SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

ICT259 Computer Networking

Seminar 5: Switching

Ms Wong Yoke Moon

SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Classpoint

- Login to classpoint.app using your mobile device like hp or tablet
- Use your preferred name
- Use code on slide

Virtual LANs

Virtual LANs (VLANs)

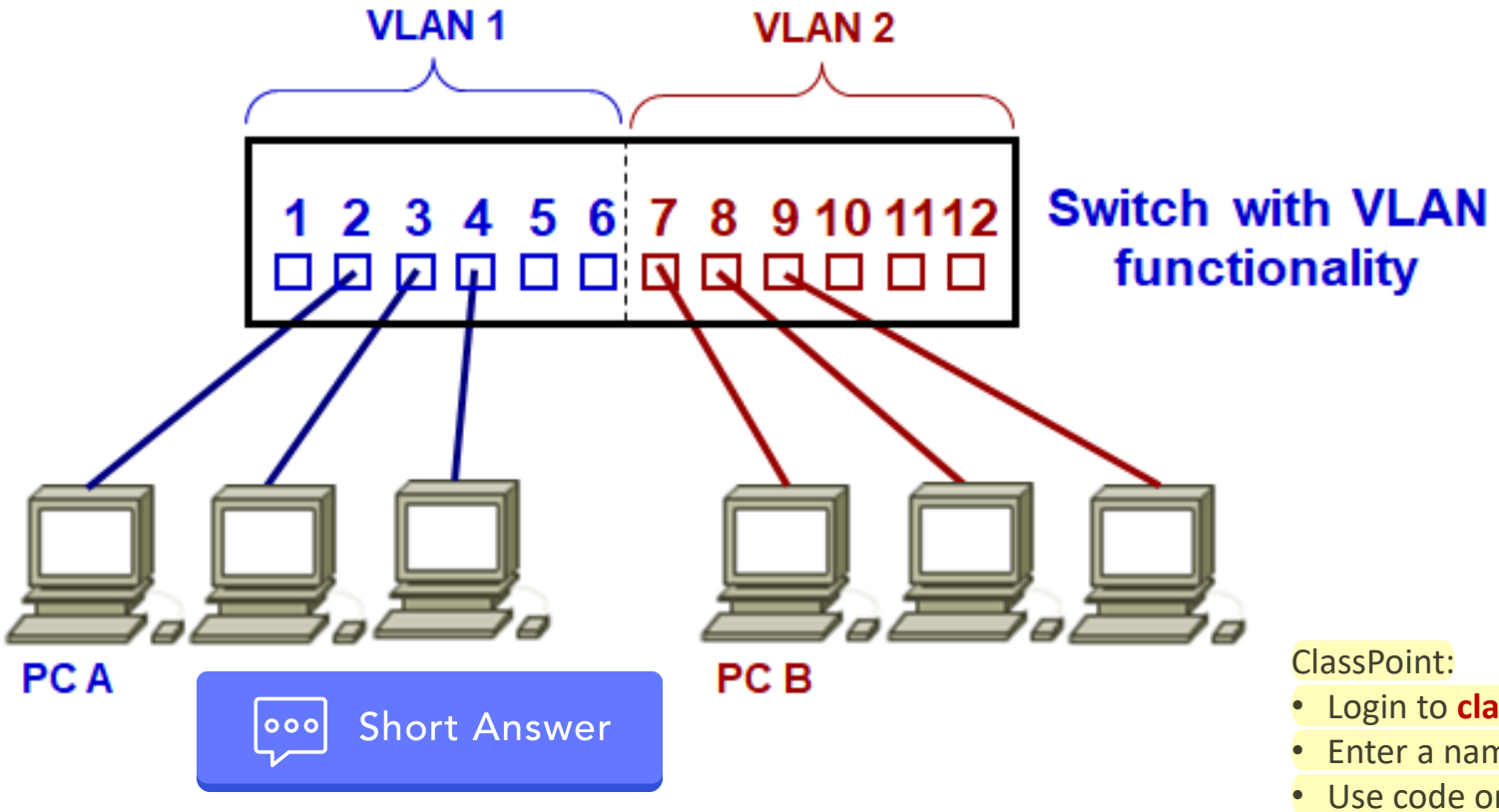
Objectives:

- **Define Virtual LANs** (VLANs) and discuss the **benefits of VLANs**
- Explain how **VLANs** are used to create **broadcast domains**
- Explain how **routers** are used for **communication between VLANs**

Pre-Lesson Activity on VLAN

Can PC A communicate with PC B?

Explain your answer.

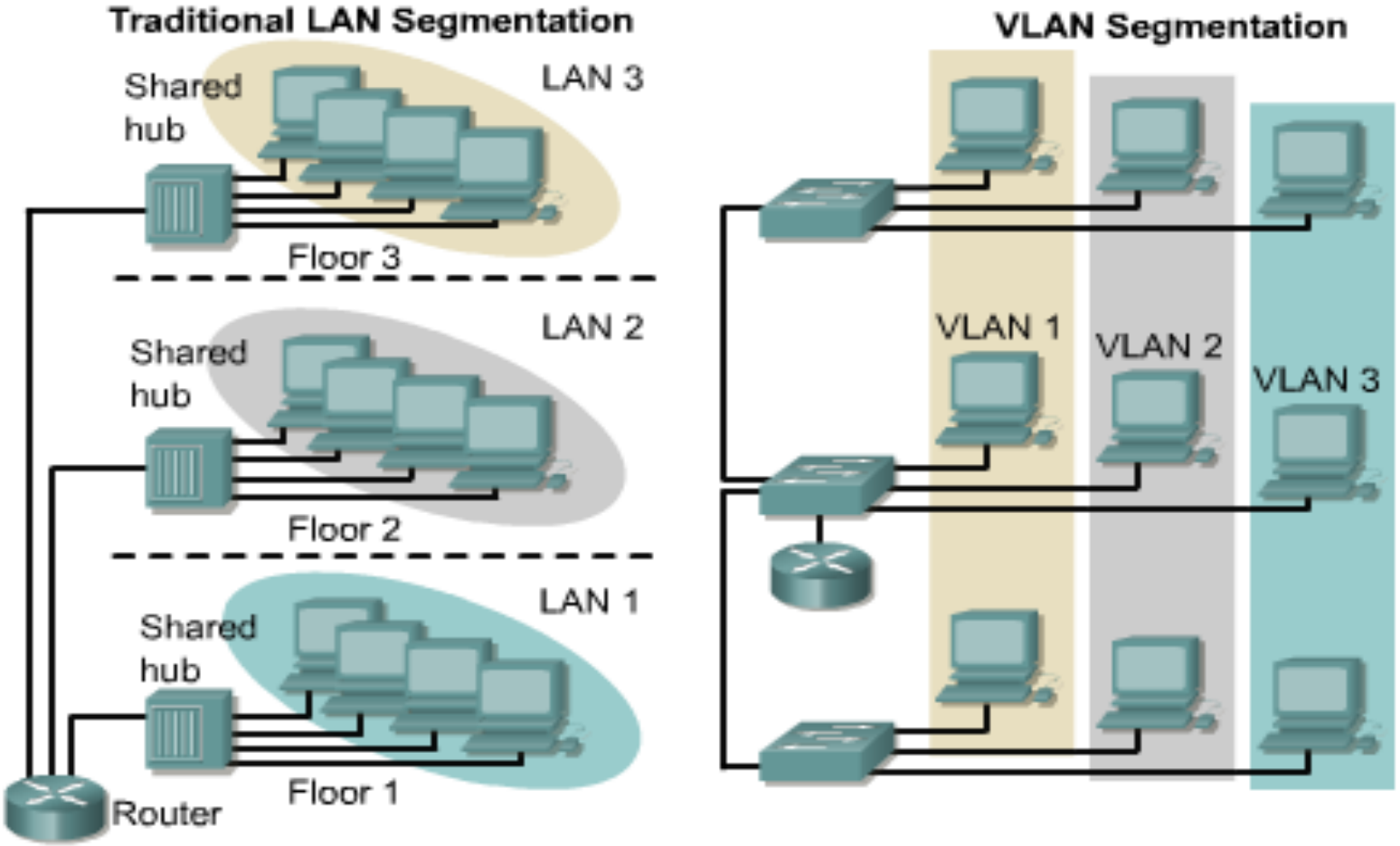


ClassPoint:

- Login to **classpoint.app**
- Enter a name
- Use code on slide

VLAN Concepts

A **VLAN** is a group of network services not restricted to a physical segment or LAN switch.

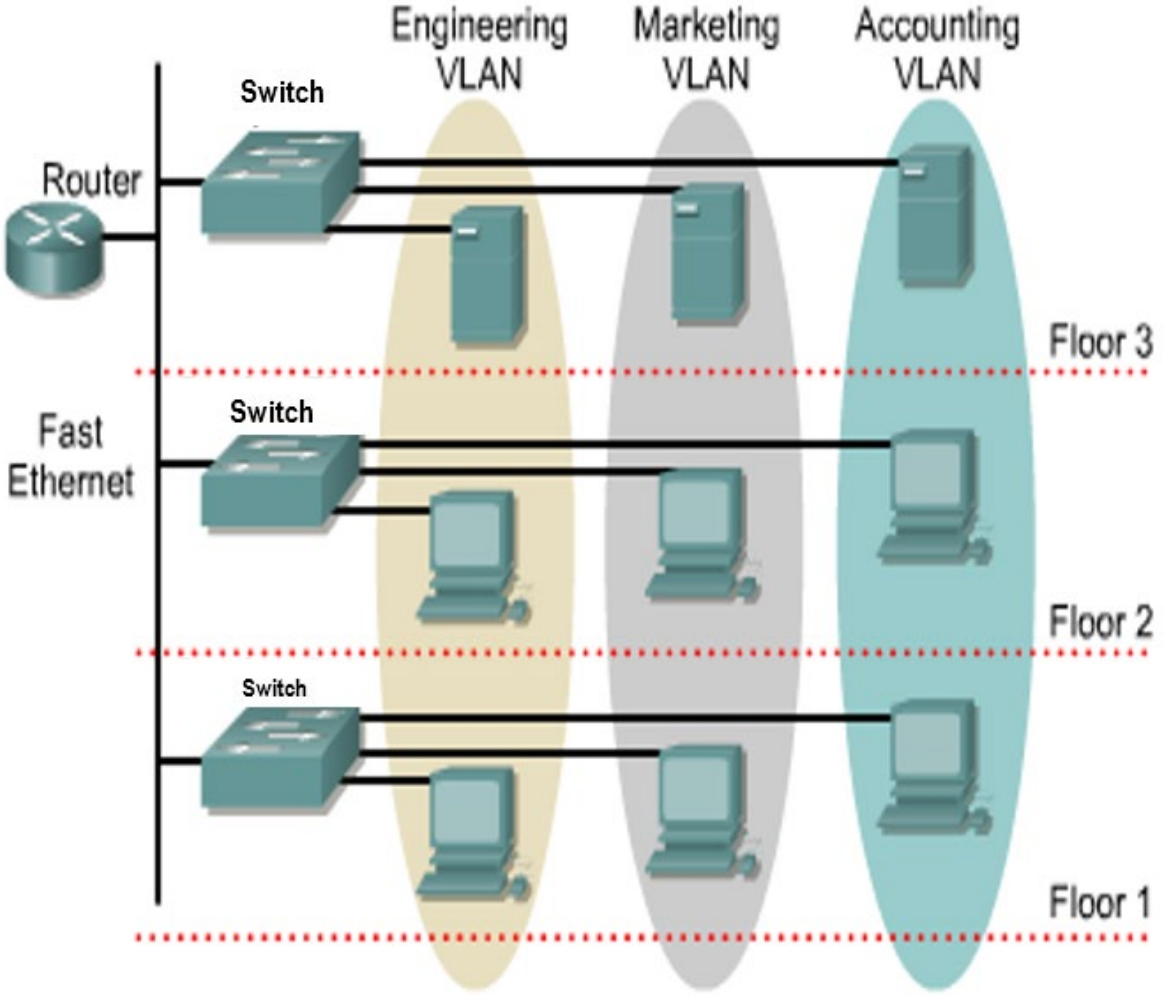


VLAN Concepts

- **VLANs logically segment switched networks** based on functions, project teams, or applications of the organization **regardless of the physical location** or connections to the network.
- All workstations and servers used by a particular workgroup share the same VLAN, regardless of the physical connection or location.
- **Configuration** or reconfiguration of VLANs is **done through software**.
- Physically moving cables and equipment is unnecessary when configuring VLANs.

VLAN Concepts

- VLANs address **scalability**, **security**, and **network management**.
- Routers in VLAN topologies provide **broadcast filtering**, **security**, and **traffic flow management**.



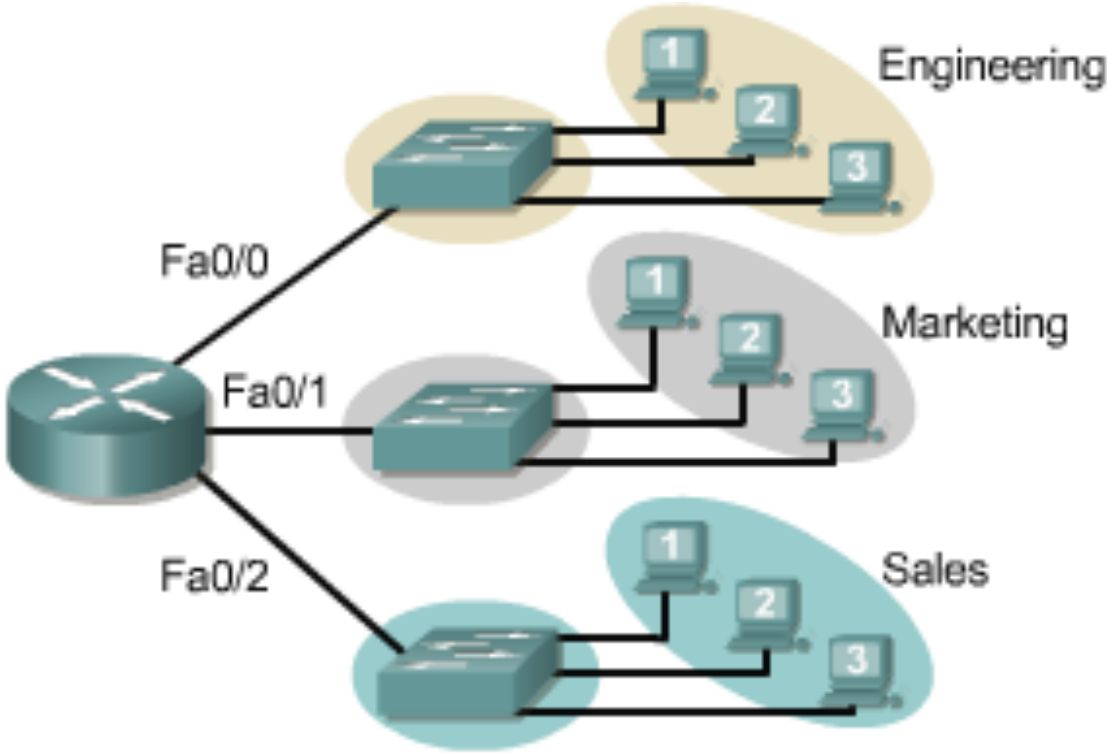
Broadcast Domains in Networks without VLANs

- In this scenario, **no VLANs** are used.

- Switch for Engineering.
- Switch for Sales.
- Switch for Marketing.

- **Each switch** treats all ports as members of **one broadcast domain**.

- **Router** is used to route packets among the **3 broadcast domains**.

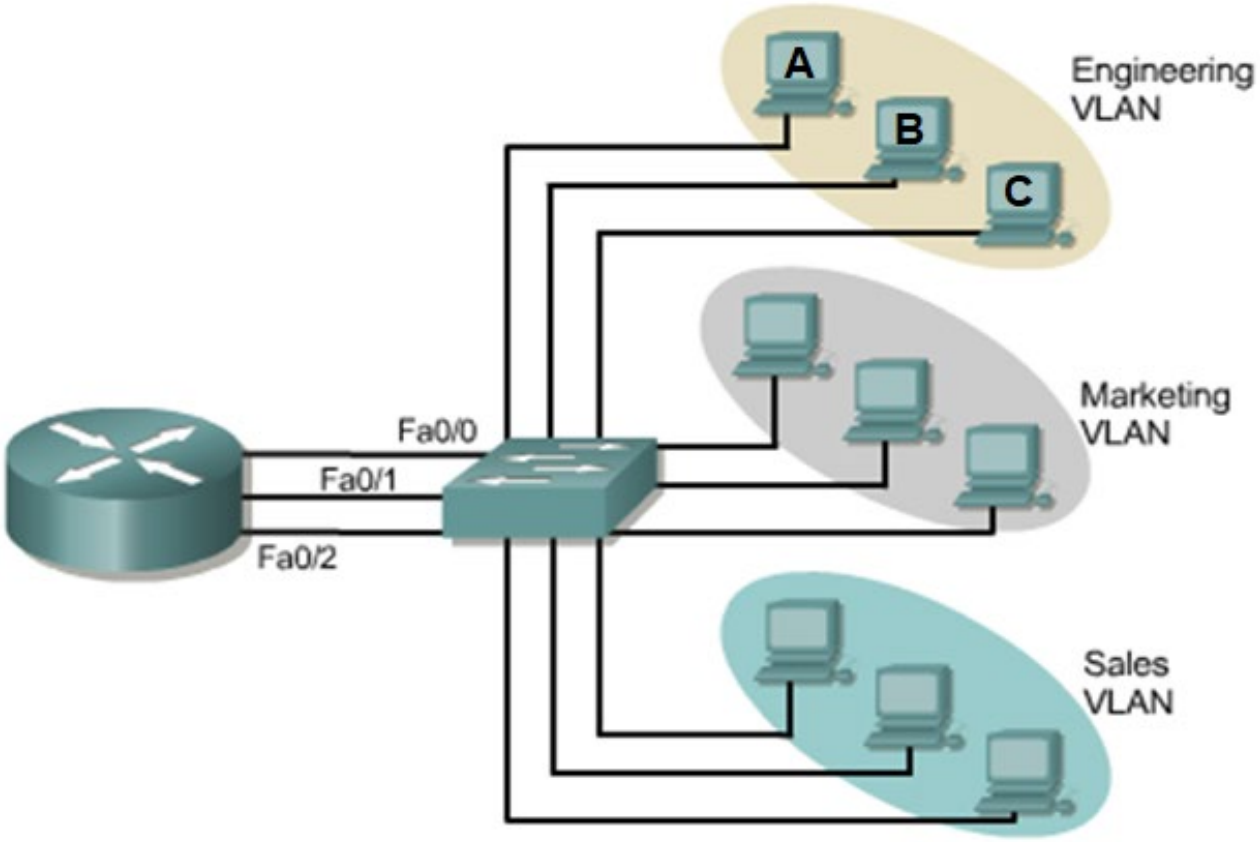


3 Broadcast Domains = 3 VLANs

- Each **VLAN** is
  - usually a **subnet**
  - a **broadcast domain**

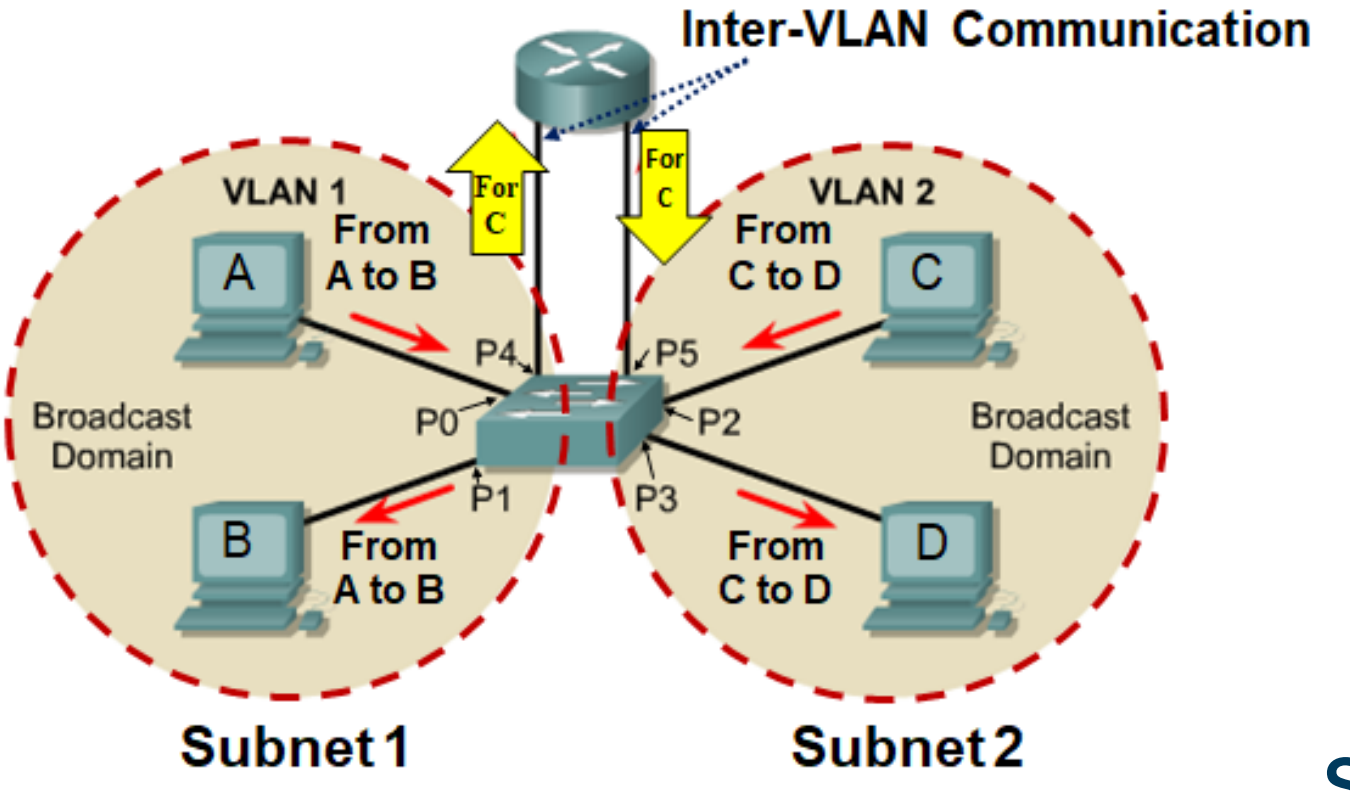
- If station A sends a broadcast frame, it reaches only stations B and C.

