Flow Control and Storm Control Configuration Guide

First Published: 2025-09-15

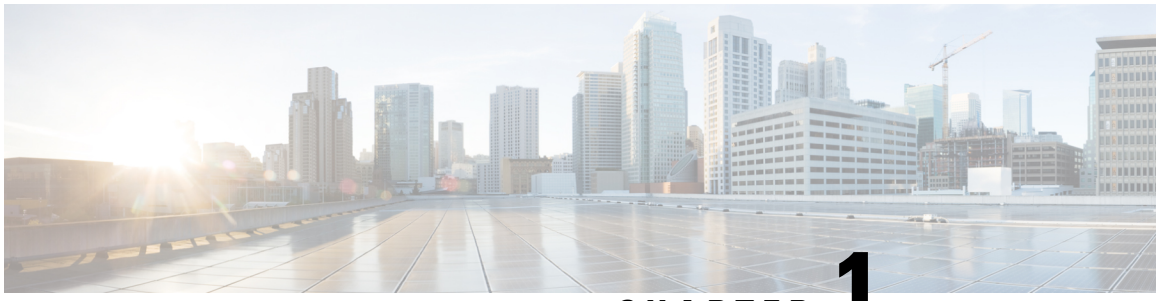
Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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



CHAPTER 1

Configure Flow Control

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 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 Contol

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:

- **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.

Types of Flow Control

In Layer 2 Cisco switches, the primary type of flow control is based on IEEE 802.3x. However, an important extension exists for lossless Ethernet environments.

- **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.
- **IEEE 802.1Qbb Priority Flow Control (PFC):**
  - PFC is an extension of 802.3x designed for **lossless Ethernet** environments, primarily in data centers where Fibre Channel over Ethernet (FCoE) or other lossless protocols are used. Unlike standard 802.3x, PFC allows for flow control on a **per-priority basis**. This means that traffic belonging to a specific QoS priority group (defined by 802.1p CoS values) can be paused independently of other traffic on the same link.
  - It Requires Data Center Bridging (DCB) capable hardware. It prevents packet loss for specific traffic classes by pausing only the congested priority queue, allowing other traffic classes to continue flowing on the same link. This mitigates head-of-line blocking for non-paused traffic.

Configure Flow Control

-

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:** `Switch# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	interface type number **Example:**	Specifies the interface for flow control configuration and enters interface configuration

	Command or Action	Purpose
	`Switch(config)# interface GigabitEthernet0/1`	mode. Replace type and number with your specific interface.

Step 4	flowcontrol {receive {on | off} | send {on | off} | {on | off}}
	Example:
	`Switch(config-if)# flowcontrol receive on`
	`Switch(config-if)# flowcontrol send on`
	`Switch(config-if)# flowcontrol on`
	`Switch(config-if)# flowcontrol off`
		Configures flow control on the interface.
		• receive on: Enables the interface to send pause frames when it experiences congestion.
		• send on: Enables the interface to process received pause frames and pause its transmission.
		• on: Enables both sending and receiving pause frames.
		• off: Disables flow control.

Step 5	End **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 6	copy running-config startup-config **Example:** `Switch# copy running-config startup-config`	Saves the running configuration to the startup configuration.

Configure Priority Flow Control

This procedure enables Priority Flow Control (PFC) on an interface and is typically part of a larger Data Center Bridging (DCB) configuration.

Procedure

	Command or Action	Purpose
Step 1	enable **Example:** `Switch# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	interface type number **Example:** `Switch(config)# interface Ethernet1/1`	Specifies the interface for PFC configuration, and enters interface configuration mode. (Note: Interface types for DCB switches may differ, e.g., Ethernet or TenGigabitEthernet).

