CSCI 5010 – Fundamentals of Data Communications

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

Student Name: Srivaishnavi Gone
Student ID: 110378712

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

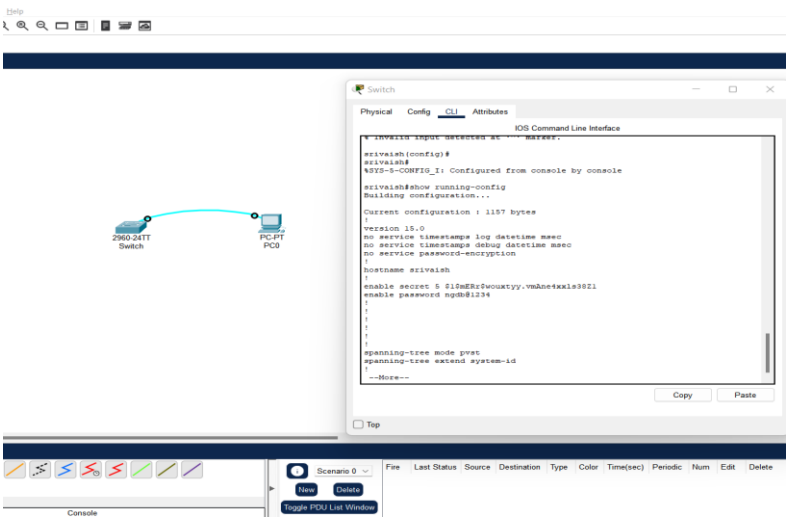
This objective will provide instructions for how to connect a PC to a Cisco device for configuration purposes.

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.”

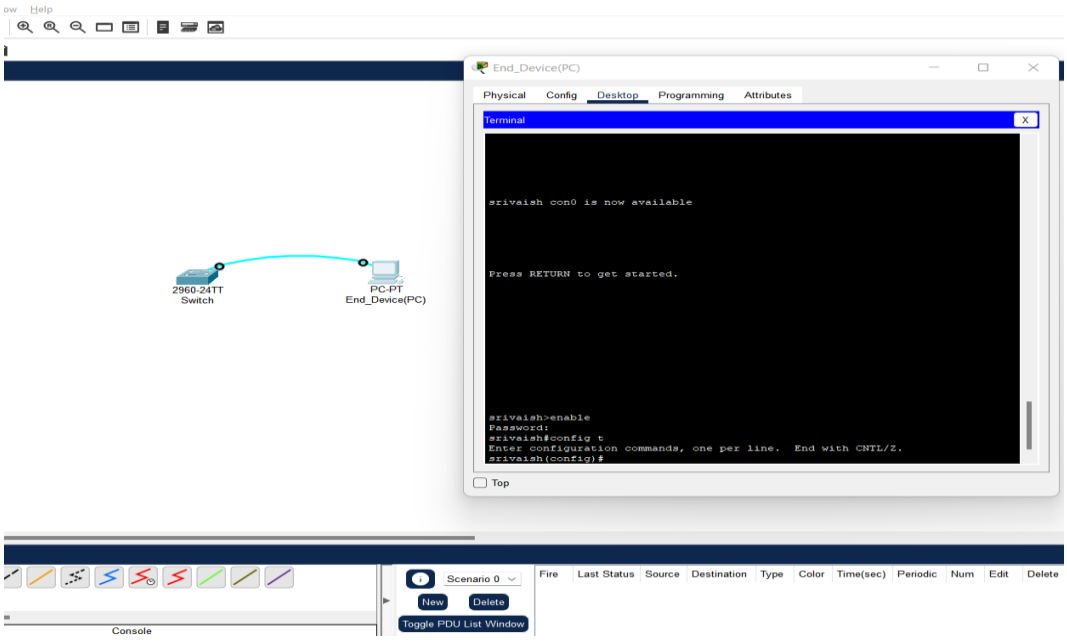


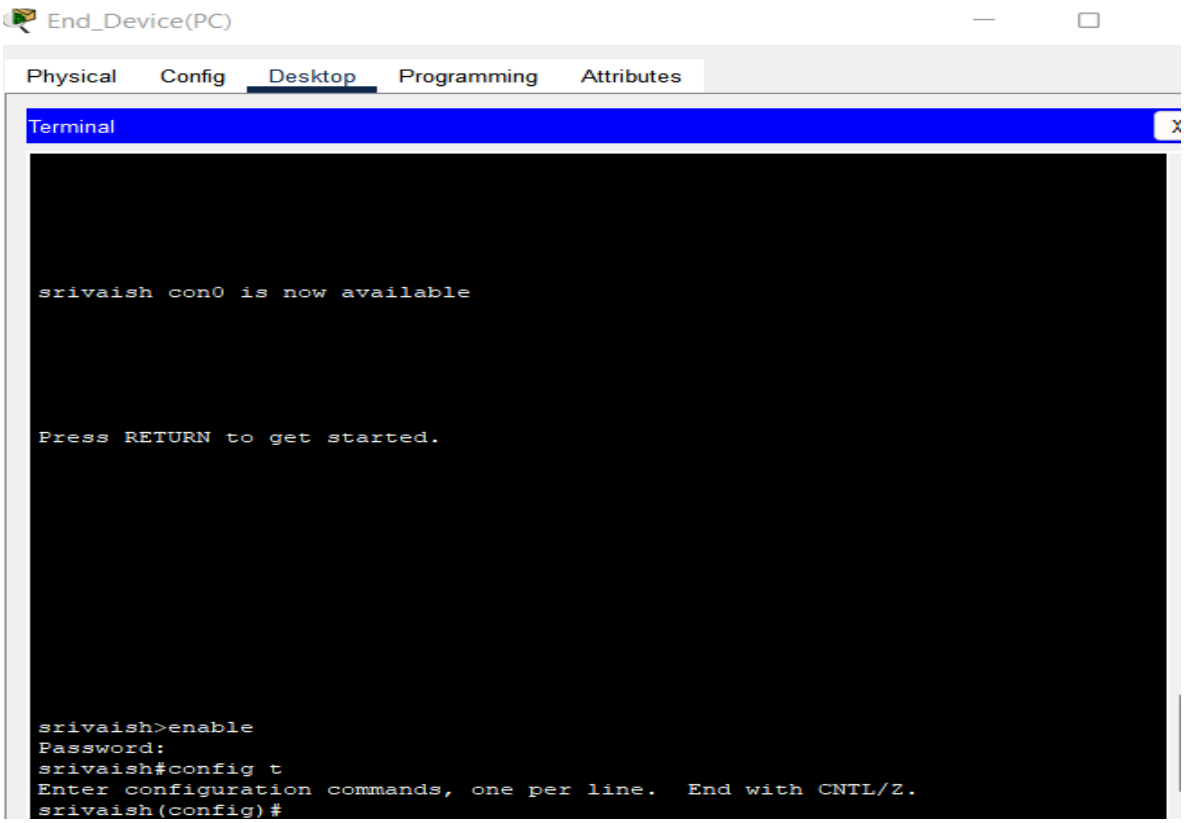
3. Create an enable password of “cisco”

```
% Invalid input detected at '^' marker.

srivaish(config)#
srivaish#
%SYS-5-CONFIG_I: Configured from console by console

srivaish#show running-config
Building configuration...

Current configuration : 1157 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname srivaish
!
enable secret 5 $1$mERr$wouxtyy.vmAne4xxls38Z1
enable password ngdb@1234
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
 --More--
```

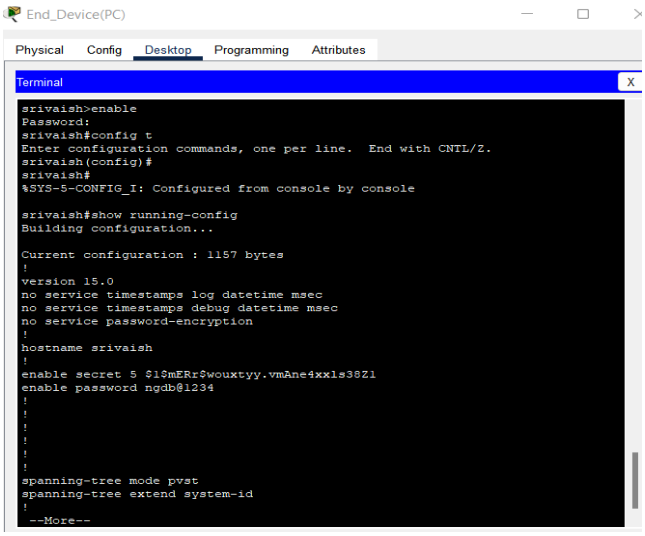
4. Create a console password of “lab”.
5. Logout from the switch and console again using the PC (PC>>Desktop>>Terminal).

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

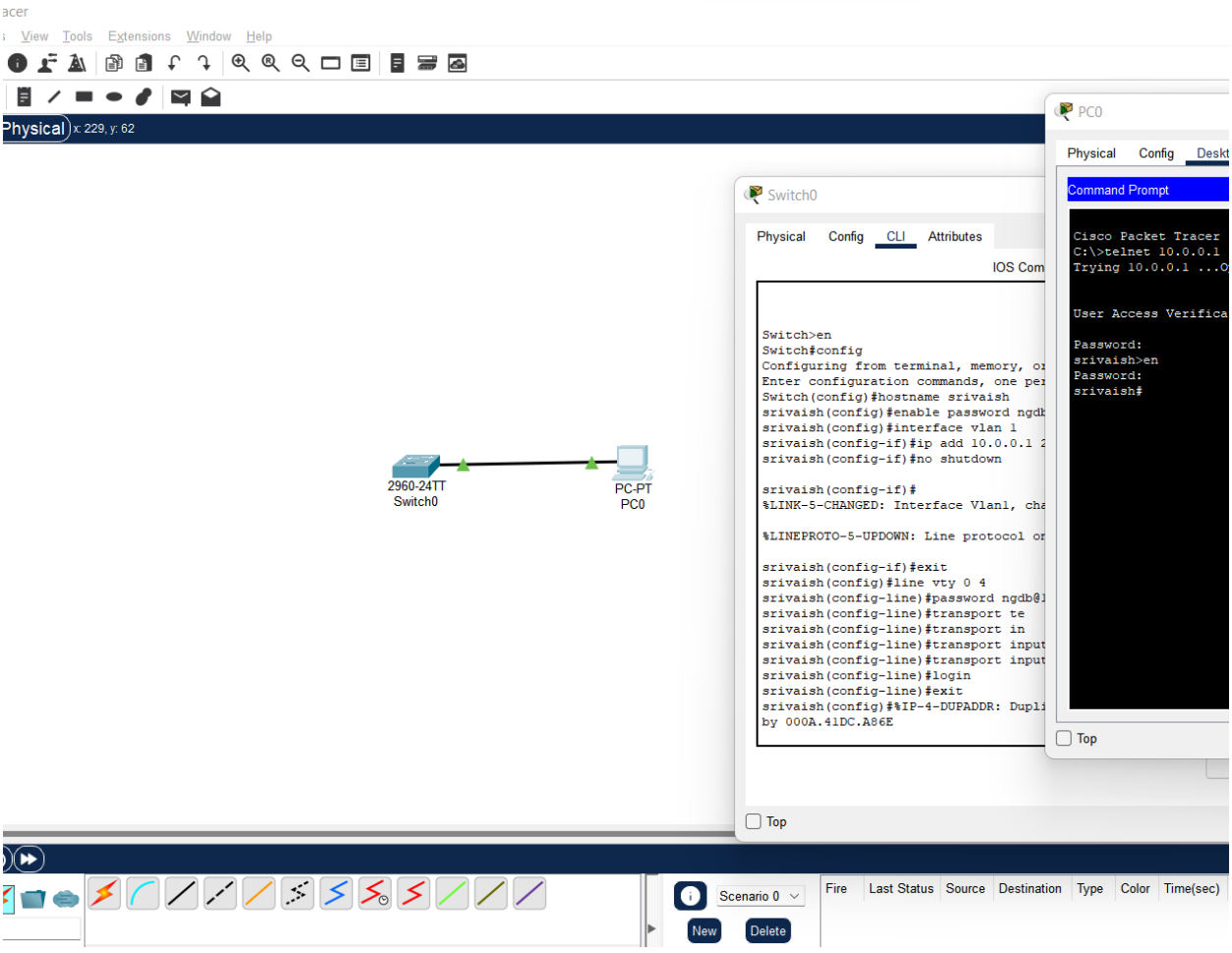


Objective 3: Creating Remote Access to Cisco Networking Device (Telnet)

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.

