Cisco IOS Performance Routing Command Reference

July 2010

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

Customer Order Number:

CONTENTS

Introduction

This document describes the commands used to configure Cisco IOS Performance Routing (PfR). For information about PfR configuration, refer to the *Cisco IOS Performance Routing Configuration Guide*.

PfR Commands

active-probe (PfR)

To configure a Performance Routing (PfR) active probe for a target prefix, use the **active-probe** command in PfR master controller configuration mode. To disable the active probe, use the **no** form of this command.

active-probe *probe-type ip-address* **target-port** *number* [**codec** *codec-name*]

no active-probe *probe-type ip-address*

Syntax Description

probe-type	Type of probe. Must be one of the following: • **echo—**Uses Internet Control Message Protocol (ICMP) echo (ping) messages. • **jitter—**Uses jitter messages. • **tcp-conn—**Uses TCP connection messages. • **udp-echo—**Uses UDP echo messages.
ip-address	Target IP address of a prefix to be monitored using the specified type of probe.
target-port	(Not specified for echo probes.) Specifies the destination port number for the active probe.
number	Port number in the range from 1 to 65535.
codec	(Optional) Only used with the jitter probe type. Specifies the codec value used for Mean Opinion Score (MOS) calculation.
codec-name	(Optional) Codec value, must be one of the following: • **g711alaw—**G.711 A Law 64000 bps. • **g711ulaw—**G.711 U Law 64000 bps. • **g729a—**G.729 8000 bps.

Command Default

No active probes are configured.

Command Modes

PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **active-probe** command is entered on a PfR master controller.

This command is used to optionally configure a master controller to command a border router to transmit active probes to a target IP address or prefix. The active probe is used to measure the delay (round-trip response time) of the target prefix to determine the performance of the current exit and to detect if the prefix is out-of-policy. The border router collects these performance statistics from the active probe and

transmits this information to the master controller, which uses this information to optimize the prefix and to select the best available exit based on default and user-defined policies. The performance information is applied to the most specific optimized prefix, which includes the active probe host address. If the prefix is optimized and is currently using the best in-policy exit link, the master controller does not take any action.

Active probing requires you to configure a specific host or target address. The target address can also be learned by PfR through the NetFlow or Top Talker and Delay learning functionality. Active probes must be sent out of a PfR-managed external interface, which may or may not be the preferred route for an Optimized Prefix (OP). PfR can be configured to use the following four types of active probes:

- ICMP Echo—A ping is sent to the target address. Configuring an ICMP echo probe does not require knowledgeable cooperation from the target device. However, repeated probing could trigger an Intrusion Detection System (IDS) alarm in the target network. If an IDS is configured in a target network that is not under your administrative control, we recommend that you notify the target network administration entity.
- Jitter—A jitter probe is sent to the target address. A target port number must be specified. A remote responder must be enabled on the target device, regardless of the configured port number. An optional codec value can be configured. The codec value is required for Mean Opinion Score (MOS) calculations.

Note In Cisco IOS Release 15.1(2)T and later releases, when you configure a jitter probe the default codec value, g729a, is not nvgened in the running configuration. In Cisco IOS Release 15.1(1)T, 12.2(33(SRE), 12.2(33)SXH, and prior releases, if you did not specify a codec value while configuring the **active-probe jitter** command, the default codec value, g729a, was displayed in the output of the **show running-config** command.

- TCP Connection—A TCP connection probe is sent to the target address. A target port number must be specified. A remote responder must be enabled if TCP messages are configured to use a port number other than TCP well-known port number 23.
- UDP Echo—A UDP echo probe is sent to the target address. A target port number must be specified. A remote responder must be enabled on the target device, regardless of the configured port number.

PfR uses Cisco IOS IP Service Level Agreements (SLAs), a standard feature in Cisco IOS software, to command a border router to transmit an active probe to the target address. No explicit IP SLA configuration is required on the master controller or the border router. Support for IP SLAs is enabled by default when the PfR process is created. However, a remote responder must be enabled on the target device when configuring an active probe using jitter, UDP echo messages, or when configuring an active probe using TCP connection messages that are configured to use a port other than the TCP well-known port number 23. The remote responder is enabled by configuring the **ip sla monitor responder** global configuration command on the target device.

Note For external BGP (eBGP) peering sessions, the IP address of the eBGP peer must be reachable from the border router via a connected route in order for active probes to be generated.

Examples

The following example configures an active probe using an ICMP reply (ping) message. The 10.4.9.1 address is the target. No explicit configuration is required on the target device.

```
Router(config)# pfr master
Router(config-pfr-mc)# active-probe echo 10.4.9.1
```

The following example configures an active probe using jitter messages. The 10.4.9.2 address is the target. The target port number must be specified when configuring this type of probe, and a remote responder must also be enabled on the target device. An optional codec value of g711alaw is specified to be used for MOS calculations.

```
Router(config)# pfr master
Router(config-pfr-mc)# active-probe jitter 10.4.9.2 target-port 1001 codec g711alaw
```

The following example configures an active probe using a TCP connection message. The 10.4.9.3 address is the target. The target port number must be specified when configuring this type of probe.

```
Router(config)# pfr master
Router(config-pfr-mc)# active-probe tcp-conn 10.4.9.3 target-port 23
```

The following example configures an active probe using UDP messages. The 10.4.9.4 address is the target. The target port number must be specified when configuring this type of probe, and a remote responder must also be enabled on the target device.

```
Router(config)# pfr master
Router(config-pfr-mc)# active-probe udp-echo 10.4.9.4 target-port 1001
```

Related Commands

Command	Description
ip sla monitor responder	Enables the IP SLAs Responder for general IP SLAs operations.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
set active-probe (PfR)	Configures a PfR active probe with a forced target assignment within a PfR map.
show pfr border active-probes	Displays connection and status information about active probes on a PfR border router.
show pfr master active-probes	Displays connection and status information about active probes on a PfR master controller.

active-probe address source (PfR)

To configure an interface on a Performance Routing (PfR) border router as the source of the active probe, use the **active-probe address source** command in PfR border router configuration mode. To configure active probing to use a default exit interface, use the **no** form of this command.

active-probe address source interface *type number*

no active-probe address source interface

Syntax Description

interface	Specifies the interface type and number.
type	Interface type.
number	Interface or subinterface number.

Command Default

The source IP address is taken from the default PfR external interface that transmits the active probe.

Command Modes

PfR border router configuration (config-pfr-br)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **active-probe address source** command is entered on a border router and allows you to specify the source interface from which active probes are transmitted. When this command is configured, the primary IP address of the specified interface is used as the active probe source. The IP address of the active probe source interface must be unique to ensure that the probe reply is routed back to the specified source interface. If the interface is not configured with an IP address, the active probe will not be generated. If the IP address is changed after the interface has been configured as an active probe source, active probing is stopped and then restarted with the new IP address. If the IP address is removed after the interface has been configured as an active probe source, active probing is stopped and is not restarted until a valid primary IP address is reconfigured.

Note For external Border Gateway Protocol (eBGP) peering sessions, the IP address of the eBGP peer must be reachable from the border router via a connected route in order for active probes to be generated.

Examples

The following example configures Fast Ethernet interface 0/0 as the active probe source:

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

The following example configures Gigabit Ethernet interface 0/0/0 as the active probe source:

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

Related Commands

Command	Description
active-probe (PfR)	Configures an active probe for a target prefix.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
set active-probe (PfR)	Configures a PfR active probe with a forced target assignment within a PfR map.

aggregation-type (PfR)

To configure a Performance Routing (PfR) master controller to aggregate learned prefixes based on the type of traffic flow, use the **aggregation-type** command in PfR Top Talker and Top Delay learning configuration mode. To set learned prefix aggregation to the default type, use the **no** form of this command.

aggregation-type {**bgp** | **non-bgp** | **prefix-length** *prefix-mask*}

no aggregation-type

Syntax Description

bgp	Configures the aggregation of learned prefixes based on the Border Gateway Protocol (BGP) routing table.
non-bgp	Configures the aggregation of learned prefixes based on any other protocol. Prefixes specified with this keyword can be learned only if they are not in the BGP routing table.
prefix-length	Configures aggregation based on the specified prefix length.
prefix-mask	Prefix mask in the range from 1 to 32. Default is 24.

Command Default

If this command is not configured or if the **no** form of this command is entered, the default prefix mask for aggregating learned prefixes is 24.

Command Modes

PfR Top Talker and Top Delay learning configuration (config-pfr-mc-learn)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **aggregation-type** command is entered on a master controller. This command is used to configure PfR to aggregate learned prefixes based on the traffic flow type. BGP prefixes or non-BGP prefixes can be aggregated, and traffic flows can be aggregated based on prefix length.

Entering the **bgp** keyword configures the aggregation of learned prefixes based on prefix entries in the BGP routing table. This keyword is used if internal BGP (iBGP) peering is enabled in the PfR managed network.

Entering the **non-bgp** keyword configures the aggregation of learned prefixes based on any other routing protocol. Prefix entries that are present in the BGP routing table are ignored when this keyword is entered.

Examples

The following example configures the aggregation of learned BGP prefixes:

```
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# aggregation-type bgp
```

Related Commands

Command	Description
learn (PfR)	Enters PfR Top Talker and Top Delay learning configuration mode to configure prefixes for PfR to learn.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

api provider (PfR)

To register an application programming interface (API) provider with a Performance Routing (PfR) master controller and to enter PfR master controller application interface provider configuration mode, use the **api provider** command in PfR master controller configuration mode. To unregister the application interface provider, use the **no** form of this command.

api provider *provider-id* [**priority** *value*]

no api provider *provider-id*

Syntax Description

provider-id	A number in the range from 1 to 65535 that represents the ID assigned to the provider. API provider IDs in the range of 1 to 100 are reserved for internal Cisco applications.
priority	(Optional) Sets the priority of the provider.
value	(Optional) A number in the range from 1 to 65535. The lower the number, the higher the priority. The default priority is 65535. API provider priority values in the range of 1 to 100 are reserved for internal Cisco applications.

Command Default

An API provider is not registered with a PfR master controller.

Command Modes

PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The PfR application interface defines the mode of communication and messaging between applications and the network for the purpose of optimizing the traffic associated with the applications. A provider is defined as an entity outside the network in which the router configured as a PfR master controller exists, for example, an ISP, or a branch office of the same company. The provider has one or more host devices running one or more applications that use the PfR application interface to communicate with a PfR master controller. A provider must be registered with a PfR master controller before an application on a host device can interface with PfR. Use the **api provider** command to register the provider, and use the **host-address** (PfR) command to configure a host device. After registration, a host device in the provider network can initiate a session with a PfR master controller. The PfR application interface provides an automated method for networks to be aware of applications and provides application-aware performance routing.

Use the optional **priority** keyword to specify a priority value for the provider when multiple providers are registered with PfR. The number 1 assigns the highest priority to any requests through the application interface. If you assign a priority, each provider must be assigned a different priority number. If you try to assign the same priority number to two different providers, an error message is displayed on the console.

Note API provider IDs and API priority values in the range of 1 to 100 are reserved for internal Cisco applications.

Use the **show pfr api provider** command to view information about the currently registered providers. Use the **show pfr master policy** command with the **dynamic** keyword to display information about policies created dynamically by an application using the PfR application interface.

Examples

The following example shows how to register a provider on a master controller. In this example, more than one provider is configured, so the priority is set for each provider. For the single host device configured for provider 101, no priority is set and the default priority value of 65535 is assigned, giving this host device a lower priority than each of the host devices configured for provider 102.

```
Router(config)# pfr master
Router(config-pfr-mc)# api provider 101
Router(config-pfr-mc-api-provider)# host-address 10.1.2.2 key-chain PFR_HOST
Router(config-pfr-mc-api-provider)# exit
Router(config-pfr-mc)# api provider 102 priority 4000
Router(config-pfr-mc-api-provider)# host-address 10.2.2.2 key-chain PFR_HOST
priority 3000
Router(config-pfr-mc-api-provider)# host-address 10.2.2.3 key-chain PFR_HOST
priority 4000
Router(config-pfr-mc-api-provider)# end
```

Related Commands

Command	Description
host-address (PfR)	Configures information about a host device used by an application interface provider to communicate with a PfR master controller.
pfr master	Enables a PfR process and configures a router as a PfR master controller.
show pfr api provider	Displays information about application interface providers registered with PfR.
show pfr master policy	Displays policy settings on a PfR master controller.

application define (PfR)

To configure a user-defined custom application to be monitored by Performance Routing (PfR), use the **application define** command in PfR master controller configuration mode. To remove the definition of a user-defined custom application to be monitored by PfR, use the **no** form of this command.

application define *application-name* {**access-list** *access-list-name* | **nbar**}

no application define *application-name*

Syntax Description

application-name	Name of the user-defined custom application.
access-list	Defines an application using an access list.
access-list-name	Name of an access list.
nbar	Defines a user-defined custom application to be identified using Network-Based Application Recognition (NBAR).

Command Default

No custom-defined applications are configured for use with PfR.

Command Modes

PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **application define** command allows a user-defined custom application to be configured on the master controller as an application that can be used in PfR configuration to create a traffic class that can be measured and controlled using PfR techniques. An access list can be used to define the traffic flows to create a custom application.

PfR supports the ability to define a custom application to be identified using NBAR. NBAR includes many defined applications, but a Packet Description Language Module (PDLM) can be used to add a new protocol to the list of supported NBAR applications. A PDLM uses a mapping of static TCP and UDP port numbers to create a custom application. The application defined by a PDLM file must be recognized on a PfR border router and configured on the master controller using the **application define** command. The PfR master controller makes a request to the border router to determine if the application is supported. Use the **show pfr master nbar application** command to check if the application is supported on each border router.

To display defined applications, use the **show pfr master defined** or the **show pfr border defined** commands.

Examples

The following example, starting in global configuration mode, shows how to define a custom application named ACCESS_DEFINE using an access list. The access list is configured to identify all TCP traffic from any destination or source and from a destination port number of 500.

```
Router(config)# ip access-list ACCESS_DEFINE
Router(config-ext-nacl)# permit tcp any any 500
Router(config-ext-nacl)# exit
Router(config)# pfr master
Router(config-pfr-mc)# application define APP_ACCESS access-list ACCESS_DEFINE
Router(config-pfr-mc)# end
```

The following example, starting in global configuration mode, shows how to define a custom application named APP_NBAR1 to be identified using NBAR and used in PfR configuration to create a traffic class that can be measured and controlled using PfR techniques.

```
Router(config)# pfr master
Router(config-pfr-mc)# application define APP_NBAR1 nbar
Router(config-pfr-mc)# end
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
show pfr border defined	Displays all applications that are defined to be monitored by a PfR border router.
show pfr master defined	Displays all applications that are defined on a PfR master controller.
show pfr master nbar application	Displays information about the status of an application identified using NBAR for each PfR border router.

backoff (PfR)

To set the backoff timer to adjust the time period for prefix policy decisions, use the **backoff** command in PfR master controller configuration mode. To set the backoff timer to the default values, use the **no** form of this command.

backoff *min-timer max-timer* [*step-timer*]

no backoff

Syntax Description

min-timer	Sets the minimum value for the backoff timer in seconds. The configurable time period for this argument is from 180 to 7200. The default timer value is 300.
max-timer	Sets the maximum value for the backoff timer in seconds. The configurable time period for this argument is from 180 to 7200. The default timer value is 3000.
step-timer	(Optional) Sets the value of the time period for the step timer in seconds. The step timer is used to add time to the out-of-policy waiting period each time the backoff timer expires and Performance Routing (PfR) is unable to find an in-policy exit. The configurable time period for this argument is from 180 to 7200. The default timer value is 300.

Command Default

PfR uses the following default values if this command is not configured or if the **no** form of this command is entered:

min-timer: 300
max-timer: 3000
step-timer: 300

Command Modes

PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **backoff** command is entered on a PfR master controller. This command is used to adjust the transition period during which the master controller holds an out-of-policy prefix. The master controller waits for the transition period before making an attempt to find an in-policy exit. This command is configured with a minimum and maximum timer value and can be configured with an optional step timer.

The *min-timer* argument is used to set the minimum transition period in seconds. If the current prefix is in-policy when this timer expires, no change is made and the minimum timer is reset to the default or configured value. If the current prefix is out-of-policy, PfR will move the prefix to an in-policy and reset the minimum timer to the default or configured value.

The *max-timer* argument is used to set the maximum length of time PfR holds an out-of-policy prefix when there are no PfR controlled in-policy prefixes. If all PfR controlled prefixes are in an out-of-policy state and the value from the *max-timer* argument expires, PfR will select the best available exit and reset the minimum timer to the default or configured value.

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. If the maximum timer expires and all PfR managed exits are out-of-policy, PfR will install the best available exit and reset the minimum timer.

Configuring a new timer value will immediately replace the existing value if the new value is less than the time remaining. If the new value is greater than the time remaining, the new timer value will be used when the existing timer value expires.

Examples

The following example sets the minimum timer to 400 seconds, the maximum timer to 4000 seconds, and the step timer to 400 seconds:

```
Router(config)# pfr master
Router(config-pfr-mc)# backoff 400 4000 400
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
set backoff (PfR)	Configures a PfR map to set the backoff timer to adjust the time period for prefix policy decisions.

border (PfR)

To enter PfR managed border router configuration mode to establish communication with a Performance Routing (PfR) border router, use the **border** command in PfR master controller configuration mode. To disable communication with the specified border router, use the **no** form of this command.

border *ip-address* [**key-chain** *key-name*]

no border *ip-address*

Syntax Description

ip-address	IP address of the border router.
key-chain	(Optional) Specifies the key used to authenticate communication between the border router and the master controller. The authentication key must be specified during the initial configuration to establish communication, but is not required to enter PfR managed border router configuration mode.
key-name	(Optional) String that represents a key.

Command Default

No communication is established between a PfR border router and a master controller.

Command Modes

PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **border** command is entered on a master controller. This command is used to establish communication between a master controller and a border router. Border key-chain configuration is required during initial configuration. Once configured, the **key-chain** keyword is optional. Communication is established between the master controller and the border router processes to allow the master controller to monitor and control prefixes and exit links. Communication must also be established on the border router using the **master** command. Passive monitoring in PfR observe mode is enabled by default when communication is established between a PfR border router and a master controller.

At least one border router must be configured to enable PfR. A maximum of ten border routers can be configured to communicate with a single master controller. The IP address that is used to specify the border router must be assigned to an interface that is physically located on the border router and the IP address must be reachable by the master controller.

Communication between the master controller and the border router is protected by key-chain authentication. The authentication key must be configured on both the master controller and the border router before communication can be established. The key-chain configuration is defined in global configuration mode on both the master controller and the border router before key-chain authentication is enabled for master controller to border router communication. For more information about key management in Cisco IOS software, see the "Managing Authentication Keys" section in the "Configuring IP Protocol-Independent Features" chapter of the *Cisco IOS IP Routing: Protocol-Independent Configuration Guide*.

When the **border** command is entered, the router enters PfR managed border router configuration mode. Local interfaces must be defined as internal or external using the **interface** (PfR) command. A single PfR master controller can support up to 20 interfaces.

Enabling a Border Router and Master Controller Process on the Same Router

A Cisco router can be configured to perform in dual operation and run a master controller process and a border router process on the same router. However, this router will use more memory than a router that is configured to run only a border router process. This factor should be considered when selecting a router for dual operation.

Examples

The following example defines a key chain named MASTER in global configuration mode and then configures a master controller to communicate with the 10.4.9.6 border router. The master controller authenticates the border router using the defined key CISCO.

```
Router(config)# key chain MASTER
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string CISCO
Router(config-keychain-key)# exit
Router(config-keychain)# exit
Router(config)# pfr master
Router(config-pfr-mc)# logging
Router(config-pfr-mc)# border 10.4.9.6 key-chain MASTER
Router(config-pfr-mc-br)# interface FastEthernet0/0 external
Router(config-pfr-mc-br)# interface FastEthernet0/1 internal
```

Related Commands

Command	Description
interface (PfR)	Configures a border router interface as a PfR-controlled external or internal interface.
key	Identifies an authentication key on a key chain.
key chain (IP)	Enables authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
master (PfR)	Establishes communication with a PfR master controller.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

clear pfr border

To reset a connection between a Performance Routing (PfR) border router and the PfR master controller, use the **clear pfr border** command in privileged EXEC mode.

clear pfr border *

Syntax Description

*	Clears a connection between a border router and the master controller.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **clear pfr border** command is entered on a border router. The border router and master controller will automatically reestablish communication after this command is entered.

Examples

The following example resets a connection between a border router and a master controller:

```
Router# clear pfr border *
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

clear pfr master

To reset a connection between a Performance Routing (PfR) master controller process and all active border router connections, use the **clear pfr master** command in privileged EXEC mode.

clear pfr master *

Syntax Description

*	Clears the master controller process and all active border router connections.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **clear pfr master** command is entered on a master controller. The master controller will restart all configured and default processes and reestablish communication with active border routers after this command is entered.

Examples

The following example resets the master controller process and all active border router connections:

```
Router# clear pfr master *
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

clear pfr master border

To reset an active Performance Routing (PfR) border router connection or all connections with a PfR master controller, use the **clear pfr master border** command in privileged EXEC mode.

clear pfr master border {***** | *ip-address*}

Syntax Description

*****	Specifies all active border router connections.
ip-address	Specifies a single border router connection.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **clear pfr master border** command is entered on a master controller.

Examples

The following example resets all border router connections to the master controller:

```
Router# clear pfr master border *
```

The following example resets a single border router connection to the master controller:

```
Router# clear pfr master border 10.4.9.6
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

clear pfr master prefix

To clear Performance Routing (PfR) controlled prefixes from the master controller database, use the **clear pfr master prefix** command in privileged EXEC mode.

clear pfr master prefix {***** | *prefix* | **inside *** | **learned** [**inside**]}

Syntax Description

*****	Clears all prefixes.
prefix	Clears a single prefix or prefix range. The prefix address and mask are entered with this argument.
inside	Clears inside prefixes.
learned	Clears learned prefixes.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **clear pfr master prefix** command is entered on a master controller.

Examples

The following example clears learned prefixes:

```
Router# clear pfr master prefix learned
```

The following example clears all inside prefixes:

```
Router# clear pfr master prefix inside *
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

clear pfr master traffic-class

To clear Performance Routing (PfR) controlled traffic classes from the master controller database, use the **clear pfr master traffic-class** command in privileged EXEC mode.

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*]

Syntax Description

access-list	(Optional) Clears information about traffic classes defined by an access list.
access-list-name	(Optional) Name of an access list.
application	(Optional) Clears information about traffic classes defined by an application.
application-name	(Optional) Name of a predefined static application using fixed ports. See Table 1.
prefix	(Optional) An IP address and bit length mask representing a prefix to be cleared.
inside	(Optional) Clears information about inside traffic classes.
learned	(Optional) Clears information about learned traffic classes.
delay	(Optional) Clears information about learned traffic classes defined using delay.
list	(Optional) Clears information about learned traffic classes defined in a PfR learn list.
list-name	(Optional) Name of a PfR learn list.
throughput	(Optional) Clears information about learned traffic classes defined using throughput.
prefix	(Optional) Clears information about traffic classes defined by a prefix.
prefix-list	(Optional) Clears information about traffic classes defined by a prefix list.
prefix-list-name	(Optional) Name of prefix list.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **clear pfr master traffic-class** command is entered on a master controller. To clear PfR-controlled traffic classes defined by an application identified using Network-Based Application Recognition (NBAR) from the master controller database, use the **clear pfr master traffic-class application nbar** command.

Table 1 displays the keywords that represent the application that can be configured with the **clear pfr master traffic-class** command. Replace the *application-name* argument with the appropriate keyword from the table.

Table 1 Static Application List Keywords

Keyword	Protocol	Port
cuseeme	TCP UDP	7648 7649 7648 7649 24032
dhcp (Client)	UDP/TCP	68
dhcp (Server)	UDP/TCP	67
dns	UDP/TCP	53
finger	TCP	79
ftp	TCP	20 21
gopher	TCP/UDP	70
http	TCP/UDP	80
httpssl	TCP	443
imap	TCP/UDP	143 220
irc	TCP/UDP	194
kerberos	TCP/UDP	88 749
l2tp	UDP	1701
ldap	TCP/UDP	389
mssql	TCP	1443
nfs	TCP/UDP	2049
nntp	TCP/UDP	119
notes	TCP/UDP	1352
ntp	TCP/UDP	123
pcany	UDP TCP	22 5632 65301 5631
pop3	TCP/UDP	110
pptp	TCP	17233
simap	TCP/UDP	585 993 (Preferred)
sirc	TCP/UDP	994
sldap	TCP/UDP	636
smtp	TCP	25
snntp	TCP/UDP	563
spop3	TCP/UDP	123
ssh	TCP	22
telnet	TCP	23

Examples

The following example shows how to clear traffic classes defined by the Secure Shell (SSH) application and the 10.1.1.0/24 prefix:

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

The following example shows how to clear traffic classes that were learned:

```
Router# clear pfr master traffic-class learned
```

Related Commands

Command	Description
clear pfr master traffic-class application nbar	Clears PfR-controlled traffic classes defined by an application identified using NBAR from the master controller database.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

clear pfr master traffic-class application nbar

To clear Performance Routing (PfR) controlled traffic classes defined by an application identified using Network-Based Application Recognition (NBAR) from the master controller database, use the **clear pfr master traffic-class application nbar** command in privileged EXEC mode.

clear pfr master traffic-class application nbar [*nbar-appl-name* [*prefix*]]

Syntax Description

nbar-appl-name	(Optional) Keyword representing the name of an application identified using NBAR. See the "Usage Guidelines" section for more details.
prefix	(Optional) An IP address and bit length mask representing a prefix to be cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **clear pfr master traffic-class application nbar** command is entered on a master controller. To clear all other types of PfR-controlled traffic classes from the master controller database, use the **clear pfr master traffic-class** command.

NBAR is capable of identifying applications based on the following three types of protocols:

- Non-UDP and non-TCP IP protocols—For example, Generic Routing Encapsulation (GRE) and Internet Control Message Protocol (ICMP).
- TCP and UDP protocols that use statically assigned port numbers—For example, CU-SeeMe desktop video conference (CU-SeeMe-Server) and Post Office Protocol over Transport Layer Security (TLS) and Secure Sockets Layer (SSL) server (SPOP3-Server).
- TCP and UDP protocols that dynamically assign port numbers and require stateful inspection—For example, Real-Time Transport Protocol audio streaming (RTP-audio) and BitTorrent File Transfer Traffic (BitTorrent).

Use the **clear pfr master traffic-class application nbar ?** command to determine if an application can be identified using NBAR and replace the *nbar-appl-name* argument with the appropriate keyword from the screen display.

The list of applications identified using NBAR and available for profiling PfR traffic classes is constantly evolving. For lists of many of the NBAR applications defined using static or dynamically assigned ports, see the "Performance Routing with NBAR/CCE Application and Recognition" module.

For more details about NBAR, see the "Classifying Network Traffic Using NBAR" section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

If the *prefix* argument is specified, only the PfR-controlled traffic class that matches the application specified by the *nbar-appl-name* argument and the destination prefix specified by the *prefix* argument are cleared. If the *prefix* argument is not specified, all PfR-controlled traffic classes that match the application specified by the *nbar-appl-name* argument, regardless of the destination prefix, are cleared.

Examples

The following example shows how to determine the keyword that represents an application identified using NBAR in order to clear the PfR traffic classes defined by the application:

```
Router# clear pfr master traffic-class application nbar ?
```

The following example shows how to clear PfR traffic classes defined by the RTP-audio application that is identified using NBAR and the 10.1.1.0/24 prefix:

```
Router# clear pfr master traffic-class application nbar rtp-audio 10.1.1.0/24
```

The following example shows how to clear all PfR traffic classes defined by applications identified using NBAR:

```
Router# clear pfr master traffic-class application nbar
```

Related Commands

Command	Description
clear pfr master traffic-class	Clears PfR-controlled traffic classes from the master controller database.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

cost-minimization (PfR)

To configure Performance Routing (PfR) cost-based optimization policies on a master controller, use the **cost-minimization** command in PfR border exit interface configuration mode. To disable a cost-based optimization policy, use the **no** form of this command.

cost-minimization {**calc** {**combined** | **separate** | **sum**} | **discard** [**daily**] {**absolute** *number* | **percent** *percentage*} | **end day-of-month** *day* [**offset** [**-**] *hh:mm*] | **fixed fee** [*cost*] | **nickname** *name* | **sampling period** *minutes* [**rollup** *minutes*] | **summer-time** *start end* [*offset*] | **tier** *percentage* **fee** *fee*}

no cost-minimization {**calc** | **discard** | **end day-of-month** *day* [**offset** [**-**] *hh:mm*] | **fixed fee** [*cost*] | **nickname** | **sampling period** | **summer-time** | **tier** *percentage*}

Syntax Description

calc	Specifies how the fee is calculated.
combined	Specifies billing based on combined egress and ingress rollup samples.
separate	Specifies billing based on separate egress and ingress rollup samples.
sum	Specifies billing based on egress and ingress rollup samples that are added and then combined.
discard	Specifies how often rollup samples are discarded.
daily	(Optional) Specifies a daily rather than monthly rollup period.
absolute *number*	Specifies an absolute number of rollup samples to be discarded. The value that can be entered for the *number* argument ranges from 1 to 1440.
percent *percentage*	Specifies a percentage of rollup samples to be discarded. The value that can be entered for the *percentage* argument ranges from 1 to 99.
end day-of-month *day*	Specifies the end billing date.
offset [**-**] *hh***:***mm*	(Optional) Specifies an offset in hours and minutes, allowing you to compensate for time zone differences. The optional "**-**" keyword is used to allow for negative hours and minutes to be specified when the time zone is ahead of UTC.
fixed fee	Specifies a nonusage-based fixed fee.
cost	(Optional) Cost for the fixed fee.
nickname *name*	Specifies a nickname for the cost structure.
sampling period *minutes*	Specifies the sampling period in minutes. The value that can be entered for the *minutes* argument ranges from 1 to 1440.
rollup *minutes*	(Optional) Specifies that samples are rolled up at the interval specified for the *minutes* argument. The value that can be entered for the *minutes* argument ranges from 1 to 1440. The minimum number that can be entered must be equal to or greater than the number that is entered for the sampling period.
summer-time	Specifies the start and end of summer time.
start	The start period is entered in following format: the week number or the words first or last, the day represented by the first three letters of the day, the month represented by the first three letters of the month, and hh:mm. For example, 1 Sun Apr 00:00.

end	The end period is entered in following format: the week number or the words first or last, the day represented by the first three letters of the day, the month represented by the first three letters of the month, and hh:mm. For example, 4 Sun Oct 23:59.
offset	(Optional) The *offset* argument allows for an offset in minutes from 1 to 120 to allow for up to two additional hours to be added in the spring and subtracted in the fall.
tier	Specifies a cost tier.
percentage	A percentage of capacity for a cost tier.
fee *fee*	Specifies the fee associated with a cost tier.

Command Default

No cost-based optimization policies are configured.

Command Modes

PfR border exit interface configuration (config-pfr-mc-br-if)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **cost-minimization** command is configured on a master controller. Cost-based optimization allows you to configure link policies based on the Internet service provider (ISP) financial cost of each exit link in your network. The **cost-minimization** command allows you to configure the master controller to send traffic over exit links that provide the most cost-effective bandwidth utilization, while still maintaining the desired performance characteristics.

Examples

The following example, starting in global configuration mode, configures cost-based optimization on a master controller. Cost optimization configuration is applied under the external interface configuration. A policy for a tiered billing cycle is configured. Calculation is configured separately for egress and ingress samples. The time interval between sampling is set to 10 minutes. These samples are configured to be rolled up every 60 minutes. In this example, summer time is configured to start the second week in March on a Sunday at 2 in the morning plus one hour, and to end on Sunday in the first week in November at 2 in the morning minus one hour. The last day of the billing cycle is on the 30th day of the month with an offset of 5 hours added to UTC to adjust for the time zone.

```
Router(config)# pfr master
Router(config-pfr-mc)# border 10.5.5.55 key-chain key
Router(config-pfr-mc-br)# interface Ethernet 0/0 external
Router(config-pfr-mc-br-if)# cost-minimization nickname ISP1
Router(config-pfr-mc-br-if)# cost-minimization summer-time 2 Sun Mar 02:00
1 Sun Nov 02:00 60
Router(config-pfr-mc-br-if)# cost-minimization end day-of-month 30 offset 23:59
Router(config-pfr-mc-br-if)# cost-minimization calc separate
Router(config-pfr-mc-br-if)# cost-minimization sampling period 10 rollup 60
Router(config-pfr-mc-br-if)# cost-minimization tier 100 fee 1000
Router(config-pfr-mc-br-if)# cost-minimization tier 90 fee 900
Router(config-pfr-mc-br-if)# cost-minimization tier 80 fee 800
Router(config-pfr-mc-br-if)# end
```

Related Commands

Command	Description
debug pfr master cost-minimization	Displays debugging information for cost-based optimization policies.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
show pfr master cost-minimization	Displays the status of cost-based optimization policies.

count (PfR)

To set the number of traffic classes to be learned by a learn list during a Performance Routing (PfR) learn session, use the **count** command in learn list configuration mode. To reset the number of traffic classes to be learned by a learn list to the default values, use the **no** form of this command.

count *number* **max** *max-number*

no count *number* **max** *max-number*

Syntax Description

number	Number representing the number of traffic classes to be learned by a learn list during a PfR learn session. The range of numbers is from 1 to 100. The default is 50.
max	Specifies the maximum number of traffic classes to be learned by a PfR learn list (over all PfR learning sessions).
max-number	Number representing the maximum number of traffic classes to be learned for a PfR learn list. The range of numbers is from 1 to 100. The default is 100.

Command Default

If this command is not configured, the number of traffic classes to be learned by a learn list during a PfR learn session is set to the default values:
number: 50
max-number: 100

Command Modes

Learn list configuration (config-pfr-mc-learn-list)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Use this command to set the number of traffic classes that a border router sends to the master controller for a learn list during a PfR learn session. An overall maximum number of traffic classes for a learn list can also be configured.

Examples

In the following example, the number of traffic classes to be learned in the first learn list (remote login traffic class) session is set to 50, and the maximum number of traffic classes to be learned for all sessions of the first learn list is set to 90. The second traffic class for file transfer traffic is configured with a maximum number of traffic classes set to 80, with 40 traffic classes set to be learned in a single session. Starting in global configuration mode, application traffic classes are defined using two PfR learn lists, LEARN_REMOTE_LOGIN_TC and LEARN_FILE_TRANSFER_TC. The remote login traffic class is configured using keywords representing Telnet and Secure Shell (SSH) traffic, and the resulting prefixes are aggregated to a prefix length of 24. The file transfer traffic class is configured using a keyword that represents FTP and is also aggregated to a prefix length of 24. A prefix-list is applied to the file transfer

traffic class to permit traffic from the 10.0.0.0/8 prefix. The master controller is configured to learn the top prefixes based on the highest outbound throughput for the filtered traffic, and the resulting traffic classes are added to the PfR application database.

```
Router(config)# ip prefix-list INCLUDE_10_NET 10.0.0.0/8
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# list seq 10 refname LEARN_REMOTE_LOGIN_TC
Router(config-pfr-mc-learn-list)# count 50 max 90
Router(config-pfr-mc-learn-list)# traffic-class application telnet ssh
Router(config-pfr-mc-learn-list)# aggregation-type prefix-length 24
Router(config-pfr-mc-learn-list)# throughput
Router(config-pfr-mc-learn-list)# exit
Router(config-pfr-mc-learn)# list seq 20 refname LEARN_FILE_TRANSFER_TC
Router(config-pfr-mc-learn-list)# count 40 max 80
Router(config-pfr-mc-learn-list)# traffic-class application ftp filter INCLUDE_10_NET
Router(config-pfr-mc-learn-list)# aggregation-type prefix-length 24
Router(config-pfr-mc-learn-list)# throughput
Router(config-pfr-mc-learn-list)# end
```

Related Commands

Command	Description
learn (PfR)	Enters PfR Top Talker and Top Delay learning configuration mode to configure PfR to automatically learn traffic classes.
list (PfR)	Creates a PfR learn list to specify criteria for learning traffic classes and enters learn list configuration mode.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

debug pfr api

To display Performance Routing (PfR) application interface debugging information, use the **debug pfr api** command in privileged EXEC mode. To stop the display of PfR application interface debugging information, use the **no** form of this command.

debug pfr api [**detail**]

no debug pfr api

Syntax Description

detail	(Optional) Displays detailed application interface debugging information.

Command Default

Detailed PfR application interface debugging messages are not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **debug pfr api** command is used to display messages about any configured PfR application interface providers or host devices. The PfR application interface defines the mode of communication and messaging between applications and the network for the purpose of optimizing the traffic associated with the applications. A provider is defined as an entity outside the network in which the router configured as a PfR master controller exists, for example, an ISP, or a branch office of the same company. The provider has one or more host devices running one or more applications that use the PfR application interface to communicate with a PfR master controller. A provider must be registered with a PfR master controller before an application on a host device can interface with PfR. Use the **api provider** (PfR) command to register the provider, and use the **host-address** (PfR) command to configure a host device. After registration, a host device in the provider network can initiate a session with a PfR master controller. The application interface provides an automated method for networks to be aware of applications and provides application-aware performance routing.

Caution When the **detail** keyword is entered, the amount of detailed output to be displayed can utilize a considerable amount of system resources. Use the **detail** keyword with caution in a production network.

Examples

The following example enables the display of PfR application interface debugging messages, and the output shows that a PfR policy failed due to a prefix that is not found:

```
Router# debug pfr api

OER api debugging is on
```

```
*May 26 01:04:07.278: OER API: Data set id received 5, data set len 9, host ip 10.3.3.3,
session id 1, requies2
*May 26 01:04:07.278: OER API: Received get current policy, session id 1 request id 22
*May 26 01:04:07.278: OER API: Recvd Appl with Prot 256 DSCP 0 SrcPrefix 0.0.0.0/0
SrcMask 0.0.0.0
*May 26 01:04:07.278: OER API:  DstPrefix 10.2.0.0/24 DstMask 255.255.255.0 Sport_min 0
Sport_max 0 Dport_mi0
*May 26 01:04:07.278: OER API: get prefix policy failed - prefix not found
*May 26 01:04:07.278: OER API: Get curr policy cmd received. rc 0
*May 26 01:04:07.278: OER API: Received send status response, status 0, session id 1,
request id 22, sequence0
*May 26 01:04:07.278: OER API: rc for data set 0
```

Table 2 describes the significant fields shown in the display. The content of the debugging messages depends on the commands that are subsequently entered at the router prompt.

