Spanning Tree Protocol Toolkit: PortFast

Introduction to the STP Toolkit

The **Spanning Tree Protocol (STP)** includes a set of optional features—often called the **STP toolkit**—that modify and enhance STP behavior. The five key features are:

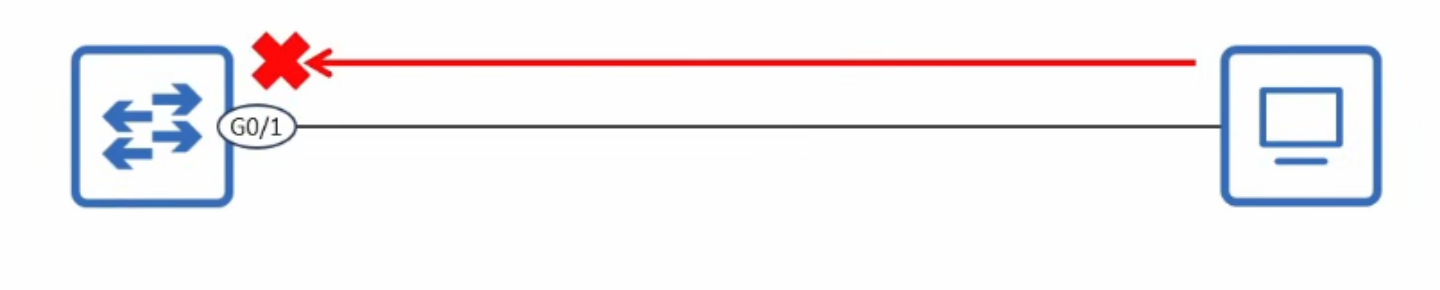
- **PortFast**: Allows switch ports connected to end hosts to immediately enter the **Forwarding** state, bypassing the **Listening** and **Learning** states.
- **BPDU Guard:** A feature that **shuts down** a port (puts it into **errdisable** state) if a BPDU is received. It is used to protect against rogue switches being connected to access ports.
- **BPDU Filter:** A feature that **prevents a port from sending or receiving BPDUs**. On access ports, it stops the port from participating in STP entirely.
- **Root Guard:** A feature that prevents a port from becoming an STP **root port**. If a superior BPDU is received, the port goes into **root-inconsistent** state, blocking traffic to protect the current root bridge.
- **Loop Guard:** A feature that **prevents alternate/root ports** from becoming designated and forwarding traffic if BPDUs stop being received. It puts the port into **loop-inconsistent** state to prevent loops caused by unidirectional link failures.

This section covers PortFast in depth; the other features are covered in subsequent videos.

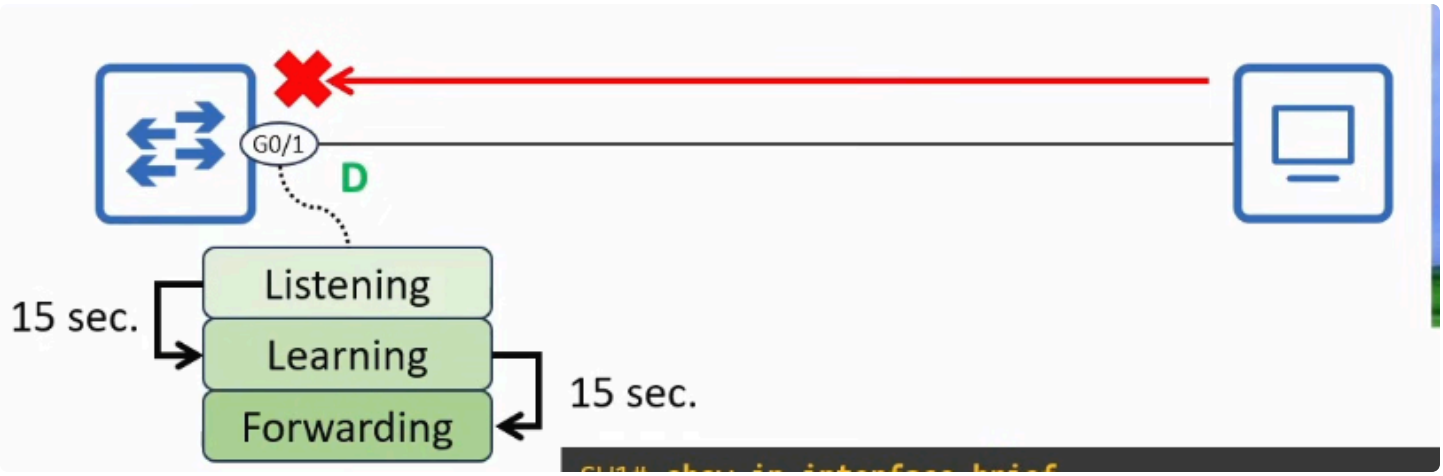
Problem: The 30-Second STP Delay

```
SW1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/1     unassigned      YES unset  up                    up
```

When an end host (e.g., a PC) connects to a switch port, the port comes up (**up/up** in `show ip interface brief`) but cannot send or receive data immediately.



