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.

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** **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 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*.

	Command or Action	Purpose
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* **Example:** `Router(config-pfr-mc-learn)# list seq 10 refname LEARN_USER_DEFINED_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_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*]	Defines a PfR traffic class using an access list.

	Command or Action	Purpose
	Example: `Router(config-pfr-mc-learn-list)# traffic-class access-list USER_DEFINED_TC`	• 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.
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.	--

	Command or Action	Purpose
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.

	Command or Action	Purpose
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.
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.
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 GigabitEthernet 0/0/0 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.

	Command or Action	Purpose
		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.
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.

	Command or Action	Purpose
		• 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.

	Command or Action	Purpose
Step 9	**mode monitor** {**active** | **both** | **passive**} **Example:** `Router(config-pfr-mc)# mode monitor active`	Configures route monitoring on a PfR master controller. • 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.

	Command or Action	Purpose
		• 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* **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 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

	Command or Action	Purpose
		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.
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.
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.

	Command or Action	Purpose
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.
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

	Command or Action	Purpose
		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*} **Example:** `Router(config-pfr-map)# set delay relative 50`	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 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:**	Creates a set clause entry to set the frequency of the PfR active probe.

	Command or Action	Purpose
	`Router(config-pfr-map)# set probe frequency 2`	• 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**]]] **Example:** `Router# show pfr master prefix 10.1.1.0/24 policy`	(Optional) Displays the status of monitored prefixes. • The *prefix*argument is entered as an IP address and bit length mask. • 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.

	Command or Action	Purpose
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 GigabitEthernet 0/0/0`	Configures an interface on a border router as the active-probe source. • The example configures interface GigabitEthernet 0/0/0 as the source interface.
Step 5	**end** **Example:** `Router(config-pfr-br)# end`	Exits PfR border router configuration mode and enters privileged EXEC mode.
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.

	Command or Action	Purpose
		• 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. • 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.

	Command or Action	Purpose
		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**}} **Example:** `Router(config-pfr-mc)# mode select-exit good`	Enables the exit link selection based on performance or policy. • 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.

	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 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*} **Example:** `Router(config)# ip prefix-list DENY_LIST deny 172.20.1.0/24`	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 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.

	Command or Action	Purpose
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.
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.
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.
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.

	Command or Action	Purpose
		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:**	Creates an IP prefix list. • IP prefix lists are used to manually select prefixes for monitoring by the PfR master controller.

	Command or Action	Purpose
	`Router(config)# ip prefix-list BLACK_HOLE_LIST seq 10 permit 10.20.21.0/24`	• 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. • 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.

	Command or Action	Purpose
		• 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.
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**] **Example:** `Router(config-ext-nacl)# permit tcp 192.168.1.0 0.0.0.255 any eq telnet`	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
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*} **Example:** `Router(config-pfr-map)# set resolve delay priority 1 variance 20`	(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.
Step 11	**end** **Example:** `Router(config-pfr-map)# end`	Exits PfR map configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
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 Optimized Edge 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.

The following example, using optional delimiters, shows the logging buffer with PfR messages for the prefix 10.1.1.0 that is OOP and has a route change.

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 Gi0/0/1
*Apr 26 23:03:14.987: %OER_MC-5-NOTICE: Route changed 10.1.1.0/24, BR 10.10.10.1, i/f
Gi0/2/0, 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 Gi0/2/0, 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
Gi0/0/1, Reason Delay, OOP Reason Loss
```

In the following example, the logging buffer contains an informational PfR message for the prefix 192.168.3.4. The message shows that due to load balancing, traffic is identified as being out-of-policy(OOP) and the traffic path has changed due to IGP, BGP or static routing. (The traffic path is not changed by PfR.)

Example:

```
Router# show logging | i 192.168.3.4
%PFR_MC-6-ROUTE_EVENT_INFO: Prefix 192.168.3.4/24: route changed to BR
10.10.10.10, i/f Gi0/0/0.100, due to routing protocol >PfR is unware.
Out of policy reason: load-balance criteria
```

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   Gi0/0/1     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.

Example:

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 GigabitEthernet 0/0/0 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 GigabitEthernet0/0/0 external
  interface GigabitEthernet0/4/2 internal
 !
 border 10.3.3.4 key-chain key2
  interface GigabitEthernet0/0/2 external
  interface GigabitEthernet0/0/1 internal
 !
 border 10.4.4.2 key-chain key3
  interface GigabitEthernet0/2/0 external
  interface GigabitEthernet0/2/1 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 Gi0/0/2
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 Gi0/0/3, 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 GigabitEthernet 0/0/0
```

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 PfR Load Balancing 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 GigabitEthernet 0/0/0 external
 max-xmit-utilization absolute 10000
 exit
 exit
 border 10.1.2.1
 interface GigabitEthernet 0/0/2 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
```

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

Related Topic	Document Title
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
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 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 1: Feature Information for Configuring Advanced 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. 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, PfR master controller functionality is supported.
OER Support for Policy-Rules Configuration	Cisco IOS XE Release 3.3S	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[1]	Cisco IOS XE Release 3.3S	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	Cisco IOS XE Release 3.3S	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	Cisco IOS XE Release 3.3S	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 Information
OER DSCP Monitoring	Cisco IOS XE Release 3.3S	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)**.
Performance Routing - Link Groups	Cisco IOS XE Release 3.3S	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[2]	Cisco IOS XE Release 3.3S	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.