Loop Guard - STP Toolkit

Introduction to Loop Guard

Loop Guard is a feature in the STP toolkit, joining:

- **PortFast**
- **BPDU Guard**
- **BPDU Filter**
- **Root Guard**

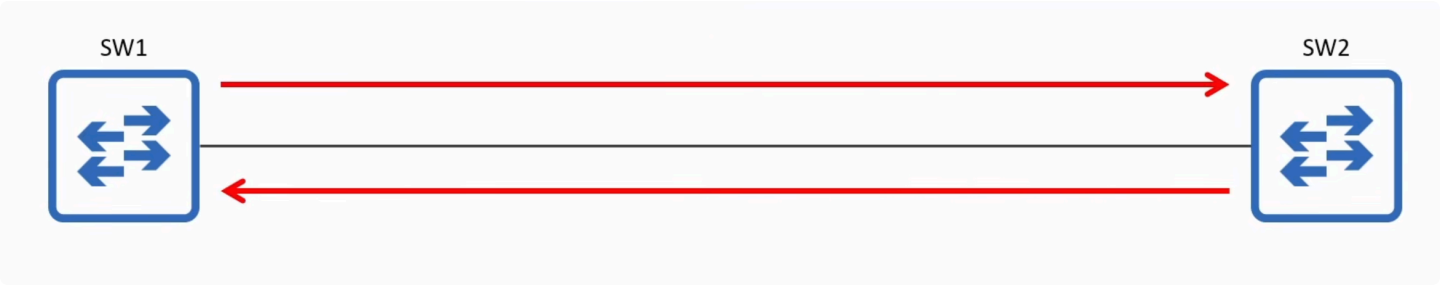
While the core purpose of Spanning Tree Protocol is to prevent Layer 2 loops, Loop Guard adds an extra line of defense.

Loop Guard: It protects the network by **disabling a port** if that port unexpectedly stops receiving BPDUs, preventing it from mistakenly transitioning to the **Forwarding** state.

This situation can arise from a software bug on a neighboring switch that halts BPDU transmission. However, the most common and instructive scenario involves a **unidirectional link**, which will be explored in depth.

Unidirectional Links Explained

Normal Link (Bidirectional)

