Configuring Traffic Storm Control

This chapter describes how to configure the traffic storm control feature in Cisco IOS Release 12.2SX.

Note For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Master Command List, at this URL:

http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

Tip For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum

This chapter consists of these sections:

Understanding Traffic Storm Control

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. The traffic storm control feature prevents LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm on physical interfaces.

Traffic storm control (also called traffic suppression) monitors incoming traffic levels over a 1-second traffic storm control interval, and during the interval it compares the traffic level with the traffic storm control level that you configure. The traffic storm control level is a percentage of the total available bandwidth of the port. Each port has a single traffic storm control level that is used for all types of traffic (broadcast, multicast, and unicast).

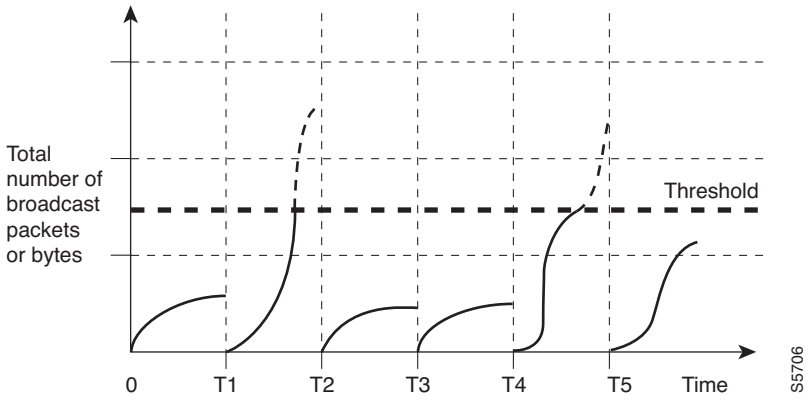
Traffic storm control monitors the level of each traffic type for which you enable traffic storm control in 1-second traffic storm control intervals.

In all releases, and by default in Release 12.2(33)SXJ and later releases, within an interval, when the ingress traffic for which traffic storm control is enabled reaches the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the traffic storm control interval ends. Release 12.2(33)SXJ and later releases support these configurable traffic storm control optional actions:

- Shutdown—When a traffic storm occurs, traffic storm control puts the port into the error-disabled state. To reenable ports, use the error-disable detection and recovery feature or the **shutdown** and **no shutdown** commands.
- Trap—When a traffic storm occurs, traffic storm control generates an SNMP trap.

Figure 57-1 shows the broadcast traffic patterns on a LAN interface over a specific 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 57-1 Broadcast Suppression



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

Traffic storm control is implemented in hardware. The traffic storm control circuitry monitors packets passing from a LAN interface to the switching bus. Using the Individual/Group bit in the packet destination address, the traffic storm control circuitry determines if the packet is unicast or broadcast, keeps track of the current count of packets within the 1-second interval and when the threshold is reached, traffic storm control filters out subsequent packets.

Because hardware traffic storm control uses a bandwidth-based method to measure traffic, the most significant implementation factor is setting the percentage of total available bandwidth that can be used by controlled traffic. Because packets do not arrive at uniform intervals, the 1-second interval during which controlled traffic activity is measured 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 a 1-second traffic storm control interval, traffic storm control drops all broadcast traffic until the end of the traffic storm control interval.
- If you enable broadcast and multicast traffic storm control, and the combined broadcast and multicast traffic exceeds the level within a 1-second traffic storm control interval, traffic storm control drops all broadcast and multicast traffic until the end of the traffic storm control interval.

- If you enable broadcast and multicast traffic storm control, and broadcast traffic exceeds the level within a 1-second traffic storm control interval, traffic storm control drops all broadcast and multicast traffic until the end of the traffic storm control interval.
- If you enable broadcast and multicast traffic storm control, and multicast traffic exceeds the level within a 1-second traffic storm control interval, traffic storm control drops all broadcast and multicast traffic until the end of the traffic storm control interval.

Default Traffic Storm Control Configuration

Traffic storm control is disabled by default.

