CSCI 5010 – Fundamentals of Data Communications

Lab 4 – VLANs, trunking and inter-VLAN routing

University of Colorado Boulder
Department of Computer Science
Network Engineering

Professor Levi Perigo, Ph.D.

Student Name :: Srivaishnavi Gone
ID :: 11087371

Summary

The foundational layer to any network revolves around switching. This lab is intended to be an overview of VLANs, trunk links and inter-VLAN routing.

The questions in the lab are intentionally vague. The purpose of this is for you not only to research, investigate, and learn the technologies, but also become proficient at interpreting both non-technical and technical questions. Being able to research and discover answers on your own will be critical as you progress in your career.

- Learn how to create VLANs within a single switch
- Learn how to create VLANs across multiple switches
- Learn how to achieve Inter-VLAN communication using trunking (802.1q) and “routing on a stick”

Objective 1 - Switch VLAN Configuration

This objective will configure multiple VLANs on a single switch.

Diagram 1

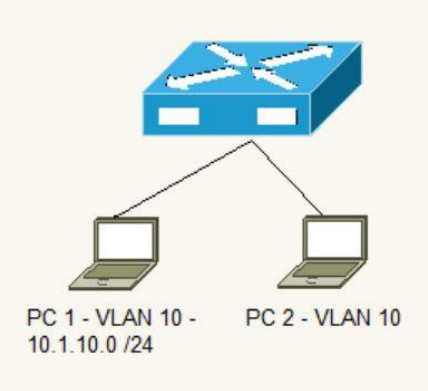
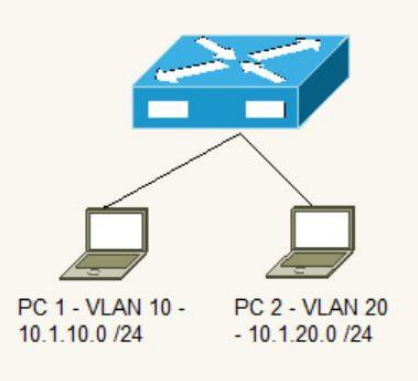
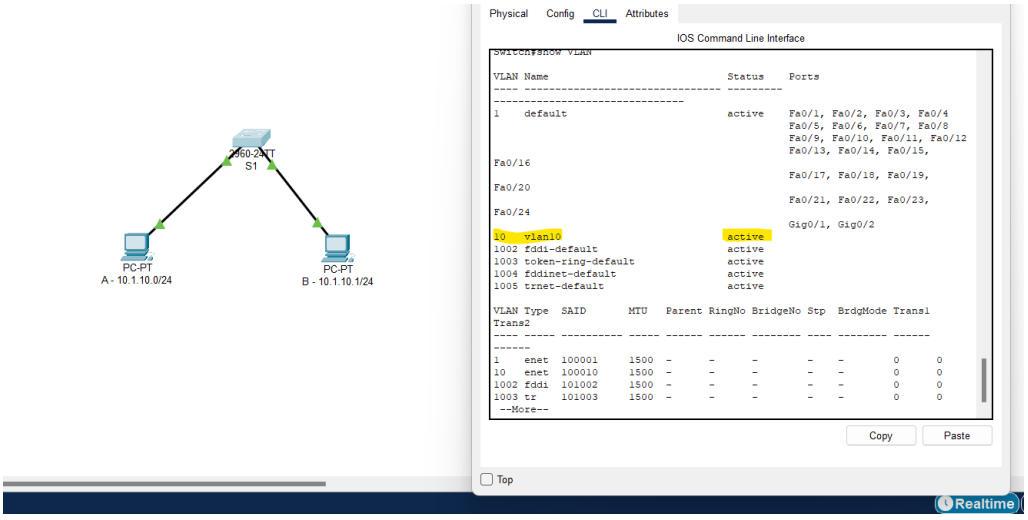


Diagram 2

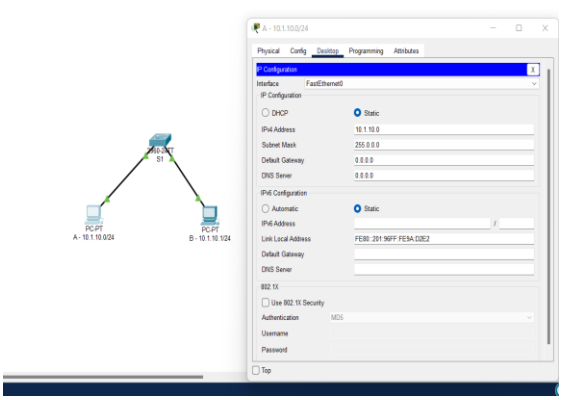


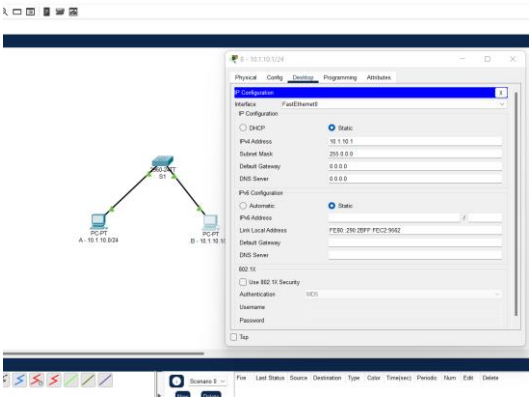
1. Use diagram 1 to verify connectivity within same VLAN (VLAN 10)
2. Assign IP addresses to the PCs
    a. Make sure the PCs are in the same subnet



b. What are the IPs you assigned to both PCs? Why do these IP subnets have to be in the same subnet? **[5 points]**

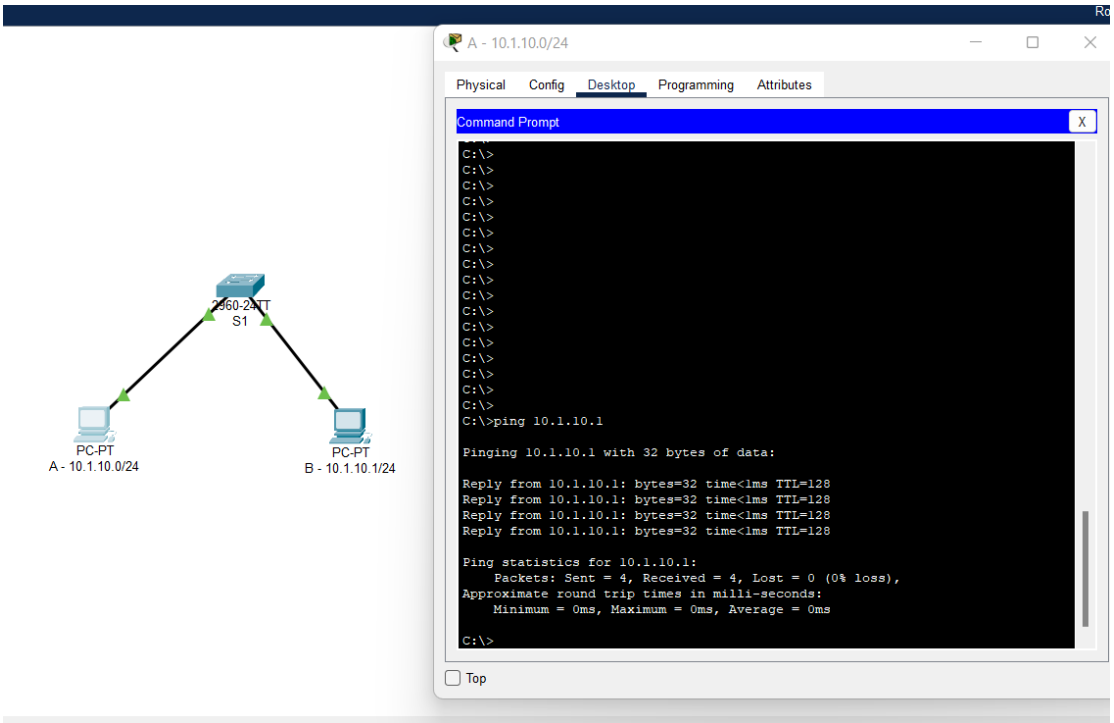
Ans: PC1: 10.1.10.0/24, PC2: 10.1.10.1/24. The IP Subnets have to be in the same subnet to route/communicate with one another within one VLAN Network. Precisely, the IP subnets of host devices within a same VLAN should have same subnet to talk to each other. The IP Addresses within the same subnet are considered to be a single network and allocated a VLAN ID. And the hosts with similar VLAN ID can traverse data traffic b/w each.



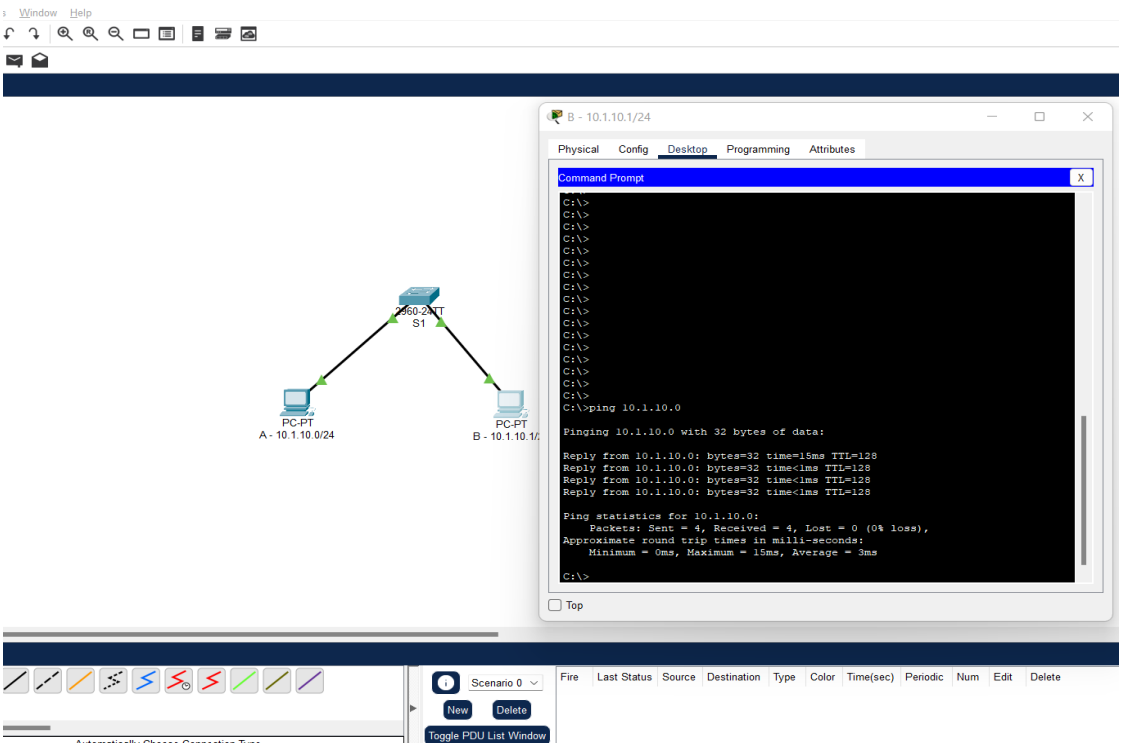


c. Verify Ping connectivity between PCs. Paste screenshot **[2 points]**

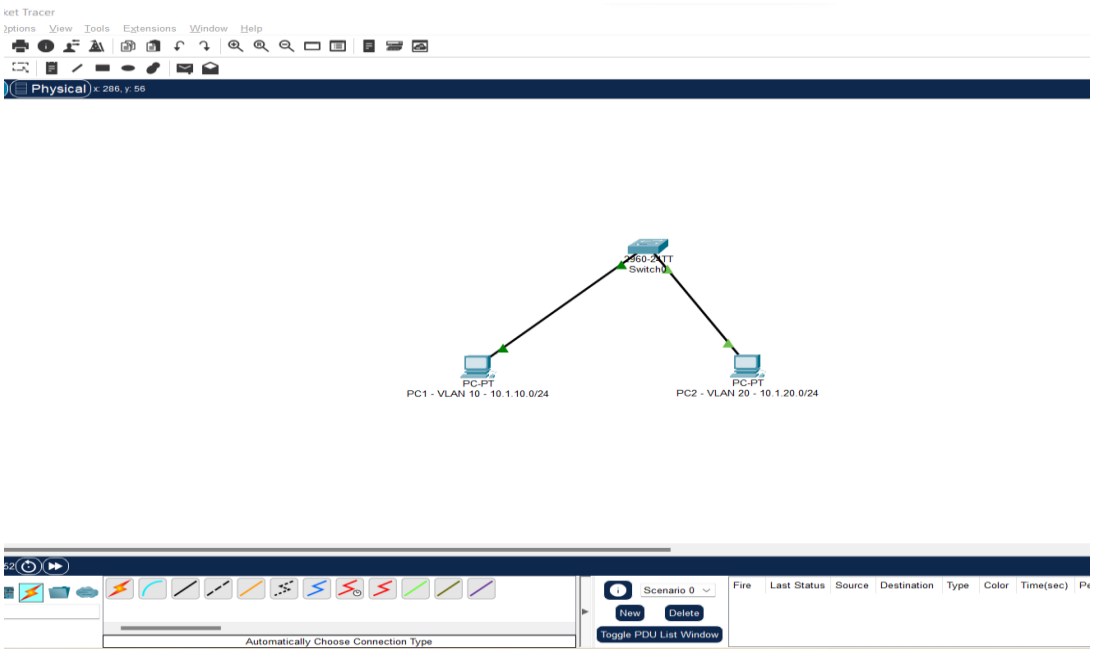
Successful Ping from PC-A to PC-B (10.1.10.0) to (10.1.10.1)



Successful Ping from PC-B to PC-A (10.1.10.1) to (10.1.10.0)



