CSCI 5010 – Fundamentals of Data Communications

Lab 2 – Introduction to Cisco IOS and Switching Spanning Tree Protocol (STP)

University of Colorado Boulder
Department of Computer Science
Network Engineering

Professor Levi Perigo, Ph.D.

Summary

This lab will provide an introduction to Cisco IOS, and how to use the Command Line Interface (CLI). For Cisco devices, the CLI is the primary way to configure and troubleshoot. It is important that you understand the basic CLI commands to navigate a Cisco device. Several videos have been linked for additional assistance and clarification, but you are also encouraged to search for other videos that may be of assistance to you.

The foundational layer to any network revolves around switching. This lab is intended to be an overview of Cisco IOS, and switching technology - STP.

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 perform basic switch configuration & troubleshooting including:
  - Switch password assignment and IOS navigation
  - How to activate/deactivate a port
  - How to change the speed and duplex of a port
  - How to verify the MAC addresses of computers connected to a specific port
- Review the usage of Spanning Tree Protocol (STP) including how switching environments behave regarding:
  - network failure
  - network loops

Part 1

Objective 1: Connect PC to Cisco Switch in Cisco Packet Tracer

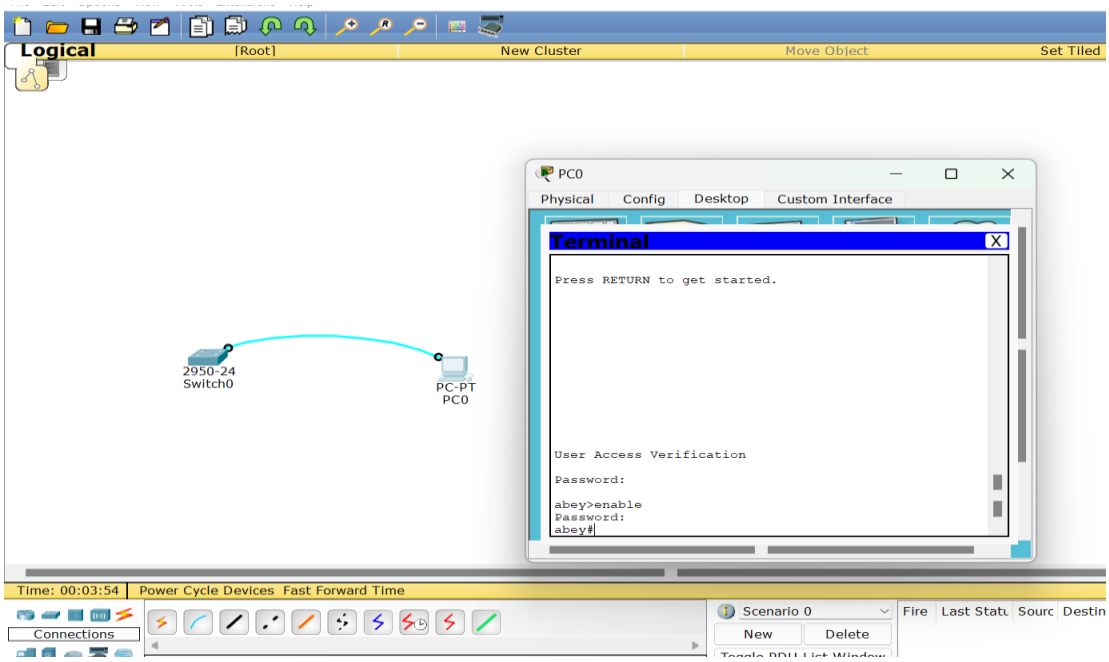
This objective will provide instructions for how to connect a PC to a Cisco device for configuration purposes.

1. Use a Cisco console cable to connect PC1 to the switch “Switch1”

Objective 2: Cisco IOS User Levels & Command Line Interface (CLI)

This objective will provide an introduction to Cisco IOS network device user levels. Cisco user levels are important to understand how to navigate the prompts of a Cisco device and determine how to configure and troubleshoot the device.

1. Follow the Cisco documentation Using the CLI.
2. Configure the hostname on the switch to be “your name.”
3. Create an enable password of “cisco”
4. Create a console password of “lab”.
5. Logout from the switch and console again using the PC (PC>>Desktop>>Terminal).
    a. Make sure to remember which password is for which level
    b. Verify the spelling and case sensitivity. Paste the screenshot of successful login. **[10 points]**



6. Paste the switch's running configuration **[5 points]**

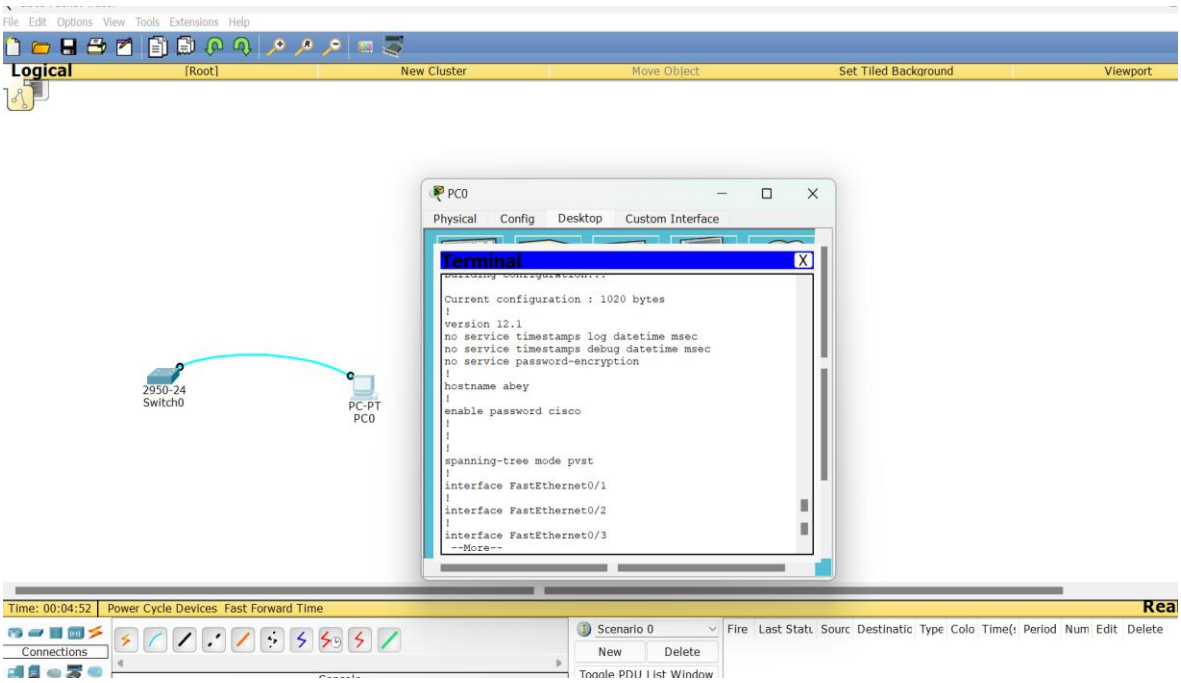
```
abey#show running-config
Building configuration...

Current configuration : 1046 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname abey
!
enable password cisco
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
```

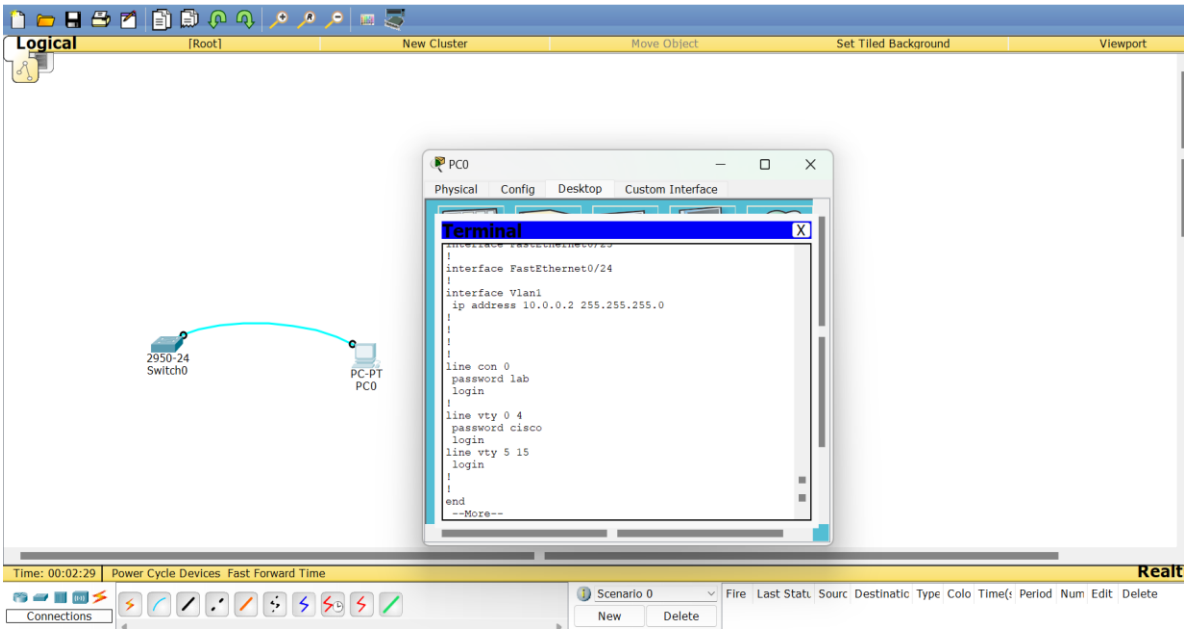
```
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
```

```
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface Vlan1
 ip address 10.0.0.2 255.255.255.0
!
!
!
!
line con 0
 password lab
 login
!
line vty 0 4
 password cisco
 login
line vty 5 15
 login
!
!
 --More--
```

a. Do you see the settings you configured?
    i. Hostname
    ii. Enable password
    iii. Console password



Its mentioned my Hostname is Abey.



