PfR SNMP Traps v1.0

The PfR SNMP Traps v1.0 feature adds trap functionality to the existing Performance Routing (PfR) MIB and introduces a new MIB, CISCO-PFR-TRAPS-MIB. Simple Network Management Protocol (SNMP) traps are generated for PfR events that require a network operator to perform an action or identify potential trends or issues. Using new CLI command configuration, traps can also be generated for specific PfR traffic class events.

Information about PfR SNMP Traps v1.0

Components of SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for monitoring and managing devices in a network.

The SNMP framework has the following components, which are described in the following sections:

PfR SNMP Trap Objects

Master Controller Admin State Change Notify

The cpfrMCEntryNotify trap is generated for certain Performance Routing (PfR) master controller (MC) events such as when the MC changes administrative status, the MC is cleared and the last time it was cleared, the MC changes to observe or route control mode, and when MC logging is enabled. The following objects are included in the notification:

- cpfrMCAdminStatus
- cpfrMCClear
- cpfrMCControlMode
- cpfrMCLastClearTime

- cpfrMCLogLevel

Border Router Entry Notify

The cpfrBREntryNotify trap is generated when a border router (BR) goes to an up or down state. The following objects are included in the notification:

- cpfrBRAddress
- cpfrBRAddressType
- cpfrBRConnFailureReason
- cpfrBRConnStatus
- cpfrBROperStatus

Interface Entry Notify

The cpfrInterfaceEntryNotify trap is generated when an external or internal interface goes to an up or down state. The following objects are included in the notification:

- cpfrBRAddress
- cpfrBRAddressType
- cpfrExitName
- cpfrExitOperStatus
- cpfrExitType

Traffic Class Status Entry Notify

The cpfrTrafficClassStatusEntryNotify trap is generated under the following conditions:

- When the **trap-enable** command is configured under global configuration mode and a traffic class moves from being a primary link to a fallback link or goes into a default or out-of-policy status.
- When the **set trap-enable** command is configured under PfR map mode and a traffic class moves from being a primary link to a fallback link or goes into a default or out-of-policy status.

The following objects are included in the notification:

- cpfrBRAddress
- cpfrBRAddressType
- cpfrExitName
- cpfrLinkGroupType
- cpfrTCLastOOPReason
- cpfrTCStatus

How to Configure PfR SNMP Traps v1.0

Enabling the Generation of PfR SNMP Traps

Perform this task in global configuration mode to enable the generation of Simple Network Management Protocol (SNMP) traps for PfR events that require a network operator to take some action.

To generate specific traffic class-based traps, use the “Enabling PfR Traffic Class SNMP Traps” or the “Enabling PfR Traffic Class SNMP Traps Using a PfR Map” task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name* | **traps** | **informs** | **version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [**pfr**]
4. **snmp-server enable traps pfr**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name* | **traps** | **informs** | **version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [**pfr**] **Example:** `Device(config)# snmp-server host 10.2.2.2 traps public pfr`	Enables the delivery of an SNMP notification to a recipient. • In this example, PfR SNMP traps are delivered to the device with the IP address of 10.2.2.2.
Step 4	**snmp-server enable traps pfr** **Example:** `Device(config)# snmp-server enable traps pfr`	Enables generation of PfR SNMP notifications.
Step 5	**exit** **Example:**	Exits global configuration mode and enters privileged EXEC mode.

	Command or Action	Purpose
	`Device(config)# exit`	

Enabling the Generation of PfR Traffic Class SNMP Traps

Perform this task to enable Simple Network Management Protocol (SNMP) traps to be generated for PfR traffic class events.