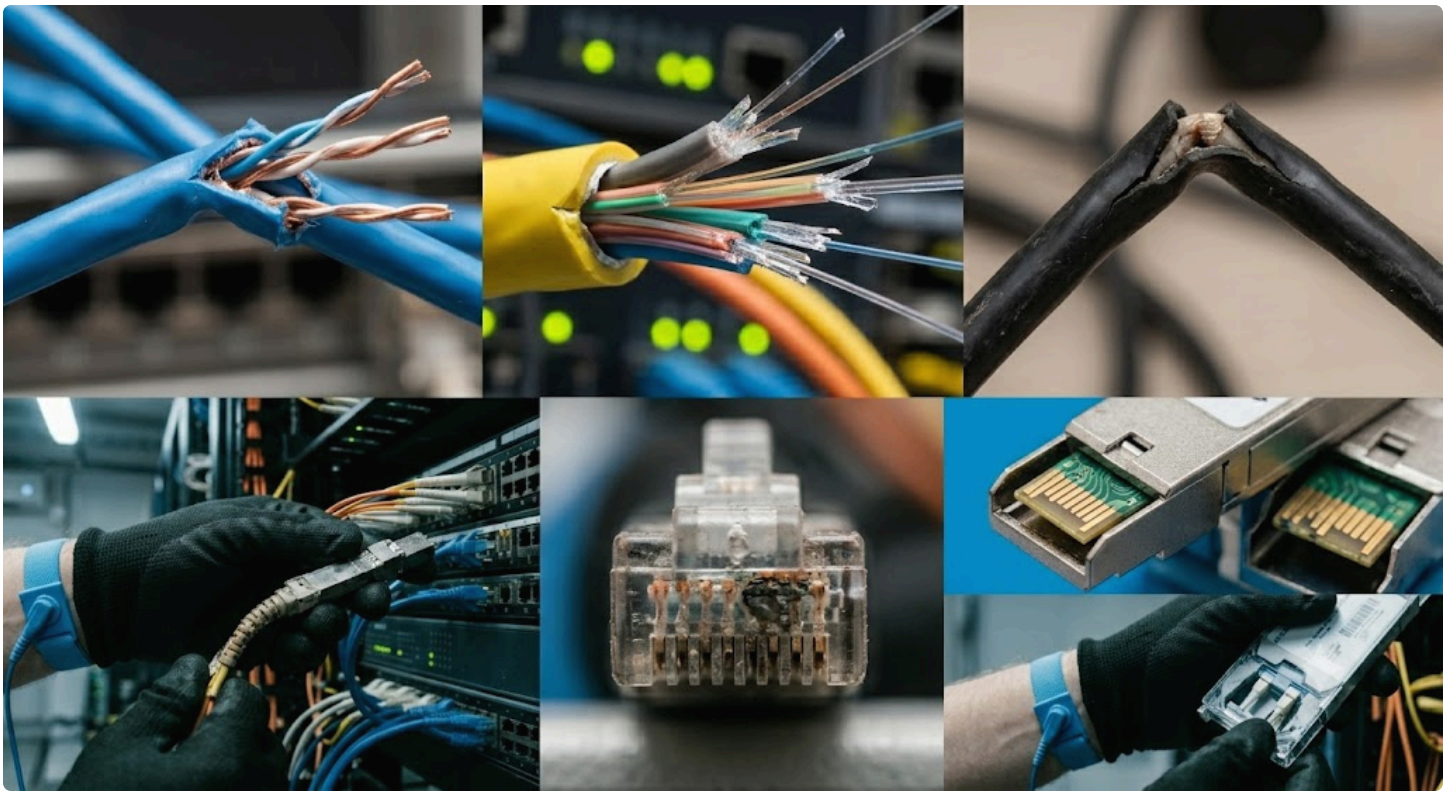


- SW1 can transmit data to SW2
- SW2 can transmit data to SW1

Unidirectional Link

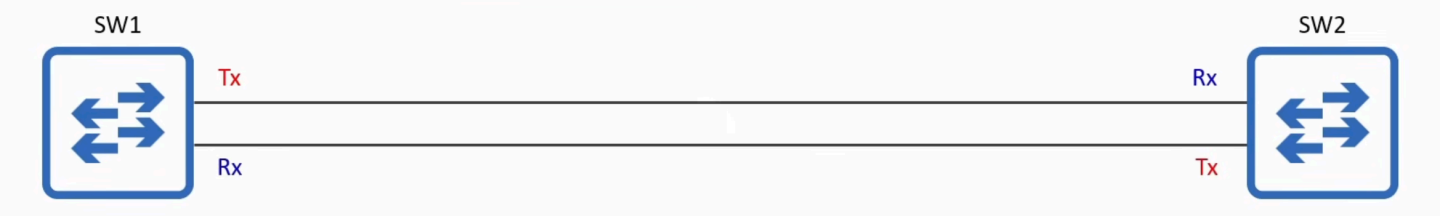
- Data flows in **only one direction**
- Example: SW1 sends frames to SW2, but SW2 **cannot** send frames to SW1

Common Cause



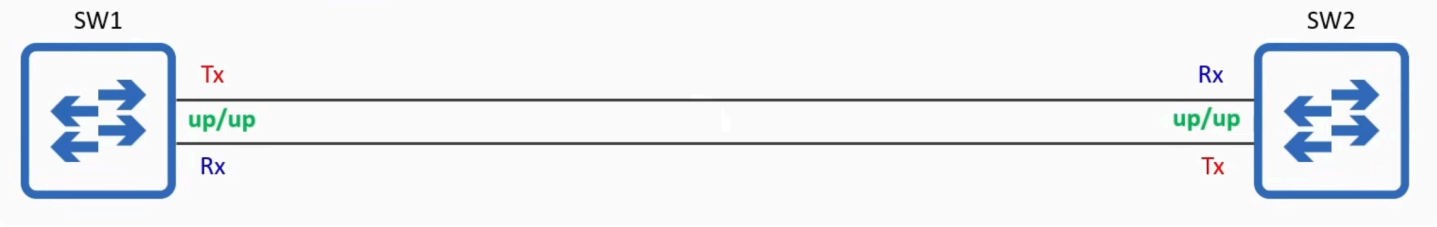
- **Layer 1 physical issue** — damaged cables, faulty connectors/SFP transceivers
- More common with **fiber-optic cables** than copper UTP

Why Fiber is More Vulnerable



- Fiber connections use **two separate fibers** (Tx → Rx, Tx → Rx)
- If **one fiber** is damaged:
  - Data flow in one direction is disrupted
  - The other direction may remain functional
- Fiber cables are fragile — bending too far can snap them

The Risk



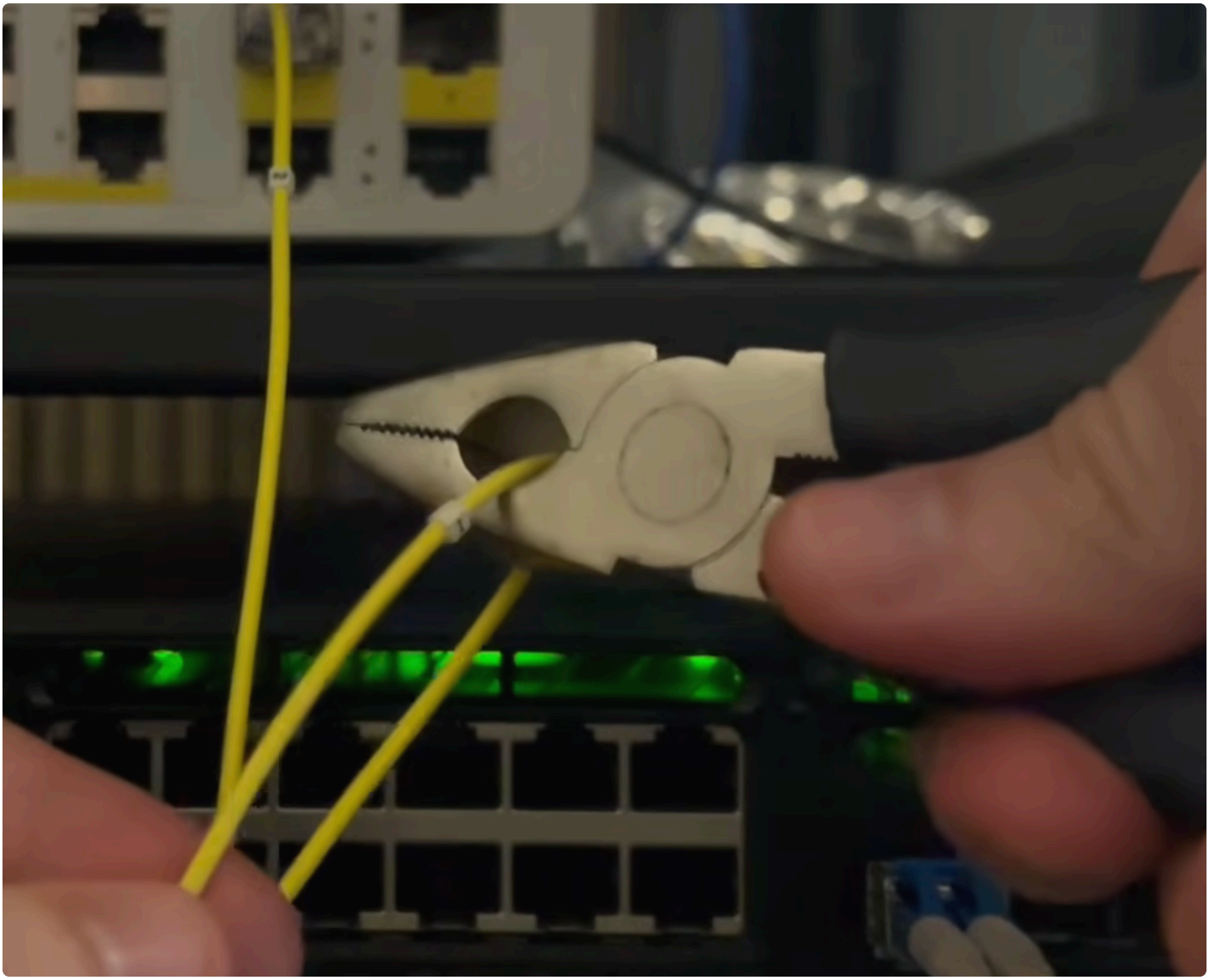
- For a fiber interface to be **up/up**, both fibers must be connected and functional
- If the devices **don't detect** a physical problem, the interface stays **up/up**
- Result: **Unidirectional link** — data only flows one way

