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:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your 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 "New and Changed Information"chapter or the Feature History table in this chapter.

Information 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:

- Access-list log packets
- Data and control packets copied to the supervisor module

- F1 Series module packets
  - rl-1 STP and Fabricpath-ISIS
  - rl-2 L3-ISIS and OTV-ISIS
  - rl-3 UDLD, LACP, CDP and LLDP
  - rl-4 Q-in-Q and ARP request
  - rl-5 IGMP, NTP, DHCP-Snoop, Port-Security and Mgmt traffic
- Layer 2 Tunneling Protocol (L2TP) packets
- Layer 2 multicast-snooping packets
- Layer 2 port-security packets
- Layer 2 storm-control packets
- Layer 2 virtual port channel (vPC) low packets
- Layer 3 control packets
- Layer 3 glean packets
- Layer 3 glean fast-path packets
- Layer 3 maximum transmission unit (MTU) check failure packets
- Layer 3 multicast data packets
- Layer 3 Time-to-Live (TTL) check failure packets
- Receive packets

Beginning in Cisco NX-OS Release 5.1, you can also configure rate limits for packets that reach the supervisor module.

Virtualization Support for Rate Limits

You can configure rate limits only in the default virtual device context (VDC), but the rate limits configuration applies to all VDCs on the Cisco NX-OS device. For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Guidelines and Limitations for Rate Limits

The rate limits feature 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).

- F1 Series modules support up to five rate limiters shared among all control traffic sent to the Supervisor module.

Note F2 Series modules do not support the five F1 Series module rate limiters.

- On F2, M1 and M2 Series modules, IP redirects will be rate limited according to the Layer 3 Time-to-Live (TTL) rate limit configured.

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.

In setting hardware rate-limiter for more than one module, the module level rate-limiter has higher precedence over system level.

Related Topics

Configuring Control Plane Policing

Default Settings for Rate Limits

This table lists the default settings for rate limits parameters.

Table 1: Default Rate Limits Parameters Settings

Parameters	Default
Access-list log packets rate limit	100 packets per second
Copy packets rate limit	30,000 packets per second

Parameters	Default
F1 Series module rate limit	RL-1: 4,500 packets per second RL-2: 1,000 packets per second RL-3: 1,000 packets per second RL-4: 100 packets per second RL-5: 1,500 packets per second **Note** These F1 Series module rate limits do not apply to F2 Series modules.
Layer 2 L2TP packets rate limit	4,096 packets per second
Layer 2 multicast-snooping packets rate limit	10,000 packets per second
Layer 2 port-security packets rate limit	Disabled
Layer 2 storm-control packets rate limit	Disabled
Layer 2 VPC low packets rate limit	4,000 packets per second
Layer 3 control packets rate limit	10,000 packets per second
Layer 3 glean packets rate limit	100 packets per second
Layer 3 glean fast-path rate limit	100 packets per second
Layer 3 MTU packets rate limit	500 packets per second
Layer 3 Time-to-Live (TTL) packets rate limit	500 packets per second
Receive packets rate limit	30,000 packets per second
Supervisor packets rate limit	10,000 packets per second

Configuring Rate Limits

You can set rate limits on supervisor-bound traffic.

SUMMARY STEPS

1. **configure terminal**
2. **hardware rate-limiter access-list-log** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
3. **hardware rate-limiter copy** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
4. **hardware rate-limiter f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5** {*packets* | **disable**}} [**module** *module* [**port** *start end*]]
5. **hardware rate-limiter layer-2 l2pt** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
6. **hardware rate-limiter layer-2 mcast-snooping** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
7. **hardware rate-limiter layer-2 port-security** {*packets* | **disable**} [**module** *module* [**port** *start end*]]

8. **hardware rate-limiter layer-2 storm-control** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
9. **hardware rate-limiter layer-2 vpc-low** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
10. **hardware rate-limiter layer-3 control** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
11. **hardware rate-limiter layer-3 glean** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
12. **hardware rate-limiter layer-3 glean-fast** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
13. **hardware rate-limiter layer-3 mtu** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
14. **hardware rate-limiter layer-3 multicast** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
15. **hardware rate-limiter layer-3 ttl** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
16. **hardware rate-limiter receive** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
17. **exit**
18. (Optional) **show hardware rate-limiter** [**access-list-log** | **copy** | **f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5**} | **layer-2** {**l2pt** | **mcast-snooping** | **port-security** | **storm-control** | **vpc-low**} | **layer-3** {**control** | **glean** | **glean-fast** | **mtu** | **multicast** | **ttl**} | **module** *module* | **receive**]
19. (Optional) **copy running-config startup-config**