Its mentioned that the console password is lab and enable password is cisco.

Objective 3: Creating Remote Access to Cisco Networking Device (Telnet)

This objective will allow you to connect remotely to the Cisco device via the network, without using a console cable in Cisco Packet Tracer. Use this "Enable Telnet" video for assistance.

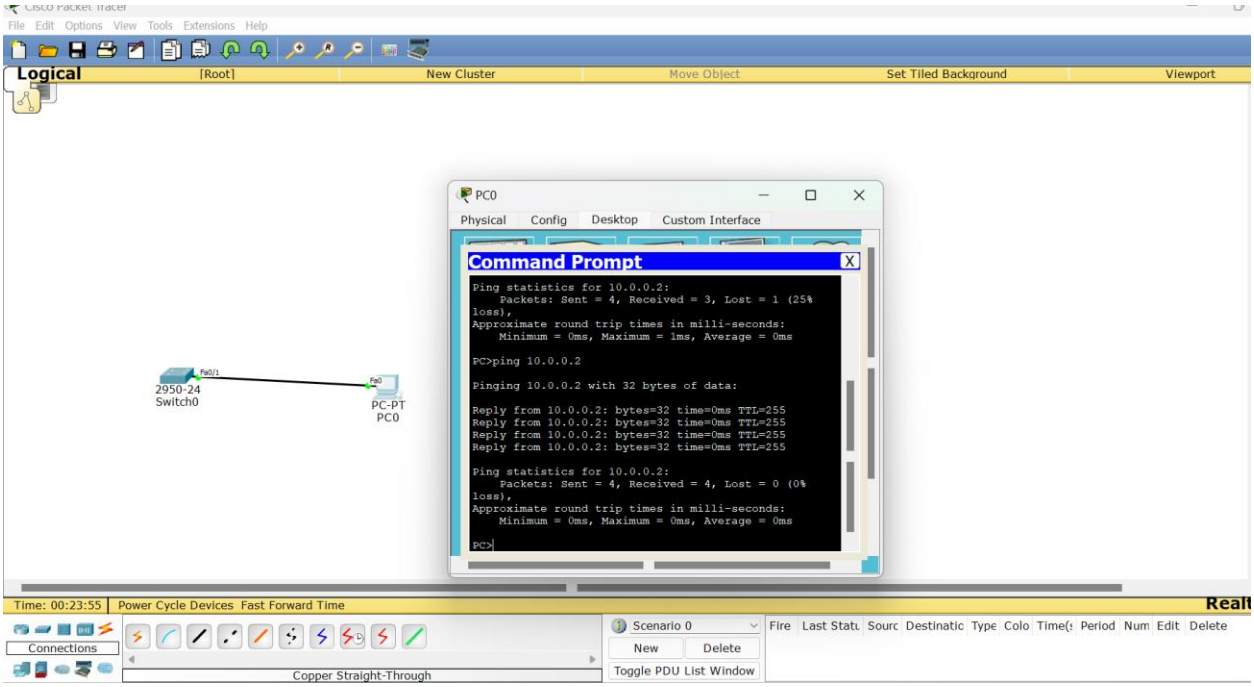
1. Configure and connect the PC and switch according to the diagram. Which cable did you use this time? **[2 points]**

   Used a copper straight through cable.

   a. Make sure the PC has an IP address (10.0.0.1) and subnet mask (255.255.255.0) in the same subnet as the switch (VLAN 1 IP - 10.0.0.2/255.255.255.0)

      Assigned PC IP address as 10.0.0.1 and made sure its in the same subnet as switch.

2. Verify the PC can ping the IP address of the switch. Paste the screenshot of the command output. **[5 points]**



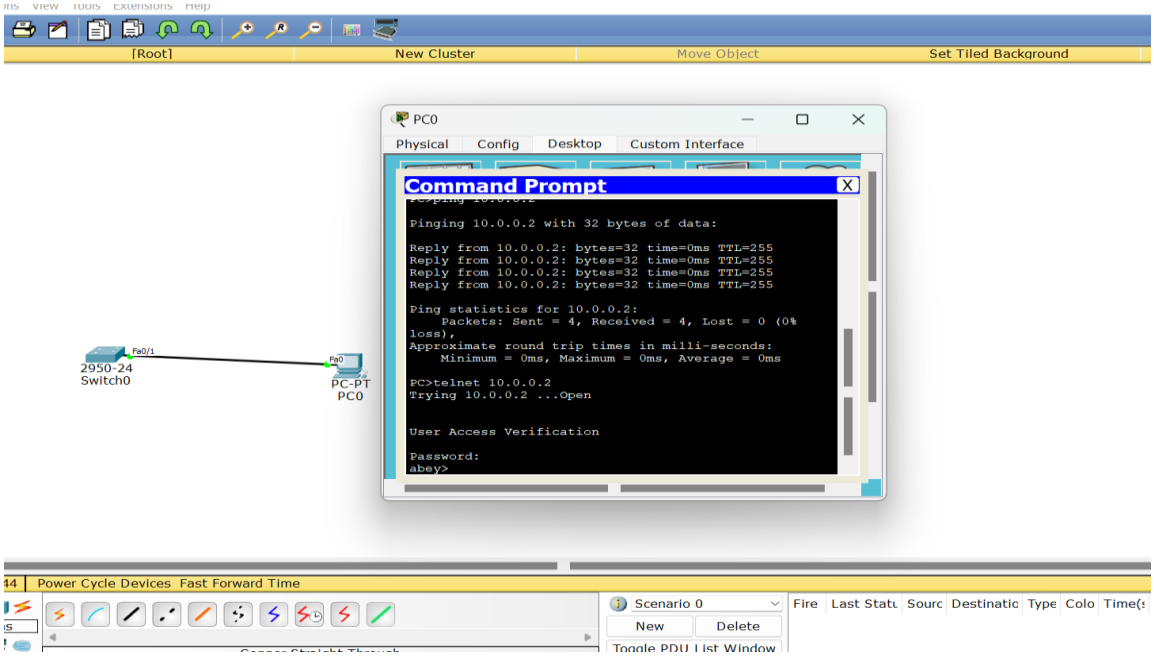
3. Configure Telnet on the switch

   a. Use all the vty lines

   b. Create a password of “telnet” as “cisco”

      Created a password named cisco so that’s why to telnet to the switch it is asking for password and when you enter the password we get access to switch.

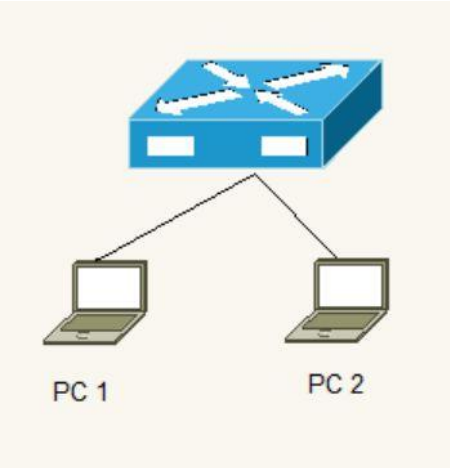
4. Use Terminal (PC>>Desktop>>Command Prompt) of the PC to Telnet to the switch. Paste the screenshot of telnet output. **[10 points]**



Part 2

Objective 1: Cisco IOS Switch Port Configuration

This objective will allow you to configure port settings on the industry standard Cisco switches.