3. Now create two different VLANs (diagram 2)

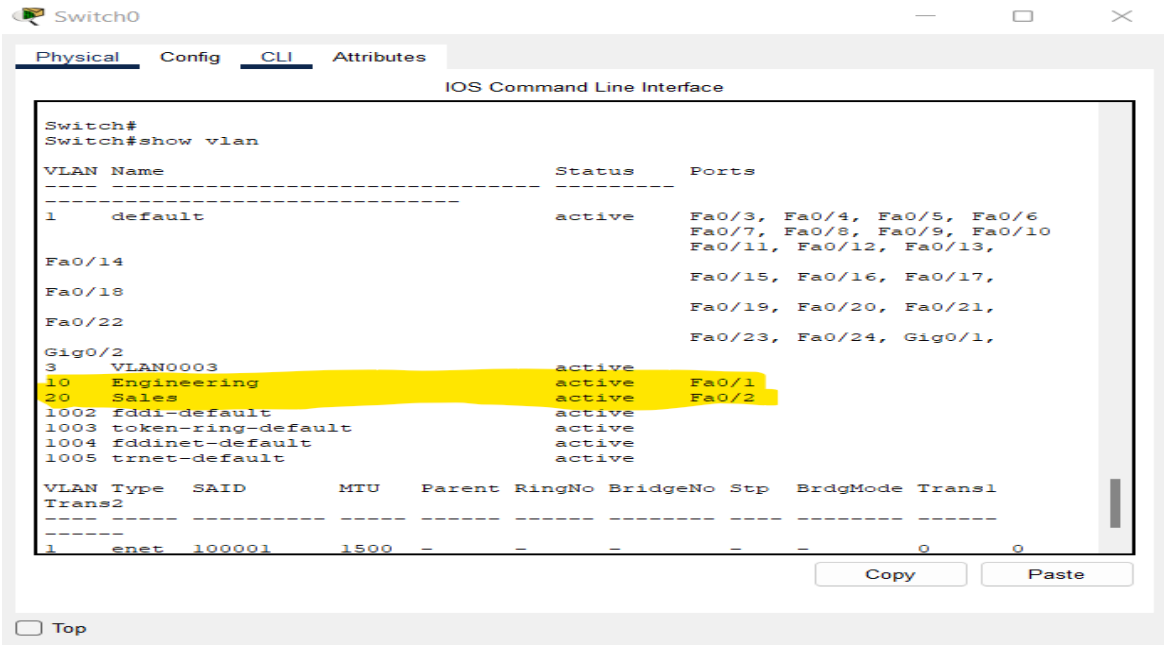


a. VLAN 10 should be named Engineering

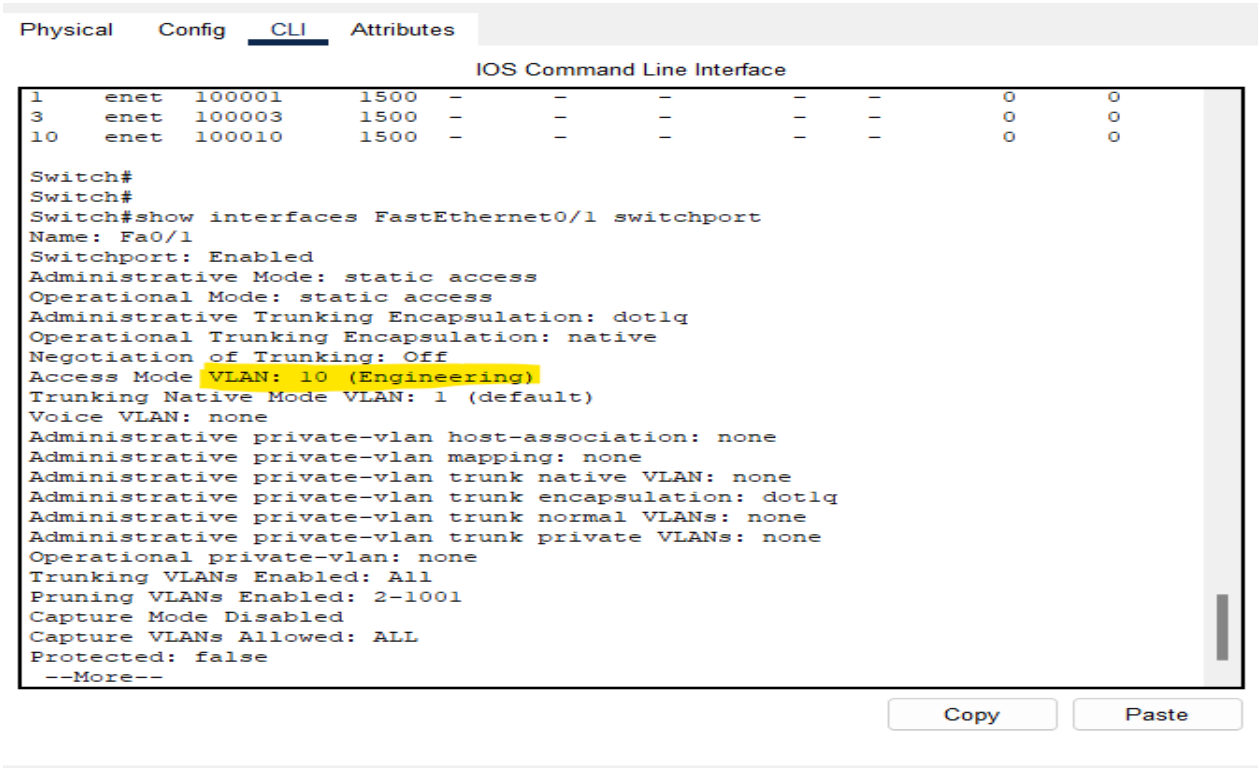
b. VLAN 20 should be named Sales

   i. Use the appropriate **show** commands on the switch to indicate this [**5 points**]

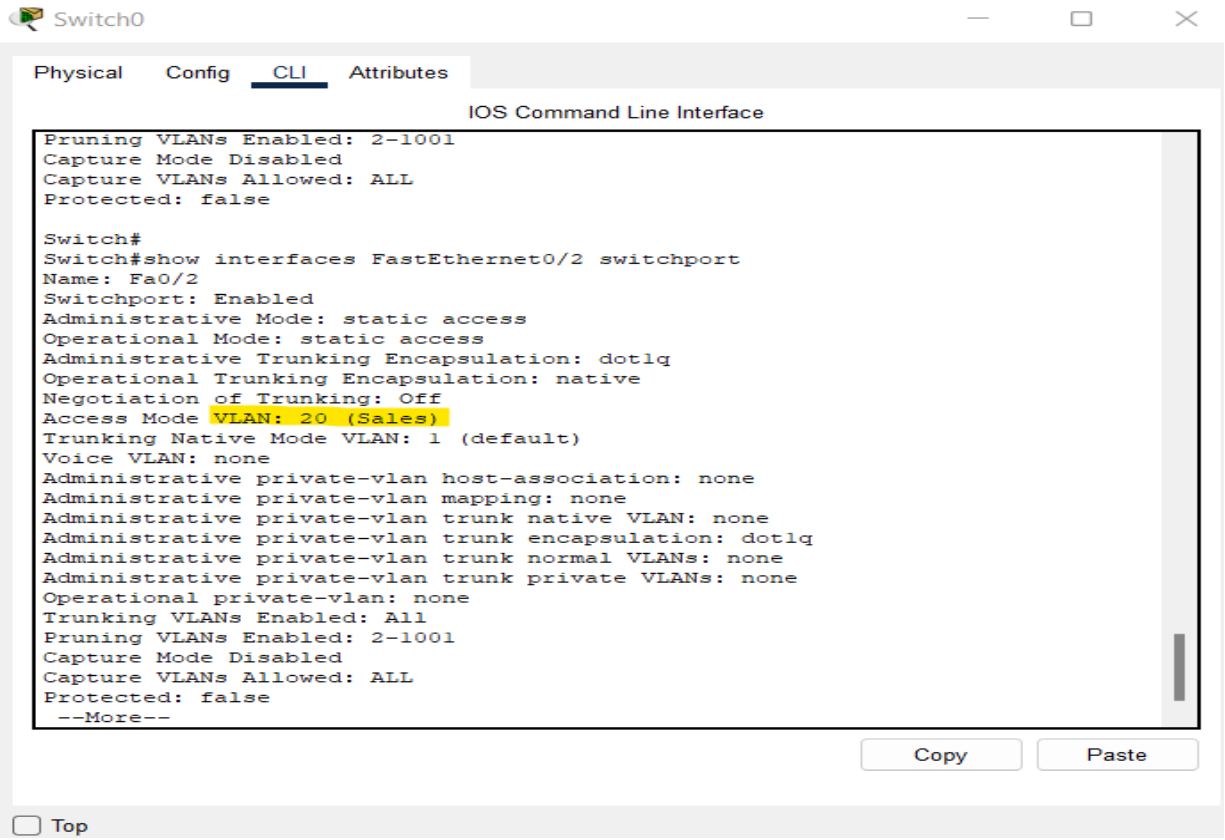
Using SHOW VLAN, SHOW Interfaces FastEtherent0/1 switchport, SHOW VLAN ALL PORTS, SHOW RUNNING-CONFIG we can see VLAN 10 is named Engineering, VLAN 20 is Sales.



4. Assign PC1 to Engineering



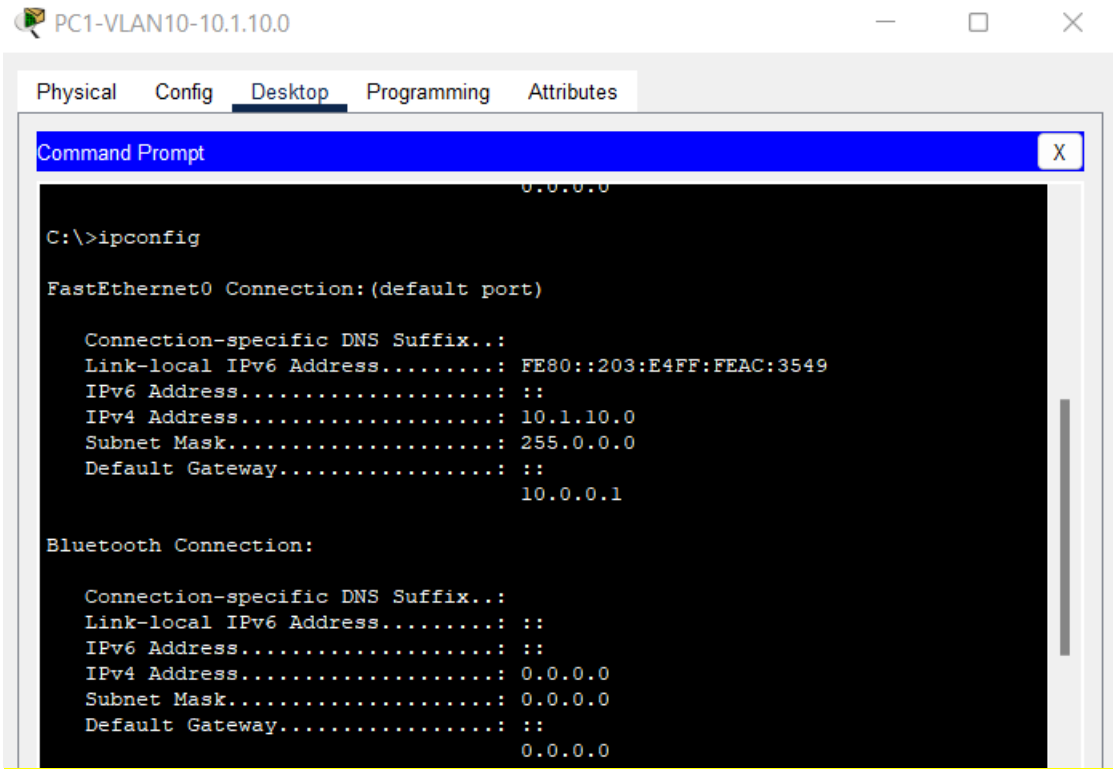
5. Assign PC2 to Sales

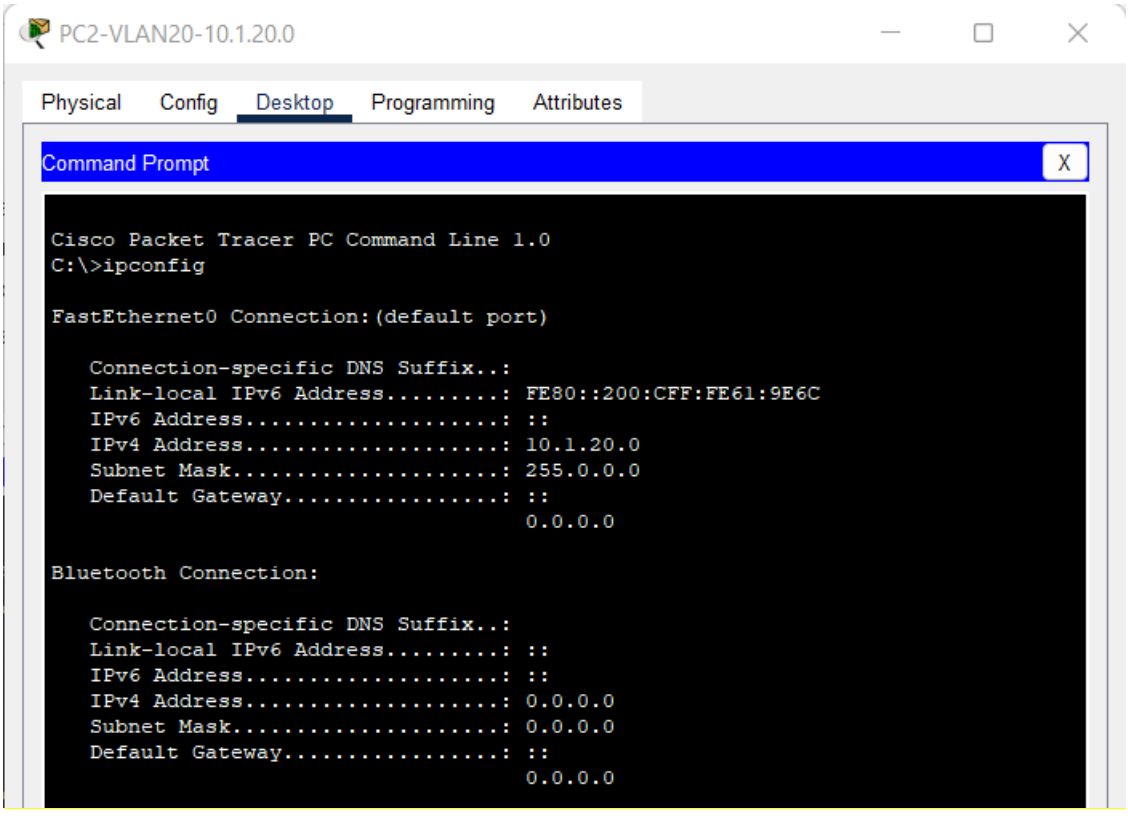


a. Assume no MAC entries exist in the switch. Explain step by step everything that happens in the network as soon as ping is initiated from PC1 towards PC2. Can PC1 ping PC2? Why or why not? [**10 points**]

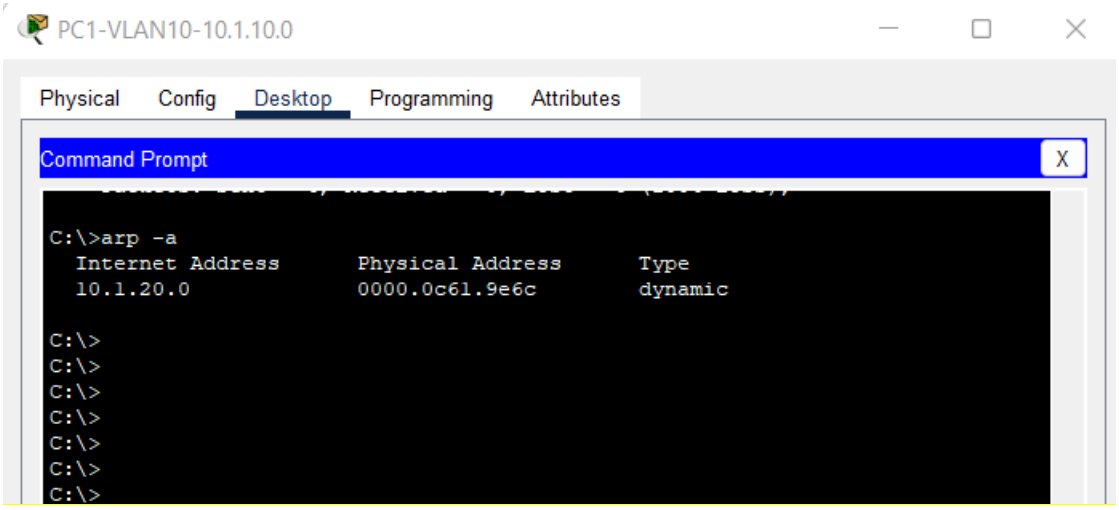
Different Network = Different VLAN = Different Broadcast Domain.
Layer-2 MAC Addresses are only significant to the Local VLAN/ Network/Broadcast domain. So, PING Fails. Packet gets dropped.

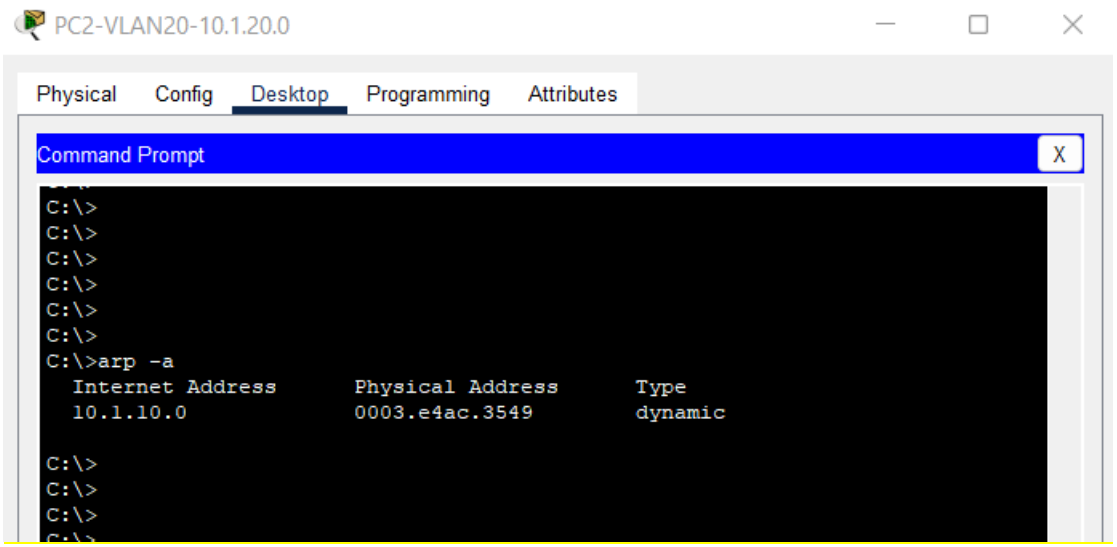
1. When Ping is initiated from PC1, the host creates IP Packet with its own IP address (10.1.10.0) as the source and (10.1.20.0) as the destination. And the first question PC1 asks itself is – is the destination host in the same network/subnet or not?
2. It answers this question by looking at its own IP address, its subnet mask and the destination IP address: using “ipconfig” command





3. PC1 will now build an Ethernet frame, enters its own source MAC address and asks itself the do I know the destination MAC address of the switch. It checks ARP Table to find an entry. If the entry is found (it is found because before enabling the vlan I tried to ping to PC2)





The Switch stores the MAC and ARP entries in the ARP Table. But the PING cannot happen because the VLAN 20 is configured on a different port and VLAN 10 is configured on a different port. And they belong to different Network. Assigning a different VLAN to switch port in a network means creating a different LANS hence the name VLAN.