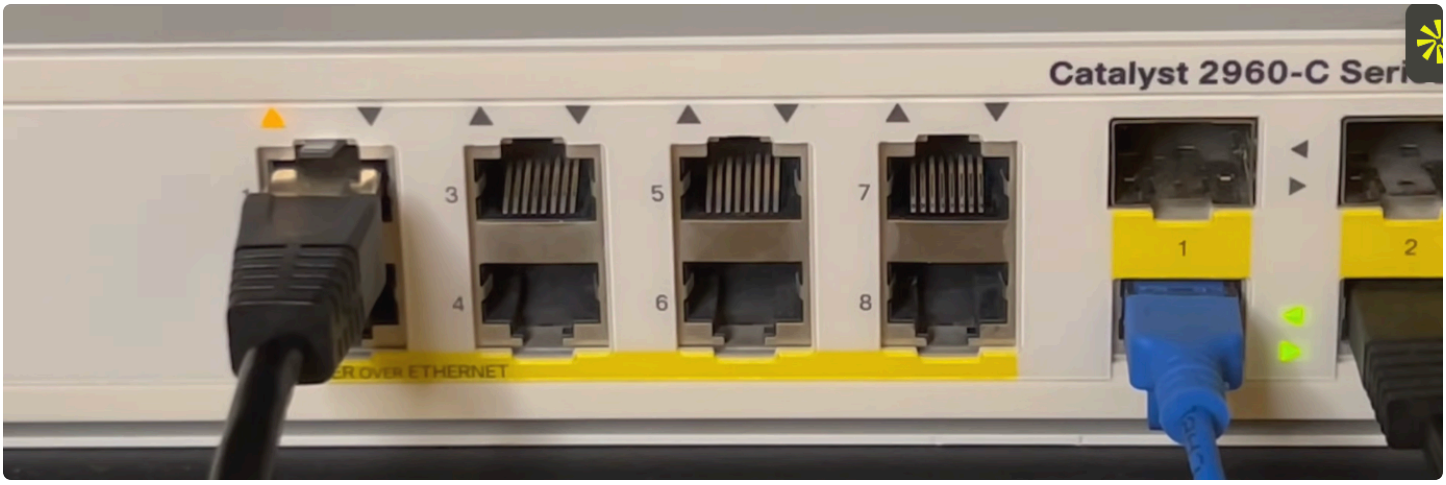
The switch, running STP, must wait through the **Listening** state (15 seconds) and **Learning** state (15 seconds) before moving to the **Forwarding** state.



This results in a **total delay of 30 seconds** before the host can communicate on the network.

> ***Key fact:*** *This wait is unnecessary because there is* ***no risk of a Layer 2 loop*** *between a switch and a single end host. Loops occur only between switches, which flood frames; PCs do not.*

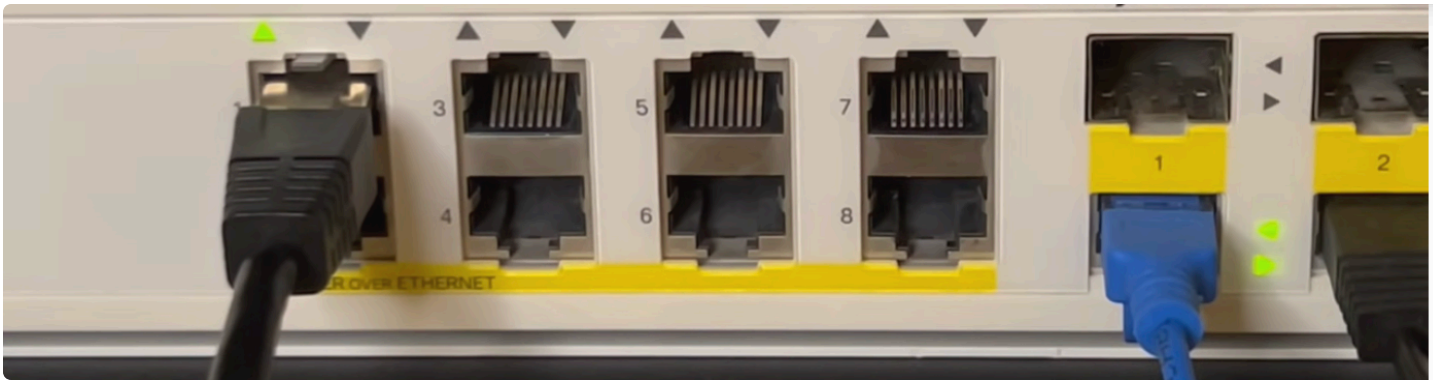
The user experience is poor: the user expects instant network access but experiences "the internet doesn't work" for 30 seconds. Even worse, the user has no awareness of STP and cannot diagnose the cause.



