Configuring Traffic Storm Control

This chapter contains the following sections:

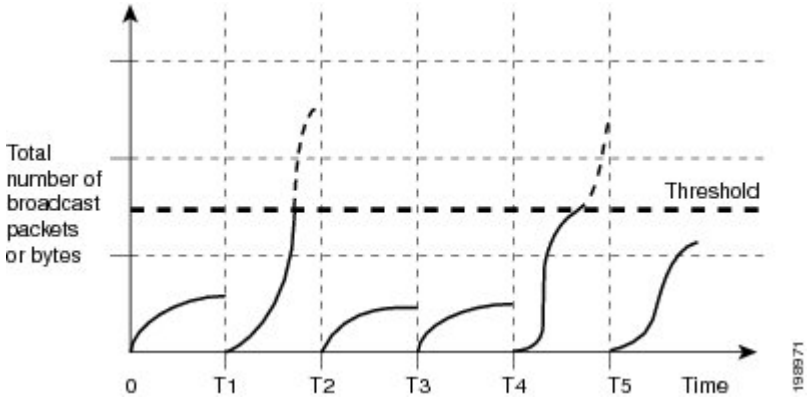
Information About Traffic Storm Control

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 Ethernet interfaces by a broadcast, unknown multicast, or unknown unicast traffic storm.

Traffic storm control (also called traffic suppression) allows you to monitor the levels of the incoming broadcast, unknown multicast, or unknown unicast traffic over a 10-microsecond 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.

The following figure shows the broadcast traffic patterns on an Ethernet interface during a specified time 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 packet granularity. For example, a higher threshold allows more packets to pass through.

Traffic storm control is implemented in the hardware. The traffic storm control circuitry monitors packets that pass from an Ethernet 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-microsecond 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-microsecond interval can affect the operation 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 10-microsecond interval, traffic storm control drops all exceeding broadcast traffic until the end of the interval.
- If you enable unknown multicast traffic storm control, and the learned multicast traffic exceeds the level within the 10-microsecond interval, traffic storm control drops all exceeding multicast traffic until the end of the interval.
- If you enable broadcast and unknown multicast traffic storm control, and broadcast traffic exceeds the level within the 10-microsecond interval, traffic storm control drops all exceeding broadcast traffic until the end of the interval.
- If you enable broadcast and unkown multicast traffic storm control, and multicast traffic exceeds the level within the 10-microsecond interval, traffic storm control drops all exceeding multicast traffic until the end of the interval.

You can configure traffic storm control to perform the following optional corrective actions when traffic exceeds the configured level:

- 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

When configuring the traffic storm control level, follow these guidelines and limitations:

- You can configure traffic storm control on a port-channel interface.
- 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.
- There are local link and hardware limitations that 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 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.
- The range of learned multicast will be changed by setting igmp snooping.
- Due to a hardware limitation, the output for the **show interface counters storm-control** command does not show ARP suppressions 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 being correctly storm suppressed.
- Due to a hardware limitation, the packet drop counter cannot distinguish between packet drops caused by a traffic storm and certain other discarded input frames. This limitation can lead to the configured action being triggered even in the absence of a traffic storm.
- Storm control is only for ingress traffic, specifically for unknown unicast, unknown multicast, and broadcast traffic.
- The link-level control protocols (LACP, LLDP and so on) are not affected in case of a traffic storm. The storm control is applied to data plane traffic only.
- The burst size values are:
  - For a 10G port, 48.68 Mbytes/390Mbits
  - For a 1G port, 25 Mbytes/200Mbits

Default Settings for Traffic Storm Control

The following 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-microsecond interval that can affect the operation of traffic storm control.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** {**ethernet** *slot*/*port* | **port-channel** *number*}	Enters interface configuration mode.
Step 3	switch(config-if)# **[no] storm-control** [**broadcast** | **multicast** | **unicast**] **level** *percentage*[.*fraction*] | [**action** {**shutdown** | **trap**}]	Configures traffic storm control for traffic on the interface. The default state is disabled.Also configures an optional corrective action that can be performed when traffic exceeds the configured level: • **shutdown**—Shuts down the port or puts it in the error-disable state. • **trap**—Generates an SNMP trap. The **no** form of this command removes the configured level or action. Although **shutdown** and **trap** actions can be specified independent of each other, the **no** form of **storm-control action** removes both actions.

Example

This example shows how to configure traffic storm control for port channels 122 and 123:

```
switch# configure terminal
switch(config)# interface port-channel 122, port-channel 123
switch(config-if-range)# storm-control unicast level 66.75
switch(config-if-range)# storm-control multicast level 66.75
switch(config-if-range)# storm-control broadcast level 66.75
switch(config-if-range)#
```

This example shows how to configure the port to shut down during a traffic storm:

```
switch# configure terminal
switch(config)# interface port-channel 122
switch(config-if)# storm-control action shutdown
```

This example shows how to configure the port to generate an SNMP trap during a traffic storm:

```
switch# configure terminal
switch(config)# interface port-channel 123
switch(config-if)# storm-control action trap
```

Verifying the Traffic Storm Control Configuration

Use the following commands to display traffic storm control configuration information:

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

Note When a storm event occurs and either a shutdown or a trap is triggered, a syslog message is generated.

This example shows how to display the storm control configuration:

```
switch(config-if)# show interface port-channel 122 counters storm-control

        [Action] S - Shut (Err Disable), T - Trap
--------------------------------------------------------------------------------
Port        UcastSupp %  McastSupp %  BcastSupp %  TotalSuppDiscards Action
--------------------------------------------------------------------------------
Po122            100.00       100.00       100.00                  0    [-T]
```

This example shows how to display the running configuration of an interface with its storm control configuration:

```
switch(config-if-range)# show running-config interface

interface Ethernet1/15

description IXIA
switchport mode trunk
spanning-tree port type edge trunk
spanning-tree bpdufilter enable
storm-control broadcast level 5.23
```

```
storm-control multicast level 0.50
storm-control unicast level 1.23
storm-control action shutdown
storm-control action trap
```

Traffic Storm Control Example Configuration

This example shows how to configure traffic storm control:

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# storm-control action trap
switch(config-if)# storm-control broadcast level 40
switch(config-if)# storm-control multicast level 40
switch(config-if)# storm-control unicast level 40
```

This example shows how to specify the number of Storm Control traps per minute:

```
switch# configure terminal
switch(config)# snmp-server enable traps storm-control trap-rate 100
switch(config)#
```