6. Enable Telnet on the switch
    a. What should be done so PC1 can Telnet to the switch? [**5 points**]

    To enable telnet to the switch, the interface FastEthernet 0/1 connecting to the VLAN10 port must be configured with telnet access. And can be done

    (Config)#Int Vlan 10

    (Config-if)#Ip add 192.168.10.1 255.255.255.0

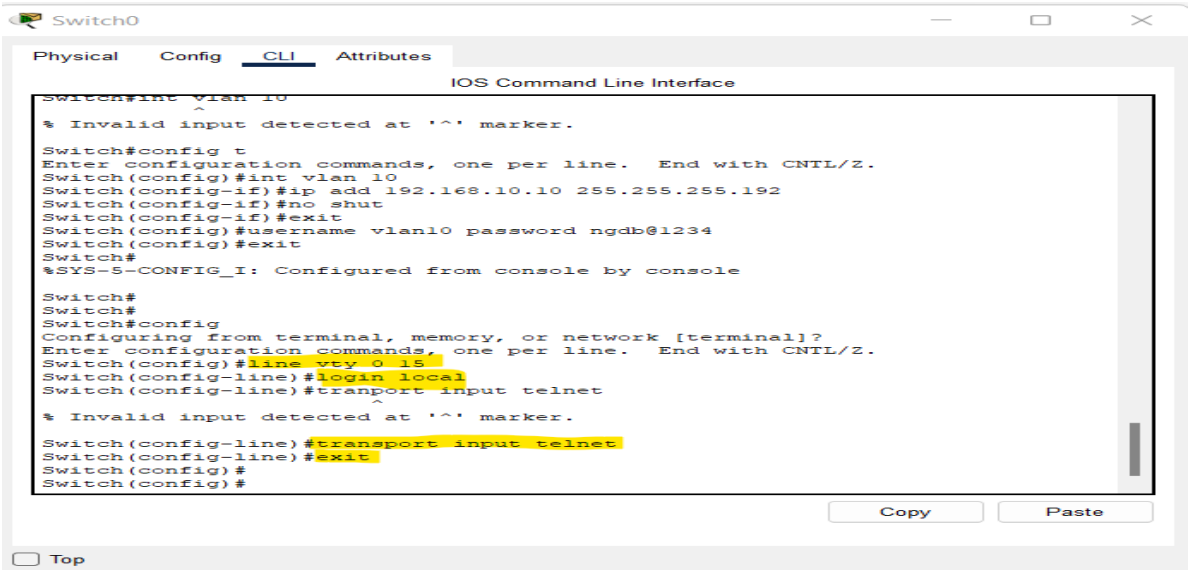
(Config-if)#no shut

(Config-if)#username Vlan10 Password Cisco

(Config-if)#line vty 0 15

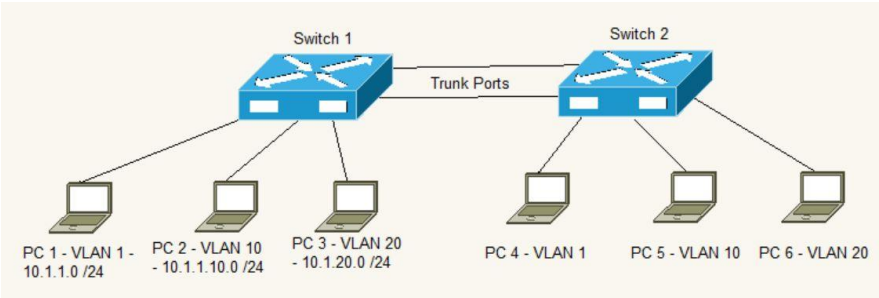
(Config-if)#login local |

(Config-if)#transport input telnet

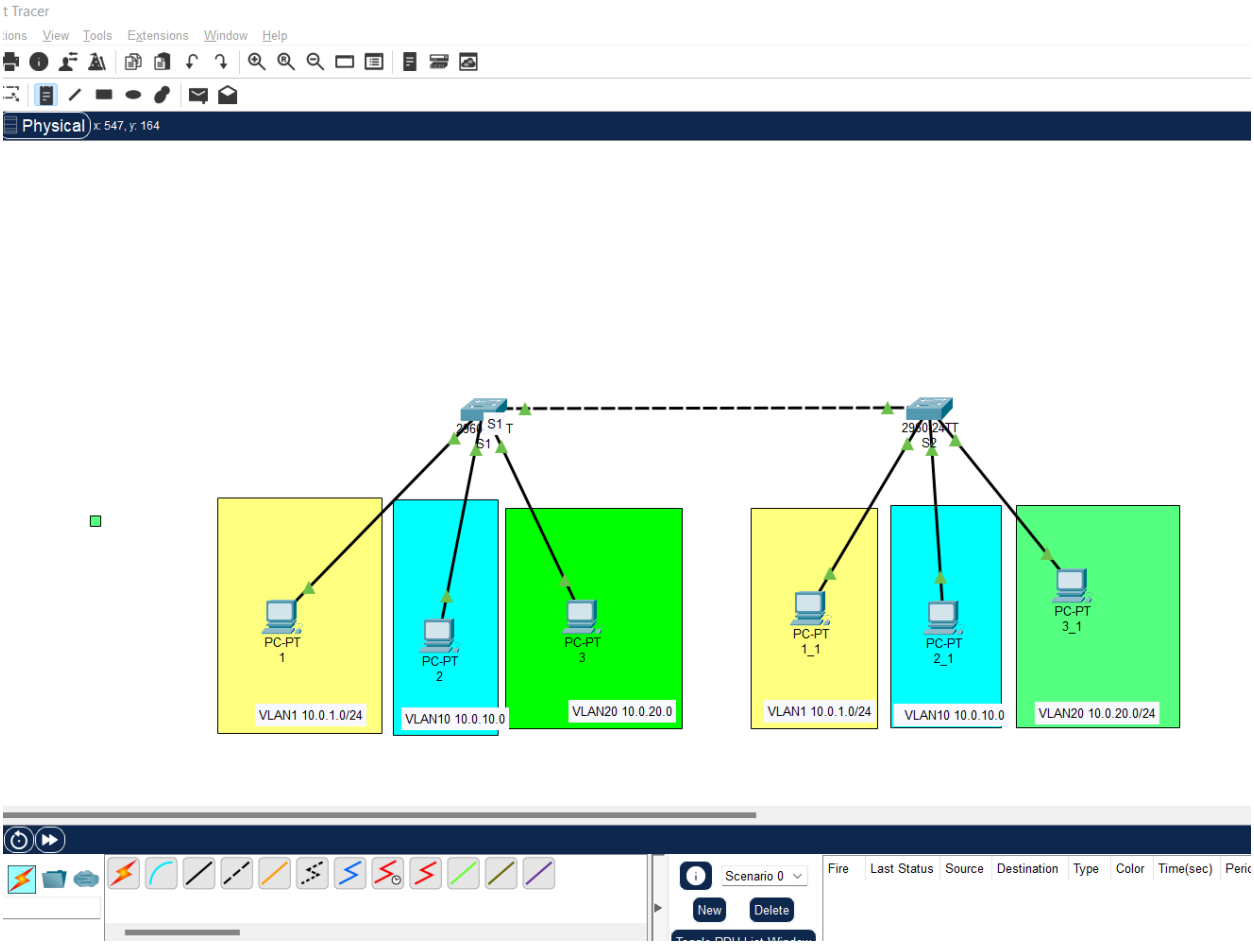


Objective 2 - Switch VLAN and Trunk Configuration

This objective will configure multiple VLANs on multiple switches and connect the switches via ports.



1. Setup the network as indicated in the diagram (*hint: Switch2 configuration should be a duplicate of Switch1*)

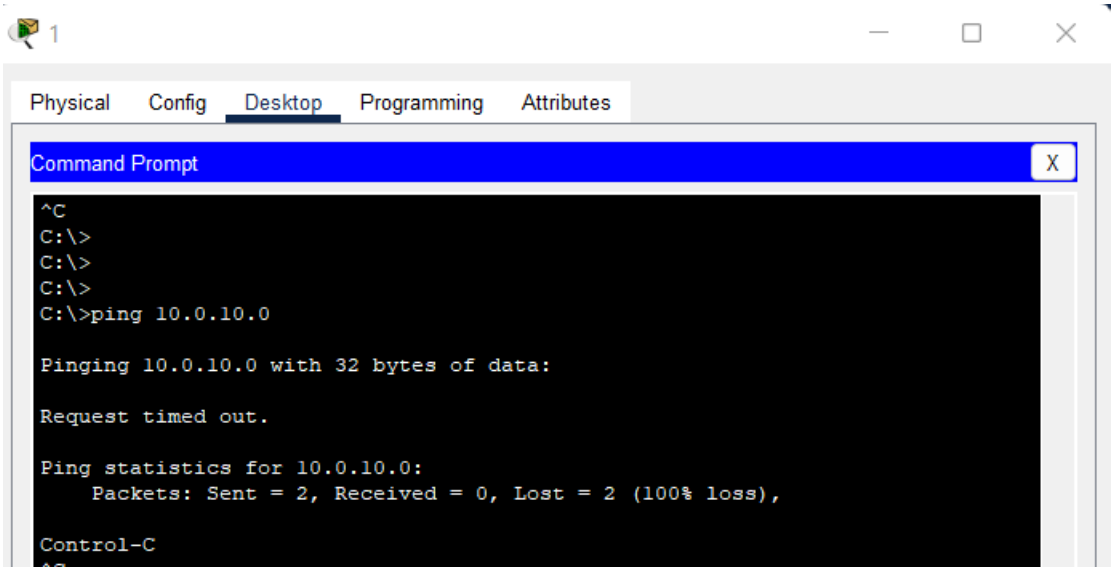


2. In what IP subnet is IP address of PC5 present? What design considerations did you have to make when choosing this IP subnet? **[3 points]**

IP Address of PC5 is 10.0.10.0 (same as PC2 because we duplicating) and its IP Subnet is a Class A network with default subnet mask of 255.0.0.0 and have 0-127 as first octet. The address is 10.0.10.0 who's first octet is "10" which is between 1 and 126. so it's a class A subnet.

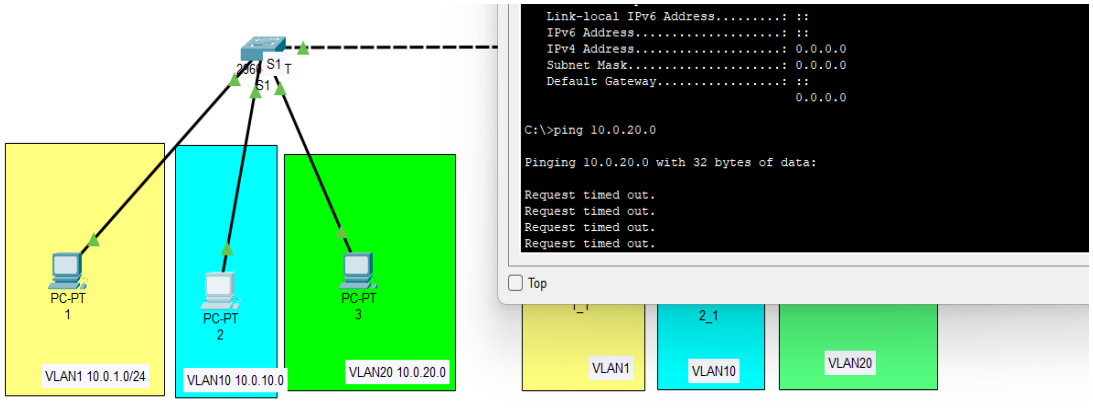
Can PC1 and PC2 Ping each other? Why or why not? [**3 points**]

No PC1 and PC2 cannot ping each other because they belong to different VLAN. And different network. Ping / communication can happen only b/w the the same VLAN. Different VLAN's means different LAN's but virtually configured switches. So ping Fails.



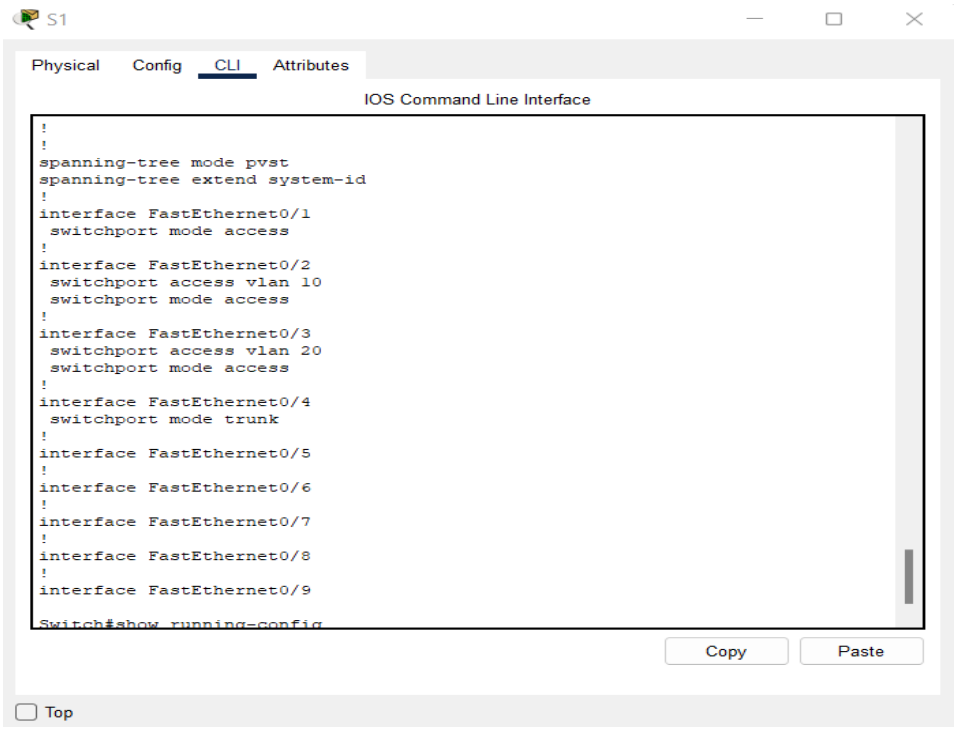
3. Can PC2 and PC3 Ping each other? Why or why not? [**3 points**]

No. PC2 and PC3 cannot ping each other because they belong to different VLAN. And different network. Like mentioned in the above answer, the objective of VLAN's is to connect the same VLAN's route/communicate with each other and enable higher security. (for ex : Sales_1 VLAN will only talk to Sales_2 not Engineering likewise PC2 can talk to PC5 but notPC2 to PC3.

