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.