Visual indicator: On a Cisco Catalyst switch, when a cable is plugged into a port, the **link light** blinks amber during the STP delay, indicating the port is up but data is blocked. After 30 seconds, the light turns green, showing the port is in the **Forwarding** state and ready to transmit data.

Solution: PortFast

PortFast is a Cisco feature that enables a switch port to **skip the Listening and Learning states** and immediately enter the **Forwarding** state when a device is connected. This eliminates the 30-second delay, providing immediate network access for the end host.



Visual demonstration: When PortFast is enabled on a port and the cable is connected, the link light turns **green immediately**—no waiting.

> ***Definition:*** *PortFast allows a switch port to bypass STP convergence on access ports, making the port operational as soon as it is enabled.*

Configuring PortFast

PortFast can be enabled in two ways:

1. Per-Interface Configuration

Enter **interface configuration mode** and use the command:

```
spanning-tree portfast
```

or (in modern IOS):

```
spanning-tree portfast edge
```

This enables PortFast **only on that specific interface**. The feature is **active only when the interface is configured as an access port**, not a trunk.

When the command is issued, a **warning message** appears:

```
%Warning: PortFast should only be enabled on ports connected to a single host.
Connecting hubs, concentrators, switches, bridges, etc... to this interface
when portfast is enabled, can cause temporary bridging loops. Use with CAUTION.
```

Critical rule: Never enable PortFast on ports connected to other switches. The entire purpose of the Listening and Learning states is to detect and prevent Layer 2 loops. PortFast bypasses those checks, so a temporary loop could form if a switch is connected.

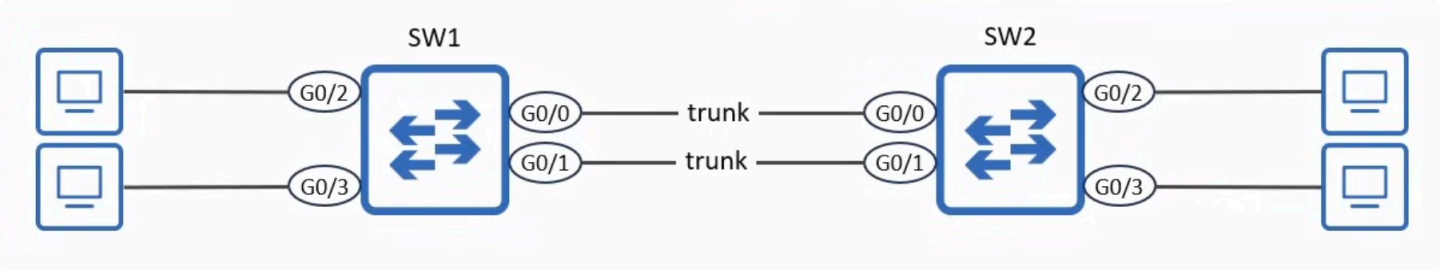
Additionally, a second message appears:

```
Portfast has been configured on GigabitEthernet0/1 but will only have effect
when the interface is in a non-trunking mode.
```

This confirms that PortFast is inactive on trunk ports by default.

1b. Portfast Demonstration in the CLI

2. Global Configuration (Default on All Access Ports)

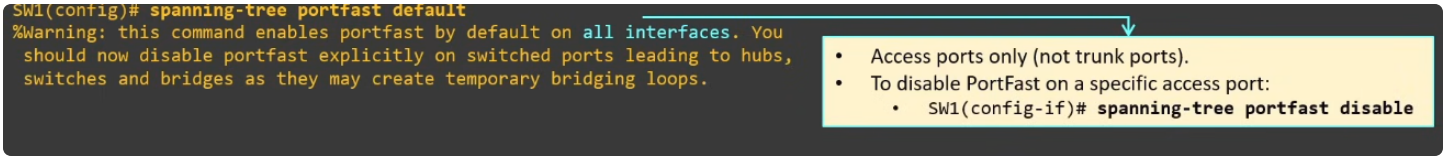


Enter **global configuration mode** and use:

```
spanning-tree portfast default
```

or:

```
spanning-tree portfast edge default
```



This command enables PortFast **by default on all access ports** (not trunk ports). A warning message is displayed, but it is somewhat misleading—it says "all interfaces," but PortFast only activates on access ports.