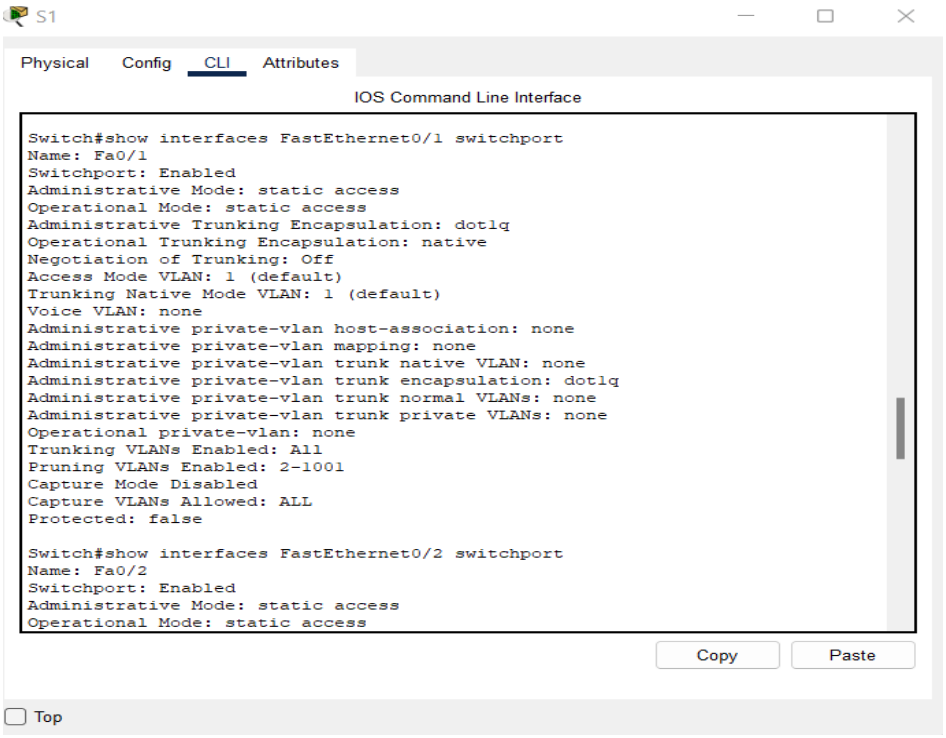


4. Configure the switches so PCs can ping within the same VLAN.
    a. Provide the relevant configuration from both switches [**5 points**]

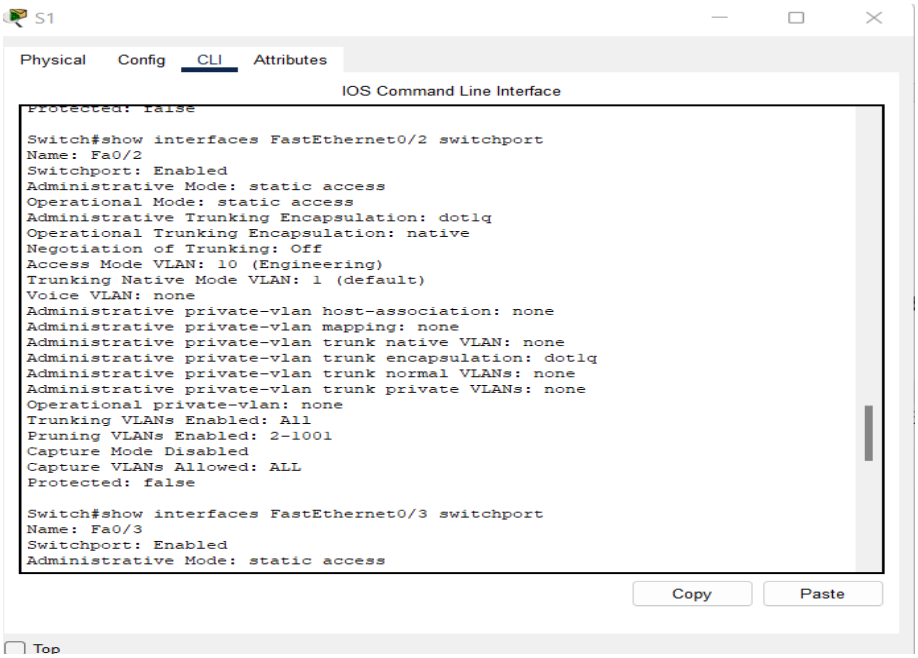
Switch 1: Configured with VLAN1, VLAN 10, VLAN 20 and Trunk Port



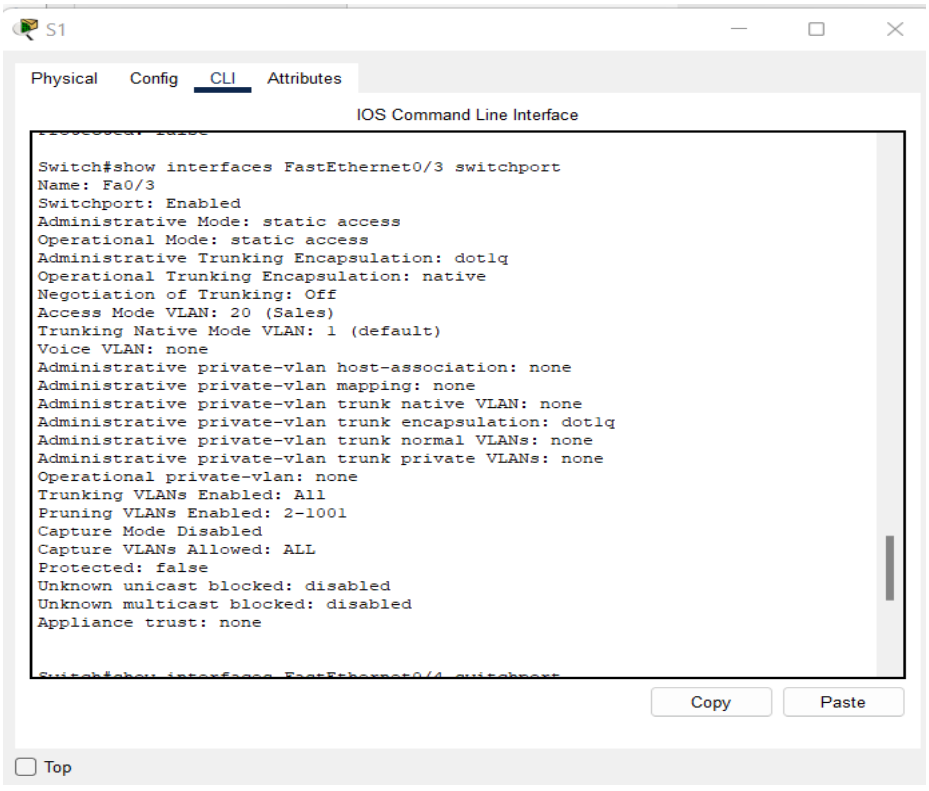
Fa0/1 VLAN 1 Configuration on S1:



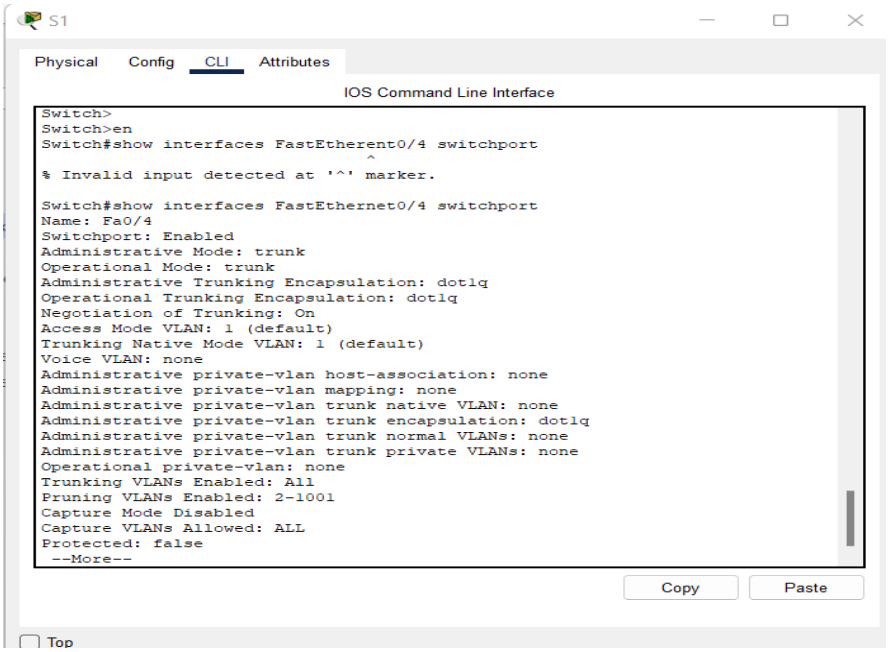
Fa0/2 VLAN 10 Configuration on S1:



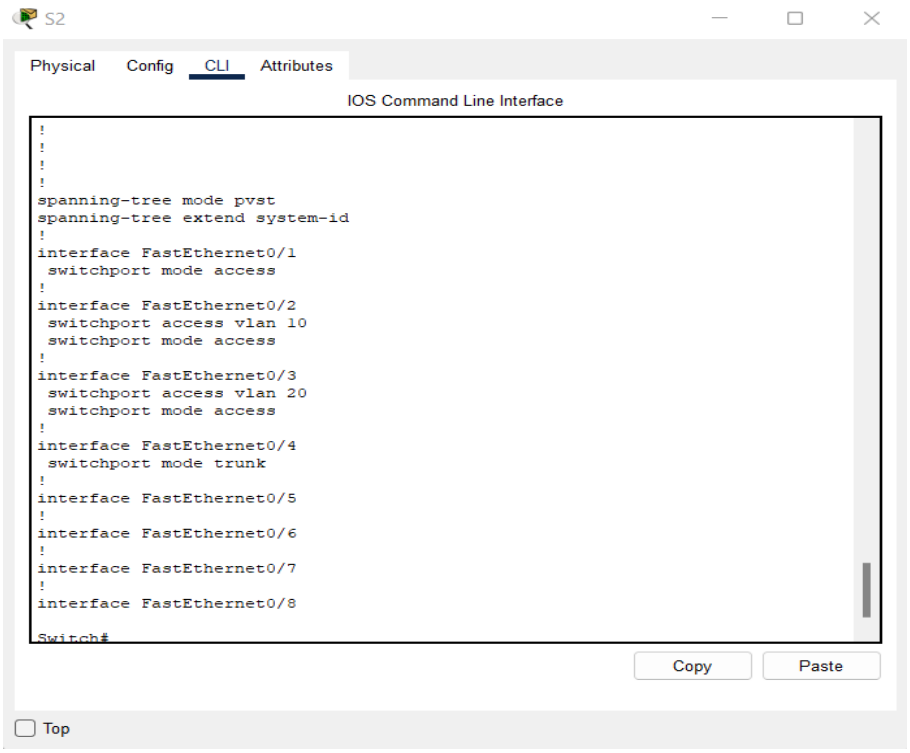
Fa0/3 VLAN 20 Configuration on S1:



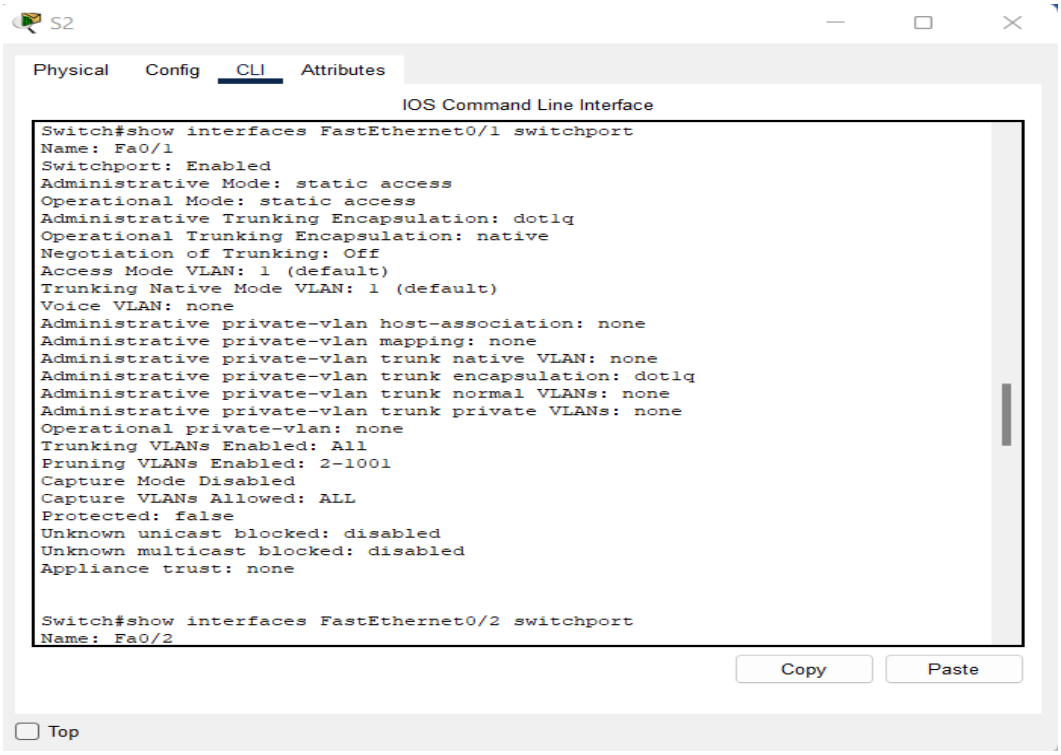
Fa0/4 VLAN 20 Configuration on S1:



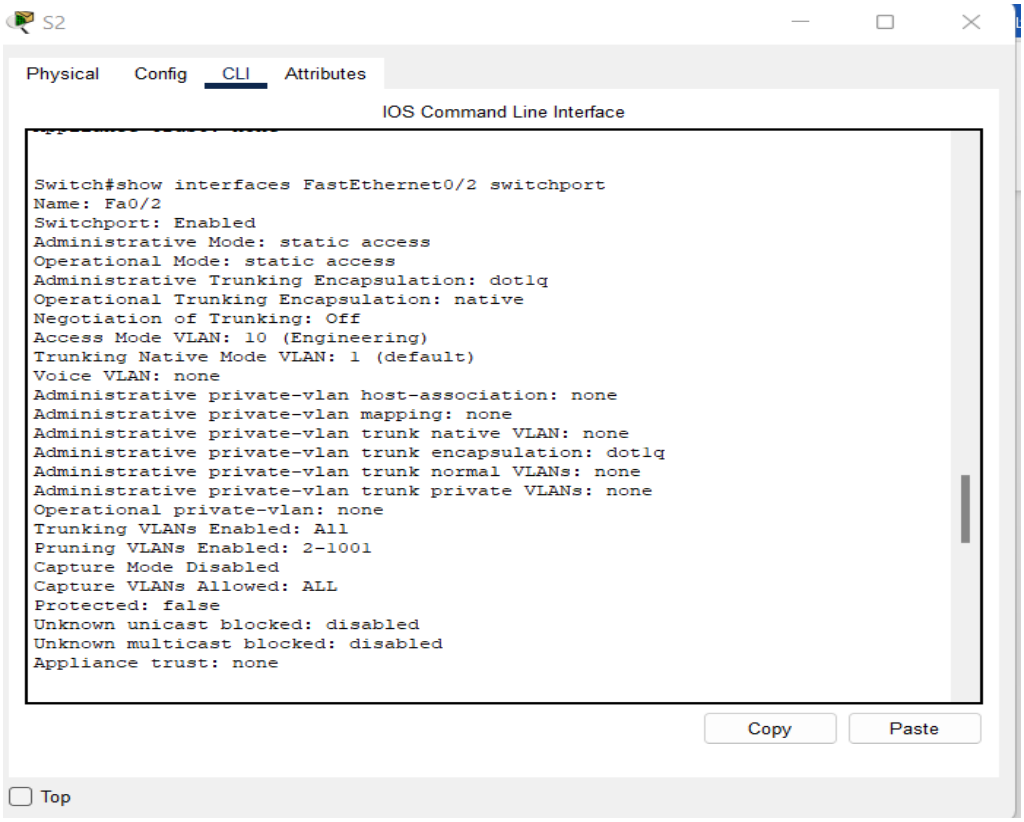
Switch 2 : Configured with VLAN1, VLAN 10, VLAN 20 and Trunk Port



