P04: Networking with Layer 2 Devices, VLAN I

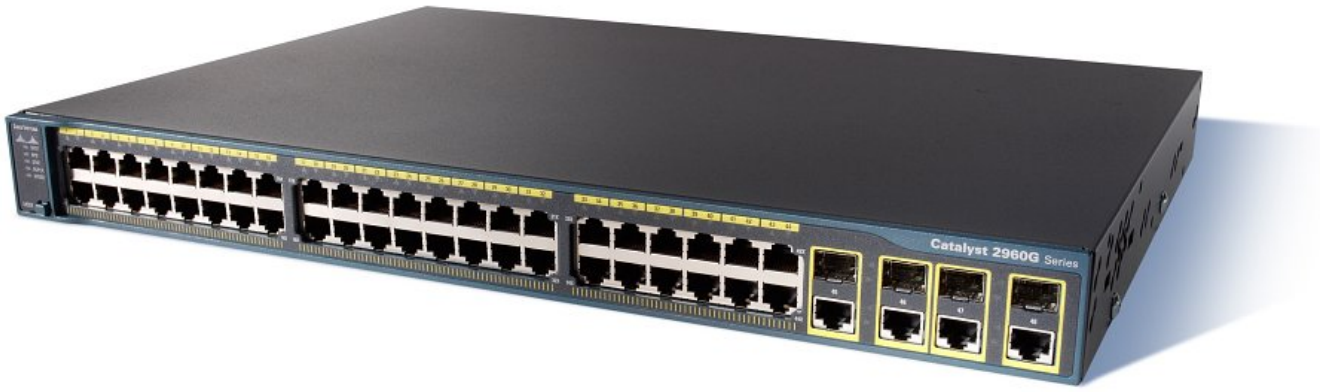
Q1: Understand the elements on the Layer 2

A network switch (also called switching hub, bridging hub, officially MAC bridge) is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer (layer 2) of the OSI model. Unlike less advanced repeater hubs, which broadcast the same data out of each of its ports and let the devices decide what data they need, a network switch forwards data only to the devices that need to receive it.

Switches for Ethernet are the most common form of network switch. Switches also exist for other types of networks including Fibre Channel, Asynchronous Transfer Mode, and InfiniBand.

Some switches can also forward data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

Commercial grade Switches and consumer grade switches (vastly vary in cost and functionality) are available in the market. The following picture is an example of a commercial grade Cisco Switch (2960)



Q2: Cisco device command modes and CLI

Cisco devices run Cisco IOS and IOS commands are used to configure a Cisco device. This section describes the CLI command mode structure. **Command modes** support specific Cisco IOS commands. For example, the interface <interface-id> command **only works** when entered in **global configuration mode**. These are the main command modes:

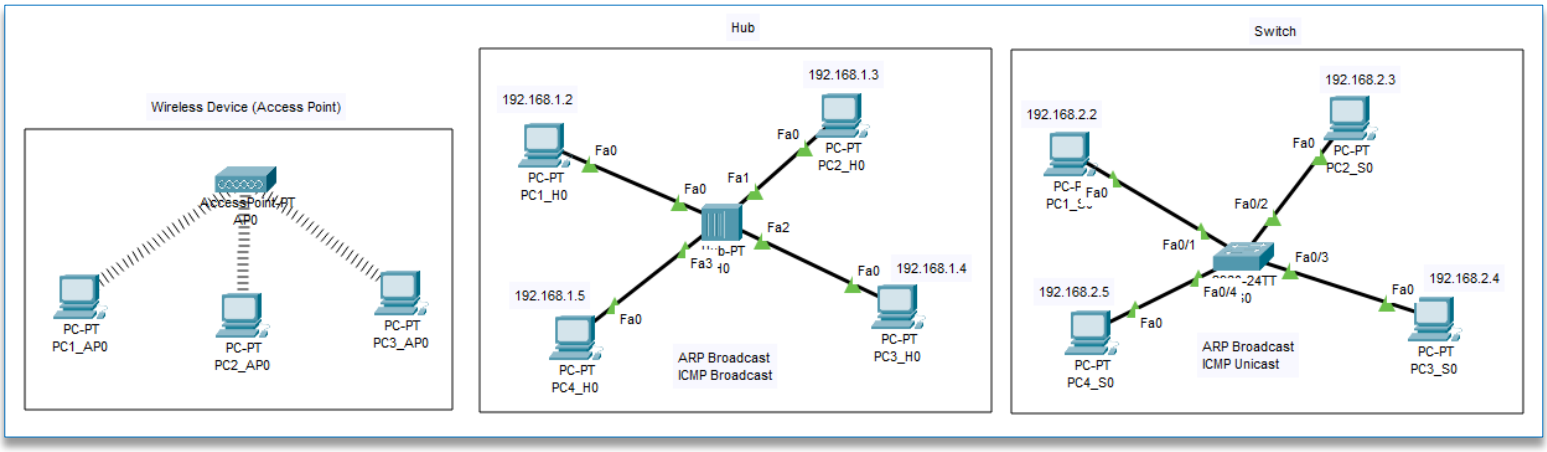
- **User EXEC**
- **Privileged EXEC**
- **Global configuration**
- Interface configuration
- Config-vlan
- VLAN configuration
- Line configuration

