

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, on page 1
- Guidelines and limitations for rate limits, on page 2
- Default settings for rate limits, on page 2
- Configure rate limits, on page 3
- Monitor rate limits, on page 5
- Clear the rate limit statistics, on page 5
- Rate limit configuration verification commands, on page 6
- Configuration examples for rate limits, on page 6
- Additional references for rate limits, on page 7

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 for the following types of redirected packets:

- Access-list log packets
- Bidirectional Forwarding Detection (BFD) packets
- Catch-all exception traffic
- Fabric Extender (FEX) traffic
- Layer 3 glean packets
- Layer 3 multicast data packets
- SPAN egress traffic

For Cisco Nexus 9300-FX/FXP/FX2/FX3, and 9300-GX platform switches and Cisco Nexus 9500 platform switches with X97160YC-EX, 9700- FX line cards, the CoPP policer rate is kilo bits per second. For other Cisco Nexus 9000 Series switches, the CoPP policer rate is in packets per second; However, it is kilo bits per second for SPAN egress traffic.

Guidelines and limitations for rate limits

Use this reference to review the 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. This rate-limiter is supported on all Cisco Nexus 9000, 9300, and 9500 Series switches .
- The rate-limiter on egress ports is limited per pipe on the Cisco Nexus 9300 and 9500 Series switches .
- Cisco Nexus 9300 and 9500 Series switches support both local and ERSPAN. However, the rate-limiter only applies to ERSPAN. You must configure e-racl ACL TCAM region to enable the rate-limiter on these switches. For more information, see the Configuring ACL TCAM Region Sizes section in the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.
- For Cisco Nexus 9348GC-FXP, 93108TC-FX, 93180YC-FX Series switches , you should not configure both, sFlow and ERSPAN.
- Logging rate-limit is enabled by default. No default configuration is shown up in **show running-config** and in **show running-config all** . Use **show logging** cli to check if rate-limit is enabled. It has a dedicated field to verify if rate-limit is enabled or disabled.

  Once no logging rate-limit config is applied, it appears in the running-config and displayed in show logging output.
- The **rate-limit cpu direction** {**input** | **output** | **both**} **pps** *packets* **action log** command is not supported on Cisco Nexus 9000 Series switches.

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

Use this reference to review the default settings for rate limits.

The following table displays default settings for rate limits.

Table 1: Default rate limits parameters settings

Parameters	Default
Access-list log packets rate limit	100 packets per second
BFD packets rate limit	10000 packets per second
Exception packets rate limit	50 packets per second
FEX packets rate limit	12000 packets per second
Layer 3 glean packets rate limit	100 packets per second
Layer 3 multicast data packets rate limit	3000 packets per second
SPAN egress rate limit	No limit
R-L Class packets rate limit	100 packets per second
SPAN packets rate limit	50 packets per second
sFLOW packets rate limit	40000 kilobits per second
VXLAN-OAM packets rate limit	1000 packets per second
100M-ethports packets rate limit	10000 packets per second
SPAN egress disabled dot1x packets rate limit	3000 packets per second
MPLS-OAM packets rate limit	300 packets per second
Netflow packets rate limit	120000 packets per second
SSX packets rate limit	120000 packets per second
UCS-mgmt packets rate limit	120000 packets per second
MDNS packets rate limit	1024 packets per second

Configure rate limits

You can set rate limits on supervisor-bound traffic.

Procedure

Step 1 Use the **hardware rate-limiter access-list-log** {*packets* | **disable**} [**module** *module* [**port** *start end*]] to configure rate limits for packets that are copied to the supervisor module for access list logging. The range is 0–10000.

Example:

```
switch#configure terminal
switch(config)# hardware rate-limiter access-list-log 200
```

Step 2 Use the **hardware rate-limiter bfd** *packets* [**module** *module* [**port** *start end*]] command to configure rate limits for bidirectional forwarding detection (BFD) packets. The range is 0–10000.

Example:

```
switch(config)#hardware rate-limiter bfd 500
```

Step 3 Use the **hardware rate-limiter exception** *packets* [**module** *module* [**port** *start end*]] command to configure rate limits for any exception traffic in the system that is not classified by the Control Plane Policing (CoPP) policy. The range is 0–10000.

