UNIVERSITY of BRADFORD

Computer Communications and Networks

VLAN

Introduction

Recap of Week 1

- Switches operate as Layer 2 devices, while routers function as Layer 3 devices.

- Switches forward packets based on **MAC addresses**, whereas routers make routing decisions using **IP addresses**.

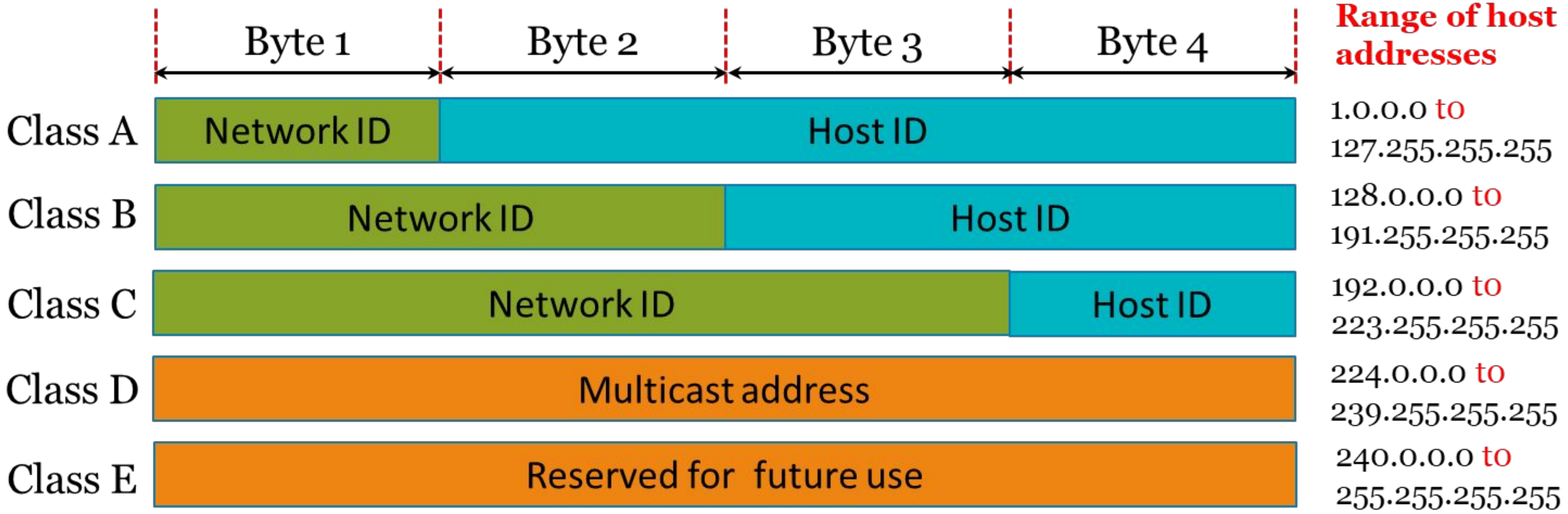
- Devices connected to a switch can communicate directly with one another under the condition that they belong to the same network.
  - **This means their Network IDs must match for communication to occur.**

This week, we will learn about **VLANs (Virtual Local Area Networks)**, which group devices logically within a network to improve performance, enhance security, and simplify management.

IP Addresses

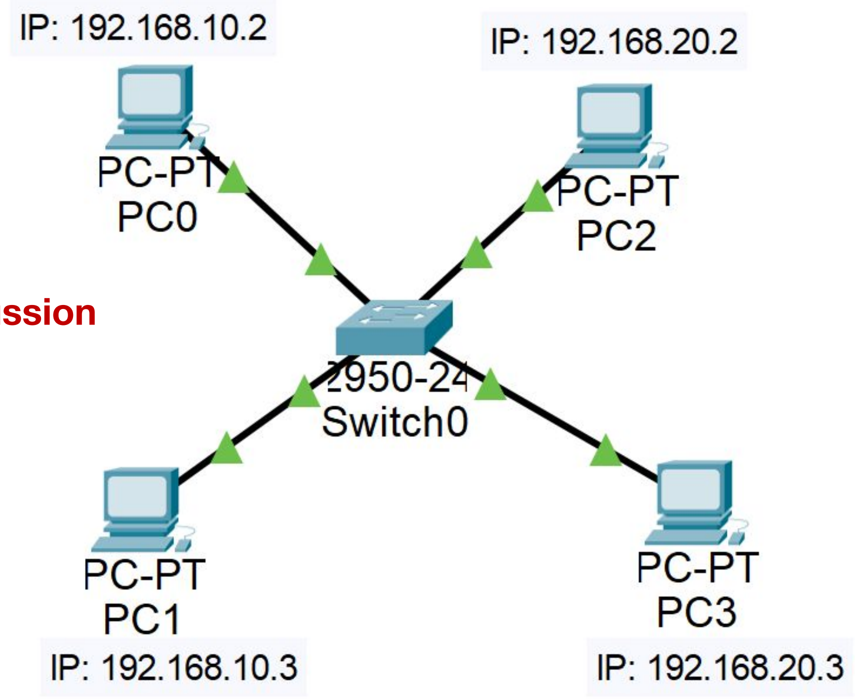
How can you determine if two computers are part of the same network?

- By examining their **Network IDs**
- In Classful IP addressing, the Network ID is identified as follows:
  - Class A: First octet (number) of the IP address
  - Class B: First two octets of the IP address
  - Class C: First three octets of the IP address



Scenario Without VLANs

- Before starting with the VLAN concept, first create the following network structure.
- Assign the IP addresses to the PCs.
- It is clear that:
  - PCs belong to two different networks.
    - **Task: answer the question posted in canvas discussion**
  - PC0 and PC1 are part of the same network.
  - PC2 and PC3 are part of the same network.



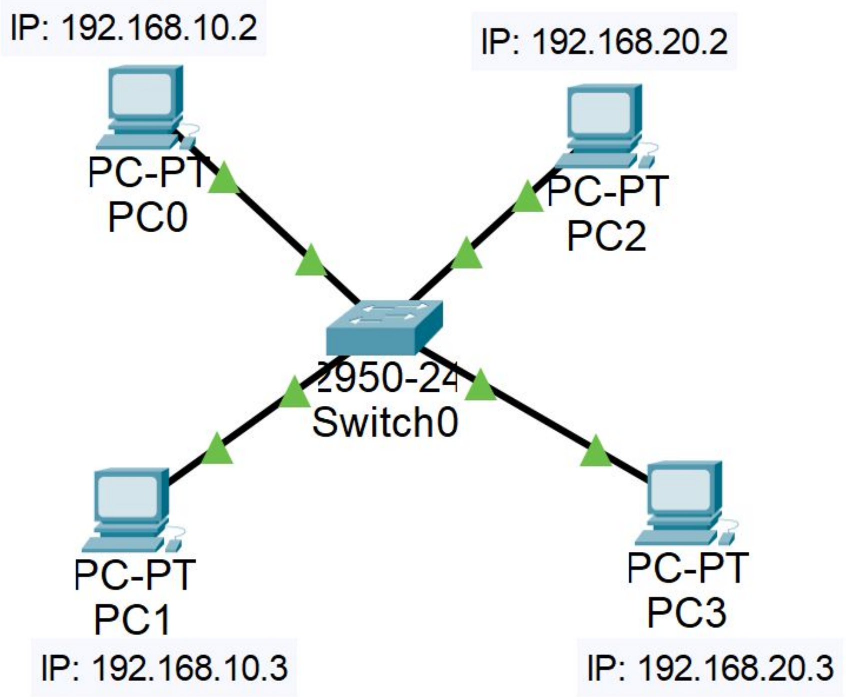
- Now, try the following:
- Send a message from PC1 to PC0.
  - It will be **successful**.
- Send a message from PC2 to PC1.
  - It will be **unsuccessful**.

Regardless of the outcome, have you observed anything noteworthy?

Scenario Without VLANs

- When all four PCs are connected to the same switch, the switch treats them as part of a single broadcast domain by default.