Command Mode	Access Method	Prompt	Exit or Access Next Mode
User EXEC	This is the first level of access. (For the switch) Change terminal settings, perform basic tasks, and list system information.	`Switch>`	Enter the **logout** command. To enter privileged EXEC mode, enter the **enable** command.
Privileged EXEC	From user EXEC mode, enter the **enable** command.	`Switch#`	To exit to user EXEC mode, enter the **disable** command. To enter global configuration mode, enter the **configure** command.
Global configuration	From privileged EXEC mode, enter the **configure** command.	`Switch(config)#`	To exit to privileged EXEC mode, enter the **exit** or **end** command, or press **Ctrl-Z**. To enter interface configuration mode, enter the **interface** configuration command.
Interface configuration	From global configuration mode, specify an interface by entering the **interface** command followed by an interface identification.	`Switch(config-if)#`	To exit to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**. To exit to global configuration mode, enter the **exit** command.
Config-vlan	In global configuration mode, enter the **vlan** *vlan-id* command.	`Switch(config-vlan)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.
VLAN configuration	From privileged EXEC mode, enter the **vlan database** command.	`Switch(vlan)#`	To exit to privileged EXEC mode, enter the **exit** command.
Line configuration	From global configuration mode, specify a line by entering the **line** command.	`Switch(config-line)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.

- Complete **PTLab 04.2.pka** and configure the devices (switch and router) via **CLI only**.
  (Hint: you may want to refer to additional materials for help in completing this task)

Q3: Simple networks with access point, hub, switch

- Open **PTLab 04.3.pka** and implement the network shown below:



- Switch to **simulation mode**
- Use **Simple PDU tool** to perform the following test cases, and fill in the table below:

Test Seq.	Source	Destination	Device	ARP Broadcast on Incoming Port	ARP Broadcast on Other ports (ex. Incoming)	ICMP Broadcast on Incoming Port	ICMP Broadcast on Other ports (ex. Incoming)	Is the device dumb in forwarding packets?
1	PC1_AP0	PC3_AP0	Access Point	N/A	N/A	Yes	Yes	Yes
2	PC3_AP0	PC3_AP0	Access Point	N/A	N/A			
3	PC1_AP0	PC3_AP0	Access Point	N/A	N/A			
1	PC1_H0	PC3_H0	Hub					
2	PC3_H0	PC1_H0	Hub					
3	PC1_H0	PC3_H0	Hub					
4	PC1_H0	PC2_H0	Hub					
1	PC1_S0	PC3_S0	Switch			No	No	No
2	PC3_S0	PC1_S0	Switch			No	No	No
3	PC1_S0	PC3_S0	Switch			No	No	No
4	PC1_S0	PC2_S0	Switch			No	No	No

ARP is used by PCs and switches to learn about the destination MAC address.

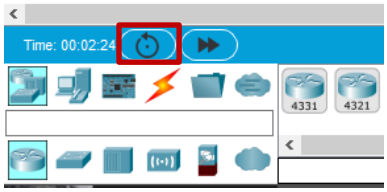
- To view the **arp table on a PC,** go to **PC->Desktop->Command Prompt**, enter arp -p
- To view the MAC address table on a switch, go to S0->CLI, enter

  Switch>en *// will take you to the privileged mode*

  Switch#show mac-address-table

Once switches/PCs learn the destination MAC address via ARP, for subsequent data communication, ARP will not be used. Hence you will not see ARP packets going around.

