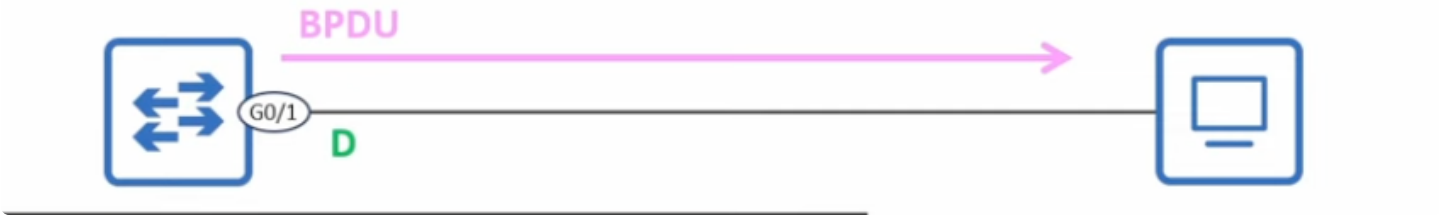
Spanning Tree Protocol Toolkit: BPDU Guard and BPDU Filter

Introduction to the STP Toolkit

This section of the CCNA course extends the **Spanning Tree Protocol** (STP) toolkit, building on the **PortFast** feature covered previously. Two additional features are essential for securing and optimizing STP behavior on switch ports connected to end hosts: **BPDU Guard** and **BPDU Filter**. These tools help prevent unauthorized switches from disrupting the STP topology and eliminate unnecessary BPDU traffic to end devices.

PortFast and BPDU Behavior Recap

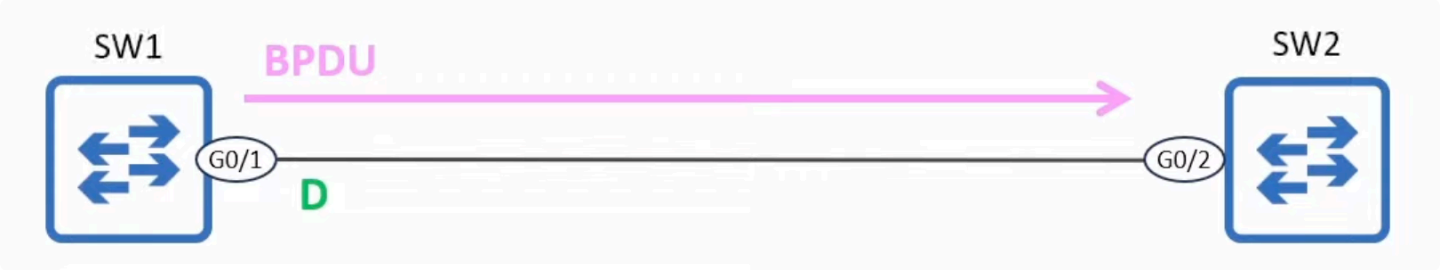
PortFast is a feature that allows a switch port to transition directly to the **Forwarding state** when a device connects, bypassing the usual Listening and Learning states. This enables end hosts (PCs, printers, routers) to communicate immediately.



- PortFast does **not** disable STP on the port. The port continues to send **BPDUs every 2 seconds**.
- PortFast-enabled ports that receive a BPDU will **revert to normal STP operation** (i.e., PortFast is disabled on that port, and it participates in STP normally).

PortFast and Unauthorized Switches – What Happens?

Scenario Setup



- SW1's G0/1 is a **PortFast-enabled port** (intended for an end host like a PC).
- A user connects an **unauthorized switch (SW2)** to that port instead.

What Happens When a Switch Connects?

- When a switch comes online **SW2**, it **assumes it is the root bridge** and begins sending BPDUs.
- SW1's PortFast-enabled port **receives a BPDU from SW2**.

PortFast's Reaction to Receiving a BPDU

- PortFast does NOT disable STP — it only skips Listening/Learning states on initial connection.
- If a PortFast-enabled port **receives a BPDU**, it **reverts to normal STP operation**:
  - PortFast is **automatically disabled** on that port.
  - The port now behaves like a regular STP port.

STP Election Example

Switch	Bridge Priority	Bridge ID
SW1	32768	Higher
SW2	4096	Lower

- SW2 has a **lower priority** → **lower bridge ID**.
- **SW2 becomes the root bridge**.
- **SW1's G0/1 becomes a root port**.

