Performance Routing Link Groups

The Performance Routing - Link Groups feature introduced the ability to define a group of exit links as a preferred set of links, or a fallback set of links for Performance Routing (PfR) to use when optimizing traffic classes specified in a PfR policy.

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 Performance Routing Link Groups

Performance Routing Link Grouping

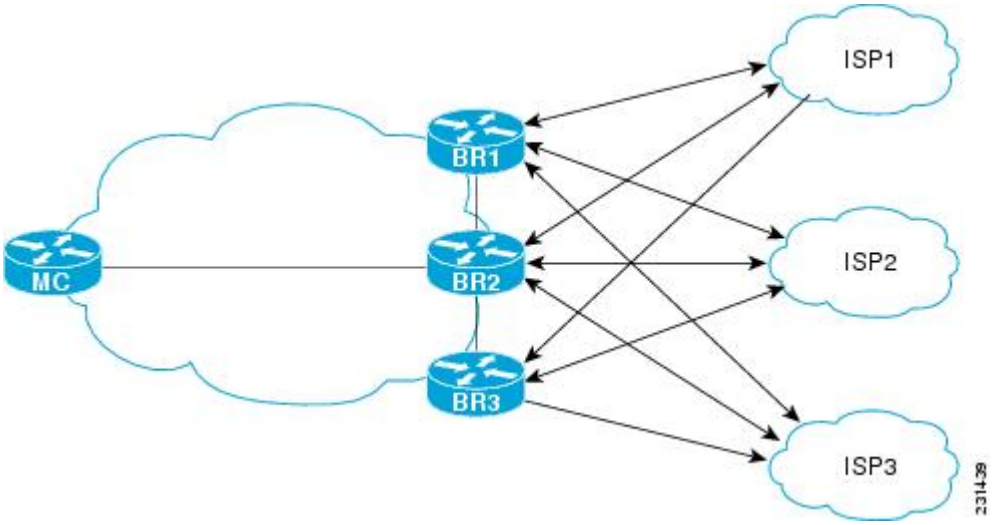
The Performance Routing Link Groups feature introduced the ability to define a group of exit links as a preferred set of links, or a fallback set of links for PfR to use when optimizing traffic classes specified in an PfR policy. PfR currently selects the best link for a traffic class based on the preferences specified in a policy and the traffic class performance—using parameters such as reachability, delay, loss, jitter or MOS—on a path out of the specified link. Bandwidth utilization, cost, and the range of links can also be considered in

selecting the best link. Link grouping introduces a method of specifying preferred links for one or more traffic classes in an PfR policy so that the traffic classes are routed through the best link from a list of preferred links, referred to as the primary link group. A fallback link group can also be specified in case there are no links in the primary group that satisfy the specified policy and performance requirements. If no primary group links are available, the traffic classes are routed through the best link from the fallback group. To identify the best exit, PfR probes links from both the primary and fallback groups.

Primary and fallback link groups can be configured at the master controller and are identified using a unique name. Link groups provide a method of grouping links such as high bandwidth links to be used, for example, by video traffic, by configuring an PfR policy to specify that the best link is to be selected from the link group that consists of only high bandwidth links. The traffic classes specified in a policy can be configured with only one primary link group and one fallback link group. The priority of a link group can vary between policies, a link group might be a primary link group for one policy, and a fallback link group for another policy.

See the figure below for an example of how to implement link grouping. Three link groups, ISP1, ISP2, and ISP3 represent different Internet Service Providers (ISPs) and all three ISPs have links to interfaces on the three border routers shown in the figure below. ISP1 links are the most expensive links, but they have the best Service Level Agreement (SLA) guarantees. ISP3 links are best effort links, and these links are the cheapest links. ISP2 links are not as good as the ISP1 links, but the ISP2 links are more reliable than the ISP3 links. The cost of the ISP2 links is higher than the ISP3 links, but lower than ISP1 links. In this situation, each ISP is created as a link group and associated with an interface on each border router shown in the figure below.

Figure 1: Link Group Diagram



Assuming four types of traffic class, video, voice, FTP, and data, each traffic class can be routed through a border router interface belonging to an appropriate link group. Video and voice traffic classes need the best links so the ISP1 link group is configured as the primary link group, with ISP2 as the fallback group. FTP traffic needs reliable links but the cost might be a factor so ISP2 is assigned as the primary group, and ISP3 is the fallback link group. Note that although ISP1 provides the most reliable links, it may be too expensive for file transfer traffic. For data traffic, ISP3 is a good choice as a primary link group, with ISP2 as the fallback group.