To reset the state of the devices, click on **Power Cycle Devices** (to reset the network), you may want to perform it before you observe the ARP behavior of the devices mentioned in the table above

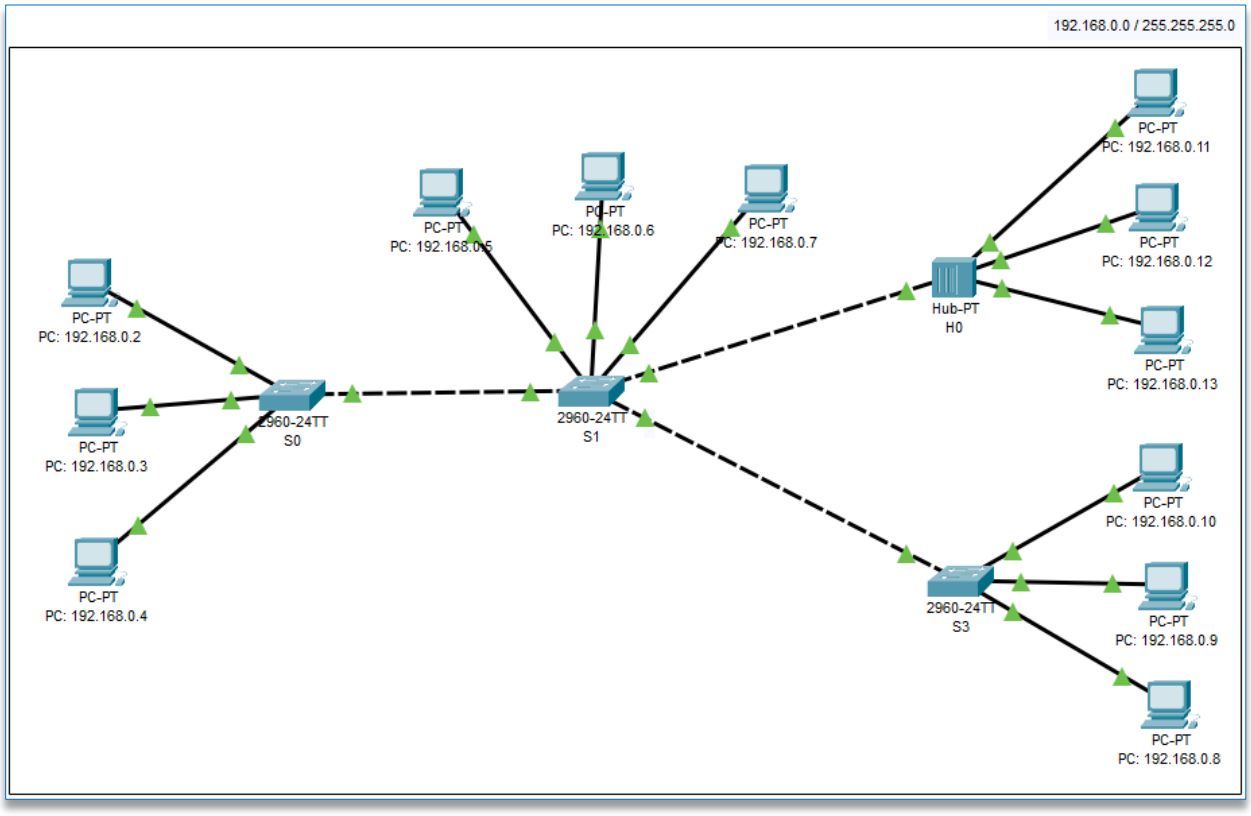


- Observe the ICMP packet at the Access Point, Hub, Switch. State the difference?

Device	Can it see Layer 1 information of the Packet?	Can it see Layer 2 information of the Packet?
Access Point		
Hub		
Switch		