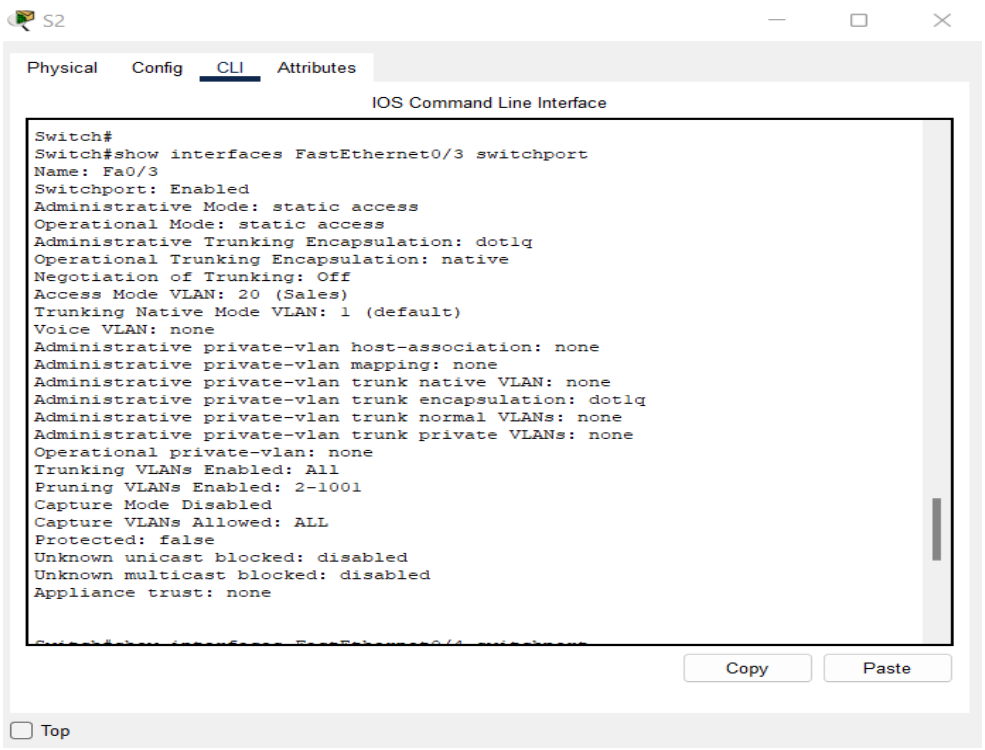
Fa0/1 VLAN 1 Configuration on S2:



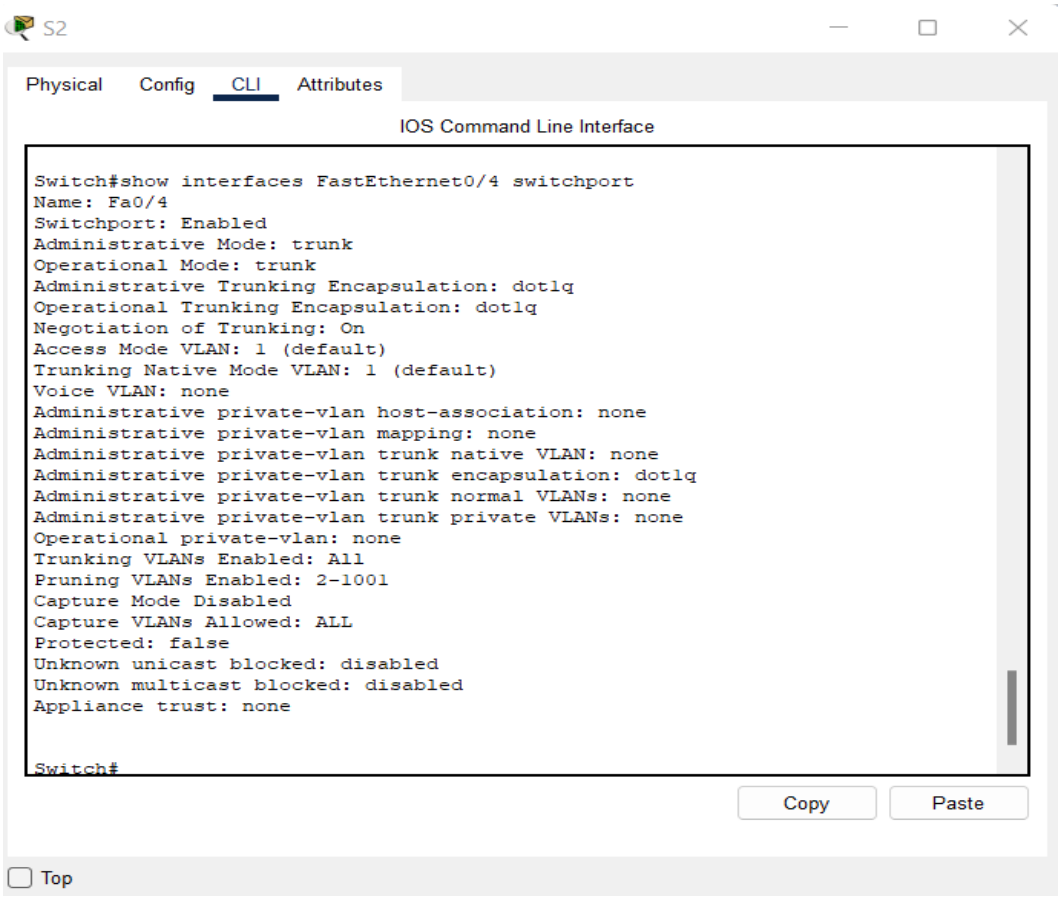
Fa0/2 VLAN 10 Configuration on S2:



Fa0/3 VLAN 20 Configuration on S2:



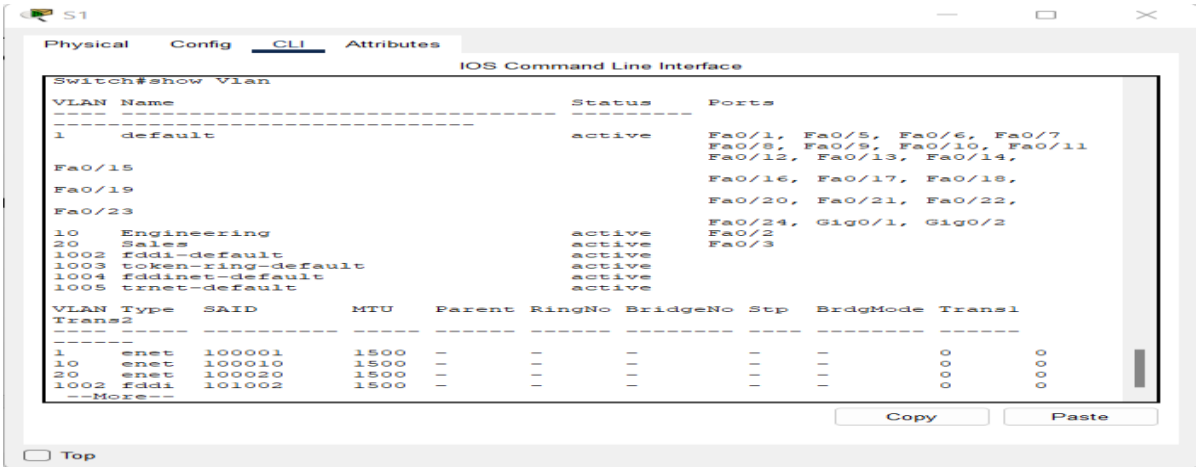
Fa0/4 Trunk Port Configuration on S2:



5. Explain what must be done to allow all PCs to Ping each other [**10 points**]

Step 1 :: Create Network Topology and configure the IP address to the host's

Step 2: Login into Switch1 CLI and first check VLAN's using "SHOW VLAN".



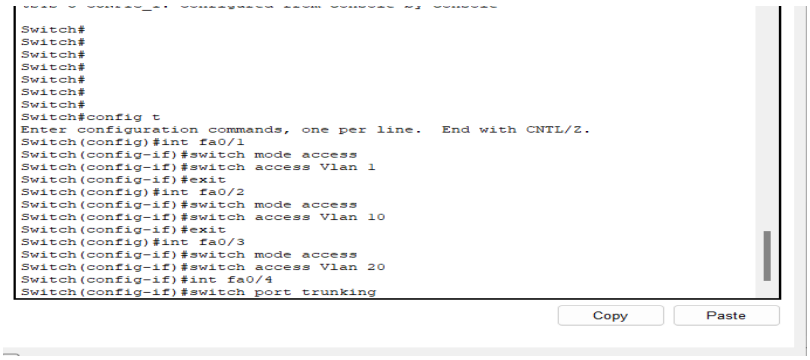
Then, Create the VLANs using :

Switch# Config t

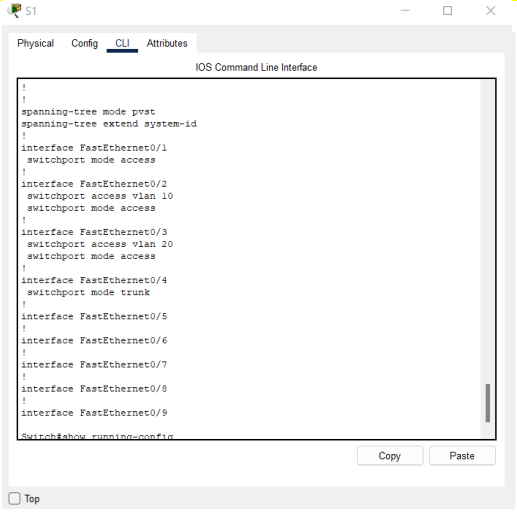
Switch(Config) Vlan 10

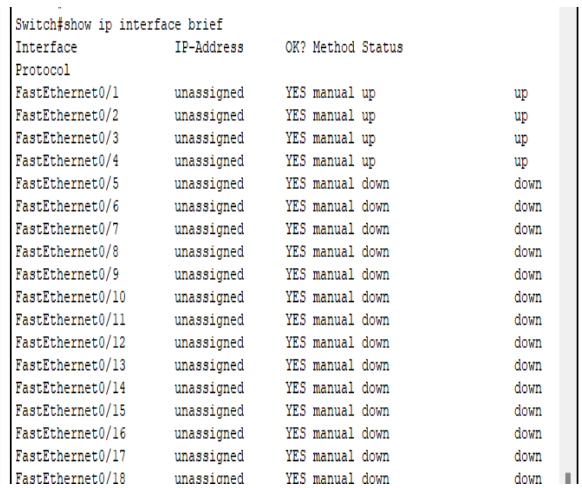
Switch(Config-line) Name Engineering / PC1 or whatever is required

Step 3: Configure the VLANS to interfaces/port using "Switch mode access"



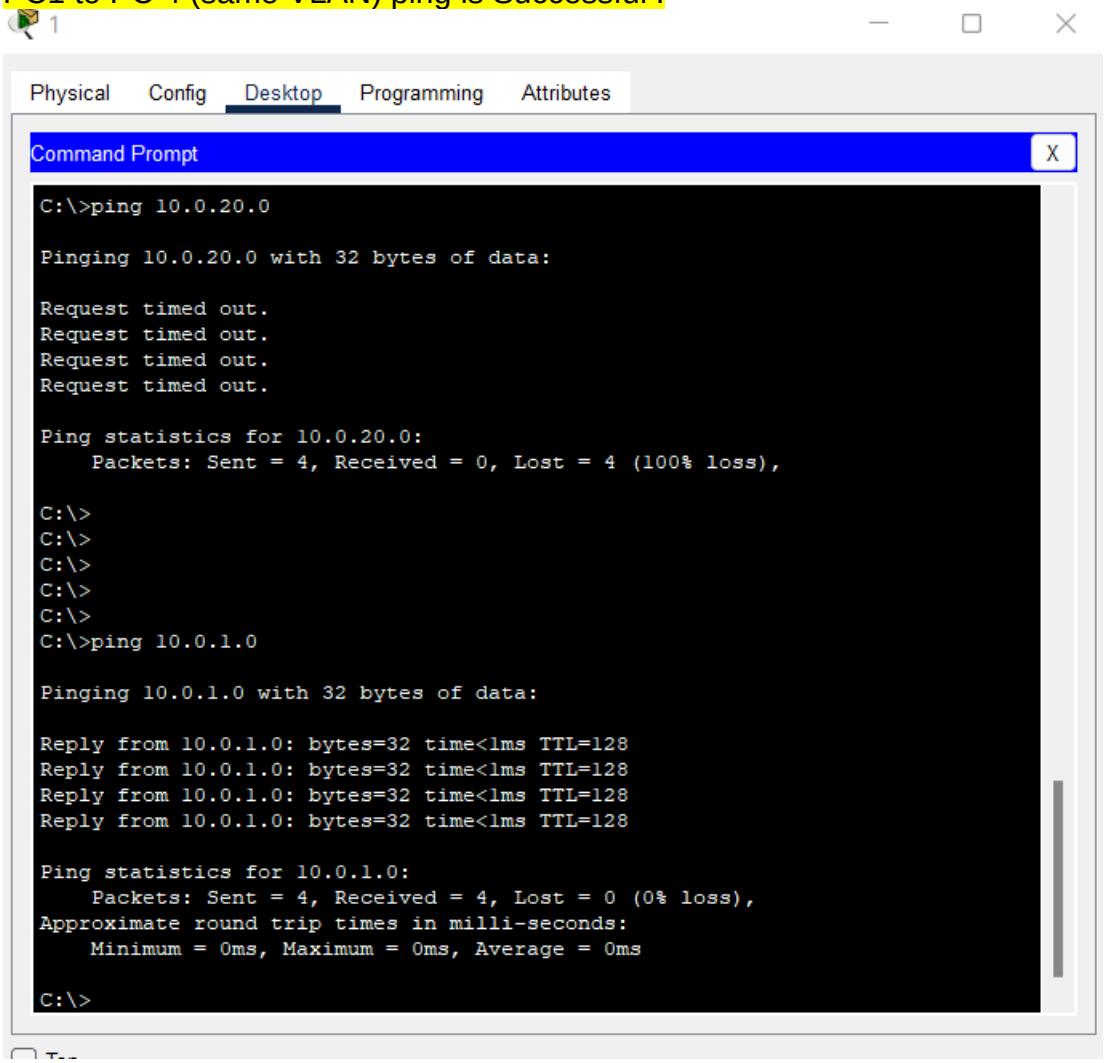
Step 4: Check the running-config and state of the interface :



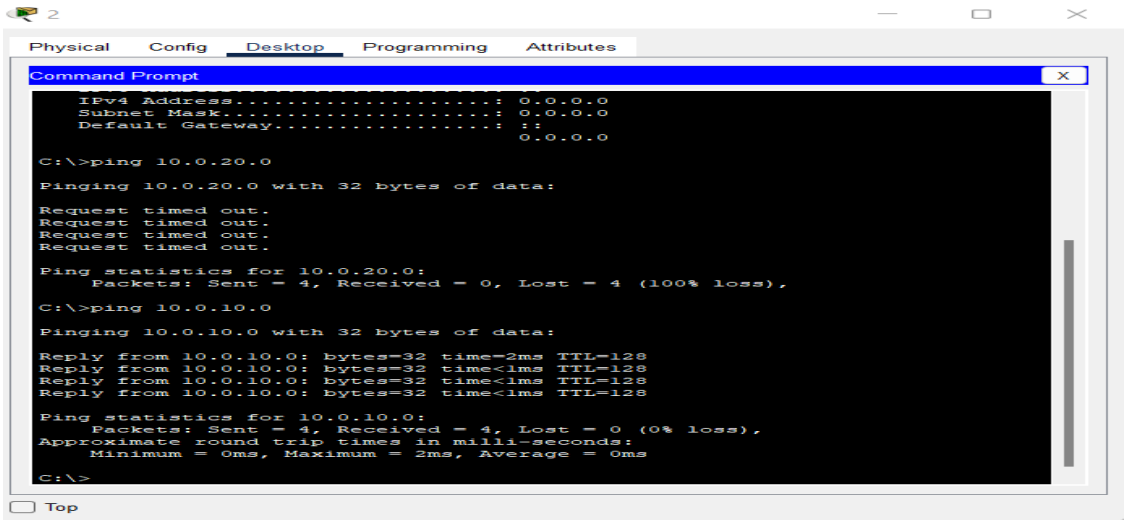


Step 5: Once the VLA's are configured and the interfaces are mapped and trunk port is enabled using "switch port Trunking" the Network is ready to route / communicate with the same VLAN's