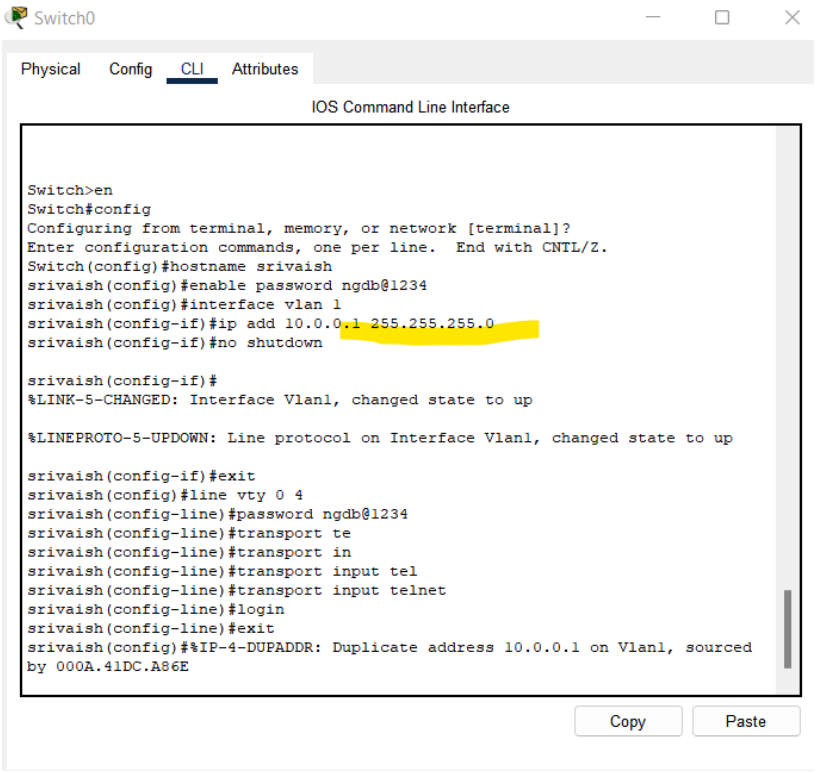
1. Configure and connect the PC and switch according to the diagram. Which cable did you use this time? **[2 points]**

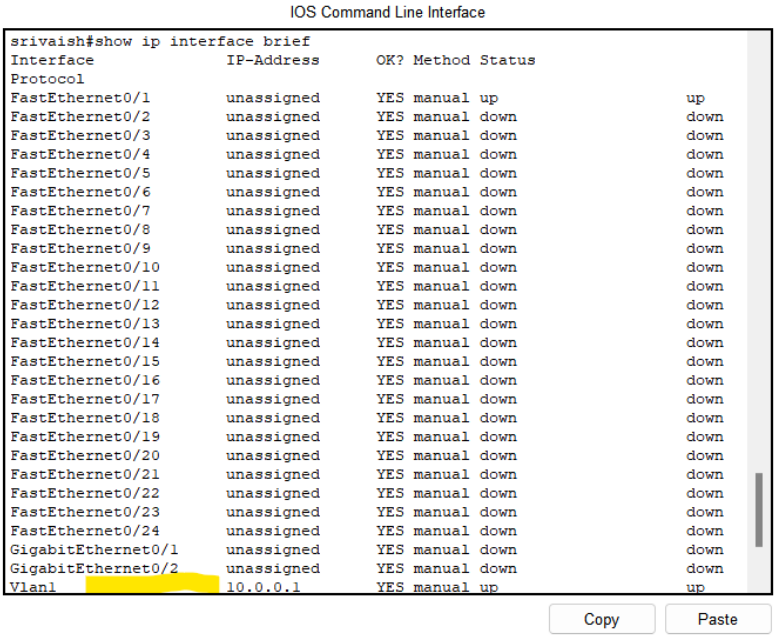
   Ans : Straight-through cable



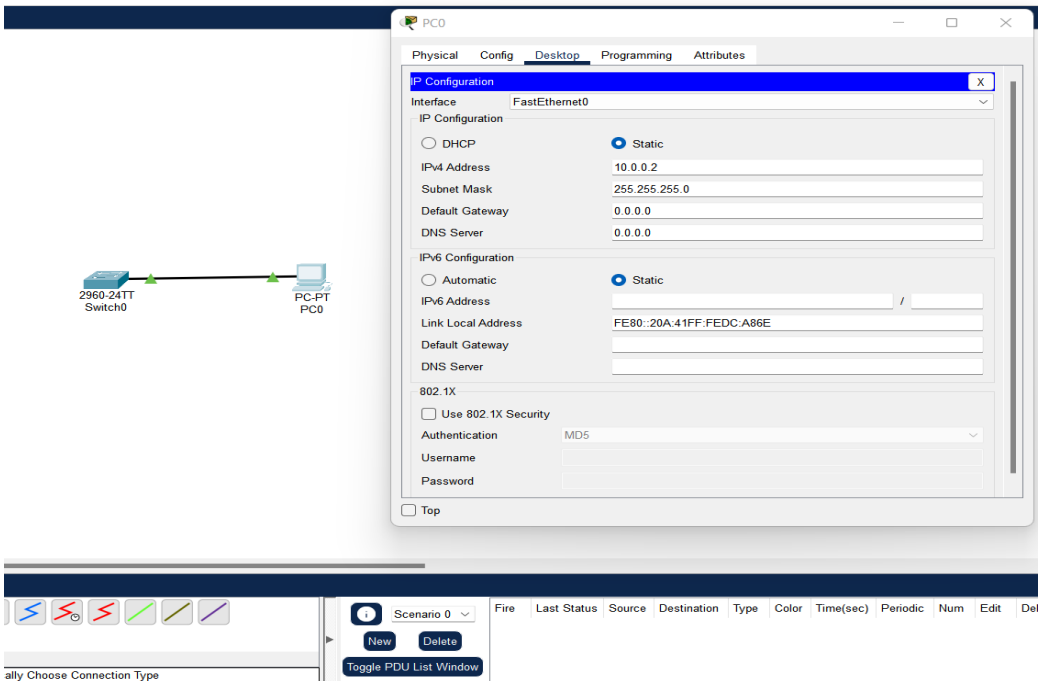
a. Make sure the PC has an IP address (10.0.0.1) and subnet mask (255.255.255.0) in the same subnet as the switch (VLAN 1 IP - 10.0.0.2/255.255.255.0)

Ans : Switch Config:



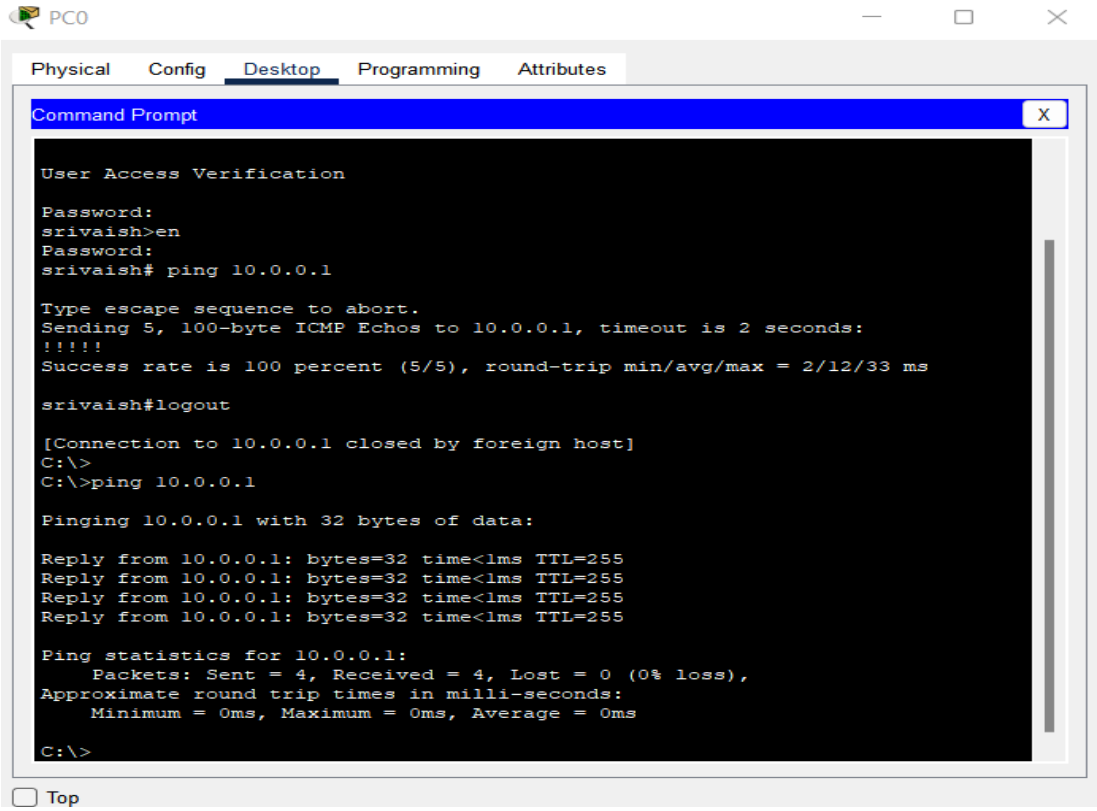


PC Config :

