Ecole Supérieure d'Informatique et du Numérique
COLLEGE OF ENGINEERING & ARCHITECTURE

Routing and Switching

Fall 2025

By: Prof. Dr. FADI Oumaima

Evaluation

Lab Report+ Quiz:**10%**

CC: **20%**

CF: **50%**

HCIA-certification: **20%**

Chapter 4 : STP: Spanning Tree Protocol

Topics:

- Importance of switching
- Operating principle
- Switching through self-learning
- STP: What is it? And why we need it?

Shared Ethernet: Reminder

Ethernet networks (IEEE 802.3) use **frame broadcasting** and the **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)** access method.

Drawbacks:

Problems caused by **collisions** on the network

Delays resulting from **network congestion**

These issues **increase** as the **demand for bandwidth grows** (for example, Ethernet used for Internet access, multimedia applications, etc.)

Ethernet Extensions

Solutions to improve performance:

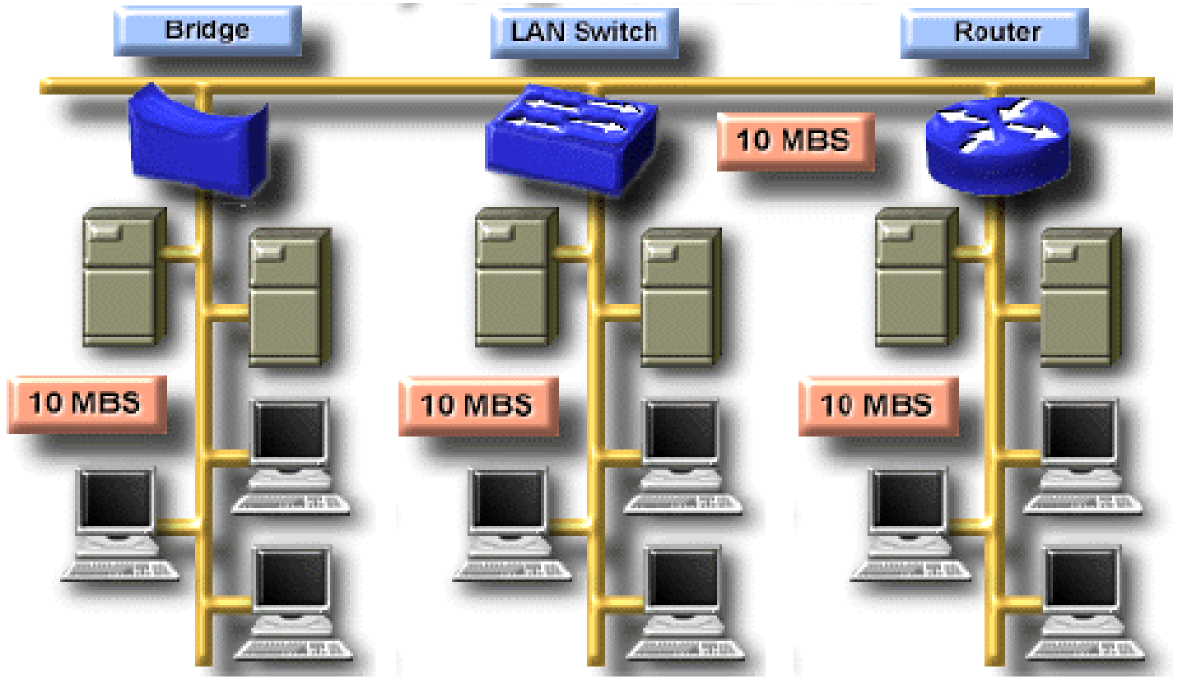
- Increase the available data rates:

Fast Ethernet, Gigabit Ethernet, etc.

- Segment the network into smaller **collision** and **broadcast domains** using:

Bridges or switches (Layer 2 devices)

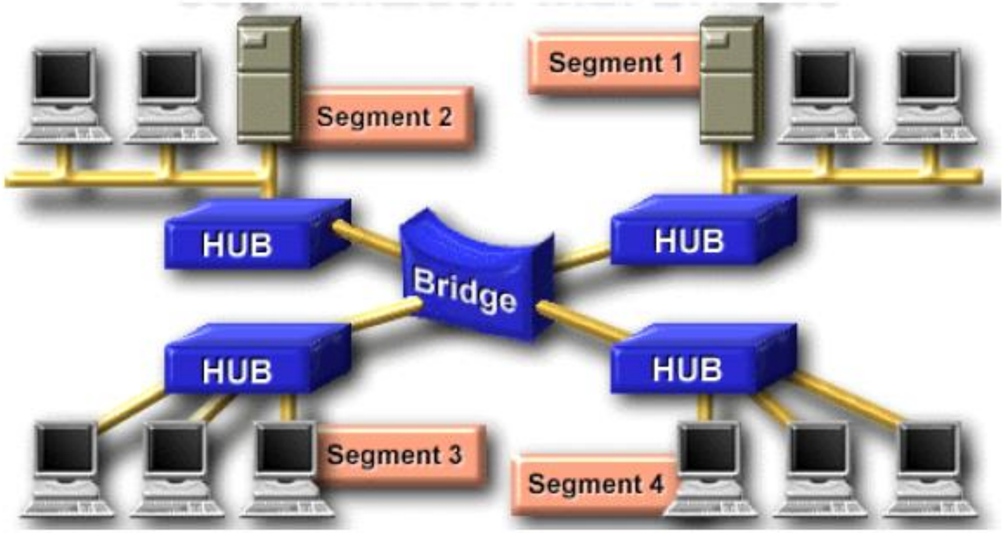
Routers (Layer 3 devices)

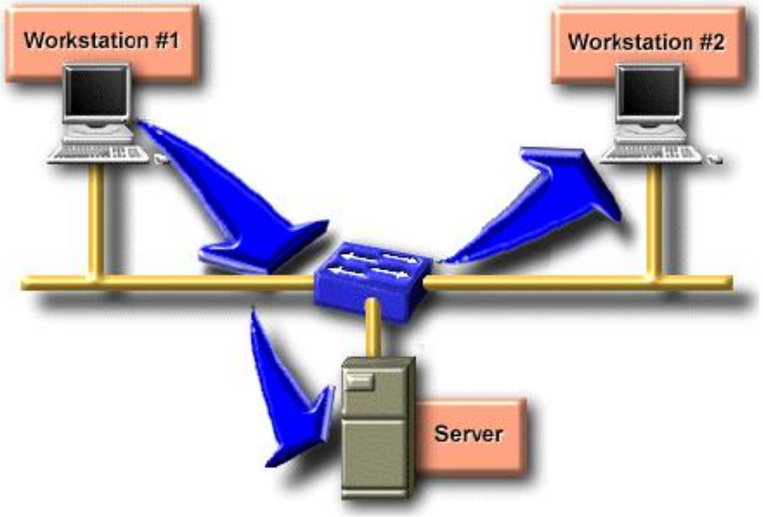


Switched Ethernet

The **switch analyzes the destination physical (MAC) address** of a frame and **forwards it only** to the segment that contains the destination device.

This allows grouping stations with **high mutual traffic** within the same segment, thereby **reducing collision domains** and improving network efficiency.





Advantages of Switching:

Dedicated Connection:

Each communication between sender and receiver uses its own dedicated path, ensuring full bandwidth and faster data transfer.

Elimination of Collisions:

Since devices no longer share a single medium, data collisions are eliminated, resulting in smoother and more reliable network performance.

Improved Network Efficiency:

Switches create multiple independent communication channels, allowing several conversations to occur simultaneously without interference.

Better Scalability:

As the number of connected devices grows, switching maintains performance by isolating traffic and minimizing congestion.

Enhanced Security:

Frames are forwarded only to their intended destinations, reducing unnecessary exposure of data to other devices on the network.

Address Management through Self-Learning

A **switching (or forwarding) table**, based on **MAC addresses**, allows the switch to determine the **output port** for each frame.