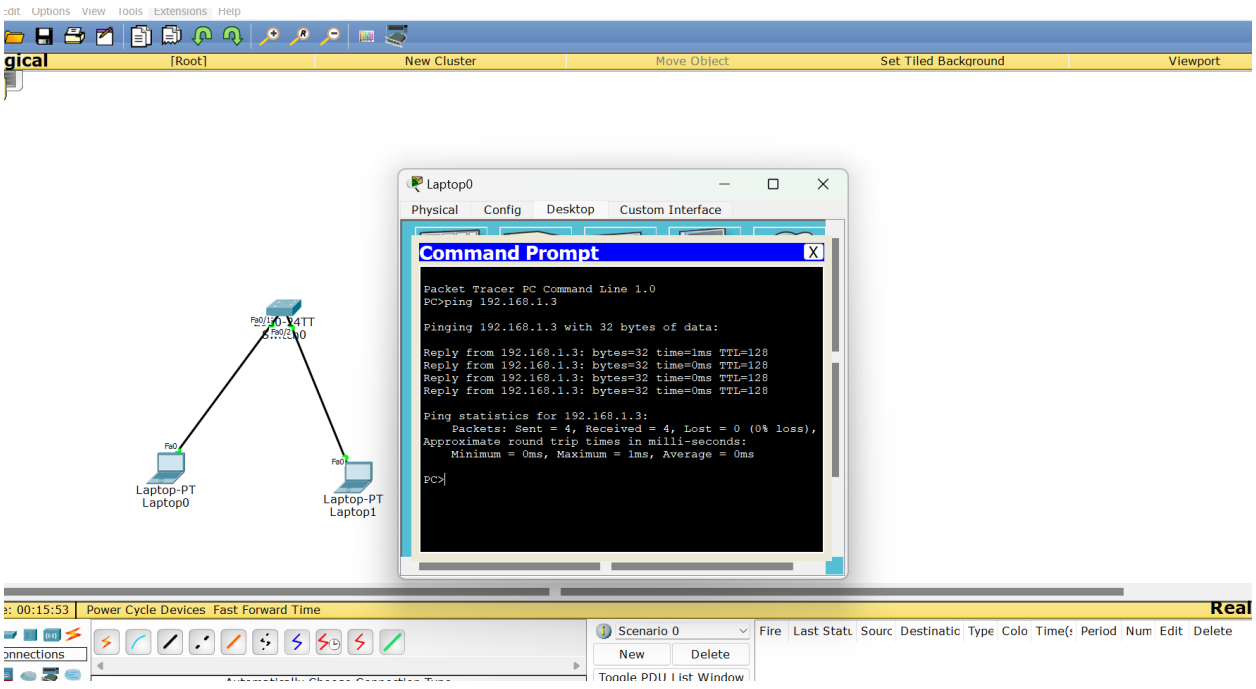
2. Connect PC1 and PC2 to a switch
3. Configure a description on the switchports connected to each PC
    a. The port connected to PC 1 should have a “description Computer 1”

b. The port connected to PC 2 should have a “description Computer 2”

4. Configure the necessary steps to ping from PC1 to PC2 (*hint: you will have to configure settings on the switch (use the default VLAN), but you will also have to configure both PCs*)

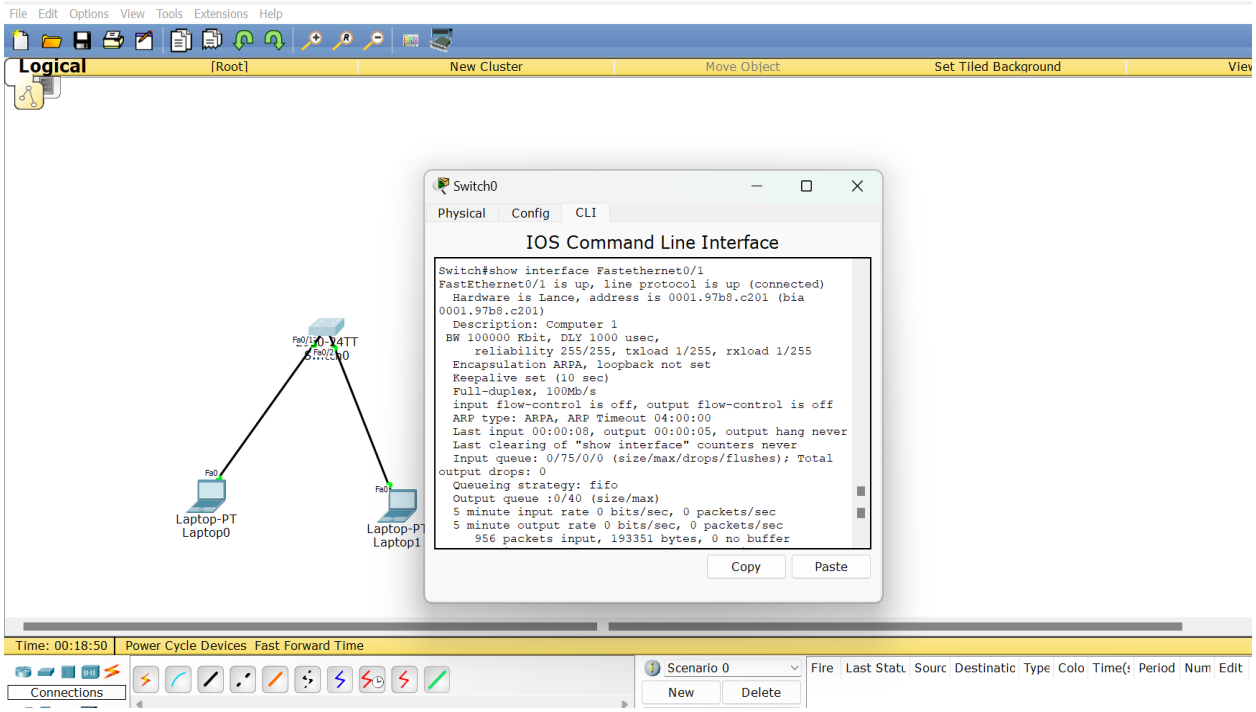
   a. List the steps you had to perform to get the PCs to ping each other [**20 points**]

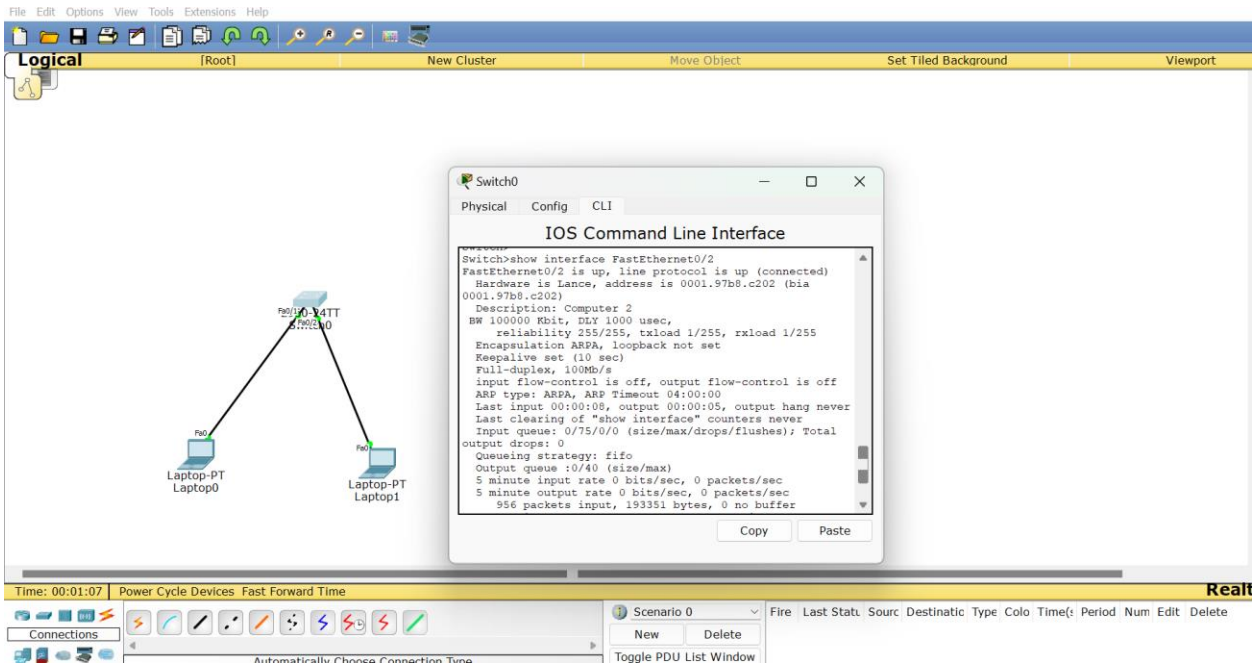
      The commands I used in switch CLI for configuration. Used enable to go into the global configuration mode and configure terminal and configure the description for the port connected to PC1 as well as PC2.By going to PC1, select Ip configuration and assigned Ip address as 192.168.1.1 and 192.168.1.3 for PC2 and subnet mask as 255.255.255.0. After Assigning the IP address and subnet mask, go to the command prompt of PC1 and use ping command. Ping 192.168.1.3 it will show successful ping replies if the configuration is correct.



5. Check the status of the switch port connected to PC1

a. Provide a screenshot of the status of the port [**2 points**]





Click Switch and go to CLI and type interface Fastethernet0/1 and FastEthernet0/2 it will show the port is up, speed and the duplex of the port.

i. Indicate that the port is up [**2 points**]

In the above two screenshots it shows FastEthernet0/1 and FastEthernet0/2 is up.

ii. Indicate the speed and duplex of the port [**2 points**]

In the above screenshots it shows it is Full-duplex and speed is 100Mb/s.