- Even though PC 0/1 and PC 2/3 are configured on different IP networks, they are still part of the same Layer 2 network (broadcast domain).
- As a result:
  - Broadcast traffic from one network (192.168.10.0/24) will reach the PCs in the other network (192.168.20.0/24).
  - This is unnecessary and wastes network bandwidth, particularly in larger networks.



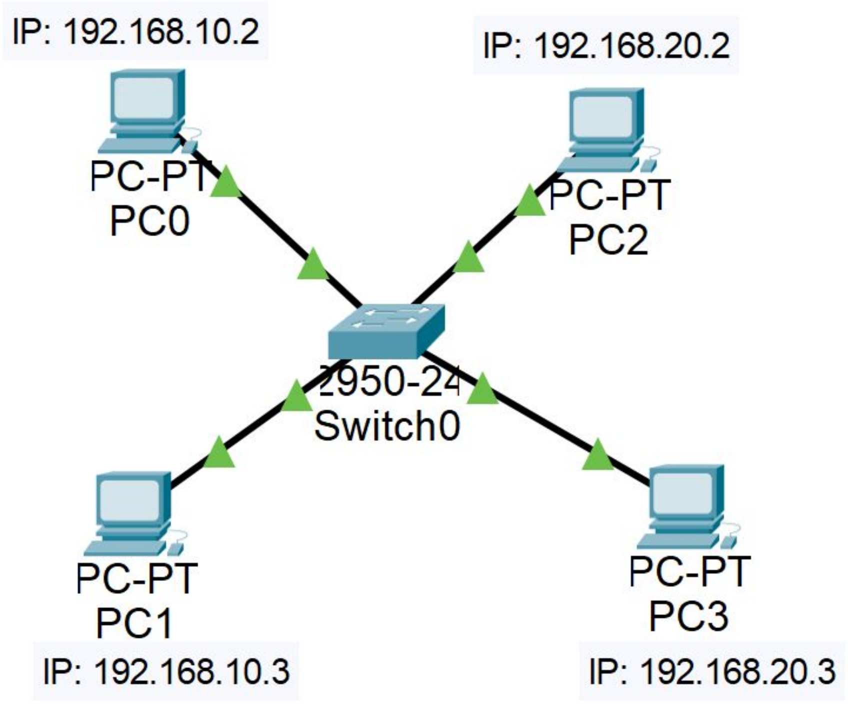
Benefits of Creating VLANs in This Scenario

- By placing PCs 0/1 in one VLAN and PCs 2/3 in another VLAN, you can segment the broadcast domains. This prevents broadcast traffic from one network from reaching the other.

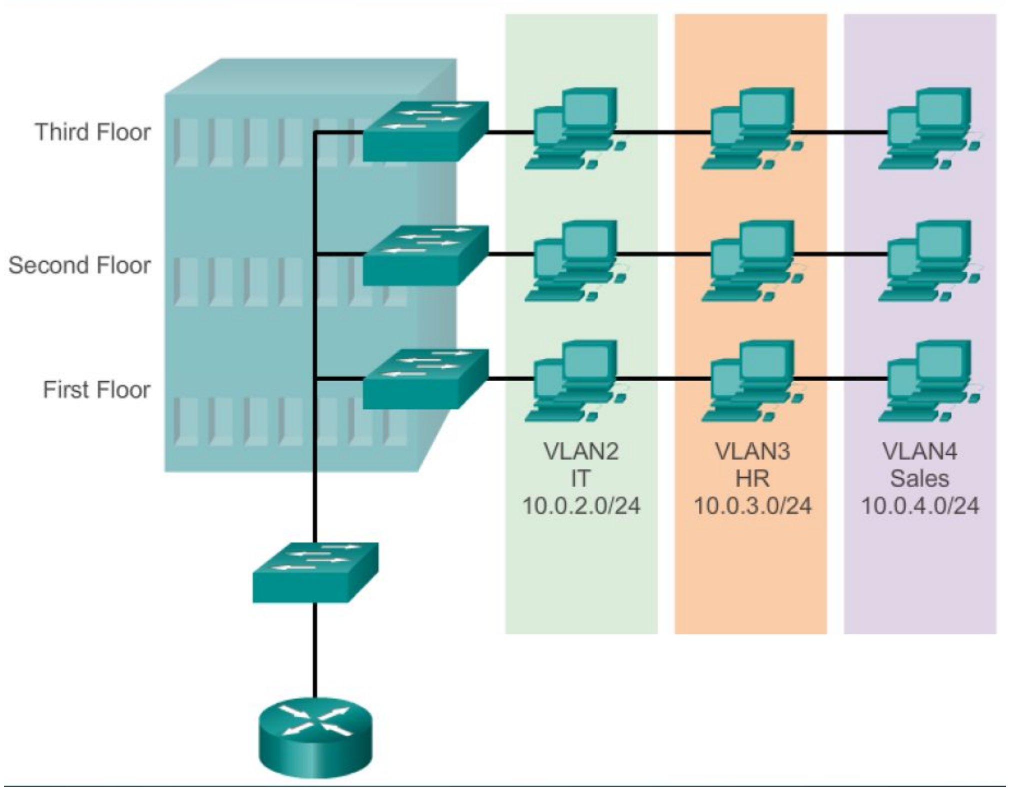
- Reducing unnecessary broadcast traffic across the entire switch improves network efficiency.

- VLANs help isolate traffic between the two networks at Layer 2. Even if someone tries to spoof an IP address from the other network, they will not be able to communicate unless explicitly allowed by routing rules.

- If the network grows, VLANs make it easier to manage segmentation without needing to redesign the physical topology.

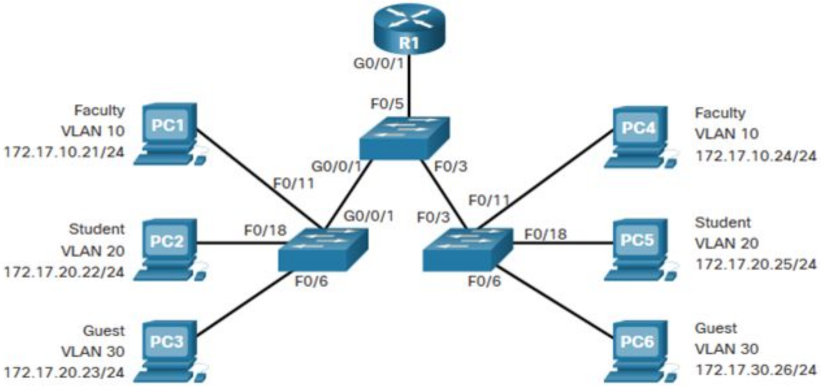


VLAN



- A VLAN is a logical partition of a Layer 2 network.
- Segments a physical network into multiple logical networks.
- Allows devices to be grouped by function or department, **independent of physical location**.
- Each VLAN will have its own unique range of IP addressing.
- Broadcasts, multicasts and unicasts are isolated in the individual VLAN.
- Enhances network security by limiting access between VLANs.
- Simplifies network management and administration.

Benefits of VLAN



Benefits of using VLANs are as follows:

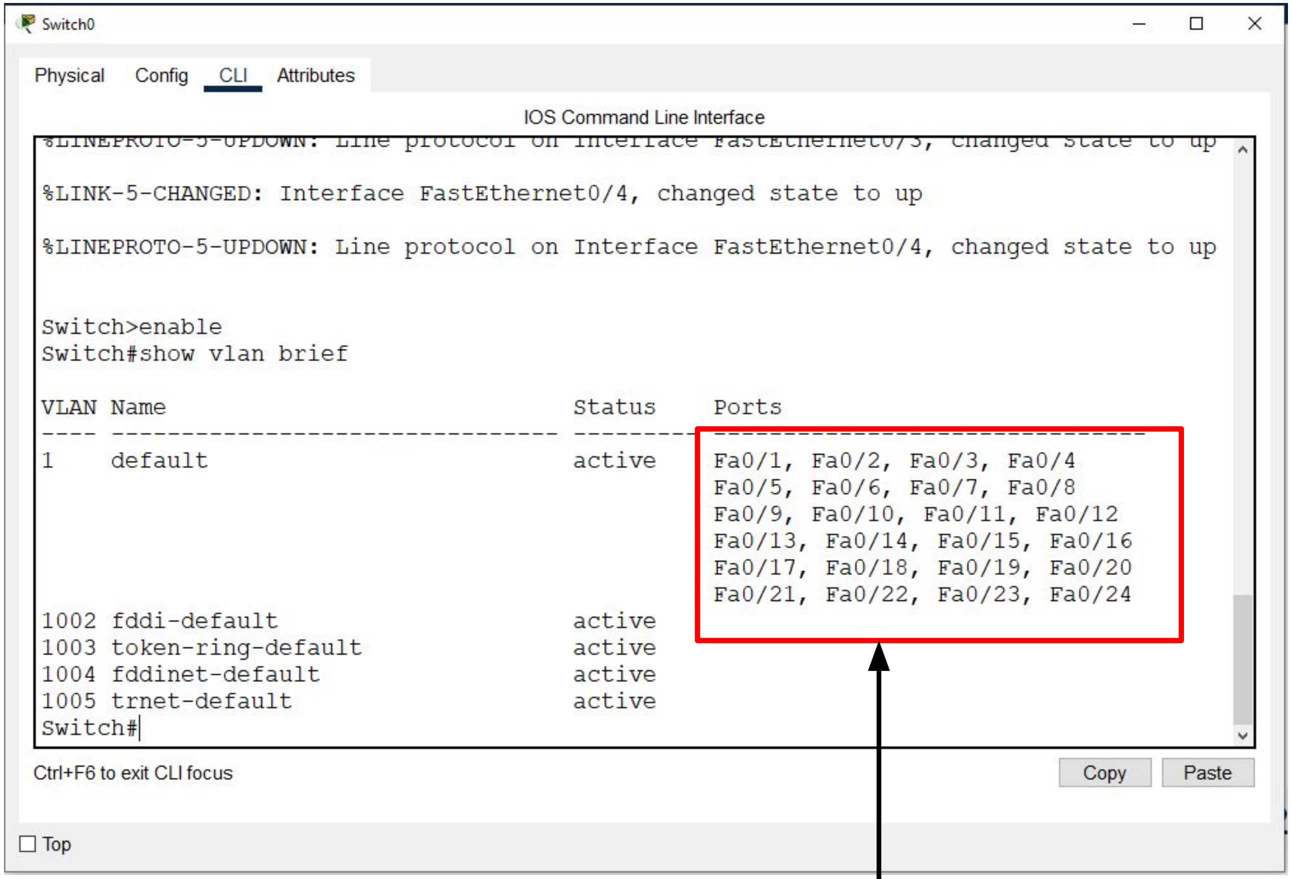
Benefits	Description
Smaller Broadcast Domains	Dividing the LAN reduces the number of broadcast domains
Improved Security	Only users in the same VLAN can communicate together
Improved IT Efficiency	VLANs can group devices with similar requirements, e.g. faculty vs. students
Reduced Cost	One switch can support multiple groups or VLANs
Better Performance	Small broadcast domains reduce traffic, improving bandwidth
Simpler Management	Similar groups will need similar applications and other network resources

Types of VLANs

Default VLAN

- VLAN 1 is default VLAN
- All ports are assigned to this VLAN
- It is the default Management VLAN
- It cannot be deleted or renamed

Note: Although VLAN1 cannot be deleted, Cisco recommends assigning its default features to other VLANs for better network management and security



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up


Switch>enable
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

24 ethernet ports available in the switch

Remember: when a VLAN is created, it should be given a numerical ID

Types of VLAN

Data VLAN

- Dedicated to user-generated traffic (email and web traffic).
- VLAN 1 is the default data VLAN because all interfaces are assigned to this VLAN.

Native VLAN

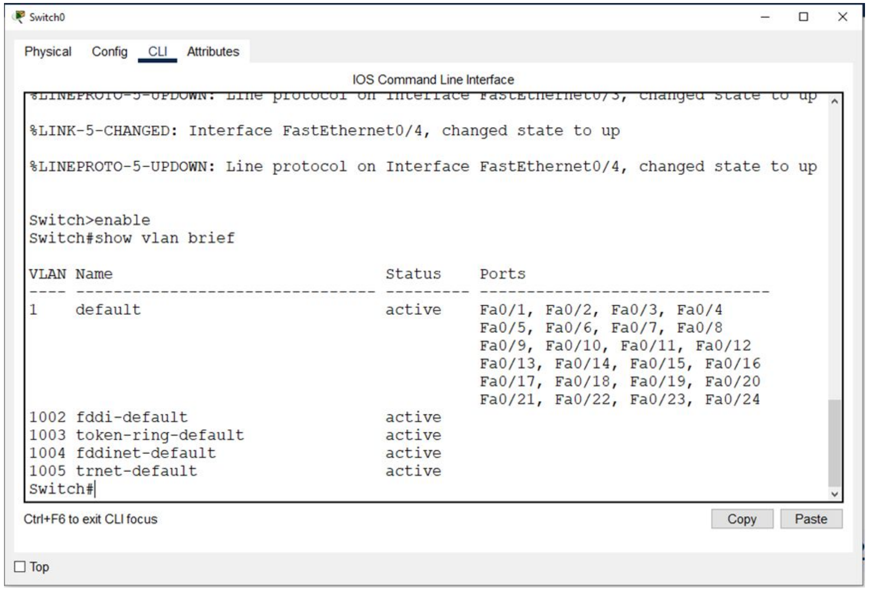
- This is used for trunk links only.
- All frames are tagged on an 802.1Q trunk link except for those on the native VLAN.

Management VLAN

- This is used for SSH/Telnet VTY traffic and should not be carried with end user traffic.

VLAN Ranges on Catalyst Switches

Catalyst switches 2960 and 3650 support over 4000 VLANs.



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up


Switch>enable
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

Normal Range VLAN 1 – 1005	Extended Range VLAN 1006 - 4095
Used in Small to Medium sized businesses	Used by Service Providers
1002 – 1005 are reserved for legacy VLANs	Are in Running-Config
1, 1002 – 1005 are auto created and cannot be deleted	Supports fewer VLAN features
Stored in the vlan.dat file in flash	Requires VTP configurations
VTP can synchronise between switches	

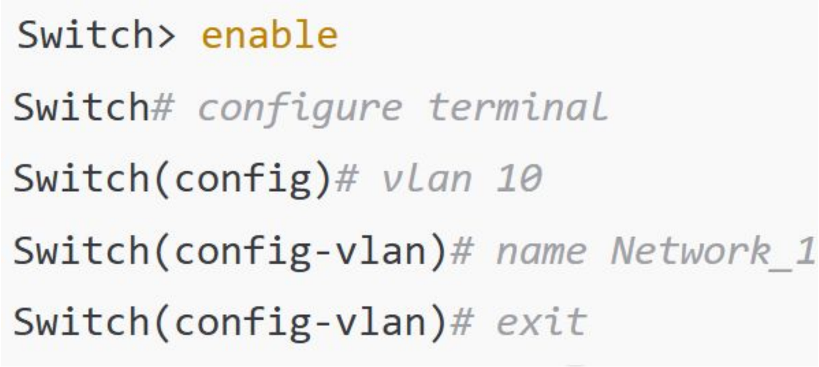
Creating a VLAN: Single-Switch Environment

VLAN details are stored in the vlan.dat file. You create VLANs in the global configuration mode.

To create a VLAN, select the desired switch and open the CLI window. Enter privileged EXEC mode by typing the **enable** command.

Now execute the following command sequentially.