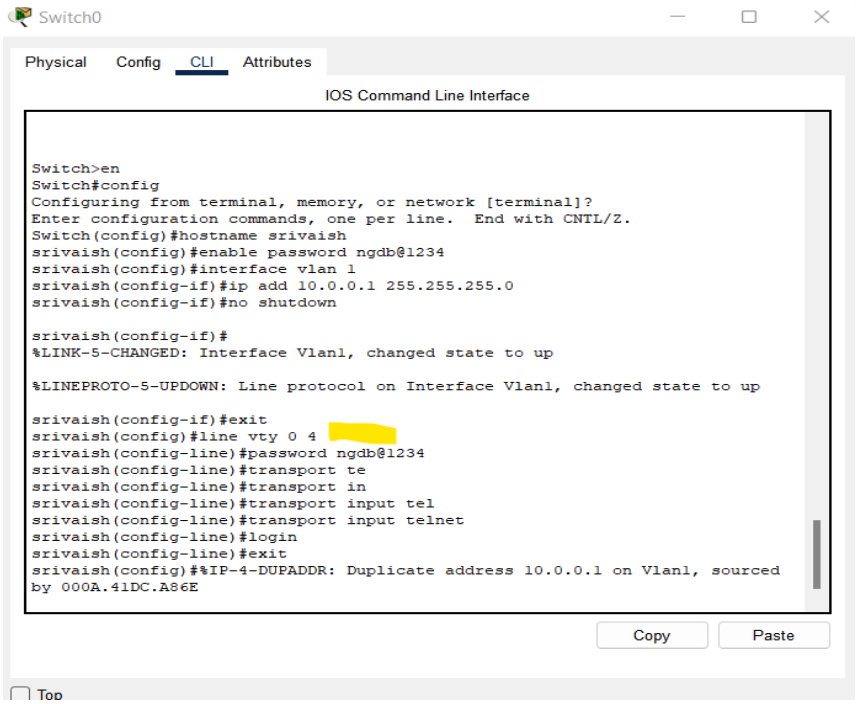


2. Verify the PC can ping the IP address of the switch. Paste the screenshot of the command output. **[5 points]**

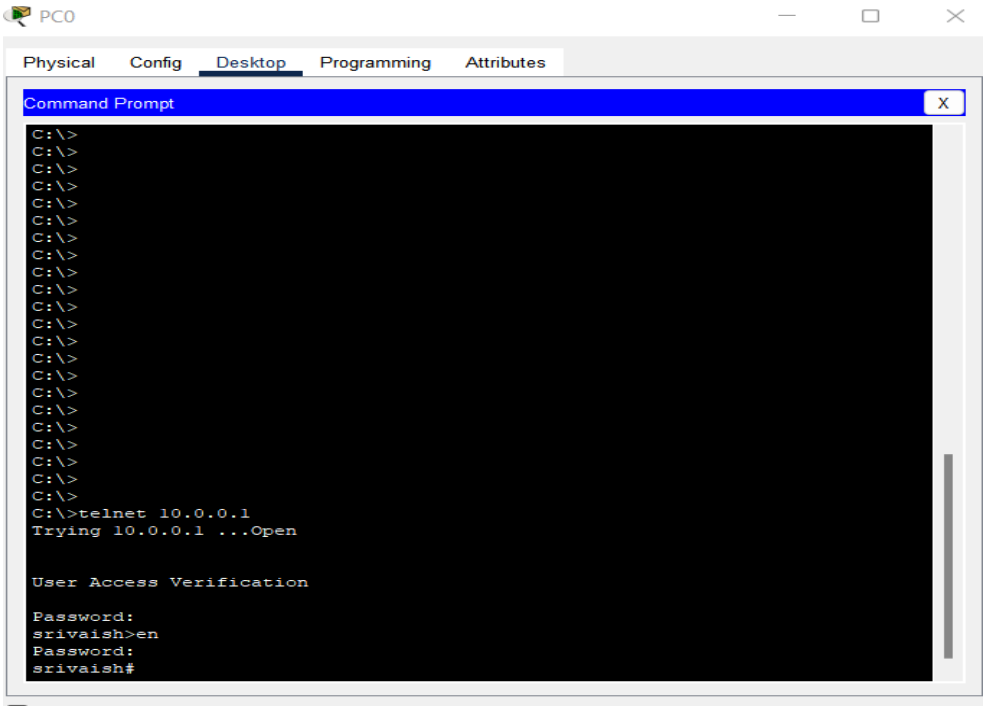
   Ans : PC Ping Switch (10.0.0.2 to 10.0.0.1)



3. Configure Telnet on the switch
    a. Use all the vty lines
    b. Create a password of “telnet” as “cisco”



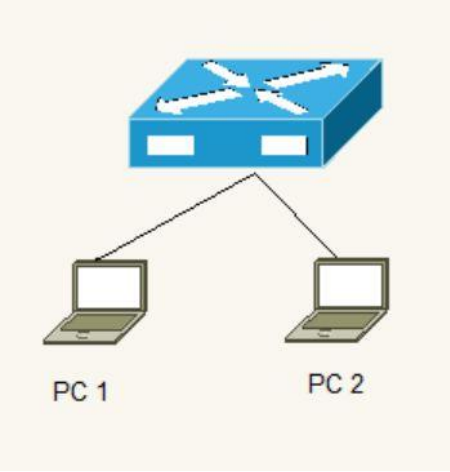
    c. Use Terminal (PC>>Desktop>>Command Prompt) of the PC to Telnet to the switch. Paste the screenshot of telnet output. **[10 point**



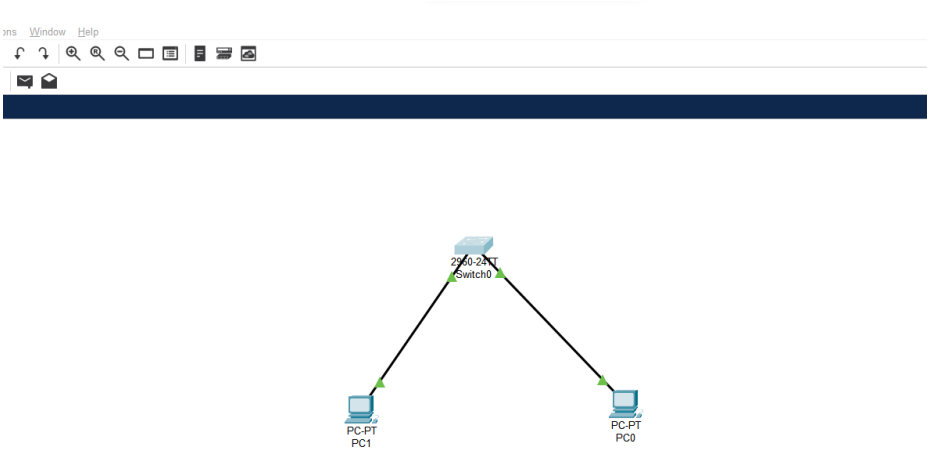
Part 2

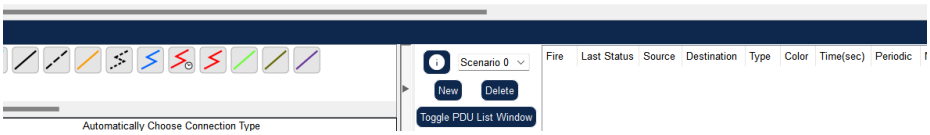
Objective 1: Cisco IOS Switch Port Configuration

