Performance Routing Configuration Guide, Cisco IOS XE Release 2

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

CONTENTS

Configuring Basic Performance Routing

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

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

This document contains an introduction to the basic concepts and tasks required to implement Performance Routing using Cisco IOS XE Software on Cisco ASR 1000 series aggregation services routers.

Note In Cisco IOS XE Release 2.6.1, only border router functionality is supported.

Finding Feature Information

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

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

Restrictions

In Cisco IOS XE Release 2.6.1 support for using a Cisco ASR 1000 series aggregation services router as a PfR border router was introduced. Only border router functionality is included in the 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 routers being used as a border router must be a router running Cisco IOS Release 15.0(1)M.

Information About Performance Routing

To configure PfR, you should understand the following concepts:

Performance Routing Overview

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

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

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

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

Performance Routing Versus Optimized Edge Routing

Cisco Performance Routing takes advantage of the vast intelligence embedded in Cisco IOS Software to determine the optimal path based upon network and application policies. Cisco Performance Routing is an evolution of the Cisco IOS Optimized Edge Routing (OER) technology with a much broader scope. OER

was originally designed to provide route control on a per destination prefix basis, but Performance Routing has expanded capabilities that facilitate intelligent route control on a per application basis. The expanded capabilities provide additional flexibility and more granular application optimization than OER.

Performance Routing Versus Classic Routing Technologies

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

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

Basic Performance Routing Deployment

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

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

PfR Border Router

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

controller. The BR enforces policy changes by injecting a preferred route to alter routing in the network. A BR process can be enabled on the same router as a master controller process.

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

PfR Master Controller

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

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

PfR Component Version

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

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

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

Note For Cisco IOS XE Release 2.6.1, and later releases, PfR supports the ASR 1000 series router as a border router only and the master controller must be running a Cisco IOS Release 15.0M image for version compatibility.

Key Chain Authentication for PfR

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

PfR-Managed Network Interfaces

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

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

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

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

The following interface types can be configured as local interfaces:

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

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

Performance Routing DMVPN mGre Support

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

PfR Network Performance Loop

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

Figure 1 PfR Network Performance Loop

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

- Profile Phase, page 7
- Apply Policy Phase, page 7
- Measure Phase, page 7
- Enforce Phase, page 8
- Verify Phase, page 8

Profile Phase

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

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

Apply Policy Phase

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

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

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

Measure Phase

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

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

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

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

Support for NetFlow or IP SLAs configuration is enabled automatically.

Enforce Phase

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

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

Verify Phase

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

PfR and the Enterprise Network

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

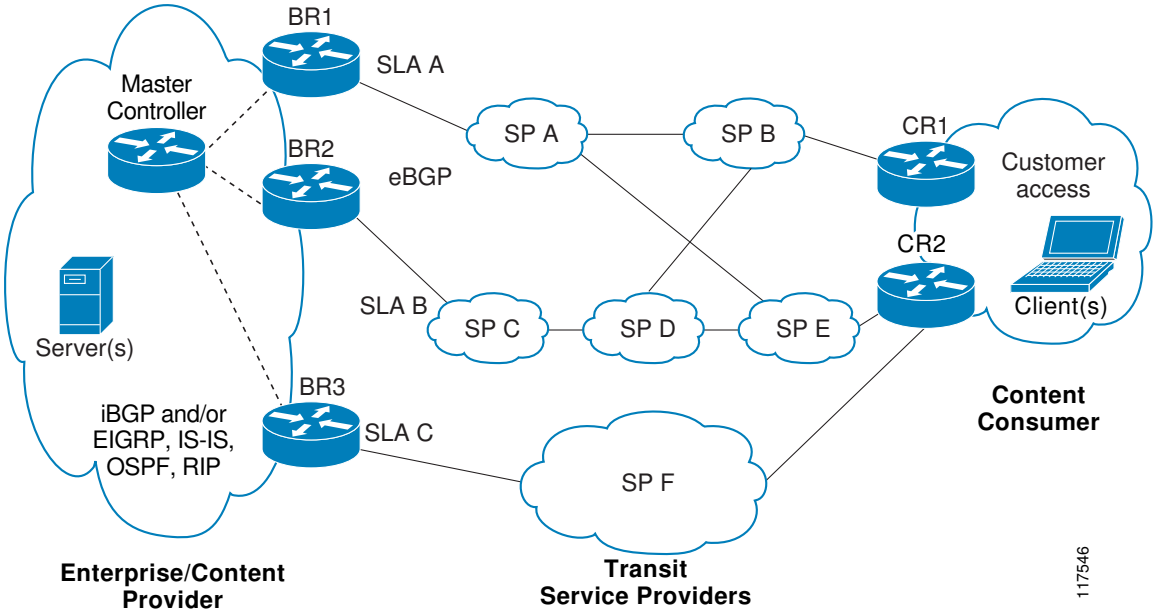
Although many of the examples used to describe PfR deployment show ISPs as the network with which the edge devices communicate, there are other solutions. The network edge can be defined as any logical separation in a network: can be another part of the network such as a data center network within the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