DETAILED STEPS

	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 30000.
Step 3	**hardware rate-limiter copy** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter copy 30000`	Configures rate limits in packets per second for data and control packets copied to the supervisor module. The range is from 0 to 30000. **Note** Layer 3 control, multicast direct-connect, and ARP request packets are controlled by the Layer 2 copy rate limiter. The first two types of packets are also controlled by Layer 3 rate limiters, and the last two types are also subject to control plane policing (CoPP).
Step 4	**hardware rate-limiter f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5** {*packets* | **disable**}} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter f1 rl-1 1000`	Configures rate limits in packets per second for F1 Series module packets. The range is from 0 to 30000. **Note** The **f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5**} rate limiters are the only rate limiters that are supported on F1 Series modules. The other rate limiters are applicable only to the F2 Series and M1 Series modules.

	Command or Action	Purpose
Step 5	**hardware rate-limiter layer-2 l2pt** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-2 l2pt 30000`	Configures rate limits in packets per second for Layer 2 tunnel protocol packets. The range is from 0 to 30000.
Step 6	**hardware rate-limiter layer-2 mcast-snooping** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-2 mcast-snooping 20000`	Configures rate limits in packets per second for Layer 2 multicast-snooping packets. The range is from 0 to 30000.
Step 7	**hardware rate-limiter layer-2 port-security** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-2 port-security 100000`	Configures rate limits in packets per second for port-security packets. The range is from 0 to 30000.
Step 8	**hardware rate-limiter layer-2 storm-control** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-2 storm-control 10000`	Configures rate limits in packets per second for broadcast, multicast, and unknown unicast storm-control traffic. The range is from 0 to 30000.
Step 9	**hardware rate-limiter layer-2 vpc-low** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-2 vpc-low 10000`	Configures rate limits in packets per second for Layer 2 control packets over the VPC low queue. The range is from 0 to 30000.
Step 10	**hardware rate-limiter layer-3 control** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-3 control 20000`	Configures rate limits in packets per second for Layer 3 control packets. The range is from 0 to 30000.
Step 11	**hardware rate-limiter layer-3 glean** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-3 glean 200`	Configures rate limits in packets per second for Layer 3 glean packets. The range is from 0 to 30000.
Step 12	**hardware rate-limiter layer-3 glean-fast** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-3 glean-fast 500`	Configures rate limits in packets per second for Layer 3 glean fast-path packets. This command sends packets to the supervisor from F2e, M1, or M2 Series modules. The range is from 0 to 30000.

	Command or Action	Purpose
		Glean fast path optimizes the processing of glean packets by the supervisor. Specifically, the line card provides the information needed to trigger an ARP within the packet and relieves the supervisor from having to look up this information. The packets sent to the supervisor using the glean fast path are rate limited **Note** Glean fast path is enabled by default. If glean fast-path programming does not occur due to adjacency resource exhaustion, the system falls back to regular glean programming.
Step 13	**hardware rate-limiter layer-3 mtu** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-3 mtu 1000`	Configures rate limits in packets per second for Layer 3 MTU failure redirected packets. The range is from 0 to 30000.
Step 14	**hardware rate-limiter layer-3 multicast** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-3 multicast 20000`	Configures rate limits in packets per second for Layer 3 multicast packets in packets per second. The range is from 0 to 30000.
Step 15	**hardware rate-limiter layer-3 ttl** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-3 ttl 1000`	Configures rate limits in packets per second for Layer 3 failed Time-to-Live redirected packets. The range is from 0 to 30000.
Step 16	**hardware rate-limiter receive** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter receive 40000`	Configures rate limits in packets per second for packets redirected to the supervisor module. The range is from 0 to 30000.

Step 17	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 18	(Optional) **show hardware rate-limiter** [**access-list-log** | **copy** | **f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5**} | **layer-2** {**l2pt** | **mcast-snooping** | **port-security** | **storm-control** | **vpc-low**} | **layer-3** {**control** | **glean** | **glean-fast** | **mtu** | **multicast** | **ttl**} | **module** *module* | **receive**] **Example:** `switch# show hardware rate-limiter`	Displays the rate limit configuration.

	Command or Action	Purpose
Step 19	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Rate Limits for Packets That Reach the Supervisor

Beginning in Cisco NX-OS Release 5.1, you can configure rate limits globally on the device for packets that reach the supervisor module. If the rate of incoming or outgoing packets exceeds the configured rate limit, the device logs a system message but does not drop any packets.

