

Flow Control and Storm Control Configuration Guide

First Published: 2025-09-15

Last Modified: 2026-07-17

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.



Read Me First

Only supported features are documented. To confirm or clarify all the supported features for a platform, go to Cisco Feature Navigator.

Read Me First



CONTENTS

PREFACE

Read Me First iii

CHAPTER 1

Configure Flow Control 1

Feature History for flow control 1

Flow control 1

Benefits of flow control 2

Restrictions and limitations of flow control 2

Type of flow control 3

Configure IEEE 802.3x Ethernet flow control 3

Verify flow control 4

CHAPTER 2

Configure Storm Control 7

Feature History for Storm Control 7

Storm Control 7

Types of Traffic Managed by Storm Control 9

How Storm Control Works for Each Traffic Type 9

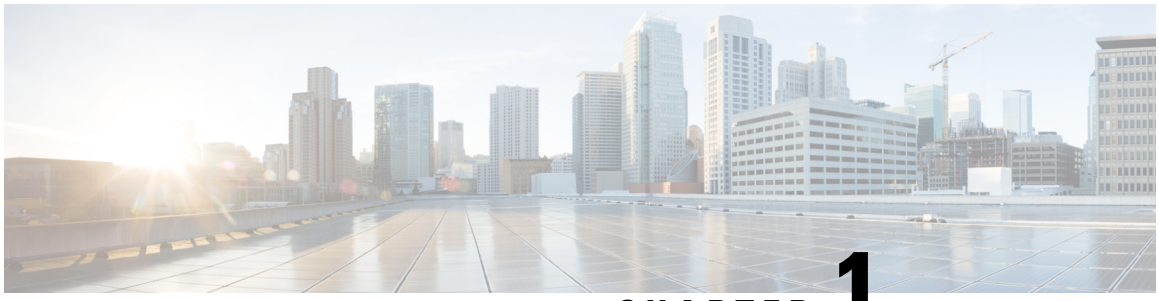
Storm Control Percentage and Bits per second Options 9

Storm Control Behavior on Port Channel Interfaces and Counters 10

Configuring Storm Control on Port Channels 10

Configure Storm Control on a Physical Interface 11

Configuring Storm Control Percentage or bps Options 13



CHAPTER 1

Configure Flow Control

- Feature History for flow control, on page 1
- Flow control, on page 1
- Configure IEEE 802.3x Ethernet flow control, on page 3
- Verify flow control, on page 4

Feature History for flow control

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Table 1:

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 26.2.1ea	Flow control: Flow control feature support has been introduced.	Cisco C9550 Series Smart Switches
Cisco IOS XE 17.18.1	Flow control is a mechanism designed to prevent a transmitting device from overwhelming a receiving device with data, ensuring that the receiver can process all incoming frames without dropping them due to buffer overflow.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

Flow control

Flow control is a mechanism designed to prevent a transmitting device from overwhelming a receiving device with data, ensuring that the receiver can process all incoming frames without dropping them due to buffer overflow.

In Layer 2 switches, flow control manages the rate of data transmission between two directly connected devices (e.g., a switch port and a server NIC, or two switch ports). When a receiving device's buffer is nearing capacity, it signals the transmitting device to temporarily pause or slow down its data transmission. This prevents packet

loss that would otherwise occur if the receiver's buffers overflowed, which would necessitate retransmissions and reduce overall network efficiency.

How it works (802.3x pause frames):

- Flow control typically operates on **full-duplex** connections, as half-duplex links use carrier sense multiple access with collision detection (CSMA/CD) for congestion management.
- The most common method for Layer 2 flow control is the use of IEEE 802.3x **pause frames**.
  - When a switch port (receiving frames) experiences congestion and its ingress buffers are becoming full, it sends a **pause frame** back to the directly connected transmitting device.
  - This pause frame contains a "pause time" value, indicating how long the transmitting device should stop sending data.
  - Upon receiving a pause frame, the transmitting device halts transmission for the specified duration.
  - Once the pause time expires, or if the receiving device sends another pause frame with a zero pause time (indicating that its buffers have cleared), the transmitting device resumes normal transmission.

