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:

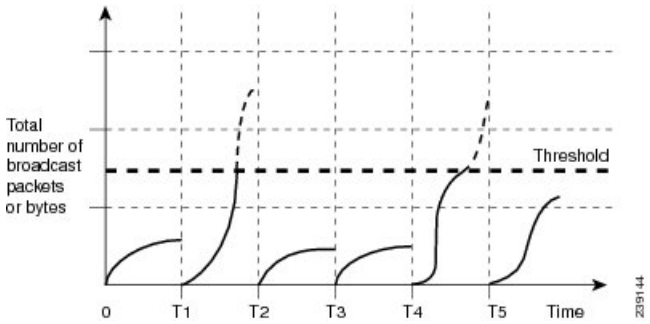
About Traffic Storm Control

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 or Layer 3 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 or Layer 3 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 or Layer 3 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.

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 nx-os image 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

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 was supported only on Cisco Nexus 9300-FX2 platform switches. Beginning with Cisco NX-OS Release 10.3(2)F, it is also supported on Cisco Nexus 9300-FX3, 9300-GX, and 9300-GX2 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.
- Storm control can be configured on physical, port-channel, and breakout interfaces.
- 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

- 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 9.2(4), the traffic storm control feature is supported on Cisco Nexus 9500 platform switches with the N9K-X96136YC-R line card and N9K-C9504-FM-R fabric module. Traffic storm control counters do not increment when the interface is flooded with the broadcast traffic.
- 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.
- Beginning with Cisco NX-OS Release 10.1(2), Storm Control feature is supported on the N9K-X9624D-R2 and N9K-C9508-FM-R2 platform switches.
- Beginning with Cisco Nexus Release 10.1(2), for Cisco Nexus N9300-FX and N9300-FX2 series switches, you can configure a two-level threshold and logging support for Broadcast, Unknown Unicast, and Multicast (BUM) traffic, and also set trap or shutdown action for each threshold level. The existing storm control configuration is now used only for one-level threshold.
- The following guidelines and limitations apply to the two-level threshold and logging support for BUM traffic feature for Cisco Nexus 10.1(2) release:
  - The new traffic storm control feature in Cisco Nexus Release 10.1(2) supports a maximum of 62 ports (as a single slice) on Cisco Nexus N9300-FX and a total of 124 ports (as two slices) on Cisco Nexus N9300-FX2.
  - Traffic storm control supports devices that are only in one storm control mode at a time, either one-level or two-level threshold. It does not support a mix of one-level threshold and two-level threshold storm control mode across ports at a time.
  - Traffic storm control monitors traffic statistics and generates system log for each level (lower and higher) and traffic type (unknown unicast, multicast, and broadcast) from Cisco Nexus Release 10.1(2).
  - The two-level threshold traffic storm control feature requires carving of a new Ternary Content Addressable Memory (TCAM) region with a fixed size of 512, and a reload of the device.
  - Traffic storm control for two-level threshold cannot coexist with the L2 Netflow feature, that is, presence of config layer2-switched flow monitor CLI, because of TCAM resource limitation.
  - The two-level threshold feature for traffic storm control does not support non-IP MC flood traffic (packet without an IP header) and packets-per-second mode.
  - Traffic storm control is not supported on Generic Online Diagnostics (GOLD) packets and sub-interface level.
  - If you were on a prior release, have upgraded to 10.1(2), and want to use the two-level storm control feature, then make sure that you configure the switch with the new storm control commands.

    - If you have configured the two-level storm control feature in version 10.1(2), and you want to downgrade to a previous version, then the new feature does not support downgrade. To downgrade, remove the configuration.

- Beginning from Cisco Nexus Release 10.2(1), Storm control does not allow to have multiple action configurations on an interface. If the previous action value is overwritten, then it considers the latest action value that is configured.
- Beginning with Cisco NX-OS Release 10.2(2)F, the storm control feature is supported on Cisco N9K-9332D-GX2B platform switches.
- Beginning with Cisco NX-OS Release 10.3(2)F, Traffic Storm Control is supported on Layer 3 interfaces, and the following guidelines and limitations are applicable:
    - Traffic storm control supports devices that are only on one-level threshold storm control mode.
    - Layer 3 packets destined for the control plane such as ARP broadcast are not suppressed by storm control and are policed by the CoPP policer. However, storm control violation actions are triggered.
    - This feature is supported only on Cisco Nexus 9300-FX, 9300-FX2, 9300-FX3, 9300-GX, and 9300-GX2 platform switches, and Cisco Nexus 9500 Series switches with FX and GX line cards.
- Beginning with Cisco NX-OS Release 10.3(3)F, the **system storm-control priority-policy drop-l3** command is introduced to prioritize storm control drop over the CoPP policer, and the following guidelines and limitations are applicable:
    - This feature applies to Layer 3 control frames.
    - This feature is supported only on Cisco Nexus 9300-FX, 9300-FX2, 9300-FX3, 9300-GX, and 9300-GX2 platform switches, and Cisco Nexus 9500 Series switches with FX and GX line cards.
    - This feature is applicable only for one-level threshold traffic storm control.

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 for One-level Threshold

You can set the percentage of total available bandwidth that the controlled traffic can use for one-level threshold.

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.

Procedure

	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:
	`switch# interface ethernet 1/1`
	`switch(config-if)#`
		Enters interface configuration mode.

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.

	Command or Action	Purpose
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.