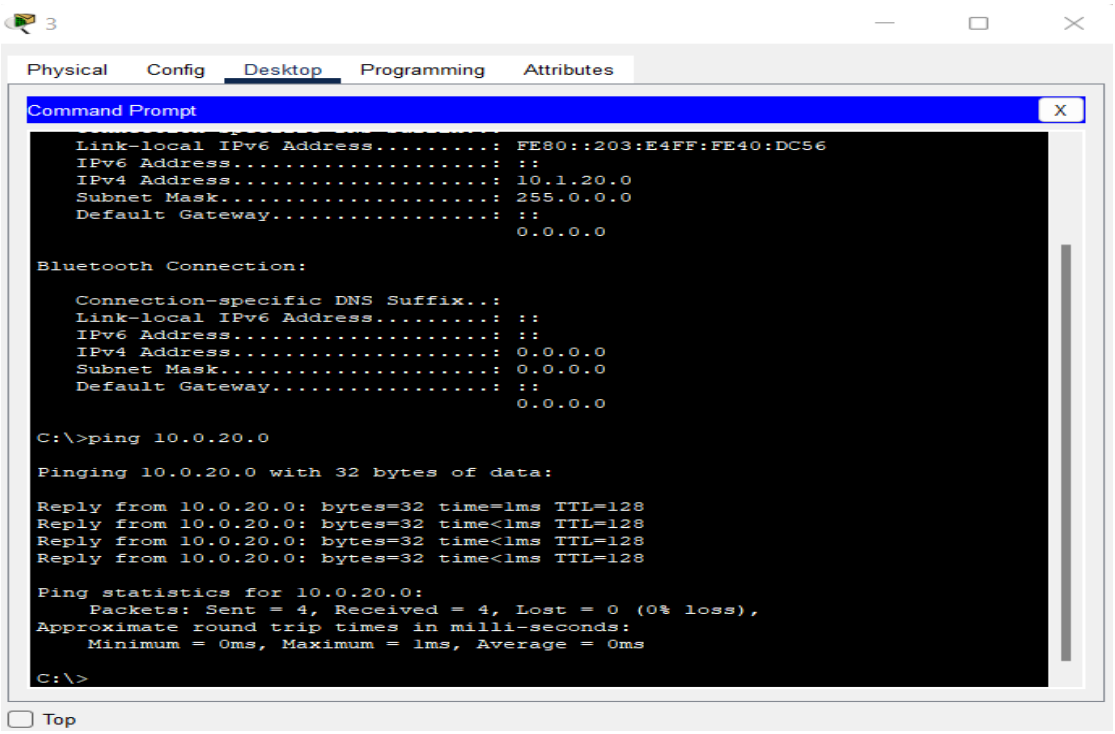
PC1 to PC 4 (same VLAN) ping is Successful :



PC 2 to PC 4 (Same VLAN) Ping is successful :

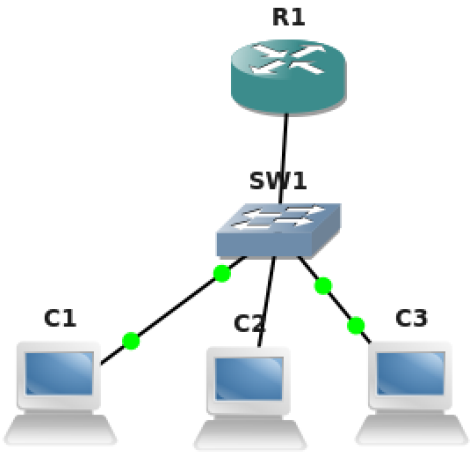


Ping from PC3 to PC6 is successful:



Objective 3 – Inter-VLAN Routing "Router on a Stick"

This objective will configure multiple VLANs on a switch, and uplink the switch to a router via a trunk port and we will use this router to route between VLANs. Since the router is using one physical port to route incoming and outgoing traffic, we call it "Router on a Stick"



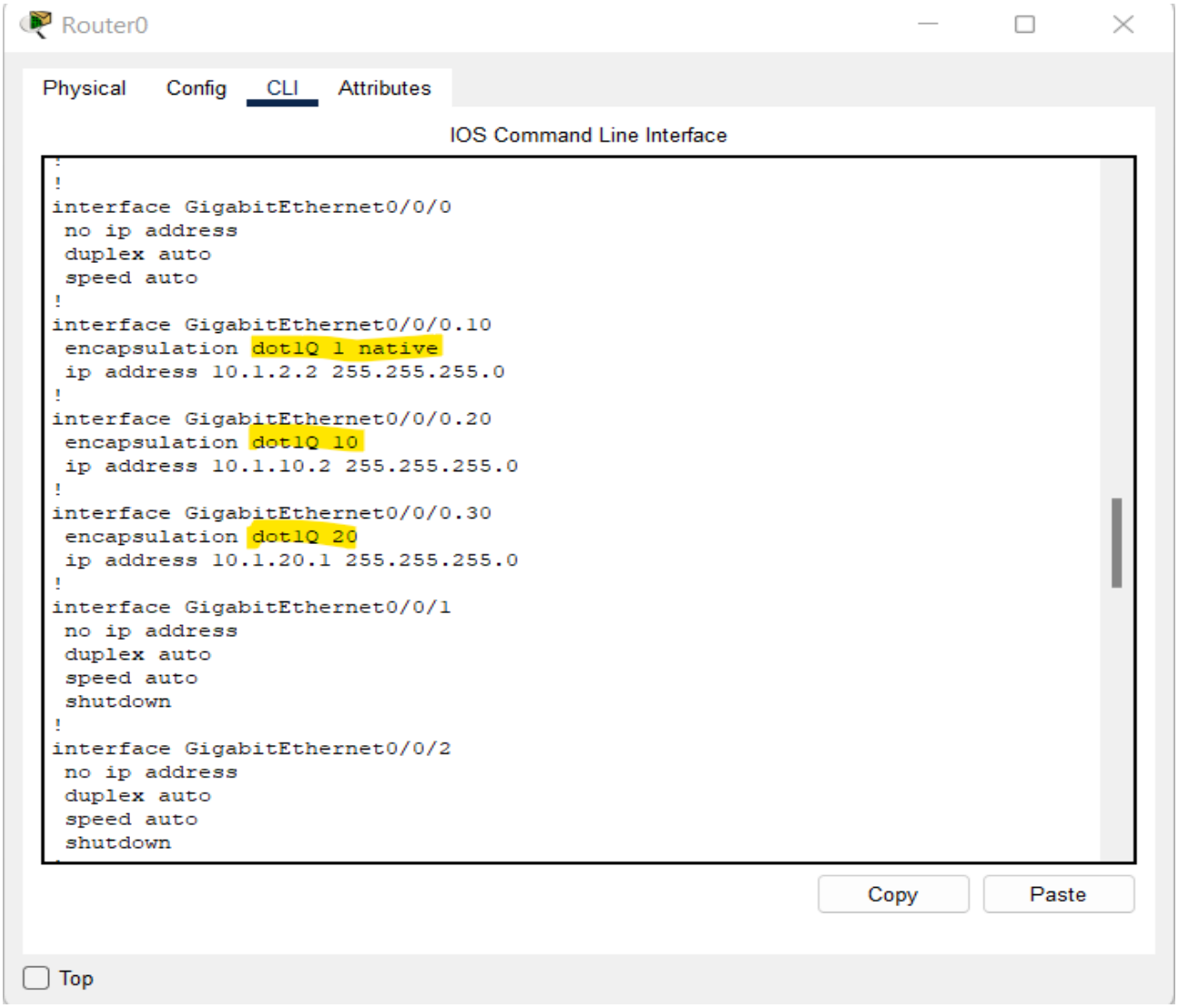
PC1- VLAN**1** – 10.1.1.0/24	PC2- VLAN**10** – 10.1.10.0/24	PC3- VLAN**20** – 10.1.20.0/24

1. What are sub-interfaces on a router? What are its advantages? **[2 points]**

A Sub-interface is a virtual interface created by dividing one physical interface into multiple logical interfaces. Example, in the below topology I have divided gigabitEthernet0/0/0 into gigabitEthernet0/0/0.10 for Vlan 1 , gigabitEthernet0/0/0.20, for Vlan 10 gigabitEthernet0/0/0.30 for Vlan 20.

2. Configure VLAN sub-interfaces on the router (VLAN1 “native”, VLAN 10, and VLAN 20).

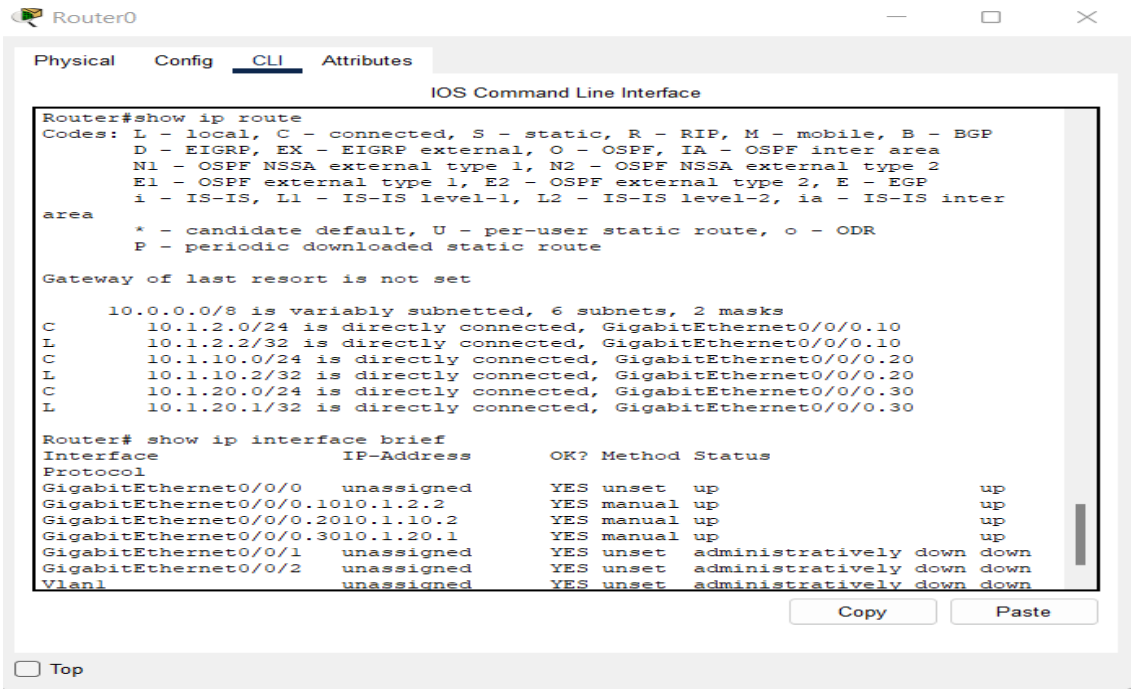
VLAN sub-interfaces on the router (VLAN1 “native”, VLAN 10, and VLAN 20) are configured with encapsulation.

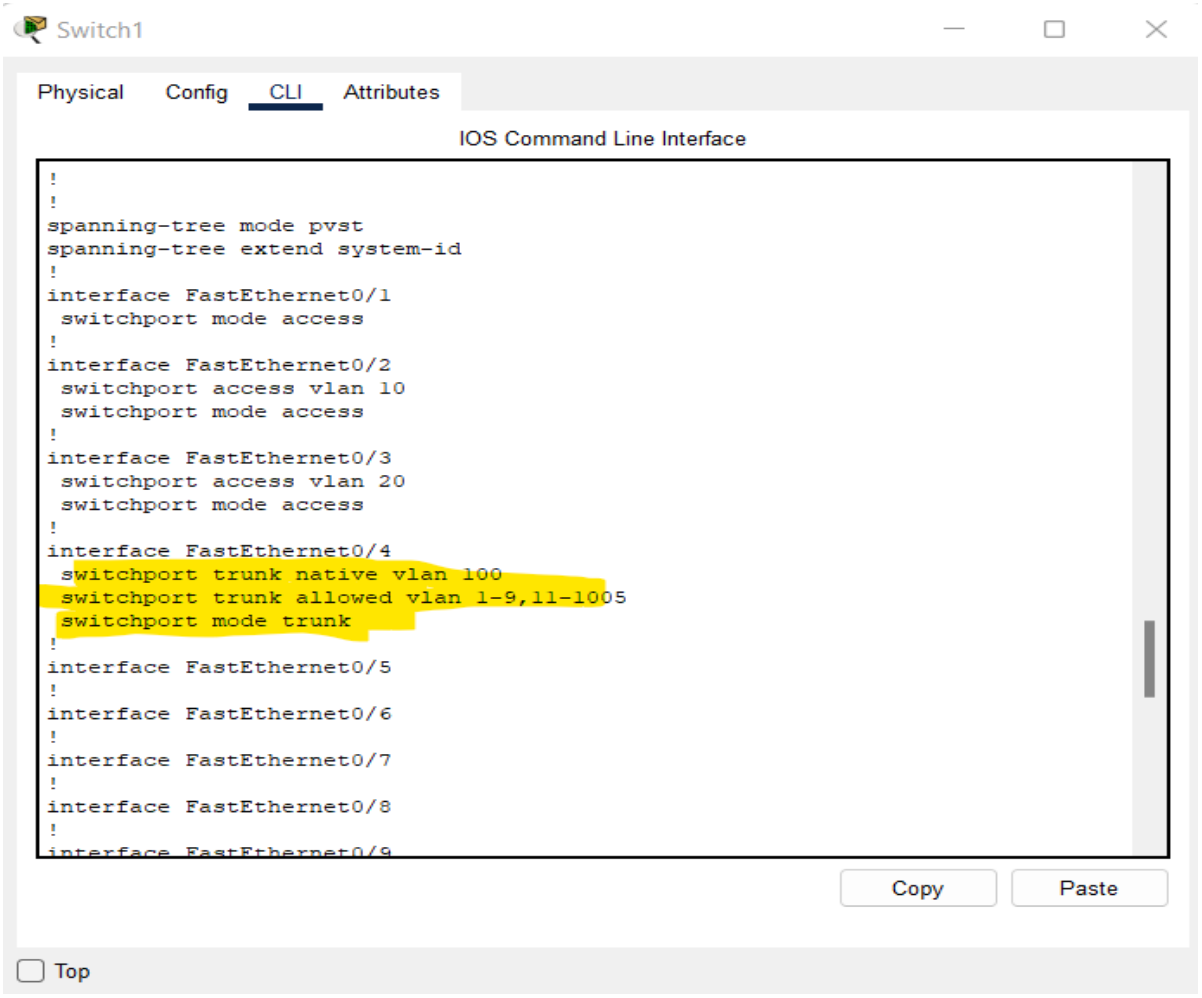


a. Submit the router configuration that indicates the trunking setup.