- Any communication between VLANs must go through the router.

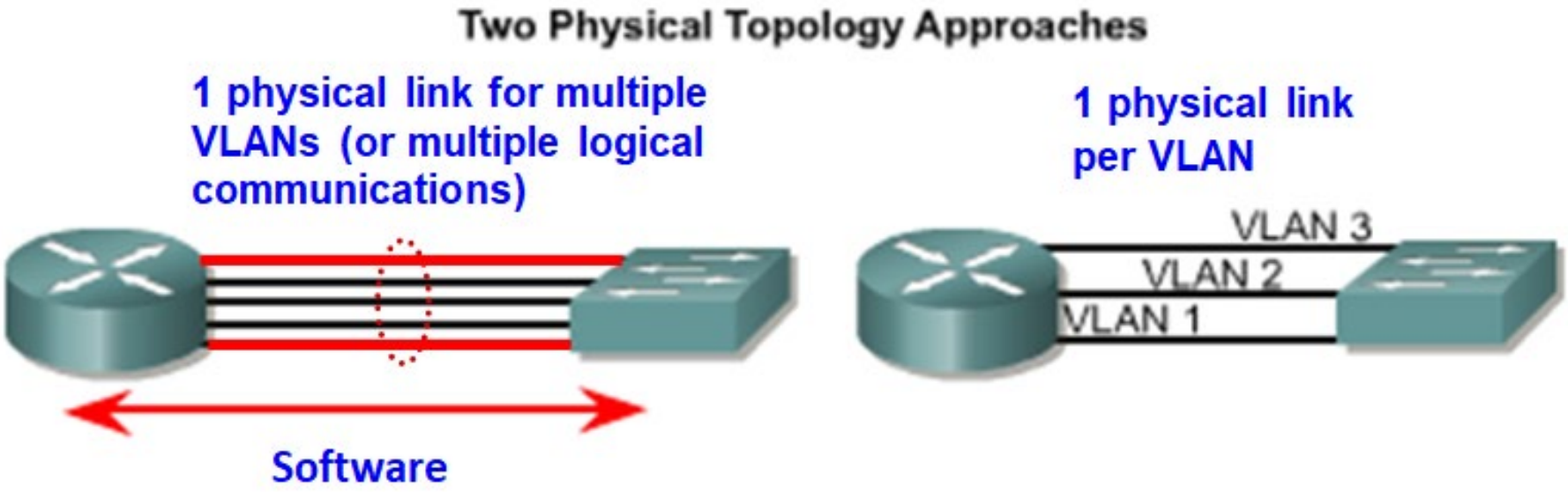


Inter-VLAN Communications

- Any communication within a VLAN is forwarded directly by the switch.
- E.g. If A transmits a frame to B, the switch forwards from port P0 to P1.
- However, if the frame has to be transmitted **between two VLANs**, the **router performs inter-VLAN routing** between the two VLANs.
- Each **VLAN** is also a **subnet**.



Communications Between VLANs

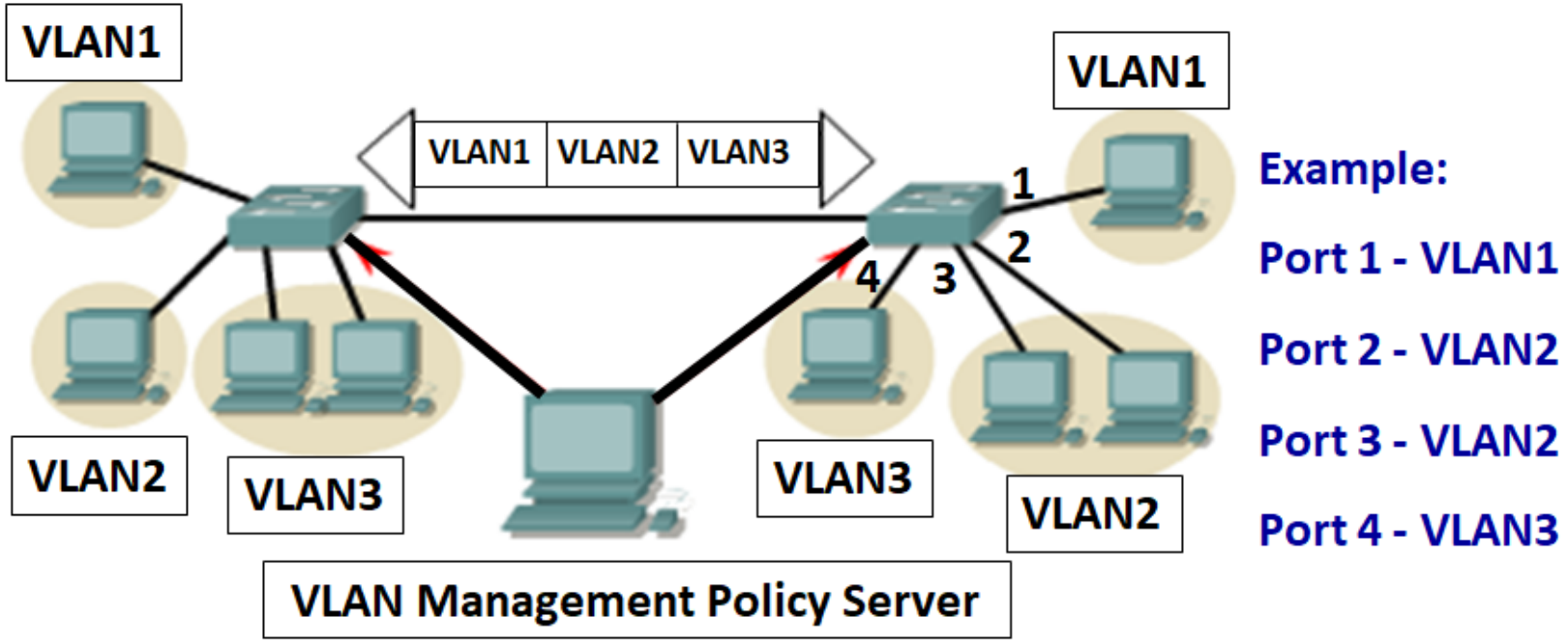


Using **routers to link VLANs** provides the following **benefits**:

- Additional **security and management** is added.
- Logical links **conserve physical ports**.
- Routers **control access** to VLANs.
- Up to 255 VLANs or more can be supported per router.

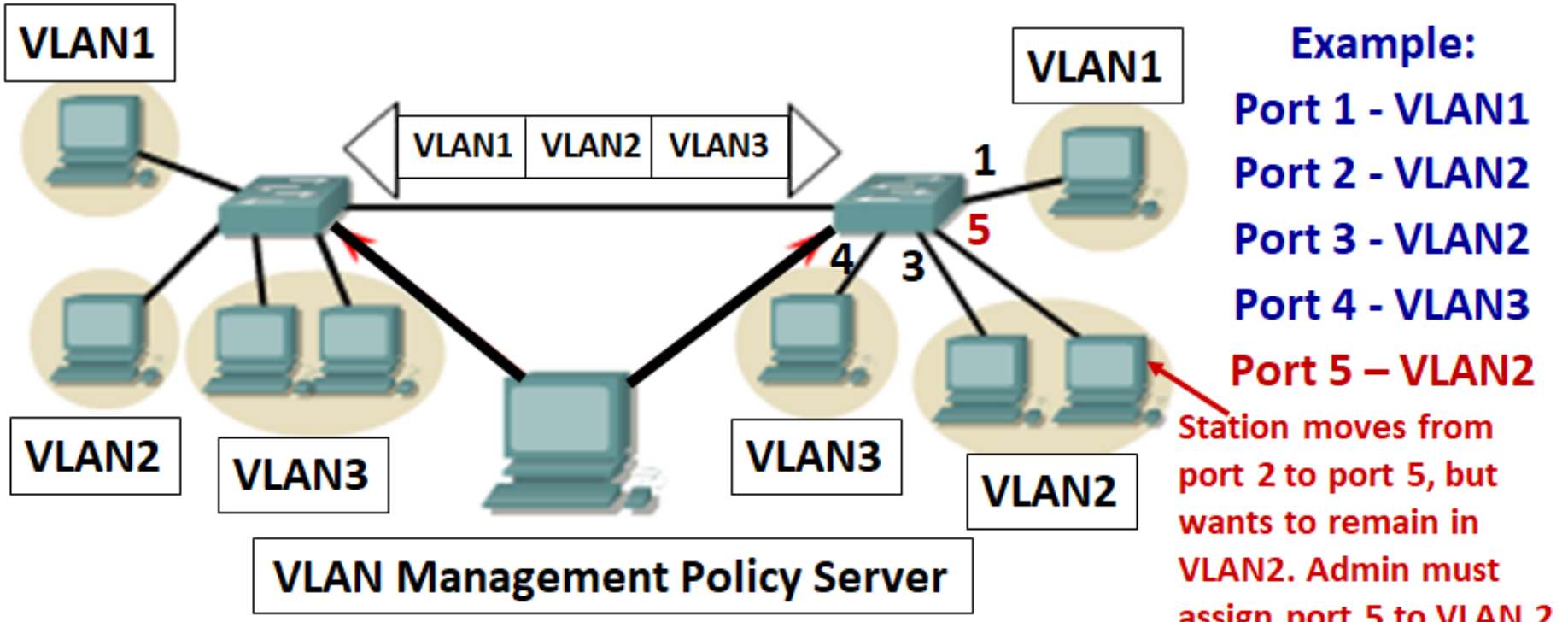
VLAN Operation

- VLAN can be created based on port.
- Referred to as **port-based** membership.
- **Each switch port** is assigned **to a different VLAN**.
- As a device is connected to the network, it automatically assumes the VLAN of the port to which it is attached.
- The use of the VLAN management policy server is beyond this course.



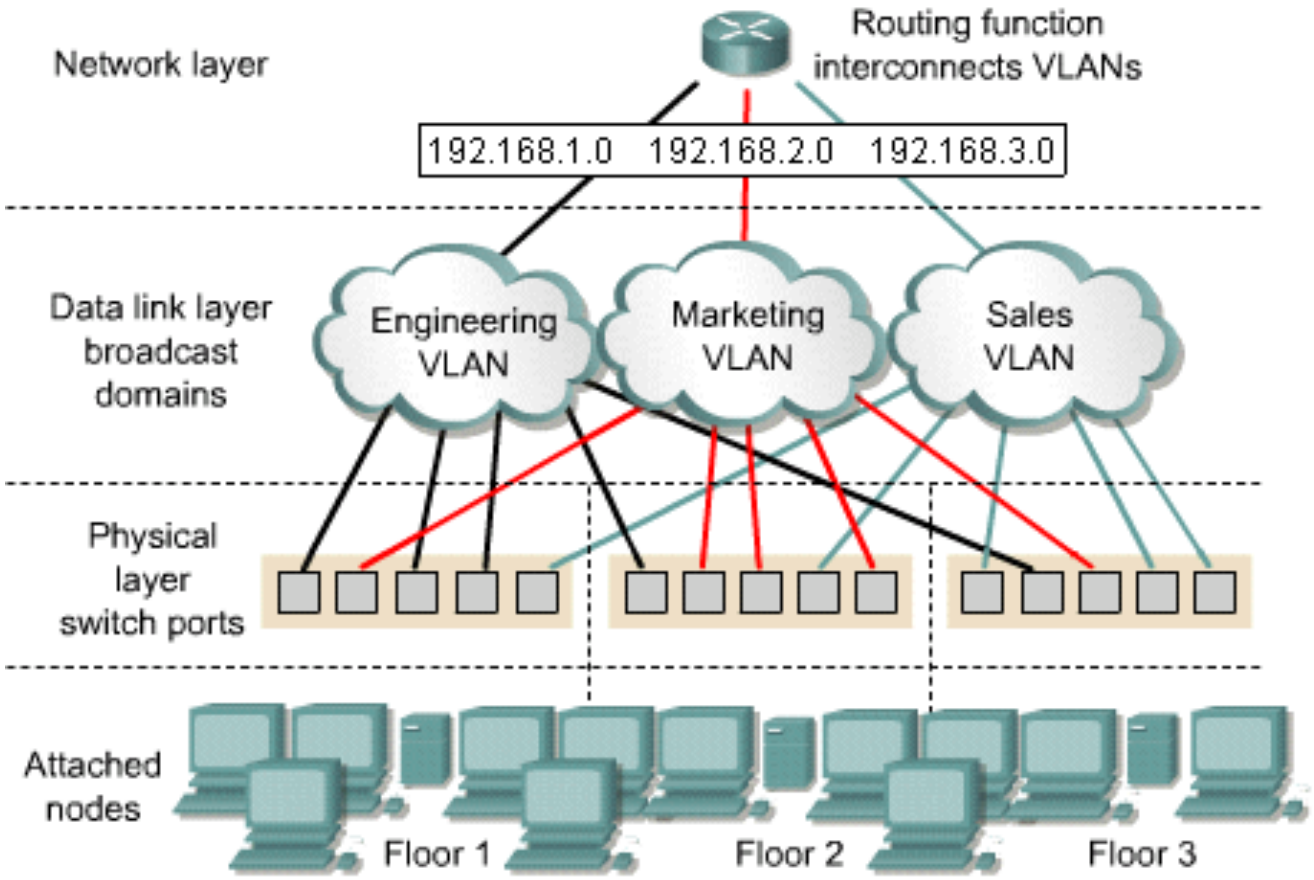
VLAN Operation

- If a user changes ports and needs to access to the same VLAN, the network administrator must manually make a port-to-VLAN assignment for the new connection.
- E.g. user moves from port 2 to port 5, but wants to remain in VLAN2. Admin must assign port 5 to VLAN 2.



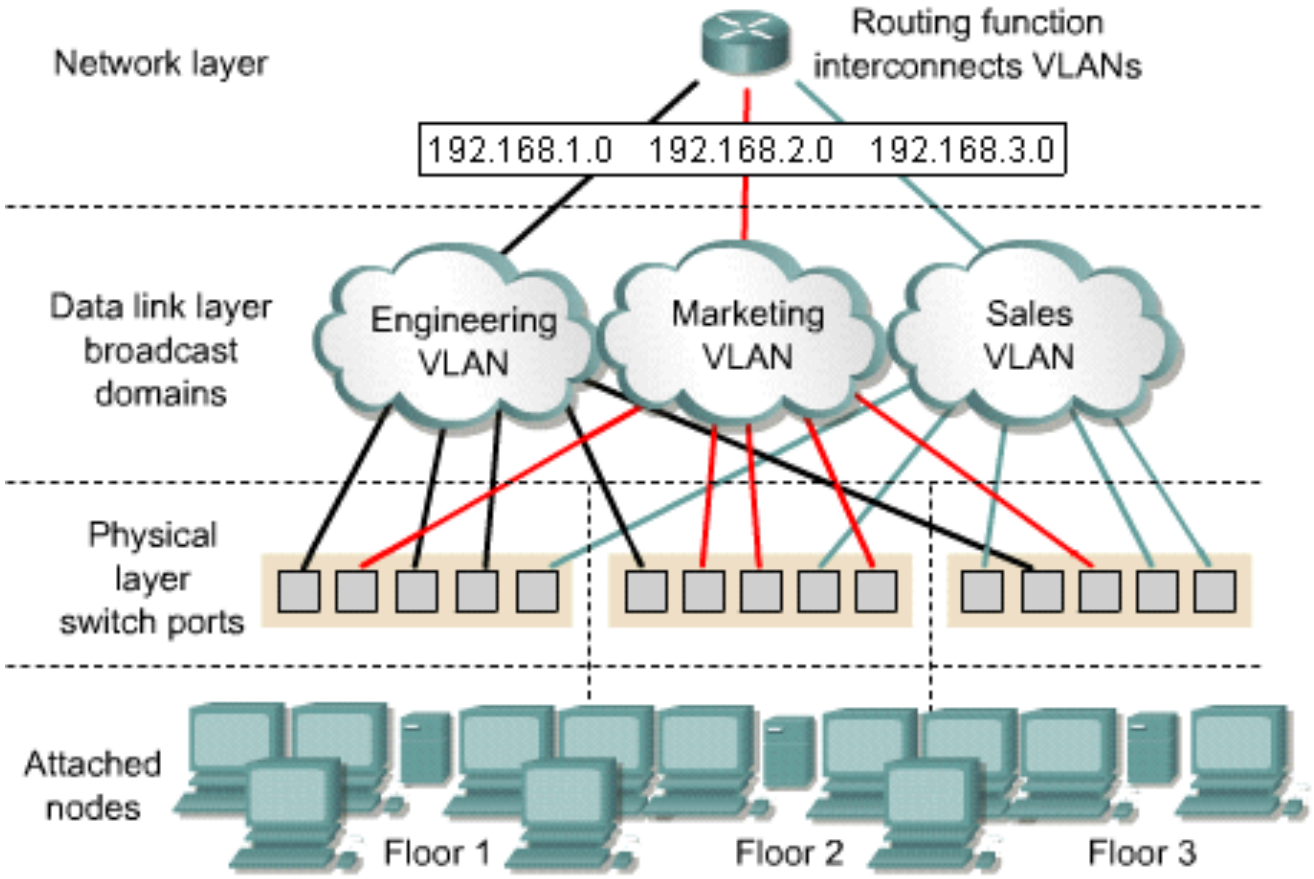
Port-based VLAN

- The port is assigned to a specific VLAN that is independent of the user or device attached to the port.