	Command or Action	Purpose
Step 4	priority-flowcontrol mode{auto | on} **Example:** `Switch(config-if)# priority-flowcontrol mode on`	Configures the PFC mode on the interface. • on: Unconditionally enables PFC. • auto: Enables PFC only if the connected peer also supports and enables it (negotiated).
Step 5	priority-flowcontrol watch-interval seconds **Example:** `Switch(config-if)# priority-flowcontrol watch-interval 10`	(Optional) Configures the interval to monitor PFC status.
Step 6	End **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 7	copy running-config startup-config **Example:** `Switch# 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

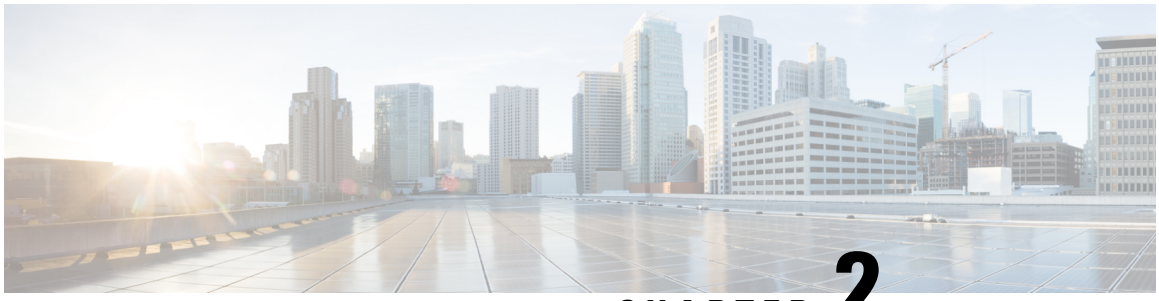
Step 1	show flowcontrol interface [type number]
	Example:
	`GigabitEthernet0/1`
	`Receive Flowcontrol: on`
	`Send Flowcontrol: on`
		Displays the flow control status (send/receive) for all interfaces or a specific interface.

Step 2	show interface [type number] counters
	Example:
	`GigabitEthernet0/1`
	`...`
	`Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0`
	`...`
	`0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored`
	`0 watchdog, 0 multicast, 0 pause input, 0 pause output`
		Shows interface counters, including pause frame counts. Look for "Pause input" and "Pause output" counters.

	Command or Action	Purpose

Step 3	show priority-flowcontrol interface [type number]
	Example:
	`Interface: Ethernet1/1`
	`Operational Mode: on`
	`Admin Mode: on`
	`Watch Interval: 10`
	`PFC Enabled: Yes`
	`Priority 0-7: Rx-On Tx-On`
		(For PFC-capable switches) Displays PFC status per interface and per priority.

Step 4	show running-config interface [type number]
	Example:
	`interface GigabitEthernet0/1`
	`flowcontrol receive on`
	`flowcontrol send 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

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 17.18.1	Storm Control/ Port Security 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 Port Security

Storm Control/ Port Security is a feature in Cisco networking devices that helps prevent traffic storms caused by broadcast, multicast, or unicast traffic overwhelming the network.

This can cause severe degradation in network performance, leading to issues such as high latency, packet loss, or even complete network outages. When packets flood the LAN, there is excessive traffic 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.

Management Traffic Control

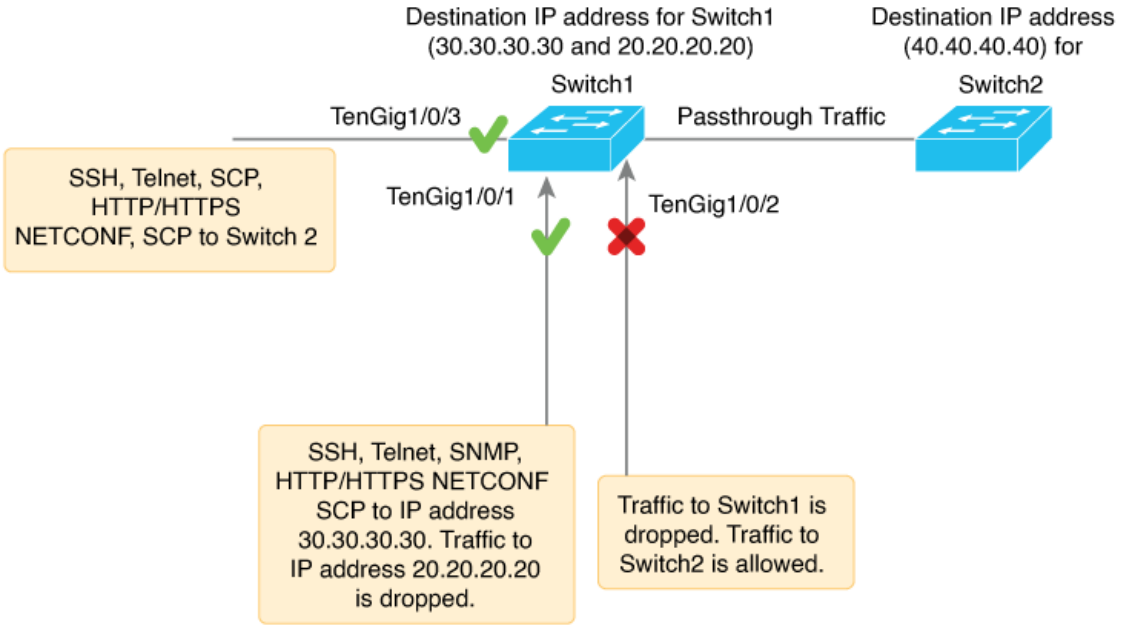
A device in a network allows traffic like SNMP, HTTP, HTTPS, Telnet, Secure Shell SSH and Netconf through any port with any IP address. Traffic flow from various interfaces to the local devices might decrease the security strength in a network. Management traffic control feature allows traffic to enter through a user-defined physical interface and restricts traffic to any other interfaces that is not defined by the user. When the feature is enabled a single IP address is assigned on the device to receive traffic. The user can configure the feature by defining an interface under the management traffic control feature. When the network protocol and the IP address is set according to the user's preference, traffic flow is allowed only through the defined interface.