Configuration Guidelines and Restrictions

When configuring traffic storm control, follow these guidelines and restrictions:

- FlexWAN Fast Ethernet port adapters and all WAN modules supporting Ethernet SPAs do not support traffic storm control.
- The following LAN switching modules do not support traffic storm control:
  - WS-X6148E-GE-45AT
  - WS-X6148A-GE-45AF
  - WS-X6148A-GE-TX
  - WS-X6148-GE-45AF
  - WS-X6148-GE-TX
  - WS-X6148V-GE-TX
  - WS-X6548-GE-45AF
  - WS-X6548-GE-TX
  - WS-X6548V-GE-TX
- The switch supports multicast and unicast traffic storm control on Gigabit and 10-Gigabit Ethernet LAN ports. Most FastEthernet switching modules do not support multicast and unicast traffic storm control, with the exception of WS-X6148A-RJ-45 and the WS-X6148-SFP.
- The switch supports broadcast traffic storm control on all LAN ports except on those modules previously noted.
- Except for BPDUs, traffic storm control does not differentiate between control traffic and data traffic.
- When multicast suppression is enabled, traffic storm control suppresses BPDUs when the multicast suppression threshold is exceeded on these modules:
  - WS-X6748-SFP
  - WS-X6724-SFP
  - WS-X6748-GE-TX
  - WS-X6748-GE-TX
  - WS-X6704-10GE
  - WS-SUP32-GE-3B

- WS-SUP32-10GE-3B
- WS-X6708-10G

When multicast suppression is enabled on the listed modules, do not configure traffic storm control on STP-protected ports that need to receive BPDUs.

Except on the listed modules, traffic storm control does not suppress BPDUs.

Configuring Traffic Storm Control

These sections describe how to configure traffic storm control:

Enabling Traffic Storm Control

To enable traffic storm control on an interface, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {{type[1] slot/port} | {port-channel number}}`	Selects an interface to configure.
Step 2	`Router(config-if)# storm-control broadcast level level[.level]`	Enables broadcast traffic storm control on the interface, configures the traffic storm control level, and applies the traffic storm control level to all traffic storm control modes enabled on the interface.
Step 3	`Router(config-if)# storm-control multicast level level[.level]` **Note** The **storm-control multicast** command is supported only on Gigabit and 10-Gigabit Ethernet interfaces.	Enables multicast traffic storm control on the interface, configures the traffic storm control level, and applies the traffic storm control level to all traffic storm control modes enabled on the interface.
Step 4	`Router(config-if)# storm-control unicast level level[.level]` **Note** The **storm-control unicast** command is supported only on Gigabit and 10-Gigabit Ethernet interfaces.	Enables unicast traffic storm control on the interface, configures the traffic storm control level, and applies the traffic storm control level to all traffic storm control modes enabled on the interface.
Step 5	`Router(config-if)# end`	Exits configuration mode.
Step 6	`Router# show running-config interface`	Verifies the configuration.

1. *type* = **fastethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

When configuring the traffic storm control level, note the following information:

- You can configure traffic storm control on the port channel interface of an EtherChannel.
- Do not configure traffic storm control on ports that are members of an EtherChannel. Configuring traffic storm control on ports that are configured as members of an EtherChannel 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.
- On these modules, these levels suppress all traffic:
  - WS-X6704-10GE: 0.33 percent or less
  - WS-X6724-SFP 10Mbps ports: 0.33 percent or less
  - WS-X6748-SFP 100Mbps ports: 0.03 percent or less
  - WS-X6748-GE-TX 100Mbps ports: 0.03 percent or less
  - WS-X6716-10G-3C, WS-X6716-10G-3CXL Oversubscription Mode: 0.29 percent or less
  - WS-X6716-10T-3C, WS-X6716-10T-3CXL Oversubscription Mode: 0.29 percent or less

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 making up the incoming traffic, the actual enforced level might differ from the configured level by several percentage points.

All routers in a VLAN see copies of all broadcast traffic. To avoid high RP CPU utilization caused by a high volume of broadcast traffic, the threshold typically is set to a very low value; for example, less than 1 percent on a Gigabit Ethernet port.

You can use the Top N feature to periodically measure the peak broadcast traffic levels of the selected ports. If you have a specific required broadcast traffic level (for example, from an application), you can use that requirement as the basis of the threshold.

Base the suppression threshold on your data, plus some additional capacity. For example, if the peak broadcast traffic that is acceptable for a port is 1 percent, a threshold of 1.5 percent might be appropriate. The faster the port speed, the less additional capacity is required.

