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:

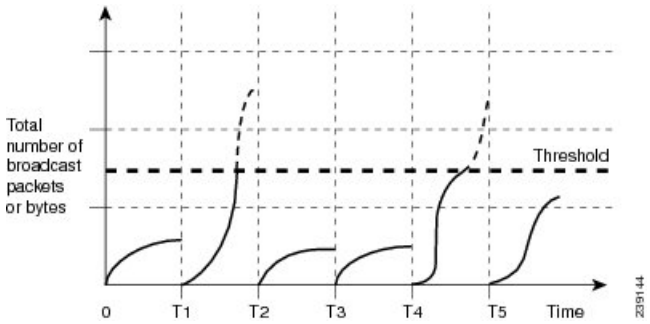
About Traffic Storm Control

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 3.9-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 Nexus 9000v 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 3.9-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 3.9-millisecond interval can affect the behavior of traffic storm control.

The following are examples of how traffic storm control operation is affected

- If you enable broadcast traffic storm control, and broadcast traffic exceeds the level within the 3.9-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 3.9-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 3.9-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 3.9-millisecond interval, traffic storm control drops all broadcast and multicast traffic until the end of the interval.

When the traffic exceeds the configured level, you can configure traffic storm control to perform the following optional corrective actions :

- Shut down—When ingress traffic exceeds the traffic storm control level that is configured on a port, traffic storm control puts the port into the error-disabled state. To reenable this port, you can use either the **shutdown** and **no shutdown** options on the configured interface, or the error-disable detection and recovery feature. You are recommended to use the **errdisable recovery cause storm-control** command for error-disable detection and recovery along with the **errdisable recovery interval** command for defining the recovery interval. The interval can range between 30 and 65535 seconds.
- Trap—You can configure traffic storm control to generate an SNMP trap when ingress traffic exceeds the configured traffic storm control level. The SNMP trap action is enabled by default. However, storm

control traps are not rate-limited by default. You can control the number of traps generated per minute by using the **snmp-server enable traps storm-control trap-rate** command.

By default, Cisco NX-OS takes no corrective action when traffic exceeds the configured level.

Guidelines and Limitations for Traffic Storm Control

Traffic storm control has the following configuration guidelines and limitations:

- The storm control feature does not work if you enable storm control on an interface where sFlow is also enabled.
- Storm control PPS option is supported only on Cisco Nexus 9300-FX2 platform switches.
- For Cisco Nexus NFE2-enabled devices, you can use the storm control-cpu to control the number of ARP packets sent to the CPU.
- You can configure traffic storm control on a port-channel interface.
- Specify the traffic storm control level as a percentage of the total interface bandwidth:
  - The pps range can be from 0 to 200000000.
  - 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.
- For Cisco Nexus 9500 Series switches with 9400 Series line cards, and Cisco Nexus 9300 Series switches, you can use the storm control CLI to specify bandwidth level either as a percentage of port capacity or packets-per-second.
- Beginning with Cisco Nexus Release 9.2(1), the error margin is greater than 1% when you configure the storm control packets-per-seconds as follows:
  - Traffic period < 60 s
  - Storm control pps <1000
- This is applicable only for Cisco Nexus 9336C-FX, Cisco Nexus 93300YC-FX, and Cisco Nexus 93240YC-FX2Z switches.
- Beginning with Cisco Nexus Release 9.2(1), you can use the percentage of port capacity or packets-per-second for the Cisco Nexus 9336C-FX2, Cisco Nexus 93300YC-FX2, and Cisco Nexus 93240YC-FX2-Z switches.
- If you have configured an SVI for the VLAN on Cisco Nexus 9200, 9300-EX platform switches, or on the N9K-X9700-FX3 line cards, storm control broadcast does not work for ARP traffic (ARP request).
- Local link and hardware limitations prevent storm-control drops from being counted separately. Instead, storm-control drops are counted with other drops in the discards counter.
- Because of hardware limitations and the method by which packets of different sizes are counted, the traffic storm control 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.

- Due to a hardware limitation, the output for the **show interface counters storm-control** command does not show ARP suppression when storm control is configured and the interface is actually suppressing ARP broadcast traffic. This limitation can lead to the configured action not being triggered but the incoming ARP broadcast traffic being correctly storm suppressed.
- Due to a hardware limitation, storm control is not supported for 400G ports beyond 70% of the port bandwidth in Cisco Nexus GX series platform switches.
- Due to a hardware limitation, the packet drop counter cannot distinguish between packet drops caused by a traffic storm and packet drops caused by other discarded input frames. This limitation can lead to the configured action being triggered even in the absence of a traffic storm.
- Due to a hardware limitation, storm suppression packet statistics are not supported on uplink ports.
- Due to a hardware limitation, storm suppression packet statistics do not include broadcast traffic on VLANs with an active switched virtual interface (SVI).
- Due to a design limitation, storm suppression packet statistics do not work if the configured level is 0.0, which is meant to suppress all incoming storm packets.
- Traffic storm control is supported on the Cisco Nexus 9300 Series switches and the Cisco Nexus 9500 Series switches with the 9700-EX/FX line card.
- Traffic storm control is not supported on Cisco N9K-M4PC-CFP2.
- Traffic storm control is not supported on FEX interfaces.
- Traffic storm control is only for ingress traffic, specifically for unknown unicast, unknown multicast, and broadcast traffic.