Table 2 debug pfr api Field Descriptions

Field	Description
OER api debugging is on	Shows that application interface debugging is enabled.
OER API	Displays a PfR application interface message.

Related Commands

Command	Description
api provider	Registers an application interface provider with a PfR master controller and enters PfR master controller application interface provider configuration mode.
host-address	Configures information about a host device used by an application interface provider to communicate with a PfR master controller.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
show pfr api provider	Displays information about application interface providers registered with PfR.

debug pfr border

To display general Performance Routing (PfR) border router debugging information, use the **debug pfr border** command in privileged EXEC mode. To stop the display of PfR debugging information, use the **no** form of this command.

debug pfr border

no debug pfr border

Syntax Description

This command has no arguments or keywords.

Command Default

No debugging messages are enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **debug pfr border** command is entered on a border router. This command is used to display debugging information about the PfR border process, controlled routes, and monitored prefixes.

Examples

The following example enables the display of general PfR debugging information:

```
Router# debug pfr border

*May  4 22:32:33.695: OER BR: Process Message, msg 4, ptr 33272128, value  140
*May  4 22:32:34.455: OER BR: Timer event, 0
```

Table 3 describes the significant fields shown in the display.

Table 3 debug pfr border Field Descriptions

Field	Description
OER BR:	Indicates debugging information for PfR border process.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

debug pfr border active-probe

To display debugging information for active probes configured on the local border router, use the **debug pfr border active-probe** command in privileged EXEC mode. To stop the display of debug event information, use the **no** form of this command.

debug pfr border active-probe [**detail**]

no debug pfr border active-probe [**detail**]

Syntax Description

detail	(Optional) Displays detailed information.

Command Default

No debugging messages are enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **debug pfr border active-probe** command is entered on a border router. This command is used to display the status and results of active probes that are configured on the local border router.

Examples

The following example enables the display of active-probe debug information on a border router:

```
Router# debug pfr border active-probe

*May  4 23:47:45.633: OER BR ACTIVE PROBE: Attempting to retrieve Probe
Statistics.
      probeType = echo, probeTarget = 10.1.5.1, probeTargetPort = 0
      probeSource = Default, probeSourcePort = 0, probeNextHop = Default
      probeIfIndex = 13
*May  4 23:47:45.633: OER BR ACTIVE PROBE: Completed retrieving Probe
Statistics.
      probeType = echo, probeTarget = 10.1.5.1, probeTargetPort = 0
      probeSource = Default, probeSourcePort = 0, probeNextHop = 10.30.30.2
      probeIfIndex = 13, SAA index = 15
*May  4 23:47:45.633: OER BR ACTIVE PROBE: Completions 11, Sum of rtt 172,
Max rtt 36, Min rtt 12
*May  4 23:47:45.693: OER BR ACTIVE PROBE: Attempting to retrieve Probe
Statistics.
      probeType = echo, probeTarget = 10.1.4.1, probeTargetPort = 0
      probeSource = Default, probeSourcePort = 0, probeNextHop = Default
      probeIfIndex = 13
*May  4 23:47:45.693: OER BR ACTIVE PROBE: Completed retrieving Probe
Statistics.
      probeType = echo, probeTarget = 10.1.4.1, probeTargetPort = 0
```

```
probeSource = Default, probeSourcePort = 0, probeNextHop = 10.30.30.2
probeIfIndex = 13, SAA index = 14
```

Table 4 describes the significant fields shown in the display.

Table 4 debug pfr border active-probe Field Descriptions

Field	Description
OER BR ACTIVE PROBE:	Indicates debugging information for Performance Routing (PfR) active probes on a border router.
Statistics	The heading for PfR active probe statistics.
probeType	The active probe type. The active probe types that can be displayed are ICMP, TCP, and UDP.
probeTarget	The target IP address of the active probe.
probeTargetPort	The target port of the active probe.
probeSource	The source IP address of the active probe. Default is displayed for a locally generated active probe.
probeSourcePort	The source port of the active probe.
probeNextHop	The next hop for the active probe.
probeIfIndex	The active probe source interface index.
SAA index	The IP SLAs collection index number.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

debug pfr border learn

To display debugging information about learned prefixes on the local border router, use the **debug pfr border learn** command in privileged EXEC mode. To stop the display of debug event information, use the **no** form of this command.

debug pfr border learn [**top** *number*]

no debug pfr border learn [**top** *number*]

Syntax Description

top *number*	(Optional) Displays debugging information about the top delay or top throughput prefixes. The number of top delay or throughput prefixes can be specified. The range of prefixes that can be specified is a number from 1 to 65535.

Command Default

No debugging messages are enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **debug pfr border learn** command is entered on a border router. This command is used to display debugging information about prefixes learned on the local border router.

Examples

The following example enables the display of active-probe debug information on a border router:

```
Router# debug pfr border learn

*May  4 22:51:31.971: OER BR LEARN: Reporting prefix 1: 10.1.5.0, throughput 201
*May  4 22:51:31.971: OER BR LEARN: Reporting 1 throughput learned prefixes
*May  4 22:51:31.971: OER BR LEARN: State change, new STOPPED, old STARTED, reason Stop
Learn
```

Table 5 describes the significant fields shown in the display.

Table 5 debug pfr border learn Field Descriptions

Field	Description
OER BR LEARN:	Indicates debugging information for the Performance Routing (PfR) border router learning process.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

debug pfr border routes

To display debugging information for Performance Routing (PfR) controlled or monitored routes on the local border router, use the **debug pfr border routes** command in privileged EXEC mode. To stop the display of debug event information, use the **no** form of this command.

debug pfr border routes {**bgp** | **eigrp** [**detail**] | **piro** [**detail**] | **static**}

no debug pfr border routes {**bgp** | **eigrp** | **piro** | **static**}

Syntax Description

bgp	Displays debugging information for Border Gateway Protocol (BGP) routes.
eigrp	Displays debugging information for Enhanced Interior Gateway Routing Protocol (EIGRP) routes.
detail	(Optional) Displays detailed debugging information. This keyword applies only to EIGRP or Protocol Independent Route Optimization (PIRO) routes.
piro	Displays debugging information for PIRO routes.
static	Displays debugging information for static routes.

Command Default

No debugging messages are enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **debug pfr border routes** command is entered on a border router. This command is used to display the debugging information about PfR-controlled or monitored routes on the local border router.

PIRO provides the ability for PfR to search for a parent route—an exact matching route, or a less specific route—in any IP Routing Information Base (RIB). If a parent route for the traffic class exists in the RIB, policy-based routing is used to control the prefix.

EIGRP route control provides the ability for PfR to search for a parent route—an exact matching route, or a less specific route—in the EIGRP routing table. If a parent route for the traffic class exists in the EIGRP routing table, temporary EIGRP routes are injected and identified by adding a configurable extended community tag value.

The following example enables the display of active-probe debug information on a border router:

```
Router# debug pfr border routes bgp

*May  4 22:35:53.239: OER BGP: Control exact prefix 10.1.5.0/24
*May  4 22:35:53.239: OER BGP: Walking the BGP table for 10.1.5.0/24
*May  4 22:35:53.239: OER BGP: Path for 10.1.5.0/24 is now under OER control
*May  4 22:35:53.239: OER BGP: Setting prefix 10.1.5.0/24 as OER net#
```

Table 6 describes the significant fields shown in the display.

Table 6 debug pfr border routes Field Descriptions

Field	Description
OER BGP:	Indicates debugging information for PfR-controlled BGP routes.
OER STATIC:	Indicates debugging information for PfR-controlled Static routes. (Not displayed in the example output.)

The following example enables the display of detailed debugging information for PIRO routes and shows that the parent route for the prefix 10.1.1.0 is found in the RIB and a route map is created to control the application. Note that detailed border PBR debugging is also active.

```
Router# debug pfr border routes piro detail

Feb 21 00:20:44.431: PIRO: Now calling ip_get_route
Feb 21 00:20:44.431: PFR PIRO: Parent lookup found parent 10.1.1.0, mask 255.255.255.0,
nexthop 10.1.1.0 for network 10.1.1.0/24
...
Feb 21 00:22:46.771: PFR PIRO: Parent lookup found parent 10.1.1.0, mask 255.255.255.0,
nexthop 10.1.1.0 for network 10.1.1.0/24
Feb 21 00:22:46.771: PFR PIRO: Control Route, 10.1.1.0/24, NH 0.0.0.0, IF Ethernet4/2
Feb 21 00:22:46.771: PIRO: Now calling ip_get_route
Feb 21 00:22:46.771: PIRO: Now calling ip_get_route
Feb 21 00:22:46.771: PFR PIRO: Parent lookup found parent 10.1.1.0, mask 255.255.255.0,
nexthop 10.1.1.0 for network 10.1.1.0/24
Feb 21 00:22:46.771: OER BR PBR(det): control app: 10.1.1.0/24, nh 0.0.0.0, if
Ethernet4/2,ip prot 256, dst opr 0, src opr 0, 0 0 0 0, src net 0.0.0.0/0, dscp 0/0
Feb 21 00:22:46.771: OER BR PBR(det): Create rmap 6468E488
Feb 21 00:22:46.775: PfR-RIB RIB_RWATCH: (default:ipv4:base) T 10.1.1.0/24 EVENT Track
start
Feb 21 00:22:46.775: PfR-RIB RIB_RWATCH: (default:ipv4:base) N 10.1.1.0/24 Adding track
Feb 21 00:22:46.775: PfR-RIB RIB_RWATCH: (default:ipv4:base) N 10.1.1.0/24 QP Schedule
query
Feb 21 00:22:46.775: PfR-RIB RIB_RWATCH: (default:ipv4:base) T 10.1.1.0/24 EVENT Query
found route
Feb 21 00:22:46.775: PfR-RIB RIB_RWATCH: (default:ipv4:base) N 10.1.1.0/24 Adding route
Feb 21 00:22:46.775: PfR-RIB RIB_RWATCH: (default:ipv4:base) R 10.1.1.0/24  d=0 p=0 ->
Updating
Feb 21 00:22:46.775: PfR-RIB RIB_RWATCH: (default:ipv4:base) R 10.1.1.0/24  d=110 p=1 ->
Et4/2 40.40.40.2 40 Notifying
Feb 21 00:22:46.775: PfR-RIB RIB_RWATCH: Adding to client notification queue
Feb 21 00:22:46.775: PfR-RIB RIB_RWATCH: (default:ipv4:base) W 10.1.1.0/24 c=0x15 Client
notified reachable
Feb 21 00:22:46.779: PFR PIRO: Route update rwinfo 680C8E14, network 10.1.1.0, mask_len 24
event Route Up
Feb 21 00:22:46.779: OER BR PBR(det): PIRO Path change notify for prefix:10.1.1.0,
masklen:24, reason:1
```

Table 7 describes the significant fields shown in the display.

Table 7 debug pfr border routes Field Descriptions

Field	Description
PFR PIRO	Indicates debugging information for Performance Routing-controlled PIRO activities.
OER BR PBR	Indicates debugging information about policy-based routing activities on the border router.
PfR-RIB RIB_RWATCH	Indicates debugging information about RIB activities.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

debug pfr border traceroute reporting

To display debugging information for traceroute probes on the local border router, use the **debug pfr border traceroute reporting** command in privileged EXEC mode. To stop the display of debug event information, use the **no** form of this command.

debug pfr border traceroute reporting [**detail**]

no debug pfr border traceroute reporting [**detail**]

Syntax Description

detail	(Optional) Displays detailed traceroute debug information.

Command Default

No debugging messages are enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **debug pfr border traceroute reporting** command is entered on a border router. This command is used to display the debugging information about traceroute probes sourced on the local border router.

Examples

The following example enables the display of active-probe debug information on a border router:

```
Router# debug pfr border traceroute reporting

May 19 03:46:23.807: OER BR TRACE(det): Received start message: msg1 458776,
msg2 1677787648, if index 19, host addr 100.1.2.1, flags 1, max ttl 30,
protocol 17, probe delay 0
May 19 03:46:26.811: OER BR TRACE(det): Result msg1 458776,
msg2 1677787648 num hops 30 sent May 19 03:47:20.919: OER BR TRACE(det):
Received start message: msg1 524312, msg2 1677787648, if index 2,
host addr 100.1.2.1, flags 1, max ttl 30, protocol 17, probe delay 0
May 19 03:47:23.923: OER BR TRACE(det): Result msg1 524312,
msg2 1677787648 num hops 3 sent
```

Table 8 describes the significant fields shown in the display.

Table 8 debug pfr border traceroute reporting Field Descriptions

Field	Description
OER BR TRACE:	Indicates border router debugging information for traceroute probes.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

debug pfr cc

To display Performance Routing (PfR) communication control debugging information for master controller and border router communication, use the **debug pfr cc** command in privileged EXEC mode. To stop the display of PfR debugging information, use the **no** form of this command.

debug pfr cc [**detail**]

no debug pfr cc [**detail**]

Syntax Description

detail	(Optional) Displays detailed information.

Command Default

No debugging messages are enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **debug pfr cc** command can be entered on a master controller or on a border router. This command is used to display messages exchanged between the master controller and the border router. These messages include control commands, configuration commands, and monitoring information. Enabling this command will cause very detailed output to be displayed and can utilize a considerable amount of system resources. This command should be enabled with caution in a production network.

Examples

The following example enables the display of PfR communication control debugging messages:

```
Router# debug pfr cc

*May  4 23:03:22.527: OER CC: ipflow prefix reset received: 10.1.5.0/24
```

Table 9 describes the significant fields shown in the display.

Table 9 debug pfr cc Field Descriptions

Field	Description
OER CC:	Indicates debugging information for PfR communication messages.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

debug pfr master border

To display debugging information for Performance Routing (PfR) border router events on a PfR master controller, use the **debug pfr master border** command in privileged EXEC mode. To stop border router event debugging, use the **no** form of this command.

debug pfr master border [*ip-address*]

no debug pfr master border

Syntax Description

ip-address	(Optional) Specifies the IP address of a border router.

Command Default

No debugging messages are enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **debug pfr master border** command is entered on a master controller. The output displays information related to the events or updates from one or more border routers.

Examples

The following example shows the status of two border routers. Both routers are up and operating normally.

```
Router# debug pfr master border

OER Master Border Router debugging is on
Router#
1d05h: OER MC BR 10.4.9.7: BR I/F update, status UP, line 1 index 1, tx bw 10000
0, rx bw 100000, time, tx ld 0, rx ld 0, rx rate 0 rx bytes 3496553, tx rate 0,
tx bytes 5016033
1d05h: OER MC BR 10.4.9.7: BR I/F update, status UP, line 1 index 2, tx bw 10000
0, rx bw 100000, time, tx ld 0, rx ld 0, rx rate 0 rx bytes 710149, tx rate 0, t
x bytes 1028907
1d05h: OER MC BR 10.4.9.6: BR I/F update, status UP, line 1 index 2, tx bw 10000
0, rx bw 100000, time, tx ld 0, rx ld 0, rx rate 0 rx bytes 743298, tx rate 0, t
x bytes 1027912
1d05h: OER MC BR 10.4.9.6: BR I/F update, status UP, line 1 index 1, tx bw 10000
0, rx bw 100000, time, tx ld 0, rx ld 0, rx rate 0 rx bytes 3491383, tx rate 0,
tx bytes 5013993
```

Table 10 describes the significant fields shown in the display.

Table 10 debug pfr master border Field Descriptions

Field	Description
OER MC BR *ip-address*:	Indicates debugging information for a border router process. The *ip-address* identifies the border router.

Related Commands

pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

debug pfr master collector

To display data collection debugging information for PfR monitored prefixes, use the **debug pfr master collector** command in privileged EXEC mode. To disable the display of this debugging information, use the **no** form of this command.

debug pfr master collector {**active-probes** [**detail** [**trace**]] | **netflow**}

no debug pfr master collector {**active-probes** [**detail** [**trace**]] | **netflow**}

Syntax Description

active-probes	Displays aggregate active probe results for a given prefix on all border routers that are executing the active probe.
detail	(Optional) Displays the active probe results from each target for a given prefix on all border routers that are executing the active probe.
trace	(Optional) Displays aggregate active probe results and historical statistics for a given prefix on all border routers that are executing the active probe.
netflow	Displays information about the passive (NetFlow) measurements received by the master controller for prefixes monitored from the border router.

Command Default

No debugging messages are enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **debug pfr master collector** command is entered on a master controller. The output displays data collection information for monitored prefixes.

Examples

debug pfr master collector active-probes Example

The following example enables the display of aggregate active probe results for the 10.1.0.0/16 prefix on all border routers that are configured to execute this active probe:

```
Router# debug pfr master collector active-probes

*May  4 22:34:58.221: OER MC APC: Probe Statistics Gathered for prefix 10.1.0.0/16 on all
exits,notifying the PDP
*May  4 22:34:58.221: OER MC APC: Summary Exit Data (pfx 10.1.0.0/16, bdr 10.2.2.2, if 13,
nxtHop Default):savg delay 13, lavg delay 14, sinits 25, scompletes 25
*May  4 22:34:58.221: OER MC APC: Summary Prefix Data: (pfx 10.1.0.0/16) sloss 0, lloss 0,
sunreach 25, lunreach 25, savg raw delay 15, lavg raw delay 15, sinits 6561, scompletes
6536, linits 6561, lcompletes 6536
*May  4 22:34:58.221: OER MC APC: Active OOP check done
```

Table 11 describes the significant fields shown in the display.

Table 11 debug pfr master collector active-probes Field Descriptions

Field	Description
OER MC APC:	Indicates debugging information for active probes from the PfR master collector.

debug pfr master collector active-probes detail Example

The following example enables the display of aggregate active probe results from each target for the 10.1.0.0/16 prefix on all border routers that are configured to execute this active probe:

```
Router# debug pfr master collector active-probes detail

*May  4 22:36:21.945: OER MC APC: Rtrv Probe Stats: BR 10.2.2.2, Type echo,
Tgt 10.1.1.1,TgtPt 0, Src Default, SrcPt 0, NxtHp Default, Ndx 13
*May  4 22:36:22.001: OER MC APC: Remote stats received: BR 10.2.2.2, Type
echo, Tgt 10.15.1, TgtPt 0, Src Default, SrcPt 0, NxtHp Default, Ndx 13
*May  4 22:36:22.313: OER MC APC: Perf data point (pfx 10.1.0.0/16, bdr
10.2.2.2, if 13, xtHop Default):  avg delay 20, loss 0, unreach 0,
initiations 2, completions 2, delay sum40, ldelay max 20, ldelay min 12
*May  4 22:36:22.313: OER MC APC: Perf data point (pfx 10.1.0.0/16, bdr
10.2.2.2, if 13, xtHop Default):  avg delay 20, loss 0, unreach 0,
initiations 2, completions 2, delay sum40, ldelay max 20, ldelay min 12
*May  4 22:36:22.313: OER MC APC: Probe Statistics Gathered for prefix
10.1.0.0/16 on al exits, notifying the PDP
*May  4 22:36:22.313: OER MC APC: Active OOP check done
```

Table 12 describes the significant fields shown in the display.

Table 12 debug pfr master collector active-probes detail Field Descriptions

Field	Description
OER MC APC:	Indicates debugging information for active probes from the PfR master collector.

debug pfr master collector active-probes detail trace Example

The following example enables the display of aggregate active probe results and historical statistics from each target for the 10.1.0.0/16 prefix on all border routers that are configured to execute this active probe:

```
Router# debug pfr master collector active-probes detail trace

*May  4 22:40:33.845: OER MC APC: Rtrv Probe Stats: BR 10.2.2.2, Type echo,
Tgt 10.1.5.1, TgtPt 0, Src Default, SrcPt 0, NxtHp Default, Ndx 13
*May  4 22:40:33.885: OER MC APC: Remote stats received: BR 10.2.2.2, Type
echo, Tgt 10.1.5.1, TgtPt 0, Src Default, SrcPt 0, NxtHp Default, Ndx 13
*May  4 22:40:34.197: OER MC APC: Remote stats received: BR 10.2.2.2, Type
echo, Tgt 10.1.2.1, TgtPt 0, Src Default, SrcPt 0, NxtHp Default, Ndx 13
*May  4 22:40:34.197: OER MC APC: Updating Probe (Type echo Tgt 10.1.2.1
TgtPt 0) Total Completes 1306, Total Attempts 1318
*May  4 22:40:34.197: OER MC APC: All stats gathered for pfx 10.1.0.0/16
Accumulating Stats
*May  4 22:40:34.197: OER MC APC: Updating Curr Exit Ref (pfx 10.1.0.0/16,
bdr 10.2.2.2, if 13, nxtHop Default) savg delay 17, lavg delay 14, savg loss
0, lavg loss 0, savg unreach 0, lavg unreach 0
*May  4 22:40:34.197: OER MC APC: Probe Statistics Gathered for prefix
```

```
10.1.0.0/16 on all exits, notifying the PDP
*May  4 22:40:34.197: OER MC APC: Active OOP check done
```

Table 13 describes the significant fields shown in the display.

Table 13 debug pfr master collector active-probes detail trace Field Descriptions

Field	Description
OER MC APC:	Indicates debugging information for active probes from the PfR master collector.

debug pfr master collector netflow Example

The following example enables the display of passive monitoring results for the 10.1.5.0/24 prefix:

```
Router# debug pfr master collector netflow

*May  4 22:31:45.739: OER MC NFC: Rcvd  egress update from BR 10.1.1.2
  prefix 10.1.5.0/24  Interval 75688  delay_sum 0  samples 0  bytes 20362  pkts 505  flows
359  pktloss 1 unreach 0
*May  4 22:31:45.739: OER MC NFC: Updating exit_ref; BR 10.1.1.2 i/f Et1/0, s_avg_delay
655, l_avg_delay 655, s_avg_pkt_loss 328, l_avg_pkt_loss 328, s_avg_flow_unreach 513,
l_avg_flow_unreach 513
*May  4 22:32:07.007: OER MC NFC: Rcvd ingress update from BR 10.1.1.3
  prefix 10.1.5.0/24  Interval 75172  delay_sum 42328  samples 77  bytes 22040  pkts 551
flows 310  pktloss 0 unreach 0
```

Table 14 describes the significant fields shown in the display.

Table 14 debug pfr master collector netflow Field Descriptions

Field	Description
OER MC NFC:	Indicates debugging information for the PfR master collector from passive monitoring (NetFlow).

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

debug pfr master cost-minimization

To display debugging information for cost-based optimization policies, use the **debug pfr master cost-minimization** command in privileged EXEC mode. To disable the display of this debugging information, use the **no** form of this command.

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

no debug pfr master cost-minimization [**detail**]

Syntax Description

detail	(Optional) Displays detailed information.

Command Default

No debugging messages are enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **debug pfr master cost-minimization** command is entered on a master controller. The output displays debugging information for cost-minimization policies.

Examples

The following example enables the display of detailed cost-based optimization policy debug information:

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

OER Master cost-minimization Detail debugging is on
*May 14 00:38:48.839: OER MC COST: Momentary target utilization for exit 10.1.1.2 i/f
Ethernet1/0 nickname ISP1 is 7500 kbps, time_left 52889 secs, cumulative 16 kb, rollup
period 84000 secs, rollup target 6000 kbps, bw_capacity 10000 kbps
*May 14 00:38:48.839: OER MC COST: Cost OOP check for border 10.1.1.2, current util: 0
target util: 7500 kbps
*May 14 00:39:00.199: OER MC COST: ISP1 calc separate rollup ended at 55 ingress Kbps
*May 14 00:39:00.199: OER MC COST: ISP1 calc separate rollup ended at 55 egress bytes
*May 14 00:39:00.199: OER MC COST: Target utilization for nickname ISP1 set to 6000,
rollups elapsed 4, rollups left 24
*May 14 00:39:00.271: OER MC COST: Momentary target utilization for exit 10.1.1.2 i/f
Ethernet1/0 nickname ISP1 is 7500 kbps, time_left 52878 secs, cumulative 0 kb, rollup
period 84000 secs, rollup target 6000 kbps, bw_capacity 10000 kbps
*May 14 00:39:00.271: OER MC COST: Cost OOP check for border 10.1.1.2, current util: 0
target util: 7500 kbps
```

Table 15 describes the significant fields shown in the display.

Table 15 debug pfr master cost-minimization detail Field Descriptions

Field	Description
OER MC COST:	Indicates debugging information for cost-based optimization on the master controller.

Related Commands

Command	Description
cost-minimization (PfR)	Configures cost-based optimization policies on a master controller.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
show pfr master cost-minimization	Displays the status of cost-based optimization policies.

debug pfr master exit

To display debug event information for Performance Routing (PfR) managed exits, use the **debug pfr master exit** command in privileged EXEC mode. To stop the display of debug event information, use the **no** form of this command.

debug pfr master exit [**detail**]

no debug pfr master exit [**detail**]

Syntax Description

detail	Displays detailed PfR managed exit information.

Command Default

No debugging messages are enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **debug pfr master exit** command is entered on a master controller. This command is used to display debugging information for master controller exit selection processes.

Examples

The following example shows output from the **debug pfr master exit** command, entered with the **detail** keyword:

```
Router# debug pfr master exit detail

*May  4 11:26:51.539: OER MC EXIT: 10.1.1.1, intf Fa4/0 INPOLICY
*May  4 11:26:52.195: OER MC EXIT: 10.2.2.3, intf Se2/0 INPOLICY
*May  4 11:26:55.515: OER MC EXIT: 10.1.1.2, intf Se5/0 INPOLICY
*May  4 11:29:14.987: OER MC EXIT: 7 kbps should be moved from 10.1.1.1, intf Fa4/0
*May  4 11:29:35.467: OER MC EXIT: 10.1.1.1, intf Fa4/0 in holddown state so skip OOP
check
*May  4 11:29:35.831: OER MC EXIT: 10.2.2.3, intf Se2/0 in holddown state so skip OOP
check
*May  4 11:29:39.455: OER MC EXIT: 10.1.1.2, intf Se5/0 in holddown state so skip OOP
check
```

Table 16 describes the significant fields shown in the display.

Table 16 debug pfr master exit detail Field Descriptions

Field	Description
OER MC EXIT:	Indicates PfR master controller exit event.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

debug pfr master learn

To display debug information for PfR master controller learning events, use the **debug pfr master learn** command in privileged EXEC mode. To stop the display of debug information, use the **no** form of this command.

debug pfr master learn [**detail**]

no debug pfr master learn [**detail**]

Syntax Description

detail	(Optional) Displays detailed information.

Command Default

No debugging messages are enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **debug pfr master learn** command is entered on a master controller. This command is used to display debugging information for master controller learning events.

Examples

The following example shows output from the **debug pfr master learn** command. The output shows PfR Top Talker debug events. The master controller is enabling prefix learning for new border router process:

```
Router# debug pfr master learn

06:13:43: OER MC LEARN: Enable type 3, state 0
06:13:43: OER MC LEARN: OER TTC: State change, new RETRY, old DISABLED, reason TT start
06:13:43: OER MC LEARN: OER TTC: State change, new RETRY, old DISABLED, reason TT start
request
06:13:43: OER MC LEARN: OER TTC: State change, new RETRY, old DISABLED, reason T
T start request
06:14:13: OER MC LEARN: TTC Retry timer expired
06:14:13: OER MC LEARN: OER TTC: State change, new STARTED, old RETRY, reason At
 least one BR started
06:14:13: %OER_MC-5-NOTICE: Prefix Learning STARTED
06:14:13: OER MC LEARN: MC received BR TT status as enabled
06:14:13: OER MC LEARN: MC received BR TT status as enabled
06:19:14: OER MC LEARN: OER TTC: State change, new WRITING DATA, old STARTED, reason
Updating DB
06:19:14: OER MC LEARN: OER TTC: State change, new SLEEP, old WRITING DATA, reason
Sleep state
```

Table 17 describes the significant fields shown in the display.

Table 17 debug pfr master learn Field Descriptions

Field	Description
OER MC LEARN:	Indicates PfR master controller learning events.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

debug pfr master prefix

To display debug events related to prefix processing on a Performance Routing (PfR) master controller, use the **debug pfr master prefix** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug pfr master prefix [*prefix* | **appl**] [**detail**]

no debug pfr master prefix [*prefix* | **appl**] [**detail**]

Syntax Description

prefix	(Optional) Specifies a single prefix or prefix range. The prefix address and mask are entered with this argument.
appl	(Optional) Displays information about prefixes used by applications monitored and controlled by a PfR master controller.
detail	(Optional) Displays detailed PfR prefix processing information.

Command Default

No debugging messages are enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **debug pfr master prefix** command is entered on a master controller. This command displays debugging information related to prefix monitoring and processing.

Examples

The following example shows the master controller searching for the target of an active probe after the target has become unreachable.

```
Router# debug pfr master prefix

OER Master Prefix debugging is on
06:01:28: OER MC PFX 10.4.9.0/24: APC last target deleted for prefix, no targets
 left assigned and running
06:01:38: OER MC PFX 10.4.9.0/24: APC Attempting to probe all exits
06:02:59: OER MC PFX 10.4.9.0/24: APC last target deleted for prefix, no targets
 left assigned and running
06:03:08: OER MC PFX 10.4.9.0/24: APC Attempting to probe all exits
06:04:29: OER MC PFX 10.4.9.0/24: APC last target deleted for prefix, no targets
 left assigned and running
06:04:39: OER MC PFX 10.4.9.0/24: APC Attempting to probe all exits
06:05:59: OER MC PFX 10.4.9.0/24: APC last target deleted for prefix, no targets
 left assigned and running
06:06:09: OER MC PFX 10.4.9.0/24: APC Attempting to probe all exits
```

Table 18 describes the significant fields shown in the display.

Table 18 debug pfr master prefix Field Descriptions

Field	Description
OER MC PFX *ip-address*:	Indicates debugging information for PfR monitored prefixes. The *ip-address* identifies the prefix.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

debug pfr master prefix-list

To display debug events related to prefix-list processing on a Performance Routing (PfR) master controller, use the **debug pfr master prefix-list** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug pfr master prefix-list *list-name* [**detail**]

no debug pfr master prefix-list *list-name*

Syntax Description

list-name	Specifies a single prefix or prefix range. The prefix address and mask are entered with this argument.
detail	(Optional) Displays detailed PfR prefix-list processing information.

Command Default

No debugging messages are enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **debug pfr master prefix-list** command is entered on a master controller. This command displays debugging information related to prefix-list processing.

Examples

The following example shows output from the **debug pfr master prefix-list** command.

```
Router# debug pfr master prefix-list

23:02:16.283: OER MC PFX 10.1.5.0/24: Check PASS REL loss: loss 0, policy 10%, notify TRUE
23:02:16.283: OER MC PFX 10.1.5.0/24: Passive REL loss in-policy
23:02:16.283: OER MC PFX 10.1.5.0/24: Check PASS REL delay: delay 124, policy 50%, notify
TRUE
23:02:16.283: OER MC PFX 10.1.5.0/24: Passive REL delay in policy
23:02:16.283: OER MC PFX 10.1.5.0/24: Prefix not OOP
23:02:16.283: OER MC PFX 10.1.5.0/24: Check PASS REL unreachable: unreachable 0, policy
50%, notify TRUE
23:02:16.283: OER MC PFX 10.1.5.0/24: Passive REL unreachable in-policy
23:02:16.283: OER MC PFX 10.1.5.0/24: Check PASS REL loss: loss 0, policy 10%, notify TRUE
23:02:16.283: OER MC PFX 10.1.5.0/24: Passive REL loss in policy
```

Table 19 describes the significant fields shown in the display.

Table 19 debug pfr master prefix-list Field Descriptions

Field	Description
OER MC PFX *ip-address*:	Indicates debugging information for PfR monitored prefixes. The *ip-address* identifies the prefix.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

debug pfr master process

To display debug information about the PfR master controller process, use the **debug pfr master process** command in privileged EXEC mode. To stop displaying debug information, use the **no** form of this command.

debug pfr master process [**detail**]

no debug pfr master process [**detail**]

Syntax Description

detail	(Optional) Displays detailed information.

Command Default

No debugging messages are enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **debug pfr master process** command is entered on a master controller.

Examples

The following is sample debug output for a master controller process:

```
Router# debug pfr master process

01:12:00: OER MC PROCESS: Main msg type 15, ptr 0, value 0
```

Table 20 describes the significant fields shown in the display.

Table 20 debug pfr master process Field Descriptions

Field	Description
OER MC PROCESS:	Indicates a master controller process debugging message.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

debug pfr master traceroute reporting

To display debug information about traceroute probes, use the **debug pfr master traceroute reporting** command in privileged EXEC mode. To stop displaying debug information, use the **no** form of this command.

debug pfr master traceroute reporting [**detail**]

no debug pfr master traceroute reporting [**detail**]

Syntax Description

detail	(Optional) Displays detailed information.

Command Default

No debugging messages are enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **debug pfr master traceroute reporting** command is entered on a master controller. This command is used to display traceroute events on a master controller.

Examples

The following is sample debug output for a master controller process:

```
Router# debug pfr master traceroute reporting detail

*May 12 18:55:14.239: OER MC TRACE: sent start message msg1 327704, msg2 167838976, if
index 2, host add 10.1.5.2, flags 1, max ttl 30, protocol 17
*May 12 18:55:16.003: OER MC TRACE: sent start message msg1 393240, msg2 167838976, if
index 2, host add 10.1.5.2, flags 1, max ttl 30, protocol 17
master#
*May 12 18:55:17.303: OER MC TRACE: Received result: msg_id1 327704, prefix 10.1.5.0/24,
hops 4, flags 1
*May 12 18:55:19.059: OER MC TRACE: Received result: msg_id1 393240, prefix 10.1.5.0/24,
hops 4, flags 1
```

Table 21 describes the significant fields shown in the display.

Table 21 debug pfr master traceroute reporting detail Field Descriptions

Field	Description
OER MC PROCESS:	Indicates master controller debugging information for traceroute probes.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

delay (PfR)

To configure PfR traffic class learning based on highest delay times or to set a delay threshold for a Performance Routing (PfR) policy, use the **delay** command in master controller, Top Talker and Top Delay learning, or learn list configuration mode. To reset the delay values to their default, use the **no** form of this command.

Master Controller Configuration Mode

delay {**relative** *percentage* | **threshold** *maximum*}

no delay

Top Talker and Top Delay Learning and Learn List Configuration Modes

delay

no delay

Syntax Description

relative *percentage*	Sets a relative delay policy based on a comparison of short-term and long-term delay percentages. The range of values that can be configured for this argument is a number from 1 to 1000. Each increment represents one tenth of a percent. The default is 500 (50 percent).
threshold *maximum*	Sets the absolute maximum delay time, in milliseconds. The range of values that can be configured for this argument is from 1 to 10000. The default is 5000.

Command Default

Master Controller Configuration Mode

PfR uses the default values if this command is not configured or if the **no** form of this command is entered. Default values:

percentage: 500 (50 percent)
maximum: 5000

Top Talker and Top Delay Learning and Learn List Configuration Modes

None

Command Modes

Master controller configuration (config-pfr-mc)
Top Talker and Top Delay learning configuration (config-pfr-mc-learn)
Learn list configuration (config-pfr-mc-learn-list)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Configuring in Master Controller Configuration Mode

Use the **delay** command entered in PfR master controller configuration mode to set the delay threshold for a traffic class within a PfR policy as a relative percentage or as an absolute value. If the configured delay threshold is exceeded, the traffic class is out-of-policy.

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 short-term measurement reflects the delay percentage within a 5-minute period. The long-term measurement reflects the delay percentage within a 60-minute period. The following formula is used to calculate this value:

Relative delay measurement = ((short-term measurement – long-term measurement) / long-term measurement) * 100

The master controller measures the difference between these two values as a percentage. If the percentage exceeds the user-defined or default value, the delay percentage is determined to be out-of-policy. For example, if the long-term delay measurement is 100 milliseconds and the short-term delay measurement is 120 milliseconds, the relative delay percentage is 20 percent.

The **threshold** keyword is used to configure the absolute maximum delay period in milliseconds.

Configuring in Top Talker and Top Delay Learning and Learn List Configuration Modes

Use the **delay** command under the Top Talker and Top Delay learning or learn list configuration mode to enable traffic class learning based on the highest delay time. PfR measures the delay for optimized prefixes when this command is enabled, and the master controller creates a list of traffic classes based on the highest delay time.

Examples

Master Controller Configuration Mode

The following example shows how to set a 20 percent relative delay threshold:

```
Router(config)# pfr master
Router(config-pfr-mc)# delay relative 200
```

Top Talker and Top Delay Learning Configuration Mode

The following example shows how to configure a master controller to learn traffic classes based on the highest delay times:

```
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# delay
```

Learn List Configuration Mode

The following example shows how to configure a master controller to learn traffic classes based on the highest delay times for a learn list named LEARN_REMOTE_LOGIN_TC for Telnet and Secure Shell (ssh) application traffic classes:

```
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# list seq 10 refname LEARN_REMOTE_LOGIN_TC
Router(config-pfr-mc-learn-list)# traffic-class application telnet ssh
Router(config-pfr-mc-learn-list)# aggregation-type prefix-length 24
Router(config-pfr-mc-learn-list)# delay
```

Related Commands

Command	Description
learn (PfR)	Enters PfR Top Talker and Top Delay learning configuration mode to configure PfR to automatically learn traffic classes.
list (PfR)	Creates a PfR learn list to specify criteria for learning traffic classes and enters learn list configuration mode.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
set delay (PfR)	Configures a PfR map to configure PfR to learn prefixes based on the lowest delay.

downgrade bgp (PfR)

To specify route downgrade options for a Performance Routing (PfR) managed interface using Border Gateway Protocol (BGP) advertisements, use the **downgrade bgp** command in PfR border exit interface configuration mode. To remove the route downgrade options, use the **no** form of this command.

downgrade bgp community *community-number*

no downgrade bgp community

Syntax Description

community	Specifies a BGP community number that will be added to the BGP advertisement.
community-number	BGP community number entered in AA:NN format. The community format consists of a 4-byte value. The first two bytes represent the autonomous system number, and the trailing two bytes represent a user-defined network number. A number in the range from 1 to 65535 can be entered for each 2-byte value.

Command Default

No route downgrade options are specified.

Command Modes

PfR border exit interface configuration (config-pfr-mc-br-if)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Use the **downgrade bgp** command to attach a BGP prepend community number to an inside prefix BGP advertisement from the network to another autonomous system such as an Internet service provider (ISP). The BGP prepend community will increase the number of autonomous system hops in the advertisement of the inside prefix from the ISP to its peers. Autonomous system prepend BGP community is the preferred method to be used for PfR BGP inbound optimization because there is no risk of the local ISP filtering the extra autonomous system hops.

Examples

The following example shows how to enforce an entrance link selection for learned inside prefixes using the BGP autonomous system number community prepend technique. The **downgrade bgp** command is configured under PfR border exit interface configuration mode to add the BGP community number 3:1 to BGP advertisements to packets that travel through this entrance link on the border router.