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

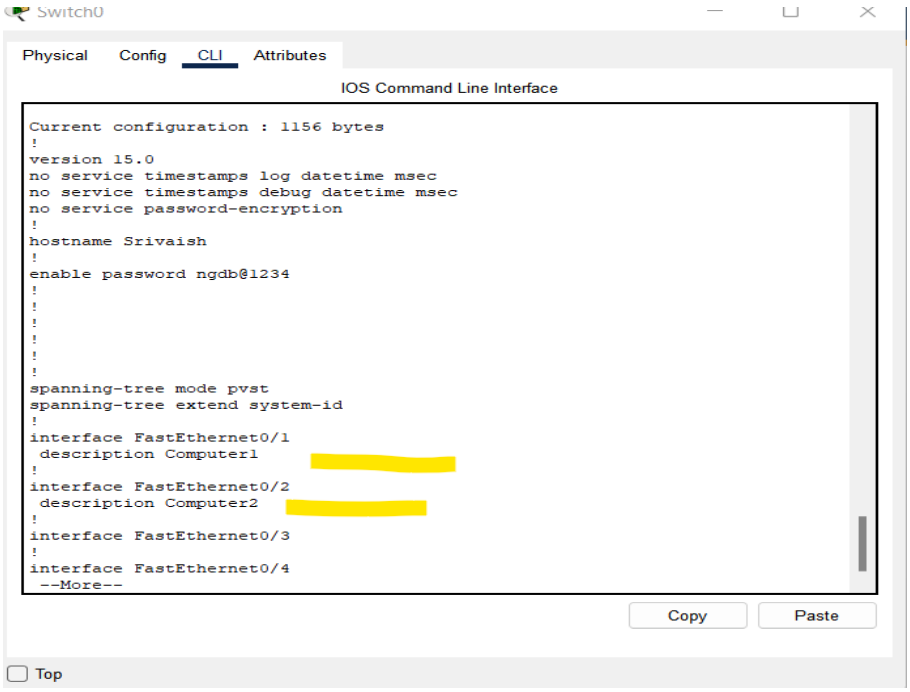


2. Connect PC1 and PC2 to a switch

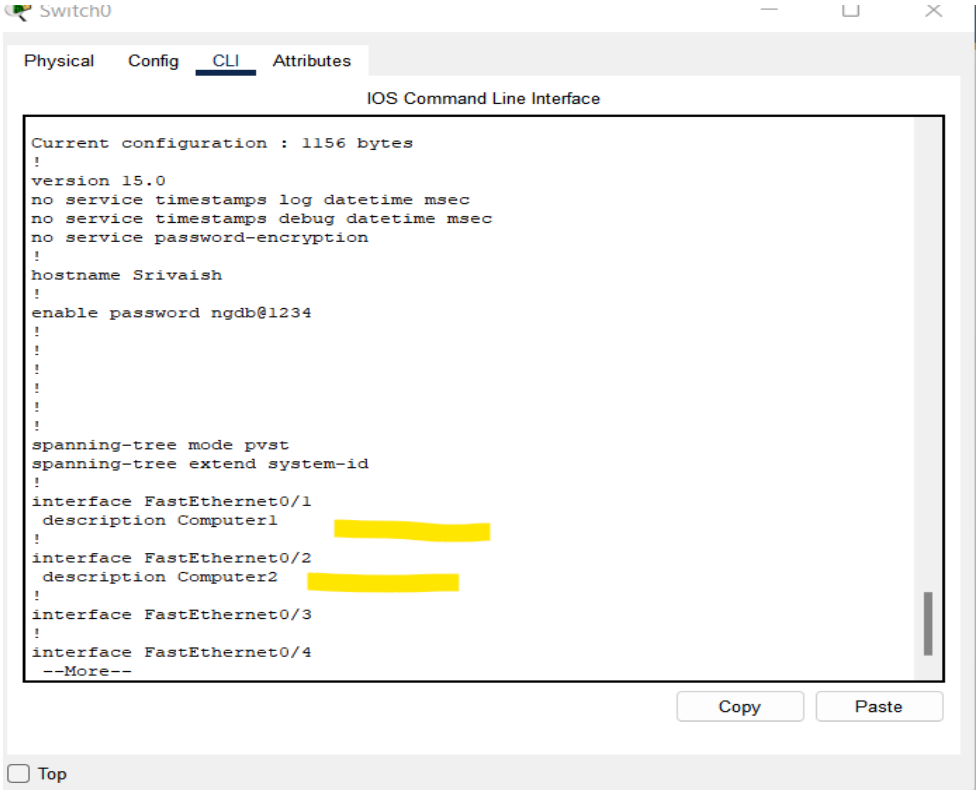




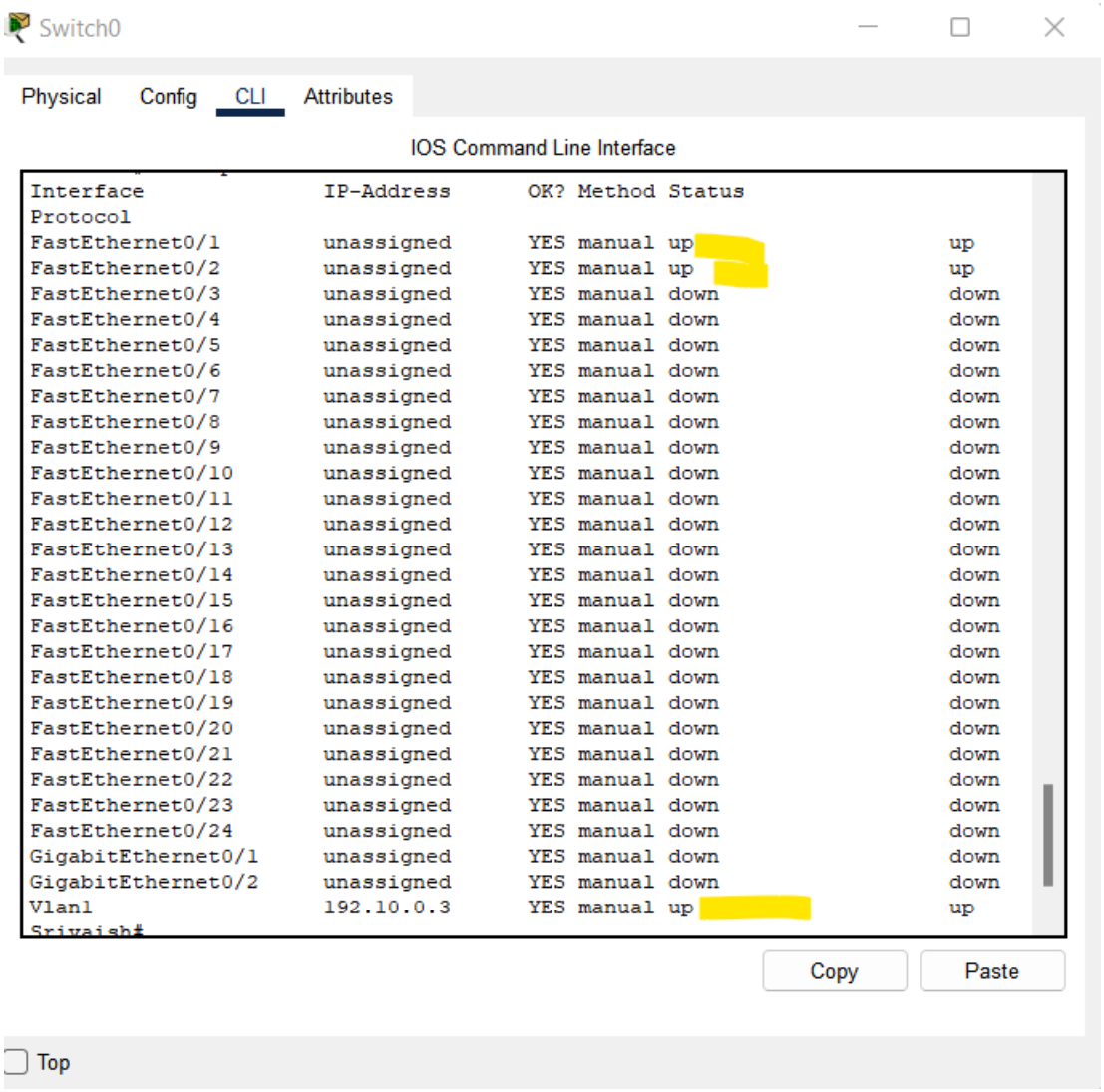
3. Configure a description on the switchports connected to each PC
    a. The port connected to PC 1 should have a “description Computer 1”



    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*)

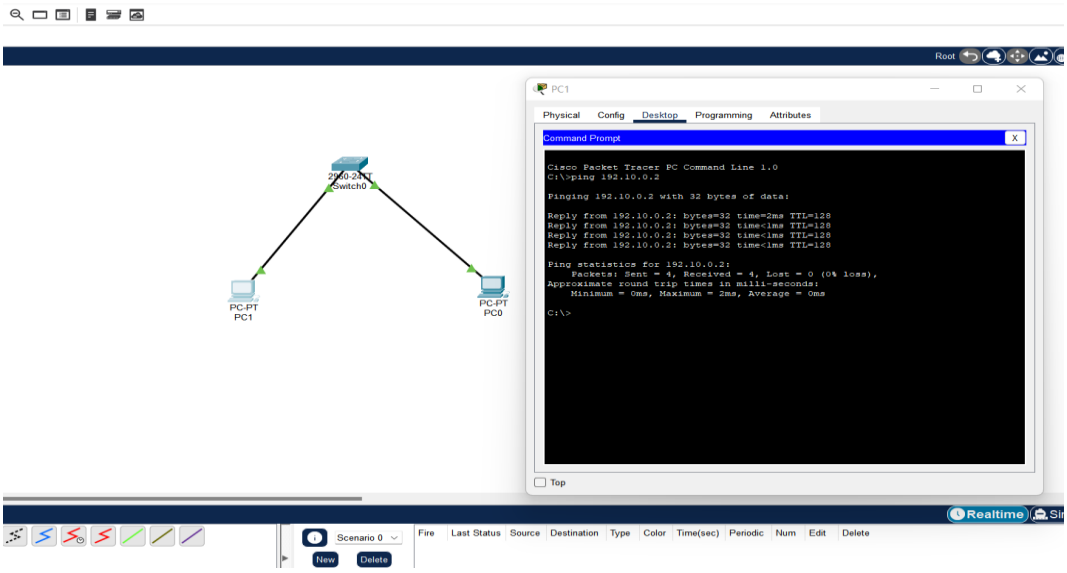


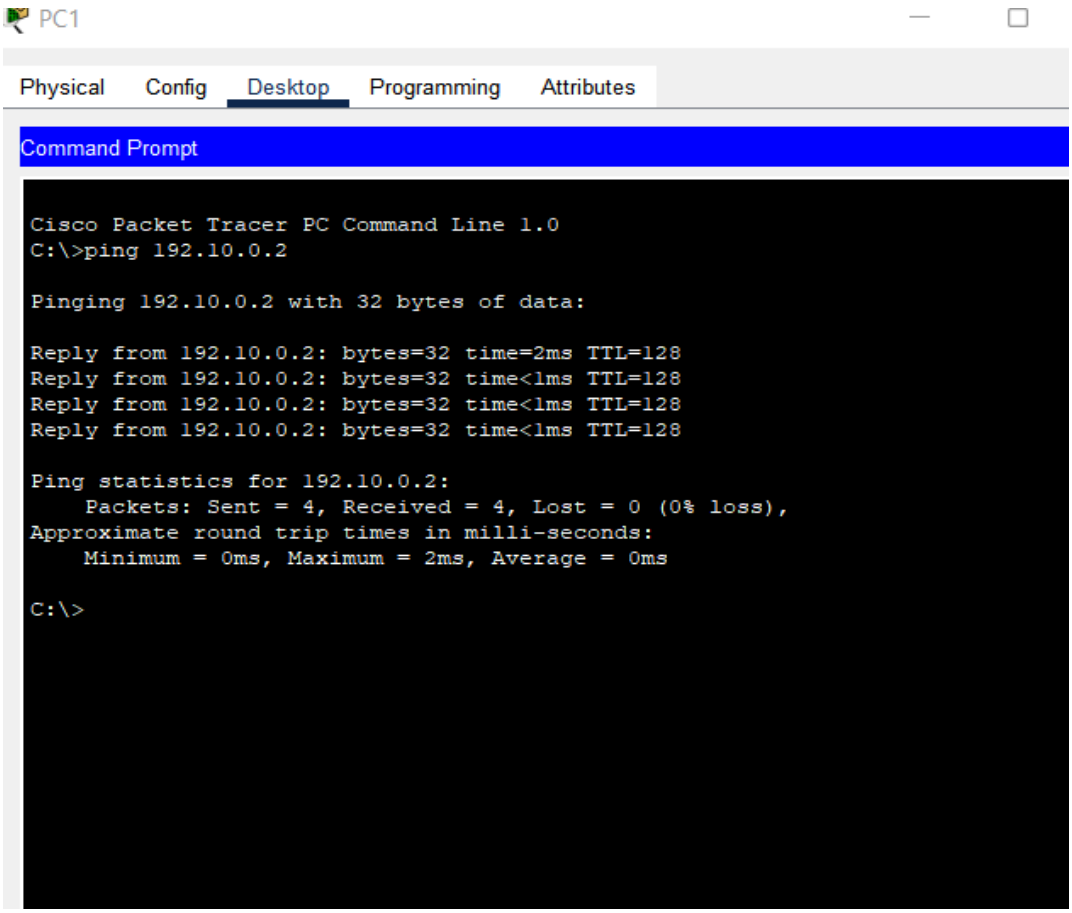
a. List the steps you had to perform to get the PCs to ping each other [**20 points**]

File Edit View

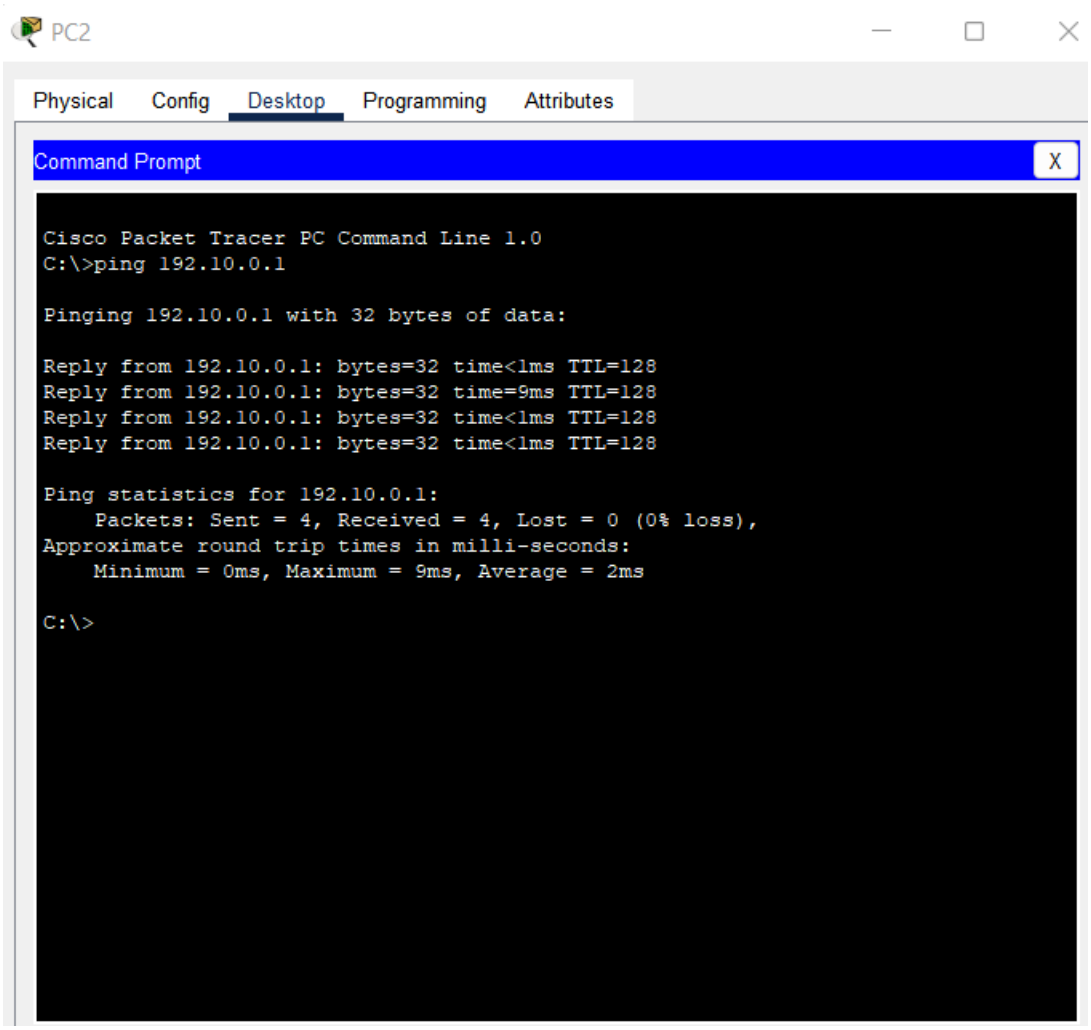
```
"#Lab2 CISCO IOS AND STP by Srivaishnavi"

STEPS:
1. Configure the static IPV4 address with 192.168.0.1 on PC1
2. Configure the 255.255.255.0 subnet mask
3. Configure the Static IPV4 address with 192.168.0.2 on PC2
4. Configure the 255.255.255.0 subnet mask
5. Interconnect both PC1, and PC2 using a Network Device - Switch.
6. Login into Switch CLI
7. Switch > : Type enable to switch from user mode to previlaged mode
8. Configure the hostname and enable password in global config mode
9. Once configured, use interface Vlan 1 command
10. And then in the (config-line) mode configure the ip address using - Ip address 0.0.0.0 255.255.255.0 subnet mask
11. type no-shutdown
12 eexit()
13. run show ip interface brief command to check whether the status of interface is up/down
14. open the Desktop > Commnad Prompt on PC1 > Do Ping <Ip Address> and the ping should happen confirming the connection estbalishment.
```

Pinging from PC 1 to PC2 (192.10.0.1 to 192.10.0.2)

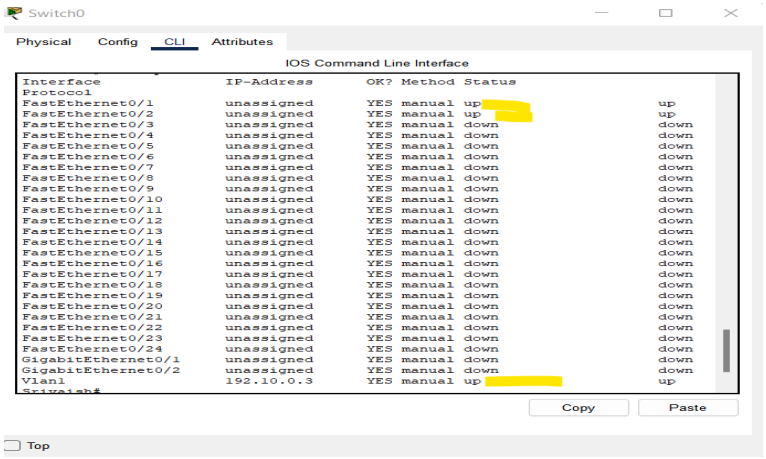




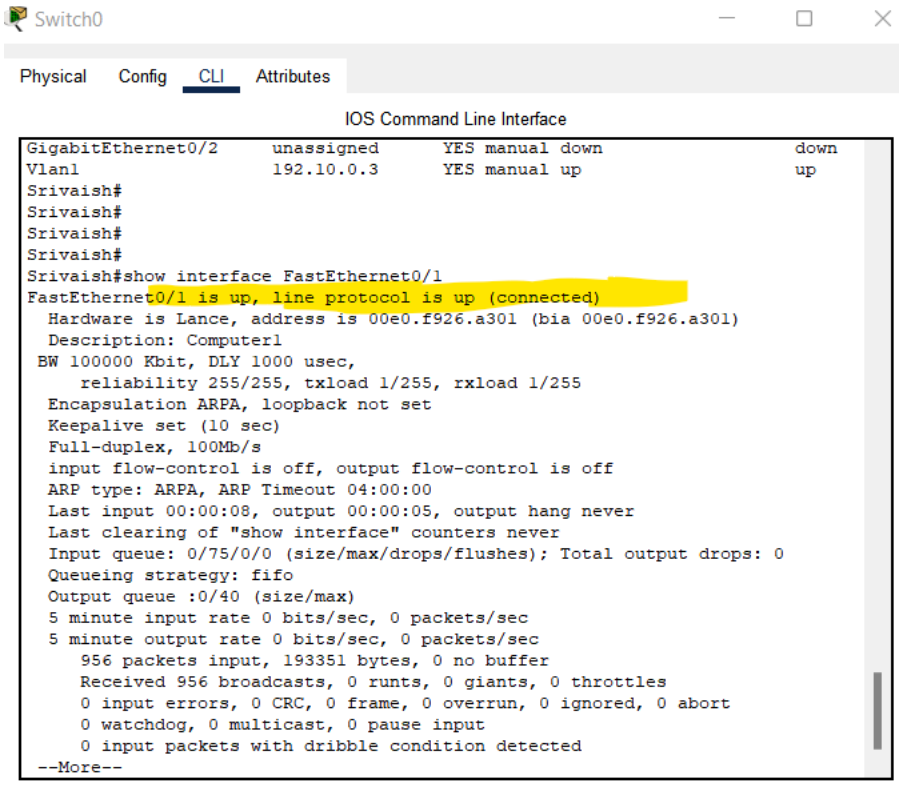
Ping from PC2 to PC1 :



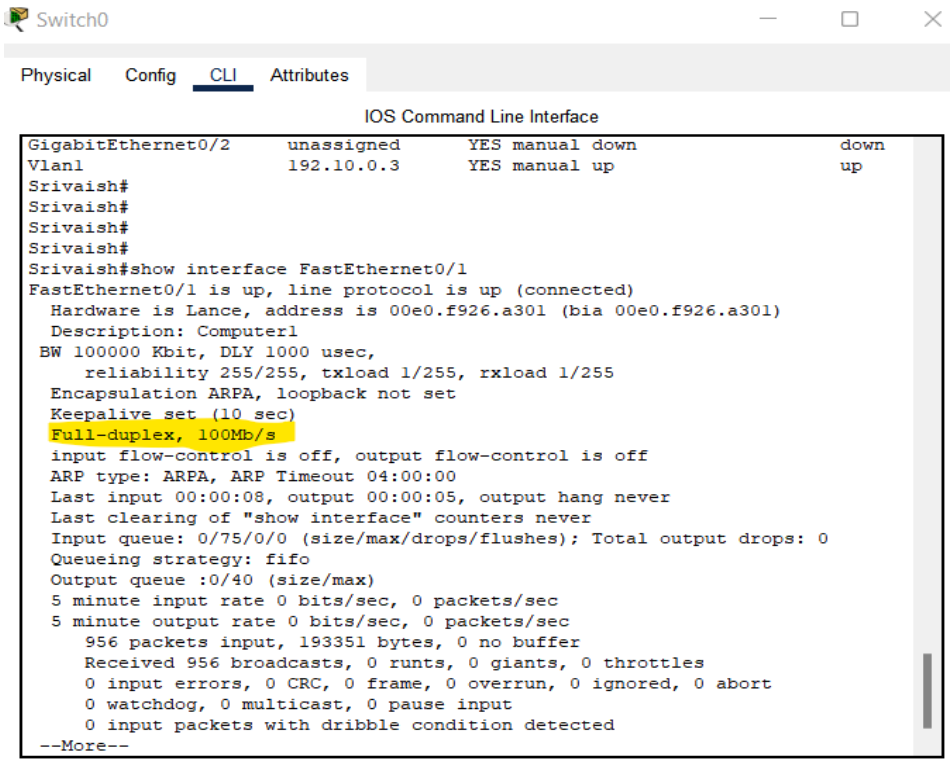
5. Check the status of the switch port connected to PC1
    a. Provide a screenshot of the status of the port [**2 points**]



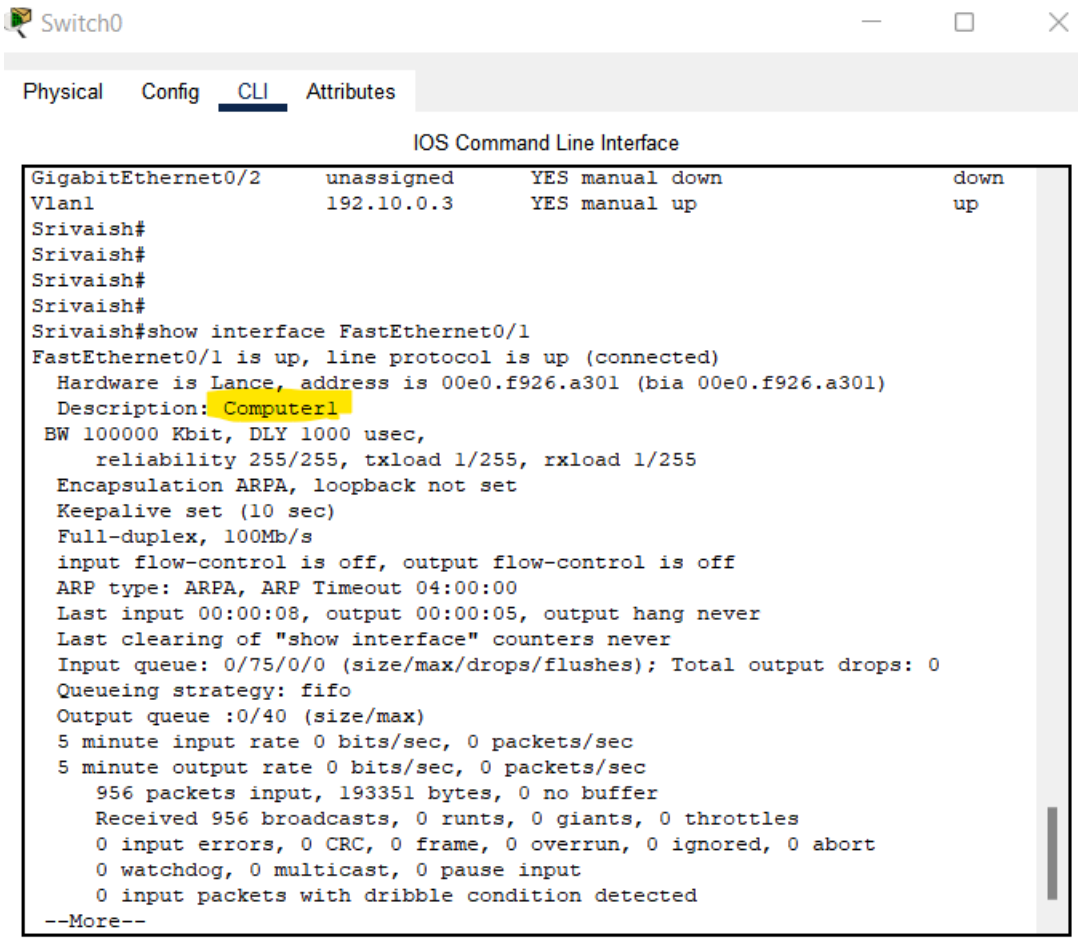
    i. Indicate that the port is up [**2 points**]



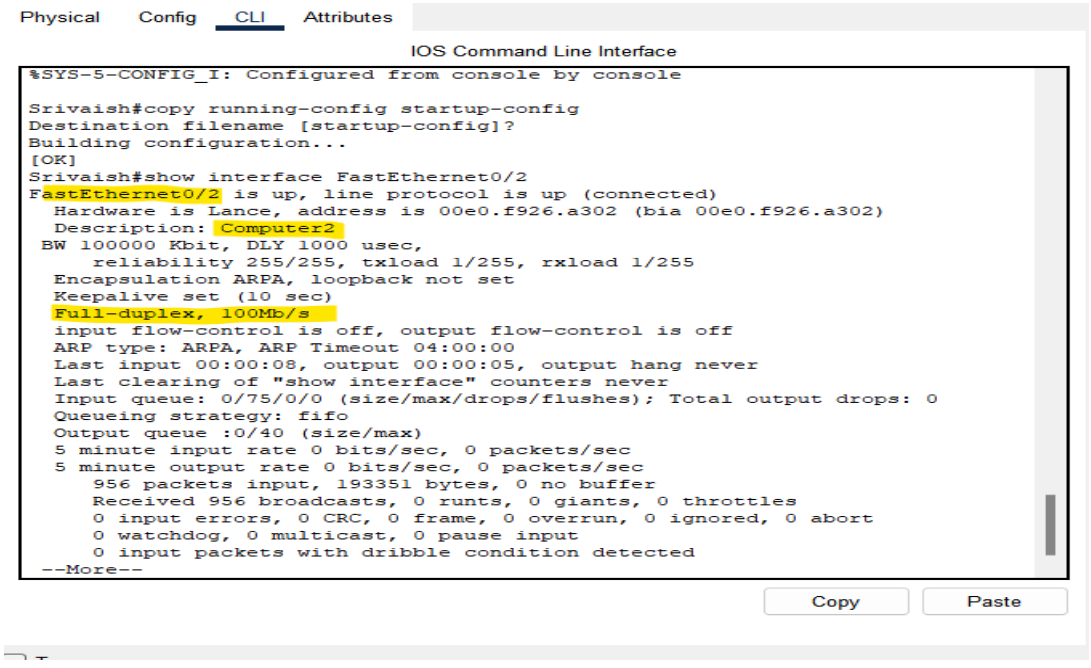
ii. Indicate the speed and duplex of the port [**2 points**]



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

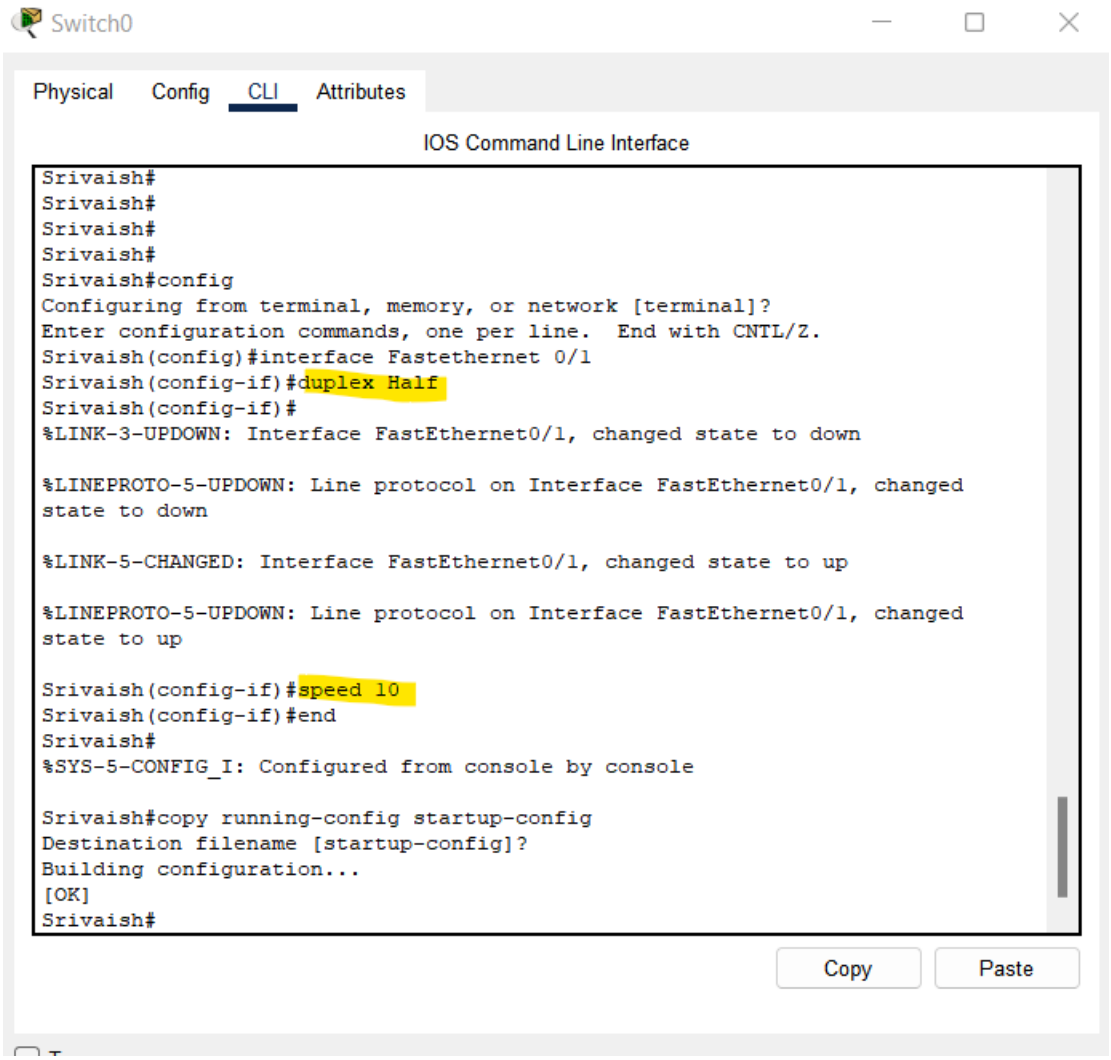


Switch port connected to PC2

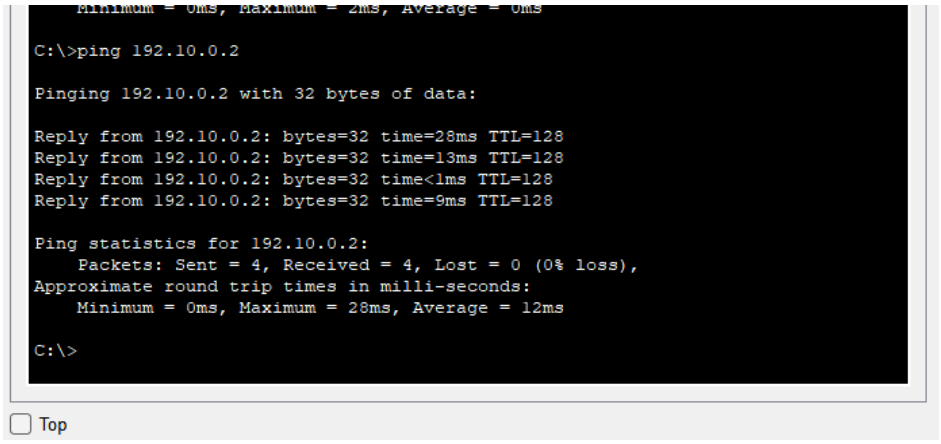


6. Configure the switch port that connects to PC1

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



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

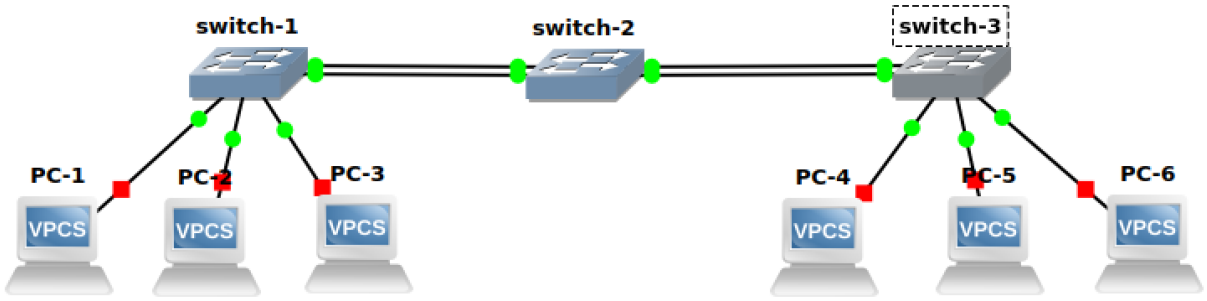


Ans : Yes. PC1 can still reach PC2 in Half-duplex mode. Because, half-

duplex devices can only transmit in one direction at one time. So the data can move in two directions b/w Tx and Rx but not at the same time.