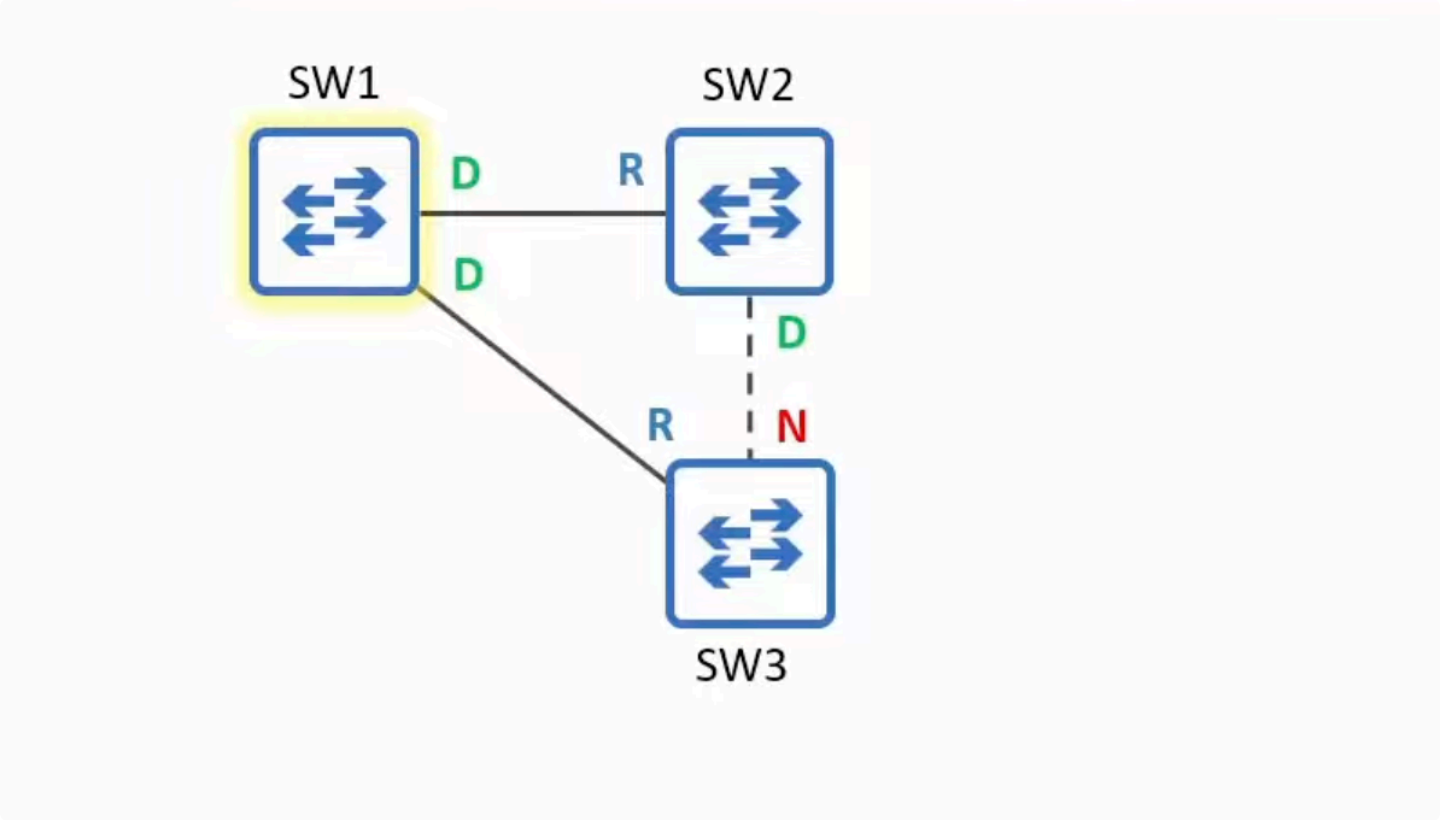
Why This Is a Problem

- The network's STP topology has been **altered by an unauthorized device**.
- SW1 was likely designed as the root bridge (e.g., connected to the main router).
- Now SW2 (Bob's switch) becomes the root bridge, which can cause:
  - Less efficient paths to the router
  - Critical links becoming blocked
  - Disruption of the carefully planned STP topology
  - Potential performance and stability issues

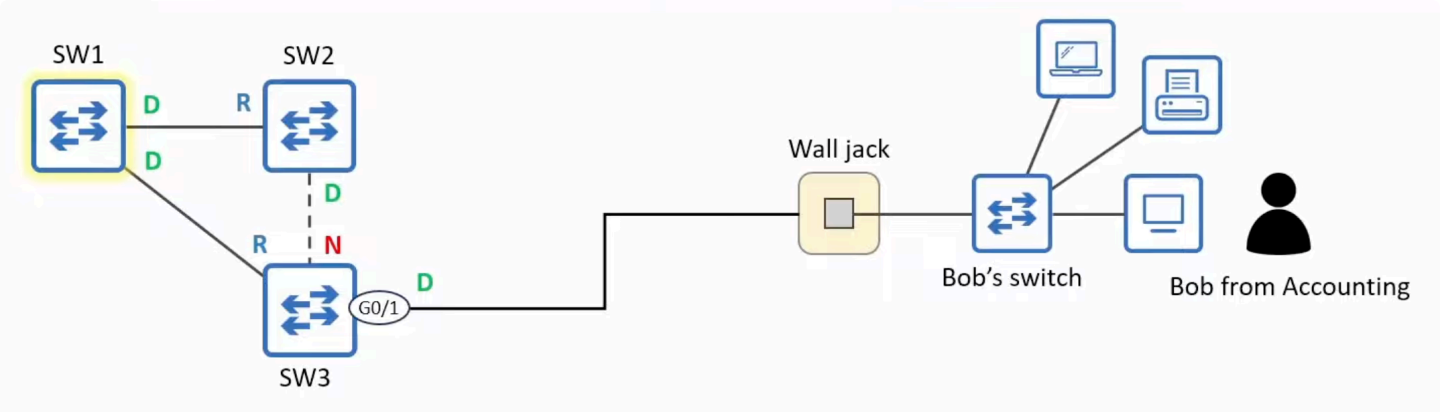
Key Takeaway

- **PortFast alone cannot prevent this** — it only skips the initial STP states.
- This is why **BPDU Guard** is needed: to error-disable the port and prevent unauthorized switches from affecting the network.

