PfR Voice Traffic Optimization Using Active Probes

This module documents a Performance Routing (PfR) solution that supports 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 provides automatic route optimization and load distribution for multiple connections between networks. PfR is an integrated Cisco IOS solution that allows you to monitor IP traffic flows and then define policies and rules based on prefix 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.

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 Voice Traffic Optimization Using Active Probes

Before implementing PfR optimization for voice traffic, you need to understand an overview of how PfR works and how to set up PfR network components. See the Understanding Performance Routing, Configuring Basic Performance Routing, and Configuring Advanced Performance Routing modules for more details.

Information About PfR Voice Traffic Optimization Using Active Probes

Voice Quality on IP Networks

Voice packets traveling through an IP network are no different from data packets. In the plain old telephone system (POTS), voice traffic travels over circuit-switched networks with predetermined paths and each phone call is given a dedicated connection for the duration of the call. Voice traffic using POTS has no resource contention issues, but voice traffic over an IP network has to contend with factors such as delay, jitter, and packet loss, which can affect the quality of the phone call.

Delay

Delay (also referred as latency) for voice packets is defined as the delay between when the packet was sent from the source device and when it arrived at a destination device. Delay can be measured as one-way delay or round-trip delay. The largest contributor to latency is caused by network transmission delay. Round-trip delay affects the dynamics of conversation and is used in Mean Opinion Score (MOS) calculations. One-way delay is used for diagnosing network problems. A caller may notice a delay of 200 milliseconds and try to speak just as the other person is replying because of packet delay. The telephone industry standard specified in ITU-T G.114 recommends the maximum desired one-way delay be no more than 150 milliseconds. Beyond a one-way delay of 150 milliseconds, voice quality is affected. With a round-trip delay of 300 milliseconds or more, users may experience annoying talk-over effects.

Jitter

Jitter means interpacket delay variance. When multiple packets are sent consecutively from source to destination, for example, 10 ms apart, and if the network is behaving ideally, the destination should be receiving them 10 ms apart. But if there are delays in the network (like queuing, arriving through alternate routes, and so on) the arrival delay between packets might be greater than or less than 10 ms. Using this example, a positive jitter value indicates that the packets arrived more than 10 ms apart. If the packets arrive 12 ms apart, then positive jitter is 2 ms; if the packets arrive 8 ms apart, then negative jitter is 2 ms. For delay-sensitive networks like VoIP, positive jitter values are undesirable, and a jitter value of 0 is ideal.

Packet Loss

Packet loss can occur due an interface failing, a packet being routed to the wrong destination, or congestion in the network. Packet loss for voice traffic leads to the degradation of service in which a caller hears the voice sound with breaks. Although average packet loss is low, voice quality may be affected by a short series of lost packets.

Mean Opinion Score (MOS)

With all the factors affecting voice quality, many people ask how voice quality can be measured. Standards bodies like the ITU have derived two important recommendations: P.800 (MOS) and P.861 (Perceptual Speech Quality Measurement [PSQM]). P.800 is concerned with defining a method to derive a Mean Opinion Score of voice quality. MOS scores range between 1 representing the worst voice quality, and 5 representing the best voice quality. A MOS of 4 is considered “toll-quality” voice.

Probes Used by PfR

PfR uses some of the IP SLA probes to help gather the data PfR requires to make its decisions.

Cisco IOS IP SLAs

Cisco IOS IP SLAs are an embedded feature set in Cisco IOS software and they allow you to analyze IP service levels for IP applications and services, to increase productivity, to lower operational costs, and to reduce occurrences of network congestion or outages. IP SLAs use active traffic monitoring--the generation of traffic in a continuous, reliable, and predictable manner--for measuring network performance. The accuracy of measured data is enhanced by enabling the IP SLAs Responder, available in Cisco routers, on the destination device. For more details about IP SLAs, see the *Cisco IOS IP SLAs Configuration Guide* .