[**10 points**]

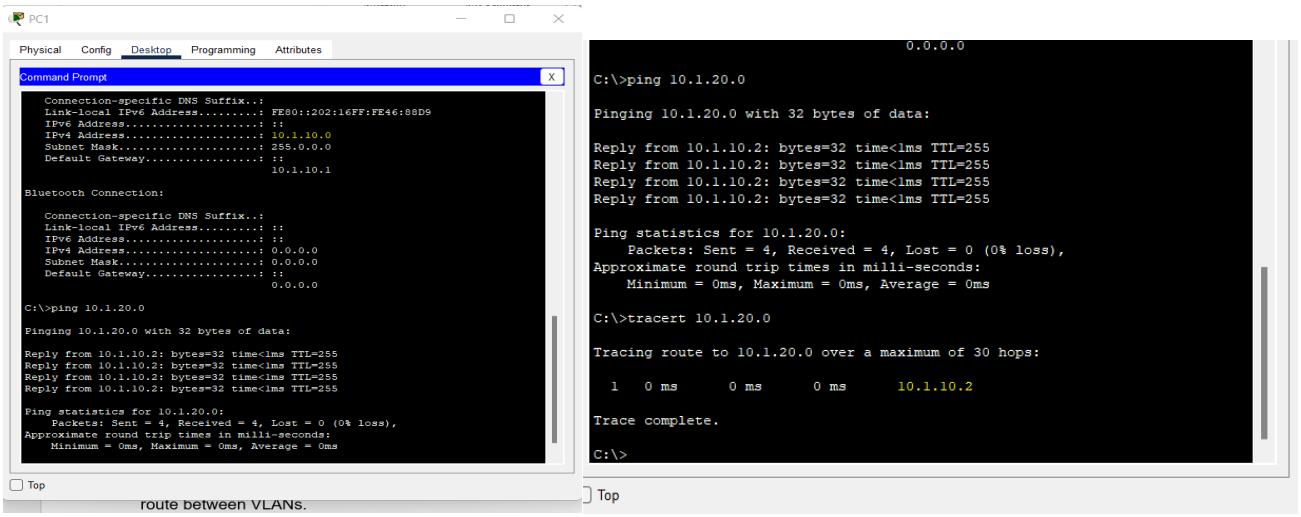
Router Configuration with encapsulation and sub-interfaces mapped to VLAN's:





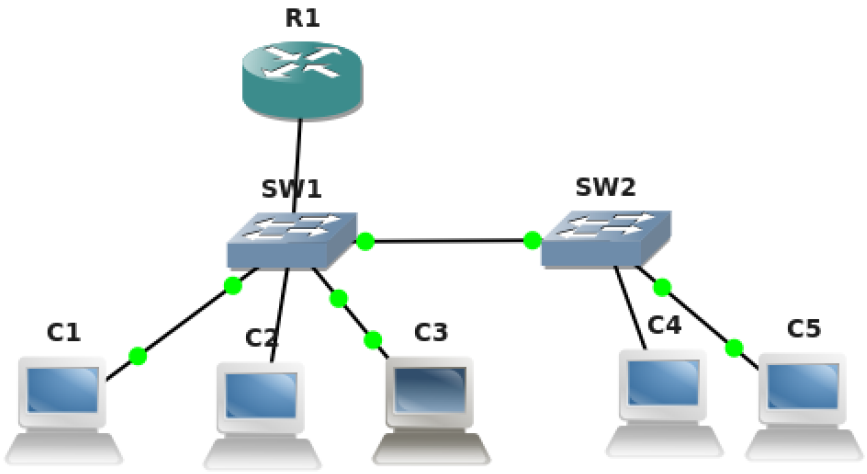
3. Verify all PCs can Ping each other.
    a. Paste screenshots of trace route from the PC to indicate the packets are traversing through the router for inter-VLAN communication. [**5 points**]

The ping command from PC1 to PC2 (10.1.10.0 to 10.1.20.0) through router sub-interface 10.1.10.2. And the Tracert from PC1 to PC2 indicatng packet traverse through router w hop



Objective 4 – Inter-VLAN Routing 2: Multiple switches

This objective will configure multiple VLANs on multiple switches and use a router to route between VLANs.

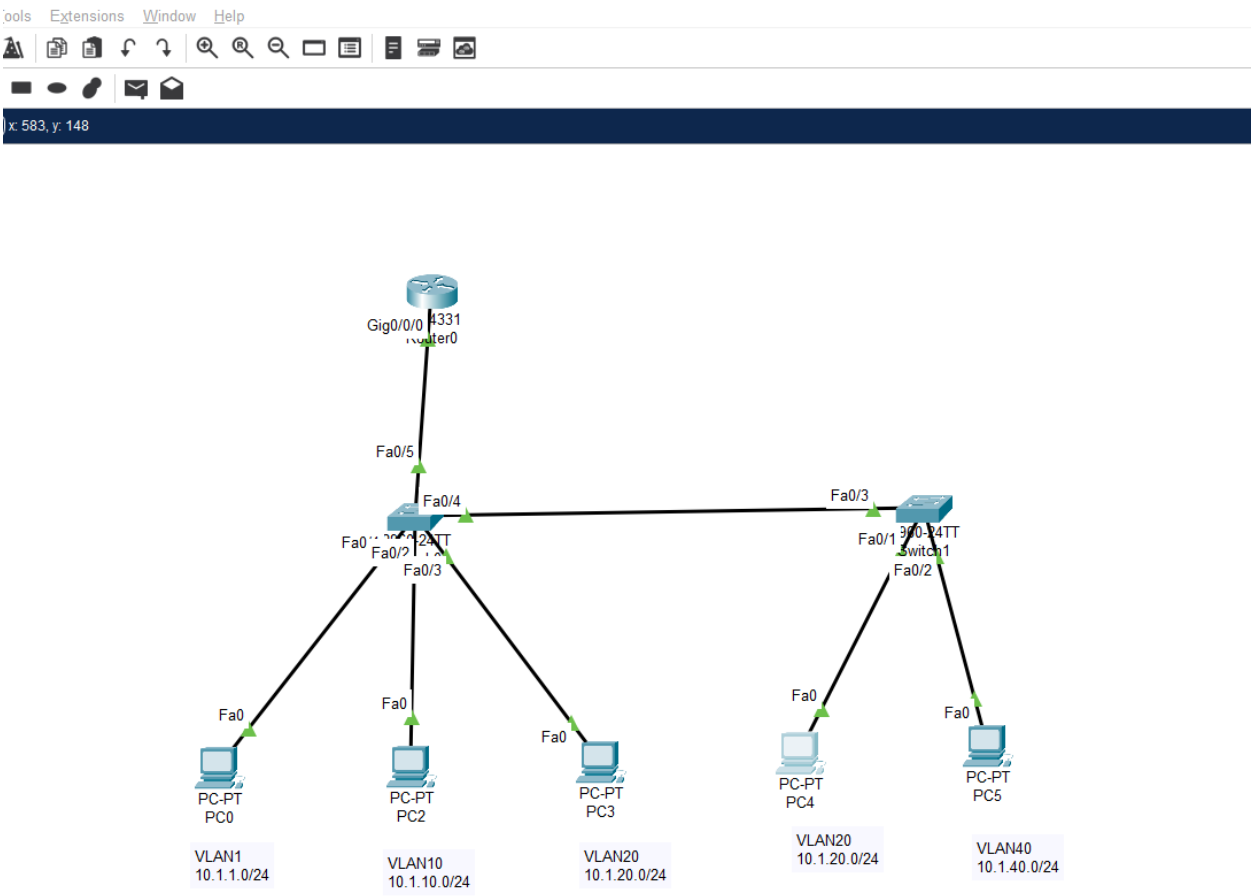


PC1- VLAN**1** – 10.1.1.0/24	PC2- VLAN**10** – 10.1.10.0/24	PC3- VLAN**20** – 10.1.20.0/24	PC4- VLAN**20** – IP subnet-?	PC5- VLAN**40** – 10.1.40.0/24

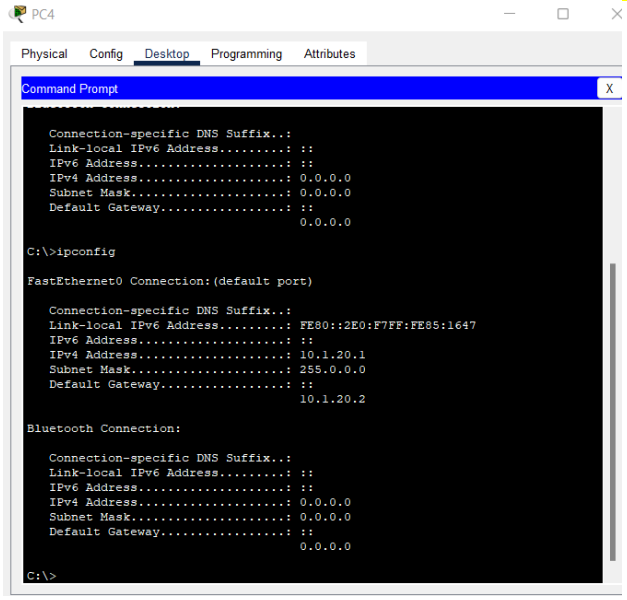
1. Look at the above diagram. What is the type of port you should configure between the two switches? (Eg: access port **or** trunk port **or** routed port **or** any other port?)
Why do you have to use this port type? Justify. **[3 points]**

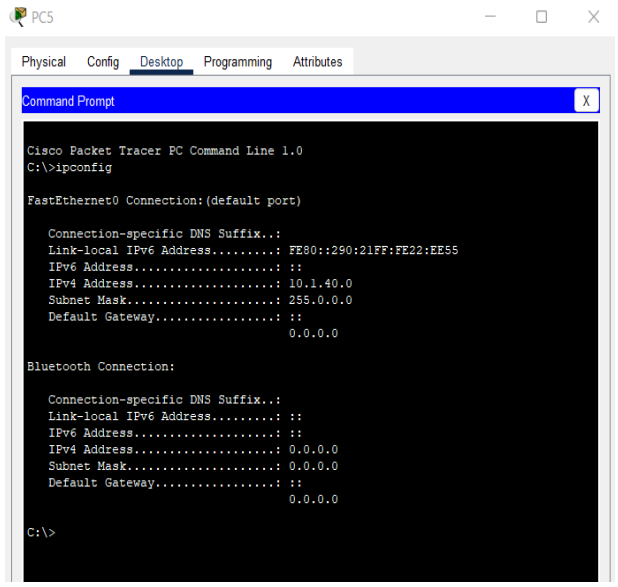
I used Trunk port between sw1 and sw2. Because unlike access link, a trunk link doesn't belong to single vlan but can carry traffic from the any number of vlan's over a point-to-point link and here each switch is connected to more than single vlan hence the usage of trunk port.

2. At the end of this lab objective all hosts must be able to ping each other. From your previous setup, you added Switch2 and hosts PC4 and PC5. What extra configurations did you have to add to this setup to establish connectivity between all hosts? Mention each device you had to configure or make changes to achieve this. Just mention snippets of extra configuration you had to add on each device you configured. Also attach screenshot of successful pings and traceroute from PC2 to PC5.
[15 points]

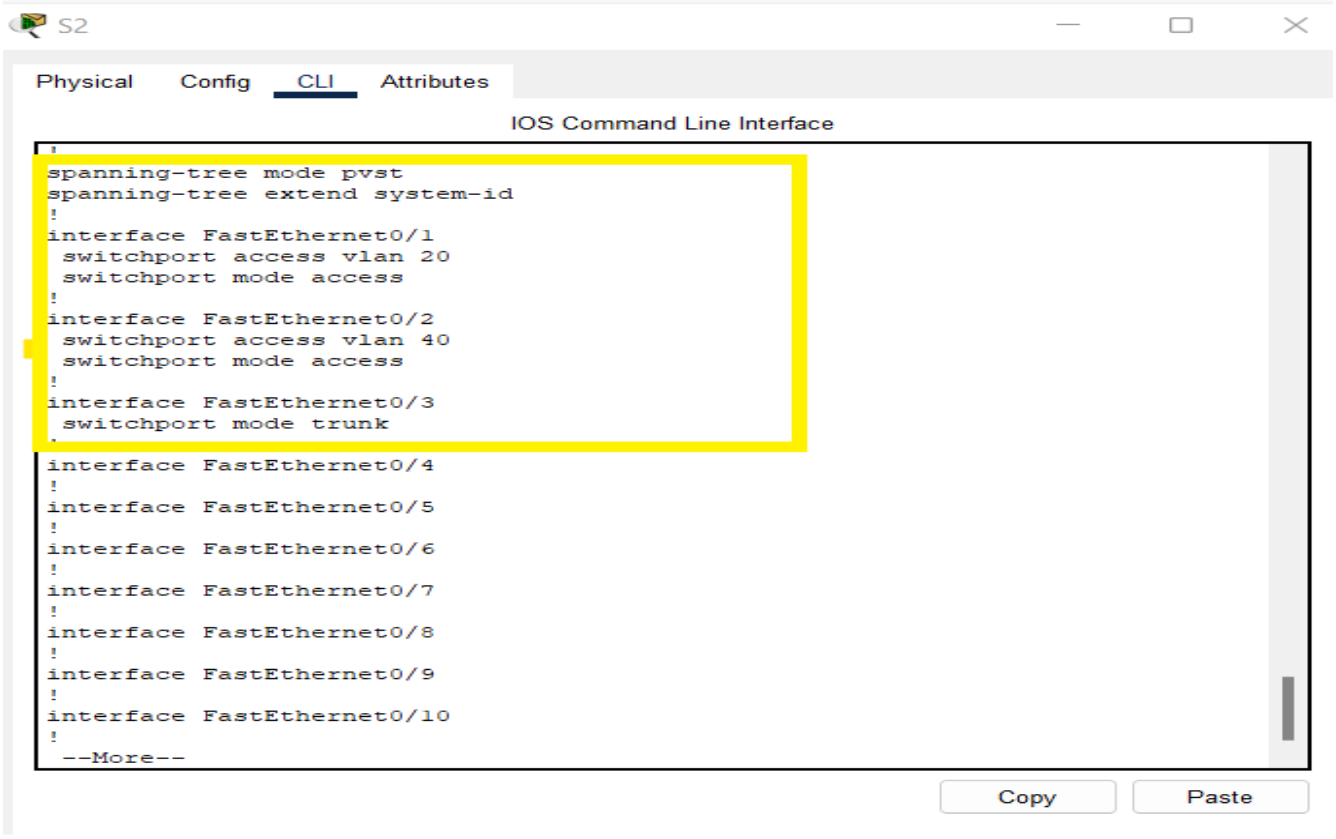


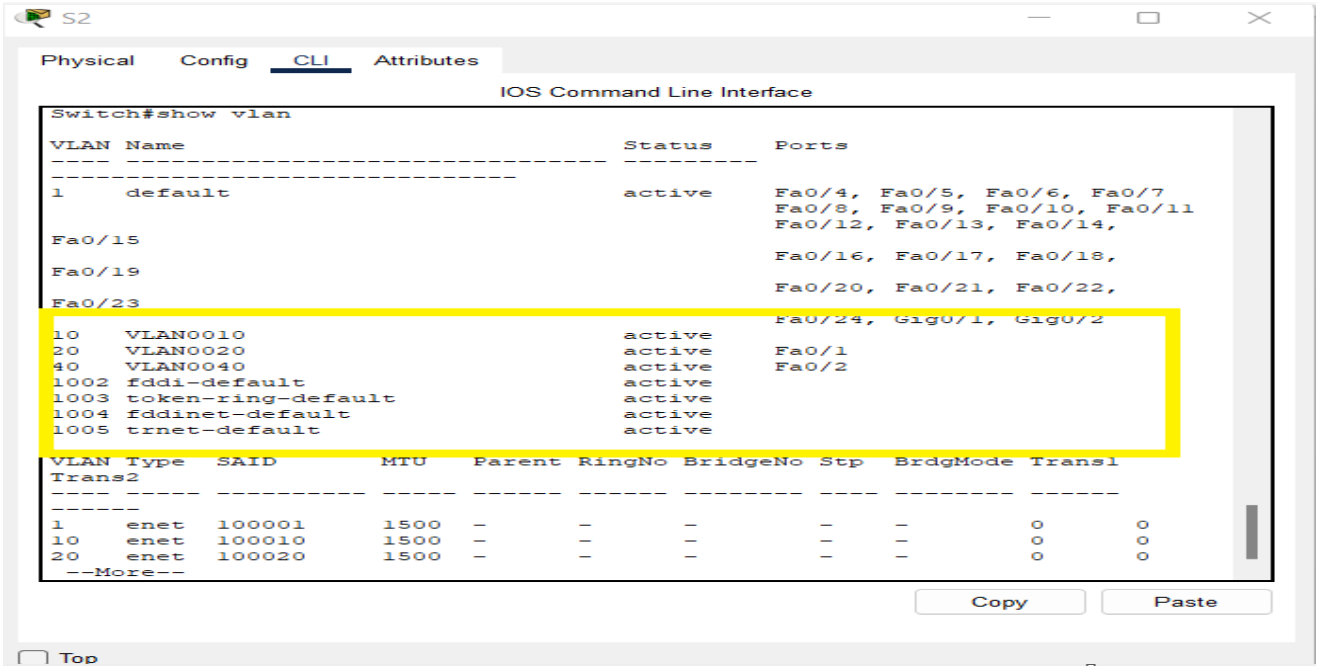
To add pc4, pc5 both the hosts are configured with ip addresses.