Detecting Fiber-Optic Link Failures

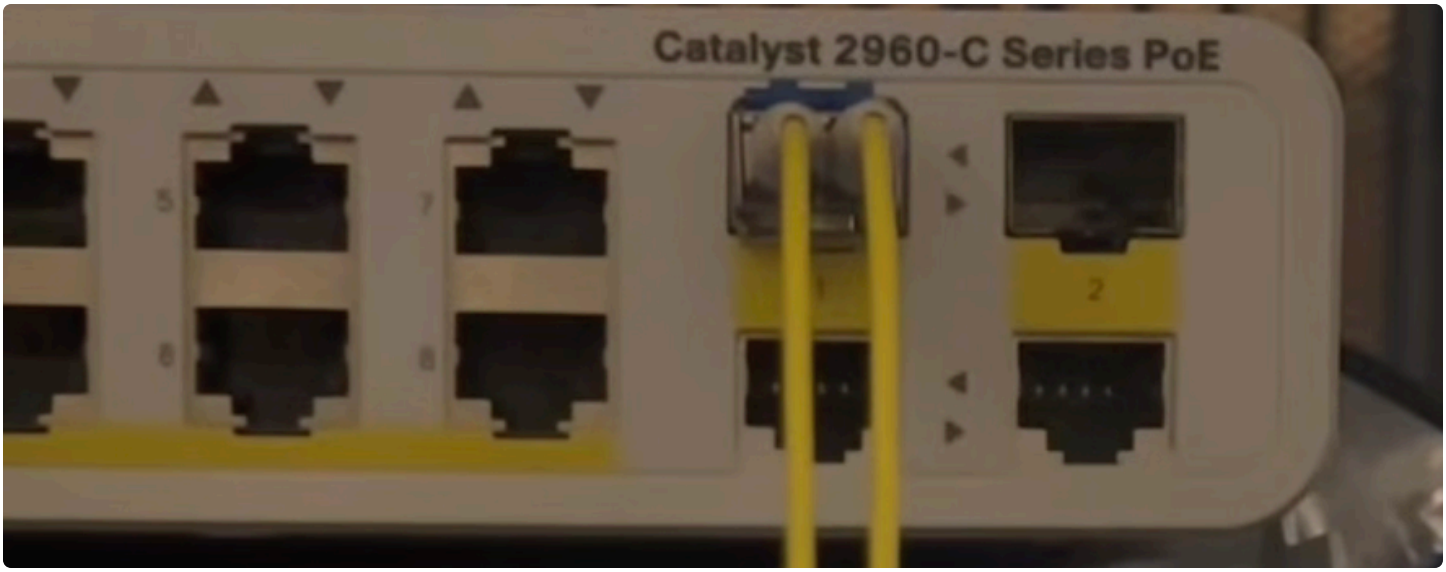
Normal Operation

- Both fibers connected on both sides
- Link lights are **green**
- Connection is functional

When a Fiber is Damaged or Disconnected

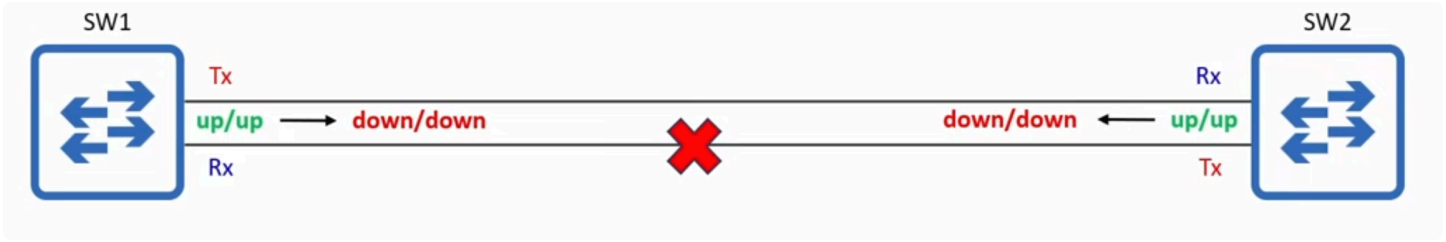


- The devices **detect** the problem
- Both switches **disable their interfaces**