Active Probe Types Used by PfR

The following types of active probes can be configured:

ICMP Echo--A ping is sent to the target address. PfR uses ICMP Echo probes, by default, when an active probe is automatically generated. Configuring an ICMP echo probe does not require knowledgeable cooperation from the target device. However, repeated probing could trigger an Intrusion Detection System (IDS) alarm in the target network. If an IDS is configured in a target network that is not under your control, we recommend that you notify the administrator of this target network.

Jitter--A jitter probe is sent to the target address. A target port number must be specified. A remote responder must be enabled on the target device, regardless of the configured port number.

TCP Connection--A TCP connection probe is sent to the target address. A target port number must be specified. A remote responder must be enabled if TCP messages are configured to use a port number other than TCP port number 23, which is well-known.

UDP Echo--A UDP echo probe is sent to the target address. A target port number must be specified. A remote responder must be enabled on the target device, regardless of which port number is configured.

Probe Frequency

The frequency of an active probe used by PfR is set by default to 60 seconds, but the frequency can be increased for each policy by configuring a lower time-interval between two probes. Increased probe frequency can reduce the response time and provide a better approximation of the MOS-low count percentage.

PfR Voice Traffic Optimization Using Active Probes

Configuring PfR to optimize voice traffic using active probes involves several decisions and subsequent branching tasks. The first step is to identify the traffic to be optimized and decide whether to use a prefix list or an access list. Use a prefix list to identify all traffic, including voice traffic, with a specific set of destination

prefixes. Use an access list to identify only voice traffic with a specific destination prefix and carried over a specific protocol.

The second step in optimizing voice traffic is to configure active probing using the **active-probe** or **set active-probe** command to specify the type of active probe to be used. PfR also provides the ability to set a forced target assignment for the active probe.

The final step in optimizing voice traffic is to configure a PfR policy to set the performance metrics that you want PfR to apply to the identified traffic.

PfR Voice Performance Metrics

PfR voice traffic optimization provides support for outbound optimization of voice traffic on the basis of the voice performance metrics, delay, packet loss, jitter, and MOS. Delay, packet loss, jitter and MOS are important quantitative quality metrics for voice traffic, and these voice metrics are measured using PfR active probes. The IP SLA jitter probe is integrated with PfR to measure jitter (source to destination) and the MOS score in addition to measuring delay and packet loss. The jitter probe requires a responder on the remote side just like the UDP Echo probe. Integration of the IP SLA jitter probe type in PfR enhances the ability of PfR to optimize voice traffic. PfR policies can be configured to set the threshold and priority values for the voice performance metrics: delay, packet loss, jitter, and MOS.

Configuring a PfR policy to measure jitter involves configuring only the threshold value and not relative changes (used by other PfR features) because for voice traffic, relative jitter changes have no meaning. For example, jitter changes from 5 milliseconds to 25 milliseconds are just as bad in terms of voice quality as jitter changes from 15 milliseconds to 25 milliseconds. If the short-term average (measuring the last 5 probes) jitter is higher than the jitter threshold, the prefix is considered out-of-policy due to jitter. PfR then probes all exits, and the exit with the least jitter is selected as the best exit.