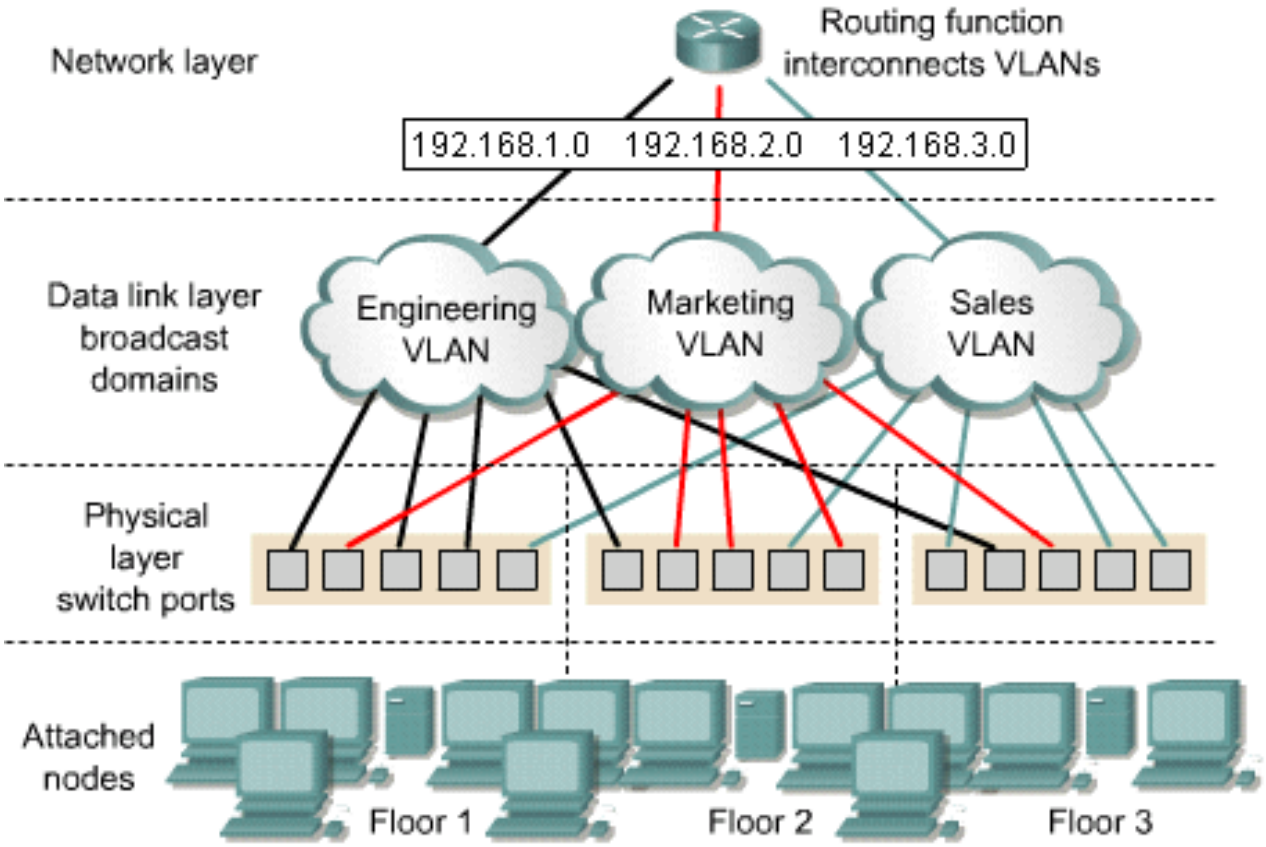
Port-based VLAN

- A single user workstation or a hub that has multiple workstations can be connected to a single switch port.
- All users who are attached to a port must be in the same VLAN.



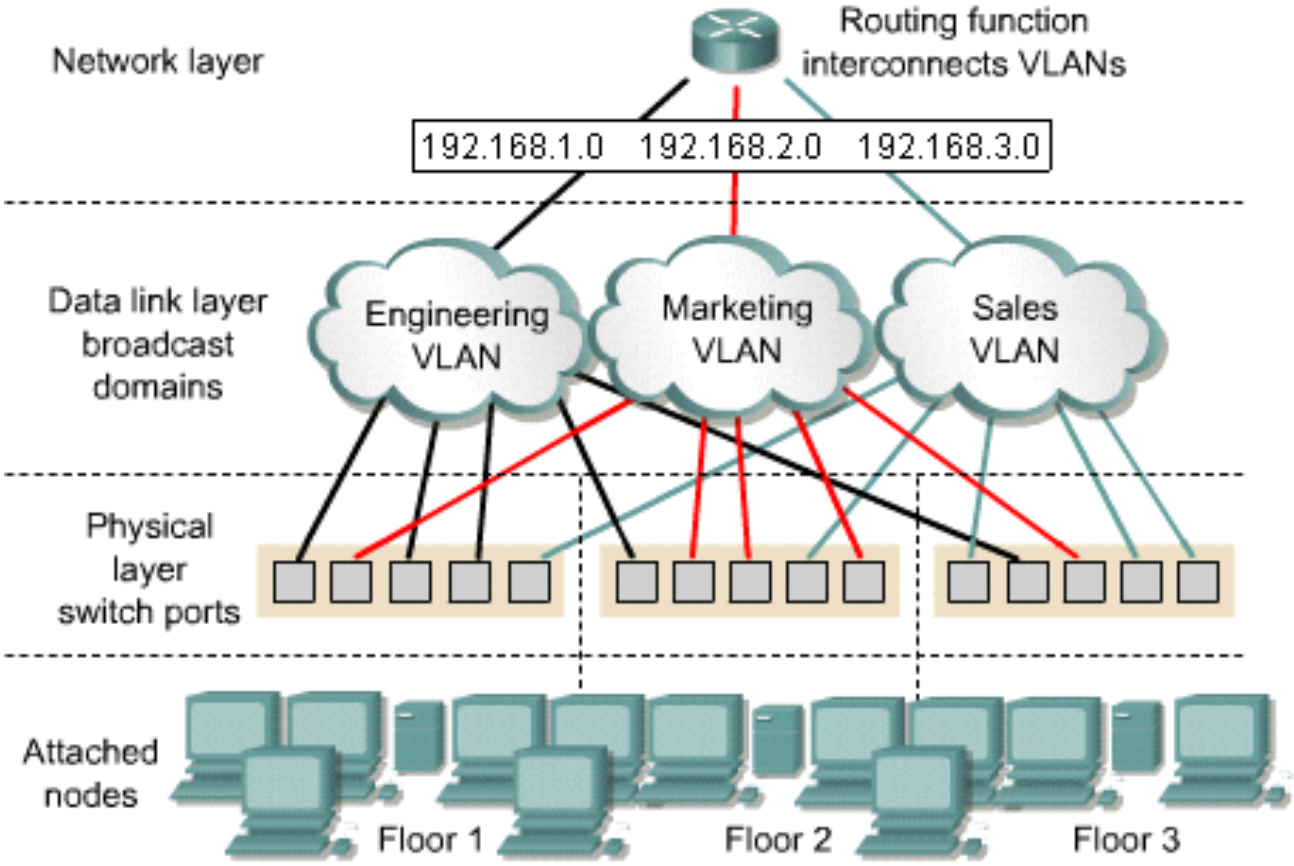
Port-based VLAN

- In the diagram below, each VLAN is on a separate network and the router is used to communicate between them.
- Each VLAN should have a unique Layer 3 network or subnet address assigned. This aids in switching packets between VLANs with routers.



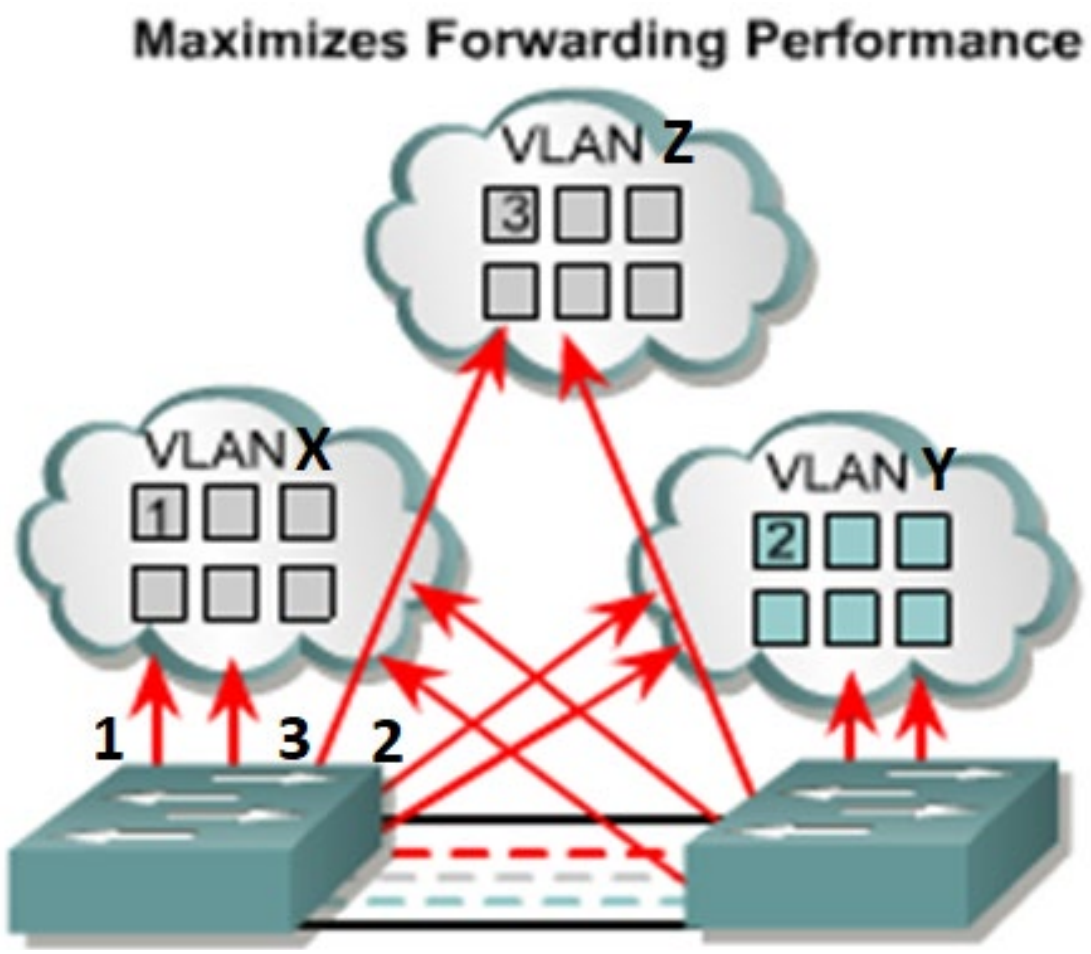
Port-based VLAN

- Ports assigned to the same VLAN share the broadcasts.
- Ports that do not belong to that VLAN do not share these broadcasts.
- This improves the overall performance of the network.



Port-based VLAN

- Network administrator configures port-by-port.
- Each port is associated with a specific VLAN.
- The network administrator is responsible for keying in the mappings between the ports and VLANs.
- Maximises security between VLANs.
- Frames do not “leak” into other domains.
- Easily controlled across networks.



Default VLAN

- The **VLAN for every port in the switch** when it is first taken out from the box. It is the factory default.
- **VLAN 1** is the **default VLAN**.
- It is also the management VLAN. VLAN Trunking Protocol (VTP) advertisements are sent on VLAN 1 (VTP will be covered later).
- It cannot be deleted.
- The **IP address of the switch** can be **configured on this VLAN**.

VLAN and MAC Address Table

Q: If a switch is connected to 3 VLANs, how many MAC address table does the switch have?

ClassPoint:
- Login to **classpoint.app**
- Enter a name
- Use code on slide

Functions of a Switch with VLANs

- The switch maintains a **separate MAC address table** for **each VLAN**.
- If a **frame** comes in on a port in **VLAN 1**, the switch **searches the MAC address table for VLAN 1**.
- When the frame is received, the switch **adds the source address**, if it is currently unknown, **to the MAC address table of VLAN 1**.
- The destination address is checked so that a decision can be made.
- For **learning, forwarding and filtering,** the **search** is made against the **MAC address table for that VLAN only**.

Advantages and Limitations of VLANs

Advantages of VLANs:

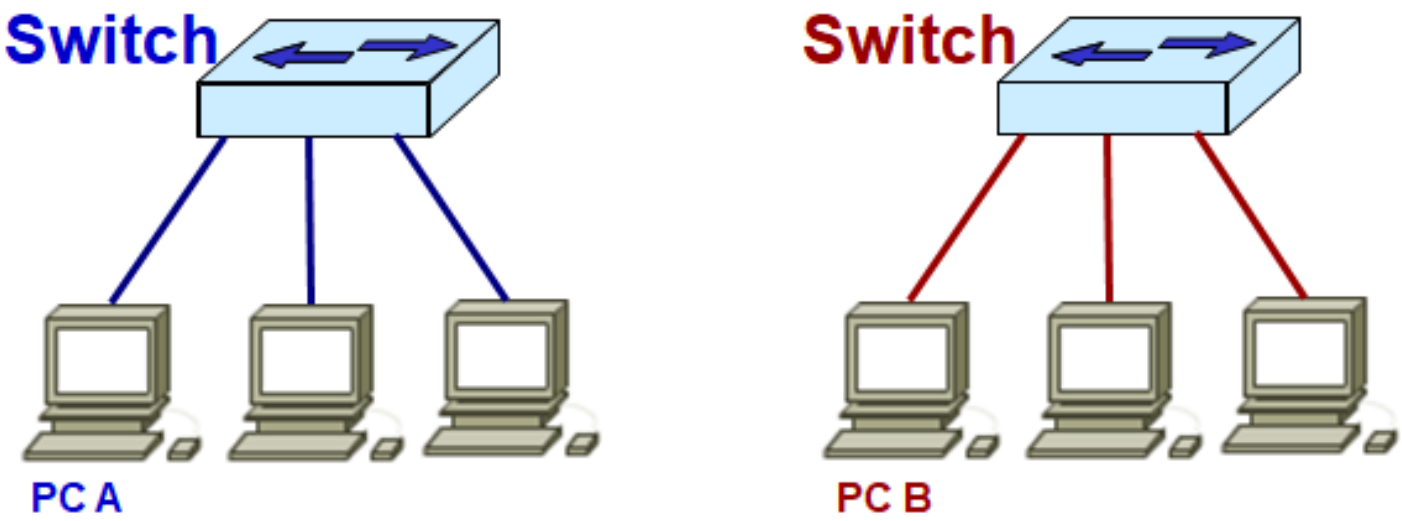
- Less expensive alternative to routers for broadcast containment.
- Allow nodes to be moved logically rather than physically.
- Improves security.

Limitations of VLANs:

- Network topologies utilising VLANs take a fair amount of planning and design.
- VLANs have been proprietary, single vendor solutions.

Concluding VLAN Concepts

Two physical LANs without connectivity:



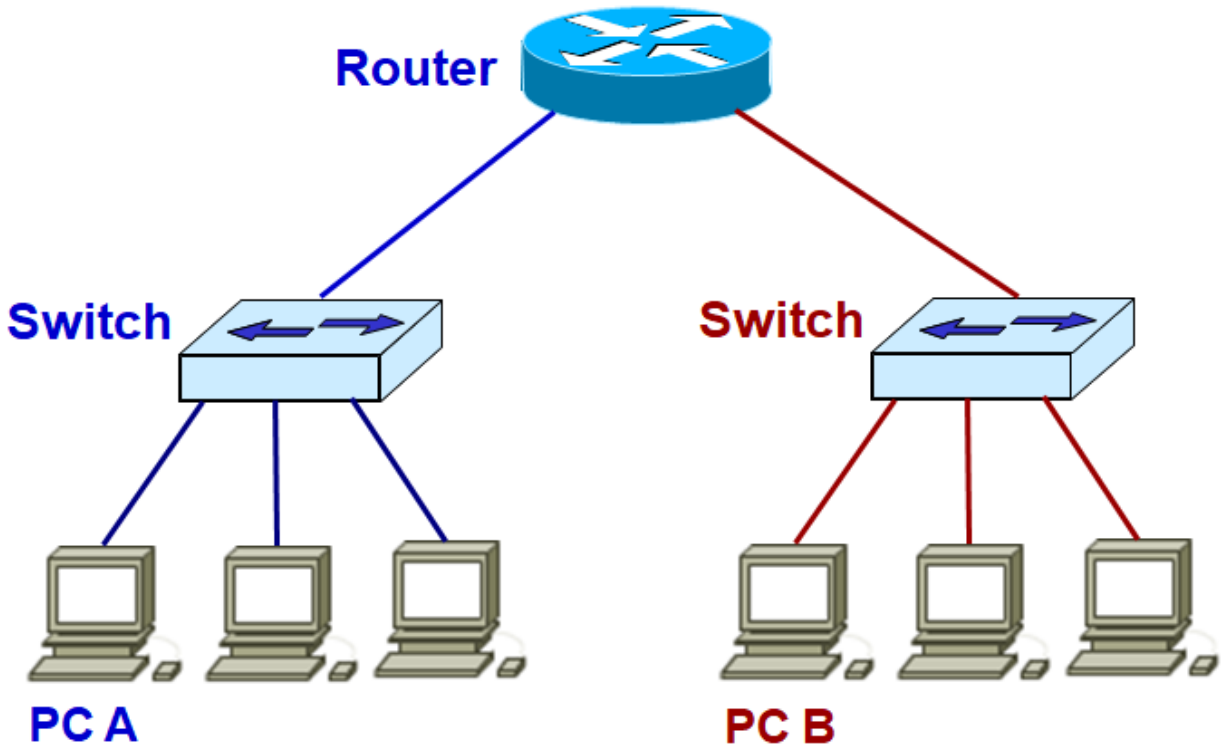
Q: What interconnecting device is needed for two LANs to communicate?

Short Answer

ClassPoint:
- Login to **classpoint.app**
- Enter a name
- Use code on slide

Concluding VLAN Concepts

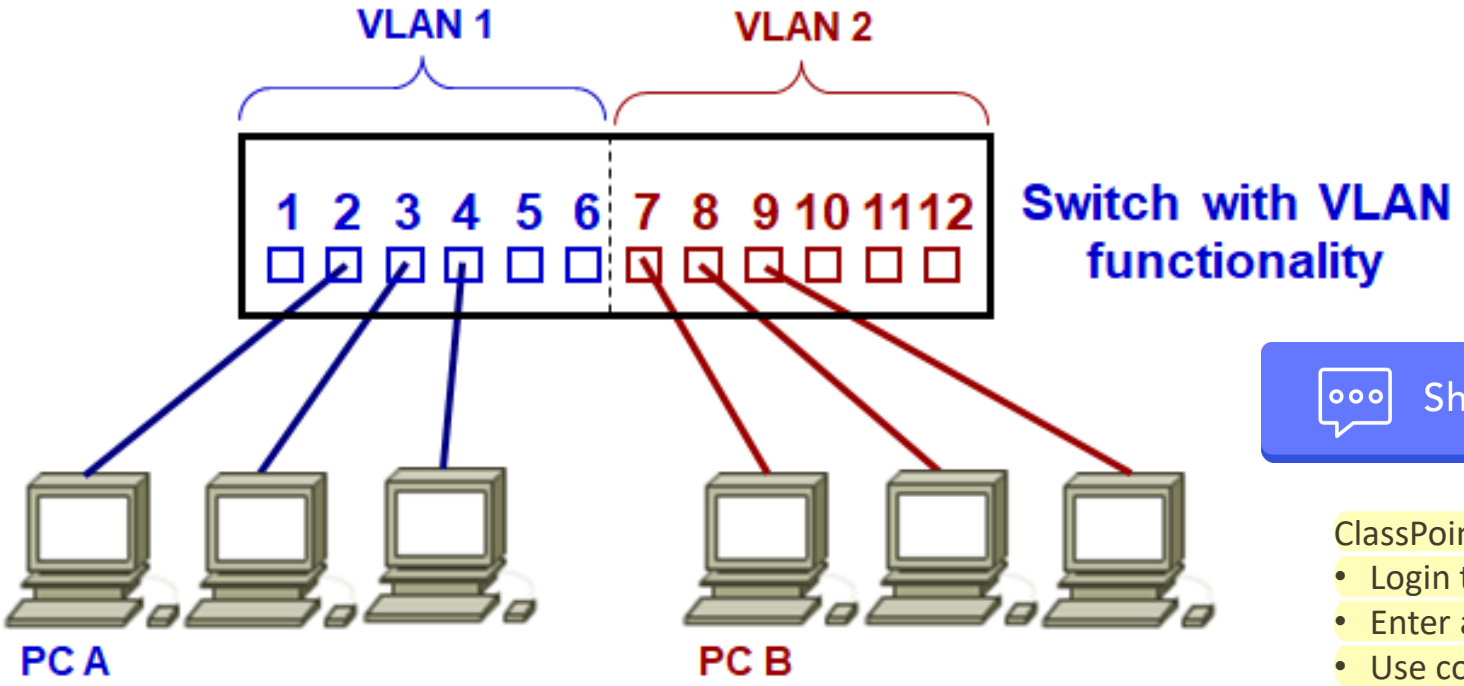
Two physical LANs with connectivity:



Concluding VLAN Concepts

Two Virtual LANs (VLANs):

- Create 2 VLANs – VLAN 1 & VLAN 2
- Configure ports 1-6 to be on VLAN 1 & ports 7-12 on VLAN 2
- 2 logical LANs = 2 VLANs = 2 networks



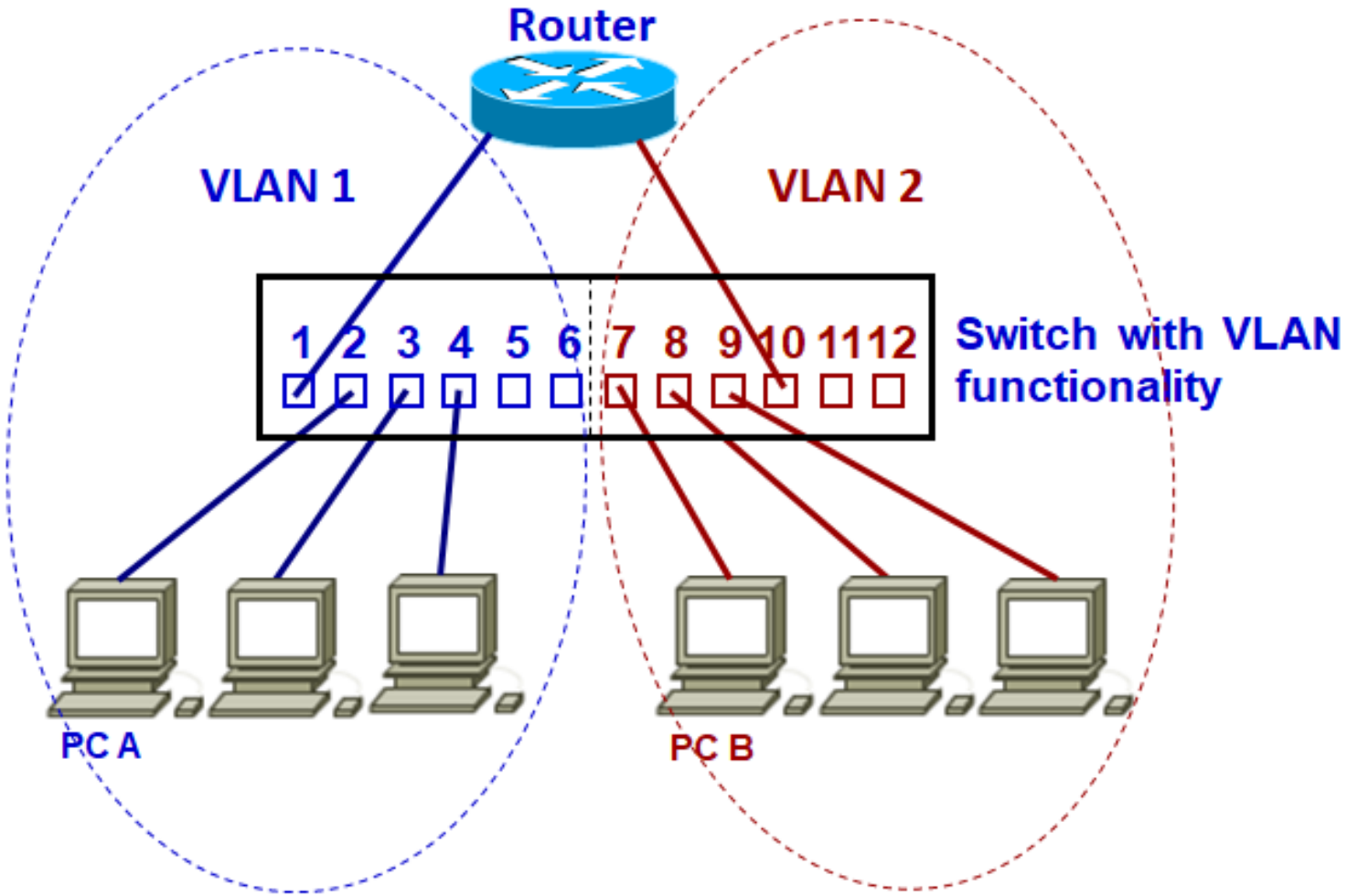
Short Answer

ClassPoint:
- Login to classpoint.app
- Enter a name
- Use code on slide

Q: Can PC A communicate with PC B? Explain your answer.

