Configuring Traffic Storm Control

This chapter describes how to configure traffic storm control on the Cisco NX-OS device.

This chapter includes the following sections:

- Finding Feature Information, on page 1
- Information About Traffic Storm Control, on page 1
- Virtualization Support for Traffic Storm Control, on page 3
- Licensing Requirements for Traffic Storm Control, on page 3
- Guidelines and Limitations for Traffic Storm Control, on page 3
- Default Settings for Traffic Storm Control, on page 4
- Configuring Traffic Storm Control, on page 4
- Verifying Traffic Storm Control Configuration, on page 5
- Monitoring Traffic Storm Control Counters, on page 6
- Configuration Example for Traffic Storm Control , on page 6
- Additional References for Traffic Storm Control, on page 6
- Feature History for Traffic Storm Control, on page 7

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://bst.cloudapps.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 Traffic Storm Control

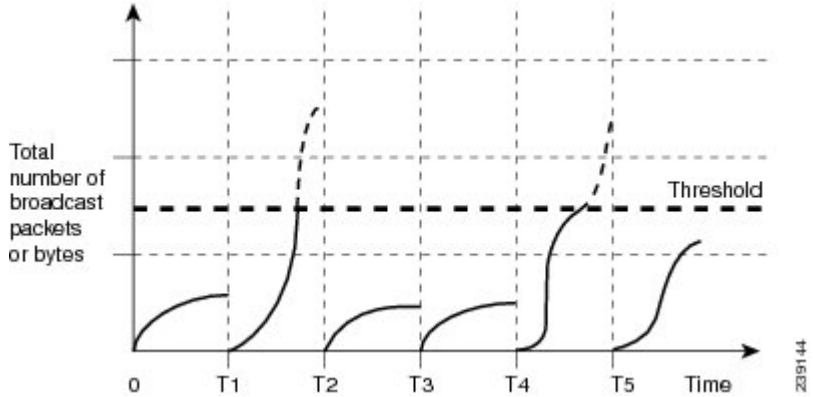
A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. You can use the traffic storm control feature to prevent disruptions on Layer 2 ports by a broadcast, multicast, or unicast traffic storm on physical interfaces.

Traffic storm control (also called traffic suppression) allows you to monitor the levels of the incoming broadcast, multicast, and unicast traffic over a 10-millisecond interval. During this interval, the traffic level, which is a percentage of the total available bandwidth of the port, is compared with the traffic storm control level that

you configured. When the ingress traffic reaches the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends.

This table shows the broadcast traffic patterns on a Layer 2 interface over a given interval. In this example, traffic storm control occurs between times T1 and T2 and between T4 and T5. During those intervals, the amount of broadcast traffic exceeded the configured threshold.

Figure 1: Broadcast Suppression



The traffic storm control threshold numbers and the time interval allow the traffic storm control algorithm to work with different levels of granularity. A higher threshold allows more packets to pass through.

Traffic storm control on the Cisco NX-OS device is implemented in the hardware. The traffic storm control circuitry monitors packets that pass from a Layer 2 interface to the switching bus. Using the Individual/Group bit in the packet destination address, the circuitry determines if the packet is unicast or broadcast, tracks the current count of packets within the 10-millisecond interval, and filters out subsequent packets when a threshold is reached.

Traffic storm control uses a bandwidth-based method to measure traffic. You set the percentage of total available bandwidth that the controlled traffic can use. Because packets do not arrive at uniform intervals, the 10-millisecond interval can affect the behavior of traffic storm control.

The following are examples of traffic storm control behavior:

- If you enable broadcast traffic storm control, and broadcast traffic exceeds the level within the 10-millisecond interval, traffic storm control drops all broadcast traffic until the end of the interval.
- If you enable broadcast and multicast traffic storm control, and the combined broadcast and multicast traffic exceeds the level within the 10-millisecond interval, traffic storm control drops all broadcast and multicast traffic until the end of the interval.
- If you enable broadcast and multicast traffic storm control, and broadcast traffic exceeds the level within the 10-millisecond interval, traffic storm control drops all broadcast and multicast traffic until the end of the interval.
- If you enable broadcast and multicast traffic storm control, and multicast traffic exceeds the level within the 10-millisecond interval, traffic storm control drops all broadcast and multicast traffic until the end of the interval.

By default, the Cisco NX-OS software takes no corrective action when the traffic exceeds the configured level. However, you can configure an Embedded Event Management (EEM) action to error-disable an interface if the traffic does not subside (drop below the threshold) within a certain time period. For information on configuring EEM, see the *Cisco Nexus 7000 Series NX-OS System Management Command Reference*.