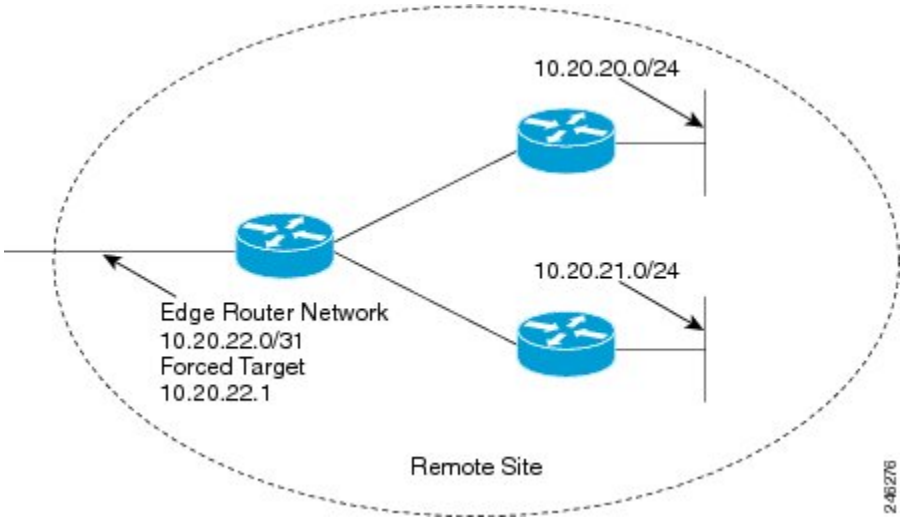
MOS policy works in a different way. There is no meaning to average MOS values, but there is meaning to the number of times that the MOS value is below the MOS threshold. For example, if the MOS threshold is set to 3.85 and if 3 out of 10 MOS measurements are below the 3.85 MOS threshold, the MOS-low-count is 30 percent. In the output of the **show** commands the field, ActPMOS, shows the number of actively monitored MOS packets with a percentage below threshold. If some of the MOS measurements are only slightly below the threshold, with percentage rounding, an ActPMOS value of zero may be displayed. When PfR runs a policy configured to measure MOS, both the MOS threshold value and the MOS-low-count percentage are considered. A prefix is considered out-of-policy if the short term (average over the last 5 probes) MOS-low-count percentage is greater than the configured MOS-low-count percentage. PfR then probes all exits, and the exit with the highest MOS value is selected as the best exit.

PfR Active Probe Forced Target Assignment

In earlier releases of the OER technology, the PfR active probe target is assigned to the longest matched prefix. There are some scenarios where you may want to use a target that does not match the destination prefix. The

example in the figure below explains a scenario in which configuring a PfR forced target assignment is more appropriate than using the longest match prefix.

Figure 1: PfR Forced Target Assignment Scenario



In the figure above we want to probe IP address 10.20.22.1 (at the edge of the network) for either network 10.20.21.0/24 or 10.20.22.0/24. Jitter is less likely to be introduced within the network so probing the edge of the network gives a measurement that is close to probing the final destination.

Forced target assignment allows you to assign a target to a group of prefixes or an application, even if they are not the longest match prefixes. Assigning a target can determine the true delay to the edge of a network rather than delay to an end host.

How to Configure PfR Voice Traffic Optimization Using Active Probes

Perform one of the first two optional tasks, depending on whether you want to use a prefix list or an access list to identify the traffic to be optimized. The third task can be used with traffic identified using an access list, and it also demonstrates how to use a forced target assignment. For an example configuration that can be used with traffic identified using a prefix list, see the “Example: Optimizing Traffic (Including Voice Traffic) Using Active Probes” section.

Identifying Traffic for PfR Using a Prefix List

Before traffic can be measured using PfR, it must be identified. Perform this task to use a prefix list to identify the traffic that PfR will probe.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length*| **permit** *network/length*}
4. **exit**

DETAILED STEPS

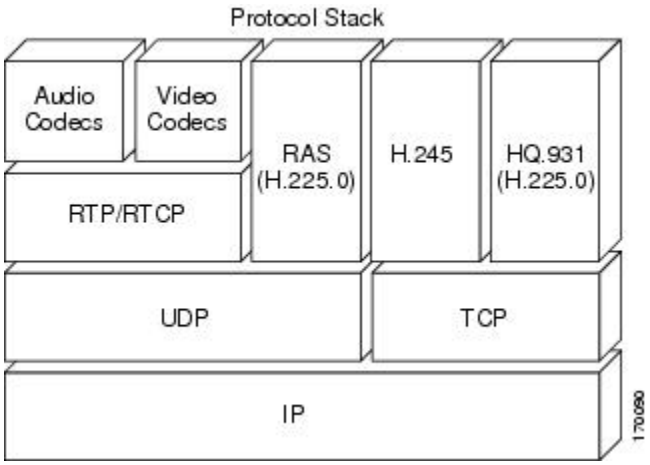
	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length*| **permit** *network/length*} **Example:** `Router(config)# ip prefix-list TRAFFIC_PFX_LIST seq 10 permit 10.20.21.0/24`	Creates an IP prefix list. • IP prefix lists are used to manually select prefixes for monitoring by the PfR master controller. • A master controller can monitor and control an exact prefix (/32), a specific prefix length, or a specific prefix length and any prefix that falls under the prefix length (for example, a /24 under a /16). • The prefixes specified in the IP prefix list are imported into a PfR map using the **match ip address** (PfR) command. • The example creates an IP prefix list named TRAFFIC_PFX_LIST that permits prefixes from the 10.20.21.0/24 subnet.
Step 4	**exit** **Example:** `Router(config)# exit`	(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Identifying Voice Traffic to Optimize Using an Access List