Note On Cisco Nexus 9000 Series switches, traffic storm control applies to unknown unicast traffic and not known unicast traffic

- When port channel members are error disabled due to a configured action, all individual member ports should be flapped to recover from the error disabled state.
- Cisco Nexus Release 9.2(1) the traffic storm control feature is not supported on Cisco Nexus 9500 platform switches with the N9K-X96136YC-R line card and N9K-C9504-FM-R fabric module.
- Beginning with Cisco Nexus Release 9.3(2), the traffic storm control feature with only rate-limiting is supported on Cisco Nexus 9500 platform switches with the N9K-X96136YC-R, N9K-X9636C-R, N9K-X9636Q-R, N9K-X9636C-RX line cards, and N9K-C9504-FM-R and N9K-C9508-FM-R fabric modules. Traffic storm control counters and storm-control action are not supported.
- The following guidelines and limitations apply to Cisco Nexus 9200 Series switches:
  - Traffic storm control with unknown multicast traffic is not supported.
  - Packet-based statistics are not supported for traffic storm control as the policer supports only byte-based statistics.
  - Traffic storm control is not supported for copy-to-CPU packets.

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 3.9-millisecond interval that can affect the behavior of traffic storm control.
- You must carve the n9k-arp-acl TCAM region before setting storm-control-cpu rate on port-channel. For information on configuring the TCAM region size, see the *Configuring ACL TCAM Region Sizes* section in the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

SUMMARY STEPS

1. **configure terminal**
2. **interface** {**ethernet** *slot*/*port* | **port-channel** *number*}
3. [**no**] **storm-control** {**broadcast** | **multicast** | **unicast**} **level** { <*level-value %*> | **pps** < *pps-value* > }
4. [**no**] **storm-control action trap**
5. [**no**] **storm-control-cpu arp rate**
6. **exit**
7. (Optional) **show running-config interface** {**ethernet** *slot*/*port* | **port-channel** *number*}
8. (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	**interface** {**ethernet** *slot*/*port*	**port-channel** *number*} **Example:**	Enters interface configuration mode.

	Command or Action	Purpose
	`switch# interface ethernet 1/1` `switch(config-if)#`	

Step 3	[**no**] **storm-control** {**broadcast** | **multicast** | **unicast**} **level** { *<level-value %>* | **pps** *< pps-value >* }
	Example:
	`switch(config-if)# storm-control unicast level 40`
	Example:
	`switch(config-if)# storm-control broadcast level pps 8000`
		Configures traffic storm control for traffic on the interface. You can also configure bandwidth level as a percentage either of port capacity or packets-per-second. The default state is disabled.

Step 4	[**no**] **storm-control action trap** **Example:** `switch(config-if)# storm-control action trap`	Generates an SNMP trap (defined in CISCO-PORT-STORM-CONTROL-MIB) and a syslog message when the traffic storm control limit is reached.
Step 5	[**no**] **storm-control-cpu arp rate** **Example:** `switch(config-if)# storm-control-cpu arp rate`	Configures traffic storm control rate for arp packets entering a port channel. This rate is divided equally among the members of the port channel.

Step 6	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 7	(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 8	(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 running-config interface	Displays the traffic storm control configuration.
show access-list storm-control arp-stats interface [ethernet | port-channel] *number*	Displays the storm control statistics for arp packets on the interface.

Monitoring Traffic Storm Control Counters

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

Command	Purpose
show interface [**ethernet** *slot*/*port* | **port-channel** *number*] **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:

```
switch# configure terminal
switch(config)# interface Ethernet1/1
switch(config-if)# storm-control broadcast level 40
switch(config-if)# storm-control multicast level 40
switch(config-if)# storm-control unicast level 40
switch(config)# storm-control-cpu arp rate 150
```

The following example checks the programmed configured rate and the statistics of dropped ARP packets:

```
switch(config)# sh access-list storm-control-cpu arp-stats
interface port-channel 132
slot  1
=======
------------------------------------------------------------------------
            ARP Policer Entry Statistics
------------------------------------------------------------------------
Interface port-channel132:
----------
Member Interface   Entry-ID  Rate     RedPacket Count     GreenPacket Count
-------------------------------------------------------------------------------
Ethernet1/35        3976        50           0                0
-------------------------------------------------------------------------------

slot  7
=======
------------------------------------------------------------------------
            ARP Policer Entry Statistics
------------------------------------------------------------------------
Interface port-channel132:
----------
Member Interface   Entry-ID  Rate     RedPacket Count     GreenPacket Count
-------------------------------------------------------------------------------
```