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

Typical Topology on Which PfR is Deployed

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

Figure 2 A Typical PfR Deployment



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

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

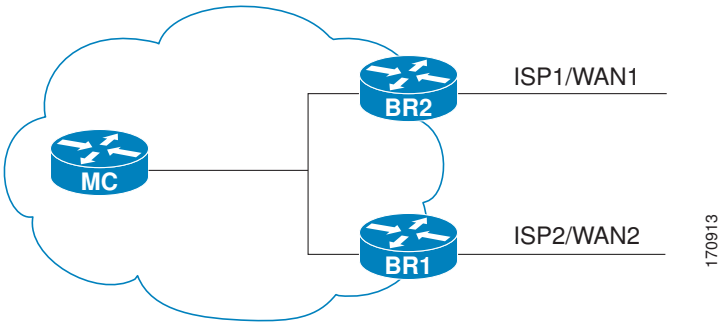
How to Configure Basic Performance Routing

Setting Up the PfR Master Controller

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

Note In Cisco IOS XE Release 2.6.1, and later releases, PfR supports the ASR 1000 series router as a border router only and the master controller must be running a Cisco IOS Release 15.0M image.

Figure 3 Master Controller and Border Router Diagram



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

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

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

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

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

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

Setting Up a PFR Border Router

Perform this task to set up a PfR border router. This task must be performed at each border router in your PfR-managed network. For an example network configuration of a master router and two border routers, see the figure below. 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, Setting Up the PfR Master Controller, to set up the master controller and define the interfaces and establish communication with the border routers.

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

Tip For Cisco IOS XE Release 2.6.1, and later releases, PfR supports the ASR 1000 series router as a border router only; the master controller cannot be enabled on an ASR 1000 series router.

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

Note

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. Repeat Step 6.
8. **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	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**key chain** *name-of-chain* **Example:** `Router(config)# key chain border1_PFR`	Enables key-chain authentication and enters key-chain configuration mode. • Key-chain authentication protects the communication session between both the master controller and the border router. The key ID and key string must match in order for communication to be established.
Step 4	**key** *key-id* **Example:** `Router(config-keychain)# key 1`	Identifies an authentication key on a key chain and enters key-chain key configuration mode. • The key ID must match the key ID configured on the master controller.
Step 5	**key-string** *text* **Example:** `Router(config-keychain-key)# key-string b1`	Specifies the authentication string for the key. • The authentication string must match the authentication string configured on the master controller. • Any level of encryption can be configured.
Step 6	**exit** **Example:** `Router(config-keychain-key)# exit`	Exits key-chain key configuration mode and returns to key-chain configuration mode.
Step 7	Repeat Step 6. **Example:** `Router(config-keychain)# exit`	Exits key-chain configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 8	**oer border** **Example:** `Router(config)# oer border`	Enters OER border router configuration mode to configure a router as a border router. • The border router must be in the forwarding path and contain at least one external and internal interface.
Step 9	**local** *type number* **Example:** `Router(config-oer-br)# local GigabitEthernet 0/0/0`	Identifies a local interface on a PfR border router as the source for communication with an PfR master controller. • A local interface must be defined.
Step 10	**master** *ip-address* **key-chain** *key-chain-name* **Example:** `Router(config-oer-br)# master 10.1.1.1 key-chain border1_PFR`	Enters OER-managed border router configuration mode to establish communication with a master controller. • An IP address is used to identify the master controller. • The value for the key-chain-name argument must match the key-chain name configured in Step 3.
Step 11	**end** **Example:** `Router(config-oer-br)# end`	Exits OER Top Talker and Top Delay learning configuration mode and returns to privileged EXEC mode.

