



Performance Routing Border Router Only Functionality

Last Updated: April 30, 2010

Performance Routing (PfR) introduced support for border router (BR) only functionality on Cisco ASR 1000 series aggregation services routers in Cisco IOS XE Release 2.6.1. On software images that support the border router only functionality, no master controller configuration is available. The master controller that communicates with the border router in this situation must be a router running Cisco IOS Release 15.0(1)M, or a later 15.0M release. In contrast to Performance Routing Border Router Only Functionality on other platforms, Cisco ASR 1000 series routers can provide full border router passive monitoring functionality as well as active monitoring capability.

- [Finding Feature Information, page 1](#)
- [Prerequisites for PfR Border Router Only Functionality, page 1](#)
- [Restrictions for PfR Border Router Only Functionality, page 2](#)
- [Information About PfR Border Router Only Functionality, page 2](#)
- [How to Configure PfR Border Router Only Functionality, page 4](#)
- [Configuration Examples for PfR Border Router Only Functionality, page 9](#)
- [Additional References, page 10](#)
- [Feature Information for PfR Border Router Only Functionality, page 11](#)

Finding Feature Information

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

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

Prerequisites for PfR Border Router Only Functionality



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

The Cisco ASR 1000 series aggregation services routers being used as PfR border routers must be running Cisco IOS XE Release 2.6.1, or a later release.

Restrictions for PfR Border Router Only Functionality

In Cisco IOS XE Release 2.6.1 support for using a Cisco ASR 1000 series router as a PfR border router was introduced. Only border router functionality is included in the Cisco IOS Release Cisco IOS XE Release 2.6.1 images; no master controller configuration is available. The master controller that communicates with the Cisco ASR 1000 series router being used as a border router must be a router running Cisco IOS Release 15.0(1)M, or a later 15.0M release.

Information About PfR Border Router Only Functionality

To configure border router only functionality, you should understand the following concepts:

- [PfR Border Router Only Functionality on ASR 1000 Series Routers, page 2](#)
- [PfR Border Router Operations, page 4](#)

PfR Border Router Only Functionality on ASR 1000 Series Routers

PfR introduced support for border router (BR) only functionality on Cisco ASR 1000 series aggregation services routers in Cisco IOS XE Release 2.6.1. On software images that support the border router only functionality, no master controller configuration is available. The master controller that communicates with the border router in this situation must be a router running Cisco IOS Release 15.0(1)M. In contrast to Border Router Only Functionality on other platforms, Cisco ASR 1000 series routers can provide full border router passive monitoring functionality as well as active monitoring capability.

PfR uses three methods of traffic class performance measurement:

- **Passive monitoring**—measuring the performance metrics of traffic class entries while the traffic is flowing through the device using NetFlow functionality. Based on the list of learned and configured prefixes, Performance Routing passively monitors TCP flags for traffic on every flow (of the current exit) to measure latency, packet loss, and reachability. Throughput-based load balancing is still supported.
- **Active monitoring**—creating a stream of synthetic traffic replicating a traffic class as closely as possible and measuring the performance metrics of the synthetic traffic. The results of the performance metrics of the synthetic traffic are applied to the traffic class in the master controller database. Active monitoring uses integrated IP Service Level Agreements (IP SLAs) functionality.
- **Both active and passive monitoring**—combining both active and passive monitoring in order to generate a more complete picture of traffic flows within the network.

The monitoring mode is configured using the command-line interface (CLI) on a master controller which sends requests to the border routers to enable monitoring modes.

Although the configuration must be performed on a master controller running a Cisco IOS 15.0(1)M image, the border router (BR) only functionality in Cisco ASR 1000 series routers supports the following features. For more details about how to understand and implement each feature, see the *Optimized Edge Routing Configuration Guide, Cisco IOS Release 15.0M*.

- **OER Active Probe Source Address**—The OER Active Probe Source Address feature allows you to configure a specific exit interface on the border router as the source for active probes.

- OER - Application Aware Routing with Static Application Mapping—The OER - Application Aware Routing with Static Application Mapping feature introduces the ability to configure standard applications using just one keyword. This feature also introduces a learn list configuration mode that allows Performance Routing (PfR) policies to be applied to traffic classes profiled in a learn list. Different policies can be applied to each learn list. New traffic-class and match traffic-class commands are introduced to simplify the configuration of traffic classes that PfR can automatically learn, or that can be manually configured.
- OER Support for Policy-Rules Configuration and Port-Based Prefix Learning—The OER Support for Policy-Rules Configuration feature introduced the capability to select an OER map and apply the configuration under OER master controller configuration mode, providing an improved method to switch between predefined OER maps.
- OER Port and Protocol Based Prefix Learning—The OER Port and Protocol Based Prefix Learning feature introduced the capability to configure a master controller to learn prefixes based on the protocol type and the TCP or UDP port number.
- OER Support for Cost-Based Optimization and Traceroute Reporting—The OER Support for Cost-Based Optimization feature introduced the capability to configure exit link policies based monetary cost and the capability to configure traceroute probes to determine prefix characteristics on a hop-by-hop basis. Performance Routing support for traceroute reporting allows you to monitor prefix performance on a hop-by-hop basis. Delay, loss, and reachability measurements are gathered for each hop from the probe source (border router) to the target prefix.
- BGP Inbound Optimization—PfR BGP inbound optimization supports best entrance selection for traffic that originates from prefixes outside an autonomous system destined for prefixes inside the autonomous system. External BGP (eBGP) advertisements from an autonomous system to an Internet service provider (ISP) can influence the entrance path for traffic entering the network. PfR uses eBGP advertisements to manipulate the best entrance selection.