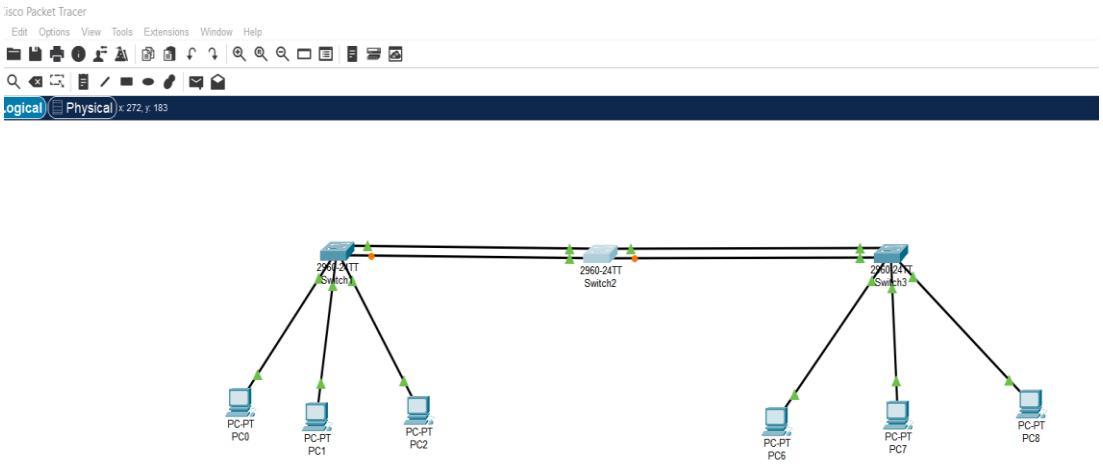
X`

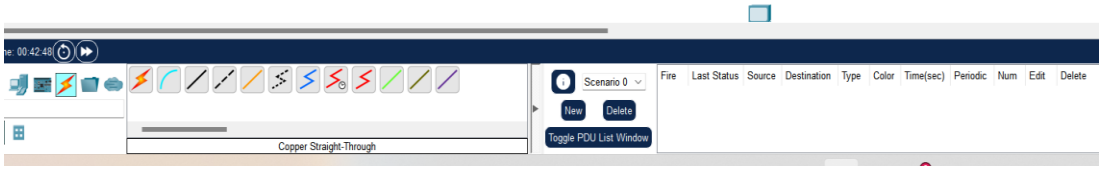
7. Now create a following topology in Cisco Packet Tracer



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

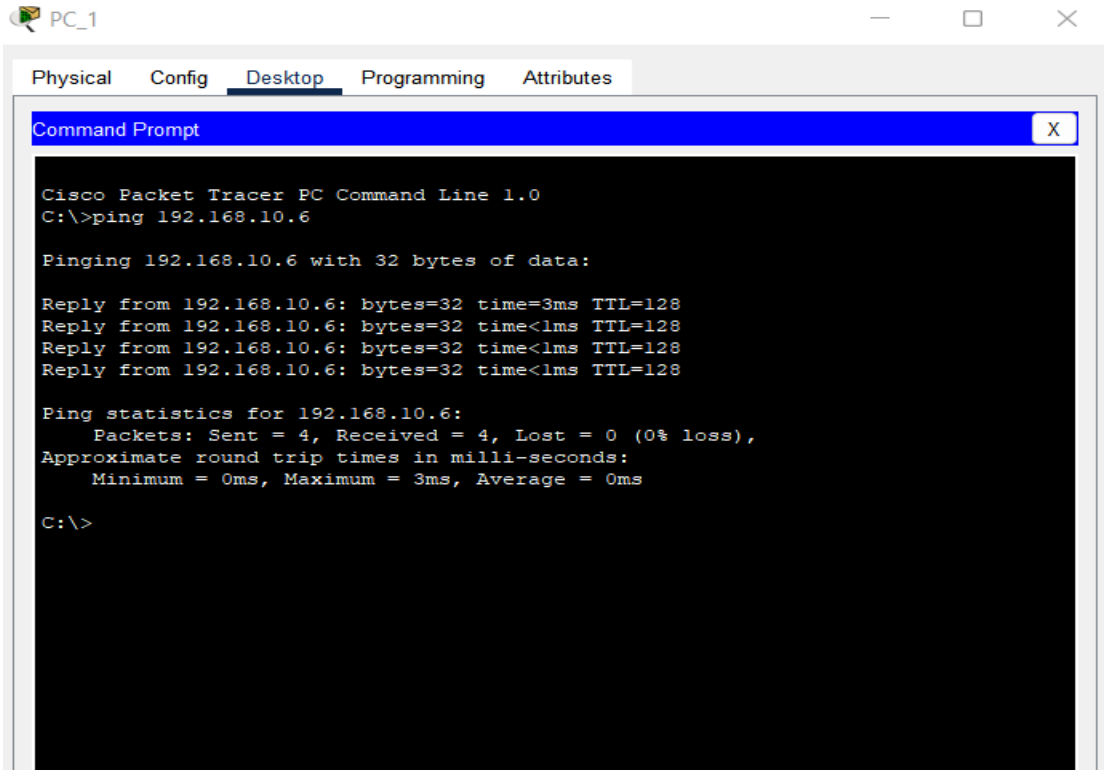
Ans :: IP Address of all hosts :: 192.168.10.1, 10.2,10.3,10.4,10.5,10.6



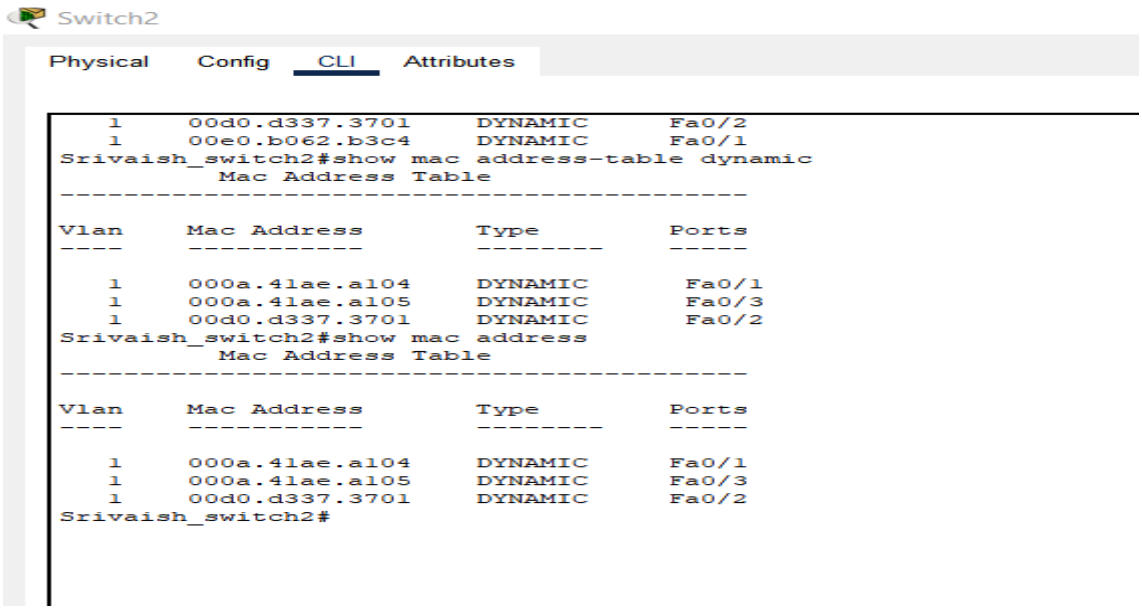


b. Ping PC-6 from PC-1. What command would you use to look at the mac-table on switch-2? Paste the screenshot showing its output. **[5 points]**

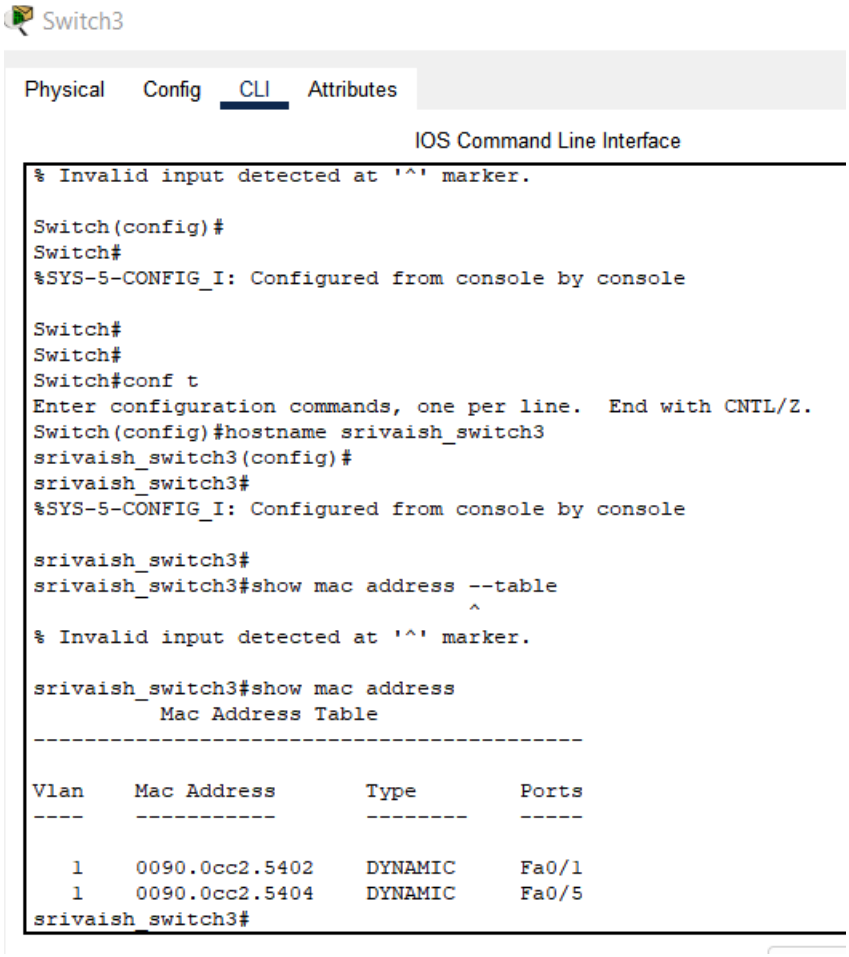
Ping : From PC_1 to PC_6 (192.168.10.1 to 192.168.10.6)