```
Router> enable
Router# configure terminal
Router(config)# pfr master
Router(config-pfr-mc)# max range receive percent 35
Router(config-pfr-mc)# border 10.1.1.2 key-chain PFR_KEY
Router(config-pfr-mc-br)# interface ethernet1/0 external
Router(config-pfr-mc-br-if)# maximum utilization receive absolute 2500
Router(config-pfr-mc-br-if)# downgrade bgp community 3:1
```

```
Router(config-pfr-mc-br-if)# exit
Router(config-pfr-mc-br)# exit
Router(config-pfr-mc)# exit
Router(config)# pfr-map INSIDE_LEARN 10
Router(config-pfr-map)# match pfr learn inside
Router(config-pfr-map)# set delay threshold 400
Router(config-pfr-map)# set resolve delay priority 1
Router(config-pfr-map)# set mode route control
Router(config-pfr-map)# end
```

Related Commands

Command	Description
border (PfR)	Enters PfR managed border router configuration mode to establish communication with a PfR border router.
max range receive (PfR)	Sets the maximum utilization range for all PfR managed entrance links.
maximum utilization receive (PfR)	Sets the maximum utilization on a single PfR managed entrance link.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

expire after (PfR)

To set the length of time for which Performance Routing (PfR) learned prefixes are kept in the central policy database, use the **expire after** command in PfR Top Talker and Top Delay learning configuration mode. To disable the expiration timer and restore default behavior, use the **no** form of this command.

expire after {**session** *number* | **time** *minutes*}

no expire after

Syntax Description

session	Configures a session-based expiration timer.
number	A number from 1 to 65535 can be entered. Each increment represents one monitoring period.
time	Configures a time-based expiration timer.
minutes	A number from 1 to 65535 can be entered. This argument is entered in minutes.

Command Default

New prefixes are not learned if router memory utilization is greater than 90 percent. Inactive prefixes are removed (oldest first) from the central policy database as memory is needed.

Command Modes

PfR Top Talker and Top Delay learning configuration (config-pfr-mc-learn)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **expire after** command is entered on a PfR master controller in PfR Top Talker and Top Delay learning configuration mode. This command is used to configure a session- or time-based expiration period for learned prefixes. Each session is equal to one monitoring period plus a periodic interval time that separates monitoring periods. The time-based expiration timer is configured in minutes.

Examples

The following example configures learned prefixes to be removed from the central policy database after 100 monitoring periods:

```
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# expire after session 100
```

Related Commands

Command	Description
learn (PfR)	Enters PfR Top Talker and Top Delay learning configuration mode to configure prefixes for PfR to learn.
max prefix (PfR)	Sets the maximum number of prefixes that the master controller will monitor or learn.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

holddown (PfR)

To configure the Performance Routing (PfR) prefix route dampening timer to set the minimum period of time for which a new exit must be used before an alternate exit can be selected, use the **holddown** command in PfR master controller configuration mode. To return the prefix route dampening timer to the default value, use the **no** form of this command.

holddown *timer*

no holddown

Syntax Description

timer	Specifies the prefix route dampening time period, in seconds. The range for this argument is from 90 to 65535. The default value is 300.

Command Default

PfR uses the default value of 300 seconds for the prefix route dampening time period if this command is not configured or if the **no** form of this command is entered.

Command Modes

PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **holddown** command is entered on a master controller. This command is used to configure the prefix route dampening timer to set the minimum period of time for which a new exit must be used before an alternate exit can be selected. The master controller puts a prefix in a holddown state during an exit change to isolate the prefix during the transition period to prevent the prefix from flapping because of rapid state changes. PfR does not implement policy changes while a prefix is in the holddown state. A prefix will remain in a holddown state for the default or configured time period. When the holddown timer expires, PfR will select the best exit based on performance and policy configuration. However, an immediate route change will be triggered if the current exit for a prefix becomes unreachable.

Configuring a new timer value will immediately replace the existing value if the new value is less than the amount of the time remaining. If the new value is greater than the amount of the time remaining, the new timer value will be used when the existing timer is reset.

Examples

The following example sets the prefix route dampening timer to 120 seconds:

```
Router(config)# pfr master
Router(config-pfr-mc)# holddown 120
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
set holddown (PfR)	Configures a PfR map to set the prefix route dampening timer to the minimum period of time for which a new exit must be used before an alternate exit can be selected.

host-address (PfR)

To configure information about a host device used by an application interface provider to communicate with a Performance Routing (PfR) master controller, use the **host-address** command in PfR master controller application interface provider configuration mode. To remove a host application interface device, use the **no** form of this command.

host-address *ip-address* **key-chain** *key-chain-name* [**priority** *value*]

no host-address *ip-address*

Syntax Description

ip-address	IP address of the host device.
key-chain	Specifies the key used as a password to authenticate communication for the host device.
key-chain-name	Name of key chain used as a password for the host device.
priority	(Optional) Sets the priority of the host device.
value	(Optional) A number in the range from 1 to 65535. The lower the number, the higher the priority. The default priority is 65535.

Command Default

A host application interface device is not configured.

Command Modes

PfR master controller application interface provider configuration (config-pfr-mc-api-provider)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The PfR application interface defines the mode of communication and messaging between applications and the network for the purpose of optimizing the traffic associated with the applications. A provider is defined as an entity outside the network in which the router configured as a PfR master controller exists, for example, an ISP or a branch office of the same company. The provider has one or more host devices running one or more applications that use the PfR application interface to communicate with a PfR master controller. A provider must be registered with a PfR master controller before an application on a host device can interface with PfR. Use the **api provider** (PfR) command to register the provider, and use the **host-address** command to configure a host device. After registration, a host device in the provider network can initiate a session with a PfR master controller. The PfR application interface provides an automated method for networks to be aware of applications and provides application-aware performance routing.

Use the optional **priority** keyword to specify a priority value for the host device when multiple host devices are configured. The number 1 assigns the highest priority to any requests from the host device. If you assign a priority, each host device must be assigned a different priority number. If you try to assign the same priority number to two different host devices, an error message is displayed on the console.

Examples

The following example shows how to configure a host application interface device on a master controller. In this example, more than one provider is registered, and a priority is set for each provider. For the single host device configured for provider 1, no priority is set and the default priority value of 65535 is assigned, giving this host device a lower priority than each of the host devices configured for provider 2.

```
Router(config)# pfr master
Router(config-pfr-mc)# api provider 1
Router(config-pfr-mc-api-provider)# host-address 10.100.2.2 key-chain PFR_HOST
Router(config-pfr-mc-api-provider)# exit
Router(config-pfr-mc)# api provider 2 priority 4000
Router(config-pfr-mc-api-provider)# host-address 10.100.2.2 key-chain PFR_HOST
priority 3000
Router(config-pfr-mc-api-provider)# host-address 10.100.2.2 key-chain PFR_HOST
priority 4000
Router(config-pfr-mc-api-provider)# end
```

Related Commands

Command	Description
api provider (PfR)	Registers an application interface provider with a PfR master controller and enters PfR master controller application interface provider configuration mode.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
show pfr api provider	Displays information about application interface providers registered with PfR.

inside bgp (PfR)

To configure Performance Routing (PfR) to learn the inside prefixes within a network, use the **inside bgp** command in PfR Top Talker and Top Delay learning configuration mode. To disable prefix learning of inside prefixes, use the **no** form of this command.

inside bgp

no inside bgp

Syntax Description

This command has no arguments or keywords.

Command Default

No inside prefixes are learned by PfR.

Command Modes

PfR Top Talker and Top Delay learning configuration (config-pfr-mc-learn)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

This command is used to implement PfR Border Gateway Protocol (BGP) inbound optimization by identifying the prefixes within a network (inside prefixes). PfR BGP inbound optimization supports best entrance selection for traffic that originates from prefixes outside an autonomous system destined for prefixes inside the autonomous system. External BGP (eBGP) advertisements from an autonomous system to another autonomous system (for example, an Internet service provider [ISP]) can influence the entrance path for traffic entering the network. PfR uses eBGP advertisements to manipulate the best entrance selection.

Examples

The following example shows how to configure a PfR master controller to automatically learn the inside prefixes in a network:

```
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# inside bgp
```

Related Commands

Command	Description
learn (PfR)	Enters PfR Top Talker and Top Delay learning configuration mode to configure prefixes for PfR to learn.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

interface (PfR)

To configure a border router interface as a Performance Routing (PfR) managed external or internal interface, use the **interface** command in PfR managed border router configuration mode. To remove an interface from PfR control, use the **no** form of this command.

interface *type number* {**external** | **internal**}

no interface *type number* {**external** | **internal**}

Syntax Description

type	Specifies the type of interface.
number	Specifies the interface or subinterface number.
external	Configures an interface as external. External interfaces are used for active monitoring and traffic forwarding. Entering the **external** keyword also enters PfR border exit interface configuration mode.
internal	Configures an interface as internal. Internal interfaces are used for passive monitoring with NetFlow.

Command Default

No border router interfaces are configured as PfR-managed interfaces.

Command Modes

PfR managed border router configuration (config-pfr-mc-br)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **interface** command is entered on a master controller. This command is used to configure external and internal interfaces on border routers to be under PfR control. External interfaces are configured as PfR managed exit links to forward traffic. External interfaces are used by the master controller to actively monitor prefix and link performance. Internal interfaces are used only for passive performance monitoring with NetFlow.

At least one external and one internal interface must be configured on each border router to allow NetFlow to monitor inbound and outbound traffic. At least two external interfaces are required in a PfR-managed network. You can configure a maximum of 20 external interfaces for a single master controller in a PfR-managed network. Loopback interfaces are supported as external or internal interfaces.

Note PfR does not support Ethernet interfaces that are Layer 2 only, for example, Ethernet switched interfaces.

Configuring an interface as external enters PfR border exit configuration mode. Under PfR border exit interface configuration mode, you can configure maximum link utilization on a per-interface basis with the **max-xmit-utilization** (PfR) command.

Note Entering the **interface** command without the **external** or **internal** keyword places the router in global configuration mode and not PfR border exit configuration mode. The **no** form of this command should be applied carefully so that active interfaces are not removed from the router configuration.

Examples

The following example configures one internal interface and two external interfaces on a border router:

```
Router(config)# pfr master
Router(config-pfr-mc)# border 10.4.9.6 key-chain BR-KEY
Router(config-pfr-mc-br)# interface FastEthernet0/1 internal
Router(config-pfr-mc-br)# interface FastEthernet0/0 external
Router(config-pfr-mc-br)# interface Serial 1/0 external
```

Related Commands

Command	Description
border (PfR)	Enters PfR-managed border router configuration mode to establish communication with a PfR border router.
local (PfR)	Identifies a local interface on a PfR border router as the source for communication with a PfR master controller.
max-xmit-utilization (PfR)	Configures maximum utilization on a single PfR-managed exit link.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

jitter (PfR)

To specify the threshold jitter value that Performance Routing (PfR) will permit for an exit link, use the **jitter** command in PfR master controller configuration mode. To reset the maximum jitter value to its default value, use the **no** form of this command.

jitter threshold *maximum*

no jitter threshold

Syntax Description

threshold	Specifies a maximum absolute threshold value for jitter. Jitter is a measure of voice quality.
maximum	Number (in milliseconds) in the range from 1 to 1000, where 1 represents the highest voice quality, and 1000 represents the lowest voice quality. The default value is 30.

Command Default

No jitter values are specified.

Command Modes

PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **jitter** command is used to specify the maximum tolerable jitter value permitted on an exit link. Jitter is a measure of voice quality where the lower the jitter value, the better the voice quality. If the jitter value is greater than the user-defined or the default value, PfR determines that the exit link is out-of-policy and searches for an alternate exit link.

Another measure of voice quality is the estimated Mean Opinion Score (MOS). Use the **mos** command and the **jitter** command in a PfR policy to define voice quality.

Examples

The following example shows how to configure the master controller to search for a new exit link if the jitter threshold value exceeds 20 milliseconds:

```
Router(config)# pfr master
Router(config-pfr-map)# jitter threshold 20
```

Related Commands

Command	Description
mos (PfR)	Specifies the threshold and percentage MOS values that PfR will permit for an exit link.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
set jitter (PfR)	Configures a PfR map to set the threshold jitter value that PfR will permit for an exit link.

keepalive (PfR)

To configure the length of time that a Performance Routing (PfR) master controller will maintain connectivity with a PfR border router after no keepalive packets have been received, use the **keepalive** command in PfR master controller configuration mode. To return the keepalive timer to the default time interval, use the **no** form of this command.

keepalive [*timer*]

no keepalive

Syntax Description

timer	(Optional) Sets the keepalive time interval, in seconds. The configurable range for this argument is from 0 to 1000. The default time interval is 5.

Command Default

PfR sets the keepalive time interval to 5 seconds if this command is not configured or if the **no** form of this command is entered.

Command Modes

PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **keepalive** command is entered on a master controller. The PfR master controller sends keepalive packets to border routers to maintain connectivity between the master controller and the border router. If the master controller does not receive keepalive packets from a border router before the keepalive timer expires and this situation happens three times in a row, then the master controller will not maintain the connection.

Examples

The following example sets the keepalive time interval to 10 seconds:

```
Router(config)# pfr master
Router(config-pfr-mc)# keepalive 10
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

learn (PfR)

To enter PfR Top Talker and Top Delay learning configuration mode to configure Performance Routing (PfR) to learn prefixes, use the **learn** command in PfR master controller configuration mode. To disable prefix learning, use the **no** form of this command.

learn

no learn

Syntax Description

This command has no arguments or keywords.

Command Default

PfR Top Talker and Top Delay learning configuration mode is not entered.

Command Modes

PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **learn** command is entered on a master controller and is used to enter PfR Top Talker and Top Delay learning configuration mode to configure a master controller to learn and optimize prefixes based on the highest throughput or the highest delay. Under the Top Talker and Top Delay learning configuration mode, you can configure prefix learning based on delay and throughput statistics. You can configure the length of the prefix learning period, the interval between prefix learning periods, the number of prefixes to learn, and the prefix learning based on protocol.

Examples

The following example enters PfR Top Talker and Top Delay learning configuration mode:

```
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)#
```

Related Commands

Command	Description
match pfr learn	Creates a match clause entry in a PfR map to match PfR-learned prefixes.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

link-group (PfR)

To configure a Performance Routing (PfR) border router exit interface as a member of a link group, use the **link-group** command in PfR border exit interface configuration mode. To remove an interface from a link group from the, use the **no** form of this command.

link-group *link-group-name* [*link-group-name* [*link-group-name*]]

no link-group *link-group-name* [*link-group-name* [*link-group-name*]]

Syntax Description

link-group-name	Name of a link group.

Command Default

No link groups are configured for a PfR border router exit interface.

Command Modes

PfR border exit interface configuration (config-pfr-mc-br-if)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Link groups are used to define a group of exit links as a preferred set of links or as a fallback set of links for PfR to use when optimizing a specified traffic class. Up to three link groups can be specified for each interface. Configure this command on a master controller to define the link group for an interface, and use the **set link-group** (PfR) command to define the primary link group and a fallback link group for a specified traffic class in a PfR map.

Use the **show pfr master link-group** command to view information about configured PfR link groups.

Examples

The following example configures one external interface on a border router as a member of the link group named VIDEO and another external interface as a member of two link groups named VOICE and DATA:

```
Router(config)# pfr master
Router(config-pfr-mc)# border 10.4.9.6 key-chain BR-KEY
Router(config-pfr-mc-br)# interface Serial 1/0 external
Router(config-pfr-mc-br-if)# link-group VIDEO
Router(config-pfr-mc-br-if)# exit
Router(config-pfr-mc-br)# interface Serial 2/0 external
Router(config-pfr-mc-br-if)# link-group VOICE DATA
Router(config-pfr-mc-br-if)# exit
Router(config-pfr-mc-br)# interface FastEthernet0/1 internal
Router(config-pfr-mc-br)# end
```

Related Commands

Command	Description
border (PfR)	Enters PfR managed border router configuration mode to establish communication with a PfR border router.
interface (PfR)	Configures a border router interface as a PfR managed external or internal interface.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
set link-group (PfR)	Specifies a link group for traffic classes defined in a PfR policy.
show pfr master link-group	Displays information about PfR link groups.

list (PfR)

To create a Performance Routing (PfR) learn list to specify criteria for learning traffic classes and to enter learn list configuration mode, use the **list** command in PfR Top Talker and Top Delay learning configuration mode. To remove the learn list, use the **no** form of this command.

list seq *number* **refname** *ref-name*

no list seq *number* **refname** *ref-name*

Syntax Description

seq	Applies a sequence number to a learn list.
number	Number representing a sequence that is used to determine the order in which learn list criteria are applied. The range of sequence numbers that can be entered is from 1 to 65535.
refname	Specifies a reference name for the PfR learn list.
ref-name	Reference name for the learn list. The name must be unique within all the configured PfR learn lists.

Command Default

No PfR learn lists are created.

Command Modes

PfR Top Talker and Top Delay learning configuration (config-pfr-mc-learn)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

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

New **traffic-class** commands were introduced under learn list configuration mode to simplify the learning of traffic classes. Three types of traffic classes—to be automatically learned—can be profiled:

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

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

Examples

The following example shows how to configure a master controller to learn top prefixes based on the highest throughput for a learn list named LEARN_REMOTE_LOGIN_TC that learns Telnet and Secure Shell (SSH) application traffic class entries:

```
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# list seq 10 refname LEARN_REMOTE_LOGIN_TC
Router(config-pfr-mc-learn-list)# traffic-class application telnet ssh
Router(config-pfr-mc-learn-list)# aggregation-type prefix-length 24
Router(config-pfr-mc-learn-list)# throughput
```

Related Commands

Command	Description
learn (PfR)	Enters PfR Top Talker and Top Delay learning configuration mode to configure PfR to automatically learn traffic classes.
pfr	Enables a PfR process and configure a router as a PfR border router or as a PfR master controller.

local (PfR)

To identify a local interface on a Performance Routing (PfR) border router as the source for communication with a PfR master controller, use the **local** command in PfR border router configuration mode. To remove the interface from the PfR border router configuration and disable communication between the border router and the master controller, use the **no** form of this command.

local *interface-type interface-number*

no local *interface-type interface-number*

Syntax Description

interface-type	Specifies the interface type.
interface-number	Specifies the interface number.

Command Default

No local interface is configured.

Command Modes

PfR border router configuration (config-pfr-br)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **local** command is configured on a PfR border router. This command is used to specify the source interface IP address that will be used for communication between a border router and a master controller.

The IP address that is configured for the local interface must also be configured on the master controller using the **border** (PfR) command and the **interface** (PfR) command.

The **no** form of this command cannot be entered while the border router process is active. The border router process must first be stopped with the **shutdown** (PfR) command. If you stop the border router process to deconfigure the local interface with the **no** form of this command, you must configure another local interface before the border router process will reestablish communication with the master controller.

Examples

The following example configures Fast Ethernet interface 0/0 as a local interface:

```
Router(config)# pfr border
Router(config-pfr-br)# local FastEthernet0/0
```

Related Commands

Command	Description
border (PfR)	Enters PfR-managed border router configuration mode to establish communication with a PfR border router.
interface (PfR)	Configures a border router interface as a PfR-managed external or internal interface.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

logging (PfR)

To enable syslog event logging for a Performance Routing (PfR) master controller or a PfR border router process, use the **logging** command in PfR master controller or PfR border router configuration mode. To disable PfR event logging, use the **no** form of this command.

logging

no logging

Syntax Description

This command has no keywords or arguments.

Command Default

Syslog event logging is not enabled for a PfR master controller or border router process.

Command Modes

PfR border router configuration (config-pfr-br)
PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **logging** command is entered on a master controller or border router. System logging is enabled and configured in Cisco IOS software under global configuration mode. The **logging** command in PfR master controller or PfR border router configuration mode is used only to enable or disable system logging under PfR. PfR system logging supports the following message types:

- *Error Messages*—These messages indicate PfR operational failures and communication problems that can impact normal PfR operation.
- *Debug Messages*—These messages are used to monitor detailed PfR operations to diagnose operational or software problems.
- *Notification Messages*—These messages indicate that PfR is performing a normal operation.
- *Warning Messages*—These messages indicate that PfR is functioning properly, but an event outside of PfR may be impacting normal PfR operation.

To modify system, terminal, destination, and other system global logging parameters, use the **logging** commands in global configuration mode. For more information about system logging commands, see the *Cisco IOS Configuration Fundamentals Command Reference*.

Cisco IOS XE Release 3.1S

This command is supported only in PfR border router configuration mode.

Examples

The following example enables PfR system logging on a master controller:

```
Router(config)# pfr master
Router(config-pfr-mc)# logging
```

The following example enables PfR system logging on a border router:

```
Router(config)# pfr border
Router(config-pfr-br)# logging
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

loss (PfR)

To set the relative or maximum packet loss limit that Performance Routing (PfR) will permit for an exit link, use the **loss** command in PfR master controller configuration mode. To return the packet loss limit to the default value, use the **no** form of this command.

loss {**relative** *average* | **threshold** *maximum*}

no loss

Syntax Description

relative *average*	Sets a relative percentage of packet loss based on a comparison of short-term and long-term packet loss percentages. The range of values that can be configured for this argument is a number from 1 to 1000. Each increment represents one tenth of a percent.
threshold *maximum*	Sets absolute packet loss based on packets per million (PPM). The range of values that can be configured for this argument is from 1 to 1000000.

Command Default

PfR uses the following default value if this command is not configured or if the **no** form of this command is entered:

relative *average*: 100 (10 percent packet loss)

Command Modes

PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **loss** command is used to specify the relative percentage or maximum number of packets that PfR will permit to be lost during transmission on an exit link. If packet loss is greater than the user-defined or default value, PfR determines that the exit link is out-of-policy and searches for an alternate exit link.

The **relative** keyword is used to configure the relative packet loss percentage. The relative packet loss percentage is based on a comparison of short-term and long-term packet loss. The short-term measurement reflects the percentage of packet loss within a 5-minute period. The long-term measurement reflects the percentage of packet loss within a 60-minute period. The following formula is used to calculate this value:

Relative packet loss = ((short-term loss – long-term loss) / long-term loss) * 100

The master controller measures the difference between these two values as a percentage. If the percentage exceeds the user-defined or default value, the exit link is determined to be out-of-policy. For example, if long-term packet loss is 200 PPM and short-term packet loss is 300 PPM, the relative loss percentage is 50 percent.

The **threshold** keyword is used to configure the absolute maximum packet loss. The maximum value is based on the actual number of PPM that have been lost.

Examples

The following example configures the master controller to search for a new exit link if the difference between long- and short-term measurements (relative packet loss) is greater than 20 percent:

```
Router(config)# pfr master
Router(config-pfr-mc)# loss relative 200
```

The following example configures PfR to search for a new exit link when 20,000 packets have been lost:

```
Router(config)# pfr master
Router(config-pfr-mc)# loss threshold 20000
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
set loss (PfR)	Configures a PfR map to set the relative or maximum packet loss limit that PfR will permit for an exit link.

master (PfR)

To establish communication with a Performance Routing (PfR) master controller, use the **master** command in PfR border router configuration mode. To disable communication with the specified master controller, use the **no** form of this command.

master *ip-address* **key-chain** *key-name*

no master

Syntax Description

ip-address	IP address of the master controller.
key-chain *key-name*	Specifies the key chain to authenticate with the master controller.

Command Default

No communication is established between a border router and a master controller.

Command Modes

PfR border router configuration (config-pfr-br)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **master** command is entered on a border router. This command is used to establish communication between a PfR border router and a master controller. Communication is established between the border router process and the master controller process to allow the master controller to monitor and control PfR exit links. PfR communication must also be established on the master controller with the **border** PfR master controller configuration command. At least one border router must be configured to enable PfR. A maximum of ten border routers can be configured to communicate with a single master controller. The IP address that is used to specify the border router must be assigned to a local interface on the border router and must be reachable by the master controller.

By default, passive monitoring in PfR observe mode is enabled when communication is established between a master controller and a border router. Communication between the master controller and the border router is protected by key-chain authentication. The authentication key must be configured on both the master controller and the border router before communication can be established. The key-chain configuration is defined in global configuration mode on both the master controller and the border router before key-chain authentication is enabled for communication between a master controller and a border router. For more information about key management in Cisco IOS software, see the "Managing Authentication Keys" section in the "Configuring IP Protocol-Independent Features" chapter of the *Cisco IOS IP Routing: Protocol-Independent Configuration Guide*.

Examples

The following example defines a key chain named MASTER in global configuration mode and then configures a PfR border router to communicate with the PfR master controller at 10.4.9.7. The master controller authenticates the border router based on the defined key CISCO.

```
Router(config)# key chain MASTER
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string CISCO
Router(config-keychain-key)# exit
Router(config-keychain)# exit
Router(config)# pfr border
Router(config-pfr-br)# master 10.4.9.7 key-chain MASTER
Router(config-pfr-br)# end
```

Related Commands

Command	Description
border (PfR)	Enters PfR managed border router configuration mode to establish communication with a PfR border router.
key	Identifies an authentication key on a key chain.
key chain (IP)	Enables authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

match ip address (PfR)

To reference an extended IP access list or an IP prefix as match criteria in a Performance Routing (PfR) map, use the **match ip address** command in PfR map configuration mode. To delete the match clause entry, use the **no** form of this command.

match ip address {**access-list** *name* | **prefix-list** *name* [**inside**]}

no match ip address

Syntax Description

access-list *name*	Specifies a named extended access list (created with the **ip access-list** command) as the match criterion in a PfR map.
prefix-list *name*	Specifies a prefix list (created with the **ip prefix-list** command) as the match criterion in a PfR map.
inside	(Optional) Specifies an inside prefix.

Command Default

No match is performed.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **match ip address** (PfR) command defines a policy, within a PfR map, for a list of prefixes. The **match ip address** (PfR) command is entered on a master controller in PfR map configuration mode. This command is used to configure a named extended access list or IP prefix list as a match criteria in a PfR map. Only one match clause can be configured for each PfR map sequence. The access list is created with the **ip access-list** command. Only named extended IP access lists are supported. The IP prefix list is created with the **ip prefix-list** command. A prefix can be any IP network number combined with a prefix mask that specifies the prefix length.

The **inside** keyword is used to support PfR BGP inbound optimization which in turn supports best entrance selection for traffic that originates from prefixes outside an autonomous system destined for prefixes inside the autonomous system. External BGP (eBGP) advertisements from an autonomous system to an Internet service provider (ISP) can influence the entrance path for traffic entering the network. PfR uses eBGP advertisements to manipulate the best entrance selection.

Examples

The following example creates a prefix list named CUSTOMER. The prefix list creates a filter for the 10.4.9.0/24 network. The **match ip address** (PfR) command configures the prefix list as match criterion in a PfR map.

```
Router(config)# ip prefix-list CUSTOMER permit 10.4.9.0/24
Router(config)# pfr-map SELECT_EXIT 10
Router(config-pfr-map)# match ip address prefix-list CUSTOMER
Router(config-pfr-map)# set mode select-exit good
```

The following example creates an extended access list named FTP. The named extended access list creates a filter for FTP traffic that is sourced from the 10.1.1.0/24 network. The **match ip address** (PfR) command configures the access list as the match criterion in a PfR map. FTP traffic is policy-routed to the first in-policy exit.

```
Router(config)# ip access-list extended FTP
Router(config-ext-nacl)# permit tcp 10.1.1.0 0.0.0.255 any eq ftp
Router(config-ext-nacl)# exit
Router(config)# pfr-map SELECT_EXIT 10
Router(config-pfr-map)# match ip address access-list FTP
Router(config-pfr-map)# set mode select-exit good
```

The following example creates a prefix list named INSIDE1. The prefix list creates a filter for the 10.2.2.0/24 network. The **match ip address** (PfR) command configures the prefix list as the match criterion in a PfR map.

```
Router(config)# ip prefix-list INSIDE1 seq 5 permit 10.2.2.0/24
Router(config)# pfr-map INSIDE_PREFIXES 10
Router(config-pfr-map)# match ip address prefix-list INSIDE1 inside
Router(config-pfr-map)# set as-path prepend 45000
```

Related Commands

Command	Description
ip access-list	Defines an IP access list.
ip prefix-list	Creates an entry in a prefix list.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.

match pfr learn

To create a match clause entry in a Performance Routing (PfR) map to match PfR-learned prefixes, use the **match pfr learn** command in PfR map configuration mode. To delete the match clause entry, use the **no** form of this command.

match pfr learn {**delay** | **inside** | **list** *refname* | **throughput**}

no match pfr learn {**delay** | **inside** | **list** |**throughput**}

Syntax Description

delay	Specifies prefixes learned based on highest delay.
inside	Specifies prefixes learned based on prefixes that are inside the network.
list	Specifies prefixes learned based on a PfR learn list.
refname	Reference name for a learn list. The name is defined using the **list** (PfR) command and must be unique within all the configured PfR learn lists.
throughput	Specifies prefixes learned based on highest throughput.

Command Default

No match is performed.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **match pfr learn** command is entered on a master controller in PfR map configuration mode. PfR can be configured to learn prefixes based on delay, inside prefix, criteria specified in a learn list, or throughput. This command is used to configure PfR learned prefixes as match criteria in a PfR map. Only one match clause can be configured for each PfR map sequence.

Examples

The following example creates a PfR map named DELAY that matches traffic learned based on delay. The set clause applies a route control policy that configures PfR to actively control this traffic.

```
Router(config)# pfr-map DELAY 20
Router(config-pfr-map)# match pfr learn delay
Router(config-pfr-map)# set mode route control
```

The following example creates a PfR map named INSIDE that matches traffic learned based on inside prefixes. The set clause applies a route control policy that configures PfR to actively control this traffic.

```
Router(config)# pfr-map INSIDE 40
Router(config-pfr-map)# match pfr learn inside
Router(config-pfr-map)# set mode route control
```

The following example creates a PfR map named LIST that matches traffic learned based on criteria defined in the PfR learn list named LEARN_LIST_TC. prefixes. The learn list policy map is activated using the **policy-rules** (PfR) command.

```
Router(config)# pfr-map LIST 40
Router(config-pfr-map)# match pfr learn LEARN_LIST_TC
Router(config-pfr-map)# exit
Router(config)# pfr master
Router(config-pfr-mc)# policy-rules LIST
```

The following example creates a PfR map named THROUGHPUT that matches traffic learned based on throughput. The set clause applies a route control policy that configures PfR to actively control this traffic.

```
Router(config)# pfr-map THROUGHPUT 30
Router(config-pfr-map)# match pfr learn throughput
Router(config-pfr-map)# set mode route control
```

Related Commands

Command	Description
learn (PfR)	Enters PfR Top Talker and Top Delay learning configuration mode to configure PfR to learn prefixes.
list (PfR)	Creates a PfR learn list to specify criteria for learning traffic classes and enters learn list configuration mode.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.
policy-rules (PfR)	Applies a configuration from a PfR map to a master controller configuration.

match traffic-class access-list (PfR)

To define a match clause using an access list in a Performance Routing (PfR) map to create a traffic class, use the **match traffic-class access-list** command in PfR map configuration mode. To remove the match clause, use the **no** form of this command.

match traffic-class access-list *access-list-name*

no match traffic-class access-list

Syntax Description

access-list-name	Name of an access list. Names cannot contain either a space or quotation marks and must begin with an alphabetic character to distinguish them from numbered access lists.

Command Default

PfR traffic classes are not defined using match criteria in a PfR map.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **match traffic-class access-list** command is used to manually configure a traffic class that matches destination prefixes in an access list used in a PfR map. Only one access list can be specified, but the access list may contain many access list entries to help define the traffic class.

Note The **match traffic-class access-list** (PfR) command, the **match traffic-class prefix-list** (PfR) command, the **match traffic-class application** (PfR) command, and the **match traffic-class application nbar** (PfR) commands are all mutually exclusive in a PfR map. Only one of these commands can be specified per PfR map.

Examples

The following example, starting in global configuration mode, shows how to define a custom traffic class using an access list. Every entry in the access list defines one destination network and can include optional criteria. A PfR map is used to match the destination prefixes and create the custom traffic class.

```
Router(config)# ip access-list extended CONFIGURED_TC
Router(config-ext-nacl)# permit tcp any 10.1.1.0 0.0.0.255 eq 500
Router(config-ext-nacl)# permit tcp any 172.16.1.0 0.0.0.255 eq 500 range 700 750
Router(config-ext-nacl)# permit tcp any 172.16.1.0 0.0.0.255 range 700 750
Router(config-ext-nacl)# permit tcp 192.168.0.0 0.0.255.255 10.1.2.0 0.0.0.255 eq 800
Router(config-ext-nacl)# exit
Router(config)# pfr-map ACCESS_MAP 10
Router(config-pfr-map)# match traffic-class access-list CONFIGURED_TC
Router(config-pfr-map)# end
```

Related Commands

Command	Description
ip access-list	Defines a standard or extended IP access list.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.

match traffic-class application (PfR)

To define a match clause using a static application mapping in a Performance Routing (PfR) map to create a traffic class, use the **match traffic-class application** command in PfR map configuration mode. To remove the match clause entry, use the **no** form of this command.

match traffic-class application *application-name* [*application-name ...*] **prefix-list** *prefix-list-name*

no match traffic-class application *application-name ...* [**prefix-list** *prefix-list-name*]

Syntax Description

application-name	Name of a predefined static application using fixed ports. See Table 22.One application must be specified, but the ellipsis shows that more than one application keyword can be specified up to a maximum of ten.
prefix-list	Specifies that the traffic flows are matched on the basis of destinations specified in a prefix list.
prefix-list-name	Name of a prefix list (created using the **ip prefix-list** command).

Command Default

PfR traffic classes are not defined using match criteria in a PfR map.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **match traffic-class application** command is used to manually configure the master controller to profile traffic destined for prefixes defined in an IP prefix list that match one or more applications. The applications are predefined with a protocol—TCP or UDP, or both—and one or more ports and this mapping is shown in Table 22. More than one application can be configured as part of the traffic class.

Note The **match traffic-class application** (PfR) command, the **match traffic-class application nbar** (PfR) command, the **match traffic-class access-list** (PfR) command, and the **match traffic-class prefix-list** (PfR) commands are all mutually exclusive in a PfR map. Only one of these commands can be specified per PfR map.

Table 22 displays the keywords that represent the application that can be configured with the **match traffic-class application** command. Replace the *application-name* argument with the appropriate keyword from the table.

Table 22 Static Application List Keywords

Keyword	Protocol	Port
cuseeme	TCP UDP	7648 7649 7648 7649 24032
dhcp (Client)	UDP/TCP	68
dhcp (Server)	UDP/TCP	67
dns	UDP/TCP	53
finger	TCP	79
ftp	TCP	20 21
gopher	TCP/UDP	70
http	TCP/UDP	80
httpssl	TCP	443
imap	TCP/UDP	143 220
irc	TCP/UDP	194
kerberos	TCP/UDP	88 749
l2tp	UDP	1701
ldap	TCP/UDP	389
mssql	TCP	1443
nfs	TCP/UDP	2049
nntp	TCP/UDP	119
notes	TCP/UDP	1352
ntp	TCP/UDP	123
pcany	UDP TCP	22 5632 65301 5631
pop3	TCP/UDP	110
pptp	TCP	17233
simap	TCP/UDP	585 993 (Preferred)
sirc	TCP/UDP	994
sldap	TCP/UDP	636
smtp	TCP	25
snntp	TCP/UDP	563
spop3	TCP/UDP	123
ssh	TCP	22
telnet	TCP	23

Examples

The following example, starting in global configuration mode, shows how to define application traffic classes in a PfR map named APP_MAP using predefined Telnet and Secure Shell (SSH) application criteria that are matched with destination prefixes specified in a prefix list, LIST1.

```
Router(config)# ip prefix-list LIST1 permit 10.1.1.0/24
Router(config)# ip prefix-list LIST1 permit 10.1.2.0/24
Router(config)# ip prefix-list LIST1 permit 172.16.1.0/24
Router(config)# pfr-map APP_MAP 10
Router(config-pfr-map)# match traffic-class application telnet ssh prefix-list LIST1
Router(config-pfr-map)# end
```

Related Commands

Command	Description
ip prefix-list	Creates an entry in a prefix list.
match traffic-class application nbar (PfR)	Defines a match clause using an NBAR application mapping in a PfR map to create a traffic class.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.

match traffic-class application nbar (PfR)

To define a match clause using an Network-Based Application Recognition (NBAR) application mapping in a Performance Routing (PfR) map to create a traffic class, use the **match traffic-class application nbar** command in PfR map configuration mode. To remove the match clause entry, use the **no** form of this command.

match traffic-class application nbar *nbar-appl-name* [*nbar-appl-name* **...**] **prefix-list** *prefix-list-name*

no match traffic-class application nbar [*nbar-appl-name* **...**]

Syntax Description

nbar-appl-name	Keyword representing the name of an application identified using NBAR. One application must be specified, but the ellipsis shows that more than one application keyword can be specified up to a maximum of ten. See the "Usage Guidelines" section for more details.
prefix-list	Specifies that the traffic flows are matched on the basis of destinations specified in a prefix list.
prefix-list-name	Name of a prefix list (created using the **ip prefix-list** command).

Command Default

PfR traffic classes identified using NBAR are not defined using match criteria in a PfR map.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **match traffic-class application nbar** command is used to manually configure the master controller to profile traffic destined for prefixes defined in an IP prefix list that match one or more applications identified using NBAR. More than one application can be configured as part of the traffic class with a maximum of ten applications entered per command line. Enter multiple **match traffic-class application nbar** command statements if you need to specify more than ten applications.

NBAR is capable of identifying applications based on the following three types of protocols:

- Non-UDP and non-TCP IP protocols—For example, Generic Routing Encapsulation (GRE) and Internet Control Message Protocol (ICMP).
- TCP and UDP protocols that use statically assigned port numbers—For example, CU-SeeMe desktop video conference (CU-SeeMe-Server), Post Office Protocol over Transport Layer Security (TLS), and Secure Sockets Layer (SSL) server (SPOP3-Server).
- TCP and UDP protocols that dynamically assign port numbers and require stateful inspection—For example, Real-Time Transport Protocol audio streaming (RTP-audio) and BitTorrent File Transfer Traffic (BitTorrent).

Use the **match traffic-class application nbar ?** command to determine if an application can be identified using NBAR and replace the *nbar-appl-name* argument with the appropriate keyword from the screen display.

The list of applications identified using NBAR and available for profiling PfR traffic classes is constantly evolving. For lists of many of the NBAR applications defined using static or dynamically assigned ports, see the "Performance Routing with NBAR/CCE Application and Recognition" module.

For more details about NBAR, see the "Classifying Network Traffic Using NBAR" section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note The **match traffic-class application nbar** (PfR) command, the **match traffic-class application** (PfR) command, the **match traffic-class access-list** (PfR) command, and the **match traffic-class prefix-list** (PfR) commands are all mutually exclusive in a PfR map. Only one of these commands can be specified per PfR map.

Examples

The following example, starting in global configuration mode, shows how to define an application traffic class in a PfR map named APP_NBAR_MAP. The traffic class consists of RTP-audio traffic identified using NBAR and matched with destination prefixes specified in a prefix list, LIST1.

The traffic streams that the PfR map profiles for the RTP-audio application are:

```
10.1.1.1
10.2.2.1
172.16.1.1
172.17.1.2
```

The traffic classes that are learned for the RTP-audio application are:

```
10.2.2.0/24
172.17.1.0/24
```

Only traffic that matches both the RTP-audio application and the destination prefixes is learned.

```
Router(config)# ip prefix-list LIST1 permit 10.2.1.0/24
Router(config)# ip prefix-list LIST1 permit 10.2.2.0/24
Router(config)# ip prefix-list LIST1 permit 172.17.1.0/24
Router(config)# pfr-map APP_NBAR_MAP 10
Router(config-pfr-map)# match traffic-class application nbar rtp-audio prefix-list LIST1
Router(config-pfr-map)# end
```

Related Commands

Command	Description
ip prefix-list	Creates an entry in a prefix list.
match traffic-class application (PfR)	Defines a match clause using a static application mapping in a PfR map to create a traffic class.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.
traffic-class application nbar (PfR)	Defines a PfR traffic class using an NBAR application mapping.

match traffic-class prefix-list (PfR)

To define a match clause using a prefix list in a Performance Routing (PfR) map to create a traffic class, use the **match traffic-class prefix-list** command in PfR map configuration mode. To remove the match clause, use the **no** form of this command.

match traffic-class prefix-list *prefix-list-name* [**inside**]

no match traffic-class prefix-list

Syntax Description

prefix-list-name	Name of a prefix list.
inside	(Optional) Specifies that the prefix list contains inside prefixes.

Command Default

PfR traffic classes are not defined using match criteria in a PfR map.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **match traffic-class prefix-list** command is used to manually configure a traffic class that matches destination prefixes in a prefix list.

Use the optional **inside** keyword to specify prefixes that are within the internal network.

Note The **match traffic-class prefix-list** (PfR) command, the **match traffic-class access-list** (PfR) command, the **match traffic-class application** (PfR), and the **match traffic-class application nbar** (PfR) commands are all mutually exclusive in a PfR map. Only one of these commands can be specified per PfR map.

Examples

The following example, starting in global configuration mode, shows how to manually configure a traffic class based only on destination prefixes. The traffic class is created using the prefix list LIST1 in a PfR map named PREFIX_MAP. Every entry in the prefix list, LIST1, defines one destination network of the traffic class.

```
Router(config)# ip prefix-list LIST1 permit 10.1.1.0/24
Router(config)# ip prefix-list LIST1 permit 10.1.2.0/24
Router(config)# ip prefix-list LIST1 permit 172.16.1.0/24
Router(config)# pfr-map PREFIX_MAP 10
Router(config-pfr-map)# match traffic-class prefix-list LIST1
Router(config-pfr-map)# end
```

Related Commands

Command	Description
ip prefix-list	Creates an entry in a prefix list.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.
traffic-class prefix-list (PfR)	Defines a PfR traffic class based only on destination prefixes.

max prefix (PfR)

To set the maximum number of prefixes that a Performance Routing (PfR) master controller will monitor or learn, use the **max prefix** command in PfR master controller configuration mode. To return the master controller to default values, use the **no** form of this command.

max prefix total *number* [**learn** *number*]

no max prefix total

Syntax Description

total *number*	Sets the total number of prefixes that the master controller will monitor. The range of values that can be entered for this argument is a number from 1 to 5000. Default value is 5000.
learn *number*	(Optional) Sets the total number of prefixes that the master controller will learn. The range of values that can be entered for this argument is a number from 1 to 2500. Default value is 2500.

Command Default

PfR uses the following default values if this command is not configured or if the **no** form of this command is entered:

- **total** *number*: 5000
- **learn** *number*: 2500

Command Modes

PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **max prefix** command is entered on a PfR master controller. This command is used to limit the number of prefix that a master controller will monitor and learn to reduce memory and system resource consumption.

Note If you configure a lower value for the **total** keyword than for the **learn** keyword, the value for the **total** keyword will also set the maximum number of prefixes that a master controller will learn.

Examples

The following example configures PfR to monitor a maximum of 3000 prefixes and to learn a maximum of 1500 prefixes:

```
Router(config)# pfr master
Router(config-pfr-mc)# max prefix total 3000 learn 1500
```

Related Commands

Command	Description
expire after (PfR)	Configures the length of time that learned prefixes are kept in the central policy database.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

max range receive (PfR)

To set the maximum utilization range for all Performance Routing (PfR) managed entrance links, use the **max range receive** command in PfR master controller configuration mode. To return the maximum utilization range for entrance links to the default value, use the **no** form of this command.

max range receive percent *maximum*

no max range receive

Syntax Description

percent	Specifies the maximum utilization range for all PfR entrance links as a percentage.
maximum	Maximum utilization range as a percentage. The range for this argument is from 1 to 100. The default is 20 percent.

Command Default

PfR uses the following default value (20 percent) if this command is not configured or if the **no** form of this command is entered:

percent *maximum*: 20

Command Modes

PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **max range receive** command is configured on a master controller. This command is used to set a threshold link utilization range for all entrance interfaces on PfR border routers.

PfR entrance link range functionality attempts to keep the entrance links within a utilization range relative to each other to ensure that the traffic load is distributed. The range is specified either as an absolute value in kilobits per second (kb/s) or as a percentage and is configured on the master controller to apply to all the entrance links on border routers managed by the master controller. For example, in a PfR-managed network with two entrance links, if the range is specified as 25 percent and the utilization of the first entrance link is 70 percent, then if the utilization of the second entrance link falls to 40 percent, the percentage range between the two entrance links will be more than 25 percent and PfR will attempt to move some traffic classes to use the second entrance to even the traffic load.

Examples

The following example shows how to enforce an entrance link selection for learned inside prefixes using the BGP autonomous system number community prepend technique. The **max range receive** command is configured under PfR master controller configuration mode to set a maximum receive range for all PfR-managed entrance links. In this example, the receive range between all the entrance links on the border routers must be within 35 percent.

```
Router> enable
Router# configure terminal
```

```
Router(config)# pfr master
Router(config-pfr-mc)# max range receive percent 35
Router(config-pfr-mc)# border 10.1.1.2 key-chain pfr
Router(config-pfr-mc-br)# interface ethernet1/0 external
Router(config-pfr-mc-br-if)# maximum utilization receive absolute 25000
Router(config-pfr-mc-br-if)# downgrade bgp community 3:1
Router(config-pfr-mc-br-if)# exit
Router(config-pfr-mc-br)# exit
Router(config-pfr-mc)# exit
Router(config)# pfr-map INSIDE_LEARN 10
Router(config-pfr-map)# match pfr learn inside
Router(config-pfr-map)# set delay threshold 400
Router(config-pfr-map)# set resolve delay priority 1
Router(config-pfr-map)# set mode route control
Router(config-pfr-map)# end
```

Related Commands

Command	Description
border (PfR)	Enters PfR-managed border router configuration mode to establish communication with a PfR border router.
downgrade bgp (PfR)	Specifies route downgrade options for a PfR-managed interface using BGP advertisements.
maximum utilization receive (PfR)	Sets the maximum utilization on a single PfR-managed entrance link.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.

maximum utilization receive (PfR)

To set the maximum utilization on a single Performance Routing (PfR) managed entrance link, use the **maximum utilization receive** command in PfR border exit interface configuration mode. To return the maximum utilization on an entrance link to the default value, use the **no** form of this command.

maximum utilization receive {**absolute** *kbps* | **percentage** *bandwidth*}

no maximum utilization receive

Syntax Description

absolute	Sets the maximum utilization on a PfR-managed entrance link to an absolute value.
kbps	Maximum utilization for a PfR-managed entrance link, in kilobits per second (kb/s). The configurable range for this argument is a number from 1 to 1000000000.
percent	Sets the maximum utilization on a PfR-managed entrance link to a bandwidth percentage.
bandwidth	Entrance link bandwidth percentage. The range for this argument is from 1 to 100. The default is 75.

Command Default

PfR uses a default maximum of 75 percent bandwidth utilization for a PfR-managed entrance link if this command is not configured or if the **no** form of this command is entered.

Command Modes

PfR border exit interface configuration (config-pfr-mc-br-if)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **maximum utilization receive** command is entered on a master controller to set the maximum utilization threshold of incoming traffic that can be transmitted over a PfR-managed entrance link interface. This command is configured on a per-entrance-link basis. Use this command with the **downgrade bgp** (PfR) command to configure PfR BGP inbound optimization. This command can also be used with the **max range receive** (PfR) command to configure entrance link load balancing.

If traffic utilization goes above the threshold, PfR tries to move the traffic from this entrance link to another underutilized entrance link.

Examples

The following example shows how to enforce an entrance link selection for learned inside prefixes using the BGP autonomous system number community prepend technique. The **maximum utilization receive** command is configured under PfR border exit interface configuration mode to set a maximum threshold value of 25000 kb/s for packets received through the entrance link Ethernet interface 1/0 on the border router.

```
Router> enable
Router# configure terminal
Router(config)# pfr master
Router(config-pfr-mc)# max range receive percent 35
Router(config-pfr-mc)# border 10.1.1.2 key-chain CISCO
Router(config-pfr-mc-br)# interface ethernet1/0 external
Router(config-pfr-mc-br-if)# maximum utilization receive absolute 25000
Router(config-pfr-mc-br-if)# downgrade bgp community 3:1
Router(config-pfr-mc-br-if)# exit
Router(config-pfr-mc-br)# exit
Router(config-pfr-mc)# exit
Router(config)# pfr-map INSIDE_LEARN 10
Router(config-pfr-map)# match pfr learn inside
Router(config-pfr-map)# set delay threshold 400
Router(config-pfr-map)# set resolve delay priority 1
Router(config-pfr-map)# set mode route control
Router(config-pfr-map)# end
```

Related Commands

Command	Description
border (PfR)	Enters PfR-managed border router configuration mode to establish communication with a PfR border router.
downgrade bgp (PfR)	Specifies route downgrade options for a PfR-managed interface using BGP advertisements.
max range receive (PfR)	Sets the maximum utilization range for all PfR-managed entrance links.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.

max-range-utilization (PfR)

To set the maximum utilization range for all Performance Routing (PfR) managed exit links, use the **max-range-utilization** command in PfR master controller configuration mode. To return the maximum utilization range to the default value, use the **no** form of this command.

max-range-utilization percent *maximum*

no max-range-utilization

Syntax Description

percent	Specifies the maximum utilization range for all PfR exit links as a percentage.
maximum	Maximum utilization range percentage. The range for this argument is from 1 to 100. The default is 20.

Command Default

PfR uses the default value of a 20 percent maximum utilization range for all PfR-managed exit links if this command is not configured or if the **no** form of this command is entered.

Command Modes

PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **max-range-utilization** command is configured on a master controller. This command is used to set a threshold link utilization range for all external interfaces on PfR border routers.

PfR exit link range functionality attempts to keep the exit links within a utilization range, relative to each other, to ensure that the traffic load is distributed. The range is specified as a percentage and is configured on the master controller to apply to all the exit links on border routers managed by the master controller. For example, in a PfR-managed network with two exit links, if the range is specified as 25 percent and the utilization of the first exit link is 70 percent, then if the utilization of the second exit link falls to 40 percent, the percentage range between the two exit links will be more than 25 percent and PfR will attempt to move some traffic classes to use the second exit to even the traffic load.

Examples

The following example sets the maximum utilization range for PfR-managed exit links to 25 percent:

```
Router(config)# pfr master
Router(config-pfr-mc)# max-range-utilization 25
```

Related Commands

Command	Description
max-xmit-utilization (PfR)	Configures maximum utilization on a single PfR managed exit link.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

max-xmit-utilization (PfR)

To set the maximum utilization on a single Performance Routing (PfR) managed exit link, use the **max-xmit-utilization** command in PfR border exit interface configuration mode. To return the maximum utilization on an exit link to the default value, use the **no** form of this command.

max-xmit-utilization {**absolute** *kbps* | **percentage** *bandwidth*}

no max-xmit-utilization

Syntax Description

absolute	Sets the maximum utilization on a PfR-managed exit link to an absolute value.
kbps	Maximum utilization for a PfR-managed exit link, in kilobits per second (kb/s). The configurable range for this argument is a number from 1 to 1000000000.
percentage	Sets the maximum utilization on a PfR-managed exit link to a bandwidth percentage.
bandwidth	Exit link bandwidth percentage. The range for this argument is from 1 to 100. The default is 75.

Command Default

PfR uses the default value of 75 percent maximum utilization on a single PfR-managed exit link if this command is not configured or if the **no** form of this command is entered.

Command Modes

PfR border exit interface configuration (config-pfr-mc-br-if)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **max-xmit-utilization** command is entered on a master controller and allows you to set the maximum utilization of outbound traffic that can be transmitted over a PfR-managed exit interface. The maximum utilization threshold can be expressed as an absolute value in kb/s or as a percentage. This command is configured on a per-exit-link basis and cannot be configured on PfR internal interfaces; internal interfaces are not used to forward traffic.

If traffic goes above the threshold, PfR tries to move the traffic from this exit link to another underutilized exit link.

Examples

The following example sets the maximum exit link utilization to 1000000 kb/s on Fast Ethernet interface 0/0:

```
Router(config-pfr-mc-br)# interface FastEthernet0/0 external
Router(config-pfr-mc-br-if)# max-xmit-utilization absolute 1000000
```

The following example sets the maximum percentage of exit utilization to 80 percent on serial interface 1/0:

```
Router(config-pfr-mc-br)# interface Serial 1/0 external
Router(config-pfr-mc-br-if)# max-xmit-utilization percentage 80
```

Related Commands

Command	Description
interface (PfR)	Configures a border router interface as a PfR-managed external or internal interface.
max-range-utilization (PfR)	Sets the maximum utilization range for all PfR-managed exit links.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

mode (PfR)

To configure route monitoring, route control, or route exit selection on a Performance Routing (PfR) master controller, use the **mode** command in PfR master controller configuration mode. To return the PfR master controller to the default monitoring, control, or exit selection state, use the **no** form of this command.

mode {**monitor** {**active** [**throughput**] | **both** | **fast** | **passive**} | **route** {**control** | **metric** {**bgp local-pref** *preference* | **eigrp tag** *community* | **static tag** *value*} | **observe**} | **select-exit** {**best** | **good**}}

no mode {**monitor** | **route** {**control** | **metric** {**bgp** | **eigrp** | **static**} | **observe**} | **select-exit**}

Syntax Description

monitor	Enables the configuration of PfR monitoring settings.
active	Enables active monitoring.
throughput	(Optional) Enables active monitoring with throughput data from passive monitoring.
both	Enables both active and passive monitoring. This is the default monitoring mode.
fast	Enables continuous active monitoring and passive monitoring.
passive	Enables passive monitoring.
route	Enables the configuration of PfR route control policy settings.
control	Enables automatic route control.
metric	Enables the configuration of route control based on the Border Gateway Protocol (BGP) local-preference, EIGRP, or for specific static routes.
bgp local-pref	Sets the BGP local preference for PfR-controlled routes.
preference	A number from 1 to 65535.
eigrp tag	Applies a community value to an EIGRP route under PfR control.
community	A number from 1 to 65535.
static tag	Applies a tag to a static route under PfR control.
value	A number from 1 to 65535.
observe	Configures PfR to passively monitor and report without making any changes. This is the default route control mode.
select-exit	Enables the exit selection based on performance or policy.
best	Configures PfR to select the best available exit based on performance or policy.
good	Configures PfR to select the first exit that is in-policy. This is the default exit selection.

Command Default

PfR uses the following default settings if this command is not configured or if the **no** form of this command is entered:

Monitoring: Both active and passive monitoring is enabled.
Route control: Observe mode route control is enabled.
Exit selection: The first in-policy exit is selected.

Command Modes PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines The **mode** command is entered on a master controller. This command is used to enable and configure control mode and observe mode settings and is used to configure passive monitoring and active monitoring. A prefix can be monitored both passively and actively.

Observe Mode

Observe mode monitoring is enabled by default. In observe mode, the master controller monitors prefixes and exit links based on default and user-defined policies and then reports the status of the network and the decisions that should be made but does not implement any changes. This mode allows you to verify the effectiveness of this feature before it is actively deployed.

Control Mode

In control mode, the master controller coordinates information from the border routers and makes policy decisions just as it does in observe mode. The master controller monitors prefixes and exits based on default and user-defined policies but then implements changes to optimize prefixes and to select the best exit. In this mode, the master controller gathers performance statistics from the border routers and then transmits commands to the border routers to alter routing as necessary in the PfR-managed network.

Passive Monitoring

The master controller passively monitors IP prefixes and TCP traffic flows. Passive monitoring is configured on the master controller. Monitoring statistics are gathered on the border routers and then reported back to the master controller. PfR uses NetFlow to collect and aggregate passive monitoring statistics on a per prefix basis. No explicit NetFlow configuration is required. NetFlow support is enabled by default when passive monitoring is enabled. PfR uses passive monitoring to measure the following information:

- *Delay*—PfR measures the average delay of TCP flows for a prefix. Delay is the measurement of the time between the transmission of a TCP synchronization message and the receipt of the TCP acknowledgment.
- *Packet Loss*—PfR measures packet loss by tracking TCP sequence numbers for each TCP flow. PfR estimates packet loss by tracking the highest TCP sequence number. If a subsequent packet is received with a lower sequence number, PfR increments the packet loss counter.
- *Reachability*—PfR measures reachability by tracking TCP synchronization messages that have been sent repeatedly without receiving a TCP acknowledgment.
- *Throughput*—PfR measures outbound throughput for optimized prefixes. Throughput is measured in bits per second (bps).

Note PfR passively monitors TCP traffic flows for IP traffic. Passive monitoring of non-TCP sessions is not supported.

Active Monitoring

PfR uses Cisco IOS IP Service Level Agreements (SLAs) to enable active monitoring. IP SLA support is enabled by default. IP SLA support allows PfR to be configured to send active probes to target IP addresses to measure the jitter and delay, determining if a prefix is out-of-policy and if the best exit is selected. The border router collects these performance statistics from the active probe and transmits this information to the master controller. The master controller uses this information to optimize the prefix and select the best available exit based on default and user-defined policies. The **active-probe** (PfR) command is used to create an active probe.

The **throughput** keyword enables the throughput data from passive mode monitoring to be considered when optimizing UDP traffic for both performance and load balancing. UDP traffic can be optimized only for performance (for example, delay, jitter, and loss) when active monitoring data is available. To enable load balancing of UDP traffic, throughput data from passive monitoring is required.

Fast Failover Monitoring

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

Optimal Exit Link Selection

The master controller can be configured to select a new exit for an out-of-policy prefix based on performance or policy. You can configure the master controller to select the first in-policy exit by entering the **good** keyword, or you can configure the master controller to select the best exit with the **best** keyword. If the **good** keyword is used and there is no in-policy exit, the prefix is uncontrolled.

Examples

The following example enables both active and passive monitoring:

```
Router(config)# pfr master
Router(config-pfr-mc)# mode monitor both
```

The following example enables fast failover monitoring:

```
Router(config)# pfr master
Router(config-pfr-mc)# mode monitor fast
```

The following example configures the master controller to enable active monitoring with throughput data from passive monitoring:

```
Router(config)# pfr master
Router(config-pfr-mc)# mode monitor active throughput
```

The following example enables control mode:

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

The following example configures the master controller to enable control mode and to enable EIGRP route control that applies a community value of 700 to EIGRP routes under PfR control:

```
Router(config)# pfr master
Router(config-pfr-mc)# mode route control
Router(config-pfr-mc)# mode route metric eigrp tag 700
```

The following example configures the master controller to select the first in-policy exit:

```
Router(config)# pfr master
Router(config-pfr-mc)# mode select-exit good
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
set mode (PfR)	Configures a PfR map to configure route monitoring, route control, or exit selection for matched traffic.

monitor-period (PfR)

To set the time period in which a Performance Routing (PfR) master controller learns traffic flows, use the **monitor-period** command in PfR Top Talker and Top Delay learning configuration mode. To return the monitoring period to the default time period, use the **no** form of this command.

monitor-period *minutes*

no monitor-period

Syntax Description

minutes	Sets the prefix learning period, in minutes. The range is from 1 to 1440. The default value is 5.

Command Default

If this command is not configured or if the **no** form of this command is entered, the default prefix learning period is 5 minutes.

Command Modes

PfR Top Talker and Top Delay learning configuration (config-pfr-mc-learn)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **monitor-period** command is configured on a master controller. This command is used to adjust the length of time during which a master controller learns traffic flows on border routers. The length of time between monitoring periods is configured with the **periodic-interval** (PfR) command. The number of prefixes that are learned is configured with the **prefixes** (PfR) command.

Examples

The following example sets the PfR monitoring period to 10 minutes on a master controller:

```
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# monitor-period 10
```

Related Commands

Command	Description
learn (PfR)	Enters PfR Top Talker and Top Delay learning configuration mode to configure prefixes for PfR to learn.
periodic-interval (PfR)	Sets the time interval between prefix learning periods.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
prefixes (PfR)	Sets the number of prefixes that PfR will learn during a monitoring period.

mos (PfR)

To specify the threshold and percentage Mean Opinion Score (MOS) values that Performance Routing (PfR) will permit for an exit link, use the **mos** command in PfR master controller configuration mode. To reset the threshold and percentage MOS values to their default value, use the **no** form of this command.

mos threshold *minimum* **percent** *percent*

no mos threshold *minimum* **percent** *percent*

Syntax Description

threshold	Specifies a threshold MOS value that represents a minimum voice quality for exit link utilization.
minimum	Number (to two decimal places) in the range from 1.00 to 5.00, where 1.00 represents the lowest voice quality and 5.00 represents the highest voice quality. The default MOS value is 3.60.
percent	Specifies a percentage value that is compared with the percentage of MOS samples that are below the MOS threshold.
percent	Number, as a percentage.

Command Default

The default MOS value is 3.60.

Command Modes

Master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **mos** command is used to determine voice quality. The number of MOS samples over a period of time that are below the threshold MOS value are calculated. If the percentage of MOS samples below the threshold is greater than the configured percentage, PfR determines that the exit link is out-of-policy and searches for an alternate exit link.

Another measure of voice quality is the jitter value. Use the **mos** (PfR) command and the **jitter** (PfR) command in a PfR policy to define voice quality.

Examples

The following example shows how to configure the master controller to search for a new exit link if more than 30 percent of the MOS samples are below the MOS threshold of 3.75:

```
Router(config)# pfr master
Router(config-pfr-mc)# mos threshold 3.75 percent 30
```

Related Commands

Command	Description
jitter	Specifies the threshold jitter value that PfR will permit for an exit link.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
set mos (PfR)	Configures a PfR map to set the threshold MOS value that PfR will permit for an exit link.

periodic (PfR)

To configure Performance Routing (PfR) to periodically select the best exit link, use the **periodic** command in PfR master controller configuration mode. To disable periodic exit selection, use the **no** form of this command.

periodic *timer*

no periodic

Syntax Description

timer	Sets the length of time, in seconds, for the periodic timer. The range of configurable values is from 90 to 7200.

Command Default

Periodic exit selection is disabled.

Command Modes

PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **periodic** command is entered on a master controller. This command is used to configure the master controller to evaluate and then make policy decisions for PfR managed exit links. When the periodic timer expires, the master controller evaluates current exit links based on default or user-defined policies. If all exit links are in-policy, no changes are made. If an exit link is out-of-policy, the affected prefixes are moved to an in-policy exit link. If all exit links are out-of-policy, the master controller will move out-of-policy prefixes to the best available exit links.

The master controller can be configured to select the first in-policy exit when the periodic timer expires, by configuring the **mode** (PfR) command with the **select-exit good** keywords. The master controller can also be configured to select the best available in-policy exit, by configuring the **mode** (PfR) command with the **select-exit best** keywords.

The periodic timer is reset to the default or configured value each time the timer expires. Configuring a new timer value will immediately replace the existing value if the new value is less than the time remaining. If the new value is greater than the time remaining, the new timer value will be used when the existing timer value expires.

Examples

The following example sets the periodic timer to 300 seconds. When the periodic timer expires, PfR will select either the best exit or the first in-policy exit.

```
Router(config)# pfr master
Router(config-pfr-mc)# periodic 300
```

Related Commands

Command	Description
mode (PfR)	Configures route monitoring or route control on a PfR master controller.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
set periodic (PfR)	Configures a PfR map to set the time period for the periodic timer.

periodic-interval (PfR)

To set the time interval between prefix learning periods, use the **periodic-interval** command in PfR Top Talker and Top Delay learning configuration mode. To set the time interval between prefix learning periods to the default value, use the **no** form of this command.

periodic-interval *minutes*

no periodic-interval

Syntax Description

minutes	Sets the time interval between prefix learning periods, in minutes. The range that can be configured for this argument is from 0 to 10080.

Command Default

Performance Routing (PfR) uses the default value of 120 minutes if this command is not configured or if the **no** form of this command is entered.

Command Modes

PfR Top Talker and Top Delay learning configuration (config-pfr-mc-learn)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **periodic-interval** command is configured on a master controller. This command is used to adjust the length of time between traffic flow monitoring periods. The length of time of the learning period is configured with the **monitor-period** (PfR) command. The number of prefixes that are monitored is configured with the **prefixes** (PfR) command.

Examples

The following example sets the length of time between PfR monitoring periods to 20 minutes on a master controller:

```
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# periodic-interval 20
```

Related Commands

Command	Description
learn (PfR)	Enters PfR Top Talker and Top Delay learning configuration mode to configure prefixes for PfR to learn.
monitor-period (PfR)	Sets the time period in which a PfR master controller learns traffic flows.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
prefixes (PfR)	Sets the number of prefixes that PfR will learn during a monitoring period.

pfr

To enable a Cisco IOS Performance Routing (PfR) process and configure a router as a PfR border router or as a PfR master controller, use the **pfr** command in global configuration mode. To disable a border router or master controller process and delete the PfR configuration from the running configuration file, use the **no** form of this command.

pfr {**border** | **master**}

no pfr {**border** | **master**}

Cisco IOS XE Release 3.1S

pfr border

no pfr border

Syntax Description

border	Designates a router as a border router and enters PfR border router configuration mode.
master	Designates a router as a master controller and enters PfR master controller configuration mode.

Command Default

PfR is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE, Release 3.1S.

Usage Guidelines

The **pfr** command is entered on a router to create a border router or master controller process to enable Cisco IOS PfR, which allows you to enable automatic outbound route control and load distribution for multihomed and enterprise networks. Configuring PfR allows you to monitor IP traffic flows and then define policies and rules based on link performance and link load distribution to alter routing and improve network performance.

Performance Routing comprises two components: the master controller (MC) and the border router (BR). A PfR deployment requires one MC and one or more BRs. Communication between the MC and the BR is protected by key-chain authentication. Depending on your Performance Routing deployment scenario and scaling requirements, the MC may be deployed on a dedicated router or may be deployed along with the BR on the same physical router.

Master Controller—The MC is a single router that acts as the central processor and database for the Performance Routing system. The MC component does not reside in the forwarding plane and, when deployed in a standalone fashion, has no view of routing information contained within the BR. The

master controller maintains communication and authenticates the sessions with the BRs. The role of the MC is to gather information from the BR or BRs to determine whether traffic classes are in or out of policy and to instruct the BRs how to ensure that traffic classes remain in policy using route injection or dynamic PBR injection.

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

Disabling a Border Router or a Master Controller

To disable a master controller or border router and completely remove the process configuration from the running configuration file, use the **no** form of this command in global configuration mode.

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

Cisco IOS XE Release 3.1S

In Cisco IOS XE Release 3.1S, only the **border** keyword is supported.

Examples

Minimum Required PfR Master Controller Configuration

The following example designates a router as a master controller and enters PfR master controller configuration mode:

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

The following is an example of the minimum required configuration on a master controller to create a PfR-managed network:

A key-chain configuration named PFR_KEY is defined in global configuration mode.

```
Router(config)# key chain PFR_KEY
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string CISCO
Router(config-keychain-key)# exit
Router(config-keychain)# exit
```

The master controller is configured to communicate with the 10.4.9.6 border router in PfR master controller configuration mode. The key chain PFR_KEY is applied to protect communication. Internal and external PfR-controlled border router interfaces are defined.

```
Router(config)# pfr master
Router(config-pfr-mc)# border 10.4.9.6 key-chain PFR_KEY
Router(config-pfr-mc-br)# interface FastEthernet0/0 external
Router(config-pfr-mc-br)# interface FastEthernet0/1 internal
Router(config-pfr-mc-br)# exit
```

Required PfR Border Router Configuration

The following example designates a router as a border router and enters PfR border router configuration mode:

```
Router(config)# pfr border
Router(config-pfr-br)#
```

The following is an example of the minimum required configuration to configure a border router in a PfR-managed network:

The key-chain configuration is defined in global configuration mode.

```
Router(config)# key chain PFR_KEY
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string CISCO
Router(config-keychain-key)# exit
Router(config-keychain)# exit
```

The key chain PFR_KEY is applied to protect communication. An interface is identified as the local source interface to the master controller.

```
Router(config)# pfr border
Router(config-pfr-br)# local FastEthernet0/0
Router(config-pfr-br)# master 10.4.9.4 key-chain PFR_KEY
Router(config-pfr-br)# end
```

Related Commands

Command	Description
border (PfR)	Enters PfR managed border router configuration mode to configure a border router.
master (PfR)	Establishes communication with a master controller.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.
shutdown (PfR)	Stops or starts a PfR master controller or a PfR border router process.

pfr-map

To enter PfR map configuration mode to configure a Performance Routing (PfR) map to apply policies to selected IP prefixes, use the **pfr-map** command in global configuration mode. To delete the PfR map, use the **no** form of this command.

pfr-map *map-name* [*sequence-number*]

no pfr-map *map-name*

Syntax Description

map-name	Name or tag for the PfR map.
sequence-number	(Optional) Sequence number for the PfR map entry. The configurable range for this argument is from 1 to 65535.

Command Default

No PfR maps are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **pfr-map** command is configured on a master controller. The operation of a PfR map is similar to the operation of a route map. A PfR map is designed to select IP prefixes or to select PfR learn policies using a match clause and then to apply PfR policy configurations using a set clause. The PfR map is configured with a sequence number like a route map, and the PfR map with the lowest sequence number is evaluated first. The operation of a PfR map differs from a route map at this point. There are two important distinctions:

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

Tips

Deny prefixes should be combined in a single prefix list and applied to the PfR map with the lowest sequence number.

A PfR map can match a prefix or prefix range with the **match ip address** (PfR) command. A prefix can be any IP network number combined with a prefix mask that specifies the prefix length. The prefix or prefix range is defined with the **ip prefix-list** command in global configuration mode. Any prefix length can be specified. A PfR map can also match PfR learned prefixes with the **match pfr learn** command. Matching can be configured for prefixes learned based on delay or based on throughput.

The PfR map applies the configuration of the set clause after a successful match occurs. A PfR set clause can be used to set policy parameters for the backoff timer, packet delay, holddown timer, packet loss, mode settings, periodic timer, resolve settings, and unreachable hosts. See the "Related Commands" section of this command reference page for a complete list of PfR set clauses.

Policies that are applied by a PfR map do not override global policies configured under PfR master controller configuration mode and PfR Top Talker and Delay learning configuration mode. Policies are overridden on a per-prefix-list basis. If a policy type is not explicitly configured in a PfR map, the default or configured values will apply. Policies applied by a PfR map take effect after the current policy or operational timer expires. The PfR map configuration can be viewed in the output of the **show running-config** command. PfR policy configuration can be viewed in the output of the **show pfr master policy** command.

Examples

The following example creates a PfR map named SELECT_EXIT that matches traffic defined in the IP prefix list named CUSTOMER and sets exit selection to the first in-policy exit when the periodic timer expires. This PfR map also sets a resolve policy that sets the priority of link utilization policies to 1 (highest priority) and allows for a 10 percent variance in exit link utilization statistics.

```
Router(config)# ip prefix-list CUSTOMER permit 10.4.9.0/24
Router(config)# pfr-map SELECT_EXIT 10
Router(config-pfr-map)# match ip address prefix-list CUSTOMER
Router(config-pfr-map)# set mode select-exit good
Router(config-pfr-map)# set resolve utilization priority 1 variance 10
```

The following example creates a PfR map named THROUGHPUT that matches traffic learned based on the highest outbound throughput. The set clause applies a relative loss policy that will permit 10 percent packet loss:

```
Router(config)# pfr-map THROUGHPUT 20
Router(config-pfr-map)# match pfr learn throughput
Router(config-pfr-map)# set loss relative 10
```

Related Commands

Command	Description
ip prefix-list	Creates an entry in a prefix list.
match ip address (PfR)	Creates a prefix list match clause entry in a PfR map to apply PfR policy settings.
match pfr learn	Creates a match clause entry in a PfR map to match PfR learned prefixes.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
set loss (PfR)	Configures a PfR map to set the relative or maximum packet loss limit that PfR will permit for an exit link.
set resolve (PfR)	Configures a PfR map to set policy priority for overlapping policies.
show pfr master policy	Displays configured and default policy settings on a PfR master controller.

policy-rules (PfR)

To apply a configuration from a Performance Routing (PfR) map to a master controller configuration, use the **policy-rules** command in PfR master controller configuration mode. To remove a configuration applied by the **policy-rules** command, use the **no** form of this command.

policy-rules *map-name*

no policy-rules

Syntax Description

map-name	Name of the PfR map.

Command Default

No configuration from a PfR map is applied to a master controller.

Command Modes

PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **policy-rules** command allows you 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 **policy-rules** command is entered on a master controller. This command is used to apply the 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.

Examples

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

```
Router(config)# pfr-map BLUE 10
Router(config-pfr-map)# match pfr learn delay
Router(config-pfr-map)# set loss relative 900
Router(config-pfr-map)# exit
Router(config)# pfr master
Router(config-pfr-mc)# policy-rules BLUE
Router(config-pfr-mc)# end
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.

port (PfR)

To optionally configure a dynamic port number for communication between a Performance Routing (PfR) master controller and border router, use the **port** command in PfR master controller or PfR border router configuration mode. To close the port and disable communication, use the **no** form of this command.

port [*port-number*]

no port

Syntax Description

port-number	(Optional) Specifies the port number. The configurable range for this argument is a number from 1 to 65535.

Command Default

Port 3949 is used for PfR communication unless a dynamic port number is configured on both the master controller and the border router. Port configuration is not shown in the running configuration file when port 3949 is used.

Command Modes

PfR border router configuration (config-pfr-br)
PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

Communication between a master controller and a border router is automatically carried over port 3949 when connectivity is established. Port 3949 is registered with IANA for PfR communication. Manual port number configuration is required only if you are running Cisco IOS Release 12.3(8)T or if you need to configure PfR communication to use a dynamic port number.

The **port** command is entered on a master controller or a border router. This command is used to specify a dynamic port number to be used for border router and master controller communication. The same port number must be configured on both the master controller and border router. Closing the port by entering the **no** form of this command disables communication between the master controller and the border router.

Cisco IOS XE Release 3.1S

This command is supported only in PfR border router configuration mode.

Examples

The following example opens port 49152 for master controller communication with a border router:

```
Router(config)# pfr master
Router(config-pfr-mc)# port 49152
```

The following example opens port 49152 for border router communication with a master controller:

```
Router(config)# pfr border
Router(config-pfr-br)# port 49152
```

The following example closes the default or user-defined port and disables communication between a master controller and border router:

```
Router(config)# pfr master
Router(config-pfr-mc)# no port
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

prefixes (PfR)

To set the number of prefixes that Performance Routing (PfR) will learn during a monitoring period, use the **prefixes** command in PfR Top Talker and Top Delay learning configuration mode. To return the number of prefixes to the default value, use the **no** form of this command.

prefixes *number*

no prefixes

Syntax Description

number	Number of prefixes that a master controller will learn during a monitoring period. The range is from 1 to 2500.

Command Default

PfR uses 100 prefixes by default if this command is not configured or if the **no** form of this command is entered.

Command Modes

PfR Top Talker and Top Delay learning configuration (config-pfr-mc-learn)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **prefixes** command is configured on a master controller. This command is used to set the number of prefixes that a master controller will learn during a monitoring period. The length of time of the learning period is configured with the **monitor-period** (PfR) command. The length of time between monitoring periods is configured with the **periodic-interval** (PfR) command.

Examples

The following example configures a master controller to learn 200 prefixes during a monitoring period:

```
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# prefixes 200
```

Related Commands

Command	Description
learn (PfR)	Enters PfR Top Talker and Top Delay learning configuration mode to configure prefixes for PfR to learn.
monitor-period (PfR)	Sets the time period in which a PfR master controller learns traffic flows.
periodic-interval (PfR)	Sets the time interval between prefix learning periods.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.

resolve (PfR)

To set the priority of a policy when multiple overlapping policies are configured, use the **resolve** command in PfR master controller configuration mode. To disable the policy priority configuration, use the **no** form of this command.

resolve {**cost priority** *value* | **delay priority** *value* **variance** *percentage* | **jitter priority** *value* **variance** *percentage* | **loss priority** *value* **variance** *percentage* | **mos priority** *value* **variance** *percentage* | **range priority** *value* | **utilization priority** *value* **variance** *percentage*}

no resolve {**cost** | **delay** | **jitter** | **loss** | **mos** | **range** | **utilization**}

Syntax Description

cost	Specifies policy priority settings for cost optimization.
priority	Sets the priority of the policy.
value	A number in the range of 1 to 10. The number 1 has the highest priority, and the number 10 has the lowest priority.
delay	Specifies policy priority settings for packet delay.
variance	Sets the allowable variance for the policy, as a percentage.
percentage	A number in the range from 1 to 100.
jitter	Specifies policy priority settings for jitter.
loss	Specifies policy priority settings for packet loss.
mos	Specifies policy priority settings for the Mean Opinion Score (MOS).
range	Specifies policy priority settings for the range.
utilization	Specifies policy priority settings for exit link utilization.

Command Default

Performance Routing (PfR) uses the following default settings if this command is not configured or if the **no** form of this command is entered:

- An unreachable prefix: highest priority
- **delay priority**: 11
- **utilization priority**: 12

Command Modes

PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **resolve** command is entered on a master controller. 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. The number 1 assigns the highest priority to a policy. The number 10 sets the lowest priority. Each policy must be assigned a different priority number. If you try to assign the same priority number to two different policy types, an error message will be displayed on the console. By default, delay has a priority value of 11 and utilization has a priority value of 12. These values can be overridden by specifying a value from 1 to 10.

Note An unreachable prefix will always have the highest priority regardless of any other settings. This is a designed behavior and cannot be overridden because an unreachable prefix indicates an interruption in a traffic flow.

The **variance** keyword is used to set an allowable variance for a user-defined policy. This keyword configures the allowable percentage by which an exit link or prefix can vary from the user-defined policy value and still be considered equivalent. For example, if an exit link delay is set to 80 absolute and a 10 percent variance is configured, exit links that have delay values from 80 to 89 percent will be considered equal.

Note Variance cannot be configured for cost or range policies.

Note You must configure a PfR active jitter probe for a target prefix using the **active-probe** (PfR) command in order for the **resolve jitter**, **resolve loss**, and **resolve mos** commands to function.

Examples

The following example shows how to set the delay policy priority to 1 and the allowable variance percentage to 20 percent:

```
Router(config)# pfr master
Router(config-pfr-mc)# resolve delay priority 1 variance 20
```

The following example shows how to set the loss policy priority to 2 and the allowable variance percentage to 30 percent:

```
Router(config)# pfr master
Router(config-pfr-mc)# resolve loss priority 2 variance 30
```

The following example shows how to set the jitter policy priority to 3 and the allowable variance percentage to 5 percent:

```
Router(config)# pfr master
Router(config-pfr-mc)# resolve jitter priority 3 variance 5
```

The following example shows how to set the MOS policy priority to 4 and the allowable variance percentage to 25 percent:

```
Router(config)# pfr master
Router(config-pfr-mc)# resolve mos priority 4 variance 25
```

The following example shows how to set the range policy priority to 5:

```
Router(config)# pfr master
Router(config-pfr-mc)# resolve range priority 5
```

The following example shows how to set the link utilization policy priority to 6 and the allowable variance percentage to 10 percent:

```
Router(config)# pfr master
Router(config-pfr-mc)# resolve utilization priority 6 variance 10
```

Related Commands

Command	Description
active-probe (PfR)	Configures a PfR active probe for a target prefix.
cost-minimization (PfR)	Configures cost-based optimization policies on a master controller.
delay (PfR)	Configures PfR to learn prefixes based on the lowest delay.
jitter (PfR)	Sets the jitter threshold value that PfR will permit for an exit link.
loss (PfR)	Sets the relative or maximum packet loss limit that PfR will permit for an exit link.
max-range-utilization (PfR)	Sets the maximum utilization range for all PfR-managed exit links.
max-xmit-utilization (PfR)	Configures maximum utilization on a single PfR-managed exit link.
mos (PfR)	Sets the MOS threshold value that PfR will permit for an exit link.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
show pfr master policy	Displays user-defined and default policy settings on an PfR master controller.

set active-probe (PfR)

To configure a Performance Routing (PfR) active probe with a forced target assignment within a PfR map, use the **set active-probe** command in PfR map configuration mode. To disable the active probe, use the **no** form of this command.

set active-probe *probe-type ip-address* **target-port** *number* [**codec** *codec-name*] [**dscp** *value*]

no set active-probe *probe-type ip-address*

Syntax Description

probe-type	Type of probe. Must be one of the following: • **echo—**Uses Internet Control Message Protocol (ICMP) echo (ping) messages. • **jitter—**Uses jitter messages. • **tcp-conn—**Uses TCP connection messages. • **udp-echo—**Uses UDP echo messages.
ip-address	Target IP address of a prefix to be monitored using the specified type of probe.
target-port	(Not specified for echo probes.) Specifies the destination port number for the active probe.
number	Port number in the range from 1 to 65535.
codec	(Optional) Only used with the jitter probe type. Specifies the codec value used for Mean Opinion Score (MOS) calculation.
codec-name	(Optional) Codec value. Must be one of the following: • **g711alaw—**G.711 A Law 64000 bps • **g711ulaw—**G.711 U Law 64000 bps • **g729a—**G.729 8000 bps
dscp	(Optional) Sets the Differentiated Services Code Point (DSCP) value.
value	(Optional) DSCP value.

Command Default

No active probes are configured with a forced target assignment.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

If the optional **dscp** keyword and *value* argument are not specified, active probes are created using the DSCP value of the traffic class. For example, the software creates two sets of probes for the following three traffic classes. Traffic class 2 is assigned a probe with a DSCP value of ef, and the other two traffic classes share a probe with a DSCP value of 0.

- Traffic class 1: 10.1.1.0/24, destination port 23
- Traffic class 2: 10.1.2.0/24, dscp ef
- Traffic class 3: 10.1.2.0/24, destination port 991

If the optional **dscp** keyword and *value* argument are provided, probes are created using the specified DSCP value. For example, if the DSCP value specified for the **set active-probe** command is cs1, only one probe is created for the three traffic classes.

Examples

The following example shows how to configure an ICMP reply (ping) message probe with a forced target assignment within a PfR map. The 10.1.2.10 address is the forced target assignment. A remote responder does not have to be enabled on the target device.

```
Router(config)# pfr-map MAP1 10
Router(config-pfr-map)# match ip prefix-list LIST1
Router(config-pfr-map)# set active-probe echo 10.1.2.10
```

The following example shows how to configure a TCP connection message probe with a forced target assignment within an PfR map. The 10.1.2.10 address is the forced target assignment, the target port is defined as 29, and the DSCP value is set to ef. A remote responder must be enabled on the target device.

```
Router(config)# pfr-map MAP2 10
Router(config-pfr-map)# match ip prefix-list LISTMAP2
Router(config-pfr-map)# set active-probe tcp-conn 10.1.2.10 target-port 29 dscp ef
```

Related Commands

Command	Description
active-probe (PfR)	Configures a PfR active probe for a target prefix.
ip sla monitor responder	Enables the IP SLAs Responder for general IP SLAs operations.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.
show pfr border active-probes	Displays connection and status information about active probes on a PfR border router.
show pfr master active-probes	Displays connection and status information about active probes on a PfR master controller.

set backoff (PfR)

To configure a Performance Routing (PfR) map to set the backoff timer to adjust the time period for prefix policy decisions, use the **set backoff** command in PfR map configuration mode. To delete the set clause entry and reset the backoff timers to the default values, use the **no** form of this command.

set backoff *min-timer max-timer* [*step-timer*]

no set backoff

Syntax Description

min-timer	Sets the minimum value for the backoff timer, in seconds. The configurable time period for this argument is from 180 to 7200. The default timer value is 300.
max-timer	Sets the maximum value for the backoff timer, in seconds. The configurable time period for this argument is from 180 to 7200. The default timer value is 3000.
step-timer	(Optional) Sets the value of the time period for the step timer, in seconds. The step timer is used to add time to the out-of-policy waiting period each time the backoff timer expires and PfR is unable to find an in-policy exit. The configurable time period for this argument is from 180 to 7200. The default timer value is 300.

Command Default

PfR uses the following default values if this command is not configured or if the **no** form of this command is entered:

min-timer: 300
max-timer: 3000
step-timer: 300

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **set backoff** command is entered on a master controller in PfR map configuration mode. This command is used to configure a PfR map to set the transition period for which the master controller holds an out-of-policy prefix. The master controller uses a backoff timer to schedule the prefix transition period for which PfR holds the out-of-policy prefix before moving the prefix to an in-policy state by selecting an in-policy exit. This command is configured with a minimum and maximum timer value and can be configured with an optional step timer.

Minimum Timer—The *min-timer* argument is used to set the minimum transition period in seconds. If the current prefix is in-policy when this timer expires, no change is made and the minimum timer is reset to the default or configured value. If the current prefix is out-of-policy, PfR will move the prefix to an in-policy and reset the minimum timer to the default or configured value.

Maximum Timer—The *max-timer* argument is used to set the maximum length of time for which PfR holds an out-of-policy prefix when there are no PfR-controlled in-policy prefixes. If all PfR-controlled prefixes are in an out-of-policy state and the value from the *max-timer* argument expires, PfR will select the best available exit and reset the minimum timer to the default or configured value.

Step Timer—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. If the maximum timer expires and all PfR-managed exits are out-of-policy, PfR will install the best available exit and reset the minimum timer.

Configuring a new timer value will immediately replace the existing value if the new value is less than the time remaining. If the new value is greater than the time remaining, the new timer value will be used when the existing timer value expires.

Examples

The following example creates a PfR map named BACKOFF that sets the minimum timer to 400 seconds, the maximum timer to 4000 seconds, and the step timer to 400 seconds for traffic from the prefix list named CUSTOMER:

```
Router(config)# pfr-map BACKOFF 70
Router(config-pfr-map)# match ip address prefix-list CUSTOMER
Router(config-pfr-map)# set backoff 400 4000 400
```

Related Commands

Command	Description
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.
periodic (PfR)	Sets the backoff timer to adjust the time period for prefix policy decisions.

set delay (PfR)

To configure a Performance Routing (PfR) map to configure PfR to set the delay threshold, use the **set delay** command in PfR map configuration mode. To delete the set clause entry and reset the delay threshold values, use the **no** form of this command.

set delay {**relative** *percentage* | **threshold** *maximum*}

no set delay

Syntax Description

relative *percentage*	Sets a relative delay policy based on a comparison of short-term and long-term delay percentages. The range of values that can be configured for this argument is a number from 1 to 1000. Each increment represents one tenth of a percent. The default is 500 (50 percent).
threshold *maximum*	Sets the absolute maximum delay time, in milliseconds. The range of values that can be configured for this argument is from 1 to 10000. The default is 5000.

Command Default

PfR uses the default values if this command is not configured or if the **no** form of this command is entered.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **set delay** command is entered on a master controller in PfR map configuration mode. This command is configured in a PfR map to set the delay threshold 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 short-term measurement reflects the delay percentage within a 5-minute time period. The long-term measurement reflects the delay percentage within a 60-minute period. The following formula is used to calculate this value:

Relative delay measurement = ((short-term measurement – long-term measurement) / long-term measurement) * 100

The master controller measures the difference between these two values as a percentage. If the percentage exceeds the user-defined or default value, the delay percentage is determined to be out-of-policy. For example, if the long-term delay measurement is 100 milliseconds and the short-term delay measurement is 120 milliseconds, the relative delay percentage is 20 percent.

The **threshold** keyword is used to configure the absolute maximum delay period in milliseconds.

If the measured delay of the prefix is higher than the configured delay threshold, the prefix is out-of-policy. If the short-term delay of the prefix is more than the long-term delay by the percentage value configured, the prefix is out-of-policy.

Examples

The following example creates a PfR map named DELAY that sets the absolute maximum delay threshold to 2000 milliseconds for traffic from the prefix list named CUSTOMER:

```
Router(config)# pfr-map DELAY 80
Router(config-pfr-map)# match ip address prefix-list CUSTOMER
Router(config-pfr-map)# set delay threshold 2000
```

Related Commands

Command	Description
delay (PfR)	Configures prefix delay parameters.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.

set holddown (PfR)

To configure a Performance Routing (PfR) map to set the prefix route dampening timer for the minimum period of time in which a new exit must be used before an alternate exit can be selected, use the **set holddown** command in PfR map configuration mode. To delete the set clause entry and resets the holddown timer to the default value, use the **no** form of this command.

set holddown *timer*

no set holddown

Syntax Description

timer	Sets the prefix route dampening time period, in seconds. The range for this argument is from 90 to 65535. The default value is 300.

Command Default

PfR uses the default value of 300 seconds for the prefix route dampening time period if this command is not configured or if the **no** form of this command is entered.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **set holddown** command is entered on a master controller in PfR map configuration mode. This command is used to configure the prefix route dampening timer for the minimum period of time in which a new exit must be used before an alternate exit can be selected. The master controller puts a prefix in a holddown state during an exit change to isolate the prefix during the transition period, preventing the prefix from flapping because of rapid state changes. PfR does not implement policy changes while a prefix is in the holddown state. A prefix will remain in a holddown state for the default or configured time period. When the holddown timer expires, PfR will select the best exit based on performance and policy configuration. However, an immediate route change will be triggered if the current exit for a prefix becomes unreachable.

Configuring a new timer value will immediately replace the existing value if the new value is less than the time remaining. If the new value is greater than the time remaining, the new timer value will be used when the existing timer is reset.

Examples

The following example creates a PfR map named HOLDDOWN that sets the holddown timer to 120 seconds for traffic from the prefix list named CUSTOMER:

```
Router(config)# pfr-map HOLDDOWN 10
Router(config-pfr-map)# match ip address prefix-list CUSTOMER
Router(config-pfr-map)# set holddown 120
```

Related Commands

Command	Description
holddown (PfR)	Configures the prefix 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-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.

set interface (PfR)

To configure a Performance Routing (PfR) map to send packets that match prefixes in an access list on PfR border routers to the null interface, use the **set interface** command in PfR map configuration mode. To delete the set clause entry, use the **no** form of this command.

set interface null0

no set interface null0

Syntax Description

null0	Specifies that packets will be sent to the null interface, which means that the packets are discarded.

Command Default

No packets are sent to the null interface.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **set interface** command is entered on a master controller in PfR map configuration mode. This command can be used for PfR black hole filtering if the border routers detect a denial-of-service (DoS) attack by directing packets to the null interface. The null interface is a virtual network interface that is similar to the loopback interface. Whereas traffic to the loopback interface is directed to the router itself, traffic sent to the null interface is discarded. This interface is always up and can never forward or receive traffic; encapsulation always fails. The null interface functions similarly to the null devices available on most operating systems. Null interfaces are used as a low-overhead method of discarding unnecessary network traffic.

Examples

The following example shows how to configure a PfR map named BLACK_HOLE_MAP to direct packets to the null interface. To use this configuration for a DoS attack, leave the access list empty until an attack is detected and add the prefix or prefixes that are determined to be the source of the attack. Subsequent packets received from the specified prefix or prefixes will be discarded.

```
Router(config)# pfr-map black-hole-map 10
Router(config-pfr-map)# match ip address access-list black-hole-list
Router(config-pfr-map)# set interface null0
```

Related Commands

Command	Description
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.
set next-hop (PfR)	Configures a PfR map to send packets that match prefixes in an access list on PfR border routers to the specified next hop.

set jitter (PfR)

To configure a Performance Routing (PfR) map to set the maximum jitter value that PfR will permit for an exit link, use the **set jitter** command in PfR map configuration mode. To delete the set clause entry, use the **no** form of this command.

set jitter threshold *maximum*

no set jitter threshold *maximum*

Syntax Description

threshold	Specifies a maximum absolute threshold value for jitter. Jitter is a measure of voice quality.
maximum	Number (in milliseconds) in the range from 1 to 1000, where 1 represents the highest voice quality, and 1000 represents the lowest voice quality. The default value is 30.

Command Default

No jitter values are set.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **set jitter** command is entered on a master controller in PfR map configuration mode. This command is used to specify the maximum tolerable jitter value permitted on an exit link. Jitter is a measure of voice quality where the lower the jitter value, the higher the voice quality. If the jitter value is greater than the user-defined or default value, PfR determines that the exit link is out-of-policy and searches for an alternate exit link.

Another measure of voice quality is the estimated Mean Opinion Score (MOS). Use the **set mos** command and the **set jitter** command in a PfR map to define voice quality.

Examples

The following example shows how to configure a PfR map named JITTER that sets the threshold jitter value. If the jitter threshold value exceeds 20 milliseconds, and more than 30 percent of the MOS samples are below the MOS threshold of 3.80 for voice quality, the master controller searches for a new exit link.

```
Router(config)# oer-map JITTER 10
Router(config-oer-map)# set jitter threshold 20
Router(config-oer-map)# set mos threshold 3.80 percent 30
```

Related Commands

Command	Description
jitter (PfR)	Specifies the threshold jitter value that PfR will permit for an exit link.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.
set mos (PfR)	Configures a PfR map to specify the threshold and percentage Mean Opinion Score (MOS) values that PfR will permit for an exit link.

set link-group (PfR)

To specify a link group for traffic classes defined in a Performance Routing (PfR) policy, use the **set link-group** command in PfR map configuration mode. To delete the set clause entry and remove the link group, use the **no** form of this command.

set link-group *link-group-name* [**fallback** *link-group-name*]

no set link-group *link-group-name*

Syntax Description

link-group-name	Name of a link group.
fallback	(Optional) Specifies a fallback link group to be used if the primary link group is out-of-policy (OOP).

Command Default

No link groups are specified for a traffic class.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **set link-group** command is entered on a master controller in PfR map configuration mode. This command is used to define a link group for the traffic class matched in a PfR map.

Introduced in Cisco IOS Release 12.4(15)T, link groups are used 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. Up to three link groups can be specified for each interface. Use the **link-group** (PfR) command to define the link group for an interface and use the **set link-group** command to define the primary link group and a fallback link group for a specified traffic class in a PfR map.

Use the **show pfr master link-group** command to view information about configured PfR link groups.

Examples

The following example shows how to configure a PfR map named link_video_map that configures PfR to create a traffic class that matches an access list named video_list. The traffic class is configured to use a link group named video as the primary link group, and a fallback group named voice. The video link group may be a set of high bandwidth links that are preferred for video traffic.

```
Router(config)# pfr-map link_video_map 10
Router(config-pfr-map)# match ip address access-list video_list
Router(config-pfr-map)# set link-group video fallback voice
```

Related Commands

Command	Description
link-group (PfR)	Configures a PfR border router exit interface as a member of a link group.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.
show pfr master link-group	Displays information about PfR link groups.

set loss (PfR)

To configure a Performance Routing (PfR) map to set the relative or maximum packet loss limit that PfR will permit for an exit link, use the **set loss** command in PfR map configuration mode. To delete the set clause entry and reset the relative percentage of packet loss to the default value, use the **no** form of this command.

set loss {**relative** *average* | **threshold** *maximum*}

no set loss

Syntax Description

relative *average*	Sets a relative percentage of packet loss based on a comparison of short-term and long-term packet loss percentages. The range of values that can be configured for this argument is a number from 1 to 1000. Each increment represents one tenth of a percent.
threshold *maximum*	Sets absolute packet loss based on packets per million (PPM). The range of values that can be configured for this argument is from 1 to 1000000.

Command Default

PfR uses a default relative percentage of 100 (10 percent) if this command is not configured or if the **no** form of this command is entered.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **set loss** command is entered on a master controller in PfR map configuration mode. This command is used to configure a PfR map to set the relative percentage or maximum number of packets that PfR will permit to be lost during transmission on an exit link. If packet loss is greater than the user-defined or the default value, PfR determines that the exit link is out-of-policy and searches for an alternate exit link.

The **relative** keyword is used to configure the relative packet loss percentage. The relative packet loss percentage is based on a comparison of short-term and long-term packet loss. The short-term measurement reflects the percentage of packet loss within a 5-minute period. The long-term measurement reflects the percentage of packet loss within a 60-minute period. The following formula is used to calculate this value:

Relative packet loss = ((short-term loss – long-term loss) / long-term loss) * 100

The master controller measures the difference between these two values as a percentage. If the percentage exceeds the user-defined or default value, the exit link is determined to be out-of-policy. For example, if long-term packet loss is 200 PPM and short-term packet loss is 300 PPM, the relative loss percentage is 50 percent.

The **threshold** keyword is used to configure the absolute maximum packet loss. The maximum value is based on the actual number of PPM that have been lost.

Examples

The following example creates a PfR map named LOSS that sets the relative percentage of acceptable packet loss for traffic from the prefix list named CUSTOMER to a 20 percent relative percentage. If the packet loss on the current exit link exceeds 20 percent, the master controller will search for a new exit.

```
Router(config)# pfr-map LOSS 10
Router(config-pfr-map)# match ip address prefix-list CUSTOMER
Router(config-pfr-map)# set loss relative 200
```

Related Commands

Command	Description
loss (PfR)	Sets the relative or maximum packet loss limit that PfR will permit for an exit link.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.

set mode (PfR)

To configure a Performance Routing (PfR) map to configure route monitoring, route control, or exit selection for matched traffic, use the **set mode** command in PfR map configuration mode. To delete the set clause entry and reset the default values, use the **no** form of this command.

set mode {**monitor** {**active** [**throughput**] | **both** | **fast** | **passive**} | **route** {**control** | **observe**} | **select-exit** {**best** | **good**}}

no set mode {**monitor** | **route** {**control** | **observe**} | **select-exit**}

Syntax Description

monitor	Enables the configuration of PfR monitoring settings.
active	Enables active monitoring.
throughput	(Optional) Enables active monitoring with throughput data from passive monitoring.
both	Enables both active and passive monitoring.
fast	Enables continuous active monitoring and passive monitoring.
passive	Enables passive monitoring.
route	Enables the configuration of PfR route control policy settings.
control	Enables automatic route control.
observe	Configures PfR to passively monitor and report without making any changes.
select-exit	Enables the exit selection based on performance or policy.
best	Configures PfR to select the best available exit based on performance or policy.
good	Configures PfR to select the first exit that is in-policy.

Command Default

PfR uses the following default settings if this command is not configured or if the **no** form of this command is entered:

- Monitoring: Both active and passive monitoring is enabled.
- Route control: Observe mode route control is enabled.
- Exit Selection: The first in-policy exit is selected.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **set mode** command is entered on a master controller in PfR map configuration mode. This command is used to configure a PfR map to enable and configure observe mode and control mode settings, passive monitoring and active monitoring, and exit link selection for traffic that is configured as match criteria.

Observe Mode

Observe mode monitoring is enabled by default. In observe mode, the master controller monitors prefixes and exit links based on default and user-defined policies and then reports the status of the network and the decisions that should be made, but it does not implement any changes. This mode allows you to verify the effectiveness of this feature before it is actively deployed.

Control Mode

In control mode, the master controller coordinates information from the border routers and makes policy decisions just as it does in observe mode. The master controller monitors prefixes and exits based on default and user-defined policies, but then it implements changes to optimize prefixes and to select the best exit. In this mode, the master controller gathers performance statistics from the border routers and then transmits commands to the border routers to alter routing as necessary in the PfR managed network.

Passive Monitoring

The master controller passively monitors IP prefixes and TCP traffic flows. Passive monitoring is configured on the master controller. Monitoring statistics are gathered on the border routers and then reported back to the master controller. PfR uses NetFlow to collect and aggregate passive monitoring statistics on a per-prefix basis. No explicit NetFlow configuration is required. NetFlow support is enabled by default when passive monitoring is enabled. PfR uses passive monitoring to measure the following information:

Delay—PfR measures the average delay of TCP flows for a prefix. Delay is the measurement of the time between the transmission of a TCP synchronization message and receipt of the TCP acknowledgement.

Packet Loss—PfR measures packet loss by tracking TCP sequence numbers for each TCP flow. PfR estimates packet loss by tracking the highest TCP sequence number. If a subsequent packet is received with a lower sequence number, PfR increments the packet loss counter.

Reachability—PfR measures reachability by tracking TCP synchronization messages that have been sent repeatedly without receiving a TCP acknowledgement.

Throughput—PfR measures outbound throughput for optimized prefixes. Throughput is measured in bits per second (bps).

Note PfR passively monitors TCP traffic flows for IP traffic. Passive monitoring of non-TCP sessions is not supported.

Active Monitoring

PfR uses Cisco IOS IP Service Level Agreements (SLAs) to enable active monitoring. IP SLAs support is enabled by default. IP SLAs support allows PfR to be configured to send active probes to target IP addresses to measure the jitter and delay, determining if a prefix is out-of-policy and if the best exit is selected. The border router collects these performance statistics from the active probe and transmits this information to the master controller. The master controller uses this information to optimize the prefix and select the best available exit based on default and user-defined policies. The **active-probe** command is used to create an active probe.

The **throughput** keyword enables the throughput data from passive mode monitoring to be considered when optimizing UDP traffic for both performance and load-balancing. UDP traffic can be optimized only for performance (for example, delay, jitter, and loss) when active monitoring data is available. To enable load-balancing of UDP traffic, throughput data from passive monitoring is required.

Fast Failover Monitoring

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

Optimal Exit Link Selection

The master controller can be configured to select a new exit for an out-of-policy prefix based on performance or policy. You can configure the master controller to select the first in-policy exit by entering the **good** keyword, or you can configure the master controller to select the best exit with the **best** keyword. If the **good** keyword is used and there is no in-policy exit, the prefix is uncontrolled.

Examples

The following example creates a PfR map named OBSERVE that configures PfR to observe and report but not control traffic from the prefix list named CUSTOMER:

```
Router(config)# pfr-map OBSERVE 80
Router(config-pfr-map)# match ip address prefix-list CUSTOMER
Router(config-pfr-map)# set mode route observe
```

Related Commands

Command	Description
mode (PfR)	Configures route monitoring or route control on a PfR master controller.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.

set mos (PfR)

To configure a Performance Routing (PfR) map to set the threshold and percentage Mean Opinion Score (MOS) values that PfR will permit for an exit link, use the **set mos** command in PfR map configuration mode. To reset the threshold MOS values to their default value, use the **no** form of this command.

set mos threshold *minimum* **percentage** *percent*

no set mos threshold *minimum* **percentage** *percent*

Syntax Description

threshold	Specifies a threshold MOS value that represents a minimum voice quality for exit link utilization.
minimum	Number (to two decimal places) in the range from 1.00 to 5.00. The number 1.00 represents the lowest voice quality, and the number 5.00 represents the highest voice quality. The default MOS value is 3.60.
percentage	Specifies a percentage value that is compared with the percentage of MOS samples that are below the MOS threshold.
percent	Number, as a percentage.

Command Default

The default MOS value is 3.60.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **set mos** command is entered on a master controller in PfR map configuration mode and is used to determine voice quality. The number of MOS samples over a period of time that are below the threshold MOS value are calculated. If the percentage of MOS samples below the threshold is greater than the configured percentage, PfR determines that the exit link is out-of-policy and searches for an alternate exit link.

Another measure of voice quality is the jitter value. Use the **set mos** (PfR) command and the **set jitter** (PfR) command in a PfR map to define voice quality.

Examples

The following example creates a PfR map named MOS that configures the master controller to search for a new exit link if more than 30 percent of the MOS samples are below the MOS threshold of 3.80.

```
Router(config)# pfr-map MOS 10
Router(config-pfr-map)# match ip address prefix-list LIST1
Router(config-pfr-map)# set mos threshold 3.80 percent 30
```

Related Commands

Command	Description
mos (PfR)	Configures the maximum MOS value that PfR will permit for an exit link.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.
set jitter (PfR)	Configures a PfR map to set the maximum jitter value that PfR will permit for an exit link.

set next-hop (PfR)

To configure a Performance Routing (PfR) map to send packets that match prefixes in an access list on PfR border routers to the specified next hop, use the **set next-hop** command in PfR map configuration mode. To delete the set clause entry, use the **no** form of this command.

set next-hop *ip-address*

no set next-hop *ip-address*

Syntax Description

ip-address	IP address of the next hop to which the packets will be sent.

Command Default

No packets that match prefixes in an access list on PfR border routers are sent to the next hop.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

This command can be used for PfR sinkhole filtering if the border routers detect a denial-of-service (DoS) attack by directing packets to the specified next hop. The packets may be saved, analyzed, or discarded at the next hop.

Examples

The following example shows how to configure a PfR map named SINKHOLE_MAP that directs packets to the specified next hop. Use this configuration in preparation for a DoS attack, leave the access list empty until an attack is detected, and add the prefix or prefixes that are determined to be the source of the attack. Subsequent packets received from the specified prefix or prefixes will be sent to the specified next hop.

```
Router(config)# pfr-map SINKHOLE_MAP 10
Router(config-pfr-map)# match ip address access-list SINKHOLE-LIST
Router(config-pfr-map)# set next-hop 10.20.24.3
```

Related Commands

Command	Description
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.
set interface (PfR)	Configures a PfR map to send packets that match prefixes in an access list on PfR border routers to the null interface.

set periodic (PfR)

To configure a Performance Routing (PfR) map to set the time period for the periodic timer, use the **set periodic** command in PfR map configuration mode. To delete the set clause entry and remove the periodic timer setting, use the **no** form of this command.

set periodic *timer*

no set periodic

Syntax Description

timer	Length of time set for the periodic timer, in seconds. The value for the *timer* argument is from 180 to 7200.

Command Default

The periodic timer is not set using a PfR map.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **set periodic** command is entered on a master controller in PfR map configuration mode. This command is used to configure a PfR map to configure PfR to periodically select the best exit based on the periodic timer value for traffic that is configured as match criteria in a PfR map. When this timer expires, PfR will automatically select the best exit, whether the current exit is in-policy or out-of-policy. The periodic timer is reset when the new exit is selected.

Examples

The following example creates a PfR map named PERIODIC that sets the periodic timer to 300 seconds for traffic from the prefix list named CUSTOMER. When the timer expires, PfR will select the best exit.

```
Router(config)# pfr-map PERIODIC 80
Router(config-pfr-map)# match ip address prefix-list CUSTOMER
Router(config-pfr-map)# set periodic 300
```

Related Commands

Command	Description
periodic (PfR)	Configures PfR to periodically select the best exit.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.

set probe (PfR)

To set the frequency of a Performance Routing (PfR) active probe, use the **set probe** command in PfR map configuration mode. To reset the frequency of a PfR active probe to its default values, use the **no** form of this command.

set probe {**frequency** *seconds* | **packets** *packet-count*}

no set probe {**frequency** *seconds* | **packets** *packet-count*}

Syntax Description

frequency	Sets the frequency of an active probe.
seconds	Number of seconds in the range from 4 to 60. The default is 60.
packets	Specifies the number of probe packets for a jitter probe.
packet-count	Number of probe packets in the range from 2 to 255. The default is 100.

Command Default

The default active probe frequency is 60 seconds.
The default number of packets per probe is 100.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **set probe** command is entered on a master controller in PfR map configuration mode. This command is used within a PfR map configuration to set the frequency of the active probes. Unless the default frequency of 60 seconds is used, configuring the set probe command will increase the frequency of the probes. Increased probe frequency results in a lower response time of PfR. The frequency can be increased for a number of policies, but if all active probes are set to an increased frequency, an Intrusion Detection Service (IDS) may be triggered.

Fast monitoring sets the active probes to continuously monitor all the exits (probe-all), and passive monitoring is enabled too. Fast failover monitoring can be used with all types of active probes: ICMP echo, jitter, TCP connection, and UDP echo. When the **mode monitor fast** command is enabled, the probe frequency can be set to a lower frequency than for other monitoring modes, to allow a faster failover ability. The minimum number of seconds was lowered from 4 seconds to 2 seconds to support the fast failover monitoring mode. Under fast monitoring with a lower probe frequency, route changes can be performed within 3 seconds of an out-of-policy situation.

Using the **packets** keyword and the *packet-count* argument, the number of probe packets per jitter probe can be set. The new keyword is supported under PfR map configuration mode only, not at a global level. The new keyword applies only to jitter probes, and the configuration affects global probes and forced probes for all traffic classes.

Examples

The following example shows how to set the frequency of an active probe to be 10 seconds using a PfR map named PROBE:

```
Router(config)# pfr-map PROBE 10
Router(config-pfr-map)# set probe frequency 10
```

The following example shows how to set the frequency of an active probe to be 2 seconds using a PfR map named FAST after the fast failover monitoring mode is enabled:

```
Router(config)# pfr-map FAST 10
Router(config-pfr-map)# set mode monitor fast
Router(config-pfr-map)# set probe frequency 2
```

The following example shows how to set the number of probe packets for a jitter probe at 33 packets using a PfR map named JITTER:

```
Router(config)# pfr-map JITTER
Router(config-pfr-map)# set probe packets 33
```

Related Commands

Command	Description
active-probe (PfR)	Configures a PfR active probe for a target prefix.
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.
set mode (PfR)	Configures a PfR map to configure route monitoring, route control, or exit selection for matched traffic.

set resolve (PfR)

To configure a PfR map to set policy priority for overlapping policies, use the **set resolve** command in PfR map configuration mode. To delete the set clause entry, use the **no** form of this command.

set resolve {**cost priority** *value* | **delay priority** *value* **variance** *percentage* | **jitter priority** *value* **variance** *percentage* | **loss priority** *value* **variance** *percentage* | **mos priority** *value* **variance** *percentage* | **range priority** *value* | **utilization priority** *value* **variance** *percentage*}

no set resolve {**cost** | **delay** | **jitter** | **loss** | **mos** | **range** | **utilization**}

Syntax Description

cost	Specifies policy priority settings for cost optimization.
priority	Sets the priority of the policy.
value	A number in the range of 1 to 10. The number 1 has the highest priority, and the number 10 has the lowest priority.
delay	Specifies policy priority settings for packet delay.
variance	Sets the allowable variance for the policy, as a percentage.
percentage	A number in the range from 1 to 100.
jitter	Specifies policy priority settings for jitter.
loss	Specifies policy priority settings for packet loss.
mos	Specifies policy priority settings for Mean Opinion Score (MOS).
range	Specifies policy priority settings for range.
utilization	Specifies policy priority settings for exit link utilization.

Command Default

PfR uses the following default settings if this command is not configured or if the **no** form of this command is entered:

- An unreachable prefix: highest priority
- delay priority: 11
- utilization priority: 12

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **set resolve** command is entered on a master controller in PfR map configuration mode. 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. The number 1 assigns the highest priority to the policy. The number 10 sets the lowest priority. Each policy must be assigned a different priority number. If you try to assign the same priority number to two different policy types, an error message will be displayed on the console.

The **variance** keyword is used to set an allowable variance for a user-defined policy. This keyword configures the allowable percentage by which an exit link or prefix can vary from the user-defined policy value and still be considered equivalent. For example, if exit link delay is set to 80 percent and a 10 percent variance is configured, exit links with delay values from 80 to 89 percent will be considered equal.

Note Variance cannot be set for cost or range policies.

Examples

The following example creates a PfR map named RESOLVE that sets the priority for delay policies to 1 for traffic learned based on highest outbound throughput. The variance is set to allow a 10 percent difference in delay statistics before a prefix is determined to be out-of-policy.

```
Router(config)# pfr-map RESOLVE 10
Router(config-pfr-map)# match pfr learn throughput
Router(config-pfr-map)# set resolve delay priority 1 variance 10
```

Related Commands

Command	Description
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.
resolve	Sets the priority of a PfR policy when multiple overlapping policies are configured.

set traceroute reporting (PfR)

To configure a Performance Routing (PfR) map to enable traceroute reporting, use the **set traceroute reporting** command in PfR map configuration mode. To delete the set clause entry, use the **no** form of this command.

set traceroute reporting [**policy** {**delay** | **loss** | **unreachable**}]

no set traceroute reporting [**policy** {**delay** | **loss** | **unreachable**}]

Syntax Description

policy	(Optional) Configures policy-based traceroute reporting.
delay	(Optional) Configures traceroute reporting based on delay policies.
loss	(Optional) Configures traceroute reporting based on packet loss policies.
unreachable	(Optional) Configures traceroute reporting based on reachability policies.

Command Default

Traceroute reporting is not enabled using a PfR map.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **set traceroute reporting** command is entered on a master controller in PfR map configuration mode. This command is used to enable continuous and policy-based traceroute probing. Traceroute probing allows you to monitor prefix performance on a hop-by-hop basis. Delay, loss, and reachability measurements are gathered for each hop from the probe source to the target prefix.

The following types of traceroute reporting are configured with this command:

Continuous—A traceroute probe is triggered for each new probe cycle. Entering this command without any keywords enables continuous reporting. The probe is sourced from the current exit of the prefix.

Policy based—A traceroute probe is triggered automatically when a prefix goes into an out-of-policy state. Entering this command with the **policy** keyword enables policy-based traceroute reporting. Policy-based traceroute probes are configured individually for delay, loss, and reachability policies. The monitored prefix is sourced from a match clause in a PfR map. Policy-based traceroute reporting stops when the prefix returns to an in-policy state.

The **show pfr master prefix** command is used to display traceroute probe results. An on-demand traceroute probe can be initiated when entering the **show pfr master prefix** command with the **current** and **now** keywords. The **set traceroute reporting** command does not have to be configured to initiate an on-demand traceroute probe.

Examples

The following example, starting in global configuration mode, enables continuous traceroute probing for prefixes that are learned based on delay:

```
Router(config)# pfr-map TRACE 10
Router(config-pfr-map)# match pfr learn delay
Router(config-pfr-map)# set traceroute reporting
```

Related Commands

Command	Description
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.
show pfr master prefix	Displays the status of monitored prefixes.
traceroute probe-delay (PfR)	Sets the time interval between traceroute probe cycles.

set unreachable (PfR)

To configure a Performance Routing (PfR) map to set the maximum number of unreachable hosts, use the **set unreachable** command in PfR map configuration mode. To delete the set clause entry and reset the relative percentage of unreachable hosts to the default value of 50 (5 percent), use the **no** form of this command.

set unreachable {**relative** *average* | **threshold** *maximum*}

no set unreachable

Syntax Description

relative *average*	Sets a relative percentage of unreachable hosts based on a comparison of short-term and long-term percentages. The range of values that can be configured for this argument is a number from 1 to a 1000. Each increment represents one tenth of a percent.
threshold *maximum*	Sets the absolute maximum number of unreachable hosts based on flows per million (fpm). The range of values that can be configured for this argument is from 1 to 1000000.

Command Default

PfR uses a default relative percentage of 50 (5 percent) unreachable hosts if this command is not configured or if the **no** form of this command is entered.