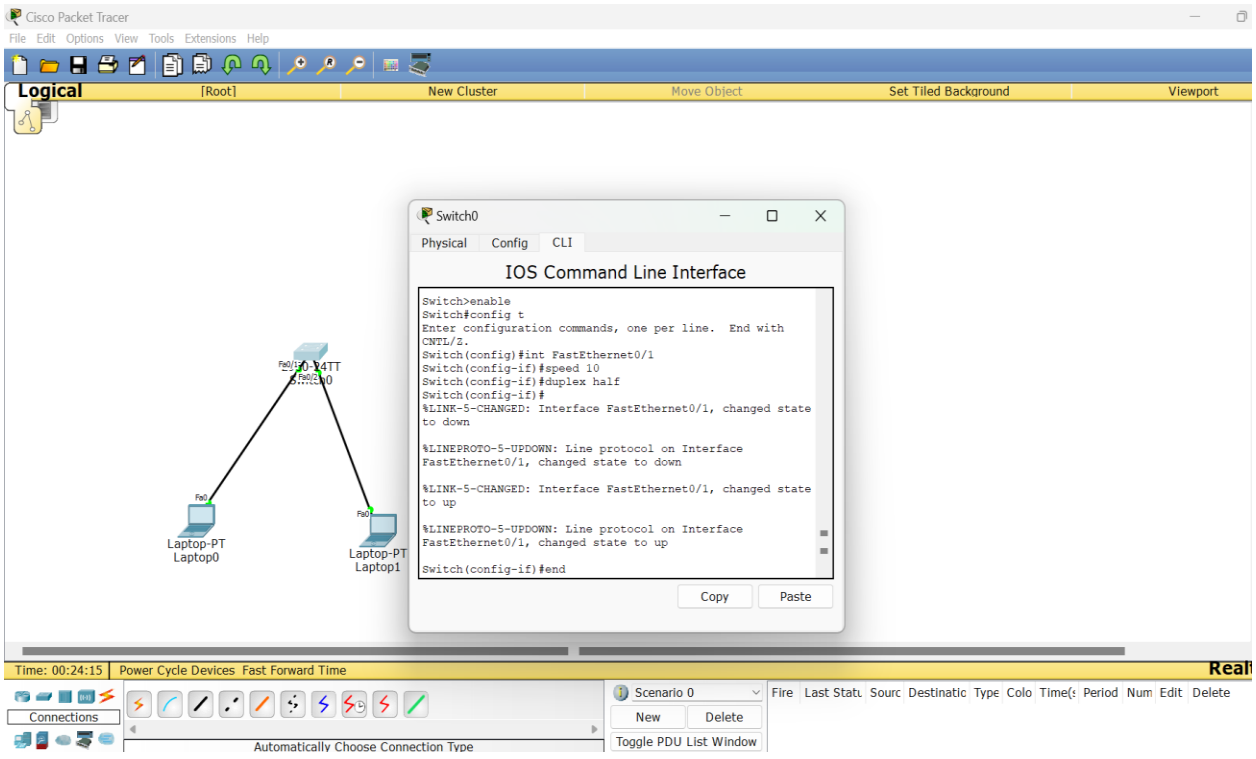
iii. Make sure it has the proper description (above)

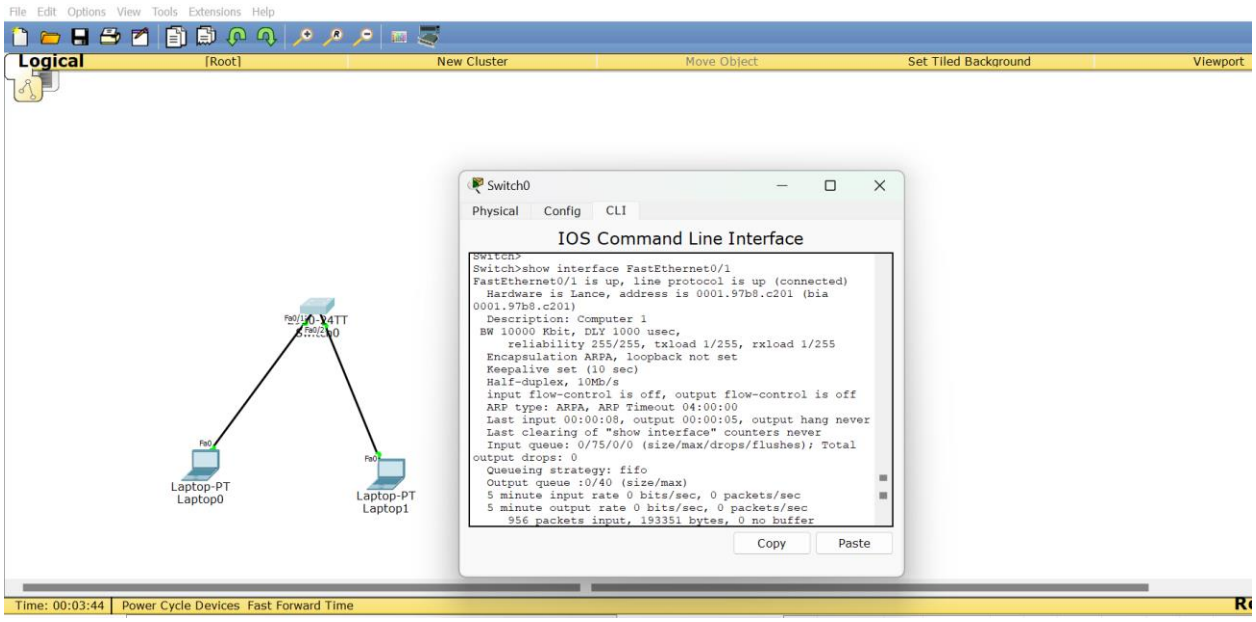
By using commands interface FastEthernet0/1 and then description Computer 1 we can get the proper description similarly for interface FastEthernet0/2. In the above screenshots it shows the description as Computer 1 and Computer 2.

6. Configure the switch port that connects to PC1

   a. Hard set the port to 10Mbps and Half Duplex

   The screenshot below shows that I have Hard set the speed as 10 using command speed 10 and half duplex command as duplex half.



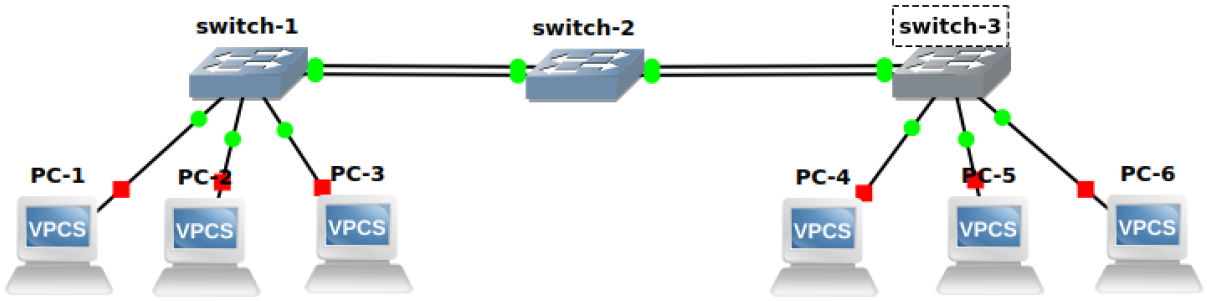


It shows that speed has reduced to 10Mb/s and it is Half-duplex.

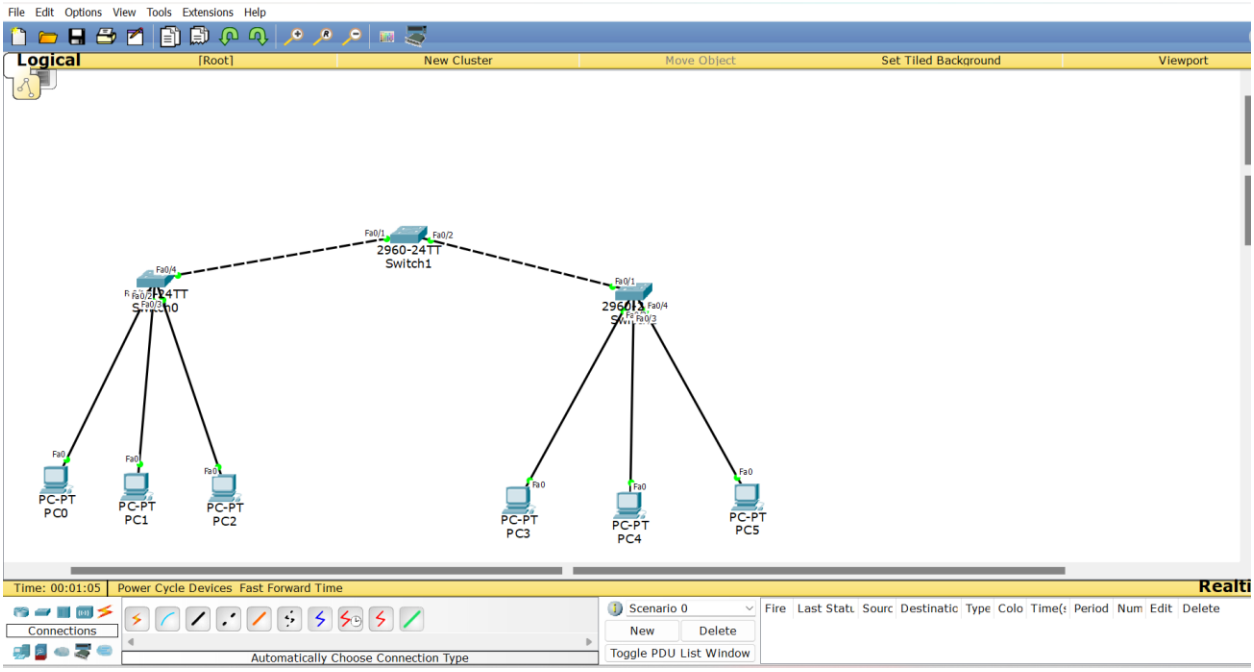
b. Can PC1 still reach PC2? Why or why not? [**2 points**]

Yes, PC1 and PC2 can communicate with each other though we have reduced the speed and changed it to Half duplex it can affect of communication between the PCs and there are chances of collisions.