The feature is supported on:

- Layer 2 physical interface.
- Layer 3 physical interface.
- Layer 2 port channel.
- Layer 3 port channel.
- App-hosting interface.

For example, in the following figure Switch1 and Switch2 are devices that are in a network. Management traffic control feature is enabled on Switch1 with the interface Tengig 1/0/1 and destination IP address 30.30.30.30. Traffic is allowed through the interface with the enabled protocols SSH, Telnet, SNMP, HTTP, HTTPS, Netconf, SCP to destination IP address 30.30.30.30. Traffic passing through interface Tengig 1/0/1 to IP address 20.20.20.20 is dropped. Management traffic control feature enables only one destination IP address to be configured. If interface TenGig 1/0/2 is not defined by the management traffic control feature

for any of the devices, traffic will not be allowed to Switch1 but can still pass through to its configured destination in the network.



Topic 2.1

Types of Traffic Managed by Storm Control (concept)

- 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.
- 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 and action for multicast packets.
- Unknown Unicast Traffic: Storm Control can limit unknown unicast flooding by dropping traffic that exceeds the configured threshold.

Storm Control Percentage option

The Percentage option in Storm Control allows administrators to specify a threshold as a percentage of the interface's bandwidth. When traffic of a specified type exceeds the configured percentage, Storm Control triggers and begins to drop excess packets, preventing the storm from affecting the rest of the network.

Key Points About the Percentage Option

Purpose:

- It limits traffic based on the percentage of the total bandwidth of the interface.
- Useful for setting dynamic thresholds relative to interface speed.

Traffic Types:

- Storm Control can monitor and limit broadcast, multicast, and unknown unicast traffic.
- You can configure it for one or more of these traffic types.

Configuration:

- The percentage value is relative to the interface's bandwidth (e.g., 10% of a 1 Gbps interface is 100 Mbps).
- Thresholds can be configured for different traffic types separately.

Action Taken: When traffic exceeds the threshold, the interface can either drop packets or shut down (depending on configuration).

Secure MAC Addresses

You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port. If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, when the MAC address of a station attempting to access the port is different from any of the identified secure MAC addresses, a security violation occurs. Also, if a station with a secure MAC address configured or learned on one secure port attempts to access another secure port, a violation is flagged.

Types of Secure MAC Addresses

The switch supports these types of secure MAC addresses:

- Static secure MAC addresses—These are manually configured by using the switchport port-security mac-address mac-address interface configuration command, stored in the address table, and added to the switch running configuration.
- Dynamic secure MAC addresses—These are dynamically configured, stored only in the address table, and removed when the switch restarts.
- Sticky secure MAC addresses—These can be dynamically learned or manually configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, when the switch restarts, the interface does not need to dynamically reconfigure them.

Sticky Secure MAC Addresses

You can configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and to add them to the running configuration by enabling sticky learning. The interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses. All sticky secure MAC addresses are added to the running configuration. The sticky secure MAC addresses do not automatically become part of the configuration file, which is the startup configuration used each time the switch restarts. If you save the sticky secure MAC addresses in the configuration file, when the switch restarts, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost. If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.