Command Modes

PfR map configuration (config-pfr-map)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **set unreachable** command is entered on a master controller in PfR map configuration mode. This command is used to set the relative percentage or the absolute maximum number of unreachable hosts, based on flows per million, that PfR will permit from a PfR-managed exit link. If the absolute number or relative percentage of unreachable hosts is greater than the user-defined or the default value, PfR determines that the exit link is out-of-policy 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 short-term measurement reflects the percentage of hosts that are unreachable within a 5-minute period. The long-term measurement reflects the percentage of unreachable hosts within a 60-minute period. The following formula is used to calculate this value:

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

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

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

Examples

The following example creates a PfR map named UNREACHABLE that configures the master controller to search for a new exit link when the difference between long- and short-term measurements (relative percentage) is greater than 10 percent for traffic learned based on highest delay:

```
Router(config)# pfr-map UNREACHABLE 10
Router(config-pfr-map)# match pfr learn delay
Router(config-pfr-map)# set unreachable relative 100
```

Related Commands

Command	Description
pfr-map	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.
unreachable (PfR)	Sets the relative percentage or maximum number of unreachable hosts that PfR permits from a PfR-managed exit link.

show pfr api provider

To display information about application programming interface providers that are registered with Performance Routing (PfR), use the **show pfr api provider** command in privileged EXEC mode.

show pfr api provider [**detail**]

Syntax Description

detail	(Optional) Displays detailed information about application interface providers.

Command Default

Detailed information about API providers is not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **show pfr api provider** command is entered on a master controller. This command is used to display application interface provider and host information including the ID of each configured provider, the priority of the provider and the host (if configured), and the IP addresses of each configured host device. The **detail** keyword is used to display more detailed information.

The PfR application interface defines the mode of communication and messaging between applications and the network for the purpose of optimizing the traffic associated with the applications. A provider is defined as an entity outside the network in which the router configured as a PfR master controller exists, for example, an ISP, or a branch office of the same company. The provider has one or more host devices running one or more applications that use the PfR application interface to communicate with a PfR master controller. A provider must be registered with a PfR master controller before an application on a host device can interface with PfR. Use the **api provider** command to register the provider, and use the **host-address** (PfR) command to configure a host device. After registration, a host device in the provider network can initiate a session with a PfR master controller. The PfR application interface provides an automated method for networks to be aware of applications and provides application-aware performance routing.

Examples

The following example shows information about configured application interface providers and host devices:

```
Router# show pfr api provider

API Version: Major 2, Minor 0
  Provider id 1, priority 4000
   Host ip 172.17.1.1, priority 4001
   Host ip 10.1.2.2, priority 3001
  Provider id 2, priority 20
  Provider id 3, priority 10
```

Table 23 describes the significant fields shown in the display.

Table 23 show pfr api provider Field Descriptions

Field	Description
API Version, Major, Minor	Version number of the application interface with major and minor releases.
Provider id	ID number of an application interface provider.
priority	Priority assigned to the policies of a provider or a host.
Host ip	IP address of a host device.

The following example shows detailed information about configured application interface providers and host devices:

```
Router# show pfr api provider detail

API Version: Major 2, Minor 0
  Provider id 1001, priority 65535
   Host ip 10.3.3.3, priority 65535
    Session id 9, Version Major 2, Minor 0
    Num pfx created 2, Num policies created 2
    Last active connection time (sec) 00:00:01
    Policy ids : 101, 102,
   Host ip 10.3.3.4, priority 65535
    Session id 10, Version Major 2, Minor 0
    Num pfx created 1, Num policies created 1
    Last active connection time (sec) 00:00:03
    Policy ids : 103,
  Provider id 2001, priority 65535
   Host ip 172.19.198.57, priority 65535
    Session id 11, Version Major 2, Minor 0
    Num pfx created 0, Num policies created 0
    All Prefix report enabled
    All exit report enabled
```

Table 24 describes the significant fields shown in the display that are different from Table 23.

Table 24 show pfr api provider detail Field Descriptions

Field	Description
Session id	Session ID is automatically allocated by PfR when an application interface provider initiates a session.
Num pfx created	Number of traffic classes created by the application interface provider application.
Num policies created	Number of policies dynamically created by the application interface provider application.
Last active connection time	Time, in seconds, since the last active connection from the application interface provider.
Policy ids	IDs assigned to each policy dynamically created by the application interface provider application.

Table 24 show pfr api provider detail Field Descriptions (continued)

Field	Description
All Prefix report enabled	Traffic class reports from the PfR master controller are enabled for the application interface provider.
All exit report enabled	Exit link reports from the PfR master controller are enabled for the application interface provider.

Related Commands

Command	Description
api provider (PfR)	Registers an application interface provider with a PfR master controller and enters PfR master controller application interface provider configuration mode.
debug pfr api provider	Displays PfR application interface debugging information.
host-address (PfR)	Configures information about a host device used by an application interface provider to communicate with a PfR master controller.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

show pfr border

To display information about a Performance Routing (PfR) border-router connection and PfR-controlled interfaces, use the **show pfr border** command in privileged EXEC mode.

show pfr border

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **show pfr border** command is entered on a PfR border router. The output displays information about the border router, the status of the master controller connection, and border router interfaces.

Examples

The following example shows the status of a border router:

```
Router# show pfr border

OER BR 10.1.1.3 ACTIVE, MC 10.1.1.1 UP/DOWN: UP 00:57:55,
  Auth Failures: 0
  Conn Status: SUCCESS, PORT: 3949
  Exits
  Et0/0           INTERNAL
  Et1/0           EXTERNAL
```

Table 25 describes the significant fields shown in the display.

Table 25 show pfr border Field Descriptions

Field	Description
OER BR	Displays the IP address and the status of the local border router (ACTIVE or DISABLED).
MC	Displays the IP address of the master controller, the connection status (UP or DOWN), the length of time that connection with master controller has been active, and the number of authentication failures that have occurred between the border router and the master controller.
Auth Failures	Displays the number of authentication failures.
Conn Status	Displays the connection status (“SUCCESS” or “FAILED”).

Table 25 show pfr border Field Descriptions (continued)

Field	Description
PORT	Displays the TCP port number used to communicate with the master controller.
Exits	Displays PfR-managed exit interfaces on the border router. This field displays the interface type, number, and PfR status (EXTERNAL or INTERNAL).

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

show pfr border active-probes

To display connection status and information about active probes on a Performance Routing (PfR) border router, use the **show pfr border active-probes** command in privileged EXEC mode.

show pfr border active-probes

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **show pfr border active-probes** command is entered on a border router. This command displays the target active-probe assignment for a given prefix and the current probing status, including the border router or border routers that are executing the active probes.

Examples

The following example shows three active probes, each configured for a different prefix. The target port, source IP address, and exit interface are displayed in the output.

```
Router# show pfr border active-probes

        PfR Border active-probes
Type      = Probe Type
Target    = Target IP Address
TPort     = Target Port
Source    = Send From Source IP Address
Interface = Exit interface
Att       = Number of Attempts
Comps   = Number of completions
N - Not applicable

Type     Target          TPort Source          Interface           Att   Comps
udp-echo 10.4.5.1           80 10.0.0.1        Et1/0                 1       0
tcp-conn 10.4.7.1           33 10.0.0.1        Et1/0                 1       0
echo     10.4.9.1            N 10.0.0.1        Et1/0                 2       2
```

Table 26 describes the significant fields shown in the display.

Table 26 show pfr border active-probes Field Description

Field	Description
Type	The active probe type.
Target	The target IP address.

Table 26 show pfr border active-probes Field Description (continued)

Field	Description
TPort	The target port.
Source	The source IP address.
Interface	The PfR-managed exit interface.
Att	The number of attempts.
Comps	The number successfully completed attempts.

Related Commands

Command	Description
active-probe (PfR)	Configures active probes to monitor PfR-controlled prefixes.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

show pfr border defined application

To display information about user-defined applications on a Performance Routing (PfR) border router, use the **show pfr border defined application** command in privileged EXEC mode.

show pfr border defined application

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **show pfr border defined application** command is entered on a PfR border router. This command displays all user-defined applications that are defined on the master controller. To define a custom application to be used by PfR, use the **application define** (PfR) command on the PfR master controller.

To display the same information on the PfR master controller, use the **show pfr master defined application** command.

Examples

The following partial output shows information about the user-defined application definitions configured for use with PfR:

```
Router# show pfr border defined application

PfR Defined Applications:

Name                 Appl_ID Dscp Prot     SrcPort     DstPort SrcPrefix
-------------------------------------------------------------------------------
telnet                     1 defa  tcp       23-23     1-65535 0.0.0.0/0
telnet                     1 defa  tcp     1-65535       23-23 0.0.0.0/0
ftp                        2 defa  tcp       21-21     1-65535 0.0.0.0/0
ftp                        2 defa  tcp     1-65535       21-21 0.0.0.0/0
cuseeme                    4 defa  tcp   7648-7648     1-65535 0.0.0.0/0
cuseeme                    4 defa  tcp   7649-7649     1-65535 0.0.0.0/0
dhcp                       5 defa  udp       68-68       67-67 0.0.0.0/0
dns                        6 defa  tcp       53-53     1-65535 0.0.0.0/0
dns                        6 defa  tcp     1-65535       53-53 0.0.0.0/0
dns                        6 defa  udp       53-53     1-65535 0.0.0.0/0
dns                        6 defa  udp     1-65535       53-53 0.0.0.0/0
finger                     7 defa  tcp       79-79     1-65535 0.0.0.0/0
finger                     7 defa  tcp     1-65535       79-79 0.0.0.0/0
gopher                     8 defa  tcp       70-70     1-65535 0.0.0.0/0
.
.
.
```

Table 27 describes the significant fields shown in the display.

Table 27 show pfr border defined application Field Descriptions

Field	Description
Name	Application name.
Appl_ID	Unique ID that identifies an application traffic class.
Dscp	Differentiated Services Code Point (DSCP) value.
Prot	Application protocol number.
SrcPort	Source application port number: a single port number or a range of port numbers.
DstPort	Destination application port number: a single port number or a range of port numbers.
SrcPrefix	IP address of the traffic class source.

Related Commands

Command	Description
application define (PfR)	Defines an application to be monitored by PfR.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
show pfr master defined application	Displays information about user-defined application definitions used on the PfR master controller.

show pfr border passive applications

To display the list of application traffic classes that are monitored by Performance Routing (PfR), use the **show pfr border passive applications** command in privileged EXEC mode.

show pfr border passive applications

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **show pfr border passive applications** command is entered on a border router. This command displays a list of application traffic classes that are monitored by the border router using NetFlow passive monitoring.

Examples

The following example displays an application traffic class that is monitored by a border router:

```
Router# show pfr border passive applications

OER Passive monitored Appl:
 + - monitor more specific

 Prefix          /Mask   Prot   Dscp    SrcPort           DstPort          Appl_ID
10.1.3.0         /24      17      ef    [1, 65535]        [3000, 4000]      1
```

Table 28 describes the significant fields shown in the display.

Table 28 show pfr border passive applications Field Descriptions

Field	Description
Prefix	IP address.
/Mask	Prefix length.
Prot	Application protocol number.
Dscp	Differentiated Services Code Point (DSCP) value.
SrcPort	Source application port number: a single port number or a range of port numbers.
DstPort	Destination application port number: a single port number or a range of port numbers.
Appl_ID	Unique ID that identifies an application traffic class.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

show pfr border passive cache learned

To display passive measurement information that is collected by NetFlow for Performance Routing (PfR) monitored learned prefixes, use the **show pfr border passive cache learned** command in privileged EXEC mode.

show pfr border passive cache learned [**application** | **traffic-class**]

Syntax Description

application	(Optional) Displays measurement information about PfR-monitored learned prefixes for an application traffic class.
traffic-class	(Optional) Displays flow cache information for PfR monitored learned prefixes.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **show pfr border passive cache learned** command is entered on a border router. This command displays real-time prefix information that is collected from the border router through NetFlow passive monitoring.

A maximum of five host addresses and five ports are collected for each prefix. The output will also show the throughput in bytes and the delay in milliseconds. If the **application** keyword is entered, the output displays information about learned prefixes that match other application criteria such as the Differentiated Services Code Point (DSCP) value, protocol, or port number. The **traffic-class** keyword displays cache information about monitored learned prefixes for a PfR traffic class.

Examples

The following example displays passive monitoring information about learned prefixes:

```
Router# show pfr border passive cache learned

 OER Learn Cache:
    State is enabled
    Measurement type: throughput, Duration: 2 min
    Aggregation type: prefix-length, Prefix length: 24
    4096 oer-flows per chunk,
    22 chunks allocated, 32 max chunks,
    1 allocated records, 90111 free records, 8913408 bytes allocated

Prefix          Mask     Pkts  B/Pk  Delay Samples   Active
Host1           Host2           Host3           Host4           Host5
dport1          dport2          dport3          dport4          dport5
10.1.5.0         /24      17K    46    300       2     45.1
10.1.5.2        10.1.5.3        0.0.0.0         0.0.0.0         0.0.0.0
1024            80              0               0               0
```

Table 29 describes the significant fields shown in the display.

Table 29 show pfr border passive cache learned Field Descriptions

Field	Description
State is	Displays PfR prefix learning status: enabled or disabled.
Measurement type	Displays how the prefix is learned. The output displays throughput, delay, or both throughput and delay.
Duration	Displays the duration of the learning period in minutes.
Aggregation type	Displays the aggregation type: BGP, non-BGP, or prefix-length.
... oer-flows per chunk	Displays number of flow records per memory chunk.
... chunks allocated	Number of memory chunks allocated.
... allocated records	Number of records currently allocated in the learn cache.
Prefix	IP address and port of the learned prefix.
Mask	Prefix length as specified in a prefix mask.
Pkts B/Pk	Number of packets and bytes per packet.
Delay Samples	Number of delay samples that NetFlow has collected.
Active	Time for which the flow has been active.

The following example uses the **application** keyword 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.

```
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
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

show pfr border passive learn

To display the configured, learned parameters to be used with passive measurement information collected by NetFlow for Performance Routing (PfR) learned traffic flows, use the **show pfr border passive learn** command in privileged EXEC mode.

show pfr border passive learn

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **show pfr border passive learn** command is entered on a border router. This command displays configured parameters including filter and aggregate application information that is collected from the border router through NetFlow passive monitoring.

Examples

The following example displays passive monitoring information about learned traffic flows:

```
Router# show pfr border passive learn

OER Border Learn Configuration :
    State is enabled
    Measurement type: throughput, Duration: 2 min
    Aggregation type: prefix-length, Prefix length: 24
    No port protocol config

 Traffic Class Filter List:
   List: SrcPrefix       SrcMask DstPrefix       DstMask
         Prot  DSCP  sport_opr sport_range    dport_opr dport_range     Grant
      1: 0.0.0.0         0       10.1.0.0        16
         17      ef  0         [1, 65535]      0        [1, 65535]      Permit

 Traffic Class Aggregate List:
   List: Prot  DSCP  sport_opr sport_range    dport_opr dport_range     Grant
      1: 17      ef  0         [1, 65535]      7        [3000, 4000]    Permit

 Keys:  protocol dscp DstPort
```

Table 30 describes the significant fields shown in the display.

Table 30 show pfr border passive learn Field Descriptions

Field	Description
State is	Displays PfR prefix learning status: enabled or disabled.
Measurement type	Displays how the prefix is learned: throughput or delay.
Duration	Displays the duration of the learning period in minutes.
Aggregation type	Displays the aggregation type: BGP, non-BGP, or prefix-length.
No port protocol config	Indicates that no port protocol has been configured.
Traffic Class Filter List	Section showing the traffic-class filter parameters.
Traffic Class Aggregate List	Section showing the traffic-class aggregation parameters.
Keys	Parameters contained in the key list.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

show pfr border passive prefixes

To display information about passive monitored prefixes, use the **show pfr border passive prefixes** command in privileged EXEC mode.

show pfr border passive prefixes

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **show pfr border passive prefixes** command is entered on a border router. The output of this command displays prefixes that are monitored by NetFlow on the border router. The prefixes displayed in the output are monitored by the master controller.

Examples

The following example shows a prefix that is passively monitored by NetFlow:

```
Router# show pfr border passive prefixes

OER Passive monitored prefixes:

Prefix          Mask   Match Type
10.1.5.0        /24     exact
```

Table 31 describes the significant fields shown in the display.

Table 31 show pfr border passive prefixes Field Descriptions

Field	Description
Prefix	IP address of the learned prefix.
Mask	The prefix length as specified in a prefix mask.
Match Type	Type of prefix being monitored: exact or nonexact.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

show pfr border routes

To display information about Performance Routing (PfR) controlled routes, use the **show pfr border routes** command in privileged EXEC mode.

show pfr border routes {**bgp** | **cce** | **eigrp** [**parent**] | **rwatch** | **static**}

Syntax Descriptions

bgp	Displays information for PfR routes controlled by Border Gateway Protocol (BGP).
cce	Displays information for PfR routes controlled by Common Classification Engine (CCE).
eigrp	Displays information for PfR routes controlled by Enhanced Interior Gateway Routing Protocol (EIGRP).
parent	(Optional) Displays information for EIGRP parent routes.
rwatch	Displays information for PfR routes that are being watched in the Routing Information Base (RIB).
static	Displays information for PfR routes controlled by static routes.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **show pfr border routes** command is entered on a border router. This command is used to display information about PfR-controlled routes on a border router. You can display information about BGP or static routes.

The **show pfr border routes cce** command displays information about PfR-controlled traffic classes that are identified using Network-Based Application Recognition (NBAR).

Examples

The following example displays BGP-learned routes on a border router:

```
Router# show pfr border routes bgp

OER BR 10.1.1.2 ACTIVE, MC 10.1.1.3 UP/DOWN: UP 00:10:08,
   Auth Failures: 0
   Conn Status: SUCCESS, PORT: 3949
BGP table version is 12, local router ID is 10.10.10.2
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
*> 10.1.0.0/16      10.40.40.2      CE                0 400 600 i
```

Table 32 describes the significant fields shown in the display.

Table 32 show pfr border routes bgp Field Descriptions

Field	Description
C-Controlled	Indicates that the monitored prefix is currently under PfR control.
X-Excluded	Indicates that the monitored prefix is controlled by a different border router.
E - Exact	Indicates that an exact prefix is controlled, but more specific routes are not.
N - Non-exact	Indicates that the prefix and all more specific routes are under PfR control.
I - Injected	Indicates that the prefix is injected into the BGP routing table. If a less specific prefix exists in the BGP table and PfR has a more specific prefix configured, then BGP will inject the new prefix and PfR will flag it as I-Injected.
XN	Indicates that the prefix and all more specific prefixes are under the control of another border router, and, therefore, that this prefix is excluded. (Not shown in the example output.)
CNI	Indicates that the prefix is injected and that this prefix and all more specific prefixes are under PfR control.
CEI	Indicates that the specific prefix is injected and under PfR control.
CN	Indicates that the prefix and all more specific prefixes are under PfR control.
CE	Indicates that the specific prefix is under PfR control.
Network	The IP address and prefix mask.
Next Hop	The next hop of the prefix.
OER	Type of PfR control.
LocPrf	The BGP local preference value.
Weight	The weight of the route.
Path	The BGP path type.

The following example displays PfR-controlled routes that are identified using NBAR:

```
Router# show pfr border routes cce

Class-map oer-class-acl-oer_cce#2-stile-telnet, permit, sequence 0, mask 24
  Match clauses:
    ip address (access-list): oer_cce#2
    stile: telnet
  Set clauses:
    ip next-hop 10.1.3.2
    interface Ethernet2/3
  Statistic:
    Packet-matched: 60
```

Table 33 describes the significant fields shown in the display.

Table 33 show pfr border routes cce Field Descriptions

Field	Description
Class-map	Indicates the name of the PfR map used to control the PfR traffic classes.
Match clauses	Indicates the match criteria being applied to the traffic classes.
ip address (access-list)	Name of the access list used to match the destination prefixes of the controlled traffic classes identified using NBAR.
stile	Protocol being controlled.
Set clauses	Indicates the set criteria being applied to the matched traffic classes.
ip next-hop	IP address of the next hop to which the controlled traffic is sent. The next hop should be to a noncontrolling router.
interface	Interface name and number through which the controlled traffic is sent. If this is an ingress interface, the border router is not controlling the traffic classes. If this is an egress interface of the border router, the route is being controlled.
Statistic	Displays statistics such as number of packets matched.

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

```
Router# show pfr border routes eigrp

Flags: C - Controlled by oer, X - Path is excluded from control,
       E - The control is exact, N - The control is non-exact

Flags Network            Parent             Tag
CE    10.1.2.0/24        10.0.0.0/8         5000
```

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

```
Router# show pfr border routes eigrp parent

Network            Gateway            Intf       Flags
10.0.0.0/8         10.40.40.2         Ethernet4  1


Child Networks

Network            Flag
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

show pfr master

To display information about a Performance Routing (PfR) master controller, use the **show pfr master** command in privileged EXEC mode.

show pfr master

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **show pfr master** command is entered on a master controller. The output of this command displays information about the status of the PfR-managed network; the output includes information about the master controller, the border routers, PfR-managed interfaces, and default and user-defined policy settings.

Examples

The following example displays the status of a PfR-managed network on a master controller:

```
Router# show pfr master

OER state: ENABLED and ACTIVE
  Conn Status: SUCCESS, PORT: 3949
  Number of Border routers: 2
  Number of Exits: 2
  Number of monitored prefixes: 10 (max 5000)

Border           Status   UP/DOWN             AuthFail
10.4.9.7         ACTIVE   UP       02:54:40          0
10.4.9.6         ACTIVE   UP       02:54:40          0

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

Default Policy Settings:
  backoff 300 3000 300
  delay relative 50
  holddown 300
  periodic 0
  mode route control
  mode monitor both
  mode select-exit best
  loss relative 10
  unreachable relative 50
```

```
resolve delay priority 11 variance 20
  resolve utilization priority 12 variance 20

Learn Settings:
  current state : SLEEP
  time remaining in current state : 4567 seconds
  throughput
  delay
  no protocol
  monitor-period 10
  periodic-interval 20
  aggregation-type bgp
  prefixes 100
  expire after time 720
```

Table 34 describes the significant fields shown in the display.

Table 34 show pfr master Field Descriptions

Field	Description
OER state	Indicates the status of the master controller. The state will be either "Enabled" or "Disabled" and "Active" or "Inactive."
Conn Status	Indicates the state of the connection between the master controller and the border router. The state is displayed as "SUCCESS" to indicate a successful connection. The state is displayed as "CLOSED" if there is no connection.
PORT:	Displays the port number that is used for communication between the master controller and the border router.
Number of Border routers	Displays the number of border routers that peer with the master controller.
Number of Exits	Displays the number of exit interfaces under PfR control.
Number of monitored prefixes	Displays the number prefixes that are actively or passively monitored.
Border	Displays the IP address of the border router.
Status	Indicates the status of the border router. This field displays either "ACTIVE" or "INACTIVE."
UP/DOWN	Displays the connection status. The output displays "DOWN" or "UP." "UP" is followed by the length of time that the connection has been in this state.
AuthFail	Displays the number of authentication failures between the master controller and the border router.
Global Settings	Displays the configuration of global PfR master controller settings.
Default Policy Settings	Displays default PfR master controller policy settings.
Learn Settings	Display PfR learning settings.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

show pfr master active-probes

To display connection and status information about active probes on a Performance Routing (PfR) master controller, use the **show pfr master active-probes** command in privileged EXEC mode.

show pfr master active-probes [**appl** | **forced**]

Syntax Description

appl	(Optional) Filters the output display that active probes generate for application traffic configured with the PfR Application-Aware Routing: PBR feature.
forced	(Optional) Filters the output display that active probes generate for voice traffic configured with a forced target assignment.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **show pfr master active-probes** command is entered on a master controller. This command is used to display the status of active probes. 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. Entering the **appl** keyword filters the output to display information about applications optimized by the master controller. Entering the **forced** keyword filters the output to display information about voice traffic that is configured with a forced target assignment optimized by the master controller.

Examples

The following example shows the status of configured and running active probes:

```
Router# show pfr master active-probes

        OER Master Controller active-probes
Border   = Border Router running this Probe
State    = Un/Assigned to a Prefix
Prefix   = Probe is assigned to this Prefix
Type     = Probe Type
Target   = Target Address
TPort    = Target Port
How      = Was the probe Learned or Configured
N - Not applicable

State      Prefix             Type     Target          TPort How
Assigned   10.1.1.1/32        echo     10.1.1.1          N Lrnd
Assigned   10.1.4.0/24        echo     10.1.4.1          N Lrnd
Assigned   10.1.2.0/24        echo     10.1.2.1          N Lrnd
Assigned   10.1.4.0/24        udp-echo 10.1.4.1      65534 Cfgd
Assigned   10.1.3.0/24        echo     10.1.3.1          N Cfgd
Assigned   10.1.2.0/24        tcp-conn 10.1.2.1         23 Cfgd
```

```
The following Probes are running:

Border          State    Prefix             Type     Target          TPort
192.168.2.3     ACTIVE   10.1.4.0/24       udp-echo 10.1.4.1       65534
172.16.1.1      ACTIVE   10.1.2.0/24       tcp-conn 10.1.2.1         23
```

Table 35 describes the significant fields shown in the display.

Table 35 show pfr master active-probes Field Descriptions

Field	Description
The following Probes exist:	Displays the status of configured active probes.
State	Displays the status of the active probe. The output displays “Assigned” or “Unassigned.”
Prefix	Displays the prefix and prefix mask of the target active probe.
Type	Displays the type of active probe. The output displays “echo,” “jitter,” “tcp-conn,” or “udp-echo.”
Target	Displays the target IP address for the active probe.
TPort	Displays the target port for the active probe.
How	Displays how the active probe was created. The output will indicate the probe is configured or learned.
The following Probes are running:	Displays the status of active probes that are running.
Border	Displays the IP address of the border router.

The following example shows the status of configured and running active probes when a jitter probe has been configured:

```
Router# show pfr master active-probes

OER Master Controller active-probes
Border   = Border Router running this Probe
State    = Un/Assigned to a Prefix
Prefix   = Probe is assigned to this Prefix
Type     = Probe Type
Target   = Target Address
TPort    = Target Port
How      = Was the probe Learned or Configured
N - Not applicable

The following Probes exist:

State      Prefix            Type         Target      TPort How    codec
Assigned   10.1.1.0/24      jitter      10.1.1.10       2000 Cfgd g711ulaw
Assigned   10.1.1.0/24        echo       10.1.1.2          N Lrnd        N

The following Probes are running:

Border          State     Prefix            Type     Target          TPort
10.1.1.2         ACTIVE   10.1.1.0/24     jitter     10.1.1.10        2000
10.1.1.2         ACTIVE   10.1.1.0/24       echo     10.1.1.6            N
10.2.2.3         ACTIVE   10.1.1.0/24     jitter     10.1.1.10        2000
10.2.2.3         ACTIVE   10.1.1.0/24       echo     10.1.1.6            N
10.1.1.1         ACTIVE   10.1.1.0/24     jitter     10.1.1.10        2000
10.1.1.1         ACTIVE   10.1.1.0/24       echo     10.1.1.6            N
```

Table 36 describes the significant fields shown in the display that are different from those in Table 35 on page 194.

Table 36 show pfr master active-probes (jitter and MOS) Field Descriptions

Field	Description
codec	Displays the codec value configured for MOS calculation. Codec values can be one of the following: g711alaw, g711ulaw, or g729a.

Related Commands

Command	Description
active-probe (PfR)	Configures active probes to monitor a PfR-controlled prefixes.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

show pfr master appl

To display information about application traffic classes that are monitored and controlled by a Performance Routing (PfR) master controller, use the **show pfr master appl** command in privileged EXEC mode.

show pfr master appl [**access-list** *name*] [**detail**] [**learned** [**delay** | **throughput**]] | [**tcp** | **udp**] [*protocol-number*] [*min-port max-port*] [**dst** | **src**] [**detail** | **policy**]

Syntax Description

access-list *name*	(Optional) Filters the output based on the specified named extended access list.
detail	(Optional) Displays detailed information.
learned	(Optional) Displays information about learned application traffic classes.
delay	(Optional) Displays information about applications learned using delay as the learning criterion.
throughput	(Optional) Displays information about applications learned using throughput as the learning criterion.
tcp	(Optional) Filters the output based on TCP traffic.
udp	(Optional) Filters the output based on UDP traffic.
protocol-number	(Optional) Filters the output based on the specified protocol number.
min-port max-port	(Optional) Filters the output based on the specified port number or range of port numbers.
dst	(Optional) Filters the output based on the destination port number.
src	(Optional) Filters the output based on the source port number.
policy	(Optional) Displays the policy for the application or port number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **show pfr master appl** command is entered on a PfR master controller. This command is used to display information about application traffic classes that are configured for monitoring and optimization.

Examples

The following example shows TCP application traffic filtered based on port 80 (HTTP):

```
Router# show pfr master appl tcp 80 80 dst policy

Prefix             Appl Prot       Port                 Port Type       Policy
-------------------------------------------------------------------------------
10.1.0.0/16        tcp             [80, 80]             dst             20
10.1.1.0/24        tcp             [80, 80]             dst             10
```

Table 37 describes the significant fields shown in the display.

Table 37 show pfr master appl Field Descriptions

Field	Description
Prefix	IP address of the monitored prefix that carries the application traffic.
Appl Prot	Application protocol.
Port	Application port number.
Port Type	Source or destination application port number.
Policy	Application policy number.

The following example shows information about learned application traffic classes:

```
Router# show pfr master appl learned

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

Prefix                Prot Port [src][dst]              DSCP Source Prefix
                         State     Time Curr BR         CurrI/F         Proto
                       PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos
                       ActSDly  ActLDly   ActSUn   ActLUn      EBw      IBw
                       ActSJit  ActPMOS
------------------------------------------------------------------------------
10.1.1.0/24            udp [1, 65535] [3000, 4000]         ef 0.0.0.0/0
                      INPOLICY*      @70 1.1.1.2          Et0/0           PBR
                              U        U        0        0        0        0
                             11        7        0        0        1        0
                              N        N
10.1.3.0/24            udp [1, 65535] [3000, 4000]         ef 0.0.0.0/0
                      INPOLICY*      @70 1.1.1.2          Et0/0           PBR
                              U        U        0        0        0        0
                              3        4        0        0        1        0

                              N        N
```

Table 38 describes the significant fields shown in the display that are different from those in Table 37.

Table 38 show pfr master appl learned Field Descriptions

Field	Description
DSCP	Differentiated Services Code Point (DSCP) value.
Source Prefix	IP address of the application source.
State	Current state of the application traffic class flow.
Time	Time, in seconds, between probe messages.

Table 38 show pfr master appl learned Field Descriptions (continued)

Field	Description
Curr BR	IP address of the border router through which the prefix associated with this application traffic class is being currently routed.
CurrI/F	Interface of the border router through which the prefix associated with this application traffic class is being currently routed.
Proto	Protocol.

The following example shows information about application traffic classes learned using delay as the learning criterion:

```
Router# show pfr master appl learned delay

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

Prefix                Prot Port [src][dst]               DSCP Source Prefix
                        State     Time Curr BR          CurrI/F          Proto
                      PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos
                      ActSDly  ActLDly   ActSUn   ActLUn      EBw      IBw
                      ActSJit  ActPMOS
------------------------------------------------------------------------------

10.1.3.0/24            udp [1, 65535] [3000, 4000]         ef 0.0.0.0/0
                      INPOLICY*      @70 1.1.1.2          Et0/0           PBR
                             U        U        0         0        0        0
                             3        4        0         0        1        0
                             N        N
```

The following example shows information about application traffic classes learned using throughput as the learning criterion:

```
Router# show pfr master appl learned throughput

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

Prefix                Prot Port [src][dst]               DSCP Source Prefix
                        State     Time Curr BR           CurrI/F          Proto
                      PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos
                      ActSDly  ActLDly   ActSUn   ActLUn      EBw      IBw
                      ActSJit  ActPMOS
------------------------------------------------------------------------------
10.1.1.0/24            udp [1, 65535] [3000, 4000]         ef 0.0.0.0/0
                      INPOLICY*      @70 1.1.1.2          Et0/0           PBR
                             U        U        0        0        0        0
                            11        7        0        0        1        0
                             N        N
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

show pfr master border

To display the status of connected Performance Routing (PfR) border routers, use the **show pfr master border** command in privileged EXEC mode.

show pfr master border [*ip-address*] [**detail** | **report** | **topology**]

Syntax Description

ip-address	(Optional) Specifies the IP address of a single border router.
detail	(Optional) Displays detailed border router information.
report	(Optional) Displays link reports related to border routers.
topology	(Optional) Displays the status of the policy based routing (PBR) requirement.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **show pfr master border** command and all the keywords are entered on a master controller. The output of this command shows the status of connections with border routers.

Examples

The following example displays the status of border router connections with a master controller:

```
Router# show pfr master border

OER state: ENABLED and ACTIVE
  Conn Status: SUCCESS, PORT: 3949
  Version: 2.2
  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
  PBR Requirements met
  Nbar Status: Inactive

Border           Status   UP/DOWN             AuthFail  Version
10.165.201.5     ACTIVE   UP       00:05:29          0  2.2
10.165.201.6     ACTIVE   UP       00:05:29          0  2.2
10.165.201.7     ACTIVE   UP       00:05:29          0  2.2
```

Table 39 describes the significant fields shown in the display. All the other fields in the output are self-explanatory.

Table 39 show pfr master border Field Descriptions

Field	Description
Border	Displays the IP address of the border router.
Status	Displays the status of the border router:“ACTIVE” or “INACTIVE.”
UP/DOWN	Displays the connection status and the length of time that the connection has been up. The output displays “DOWN” or “UP.” The up time is displayed in weeks, days, hours, minutes, and seconds.
AuthFail	Displays the number of authentication failures between the master controller and the border router.
Version	Displays the version for all of the border routers configured on the master controller.

The following example displays detailed information about border router connections with a master controller:

```
Router# show pfr master border detail


Border          Status   UP/DOWN             AuthFail  Version
10.1.1.2        ACTIVE   UP       14:03:40          0  3.0
 Et2/0          EXTERNAL UP
 Et0/0          INTERNAL UP
 Et1/0          EXTERNAL UP

 External            Capacity      Max BW   BW Used    Load Status          Exit Id
 Interface             (kbps)       (kbps)    (kbps)    (%)
 ---------       --  --------      ------   -------    ---- ------          -------
 Et2/0           Tx       800         600       226      28 UP                   2
                 Rx                   800         0       0
 Et1/0           Tx       800         600        97      12 UP                   1
                 Rx                   800        55       6
```

Table 40 describes the significant fields shown in the display.

Table 40 show pfr master border detail Field Descriptions

Field	Description
Border	Displays the IP address of the border router.
Status	Displays the status of the border router:“ACTIVE” or “INACTIVE.”
UP/DOWN	Displays the connection status and the length of time that the connection has been up. The output displays “DOWN” or “UP.” The up time is displayed in weeks, days, hours, minutes, and seconds.
AuthFail	Displays the number of authentication failures between the master controller and the border router.
External Interface	Displays the external PfR controlled interface.
Tx	Displays the percentage of interface utilization in the outbound direction.
Rx	Displays the percentage of interface utilization in the inbound direction.
Capacity	Displays the capacity of the interface in kilobytes per second.

Table 40 show pfr master border detail Field Descriptions (continued)

Field	Description
Max BW	Displays the maximum usable bandwidth in kilobytes per second as configured on the interface.
BW Used	Displays the amount of bandwidth in use in kilobytes per second.
Load	Displays the amount of bandwidth in use as a percentage of the total capacity of the interface.
Status	Displays the status of the link.
Exit Id	Displays the ID number assigned by the master controller to identify the exit.

The following example displays whether the PBR requirement for the application control by PfR is met or not:

```
Router# show pfr master border topology

LocalBR         LocalEth          RemoteBR       RemoteEth      nbar_type
------------------------------------------------------------------------------
10.165.201.4    Ethernet0/0       10.165.202.2   Ethernet0/0    Directly Connected
10.165.201.4    Ethernet0/0       10.165.201.3   Ethernet0/0    Directly Connected
10.165.201.3    Ethernet0/0       10.165.201.4   Ethernet0/0    Directly Connected
10.165.201.3    Ethernet0/0       10.165.201.3   Ethernet0/0    Directly Connected
10.165.201.2    Ethernet0/0       10.165.201.4   Ethernet0/0    Directly Connected
10.165.201.2    Ethernet0/0       10.165.201.2   Ethernet0/0    Directly Connected
PBR Requirements met
```

Table 41 describes the significant fields shown in the display.

Table 41 show pfr master border topology Field Descriptions

Field	Description
LocalBR	Displays the local border router.
LocalEth	Displays the local interface connection for the local border router.
RemoteBR	Displays the remote border router that is connected with the local border router.
RemoteEth	Displays the remote interface connection for the remote border router.
nbar_type	Displays the type of NBAR connection for each of the border routers. Three types of connection status are available: Directly Connected, One-How-Away Neighbor, and Not Connected.

The following example displays the border router link report:

```
Router# show pfr master border report

Border          Status   UP/DOWN             AuthFail  Version
10.165.202.132  ACTIVE   UP       00:05:54          0  2.2
10.165.202.131  ACTIVE   UP       00:05:57          0  2.2
10.165.202.130  ACTIVE   UP       00:06:00          0  2.2
10.165.202.129  ACTIVE   UP       00:06:03          0  2.2
```

Table 42 describes the significant fields shown in the display.

Table 42 show pfr master border report Field Descriptions

Field	Description
Border	Displays the IP address of the border router.
Status	Displays the status of the border router:“ACTIVE” or “INACTIVE.”
UP/DOWN	Displays the connection status and the length of time that the connection has been up. The output displays “DOWN” or “UP.” The up time is displayed in weeks, days, hours, minutes, and seconds.
AuthFail	Displays the number of authentication failures between the master controller and the border router.
Status	Displays the status of the link.
Version	Displays the version for all of the border routers configured on the master controller.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

show pfr master cost-minimization

To display the status of cost-based optimization policies, use the **show pfr master cost-minimization** command in privileged EXEC mode.

show pfr master cost-minimization {**billing-history** | **border** *ip-address* [*interface*] | **nickname** *name*}

Syntax Description

billing-history	Deploys the billing history
border *ip-address*	Displays information for a single border router.
interface	(Optional) Displays information for only the specified interface.
nickname *name*	Displays information for the service provider. A nickname must be configured before output will be displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **show pfr master cost-minimization** command is entered on a master controller. The output of this command shows the status of cost-based policies.

Examples

The following example displays the billing history for cost policies:

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

Billing History for the past three months

        ISP2 on 10.1.1.2         Ethernet0/0
  80-percent on 10.1.1.1         Ethernet0/0
                Mon1                 Mon2                 Mon3
Nickname     SustUtil       Cost   SustUtil       Cost   SustUtil       Cost
----------    ------------------    ------------------   ------------------
      ISP2        ---NA---      1737222676 1737222676        ---NA---
80-percent        ---NA---      1737231684 1737231684        ---NA---

----------    ------------------    ------------------   ------------------
Total Cost                    0            3474454360                    0
```

Table 43 describes the significant fields shown in the display.

