh 0.0.0.0, if
GigabitEthernet0/0/2,ip prot 256,dst opr 0,src opr 0, 0 0 0 0,rc net 0.0.0.0/0,dscp 0/0
Apr 21 21:42:55.543: OER BR PBR(det): Create rmap 65DC1CE8
Apr 21 21:42:55.547: PFR PIRO: Parent lookup found parent 10.1.1.0, mask 24, nexthop
10.40.40.2
```

Where to Go Next

For information about other Performance Routing features or general conceptual material, see the documents in the “Related Documents” section.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco PfR commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples	Cisco IOS Performance Routing Command Reference
Basic PfR configuration	"Configuring Basic Performance Routing" module
Concepts required to understand the Performance Routing operational phases	"Understanding Performance Routing" module
Advanced PfR configuration	"Configuring Advanced Performance Routing" module
IP SLAs overview	*IP SLAs Configuration Guide*

Related Topic	Document Title
PfR home page with links to PfR-related content on our DocWiki collaborative environment	PfR:Home

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

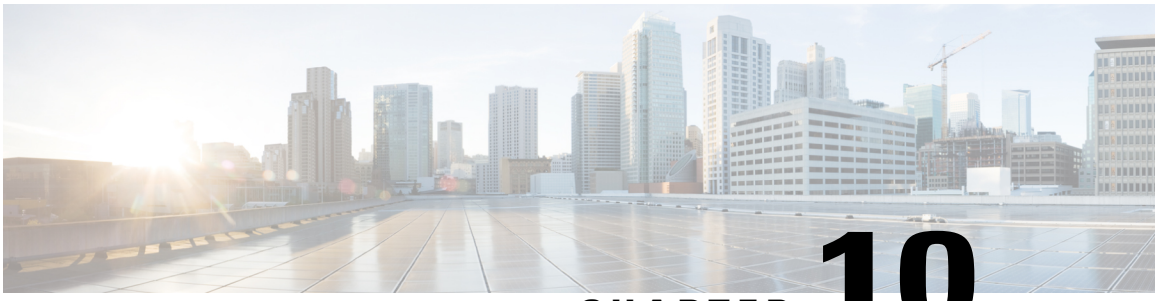
Feature Information for Performance Routing PIRO

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 11: Feature Information for Performance Routing PIRO

Feature Name	Releases	Feature Information
PfR - Protocol Independent Route Optimization (PIRO)	12.2(33)SRE 12.4(24)T	PIRO introduced the ability of PfR to search for a parent route--an exact matching route, or a less specific route--in the IP Routing Information Base (RIB), allowing PfR to be deployed in any IP-routed environment including Interior Gateway Protocols (IGPs) such as OSPF and IS-IS. The following commands were modified by this feature: **debug pfr border routes**and **show pfr master prefix**.



CHAPTER 10

PfR Simplification Phase 1

Performance Routing (PfR) is an advanced Cisco technology to allow businesses to complement traditional IP routing technologies such as Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Routing Information Protocol Version 2 (RIPv2), and Border Gateway Protocol (BGP) with additional serviceability parameters to select the best egress or ingress path. It complements these traditional IP routing technologies with additional intelligence. PfR can select an egress or ingress WAN interface based upon parameters like reachability, delay, cost, jitter, Mean Opinion Score (MOS) score, or it can use interface parameters like load, throughput, and monetary cost. Traditional IP routing technologies generally focus on creating a loop-free topology based upon the shortest or least cost path.

Although PfR automatically enables IP SLA or NetFlow technologies, the initial configuration of PfR is more complicated than for traditional IP routing technologies due to PfR policy definition and the setting of many performance parameters. Cisco used feedback from customers to reduce the complexity of PfR configuration and align default values to match customer requirements. Phase 1 of the PfR simplification project introduces dynamic tunnels between PfR border routers, revised default values, removal of some CLI, and changes to default behavior. The changes result in fewer configuration steps before PfR is implemented in your network.

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 Table at the end of this document.

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 PfR Simplification Phase 1

CLI and Default Value Changes to Simplify PfR

With CSCtr26978 a series of CLI and default value changes designed to make configuration of PfR simpler were introduced. Some commands and keywords were removed, and defaults changed to reflect customer environments.

Enforce Route Control by Default

In response to customer feedback, with CSCtr26978 the **mode route control** command is now the default behavior instead of the **mode route observe** command. In control mode, the master controller coordinates information from the border routers and makes policy decisions. The master controller monitors prefixes and exits based on default and user-defined policies, and implements changes to optimize prefixes and to select the best exit.

If you want to passively monitor and report without making any changes, you can still configure PfR to use the observe mode. In observe mode, the master controller monitors prefixes and exit links based on default and user-defined policies and then reports the status of the network and the decisions that should be made, but it does not implement any changes.

Default Change for Mode Verify Bidirectional CLI

In response to customer feedback, with CSCtr26978 the default behavior changed to disable the verification of bidirectional traffic. If you need to verify bidirectional traffic, configure the **mode verify bidirectional** command in master controller configuration mode.

CLI Default Value Changes to Simplify PfR

Command	Default Before CSCtr26978	Default After CSCtr26978
backoff	300, 3000, 300 seconds	90, 900, 90 seconds
holddown	300 seconds	90 seconds
max-xmit-utilization	75 percent	90 percent
monitor-period	5 minutes	1 minute
periodic-interval	120 minutes	0 minutes

Removal of PfR API and Proxy CLI

All CLI commands and functionality involved with the PfR application programming interface (API) and proxy process were removed to simplify PfR. With CSCtr26978, the following CLI commands were removed:

- **api provider (PfR)**
- **debug pfr api**

- **host-address (PfR)**
- **show api provider (PfR)**
- **show pfr proxy**

Removal of OER CLI

Although the Optimized Edge Routing (OER) syntax was replaced in most images with the PfR syntax, the OER syntax is still recognized. When you enter OER syntax the software changes the syntax to the new PfR syntax in the running configuration. With CSCtr26978, the OER syntax was removed.

Removal of Mode Select-Exit CLI

For most customer deployments we do not recommend using the passive monitoring mode with the exit selection of select-exit best because the statistics may change by the time all the links have been examined and the decision may not be accurate. To simplify the PfR configuration, with CSCtr26978 the default behavior is now select-exit good where the first in-policy link is selected. The **mode select-exit** command and **best** and **good** keywords have been removed.

Load Balancing With Link Groups and Resolver Changes

With CSCtr33991 changes were introduced to the PfR link group and resolver behaviors to simplify the configuration and understanding of PfR. The limitation of configuring a range resolver and link grouping at the same time was removed. Without any awareness of link group configuration, load balancing was performed across all the links. Link groups provide the ability to define a group of exit links as a preferred set of links, or a fallback set of links for PfR to use when optimizing traffic classes specified in a PfR policy.

To further simplify PfR, CSCtr33991 changed the behavior where range resolvers are considered after performance resolvers (such as delay, throughput, or loss).

Note The cost resolver cannot be configured with a performance resolver.

Delay, Range, and Utilization Resolver Changes

Before CSCtr3399	After CSCtr3399
Support of utilization and range resolvers.	With CSCtr33991, the **range** and **utilization** keywords in the **resolve** and **set resolve** commands were removed to disable support for the utilization and range resolvers.
Delay, range, and utilization resolvers are the default resolvers in the default global policy.	PfR automatically performs load balancing; default resolvers were removed from the default global policy.

Performance Resolver and Link Group Load Balancing

Before PfR performs load balancing traffic across available exits, rules to consider configured performance resolvers (such as delay or loss) and any configured link group were introduced with CSCtr33991. The rules are evaluated in the following order:

1. If no performance resolver is configured and no link group is used, PfR automatically performs load balancing across all links.
2. If no performance resolver is configured but link group is used, PfR automatically performs load balancing within the primary link group.
3. If performance resolvers are configured but no link group is used, PfR automatically performs load balancing across qualified links after those performance resolvers.
4. If performance resolvers are configured and a link group is used, PfR automatically performs load balancing across qualified links within the primary link group.

Load Balancing Within a Link Group

With CSCtr33991, the behavior of triggering range out-of-policy (OOP) for an exit by comparing the load of an exit to all other exits, is changed to comparing the load of an exit with all the exits in the same link group.

The maximum utilization (soft limit) of all the PfR-managed exit links is checked before PfR calls a resolver and, if none of the exits is below the soft limit, the exit selection is performed by ignoring the soft limit.

The existing behavior of moving any traffic class to balance the traffic load has been replaced by the ability to move any traffic class in the link group (whether primary or fallback) to balance the traffic load.

When any performance resolver is configured, the following rules apply in the specified order:

1. If only one qualified link is in the primary group, move traffic classes to this link.
2. If more than one qualified link is in the primary group, move traffic classes and perform load balancing across these links.
3. If more than one qualified link is in the fallback group, move traffic classes to one of the fallback group links.
4. If no qualified link is in both the primary and fallback groups, do not move the traffic class.
5. If no links are under the maximum utilization (soft limit) in the primary or fallback link groups, ignore the soft limit and move traffic classes to the best link.

When no performance resolver is configured, the following rules apply in the specified order:

1. If one or more qualified links are under the maximum utilization in the primary group, perform load balancing across these links in the primary group.
2. If more than one qualified link is in the fallback group, move traffic classes to one of the fallback group links.
3. If no links are under the maximum utilization (soft limit) in the primary or fallback link groups, perform load balancing across the primary group links.

Automatic Enable of Throughput Learning

To simplify PfR configuration, CSCtr2697 enabled PfR learn mode using throughput-based learning by default.

After feedback from customers, the default periodic interval of 120 minutes was changed to 90 minutes and the default monitor period was changed from 5 minutes to 1 minute.

The automatic enabling of PfR learn mode can be switched off using the **no learn** command if manual configuration is preferred.

Automatic PBR Route Control When No Parent Route Exists

When a PfR master controller (MC) decides to control a prefix using a protocol BGP, for example, it sends the control request to a selected PfR border router (BR). If the MC receives the successful control notification from the BR, it will notify all the other BRs to exclude the prefix. Some BRs may not have a parent route to this prefix via the same protocol. When no parent route exists for the prefix, this is detected as a RIB mismatch, the prefix is moved into a default state, and the control procedure begins again.

To simplify PfR, CSCtr26978 introduced new behavior when no parent route is detected. In this situation, PfR automatically switches to using dynamic policy-based routing (PBR) instead of trying all the other routing protocols in the following order; BGP, EIGRP, static, and PBR. With CSCtr26978, the existing **mode route protocol pbr** command behavior was enabled by default. Configuration of the **no mode route protocol pbr** command initially sets the traffic classes to be uncontrolled and PfR then uses a single protocol to control the traffic class in the following order: BGP, EIGRP, static, and PBR.

Dynamic PBR Support for PfR

The PfR BR Automatic Adjacencies feature introduces dynamic PBR support. In dynamic route maps, the PBR requirement for both interface and next-hop information is now supplied by PfR in a single set clause. To display the route map or policy information use the **show route-map dynamic** command or the **show ip policy** command.

How to Configure PfR Simplification Phase 1

Enabling PfR Route Observe Mode

With CSCtr26978, the **mode route control** command behavior is the default. Perform this task at the master controller to configure PfR to use route observe mode instead of the default route control mode. In route observe mode, the master controller monitors prefixes and exit links based on default and user-defined policies and then reports the status of the network and the decisions that should be made, but it does not implement any changes. In route control mode, the master controller coordinates information from the borders routers in the same way as route observe mode, but commands are sent back to the border routers to alter routing in the PfR managed network to implement the policy decisions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **mode route observe**
5. **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.
Step 3	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure a router as a master controller and to configure global operations and policies.
Step 4	**mode route observe** **Example:** `Router(config-pfr-mc)# mode route observe`	Configures PfR to passively monitor and report without making any changes.
Step 5	**end** **Example:** `Router(config-pfr-mc)# end`	Exits PfR master controller configuration mode and returns to privileged EXEC mode.

Disabling Automatic PBR Route Control

Perform this task at the master controller to disable the default route control behavior when a RIB mismatch is found and allow PfR to use a single protocol to control a traffic class.

Note With CSCtr26978, the **no mode route protocol pbr** command behavior is enabled by default. Perform this task to override the default behavior.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **no mode route protocol pbr**
5. **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.
Step 3	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure a router as a master controller and to configure global operations and policies.
Step 4	**no mode route protocol pbr** **Example:** `Router(config-pfr-mc)# no mode route protocol pbr`	Disables the automatic PBR route control. • Sets the traffic classes to be uncontrolled and PfR then uses a single protocol to control the traffic class in the following order; BGP, EIGRP, static, and PBR.
Step 5	**end** **Example:** `Router(config-pfr-mc)# end`	Exits PfR master controller configuration mode and returns to privileged EXEC mode.

Configuration Examples for PfR Simplification Phase 1

Example: Verifying PfR Simplification Default Changes

The following example outputs, from privileged EXEC mode, display the new default values and behavior introduced to simplify PfR.

The following partial output shows the default behavior introduced with CSCtr26978; the backoff timer values are 90, 900, and 90 seconds, hold-down is set to 90 seconds, mode route control is enabled, and mode select-exit best is removed.