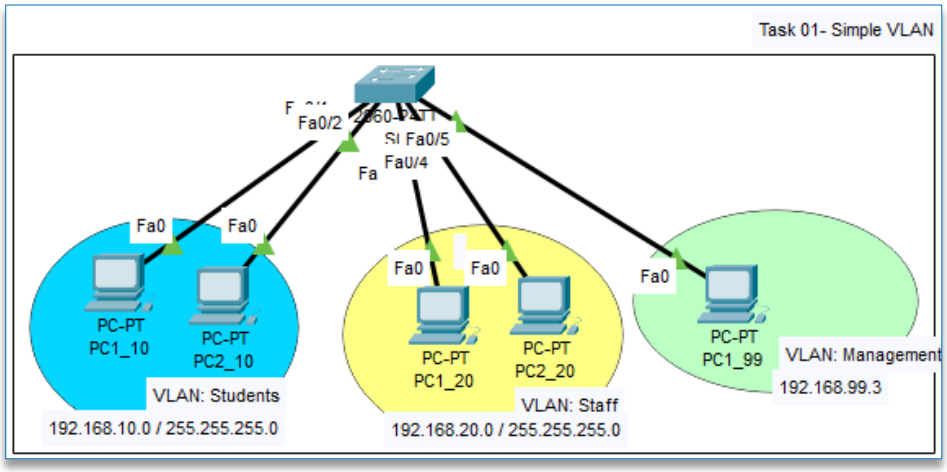
Q4: Complex network with cascading switches

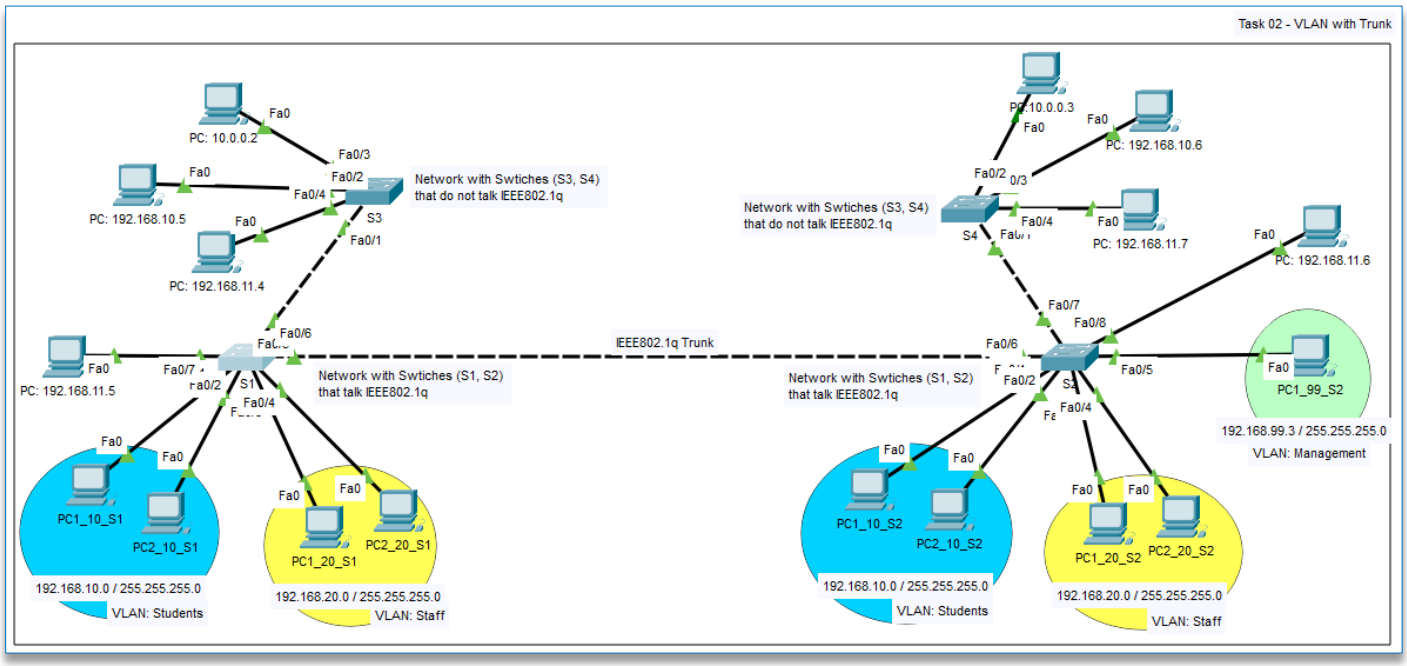
- Open **PTLab 04.4.pka** and implement the network shown below:



Q5: VLAN with switches (intra-VLANs, not Inter-VLAN)