- What to Do Next, page 17

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 Additional References section for information about further OER and PfR feature customization using the OER syntax.

Otherwise, routing protocol peering or static redistribution must be configured between the border routers and other routers in the PfR-managed network. You can proceed to the "Setting Up OER Network Components" module in the Optimized Edge Routing Configuration Guide for information about routing protocol peering or static redistribution.

Configuration Examples for Configuring Basic Performance Routing

This section contains the following examples:

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
Information and configuration for the border router only functionality for Cisco IOS XE releases	"Performance Routing Border Router Only Functionality" module
Concepts and configuration tasks required to implement OER and PfR features using the OER syntax.	*Optimized Edge Routing Configuration Guide*

Technical Assistance

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

Feature Information for Configuring Basic Performance Routing

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

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

Table 1 Feature Information for Configuring Basic Performance Routing

Feature Name	Releases	Feature Information
Optimized Edge Routing	Cisco IOS XE Release 2.6.1	OER was introduced. Performance Routing is an extension of OER. **Note** In Cisco IOS XE Release 2.6.1, only OER syntax is available. **Note** Only border router functionality is included in the 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 routers being used as a border router must be a router running Cisco IOS Release 15.0(1)M.

Performance Routing Border Router Only Functionality

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

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

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 22
- PfR Border Router Operations, page 24

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 24
- Displaying PfR Border Router Information, page 27

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	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**key chain** *name-of-chain* **Example:** `Router(config)# key chain border1_PFR`	Enables key-chain authentication and enters key-chain configuration mode. • Key-chain authentication protects the communication session between both the master controller and the border router. The key ID and key string must match in order for communication to be established.

	Command or Action	Purpose
Step 4	**key** *key-id* **Example:** `Router(config-keychain)# key 1`	Identifies an authentication key on a key chain and enters key-chain key configuration mode. • The key ID must match the key ID configured on the master controller.
Step 5	**key-string** *text* **Example:** `Router(config-keychain-key)# key-string b1`	Specifies the authentication string for the key. • The authentication string must match the authentication string configured on the master controller. • Any level of encryption can be configured.
Step 6	**exit** **Example:** `Router(config-keychain-key)# exit`	Exits key-chain key configuration mode and returns to key-chain configuration mode.
Step 7	Repeat Step 6. **Example:** `Router(config-keychain)# exit`	Exits key-chain configuration mode and returns to global configuration mode.
Step 8	**oer border** **Example:** `Router(config)# oer border`	Enters OER border router configuration mode to configure a router as a border router. • The border router must be in the forwarding path and contain at least one external and internal interface.
Step 9	**local** *type number* **Example:** `Router(config-oer-br)# local GigabitEthernet 0/0/0`	Identifies a local interface on a PfR border router as the source for communication with an PfR master controller. • A local interface must be defined.
Step 10	**master** *ip-address* **key-chain** *key-chain-name* **Example:** `Router(config-oer-br)# master 10.1.1.1 key-chain border1_PFR`	Enters OER-managed border router configuration mode to establish communication with a master controller. • An IP address is used to identify the master controller. • The value for the key-chain-name argument must match the key-chain name configured in Step 3.

	Command or Action	Purpose
Step 11	**end** **Example:** `Router(config-oer-br)# end`	Exits OER Top Talker and Top Delay learning configuration mode and returns to privileged EXEC mode.