Task	IOS Command
Enter global configuration mode.	Switch# **configure terminal**
Create a VLAN with a valid ID number.	Switch(config)# **vlan** *vlan-id*
Specify a unique name to identify the VLAN.	Switch(config-vlan)# **name** *vlan-name*
Return to the privileged EXEC mode.	Switch(config-vlan)# **end**



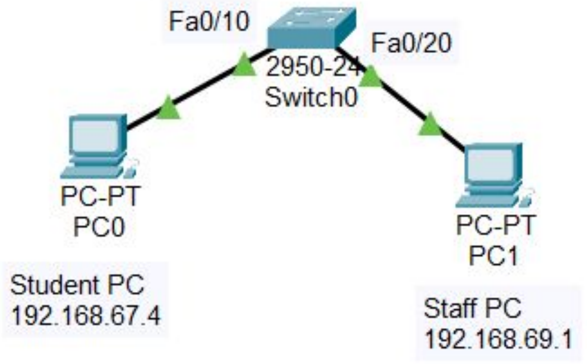
```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name Network_1
Switch(config-vlan)# exit
```

Repeat the above process to create as many VLANs as required

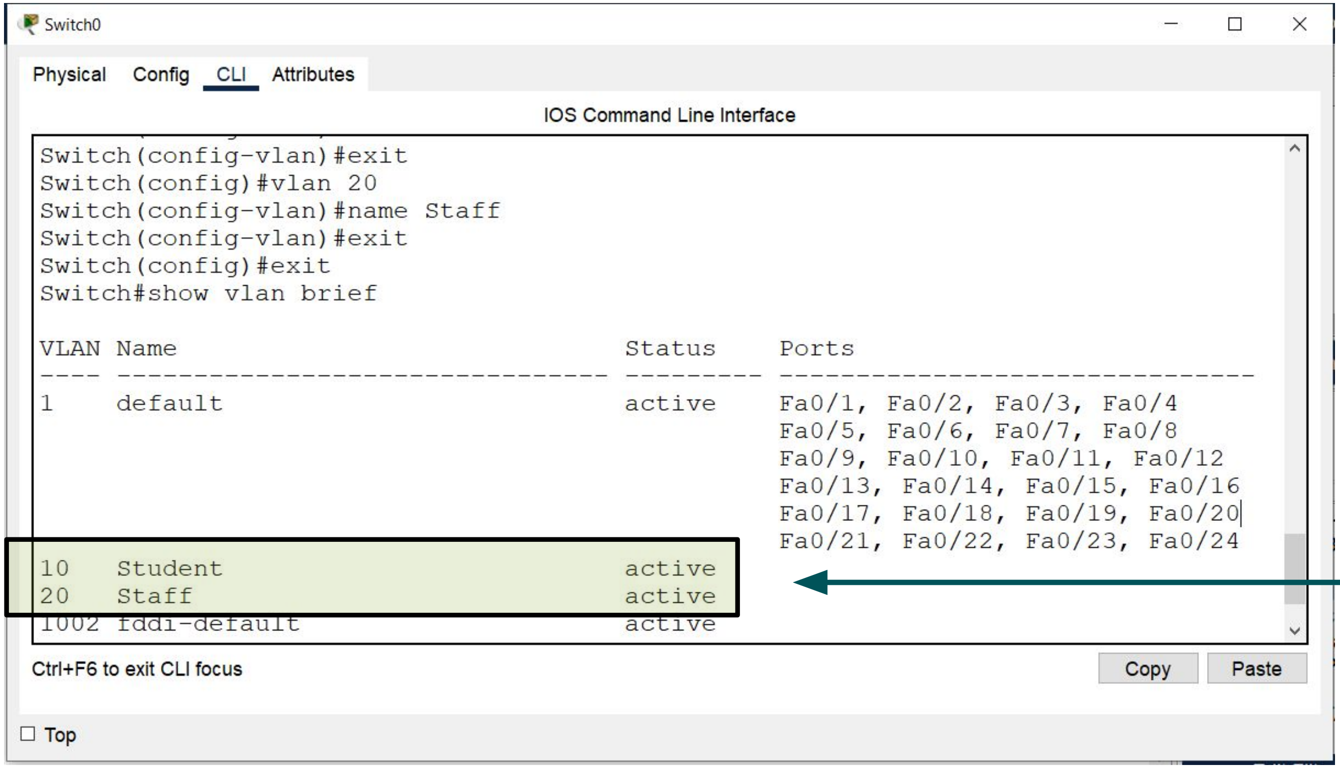
Creating a VLAN: Single-Switch Environment

Consider this network architecture.

- PC0 (192.168.67.4) is connected to Fa0/10 of the switch.
- PC1 (192.168.69.1) is connected to Fa0/20 of the switch.



Following the instructions on slide 12, create two VLANs—VLAN 10 and VLAN 20—and assign them the names 'Student' and 'Staff', respectively.



```
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Staff
Switch(config-vlan)#exit
Switch(config)#exit
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   Student                          active
20   Staff                            active
1002 fddi-default                     active
```

Two active VLANs without port assigned to them yet

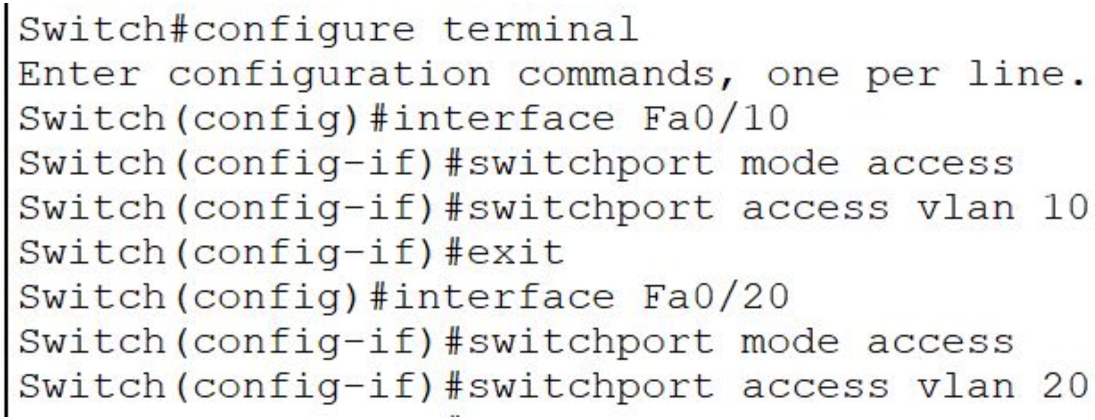
Assign Switch Ports to VLANs

Once the VLAN is created, we can then assign it to the correct interfaces/ethernet ports.

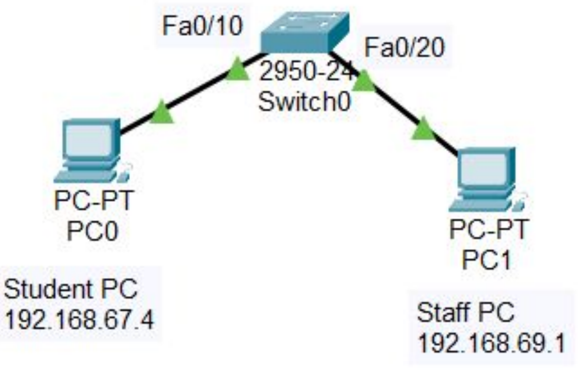
Task	Command
Enter global configuration mode.	Switch# **configure terminal**
Enter interface configuration mode.	Switch(config)# **interface** *interface-id*
Set the port to access mode.	Switch(config-if)# **switchport mode access**
Assign the port to a VLAN.	Switch(config-if)# **switchport access vlan** *vlan-id*
Return to the privileged EXEC mode.	Switch(config-if)# **exit**