7. Now create a following topology in Cisco Packet Tracer



a. Provide the screenshot of the created topology in Cisco Packet Tracer. Assign IPs to all the hosts. **[5 points]**



The assigned IP addresses are:-

PC0-192.168.1.1

PC1-192.168.1.2

PC2-192.168.1.3

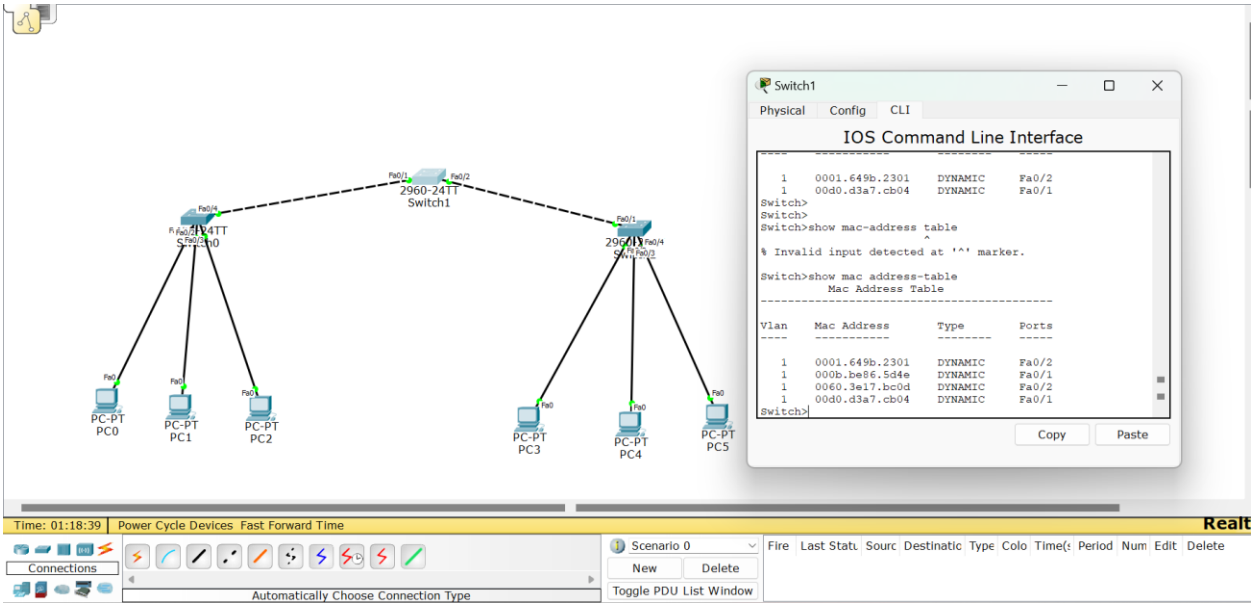
PC3-192.168.1.4

PC4-192.168.1.5

PC5-192.168.1.6

b. Ping PC-6 from PC-1. What command would you use to look at the mac-table on switch-2? Paste the screenshot showing its output. **[5 points]**

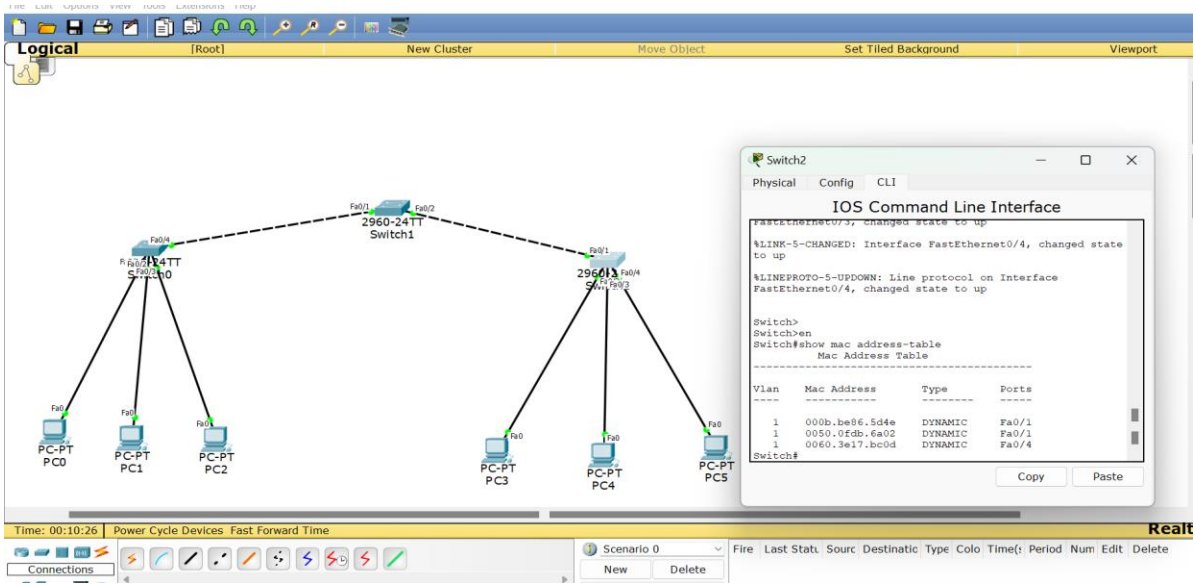
After Pinging PC5 from PC0 to check the mac address use command show mac address-table.



PC0 MAC address is 000b.be86.5d4e.

PC5 MAC address is 0060.3e17.bc0d.

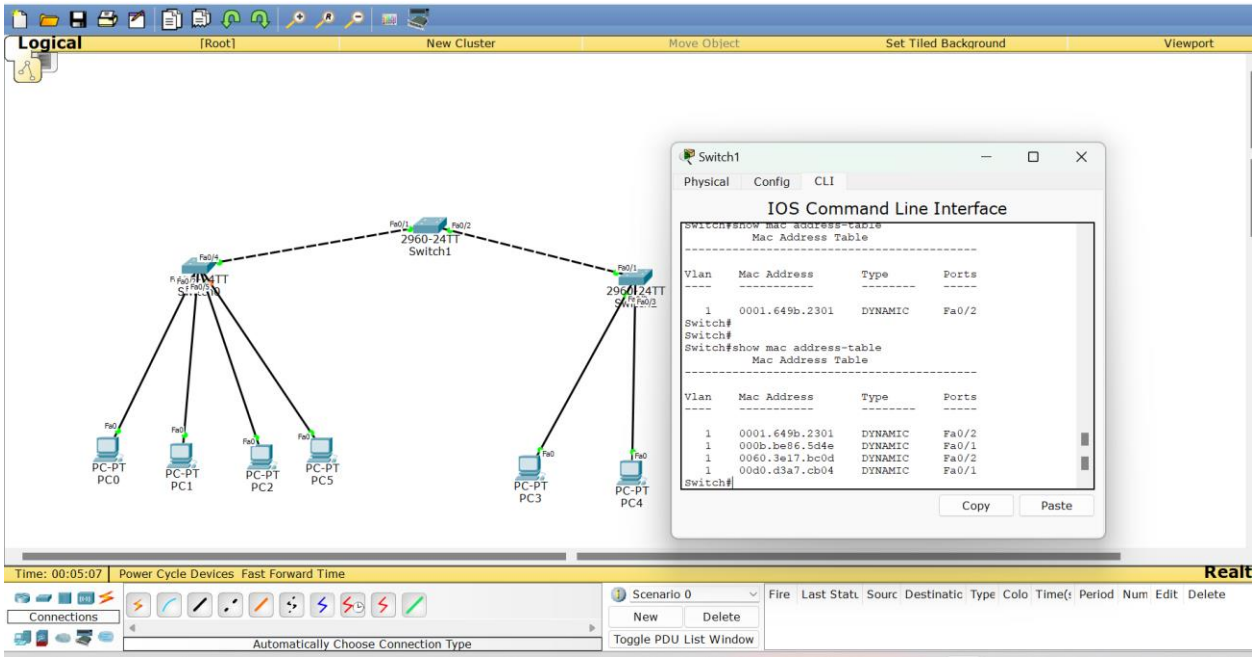
c. Interpret the mac-table of switch-3 and briefly explain it. **[5 points]**



So when ping PC-5 from PC-0, it creates the ARP request since there is no entries in the ARP table it will broadcast and goes to the switch 1 and it floods to other PCs and switch 2 and switch 3. So as soon as the data reaches switch 3 it records the entry in the MAC table the Source MAC and the source MAC address and port its entering from. So, during the ARP process the ARP reply from PC-5 will have