```
.
.
.
Default Policy Settings:
  backoff 90 900 90
  delay relative 50
  holddown 90
  periodic 0
  probe frequency 56
  number of jitter probe packets 100
  mode route control
  mode monitor both
  loss relative 10
  jitter threshold 20
  mos threshold 3.60 percent 30
  unreachable relative 50
  resolve delay priority 11 variance 20
  resolve range priority 12 variance 0
  resolve utilization priority 13 variance 20
.
.
.
```

The following partial output shows the new default behavior introduced with CSCtr26978; learn mode is enabled, the monitor period is set to 1 minute, and the periodic interval is set to 0 minutes:

```
.
.
.
Learn Settings:
  current state : ENABLED
  time remaining in current state : 0 seconds
  throughput
  no delay
  no inside bgp
  monitor-period 1
  periodic-interval 0
  aggregation-type prefix-length 24
  prefixes 100 appls 100
  expire after time 720
```

Additional References for PfR

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco PfR commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS Performance Routing Command Reference
Basic PfR configuration	"Configuring Basic Performance Routing" module
Concepts required to understand the Performance Routing operational phases	"Understanding Performance Routing" module
Advanced PfR configuration	"Configuring Advanced Performance Routing" module
PfR home page with links to PfR-related content on our DocWiki collaborative environment	PfR:Home

MIBs

MIB	MIBs Link
CISCO-PFR-MIB CISCO-PFR-TRAPS-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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

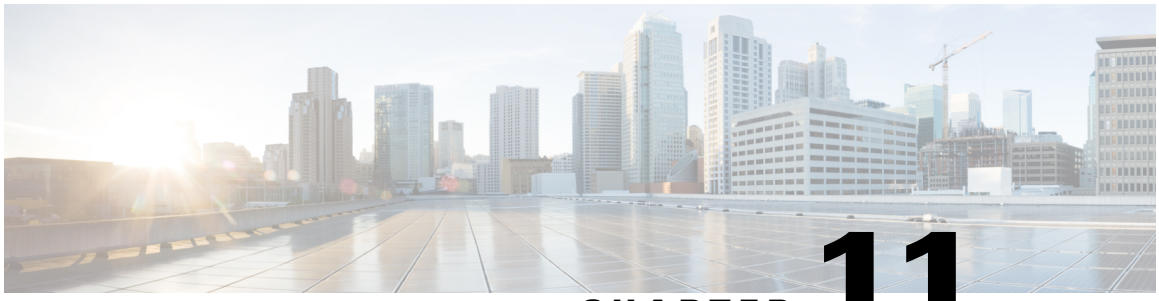
Feature Information for PfR Simplification Phase 1

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 12: Feature Information for PfR Simplification Phase 1

Feature Name	Releases	Feature Information
PfR BR Automatic Adjacencies	15.2(2)S 15.2(3)T Cisco IOS XE Release 3.6S	The PfR BR Automatic Adjacencies feature introduces dynamic PBR support. In dynamic route maps, the PBR requirement for both interface and next-hop information is supplied by PfR in a single set clause. No commands were introduced or modified.



CHAPTER 11

Static Application Mapping Using Performance Routing

The OER - Application Aware Routing with Static Application Mapping feature introduces the ability to configure standard applications using just one keyword to simplify the configuration of traffic classes that PfR can automatically learn, or that can be manually configured. This feature also introduces a learn list configuration mode that allows Performance Routing (PfR) policies to be applied to traffic classes profiled in a learn list. Different policies can be applied to each learn list.

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 Table at the end of this document.

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.

PrerequisitesforStaticApplicationMappingUsingPerformance Routing

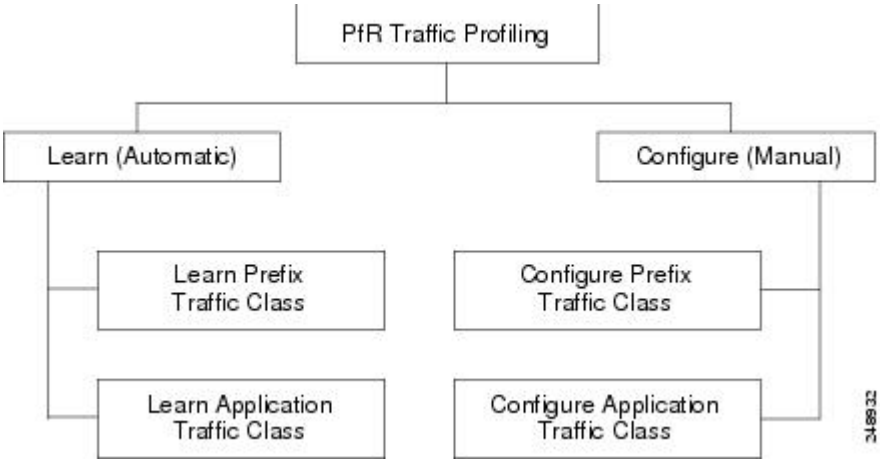
Cisco Express Forwarding (CEF) must be enabled on all participating devices. No other switching path is supported, even if otherwise supported by Policy-Based Routing (PBR).

Information About Static Application Mapping Using Performance Routing

Performance Routing Traffic Class Profiling

Before optimizing traffic, Performance Routing (PfR) must determine the traffic classes from the traffic that is flowing through the border routers. To optimize traffic routing, subsets of the total traffic must be identified; and these traffic subsets are named traffic classes. The list of traffic-class entries is named a Monitored Traffic Class (MTC) list. The entries in the MTC list can be profiled either by automatically learning the traffic flowing through the device or by manually configuring the traffic classes. Learned and configured traffic classes can both exist in the MTC list at the same time. Both the learn mechanism and the configure mechanism for traffic classes are implemented during the PfR profile phase. The overall structure of the PfR traffic class profile process and its components can be seen in the figure below.

Figure 16: PfR Traffic Class Profiling Process



PfR can automatically learn the traffic classes while monitoring the traffic flow through border routers using the embedded NetFlow capability. Although the goal is to optimize a subset of the traffic, you may not know all the exact parameters of this traffic, and PfR provides a method to automatically learn the traffic and create traffic classes by populating the MTC list. Within the automatic traffic class learning process, there are three components:

- Automatic learning of prefix-based traffic classes

- Automatic learning of application-based traffic classes
- Using learn lists to categorize both prefix-based and application-based traffic classes

PfR can be manually configured to create traffic classes for monitoring and subsequent optimizing. Automatic learning generally uses a default prefix length of /24, but manual configuration allows exact prefixes to be defined. Within the manual traffic class configuration process, there are two components:

- Manually configuring prefix-based traffic classes
- Manually configuring application-based traffic classes

The ultimate objective of the profile phase is to select a subset of traffic that is flowing through the network. This subset of traffic—the traffic classes in the MTC list—represents the classes of traffic that must be routed based on the best-performance path available.

More details about each of the traffic class profiling components in the figure above are contained in the "Understanding Performance Routing" module.

Static Application Mapping Using PfR

The OER - Application Aware Routing with Static Application Mapping feature introduced the ability to define an application using a keyword to simplify the configuration of application-based traffic classes. PfR uses well-known applications with fixed ports, and more than one application may be configured at the same time. The list of static applications available for profiling Performance Routing traffic classes is constantly evolving. Use the **traffic-class application ?** command to determine if a static application is available for use with Performance Routing.

The table below displays a partial list of static applications that can be configured with Performance Routing. The applications are considered static because they are defined with fixed port and protocols as shown in the table. Configuration is performed on a master controller under learn list configuration mode.

Table 13: Static Application List

Application	Keyword	Protocol	Port
CU-SeeMe-Server --CU-SeeMe desktop video conference	**cuseeme**	TCP UDP	7648 7649 7648 7649 24032
DHCP-Client --Dynamic Host Configuration Protocol client	**dhcp (Client)**	UDP/TCP	68
DHCP-Server --Dynamic Host Configuration Protocol server	**dhcp (Server)**	UDP/TCP	67
DNS --Domain Name Server lookup	**dns**	UDP/TCP	53
FINGER-Server --Finger server	**finger**	TCP	79

Application	Keyword	Protocol	Port
FTP --File Transfer Protocol	**ftp**	TCP	20, 21
GOPHER-Server --Gopher server	**gopher**	TCP/UDP	70
HTTP-- Hypertext Transfer Protocol, World Wide Web traffic	**http**	TCP/UDP	80
HTTPSSL-Server-- Hypertext Transfer Protocol over TLS/SSL, Secure World Wide Web traffic server	**secure-http**	TCP	443
IMAP-Server --Internet Message Access Protocol server	**imap**	TCP/UDP	143 220
SIMAP-Server --Secure Internet Message Access Protocol server	**secure-imap**	TCP/UDP	585 993 (Preferred)
IRC-Server --Internet Relay Chat server	**irc**	TCP/UDP	194
SIRC-Server --Secure Internet Relay Chat server	**secure-irc**	TCP/UDP	994
Kerberos-Server --Kerberos server	**kerberos**	TCP/UDP	88 749
L2TP-Server --L2F/L2TP tunnel Layer 2 Tunnel Protocol server	**l2tp**	UDP	1701
LDAP-Server --Lightweight Directory Access Protocol server	**ldap**	TCP/UDP	389
SLDAP-Server --Secure Lightweight Directory Access Protocol server	**secure-ldap**	TCP/UDP	636
MSSQL-Server --MS SQL server	**mssql**	TCP	1443

Application	Keyword	Protocol	Port
NETBIOS-Server --NETBIOS server	**netbios**	UDP TCP	137 138 137 139
NFS-Server --Network File System server	**nfs**	TCP/UDP	2049
NNTP-Server --Network News Transfer Protocol	**nntp**	TCP/UDP	119
SNNTP-Server --Network News Transfer Protocol over TLS/SSL	**secure-nntp**	TCP/UDP	563
NOTES-Server --Lotus Notes server	**notes**	TCP/UDP	1352
NTP-Server --Network Time Protocol server	**ntp**	TCP/UDP	123
PCanywhere-Server --Symantec pcANYWHERE	**pcany**	UDP TCP	22 5632 65301 5631
POP3-Server --Post Office Protocol server	**pop3**	TCP/UDP	110
SPOP3-Server --Post Office Protocol over TLS/SSL server	**secure-pop3**	TCP/UDP	123
PPTP-Server --Point-to-Point Tunneling Protocol server	**pptp**	TCP	17233
SSH --Secured Shell	**ssh**	TCP	22
SMTP-Server --Simple Mail Transfer Protocol server	**smtp**	TCP	25
Telnet --Telnet	**telnet**	TCP	23

The master controller is configured to learn the top prefixes based on highest outbound throughput or delay for the filtered traffic, and the resulting traffic classes are added to the PfR application database to be passively and actively monitored.

Learn List Configuration Mode

The Learn List feature introduced a new configuration mode named learn list. Learn lists are a way to categorize learned traffic classes. In each learn list, different criteria including prefixes, application definitions, filters, and aggregation parameters for learning traffic classes can be configured. A traffic class is automatically learned by PfR based on each learn list criteria, and each learn list is configured with a sequence number. The sequence number determines the order in which learn list criteria are applied. Learn lists allow different PfR policies to be applied to each learn list; in previous releases, the traffic classes could not be divided, and an PfR policy was applied to all the learned traffic classes.

Four types of traffic classes--to be automatically learned or manually configured--can be profiled:

- Traffic classes based on destination prefixes
- Traffic classes representing custom application definitions using access lists
- Traffic classes based on a static application mapping name with optional prefix lists to define destination prefixes

The **traffic-class** commands are used under learn list mode to simplify the automatic learning of traffic classes. Only one type of **traffic-class** command can be specified per learn list, and the **throughput** (PfR) and **delay** (PfR) commands are also mutually exclusive within a learn list.

The **match traffic-class** commands are used under PfR map configuration mode to simplify the manual configuration of traffic classes. Only one type of **match traffic-class** command can be specified per PfR map.

Note In addition to profiling the traffic and configuring the learn list parameters, the learn list must be referenced in a PfR policy using a PfR map and the **match pfr learn** command with the **list** keyword. To activate the policy, the **policy-rules** (PfR) command must be used.

How to Configure Static Application Mapping Using Performance Routing

Defining a Learn List to Automatically Learn Traffic Classes Using Static Application Mapping

Perform this task at the master controller to define a learn list using static application mapping. Within a learn list, a keyword that represents an application can be used to identify specific application traffic classes. The defined learn list will contain traffic classes to be automatically learned by PfR using the static application mapping. The resulting traffic classes can be filtered by a prefix list, if required.

In this task, a learn list is configured to create a traffic class using static application mapping keywords. Learn lists allow different PfR policies to be applied to each learn list. The resulting prefixes are aggregated to a prefix length of 24. A prefix list is applied to the traffic class to permit traffic from the 10.0.0.0/8 prefix. The master controller is configured to learn the top prefixes based on highest outbound throughput for the filtered traffic, and the resulting traffic class is added to the PfR application database.

The learn list is referenced in a PfR policy using a PfR map and activated using the **policy-rules** (PfR) command.

To display information about the configured learn lists and the traffic classes learned by PfR, use the "Displaying and Resetting Traffic Class and Learn List Information" section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length* }
4. **pfr master**
5. **policy-rules** *map-name*
6. **learn**
7. **list seq** *number* **refname** *refname*
8. **traffic-class application** *application-name...* [**filter** *prefix-list-name*]
9. **aggregation-type** {**bgp non-bgp prefix-length**} *prefix-mask*
10. **throughput**
11. **exit**
12. Repeat Step 7 to Step 11 to configure additional learn lists
13. **exit**
14. Repeat Step 13 to return to global configuration mode.
15. **pfr-map** *map-name sequence-number*
16. **match pfr learn list** *refname*
17. **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.
Step 3	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length* }	Creates an IP prefix list to filter prefixes for learning. • An IP prefix list is used under learn list configuration mode to filter IP addresses that are learned.

	Command or Action	Purpose
	Example: `Router(config)# ip prefix-list INCLUDE_10_NET permit 10.0.0.0/8`	• The example creates an IP prefix list named INCLUDE_10_NET for PfR to profile the prefix, 10.0.0.0/8.
Step 4	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure a Cisco router as a master controller and to configure master controller policy and timer settings.
Step 5	**policy-rules** *map-name* **Example:** `Router(config-pfr-mc)# policy-rules LL_REMOTE_MAP`	Selects a PfR map and applies the configuration under PfR master controller configuration mode. • Use the *map-name* argument to specify the PfR map name to be activated. • The example applies the PfR map named LL_REMOTE_MAP that includes the learn list configured in this task.
Step 6	**learn** **Example:** `Router(config-pfr-mc)# learn`	Enters PfR Top Talker and Top Delay learning configuration mode to automatically learn traffic classes.
Step 7	**list seq** *number* **refname** *refname* **Example:** `Router(config-pfr-mc-learn)# list seq 10 refname LEARN_REMOTE_LOGIN_TC`	Creates an PfR learn list and enters learn list configuration mode. • Use the **seq** keyword and *number* argument to specify a sequence number used to determine the order in which learn list criteria is applied. • Use the **refname** keyword and *refname* argument to specify a reference name for the learn list. • The example creates a learn list named LEARN_REMOTE_LOGIN_TC.
Step 8	**traffic-class application** *application-name...* [**filter** *prefix-list-name*] **Example:** `Router(config-pfr-mc-learn-list)# traffic-class application telnet ssh`	Defines an PfR traffic class using a pre-defined static application. • Use the *application-name* argument to specify one or more keywords that represent pre-defined static applications. The ellipses are used to show that more than one application keyword can be specified. • The example defines a traffic class as containing telnet and ssh traffic.
Step 9	**aggregation-type** {**bgp non-bgp prefix-length**} *prefix-mask*	(Optional) Configures a master controller to aggregate learned prefixes based on traffic flow type.

	Command or Action	Purpose
	Example: `Router(config-pfr-mc-learn-list)# aggregation-type prefix-length 24`	• The **bgp** keyword configures prefix aggregation based on entries in the BGP routing table. This keyword is used if BGP peering is enabled in the network. • The **non-bgp** keyword configures learned prefix aggregation based on static routes. Entries in the BGP routing table are ignored when this keyword is entered. • The **prefix-length** keyword configures aggregation based on the specified prefix length. The range of values that can be configured for this argument is a prefix mask from 1 to 32. • If this command is not specified, the default aggregation is performed based on a /24 prefix length. • The example configures prefix length aggregation based on a /24 prefix length.
Step 10	**throughput** **Example:** `Router(config-pfr-mc-learn-list)# throughput`	Configures the master controller to learn the top prefixes based on the highest outbound throughput. • When this command is enabled, the master controller will learn the top prefixes across all border routers according to the highest outbound throughput. • The example configures a master controller to learn the top prefixes based on highest outbound throughput for the LEARN_REMOTE_LOGIN_TC traffic class.
Step 11	**exit** **Example:** `Router(config-pfr-mc-learn-list)# exit`	Exits learn list configuration mode, and returns to PfR Top Talker and Top Delay learning configuration mode.
Step 12	Repeat Step 7 to Step 11 to configure additional learn lists	--
Step 13	**exit** **Example:** `Router(config-pfr-mc-learn)# exit`	Exits PfR Top Talker and Top Delay learn configuration mode, and returns to PfR master controller configuration mode.
Step 14	Repeat Step 13 to return to global configuration mode.	--
Step 15	**pfr-map** *map-name sequence-number*	Enters PfR map configuration mode to configure a PfR map.

	Command or Action	Purpose
	Example: `Router(config)# pfr-map LL_REMOTE_MAP 10`	• Only one match clause can be configured for each PfR map sequence. • The example creates a PfR map named LL_REMOTE_MAP.
Step 16	**match pfr learn list** *refname* **Example:** `Router(config-oer-map)# match pfr learn list LEARN_REMOTE_LOGIN_TC`	Creates a match clause entry in a PfR map to match PfR learned prefixes. • The example defines a traffic class using the criteria defined in the PfR learn list named LEARN_REMOTE_LOGIN_TC. **Note** Only the syntax relevant to this task is used here.
Step 17	**end** **Example:** `Router(config-oer-map)# end`	(Optional) Exits OER map configuration mode and returns to privileged EXEC mode.

Example

In this example, two learn lists are configured to identify remote login traffic and file transfer traffic. The remote login traffic class is configured using keywords representing Telnet and Secure Shell (SSH) traffic, and the resulting prefixes are aggregated to a prefix length of 24. The file transfer traffic class is configured using a keyword that represents FTP and is also aggregated to a prefix length of 24. A prefix list is applied to the file transfer traffic class to permit traffic from the 10.0.0.0/8 prefix. The master controller is configured to learn the top prefixes based on highest outbound throughput for the filtered traffic, and the resulting traffic classes are added to the PfR application database. PfR maps are configured to match the learn lists and the File Transfer traffic class is activated using the **policy-rules** (PfR) command.