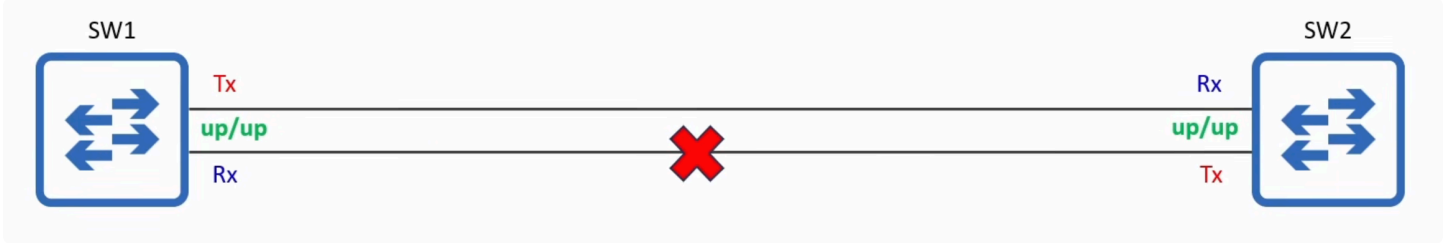
- **Result:** Link is disabled entirely so the link lights remain off.

Unidirectional Links — When Detection Fails



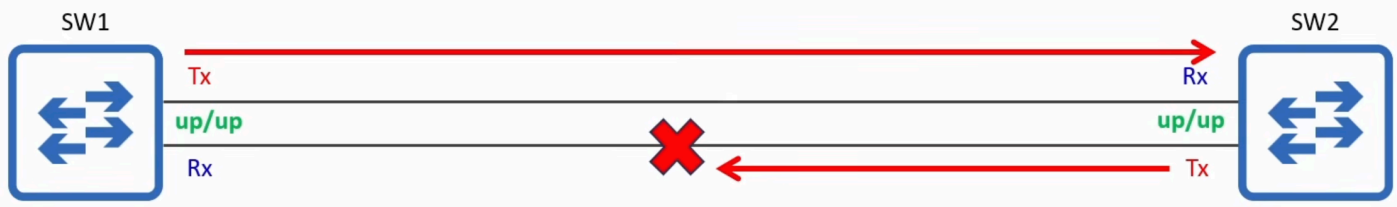
- A **detected** fiber failure = **No unidirectional link**
  - Link goes completely down → **No loop risk**
- **But** — not all physical problems are detected by the devices

The Dangerous Scenario



- A problem on one fiber prevents data transmission
- The devices **fail to detect** the issue
- Interfaces remain **up/up**

Result: Unidirectional link

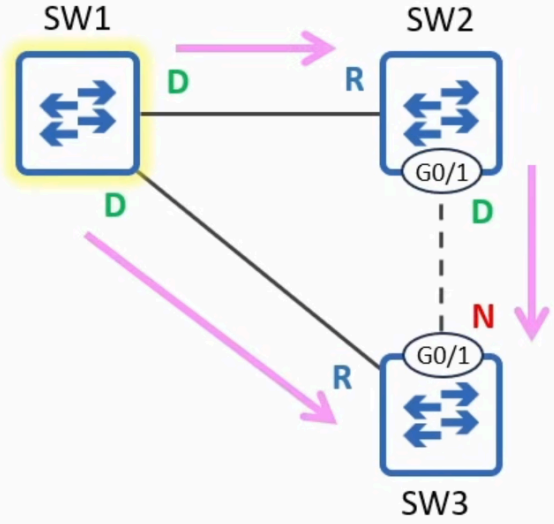


- SW1 can transmit data to SW2
- SW2's transmitted data **cannot** reach SW1
- Both switches think the connection is fully operational
- Actually, communication only works **one way**

> ***Important: The dangerous scenario is when devices fail to detect the physical problem, allowing the interface to remain up/up despite only one direction working.***

The STP Problem with Unidirectional Links

Normal Operation



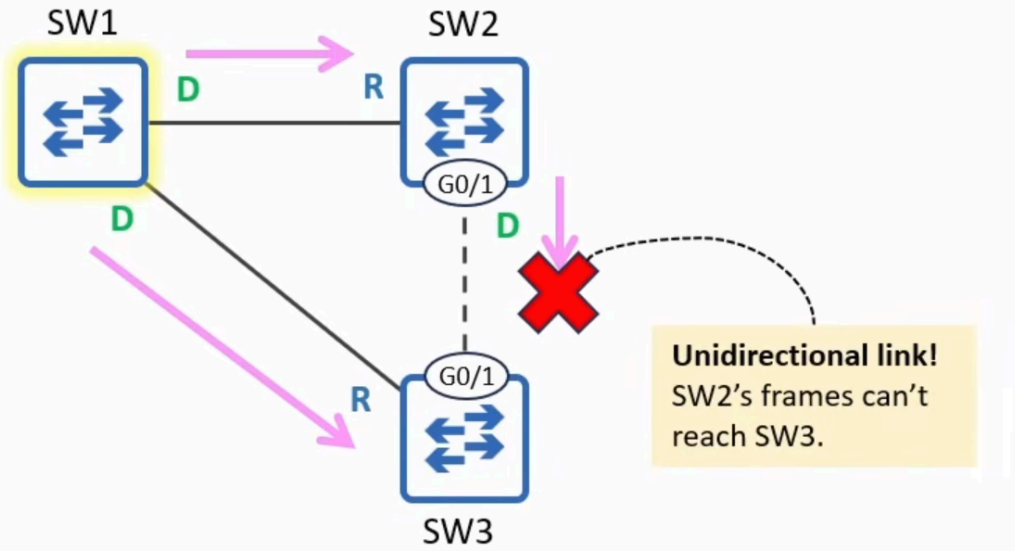
- BPDUs originate from the Root Bridge every 2 seconds
- BPDUs are forwarded out of **Designated ports**

- Switches use BPDUs to determine STP topology (Forwarding vs. Blocking ports)
    - These BPDU's are how switches share information with eachother to determine the stp topology.