Benefits of flow control

- **Prevents packet loss:** The primary benefit is to avoid dropping frames due to receiver buffer exhaustion, which improves data integrity.
- **Improves network efficiency:** By preventing drops, it reduces the need for higher-layer protocols (like TCP) to detect lost packets and initiate costly retransmissions, leading to better throughput.
- **Manages congestion:** Provides a local, immediate response to congestion at the physical link level.

Restrictions and limitations of flow control

While beneficial for preventing local packet loss, Layer 2 flow control has important restrictions and limitations:

- **Receive-only support:** Only flow control receive is supported. The switch can honor incoming IEEE 802.3x pause frames from the link partner, but it cannot send pause frames to request the peer to stop transmitting.
- **Head-of-line blocking (HOLB):** If a switch port is paused, it stops all traffic destined for that port, even if some of that traffic could be forwarded to other, uncongested ports within the switch. This can lead to reduced overall switch throughput and affect traffic that is not contributing to the congestion
- **Congestion propagation:** Pausing one link can cause congestion to back up to the upstream device, potentially propagating congestion throughout the network rather than isolating it. This can lead to a cascading effect where congestion spreads across the network.
- **Lack of Quality of Service (QoS) awareness:** Standard 802.3x flow control is not application-aware. It treats all traffic equally, regardless of its priority or sensitivity to delay. Higher-layer QoS mechanisms are needed for differentiated treatment of traffic.
- **Unsuitable for complex topologies:** In large or complex network topologies, enabling 802.3x flow control can lead to unpredictable behavior and make troubleshooting difficult due to the propagation of

pause frames. It is often recommended only for specific point-to-point connections, such as between a server and a switch.

- **Not always enabled:** Due to the potential for head-of-line blocking and congestion propagation, flow control is often disabled by default on switch ports or configured cautiously. The typical default configuration for 802.3x flow control on Cisco switches is disabled by default on many platforms to prevent HOLB and congestion propagation, but can vary.

Type of flow control

In Layer 2 Cisco switches, the primary type of flow control is based on IEEE 802.3x.

IEEE 802.3x Ethernet flow control (pause frames):

This is the standard mechanism described previously, where a congested receiving device sends a pause frame to the transmitting device, causing it to stop all data transmission for a specified period. This operates on full-duplex links, affects all traffic on the link, and is commonly supported on most Ethernet interfaces.

Configure IEEE 802.3x Ethernet flow control

This procedure enables or disables flow control on a specific interface.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Device(config)# interface GigabitEthernet0/1`	Specifies the interface for flow control configuration and enters interface configuration mode. Replace type and number with your specific interface.
Step 4	**flowcontrol receive {desired | on | off}** **Example:** `Device(config-if)# flowcontrol receive on`	Configures flow control on the interface. • **desired**—Allows but do not require flow-control packets on port. **off**—Disables flow-control packets on port **on**—Enables flow-control packets on port

	Command or Action	Purpose
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves the running configuration to the startup configuration.

Verify flow control

After configuring flow control, use these commands in privileged EXEC mode to verify its operation:

Procedure

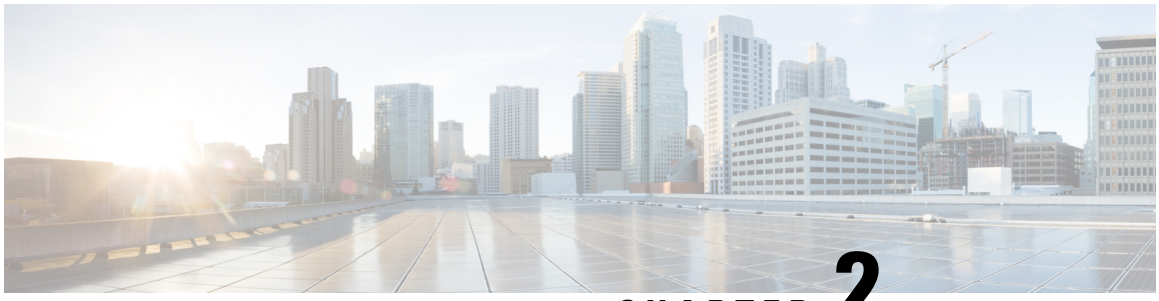
	Command or Action	Purpose

Step 1	**show flowcontrol interface** *interface-id*
	Example:
	`Device# show flowcontrol interface fif1/0/1`
	`%CLEAR-5-COUNTERS: Clear counter on all interfaces by console`
	`Port Send FlowControl Receive FlowControl RxPause TxPause`
	`admin oper admin oper`
	`------------ -------- -------- -------- -------- ------- -------`
	`Fif1/0/1 Unsupp. Unsupp. on on 0 0`
		Displays the flow control status (send/receive) for all interfaces or a specific interface.

Step 2	**show interface** *interface-id* **counters**
	Example:
	`Device# show interface fif1/0/1 counters`
	`Port InOctets InUcastPkts InMcastPkts InBcastPkts`
	`Fif1/0/1 68719989 57270 3 0`
	`Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts`
	`Fif1/0/1 1810 17 16 0`
		Shows interface counters, including pause frame counts. Look for "Pause input" and "Pause output" counters.

	Command or Action	Purpose

Step 3	**show running-config interface** *interface-id*
	Example:
	`interface GigabitEthernet0/1`
	`flowcontrol receive on`
	`!`
		Displays the running configuration for a specific interface, which includes flow control commands if configured.



CHAPTER 2

Configure Storm Control

- Feature History for Storm Control, on page 7
- Storm Control, on page 7
- Types of Traffic Managed by Storm Control, on page 9
- Storm Control Percentage and Bits per second Options, on page 9
- Storm Control Behavior on Port Channel Interfaces and Counters, on page 10
- Configuring Storm Control on Port Channels, on page 10
- Configure Storm Control on a Physical Interface, on page 11
- Configuring Storm Control Percentage or bps Options, on page 13

Feature History for Storm Control

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Table 2:

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 26.2.1ea	Storm Control: Storm Control feature support has been introduced.	Cisco C9550 Series Smart Switches
Cisco IOS XE 17.18.1	Storm Control is a feature in Cisco networking devices that helps prevent traffic storms caused by broadcast, multicast, or unicast traffic overwhelming the network.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

Storm Control

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic

and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configurations, or users issuing a denial-of-service attack can cause a storm.

Storm control (or traffic suppression) monitors packets passing from an interface to the switching bus and determines if the packet is unicast, multicast, or broadcast. The switch counts the number of packets of a specified type received within the 1-second time interval and compares the measurement with a predefined suppression-level threshold.

Measured Traffic Activity

Storm control uses one of these methods to measure traffic activity:

- Bandwidth as a percentage of the total available bandwidth of the port that can be used by the broadcast, multicast, or unicast traffic
- Traffic rate in bits per second at which broadcast, multicast, or unicast packets are received

With each method, when the rising threshold is reached, the port blocks only the excessive traffic above the threshold. If the falling suppression level is not specified, the device blocks all traffic until the traffic rate drops below the rising suppression level. In general, the higher the level, the less effective the protection against broadcast storms.



Note When the storm control threshold for multicast traffic is reached, all multicast traffic except control traffic, such as bridge protocol data unit (BDPU) and Cisco Discovery Protocol frames, are blocked. However, the device does not differentiate between routing updates, such as OSPF, and regular multicast data traffic, so both types of traffic are blocked.

Traffic Patterns

Broadcast traffic exceeded the configured threshold during the intervals from T1 to T2 and from T4 to T5. When the specified traffic exceeds this threshold, storm control drops the excess traffic only during the interval when the storm occurs. In the following interval (such as T3), if broadcast traffic is below the threshold, it is forwarded as usual.

The combination of the storm-control suppression level and the 1-second time interval controls the way the storm control algorithm works. A higher threshold allows more packets to pass through. A threshold value of 100 percent means that no limit is placed on the traffic. A value of 0.0 means that all broadcast, multicast, or unicast traffic on that port is blocked.