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.

Spillover

Performance routing link groups can be used to support spillover. Spillover is when there are two paths through the network--traffic engineering (TE) tunnels, for example--to the same provider edge (PE) router, but the tunnels take different paths across the network and the traffic is sent through one tunnel until it reaches a traffic load threshold when it spills over to the second tunnel. Using PfR link groups one tunnel is created as a primary link group and the second tunnel is the fallback link group. When the first tunnel goes out of policy, PfR switches to the fallback tunnel link group, which provides the spillover capacity until the traffic load on the first tunnel drops below the threshold. The tunnels must be established before the PfR link groups are configured.

How to Configure Performance Routing Link Groups

Implementing Performance Routing Link Groups

Perform this task on a master controller to set up some performance routing link groups by identifying an exit link on a border router as a member of a link group, and to create a PfR map to specify link groups for traffic classes defined in a PfR policy. In this task, a link group is set up for video traffic and a set of high bandwidth exit links are identified as members of the video link group which is identified as a primary link group. A fallback link group is also specified.

A PfR policy is created using an PfR map where the primary and fall link groups are specified for traffic classes matching the PfR map criteria. PfR probes both the primary and fallback group links and selects the best link in the primary link group for the traffic class specified in this task. If none of the primary links are within policy, PfR selects the bast link from the fallback group. For more details about link groups, see the “Performance Routing Link Grouping” section.

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.

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. **link-group** *link-group-name* [*link-group-name* [*link-group-name*]]
7. **exit**
8. Repeat Step 5 through Step 7 with appropriate changes to set up link groups for all the external interface.
9. **interface** *type number* **internal**
10. **exit**
11. **ip access-list** {**standard** | **extended**} *access-list-name*
12. [*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**dscp** *dscp-value*]
13. Repeat Step 12 for more access list entries, as required.
14. **exit**
15. **pfr-map** *map-name sequence-number*
16. **match traffic-class access-list** *access-list-name*
17. **set link-group** *link-group-name* [**fallback** *link-group-name*]
18. **end**
19. **show pfr master link-group** [*link-group-name*]

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. • 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).

	Command or Action	Purpose
Step 4	**border** *ip-address* [**key-chain** *key-chain-name*] **Example:** `Router(config-pfr-mc)# border 192.168.1.2 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 a 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 when the border router is set up. **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 a 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 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. **Tip** Configuring an interface as a PfR-managed external interface on a router enters PfR 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** (PfR) 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	**link-group** *link-group-name* [*link-group-name* [*link-group-name*]] **Example:** `Router(config-pfr-mc-br-if)# link-group VIDEO`	Configures a PfR border router exit interface as a member of a link group. • Use the *link-group-name* to specify the link group name for the interface. • Up to three link groups can be specified for each interface. • In this example, the GigabitEthernet 0/0/0 external interface is configured as a member of the link group named VIDEO. **Note** The **link-group** (PfR) command associates a link group with an interface. Another step, Step 17, uses the **set link-group** (PfR) command to identify the link group as a primary or fallback group for traffic classes defined in a PfR map.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config-pfr-mc-br-if)# exit`	Exits PfR-managed border exit interface configuration mode and returns to PfR-managed border router configuration mode.
Step 8	Repeat Step 5 through Step 7 with appropriate changes to set up link groups for all the external interface.	--
Step 9	**interface** *type number* **internal** **Example:** `Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/1 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.
Step 10	**exit** **Example:** `Router(config-pfr-mc-br)# exit`	Exits PfR-managed border configuration mode and returns to global configuration mode.
Step 11	**ip access-list** {**standard** | **extended**} *access-list-name* **Example:** `Router(config)# ip access-list extended ACCESS_VIDEO`	Defines an IP access list by name and enters extended named access list configuration mode. • PfR supports only named access lists. • The example creates an extended IP access list named ACCESS_VIDEO.
Step 12	[*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**dscp** *dscp-value*] **Example:** `Router(config-ext-nacl)# permit tcp any any 500`	Sets conditions to allow a packet to pass a named IP access list. • The example is configured to identify all TCP traffic from any destination or source and from destination port number of 500. This specific TCP traffic is to be optimized.
Step 13	Repeat Step 12 for more access list entries, as required.	--
Step 14	**exit** **Example:** `Router(config-ext-nacl)# exit`	(Optional) Exits extended named access list configuration mode and returns to global configuration mode.
Step 15	**pfr-map** *map-name sequence-number*	Enters PfR map configuration mode to configure a PfR map.