Concluding VLAN Concepts

Two VLANs with connectivity:



Virtual LANs Summary

- VLAN technology is **cost effective** and an **efficient way** of **grouping** network **users into virtual workgroups** regardless of their physical placement.
- There are various **benefits of VLANs**.
- VLANs can be used to **create broadcast domains**.
- **Routers** are used for **communication between VLANs**.
- VLANs can be created **based on ports**.

802.1Q Trunking

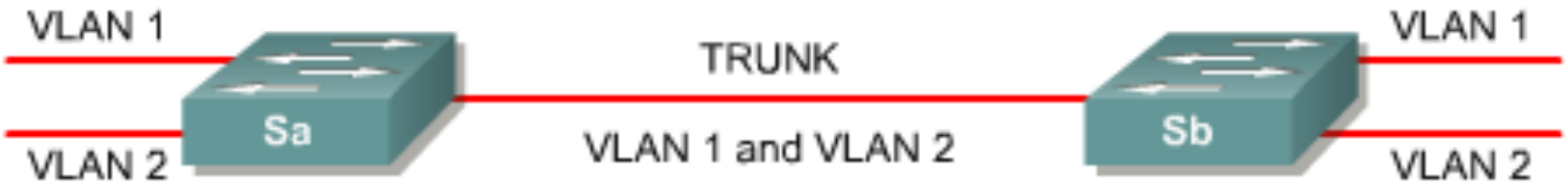
802.1Q Trunking

Objectives:

- Explain the **functions** of **VLAN trunking**
- Describe how **trunking enables the implementation of VLANs** in a large network
- Explain the difference between **physical and logical interfaces**

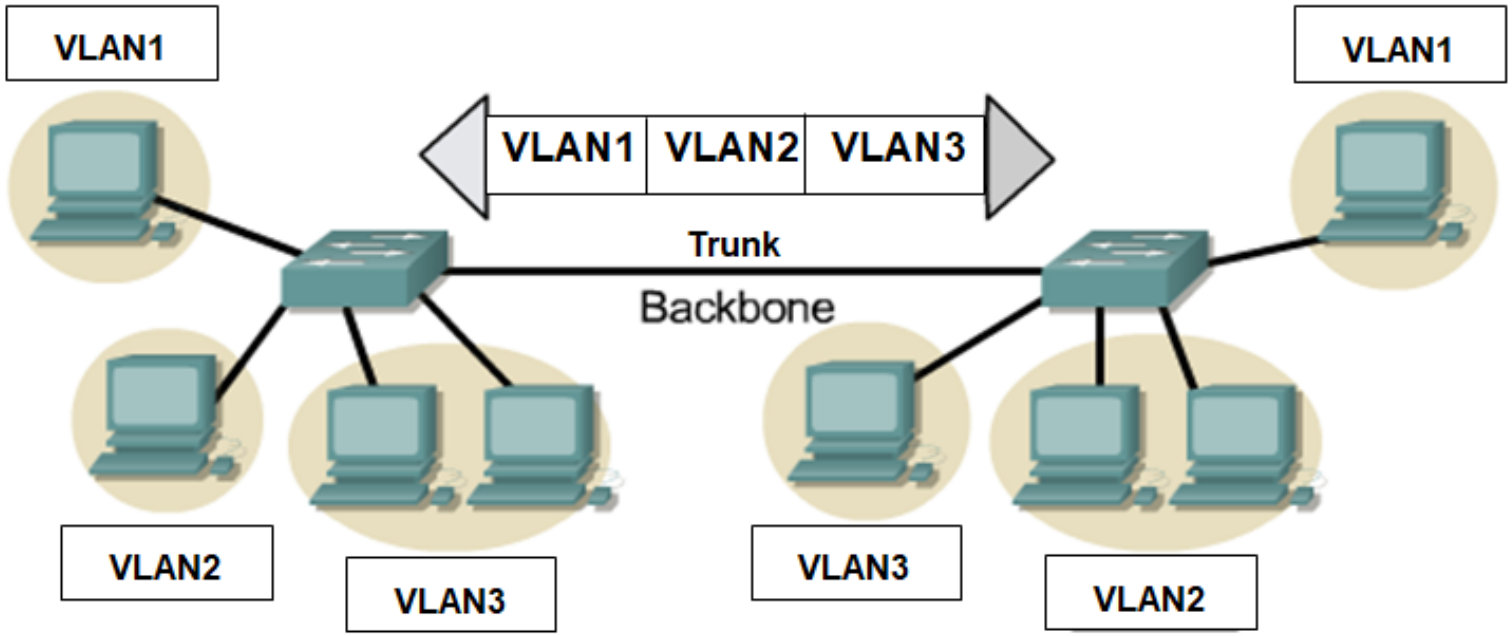
Trunking Concepts

- A **trunk** is a physical connection that carries **multiple logical links**.
- In a VLAN switching environment, a trunk is a point-to-point link that supports several VLANs.
- The purpose of a trunk is to **save ports** when creating a link between two switches that are implementing VLANs.



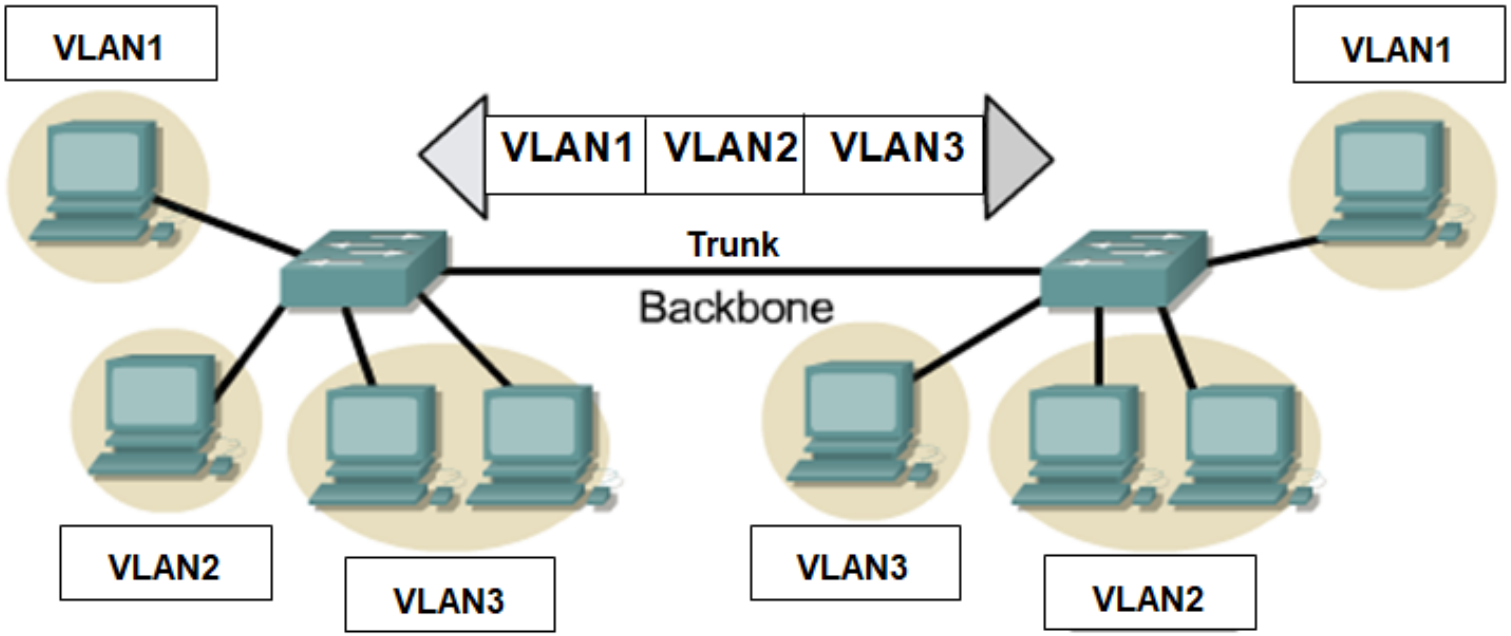
Trunking Operation

- **Trunking protocols** were created to effectively **manage** the transmission of frames from **different VLANs on a single physical link**.
- Trunking protocols **establish an agreement** for the distribution of frames according to their associated VLAN ports at both ends of the trunk.



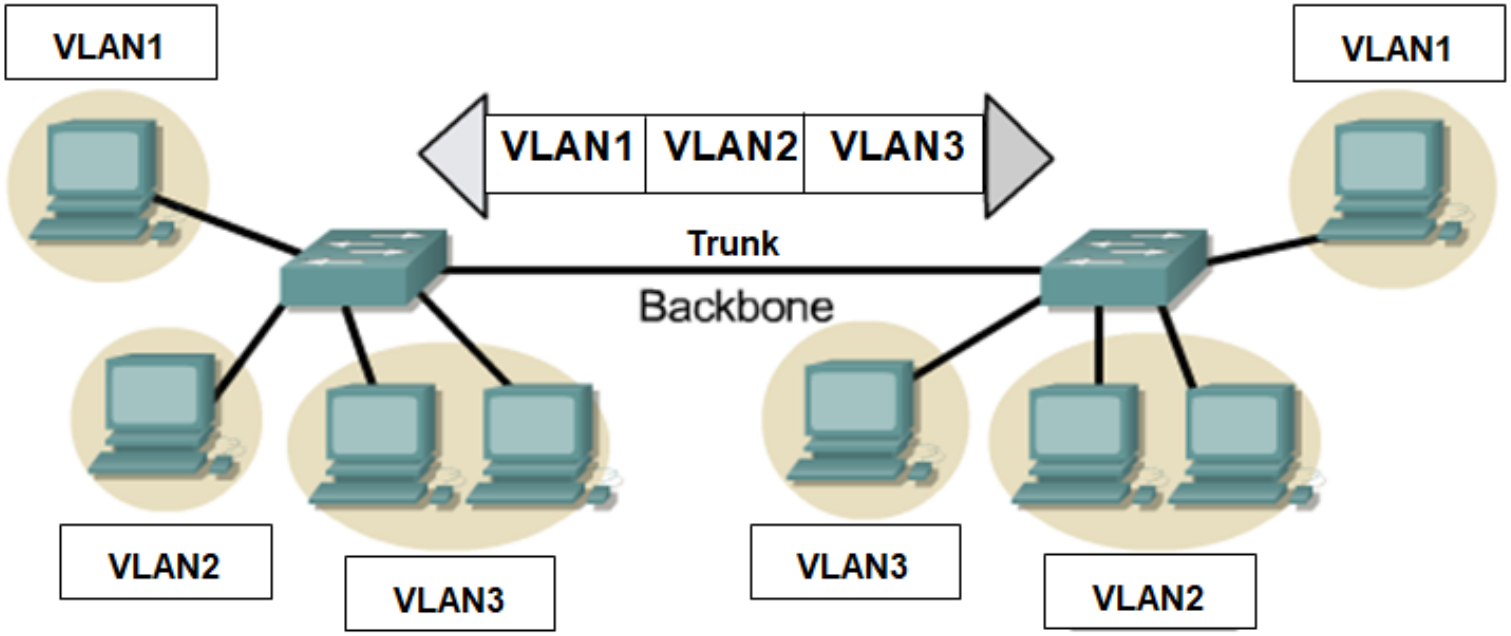
Frame Tagging

- Frame tagging is the standard **trunking mechanism** recommended by IEEE.
- In frame tagging, **each frame** sent on the trunk link is **tagged with a VLAN ID** in the **header of each frame** to identify which VLAN it belongs to.
- The tag is **added on the way out of a trunk link** and **removed at the other end** of the trunk link.



Frame Tagging

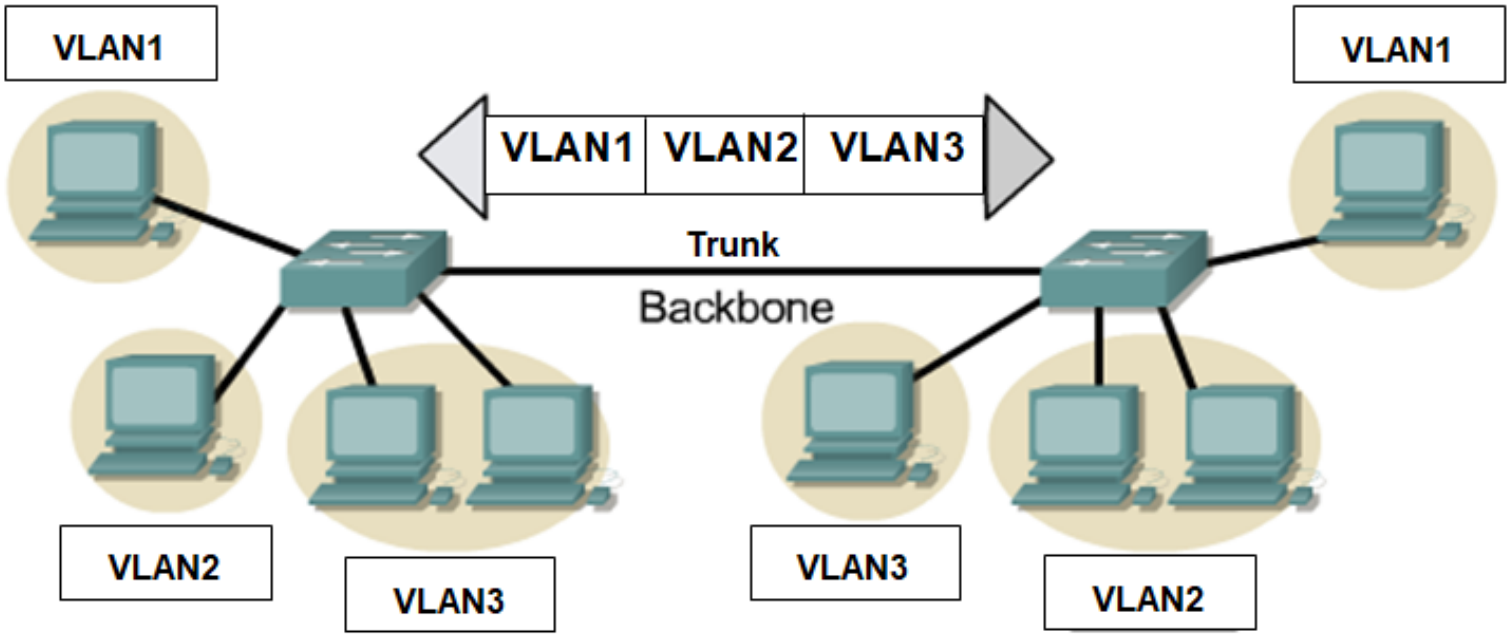
- When the frame **exits the trunk link**, the switch **examines the VLAN tag**, **removes the tag** before **forwarding** the frame **to the target end station**.



Frame Tagging

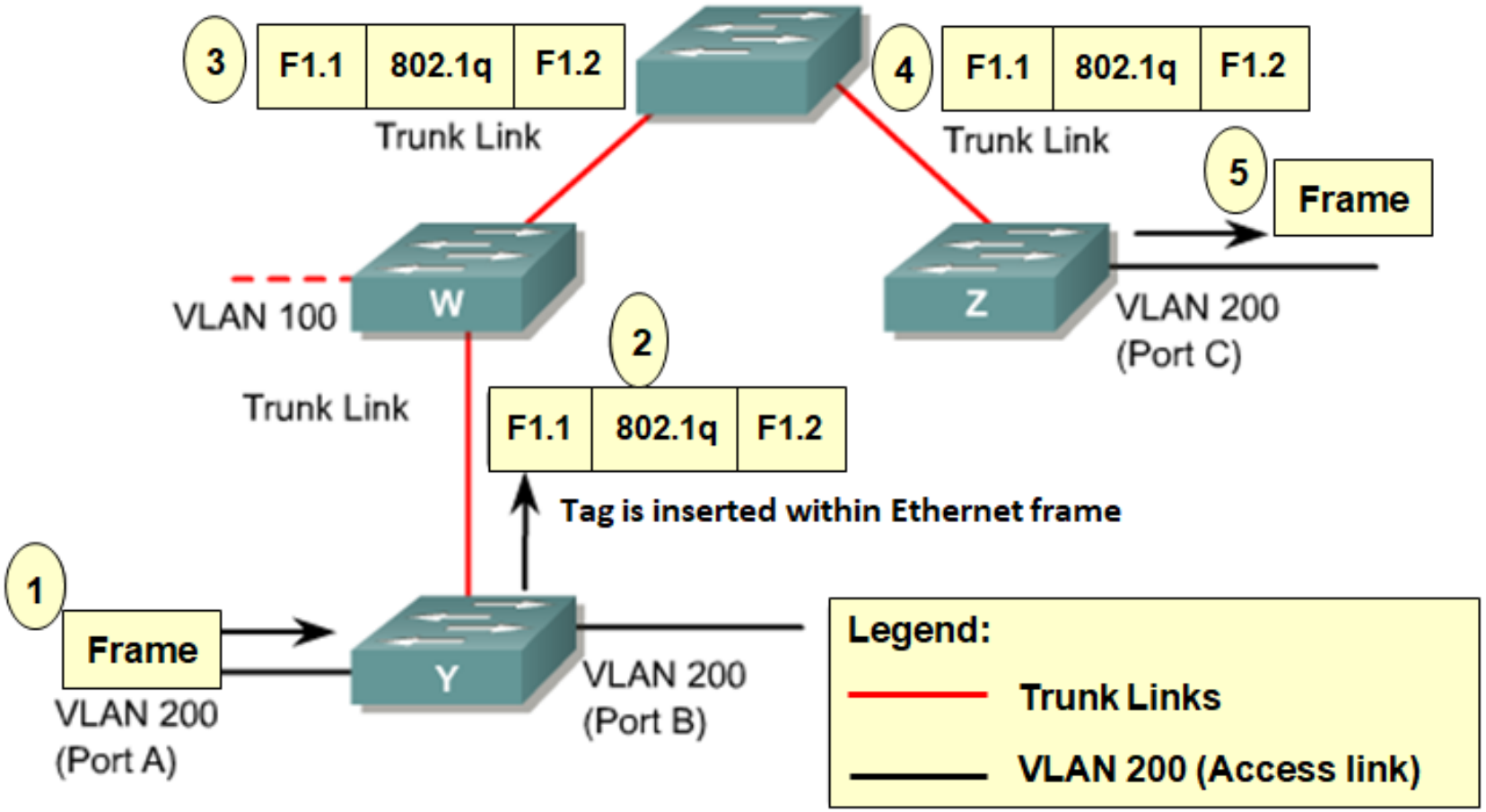
The most common tagging scheme for Ethernet s is:

- **802.1Q** – IEEE standard method for inserting VLAN membership information into Ethernet frames.



IEEE 802.1Q Tagging Protocol

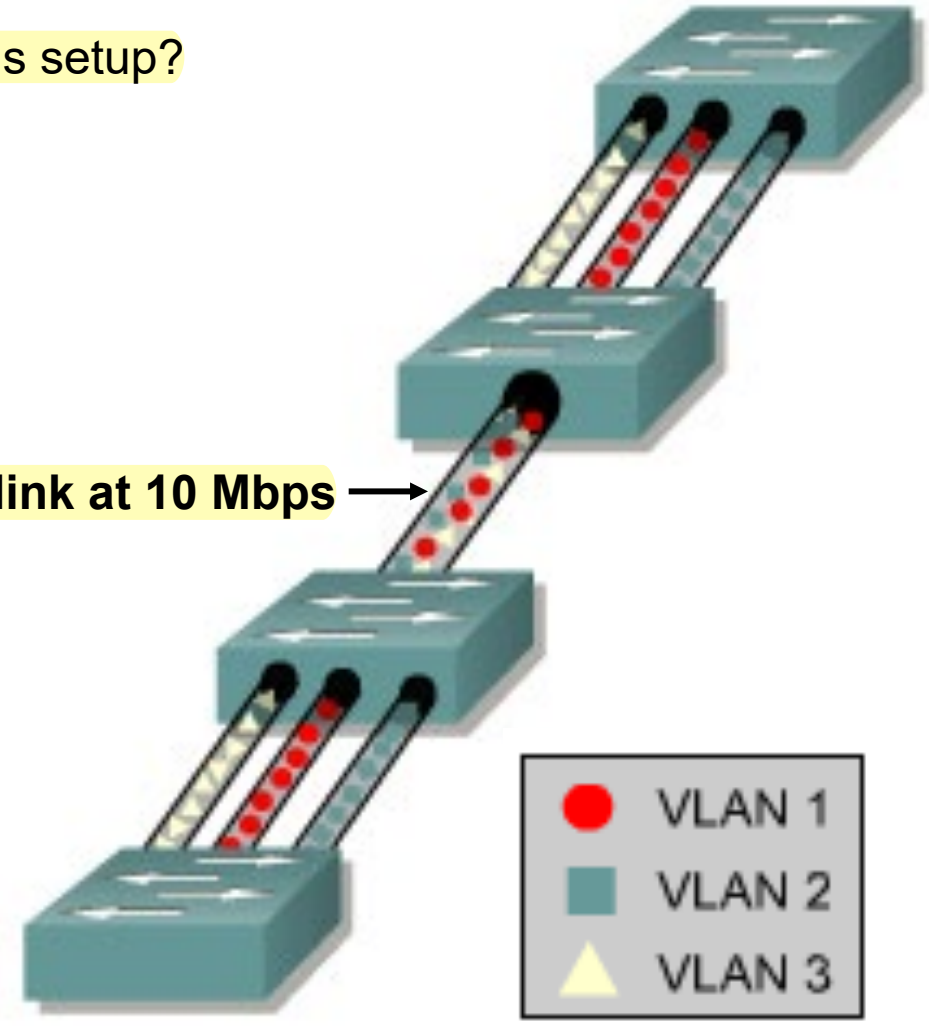
E.g. An Ethernet frame from VLAN 200 at Switch Y is destined for a device in VLAN 200 at Switch Z.



VLANs and Trunking

Q: Can trunking be implemented for this setup?

Explain your answer.



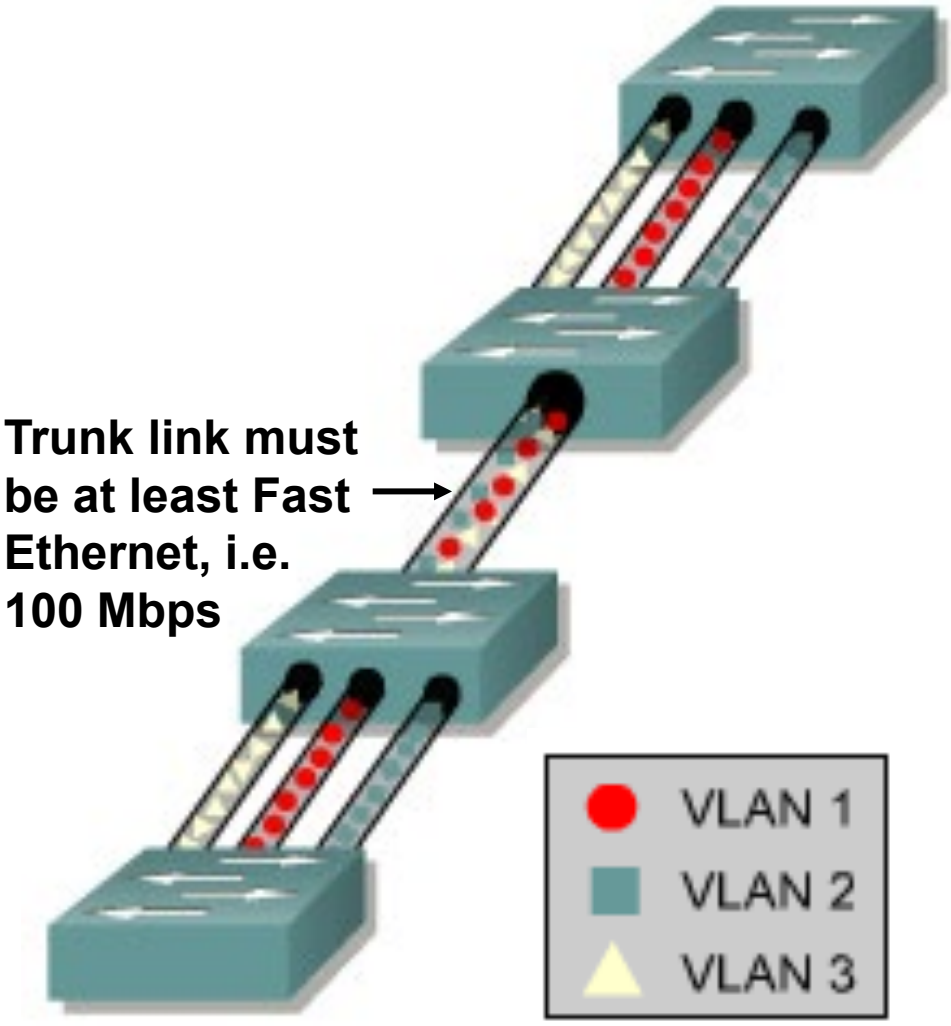
Short Answer

ClassPoint:

- Login to **classpoint.app**
- Enter a name
- Use code on slide

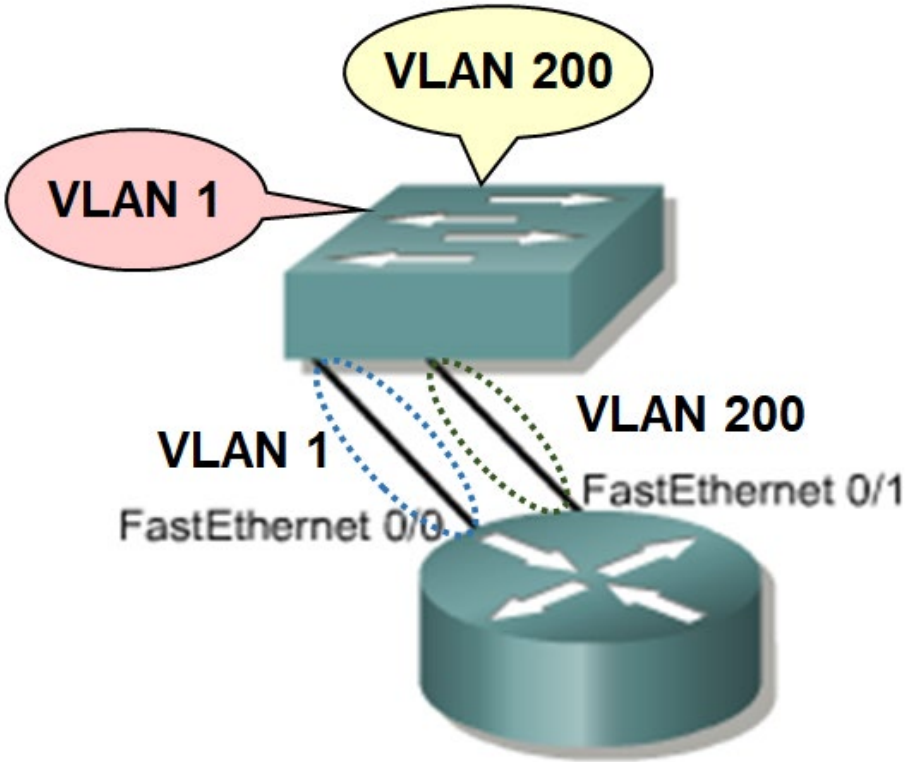
VLANs and Trunking

- A trunk link does not belong to a specific VLAN.
- The responsibility of a trunk link is to act as a **passage** for VLANs between switches and/or routers.



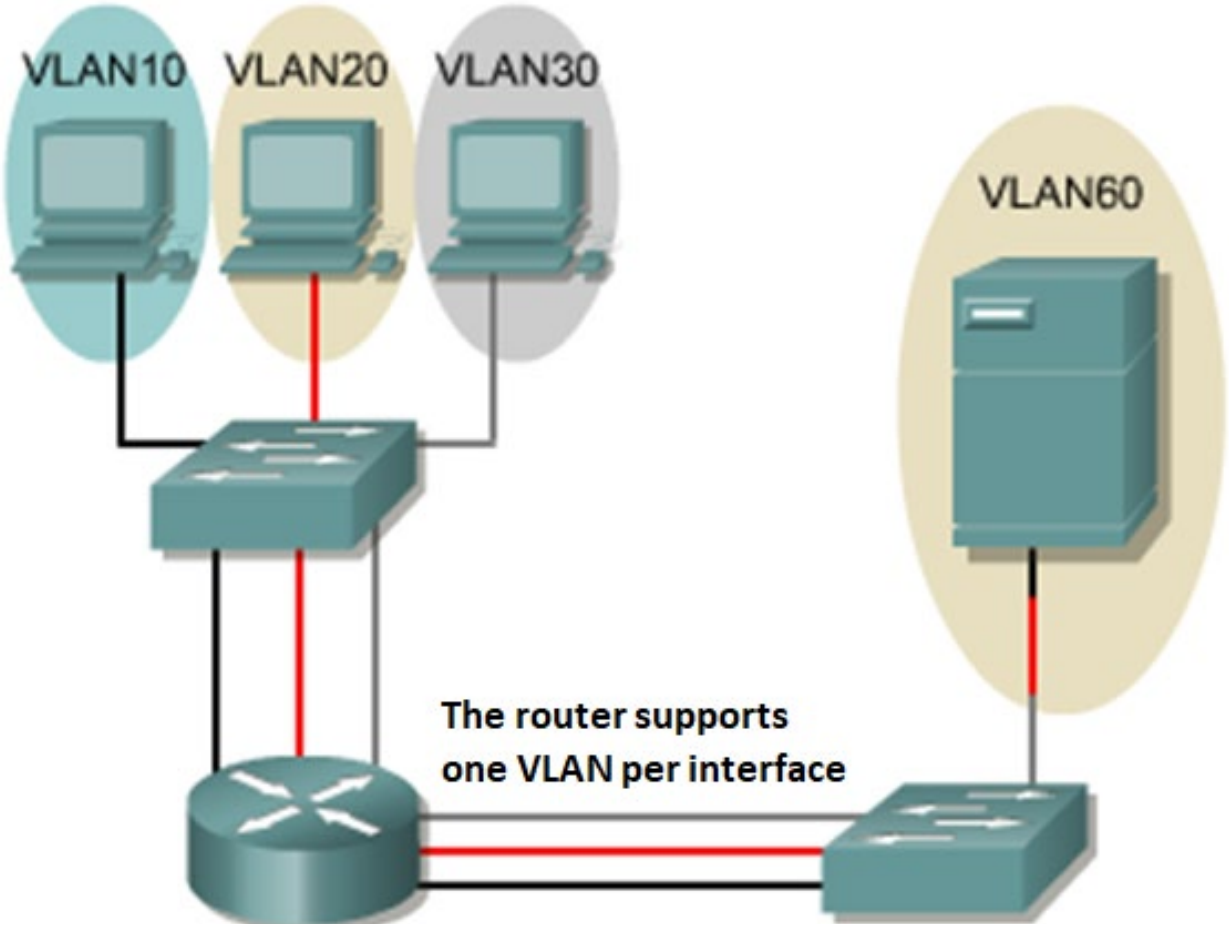
Non-Trunk VLAN Environment

- When a host in **one broadcast domain** wishes **to** communicate with a host in **another broadcast domain**, a router is needed.
- To route traffic between VLAN 1 and VLAN 200 in a **non-trunk VLAN environment**, the router must be connected to a port in VLAN 1 and a port in VLAN 200.



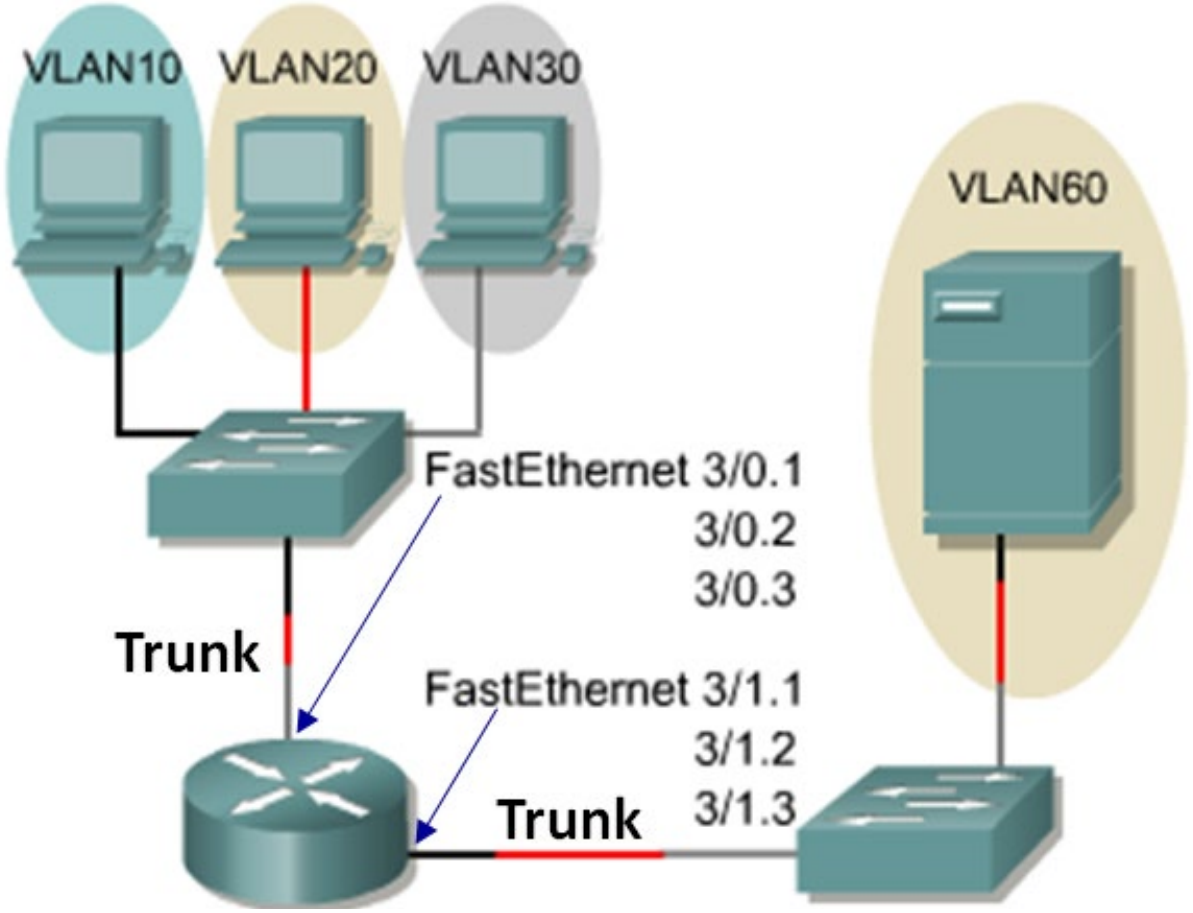
Non-Trunk VLAN Environment

- In a traditional situation, a network with 3 VLANs would require 3 physical connections between the switch and a router.



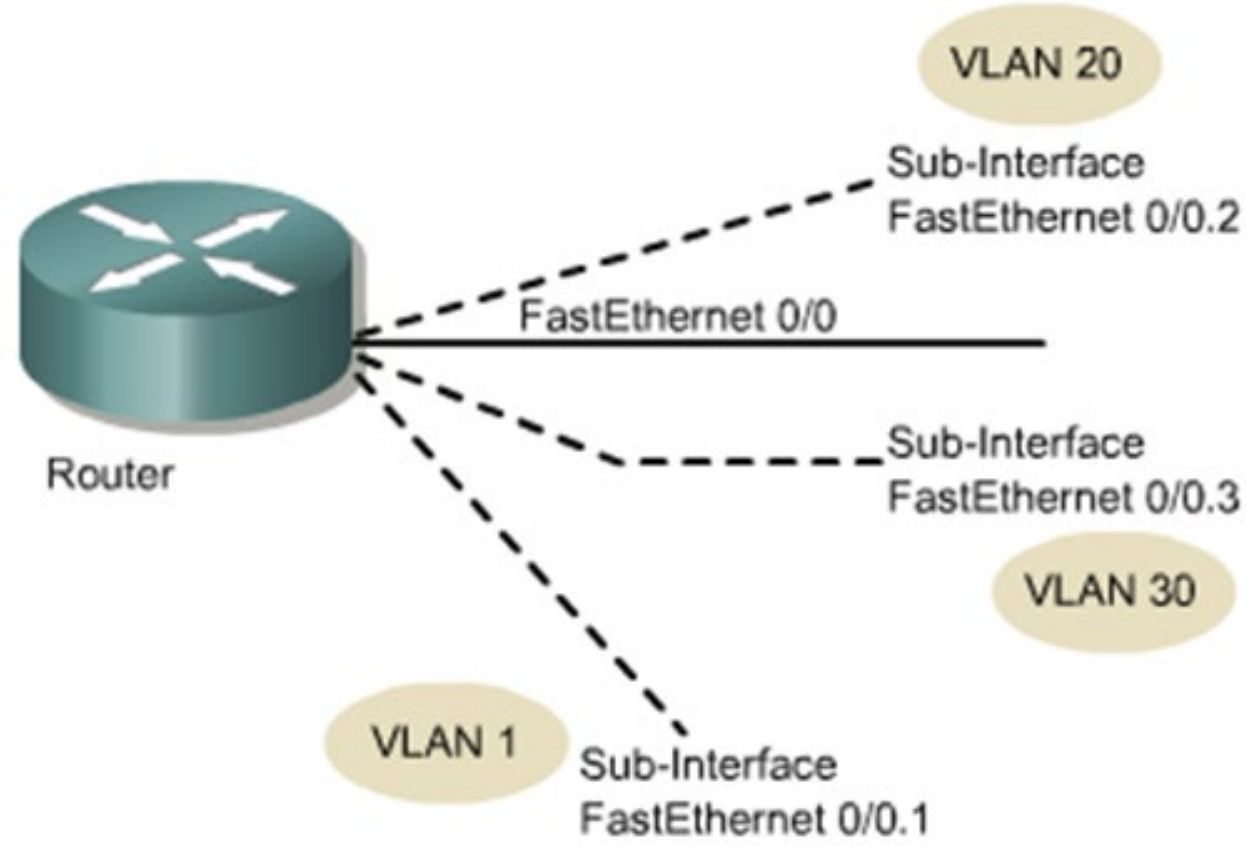
Trunked VLAN Environment

- Due to technological advances, network designers are using trunk links to connect router to switches.
- In the diagram given below, a single trunk link can support multiple VLANs.