To disable PortFast on a specific access port after enabling it globally, enter interface configuration mode and use:

```
spanning-tree portfast disable
```

This is useful if an access port is mistakenly connected to another switch (though switch-to-switch links are typically trunks).

Verifying PortFast

After enabling PortFast globally on **SW1** using the command `spanning-tree portfast default`, verification was performed on two interfaces to confirm the feature's scope.

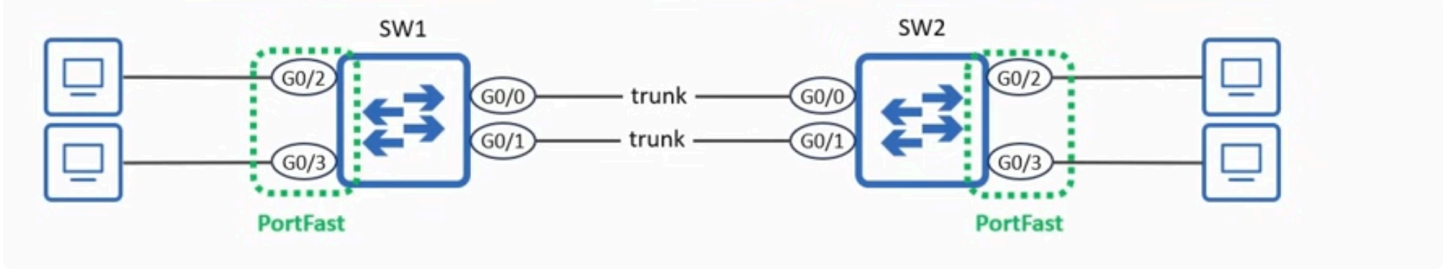
1. Access Port (G0/2 on SW1) — PortFast Active

The following command was used to inspect the access port:

```
SW1# show spanning-tree interface g0/2 detail
```

The relevant output line confirms PortFast is enabled:

```
The port is in the portfast edge mode by default
```

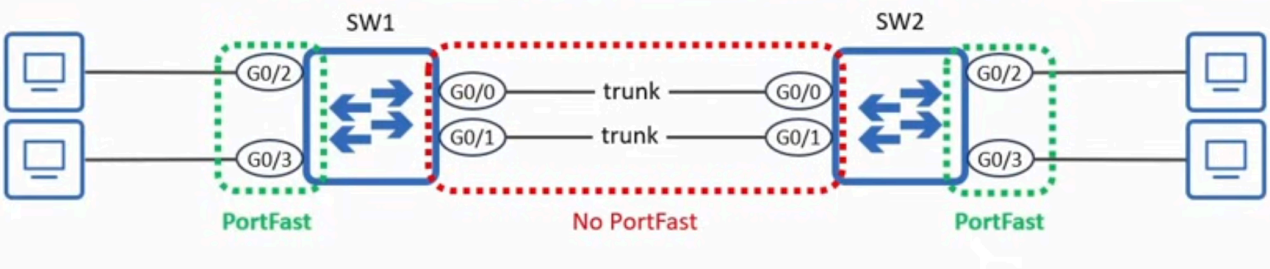


This indicates that PortFast has been activated on the access port **G0/2**, along with the three other access ports on **SW1** connected to end hosts.

2. Trunk Port (G0/1 on SW1) — PortFast Inactive

The same command was applied to the trunk interface:

```
SW1# show spanning-tree interface g0/1 detail
```



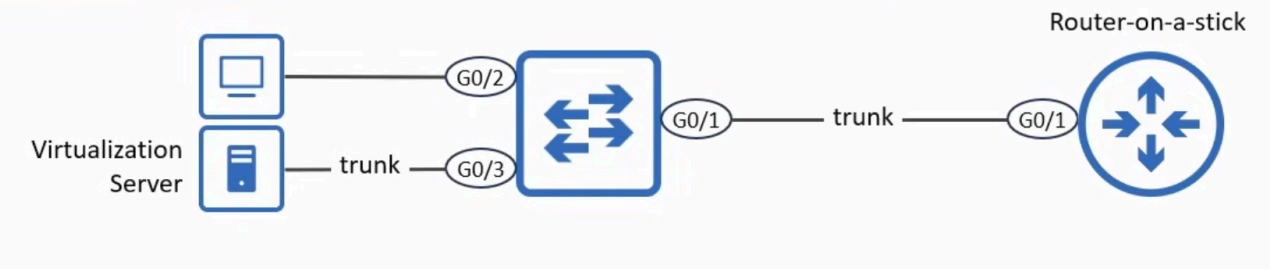
In this case, the output **contains no reference to PortFast**, confirming the feature is **not** enabled on the trunk port.