Note Because packets do not arrive at uniform intervals, the 1-second time interval during which traffic activity is measured can affect the behavior of storm control.

You use the **storm-control** interface configuration commands to set the threshold value for each traffic type.

Storm Control Using a Hardware Rate Limiter

Traffic storm control monitors incoming traffic levels over a configured interval. However, the reaction time taken by storm control is slightly slower as it is based on statistics counters to identify a storm. With the hardware rate limiter, the action is taken at the ASIC level, and as a result, the storm control action starts

immediately; as soon as the traffic rate reaches the set threshold level. The hardware rate limiter implements policers for broadcast, multicast, unicast, and unknown unicast traffic.

Types of Traffic Managed by Storm Control

- Broadcast Traffic: Broadcast packets are sent to all devices in the same broadcast domain (e.g., ARP requests, DHCP Discover messages). Excessive broadcast traffic can lead to a broadcast storm, overwhelming network devices and causing degraded performance.
- Multicast Traffic: Multicast packets are sent to a group of devices that have explicitly joined a multicast group (e.g., video streaming or IP telephony). If misconfigured or excessively generated, multicast traffic can cause a multicast storm, affecting network performance.
- Unicast Traffic: Unicast packets are sent to a specific MAC address. When a switch receives these packets, it checks its MAC address table to identify the corresponding port within the VLAN and forwards the packets accordingly. If the number of unicast packets exceeds the configured storm control threshold, storm control automatically filters and drops the excess packets to prevent network congestion.
- Unknown Unicast Traffic: Unknown unicast packets are destined for a specific MAC address, but the switch does not have the destination MAC in its MAC address table. These packets are flooded to all ports in the VLAN. Excessive unknown unicast traffic can lead to an unknown unicast storm, consuming bandwidth and overwhelming devices.

How Storm Control Works for Each Traffic Type

Storm Control uses thresholds to monitor and limit the traffic rate for each traffic type. When traffic exceeds the configured threshold, the switch takes action, such as dropping packets or shutting down the interface.

- Broadcast Traffic: Storm Control monitors the rate of broadcast packets and drops packets exceeding the threshold.
- Multicast Traffic: Storm Control applies similar monitoring as broadcast traffic and action for multicast packets.
- Unicast Traffic: Storm Control can limit unicast flooding by dropping traffic that exceeds the configured threshold.
- Unknown Unicast Traffic: Storm Control can limit unknown unicast flooding by dropping traffic that exceeds the configured threshold.

Storm Control Percentage and Bits per second Options

- Percentage: Enables administrators to specify a threshold as a percentage of the total available bandwidth of the interface, for example, 10% of a 10Gbps link.
- Bits per second (bps): Defines the threshold in bits per second, allowing granular control independent of the interface speed.

When traffic of a specified type exceeds the configured percentage or bps, Storm Control activates and drops excess packets, preventing the storm from affecting the rest of the network.

Storm Control Behavior on Port Channel Interfaces and Counters

When Storm Control is applied to PortChannel interfaces (also known as EtherChannels), it behaves slightly differently compared to individual physical interfaces. A PortChannel interface is a logical interface that aggregates multiple physical links. When Storm Control is applied to an EtherChannel, the configuration propagates to the underlying physical interfaces (members).

Configuring Storm Control on Port Channels

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface port-channel***number* **Example:** `Device(config)# interface Port-channel1`	Specifies the Port-channel interface to be configured, and enters interface configuration mode.

Step 4	**storm-control broadcast level {***value* **| bps** *value***}**
	Example:
	`Device(config-if)# storm-control broadcast level 15`
	Example:
	`Device(config-if)# storm-control broadcast level bps 15000000`
		Configures the broadcast storm control level as a rising threshold percentage of the interface bandwidth or as a suppression level in bits per second.