Before voice traffic can be measured, it must be identified. Perform this task to use an access list to identify the voice traffic.

Voice traffic uses a variety of protocols and streams on the underlying IP network. The figure below is a representation of the protocol options available for carrying voice traffic over IP. Most signaling traffic for voice is carried over TCP. Most voice calls are carried over User Datagram Protocol (UDP) and Real-Time Transport Protocol (RTP). You can configure your voice devices to use a specific range of destination port numbers over UDP to carry voice call traffic.

Figure 2: Protocol Stack Options Available for Voice Traffic



SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list** {**standard** | **extended**} *access-list-name*
4. [*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**log**] [**time-range** *time-range-name*] [**fragments**]
5. **exit**

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	**ip access-list** {**standard** | **extended**} *access-list-name* **Example:** `Router(config)# ip access-list extended VOICE_ACCESS_LIST`	Defines an IP access list by name. • PfR supports only named access lists. • The example creates an extended IP access list named VOICE_ACCESS_LIST.
Step 4	[*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**log**] [**time-range** *time-range-name*] [**fragments**] **Example:** `Router(config-ext-nacl)# permit udp any range 16384 32767 10.20.20.0 0.0.0.15 range 16384 32767`	Defines the extended access list. • Any protocol, port, or other IP packet header value can be specified. • The example is configured to identify all UDP traffic ranging from a destination port number of 16384 to 32767 from any source to a destination prefix of 10.20.20.0/24. This specific UDP traffic is to be optimized.
Step 5	**exit** **Example:** `Router(config)# exit`	(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Configuring PfR Voice Probes with a Target Assignment

After identifying the traffic (in this example, voice traffic identified using an access list) to be optimized, perform this task to configure the PfR jitter probes and assign the results of the jitter probes to optimize the identified traffic. In this task, the PfR active voice probes are assigned a forced target for PfR instead of the usual longest match assigned target. Before configuring the PfR jitter probe on the source device, the IP SLAs Responder must be enabled on the target device (the operational target). The IP SLAs Responder is available only on Cisco IOS software-based devices. Start this task at the network device that runs the IP SLAs Responder.

Note The device that runs the IP SLAs Responder does not have to be configured for PfR.

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

Before You Begin

Before configuring this task, perform the Identifying Voice Traffic to Optimize Using an Access List task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla monitor responder**
4. **exit**
5. Move to the network device that is the PfR master controller.
6. **enable**
7. **configure terminal**
8. **pfr-map** *map-name sequence-number*
9. **match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*}
10. **set active-probe** *probe-type ip-address* [**target-port** *number*] [**codec** *codec-name*]
11. **set probe frequency** *seconds*
12. **set jitter threshold** *maximum*
13. **set mos** {**threshold** *minimum* **percent** *percent*}
14. **set resolve** {**cost priority** *value* | **delay priority** *value* **variance** *percentage* | **jitter priority** *value* **variance** *percentage* | **loss priority** *value* **variance** *percentage* | **mos priority** *value* **variance** *percentage* | **range priority** *value* | **utilization priority** *value* **variance** *percentage*}
15. **set resolve mos priority** *value* **variance** *percentage*
16. **set delay** {**relative** *percentage* | **threshold** *maximum*}
17. **exit**
18. **pfr master**
19. **policy-rules** *map-name*
20. **end**
21. **show pfr master active-probes** [**appl**| **forced**]
22. **show pfr master policy** {*sequence-number*|*policy-name* | **default**}