Key Point

When PortFast is configured globally using `spanning-tree portfast default`, it is **only applied to access ports**. Trunk ports, such as those connecting **SW1** to **SW2**, remain unaffected and continue to participate in standard STP convergence. This behavior is by design, as enabling PortFast on trunk links could introduce temporary Layer 2 loops.

PortFast on Trunk Ports

While PortFast is typically used on access ports, there are legitimate scenarios where it should be enabled on a **trunk port**:



- **Virtualization server**:
  - A server running virtual machines (VMs) in multiple VLANs often connects via a trunk link.
  - VMs are end hosts—they do not cause Layer 2 loops—so PortFast is safe.
- **Router-on-a-stick**:
  - A trunk link between a switch and a router.
  - Routers do not flood frames like switches, and therefore cannot create Layer 2 loops.

Configuration: PortFast on a trunk must be configured **per-interface** in interface configuration mode. The command is:

```
spanning-tree portfast trunk
```

or:

```
spanning-tree portfast edge trunk
```

The same warning about temporary loops appears, but it is safe on trunks to devices that cannot cause loops.

Verification with `show spanning-tree interface detail` will show:

```
The port is in portfast edge trunk mode
```

> ***Note:*** *For the CCNA exam, be familiar with enabling PortFast on trunks, but most scenarios involve access ports.*

The "Edge" Keyword Clarification

In modern Cisco switches, when you configure PortFast using the commands above, the switch automatically adds the **EDGE** keyword to the running configuration. This identifies PortFast as **PortFast Edge** (the standard CCNA variant) as opposed to **PortFast Network** (used for Bridge Assurance, which is not a CCNA topic).

Examples of automatic edge addition:

Command configured	Running-config equivalent
`spanning-tree portfast`	`spanning-tree portfast edge`
`spanning-tree portfast trunk`	`spanning-tree portfast edge trunk`
`spanning-tree portfast default`	`spanning-tree portfast edge default`
`spanning-tree portfast disable`	*(no edge keyword)*

Verifying the Automatic Addition of the EDGE Keyword

To confirm how modern Cisco switches handle the PortFast configuration, the following command was issued on **SW1's G0/1** interface:

```
SW1(config-if)# spanning-tree portfast
```

After applying the configuration, the running configuration for the interface was inspected using:

```
SW1# show running-config interface g0/1
```

The output revealed that the switch **automatically appended the EDGE keyword** to the command, even though it was not explicitly configured:

```
interface GigabitEthernet0/1
 spanning-tree portfast edge
```

This demonstrates that when `spanning-tree portfast` is configured, the switch internally converts it to `spanning-tree portfast edge`.

Key Points for the CCNA Exam

- The type of PortFast covered in the CCNA curriculum is **PortFast Edge**.
- Both command versions — with and without the **EDGE** keyword — produce the **same effect**.
- You should be familiar with both syntaxes for the exam.

Important Lab Note (Packet Tracer)

- The current version of **Packet Tracer** does **not** support the **EDGE** keyword.
- If you attempt to configure `spanning-tree portfast edge` in Packet Tracer, the command will be **rejected**.
- Use the non-edge version (`spanning-tree portfast`) when working in Packet Tracer labs.

Summary of PortFast

- **Problem:** When a host connects to a switch port, STP imposes a **30-second delay** (15s Listening + 15s Learning) before data can be transmitted. This creates a poor user experience.
- **Solution: PortFast** allows the port to **immediately enter the Forwarding state**, bypassing Listening and Learning.
- **Configuration methods:**
  - **Per-interface:** `spanning-tree portfast` (only on access ports)
  - **Global default:** `spanning-tree portfast default` (enables on all access ports)
  - **Per-interface disable:** `spanning-tree portfast disable`
  - **On trunk ports:** `spanning-tree portfast trunk`
- **Safety rule:** PortFast **must not** be configured on ports connected to other switches, as it can cause temporary Layer 2 loops.
- **Allowed trunk scenarios:** Router-on-a-stick and virtualization servers are acceptable because those devices do not create loops.
- **Verification:** Use `show spanning-tree interface <int> detail` to see “portfast edge mode.”
- **Edge keyword:** Automatically added by the switch; both versions of commands work. Packet Tracer does not support the EDGE keyword.