Example Network

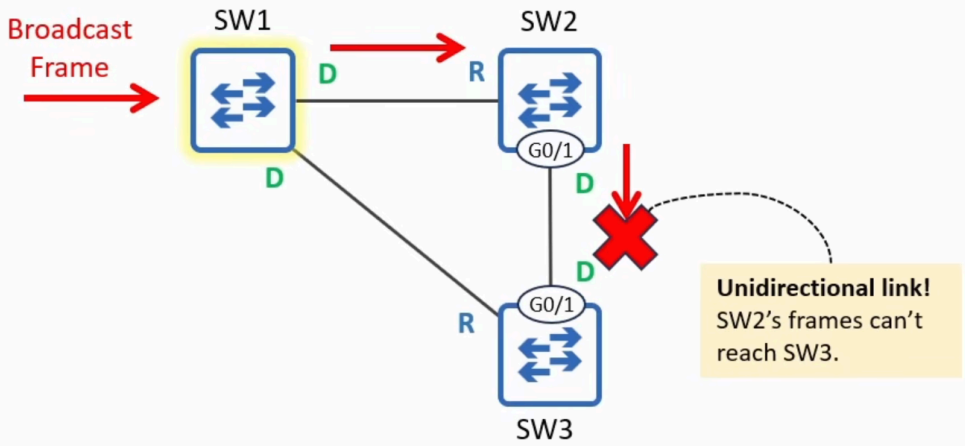
- SW3 G0/1 is a **non-designated blocking port** (receives superior BPDUs from SW2)
    - SW2 has a superior root cost or bridge ID.

If the SW2-SW3 link becomes unidirectional and SW2's BPDU's can't reach, What Happens with a Unidirectional Link?

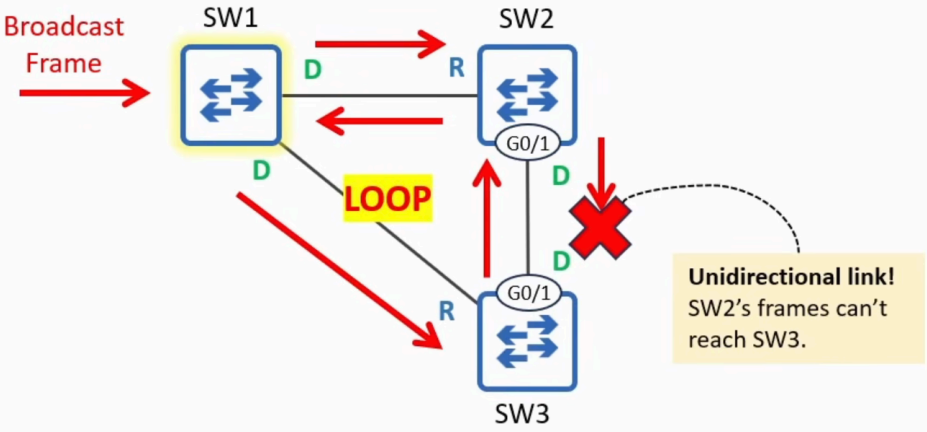


1. SW2 ↔ SW3 link becomes unidirectional (SW2's frames can't reach SW3)
2. SW3 **stops receiving BPDUs** from SW2
3. SW3 assumes **no loop exists**
4. After **Max Age timer** expires:
    - SW3 G0/1 becomes a **Designated port**
    - Starts forwarding BPDU's to SW2.
    - Because SW3's BPDU's are inferior to SW2. SW2 starts ignoring SW3's BPDU's.
5. SW2 and SW3 both in the forwarding state → **Layer 2 loop** is created
    - Meaning with what a loop from SW1 --> SW2 --> SW3

Loop Path - How the loop works

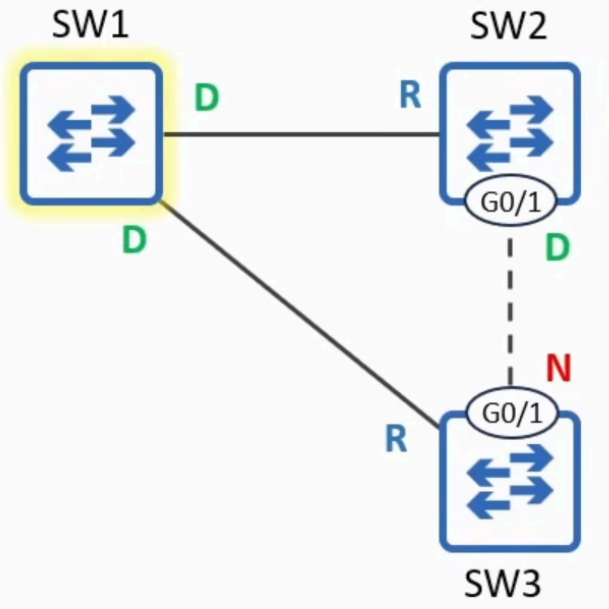


- If SW1 Receives a Broadcast frame one one of its interfaces it will flood the frame towards to SW2 and SW3.
- Frame flooded to SW2 **can't** reach SW3 because of the unidirectional link.



- Frame to SW3 **loops** around SW1 → SW3 → SW2 → SW1
    - Each switch that receives the frame will flooded repeatidly.
        - This is the key problem with a Unidirectional link in a LAN using STP.
        - SW3 G0/a stops receiving BPDU's.
            - Thinks it should become a designated port.
            - Starts Fowarding frames.
            - Then causes a loop.
            - It would be better if the hardware issue cause the link to go down entirely.
                - In that case SW2 and SW3 would both disable their G0/1 Ports.
                - Ans there would be no loop.
- So what is the solution to dealing with a situation where a hardware issue causes a unidirectional link?
    - The answer is Loop guard.

How Loop Guard Solves the Problem



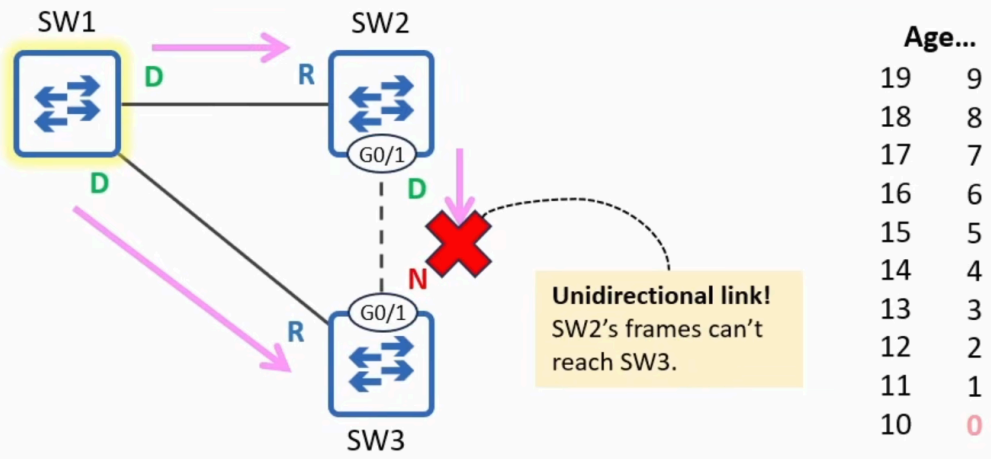
- Loop Guard **doesn't prevent** physical unidirectional links

- It **detects** them and **prevents Layer 2 loops**

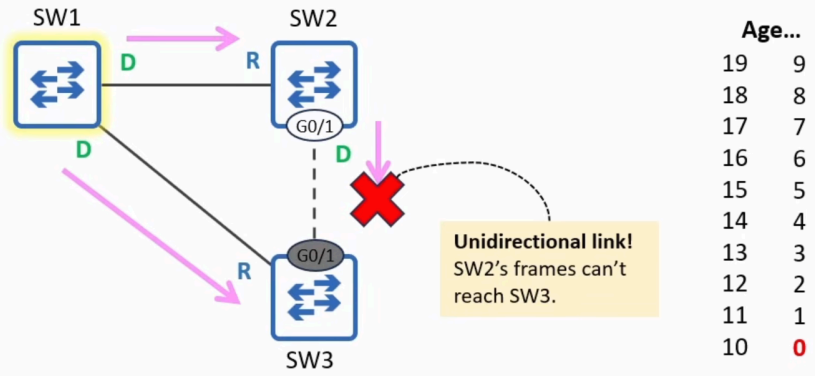
Loop Guard Behavior

- When a Loop Guard-enabled port's **Max Age timer reaches 0**:
  - Does **NOT** become a Designated port
  - Enters the **Broken (Loop Inconsistent)** state
  - The port is **blocked**
- Similar to Root Guard's **Broken (Root Inconsistent)** state
- In both cases: the port remains **up/up** — STP blocks it, but the interface is not shut down

Example



- Loop Guard enabled on SW3 G0/1
- SW2 ↔ SW3 link becomes unidirectional (SW2's frames can't reach SW3)
- Max Age timer on SW3 G0/1 counts down



- **With Loop Guard:** Port enters broken state → **no loop**
- **Without Loop Guard:** Port becomes Designated → **loop**

Recovery

- **Automatic** — when the physical issue is resolved and the port starts receiving BPDUs again, it is automatically re-enabled

Configuration

Method 1: Per-Port

```
SW3(config)# interface gigabitEthernet 0/1
SW3(config-if)# spanning-tree guard loop
n
```

Method 2: Global Default

```
SW3(config)# spanning-tree loopguard default
```

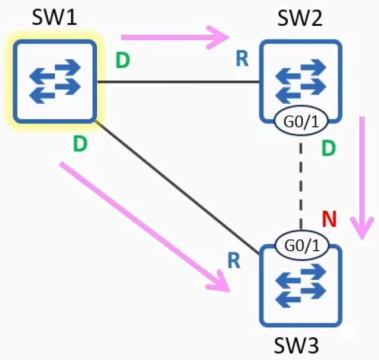
- Enables Loop Guard on **all ports** by default
- Disable on specific ports if needed:

```
SW3(config)# interface gigabitEthernet 0/1
SW3(config-if)# spanning-tree guard none
```

Where to Apply Loop Guard

- Enable on ports that are **not Designated**:
  - **Root ports**
  - **Non-designated ports**
- These are ports **supposed to receive BPDUs** from Designated ports
- If they stop receiving BPDUs, Loop Guard will block them to prevent loops

CLI Scenerio 1 - Normal Operation



Per-Port Configuration:

```
SW3(config)# interface gigabitEthernet 0/1
SW3(config-if)# spanning-tree guard loop
```

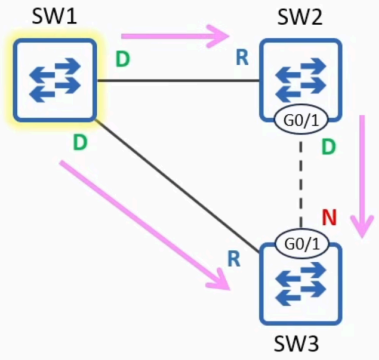
Check status:

```
SW3(config-if)# show spanning-tree interface detail
```

```
SW3(config)# interface g0/1
SW3(config-if)# spanning-tree guard loop
SW3(config-if)# do show spanning-tree interface g0/1 detail
 Port 2 (GigabitEthernet0/1) of VLAN0001 is alternate blocking
   Port path cost 4, Port priority 128, Port Identifier 128.2.
   Designated root has priority 1, address 5254.001a.9d29
   Designated bridge has priority 28673, address 5254.0019.f184
   Designated port id is 128.2, designated path cost 4
   Timers: message age 3, forward delay 0, hold 0
   Number of transitions to forwarding state: 0
   Link type is point-to-point by default
   Loop guard is enabled on the port
   BPDU: sent 0, received 359
```

- Output shows: `Loop guard is enabled on the port`

Global Default Configuration:




```
SW3(config)# spanning-tree loopguard default
```

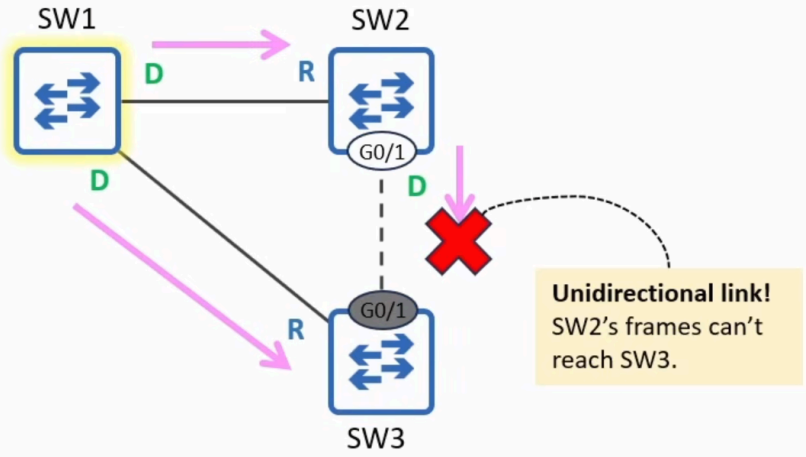
Check status:

```
SW3(config)# show spanning-tree interface detail
```

```
SW3(config)# spanning-tree loopguard default
SW3(config)# do show spanning-tree interface g0/1 detail
 Port 2 (GigabitEthernet0/1) of VLAN0001 is alternate blocking
   Port path cost 4, Port priority 128, Port Identifier 128.2.
   Designated root has priority 1, address 5254.001a.9d29
   Designated bridge has priority 28673, address 5254.0019.f184
   Designated port id is 128.2, designated path cost 4
   Timers: message age 3, forward delay 0, hold 0
   Number of transitions to forwarding state: 0
   Link type is point-to-point by default
   Loop guard is enabled on the port by default
   BPDU: sent 0, received 359
```

- Output shows: `Loop guard is enabled on the port by default`

CLI Scenerio 2 - Loop Guard Blocks a Port



CLI message:

```
%SPANTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port GigabitEthernet0/1 on VLAN0001.
```

```
Loop guard blocking port GigabitEthernet0/1
```

Show spanning-tree output:

```
%SPANTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port GigabitEthernet0/1 on VLAN0001.

SW3(config-if)# do show spanning-tree

!output omitted

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Root FWD 4         128.1    P2p
Gi0/1               Desg BKN*4         128.2    P2p *LOOP_Inc
```

BKN = Broken
LOOP_Inc = Loop Inconsistent

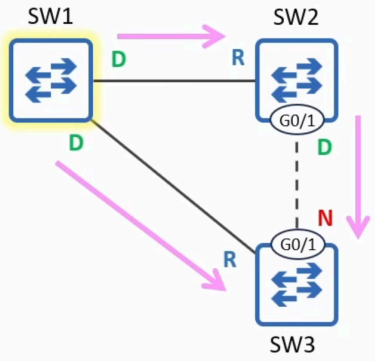
```
SW3# show spanning-tree
```

- Status: **BKN** (Broken)
- Additional info: **LOOP_Inc** (Loop Inconsistent)

Why it blocked:

- Port stopped receiving BPDUs
- Example: Sharp bend in fiber degrades signal → SW2's BPDUs can't reach SW3

CLI Scenario 3. - Automatic Recovery from blocked port



- If the physical issue is resolved (e.g., cable adjusted, data flows again):
  - Port starts receiving BPDUs from SW2 again

```
%SPANTREE-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port GigabitEthernet0/1 on VLAN0001.
```

  - Loop Guard **automatically unblocks** the port
- In `show spanning-tree`:

```
%SPANTREE-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port GigabitEthernet0/1 on VLAN0001.

SW3(config-if)# do show spanning-tree

!output omitted

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Root FWD 4         128.1    P2p
Gi0/1               Altn BLK 4         128.2    P2p
```

```
SW3(config)# spanning-tree loopguard default
```