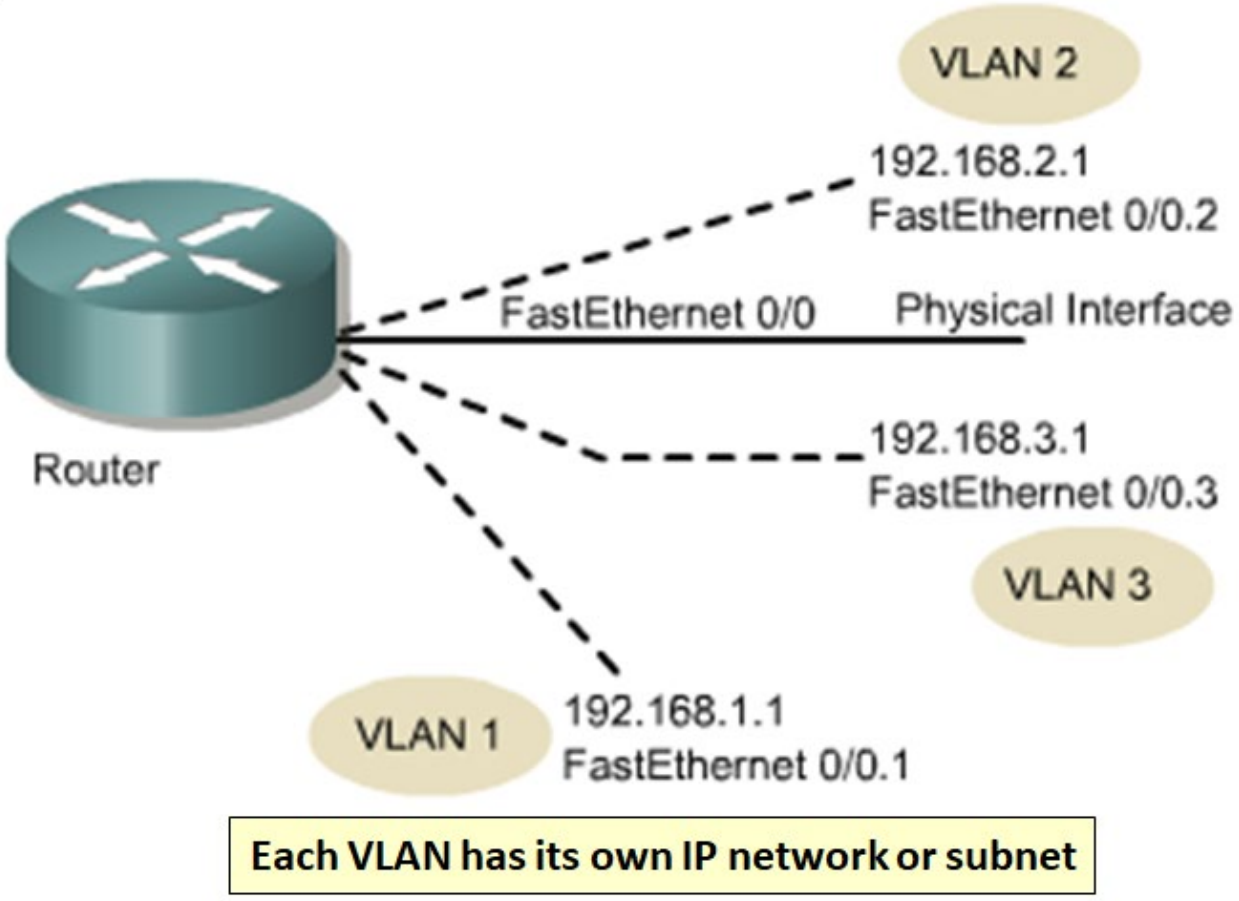
Dividing Physical Interface into Subinterfaces

- A **subinterface** is a **logical interface within a physical interface**, such as the Fast Ethernet interface on a router.
- **Multiple subinterfaces** can **exist** on **a single physical interface**.



Dividing Physical Interface into Subinterfaces

- **Each subinterface** supports one VLAN and is **assigned one IP address**.
- For **multiple devices** on the same VLAN to communicate, the IP addresses of all devices must be on the **same network** or subnetwork.



802.1Q Trunking Summary

- Trunking is implemented on a VLAN network environment to allow the **extension of VLANs across the network**.
- The **most common trunking protocol** that allows and manage the flow of different VLANs frames is **IEEE 802.1Q**.
- When an end station in one VLAN needs to communicate with an end station in another VLAN, **inter-VLAN routing** is required.

Spanning Tree Protocol (STP)

Spanning Tree Protocol (STP)

Objectives:

- Explain the **importance of Redundant Topologies**
- Explain the **problem of loops** and broadcast storms **as a result of redundant topologies**
- Explain **Spanning Tree Protocol** (STP) as a viable **solution**
- Explain **Spanning Tree Protocol operations**
- Describe the contents of the **Bridge PDU** (BPDU) and how it helps to configure the STP topology
- Describe the **role of the BPDU in recalculation** of the network during outages and failures.

Redundant Topologies

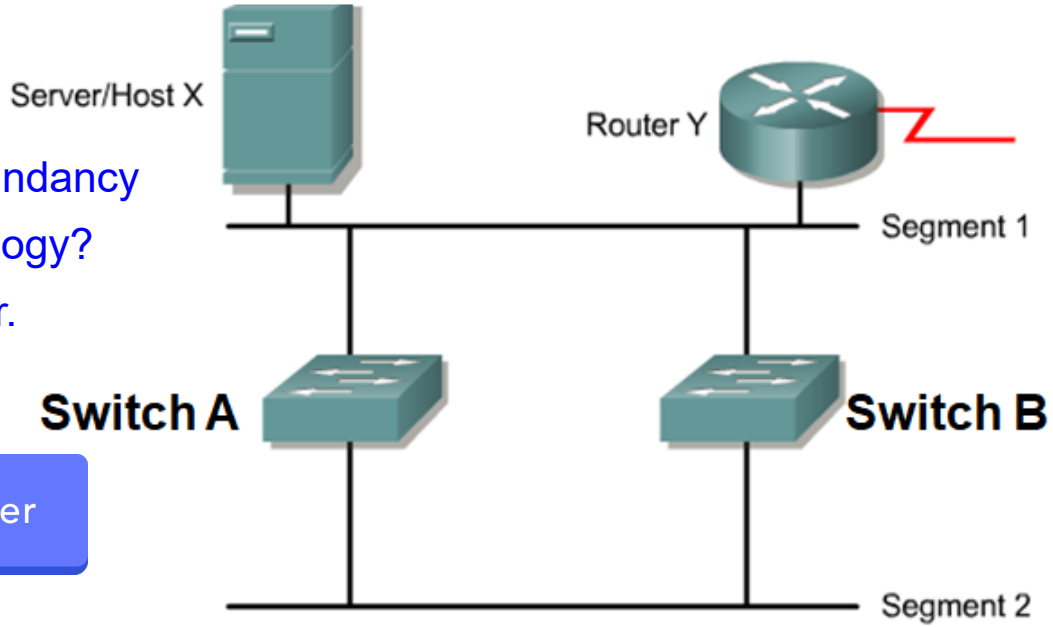
- **Redundant networking topologies** are designed to ensure that networks continue to function in the presence of a **single point of failure**.

- All networks need redundancy for **enhanced reliability**.

Simple Redundant Switch Topology

- Switch A and switch B cater to a **simple redundant topology**.
- If **Switch A fails**, frames from segment 1 can reach segment 2 **via Switch B**, and vice versus if Switch B fails.
- But if **Switch B is not installed**, then the link between segment 1 and segment 2 **completely fails** if Switch A fails.

Q: Is there any redundancy in this network topology? Explain your answer.



Short Answer

ClassPoint:
- Login to **classpoint.app**
- Enter a name
- Use code on slide

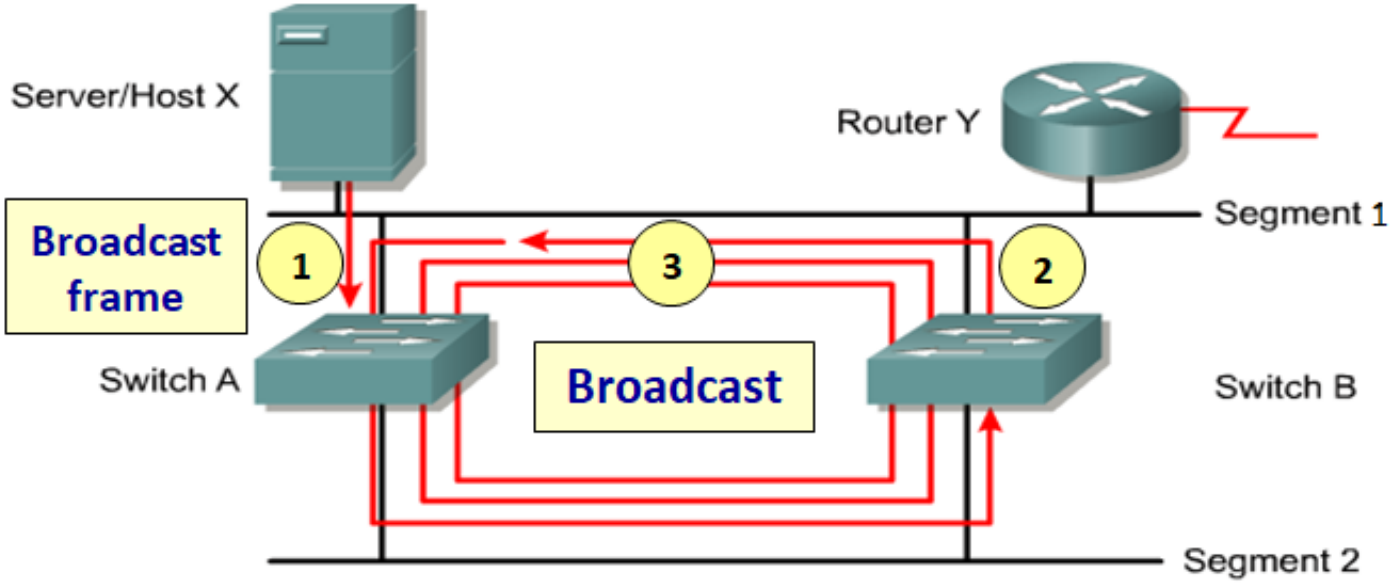
This leads to problems such as broadcast storms

Problem 1: Broadcast Storm

① Since the switch's response to a **broadcast frame** is to **forward on all its ports**, a broadcast frame from segment 1 is forwarded to segment 2 via switch A.

② As it reaches switch B, switch B forwards to segment 1.

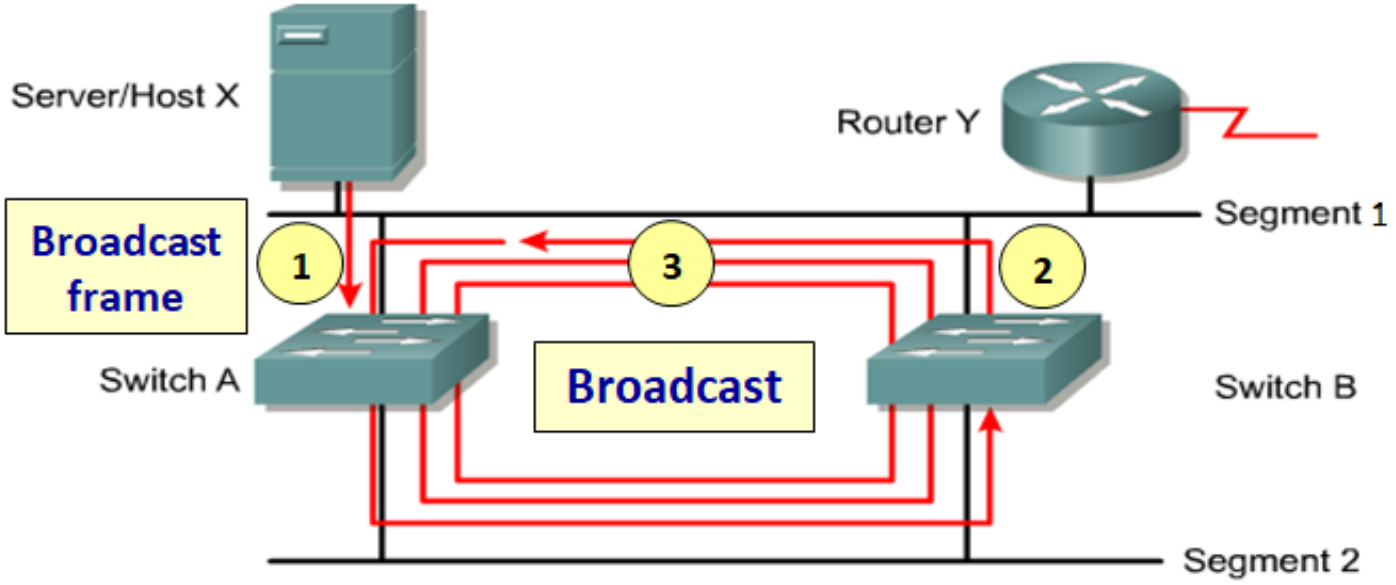
③ The **frame loops around** the links **indefinitely**. This is the **bridging loop**.



Host X sends a broadcast frame.
Switches continue to propagate broadcast over and over.

Problem 1: Broadcast Storm

- Since there is **no Time-To-Live (TTL) feature for frames**, the frame will not be discarded by any of the devices shown.
- With time, more broadcast frames are transmitted (due to ARP for example), and the **amount of broadcast** circling the network **increases** and a significant **drop in performance**.

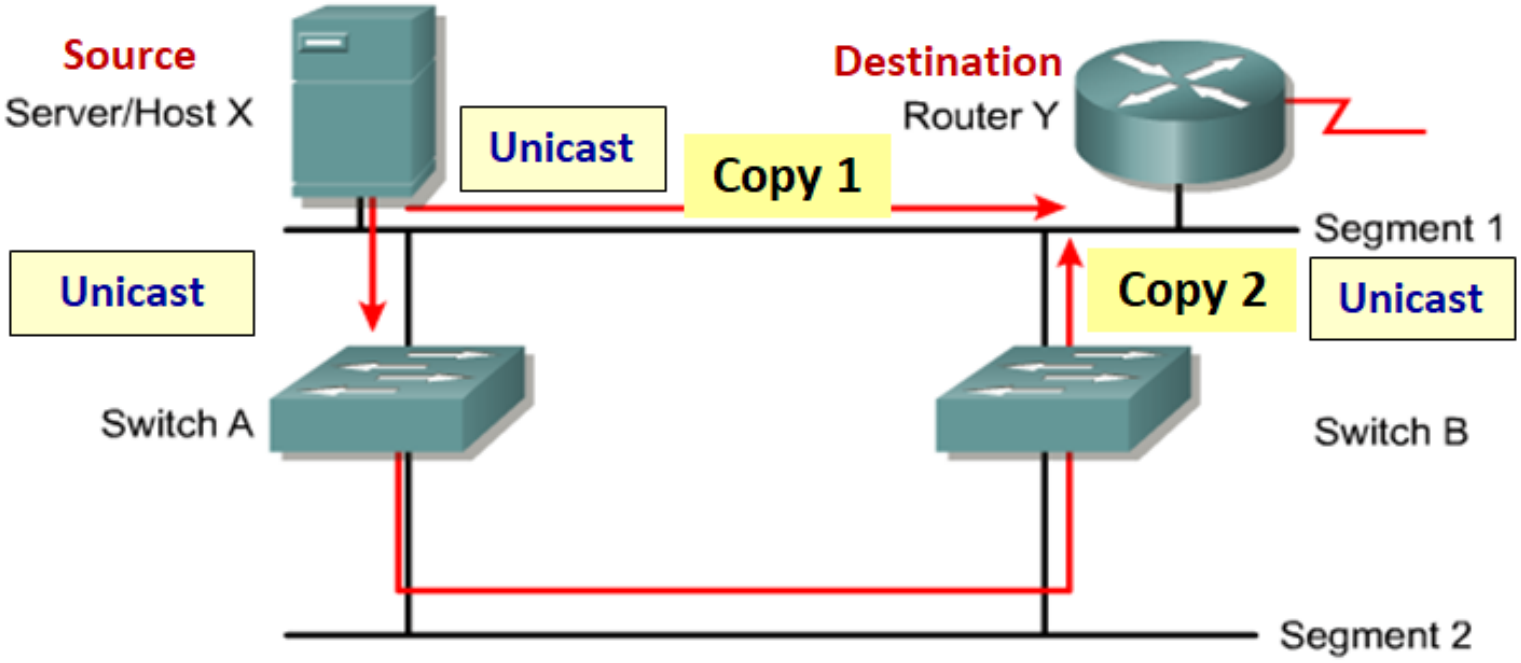


Host X sends a broadcast frame.

Switches continue to propagate broadcast over and over.

Problem 2: Multiple Frame Transmissions

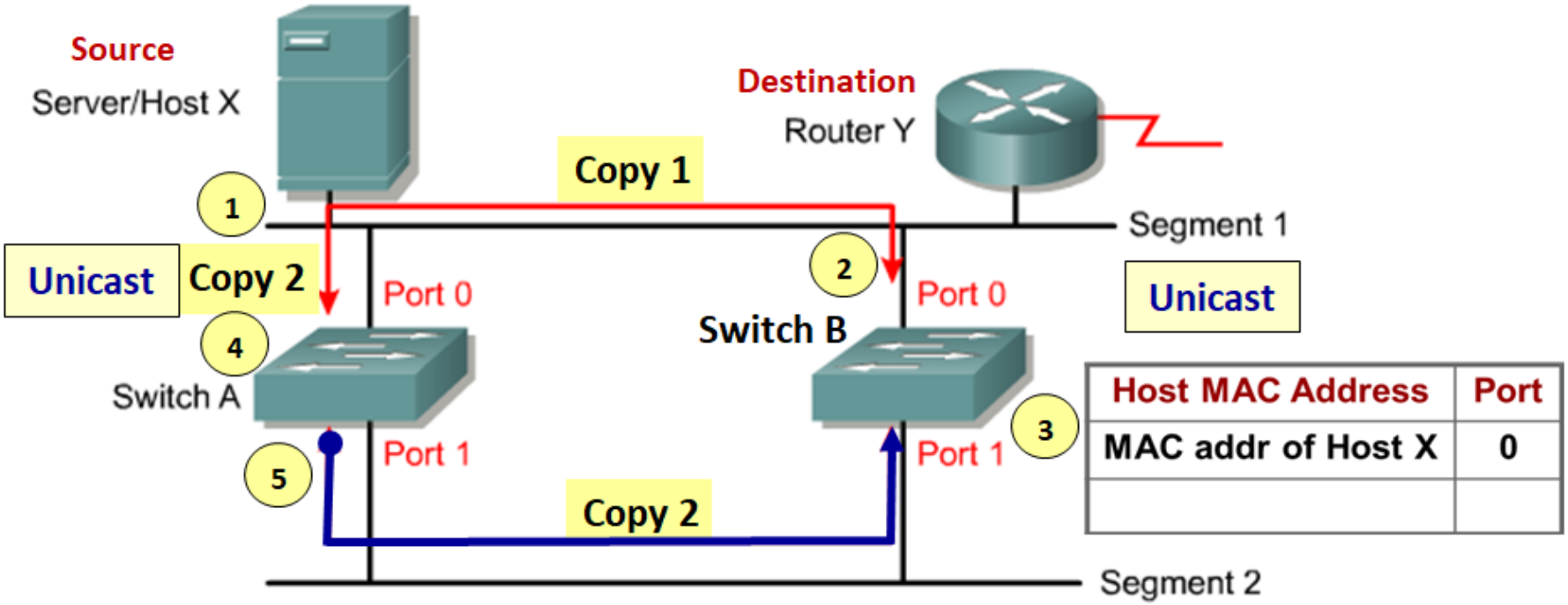
- After a long time of inactivity, the switch's MAC-address-table becomes empty.
- As **Host X transmits** a frame meant for **Router Y**, it **takes multiple paths**.
- As the **frame reaches Switch A**, it is **forwarded on all ports**.
- When the same frame reaches **Switch B**, which in turns **forwards it to Segment 1**.
- The **router** now has to **process** the frame that traversed Segment 1 only (**Copy 1**), and a second copy that traversed Switch A and Switch B (**Copy 2**) => more processing.



Problem 3: MAC Address Table Instability

Causes of MAC Address Table Instability

1. **Host X** sends out an **unicast frame**.
2. A copy (**Copy 1**) arrives at **Port 0 of Switch B**.
3. Switch B records a mapping between **MAC address of Host X and Port 0**.
4. A second copy (**Copy 2**) arrives at **Port 0 of Switch A**.
5. **Switch A forwards** the frame (**Copy 2**) **out of Port 1**.