Port Security Aging

You can use port security aging to set the aging time for all secure addresses on a port.

Two types of aging are supported per port:

- Absolute—The secure addresses on the port are deleted after the specified aging time.
- Inactivity—The secure addresses on the port are deleted only if the secure addresses are inactive for the specified aging time.

Port Security and Switch Stacks

- When a switch joins a stack, the new switch will get the configured secure addresses. All dynamic secure addresses are downloaded by the new stack member from the other stack members.
- When a switch (either the active switch or a stack member) leaves the stack, the remaining stack members are notified, and the secure MAC addresses configured or learned by that switch are deleted from the secure MAC address table.

Table 3: Default Port Security Configuration

Feature	Default Setting
Port security	Disabled on a port.

Feature	Default Setting
Sticky address learning	Disabled.
Maximum number of secure MAC addresses per port	One address
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded.
Port security aging	Disabled. Aging time is 0. Static aging is disabled. Type is absolute.

Storm Control 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, so understanding how Storm Control works in this context is important for effective traffic management.

•

Restrictions for Port Security

- The maximum number of secure MAC addresses that you can configure on a switch is set by the maximum number of available MAC addresses allowed in the system. This number is the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces.
- Port Security is not supported on EtherChanel interfaces.
- Port Security is not supported on private VLAN ports.
- We recommend that you do not enable port security on an 802.1X authenticator interface.

When port-security is disabled on a port, the 802.1X sessions on the port get removed, because the aging timer and inactivity type is still configured. To ensure that the 802.1X sessions are not removed, when disabling port-security, disable the aging timer and inactivity type by removing the following commands:

- **switchport port-security aging time 1**
- **switchport port-security aging type inactivity**

Port Security Configuration Guidelines

The following guidelines are applicable during port security configuration:

- Port security can only be configured on static access ports or trunk ports. A secure port cannot be a dynamic access port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).

- Voice VLAN is only supported on access ports and not on trunk ports, even though the configuration is allowed.
- When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the phone.
- When a trunk port configured with port security and assigned to an access VLAN for data traffic and to a voice VLAN for voice traffic, entering the **switchport voice** and **switchport priority extend** interface configuration commands has no effect.

When a connected device uses the same MAC address to request an IP address for the access VLAN and then an IP address for the voice VLAN, only the access VLAN is assigned an IP address.

- When you enter a maximum secure address value for an interface, and the new value is greater than the previous value, the new value overwrites the previously configured value. If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.
- The switch does not support port security aging of sticky secure MAC addresses.

Security Violations

It is a security violation when one of these situations occurs:

- The maximum number of secure MAC addresses have been added to the address table, and a station whose MAC address is not in the address table attempts to access the interface.
- An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.
- Running diagnostic tests with port security enabled.

You can configure the interface for one of three violation modes, based on the action to be taken if a violation occurs:

- protect—when the number of secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.

Note We do not recommend configuring the protect violation mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.

- restrict—when the number of secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable

addresses. In this mode, you are notified that a security violation has occurred. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.

- shutdown—a port security violation causes the interface to become error-disabled and to shut down immediately, and the port LED turns off. When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause** psecure-violation global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands. This is the default mode.

This table shows the violation mode and the actions taken when you configure an interface for port security.

Table 4: Security Violation Mode Actions

Violation Mode	Traffic is forwarded	Sends SNMP trap	Sends syslog message	Displays error message	Violation counter increments	Shuts down port
protect	No	No	No	No	No	No
restrict	No	Yes	Yes	No	Yes	No
shutdown	No	No	No	No	Yes	Yes
shutdown vlan	No	No	Yes	No	Yes	No

Configuration Guidelines for Management Traffic Control

- You cannot configure IPv6 address configurations in the management traffic control feature.
- VRF based IP configuration is not supported on the management traffic control feature.
- The management traffic control feature is not supported on interfaces like port-channel member, SVI, stack-port and management port.

MAC Address Table Creation

With multiple MAC addresses supported on all ports, you can connect any port on the device to other network devices. The device provides dynamic addressing by learning the source address of packets it receives on each port and adding the address and its associated port number to the address table. As devices are added or removed from the network, the device updates the address table, adding new dynamic addresses and aging out those that are not in use.