Table 43 show pfr master cost-minimization billing-history Field Descriptions

Field	Description
Nickname	The nickname assigned to the service provider.
SustUtil	The sustained utilization of the exit link.

Table 43 show pfr master cost-minimization billing-history Field Descriptions (continued)

Field	Description
Cost	The financial cost of the link.
Total Cost	The total financial cost for the month.

The following example displays cost optimization information only for Ethernet interface 1/0:

```
Router# show pfr master cost-minimization border 10.1.1.2 Ethernet1/0

 Nickname  : ispname          Border: 10.1.1.2         Interface: Et1/0
 Calc type : Combined
 Start Date: 20
 Fee       : Tier Based
             Tier1 : 100, fee: 10000
             Tier2 : 90, fee: 9000
 Period    : Sampling 22, Rollup 1400
 Discard   : Type Percentage, Value 22

 Rollup Information:
 Total           Discard         Left            Collected
 60              13              36              0

 Current Rollup Information:
   MomentaryTgtUtil:         7500 Kbps    CumRxBytes:             38669
  StartingRollupTgt:         7500 Kbps    CumTxBytes:             39572
   CurrentRollupTgt:         7500 Kbps    TimeRemain:          09:11:01

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

 1   : 0            2   : 0
```

Table 44 describes the significant fields shown in the display.

Table 44 show pfr master cost-minimization border Field Descriptions

Field	Description
Nickname	Nickname of the service provider.
Border	IP address of the border router.
Interface	Interface for which the cost policy is configured.
Calc type	Displays the configured billing method.
Start Date	Displays the starting date of the billing period.
Fee	Displays the billing type (fixed or tiered) and the billing configuration.
Period	Displays the sampling and rollup configuration.
Discard	Displays the discard configuration, type, and value.
Rollup Information	Displays rollup statistics.
Current Rollup Information	Displays rollup statistics for the current sampling cycle.
Rollup Utilization	Displays rollup utilization statistics in kilobytes per second.

The following example displays cost optimization information for the specified service provider:

```
Router# show pfr master cost-minimization nickname ISP1

 Nickname  : ISP1             Border: 10.1.1.2         Interface: Et1/0
 Calc type : Combined
 Start Date: 20
 Fee       : Tier Based
             Tier1 : 100, fee: 10000
             Tier2 : 90, fee: 9000
 Period    : Sampling 22, Rollup 1400
 Discard   : Type Percentage, Value 22

 Rollup Information:
 Total           Discard         Left            Collected
 60              13              36              0

 Current Rollup Information:
   MomentaryTgtUtil:         7500 Kbps    CumRxBytes:            38979
  StartingRollupTgt:         7500 Kbps    CumTxBytes:            39692
   CurrentRollupTgt:         7500 Kbps    TimeRemain:        09:10:49

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

 1   : 0           2   : 0
```

Related Commands

Command	Description
cost-minimization (PfR)	Configures cost-based optimization policies on a master controller.
debug pfr master cost-minimization	Displays debugging information for cost-based optimization policies.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

show pfr master defined application

To display information about user-defined application definitions on a Performance Routing (PfR) master controller, use the **show pfr master defined application** command in privileged EXEC mode.

show pfr master defined application

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **show pfr master defined application** command is entered on a PfR master controller. This command displays all applications that are user-defined. To define a custom application to be used by PfR, use the **application define** (PfR) command on the PfR master controller.

To display the same information on a PfR border router, use the **show pfr border defined application** command.

Examples

The following partial example output shows information about the user-defined applications configured for use with PfR:

```
Router# show pfr master defined application

OER Defined Applications:
Name                 Appl_ID Dscp Prot     SrcPort     DstPort SrcPrefix
-------------------------------------------------------------------------------
telnet                     1 defa  tcp       23-23     1-65535 0.0.0.0/0
telnet                     1 defa  tcp     1-65535       23-23 0.0.0.0/0
ftp                        2 defa  tcp       21-21     1-65535 0.0.0.0/0
ftp                        2 defa  tcp     1-65535       21-21 0.0.0.0/0
cuseeme                    4 defa  tcp   7648-7648     1-65535 0.0.0.0/0
cuseeme                    4 defa  tcp   7649-7649     1-65535 0.0.0.0/0
cuseeme                    4 defa  tcp     1-65535   7648-7648 0.0.0.0/0
dhcp                       5 defa  udp       68-68       67-67 0.0.0.0/0
dns                        6 defa  tcp       53-53     1-65535 0.0.0.0/0
dns                        6 defa  tcp     1-65535       53-53 0.0.0.0/0
dns                        6 defa  udp       53-53     1-65535 0.0.0.0/0
dns                        6 defa  udp     1-65535       53-53 0.0.0.0/0
finger                     7 defa  tcp       79-79     1-65535 0.0.0.0/0
finger                     7 defa  tcp     1-65535       79-79 0.0.0.0/0
gopher                     8 defa  tcp       70-70     1-65535 0.0.0.0/0
.
.
.
```

Table 45 describes the significant fields shown in the display.

Table 45 show pfr master defined application Field Descriptions

Field	Description
Name	Application name .
Appl_ID	Application ID.
Dscp	Differentiated Services Code Point (DSCP) value.
Prot	Protocol.
SrcPort	Source port number for the traffic class.
DstPort	Destination port number for the traffic class.
SrcPrefix	IP address of the traffic class source.

Related Commands

Command	Description
application define (PfR)	Defines a user-defined application to be monitored by PfR.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
show pfr border defined application	Displays information about user-defined application definitions used on a PfR border router.

show pfr master learn list

To display configuration information about Performance Routing (PfR) learn lists, use the **show pfr master learn list** command in privileged EXEC mode.

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

Syntax Description

list-name	(Optional) Name of a learn list.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **show pfr master learn list** command is entered on a PfR master controller. This command is used to display configuration information about learn lists. Learn lists are a way to categorize learned traffic classes. In each learn list, different criteria for learning traffic classes including prefixes, application definitions, filters, and aggregation parameters can be configured. A traffic class is automatically learned by PfR based on each learn list criteria, and each learn list is configured with a sequence number. The sequence number determines the order in which learn list criteria are applied. Learn lists allow different PfR policies to be applied to each learn list.

Examples

The following example shows how to display configuration information about two learn lists, LIST1 and LIST2:

```
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
```

Table 46 describes the significant fields shown in the display.

Table 46 show pfr master learn list Field Descriptions

Field	Description
Learn-List	Identifies the PfR learn list name and sequence number.
Application	Application protocol.
Aggregation-type	Type of TCF aggregation.
Learn type	Throughput or delay.
Policies assigned	Application policy number.
Application Count	Number of applications learned.
Application Learned	Type of application learned.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

show pfr master link-group

To display information about Performance Routing (PfR) link groups, use the **show pfr master link-group** command in privileged EXEC mode.

show pfr master link-group [*link-group-name*]

Syntax Description

link-group-name	(Optional) Name of a link group.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **show pfr master link-group** command is entered on a PfR master controller. This command is used to display information about link groups including the link group name, the border router, and the interface on the border router that is the exit link, and the ID of the exit link.

Link groups are used to define a group of exit links as a preferred set of links or as a fallback set of links for PfR to use when optimizing a specified traffic class. Up to three link groups can be specified for each interface. Use the **link-group** (PfR) command to define the link group for an interface, and use the **set link-group** (PfR) command to define the primary link group and a fallback link group for a specified traffic class in an PfR map.

Examples

The following example displays information about all configured link groups:

```
Router# show pfr master link-group

link group video
  Border           Interface       Exit id
  192.168.1.2      Serial2/0       1
 link group voice
  Border           Interface       Exit id
  192.168.1.2      Serial2/0       1
  192.168.1.2      Serial3/0       2
  192.168.3.2      Serial4/0       4
 link group data
  Border           Interface       Exit id
  192.168.3.2      Serial3/0       3
```

Table 47 describes the significant fields shown in the display.

Table 47 show pfr master link-group Field Descriptions

Field	Description
link group	Name of the link group.
Border	IP address of the border router on which the exit link exists.

Table 47 show pfr master link-group Field Descriptions (continued)

Field	Description
Interface	Type and number of the interface on the border router that is the exit link.
Exit id	ID number of the exit link.

The following example displays information only about the link group named voice:

```
Router# show pfr master link-group voice

link group voice
  Border           Interface       Exit id
  192.168.1.2      Serial2/0       1
  192.168.1.2      Serial3/0       2
  192.168.3.2      Serial4/0       4
```

Related Commands

Command	Description
link-group (PfR)	Configures a PfR border router exit interface as a member of a link group.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
set link-group (PfR)	Specifies a link group for traffic classes defined in a PfR policy.

show pfr master nbar application

To display information about the status of an application identified using Network-Based Application Recognition (NBAR) for each Performance Routing (PfR) border router, use the **show pfr master nbar application** command in privileged EXEC mode.

show pfr master nbar application

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **show pfr master nbar application** command is entered on a PfR master controller. This command is used to verify the validity of an application that is identified using NBAR at each PfR border router. If the NBAR application is not supported on one or more border routers, all the traffic classes related to that NBAR application are marked inactive and cannot be optimized using PfR.

NBAR is capable of identifying applications based on the following three types of protocols:

- Non-UDP and non-TCP IP protocols—For example, Generic Routing Encapsulation (GRE) and Internet Control Message Protocol (ICMP).
- TCP and UDP protocols that use statically assigned port numbers—For example, CU-SeeMe desktop video conference (CU-SeeMe-Server) and Post Office Protocol over Transport Layer Security (TLS) and Secure Sockets Layer (SSL) server (SPOP3-Server).
- TCP and UDP protocols that dynamically assign port numbers and require stateful inspection—For example, Real-Time Transport Protocol audio streaming (RTP-audio) and BitTorrent File Transfer Traffic (BitTorrent).

The list of applications identified using NBAR and available for profiling of PfR traffic classes is constantly evolving. For lists of many of the NBAR applications defined using static or dynamically assigned ports, see the "Performance Routing with NBAR/CCE Application Recognition" module.

For more details about NBAR, see the "Classifying Network Traffic Using NBAR" section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Examples

The following partial output shows information about the status of a number of applications identified using NBAR at three PfR border routers. In this example, applications based on BGP, BitTorrent, and HTTP protocols are valid at all three PfR border routers, and traffic classes for these applications are active. While applications such as ConnectionLess Network Service (CLNS) and KaZaA are invalid on at least one border router, all traffic classes based on these application are marked inactive.

```
Router# show pfr master nbar application
```

```
NBAR Appl                  10.1.1.4        10.1.1.2        10.1.1.3
-----------------------------------------------------------------------
aarp                        Invalid         Invalid         Invalid
appletalk                   Invalid         Invalid         Invalid
arp                         Invalid         Invalid         Invalid
bgp                           Valid           Valid           Valid
bittorrent                    Valid           Valid           Valid
bridge                      Invalid         Invalid         Invalid
bstun                       Invalid         Invalid         Invalid
cdp                         Invalid         Invalid         Invalid
citrix                      Invalid         Invalid         Invalid
clns                          Valid         Invalid         Invalid
clns_es                     Invalid         Invalid         Invalid
clns_is                     Invalid         Invalid         Invalid
cmns                        Invalid         Invalid         Invalid
compressedtcp               Invalid         Invalid         Invalid
cuseeme                     Invalid         Invalid         Invalid
decnet                      Invalid         Invalid         Invalid
decnet_node                 Invalid         Invalid         Invalid
decnet_router-l1            Invalid         Invalid         Invalid
decnet_router-l2            Invalid         Invalid         Invalid
dhcp                        Invalid         Invalid         Invalid
directconnect               Invalid         Invalid         Invalid
dlsw                        Invalid         Invalid         Invalid
dns                         Invalid         Invalid         Invalid
edonkey                     Invalid         Invalid         Invalid
egp                         Invalid         Invalid         Invalid
eigrp                       Invalid         Invalid         Invalid
exchange                    Invalid         Invalid         Invalid
fasttrack                   Invalid         Invalid         Invalid
finger                      Invalid         Invalid         Invalid
ftp                         Invalid         Invalid         Invalid
gnutella                    Invalid         Invalid         Invalid
Morpheus                    Invalid         Invalid         Invalid
gopher                      Invalid         Invalid         Invalid
gre                         Invalid         Invalid         Invalid
h323                        Invalid         Invalid         Invalid
http                          Valid           Valid           Valid
icmp                        Invalid         Invalid         Invalid
imap                        Invalid         Invalid         Invalid
ip                          Invalid         Invalid         Invalid
ipinip                      Invalid         Invalid         Invalid
ipsec                       Invalid         Invalid         Invalid
ipv6                        Invalid         Invalid         Invalid
ipx                         Invalid         Invalid         Invalid
irc                         Invalid         Invalid         Invalid
kazaa2                        Valid         Invalid           Valid
.
.
.
```

Table 48 describes the significant fields shown in the display.

Table 48 show pfr master nbar application Field Descriptions

Field	Description
NBAR Appl	Application name.
10.1.1.4	IP address of a PfR border router.
10.1.1.2	IP address of a PfR border router.
10.1.1.3	IP address of a PfR border router.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
show pfr master traffic-class application nbar	Displays information about application traffic classes that are identified using NBAR and that are monitored and controlled by a PfR master controller.

show pfr master policy

To display policy settings on a Performance Routing (PfR) master controller, use the **show pfr master policy** command in privileged EXEC mode.

show pfr master policy {*sequence-number* | *policy-name* | **default** | **dynamic**}

Syntax Description

sequence-number	Displays only the specified PfR map sequence.
policy-name	Displays only the specified PfR map name.
default	Displays the default policy information.
dynamic	Displays dynamic policy information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **show pfr master policy** command is entered on a master controller. The output of this command displays default policy and policies configured with a PfR map.

The PfR application provider interface (API) defines the mode of communication and messaging between applications and the network for the purpose of optimizing the traffic associated with the applications. A provider is defined as an entity outside the network in which the router configured as an PfR master controller exists, for example, an ISP, or a branch office of the same company. The provider has one or more host devices running one or more applications that use the PfR API to communicate with a PfR master controller. The PfR API allows applications running on a host device in the provider network to dynamically create policies to influence the existing traffic classes, or specify new traffic class criteria. The **dynamic** keyword displays the policies dynamically created by an API provider application.

Examples

The following example displays default policy and policies configured in a PfR map named CUSTOMER. The asterisk(*) character is displayed next to policy settings that override default settings.

```
Router# show pfr master policy

* Overrides Default Policy Setting

Default Policy Settings:
  backoff 300 3000 300
  delay relative 50
  holddown 300
  periodic 0
  mode route control
  mode monitor both
  mode select-exit best
  loss relative 10
  unreachable relative 50
```

```
  resolve delay priority 11 variance 20
  resolve utilization priority 12 variance 20
pfr-map CUSTOMER 10
  match ip prefix-lists: NAME
  backoff 300 3000 300
  delay relative 50
  holddown 300
  periodic 0
  mode route control
  mode monitor both
  mode select-exit best
  loss relative 10
  unreachable relative 50
 *resolve utilization priority 1 variance 10
 *resolve delay priority 11 variance 20
 *probe frequency 30
pfr-map CUSTOMER 20
  match ip prefix-lists:
  match pfr learn delay
  backoff 300 3000 300
  delay relative 50
  holddown 300
  periodic 0
 *mode route control
  mode monitor both
  mode select-exit best
  loss relative 10
  unreachable relative 50
  resolve delay priority 11 variance 20
  resolve utilization priority 12 variance 20
```

Table 49 describes the significant fields shown in the display.

Table 49 show pfr master policy Field Descriptions

Field	Description
Default Policy Settings:	Displays PfR default configuration settings under this heading.
pfr-map...	Displays the PfR map name and sequence number. The policy settings applied in the PfR map are displayed under this heading.

The following example displays dynamic policies created by applications using the PfR application interface. The asterisk(*) character is displayed next to policy settings that override default settings.

```
Router# show pfr master policy dynamic
Dynamic Policies:

  proxy id 10.3.3.3
  sequence no. 18446744069421203465, provider id 1001, provider priority 65535
    host priority 65535, policy priority 101, Session id 9
  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
next-hop not set
forwarding interface not set
resolve delay priority 11 variance 20
resolve utilization priority 12 variance 20

proxy id 10.3.3.3
sequence no. 18446744069421269001, provider id 1001, provider priority 65535
  host priority 65535, policy priority 102, Session id 9
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
next-hop not set
forwarding interface not set
resolve delay priority 11 variance 20
resolve utilization priority 12 variance 20

proxy id 10.3.3.4
sequence no. 18446744069421334538, provider id 1001, provider priority 65535
  host priority 65535, policy priority 103, Session id 10
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
next-hop not set
forwarding interface not set
resolve delay priority 11 variance 20
resolve utilization priority 12 variance 20
```

Table 50 describes the significant fields shown in the display.

Table 50 show pfr master policy dynamic Field Descriptions

Field	Description
Dynamic Policies:	Displays PfR dynamic policy configurations under this heading.
proxy id	IP address of the host application interface device that created the policy.
sequence no.	Number indicating the sequence in which the policy was run.
provider id	ID number of the application interface provider.

Table 50 show pfr master policy dynamic Field Descriptions (continued)

Field	Description
provider priority	The priority assigned to the application interface provider. If a priority has not been configured, the default priority is 65535.
host priority	The priority assigned to the host application interface device. If a priority has not been configured, the default priority is 65535.
policy priority	The priority assigned to the policy.
Session id	ID number of the application interface provider session.

Related Commands

Command	Description
api provider (PfR)	Registers an application interface provider with a PfR master controller and enters PfR master controller application interface provider configuration mode.
host-address (PfR)	Configures information about a host device used by an application interface provider to communicate with an PfR master controller.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

show pfr master prefix

To display the status of monitored prefixes, use the **show pfr master prefix** command in privileged EXEC mode.

show pfr master prefix [**detail** | **inside** [**detail**] | **learned** [**delay** | **inside** | **throughput**] | *prefix* [**detail** | **policy** | **report** | **traceroute** [*exit-id* | *border-address* | **current**] [**now**]]]

Syntax Description

detail	(Optional) Displays detailed prefix information about the specified prefix or all prefixes.
inside	(Optional) Displays detailed prefix information about inside prefixes.
learned	(Optional) Displays information about learned prefixes.
delay	(Optional) Displays information about learned prefixes based on delay.
throughput	(Optional) Displays information about learned prefixes based on throughput.
prefix	(Optional) Specifies the prefix, entered as an IP address and bit length mask.
policy	(Optional) Displays policy information for the specified prefix.
report	(Optional) Displays detailed performance information and information about report requests from Performance Routing (PfR) application interface providers for the specified prefix.
traceroute	(Optional) Displays path information from traceroute probes.
exit-id	(Optional) Displays path information based on the PfR assigned exit ID.
border-address	(Optional) Display path information sourced from the specified border router.
current	(Optional) Displays traceroute probe statistics from the most recent traceroute probe.
now	(Optional) Initiates a new traceroute probe and displays the statistics that are returned.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **show pfr master prefix** command is entered on a master controller. 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. The output can be filtered to display information for only a single prefix, learned prefixes, inside prefixes, and prefixes learned based on delay or throughput.

The **traceroute** keyword is used to display traceroute probe results. The output generated by this keyword provides hop by hop statistics to the probe target network. The output can be filtered to display information only for the exit ID (PfR assigns an ID number to each exit interface) or for the specified border router. The **current** keyword displays traceroute probe results from the most recent traceroute probe. The **now** keyword initiates a new traceroute probe and displays the results.

Examples

The following example shows the status of a monitored prefix:

```
Router# show pfr master prefix

OER Prefix Stats:
  Dly: Delay in ms
  EBw: Egress Bandwidth
  IBw: Ingress Bandwidth

Prefix      State     Curr BR   CurrI/F  Dly   EBw   IBw
------------------------------------------------------------
10.1.5.0/24 INPOLICY  10.1.1.2  Et1/0     19     1     1
```

Table 51 describes the significant fields shown in the display.

Table 51 show pfr master prefix Field Descriptions

Field	Description
Prefix	IP address and prefix length.
State	Status of the prefix.
Curr BR	Border router from which these statistics were gathered.
Curr I/F	Current exit link interface on the border router.
Dly	Delay in milliseconds.
EBw	Egress bandwidth.
IBw	Ingress bandwidth.

The following output shows the detailed status of a monitored prefix:

```
Router# show pfr master prefix detail

Prefix: 10.1.1.0/26
   State: DEFAULT*      Time Remaining: @7
   Policy: Default

   Policy: Default

   Most recent data per exit
   Border          Interface           PasSDly  PasLDly  ActSDly  ActLDly
  *10.2.1.1        Et1/0                   181      181      250      250
   10.2.1.2        Et2/0                     0        0      351      351
   10.3.1.2        Et3/0                     0        0       94      943

   Latest Active Stats on Current Exit:
   Type     Target          TPort Attem Comps      DSum     Min     Max     Dly
   echo     10.1.1.1            N     2     2       448     208     240     224
   echo     10.1.1.2            N     2     2       488     228     260     244
   echo     10.1.1.3            N     2     2       568     268     300     284

Prefix performance history records
```

```
 Current index 2, S_avg interval(min) 5, L_avg interval(min) 60

Age       Border          Interface       OOP/RteChg Reasons
Pas: DSum  Samples  DAvg  PktLoss Unreach    Ebytes    Ibytes      Pkts   Flows
Act: Dsum Attempts  DAvg    Comps Unreach
00:00:03  10.1.1.1        Et1/0
        0         0     0        0       0         0         0         0       0
     1504         6   250        6       0
```

Table 52 describes the significant fields shown in the display.

Table 52 show pfr master prefix detail Field Descriptions

Field	Description
Prefix	IP address and prefix length.
State	Status of the prefix.
Time Remaining	Time remaining in the current prefix learning cycle.
Policy	The state that the prefix is in. Possible values are Default, In-policy, Out-of-policy, Choose, and Holddown.
Most recent data per exit	Border router exit link statistics for the specified prefix. The asterisk (*) character indicates the exit that is being used.
Latest Active Stats on Current Exit	Active probe statistics. This field includes information about the probe type, target IP address, port number, and delay statistics.
Type	The type of active probe. Possible types are ICMP echo, TCP connect, or UDP echo. The example uses default ICMP echo probes (default TCP), so no port number is displayed.
Prefix performance history records	Displays border router historical statistics. These statistics are updated about once a minute and stored for 1 hour.

The following example shows prefix statistics from a traceroute probing:

```
Router# show pfr master prefix 10.1.5.0/24 traceroute

* - current exit, + - control more specific
Ex - Exit ID, Delay in msec
------------------------------------------------------------------------------

Path for Prefix: 10.1.5.0/24         Target: 10.1.5.2
Exit ID: 2, Border: 10.1.1.3         External Interface: Et1/0
Status: DONE, How Recent: 00:00:08 minutes old
Hop  Host            Time(ms) BGP
1    10.1.4.2        8        0
2    10.1.3.2        8        300
3    10.1.5.2        20       50
------------------------------------------------------------------------------
Exit ID: 1, Border: 10.1.1.2         External Interface: Et1/0
Status: DONE, How Recent: 00:00:06 minutes old
Hop  Host            Time(ms) BGP
1    0.0.0.0         3012     0
2    10.1.3.2        12       100
3    10.1.5.2        12       50
------------------------------------------------------------------------------
```

Table 53 describes the significant fields shown in the display.

Table 53 show pfr master prefix traceroute Field Descriptions

Field	Description
Path for Prefix	Specified IP address and prefix length.
Target	Traceroute probe target.
Exit ID	PfR assigned exit ID.
Status	Status of the traceroute probe.
How Recent	Time since last traceroute probe.
Hop	Hop number of the entry.
Host	IP address of the entry.
Time	Time, in milliseconds, for the entry.
BGP	BGP autonomous system number for the entry.

The following example shows prefix statistics including Jitter and MOS percentage values when the Jitter probe is configured for the 10.1.5.0 prefix:

```
Router# show pfr master prefix 10.1.5.0/24

OER Prefix Statistics:
 Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
 P - Percentage below threshold, Jit - Jitter, 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                  State     Time Curr BR         CurrI/F         Protocol
                      PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos
                      ActSDly  ActLDly   ActSUn   ActLUn      EBw      IBw
                     %ActSJit %ActPMOS
--------------------------------------------------------------------------------
10.1.1.0/24          DEFAULT*       @3 10.1.1.1         Et5/0           U
                            U        U        0        0        0        0
                            6        6   400000   400000       17        1
                         1.45       25
```

Table 54 describes the significant fields shown in the display that are different from Table 51 on page 221 and Table 52 on page 222.

Table 54 show pfr master prefix (Jitter and MOS) Field Descriptions

Field	Description
Protocol	Protocol: U (UDP).
PasSDly	Delay, in milliseconds, in short-term statistics from passive probe monitoring. If no statistics are reported, it displays U for unknown.
PasLDly	Delay, in milliseconds, in long-term statistics from passive probe monitoring. If no statistics are reported, it displays U for unknown.
PasSUn	Number of passively monitored short-term unreachable packets in flows-per-million.
PasLUn	Number of passively monitored long-term unreachable packets in flows-per-million.

Table 54 show pfr master prefix (Jitter and MOS) Field Descriptions (continued)

Field	Description
PasSLos	Number of passively monitored short-term lost packets in packets-per-million.
PasLLos	Number of passively monitored long-term lost packets in packets-per-million.
ActSDly	Number of actively monitored short-term delay packets.
ActLDly	Number of actively monitored long-term delay packets.
ActSUn	Number of actively monitored short-term unreachable packets in flows-per-million.
ActLUn	Number of actively monitored long-term unreachable packets in flows-per-million.
ActSJit	Number of actively monitored short-term jitter packets.
ActPMOS	Number of actively monitored MOS packets with a percentage below threshold.

The following example shows detailed prefix statistics when Jitter or MOS are configured as a priority:

```
Router# show pfr master prefix 10.1.1.0/24 detail

Prefix: 10.1.1.0/24
   State: DEFAULT*    Time Remaining: @9
   Policy: Default

   Most recent data per exit
   Border          Interface         PasSDly  PasLDly  ActSDly  ActLDly
  *10.1.1.1        Et5/0                   0        0        6        6
   10.2.2.3        Et2/0                   0        0        7        7
   10.1.1.2        Et0/0                   0        0       14       14

   Most recent voice data per exit
   Border          Interface         ActSJit  ActPMOS
  *10.1.1.1        Et5/0                2.00        0
   10.2.2.3        Et2/0                2.01       20
   10.1.1.2        Et0/0                4.56       50

   Latest Active Stats on Current Exit:
   Type     Target          TPort Attem Comps    DSum     Min     Max     Dly
   udpJit   10.1.1.8         2000     2     2       8       4       4       4
   udpJit   10.1.1.7         3000     2     2      20       4      16      10
   udpJit   10.1.1.6         4000     2     2       8       4       4       4
   echo     10.1.1.4            N     2     0       0       0       0       0
   echo     10.1.1.3            N     2     0       0       0       0       0

Latest Voice Stats on Current Exit:
   Type     Target          TPort     Codec Attem Comps  JitSum     MOS
   udpJit   10.1.1.8         2000  g711alaw     2     2    2.34    4.56
   udpJit   10.1.1.7         3000  g711ulaw     2     2    2.56    4.11
   udpJit   10.1.1.6         4000     g729a     2     2    1.54    3.57
   udpJit   10.1.1.5         4500      none     2     2    1.76      NA

Prefix performance history records
 Current index 3, S_avg interval(min) 5, L_avg interval(min) 60

Age       Border          Interface       OOP/RteChg Reasons
Pas: DSum  Samples  DAvg  PktLoss  Unreach   Ebytes   Ibytes     Pkts    Flows
Act: Dsum Attempts  DAvg    Comps  Unreach   Jitter LoMOSCnt    MOSCn
00:00:07  10.1.1.1        Et5/0
        0        0     0        0        0     5920        0      148        1
       36       10     6        6        4        2        1        1
```

```
00:01:07  10.1.1.1         Et5/0
        0         0      0         0         0    12000    12384       606        16
       36        10      6         6         4        3        0         1
00:02:07  10.1.1.1         Et5/0
        0         0      0         0         0   409540    12040       867         9
       36        10      6         6         4       15        1         1
```

Table 55 describes the significant fields shown in the display that are different from Table 52 on page 222.

Table 55 show pfr master prefix detail (Jitter or MOS Priority) Field Descriptions

Field	Description
Codec	Displays the codec value configured for MOS calculation. Codec values can be one of the following: g711alaw, g711ulaw, or g729a.
JitSum	Summary of jitter.
MOS	MOS value.
Jitter	Jitter value.
LoMOSCnt	MOS-low count.

The following example shows prefix statistics including information about application interface provider report requests for the 10.1.1.0 prefix:

```
Router# show pfr master prefix 10.1.1.0/24 report

Prefix Performance Report Request
   Created by: Provider 1001, Host 10.3.3.3, Session 9
   Last report sent 3 minutes ago, context 589855, frequency 4 min

Prefix Performance Report Request
   Created by: Provider 1001, Host 10.3.3.4, Session 10
   Last report sent 1 minutes ago, context 655372, frequency 3 min

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

Prefix                  State     Time Curr BR         CurrI/F         Protocol
                     PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos
                     ActSDly  ActLDly   ActSUn   ActLUn      EBw      IBw
                     ActSJit  ActPMOS  ActSLos  ActLLos
------------------------------------------------------------------------------
10.1.1.0/24             INPOLICY        0 10.3.3.3        Et4/3           BGP
                               N        N        N        N        N        N
                             138      145        0        0        N        N
                               N        N
```

Table 56 describes the significant fields shown in the display that are different from Table 51 on page 221, Table 53 on page 223 and Table 55 on page 225.

Table 56 show pfr master prefix report Field Descriptions

Field	Description
Provider	Application interface provider ID.
Host	IP address of a host device in the application interface provider network.
Session	Session number automatically allocated by PfR when an application interface provider initiates a session.
Last report sent	The number of minutes since a report was sent to the application interface provider.
ActSLos	Number of actively monitored short-term lost packets in packets-per-million.
ActLDly	Number of actively monitored long-term lost packets in packets-per-million.

PIRO provides the ability for PfR to search for a parent route—an exact matching route, or a less specific route—in any IP Routing Information Base (RIB). The following example shows that the protocol displayed for the prefix 10.1.0.0 is RIB-PBR, which means that the parent route for the traffic class exists in the RIB and policy-based routing is used to control the prefix.

```
Router# show pfr master prefix 10.1.0.0

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

Prefix                  State     Time Curr BR         CurrI/F         Protocol
                      PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos
                      ActSDly  ActLDly   ActSUn   ActLUn      EBw      IBw
                      ActSJit  ActPMOS  ActSLos  ActLLos
------------------------------------------------------------------------------
10.1.0.0/24          INPOLICY        0 10.11.1.3       Et1/0           RIB-PBR
                          129      130        0        0      214      473
                            U        U        0        0       33        3
                            N        N
```

EIGRP route control provides the ability for PfR to search for a parent route—an exact matching route, or a less specific route—in the EIGRP routing table. In this example, the protocol displayed for the prefix 10.1.0.0 is EIGRP and this means that the parent route for the traffic class exists in the EIGRP routing table and OER is controlling the prefix.

```
Router# show pfr master prefix 10.1.0.0

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

```
 # - Prefix monitor mode is Special, & - Blackholed Prefix
 % - Force Next-Hop, ^ - Prefix is denied

Prefix                  State     Time Curr BR         CurrI/F         Protocol
                      PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos
                      ActSDly  ActLDly   ActSUn   ActLUn      EBw      IBw
                      ActSJit  ActPMOS
------------------------------------------------------------------------------
10.1.0.0/16           DEFAULT*      @69 10.1.1.1        Gi1/22          EIGRP
                            U        U        0        0        0        0
                            U        U        0        0       22        8
                            N        N
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
set traceroute reporting (PfR)	Configures an PfR map to enable traceroute reporting.
traceroute probe-delay (PfR)	Sets the time interval between traceroute probe cycles.

show pfr master traffic-class

To display information about traffic classes that are monitored and controlled by a Performance Routing (PfR) master controller, use the **show pfr master traffic-class** command in privileged EXEC mode.

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**]

Syntax Description

access-list	(Optional) Displays information about traffic classes defined by an access list.
access-list-name	(Optional) Name of an access list. Names cannot contain either a space or quotation marks and must begin with an alphabetic character to distinguish them from numbered access lists.
application	(Optional) Displays information about application traffic classes.
application-name	(Optional) Name of a predefined static application using fixed ports. See Table 57.
prefix	(Optional) An IP address and bit length mask representing a prefix to be cleared.
inside	(Optional) Displays information about inside traffic classes.
learned	(Optional) Displays information about learned traffic classes.
delay	(Optional) Displays information about learned traffic classes defined using delay.
list	(Optional) Displays information about learned traffic classes defined in a PfR learn list.
list-name	(Optional) Name of an PfR learn list.
throughput	(Optional) Displays information about learned traffic classes defined using throughput.
prefix	(Optional) Displays information about traffic classes defined by a specified destination prefix.
prefix-list	(Optional) Displays information about traffic classes defined by a prefix list.
prefix-list-name	(Optional) Name of a prefix list. Names cannot contain either a space or quotation marks and must begin with an alphabetic character to distinguish them from numbered access lists.
active	(Optional) Displays active performance monitoring information only.
passive	(Optional) Displays passive performance monitoring information only.
status	(Optional) Displays status information only.
detail	(Optional) Displays detailed information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **show pfr master traffic-class** command is entered on an PfR master controller. This command is used to display information about traffic classes that are configured for monitoring and optimization. The **traffic-class** and **match traffic-class** commands simplify the learning of traffic classes. Four types of traffic classes can be automatically learned using a **traffic-class** command in a learn list, or manually configured using a **match traffic-class** command in a PfR map:

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

If none of the **active**, **passive**, or **status** keywords is specified, then the output will display the active, passive, and status information for the traffic classes. To restrict the amount of output, you can specify one or two of the **active**, **passive**, or **status** keywords, but the order of the keywords is important. If you specify the **active** keyword first then the **passive** or **status** keywords can be entered, if you specify the **passive** keyword first, then only the **status** keyword can be entered. The **status** keyword can be entered only by itself; the **active** and **passive** keywords are not accepted if they follow the **status** keyword. The optional **detail** keyword will display detailed output for the traffic classes.

To display information about traffic classes identified using NBAR, use the **show pfr master traffic-class application nbar** command.

Table 57 displays the keywords that represent the application that can be configured with the **show pfr master traffic-class** command. Replace the *application-name* argument with the appropriate keyword from the table.

Table 57 Static Application List Keywords

Keyword	Protocol	Port
cuseeme	TCP/UDP	7648 7649 7648 7649 24032
dhcp (Client)	UDP/TCP	68
dhcp (Server)	UDP/TCP	67
dns	UDP/TCP	53
finger	TCP	79
ftp	TCP	20 21
gopher	TCP/UDP	70
http	TCP/UDP	80
httpssl	TCP	443
imap	TCP/UDP	143 220
irc	TCP/UDP	194
kerberos	TCP/UDP	88 749
l2tp	UDP	1701
ldap	TCP/UDP	389

Table 57 Static Application List Keywords (continued)

Keyword	Protocol	Port
mssql	TCP	1443
nfs	TCP/UDP	2049
nntp	TCP/UDP	119
notes	TCP/UDP	1352
ntp	TCP/UDP	123
pcany	UDP TCP	22 5632 65301 5631
pop3	TCP/UDP	110
pptp	TCP	17233
simap	TCP/UDP	585 993 (Preferred)
sirc	TCP/UDP	994
sldap	TCP/UDP	636
smtp	TCP	25
snntp	TCP/UDP	563
spop3	TCP/UDP	123
ssh	TCP	22
telnet	TCP	23

Examples

The following example shows information about traffic classes destined for the 10.1.1.0/24 prefix:

```
Router# show pfr master traffic-class

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

DstPrefix                   Appl_ID Dscp Prot     SrcPort     DstPort SrcPrefix
          Flags              State     Time            CurrBR  CurrI/F Protocol
         PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos      EBw      IBw
         ActSDly  ActLDly   ActSUn   ActLUn  ActSJit  ActPMOS  ActSLos  ActLLos
-------------------------------------------------------------------------------
10.1.1.0/24               N defa    N           N           N N
               #          OOPOLICY       32         10.11.1.3    Et1/0      BGP
               N        N        N        N        N        N        N      IBwN
             130      134        0        0        N        N
```

The following example of the **show pfr master traffic-class** command with the **inside** keyword shows information about traffic classes:

```
Router# show pfr master traffic-class inside

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 (inside)  Appl_ID Dscp Prot     SrcPort     DstPort SrcPrefix
           Flags             State     Time            CurrBR  CurrI/F Protocol
         PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos      EBw      IBw
         ActSDly  ActLDly   ActSUn   ActLUn  ActSJit  ActPMOS  ActSLos  ActLLos
-------------------------------------------------------------------------------
10.0.0.0/16               N    N    N           N           N N
                          DEFAULT*        0                 U                 U
```

Table 58 describes the significant fields shown in the display.

Table 58 show pfr master traffic-class Field Descriptions

Field	Description
DstPrefix	Destination IP address and prefix length for the traffic class.
Appl_ID	Application ID.
Dscp	Differentiated Services Code Point (DSCP) value.
Prot	Protocol.
SrcPort	Source port number for the traffic class.
DstPort	Destination port number for the traffic class.
SrcPrefix	IP address of the traffic class source.
Flags	Special characteristics for the traffic class.
State	Current state of the traffic class.
Time	Time, in seconds, between monitoring messages.
Curr BR	IP address of the border router through which this traffic class is being currently routed.
CurrI/F	Interface of the border router through which this traffic class is being currently routed.
Protocol	Protocol. A value of U means unknown; there is no measurement data.
PasSDly	Passive monitoring short term delay in milliseconds.
PasLDly	Passive monitoring long term delay in milliseconds.
PasSUn	Number of passively monitored short-term unreachable packets in flows per million.
PasLUn	Number of passively monitored long-term unreachable packets in flows per million.
PasSLos	Number of passively monitored short-term lost packets in packets per million.