This table is **built and updated dynamically** by analyzing incoming frames — the switch **learns the MAC addresses** of devices connected to each port.

When a switch receives a frame on port **X**, it examines the **destination address (D):**

- If the destination device is **on the same port X**, the frame is **not forwarded**.
- If **D** corresponds to another port **Y** (found in the table), the frame is **forwarded to Y**.
- If **D** is **unknown**, the frame is **broadcast to all ports except X**.

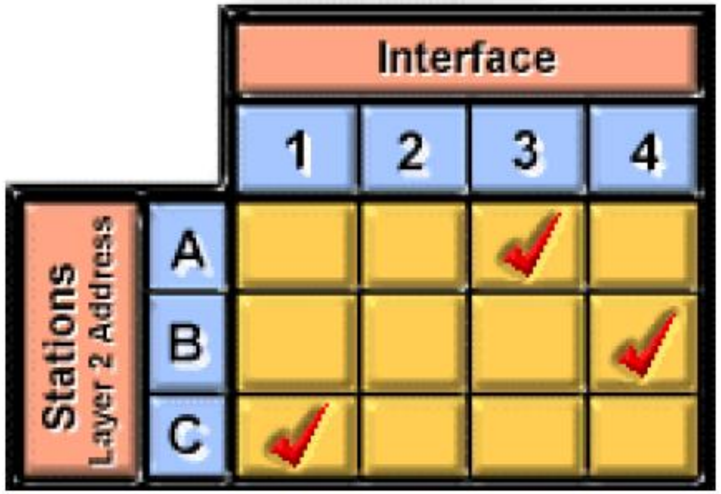
Note: Since a switch's memory is not infinite, entries in the table are **automatically removed after a certain time** (aging process).

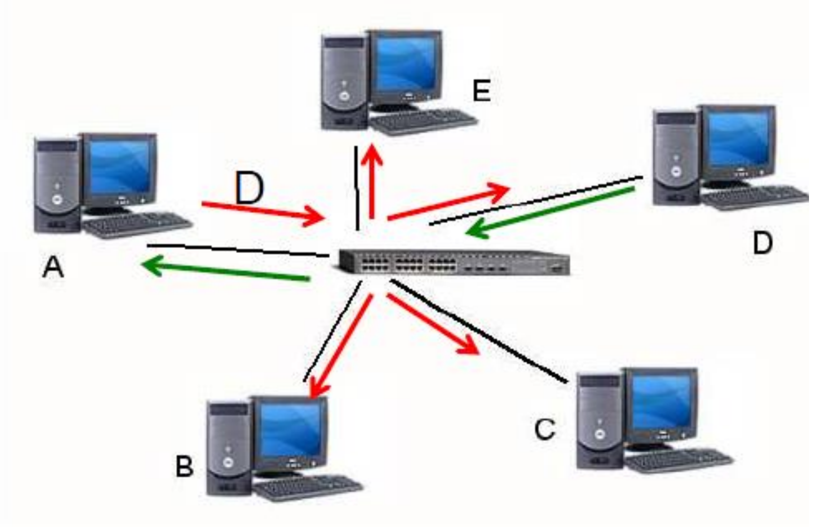
Example of Self-Learning

The switch receives a frame on **port 3** destined for the **MAC address of device D**.

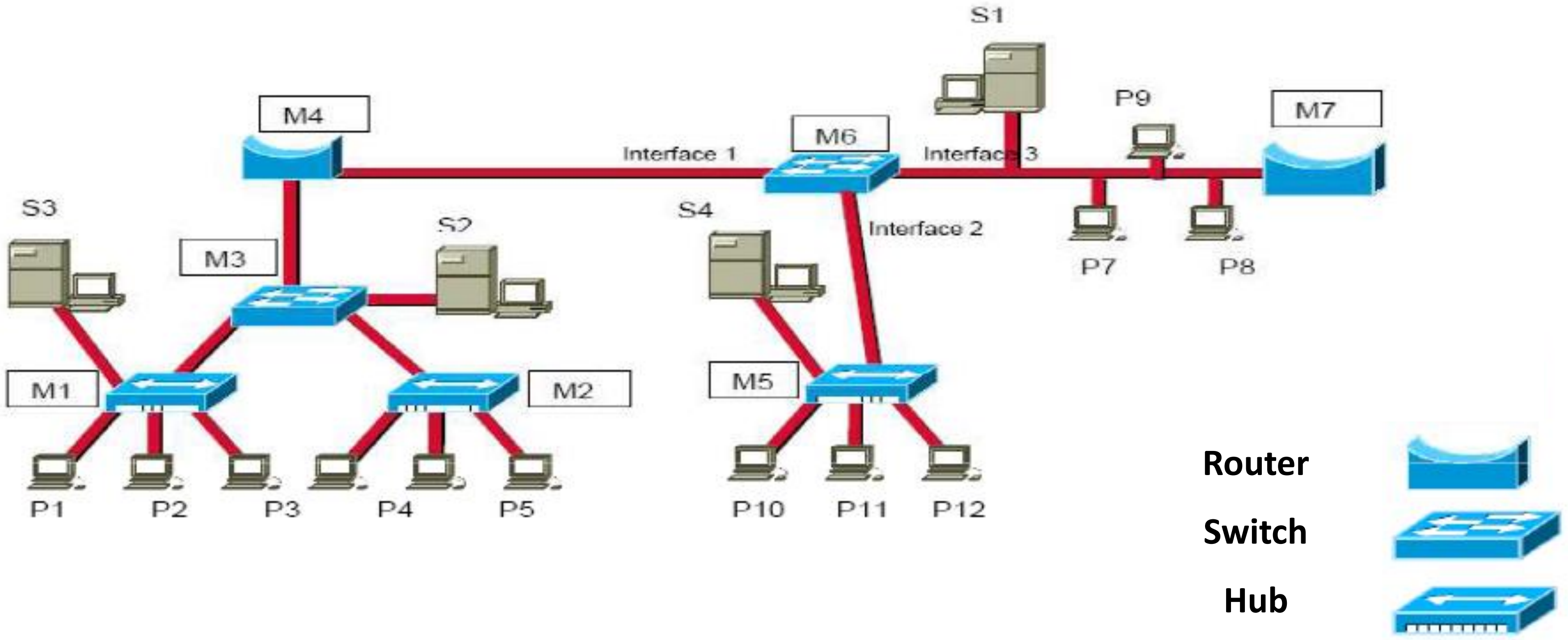
The switch **does not find** D’s MAC address in its **switching table**, so it **forwards the frame to all ports except port 3** (flooding).

When the switch **receives a reply from D**, it then **associates D’s MAC address with the port number** where the reply arrived.