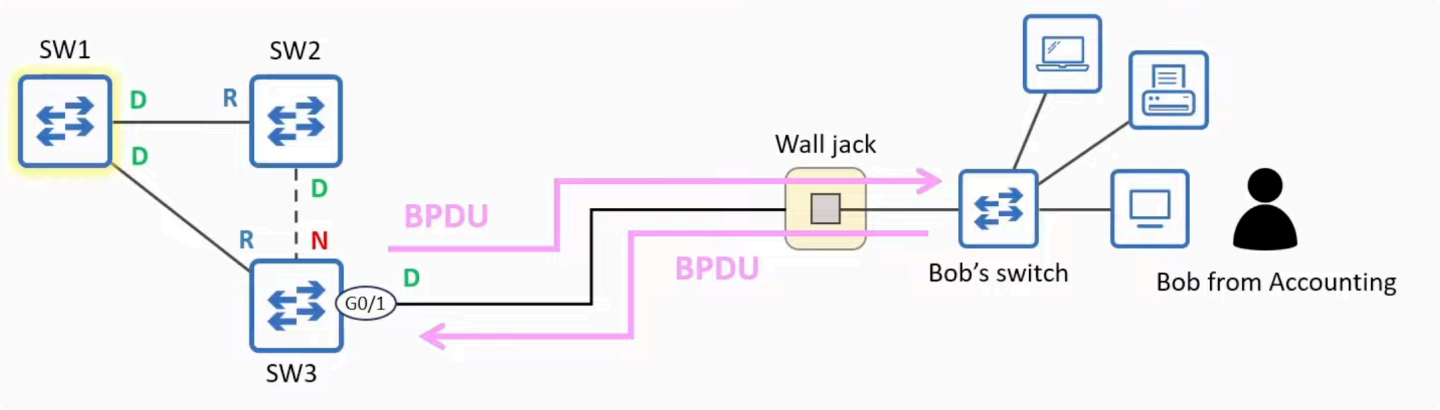
The Problem: Unauthorized Switch Connection



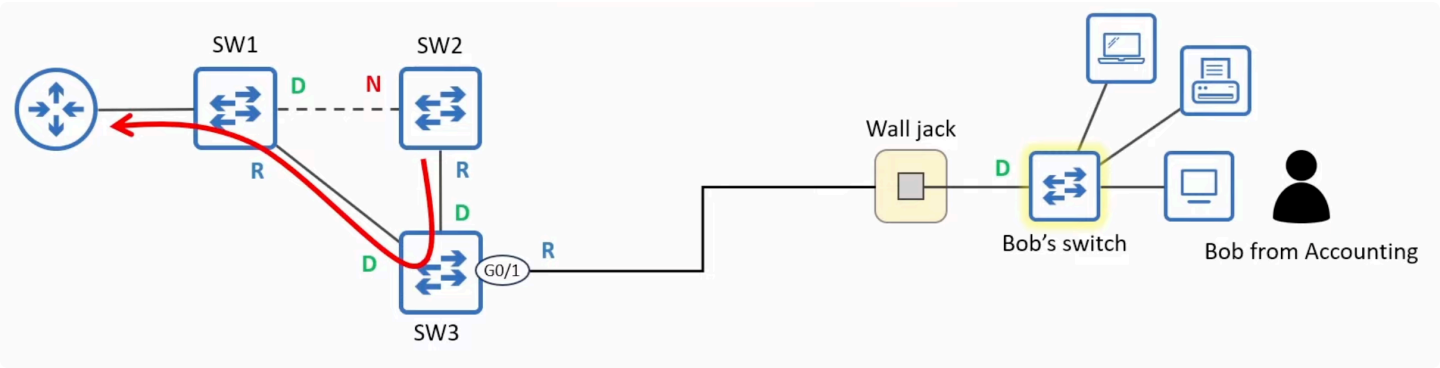
Consider a standard office setup: There's a simple LAN with 3 switches which includes SW1, SW2, and SW3. SW1 is the root bridge with all designated ports. SW2 and SW3 each have one root port leading towards SW1. Finally the link between SW2 and SW3 is blocked.



A wall jack connected to a switch (SW3), intended for an end host. A user ("Bob from Accounting") connects a personal switch to that wall jack to add more ports for his printer and laptop.



This new switch begins exchanging BPDUs with SW3, potentially altering the STP topology.



- If Bob's switch has a lower **bridge ID** (e.g., priority 4096 vs. the root bridge's 32768), it could become the **root bridge**, causing inefficient paths and possibly blocking critical links.
- The intended root bridge (connected to the router) might lose its optimal path, degrading network performance.