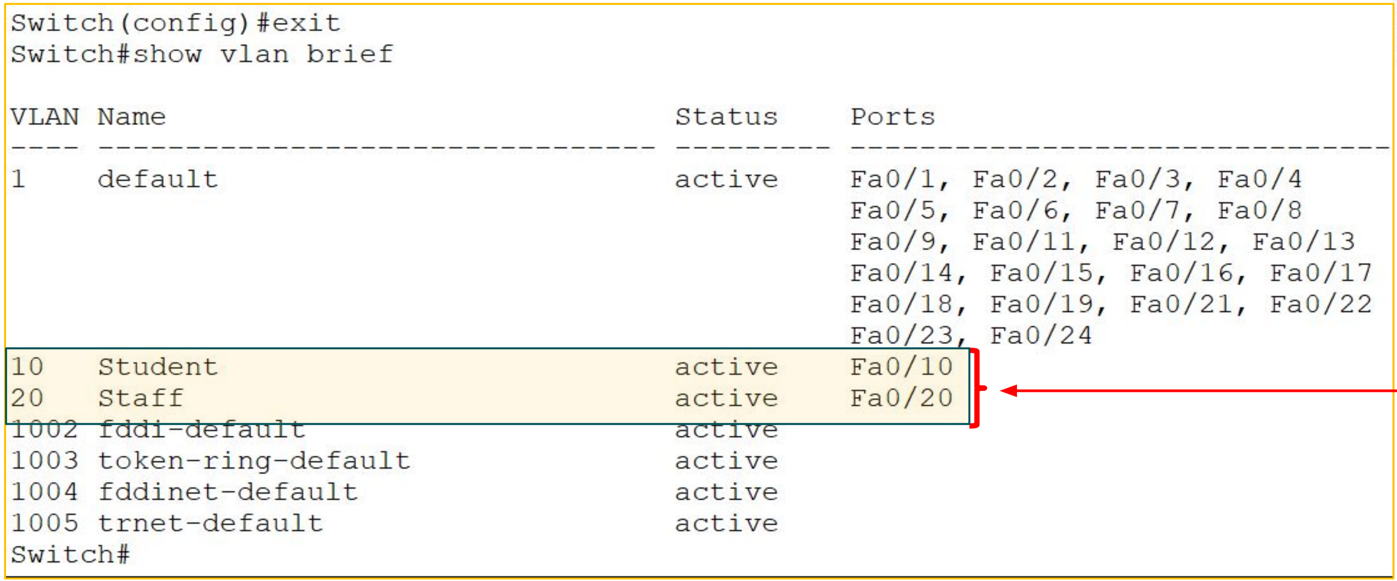
Assign Switch Ports to VLANs

- We will assign port Fa0/10 to VLAN 10 and port Fa0/20 to VLAN 20.



```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface Fa0/10
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface Fa0/20
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
```





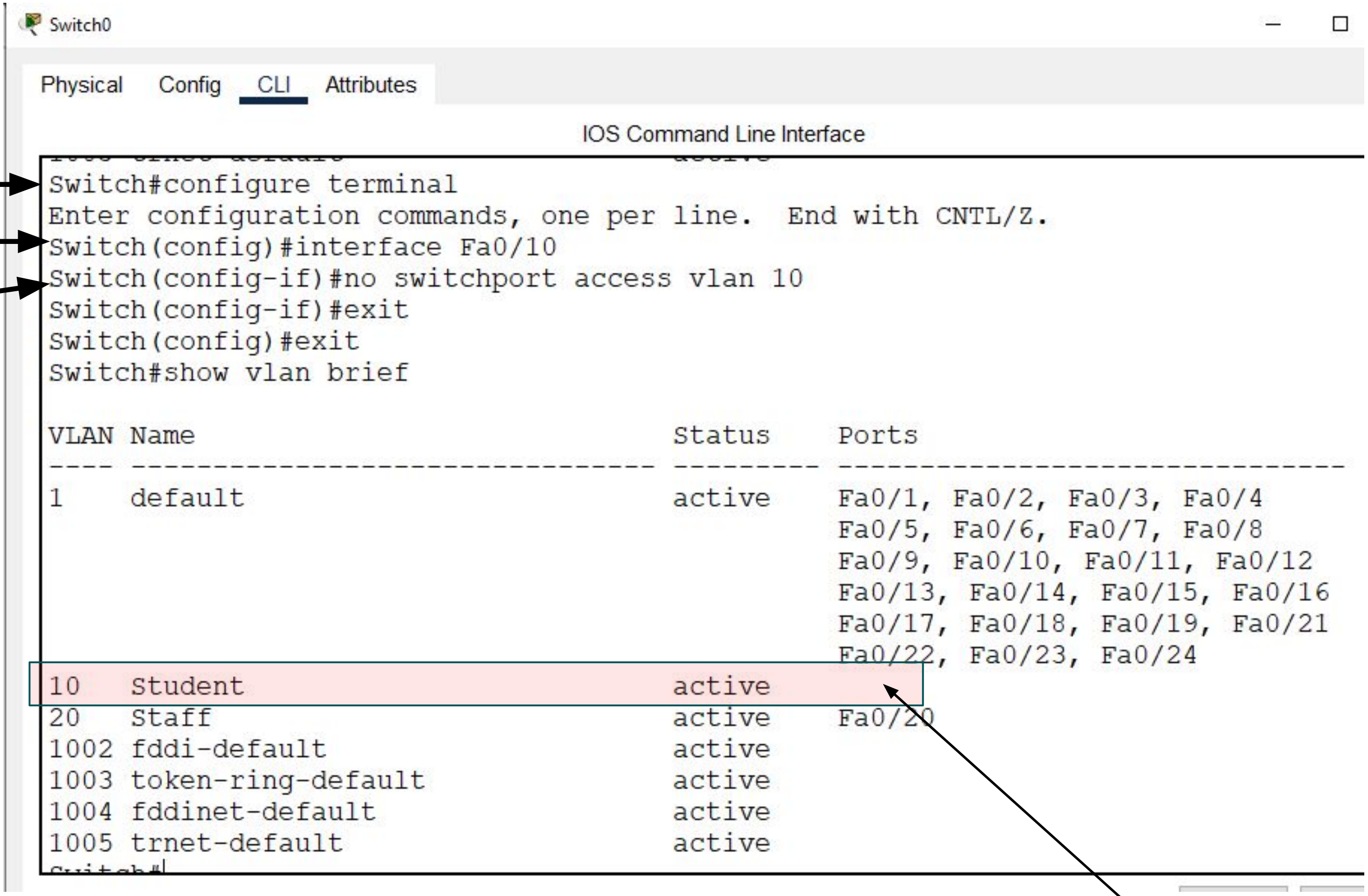
```
Switch(config)#exit
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
10   Student                          active    Fa0/10
20   Staff                            active    Fa0/20
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

Ports assigned

UNIVERSITY of BRADFORD

Changing VLAN Port Membership



```
1005 trnet-default                    active
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface Fa0/10
Switch(config-if)#no switchport access vlan 10
Switch(config-if)#exit
Switch(config)#exit
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24
10   Student                          active
20   Staff                            active    Fa0/20
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