Self Learning: Exercice



Consider a local network whose architecture is given in the figure above:

A. P1 sends a frame with destination MAC address FF:FF:FF:FF:FF:FF. Who receives this frame?

B. Provide the switching table of M6, assuming all stations on the network have communicated at least once.

C. If we replace router M4 with a switch, how does this change communications between different points of the network?

Switching Techniques

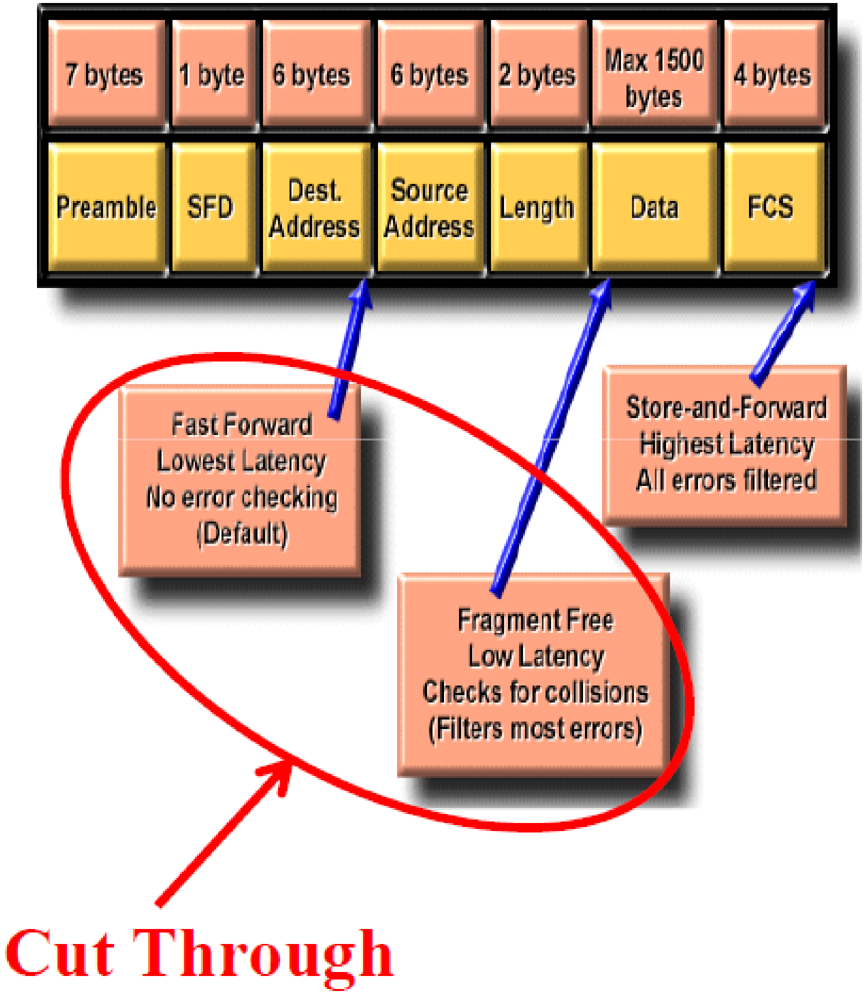
- Cut-through switching

Accepts the frame and **starts reading the destination address** to forward it directly to the output port.

No error checking (may forward erroneous frames).

- Store-and-forward switching

Accepts the incoming frame, **stores it temporarily**, **checks it for errors**, then forwards it to the output port.



Switched Ethernet: Performance

The network is based on **switches**.

Advantages:

- **Faster:** no collisions if the network is fully switched.
- **Uniform interfaces:** e.g., twisted pair cabling.
- **Scalable and configurable:** supports VLANs.

Drawback:

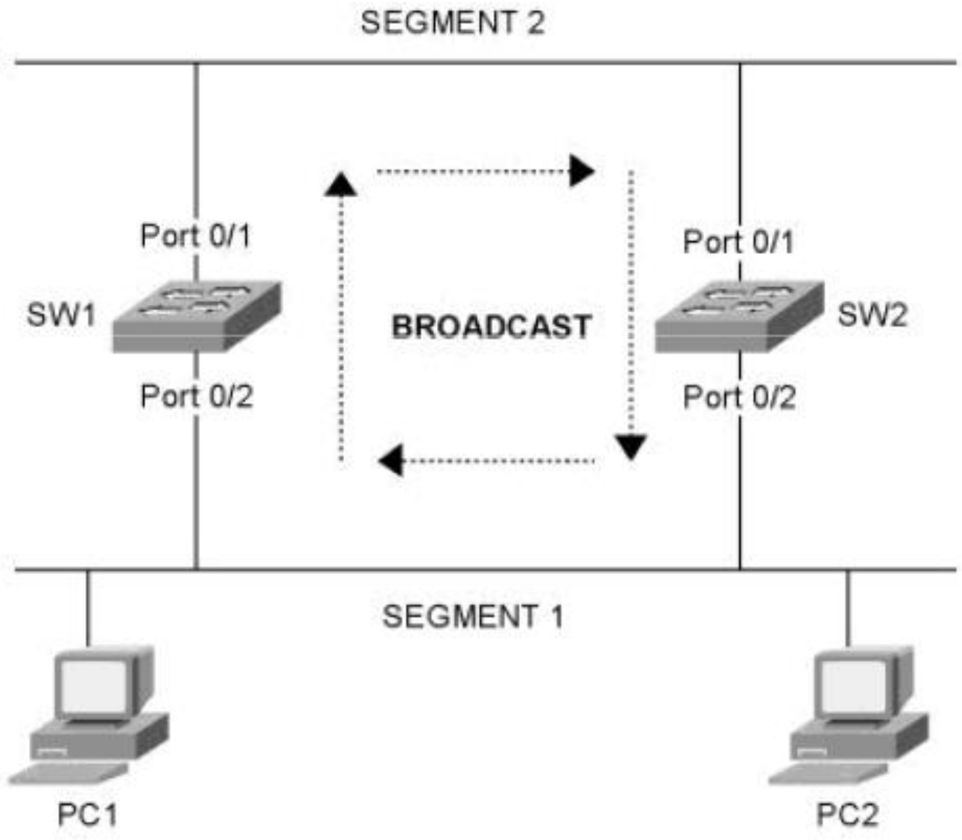
- **Loops can occur** in a redundant network topology.

Switched Ethernet and Loop Problem

When interconnecting switches, **redundant paths** are needed to increase reliability.

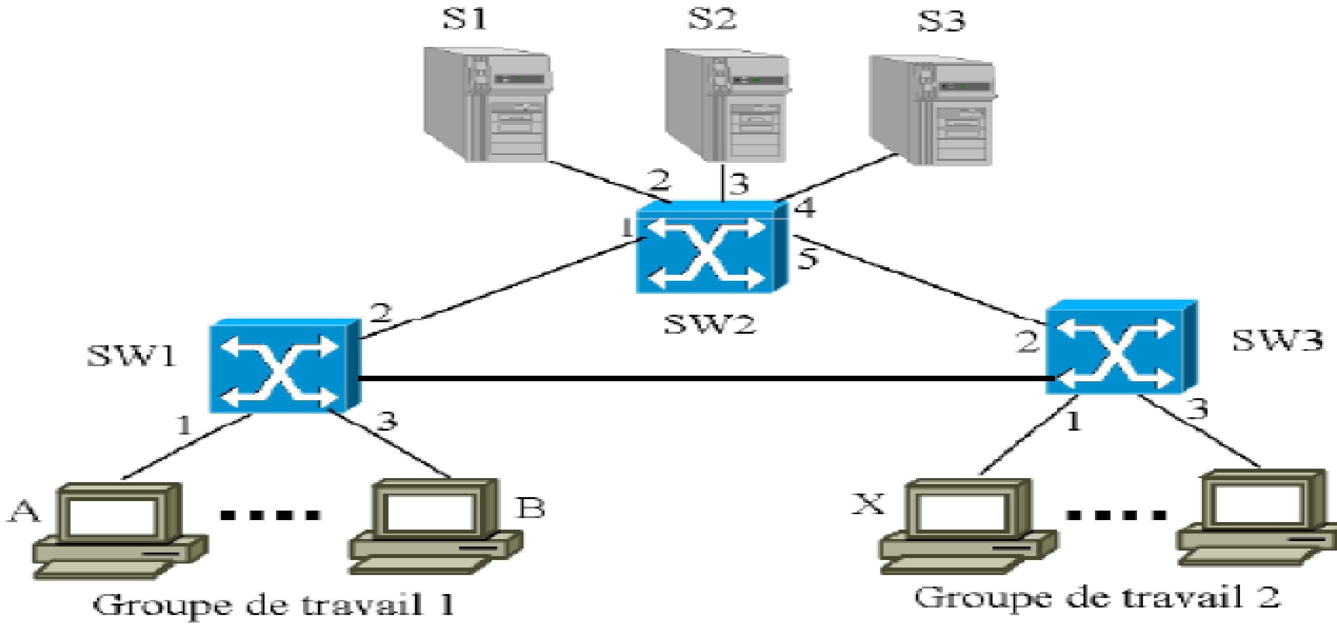
However, redundancy can create **loops**, which may cause several problems:

- **Frames can circulate indefinitely** because they don’t have a time-to-live (TTL) like IP packets.
- **Broadcast storms**: excessive broadcast traffic that can overwhelm the network.
- **Multiple copies of Ethernet frames** being delivered.
- **Errors in the switching tables**, leading to incorrect forwarding.