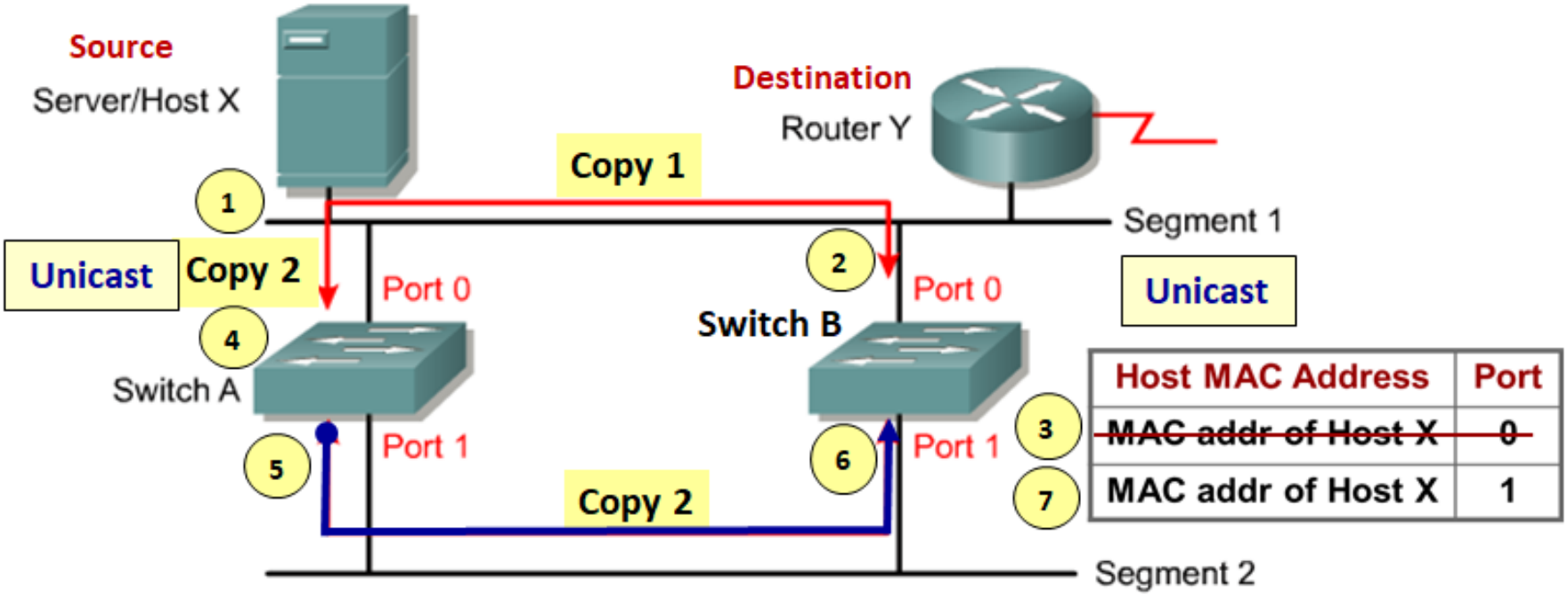


Problem 3: MAC Address Table Instability

Causes of MAC Address Table Instability

6. **Copy 2** arrives at **Port 1 of Switch B**.
7. Switch B removes the previous entry and incorrectly **maps the MAC address of Host X to Port 1**.
8. Likewise, this **incorrect mapping** also **happens to Switch A**.

In a **redundant switched network**, switches can learn the **wrong information**. A switch can learn that a MAC address is on a port when it is not.



Redundancy Problems

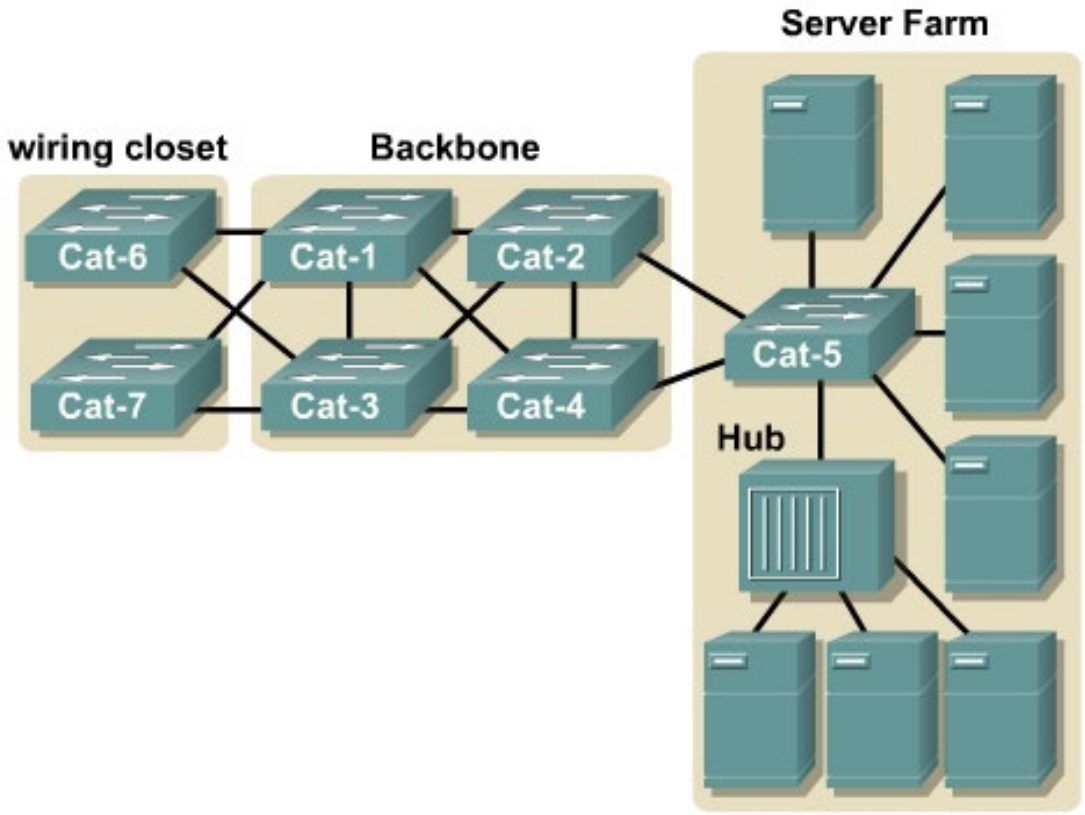
Q: Which of the 3 redundancy problems is the most severe?

A. Broadcast storm
B. Multiple Frame Transmission
C. MAC Address Table Instability

ClassPoint:
- Login to **classpoint.app**
- Enter a name
- Use code on slide

Using Bridging loops for Redundancy

- The following illustrates how a typical large enterprise would design its LAN.
- It is obvious that there **are redundant links** which can **lead to bridging loops**.

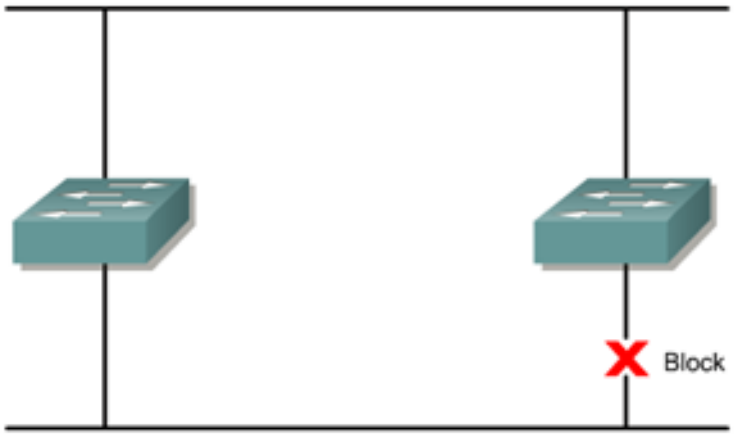


Spanning Tree Protocol (IEEE 802.1d)

Objective: To provide a **loop-free** redundant network topology based on switches.

Approach: Place one or more **redundant links on "Block" mode**.

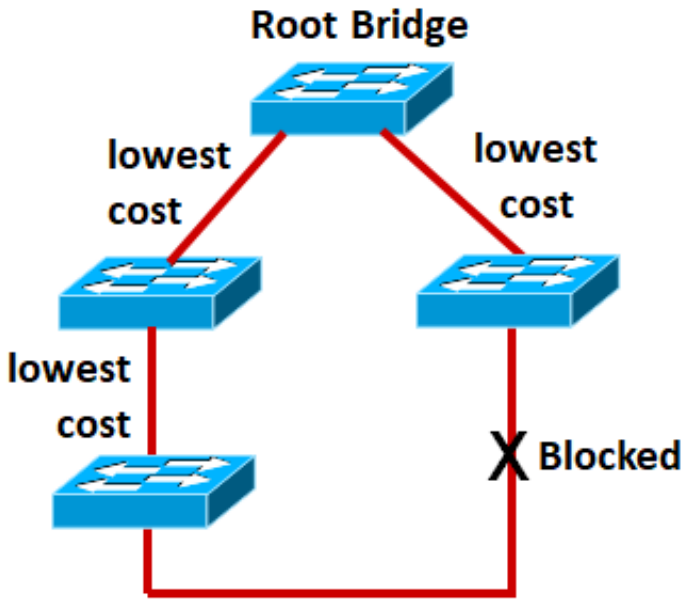
This "Block" mode does not allow frames to travel through the switch port. However, when called upon, it can change to forwarding mode.



Provides a loop-free redundant network topology by placing certain ports in the blocking state.

Spanning Tree Protocol (IEEE 802.1d)

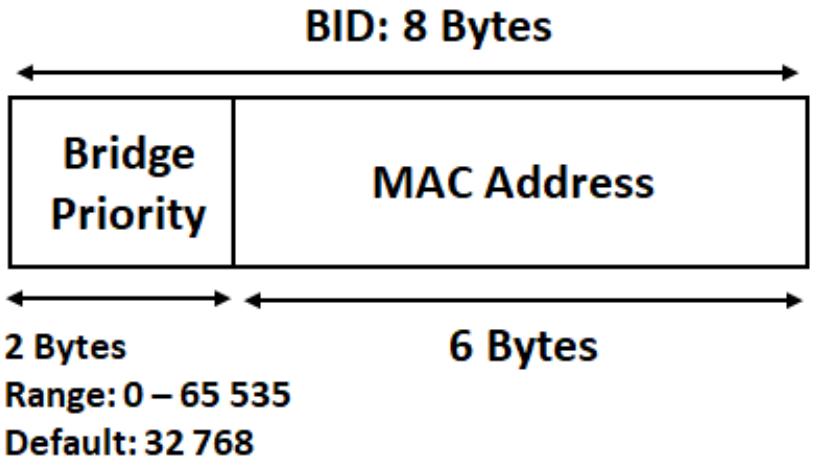
- Spanning-Tree Protocol (STP) elects a **root bridge** and constructs a topology that has the **lowest cost path** from the **root bridge to every node**.
- The resulting tree **originates** from the **root bridge**.
- **Redundant links** that are not part of the lowest cost path tree are **blocked**.
- A **loop–free topology** is possible because certain paths are blocked.

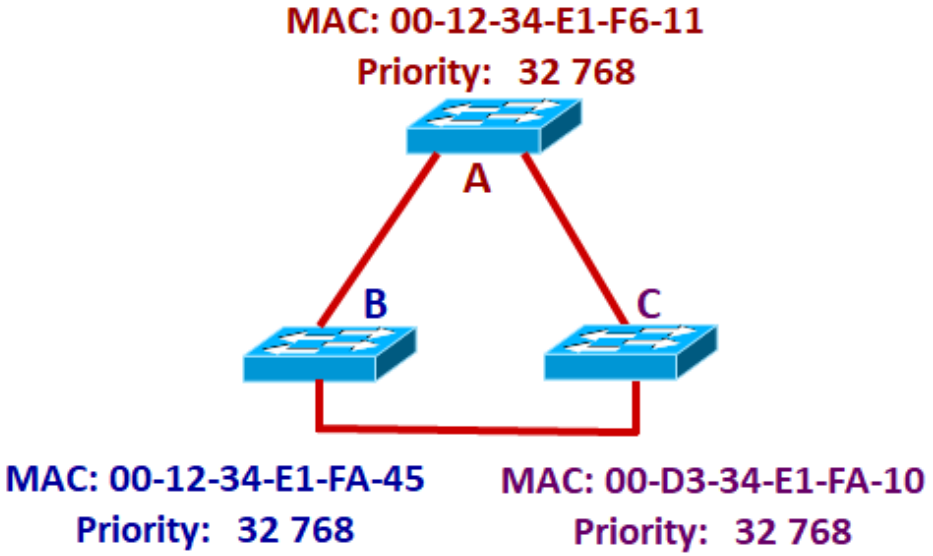


* In this course, the terms bridge and switch are synonymous.

Bridge IDs (BIDs) and Election of Root Bridge

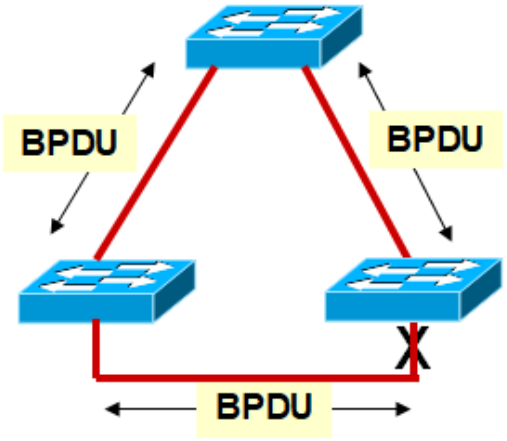
- Bridge ID (BID) is used to identify each bridge or switch.
- The **BID** consists of a **priority** value and the bridge **MAC** address.
- The default priority is 32 768. The switch or bridge that has the **lowest priority** will be elected as the **root bridge**.
- If the **priority** is the **same**, the switch with the **lowest MAC** address will be the **root bridge**.
- In the example, **Switch A** is the root bridge since it has the lowest MAC address.

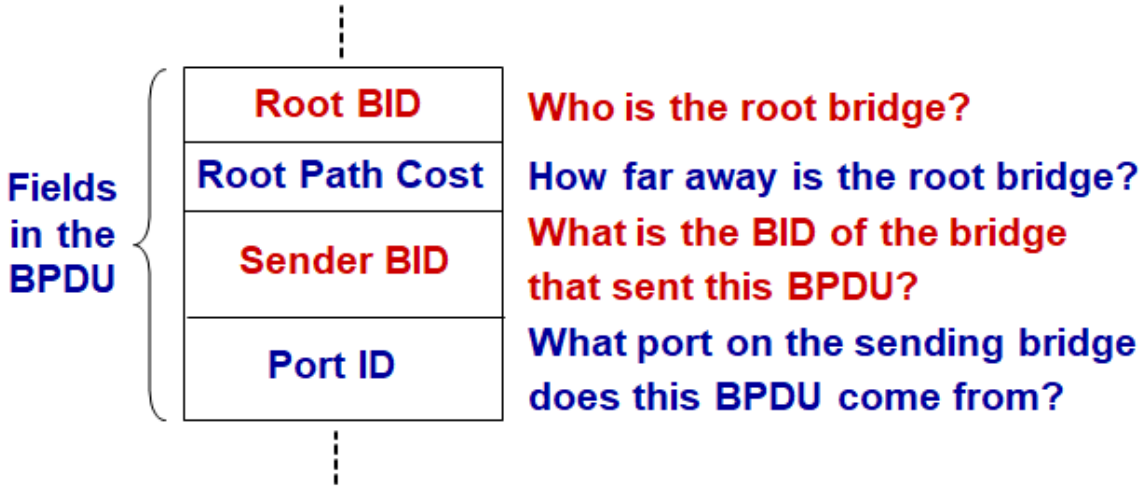




Bridge Protocol Data Unit (BPDU)

- STP requires switches to **exchange messages** to detect bridging loops.
- The messages that switches send are called **Bridge Protocol Data Units** (BPDUs). The essential information in each BPDU are given below.
- These essential information are required in **electing the root bridge** and **calculating the lowest cost** path tree.
- After the root bridge is elected and the network operates, the switches and bridges still send BPDUs which function as **keepalive messages** (meaning a BPDU sent from a switch indicates the link to that switch is still functional).





Spanning Tree Port Cost

- The spanning tree protocol (STP) uses **link speed** to calculate the cost of travelling on that specific link. The **lower the cost**, the **better the link**.
- Switches will construct a "tree" to indicate the shortest path to all segments on the network.
- The shortest path is indicated by the **lowest accumulated cost from the top of the tree** to every segment.

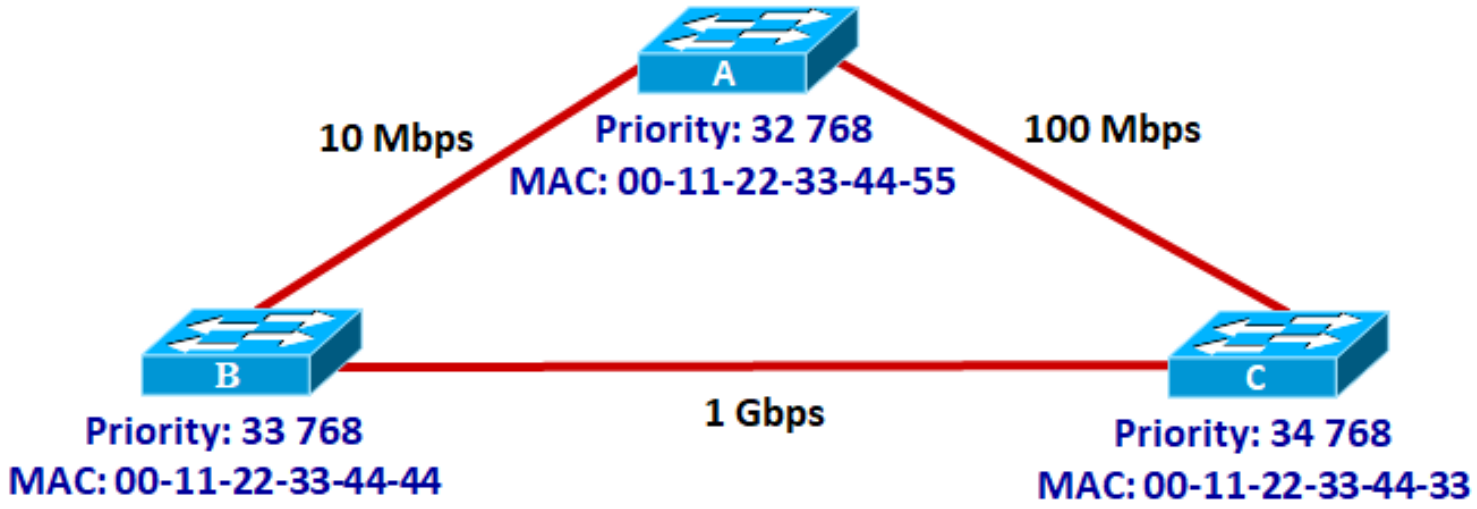
Ethernet Speed	IEEE Port Cost
10 Mbps	100
100 Mbps	19
1 Gbps	4
10 Gbps	2

Steps to obtain Spanning Tree

Example: For the switched network shown below,

(i) Determine the **root bridge**.

(ii) Assign **root ports**, **designated ports** and **non-designated ports** to the switched network.



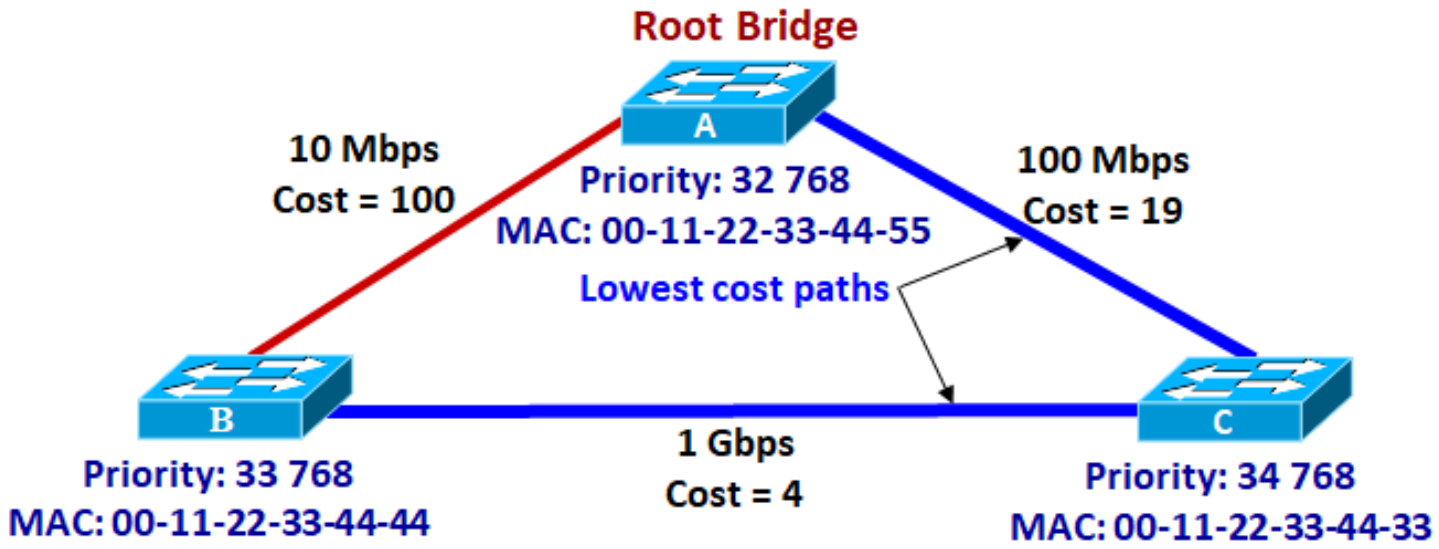
Step 1: Elect the **Root Bridge** based on **lowest priority**. If **priority is the same**, then **lowest MAC address**.