Table 58 show pfr master traffic-class Field Descriptions (continued)

Field	Description
PasLLos	Number of passively monitored long-term lost packets in packets per million.
EBw	Egress bandwidth.
IBw	Ingress bandwidth.
ActSDly	Active monitoring short-term delay in milliseconds.
ActLDly	Active monitoring long-term delay in milliseconds.
ActSUn	Number of actively monitored short-term unreachable packets in flows per million.
ActLUn	Number of actively monitored long-term unreachable packets in flows per million.
ActSJit	Number of actively monitored short-term jitter packets.
ActPMOS	Number of actively monitored Mean Opinion Score (MOS) packets with a percentage below threshold.
ActSLos	Number of actively monitored short-term packets lost.
ActLLos	Number of actively monitored long-term packets lost.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
show pfr master traffic-class application nbar	Displays information about application traffic classes that are identified using NBAR and are monitored and controlled by an PfR master controller.

show pfr master traffic-class application nbar

To display information about application traffic classes that are identified using Network-Based Application Recognition (NBAR) and are monitored and controlled by a Performance Routing (PfR) master controller, use the **show pfr master traffic-class application nbar** command in privileged EXEC mode.

show pfr master traffic-class application nbar *nbar-appl-name* [*prefix*] [[**active passive status**] | **detail**]

Syntax Description

nbar-appl-name	Name of a dynamic application identified using NBAR. See the Usage Guidelines section for more details.
prefix	(Optional) An IP address and bit length mask representing a prefix.
active	(Optional) Displays active performance monitoring information only.
passive	(Optional) Displays passive performance monitoring information only.
status	(Optional) Displays status information only.
detail	(Optional) Displays detailed information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **show pfr master traffic-class application nbar** command is entered on a PfR master controller. This command is used to display information about application traffic classes that are identified using NBAR. To display information about traffic classes defined using static application mapping, use the **show pfr master traffic-class** command.

The optional **detail** keyword will display detailed output for the NBAR application traffic classes. If the **detail** keyword is not specified, and if none of the **active**, **passive**, or **status** keywords is specified, then the output will display the active, passive, and status information for the traffic classes. To restrict the amount of output, specify just one or two of the **active**, **passive**, or **status** keywords. If specified, the **active**, **passive**, or **status** keywords must be specified in the order shown in the syntax.

NBAR is capable of identifying applications based on the following three types of protocols:

- Non-UDP and Non-TCP IP protocols—For example, Generic Routing Encapsulation (GRE), and Internet Control Message Protocol (ICMP).
- TCP and UDP protocols that use statically assigned port numbers—For example, CU-SeeMe desktop video conference (CU-SeeMe-Server) and Post Office Protocol over Transport Layer Security (TLS) and Secure Sockets Layer (SSL) server (SPOP3-Server).
- TCP and UDP protocols that dynamically assign port numbers and require stateful inspection—For example, Real-Time Transport Protocol audio streaming (RTP-audio) and BitTorrent File Transfer Traffic (BitTorrent).

The list of applications identified using NBAR and available for profiling PfR traffic classes is constantly evolving. For lists of many of the NBAR applications defined using static or dynamically assigned ports, see the "Performance Routing with NBAR/CCE Application Recognition" module.

For more details about NBAR, see the "Classifying Network Traffic Using NBAR" section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

If the *prefix* argument is specified, only the PfR-controlled traffic class that matches the application specified by the *nbar-appl-name* argument and the destination prefix specified by the *prefix* argument are displayed. If the *prefix* argument is not specified, all PfR-controlled traffic classes that match the application specified by the *nbar-appl-name* argument, regardless of the destination prefix, are displayed.

Examples

The following example shows information about traffic classes consisting of Real-time Transport Protocol streaming audio (RTP-audio) traffic:

```
Router# show pfr master traffic-class application nbar rtp-audio

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      EBw      IBw
         ActSDly  ActLDly   ActSUn   ActLUn  ActSJit  ActPMOS
------------------------------------------------------------------------------
100.1.1.0/28        RTP-Audio defa    N           N           N 0.0.0.0/0
                            DEFAULT*      461         101.1.1.2    Et1/0        U
              U         U         0         0         1         2
            150       130         0         0        15         0

100.1.1.16/28       RTP-Audio defa    N           N           N 0.0.0.0/0
                            DEFAULT*      461         101.1.1.2    Et1/0        U
              U         U         0         0         1         2
            250       200         0         0        30         0
```

Table 59 describes the significant fields shown in the display.

Table 59 show pfr master traffic-class Field Descriptions

Field	Description
DstPrefix	Destination IP address and prefix length for the traffic class.
Appl_ID	Application ID. The application can be a static application or an NBAR identified application.
Dscp	Differentiated Services Code Point (DSCP) value.
Prot	Protocol.
SrcPort	Source port number for the traffic class.
DstPort	Destination port number for the traffic class.

Table 59 show pfr master traffic-class Field Descriptions (continued)

Field	Description
SrcPrefix	IP address of the traffic class source.
Flags	Special characteristics for the traffic class, see the key above for details.
State	Current state of the traffic class.
Time	Time, in seconds, between monitoring messages.
Curr BR	IP address of the border router through which this traffic class is being currently routed.
CurrI/F	Interface of the border router through which this traffic class is being currently routed.
Protocol	Protocol. If the traffic class is being controlled by PfR this field displays on of the following: BGP, STATIC, or CCE. A value of U means unknown; PfR is not controlling the traffic class.
PasSDly	Passive monitoring short term delay in milliseconds.
PasLDly	Passive monitoring long term delay in milliseconds.
PasSUn	Number of passively monitored short term unreachable packets in flows-per-million.
PasLUn	Number of passively monitored long term unreachable packets in flows-per-million.
PasSLos	Number of passively monitored short term lost packets in packets-per-million.
PasLLos	Number of passively monitored long term lost packets in packets-per-million.
EBw	Egress bandwidth.
IBw	Ingress bandwidth.
ActSDly	Active monitoring short term delay in milliseconds.
ActLDly	Active monitoring long term delay in milliseconds.
ActSUn	Number of actively monitored short term unreachable packets in flows-per-million.
ActLUn	Number of actively monitored long term unreachable packets in flows-per-million.
ActSJit	Number of actively monitored short term jitter packets.
ActPMOS	Number of actively monitored Mean Opinion Score (MOS) packets with a percentage below threshold.

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
show pfr master traffic-class	Displays information about traffic classes that are monitored and controlled by an PfR master controller.

show pfr proxy

To display Performance Routing (PfR) proxy information, use the **show pfr proxy** command in privileged EXEC mode.

show pfr proxy

Syntax Description

This command has no arguments or keywords.

Command Default

No debugging messages are enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The show pfr proxy command is entered on a master controller. This command is used to display IP address information and connection status of a PfR proxy.

Examples

The following is sample output from the **show pfr proxy** command:

```
Router# show pfr proxy

OER PROXY 0.0.0.0 DISABLED, MC 0.0.0.0 UP/DOWN: DOWN
  Conn Status: NOT OPEN, Port 3949
```

Table 60 describes the significant fields shown in the display.

Table 60 show pfr proxy Field Descriptions

Field	Description
OER PROXY	Displays the IP address and status of the PfR proxy.
MC	Displays the IP address of the master controller (MC).
UP/DOWN:	Displays the connection status — UP or DOWN.
Conn Status:	Displays the connection status — OPEN or NOT OPEN.
Port	Displays the TCP port number used to communicate with the master controller.

Related Commands

Command	Description
show pfr api	Displays information about PfR application interface clients.

shutdown (PfR)

To stop a Performance Routing (PfR) master controller or PfR border router process without removing the PfR process configuration, use the **shutdown** command in PfR master controller or PfR border router configuration mode. To start a stopped PfR process, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

No master controller or border router is stopped.

Command Modes

PfR master controller configuration (config-pfr-mc)
PfR border router configuration (config-pfr-br)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **shutdown** command is entered on a master controller or border router. Entering the **shutdown** command stops an active master controller or border router process but does not remove any configuration parameters. The **shutdown** command is displayed in the running configuration file when enabled. To disable a master controller or border router and completely remove the process configuration from the running configuration file, use the **no pfr master** or **no pfr border** command in global configuration mode.

Cisco IOS XE Release 3.1S

This command is supported only in PfR border router configuration mode.

Examples

The following example stops an active PfR border router session:

```
Router(config)# pfr border
Router(config-pfr-br)# shutdown
```

The following example starts an inactive PfR master controller session:

```
Router(config)# pfr master
Router(config-pfr-mc)# no shutdown
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

throughput (PfR)

To configure Performance Routing (PfR) to learn the top prefixes based on the highest outbound throughput, use the **throughput** command in Top Talker and Top Delay learning configuration mode or learn list configuration mode. To disable learning based on outbound throughput, use the **no** form of this command.

throughput

no throughput

Syntax Description

This command has no arguments or keywords.

Command Default

No prefixes are learned based on outbound throughput.

Command Modes

PfR Top Talker and Top Delay learning configuration (config-pfr-mc-learn)
Learn list configuration (config-pfr-mc-learn-list)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **throughput** command is entered on a master controller. The master controller creates a list of prefixes based on the highest outbound throughput. This command is used to configure a master controller to learn prefixes based on the highest outbound packet throughput. When this command is enabled, PfR will learn the top prefixes across all border routers according to the highest outbound throughput.

Examples

Top Talker and Top Delay Learning Configuration Mode

The following example shows how to configure a master controller to learn the top prefixes based on the highest outbound throughput:

```
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# throughput
```

Learn List Configuration Mode

The following example shows how to configure a master controller to learn top prefixes based on the highest throughput for a learn list named LEARN_REMOTE_LOGIN_TC that learns Telnet and Secure Shell (SSH) application TCF entries:

```
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# list seq 10 refname LEARN_REMOTE_LOGIN_TC
Router(config-pfr-mc-learn-list)# traffic-class application telnet ssh
```

```
Router(config-pfr-mc-learn-list)# aggregation-type prefix-length 24
Router(config-pfr-mc-learn-list)# throughput
```

Related Commands

Command	Description
learn (PfR)	Enters PfR Top Talker and Top Delay learning configuration mode to configure prefixes for PfR to learn.
list (PfR)	Creates a PfR learn list to specify criteria for learning traffic classes and enters learn list configuration mode.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

traceroute probe-delay (PfR)

To set the time interval between traceroute probe cycles, use the **traceroute probe-delay** command in Performance Routing (PfR) master controller configuration mode. To set the interval between probes to the default value, use the **no** form of this command.

traceroute probe-delay *milliseconds*

no traceroute probe-delay

Syntax Description

milliseconds	Configures the time interval, in milliseconds, between traceroute probes. The configurable range for this argument is a number from 0 to 65535.

Command Default

The default time interval between traceroute probes is 10,000 milliseconds when this command is not configured or when the **no** form is entered.

Command Modes

PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **traceroute probe-delay** command is entered on a master controller. This command is used to set the delay interval between traceroute probes.

Continuous and policy-based traceroute reporting is configured with the **set traceroute reporting** (PfR) command. The time interval between traceroute probes is configured with the **traceroute probe-delay** command in PfR master controller configuration mode. On-demand traceroute probes are triggered by entering the **show pfr master prefix** (PfR) command with the **current** and **now** keywords.

Examples

The following example, which starts in global configuration mode, sets the delay interval between traceroute probes to 10000 milliseconds:

```
Router(config)# pfr master
Router(config-pfr-mc)# traceroute probe-delay 10000
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
set traceroute reporting (PfR)	Configures a PfR map to enable traceroute reporting.
show pfr master prefix (PfR)	Displays the status of monitored prefixes.

traffic-class access-list (PfR)

To define a Performance Routing (PfR) application traffic class using an access list applied to learned traffic flows, use the **traffic-class access-list** command in learn list configuration mode. To disable the definition of PfR-learned traffic flows into application traffic classes using an access list, use the **no** form of this command.

traffic-class access-list *access-list-name* [**filter** *prefix-list-name*]

no traffic-class access-list

Syntax Description

access-list-name	Name of an access list. Names cannot contain either a space or quotation marks and must begin with an alphabetic character to distinguish them from numbered access lists.
filter	(Optional) Specifies that the traffic flows are filtered on the basis of a prefix list.
prefix-list-name	(Optional) Name of a prefix list (created using the **ip prefix-list** command).

Command Default

PfR application traffic classes are not defined using an access list.

Command Modes

Learn list configuration (config-pfr-mc-learn-list)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **traffic-class access-list** command is used to configure the master controller to automatically learn application traffic defined in an access list. Only one access list can be specified, but the access list may contain many access list entries (ACEs) to help define the traffic class parameters.

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

Note The **traffic-class access-list** command, the **traffic-class application** command, and the **traffic-class prefix-list** commands are all mutually exclusive in a PfR learn list. Only one of these commands can be specified per PfR learn list.

Examples

The following example, starting in global configuration mode, shows how to define a custom application traffic class using an access list. Every entry in the access list defines one application, and the destination network of the traffic class is determined by the specified aggregation method. After the access list is configured, the master controller automatically learns the defined application traffic based on highest throughput. A prefix list may be used to filter the traffic flows by destination prefix.

```
Router(config)# ip access-list extended USER_DEFINED_TC
Router(config-ext-nacl)# permit tcp any any 500
Router(config-ext-nacl)# permit tcp any any range 700 750
Router(config-ext-nacl)# permit udp 10.1.1.1 0.0.0.0 any
Router(config-ext-nacl)# permit ip any any dscp ef
Router(config-ext-nacl)# exit
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# list seq 10 refname LEARN_USER_DEFINED_TC
Router(config-pfr-mc-learn-list)# traffic-class access-list USER_DEFINED_TC
Router(config-pfr-mc-learn-list)# aggregation-type prefix-length 24
Router(config-pfr-mc-learn-list)# throughput
Router(config-pfr-mc-learn-list)# end
```

Related Commands

Command	Description
aggregation-type (PfR)	Configures a PfR master controller to aggregate learned prefixes based on the type of traffic flow.
ip access-list	Defines a standard or extended IP access list.
ip prefix-list	Creates an entry in a prefix list.
learn (PfR)	Enters PfR Top Talker and Top Delay learning configuration mode to configure prefixes for PfR to learn.
list (PfR)	Creates a PfR learn list to specify criteria for learning traffic classes and enters learn list configuration mode.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

traffic-class aggregate (PfR)

To aggregate Performance Routing (PfR) learned traffic flows into application traffic classes using an access list, use the **traffic-class aggregate** command in PfR Top Talker and Top Delay learning configuration mode. To disable the aggregation of PfR-learned traffic flows into application traffic classes using an access list, use the **no** form of this command.

traffic-class aggregate access-list *access-list-name*

no traffic-class aggregate access-list *access-list-name*

Syntax Description

access-list	Specifies that an IP access list is to be used to aggregate the PfR-learned traffic flows into application traffic classes.
access-list-name	Name of the access list. Names cannot contain either a space or quotation marks and must begin with an alphabetic character to distinguish them from numbered access lists.

Command Default

PfR-learned traffic flows are not aggregated into application traffic classes using an access list.

Command Modes

PfR Top Talker and Top Delay learning configuration (config-pfr-mc-learn)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **traffic-class aggregate** command can be used with the **traffic-class filter** (PfR) and **traffic-class keys** (PfR) commands to configure the master controller to automatically learn defined application traffic. Only one access list can be specified, but the access list may contain many access list entries to help define the traffic class parameters.

Note The **traffic-class aggregate** command is different from the **aggregation-type** (PfR) command that aggregates learned prefixes based on the type of traffic flow. The **traffic-class aggregate** command introduces the ability to use an access list to aggregate learned traffic flows to create an application traffic class. Both commands can be used in the same configuration.

Examples

The following example, starting in global configuration mode, configures the master controller to automatically learn defined application traffic. In this example, two access lists are created to identify and define voice traffic in the network. Using the **traffic-class aggregate** (PfR) and the **traffic-class filter** (PfR) commands with the access lists, only voice traffic with a Differentiated Services Code Point (DSCP) bit set to ef, a User Datagram Protocol (UDP), and a destination port in the range of 3000 to 4000 is learned and added to the PfR application database on the master controller.

```
Router(config)# ip access-list extended voice-filter-acl
Router(config-ext-nacl)# permit udp any 10.1.0.0 0.0.255.255 dscp ef
Router(config-ext-nacl)# exit
Router(config)# ip access-list extended voice-agg-acl
Router(config-ext-nacl)# permit udp any any range 3000 4000 dscp ef
Router(config-ext-nacl)# exit
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# aggregation-type prefix-length 24
Router(config-pfr-mc-learn)# throughput
Router(config-pfr-mc-learn)# traffic-class filter access-list voice-filter-acl
Router(config-pfr-mc-learn)# traffic-class aggregate access-list voice-agg-acl
Router(config-pfr-mc-learn)# traffic-class keys protocol dport dscp
Router(config-pfr-mc-learn)# end
```

Related Commands

Command	Description
aggregation-type (PfR)	Configures a PfR master controller to aggregate learned prefixes based on the type of traffic flow.
ip access-list	Defines a standard or extended IP access list.
learn (PfR)	Enters PfR Top Talker and Top Delay learning configuration mode to configure prefixes for PfR to learn.
list (PfR)	Creates a PfR learn list to specify criteria for learning traffic classes and enters learn list configuration mode.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
traffic-class filter (PfR)	Filters uninteresting traffic from PfR-learned traffic flows using an access list.
traffic-class keys (PfR)	Specifies a key list used by an PfR border router to aggregate the traffic flows into learned application classes.

traffic-class application (PfR)

To define a Performance Routing (PfR) traffic class using a predefined static application, use the **traffic-class application** command in learn list configuration mode. To remove the definition of a PfR-learned traffic class using a predefined static application, use the **no** form of this command.

traffic-class application *application-name* [*application-name ...*] [**filter** *prefix-list-name*]

no traffic-class application *application-name ...* [**filter** *prefix-list-name*]

Syntax Description

application-name	Name of a predefined static application using fixed ports. See Table 61. One application must be specified, but the ellipsis shows that more than one application keyword can be specified up to a maximum of ten.
filter	(Optional) Specifies that the traffic flows are filtered on the basis of a prefix list.
prefix-list-name	(Optional) Name of a prefix list (created using the **ip prefix-list** command).

Command Default

PfR traffic classes are not defined using a static application mapping.

Command Modes

Learn list configuration (config-pfr-mc-learn-list)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **traffic-class application** command is used to configure the master controller to automatically learn traffic using a keyword that represents an application. PfR maps the application keyword to a protocol—TCP or UDP, or both—and one or more ports, and this mapping is shown in Table 61. More than one application can be configured as part of the traffic class.

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

Note The **traffic-class application** (PfR) command, the **traffic-class access-list** (PfR) command, the **traffic-class application nbar** (PfR) command, and the **traffic-class prefix-list** (PfR) commands are all mutually exclusive in a PfR learn list. Only one of these commands can be specified per PfR learn list.

Table 61 displays the keywords that represent the application that can be configured with the **traffic-class application** command. Replace the *application-name* argument with the appropriate keyword from the table.

Table 61 Static Application List Keywords

Keyword	Protocol	Port
cuseeme	TCP UDP	7648 7649 7648 7649 24032
dhcp (Client)	UDP/TCP	68
dhcp (Server)	UDP/TCP	67
dns	UDP/TCP	53
finger	TCP	79
ftp	TCP	20 21
gopher	TCP/UDP	70
http	TCP/UDP	80
httpssl	TCP	443
imap	TCP/UDP	143 220
irc	TCP/UDP	194
kerberos	TCP/UDP	88 749
l2tp	UDP	1701
ldap	TCP/UDP	389
mssql	TCP	1443
nfs	TCP/UDP	2049
nntp	TCP/UDP	119
notes	TCP/UDP	1352
ntp	TCP/UDP	123
pcany	UDP TCP	22 5632 65301 5631
pop3	TCP/UDP	110
pptp	TCP	17233
simap	TCP/UDP	585 993 (Preferred)
sirc	TCP/UDP	994
sldap	TCP/UDP	636
smtp	TCP	25
snntp	TCP/UDP	563
spop3	TCP/UDP	123
ssh	TCP	22
telnet	TCP	23

Examples

The following example, starting in global configuration mode, shows how to define application traffic classes using two PfR learn lists, LEARN_REMOTE_LOGIN_TC and LEARN_FILE_TRANSFER_TC. The number of traffic classes to be learned in both learn list sessions is set to 50, and the maximum number of traffic classes to be learned for all sessions of the learn list is set to 90. The remote login traffic class is configured using keywords representing Telnet and Secure Shell (SSH) traffic, and the resulting prefixes are aggregated to a prefix length of 24. The file transfer traffic class is configured using a keyword that represents FTP and is also aggregated to a prefix length of 24. A prefix list is applied to the file transfer traffic class to permit traffic from the 10.0.0.0/8 prefix. The master controller is configured to learn the top prefixes based on highest outbound throughput for the filtered traffic, and the resulting traffic classes are added to the PfR application database to be passively and actively monitored.

```
Router(config)# ip prefix-list INCLUDE_10_NET 10.0.0.0/8
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# list seq 10 refname LEARN_REMOTE_LOGIN_TC
Router(config-pfr-mc-learn-list)# count 50 max 90
Router(config-pfr-mc-learn-list)# traffic-class application telnet ssh
Router(config-pfr-mc-learn-list)# aggregation-type prefix-length 24
Router(config-pfr-mc-learn-list)# throughput
Router(config-pfr-mc-learn-list)# exit
Router(config-pfr-mc-learn)# list seq 20 refname LEARN_FILE_TRANSFER_TC
Router(config-pfr-mc-learn-list)# count 50 max 90
Router(config-pfr-mc-learn-list)# traffic-class application ftp filter INCLUDE_10_NET
Router(config-pfr-mc-learn-list)# aggregation-type prefix-length 24
Router(config-pfr-mc-learn-list)# throughput
Router(config-pfr-mc-learn-list)# end
```

Related Commands

Command	Description
aggregation-type (PfR)	Configures a PfR master controller to aggregate learned prefixes based on the type of traffic flow.
ip prefix-list	Creates an entry in a prefix list.
learn (PfR)	Enters PfR Top Talker and Top Delay learning configuration mode to configure prefixes for PfR to learn.
list (PfR)	Creates a PfR learn list to specify criteria for learning traffic classes and enters learn list configuration mode.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
traffic-class application nbar (PfR)	Defines a PfR traffic class using an NBAR application mapping.

traffic-class application nbar (PfR)

To define a Performance Routing (PfR) traffic class using a Network-Based Application Recognition (NBAR) application mapping, use the **traffic-class application nbar** command in learn list configuration mode. To remove the definition of a PfR-learned traffic class using an application identified using NBAR, use the **no** form of this command.

traffic-class application nbar *nbar-app-name* [*nbar-app-name* **...**] [**filter** *prefix-list-name*]

no traffic-class application nbar [*nbar-app-name* **...**]

Syntax Description

nbar-app-name	Keyword representing the name of a dynamic application identified using NBAR. One application must be specified, but the ellipsis shows that more than one application keyword can be specified, up to a maximum of ten. See the "Usage Guidelines" section for more details.
filter	(Optional) Specifies that the traffic flows are filtered on the basis of a prefix list.
prefix-list-name	(Optional) Name of a prefix list (created using the **ip prefix-list** command).

Command Default

PfR traffic classes are not defined using an NBAR application mapping.

Command Modes

Learn list configuration (config-pfr-mc-learn-list)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **traffic-class application nbar** command is used to configure the master controller to automatically learn traffic using a keyword that represents an application that can be identified using NBAR. More than one application can be configured as part of the traffic class with a maximum of ten applications entered per command line. Enter multiple **traffic-class application nbar** command statements if you need to specify more than ten applications.

NBAR is capable of identifying applications based on the following three types of protocols:

- Non-UDP and non-TCP IP protocols—For example, Generic Routing Encapsulation (GRE) and Internet Control Message Protocol (ICMP).
- TCP and UDP protocols that use statically assigned port numbers—For example, CU-SeeMe desktop video conference (CU-SeeMe-Server), Post Office Protocol over Transport Layer Security (TLS), and Secure Sockets Layer (SSL) server (SPOP3-Server).
- TCP and UDP protocols that dynamically assign port numbers and require stateful inspection—For example, Real-Time Transport Protocol audio streaming (RTP-audio) and BitTorrent File Transfer Traffic (BitTorrent).

Use the **traffic-class application nbar ?** command to determine if an application can be identified using NBAR and replace the *nbar-app-name* argument with the appropriate keyword from the screen display.

The list of applications identified using NBAR and available for profiling PfR traffic classes is constantly evolving. For lists of many of the NBAR applications defined using static or dynamically assigned ports, see the "Performance Routing with NBAR/CCE Application and Recognition" module.

For more details about NBAR, see the "Classifying Network Traffic Using NBAR" section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note The **traffic-class application nbar** (PfR) command, the **traffic-class application** (PfR) command, the **traffic-class access-list** (PfR) command, and the **traffic-class prefix-list** (PfR) commands are all mutually exclusive in a PfR map. Only one of these commands can be specified per PfR map.

Examples

The following example, starting in global configuration mode, shows how to define application traffic classes identified by using NBAR and two PfR learn lists, LEARN_VOICE_TC and LEARN_VIDEO_TC. The number of traffic classes to be learned in both learn list sessions is 50, and the maximum number of traffic classes to be learned for all sessions of the learn list is 90.

The Voice over IP (VoIP) traffic class is configured using keywords representing RTP-Audio and the resulting prefixes are aggregated to a prefix length of 24. The video traffic class is configured using a keyword that represents RTP-video and is also aggregated to a prefix length of 24. A prefix list is applied to the video traffic class to match traffic for the destination prefix of 10.0.0.0/8. The master controller is configured to learn the top prefixes based on highest outbound throughput for the learned traffic, and the resulting traffic classes are added to the PfR application database.

The traffic streams that the learn list profiles for both the RTP-audio and the RTP-video applications are:

```
10.1.1.1
10.1.2.1
172.17.1.1
172.17.2.1
```

The traffic classes that are learned for each application are:

```
10.1.1.0/24 rtp-audio
10.1.2.0/24 rtp-audio
172.17.1.0/24 rtp-audio
172.17.2.0/24 rtp-audio

10.1.1.0/24 rtp-video
10.1.2.0/24 rtp-video
```

The difference in traffic classes learned is due to the optional INCLUDE_10_NET prefix list that only includes RTP-video application traffic with a destination prefix that matches the prefix 10.0.0.0/8.

```
Router(config)# ip prefix-list INCLUDE_10_NET 10.0.0.0/8
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# list seq 10 refname LEARN_VOICE_TC
Router(config-pfr-mc-learn-list)# count 50 max 90
Router(config-pfr-mc-learn-list)# traffic-class application nbar rtp-audio
Router(config-pfr-mc-learn-list)# aggregation-type prefix-length 24
Router(config-pfr-mc-learn-list)# throughput
Router(config-pfr-mc-learn-list)# exit
Router(config-pfr-mc-learn)# list seq 20 refname LEARN_VIDEO_TC
Router(config-pfr-mc-learn-list)# count 50 max 90
Router(config-pfr-mc-learn-list)# traffic-class application nbar rtp-video
filter INCLUDE_10_NET
Router(config-pfr-mc-learn-list)# aggregation-type prefix-length 24
Router(config-pfr-mc-learn-list)# throughput
Router(config-pfr-mc-learn-list)# end
```

Related Commands

Command	Description
aggregation-type (PfR)	Configures a PfR master controller to aggregate learned prefixes based on the type of traffic flow.
ip prefix-list	Creates an entry in a prefix list.
learn (PfR)	Enters PfR Top Talker and Top Delay learning configuration mode to configure prefixes for PfR to learn.
list (PfR)	Creates a PfR learn list to specify criteria for learning traffic classes and enters learn list configuration mode.
match traffic-class application (PfR)	Defines a match clause using a static application mapping in a PfR map to create a traffic class.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

traffic-class filter (PfR)

To filter uninteresting traffic from Performance Routing (PfR) learned traffic flows using an access list, use the **traffic-class filter** command in PfR Top Talker and Top Delay learning configuration mode. To disable the filtering of PfR-learned traffic flows using an access list, use the **no** form of this command.

traffic-class filter access-list *access-list-name*

no traffic-class filter access-list *access-list-name*

Syntax Description

access-list	Specifies that an IP access list is to be used to filter uninteresting traffic from PfR-learned traffic flows.
access-list-name	Name of the access list. Names cannot contain either a space or quotation marks and must begin with an alphabetic character to distinguish them from numbered access lists.

Command Default

Uninteresting traffic is not filtered from PfR traffic flows using an access list.

Command Modes

PfR Top Talker and Top Delay learning configuration (config-pfr-mc-learn)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

PfR is used to optimize the performance of selected traffic flows in your network. While defining the selected traffic flows, this command is used to filter out traffic that you are not interested in optimizing.

The **traffic-class filter** command can be used with the **traffic-class aggregate** (PfR) and **traffic-class keys** (PfR) commands to configure the master controller to automatically learn defined application traffic. Only one access list can be specified, but the access list may contain many access list entries (ACEs) to help define the traffic class parameters.

Examples

The following example, starting in global configuration mode, configures the master controller to automatically learn defined application traffic. In this example, two access lists are created to identify and define voice traffic in the network. Using the **traffic-class aggregate** (PfR) and the **traffic-class filter** commands with the access lists, only voice traffic with a Differentiated Services Code Point (DSCP) bit set to ef, a User Datagram Protocol (UDP), and a destination port in the range of 3000 to 4000 is learned and added to the PfR application database on the master controller.

```
Router(config)# ip access-list extended voice-filter-acl
Router(config-ext-nacl)# permit udp any 10.1.0.0 0.0.255.255 dscp ef
Router(config-ext-nacl)# exit
Router(config)# ip access-list extended voice-agg-acl
Router(config-ext-nacl)# permit udp any any range 3000 4000 dscp ef
Router(config-ext-nacl)# exit
Router(config)# pfr master
```

```
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# aggregation-type prefix-length 24
Router(config-pfr-mc-learn)# throughput
Router(config-pfr-mc-learn)# traffic-class filter access-list voice-filter-acl
Router(config-pfr-mc-learn)# traffic-class aggregate access-list voice-agg-acl
Router(config-pfr-mc-learn)# traffic-class keys dscp protocol dport
Router(config-pfr-mc-learn)# end
```

Related Commands

Command	Description
aggregation-type (PfR)	Configures a PfR master controller to aggregate learned prefixes based on the type of traffic flow.
ip access-list	Defines a standard or extended IP access list.
learn (PfR)	Enters PfR Top Talker and Top Delay learning configuration mode to configure prefixes for PfR to learn.
list (PfR)	Creates a PfR learn list to specify criteria for learning traffic classes and enters learn list configuration mode.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
traffic-class aggregate (PfR)	Aggregates PfR learned traffic flows into application traffic classes using an access list.
traffic-class keys (PfR)	Specifies a key list used by a PfR border router to aggregate the traffic flows into learned application classes.

traffic-class keys (PfR)

To specify a key list of fields in the traffic flows that a Performance Routing (PfR) border router uses to aggregate traffic flows into application traffic classes, use the **traffic-class keys** command in PfR Top Talker and Top Delay learning configuration mode. To remove the key list, use the **no** form of this command.

traffic-class keys [**default** | [**dscp**] [**protocol** [**dport**] [**sport**]]]

no traffic-class keys [**default** | [**dscp**] [**protocol** [**dport**] [**sport**]]]

Syntax Description

default	(Optional) Aggregates the traffic flows into application traffic classes on the basis of protocol and destination port.
dscp	(Optional) Aggregates the traffic flows into application traffic classes on the basis of a Differentiated Services Code Point (DSCP) value.
protocol	(Optional) Aggregates the traffic flows into application traffic classes on the basis of the protocol.
dport	(Optional) Aggregates the traffic flows into application traffic classes on the basis of the destination port.
sport	(Optional) Aggregates the traffic flows into application traffic classes on the basis of the source port.

Command Default

No PfR traffic class key lists are created.

Command Modes

PfR Top Talker and Top Delay learning configuration (config-pfr-mc-learn)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **traffic-class keys** command can be used with the **traffic-class filter** (PfR) and **traffic-class aggregate** (PfR) commands to configure the master controller to automatically learn defined application traffic. This command is used only if the **traffic-class aggregate** (PfR) command is not configured or returns no matches.

Examples

In this example, only voice traffic with a DSCP bit set to ef, a User Datagram Protocol (UDP), and a destination port in the range of 3000 to 4000 is learned and added to the PfR application database on the master controller.

```
Router(config)# ip access-list extended voice-filter-acl
Router(config-ext-nacl)# permit udp any 10.1.0.0 0.0.255.255 dscp ef
Router(config-ext-nacl)# exit
Router(config)# ip access-list extended voice-agg-acl
Router(config-ext-nacl)# permit udp any any range 3000 4000 dscp ef
Router(config-ext-nacl)# exit
```

```
Router(config)# pfr master
Router(config-pfr-master)# learn
Router(config-pfr-master-learn)# aggregation-type prefix-length 24
Router(config-pfr-master-learn)# throughput
Router(config-pfr-master-learn)# traffic-class filter access-list voice-filter-acl
Router(config-pfr-master-learn)# traffic-class aggregate access-list voice-agg-acl
Router(config-pfr-master-learn)# traffic-class keys dscp protocol dport
Router(config-pfr-master-learn)# end
```

Related Commands

Command	Description
learn (PfR)	Enters PfR Top Talker and Top Delay learning configuration mode to configure prefixes for PfR to learn.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
traffic-class aggregate (PfR)	Aggregates PfR-learned traffic flows into application traffic classes using an access list.
traffic-class filter (PfR)	Filters uninteresting traffic from PfR-learned traffic flows using an access list.

traffic-class prefix-list (PfR)

To define a Performance Routing (PfR) traffic class using a prefix list applied to learned traffic classes, use the **traffic-class prefix-list** command in learn list configuration mode. To disable the definition of PfR-learned traffic flows into traffic classes using a prefix list, use the **no** form of this command.

traffic-class prefix-list *prefix-list-name* [**inside**]

no traffic-class prefix-list

Syntax Description

prefix-list-name	Name of a prefix list. Names cannot contain either a space or quotation marks and must begin with an alphabetic character to distinguish them from numbered access lists.
inside	(Optional) Specifies that the prefix list contains inside prefixes.

Command Default

PfR application traffic classes are not defined using a prefix list.

Command Modes

Learn list configuration (config-pfr-mc-learn-list)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **traffic-class prefix-list** command is used to configure the master controller to automatically learn traffic based only on destination prefixes. Use the optional **inside** keyword to specify prefixes that are within the internal network.

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

Note The **traffic-class prefix-list** command, the **traffic-class application** (PfR) command, the **traffic-class application nbar** (PfR) command, and the **traffic-class access-list** (PfR) commands are all mutually exclusive in a PfR learn list. Only one of these commands can be specified per PfR learn list.

Examples

The following example, starting in global configuration mode, shows how to define traffic classes based only on destination prefixes for a learn list named LEARN_PREFIX_TC. The traffic classes are created using the prefix list, LEARN_LIST1, in which every entry in the prefix list defines one destination network of a traffic class. After the prefix list is configured, the master controller automatically learns the traffic classes based on the highest throughput.

```
Router(config)# ip prefix-list LEARN_LIST1 permit seq 10 10.0.0.0/8
Router(config)# ip prefix-list LEARN_LIST1 permit seq 20 172.16.0.0/16
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# list seq 10 refname LEARN_PREFIX_TC
Router(config-pfr-mc-learn-list)# aggregation-type prefix-length 24
Router(config-pfr-mc-learn-list)# traffic-class prefix-list LEARN_LIST1
Router(config-pfr-mc-learn-list)# throughput
Router(config-pfr-mc-learn-list)# end
```

Related Commands

Command	Description
aggregation-type (PfR)	Configures a PfR master controller to aggregate learned prefixes based on the type of traffic flow.
ip prefix-list	Creates an entry in a prefix list.
learn (PfR)	Enters PfR Top Talker and Top Delay learning configuration mode to configure prefixes for PfR to learn.
list (PfR)	Creates a PfR learn list to specify criteria for learning traffic classes and enters learn list configuration mode.
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.

unreachable (PfR)

To set the relative percentage or maximum number of unreachable hosts that Performance Routing (PfR) permits from a PfR-managed exit link, use the **unreachable** command in PfR master controller configuration mode. To return the relative percentage of unreachable hosts to the default value, use the **no** form of this command.

unreachable {**relative** *average* | **threshold** *maximum*}

no unreachable

Syntax Description

relative *average*	Sets a relative percentage of unreachable hosts based on a comparison of short-term and long-term percentages. The range of values that can be configured for this argument is a number from 1 to a 1000. Each increment represents one tenth of a percent.
threshold *maximum*	Sets the absolute maximum number of unreachable hosts based on flows per million (fpm). The range of values that can be configured for this argument is from 1 to 1000000.

Command Default

PfR uses a default relative percentage of 50 (5 percent) unreachable hosts if this command is not configured or if the **no** form of this command is entered.

Command Modes

PfR master controller configuration (config-pfr-mc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **unreachable** command is entered on a master controller. This command is used to set the relative percentage or the absolute maximum number of unreachable hosts, based on flows per million, that PfR will permit from a PfR-managed exit link. If the absolute number or relative percentage of unreachable hosts is greater than the user-defined or the default value, PfR determines that the exit link is out-of-policy 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 short-term measurement reflects the percentage of hosts that are unreachable within a 5-minute period. The long-term measurement reflects the percentage of unreachable hosts within a 60-minute period. The following formula is used to calculate this value:

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

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

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

Examples

The following example configures the master controller to search for a new exit link when the difference between long- and short-term measurements (relative percentage) is greater than 10 percent:

```
Router(config)# pfr master
Router(config-pfr-mc)# unreachable relative 100
```

The following example configures PfR to search for a new exit link when 10,000 hosts are unreachable:

```
Router(config)# pfr master
Router(config-pfr-mc)# unreachable threshold 10000
```

Related Commands

Command	Description
pfr	Enables a PfR process and configures a router as a PfR border router or as a PfR master controller.
set unreachable (PfR)	Configures a PfR map to set the relative percentage or maximum number of unreachable hosts that PfR permits from a PfR-managed exit link.