Example of a Broadcast Storm

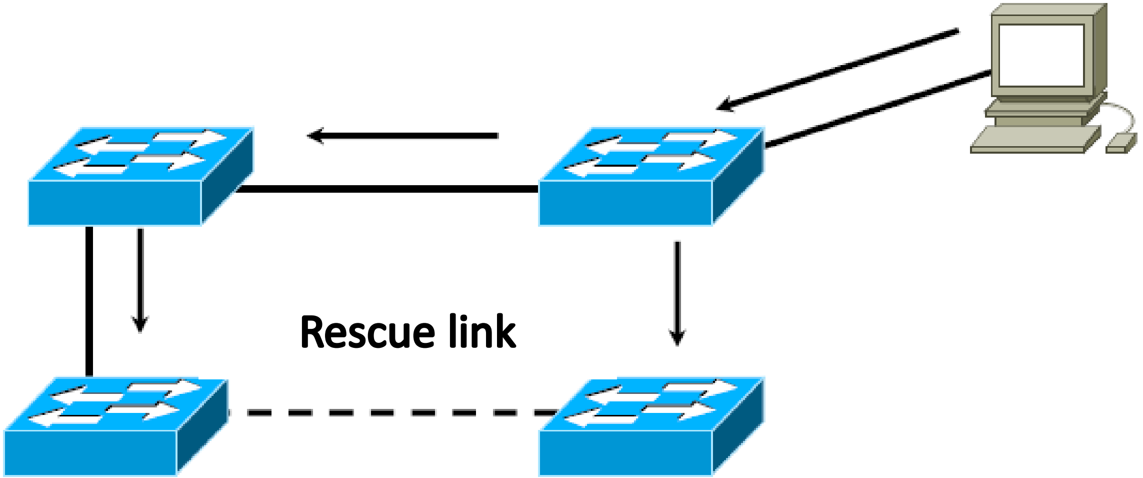
- Consider the following Ethernet network, composed of three Ethernet switches SW1, SW2, SW3, whose ARP caches are empty.
- What problem occurs after activating the self-learning mechanism in the three switches?



Solution :
Spanning Tree algorithm
IEEE 802.1

The Goal of STP (Spanning Tree Protocol)

- ✓ The objective of **STP** is to **prevent loops** in the network while still **allowing redundant paths**.
- ✓ STP **detects where loops exist** and **blocks redundant links** to maintain a loop-free topology.
- ✓ These blocked links are **kept as backups**, so they can be **activated in case of a failure**, providing **resilience to topology changes and equipment failures**.

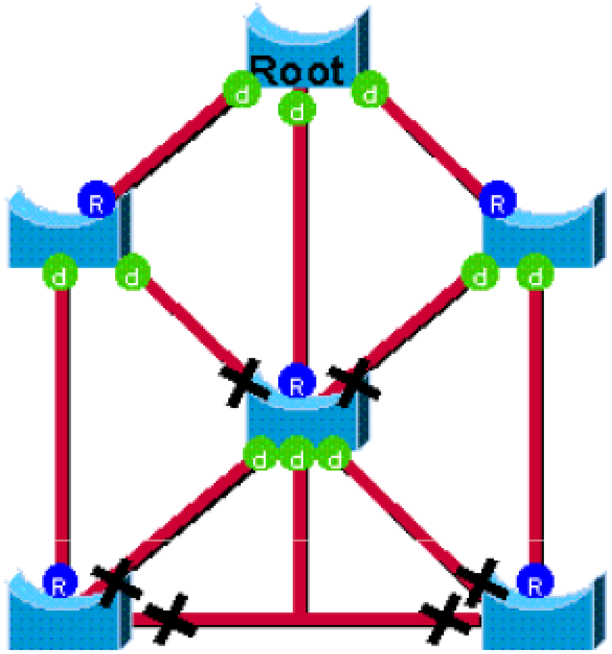


Spanning Tree Algorithm (STA)

- The **STP protocol** uses the **Spanning Tree Algorithm**, implemented by switches to create a **loop-free logical topology**.
- The algorithm was **developed by Radia Perlman** and is defined in the **IEEE 802.1D standard**.
- It allows switches to **communicate with each other** by exchanging special frames called **BPDUs (Bridge Protocol Data Units)**.
- These exchanges occur at **regular intervals**, enabling the network to **detect loops** and form a **loop-free spanning tree**.

Foundations of the STA (Spanning Tree Algorithm)

- ✓ STA identifies a **reference point called the Root Bridge**, from which the spanning tree is constructed.
- ✓ STA then determines the **available paths to the root**. If multiple paths exist, it **selects the best path** and **blocks the others** by disabling certain ports.
- ✓ Each **non-root bridge** determines its **root port**, which is the port with the **lowest path cost to the Root Bridge**.
- ✓ Once the root ports are identified, STA determines the **designated port** on each segment — the port with the **lowest cost to the root for that segment**.
  - ✓ Essentially, devices on each segment decide **which port to use to reach the root**.
- ✓ Finally, all ports that are **neither root ports nor designated ports** become **blocked ports**.



STP Concepts

Two key concepts are used by the **STA algorithm** to create a **loop-free topology:**

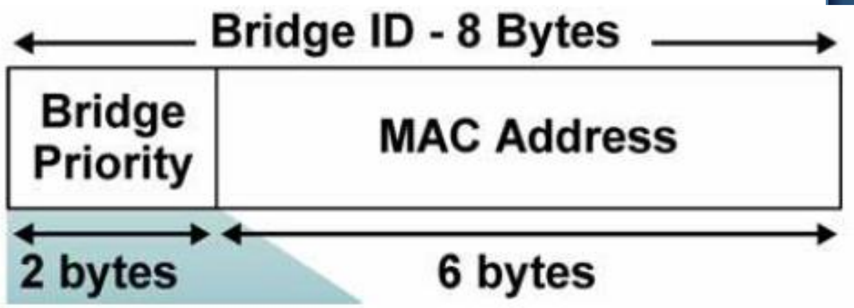
Bridge ID (BID):

Identifies switches and is used during the **Root Bridge election** process.

Composed of a **2-byte Bridge Priority field** and the **switch's MAC address**, making the BID **unique**.

The switch with the **lowest priority** becomes the Root Bridge; if priorities equal, the **lowest MAC address** breaks the tie.

Default Cisco switch priority: 32768 (0x8000).



Path Cost:

Used to determine the **best paths** to the Root Bridge.

Cost is based on the **link bandwidth** — lower cost corresponds to higher-speed links.

Path Cost

Path cost is used to identify the **"least expensive" or "fastest" path** to the Root Bridge.

The **path cost (or port cost)** is based on the **link bandwidth**.

The following table shows **IEEE-specified cost values** according to link speed:

Port speed	Port Cost (IEEE)
10 Gbps	2
1 Gbps	4
100 Mbps	19
10 Mbps	100

BPDU (Bridge Protocol Data Unit)

All switches (bridges) exchange **BPDU messages**, which allow the **STP topology to be configured**.

802.1D BPDU format: fields have specific byte lengths (as defined by the standard).

BPDUs are **encapsulated in Ethernet 802.3 frames** and sent in **multicast** to all interfaces.

