CHAPTER 21

Configuring Rate Limits

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

This chapter includes the following topics:

Information About Rate Limits

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

- Access list logging packets
- Data and control packets copied to the supervisor module
- Layer 2 storm control packets
- Layer 2 port security packets
- Layer 3 glean packets
- Layer 3 maximum transmission unit (MTU) check failure packets
- Layer 3 multicast directly connected packets
- Layer 3 multicast local group packets

- Layer 3 multicast Reverse Path Forwarding (RPF) leak packets
- Layer 3 Time-to-Live (TTL) check failure packets
- Receive packets

You can also configure rate limits for Layer 3 control packets.

Virtualization Support

You can configure rate limits only in the default virtual device context (VDC), but the rate limits configuration applies to all VDCs on the NX-OS device. For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.0*.

Licensing Requirements for Rate Limits

The following table shows the licensing requirements for this feature:

Product	License Requirement
NX-OS	Rate limits require no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the *Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0*.

Guidelines and Limitations

Rate limits has the following configuration guidelines and limitations:

- You can set rate limits only for supervisor-bound egress exception and egress redirected traffic. Use control plane policing (CoPP) for other types of traffic (see Chapter 20, "Configuring Control Plane Policing").

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.

Configuring Rate Limits

You can set rate limits on egress traffic.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **platform rate-limit access-log-list** *packets*
   platform rate-limit copy *packets*
   platform rate-limit layer-2 port-security *packets*
   platform rate-limit layer-2 storm-control *packets*
   platform rate-limit layer-3 control *packets*
   platform rate-limit layer-3 glean *packets*
   platform rate-limit layer-3 mtu *packets*
   platform rate-limit layer-3 multicast {**directly-connected** | **local-groups** | **rpf-leak**} *packets*
   platform rate-limit layer-3 ttl *packets*
   platform rate-limit receive *packets*
3. **exit**
4. **show hardware rate-limit**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.

	Command	Purpose
Step 2	**platform rate-limit access-list-log** *packets* **Example:** `switch(config)# platform rate-limit 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 from1 to 33554431. The default rate is 100.
	platform rate-limit copy *packets* **Example:** `switch(config)# platform rate-limit copy 40000`	Configures rate limits in packets per second for data and control packets copied to the supervisor module. The range is from1 to 33554431. The default rate is 30000.
	platform rate-limit layer-2 port-security *packets* **Example:** `switch(config)# platform rate-limit control 100`	Configures rate limits in packets per second for port security packets. The range is from1 to 33554431. The default is disabled.
	platform rate-limit layer-2 storm-control *packets* **Example:** `switch(config)# platform rate-limit control 100`	Configures rate limits in packets per second for storm control packets. The range is from1 to 33554431. The default is disabled.
	platform rate-limit layer-3 control *packets* **Example:** `switch(config)# platform rate-limit control 20000`	Configures rate limits in packets per second for Layer-3 control packets. The range is from1 to 33554431. The default rate is 10000.
	platform rate-limit layer-3 glean *packets* **Example:** `switch(config)# platform rate-limit layer-3 glean 200`	Configures rate limits in packets per second for Layer-3 glean packets. The range is from1 to 33554431. The default rate is 100.
	platform rate-limit layer-3 mtu *packets* **Example:** `switch(config)# platform rate-limit layer-3 mtu 1000`	Configures rate limits in packets per second for Layer-3 MTU failure redirected packets. The range is from1 to 33554431. The default rate is 500.
	platform rate-limit layer-3 multicast {**directly-connected** | **local-groups** | **rpf-leak**} *packets* **Example:** `switch(config)# platform rate-limit layer-3 multicast local-groups 20000`	Configures rate limits in packets per second for Layer-3 multicast directly connected, local groups, or RPF leak redirected packets in packets per second. The range is from1 to 33554431. The default rate is 10000 for directly connected packets, 10000 for local groups packets, and 500 for RPF leak packets.
	platform rate-limit layer-3 ttl *packets* **Example:** `switch(config)# platform rate-limit layer-3 ttl 1000`	Configures rate limits in packets per second for Layer-3 failed Time-to-Live redirected packets. The range is from1 to 33554431. The default rate is 500.
	platform rate-limit receive *packets* **Example:** `switch(config)# platform rate-limit receive 40000`	Configures rate limits in packets per second for packets redirected to the supervisor module. The range is from1 to 33554431. The default rate is 30000.