- What to Do Next, page 27

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    10.1.2.0/24       10.0.0.0/8        5000
```

Configuration Examples for PfR Border Router Only Functionality

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

Feature Information for 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 2 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	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. **Note** In Cisco IOS XE Release 2.6.1, only OER syntax is available. The following commands were introduced or modified by this feature: **show oer border passive cache**, **show oer master prefix**.

Performance Routing with NAT

Performance Routing (PfR) introduced support for the control of traffic class routing using static routing in networks using NAT with the introduction of a new keyword to an existing NAT command. When PfR and NAT functionality are configured on the same router and PfR controls the routing for a traffic class using static routing, some applications may fail to operate due to dropped packets. This dropping of packets behavior is seen when static routing is used to connect to multiple ISPs from the same router, PfR uses static routing to control the traffic class routing, and one or more of the ISPs use Unicast Reverse Path Forwarding (Unicast RPF) filtering for security reasons. The Cisco IOS XE Release 2 implementation of the PfR support for NAT is explained.

When the new keyword is configured, new NAT translations are given the source IP address of the interface that PfR has selected for the packet and PfR forces existing flows to be routed through the interface for which the NAT translation was created.

Finding Feature Information

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

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

Prerequisites for Performance Routing with NAT

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 Performance Routing with NAT

- On Cisco ASR 1000 Series Aggregation Services Routers running Cisco IOS XE Release 2.6.1, and later releases, the ability of PfR to control traffic class routing using static routing in networks using NAT does not support tunnels interfaces or DMVPN implementations.
- 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 Performance Routing with NAT

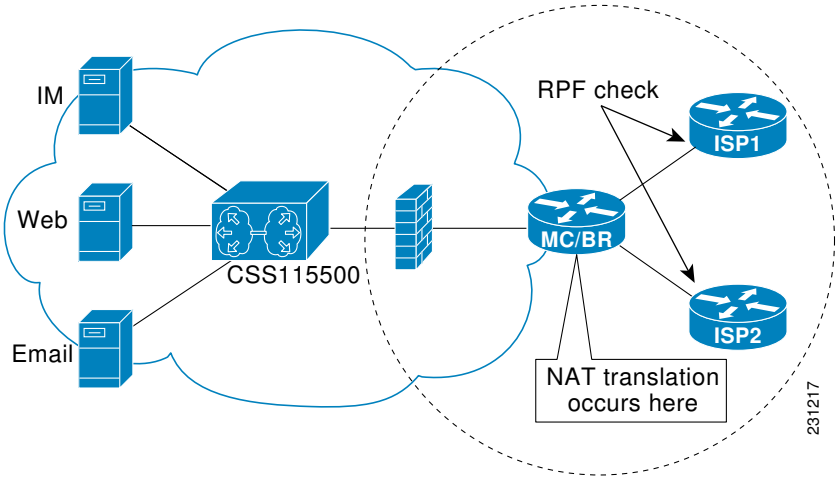
To configure PfR with NAT, you should understand the following concepts:

- PfR and NAT, page 34
- Network Address Translation (NAT), page 35
- Inside Global Addresses Overloading, page 35

PfR and NAT

When Cisco IOS PfR and NAT functionality are configured on the same router and PfR controls the routing for a traffic class using static routing, some applications may fail to operate due to dropped packets. This dropping of packets behavior is seen when static routing is used to connect to multiple ISPs from the same router, PfR uses static routing to control the traffic class routing, and one or more of the ISPs use Unicast Reverse Path Forwarding (Unicast RPF) filtering for security reasons. Packets are dropped at the ingress router performing Unicast RPF because PfR changes the route for an outgoing packet for a traffic class from one exit interface to another after the NAT translation from a private IP address to a public IP address is performed. When the packet is transmitted, Unicast RPF filtering at the ingress router (for example, an ISP router) will show a different source IP address from the source IP address pool assigned by NAT, and the packet is dropped. For example, the figure below shows how PfR works with NAT.

Figure 4 PfR with NAT



The NAT translation occurs at the router that is connected to the internal network, and this router can be a border router or a combined master controller and border router. If PfR changes routes to optimize traffic class performance and to perform load balancing, traffic from the border router in the figure above that was routed through the interface to ISP1 may be rerouted through the interface to ISP2 after the traffic performance is measured and policy thresholds are applied. The RPF check occurs at the ISP routers and any packets that are now routed through ISP2 will fail the RPF check at the ingress router for ISP2 because the IP address of the source interface has changed.

Note Only border router functionality is included in Cisco IOS XE Release 2.6, 3.1S and 3.2S images; no master controller configuration is available. The master controller that communicates with the Cisco ASR 1000 series router being used as a border router must be a router running Cisco IOS Release 15.0(1)M, or a later 15.0M release. In the diagram above, the router is just a border router, not a combined master controller and border router.

The solution involves a minimal configuration change with a new keyword, **oer**, that has been added to the**ip nat inside source** command. When the**oer** keyword is configured, new NAT translations are given the source IP address of the interface that PfR has selected for the packet and PfR forces existing flows to be routed through the interface for which the NAT translation was created. For example, PfR is configured to manage traffic on a border router with two interfaces, InterfaceA to ISP1 and InterfaceB to ISP2 in the figure above. PfR is first configured to control a traffic class representing Web traffic and the NAT translation for this traffic already exists with the source IP address in the packets set to InterfaceA. PfR measures the traffic performance and determines that InterfaceB is currently the best exit for traffic flows, but PfR does not change the existing flow. When PfR is then configured to learn and measure a traffic class representing e-mail traffic, and the e-mail traffic starts, the NAT translation is done for InterfaceB. The PfR static routing NAT solution is a single box solution and configurations with interfaces on multiple routers using NAT and managed by PfR are not supported. Network configurations using NAT and devices such as PIX firewalls that do not run Cisco IOS software are not supported.

Network Address Translation (NAT)

NAT enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) address in the internal network into legal addresses before packets are forwarded onto another network. NAT can be configured to advertise only one address for the entire network to the outside world. This ability provides additional security, effectively hiding the entire internal network behind that one address.

NAT is also used at the Enterprise edge to allow internal users access to the Internet and to allow Internet access to internal devices such as mail servers.

For more details about NAT, see the “Configuring NAT for IP Address Conservation” chapter of the *Cisco IOS IP Addressing Services Configuration Guide*.

Inside Global Addresses Overloading

You can conserve addresses in the inside global address pool by allowing the router to use one global address for many local addresses. When this overloading is configured, the router maintains enough information from higher-level protocols (for example, TCP or UDP port numbers) to translate the global address back to the correct local address. When multiple local addresses map to one global address, the TCP or UDP port numbers of each inside host distinguish between the local addresses.

How to Configure Performance Routing with NAT

This section contains the following tasks:

Configuring PfR to Control Traffic with Static Routing in Networks Using NAT

Perform this task to allow PfR to control traffic with static routing in a network using NAT. This task allows PfR to optimize traffic classes while permitting your internal users access to the internet.

When Cisco IOS PfR and NAT functionality are configured on the same router and PfR controls the routing for a traffic class using static routing, some applications may fail to operate due to dropped packets. This dropping of packets behavior is seen when static routing is used to connect to multiple ISPs from the same router, PfR uses static routing to control the traffic class routing, and one or more of the ISPs use Unicast Reverse Path Forwarding (Unicast RPF) filtering for security reasons.

In this task, the **oer** keyword is used with the **ip nat inside source** command. When the **oer** keyword is configured, new NAT translations are given the source IP address of the interface that PfR has selected for the packet and PfR forces existing flows to be routed through the interface where the NAT translation was created. This task uses a single IP address but an IP address pool can also be configured. For a configuration example using an IP address pool, see the configuration examples section.

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.

Note The PfR static routing NAT solution is a single box solution and configurations with interfaces on multiple routers using NAT and managed by PfR are not supported.

For more details about configuring NAT, see the “Configuring NAT for IP Address Conservation” chapter of the*Cisco IOS IP Addressing Services Configuration Guide*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**permit** | **deny**} *ip-address*mask
4. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
5. **match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*}
6. **match interface** *interface-type interface-number* [*...interface-type interface-number*]
7. **exit**
8. Repeat Step 4 through Step 7 for more route map configurations, as required.
9. **ip nat inside source** {**list** {*access-list-number* | *access-list-name*} | **route-map** *map-name*} {**interface** *type number* | **pool** *name*} [**mapping-id** *map-id* | **overload** | **reversible** | **vrf** *vrf-name*] [**oer**]
10. **interface** *type number*
11. **ip address** *ip-address mask*
12. **ip nat inside**
13. **exit**
14. **interface** *type number*
15. **ip address** *ip-address mask*
16. **ip nat outside**
17. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* {**permit**	**deny**} *ip-address*mask **Example:** `Router(config)# access-list 1 permit 10.1.0.0 0.0.255.255`	Defines a standard access list permitting the IP addresses that are to be translated. • The access list must permit only those addresses that are to be translated. (Remember that there is an implicit "deny all" at the end of each access list.) An access list that is too permissive can lead to unpredictable results.

	Command or Action	Purpose
Step 4	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **Example:** `Router(config)# route-map isp-1 permit 10`	Enters route-map configuration mode to configure a route map. • The example creates a route map named BGP.