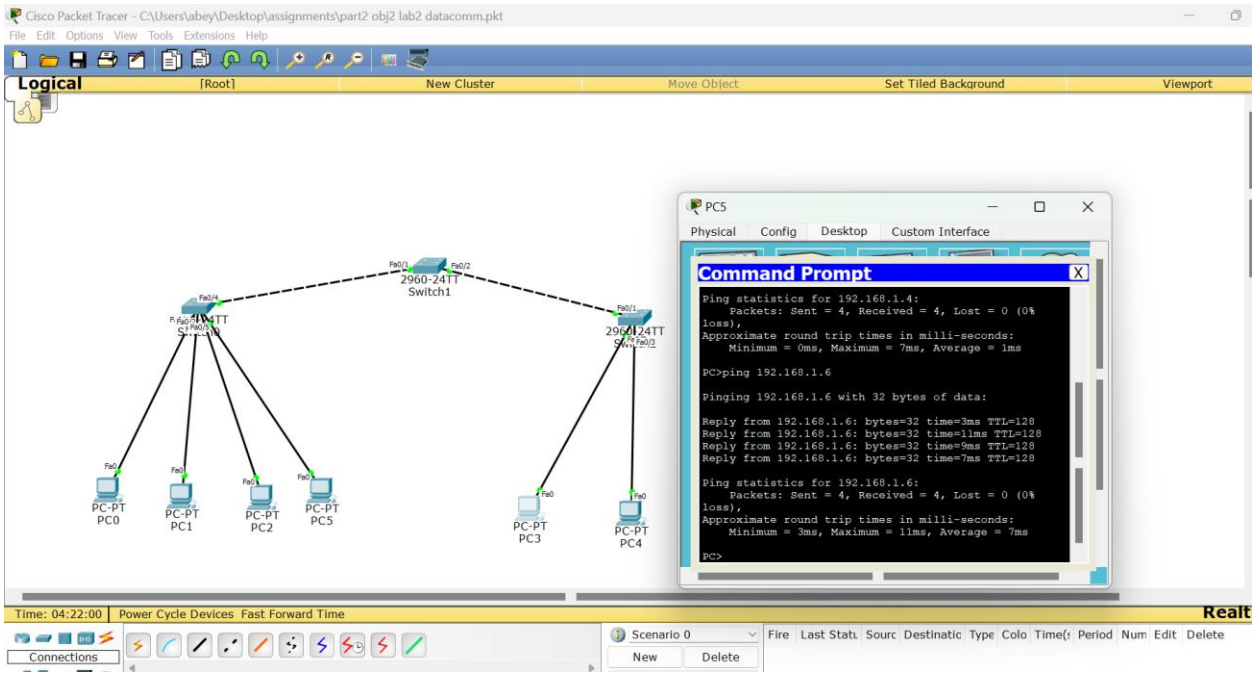
the destination MAC address and when it enters switch 3 it will also give an entry in the MAC table and the port status its entering from. So that's why the MAC table displays the PC-0 which is the source MAC address as 000b.be86.5d4e and Destination MAC address as 0060.3e17.bc0d.

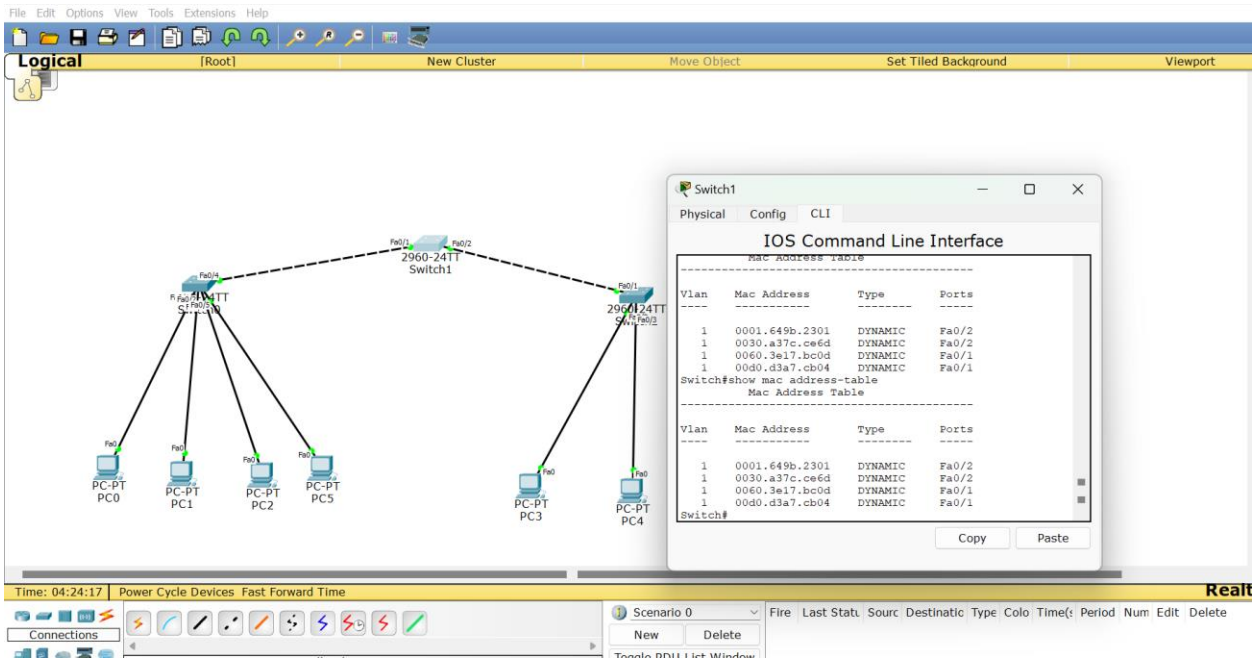
8. Now disconnect PC-6 from switch-3 and connect it to switch-1. Did you notice any change in the mac-table of switch-2? Yes or No? Why so? Paste the screenshot of the output. **[10 points]**



No, there is no change in the MAC table because I have just removed the connection and MAC address takes time to get updated. Once we ping only, we will know that the connection is terminated and those MAC addresses won't be visible.

a. Now ping PC-6 from PC-4. Check the mac-table once again on switch-2. Did you notice any change in the mac-table of switch-2? Yes or No? Why so? Paste the screenshot of the output. **[10 points]**





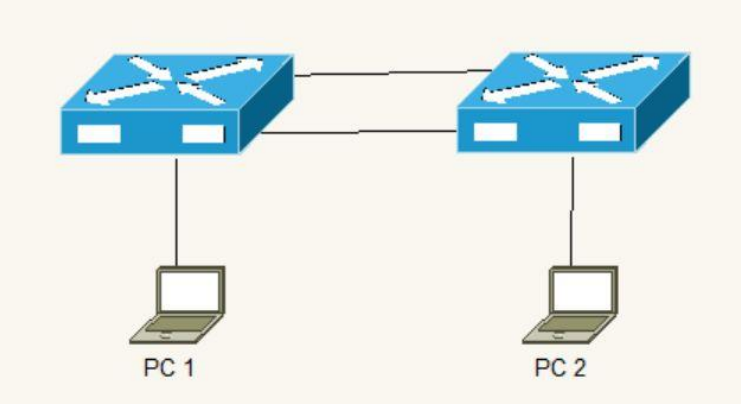
Yes, there is a change in the MAC table it shows the MAC address of PC3 and PC5.while pinging PC5 , since it does not have the MAC address of PC5 it will broadcast the data and all the PCs and switch 1,2,3 will receive the data but only PC5 will reply because the ARP request dedicated for PC5 based on the IP address will reply back to PC3 in a unicast way so the packet will pass through switch 2. Hence the MAC address will be shown in MAC table which is PC5 MAC address

and PC3 MAC address will be shown which is 0060.3e17.bc0d(PC5 MAC address) and 0030.a37c.ce6d(PC3 MAC address).