Step 3	**exit**
	
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

	Command	Purpose
Step 4	**show hardware rate-limit** [**access-list-log** | **copy** | **layer-2** {**port-security** | **storm-control**} | **layer-3** {**control** | **glean** | **mtu** | **multicast** {**directly-connected** | **local-groups** | **rpf-leak**} | **ttl**} | **receive**] **Example:** switch# show running-config | include rate-limit	(Optional) Displays the rate limit configuration.
Step 5	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Displaying the Rate Limit Statistics

You can display the rate limit statistics.

BEFORE YOU BEGIN

Ensure that you are in the default VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **show hardware rate-limit [access-list-log | copy | layer-2 storm-control | layer-3 {control | glean | mtu | multicast {directly-connected | local-groups | rpf-leak} | ttl} | receive]**

DETAILED STEPS

	Command	Purpose
Step 1	**show hardware rate-limit** [**access-list-log** | **copy** | **layer-2** {**port-security** | **storm-control**} | **layer-3** {**control** | **glean** | **mtu** | **multicast** {**directly-connected** | **local-groups** | **rpf-leak**} | **ttl**} | **receive**] **Example:** switch# show hardware rate-limit layer-3 glean	Displays the rate limit statistics.

For detailed information about the fields in the output from this command, see to the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*.

Clearing the Rate Limit Statistics

You can clear the rate limit statistics.

BEFORE YOU BEGIN

Ensure that you are in the default VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **show hardware rate-limit** [**access-list-log** | **copy** | **layer-2** {**port-security** | **storm-control**}| **layer-3** {**control** | **glean** | **mtu** | **multicast** {**directly-connected** | **local-groups** | **rpf-leak**} | **ttl**} | **receive**]
2. **clear hardware rate-limit** {**all** | **access-list-log** | **copy** | **layer-2 storm-control** | **layer-3** {**control** | **glean** | **mtu** | **multicast** {**directly-connected** | **local-groups** | **rpf-leak**} | **ttl**} | **receive**}

DETAILED STEPS

	Command	Purpose
Step 1	**show hardware rate-limit** [**access-list-log** | **copy** | **layer-2** {**port-security** | **storm-control**} | **layer-3** {**control** | **glean** | **mtu** | **multicast** {**directly-connected** | **local-groups** | **rpf-leak**} | **ttl**} | **receive**] **Example:** `switch# show hardware rate-limit layer-3 glean`	(Optional) Displays the rate limit statistics.
Step 2	**clear hardware rate-limiter** {**all** | **access-list-log** | **copy** | **layer-2** {**port-security** | **storm-control**} | **layer-3** {**control** | **glean** | **mtu** | **multicast** {**directly-connected** | **local-groups** | **rpf-leak**} | **ttl**} | **receive**} **Example:** `switch# clear hardware rate-limiter`	Clears the rate limit statistics.

Verifying the Rate Limits Configuration

To display the rate limits configuration information, perform the following task:

Command	Purpose
1. **show hardware rate-limit** [**access-list-log** | **copy** | **layer-2** {**port-security** | **storm-control** | **layer-3** {**control** | **glean** | **mtu** | **multicast** {**directly-connected** | **local-groups** | **rpf-leak**} | **ttl**} | **receive**]	Displays the rate limit configuration.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*.

Rate Limits Example Configuration

The following example shows how to configure rate limits:

```
platform rate-limit layer-3 control 20000
platform rate-limit copy 40000
```

Default Settings

Table 21-1 lists the default settings for rate limits parameters.

Table 21-1 Default Rate Limits Parameters

Parameters	Default
Access-list-log packets rate limit	100 packets per second
Copy packets rate limit	30,000 packets per second
Layer 2 port-security packet rate limit	Disabled
Layer 2 storm-control packets rate limit	Disabled
Layer 3 control packets rate limit	10,000 packets per second
Layer 3 glean packets rate limit	100 packets per second
Layer 3 MTU packets rate limit	500 packets per second
Layer 3 multicast directly-connected packets rate limit	10,000 packets per second
Layer 3 multicast local-groups packets rate limit	10,000 packets per second
Layer 3 multicast rpf-leak packets rate limit	500 packets per second
Receive packets rate limit	30,000 packets per second

Additional References

For additional information related to implementing rate limits, see the following sections:

- Related Documents, page 21-8

Related Documents

Related Topic	Document Title
Licensing	*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*

Feature History for Rate Limits

Table 21-2 lists the release history for this feature.

Table 21-2 Feature History for IP ACLs

Feature Name	Releases	Feature Information
Port security packet rate limiting	4.0(3)	Rate limiting for port security packet was added to the **platform rate-limit**, **clear hardware rate-limit**, and **show hardware rate-limit** commands.
Rate limits	4.0(1)	This feature was introduced.