```
ip prefix-list INCLUDE_10_NET 10.0.0.0/8
pfr master
 policy-rules LL_FILE_MAP
 learn
  list seq 10 refname LEARN_REMOTE_LOGIN_TC
   traffic-class application telnet ssh
   aggregation-type prefix-length 24
   throughput
   exit
  list seq 20 refname LEARN_FILE_TRANSFER_TC
   traffic-class application ftp filter INCLUDE_10_NET
   aggregation-type prefix-length 24
   throughput
   exit
  exit
 exit
pfr-map LL_REMOTE_MAP 10
 match pfr learn list LEARN_REMOTE_LOGIN_TC
 exit
pfr-map LL_FILE_MAP 20
 match pfr learn list LEARN_FILE_TRANSFER_TC
 end
```

Manually Selecting Traffic Classes Using Static Application Mapping

Perform this task to manually select traffic classes using static application mapping. Use this task when you know the destination prefixes and the applications that you want to select for the traffic classes. In this task, an IP prefix list is created to define the destination prefixes, and static applications are defined using the **match traffic-class application** (PfR) command. Using a PfR map, each prefix is matched with each application to create the traffic classes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*}
4. Repeat Step 3 for more prefix list entries, as required.
5. **pfr-map** *map-name sequence-number*
6. **match traffic-class application** *application-name* **prefix-list** *prefix-list-name*
7. **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.
Step 3	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} **Example:** `Router(config)# ip prefix-list LIST1 permit 10.1.1.0/24`	Creates a prefix list to specify destination prefix-based traffic classes. • The example specifies a destination prefix of 10.1.1.0/24 to be used to filter application traffic classes.
Step 4	Repeat Step 3 for more prefix list entries, as required.	--
Step 5	**pfr-map** *map-name sequence-number* **Example:** `Router(config)# pfr-map APPLICATION_MAP 10`	Enters PfR map configuration mode to configure a PfR map. • Only one match clause can be configured for each PfR map sequence.

	Command or Action	Purpose
		• Permit sequences are first defined in an IP prefix list and then applied with the **match traffic-class** command in Step 6. • The example creates a PfR map named APPLICATION_MAP.
Step 6	**match traffic-class application** *application-name* **prefix-list** *prefix-list-name* **Example:** `Router(config-pfr-map)# traffic-class application telnet ssh prefix-list LIST1`	Manually configures one or more static applications as match criteria against a prefix list to create traffic classes using a PfR map. • Use the *application-name* argument to specify one or more keywords that represent pre-defined static applications. • The example defines traffic classes as application X with destination prefix Y, where X is Telnet or Secure Shell and Y is a destination address defined in the IP prefix list named LIST1.
Step 7	**end** **Example:** `Router(config-pfr-map)# end`	(Optional) Exits PfR map configuration mode and returns to privileged EXEC mode.

Displaying and Resetting Traffic Class and Learn List Information

Perform this task to display traffic class and learn list information and optionally, to reset some traffic class information. These commands can be entered on a master controller after learn lists are configured and traffic classes are automatically learned, or when traffic classes are manually configured using a PfR map. The commands can be entered in any order and all the commands are optional.

SUMMARY STEPS

1. **enable**
2. **show pfr master traffic-class** [**access-list** *access-list-name*| **application** *application-name*[*prefix*] | **inside** | **learned**[**delay** | **inside** | **list** *list-name*| **throughput**] | **prefix** *prefix*| **prefix-list** *prefix-list-name*] [**active**| **passive**| **status**] [**detail**]
3. **show pfr master learn list** [*list-name*]
4. **clear pfr master traffic-class** [**access-list** *access-list-name*| **application** *application-name*[*prefix*]| **inside** | **learned**[**delay** | **inside** | **list** *list-name*| **throughput**]| **prefix** *prefix*| **prefix-list** *prefix-list-name*]

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 2 **show pfr master traffic-class** [**access-list** *access-list-name*| **application** *application-name*[*prefix*] | **inside** | **learned**[**delay** | **inside** | **list** *list-name*| **throughput**] | **prefix** *prefix*| **prefix-list** *prefix-list-name*] [**active**| **passive**| **status**] [**detail**]

This command is used to display information about traffic classes learned or manually configured under PfR learn list configuration mode.

Example:

```
Router# show pfr master traffic-class
OER Prefix Statistics:
 Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
 P - Percentage below threshold, Jit - Jitter (ms),
 MOS - Mean Opinion Score
 Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
 E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
 U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
 # - Prefix monitor mode is Special, & - Blackholed Prefix
 % - Force Next-Hop, ^ - Prefix is denied

DstPrefix           Appl_ID Dscp Prot     SrcPort     DstPort SrcPrefix
          Flags              State     Time            CurrBR  CurrI/F Protocol
         PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos      EBw      IBw
         ActSDly  ActLDly   ActSUn   ActLUn  ActSJit  ActPMOS
--------------------------------------------------------------------------------
10.1.1.0/24               N defa    N           N           N N
               #          OOPOLICY       32         10.11.1.3  Gi0/0/1      BGP
              N        N        N        N        N        N        N      IBwN
            130      134        0        0        N        N
```

Step 3 **show pfr master learn list** [*list-name*]

This command is used to display one or all of the configured PfR learn lists. In this example, the information about two learn lists is displayed.

Example:

```
Router# show pfr master learn list
Learn-List LIST1 10
   Configuration:
    Application: ftp
    Aggregation-type: bgp
    Learn type: thruput
    Policies assigned: 8 10
   Stats:
    Application Count: 0
    Application Learned:
 Learn-List LIST2 20
   Configuration:
    Application: telnet
    Aggregation-type: prefix-length 24
    Learn type: thruput
    Policies assigned: 5 20
   Stats:
    Application Count: 2
    Application Learned:
```

```
Appl Prefix 10.1.5.0/24 telnet
Appl Prefix 10.1.5.16/28 telnet
```

Step 4 **clear pfr master traffic-class** [**access-list** *access-list-name*| **application** *application-name*[*prefix*]| **inside** | **learned**[**delay** | **inside** | **list** *list-name*| **throughput**]| **prefix** *prefix*| **prefix-list** *prefix-list-name*]
This command is used to clear PfR controlled traffic classes from the master controller database. The following example clears traffic classes defined by the Telnet application and the 10.1.1.0/24 prefix:

Example:

```
Router# clear pfr master traffic-class application telnet 10.1.1.0/24
```

Configuration Examples for Static Application Mapping Using Performance Routing

Example Defining a Learn List to Automatically Learn Traffic Classes Using Static Application Mapping

The following example defines application traffic classes using static application mapping. In this example, the following two PfR learn lists are defined:

- LEARN_REMOTE_LOGIN_TC--Remote login traffic represented by Telnet and SSH.
- LEARN_FILE_TRANSFER_TC--File transfer traffic represented by FTP and filtered by the 10.0.0.0/8 prefix.

The goal is to optimize the remote login traffic using one policy (POLICY_REMOTE), and to optimize the file transfer traffic using a different policy (POLICY_FILE). This task configures traffic class learning based on the highest delay. The **policy-rules** (PfR) command activates the remote traffic class learn list. To activate the file transfer traffic class, replace the POLICY_REMOTE map name with the POLICY_FILE map name using the **policy-rules** (PfR) command.

```
ip prefix-list INCLUDE_10_NET 10.0.0.0/8
pfr master
 policy-rules POLICY_REMOTE 10
 learn
 list seq 10 refname LEARN_REMOTE_LOGIN_TC
 traffic-class application telnet ssh
 aggregation-type prefix-length 24
 delay
 exit
 list seq 20 refname LEARN_FILE_TRANSFER_TC
 traffic-class application ftp filter INCLUDE_10_NET
 aggregation-type prefix-length 24
 delay
 exit
 exit
pfr-map POLICY_REMOTE 10
 match pfr learn list LEARN_REMOTE_LOGIN_TC
 exit
```

```
pfr-map POLICY_FILE 20
 match pfr learn list LEARN_FILE_TRANSFER_TC
 end
```

Example Defining a Learn List for Automatically Learned Prefix-Based Traffic Classes

The following example configured on the master controller, defines a learn list that will contain traffic classes that are automatically learned based only on a prefix list. In this example, there are three branch offices and the goal is to optimize all the traffic going to branch offices A and B using one policy (Policy1), and to optimize traffic going to branch office C using a different policy (Policy2).

Branch A is defined as any prefix that matches 10.1.0.0./16, Branch B is defined as any prefix that matches 10.2.0.0./16, and Branch C is defined as any prefix that matches 10.3.0.0./16.

This task configures prefix learning based on the highest outbound throughput. The **policy-rules** (PfR) command activates the traffic class learn list configured for branch offices A and B.

```
ip prefix-list BRANCH_A_B permit seq 10 10.1.0.0/16
ip prefix-list BRANCH_A_B permit seq 20 10.2.0.0/16
ip prefix-list BRANCH_C permit seq 30 10.3.0.0/16
pfr master
 policy-rules POLICY1
 learn
  list seq 10 refname LEARN_BRANCH_A_B
   traffic-class prefix-list BRANCH_A_B
   throughput
   exit
  list seq 20 refname LEARN_BRANCH_C
   traffic-class prefix-list BRANCH_C
   throughput
   exit
  exit
 exit
pfr-map POLICY1 10
 match pfr learn list LEARN_BRANCH_A_B
 exit
pfr-map POLICY2 10
 match pfr learn list LEARN_BRANCH_C
 end
```

Example Defining a Learn List for Automatically Learned Application Traffic Classes Using an Access List

The following example creates an access list that defines custom application traffic classes. In this example, the custom application consists of four criteria:

- Any TCP traffic on destination port 500
- Any TCP traffic on ports in the range from 700 to 750
- Any UDP traffic on source port 400
- Any IP packet marked with a DSCP bit of ef

The goal is to optimize the custom application traffic using a learn list that is referenced in a PfR policy named POLICY_CUSTOM_APP. This task configures traffic class learning based on the highest outbound throughput. The **policy-rules** (PfR) command activates the custom application traffic class learn list.

```
ip access-list extended USER_DEFINED_TC
 permit tcp any any 500
 permit tcp any any range 700 750
 permit udp any eq 400 any
 permit ip any any dscp ef
 exit
pfr master
 policy-rules POLICY_CUSTOM_APP
 learn
  list seq 10 refname CUSTOM_APPLICATION_TC
   traffic-class access-list USER_DEFINED_TC
   aggregation-type prefix-length 24
   throughput
   exit
  exit
 exit
pfr-map POLICY_CUSTOM_APP 10
 match pfr learn list CUSTOM_APPLICATION_TC
 end
```

Example Manually Selecting Traffic Classes Using Static Application Mapping

The following example starting in global configuration mode, configures a PfR map to include application traffic predefined as telnet or Secure Shell and destined to prefixes in the 10.1.1.0/24 network, 10.1.2.0/24 network, and 172.16.1.0/24 network.

```
ip prefix-list LIST1 permit 10.1.1.0/24
ip prefix-list LIST1 permit 10.1.2.0/24
ip prefix-list LIST1 permit 172.16.1.0/24
pfr-map PREFIXES 10
 match traffic-class application telnet ssh prefix-list LIST1
 end
```

Example Manually Selecting Prefix-Based Traffic Classes Using a Prefix List

The following example configured on the master controller, manually selects traffic classes based only on destination prefixes. Use this task when you know the destination prefixes that you want to select for the traffic classes. An IP prefix list is created to define the destination prefixes and using a PfR map, the traffic classes are profiled.

```
ip prefix-list PREFIX_TC permit 10.1.1.0/24
ip prefix-list PREFIX_TC permit 10.1.2.0/24
ip prefix-list PREFIX_TC permit 172.16.1.0/24
pfr-map PREFIX_MAP 10
 match traffic-class prefix-list PREFIX_TC
 end
```

Example Manually Selecting Application Traffic Classes Using an Access List

The following example configured on the master controller, manually selects traffic classes using an access list. Each access list entry is a traffic class that must include a destination prefix and may include other optional parameters.