The cpfrTrafficClassStatusEntryNotify trap is generated under the following conditions:

- When the **trap-enable** command is configured in PfR master controller configuration mode.
- When a traffic class moves from being a primary link to a fallback link.
- When a traffic class goes into a default or out-of-policy status.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **trap-enable**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**pfr master** **Example:** `Device(config)# pfr master`	Enters PfR master controller configuration mode to configure a Cisco router as a master controller.
Step 4	**trap-enable** **Example:** `Device(config-pfr-mc)# trap-enable`	Enables generation of PfR traffic class SNMP traps. • An SNMP trap is generated if a traffic class moves from being a primary link to a fallback link, goes into a default status, or goes into an out-of-policy (OOP) status.

	Command or Action	Purpose

Step 5	**end**
	Example:
	`Device(config-pfr-mc)# end`
		Exits PfR master controller configuration mode and enters privileged EXEC mode.

Enabling the Generation of PfR Traffic Class SNMP Traps Using a PfR Map

Perform this task to enable PfR Simple Network Management Protocol (SNMP) traps within a PfR map.

The cpfrTrafficClassStatusEntryNotify trap is generated under the following conditions:

- When the **set trap-enable** command is configured in PfR map configuration mode.
- When a traffic class moves from being a primary link to a fallback link.
- When a traffic class goes into a default or out-of-policy status.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr-map** *map-name sequence-number*
4. **match pfr learn** {**delay** | **inside** | **list** *ref-name* | **throughput**}
5. **set trap-enable**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**pfr-map** *map-name sequence-number* **Example:** `Device(config)# pfr-map TRAP_1 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.

	Command or Action	Purpose

Step 4	**match pfr learn** {**delay** | **inside** | **list** *ref-name* | **throughput**}
	Example:
	`Device(config-pfr-map)# match pfr learn list TRAP_1`
		References an extended IP access list or IP prefix as match criteria in a PfR map.

Step 5	**set trap-enable** **Example:** `Device(config-pfr-map)# set trap-enable`	Creates a set clause in a PfR map to enable the generation of PfR traffic class traps. • A PfR SNMP trap is generated if a traffic class moves from being a primary link to a fallback link, goes into a default status, or goes into an out-of-policy (OOP) status.

Step 6	**end**
	Example:
	`Device(config-pfr-map)# end`
		(Optional) Exits PfR map configuration mode and returns to privileged EXEC mode.

Configuration Examples for PfR SNMP Traps v1.0

Example: Enabling the Generation of PfR SNMP Traps

The following example shows how to enable the generation of PfR Simple Network Management Protocol (SNMP) traps:

```
Device> enable
Device# configure terminal
Device(config)# snmp-server host 10.2.2.2 traps public pfr
Device(config)# snmp-server enable traps pfr
```

Example: Enabling the Generation of PfR Traffic Class SNMP Traps

The following example shows the commands used to enable the generation of Simple Network Management Protocol (SNMP) traps for PfR traffic class events.

```
Device> enable
Device# configure terminal
Device(config)# pfr-master
Device(config-pfr-mc)# trap-enable
```

Example: Enabling the Generation of PfR Traffic Class SNMP Traps Using a PfR Map

The following example shows how to enable the generation of Simple Network Management Protocol (SNMP) traps for PfR traffic class events using a PfR map.

```
Device> enable
Device# configure terminal
Device(config)# pfr-map TRAPMAP 20
Device(config-pfr-map)# match pfr learn list TRAP-LIST
Device(config-pfr-map)# set mode monitor passive
Device(config-pfr-map)# set delay threshold 150
Device(config-pfr-map)# set resolve delay priority 1 variance 1
Device(config-pfr-map)# set trap-enable
```

Feature Information for PfR SNMP Traps v1.0

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 SNMP Traps v1.0

Feature Name	Releases	Feature Information
PfR SNMP Traps v1.0	Cisco IOS XE 3.7S	The PfR SNMP Traps v1.0 feature adds trap functionality to the existing PfR MIB. SNMP traps are generated for PfR events that require a network operator to perform an action or identify potential trends or issues The following commands were introduced or modified: **set trap-enable**, **snmp-server host**, **snmp-server enable traps pfr**, **trap-enable**.