The aging interval is globally configured. However, the device maintains an address table for each VLAN, and STP can accelerate the aging interval on a per-VLAN basis. The device sends packets between any combination of ports, based on the destination address of the received packet. Using the MAC address table, the device forwards the packet only to the port associated with the destination address. If the destination address is on the port that sent the packet, the packet is filtered and not forwarded. The device always uses the store-and-forward method: complete packets are stored and checked for errors before transmission.

Enabling and Configuring Port Security

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 gigabitethernet 1/0/1`	Specifies the interface to be configured, and enters interface configuration mode.
Step 4	switchport mode {access | trunk} **Example:** `Device(config-if)# switchport mode access`	Sets the interface switchport mode as access or trunk; an interface in the default mode (dynamic auto) cannot be configured as a secure port.
Step 5	switchport voice vlan vlan-id **Example:** `Device(config-if)# switchport voice vlan 22`	Enables voice VLAN on a port. • vlan-id —Specifies the VLAN to be used for voice traffic.
Step 6	switchport port-security **Example:** `Device(config-if)# switchport port-security`	Enables port security on the interface. **Note** Under certain conditions, when port security is enabled on the member ports in a switch stack, the DHCP and ARP packets would be dropped. As a workaround, shutdown the interface and then configure the no shutdown command.
Step 7	switchport port-security [maximum value [vlan {vlan-list | {access | voice}}]] **Example:** `Device(config-if)# switchport port-security maximum 20`	(Optional) Sets the maximum number of secure MAC addresses for the interface. The maximum number of secure MAC addresses that you can configure on a switch or switch stack is set by the maximum number of available MAC addresses allowed in the system. This number is the total of available MAC addresses, including those used for other

	Command or Action	Purpose
		Layer 2 functions and any other secure MAC addresses configured on interfaces.
Step 8	switchport port-security violation {protect | restrict | shutdown | shutdown vlan} **Example:** `Device(config-if)# switchport port-security violation restrict`	(Optional) Sets the violation mode, the action to be taken when a security violation is detected.
Step 9	switchport port-security [mac-address mac-address [vlan {vlan-id | {access | voice}}]] **Example:** `Device(config-if)# switchport port-security mac-address 00:A0:C7:12:C9:25 vlan 3 voice`	Enters a secure MAC address for the interface. You can use this command to enter the maximum number of secure MAC addresses. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned.
Step 10	switchport port-security mac-address sticky **Example:** `Device(config-if)# switchport port-security mac-address sticky`	(Optional) Enables sticky learning on the interface.
Step 11	switchport port-security mac-address sticky [mac-address | vlan {vlan-id | {access | voice}}] **Example:** `Device(config-if)# switchport port-security mac-address sticky 00:A0:C7:12:C9:25 vlan voice`	(Optional) Enters a sticky secure MAC address, repeating the command as many times as necessary. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned, are converted to sticky secure MAC addresses, and are added to the running configuration.
Step 12	end **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Example

What to do next

-

Enabling and Configuring Port Security Aging

Use this feature to remove and add devices on a secure port without manually deleting the existing secure MAC addresses and to still limit the number of secure addresses on a port. You can enable or disable the aging of secure addresses on a per-port basis.

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 to be configured, and enters interface configuration mode.

Step 4	switchport port-security aging {static | time time | type {absolute | inactivity}}
	Example:
	`Device(config-if)# switchport port-security aging time 120`
		Enables or disables static aging for the secure port, or sets the aging time or type.
		• static —to enable aging for statically configured secure addresses on this port.
		• time —time specifies the aging time for this port. The valid range is from 0 to 1440 minutes.
		• type —to select one of these keywords:
		  • absolute —Sets the aging type as absolute aging. All the secure addresses on this port age out exactly after the time (minutes) specified lapses and are removed from the secure address list.
		  • inactivity —Sets the aging type as inactivity aging. The secure addresses on this port age out only if there is no data traffic from the secure source addresses for the specified time period.