```
ip access-list extended ACCESS_TC
 permit tcp any 10.1.1.0 0.0.0.255 eq 500
 permit tcp any 172.17.1.0 0.0.255.255 eq 500
 permit tcp any 172.17.1.0 0.0.255.255 range 700 750
 permit tcp 192.168.1.1 0.0.0.0 10.1.2.0 0.0.0.255 eq 800any any dscp ef
 exit
pfr-map ACCESS_MAP 10
 match traffic-class access-list ACCESS_TC
```

Where To Go Next

For information about other Performance Routing features or general conceptual material, see the documents in the “Related Documents” section.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco PfR commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples	Cisco IOS Performance Routing Command Reference
Basic PfR configuration	"Configuring Basic Performance Routing" module
Concepts required to understand the Performance Routing operational phases	"Understanding Performance Routing" module
Advanced PfR configuration	"Configuring Advanced Performance Routing" module
IP SLAs overview	*IP SLAs Configuration Guide*
PfR home page with links to PfR-related content on our DocWiki collaborative environment	PfR:Home

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

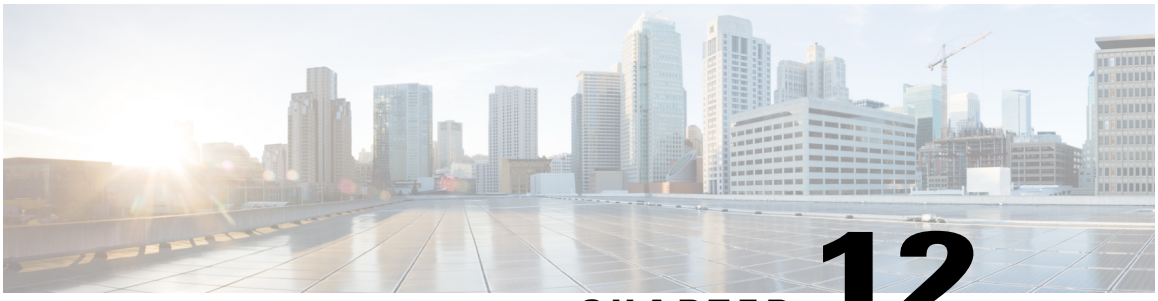
Feature Information for Static Application Mapping Using Performance Routing

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 14: Feature Information for Static Application Mapping Using Performance Routing

Feature Name	Releases	Feature Configuration Information
OER - Application Aware Routing with Static Application Mapping	12.4(15)T	The OER - Application Aware Routing with Static Application Mapping feature introduces the ability to configure standard applications using just one keyword. This feature also introduces a learn list configuration mode that allows Performance Routing (PfR) policies to be applied to traffic classes profiled in a learn list. Different policies can be applied to each learn list. New **traffic-class** and **match traffic-class** commands are introduced to simplify the configuration of traffic classes that PfR can automatically learn, or that can be manually configured. The following commands were introduced or modified by this feature: **clear pfr master traffic-class**, **count (PfR)**, **delay (PfR)**,**list (PfR)**, **match traffic-class access-list (PfR)**, **match traffic-class application (PfR)**, **match traffic-class prefix-list (PfR)**, **show pfr border defined application**, **show pfr master defined application**, **show pfr master learn list**, **show pfr master traffic-class**, **throughput (PfR)**, **traffic-class access-list (PfR)**, **traffic-class application (PfR), traffic-class prefix-list (PfR)**.



CHAPTER 12

Performance Routing Traceroute Reporting

Performance Routing (PfR) support for traceroute reporting allows you to monitor prefix performance on a hop-by-hop basis. Delay, loss, and reachability measurements are gathered for each hop from the probe source (border router) to the target prefix.

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 Table at the end of this document.

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 Performance Routing Traceroute Reporting

PfR Logging and Reporting

Cisco IOS PfR supports standard syslog functions. The notice level of syslog is enabled by default. System logging is enabled and configured in Cisco IOS software under global configuration mode. The **logging**(PfR)

command in PfR master controller or PfR border router configuration mode is used only to enable or disable system logging under PfR. PfR system logging supports the following message types:

- Error Messages--These messages indicate PfR operational failures and communication problems that can impact normal PfR operation.
- Debug Messages--These messages are used to monitor detailed PfR operations to diagnose operational or software problems.
- Notification Messages--These messages indicate that PfR is performing a normal operation.
- Warning Messages--These messages indicate that PfR is functioning properly but an event outside of PfR may be impacting normal PfR operation.

Note With CSCtx06699, PfR syslog levels are added to minimize the number of messages displayed, and a syslog notice is added to display when 30 percent of the traffic classes are out-of-policy.

Note With CSCts74631, PfR syslog levels are added to minimize the number of messages displayed, a syslog notice is added to display when 30 percent of the traffic classes are out-of-policy, and new syslog alerts are added for a PfR version mismatch, an MC-BR authentication error, and when minimum PfR requirements are not met and the master controller is disabled because there are less than two operational external interfaces.

To modify system, terminal, destination, and other system global logging parameters, use the logging commands in global configuration mode. For more information about global system logging configuration, see to the "Troubleshooting, Logging, and Fault Management" section of the *Cisco IOS Network Management Configuration Guide*.

PfR Troubleshooting Using Traceroute Reporting

Although PfR provides the ability to diagnose issues using **syslog** and **debug** command-line interface (CLI) commands, support for traceroute reporting was introduced in the OER Support for Cost-Based Optimization and Traceoute Reporting feature. Using traceroute reporting, PfR reports traffic class performance by determining the delay on a hop-by-hop basis using traceroute probes.

Prior to traceroute reporting there was no method for measuring the delay per hop for situations such as an unexpected round trip delay value being reported for a traffic class on an exit link. PfR uses UDP traceroutes to collect per-hop delay statistics. A traceroute is defined as tracing the route to the device with the given IP address or the hostname and is useful in detecting the location of a problem that exists in the path to the device. Although traditional UDP-based traceroutes are used by default, PfR can be configured to send TCP SYN packets to specific ports that may be permitted through a firewall.

Traceroute reporting is configured on the master controller. Traceroute probes are sourced from the border router exit. This feature allows you to monitor traffic class performance on a hop-by-hop basis. When traceroute reporting is enabled, the autonomous system number, the IP address, and delay measurements are gathered for each hop from the probe source to the target prefix. By default, traceroute probes are sent only when the traffic class goes OOP. TCP-based traceroutes can be configured manually and the time interval between traceroute probes can be modified. By default, per-hop delay reporting is not enabled.

Traceroute probes are configured using the following methods:

- Periodic--A traceroute probe is triggered for each new probe cycle. The probe is sourced from the current exit of the traffic class when the option to probe only one exit is selected. If the option to probe all exits is selected, the traceroute probe is sourced from all available exits.
- Policy based--A traceroute probe is triggered automatically when a traffic class goes into an out-of-policy state. Traceroute reporting can be enabled for all traffic classes specified in the match clause of an PfR map. Policy based traceroute reporting stops when the traffic class returns to an in-policy state.
- On demand--A trace route probe can be triggered on an on demand basis when periodic traceroute reporting is not required, or the per-hop statistics are not required for all paths. Using optional keywords and arguments of the **show pfr master prefix** command, you can start traceroute reporting for a specific traffic class on a specific path, or all paths.

How to Configure Performance Routing Traceroute Reporting

Configuring PfR Traceroute Reporting

Perform this task at the master controller to configure traceroute reporting. When using a PfR active probe there are situations when a host address does not respond to the PfR probe message. The reason for no response to the probe message may be due to a firewall or other network issue but PfR assumes the host address to be unreachable and releases control of the prefix. Prior to traceroute reporting there was no method for measuring the delay per hop for situations such as an unexpected round trip delay value being reported for a traffic class on an exit link. The solution for both the non-responding target address and the lack of per-hop delay information involves using UDP, and optionally TCP, traceroutes. Traceroute reporting is configured on a master controller, but the traceroute probes are sourced from the border router exits.

In this task, the three methods of configuring traceroute probes are used. Periodic and policy-based traceroute reporting are configured with the **set traceroute reporting** (PfR) command using a PfR map. On-demand traceroute probes are triggered by entering the **show pfr master prefix** command with certain parameters. This task also shows to modify the time interval between traceroute probes using the **traceroute probe-delay** (PfR) command.

When traceroute reporting is enabled, the default time interval between traceroute probes is 1000 milliseconds.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **traceroute probe-delay** *milliseconds*
5. **exit**
6. **pfr-map** *map-name sequence-number*
7. **match pfr learn** {**delay** | **throughput**}
8. **set traceroute reporting** [**policy** {**delay** | **loss** | **unreachable**}]
9. **end**
10. **show pfr master prefix** [**detail** | **learned** [**delay** | **throughput**] | *prefix* [**detail** | **policy** | **traceroute** [*exit-id* | *border-address* | **current**] [**now**]]]

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.
Step 3	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure a router as a master controller and to configure global operations and policies.
Step 4	**traceroute probe-delay** *milliseconds* **Example:** `Router(config-pfr-mc)# traceroute probe-delay 500`	Sets the time interval between traceroute probe cycles. • The default time interval between traceroute probes is 1000 milliseconds. • The example sets the probe interval to a 500 milliseconds.
Step 5	**exit** **Example:** `Router(config-pfr-mc)# exit`	Exits PfR master controller configuration mode, and returns to global configuration mode.
Step 6	**pfr-map** *map-name sequence-number* **Example:** `Router(config)# pfr-map TRACEROUTE 10`	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes. • Only one match clause can be configured for each PfR map sequence. • The example creates a PfR map named TRACEROUTE.
Step 7	**match pfr learn** {**delay** | **throughput**} **Example:** `Router(config-pfr-map)# match pfr learn delay`	Creates a match clause entry in a PfR map to match learned prefixes. • Can be configured to learn prefixes based on highest delay or highest outbound throughput. • Only a single match clause can be configured for each PfR map sequence. • The example creates a match clause entry that matches traffic learned based on highest delay.

	Command or Action	Purpose
Step 8	**set traceroute reporting** [**policy** {**delay** | **loss** | **unreachable**}] **Example:** `Router(config-pfr-map)# set traceroute reporting`	Enables traceroute reporting. • Monitored prefixes must be included in a PfR map. These can be learned or manually selected prefixes. • Entering this command with no keywords enables continuous monitoring. • Entering this command with the policy keyword enables policy-based trace route reporting.
Step 9	**end** **Example:** `Router(config-pfr-map)# end`	Exits PfR master controller configuration mode, and returns to privileged EXEC mode.
Step 10	**show pfr master prefix** [**detail** | **learned** [**delay** | **throughput**] | *prefix* [**detail** | **policy** | **traceroute** [*exit-id* | *border-address* | **current**] [**now**]]] **Example:** `Router# show pfr master prefix 10.5.5.5 traceroute now`	Displays the status of monitored prefixes. • An on-demand traceroute probe is initiated by entering the **current** and **now** keywords. • The **current** keyword displays the results of the most recent traceroute probe for the current exit. • Traceroute probe results can be displayed for the specified border router exit by entering the *exit-id* or *border-address*argument. • The example initiates an on-demand traceroute probe for the 10.5.5.55 prefix.

Configuration Examples for Performance Routing Traceroute Reporting

Example Configuring PfR Traceroute Reporting

The following example, starting in global configuration mode, configures continuous traceroute reporting for traffic classes learned on the basis of delay:

```
Router(config)# pfr master
Router(config-pfr-mc)# traceroute probe-delay 10000
Router(config-pfr-mc)# exit
Router(config)# pfr-map TRACE 10
```

```
Router(config-pfr-map)# match pfr learn delay
Router(config-pfr-map)# set traceroute reporting
Router(config-pfr-map)# end
```

The following example, starting in privileged EXEC mode, initiates an on-demand traceroute probe for the 10.5.5.5 prefix:

```
Router# show pfr master prefix 10.5.5.55 traceroute current now

Path for Prefix: 10.5.5.0/24         Target: 10.5.5.5
Exit ID: 2, Border: 10.1.1.3         External Interface: Et1/0
Status: DONE, How Recent: 00:00:08 minutes old
Hop  Host            Time(ms) BGP
1    10.1.4.2        8        0
2    10.1.3.2        8        300
3    10.5.5.5        20       50
```

Where to Go Next

For information about other Performance Routing features or general conceptual material, see the documents in the “Related Documents” section.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco PfR commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples	Cisco IOS Performance Routing Command Reference
Basic PfR configuration	"Configuring Basic Performance Routing" module
Concepts required to understand the Performance Routing operational phases	"Understanding Performance Routing" module
Advanced PfR configuration	"Configuring Advanced Performance Routing" module
IP SLAs overview	*IP SLAs Configuration Guide*
PfR home page with links to PfR-related content on our DocWiki collaborative environment	PfR:Home

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

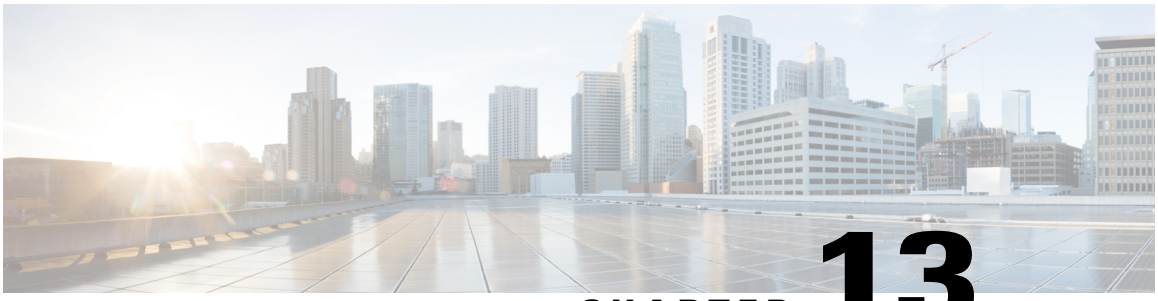
Feature Information for Performance Routing Traceroute Reporting

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 15: Feature Information for Performance Routing Traceroute Reporting

Feature Name	Releases	Feature Information
OER Support for Cost-Based Optimization and Traceroute Reporting	12.3(14)T, 12.2(33)SRB	Performance Routing support for traceroute reporting allows you to monitor prefix performance on a hop-by-hop basis. Delay, loss, and reachability measurements are gathered for each hop from the probe source (border router) to the target prefix. The following commands were introduced or modified by this feature: **set traceroute reporting (PfR)**, **traceroute probe-delay (PfR)**, and **show pfr master prefix**.



CHAPTER 13

PfR Voice Traffic Optimization Using Active Probes

This module documents a Performance Routing (PfR) solution that supports outbound optimization of voice traffic based on the voice metrics, jitter and Mean Opinion Score (MOS). Jitter and MOS are important quantitative quality metrics for voice traffic and these voice metrics are measured using PfR active probes.

PfR provides automatic route optimization and load distribution for multiple connections between networks. PfR is an integrated Cisco IOS solution that allows you to monitor IP traffic flows and then define policies and rules based on prefix performance, link load distribution, link bandwidth monetary cost, and traffic type. PfR provides active and passive monitoring systems, dynamic failure detection, and automatic path correction. Deploying PfR enables intelligent load distribution and optimal route selection in an enterprise network.

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 Table at the end of this document.

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.

Prerequisites for PfR Voice Traffic Optimization Using Active Probes

Before implementing PfR optimization for voice traffic, you need to understand an overview of how PfR works and how to set up PfR network components. See the Understanding Performance Routing, Configuring Basic Performance Routing, and Configuring Advanced Performance Routing modules for more details.

Information About PfR Voice Traffic Optimization Using Active Probes

Voice Quality on IP Networks

Voice packets traveling through an IP network are no different from data packets. In the plain old telephone system (POTS), voice traffic travels over circuit-switched networks with predetermined paths and each phone call is given a dedicated connection for the duration of the call. Voice traffic using POTS has no resource contention issues, but voice traffic over an IP network has to contend with factors such as delay, jitter, and packet loss, which can affect the quality of the phone call.

Delay

Delay (also referred as latency) for voice packets is defined as the delay between when the packet was sent from the source device and when it arrived at a destination device. Delay can be measured as one-way delay or round-trip delay. The largest contributor to latency is caused by network transmission delay. Round-trip delay affects the dynamics of conversation and is used in Mean Opinion Score (MOS) calculations. One-way delay is used for diagnosing network problems. A caller may notice a delay of 200 milliseconds and try to speak just as the other person is replying because of packet delay. The telephone industry standard specified in ITU-T G.114 recommends the maximum desired one-way delay be no more than 150 milliseconds. Beyond a one-way delay of 150 milliseconds, voice quality is affected. With a round-trip delay of 300 milliseconds or more, users may experience annoying talk-over effects.

Jitter

Jitter means interpacket delay variance. When multiple packets are sent consecutively from source to destination, for example, 10 ms apart, and if the network is behaving ideally, the destination should be receiving them 10 ms apart. But if there are delays in the network (like queuing, arriving through alternate routes, and so on) the arrival delay between packets might be greater than or less than 10 ms. Using this example, a positive jitter value indicates that the packets arrived more than 10 ms apart. If the packets arrive 12 ms apart, then positive jitter is 2 ms; if the packets arrive 8 ms apart, then negative jitter is 2 ms. For delay-sensitive networks like VoIP, positive jitter values are undesirable, and a jitter value of 0 is ideal.

Packet Loss

Packet loss can occur due an interface failing, a packet being routed to the wrong destination, or congestion in the network. Packet loss for voice traffic leads to the degradation of service in which a caller hears the voice sound with breaks. Although average packet loss is low, voice quality may be affected by a short series of lost packets.

Mean Opinion Score (MOS)

With all the factors affecting voice quality, many people ask how voice quality can be measured. Standards bodies like the ITU have derived two important recommendations: P.800 (MOS) and P.861 (Perceptual Speech Quality Measurement [PSQM]). P.800 is concerned with defining a method to derive a Mean Opinion Score of voice quality. MOS scores range between 1 representing the worst voice quality, and 5 representing the best voice quality. A MOS of 4 is considered “toll-quality” voice.

Probes Used by PfR

PfR uses some of the IP SLA probes to help gather the data PfR requires to make its decisions.

Cisco IOS IP SLAs

Cisco IOS IP SLAs are an embedded feature set in Cisco IOS software and they allow you to analyze IP service levels for IP applications and services, to increase productivity, to lower operational costs, and to reduce occurrences of network congestion or outages. IP SLAs use active traffic monitoring--the generation of traffic in a continuous, reliable, and predictable manner--for measuring network performance. The accuracy of measured data is enhanced by enabling the IP SLAs Responder, available in Cisco routers, on the destination device. For more details about IP SLAs, see the *Cisco IOS IP SLAs Configuration Guide* .

Active Probe Types Used by PfR

The following types of active probes can be configured:

ICMP Echo--A ping is sent to the target address. PfR uses ICMP Echo probes, by default, when an active probe is automatically generated. Configuring an ICMP echo probe does not require knowledgeable cooperation from the target device. However, repeated probing could trigger an Intrusion Detection System (IDS) alarm in the target network. If an IDS is configured in a target network that is not under your control, we recommend that you notify the administrator of this target network.

Jitter--A jitter probe is sent to the target address. A target port number must be specified. A remote responder must be enabled on the target device, regardless of the configured port number.

TCP Connection--A TCP connection probe is sent to the target address. A target port number must be specified. A remote responder must be enabled if TCP messages are configured to use a port number other than TCP port number 23, which is well-known.

UDP Echo--A UDP echo probe is sent to the target address. A target port number must be specified. A remote responder must be enabled on the target device, regardless of which port number is configured.

Probe Frequency

The frequency of an active probe used by PfR is set by default to 60 seconds, but the frequency can be increased for each policy by configuring a lower time-interval between two probes. Increased probe frequency can reduce the response time and provide a better approximation of the MOS-low count percentage.

PfR Voice Traffic Optimization Using Active Probes

Configuring PfR to optimize voice traffic using active probes involves several decisions and subsequent branching tasks. The first step is to identify the traffic to be optimized and decide whether to use a prefix list or an access list. Use a prefix list to identify all traffic, including voice traffic, with a specific set of destination

prefixes. Use an access list to identify only voice traffic with a specific destination prefix and carried over a specific protocol.

The second step in optimizing voice traffic is to configure active probing using the **active-probe** or **set active-probe** command to specify the type of active probe to be used. PfR also provides the ability to set a forced target assignment for the active probe.

The final step in optimizing voice traffic is to configure a PfR policy to set the performance metrics that you want PfR to apply to the identified traffic.

PfR Voice Performance Metrics

PfR voice traffic optimization provides support for outbound optimization of voice traffic on the basis of the voice performance metrics, delay, packet loss, jitter, and MOS. Delay, packet loss, jitter and MOS are important quantitative quality metrics for voice traffic, and these voice metrics are measured using PfR active probes. The IP SLA jitter probe is integrated with PfR to measure jitter (source to destination) and the MOS score in addition to measuring delay and packet loss. The jitter probe requires a responder on the remote side just like the UDP Echo probe. Integration of the IP SLA jitter probe type in PfR enhances the ability of PfR to optimize voice traffic. PfR policies can be configured to set the threshold and priority values for the voice performance metrics: delay, packet loss, jitter, and MOS.

Configuring a PfR policy to measure jitter involves configuring only the threshold value and not relative changes (used by other PfR features) because for voice traffic, relative jitter changes have no meaning. For example, jitter changes from 5 milliseconds to 25 milliseconds are just as bad in terms of voice quality as jitter changes from 15 milliseconds to 25 milliseconds. If the short-term average (measuring the last 5 probes) jitter is higher than the jitter threshold, the prefix is considered out-of-policy due to jitter. PfR then probes all exits, and the exit with the least jitter is selected as the best exit.

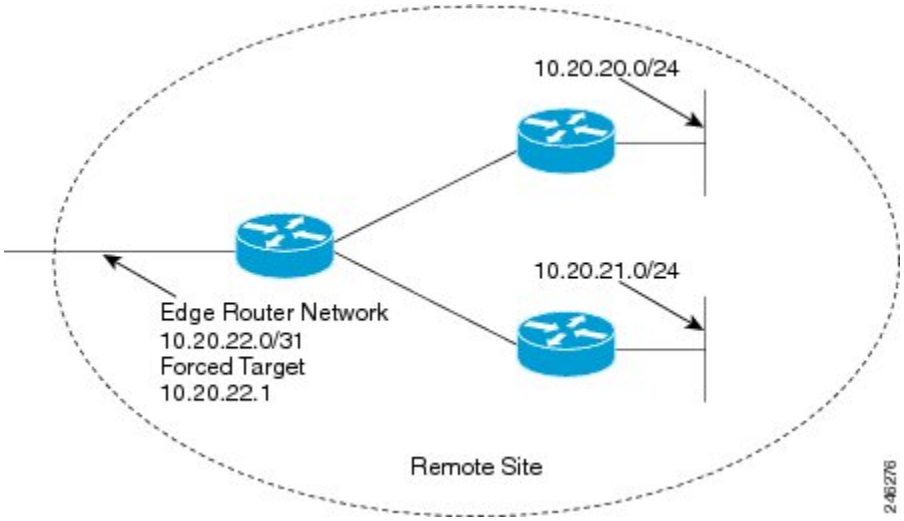
MOS policy works in a different way. There is no meaning to average MOS values, but there is meaning to the number of times that the MOS value is below the MOS threshold. For example, if the MOS threshold is set to 3.85 and if 3 out of 10 MOS measurements are below the 3.85 MOS threshold, the MOS-low-count is 30 percent. In the output of the **show** commands the field, ActPMOS, shows the number of actively monitored MOS packets with a percentage below threshold. If some of the MOS measurements are only slightly below the threshold, with percentage rounding, an ActPMOS value of zero may be displayed. When PfR runs a policy configured to measure MOS, both the MOS threshold value and the MOS-low-count percentage are considered. A prefix is considered out-of-policy if the short term (average over the last 5 probes) MOS-low-count percentage is greater than the configured MOS-low-count percentage. PfR then probes all exits, and the exit with the highest MOS value is selected as the best exit.

PfR Active Probe Forced Target Assignment

In earlier releases of the OER technology, the PfR active probe target is assigned to the longest matched prefix. There are some scenarios where you may want to use a target that does not match the destination prefix. The

example in the figure below explains a scenario in which configuring a PfR forced target assignment is more appropriate than using the longest match prefix.

Figure 17: PfR Forced Target Assignment Scenario



In the figure above we want to probe IP address 10.20.22.1 (at the edge of the network) for either network 10.20.21.0/24 or 10.20.22.0/24. Jitter is less likely to be introduced within the network so probing the edge of the network gives a measurement that is close to probing the final destination.

Forced target assignment allows you to assign a target to a group of prefixes or an application, even if they are not the longest match prefixes. Assigning a target can determine the true delay to the edge of a network rather than delay to an end host.

How to Configure PfR Voice Traffic Optimization Using Active Probes

Perform one of the first two optional tasks, depending on whether you want to use a prefix list or an access list to identify the traffic to be optimized. The third task can be used with traffic identified using an access list, and it also demonstrates how to use a forced target assignment. For an example configuration that can be used with traffic identified using a prefix list, see the “Example: Optimizing Traffic (Including Voice Traffic) Using Active Probes” section.

Identifying Traffic for PfR Using a Prefix List

Before traffic can be measured using PfR, it must be identified. Perform this task to use a prefix list to identify the traffic that PfR will probe.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length*| **permit** *network/length*}
4. **exit**

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.
Step 3	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length*| **permit** *network/length*} **Example:** `Router(config)# ip prefix-list TRAFFIC_PFX_LIST seq 10 permit 10.20.21.0/24`	Creates an IP prefix list. • IP prefix lists are used to manually select prefixes for monitoring by the PfR master controller. • A master controller can monitor and control an exact prefix (/32), a specific prefix length, or a specific prefix length and any prefix that falls under the prefix length (for example, a /24 under a /16). • The prefixes specified in the IP prefix list are imported into a PfR map using the **match ip address** (PfR) command. • The example creates an IP prefix list named TRAFFIC_PFX_LIST that permits prefixes from the 10.20.21.0/24 subnet.
Step 4	**exit** **Example:** `Router(config)# exit`	(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Identifying Voice Traffic to Optimize Using an Access List

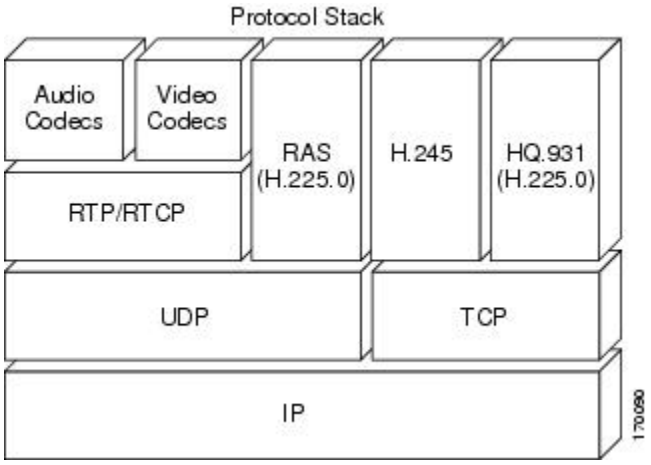
Before voice traffic can be measured, it must be identified. Perform this task to use an access list to identify the voice traffic.

Identifying Voice Traffic to Optimize Using an Access List

Before voice traffic can be measured, it must be identified. Perform this task to use an access list to identify the voice traffic.

Voice traffic uses a variety of protocols and streams on the underlying IP network. The figure below is a representation of the protocol options available for carrying voice traffic over IP. Most signaling traffic for voice is carried over TCP. Most voice calls are carried over User Datagram Protocol (UDP) and Real-Time Transport Protocol (RTP). You can configure your voice devices to use a specific range of destination port numbers over UDP to carry voice call traffic.

Figure 18: Protocol Stack Options Available for Voice Traffic



SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list** {**standard** | **extended**} *access-list-name*
4. [*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**log**] [**time-range** *time-range-name*] [**fragments**]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip access-list** {**standard** | **extended**} *access-list-name* **Example:** `Router(config)# ip access-list extended VOICE_ACCESS_LIST`	Defines an IP access list by name. • PfR supports only named access lists. • The example creates an extended IP access list named VOICE_ACCESS_LIST.
Step 4	[*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**log**] [**time-range** *time-range-name*] [**fragments**] **Example:** `Router(config-ext-nacl)# permit udp any range 16384 32767 10.20.20.0 0.0.0.15 range 16384 32767`	Defines the extended access list. • Any protocol, port, or other IP packet header value can be specified. • The example is configured to identify all UDP traffic ranging from a destination port number of 16384 to 32767 from any source to a destination prefix of 10.20.20.0/24. This specific UDP traffic is to be optimized.
Step 5	**exit** **Example:** `Router(config)# exit`	(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Configuring PfR Voice Probes with a Target Assignment

After identifying the traffic (in this example, voice traffic identified using an access list) to be optimized, perform this task to configure the PfR jitter probes and assign the results of the jitter probes to optimize the identified traffic. In this task, the PfR active voice probes are assigned a forced target for PfR instead of the usual longest match assigned target. Before configuring the PfR jitter probe on the source device, the IP SLAs Responder must be enabled on the target device (the operational target). The IP SLAs Responder is available only on Cisco IOS software-based devices. Start this task at the network device that runs the IP SLAs Responder.

Note The device that runs the IP SLAs Responder does not have to be configured for PfR.

Note Policies applied in a PfR map do not override global policy configurations.

Before You Begin

Before configuring this task, perform the Identifying Voice Traffic to Optimize Using an Access List task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla monitor responder**
4. **exit**
5. Move to the network device that is the PfR master controller.
6. **enable**
7. **configure terminal**
8. **pfr-map** *map-name sequence-number*
9. **match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*}
10. **set active-probe** *probe-type ip-address* [**target-port** *number*] [**codec** *codec-name*]
11. **set probe frequency** *seconds*
12. **set jitter threshold** *maximum*
13. **set mos** {**threshold** *minimum* **percent** *percent*}
14. **set resolve** {**cost priority** *value* | **delay priority** *value* **variance** *percentage* | **jitter priority** *value* **variance** *percentage* | **loss priority** *value* **variance** *percentage* | **mos priority** *value* **variance** *percentage* | **range priority** *value* | **utilization priority** *value* **variance** *percentage*}
15. **set resolve mos priority** *value* **variance** *percentage*
16. **set delay** {**relative** *percentage* | **threshold** *maximum*}
17. **exit**
18. **pfr master**
19. **policy-rules** *map-name*
20. **end**
21. **show pfr master active-probes** [**appl**| **forced**]
22. **show pfr master policy** {*sequence-number*|*policy-name* | **default**}

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	**ip sla monitor responder** **Example:** `Router(config)# ip sla monitor responder`	Enables the IP SLAs Responder.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	Move to the network device that is the PfR master controller.	--
Step 6	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 7	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 8	**pfr-map** *map-name sequence-number* **Example:** `Router(config)# pfr-map TARGET_MAP 10`	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes. • Only one match clause can be configured for each PfR map sequence. • Deny sequences are first defined in an IP prefix list and then applied with the **match ip address** (PfR) command in Step 9 . • The example creates a PfR map named TARGET_MAP.
Step 9	**match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*} **Example:** `Router(config-pfr-map)# match ip address access-list VOICE_ACCESS_LIST`	References an extended IP access list or IP prefix as match criteria in a PfR map. • Only a single match clause can be configured for each PfR map sequence. • The example configures the IP access list named VOICE_ACCESS_LIST as match criteria in a PfR map. The access list was created in the "Identifying Voice Traffic to Optimize Using an Access List" task.
Step 10	**set active-probe** *probe-type ip-address* [**target-port** *number*] [**codec** *codec-name*]	Creates a set clause entry to assign a target prefix for an active probe. • The **echo** keyword is used to specify the target IP address of a prefix to actively monitor using Internet Control Message Protocol (ICMP) echo (ping) messages.

	Command or Action	Purpose
	Example: `Router(config-pfr-map)# set active-probe jitter 10.20.22.1 target-port 2000 codec g729a`	• The **jitter** keyword is used to specify the target IP address of a prefix to actively monitor using jitter messages. • The **tcp-conn** keyword is used to specify the target IP address of a prefix to actively monitor using Internet Control Message Protocol (ICMP) echo (ping) messages. • The **udp-echo** keyword is used to specify the target IP address of a prefix to actively monitor using Internet Control Message Protocol (ICMP) echo (ping) messages. • The example creates a set clause entry to specify the target IP address of a prefix and a specific port number to actively monitor using jitter.
Step 11	**set probe frequency** *seconds* **Example:** `Router(config-pfr-map)# set probe frequency 10`	Creates a set clause entry to set the frequency of the PfR active probe. • The *seconds* argument is used to set the time, in seconds, between the active probe monitoring of the specified IP prefixes. • The example creates a set clause to set the active probe frequency to 10 seconds.
Step 12	**set jitter threshold** *maximum* **Example:** `Router(config-pfr-map)# set jitter threshold 20`	Creates a set clause entry to configure the jitter threshold value. • The **threshold** keyword is used to configure the maximum jitter value, in milliseconds. • The example creates a set clause that sets the jitter threshold value to 20 for traffic that is matched in the same PfR map sequence.
Step 13	**set mos** {**threshold** *minimum* **percent** *percent*} **Example:** `Router(config-pfr-map)# set mos threshold 4.0 percent 30`	Creates a set clause entry to configure the MOS threshold and percentage values used to decide whether an alternate exit is be selected. • The **threshold** keyword is used to configure the minimum MOS value. • The **percent** keyword is used to configure the percentage of MOS values that are below the MOS threshold. • PfR calculates the percentage of MOS values below the MOS threshold that are recorded in a five-minute period. If the percentage value exceeds the configured percent value or the default value, the master controller searches for alternate exit links. • The example creates a set clause that sets the threshold MOS value to 4.0 and the percent value to 30 percent for traffic that is matched in the same PfR map sequence.
Step 14	**set resolve** {**cost priority** *value* | **delay priority** *value* **variance** *percentage* | **jitter priority** *value* **variance** *percentage* | **loss priority** *value* **variance**	Creates a set clause entry to configure policy priority or resolve policy conflicts. • This command is used to set priority for a policy type when multiple policies are configured for the same prefix. When this command is

	Command or Action	Purpose
	percentage | **mos priority** *value* **variance** *percentage* | **range priority** *value* | **utilization priority** *value* **variance** *percentage*} **Example:** `Router(config-pfr-map)# set resolve jitter priority 1 variance 10`	configured, the policy with the highest priority will be selected to determine the policy decision. • The **priority** keyword is used to specify the priority value. Configuring the number 1 assigns the highest priority to a policy. Configuring the number 10 assigns the lowest priority. • Each policy must be assigned a different priority number. • The **variance**keyword is used to set an allowable variance for a user-defined policy. This keyword configures the allowable percentage that an exit link or prefix can vary from the user-defined policy value and still be considered equivalent. • Variance cannot be configured for cost or range policies. • The example creates set clause that configures the priority for jitter policies to 1 for voice traffic. The variance is configured to allow a 10 percent difference in jitter statistics before a prefix is determined to be out-of-policy.
Step 15	**set resolve mos priority** *value* **variance** *percentage* **Example:** `Router(config-pfr-map)# set resolve mos priority 2 variance 15`	Creates a set clause entry to configure policy priority or resolve policy conflicts. • The example creates set clause that configures the priority for MOS policies to 2 for voice traffic. The variance is configured to allow a 15 percent difference in MOS values before a prefix is determined to be out-of-policy. **Note** Only the syntax applicable to this task is used in this example. For more details, see Step 14.
Step 16	**set delay** {**relative** *percentage* | **threshold** *maximum*} **Example:** `Router(config-pfr-map)# set delay threshold 100`	Creates a set clause entry to configure the delay threshold. • The delay threshold can be configured as a relative percentage or as an absolute value for match criteria. • The **relative** keyword is used to configure a relative delay percentage. The relative delay percentage is based on a comparison of short-term and long-term measurements. • The **threshold** keyword is used to configure the absolute maximum delay period in milliseconds. • The example creates a set clause that sets the absolute maximum delay threshold to 100 milliseconds for traffic that is matched in the same PfR map sequence.
Step 17	**exit** **Example:** `Router(config-pfr-map)# exit`	Exits PfR map configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 18	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure a router as a master controller. • A master controller and border router process can be enabled on the same router (for example, in a network that has a single router with two exit links to different service providers).
Step 19	**policy-rules** *map-name* **Example:** `Router(config-pfr-mc)# policy-rules TARGET_MAP`	Applies a configuration from a PfR map to a master controller configuration in PfR master controller configuration mode. • Reentering this command with a new PfR map name will immediately overwrite the previous configuration. This behavior is designed to allow you to quickly select and switch between predefined PfR maps. • The example applies the configuration from the PfR map named TARGET_MAP.
Step 20	**end** **Example:** `Router(config-pfr-mc)# end`	Exits PfR master controller configuration mode and enters privileged EXEC mode.
Step 21	**show pfr master active-probes** [**appl**| **forced**] **Example:** `Router# show pfr master active-probes forced`	Displays connection and status information about active probes on a PfR master controller. • The output from this command displays the active probe type and destination, the border router that is the source of the active probe, the target prefixes that are used for active probing, and whether the probe was learned or configured. • The **appl** keyword is used to filter the output to display information about applications optimized by the master controller. • The **forced** keyword is used to show any forced targets that are assigned. • The example displays connection and status information about the active probes generated for voice traffic configured with a forced target assignment.
Step 22	**show pfr master policy** {*sequence-number*|*policy-name* | **default**} **Example:** `Router# show pfr master policy TARGET_MAP`	Displays policy settings on a PfR master controller. • This command is used to configure a PfR map to configure the relative percentage or maximum number of packets that PfR will permit to be lost during transmission on an exit link. If packet loss is greater than the user-defined or the default value, the master controller determines that the exit link is out-of-policy. • The *sequence-number* argument is used to display policy settings for the specified PfR map sequence.

	Command or Action	Purpose
		• The *policy-name* argument is used to display policy settings for the specified PfR policy map name. • The**default**keyword is used to display only the default policy settings. • The example displays the policy settings configured for the TARGET_MAP policy.

Examples

This example shows output from the **show pfr master active-probes forced** command. The output is filtered to display only connection and status information about the active probes generated for voice traffic configured with a forced target assignment.

```
Router# show pfr master active-probes forced
OER Master Controller active-probes
Border   = Border Router running this Probe
Policy   = Forced target is configure under this policy
Type     = Probe Type
Target   = Target Address
TPort    = Target Port
N - Not applicable
The following Forced Probes are running:
Border          State    Policy            Type     Target          TPort
10.20.20.2     ACTIVE    40                jitter   10.20.22.1      3050
10.20.21.3     ACTIVE    40                jitter   10.20.22.4      3050
```

Configuration Examples for PfR Voice Traffic Optimization Using Active Probes

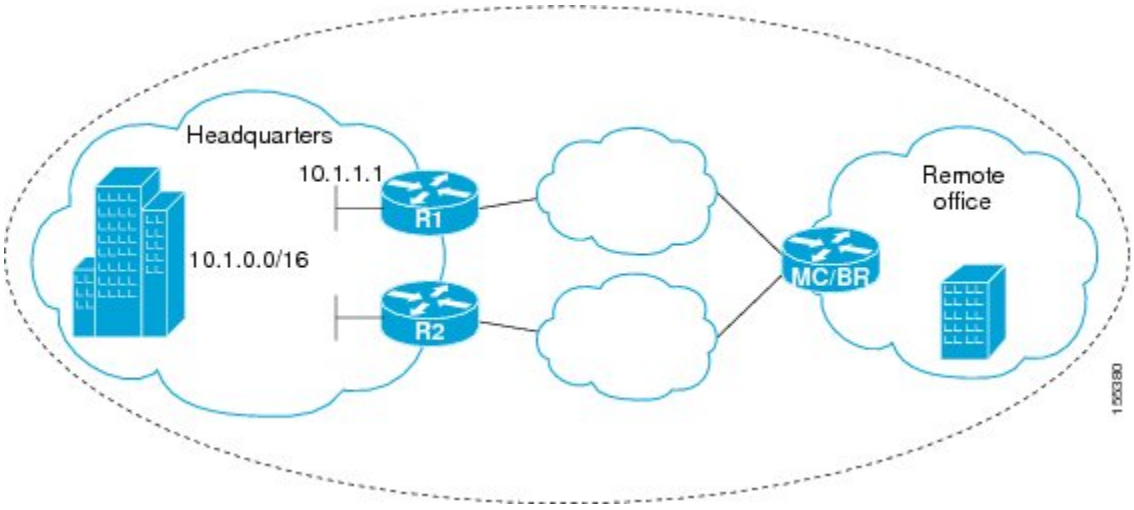
The following examples show both how to use an access list to identify only voice traffic to be optimized by PfR and to use a prefix list to identify traffic that includes voice traffic to be optimized by PfR.

Example Optimizing Only Voice Traffic Using Active Probes

The figure below shows that voice traffic originating at the remote office and terminating at the headquarters has to be optimized to select the best path out of the remote office network. Degradation in voice (traffic)

quality is less likely to be introduced within the network, so probing the edge of the network gives a measurement that is close to probing the final destination.

Figure 19: PfR Network Topology Optimizing Voice Traffic Using Active Probes



This configuration optimizes voice traffic to use the best performance path, whereas all other traffic destined to the same network--10.1.0.0/16--will follow the best path as indicated by a traditional routing protocol, for example BGP, that is configured on the device. As part of this optimization, PfR will use policy based routing (PBR) to set the best exit link for voice traffic within a device.

The following configuration is performed on the edge router R1 in the figure above in the headquarters network to enable the IP SLAs Responder.

```
enable
configure terminal
 ip sla responder
 exit
```

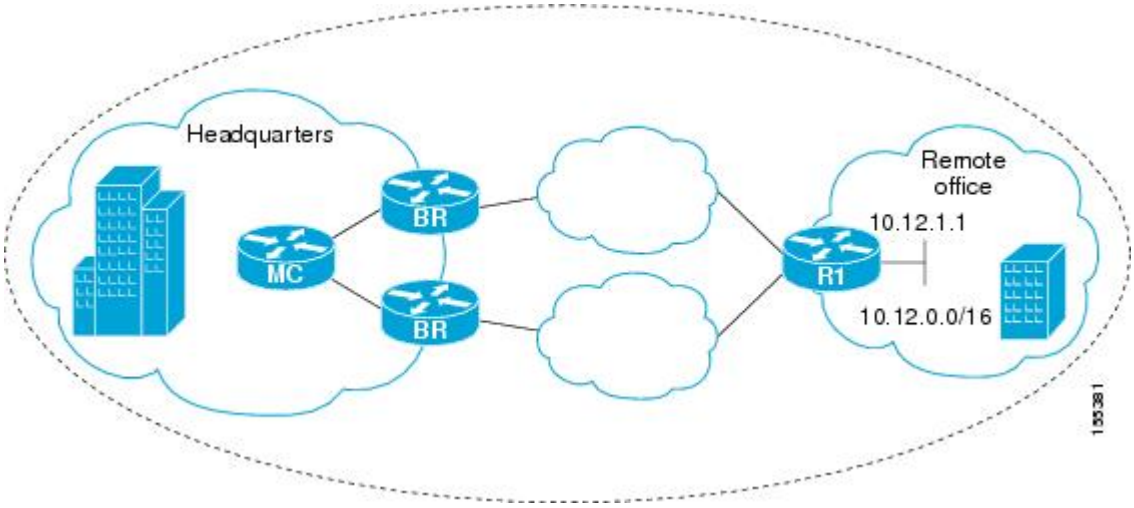
The following configuration is performed on the edge router MC/BR (which is both a PfR master controller and border router) in the figure above in the remote office network to optimize voice traffic using active probes.

```
enable
configure terminal
ip access-list extended Voice_Traffic
 10 permit udp any 10.1.0.0 0.0.255.255 range 16384 32767
 exit
pfr-map Voice_MAP 10
 match ip address access-list Voice_Traffic
 set active-probe jitter 10.1.1.1 target-port 1025 codec g711alaw
 set delay threshold 300
 set mos threshold 3.76 percent 30
 set jitter threshold 15
 set loss relative 5
 resolve mos priority 1
 resolve jitter priority 2
 resolve delay priority 3
 resolve loss priority 4
```

Example Optimizing Traffic (Including Voice Traffic) Using Active Probes

The figure below shows that traffic originating in the headquarters network and destined for the remote office network has to be optimized based on voice traffic metrics. Voice traffic is one of the most important traffic classes that travel from the headquarters to the remote office network, so the voice traffic must be prioritized to be optimized. Degradation in voice packet quality is less likely to be introduced within the network, so probing the edge of the network gives a measurement that is close to probing the final destination.

Figure 20: PfR Network Topology for Optimizing All Traffic Using Active Probes



This configuration optimizes all traffic, including voice traffic, destined for the 10.12.0.0/16 network. The PfR optimization is based on the measurement of voice performance metrics with thresholding values using active probes. As part of the optimization, PfR will introduce a BGP or a static route into the headquarters network. For more details about BGP and static route optimization, see the "Understanding Performance Routing" module.

The following configuration is performed on router R1 in the figure above in the remote office network to enable the IP SLAs Responder.

```
enable
configure terminal
 ip sla responder
 exit
```

The following configuration is performed on one of the BR routers in the figure above in the headquarters network to optimize all traffic (including voice traffic) using active probes.

```
enable
configure terminal
 ip prefix-list All_Traffic_Prefix permit 10.12.0.0/16
 pfr-map Traffic_MAP 10
 match ip address prefix-list All_Traffic_Prefix
 set active-probe jitter 10.12.1.1 target-port 1025 codec g711alaw
! port 1025 for the target probe is an example.
 set delay threshold 300
 set mos threshold 3.76 percent 30
 set jitter threshold 15
 set loss relative 5
 resolve mos priority 1
```

```
resolve jitter priority 2
resolve delay priority 3
resolve loss priority 4
```

Where to Go Next

This document describes a specific implementation of PfR and presumes that you are familiar with the PfR technology. If you want to review more information about PfR, see the documents that are listed under “Related Documents” section.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco PfR commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples	Cisco IOS Performance Routing Command Reference
Basic PfR configuration	"Configuring Basic Performance Routing" module
Concepts required to understand the Performance Routing operational phases	"Understanding Performance Routing" module
Advanced PfR configuration	"Configuring Advanced Performance Routing" module
IP SLAs overview	*IP SLAs Configuration Guide*
PfR home page with links to PfR-related content on our DocWiki collaborative environment	PfR:Home

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 PfR Voice Traffic Optimization Using Active Probes

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 16: Feature Information for PfR Voice Traffic Optimization Using Active Probes

Feature Name	Releases	Feature Information
PfR Voice Traffic Optimization	12.4(6)T 12.2(33)SRB	The PfR Voice Traffic Optimization feature provides support for outbound optimization of voice traffic based on the voice metrics, jitter and Mean Opinion Score (MOS). Jitter and MOS are important quantitative quality metrics for voice traffic and these voice metrics are measured using PfR active probes. The following commands were introduced or modified by this feature: **active-probe (PfR)**, **jitter (PfR)**, **mos (PfR)**, **resolve (PfR)**, **set active-probe (PfR)**, **set jitter (PfR)**, **set mos (PfR)**, **set probe (PfR)**, **set resolve (PfR)**, **show pfr master active-probes**, **show pfr master policy**, and **show pfr master prefix**.

INDEX

N