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ip sla monitor responder** **Example:** `Router(config)# ip sla monitor responder`	Enables the IP SLAs Responder.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	Move to the network device that is the PfR master controller.	--
Step 6	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 7	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 8	**pfr-map** *map-name sequence-number* **Example:** `Router(config)# pfr-map TARGET_MAP 10`	Enters PfR map configuration mode to configure a PfR map to apply policies to selected IP prefixes. • Only one match clause can be configured for each PfR map sequence. • Deny sequences are first defined in an IP prefix list and then applied with the **match ip address** (PfR) command in Step 9 . • The example creates a PfR map named TARGET_MAP.
Step 9	**match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*} **Example:** `Router(config-pfr-map)# match ip address access-list VOICE_ACCESS_LIST`	References an extended IP access list or IP prefix as match criteria in a PfR map. • Only a single match clause can be configured for each PfR map sequence. • The example configures the IP access list named VOICE_ACCESS_LIST as match criteria in a PfR map. The access list was created in the "Identifying Voice Traffic to Optimize Using an Access List" task.
Step 10	**set active-probe** *probe-type ip-address* [**target-port** *number*] [**codec** *codec-name*]	Creates a set clause entry to assign a target prefix for an active probe. • The **echo** keyword is used to specify the target IP address of a prefix to actively monitor using Internet Control Message Protocol (ICMP) echo (ping) messages.

	Command or Action	Purpose
	Example: `Router(config-pfr-map)# set active-probe jitter 10.20.22.1 target-port 2000 codec g729a`	• The **jitter** keyword is used to specify the target IP address of a prefix to actively monitor using jitter messages. • The **tcp-conn** keyword is used to specify the target IP address of a prefix to actively monitor using Internet Control Message Protocol (ICMP) echo (ping) messages. • The **udp-echo** keyword is used to specify the target IP address of a prefix to actively monitor using Internet Control Message Protocol (ICMP) echo (ping) messages. • The example creates a set clause entry to specify the target IP address of a prefix and a specific port number to actively monitor using jitter.
Step 11	**set probe frequency** *seconds* **Example:** `Router(config-pfr-map)# set probe frequency 10`	Creates a set clause entry to set the frequency of the PfR active probe. • The *seconds* argument is used to set the time, in seconds, between the active probe monitoring of the specified IP prefixes. • The example creates a set clause to set the active probe frequency to 10 seconds.
Step 12	**set jitter threshold** *maximum* **Example:** `Router(config-pfr-map)# set jitter threshold 20`	Creates a set clause entry to configure the jitter threshold value. • The **threshold** keyword is used to configure the maximum jitter value, in milliseconds. • The example creates a set clause that sets the jitter threshold value to 20 for traffic that is matched in the same PfR map sequence.
Step 13	**set mos** {**threshold** *minimum* **percent** *percent*} **Example:** `Router(config-pfr-map)# set mos threshold 4.0 percent 30`	Creates a set clause entry to configure the MOS threshold and percentage values used to decide whether an alternate exit is be selected. • The **threshold** keyword is used to configure the minimum MOS value. • The **percent** keyword is used to configure the percentage of MOS values that are below the MOS threshold. • PfR calculates the percentage of MOS values below the MOS threshold that are recorded in a five-minute period. If the percentage value exceeds the configured percent value or the default value, the master controller searches for alternate exit links. • The example creates a set clause that sets the threshold MOS value to 4.0 and the percent value to 30 percent for traffic that is matched in the same PfR map sequence.
Step 14	**set resolve** {**cost priority** *value* | **delay priority** *value* **variance** *percentage* | **jitter priority** *value* **variance** *percentage* | **loss priority** *value* **variance**	Creates a set clause entry to configure policy priority or resolve policy conflicts. • This command is used to set priority for a policy type when multiple policies are configured for the same prefix. When this command is

	Command or Action	Purpose
	percentage | **mos priority** *value* **variance** *percentage* | **range priority** *value* | **utilization priority** *value* **variance** *percentage*} **Example:** `Router(config-pfr-map)# set resolve jitter priority 1 variance 10`	configured, the policy with the highest priority will be selected to determine the policy decision. • The **priority** keyword is used to specify the priority value. Configuring the number 1 assigns the highest priority to a policy. Configuring the number 10 assigns the lowest priority. • Each policy must be assigned a different priority number. • The **variance**keyword is used to set an allowable variance for a user-defined policy. This keyword configures the allowable percentage that an exit link or prefix can vary from the user-defined policy value and still be considered equivalent. • Variance cannot be configured for cost or range policies. • The example creates set clause that configures the priority for jitter policies to 1 for voice traffic. The variance is configured to allow a 10 percent difference in jitter statistics before a prefix is determined to be out-of-policy.
Step 15	**set resolve mos priority** *value* **variance** *percentage* **Example:** `Router(config-pfr-map)# set resolve mos priority 2 variance 15`	Creates a set clause entry to configure policy priority or resolve policy conflicts. • The example creates set clause that configures the priority for MOS policies to 2 for voice traffic. The variance is configured to allow a 15 percent difference in MOS values before a prefix is determined to be out-of-policy. **Note** Only the syntax applicable to this task is used in this example. For more details, see Step 14.
Step 16	**set delay** {**relative** *percentage* | **threshold** *maximum*} **Example:** `Router(config-pfr-map)# set delay threshold 100`	Creates a set clause entry to configure the delay threshold. • The delay threshold can be configured as a relative percentage or as an absolute value for match criteria. • The **relative** keyword is used to configure a relative delay percentage. The relative delay percentage is based on a comparison of short-term and long-term measurements. • The **threshold** keyword is used to configure the absolute maximum delay period in milliseconds. • The example creates a set clause that sets the absolute maximum delay threshold to 100 milliseconds for traffic that is matched in the same PfR map sequence.
Step 17	**exit** **Example:** `Router(config-pfr-map)# exit`	Exits PfR map configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 18	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR 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 19	**policy-rules** *map-name* **Example:** `Router(config-pfr-mc)# policy-rules TARGET_MAP`	Applies a configuration from a PfR map to a master controller configuration in PfR master controller configuration mode. • Reentering this command with a new PfR map name will immediately overwrite the previous configuration. This behavior is designed to allow you to quickly select and switch between predefined PfR maps. • The example applies the configuration from the PfR map named TARGET_MAP.
Step 20	**end** **Example:** `Router(config-pfr-mc)# end`	Exits PfR master controller configuration mode and enters privileged EXEC mode.
Step 21	**show pfr master active-probes** [**appl**| **forced**] **Example:** `Router# show pfr master active-probes forced`	Displays connection and status information about active probes on a PfR master controller. • The output from this command displays the active probe type and destination, the border router that is the source of the active probe, the target prefixes that are used for active probing, and whether the probe was learned or configured. • The **appl** keyword is used to filter the output to display information about applications optimized by the master controller. • The **forced** keyword is used to show any forced targets that are assigned. • The example displays connection and status information about the active probes generated for voice traffic configured with a forced target assignment.
Step 22	**show pfr master policy** {*sequence-number*|*policy-name* | **default**} **Example:** `Router# show pfr master policy TARGET_MAP`	Displays policy settings on a PfR master controller. • 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 *sequence-number* argument is used to display policy settings for the specified PfR map sequence.

	Command or Action	Purpose
		• The *policy-name* argument is used to display policy settings for the specified PfR policy map name. • The **default** keyword is used to display only the default policy settings. • The example displays the policy settings configured for the TARGET_MAP policy.

Examples

This example shows output from the **show pfr master active-probes forced** command. The output is filtered to display only connection and status information about the active probes generated for voice traffic configured with a forced target assignment.

```
Router# show pfr master active-probes forced
OER Master Controller active-probes
Border   = Border Router running this Probe
Policy   = Forced target is configure under this policy
Type     = Probe Type
Target   = Target Address
TPort    = Target Port
N - Not applicable
The following Forced Probes are running:
Border          State    Policy            Type     Target          TPort
10.20.20.2     ACTIVE    40                jitter   10.20.22.1      3050
10.20.21.3     ACTIVE    40                jitter   10.20.22.4      3050
```

Configuration Examples for PfR Voice Traffic Optimization Using Active Probes

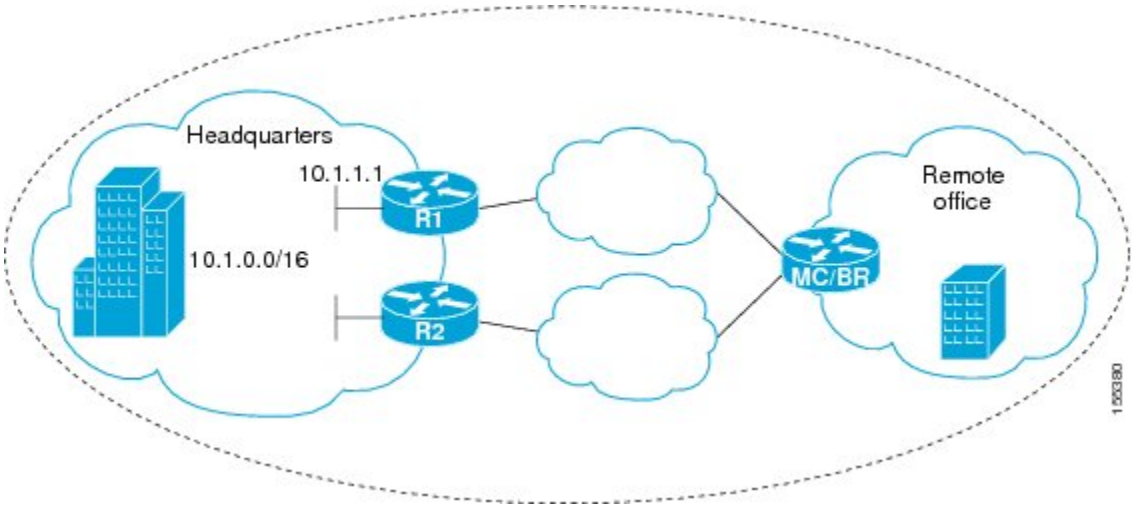
The following examples show both how to use an access list to identify only voice traffic to be optimized by PfR and to use a prefix list to identify traffic that includes voice traffic to be optimized by PfR.

Example Optimizing Only Voice Traffic Using Active Probes

The figure below shows that voice traffic originating at the remote office and terminating at the headquarters has to be optimized to select the best path out of the remote office network. Degradation in voice (traffic)

quality is less likely to be introduced within the network, so probing the edge of the network gives a measurement that is close to probing the final destination.

Figure 3: PfR Network Topology Optimizing Voice Traffic Using Active Probes



This configuration optimizes voice traffic to use the best performance path, whereas all other traffic destined to the same network--10.1.0.0/16--will follow the best path as indicated by a traditional routing protocol, for example BGP, that is configured on the device. As part of this optimization, PfR will use policy based routing (PBR) to set the best exit link for voice traffic within a device.

The following configuration is performed on the edge router R1 in the figure above in the headquarters network to enable the IP SLAs Responder.

```
enable
configure terminal
 ip sla responder
 exit
```