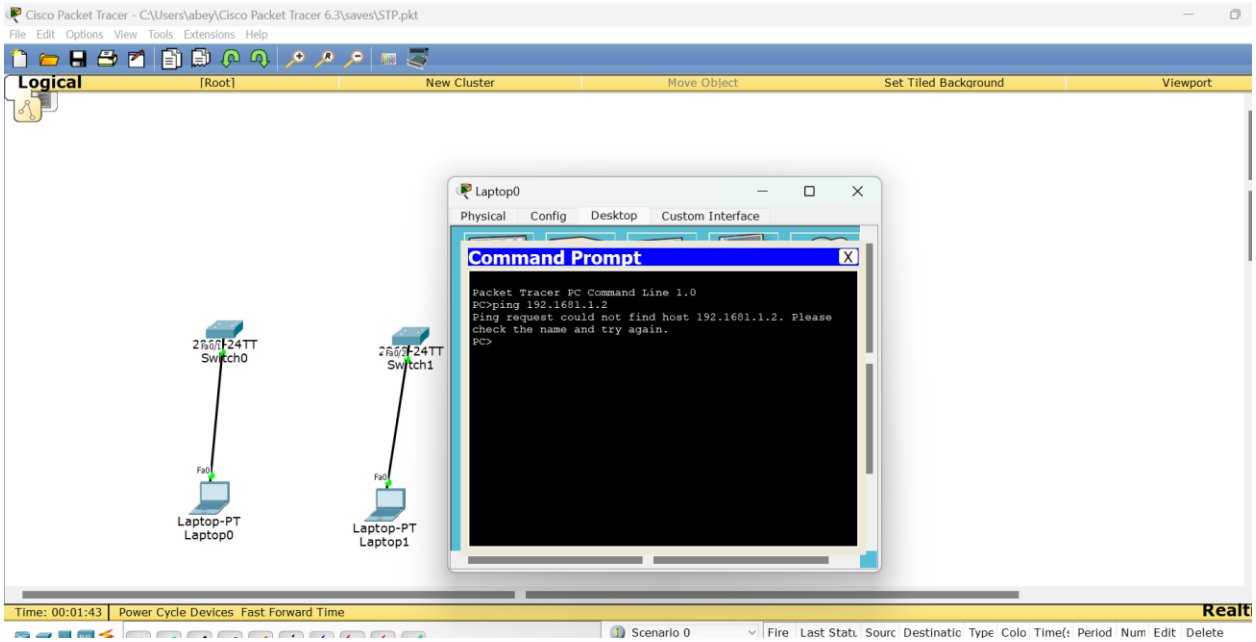
My PC3 is PC4 and PC5 is PC6.

Objective 2: Spanning Tree Protocol (STP)

This objective will indicate how STP prevents loops and provides redundancy.

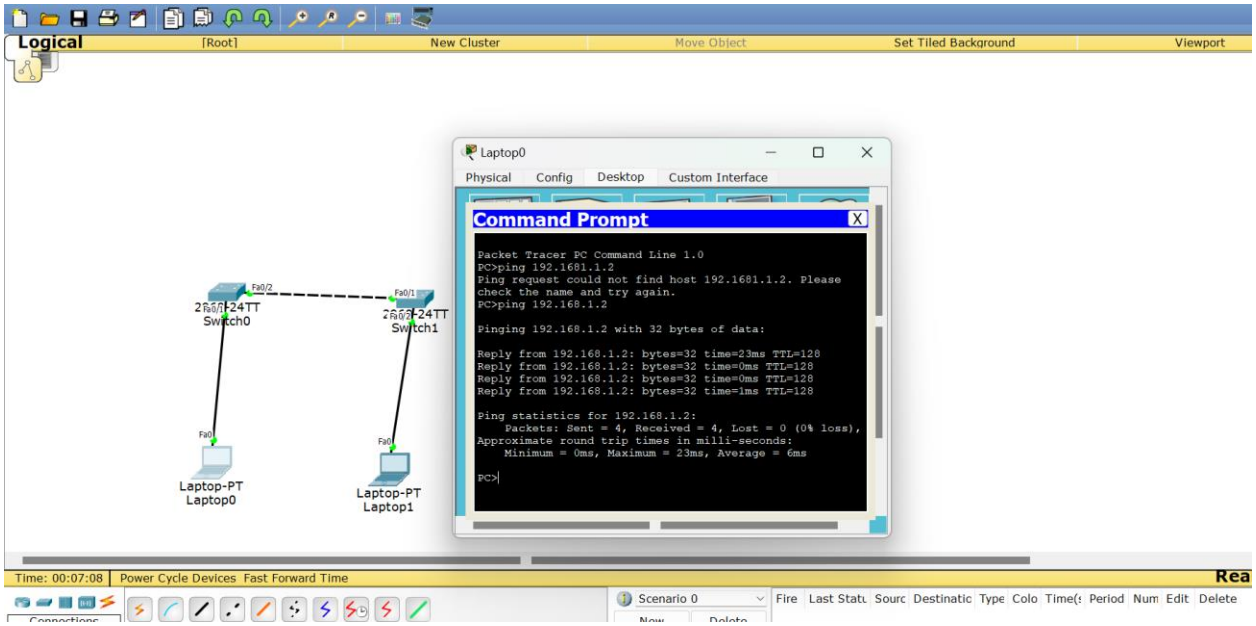


7. Connect PC1 to Switch1 and PC2 to Switch 2
    a. Verify PCs can Ping each other



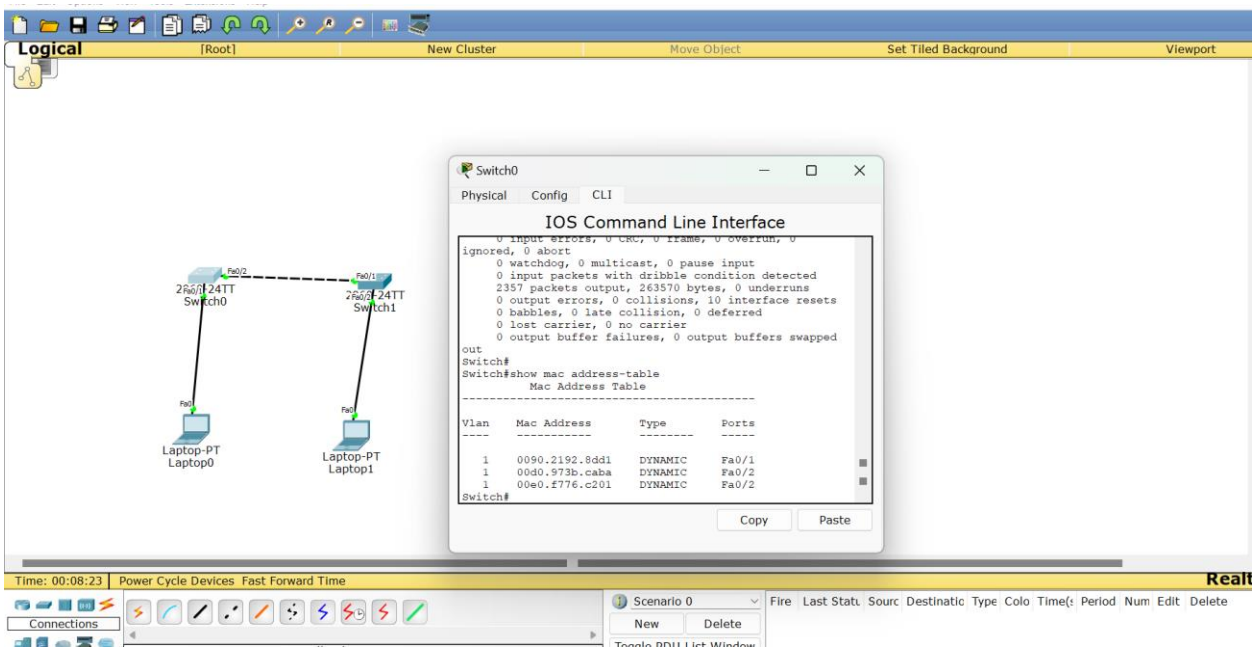
Since there is no connection between the switches, we cant ping each other since it host can't be found.

8. Interconnect the switches
    a. Verify PCs can Ping each other



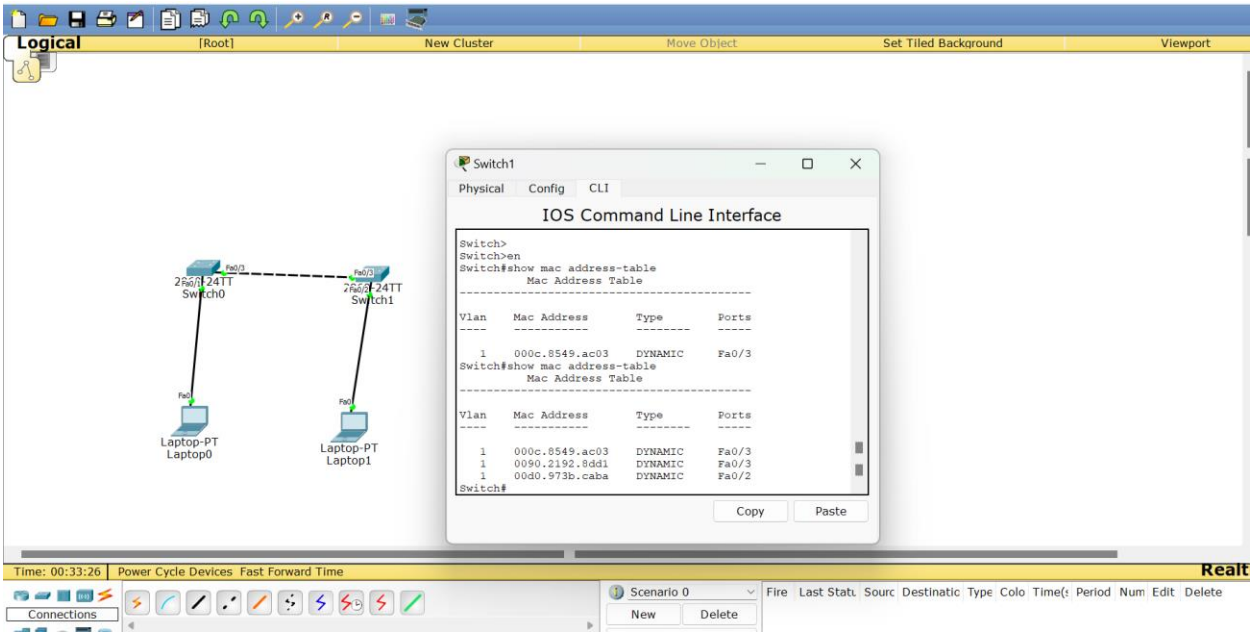
After interconnecting the switches and if you ping, the PC will ping each other.