**Note**

On Cisco ASR 1000 series aggregation services routers in Cisco IOS XE Release 2.6.1, the maximum number of internal prefixes that can be learned during a monitoring period is 30.

- DSCP Monitoring—OER DSCP Monitoring introduced automatic learning of traffic classes based on protocol, port numbers, and DSCP value. Traffic classes can be defined by a combination of keys comprising of protocol, port numbers, and DSCP values, with the ability to filter out traffic that is not required, and the ability to aggregate the traffic in which you are interested. Layer 4 information such as protocol, port number, and DSCP information is now sent to the master controller database in addition to the Layer 3 prefix information. The new functionality allows OER to both actively and passively monitor application traffic.
- Performance Routing - Protocol Independent Route Optimization (PIRO)—PIRO introduced the ability of PfR to search for a parent route—an exact matching route, or a less specific route—in the IP Routing Information Base (RIB), allowing PfR to be deployed in any IP-routed environment including Interior Gateway Protocols (IGPs) such as OSPF and IS-IS.
- Fast Failover Monitoring—Fast Failover Monitoring introduced the ability to configure a fast monitoring mode. In fast failover monitoring mode, all exits are continuously probed using active monitoring and passive monitoring. The probe frequency can be set to a lower frequency in fast failover monitoring mode than for other monitoring modes, to allow a faster failover capability. Fast failover monitoring can be used with all types of active probes: ICMP echo, jitter, TCP connection, and UDP echo.
- EIGRP mGRE DMVPN Integration—The PfR EIGRP feature introduces PfR route control capabilities based on EIGRP by performing a route parent check on the EIGRP database. This feature

also adds support for mGRE Dynamic Multipoint VPN (DMVPN) deployments that follow a hub-and-spoke network design.

- OER Voice Traffic Optimization—The PfR Voice Traffic Optimization feature provides support for outbound optimization of voice traffic based on the voice metrics, jitter and Mean Opinion Score (MOS). Jitter and MOS are important quantitative quality metrics for voice traffic and these voice metrics are measured using PfR active probes.

PfR Border Router Operations

PfR is configured on Cisco routers using Cisco IOS command-line interface (CLI) configurations. Performance Routing comprises two components: the Master Controller (MC) and the Border Router (BR). A PfR deployment requires one MC and one or more BRs. Communication between the MC and the BR is protected by key-chain authentication.

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.

How to Configure PfR Border Router Only Functionality

This section contains the following tasks:

- [Setting Up a PfR Border Router, page 4](#)
- [Displaying PfR Border Router Information, page 7](#)

Setting Up a PfR Border Router

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

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

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

- Perform the task, [Configuring the PfR Master Controller Example](#), to set up the master controller and define the interfaces and establish communication with the border routers. Only border router functionality is included in Cisco IOS XE Release 2.6.1 images; no master controller configuration is available. The master controller that communicates with the Cisco ASR 1000 series router being used as a border router must be a router running Cisco IOS Release 15.0(1)M, or a later 15.0M release.

- Each border router must have at least one external interface that is either used to connect to an ISP or is used as an external WAN link. A minimum of two external interfaces are required in a PFR-managed network.
- Each border router must have at least one internal interface. Internal interfaces are used for only passive performance monitoring with NetFlow. Internal interfaces are not used to forward traffic.
- Each border router must have at least one local interface. Local interfaces are used only for master controller and border router communication. A single interface must be configured as a local interface on each border router.



Note

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>

Command or Action	Purpose
<p>Step 3 key chain <i>name-of-chain</i></p> <p>Example:</p> <pre>Router(config)# key chain border1_PFR</pre>	<p>Enables key-chain authentication and enters key-chain configuration mode.</p> <ul style="list-style-type: none"> Key-chain authentication protects the communication session between both the master controller and the border router. The key ID and key string must match in order for communication to be established.
<p>Step 4 key <i>key-id</i></p> <p>Example:</p> <pre>Router(config-keychain)# key 1</pre>	<p>Identifies an authentication key on a key chain and enters key-chain key configuration mode.</p> <ul style="list-style-type: none"> The key ID must match the key ID configured on the master controller.
<p>Step 5 key-string <i>text</i></p> <p>Example:</p> <pre>Router(config-keychain-key)# key- string bl</pre>	<p>Specifies the authentication string for the key.</p> <ul style="list-style-type: none"> The authentication string must match the authentication string configured on the master controller. Any level of encryption can be configured.
<p>Step 6 exit</p> <p>Example:</p> <pre>Router(config-keychain-key)# exit</pre>	<p>Exits key-chain key configuration mode and returns to key-chain configuration mode.</p>
<p>Step 7 Repeat Step 6.</p> <p>Example:</p> <pre>Router(config-keychain)# exit</pre>	<p>Exits key-chain configuration mode and returns to global configuration mode.</p>
<p>Step 8 oer border</p> <p>Example:</p> <pre>Router(config)# oer border</pre>	<p>Enters OER border router configuration mode to configure a router as a border router.</p> <ul style="list-style-type: none"> The border router must be in the forwarding path and contain at least one external and internal interface.
<p>Step 9 local <i>type number</i></p> <p>Example:</p> <pre>Router(config-oer-br)# local GigabitEthernet 0/0/0</pre>	<p>Identifies a local interface on a PFR border router as the source for communication with an PFR master controller.</p> <ul style="list-style-type: none"> A local interface must be defined.