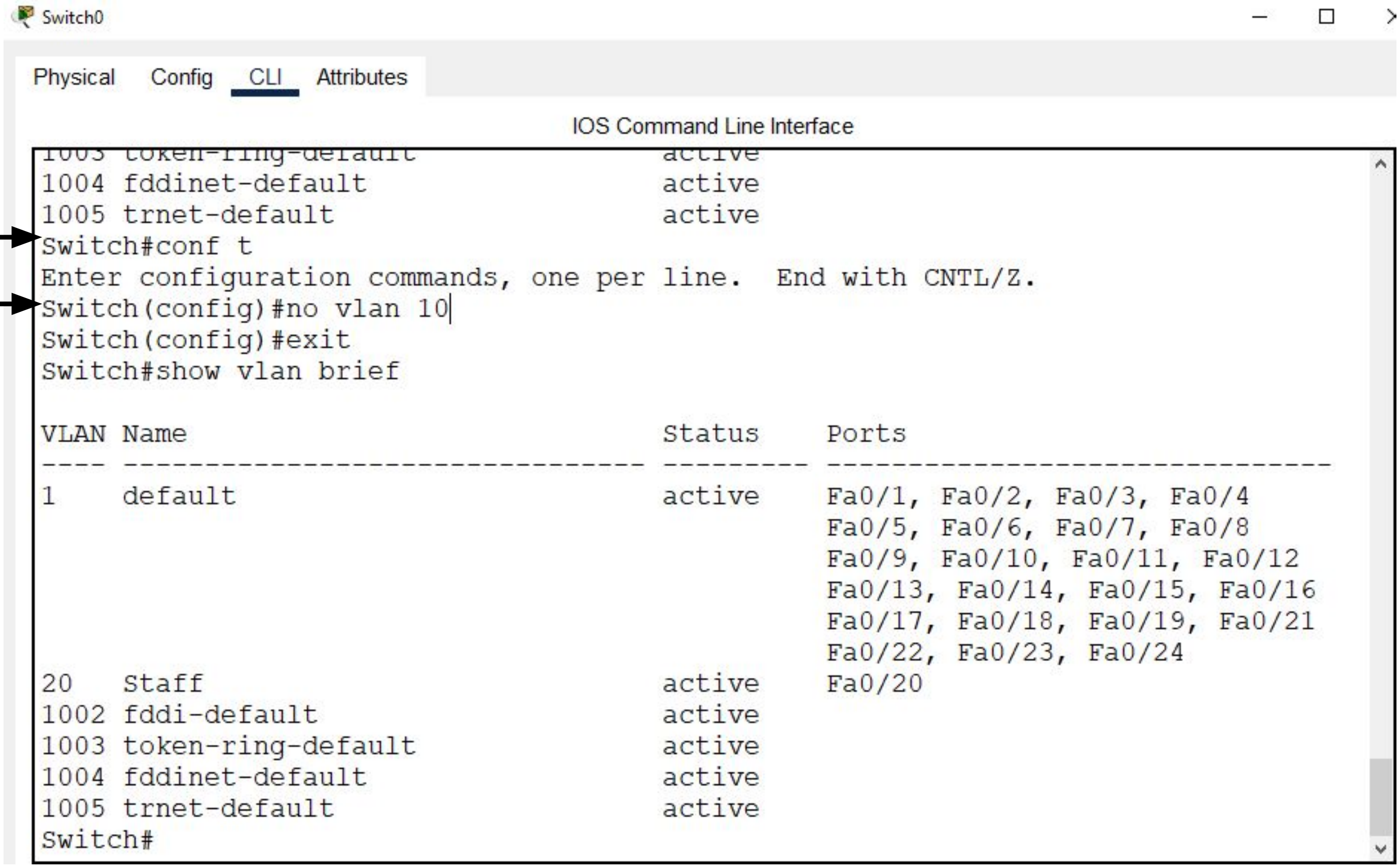
Enter global configuration mode

Enter interface configuration mode

Remove a port from VLAN 10

Port removed

Deleting a VLAN



Enter global configuration mode

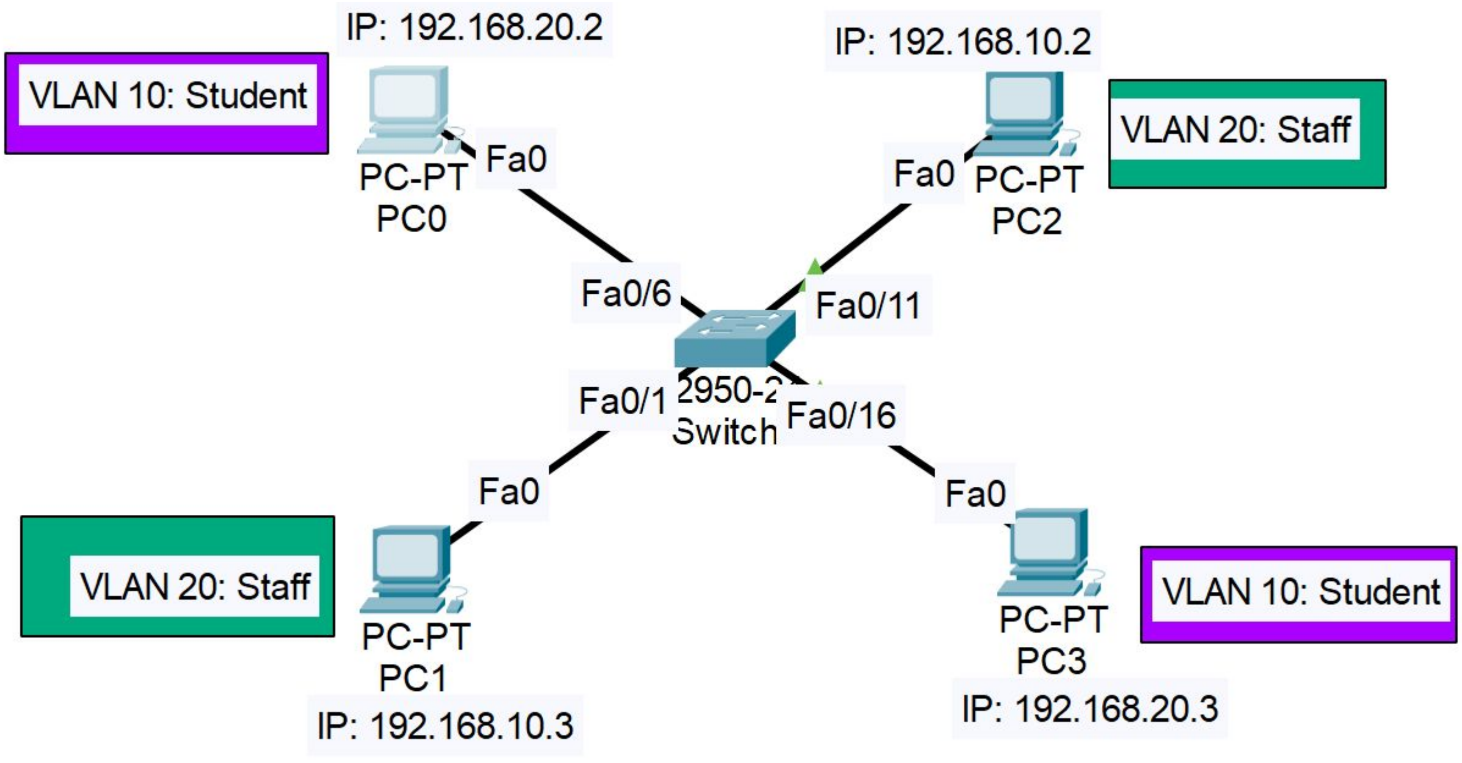
delete VLAN 10

```
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no vlan 10
Switch(config)#exit
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24
20   Staff                            active    Fa0/20
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

VLAN: Exercise 1

- Create this network.
- **Ensure that you connect the PCs to the correct ports on the switch as illustrated here.**
- Assign the IP addresses to the PCs.
- Create two VLANS—VLAN 10: Student and VLAN 20: Staff.
- Assign appropriate switch ports to the VLANS.



Task : After completing all steps, use the **show vlan brief** command to verify the VLAN status. Capture a screenshot of the output and upload it to the Canvas discussion.

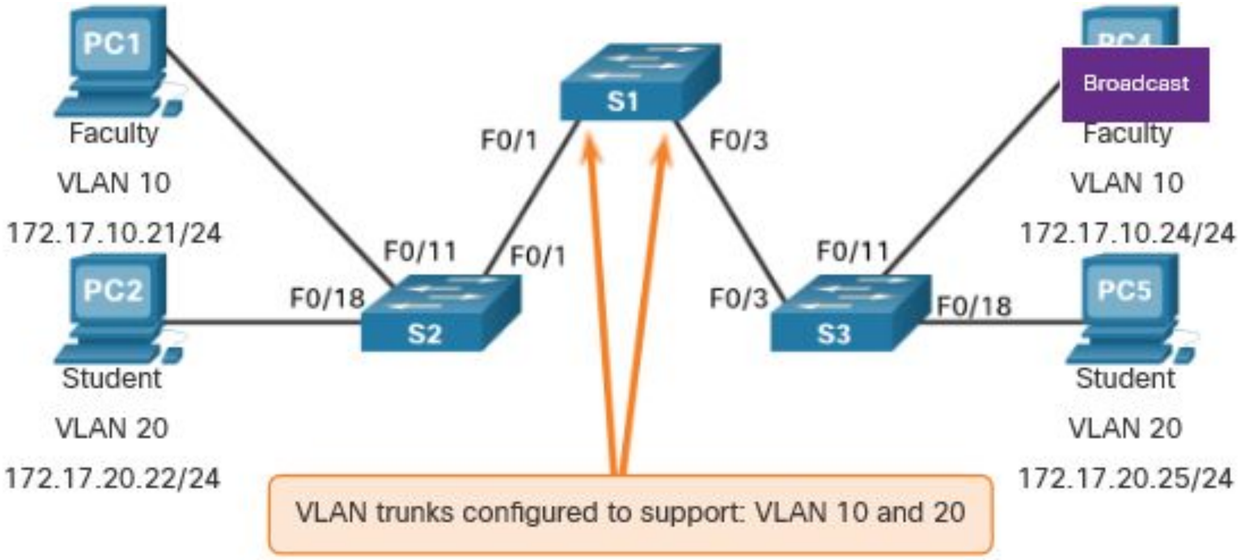
Creating a VLAN: Multi-Switch Environment

VLAN Trunks

- A VLAN trunk is a connection between switches (or between a switch and a router) that allows multiple VLANs to pass through a single physical link.