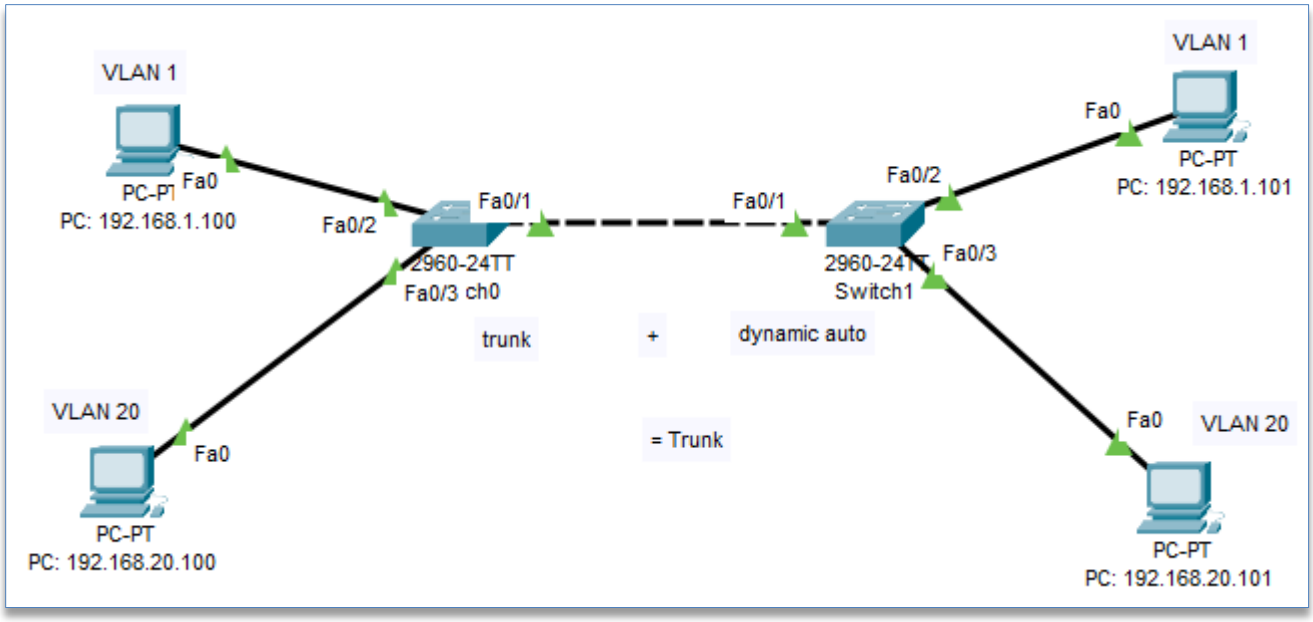
- Open **PTLab 04.5.pka** and implement the networks shown below:





Q6: VLAN with a Trunk Port – Dynamic Trunking Protocol

- Open **PTLab 04.6.pka** and implement the network shown below:



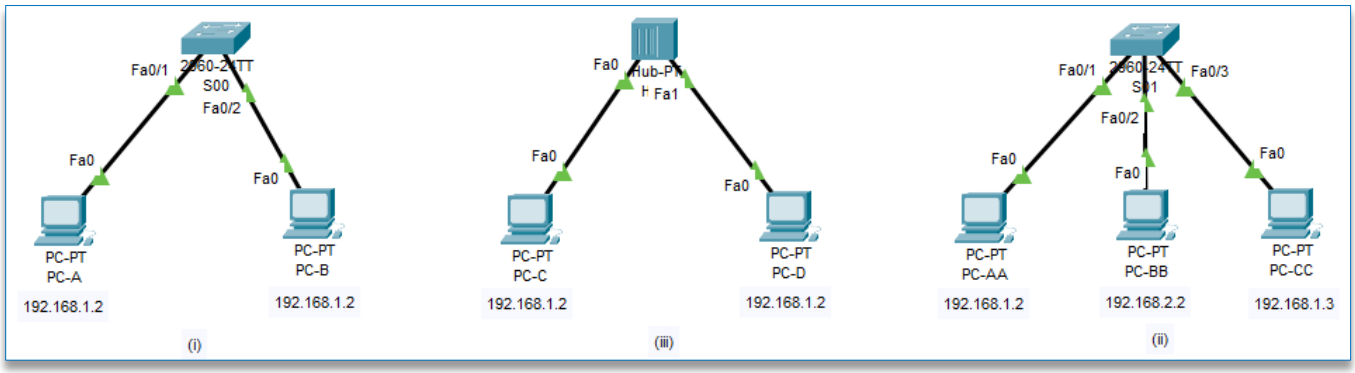
1. Why is **not** necessary to configure both end of a link when it the link needs to a trunk or access link?
2. Complete the following table and determine the resulting the link type if Swtich0-fa0/1 and Swtich1-fa0/1 modes (Administrative Mode) are as shown below:

DTP auto-negotiation resulting link states

Port Mode	Access	Trunk	Dynamic Auto	Dynamic Desirable
Access	*access*	*not recommended (dead link)*	*access*	*access*
Trunk	*not recommended (dead link)*	*trunk*	*trunk*	*trunk*
Dynamic Auto				
Dynamic Desirable				

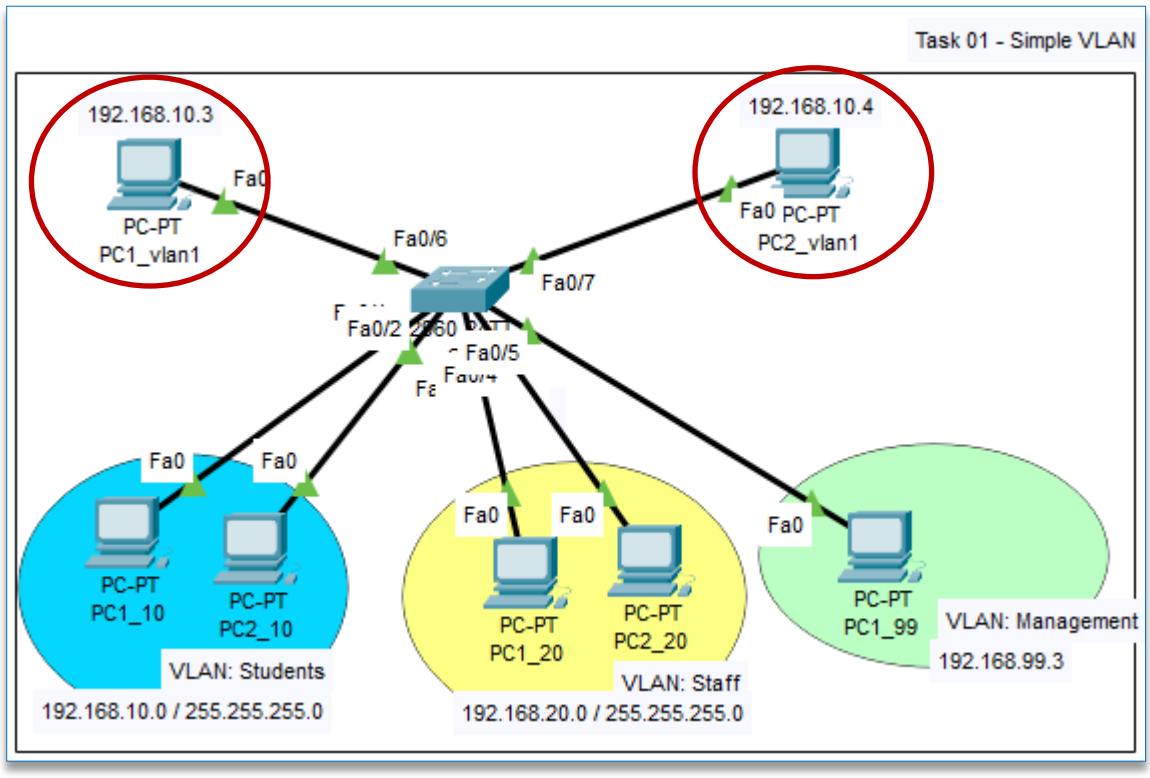
Q7: Try me! Questions

1. Implement the simple networks below: (use the exact IP addresses as shown in the diagram)



   a. Send an ICMP packet from PC-A to PC-B (via the switch), was the communication successful? why?
   b. Send an ICMP packet from PC-C to PC-D (via the hub), was the communication successful? why?
   c. Send an ICMP packet from PC-AA to PC-BB (via the switch), was the communication successful? why?
   d. Send an ICMP packet from PC-AA to PC-CC (via the switch), was the communication successful? why? (Hint: Look into arp -a table of relevant PCs)