	Command or Action	Purpose
	Example: `Router(config)# pfr-map VIDEO_MAP 10`	• Only one match clause can be configured for each PfR map sequence. • Permit sequences are first defined in an IP prefix list and then applied with the **match ip address** (PfR) command in Step 16 . • The example creates n PfR map named VIDEO_MAP.
Step 16	**match traffic-class access-list** *access-list-name* **Example:** `Router(config-pfr-map)# traffic-class access-list ACCESS_VIDEO`	Manually configures an access list as match criteria used to create traffic classes using a PfR map. • Each access list entry must contain a destination prefix and may include other optional parameters. • The example defines a traffic class using the criteria defined in the access list named ACCESS_VIDEO.
Step 17	**set link-group** *link-group-name* [**fallback** *link-group-name*] **Example:** `Router(config-pfr-map)# set link-group video fallback voice`	Specifies a link group for traffic classes defined in a PfR map to create a PfR policy. • Use the *link-group-name* to specify the primary link group name for the policy. • Use the **fallback** keyword to specify the fallback link group name for the policy. • The example specifies the VIDEO link group as the primary link group for the traffic class matching the access list ACCESS_VIDEO. The link group VOICE is specified as the fallback link group.
Step 18	**end** **Example:** `Router(config-pfr-map)# end`	(Optional) Exits PfR map configuration mode and returns to privileged EXEC mode.
Step 19	**show pfr master link-group** [*link-group-name*] **Example:** `Router# show pfr master link-group`	Displays information about configured PfR link groups. • Use the optional *link-group-name* argument to display information for the specified PfR link group. • If the *link-group-name* argument is not specified, information about all PfR link groups is displayed. • The example displays information about all configured link groups.

Example

The example output from the **show pfr master link-group** command displays information about performance routing link groups configured using PfR. In this example, the VIDEO link group is shown with other configured link groups.

```
Router# show pfr master link-group

link group video
  Border           Interface       Exit id
  192.168.1.2      Gi0/0/0         1
 link group voice
  Border           Interface       Exit id
  192.168.1.2      Gi0/0/0         1
  192.168.1.2      Gi0/0/1         2
  192.168.3.2      Gi0/0/3         4
 link group data
  Border           Interface       Exit id
  192.168.3.2      Gi0/0/2         3
```

Configuration Examples for Performance Routing Link Groups

Example Implementing Performance Routing Link Groups

The following example shows how to implement link groups. In this example, a PfR map named VIDEO_MAP is created to configure PfR to define a traffic class that matches an access list named ACCESS_VIDEO. The traffic class is configured to use a link group named VIDEO as the primary link group, and a fallback group named VOICE. The VIDEO link group may be a set of high bandwidth links that are preferred for video traffic.

```
enable
configure terminal
border 10.1.4.1
 interface GigabitEthernet 0/0/0 external
  link-group VIDEO
  exit
 interface GigabitEthernet 0/0/2 external
  link-group VOICE
  exit
 interface GigabitEthernet 0/0/1 internal
 exit
ip access-list extended ACCESS_VIDEO
 permit tcp any 10.1.1.0 0.0.0.255 eq 500
 permit tcp any 172.17.1.0 0.0.255.255 eq 500
 permit tcp any 172.17.1.0 0.0.255.255 range 700 750
 permit tcp 192.168.1.1 0.0.0.0 10.1.2.0 0.0.0.255 eq 800 any any dscp ef
 exit
pfr-map VIDEO_MAP 10
 match traffic-class access-list ACCESS_VIDEO
 set link-group VIDEO fallback VOICE
 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 Performance Routing Link Groups

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 Performance Routing Link Groups

Feature Name	Releases	Feature Information
Performance Routing - Link Groups	Cisco IOS XE Release 3.3S	The Performance Routing - Link Groups feature introduces the ability to define a group of exit links as a preferred set of links, or a fallback set of links for PfR to use when optimizing traffic classes specified in a PfR policy. The following commands were introduced or modified by this feature: **link-group (PfR)**, **set link-group (PfR)**, and **show pfr master link-group**.