- A VLAN trunk is typically established between switches to enable communication between devices in the same VLAN, even when they are physically connected to different switches.
- A VLAN trunk is not tied to a specific VLAN, and the trunk ports used to establish the trunk link are not assigned to any single VLAN.
- Traffic from different VLANs is tagged using the **802.1Q** protocol to identify which VLAN it belongs to.

Creating a VLAN: Multi-Switch Environment

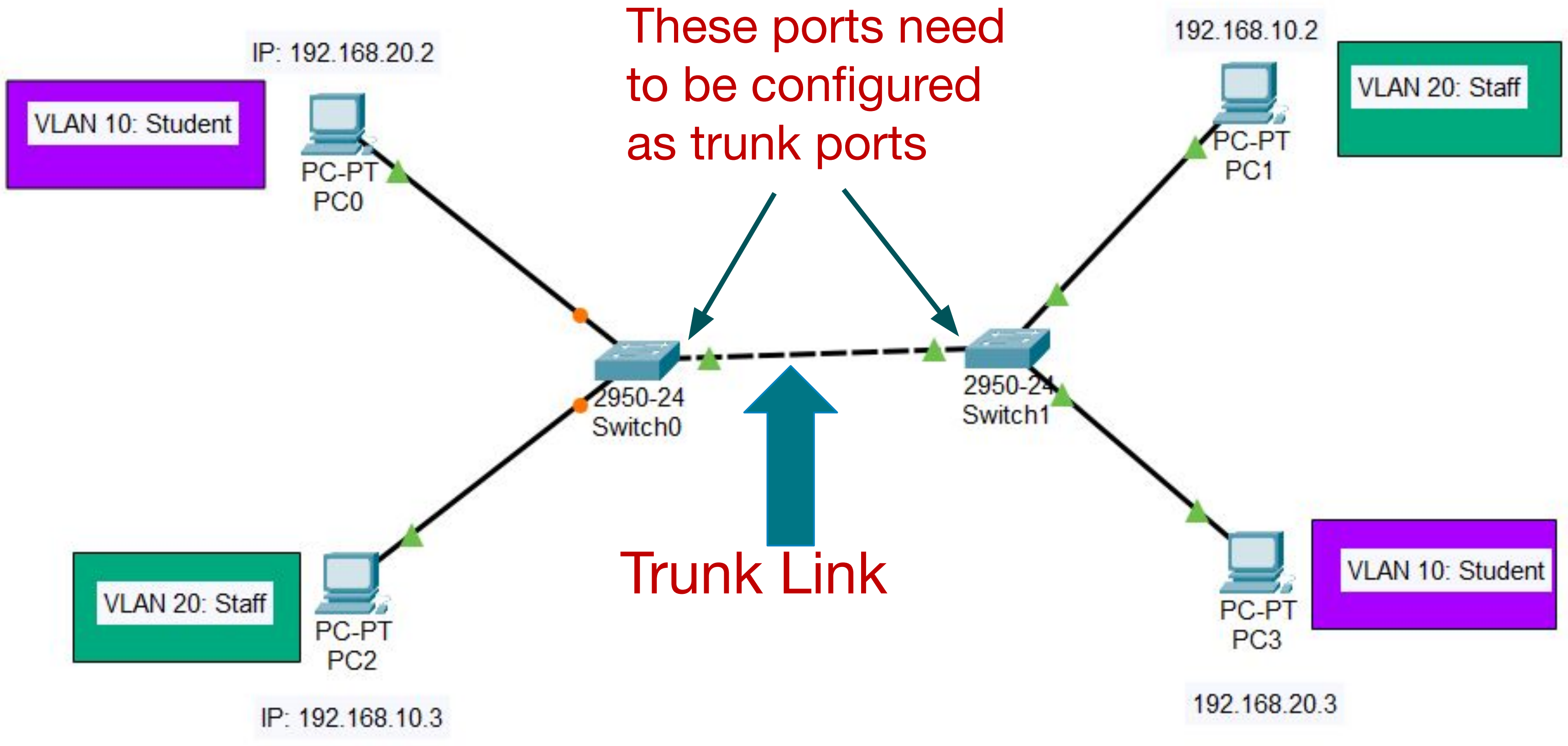
VLAN Trunks



PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame only out ports configured for VLAN10.

Creating a VLAN: Multi-Switch Environment

PCs in two VLANS are connected via two switches



These ports need to be configured as trunk ports

Trunk Link

Configuring Trunk Links

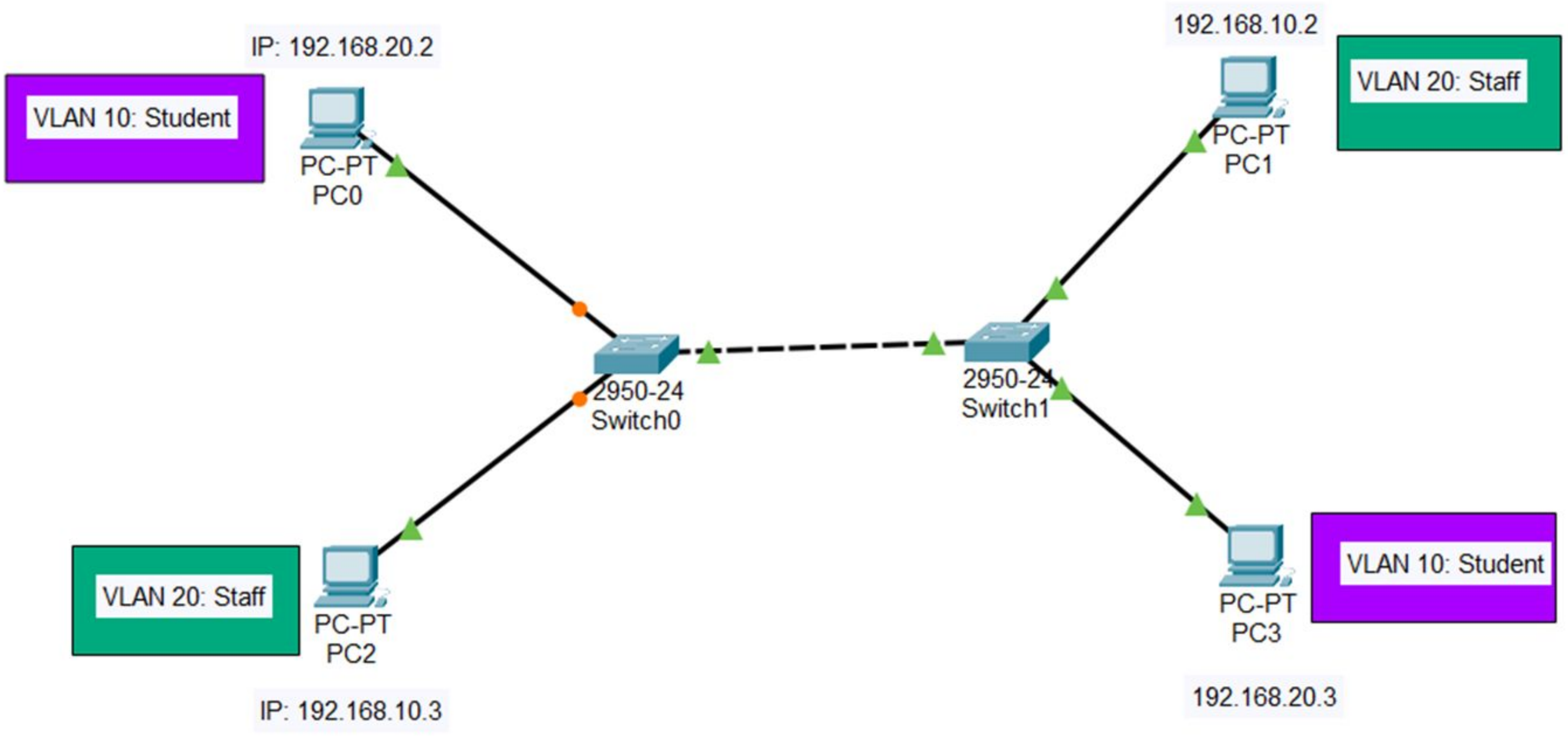
Task	Command
Enter global configuration mode.	Switch# **configure terminal**
Enter interface configuration mode.	Switch(config)# **interface** *interface-id*
Set the port to access mode.	Switch(config-if)# **switchport mode trunk**
Return to global configuration mode.	Switch(config-if)# **exit**
Save the configuration	Switch(config)# **do wr**

By default, all VLANs are allowed on a trunk port.

If you want to limit the trunk link to carry traffic for only specific VLANs (e.g., VLAN 10 and VLAN 20), then you need the command:

```
switchport trunk allowed vlan 10,20
```

Multi-Switch VLAN: Exercise 1

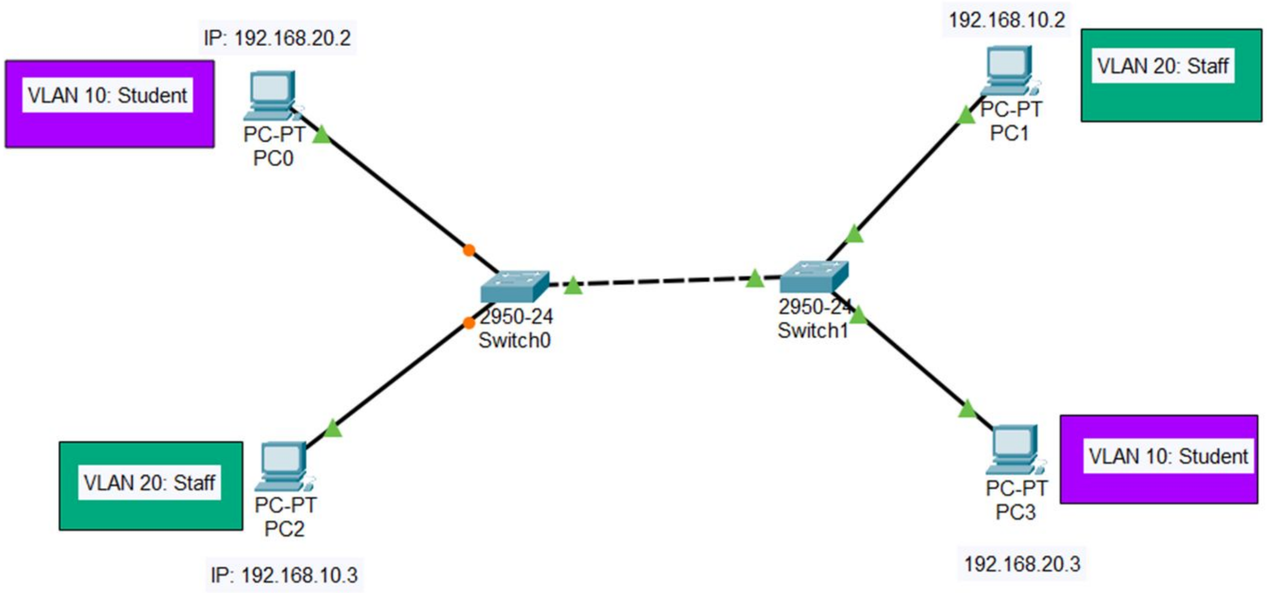


1. Set the IP addresses to the PCs
2. Create VLAN 10: Student and VLAN 20: Staff on each switch
3. Configure Trunk Links
4. Check the connections by using ping command

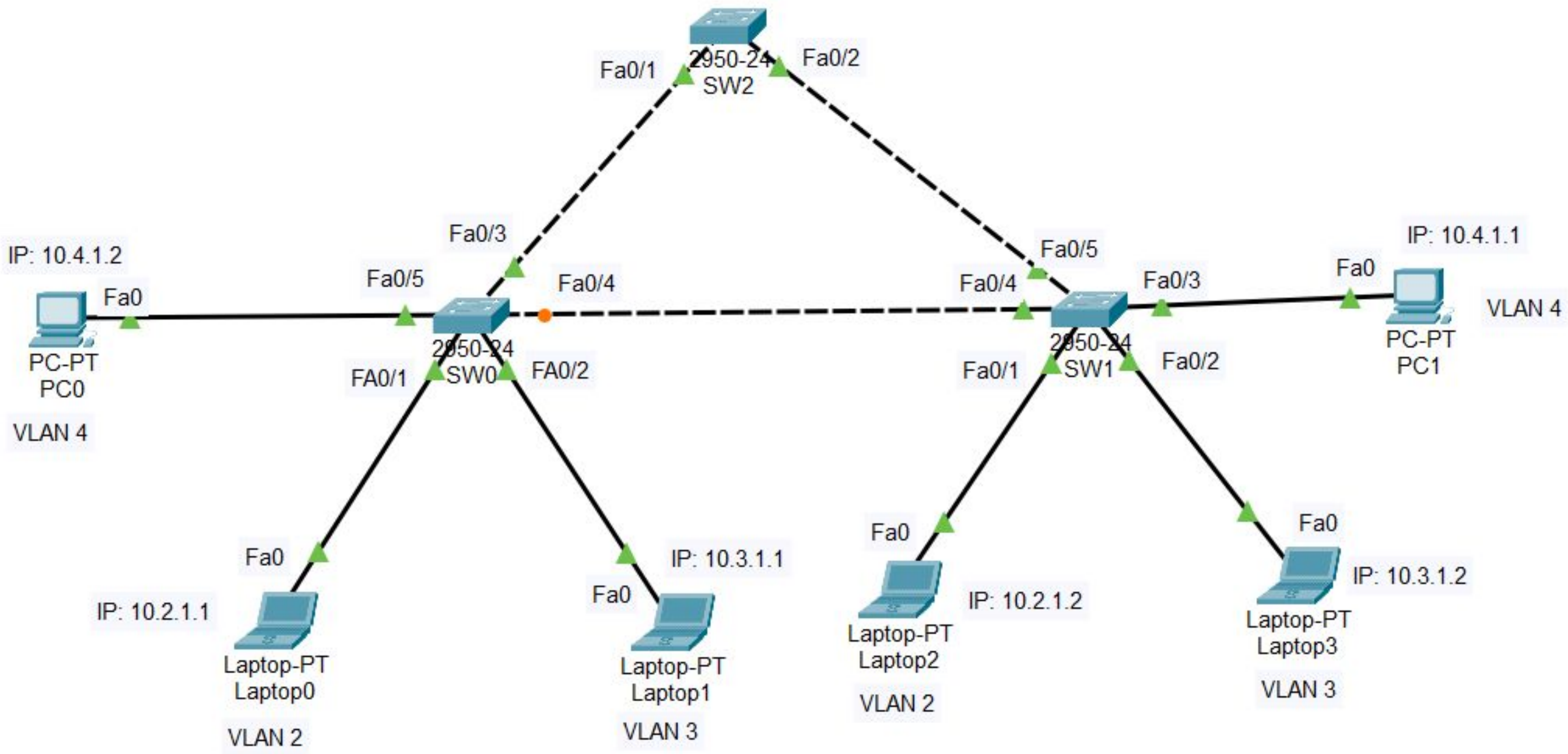
Multi-Switch VLAN: Exercise

In the network you have just created, despite being geographically separated and connected to different switches, PC0 and PC3 can communicate because they share the same network ID. The same applies to PC1 and PC2. Given that devices with the same network ID can already communicate without VLANs, what advantages do VLANs offer in this scenario?

Post your answer in the Canvas Discussion under Question 3.



Multi-Switch VLAN: Exercise 2



1. Assign IP addresses to the PCs and Laptops
2. Create VLAN 2, VLAN 3, and VLAN 4 on switches SW0 and SW1
3. Configure Trunk Links in all three switches
4. Check the connections by using ping command