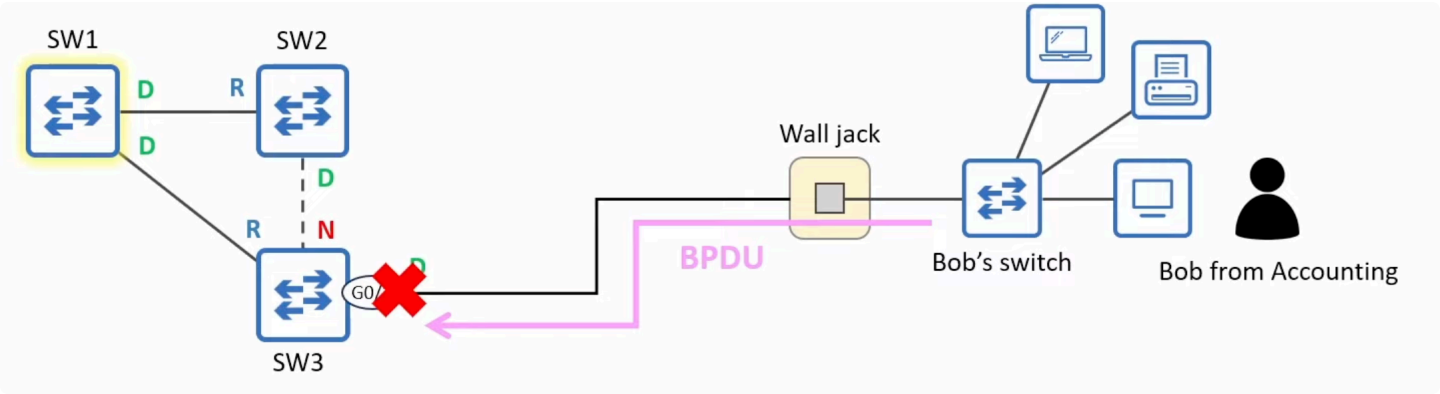
PortFast alone cannot prevent this because it only skips the initial STP states; it still allows STP to engage after receiving a BPDU. **BPDU Guard** is designed to solve this problem.

BPDU Guard

BPDU Guard protects the network by automatically **error-disabling** a switch port if it receives any BPDU. This action prevents unauthorized switches from participating in STP.

How BPDU Guard Works

- A port with BPDU Guard enabled continues to send BPDUs (like a normal STP port).
- If the port receives a BPDU, it immediately transitions to the **err-disabled state** (error-disabled). No data or BPDUs can be sent or received.
- This effectively disconnects the unauthorized switch, forcing the user to contact IT support.



Example: If bob connects his switch to the wall jack and it sends a bpdu to SW3, SW3 will do the following:

- Error disable its G0/1 port.
  - In effect this disables the port and it can no longer send or receive data and bpdu's.
- This prevents Bob's switch from effecting the STP topology.

Configuring BPDU Guard

BPDU Guard can be configured in two ways, similar to PortFast:

1. **Per-port configuration** (interface config mode):

   ```
   SW3(config-if)# spanning-tree bpduguard enable
   ```

   This enables BPDU Guard only on the specific interface.

2. **Global default configuration** (global config mode):

   ```
   SW3(config)# spanning-tree portfast bpduguard default
   ```

   (Optionally, you can add the `edge` keyword: `spanning-tree portfast edge bpduguard default`.)

   This enables BPDU Guard on all **PortFast-enabled ports** (not all access ports). This distinction is important for the CCNA exam.

To disable BPDU Guard on a specific port (e.g., a port that should connect to another switch), use:

```
SW3(config-if)# spanning-tree bpduguard disable
```

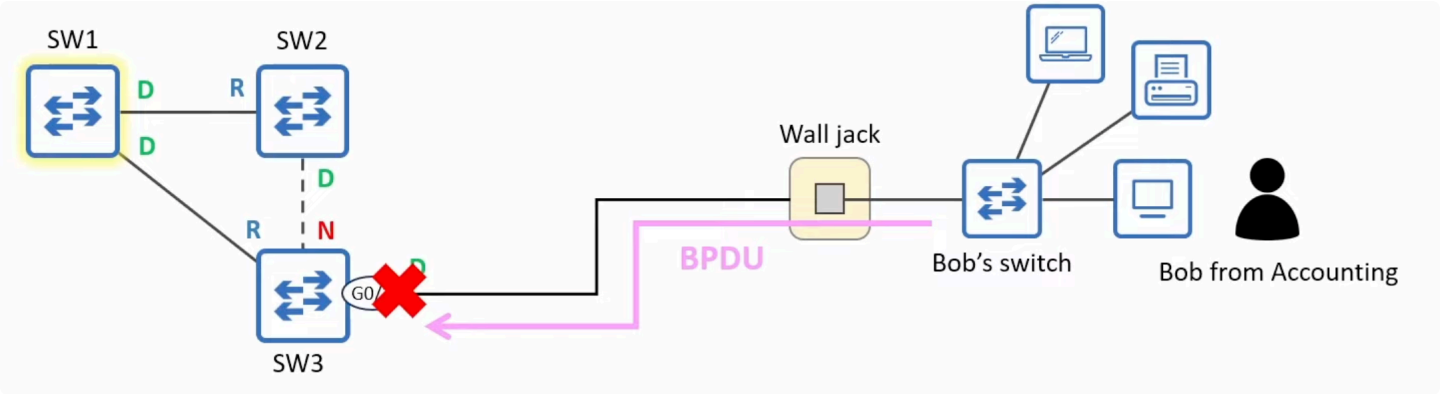
Verifying BPDU Guard

Use the `show spanning-tree interface <interface> detail` command to view the BPDU Guard status:

```
SW3# show spanning-tree interface g0/1 detail
```

The output will indicate whether BPDU Guard is enabled and whether it was configured per-port or by default.

Handling the Err-Disabled State

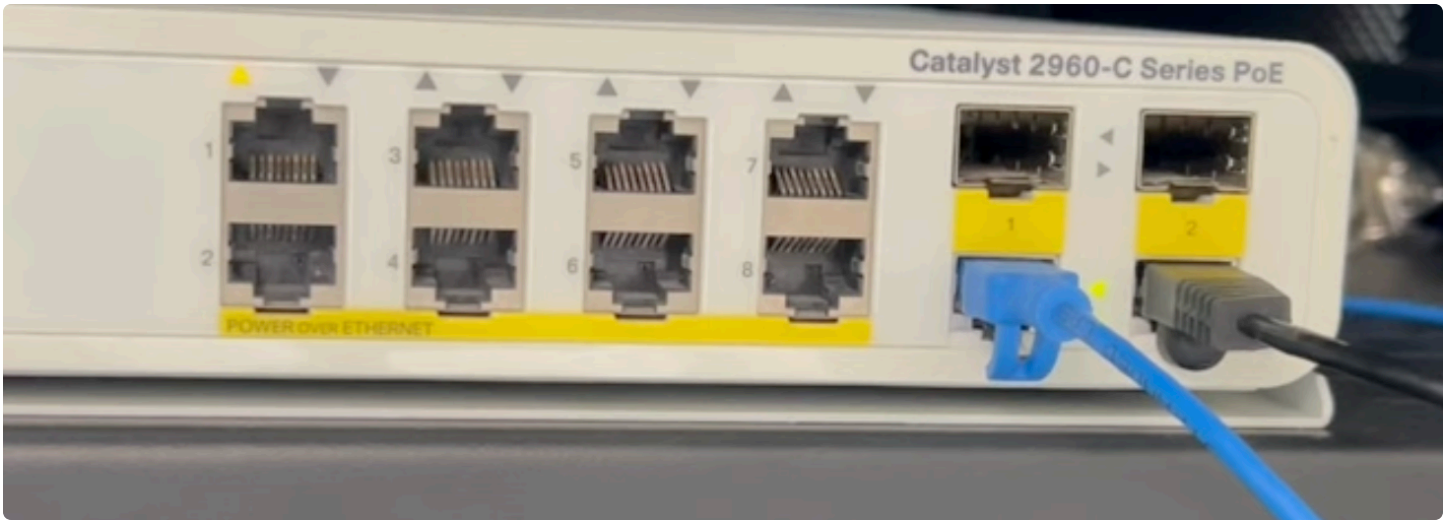


Example on BPDU Guard: SW3 guard-enabled port has received a BPDU from Bob's switch, so it is error-disabled.

- In SW3's CLI you see a message appear.
- When a BPDU Guard-enabled port receives a BPDU, the switch generates console messages:

```
%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port GigabitEthernet0/1 with BPDU
Guard enabled. Disabling port.
%PM-4-ERR_DISABLE: bpduguard error detected on G0/1, putting G0/1 in err-disable
state
%LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to down
SW3# show spanning-tree interface g0/1 detail
GigabitEthernet0/1 is down, line protocol is down (err-disabled)
!output omitted
```

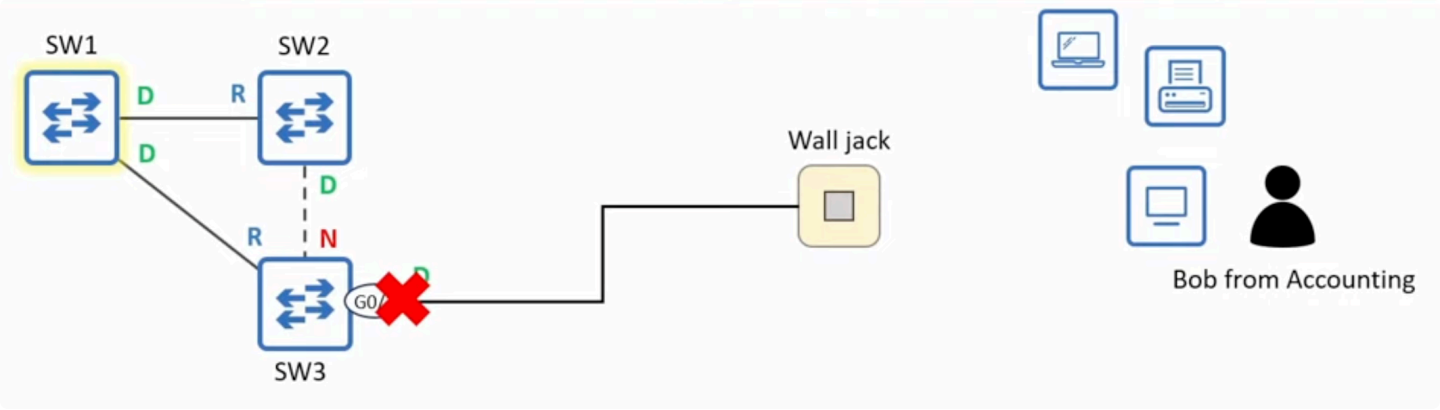
ErrDisable: is a Cisco switch feature that disables a port under certain conditions, such as a BPDU Guard violationl.



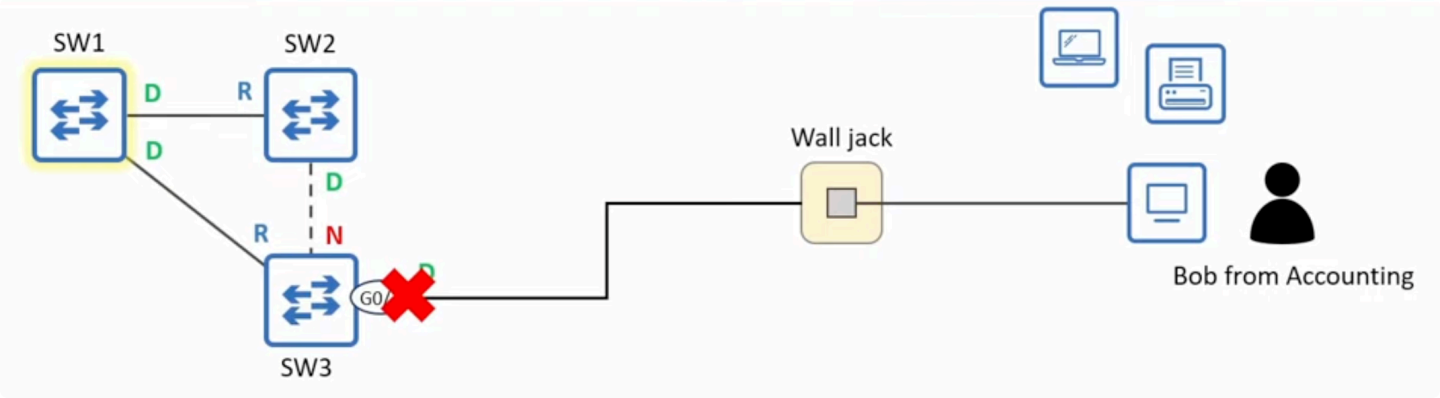
Let's see BPDU Guard in action on a Cisco Switch. I've configured PortFast and BPDU Guard on port 1 on the left of the top switch, below it is another Cisco Swtich so lets connect them. The port's link light may remain solid amber even after the cable is disconnected, indicating the err-disabled state.

Recovering an Err-Disabled Port

Before entering any commands we have to fix the underlying issue first.



- disconnect the unauthorized switch.
- This is key because if you renable the port without disconnecting Bob's switch, the port will be error-disabled again immediately.
- In this example if you re-enable switch 3''s G0/a port it will just receive another BPDU from bod's switch and be disabled again right away. So disconnecting Bob's switch from the wall jack.



- Now we can reconnect Bob's PC.

There are Two methods that exist to re-enable the port that has been err-disabled:

1. **Manual recovery** – Use the `shutdown` and `no shutdown` commands:

```
SW3(config-if)# shutdown
SW3(config-if)# no shutdown
```

This resets the port.

2. **Automatic recovery with ErrDisable Recovery** – This feature re-enables err-disabled ports after a configurable period. By default, **ErrDisable Recovery is disabled**.

Recovering an Err-Disabled Port with ErrDisable Recovery

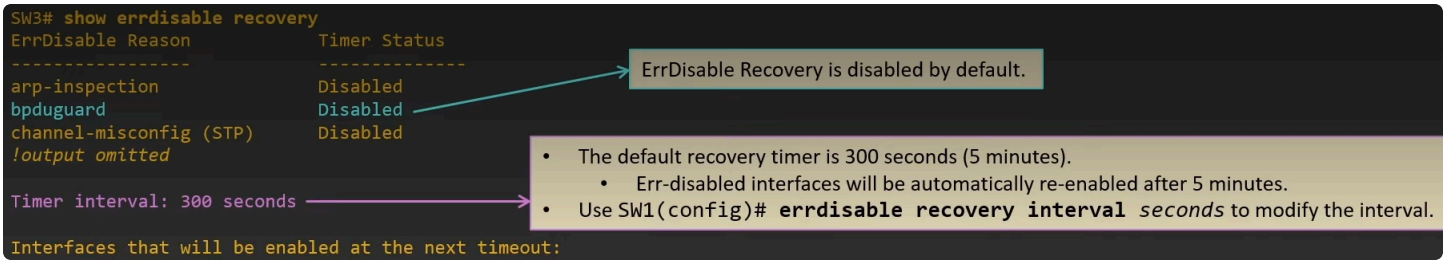
Overview

ErrDisable Recovery is a feature that **automatically re-enables err-disabled ports** after a certain period of time.

Viewing ErrDisable Recovery Status

```
SW1# show errdisable recovery
```

Output highlights:



- Lists all "errdisable reasons" and their recovery status.
- **BPDU Guard** is second on the list (after `arp-inspection`/DAI).
- ErrDisable Recovery is **disabled by default** — err-disabled ports will not automatically recover unless you enable it.
- Default recovery timer: **300 seconds (5 minutes)** .

Use ErrDisable Recovery cause to enable ErrDisable Recovery for ports disabled by a particular cause.

Step 1 – Enable recovery for a specific cause:

```
SW1(config)# errdisable recovery cause bpduguard
```

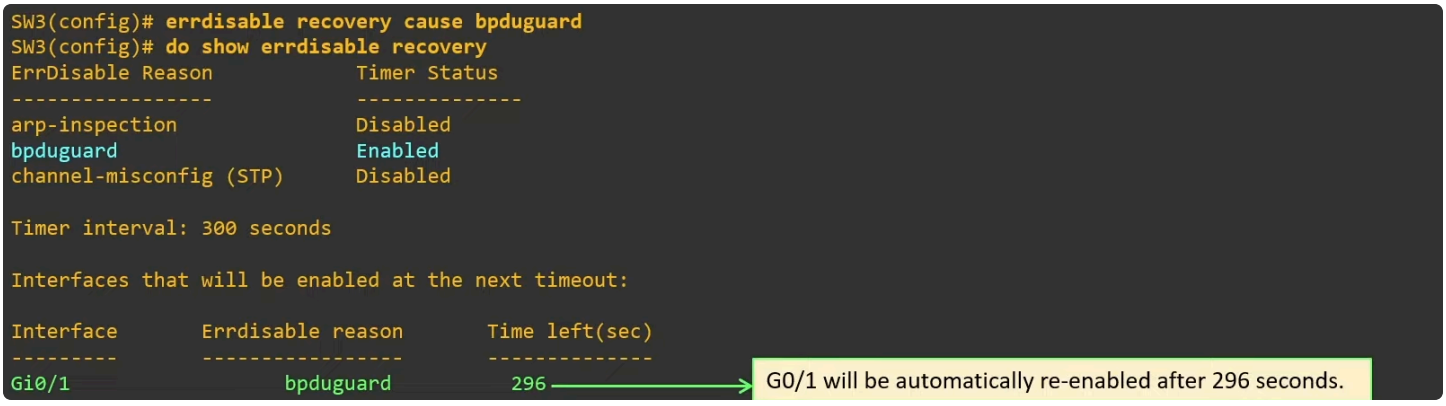
- The `cause` refers to the feature that disabled the port (e.g., `bpduguard`, `arp-inspection`, etc.).
- Even if you modify the interval, you **still must enable** ErrDisable Recovery for it to work.

Step 2 – (Optional) Modify the recovery interval:

```
SW1(config)# errdisable recovery interval <seconds>
```

- This changes the timer from the default 300 seconds to whatever you specify.

Behavior After Enabling



- After enabling, `show errdisable recovery` shows **enabled** for BPDU Guard.
- The interface (e.g., G0/1) will be listed at the bottom with a countdown timer (e.g., 296 seconds).
- When the timer reaches **0**, the interface is **automatically re-enabled**.

Critical Point — Fix the Underlying Problem First

Even if you use ErrDisable Recovery, you **still have to solve the underlying problem**. In our scenario:

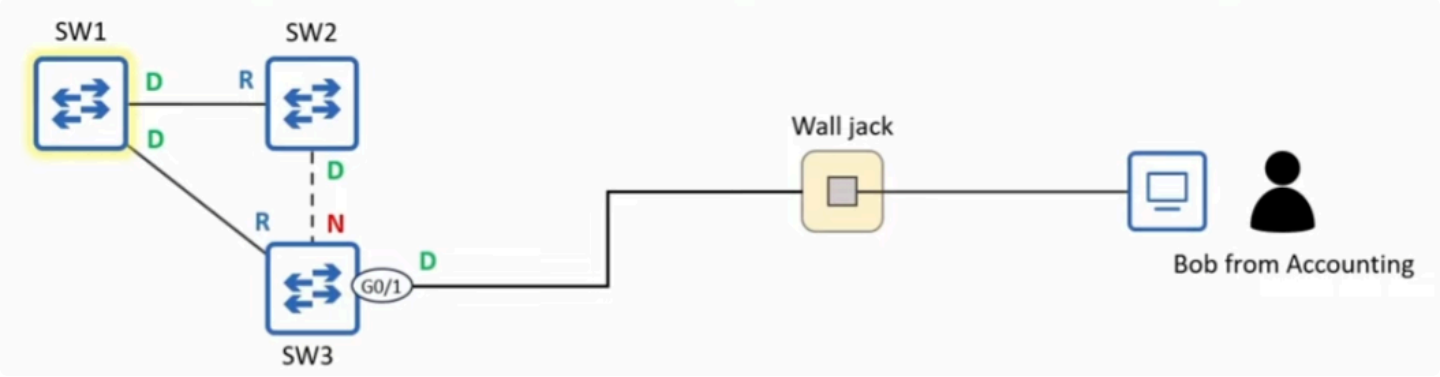
- If Bob's switch is **still connected** to G0/1 when the port recovers...
- The port will receive another BPDU...
- And it will be **disabled again immediately**.

You must disconnect the unauthorized switch before recovery will be effective.

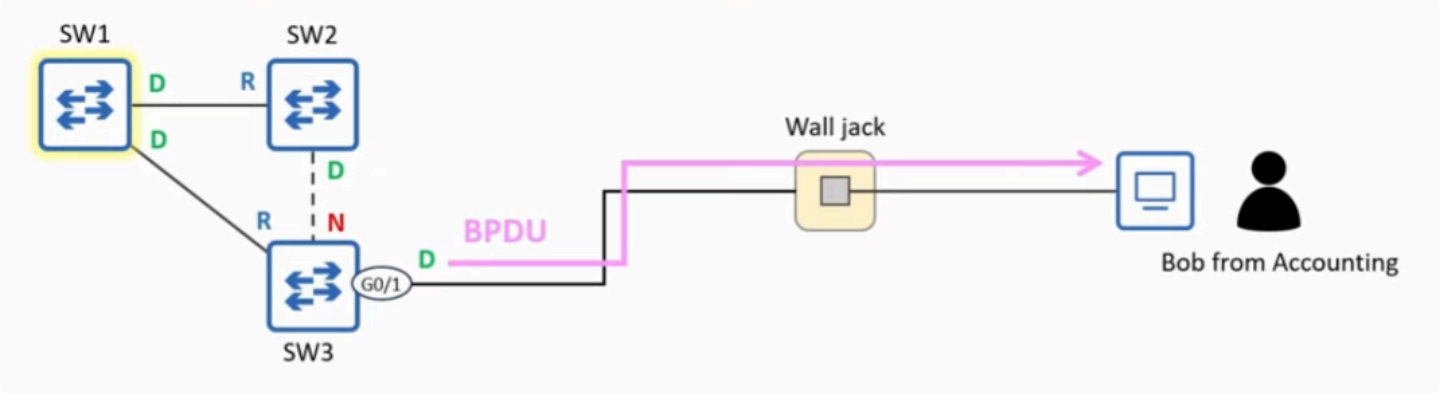
BPDU Filter

BPDU Filter prevents a switch port from sending BPDUs. This addresses the issue that PortFast-enabled ports (even with BPDU Guard) still send BPDUs every 2 seconds to end hosts—unnecessary traffic that also leaks STP topology information.

The Problem BPDU Filter Solves



A switch port connected to an end host **continues sending BPDUs every 2 seconds** — regardless of whether PortFast and BPDU Guard are enabled.



So even though Bob's PC doesn't run spanning tree and simply ignores any BPDUs, SW3 keeps sending BPDUs to Bob's PC, once every 2 seconds.

Why Sending BPDUs to End Hosts is Undesirable

1. **Wastes bandwidth and processing power** — although minimal, it's still unnecessary.
2. **Security concern** — BPDUs contain information about the LAN's STP topology. If maximum security is a concern, you should avoid sending this info to user devices.

How BPDU Filter Works

Unlike BPDU Guard, BPDU Filter does **not** error-disable the port when a BPDU is received. How the port reacts depends entirely on the **configuration method**.

- If you enbale it on SW3's G0/1 interface it will simply stop sending BPDU's.
- Unlike BPDU Guard, it does not disable the port if it receives a BPDU.

BPDU Filter Configuration Methods

1. **Per-port configuration** (interface config mode):

   ```
   SW3(config-if)# spanning-tree bpdufilter enable
   ```

   - The port will **not send** BPDUs.
   - The port will **ignore any BPDUs it receives** (effectively disabling STP on that port).
   - **Risky:** If this port is connected to another switch, a layer-2 loop can form permanently, potentially causing a broadcast storm and bringing down the network. Use with extreme caution.

2. **Global default configuration** (global config mode):

```
SW3(config)# spanning-tree portfast bpdufilter default
```

(Optionally, `spanning-tree portfast edge bpdufilter default`.)

- This activates BPDU Filter on all **PortFast-enabled ports**.
- The port will **not send BPDUs** under normal conditions.
- **If a BPDU is received**, PortFast and BPDU Filter are automatically disabled, and the port operates as a **normal STP port** (including sending BPDUs).
- This provides the best of both worlds: no unnecessary BPDU transmission to end hosts, but the ability to react properly if a switch is connected.

To disable BPDU Filter on a specific port:

```
SW3(config-if)# spanning-tree bpdufilter disable
```

Recommendations

- **Only enable BPDU Filter globally** (default mode) unless there is a very specific, justified reason to use per-port configuration.
- Per-port BPDU Filter disables STP entirely on that port, which is dangerous and generally unnecessary.

Interaction Between BPDU Guard and BPDU Filter

Both features can be enabled on the same port simultaneously, but the outcome depends on the BPDU Filter configuration:

- **If BPDU Filter is enabled globally (default)** and a BPDU is received:
  - BPDU Filter is disabled.
  - BPDU Guard then triggers, error-disabling the port.

- **If BPDU Filter is enabled per-port** and a BPDU is received:
  - BPDU Filter ignores the BPDU.
  - BPDU Guard is **not triggered** because the BPDU is never processed.
  - In this case, BPDU Guard has no effect.

This reinforces the recommendation to use BPDU Filter only via global default; otherwise, BPDU Guard becomes ineffective.

Summary of STP Toolkit Features

Feature	Purpose	Behavior When BPDU Received	Configuration Options
PortFast	Immediate forwarding for end hosts	PortFast is disabled; port reverts to normal STP	Per-port or global default
BPDU Guard	Prevent unauthorized switch connections	Port enters err-disabled state	Per-port (`enabled`) or global default (on PortFast ports); disable on specific port
BPDU Filter	Prevent sending BPDUs to end hosts	**Per-port:** BPDUs ignored – STP disabled. **Global default:** BPDU Filter and PortFast disabled – normal STP resumes	Per-port (`enabled`) or global default (on PortFast ports); disable on specific port

Additional Considerations

- **ErrDisable Recovery** must be enabled separately for each cause (e.g., `bpduguard`, `arp-inspection`, etc.). Manual recovery with `shutdown/no shutdown` is always available.
- Always resolve the underlying issue before recovering an err-disabled port.
- The CCNA also expects knowledge of **Root Guard** and **Loop Guard**, which are covered in a subsequent video.

Final Recommendation

Enable **BPDU Guard** on all end-host ports (either per-port or globally). Enable **BPDU Filter only via global default mode**, which activates it on PortFast-enabled ports. This combination provides security against unauthorized switches and eliminates unnecessary BPDU traffic, while still allowing the network to react appropriately if a switch is inadvertently connected. Avoid per-port BPDU Filter unless you fully understand the risk of disabling STP on a port.