Virtualization Support for Traffic Storm Control

Traffic storm control configuration and operation are local to the virtual device context (VDC).

For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Licensing Requirements for Traffic Storm Control

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	Traffic storm control requires 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 an explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

Guidelines and Limitations for Traffic Storm Control

When configuring the traffic storm control level, note the following guidelines and limitations:

- Only one suppression level is shared by all three suppression modes i.e., unicast, multicast, and broadcast. For example, if you set the broadcast level to 30 and then set the multicast level to 40, both levels are enabled and set to 40.
- You can configure traffic storm control on a port-channel interface.
- Do not configure traffic storm control on interfaces that are members of a port-channel interface. Configuring traffic storm control on interfaces that are configured as members of a port channel puts the ports into a suspended state.
- When you use the **storm-control unicast level** *percentage* command on a module, both the unknown and known unicast traffic gets discarded after reaching the threshold value. This is the hardware limitation and applicable across all linecards.
- Traffic storm control on all Cisco FEX devices connected to Cisco Nexus 7000 series switches has following guidelines and limitations:
  - Traffic storm control is not supported on HIF ports.
  - Traffic storm control is supported only on NIF ports.
- Specify the level as a percentage of the total interface bandwidth:
  - The level can be from 0 to 100.
  - The optional fraction of a level can be from 0 to 99.
  - 100 percent means no traffic storm control.
  - 0.0 percent suppresses all traffic.

Because of hardware limitations and the method by which packets of different sizes are counted, the level percentage is an approximation. Depending on the sizes of the frames that make up the incoming traffic, the actual enforced level might differ from the configured level by several percentage points.

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 Traffic Storm Control

This table lists the default settings for traffic storm control parameters.

Table 1: Default Traffic Storm Control Parameters

Parameters	Default
Traffic storm control	Disabled
Threshold percentage	100

Configuring Traffic Storm Control

You can set the percentage of total available bandwidth that the controlled traffic can use.

Note Traffic storm control uses a 10-millisecond interval that can affect the behavior of traffic storm control.

SUMMARY STEPS

1. **configure terminal**
2. **interface** {**ethernet** *slot*/*port* | **port-channel** *number*}
3. **storm-control** {**broadcast** | **multicast** | **unicast**} **level** *percentage*[**.***fraction*]
4. **exit**
5. (Optional) **show running-config interface** {**ethernet** *slot*/*port* | **port-channel** *number*}
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

Step 2	**interface** {**ethernet** *slot*/*port* | **port-channel** *number*}
	Example:
	`switch# interface ethernet 1/1`
	`switch(config-if)#`
		Enters interface configuration mode.

Step 3	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** *percentage*[**.***fraction*] **Example:** `switch(config-if)# storm-control unicast level 40`	Configures traffic storm control for traffic on the interface. The default state is disabled. **Note** The **storm-control unicast** command configures traffic storm control for all the unicast packets.

Step 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 5	(Optional) **show running-config interface** {**ethernet** *slot*/*port* | **port-channel** *number*} **Example:** `switch(config)# show running-config interface ethernet 1/1`	Displays the traffic storm control configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Verifying Traffic Storm Control Configuration

To display traffic storm control configuration information, perform one of the following tasks:

Command	Purpose
show interface [**ethernet** *slot*/*port* | **port-channel** *number*] **counters storm-control**	Displays the traffic storm control configuration for the interfaces.
show running-config interface	Displays the traffic storm control configuration.

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

Monitoring Traffic Storm Control Counters

You can monitor the counters the Cisco NX-OS device maintains for traffic storm control activity.

SUMMARY STEPS

1. **show interface** [**ethernet** *slot*/*port* | **port-channel** *number*] **counters storm-control**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**show interface** [**ethernet** *slot*/*port* | **port-channel** *number*] **counters storm-control** **Example:** `switch# show interface counters storm-control`	Displays the traffic storm control counters.

Configuration Example for Traffic Storm Control

The following example shows how to configure traffic storm control:

```
interface Ethernet1/1
  storm-control broadcast level 40
  storm-control multicast level 40
  storm-control unicast level 40
```

Additional References for Traffic Storm Control

This section includes additional information related to implementing traffic storm control.

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 Traffic Storm Control

This table lists the release history for this feature.

Table 2: Feature History for Traffic Storm Control

Feature Name	Releases	Feature Information	
Traffic storm control	6.0(1)	No change from Release 5.2.	
Traffic storm control	4.2(1)	No change from Release 4.1.	