And the switch 2 is configured with the VLAN 20 and VLAN 40 configurations





S2

Physical Config CLI Attributes

IOS Command Line Interface

```
Switch#
Switch#
Switch#show interfaces Fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Access Mode VLAN: 20 (VLAN0020)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

 --More--
```

Copy Paste

S2

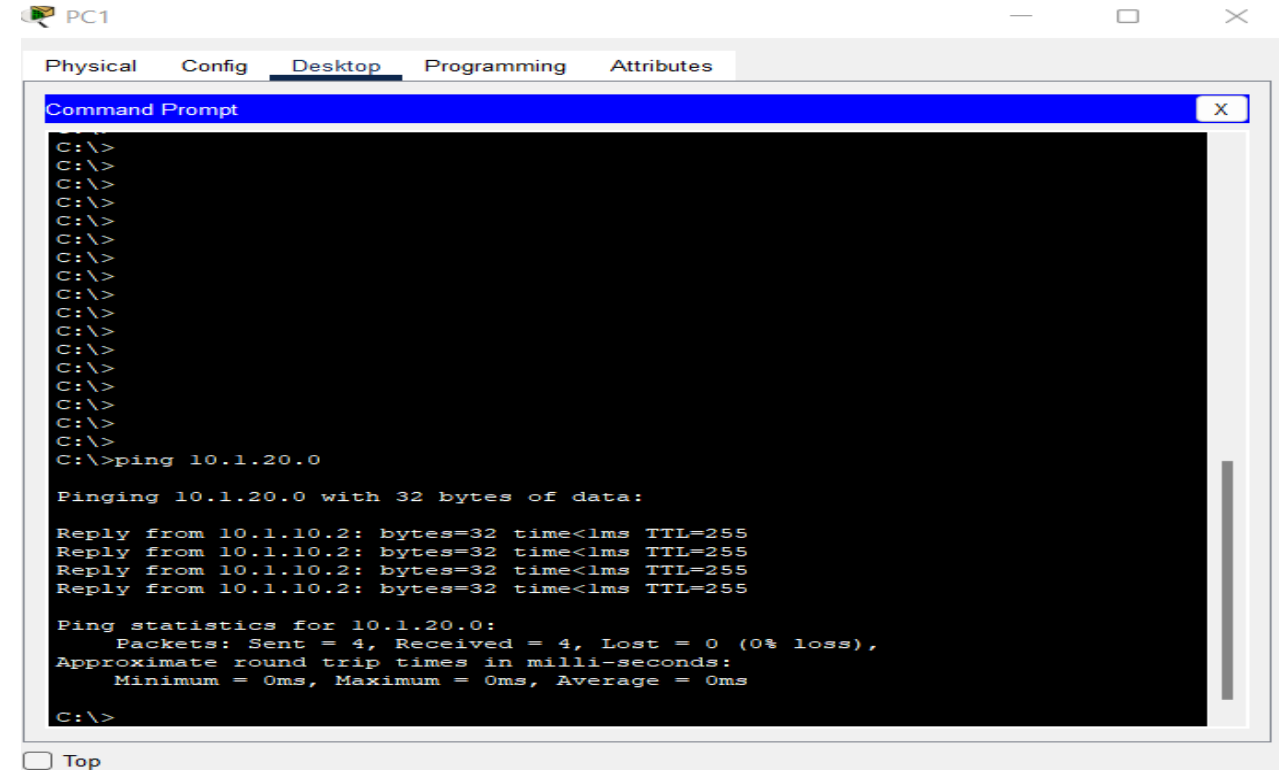
Physical Config CLI Attributes

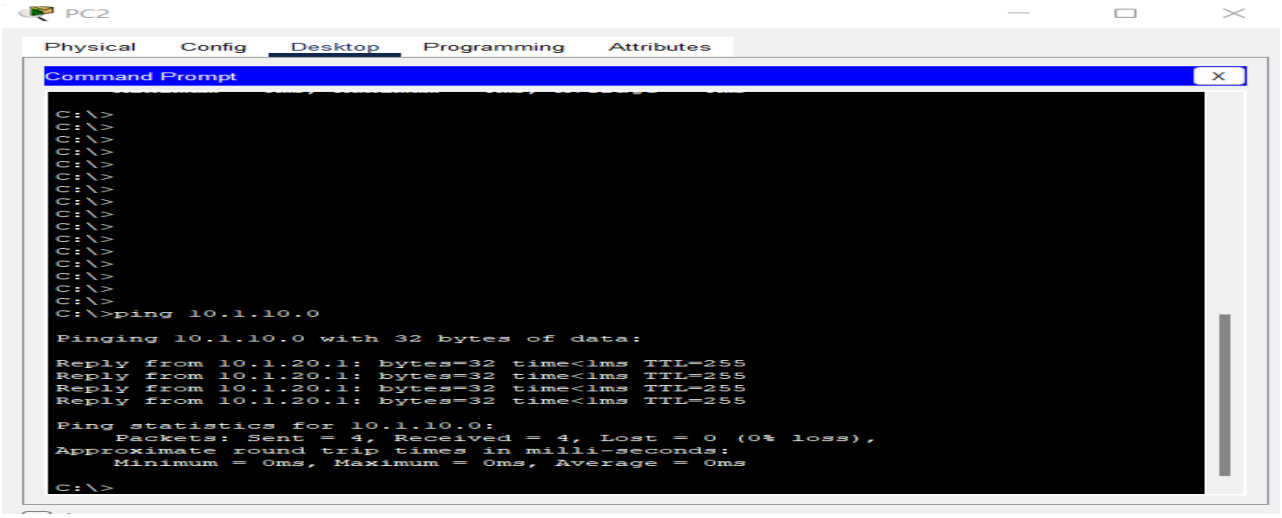
IOS Command Line Interface

```
Unknown multicast blocked: disabled
Appliance trust: none


Switch#
Switch#
Switch#show interfaces Fa0/3 switchport
Name: Fa0/3
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
 --More--
```

Copy Paste

Successful ping between PC's





Report Questions [23 pts]

1. What are two advantages of using VLANs? [**2 points**]

VLANS reduce the size of broadcast domains

VLANs utilize packet filtering to enhance network security.

VLAN does logical grouping of devices by function rather than location

VLAN enhances the performances and reduces the latency.

2. Can a PC from any VLAN telnet into a switch? Why or why not? If not, what must be done to make it work? [**2 points**]

   Not PC from any VLAN can telnet into a switch. The VLAN configured with telnet can only telnet. In order to access the switch via telnet, first configure the SVI on the switch with the ip address. This SVI could be part of VLAN 10 or 20 or any VLAN used. And create a username and password to do the telnet. Telnet can be done by following command

   Line vty 0 15

   Transport input telnet

   Login

3. What are access ports and what are trunk ports? Explain the difference **[3 points]**

   Access and Trunk ports are a medium to connect devices b/w switches and routers to enable communication.

   Access port: An access port is connection on a switch that tramsits data to and from a single / specific vlan.

   Trunk port: A trunk port is able to transmit data from multiple vlans

   Access can be configured using following commannds

   (config)#interface fa0/0

   (Config-if) #switchport mode access

   Trunk port should be configured using following command

   #Interface fa0/0

   #Switchport trunk encapsulation dot1q

   #Switchport mode trunk

4. What is the benefit of using a trunk port? [**2 points**]

   The trunk port allows Mutli VLAN data transmission on it. Which can add bandwidth and reduce the latency between data transmission by using tagging in order to reach the right destination/end point.

5. Describe what must be done to route between VLANs. [**2 points**]

   VLANS should be created and configured and mapped to interface/ports to which host VLAN is connected to.

(config)#Interface <interface>

(config-if)#Switch Mode Access

(config-if)#Switch Access VLAN ID

Should be configured in the switch network to enable route between VLANs.

6. In Objective 4, let us say you issued a ping from PC2 to PC5. Explain how the ping packets flow through the network, paying attention to each step when switches forward the packet and routers route the packet. If necessary, mention any ARPs that may need to be issued to establish this communication.

   [12 points]

   Step 1 :

   When PC2 initiates PING request, it This host creates an IP packet with its own IP address (192.168.1.1) as the source and the (192.168.2.2) destination. And builds the ethernet frame entering its own MAC Address. But it requires MAC Address of PC5 to perform ping operation. So it checks the ARP Table to to identify if the MAC address of the default gateway is available or not. Checks its arp table usinhg “arp -a” command.

```
Reply from 10.1.10.2: bytes=32 time<1ms TTL=255
Reply from 10.1.10.2: bytes=32 time<1ms TTL=255
Reply from 10.1.10.2: bytes=32 time<1ms TTL=255
Reply from 10.1.10.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.1.20.0:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>arp -a
  Internet Address      Physical Address      Type
  10.1.20.0             0002.17dc.4701        dynamic

C:\>
```

   Because ARP is not available in the table, it sends out for an ARP Request using the broadcast frame (ff:ff:ff:ff) on every port except the port in which its sending and receiving the information out. By default ARP is enabled. Else interface encapsulation should be configured to define static ARP entries.

   Device > enable

   Device(Config#) Config Terminal

   Device(Config#) arp 10.0.0.1 aabb:gghh:cc03:8200:arpa

   Device(Config#) end

   And to display the type of ARP used on an interface execute the SHOW INTERFACES <interface> command

```
Switch>
Switch>en
Switch#show arp

Switch#
Switch#
Switch#show interfaces GigabitEthernet0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 00d0.97a7.ce19 (bia 00d0.97a7.ce19)
 BW 1000000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
 --More--
```

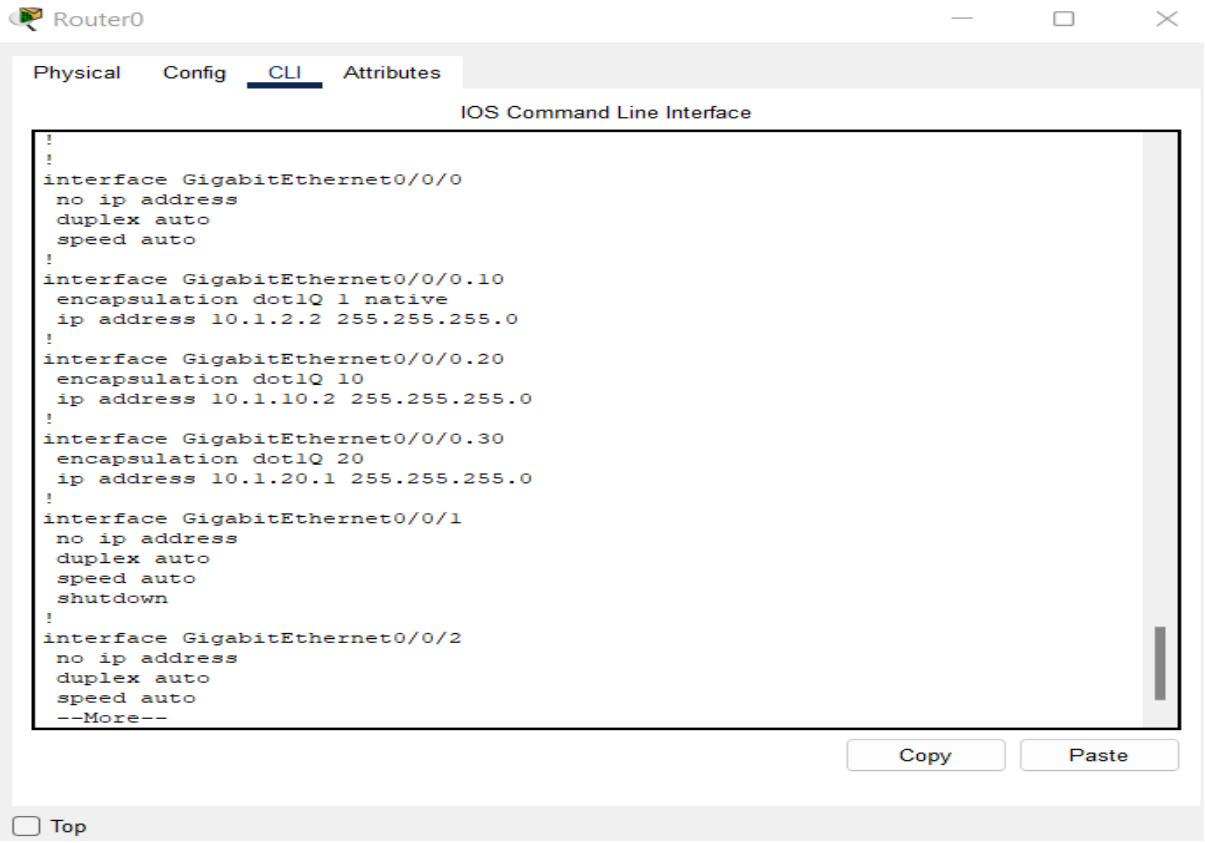
Once the destination MAC address is received from the destination device, the PC2 prepares a ethernet frame that carries packet with Source MAC | Destination MAC | Source IP | Destination IP.

And the frame will be routed to Switch0, switch chescks the VLAN ID, and when the VLANID of the source MAC and destination MAC are different, the IP is routed to Layer3 device aka Defalt Gateway or Router using the Trunk Port. At the router, the sub-interfaces are configured with the VLAN ID using encapsulation to enable traffic flow between the VLAN's.

From the router the packet is forwarded to Switch1.The S1 performs the same operation as building the Ethernet Frame with SOURCE MAC| BROADCAST FRAME|SOURCE IP|DESTINATION IP and sends out ARP request. Once the ARP MAC is received the SWITCH 2 checks the VLAN ID and the port the VLAN ID is configured on and forward the packet to PC5.

```
Router>en
Router#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0/0   unassigned      YES unset  up                    up
GigabitEthernet0/0/0.10 10.1.2.2       YES manual up                    up
GigabitEthernet0/0/0.20 10.1.10.2      YES manual up                    up
GigabitEthernet0/0/0.30 10.1.20.1      YES manual up                    up
GigabitEthernet0/0/1   unassigned      YES unset  administratively down down
GigabitEthernet0/0/2   unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router#show vlan

VLAN Name                             Status    Ports
```

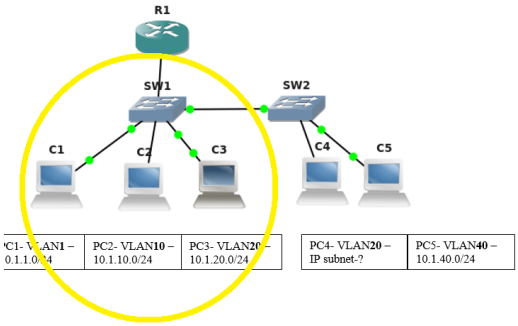
```
C:\>
C:\>ping 10.1.20.0

Pinging 10.1.20.0 with 32 bytes of data:

Reply from 10.1.10.2: bytes=32 time<1ms TTL=255
Reply from 10.1.10.2: bytes=32 time<1ms TTL=255
Reply from 10.1.10.2: bytes=32 time<1ms TTL=255
Reply from 10.1.10.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.1.20.0:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



Extra Credit [13 points]

1. What is a broadcast domain? How many broadcast domains are there in the topology in Objective 4? **[3 points]**

A broadcast domain is the logical division of the network in which all the nodes of the devices can reach other by broadcast at the data link layer (layer 2 segment). A broadcast domain can be within same LAN or van be bridged to other LAN's.
There is only one Broadcast domain in Objective4 topology



2. From your setup in objective 4,

- On Switch-1 port (connected to Switch-2), configure VLAN 10 as native-vlan.
- On Switch-2 port (connected to Switch-1), configure VLAN 20 as native-vlan.

Give it a minute. Do you observe any debug/warning messages on either of your switches? If yes, paste the message here. **[8 points]**

YES. %CDP-4-NATIVE_VLAN_MISMATCH : NATIVE VLAN MISMATCH DISCOVERED

On Switch1 :

```
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/4
Switch(config-if)#switch mode trunk
Switch(config-if)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/4 (100), with Switch FastEthernet0/3 (1).
```

Copy Paste

Top

On Switch2 :

Switch2

Physical Config CLI Attributes

IOS Command Line Interface

```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/3 (1), with Switch FastEthernet0/4 (100).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/3 (1), with Switch FastEthernet0/4 (100).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/3 (1), with Switch FastEthernet0/4 (100).


Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 20
Switch(config-if)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/3 (20), with Switch FastEthernet0/4 (100).
```

Copy Paste

Top

To your best knowledge, explain what you think it means **[2 points]**

The native VLAN is a VLAN that is not tagged in a trunk, making its frames transmission unchanged, I think, NATIVE VLAN MISMATCH DISCOVERED means, that you have a device plugged into your cisco switch that has different native vlan than the switch. And it occurs when two connected switch ports are configured with different VLANS. Basically, the receiving end of switch is not having the native vlan details, means it's not tagging your vlan details to the frame.

Total Score = _____/122