Configuring Rate Limits

This chapter describes how to configure rate limits for supervisor-bound traffic on Cisco NX-OS devices.

This chapter includes the following sections:

About Rate Limits

Rate limits can prevent redirected packets for exceptions from overwhelming the supervisor module on a Cisco NX-OS device. You can configure rate limits in packets per second for the following types of redirected packets:

- Bidirectional forwarding detection (BFD) packets
- Sflow

Guidelines and Limitations for Rate Limits

Rate limits has the following configuration guidelines and limitations:

- You can set rate limits for supervisor-bound exception and redirected traffic. Use control plane policing (CoPP) for other types of supervisor-bound traffic.

Note Hardware rate-limiters protect the supervisor CPU from excessive inbound traffic. The traffic rate allowed by the hardware rate-limiters is configured globally and applied to each individual I/O module. The resulting allowed rate depends on the number of I/O modules in the system. CoPP provides more granular supervisor CPU protection by utilizing the modular quality-of-service CLI (MQC).

- You can configure a hardware rate-limiter to show statistics for outbound traffic on SPAN egress ports.

Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Default Settings for Rate Limits

This table lists the default settings for rate limits parameters.

Table 1: Default Rate Limits Parameters Settings

Parameters	Default
BFD packets rate limit	10,000 packets per second
Sflow	40,000 packets per second

Configuring Rate Limits

You can set rate limits on supervisor-bound traffic.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**hardware rate-limiter access-list-log** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter access-list-log 200`	Configures rate limits in packets per second for packets copied to the supervisor module for access list logging. The range is from 0 to 10000.

	Command or Action	Purpose
Step 3	**hardware rate-limiter bfd** *packets* [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter bfd 500`	Configures rate limits in packets per second for bidirectional forwarding detection (BFD) packets. The range is from 0 to 10000.
Step 4	**hardware rate-limiter exception** *packets* [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter exception 500`	Configures rate limits in packets per second for any exception traffic in the system that is not classified by the Control Plane Policing (CoPP) policy. The range is from 0 to 10000.
Step 5	**hardware rate-limiter layer-3 glean** *packets* [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-3 glean 500`	Configures rate limits in packets per second for Layer 3 glean packets. The range is from 0 to 10000. A node receiving traffic for a particular destination might be unable to forward traffic because it is unaware of the rewrite information or the physical layer interface behind which the destination resides. During this time, it is possible to install a glean entry in the data path for that destination. Because this might not be a pointer to the global punt adjacency, a reserved module or port value is used to punt such packets to the supervisor. This glean rate can be controlled using the given rate limiter. **Note** The CoPP policy controls the rate of glean packets that are forwarded due to global punt adjacency, and this rate limiter controls the destination-specific glean packets.
Step 6	**hardware rate-limiter layer-3 multicast local-groups** *packets* **Example:** `switch(config)# hardware rate-limiter layer-3 multicast local-groups 300`	Configures rate limits in packets per second for Layer 3 multicast data packets that are punted for initiating a shortest-path tree (SPT) join. The range is from 0 to 10000.
Step 7	**hardware rate-limiter span-egress** *rate* [**module** *module*] **Example:** `switch(config)# hardware rate-limiter span-egress 123`	Configures rate limits in kilobits per second for SPAN for egress traffic. The range is from 0 to 100000000. **Note** You should not configure both sFlow and the SPAN egress rate-limiter.

	Command or Action	Purpose
Step 8	(Optional) **show hardware rate-limiter** [**access-list-log | bfd |exception | fex | layer-3 glean | layer-3 multicast local-groups | span-egress |module** *module*] **Example:** `switch# show hardware rate-limiter`	Displays the rate limit configuration. The module range is from 1 to 30.
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Monitoring Rate Limits

You can monitor rate limits.

Procedure

	Command or Action	Purpose
Step 1	**show hardware rate-limiter** [**access-list-log** | **bfd** | **exception** | **fex** | **layer-3 glean** | **layer-3 multicast local-groups** | **span-egress** | **module** *module*] **Example:** `switch# show hardware rate-limiter access-list-log`	Displays the rate limit statistics.

Clearing the Rate Limit Statistics

You can clear the rate limit statistics.

Procedure

	Command or Action	Purpose
Step 1	**clear hardware rate-limiter** {**all** | **access-list-log** | **bfd** | **exception** | **fex** | **layer-3 glean** | **layer-3 multicast local-groups** [**module** *module*] } **Example:** `switch# clear hardware rate-limiter access-list-log`	Clears the rate limit statistics.

Verifying the Rate Limit Configuration

To display the rate limit configuration information, perform the following tasks:

Command	Purpose
show hardware rate-limiter [**access-list-log** | **bfd** | **exception** | **fex** | **layer-3 glean** | **layer-3 multicast local-groups** | **module** *module*]	Displays the rate limit configuration.

Configuration Examples for Rate Limits

The following example shows how to configure rate limits for packets copied to the supervisor module for access list logging:

```
switch(config)# hardware rate-limiter access-list-log
switch(config)# show hardware rate-limiter access-list-log
Units for Config: packets per second
Allowed, Dropped & Total: aggregated since last clear counters


Module: 4
  R-L Class           Config           Allowed         Dropped             Total
 +------------------+--------+---------------+---------------+-----------------
+
  access-list-log         100               0               0                 0

  Port group with configuration same as default configuration
      Eth4/1-36

Module: 22
  R-L Class           Config           Allowed         Dropped             Total
 +------------------+--------+---------------+---------------+-----------------
+
  access-list-log         100               0               0                 0

  Port group with configuration same as default configuration
      Eth22/1-0
```

Additional References for Rate Limits

This section includes additional information related to implementing rate limits.

Related Documents

Related Topic	Document Title
Cisco NX-OS licensing	*Cisco NX-OS Licensing Guide*