Prioritizing Storm-control Policer Over the CoPP Policer

By default, the Layer 3 control packets such as ARP broadcast are dropped by the storm-control policer, but policed by the CoPP policer and sent to CPU. This is because, for control packets, the storm-control policer has a lower priority compared to the CoPP policer. Enabling the prioritize storm policer over the CoPP policer feature allows for increasing the priority of the storm-control policer over the CoPP policer for Layer 3 control packets. Consequently, the Layer 3 control packets such as ARP broadcast are dropped completely and not policed further by the CoPP policer, but policed by the storm-control policer.

Note When this feature is enabled, and if the incoming traffic is above the configured threshold value for a specific traffic type (multicast and broadcast), then the storm-control policer may not have control on the packets that get dropped. In this scenario, even the genuine Layer 3 control packets of that specific traffic type (multicast and broadcast) may get dropped.

Use the following command to prioritize the storm-control policer over the CoPP policer:

[**no**] **system storm-control priority-policy drop-l3**

Use the **no** form of this command to disable this feature.

Configuring Traffic Storm Control for Two-level Threshold

You can set the percentage of total available bandwidth that the controlled traffic can use for two-level threshold.

Procedure

	Command or Action	Purpose
Step 1	**system storm control multi-threshold** **Example:** `switch# system storm control multi-threshold`	Enters global CLI. This command is required only for configuring two-level threshold.

	Command or Action	Purpose
Step 2	**hardware access-list tcam region ing-storm-control 512** **Example:** `switch# hardware access-list tcam region ing-storm-control 512`	Carves a new TCAM region with a fixed size of 512 for the two-level threshold. After running the command, make sure that you reload the device.

Step 3	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 4	**interface** {**ethernet** *slot*/*port* | **port-channel** *number*}
	Example:
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		Enters interface configuration mode.

Step 5	[**no**] **storm-control multiunicast** {**level1** <*level-value %*> | **level2** <*level-value %*>} **Example:** `switch(config-if)# storm-control multi unicast level1 5 level2 10`	Configures traffic storm control for traffic on the interface for two-level threshold. You can also configure bandwidth level as a percentage of port capacity. The default state is disabled.
Step 6	[**no**] **storm-control multi action1** {**trap** | **shutdown**} **action2** {**trap** | **shutdown**} **Example:** `switch(config-if)# storm-control multi action1 trap action2 shutdown`	Generates the following: • An SNMP trap (defined in CISCO-PORT-STORM-CONTROL-MIB) to monitor the storm control. • A syslog message when the traffic storm control limit is reached. You can also configure the trap or shutdown action for the lower and higher level of storm control threshold. However, if you configure shutdown on lower threshold (level1) for a port, you must configure shutdown for higher threshold (level2) for that port.

Step 7	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 8	(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.

	Command or Action	Purpose
Step 9	(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 for one-level and two-level thresholds.

Command	Purpose
The following row is applicable only to one-level threshold.	
show interface [**ethernet** *slot*/*port* | **port-channel** *number*] **counters storm-control**	Displays the traffic storm control counters.
The following rows are applicable only to two-level threshold.	
show interface [**ethernet** *slot*/*port* | **port-channel** *number*] **counters storm-control multi-threshold**	Displays the list of the configured storm control values for all interfaces.
show interface [**ethernet** *slot*/*port* | **port-channel** *number*] **counters storm-control multi-threshold**	Displays the list of the configured storm control values for the interface.
show interface [**ethernet** *slot*/*port* | **port-channel** *number*] **counters storm-control multi-threshold unicast**	Displays the list of the unicast drops for both level1 and level2.
show interface [**ethernet** *slot*/*port* | **port-channel** *number*] **counters storm-control multi-threshold broadcast**	Displays the list of the broadcast drops for both level1 and level2.
show interface [**ethernet** *slot*/*port* | **port-channel** *number*] **counters storm-control multi-threshold multicast**	Displays the list of the multicast drops for both level1 and level2.

Configuration Examples for Traffic Storm Control

The following example shows how to configure traffic storm control for one-level threshold:

```
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 shows how to configure traffic storm control for two-level threshold:

```
switch# system storm control multi-threshold
switch# hardware access-list tcam region ing-storm-control 512
switch# configure terminal
switch(config)# interface Ethernet1/1
switch(config-if)# storm-control multi broadcast level1 5 level2 10
switch(config-if)# storm-control multi multicast level1 5 level2 10
switch(config-if)# storm-control multi unicast level1 5 level2 10
switch(config-if)# storm-control multi action1 trap action2 shutdown
```

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
-------------------------------------------------------------------------------
```

System Log Examples for Traffic Storm Control

The following example shows the system log for traffic storm control with one-level threshold:

- `%ETHPORT-5-STORM_CONTROL_ABOVE_THRESHOLD: Traffic in port Ethernet1/5 exceeds the configured threshold , action - Trap`

The following example shows the system log for traffic storm control with two-level threshold:

- `%ETHPORT-5-STORM_CONTROL_ABOVE_THRESHOLD: Traffic in port Ethernet1/5 exceeds the configured Broadcast threshold level1[10%], action - Trap`

- `%ETHPORT-5-STORM_CONTROL_ABOVE_THRESHOLD: Traffic in port Ethernet1/5 exceeds the configured Broadcast threshold level1[15%], action - Shutdown`

Note The system log message includes the specific traffic type that exceeded the threshold and the level at which the traffic type reached the storm control action on an interface.

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*