



CHAPTER 18

Configuring Traffic Storm Control

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

This chapter includes the following sections:

- [Information About Traffic Storm Control, page 18-1](#)
- [Virtualization Support For Traffic Storm Control, page 18-3](#)
- [Licensing Requirements for Traffic Storm Control, page 18-3](#)
- [Guidelines and Limitations, page 18-3](#)
- [Configuring Traffic Storm Control, page 18-3](#)
- [Verifying Traffic Storm Control Configuration, page 18-5](#)
- [Traffic Storm Control Example Configuration, page 18-5](#)
- [Default Settings, page 18-6](#)
- [Additional References, page 18-6](#)

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 unknown 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 1-second 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.

[Figure 18-1](#) 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.

Send document comments to nexus7k-docfeedback@cisco.com

Figure 18-1 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 1-second 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 1-second 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 1-second 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 1-second 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 1-second 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 1-second interval, traffic storm control drops all broadcast and multicast traffic until the end of the interval.

By default, the 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 threshold) within a certain time period. For information on configuring EEM, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.0*.

Send document comments to nexus7k-docfeedback@cisco.com

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, Release 4.0*.

Licensing Requirements for Traffic Storm Control

The following table shows the licensing requirements for this feature:

Product	License Requirement
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 a complete explanation of the NX-OS licensing scheme, see the <i>Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0</i> .

Guidelines and Limitations

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

- 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.
- 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.

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 1-second interval that can affect the behavior of traffic storm control.

Send document comments to nexus7k-docfeedback@cisco.com

BEFORE YOU BEGIN

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

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: switch# config t switch(config)#	Enters global configuration mode.
Step 2	interface { <i>ethernet slot/port</i> port-channel number } Example: switch# interface ethernet 1/1 switch(config-if)#	Enters interface configuration mode.
Step 3	storm-control { broadcast multicast unicast } level <i>percentage</i> [<i>.fraction</i>] Example: switch(config-if)# storm-control unicast level 40	Configures traffic storm control for traffic on the interface. The default state is disabled.
Step 4	exit Example: switch(config-if)# exit switch(config)#	Exits interface configuration mode.
Step 5	show running-config interface { <i>ethernet slot/port</i> port-channel number } Example: switch(config)# show running-config interface ethernet 1/1	(Optional) Displays the traffic storm control configuration.
Step 6	copy running-config startup-config Example: switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Verifying Traffic Storm Control Configuration

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

Command	Purpose
<code>show interface [ethernet slot/port port-channel number] counters storm-control</code>	Displays the traffic storm control configuration for the interfaces.
<code>show running-config interface</code>	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, Release 4.0](#).

Displaying Traffic Storm Control Counters

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

BEFORE YOU BEGIN

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

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose
Step 1	<pre>switch# show interface [ethernet slot/port port-channel number] counters storm-control</pre> <p>Example:</p> <pre>switch# show interface counters storm-control</pre>	Displays the traffic storm control counters.

For detailed information about the fields in the output from this command, see the [Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0](#).

Traffic Storm Control Example Configuration

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
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Default Settings

Table 18-1 lists the default settings for traffic storm control parameters.

Table 18-1 **Default Traffic Storm Control Parameters**

Parameters	Default
Traffic storm control	Disabled.
Threshold percentage	100.

Additional References

For additional information related to implementing traffic storm control, see the following sections:

- [Related Documents, page 18-6](#)

Related Documents

Related Topic	Document Title
NX-OS 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