Step 5	end **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Changing the Address Aging Time

Follow these steps to configure the dynamic address table aging time:

Procedure

	Command or Action	Purpose
Step 1	enable **Example:** `Device> enable`	
Step 2	configure terminal **Example:** `Device# configure terminal`	
Step 3	mac address-table aging-time [0 | 10-1000000] [routed-mac | vlan vlan-id] **Example:** `Device(config)# mac address-table aging-time 500 vlan 2`	
Step 4	end **Example:** `Device(config)# end`	

Configuring Management Traffic Control

Procedure

	Command or Action	Purpose
Step 1	enable **Example:** `Device> enable`	
Step 2	configure terminal **Example:** `Device# configure terminal`	

Step 3	interface interface-id
	Example:
	`Device# mgmt-traffic control ipv4`
	`Device(config-mtc-ipv4)#`	

	Command or Action	Purpose

Step 4	mgmt-traffic control ipv4
	Example:
	`Device(config-mtc-ipv4)# interface gigabitethernet1/0/1`
	`Device(config-mtc-ipv4)#`	

Step 5	protocol{[telnet http https netconf scp snmp ssh]}
	Example:
	`Device(config-mtc-ipv4)# protocol telnet http https netconf scp snmp ssh`
	`Device(config-mtc-ipv4)#`	

Step 6	address ip-address
	Example:
	`Device(config-mtc-ipv4)# address 30.30.30.30`
	`Device(config-mtc-ipv4)#`	

Step 7	end **Example:** `Device(config-mtc-ipv4)# end`	

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-channelnumber **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 **Example:**	Configures the broadcast storm control level as a percentage of the interface's bandwidth.

	Command or Action	Purpose
	`Device(config-if)# storm-control broadcast level 15`	
Step 5	storm-control multicast level value **Example:** `Device(config-if)# storm-control multicast level 20`	Configures the multicast storm control level as a percentage of the interface's bandwidth.
Step 6	storm-control unicast level value **Example:** `Device(config-if)# storm-control unicast level 10`	Configures the unknown unicast storm control level as a percentage of the interface's bandwidth.

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 type number **Example:** `Device(config)# interface GigabitEthernet1/0/1`	Specifies the physical interface to be configured, and enters interface configuration mode.
Step 4	storm-control broadcast level value **Example:** `Device(config-if)# storm-control broadcast level 10`	Configures the broadcast storm control level as a percentage of the interface's bandwidth.
Step 5	storm-control multicast level value **Example:** `Device(config-if)# storm-control multicast level 15`	Configures the multicast storm control level as a percentage of the interface's bandwidth.

	Command or Action	Purpose
Step 6	storm-control action {drop | shutdown | trap} **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 Option

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
	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.

Default MAC Address Table Settings (reference)

The following table shows the default settings for the MAC address table.

Table 5:

Feature	Default Setting
Aging Time	300 seconds
Dynamic addresses	Automatically learned
Static addresses	None configured

Port Security Configuration Guidelines

The following guidelines are applicable during port security configuration:

- Port security can only be configured on static access ports or trunk ports. A secure port cannot be a dynamic access port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- Voice VLAN is only supported on access ports and not on trunk ports, even though the configuration is allowed.
- When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the phone.
- When a trunk port configured with port security and assigned to an access VLAN for data traffic and to a voice VLAN for voice traffic, entering the **switchport voice** and **switchport priority extend** interface configuration commands has no effect.

When a connected device uses the same MAC address to request an IP address for the access VLAN and then an IP address for the voice VLAN, only the access VLAN is assigned an IP address.

- When you enter a maximum secure address value for an interface, and the new value is greater than the previous value, the new value overwrites the previously configured value. If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.
- The switch does not support port security aging of sticky secure MAC addresses.

Port Security Compatibility with Other Features

Table 6:

Type of Port or Feature on Port	Compatible with Port Security
DTP port	No

Type of Port or Feature on Port	Compatible with Port Security
Trunk Port	Yes
Dynamic-access port	No
Routed port	No
SPAN source port	Yes
SPAN destination port	No
EtherChannel	No
Tunneling port	Yes
Protected port	Yes
IEEE 802.1x port	Yes
Voice VLAN port	Yes
IP source guard	Ye
Dynamic Address Resolution Protocol (ARP) inspection	Yes
Flex Links	Yes

Management Traffic Control (Supported protocols and ports)

Table 7:

Protocol	Keyword	Port Number
HTTPS	TCP	443
TELNET	TCP	23
SSH	TCP	22
NETCONF-SSH	TCP	830
SNMP	UDP	161
HTTP	TCP	80