2	1	1	1	8	4	8	2	2	2	2	2
Protocol identifier	Version	Message type	Flags	Root ID	Root path cost	Bridge ID	Port ID	Message age	Maximum age	Hello time	Forward delay

Key information contained in a BPDU:

- **Root ID:** the Root Bridge identifier as perceived by the sending bridge.
- **Root Path Cost:** the cost from the sending bridge to the presumed Root Bridge.
- **Bridge ID:** identifier of the sending bridge.
- **Port ID:** the port number on which the BPDU is sent.

Fields of a BPDU Frame

Protocol Identifier, Version, and Message Type: not really used; the **Flags** field indicates if there has been a **topology change**.

Message Age: time elapsed since the BPDU was sent.

Maximum Age: specifies when the BPDU should be discarded (acts like a TTL for BPDUs).

Hello Time: interval between sending BPDUs (default **2 seconds**).

Forward Delay: time to wait before transitioning to a new port state (e.g., **15 seconds** to move from Listening to Forwarding).

BPDU

Allows:

- ✓ Communication between switches (bridges)
- ✓ Election of the Root Bridge

Bytes	Field
2	Protocol ID
1	Version
1	Message Type
1	Flags
8	Root ID
4	Cost of Path
8	Bridge ID
2	Port ID
2	Message Age
2	Maximum Time
2	Hello Time
2	Forward Delay

Who is the root bridge?

How far away is the root bridge?

What is the BID of the bridge that sent this BPDU?

What port on the sending bridge

BPDU

- ✓ BPDU are exchanged regularly every 2 seconds

Bytes	Field
2	Protocol ID
1	Version
1	Message Type
1	Flags
8	Root ID
4	Cost of Path
8	Bridge ID
2	Port ID
2	Message Age
2	Maximum Time
2	Hello Time
2	Forward Delay

```
Protocol Id:   0
Version ID:    0
Message Type:  0  Configuration Message
Flags:         %00000000
Root ID:       0x8000/ 00:D0:C0:F5:18:C0
Cost :         0x00000000  (0)
Bridge ID:     0x8000/ 00:D0:C0:F5:18:C0
Port ID:       0x8001/ Port1
Message Age:   0/256 seconds
Maximum Age:   5120/256 seconds
 (20seconds)
Hello Time:    512/256 (2  seconds)
Forward Delay: 3840/256 (15seconds)
```

The “Spanning Tree” in Three Steps

Step 1: Root Bridge Election

Based on **switch priority**

If priorities are equal, based on **switch MAC address**

Step 2: Root Port Selection

Consider **path cost** to the root

Each non-root switch selects the **port with the lowest path cost** to the Root Bridge

Step 3: Designated Port Selection

For each network segment, the switch with the **lowest path cost to the root**

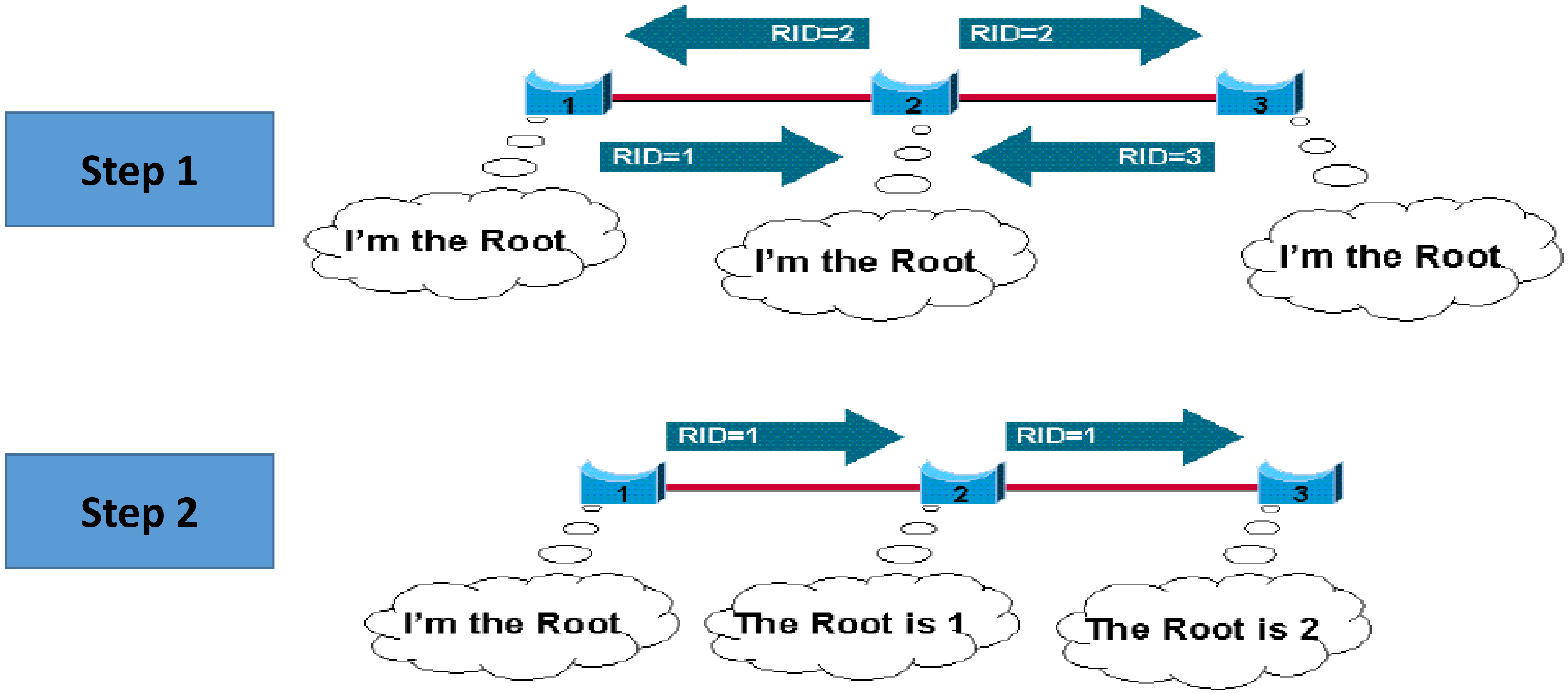
designates its port as the **Designated Port**

Step 1: Root Bridge Election

Only **one switch can become the Root Bridge**, determined as follows:

The **switch with the lowest priority**

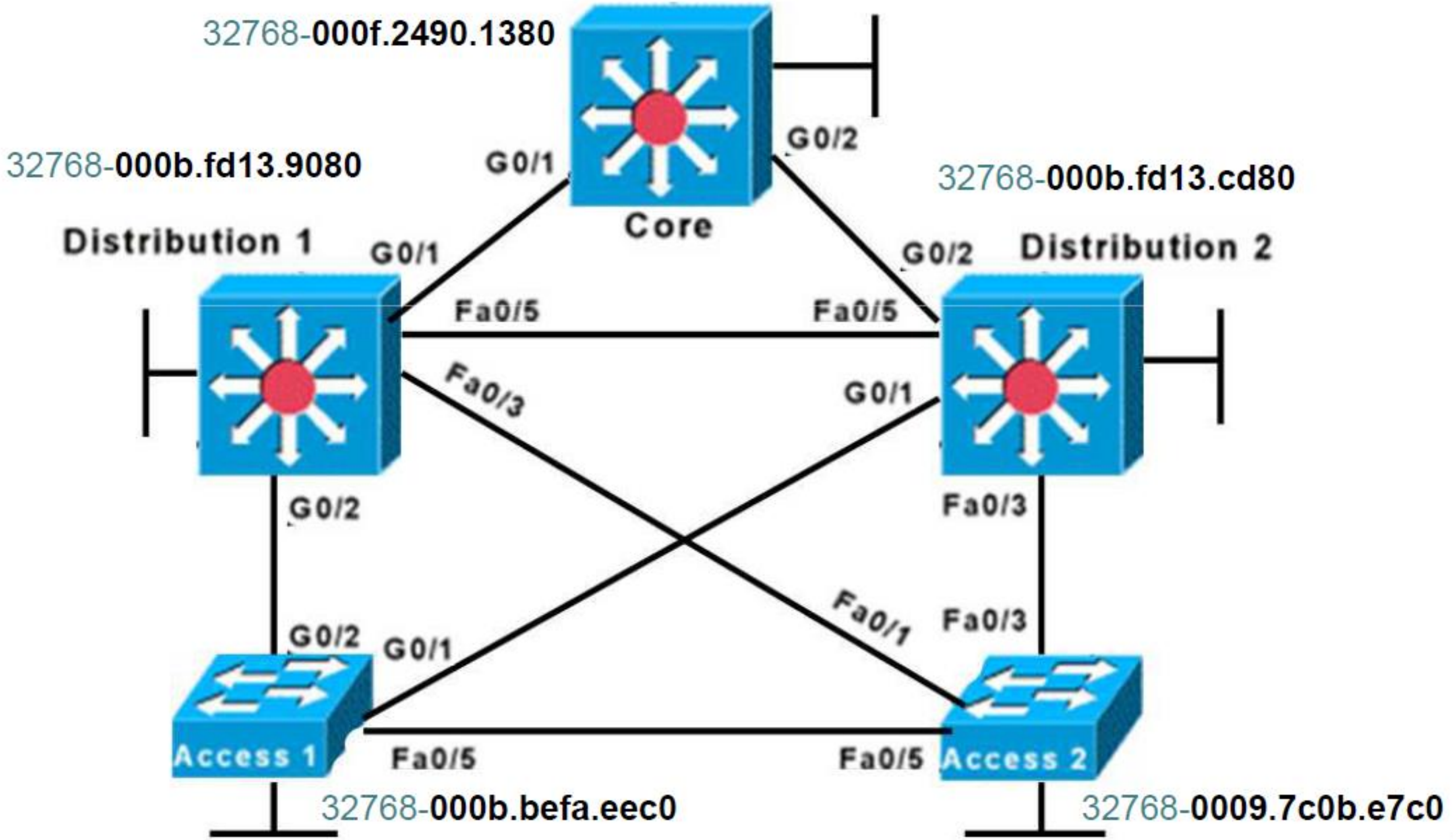
If priorities are equal, the **switch with the lowest MAC address**



Step 2: Root Port Selection

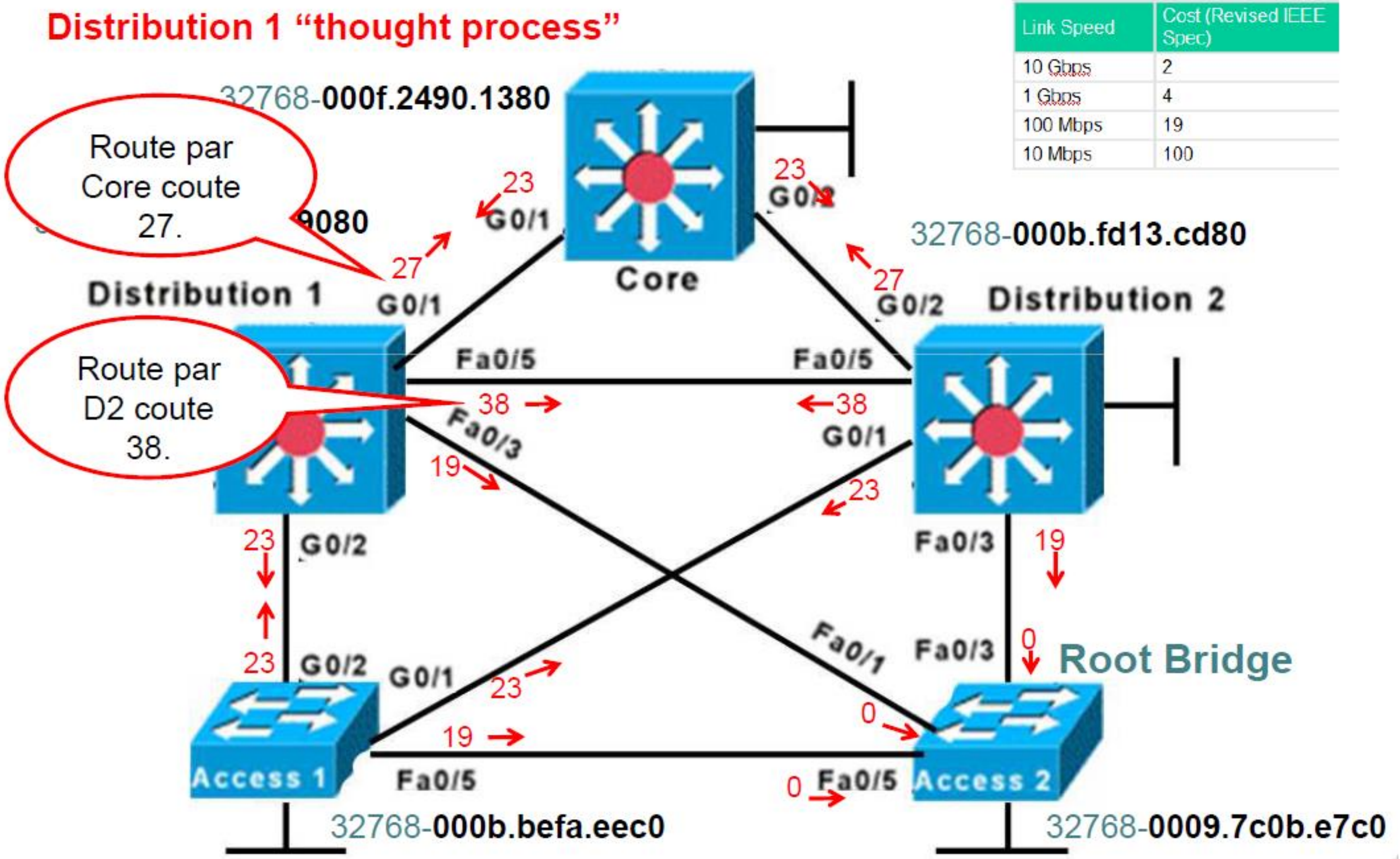
- Once the **Root Bridge** is selected, switches must identify **redundant paths** to the Root Bridge and allow only **one active path**, **blocking all others**.
- Switches accomplish this by **exchanging BPDUs**.
- **How does a switch determine which port to use (the Root Port) and which ports to block?**
  - The **port with the lowest path cost to the Root Bridge** is chosen as the **Root Port**.
  - All other ports that lead to the root via higher-cost paths are **blocked**.

Example



32768-000f.2490.1380
32768-000b.fd13.9080
G0/1
G0/2
32768-000b.fd13.cd80
Core
Distribution 1
G0/1
G0/2
Distribution 2
Fa0/5
Fa0/5
Fa0/3
G0/1
G0/2
Fa0/3
Fa0/1
Fa0/3
G0/2
G0/1
Access 1
Fa0/5
Fa0/5
Access 2
32768-000b.befa.eec0
32768-0009.7c0b.e7c0

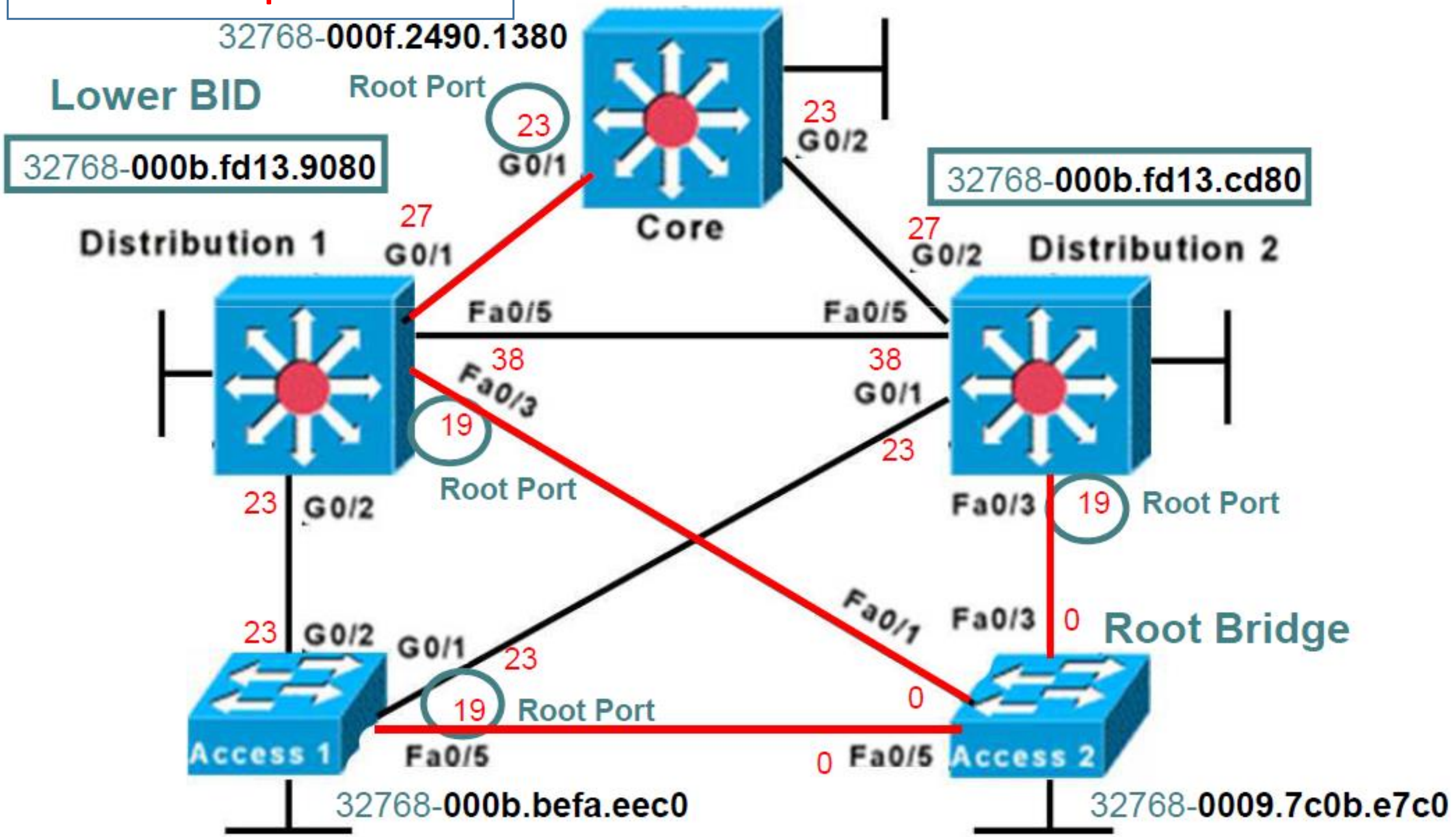
Example: Root port



Link Speed	Cost (Revised IEEE Spec)
10 Gbps	2
1 Gbps	4
100 Mbps	19
10 Mbps	100

Example: Root port

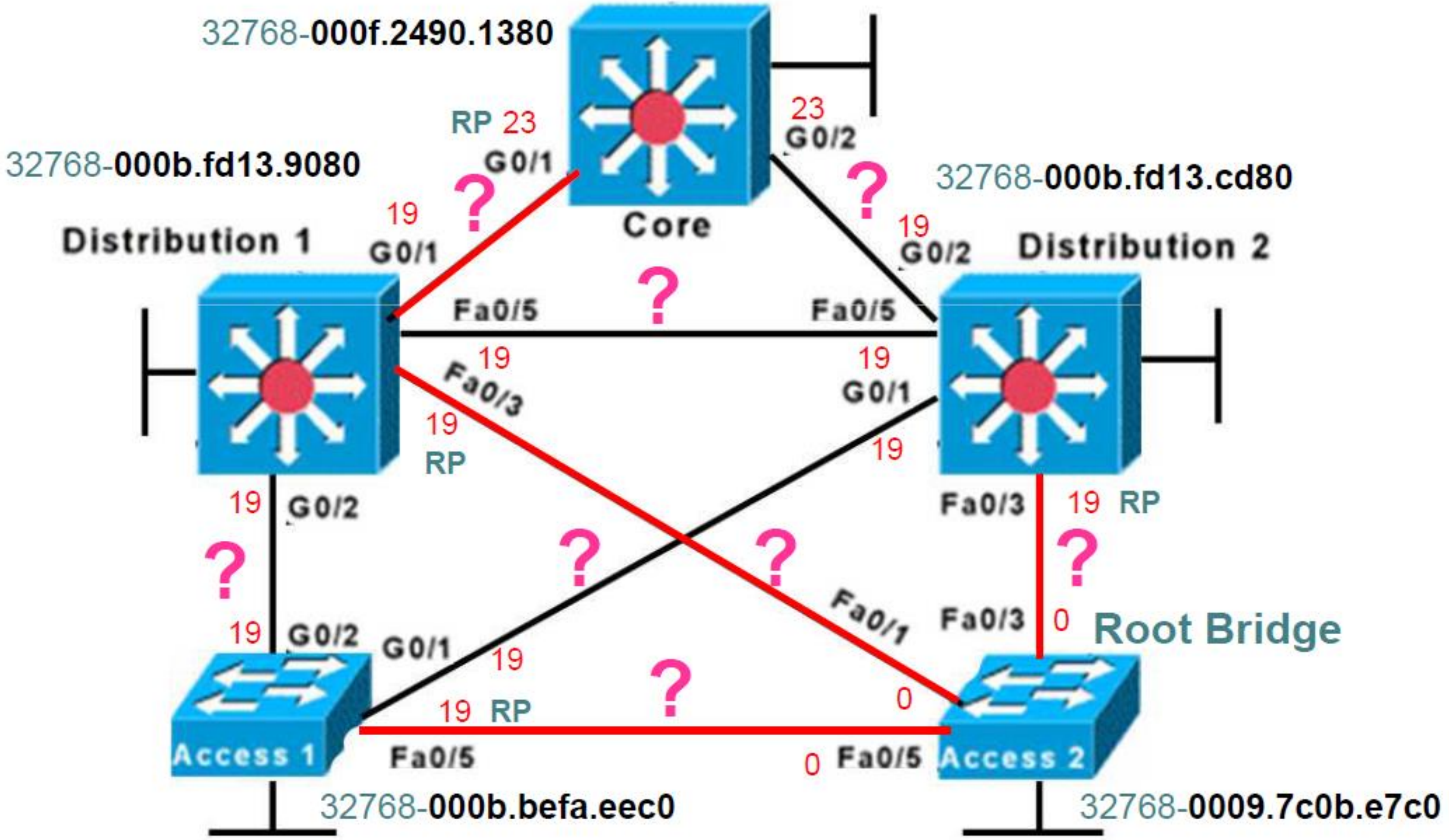
Case of equal costs



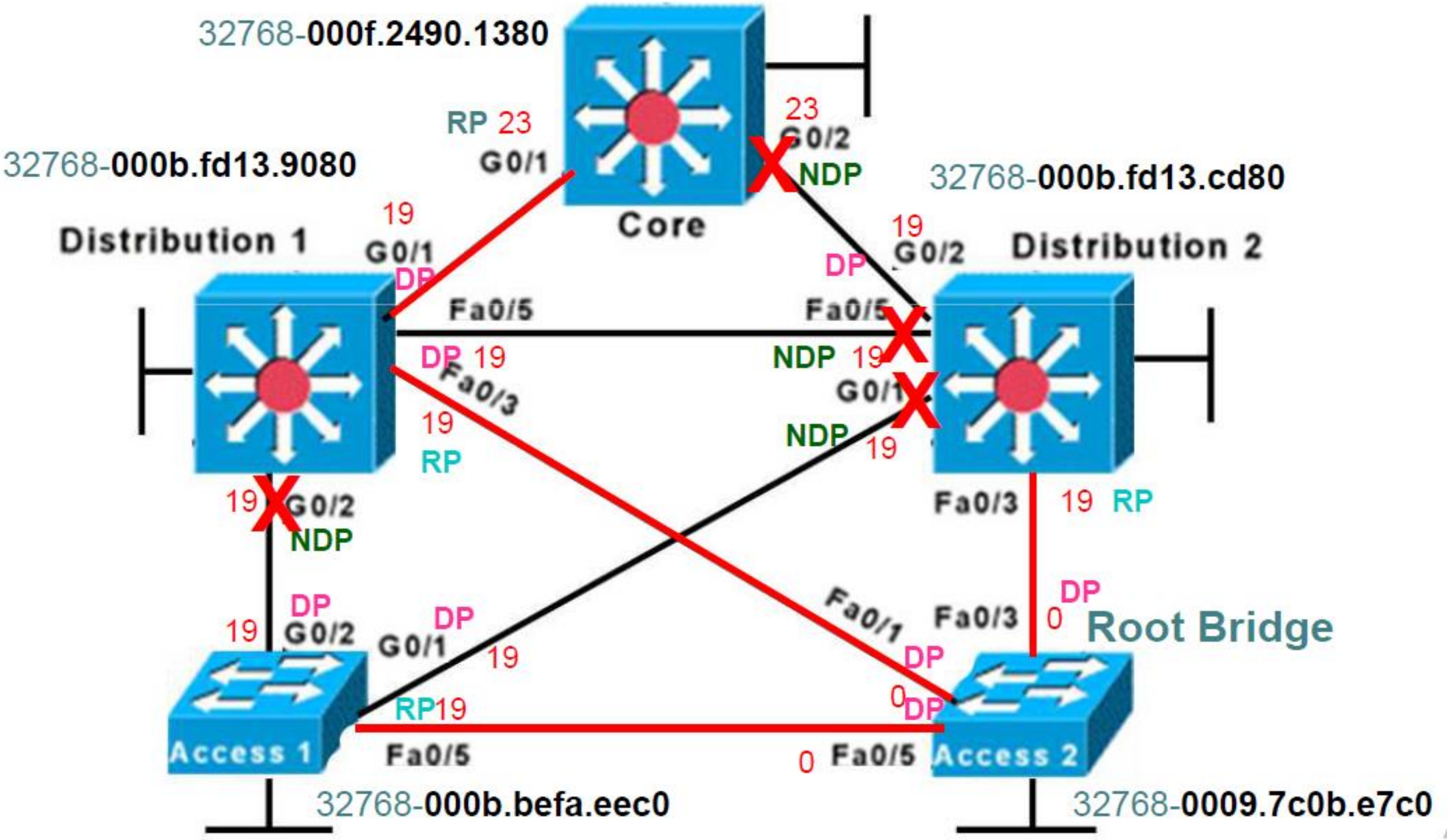
Step 3: Designated Port Selection

- The **Designated Port** is the **unique port on a switch** that **handles data traffic** (both incoming and outgoing) for a given network segment with respect to the Root Bridge.
- It can also be seen as the port that **advertises the lowest path cost to the Root Bridge** for that segment.

Example: Designated port



Example: Designated port



STP qsts

1. What is the first step of the STP process?
2. How can a network administrator influence which switch becomes the STP Root Bridge?
3. For what purpose do switches use the information contained in BPDU messages?
4. On what criterion is the choice of a port to block based when two ports have equal cost?
5. Do non-root switches have only one root port? True or False?

STP qsts

What is the first step of the STP process?
Answer: Election of the **Root Bridge**. The switch with the **lowest Bridge ID (priority + MAC address)** becomes the root.
How can a network administrator influence which switch becomes the STP Root Bridge?