Note You can also configure rate limits for packets that reach the supervisor module on a particular interface. For more information, see the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **rate-limit cpu direction** {**input** | **output** | **both**} **pps** *packets* **action log**
3. (Optional) **exit**
4. (Optional) **show system internal pktmgr internal control sw-rate-limit**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	[**no**] **rate-limit cpu direction** {**input**	**output**	**both**} **pps** *packets* **action log** **Example:** `switch(config)# rate-limit cpu direction both pps 100 action log`	Configures rate limits in packets per second for packets that reach the supervisor module and logs a system message if the rate of incoming or outgoing packets exceeds the rate limit. The range is from 1 to 100000. The default rate is 10000.
Step 3	(Optional) **exit** **Example:** `switch(config)# exit`	Exits global configuration mode.
Step 4	(Optional) **show system internal pktmgr internal control sw-rate-limit** **Example:**	Displays the inband and outband global rate limit configuration for packets that reach the supervisor module.

	Command or Action	Purpose
	`switch# show system internal pktmgr internal control sw-rate-limit`	
Step 5	(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.

SUMMARY STEPS

1. **show hardware rate-limiter** [**access-list-log** | **copy** | **f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5**} | **layer-2** {**l2pt** | **mcast-snooping** | **port-security** | **storm-control** | **vpc-low**} | **layer-3** {**control** | **glean** | **glean-fast** | **mtu** | **multicast** | **ttl**} | **module** *module* | **receive**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show hardware rate-limiter** [**access-list-log**	**copy**	**f1** {**rl-1**	**rl-2**	**rl-3**	**rl-4**	**rl-5**}	**layer-2** {**l2pt**	**mcast-snooping**	**port-security**	**storm-control**	**vpc-low**}	**layer-3** {**control**	**glean**	**glean-fast**	**mtu**	**multicast**	**ttl**}	**module** *module*	**receive**] **Example:** `switch# show hardware rate-limiter layer-3 glean`	Displays the rate limit statistics.

Clearing the Rate Limit Statistics

You can clear the rate limit statistics.

SUMMARY STEPS

1. **clear hardware rate-limiter** {**all** | **access-list-log** | **copy** | **f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5**} | **layer-2** {**l2pt** | **mcast-snooping** | **port-security** | **storm-control** | **vpc-low**} | **layer-3** {**control** | **glean** | **glean-fast** | **mtu** | **multicast** | **ttl**} | **receive**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**clear hardware rate-limiter** {**all**	**access-list-log**	**copy**	**f1** {**rl-1**	**rl-2**	**rl-3**	**rl-4**	**rl-5**}	**layer-2** {**l2pt**	**mcast-snooping**	**port-security**	**storm-control**	**vpc-low**}	Clears the rate limit statistics.

	Command or Action	Purpose
	| **layer-3** {**control** | **glean** | **glean-fast** | **mtu** | **multicast** | **ttl**} | **receive**} **Example:** `switch# clear hardware rate-limiter`	

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** | **copy** | **f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5**} | **layer-2** {**l2pt** | **mcast-snooping** | **port-security** | **storm-control** | **vpc-low**} | **layer-3** {**control** | **glean** | **glean-fast** | **mtu** | **multicast** | **ttl**} | **module** *module* | **receive**]	Displays the rate limit configuration.
show system internal pktmgr interface ethernet *slot*/*port*	Displays the inband and outband rate limit configuration for packets that reach the supervisor module on a specific interface.
show system internal pktmgr internal control sw-rate-limit	Displays the inband and outband global rate limit configuration for packets that reach the supervisor module.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Configuration Examples for Rate Limits

The following example shows how to configure rate limits:

```
switch(config)# hardware rate-limiter layer-3 control 20000
switch(config)# hardware rate-limiter copy 30000
```

The following example shows how to configure rate limits globally on the device for packets that reach the supervisor module:

```
switch(config)# rate-limit cpu direction both pps 1000 action log
switch(config)# show system internal pktmgr internal control sw-rate-limit
inband pps global threshold 1000  outband pps global threshold 1000
```

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*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*

Feature History for Rate Limits

This table lists the release history for this feature.

Table 2: Feature History for Rate Limits

Feature Name	Releases	Feature Information
Rate limits	6.2(2)	Added support for Layer 3 glean fast-path packets.
Rate limits	6.0(1)	Added support for F2 Series modules.
Rate limits	5.2(1)	No change from Release 5.1.
Rate limits	5.1(1)	Added support for F1 Series module packets.
Rate limits	5.1(1)	Added the ability to configure rate limits for packets that reach the supervisor module and to log a system message if the rate limit is exceeded.
Rate limits	5.1(1)	Added options to disable rate limits and to configure rate limits for a specific module and port range.
Rate limits	5.0(2)	Added support for Layer 2 Tunnel Protocol (L2TP) packets.
Rate limits	4.2(1)	No change from Release 4.1.