Command or Action	Purpose
<p>Step 10 <code>master ip-address key-chain key-chain-name</code></p> <p>Example:</p> <pre>Router(config-oer-br)# master 10.1.1.1 key-chain border1_PFR</pre>	<p>Enters OER-managed border router configuration mode to establish communication with a master controller.</p> <ul style="list-style-type: none"> • An IP address is used to identify the master controller. • The value for the key-chain-name argument must match the key-chain name configured in Step 3.
<p>Step 11 <code>end</code></p> <p>Example:</p> <pre>Router(config-oer-br)# end</pre>	<p>Exits OER Top Talker and Top Delay learning configuration mode and returns to privileged EXEC mode.</p>

- [What to Do Next, page 7](#)

What to Do Next

If your network is configured to use only static routing, no additional configuration is required. The PfR-managed network should be operational, as long as valid static routes that point to external interfaces on the border routers are configured. You can proceed to the “Where To Go Next” for information about further PfR customization.

Displaying PfR Border Router Information

Although PfR features are mostly configured on a master controller, the border routers actually collect the performance information and a number of **show** commands can be run on a border router. The commands in this task are entered on a border router through which the application traffic is flowing. The **show** commands can be entered in any order.

SUMMARY STEPS

1. `enable`
2. `show oer border`
3. `show oer border active-probes`
4. `show oer border passive prefixes`
5. `show oer border routes {bgp | cce | eigrp [parent] | rwatch | static}`

DETAILED STEPS

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

Example:

```
Router> enable
```

Step 2**show oer border**

Displays information about a PfR border router connection and PfR controlled interfaces.

Example:

```
Router# show oer 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
```

Step 3**show oer border active-probes**

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. 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.

Example:

```
Router# show oer border active-probes
```

```
OER 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

Step 4**show oer border passive prefixes**

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

Example:

```
Router# show oer border passive prefixes
```

```
OER Passive monitored prefixes:
Prefix      Mask    Match Type
10.1.5.0    /24    exact
```

Step 5**show oer border routes {bgp | cce | eigrp [parent] | rwatch | static}**

This command is used to display information about PfR-controlled routes on a border router. 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.

Example:

```
Router# show oer 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 10.1.1.2.0/24   10.0.0.0/8  5000
```

Configuration Examples for PFR Border Router Only Functionality

- [Configuring the PFR Master Controller Example, page 9](#)
- [Configuring a PFR Border Router Example, page 10](#)

Configuring the PFR Master Controller Example

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

**Note**

This configuration is performed on a master controller. Only border router functionality is included in Cisco IOS XE Release 2.6.1 images; no master controller configuration is available. The master controller that communicates with the Cisco ASR 1000 series router being used as a border router must be a router running Cisco IOS Release 15.0(1)M, or a later 15.0M release.

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

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

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

Configuring a PfR Border Router Example

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

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

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

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

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco OER commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples	Cisco IOS Optimized Edge Routing Command Reference
Concepts and configuration tasks required to implement OER and PfR features using the OER syntax.	Optimized Edge Routing Configuration Guide

Technical Assistance

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

Feature Information for PfR Border Router Only Functionality

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

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

Table 1 **Feature Information for PfR Border Router Only Functionality**

Feature Name	Releases	Feature Information
OER Border Router Only Functionality	Cisco IOS XE Release 2.6.1	<p>Performance Routing (PfR) introduced support for border router (BR) only functionality on Cisco ASR 1000 series aggregation services routers in Cisco IOS XE Release 2.6.1. On software images that support the border router only functionality, no master controller configuration is available. The master controller that communicates with the border router in this situation must be a router running Cisco IOS Release 15.0(1)M. In contrast to Border Router Only Functionality on other platforms, Cisco ASR 1000 series routers can provide full border router passive monitoring functionality as well as active monitoring capability.</p> <p>Note In Cisco IOS XE Release 2.6.1, only OER syntax is available.</p> <p>The following commands were introduced or modified by this feature: show oer border passive cache, show oer master prefix.</p>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

© 2010-2012 Cisco Systems, Inc. All rights reserved.