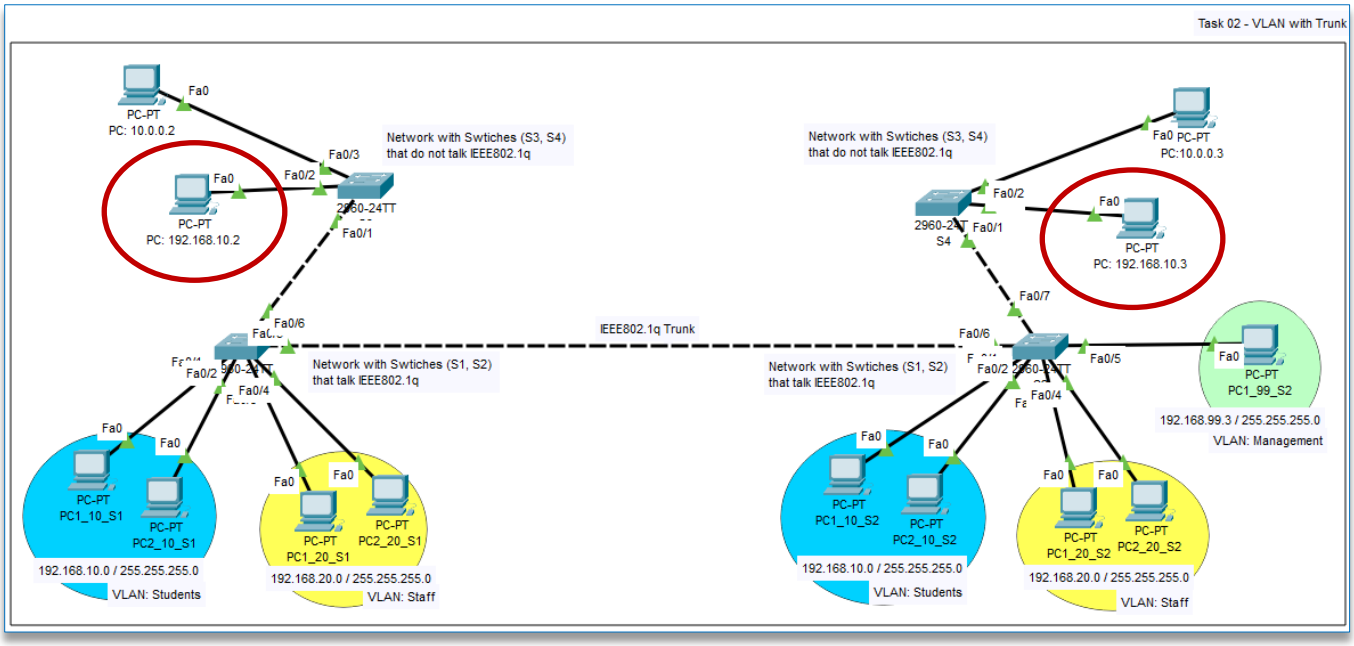
2. In Q5, *Task 01 – Simple VLAN Network:* Extend the network by adding **PC1_vlan1** (IP: 192.168.10.3) and **PC2_vlan1** (IP: 192.168.10.4) as shown below:



   a. Send an ICMP packet from PC1_vlan1 to PC2_vlan1, was the communication successful? why?
   b. PC1_vlan1 (IP: 192.168.10.3) to PC1_10 (IP: 192.168.10.2) are on the same network (192.168.10.0 / 255.255.255.0) considering the IP addresses. Try to send a message from PC1_vlan1 to PC1_10. Why does it fail?
   c. PC1_vlan1 (IP: 192.168.10.3) to PC2_10 (IP: 192.168.10.3) has the same IP address. Try to send a

message from PC1_vlan1 to PC2_10. Why does it fail?

3. In Q5, *Task 02 – VLAN with Trunk Network,* change the IP addresses of those PCs highlighted as shown in the diagram below (IP: 192.168.10.2, IP: 192.168.10.3):



   a. Send an ICMP packet from PC: 192.168.10.2 to PC: 192.168.10.3. Which PC will receive and respond to the ICMP packet? Is it PC: 192.168.10.3? or PC2_10_S1 (which has the same IP address 192.168.10.3)? Explain why?

4. In Q5, *Task 02 – VLAN with Trunk Network,* why do Switches show the message "%CDP-4-NATIVE_VLAN_MISMATCH: …" ?

Summary

1. Understand the elements on Layer 2
2. Cisco device command modes and CLI
3. Simple networks with access point, hub, switch
4. Complex network with cascading switches
5. VLAN with switches (intra-VLANs, not Inter-VLAN)
6. VLAN with a trunk port – Dynamic Trunking Protocol
7. **Try me! Questions**