Example:

```
switch(config)#hardware rate-limiter exception 500
```

Step 4 use the **hardware rate-limiter fex** *packets* [**module** *module* [**port** *start end*]] command to configure rate limits for supervisor-bound FEX traffic. The range is 0–10000.

Example:

```
switch(config)#hardware rate-limiter fex 500
```

Step 5 Use the **hardware rate-limiter layer-3 glean** *packets* [**module** *module* [**port** *start end*]] command to configure rate limits for Layer 3 glean packets. The range is 0–10000.

Example:

```
switch(config)#hardware rate-limiter layer-3 glean 500
```

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 to CPU due to hit of global punt adjacency. The Layer 3 glean hardware rate-limiter limits the number of glean packets that are redirected to CPU by sup-redirect acess-list. This is used in special cases such as, in the VXLAN environment when the packet is received from an unknown VTEP.

Step 6 Use the **hardware rate-limiter layer-3 multicast local-groups** *packets* [**module** *module* [**port** *start end*]] command to configure rate limits for Layer 3 multicast data packets that are punted for initiating a shortest-path tree (SPT) join. The range is 0–10000.

Example:

```
switch(config)#hardware rate-limiter layer-3 multicast local-groups 300
```

Step 7 Use the **hardware rate-limiter span-egress** *rate* [**module** *module*] command to configure rate limits for SPAN for egress traffic. The range is 0–100000000.

Example:

```
switch(config)#hardware rate-limiter span-egress 123
```

Note
You should not configure both sFlow and the SPAN egress rate-limiter.

Step 8 (Optional) Use the **show hardware rate-limiter** [**access-list-log | bfd |exception | fex | layer-3 glean | layer-3 multicast local-groups |**] | **module** *module*] command to display the rate limit configuration. The module range is 1–30.

Example:

```
switch#show hardware rate-limiter
```

Step 9 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration. the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Monitor rate limits

You can monitor rate limits.

Procedure

Use the **show hardware rate-limiter** [**access-list-log** | **bfd** | **exception** | **fex** | **layer-3 glean** | **layer-3 multicast local-groups** | **span-egress** | **module** *module*] command to display the rate limit statistics.

Example:

```
switch#show hardware rate-limiter access-list-log
```

Clear the rate limit statistics

You can clear the rate limit statistics.

Procedure

Use the **clear hardware rate-limiter** {**all** | **access-list-log** | **bfd** | **exception** | **fex** | **layer-3 glean** | **layer-3 multicast local-groups** | **span-egress** [**module** *module*]} command to clear the rate limit statistics.

Example:

```
switch#clear hardware rate-limiter access-list-log
```

Rate limit configuration verification commands

Use this reference to verify the Rate limit configuration.

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

Table 2: Rate limit configuration verification commands

Command	Purpose
show hardware rate-limiter [**access-list-log** | **bfd** | **exception** | **fex** | **layer-3 glean** | **layer-3 multicast local-groups** | **span-egress** | **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#configure terminal
switch(config)#hardware rate-limiter access-list-log 200
switch(config)#exit
switch#show hardware rate-limiter access-list-log
Units for Config: kilo bits 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
```

The following example shows how the SPAN egress rate limiter might be in conflict with sFlow:

```
switch#configure terminal
switch(config)#hardware rate-limiter span-egress 123
Warning: This span-egress rate-limiter might affect functionality of sFlow
switch(config)#exit
switch#show hardware rate-limiter span-egress
Units for Config: kilo bits per second
Allowed, Dropped & Total: aggregated since Module: 1
R-L Class          Config            Allowed        Dropped           Total
+----------------+----------+--------------+--------------+----------------+
```

```
L3 glean                100            0              0              0
L3 mcast loc-grp       3000            0              0              0
access-list-log         100            0              0              0
bfd                   10000            0              0              0
exception                50            0              0              0
fex                    3000            0              0              0
span                     50            0              0              0
dpss                   6400            0              0              0
span-egress             123            0              0              0
<<configured
```

Additional references for rate limits

This section includes additional information related to implementing rate limits.

Table 3: Related documents

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