Answer: By **changing the switch priority**. A lower priority increases the chance of becoming the Root Bridge. If priorities are equal, the MAC address is used.
For what purpose do switches use the information contained in BPDU messages?
Answer:

- To **elect the Root Bridge**
- To **determine root ports and designated ports**
- To **detect loops and maintain a loop-free topology**

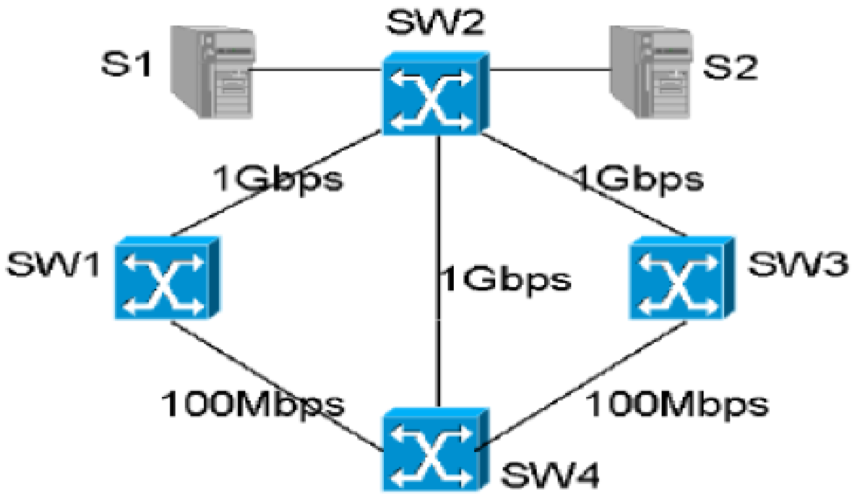
On what criterion is the choice of a port to block based when two ports have equal cost?
Answer: The switch uses **tie-breaking rules**:

- Lowest **upstream Bridge ID**
- Lowest **Port ID**

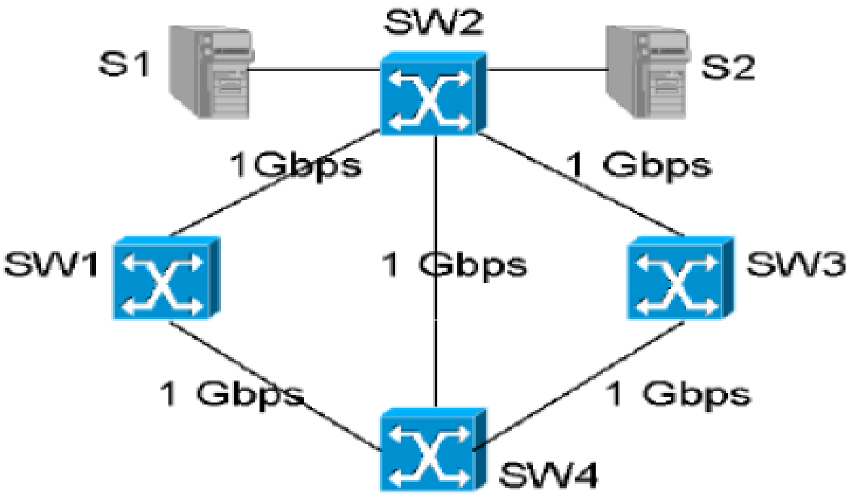
Do non-root switches have only one root port? True or False?
Answer: True.
Explanation: Each non-root switch has **a single root port**, which is the port with the **lowest path cost to the Root Bridge**. All other ports may be designated or blocked depending on the segment.

STP Exercise

- Each switch in the two networks below has a **Bridge ID (BID)**. Let’s assume the IDs are **1, 2, 3, and 4** for switches **SW1, SW2, SW3, and SW4**, respectively.
- For each of the two networks, **indicate the spanning tree resulting from the STP protocol**.
- For each of the two networks, state whether the resulting spanning tree is the **most optimal tree**. If it is not, **what should be done to make the resulting tree more optimal**?



Network 1



Network 2