Step 5	**match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*} **Example:** `Router(config-route-map)# match ip address access-list 1`	Creates an access list or prefix list match clause entry in a route map to identify traffic to be translated by NAT. • The example references the access list created in Step 3 that specifies the 10.1.0.0 0.0.255.255. prefix as match criteria.
Step 6	**match interface** *interface-type interface-number* [*...interface-type interface-number*] **Example:** `Router(config-route-map)# match interface serial 1/0`	Creates a match clause in a route map to distribute any routes that match out one of the interfaces specified. • The example creates a match clause to distribute routes that pass the match clause in Step 5 through serial interface 1/0.
Step 7	**exit** **Example:** `Router(config-route-map)# exit`	Exits route-map configuration mode and returns to global configuration mode.
Step 8	Repeat Step 4 through Step 7 for more route map configurations, as required.	—
Step 9	**ip nat inside source** {**list** {*access-list-number* | *access-list-name*} | **route-map** *map-name*} {**interface** *type number* | **pool** *name*} [**mapping-id** *map-id* | **overload** | **reversible** | **vrf** *vrf-name*] [**oer**] **Example:** `Router(config)# ip nat inside source interface GigabitEthernet 1/0/0 overload oer`	Establishes dynamic source translation with overloading, specifying the interface. • Use the **interface** keyword and type and number arguments to specify an interface. • Use the **oer** keyword to allow PfR to operate with NAT and control traffic class routing using static routing.
Step 10	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 1/0/0`	Specifies an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 11	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.114.11.8 255.255.255.0`	Sets a primary IP address for the interface.
Step 12	**ip nat inside** **Example:** `Router(config-if)# ip nat inside`	Marks the interface as connected to the inside.
Step 13	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to configuration mode.
Step 14	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 1/1/0`	Specifies a different interface and returns to interface configuration mode.
Step 15	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 172.17.233.208 255.255.255.0`	Sets a primary IP address for the interface.
Step 16	**ip nat outside** **Example:** `Router(config-if)# ip nat outside`	Marks the interface as connected to the outside.
Step 17	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for Performance Routing with NAT

The following example in this section shows a sample PfR link group configuration:

Configuring PfR to Control Traffic with Static Routing in Networks Using NAT Example

The following configuration example configures a master controller to allow PfR to control traffic with static routing in a network using NAT. This example shows how to use a pool of IP addresses for the NAT translation.

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.

In this example, a border router is connected to the Internet through two different ISPs. The configuration below allows PfR to optimize traffic classes while permitting the internal users access to the internet. In this example the traffic classes to be translated using NAT are specified using an access list and a route map. The use of a pool of IP addresses for NAT translation is then configured and the **oer** keyword is added to the **ip nat inside source** command to configure PfR to keep existing traffic classes flowing through the interface that is the source address that was translated by NAT. New NAT translations can be given the IP address of the interface that PfR has selected for the packet.

Note The PfR static routing NAT solution is a single box solution and configurations with interfaces on multiple routers using NAT and managed by PfR are not supported.

```
Router(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Router(config)# route-map isp-2 permit 10BGP permit 10
Router(config-route-map)# match ip address access-list 1
Router(config-route-map)# match interface serial 2/0
Router(config-route-map)# exit
Router(config)# ip nat pool ISP2 209.165.201.1 209.165.201.30 prefix-length 27
Router(config)# ip nat inside source route-map isp-2 pool ISP2 oer
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.1.11.8 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)# exit

Router(config)# interface serial 1/0
Router(config-if)# ip address 192.168.3.1 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# exit

Router(config)# interface serial 2/0
Router(config-if)# ip address 172.17.233.208 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# end
```

Feature Information for Performance Routing with NAT

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

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

Table 3 Feature Information for Performance Routing with NAT

Feature Name	Releases	Feature Information
Support for NAT and Static Routing[1]	Cisco IOS XE Release 2.6.1	Support to allow PfR to control traffic class routing using static routing in networks using NAT. This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. **Note** In Cisco IOS XE Release 2.6.1, only OER syntax is available. The following command was modified by this feature: **ip nat inside source**.

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