(i) **Switch A** is the **root bridge** because it has the lowest bridge priority.

Steps to obtain Spanning Tree

Step 2: Find the **lowest cost** path **from** each **non-root switch to the Root Bridge**.

- Convert the link **speed to cost**.
- **Compare** the various **cost paths** from each non-root switch to the Root and **select the lowest cost path**.



The **cost path** from a specific non-root switch to the Root is the **accumulated total path cost for all the links in the path** from the non-root switch to the Root.

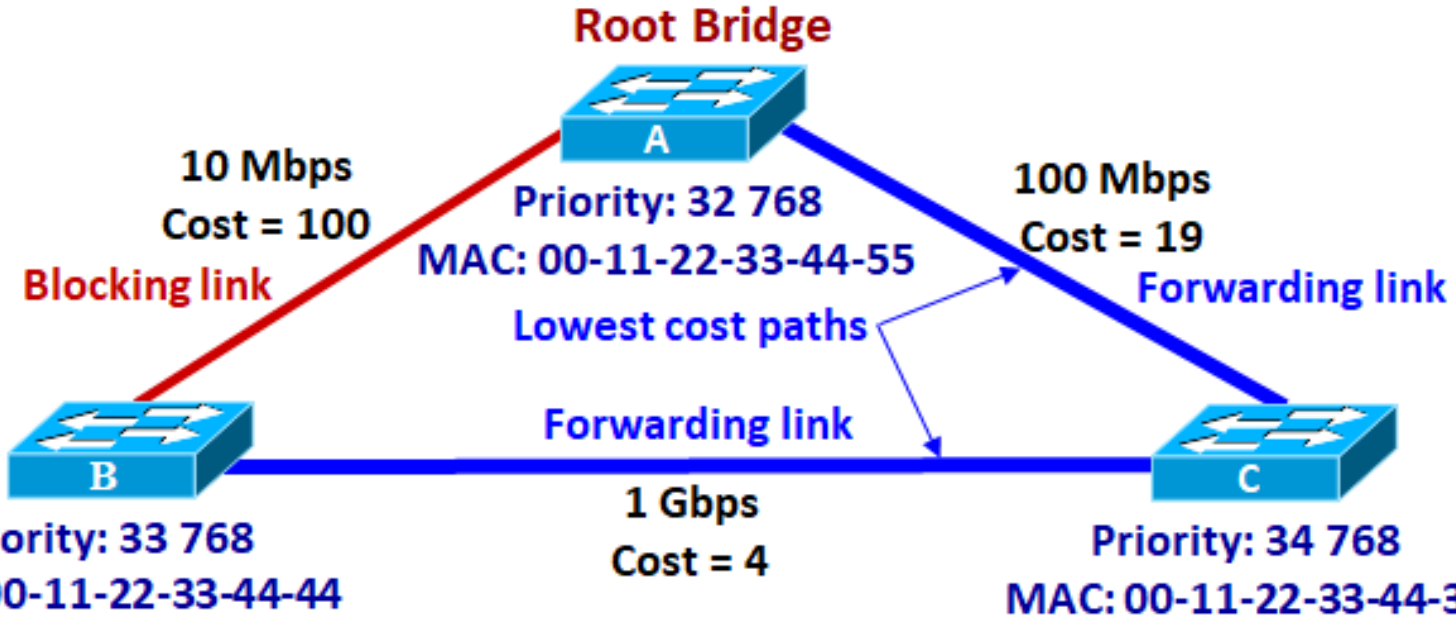
Lowest cost path from Switch B to Root = 4 + 19 = 23 (Path B→A, cost = 100, is higher)

Lowest cost path from Switch C to Root = 19 (Path C→B→A, cost = 4+100 =104, is higher)

Steps to obtain Spanning Tree

Step 2

- **Lowest cost paths** are **Forwarding links**. All others are Blocking links.
- When switches operate, they will send BPDUs which help to determine the **root bridge**, **root ports**, **designated ports** and **non-designated ports**.
- **Rules** to observe when switches elect the root bridge and ports.
  - **One root bridge per network**
  - **One root port per non-root bridge**
  - **One designated port per segment**
  - **Non-designated ports are unused**

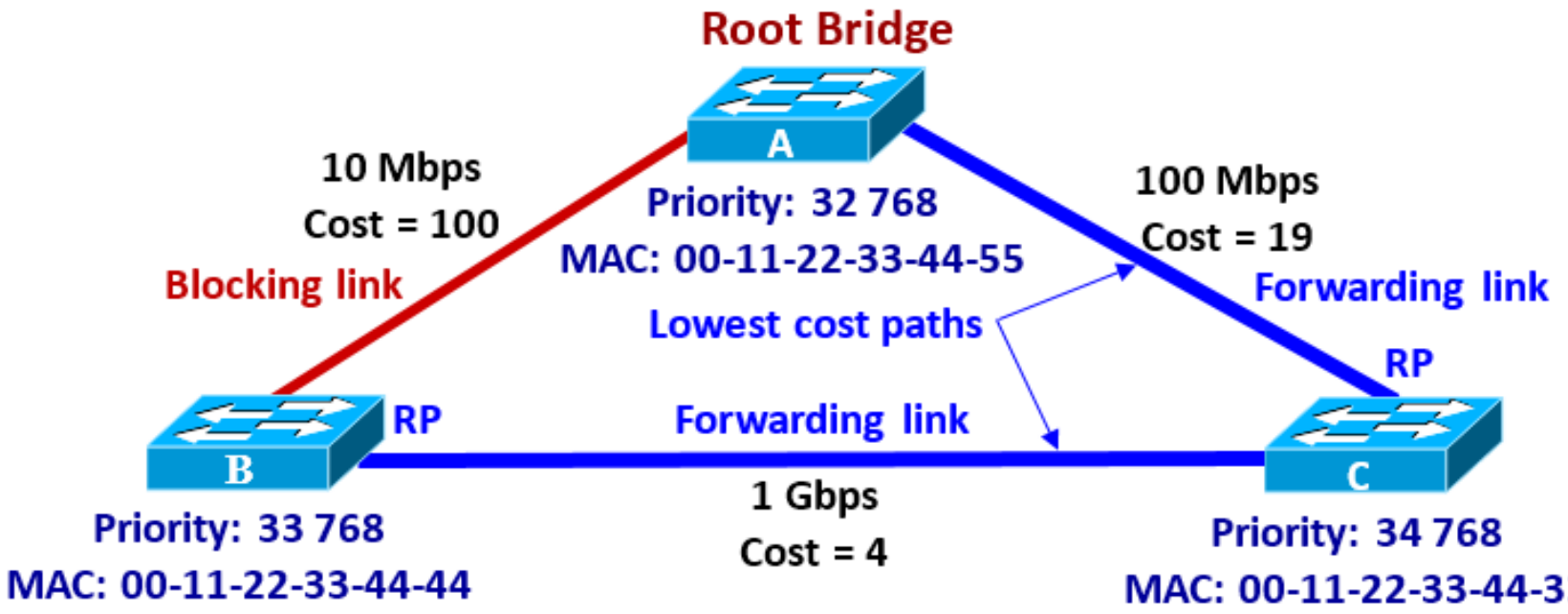


Steps to obtain Spanning Tree

Step 3: Assign **Root Ports (RP)** using the following rule:

- One root port per non-root bridge

- For each non-root bridge, there is a root port.
- The **Root port** is the **port** on the non-root bridge that **leads to the root bridge along the lowest cost path**.

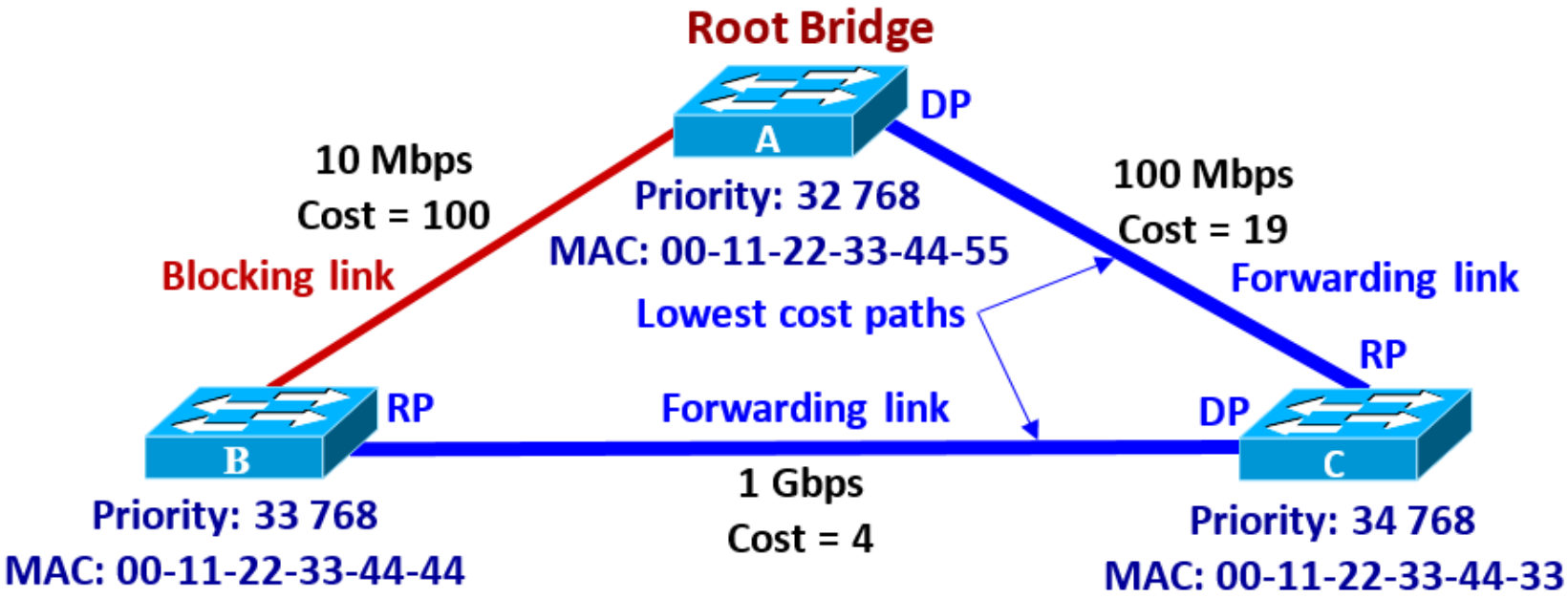


Steps to obtain Spanning Tree

Step 4: Assign **Designated Ports (DP)** using the following rule:

- One designated port per segment

- A segment is a link between switches. Each link has 2 ends.
- For **forwarding link**, the remaining **unassigned end** of the segment is the **designated port**.

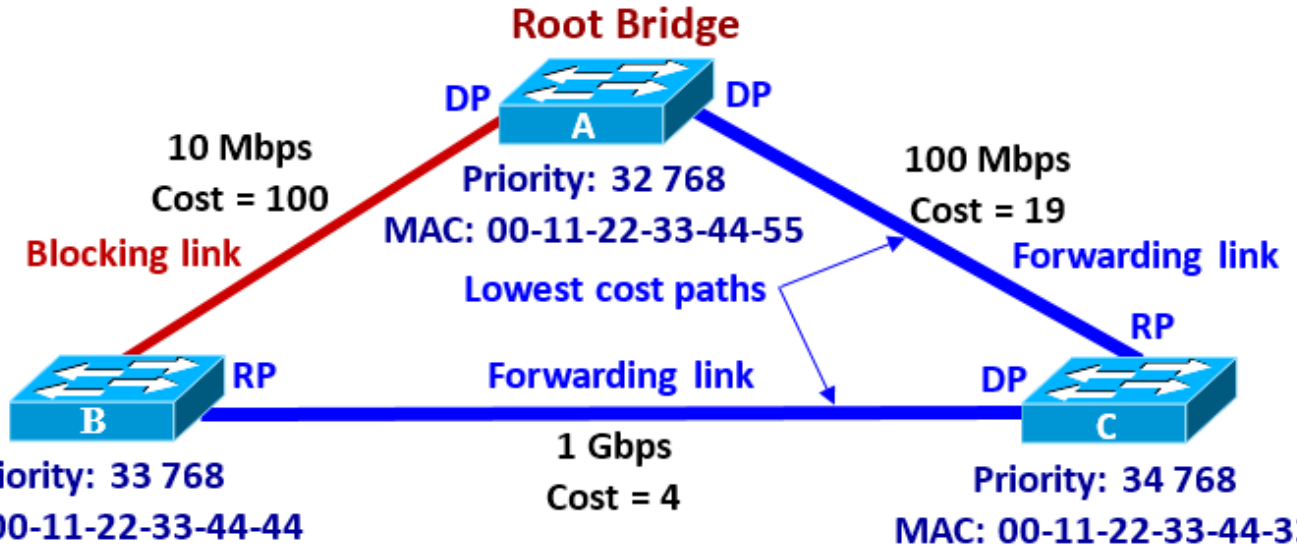


Steps to obtain Spanning Tree

Step 4: Assign **Designated Ports (DP)** using the following rule:

- One designated port per segment

- For **blocking link**, do the following to the 2 switches connected to the blocking link:
  1. Find the **lowest cost from each switch to the root**. Lowest cost from Switch B to root is 23. Likewise, lowest cost from Switch A to root is 0.
  2. The **port** attached to the switch **with the lowest cost is the designated port**. Thus, the port at Switch A is the designated port.
  3. If there is **a tie** in the lowest cost, the port attached to the switch with the **lowest Bridge ID** will be the designated port.

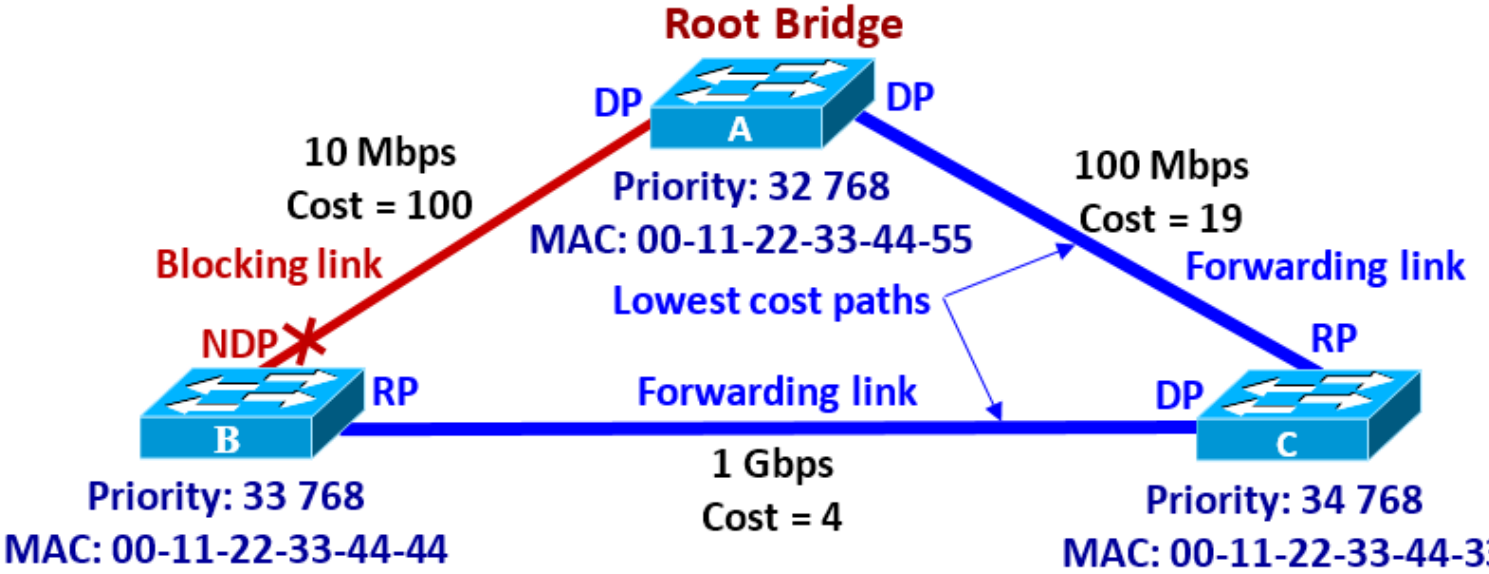


Steps to obtain Spanning Tree

Step 5: Assign **Non-Designated Ports (NDP)** using the following rule:

- Non-designated ports are unused (inactive)

- **Each blocking link** has **a non-designated port**. All remaining unassigned ports are non-designated ports.
- **Non-designated ports** are **blocking ports**, which are disabled or shutdown. It is usually indicated by an X. The LED light on the port is not lighted.
- **Root and designated ports** are **forwarding ports** and has green LED lights.
- The forwarding links form the spanning tree and will be active under normal operation.



Summary of Steps to obtain Spanning Tree

1. **Elect the Root Bridge** based on **lowest priority**. If priority is the same, then **lowest MAC address**.
2. **Find the lowest cost path** from each non-root switch to the Root Bridge. **Lowest cost paths** are **Forwarding links**. All others are Blocking links.
3. Assign **root ports**, **designated ports** and **non-designated ports** in the order given to the entire switched network using the following rules:
   - **One root port per non-root bridge**
   - **One designated port per segment**
   - **Non-designated ports are unused**

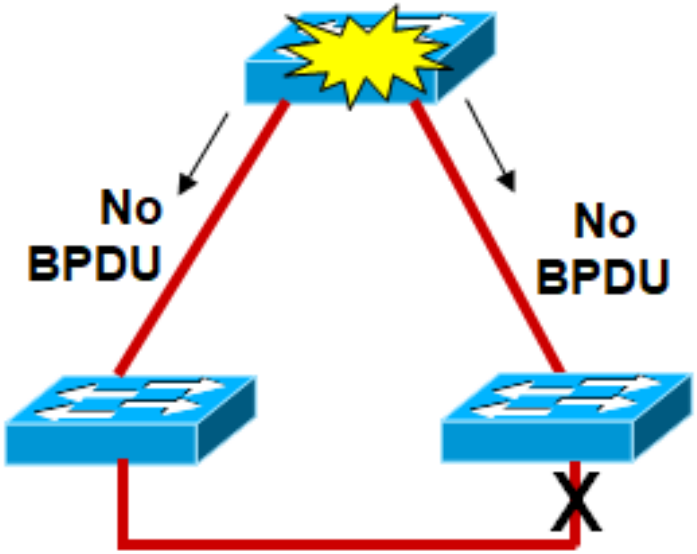
   Root and **designated** ports are **forwarding ports**.

   Non-designated ports are **blocking** ports.

The forwarding links form the spanning tree.

Spanning Tree Recalculation

- Switches **sent BPDU** (or update) to each other **every 2 sec** after the network is at a steady state.
- If switches did not receive a BPDU **after waiting for 20 sec** (10 updates), they assume a **switch or a link has failed**.
- The spanning tree protocol will isolate the failure, proceed to **re-elect the root** bridge and **recalculate the spanning tree**.



STP Summary

- **Redundant topology** helps to **solve single point of failure**.
- **Redundant topology** gives rise to **bridging loops** and sometimes **undesirable broadcast storms**.
- **Spanning Tree Protocol** (IEEE 802.1d) provides a **loop-free** switch **topology.**
- STP uses the **bridge priority** and bridge **MAC address** to **elect the root bridge**.
- It employs **Bridge Protocol Data Units** (BPDUs) to **elect a root bridge** and form a **least cost path tree**.
- Certain links can be placed on a **blocking** ("standby") mode to eliminate the loop.
- When called upon, such links can be upgraded to **forwarding** ("active") mode.
- **Loss of BPDUs** => switch or link **failure** => **recalculation of topology**.

SUSS
SINGAPORE UNIVERSITY
OF SOCIAL SCIENCES

Thank You.