

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.