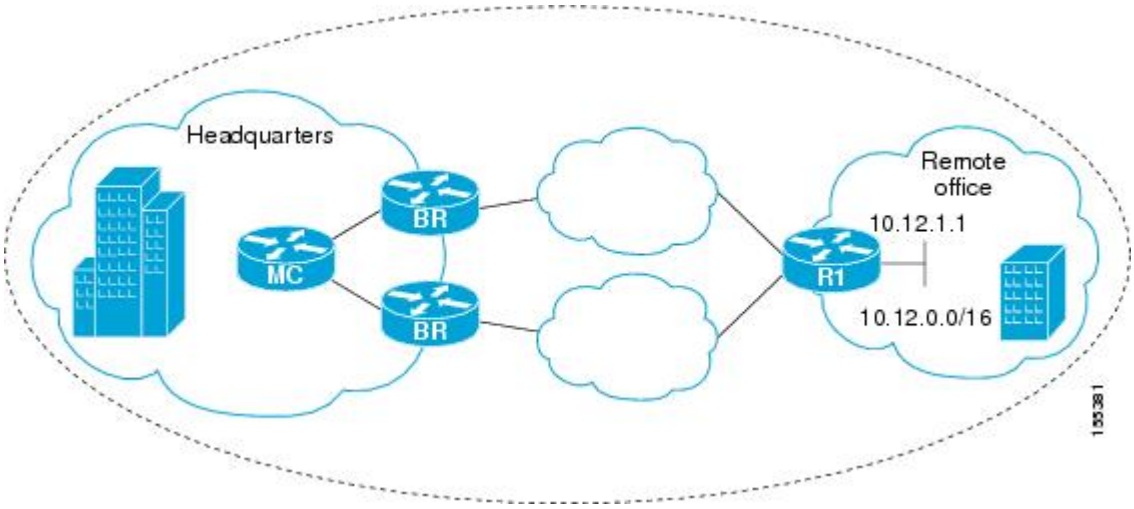
The following configuration is performed on the edge router MC/BR (which is both a PfR master controller and border router) in the figure above in the remote office network to optimize voice traffic using active probes.

```
enable
configure terminal
ip access-list extended Voice_Traffic
 10 permit udp any 10.1.0.0 0.0.255.255 range 16384 32767
 exit
pfr-map Voice_MAP 10
 match ip address access-list Voice_Traffic
 set active-probe jitter 10.1.1.1 target-port 1025 codec g711alaw
 set delay threshold 300
 set mos threshold 3.76 percent 30
 set jitter threshold 15
 set loss relative 5
 resolve mos priority 1
 resolve jitter priority 2
 resolve delay priority 3
 resolve loss priority 4
```

Example Optimizing Traffic (Including Voice Traffic) Using Active Probes

The figure below shows that traffic originating in the headquarters network and destined for the remote office network has to be optimized based on voice traffic metrics. Voice traffic is one of the most important traffic classes that travel from the headquarters to the remote office network, so the voice traffic must be prioritized to be optimized. Degradation in voice packet quality is less likely to be introduced within the network, so probing the edge of the network gives a measurement that is close to probing the final destination.

Figure 4: PfR Network Topology for Optimizing All Traffic Using Active Probes



This configuration optimizes all traffic, including voice traffic, destined for the 10.12.0.0/16 network. The PfR optimization is based on the measurement of voice performance metrics with thresholding values using active probes. As part of the optimization, PfR will introduce a BGP or a static route into the headquarters network. For more details about BGP and static route optimization, see the "Understanding Performance Routing" module.

The following configuration is performed on router R1 in the figure above in the remote office network to enable the IP SLAs Responder.

```
enable
configure terminal
 ip sla responder
 exit
```

The following configuration is performed on one of the BR routers in the figure above in the headquarters network to optimize all traffic (including voice traffic) using active probes.

```
enable
configure terminal
 ip prefix-list All_Traffic_Prefix permit 10.12.0.0/16
 pfr-map Traffic_MAP 10
 match ip address prefix-list All_Traffic_Prefix
 set active-probe jitter 10.12.1.1 target-port 1025 codec g711alaw
! port 1025 for the target probe is an example.
 set delay threshold 300
 set mos threshold 3.76 percent 30
 set jitter threshold 15
 set loss relative 5
 resolve mos priority 1
```

```
resolve jitter priority 2
resolve delay priority 3
resolve loss priority 4
```

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 PfR Voice Traffic Optimization Using Active Probes

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

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

Table 1: Feature Information for PfR Voice Traffic Optimization Using Active Probes

Feature Name	Releases	Feature Information
PfR Voice Traffic Optimization	Cisco IOS XE Release 3.3S	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. The following commands were introduced or modified by this feature: **active-probe (PfR)**, **jitter (PfR)**, **mos (PfR)**, **resolve (PfR)**, **set active-probe (PfR)**, **set jitter (PfR)**, **set mos (PfR)**, **set probe (PfR)**, **set resolve (PfR)**, **show pfr master active-probes**, **show pfr master policy**, and **show pfr master prefix**.