Step 5	**storm-control multicast level {***value* **| bps** *value***}**
	Example:
	`Device(config-if)# storm-control multicast level 20`
	Example:
	`Device(config-if)# storm-control multicast level bps 20000000`
		Configures the multicast storm control level as a percentage of the interface's bandwidth.

	Command or Action	Purpose

Step 6	**storm-control unicast level {***value* **| bps** *value***}**
	Example:
	`Device(config-if)# storm-control unicast level 10`
	Example:
	`Device(config-if)# storm-control unicast level bps 10000000`
		Configures the unicast storm control level as a rising threshold percentage of the interface bandwidth or as a suppression level in bits per second.

Step 7	**storm-control unknown-unicast level {***value* **| bps** *value***}**
	Example:
	`Device(config-if)# storm-control unknown-unicast level 10`
	Example:
	`Device(config-if)# storm-control unknown-unicast level bps 10000000`
		Configures the unknown unicast storm control level as a rising threshold percentage of the interface bandwidth or as a suppression level in bits per second.

Step 8	**storm-control action {shutdown | trap}**
	Example:
	`Device(config-if)# storm-control action shutdown`
	Example:
	`Device(config-if)# storm-control action trap`
		Specifies the action to take when the traffic threshold is exceeded.
		Note
		On Cisco C9550 Series Smart Switches, the **storm-control {broadcast | multicast | unicast | unknown-unicast} level** command supports only a single rising threshold value (`0.00` to `100.00`) or the `bps` option. Falling thresholds are not supported.

Configure Storm Control on a Physical Interface

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:**	Specifies the physical interface to be configured, and enters interface configuration mode.

	Command or Action	Purpose
	`Device(config)# interface GigabitEthernet1/0/1`	

Step 4	**storm-control broadcast level {***value* **| bps** *value***}**
	Example:
	`Device(config-if)# storm-control broadcast level 15`
	Example:
	`Device(config-if)# storm-control broadcast level bps 15000000`
		Configures the broadcast storm control level as a rising threshold percentage of the interface bandwidth or as a suppression level in bits per second.

Step 5	**storm-control multicast level {***value* **| bps** *value***}**
	Example:
	`Device(config-if)# storm-control multicast level 20`
	Example:
	`Device(config-if)# storm-control multicast level bps 20000000`
		Configures the multicast storm control level as a percentage of the interface's bandwidth.

Step 6	**storm-control unicast level {***value* **| bps** *value***}**
	Example:
	`Device(config-if)# storm-control unicast level 10`
	Example:
	`Device(config-if)# storm-control unicast level bps 10000000`
		Configures the unicast storm control level as a rising threshold percentage of the interface bandwidth or as a suppression level in bits per second.

Step 7	**storm-control unknown-unicast level {***value* **| bps** *value***}**
	Example:
	`Device(config-if)# storm-control unknown-unicast level 10`
	Example:
	`Device(config-if)# storm-control unknown-unicast level bps 10000000`
		Configures the unknown unicast storm control level as a rising threshold percentage of the interface bandwidth or as a suppression level in bits per second.

Step 8	**storm-control action {shutdown | trap}**
	Example:
	`Device(config-if)# storm-control action shutdown`
	Example:
	`Device(config-if)# storm-control action trap`
		Defines the action the interface takes when the traffic threshold is exceeded. In this case, it sends an SNMP trap notification.

Configuring Storm Control Percentage or bps Options

Procedure

	Command or Action	Purpose
Step 1	enable **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	configure terminal **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	interface interface-id **Example:** `Device(config)# interface GigabitEthernet1/0/1`	Specifies the interface on which to configure Storm Control, and enters interface configuration mode.

Step 4	storm-control {broadcast | multicast | unicast} level {value | bps value}
	Example:
	`Device(config-if)# storm-control broadcast level 10`
	`Device(config-if)# storm-control multicast level 15`
		Sets the percentage threshold for broadcast, multicast, or unknown unicast traffic.

Step 5	storm-control action {drop | shutdown | trap} **Example:** `Device(config-if)# storm-control action shutdown`	Defines the action the interface takes when the traffic threshold is exceeded. In this case, it shuts down the interface.