9. Use the appropriate IOS command to verify which ports on the switch map to the MAC addresses from PC1 and PC2
    a. Explain your findings [**2 points**]



In switch 1, while pinging the data from PC1 it passes through port Fa0/1 of switch 1 and MAC address of PC1 is entered in the MAC table which is 0090.2192.8dd1 and when the reply comes back from PC2 it passes through port Fa0/2 of switch1 and MAC address of PC2 is entered in the MAC table which is 00d0.973b.caba.

In switch 2, while pinging the data from PC1 it passes through port Fa0/3 of switch 2 and MAC address of PC1 is entered in the MAC table which is 0090.2192.8dd1 and when the reply comes back from PC2 it passes through port Fa0/2 of switch2 and MAC address of PC2 is entered in the MAC table which is 00d0.973b.caba.



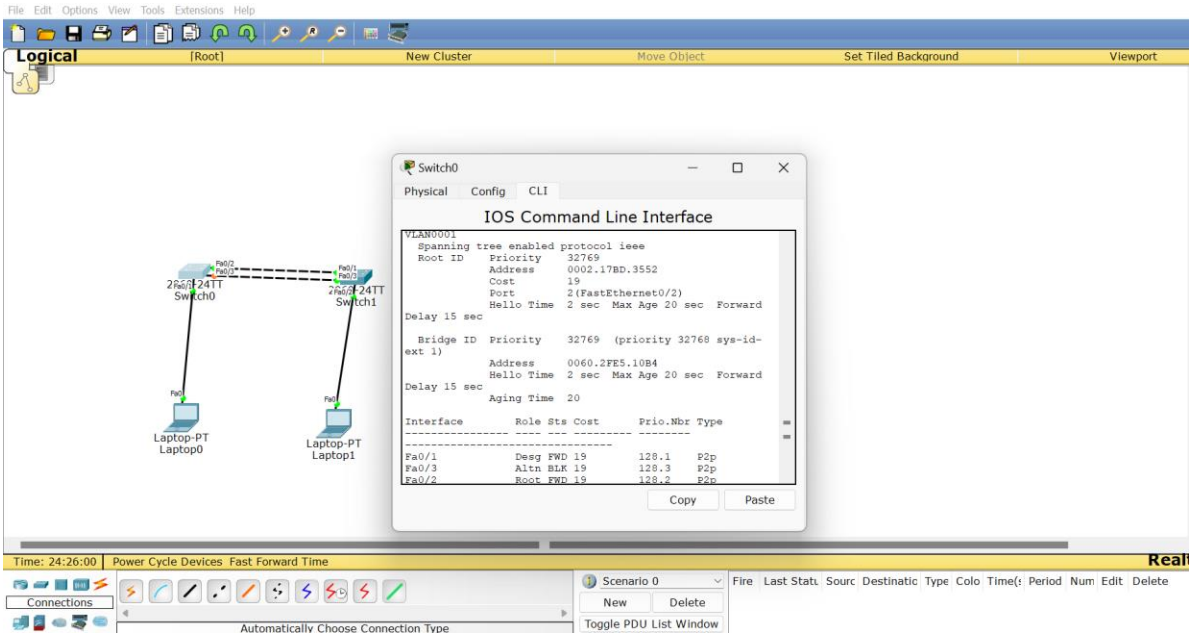
10. Add an additional link between Switch1 and Switch2
    a. Explain what should happen in this case [**5 points**]

    Since an extra link is added that's when STP is created and detects and eliminates network loops which leads to traffic such as DOS (Denial of Service). So STP will prevent it from having a loop by blocking one of its paths. If there is any failure in the active link it unlocks the other link and passes traffic in that link and it ensures constant network connection.

    b. Verify the switches resolved the problem above, indicate how you can

determine this in the Cisco switch (*hint: Spanning-tree blocked*) [**5 points**]

By using command Show spanning-tree it will show: -



show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 0002.17BD.3552

Cost 19

Port 2(FastEthernet0/2)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 0060.2FE5.10B4

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------- ---- --- --------- -------- --------------------------------

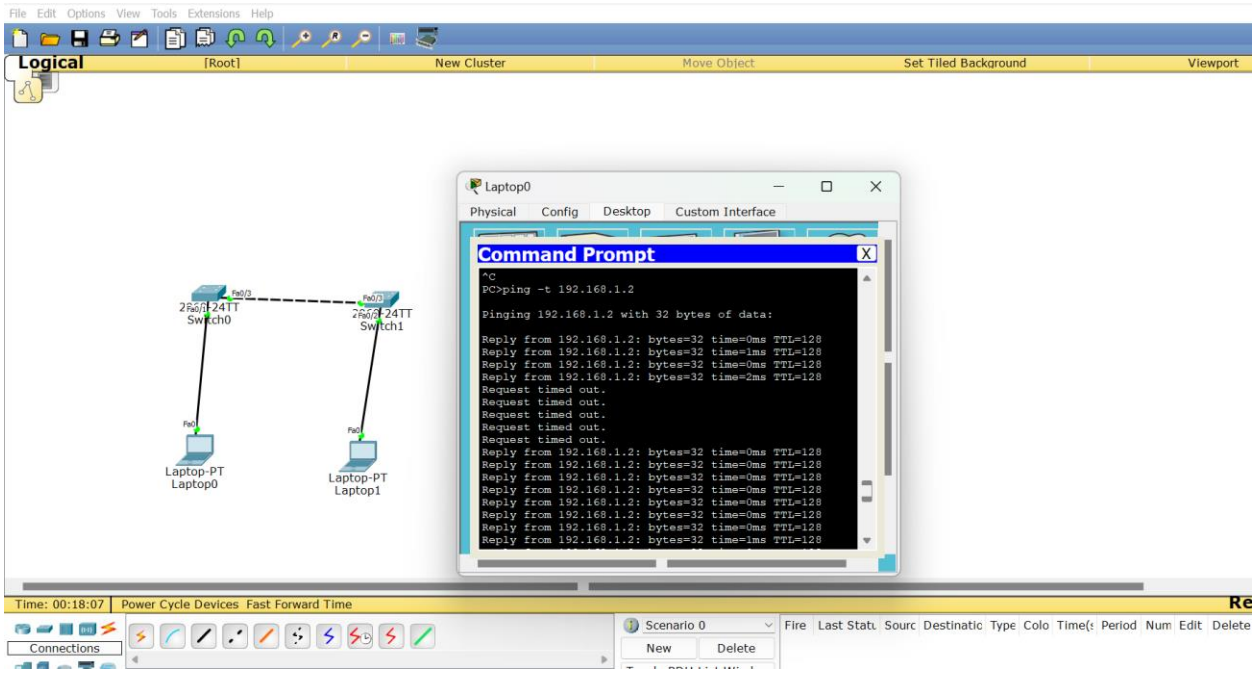
Fa0/1 Desg FWD 19 128.1 P2p

Fa0/3 Altn BLK 19 128.3 P2p

Fa0/2 Root FWD 19 128.2 P2p

It says that Fa0/3 is blocked so if a failure occurs in active link, STP will unblock the port for network connectivity. Fa0/1 is the designated port for its segment and its actively sending traffic and Fa0/2 is the root port is the best path to the root bridge and actively forwarding traffic.

11. Issue a continuous ping from PC1 to PC2
    a. Unplug one of the cables interconnecting the switches
    b. Did the pings fail? If so, for how long? If they didn't fail, why not? [**5 points**]



From the screenshot yes the ping failed for few seconds (30-50 seconds) it means that STP detects a change in topology and is taking time to unblock the previously blocked port to maintain the network connectivity.

Report Questions

1. What is the length of the MAC address? How is it divided? [**2 points**]

   The length of the MAC address is 48bits or 6bytes long. The first 24bit is for vendor specific and the rest 24bit is assigned for host specific.

2. Why are switches faster than routers? [**2 points**]

   Switches forward data based on MAC address. Whenever data comes to switch it just stores

and forwards it. It broadcasts and unicast data. Whereas a router it must look at the Destination IP address and forwarding table then send the data that path, so router must do some amount of work before sending any data which can reduce the speed. Hence switches are faster than routers.

3. Explain how ARP works. [**5 points**]

   ARP stands for Address resolution protocol. It is used to find the destination mac address. To send data to another device on the same local network, it knows the destination IP address but does not know the MAC address. So, in case I'm sending data from Host A to Host B, host A sends a ARP request to all the devices in the network as broadcast. The Arp request will have a Source IP, Destination IP and Source Mac address but with broadcast MAC (FF: FF: FF: FF: FF: FF). Every device in the network will receive the ARP request but only the device with the matching IP Address will reply with an ARP reply with the Destination Mac address. The ARP reply will always be a unicast message since it knows who the source host asked for the MAC address.

Total Score = _____/121