Use the **show interfaces counters storm-control** command to monitor the effect of the values that you configure, and increase the configured threshold if the TotalSuppDiscards column shows nonzero values.

This example shows how to enable multicast traffic storm control on Gigabit Ethernet interface 3/16 and how to configure the traffic storm control level at 0.5 percent:

```
Router# configure terminal
Router(config)# interface gigabitethernet 3/16
Router(config-if)# storm-control multicast level 0.5
Router(config-if)# end
```

This example shows how the traffic storm control level configured for one mode affects all other modes that are already configured on the Gigabit Ethernet interface 4/10:

```
Router# show run inter gig4/10
Building configuration...

Current configuration : 176 bytes
!
Router# interface GigabitEthernet4/10
Router# switchport
Router# switchport mode access
Router# storm-control broadcast level 0.5
Router# storm-control multicast level 0.5
Router# spanning-tree portfast edge
Router# end

Router# configure terminal
Router(config)# interface gigabitethernet 4/10
Router(config-if)# storm-control unicast level 0.7
Router(config-if)# end

Router# show interfaces gig4/10 counters storm-control

Port      UcastSupp %     McastSupp %     BcastSupp %  TotalSuppDiscards
Gi4/10      00.70           00.70           00.70              0

Router#
```

Configuring the Traffic Storm Control Shutdown Mode

To configure the traffic storm control shutdown mode on an interface, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {{`*type*[1] *slot/port*`} | {port-channel` *number*`}}`	Selects an interface to configure.
Step 2	`Router(config-if)# storm-control action shutdown`	(Optional) Configures traffic storm control to error-disable ports when a traffic storm occurs. • Enter the **no storm-control action shutdown** command to revert to the default action (drop). • Use the error disable detection and recovery feature, or the **shutdown** and **no shutdown** commands to reenable ports.
Step 3	`Router(config-if)# end`	Exits configuration mode.
Step 4	`Router# show running-config` *interface*	Verifies the configuration.

1. *type* = **fastethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to configure the traffic storm control shutdown mode on Gigabit Ethernet interface 3/16:

```
Router# configure terminal
Router(config)# interface gigabitethernet 3/16
Router(config-if)# storm-control action shutdown
Router(config-if)# end
```

Configuring Traffic Storm Control SNMP Traps

To configure traffic storm control SNMP traps, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {{type[1] slot/port} | {port-channel number}}`	Selects an interface to configure.
Step 2	`Router(config-if)# storm-control action trap`	Configures traffic storm control to generate an SNMP trap when a storm is detected on the port.
Step 3	`Router(config-if)# exit`	Exits interface configuration mode.
Step 4	`Router(config)# snmp-server enable traps storm-control trap-rate value`	Configures the maximum number of storm-control traps sent per minute. The range is 0 to 1000; the default is 0 (no limit is imposed; a trap is sent at every occurrence).
Step 5	`Router(config)# end`	Exits configuration mode.
Step 6	`Router# show running-config interface`	Verifies the interface configuration.

1. *type* = **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to configure Gigabit Ethernet interface 3/16 to send an SNMP trap when a traffic storm is detected on the port and how to revert traffic storm control trap rate limiting to the default value:

```
Router# configure terminal
Router(config)# interface gigabitethernet 3/16
Router(config-if)# storm-control action trap
Router(config-if)# exit
Router(config)# snmp-server enable traps storm-control trap-rate 0
Router(config)# end
```

Displaying Traffic Storm Control Settings

To display traffic storm control information, use the commands described in Table 57-1.

Table 57-1 Commands for Displaying Traffic Storm Control Status and Configuration

Command	Purpose
`Router# show interfaces [{type[1] slot/port} | {port-channel number}] switchport`	Displays the administrative and operational status of all Layer 2 LAN ports or the specified Layer 2 LAN port.

`Router# show interfaces [{type[1] slot/port} | {port-channel number}] counters storm-control`
 	
`Router# show interfaces counters storm-control [module slot_number]`
	Displays the total number of packets discarded for all three traffic storm control modes, on all interfaces or on the specified interface.

1. *type* = **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

Note The **show interfaces** [{*interface_type slot/port*} | {**port-channel** *number*}] **counters** command does not display the discard count. You must the **storm-control** keyword to display the discard count.

Tip For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum