BGP Inbound Optimization Using Performance Routing

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

Finding Feature Information

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

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

Information About BGP Inbound Optimization Using Performance Routing

BGP Inbound Optimization

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

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

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

Prefix Traffic Class Learning Using PfR

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

PfR can automatically learn two types of prefixes:

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

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

PfR Link Utilization Measurement

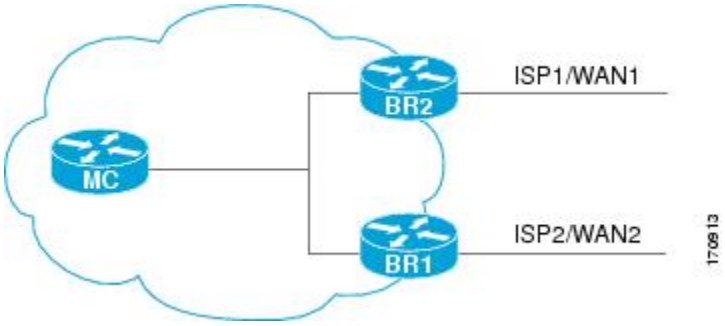
Link Utilization Threshold

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

Link Utilization Range

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

Figure 1: PfR network diagram



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

PfR Link Policies

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

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

The following performance characteristics are managed by link policies:

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

Traffic Load

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

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

Range

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

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

PfR Entrance Link Selection Control Techniques

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

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

BGP Autonomous System Number Prepend

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

BGP Autonomous System Number Community Prepend

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

PfR Map Operation for Inside Prefixes

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

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

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

Note Match precedence priority is not supported in PfR maps.

How to Configure BGP Inbound Optimization Using Performance Routing

Configuring PfR to Automatically Learn Traffic Classes Using Inside Prefixes

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

Before You Begin

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

Manually Selecting Inside Prefixes for PfR Monitoring

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

Modifying the PfR Link Utilization for Inbound Traffic

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **border** *ip-address* [**key-chain** *key-chain-name*]
5. **interface** *type number* **external**
6. **maximum utilization receive** {**absolute** *kbps* | **percent** *percentage*}
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure a router as a master controller and to configure global operations and policies.
Step 4	**border** *ip-address* [**key-chain** *key-chain-name*] **Example:** `Router(config-pfr-mc)# border 10.1.1.2`	Enters PfR-managed border router configuration mode to establish communication with a border router. • An IP address is configured to identify the border router. • At least one border router must be specified to create an PfR-managed network. A maximum of ten border routers can be controlled by a single master controller.

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

Modifying the PfR Entrance Link Utilization Range

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

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **max range receive percent** *percentage*
5. **end**

DETAILED STEPS

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

Configuring and Applying a PfR Policy to Learned Inside Prefixes

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

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr-map** *map-name sequence-number*
4. **match pfr learn inside**
5. **set delay** {**relative** *percentage* | **threshold** *maximum*}
6. **set loss** {**relative** *average* | **threshold** *maximum*}
7. **set unreachable** {**relative** *average* | **threshold** *maximum*}
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**pfr-map** *map-name sequence-number*	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes.

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

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

Configuring and Applying a PfR Policy to Configured Inside Prefixes

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr-map map-name** *sequence-number*
4. **match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name* [**inside**]
5. **set delay** {**relative** *percentage* | **threshold** *maximum*}
6. **set loss** {**relative** *average* | **threshold** *maximum*}
7. **set unreachable** {**relative** *average* | **threshold** *maximum*}
8. **end**

DETAILED STEPS

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

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

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

Configuration Examples for BGP Inbound Optimization Using Performance Routing

Example Configuring PfR to Automatically Learn Traffic Classes Using Inside Prefixes

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

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

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

Example Manually Selecting Inside Prefixes for PfR Monitoring

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

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

Example Modifying the PfR Link Utilization for Inbound Traffic

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

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

Example Modifying the PfR Entrance Link Utilization Range

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

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

Example Configuring and Applying a PfR Policy to Learned Inside Prefixes

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

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

Example Configuring and Applying a PfR Policy to Configured Inside Prefixes

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

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

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco IOS PfR commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS Performance Routing Command Reference
Basic PfR configuration for Cisco IOS XE releases	“Configuring Basic Performance Routing” module
Information about configuration for the border router only functionality for Cisco IOS XE Releases 3.1 and 3.2	“Performance Routing Border Router Only Functionality” module
Concepts required to understand the Performance Routing operational phases for Cisco IOS XE releases	“Understanding Performance Routing” module
Advanced PfR configuration for Cisco IOS XE releases	“Configuring Advanced Performance Routing” module
IP SLAs overview	“Cisco IOS IP SLAs Overview” module
PfR home page with links to PfR-related content on our DocWiki collaborative environment	PfR:Home

MIBs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for BGP Inbound Optimization Using Performance Routing

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

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

Table 1: Feature Information for BGP Inbound Optimization Using Performance Routing

Feature Name	Releases	Feature Information
OER BGP Inbound Optimization	Cisco IOS XE Release 3.3.S	PfR BGP inbound optimization supports best entrance selection for traffic that originates from prefixes outside an autonomous system destined for prefixes inside the autonomous system. External BGP (eBGP) advertisements from an autonomous system to an Internet service provider (ISP) can influence the entrance path for traffic entering the network. PfR uses eBGP advertisements to manipulate the best entrance selection. The following commands were introduced or modified by this feature: **clear pfr master prefix**, **downgrade bgp (PfR)**, **inside bgp (PfR)**, **match ip address (PfR)**, **match pfr learn**, **max range receive (PfR)**, **maximum utilization receive (PfR)**, **show pfr master prefix**.
expire after command[1]	Cisco IOS XE Release 3.3.S	The**expire after (PfR)**command is used to set an expiration period for learned prefixes. By default, the master controller removes inactive prefixes from the central policy database as memory is needed. This command allows you to refine this behavior by setting a time or session based limit. The time based limit is configured in minutes. The session based limit is configured for the number of monitor periods (or sessions).

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