  - G0/1 status changes from **BKN** (Broken) → **BLK** (Blocking)
  - "Loop Inconsistent" label disappears
- **No manual commands needed** — like Root Guard, Loop Guard automatically re-enables the port when the problem is fixed

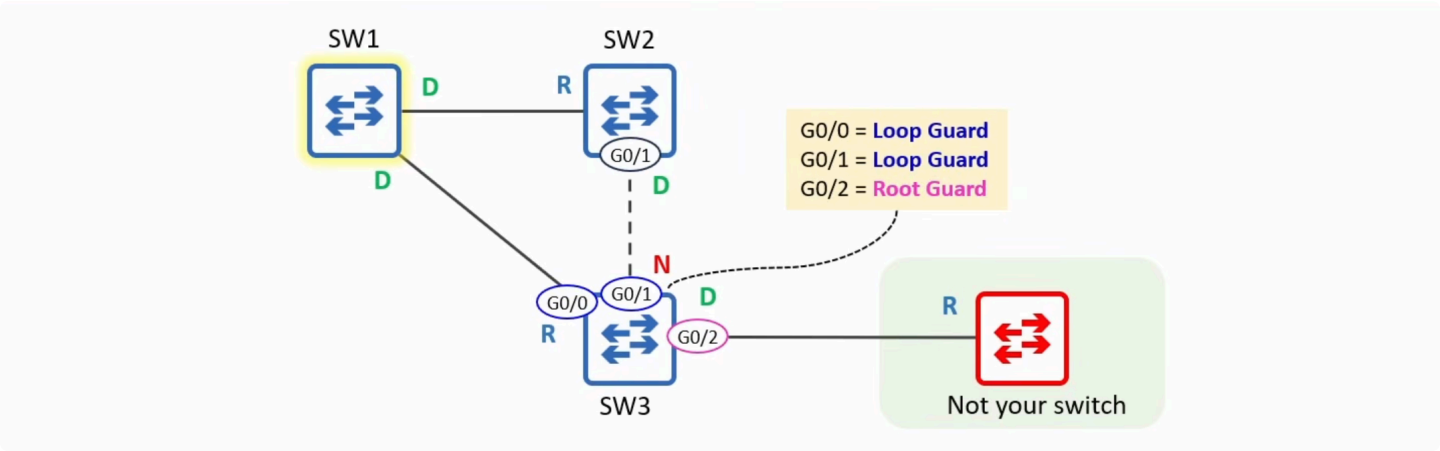
Loop Guard vs. Root Guard

Mutually Exclusive

- Loop Guard and Root Guard **cannot** be enabled on the same port at the same time
- They serve **opposite purposes**:

Feature	Purpose	Trigger
Root Guard	Prevents Designated ports from becoming Root ports	Designated port receives **superior BPDUs** → blocked
Loop Guard	Prevents Root/Non-Designated ports from becoming Designated ports	Port **stops receiving BPDUs** → blocked

Where to Apply Each (SW3 Example)



- **G0/0 and G0/1** → Loop Guard (supposed to receive BPDUs from SW1 and SW2)
- **G0/2** → Root Guard (designated port facing an untrusted switch)

> ***Configuring Root Guard on G0/0/G0/1 would block them immediately, cutting off LAN communication.***

Command Interaction

If Loop Guard is on a port, then you configure Root Guard:

```
SW3(config)# interface gigabitEthernet 0/1
SW3(config-if)# spanning-tree guard loop
SW3(config-if)# spanning-tree guard root
```

- Root Guard **replaces** Loop Guard on the port

If Root Guard is on a port, then you configure Loop Guard:

```
SW3(config)# interface gigabitEthernet 0/1
SW3(config-if)# spanning-tree guard root
SW3(config-if)# spanning-tree guard loop
```

- Loop Guard **replaces** Root Guard on the port

If Loop Guard is enabled globally, then Root Guard is configured on a port:

```
SW3(config)# spanning-tree loopguard default
SW3(config)# interface gigabitEthernet 0/1 #Applies to only 1 interface
SW3(config-if)# spanning-tree guard root
```

- Loop Guard is **disabled on that port** — Root Guard takes effect

IOS Command Rule

- The **more specific** command takes effect over the less specific
- Interface commands override global commands
- This applies to other STP features too (PortFast, BPDU Guard, BPDU Filter)

Loop Guard Summary

Purpose

- Protects the network by **blocking a port** if it unexpectedly stops receiving BPDUs
- This could be caused by:
  - **Software bug** on a neighboring switch
  - **Hardware issue** causing a unidirectional link

Unidirectional Links

- A link where data flows in **only one direction** (should be bidirectional)
- Typically caused by **Layer 1 issues on fiber-optic cables**
- Devices **fail to detect** the issue → interfaces stay up/up
- BPDUs stop reaching the neighboring switch
- Root/Non-Designated port stops receiving BPDUs → becomes **Designated** → **Layer 2 loop**

Loop Guard Behavior

- Port stops receiving BPDUs → enters **Broken (Loop Inconsistent)** state
- Port is effectively **disabled** (but remains up/up)
- Starts receiving BPDUs again → **automatically re-enabled**

Configuration

Method	Command	Scope
Per-Port	`spanning-tree guard loop` (interface mode)	Single port
Global Default	`spanning-tree loopguard default` (global mode)	All ports
Disable Per-Port	`spanning-tree guard none` (interface mode)	Remove from specific port

Key Reminders

- Enable on **Root** and **Non-Designated** ports (ports that should receive BPDUs)
- Loop Guard and Root Guard are **mutually exclusive** — only one active per port
- Configuring one **displaces** the other on the same port
- **More specific command** (interface) overrides less specific (global)