Command to see the Mac_Table : SHOW MAC ADDRESS—TAB

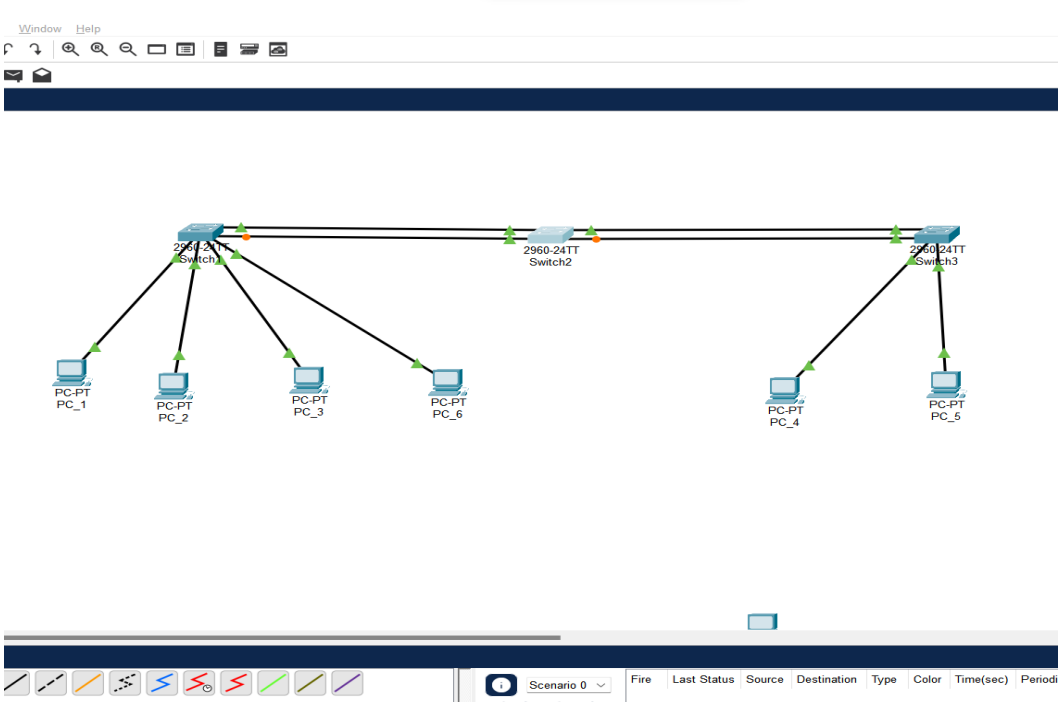


c. Interpret the mac-table of switch-3 and briefly explain it. **[5 points]**



SWITCH_3 Mac address table constitutes the Mac Addresses shows the no. of Vlan connectiosn per port. And the type of ports/interfaces used in the connection and the type of the connection. Fa0/1, Fa0/5 are connecting ports b/w Switch2 and Switc3.

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]**




```
Srivaish_switch2>
Srivaish_switch2>en
Password:
Srivaish_switch2#show mac address
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    000a.41ae.a104    DYNAMIC     Fa0/1
   1    000a.41ae.a105    DYNAMIC     Fa0/3
   1    00d0.d337.3701    DYNAMIC     Fa0/2
Srivaish_switch2#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    00d0.d337.3701    DYNAMIC      Fa0/2
Srivaish_switch2#
```

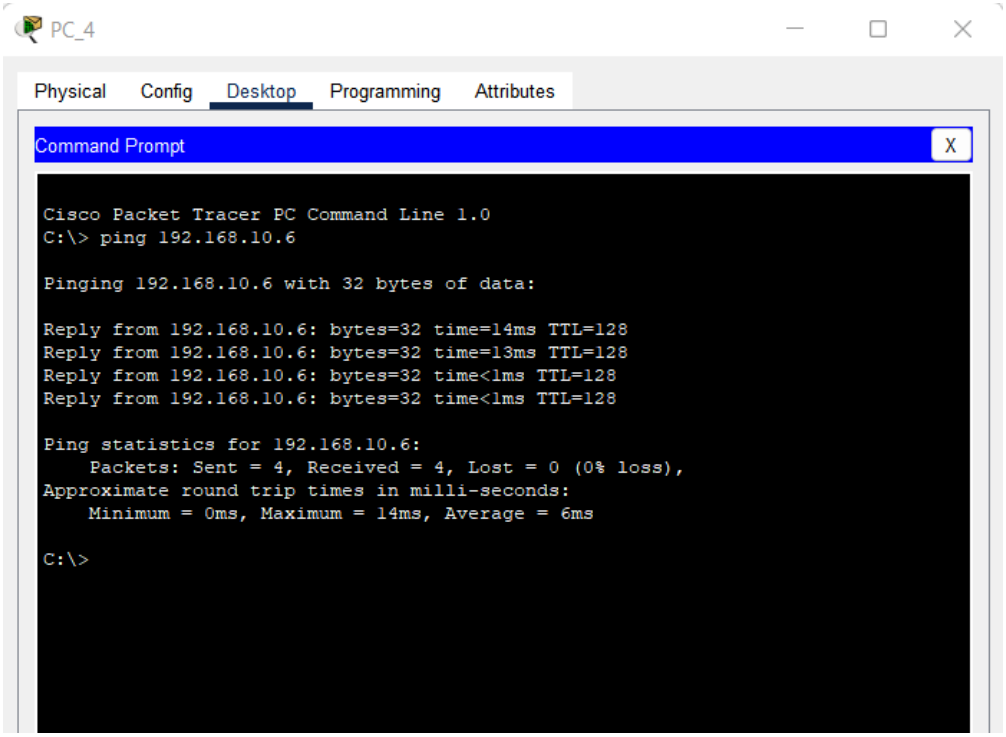
Copy Paste

Top

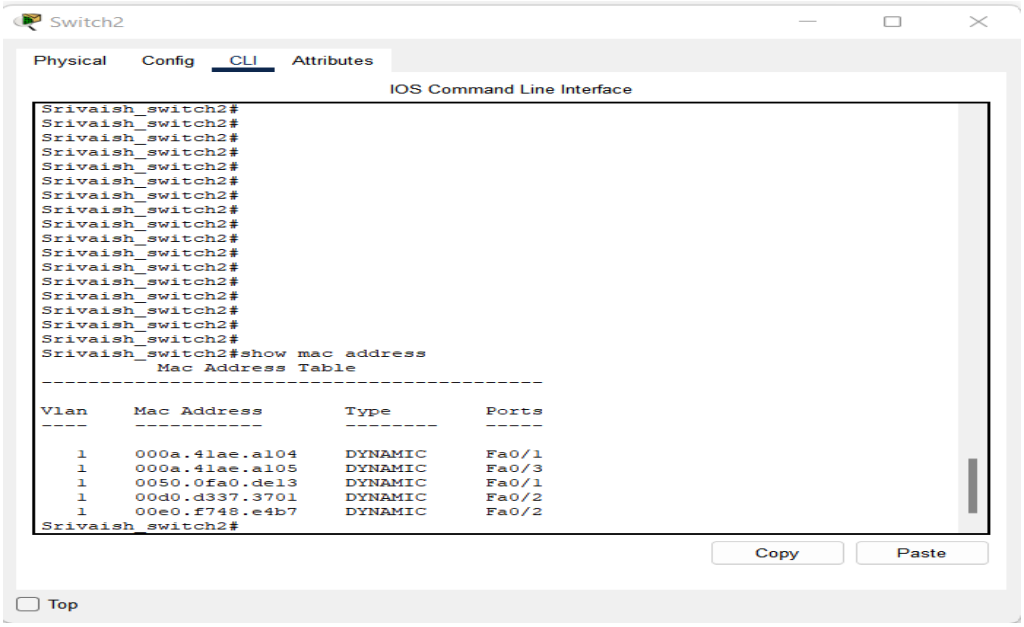
YES. There is a change in the dynamic mac address table. Because of change in the port connection, the interface mac address is changed.

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]**

Ping from PC4 to PC6 (192.168.10.4 to 192.168.10.6)

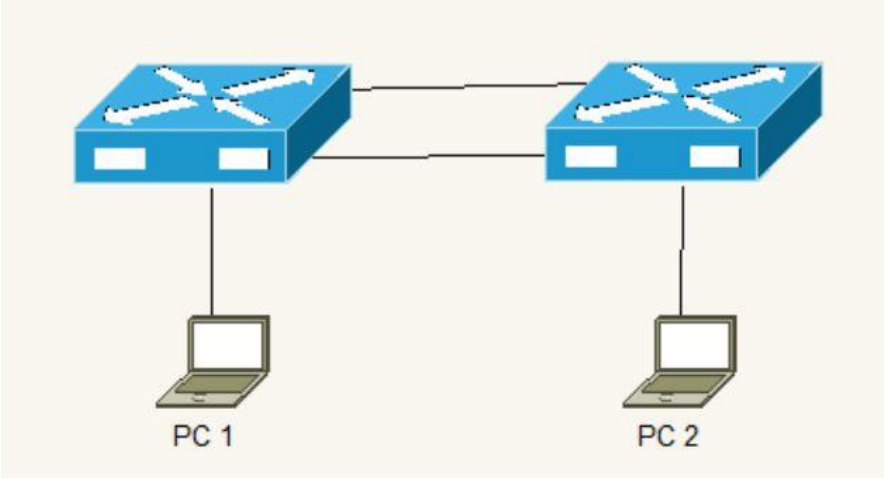


YES. The MAC Address table is updated with the dynamic address of new interface/port connections



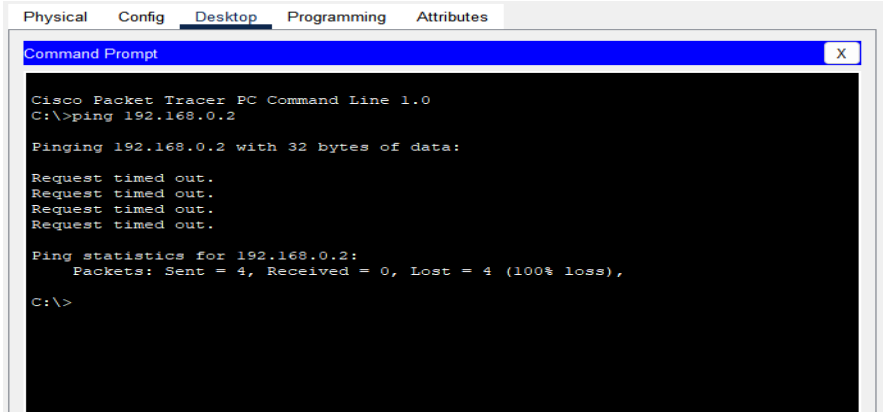
Objective 2: Spanning Tree Protocol (STP)

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

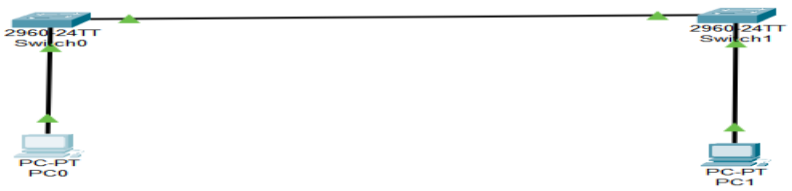


7. Connect PC1 to Switch1 and PC2 to Switch 2

a. Verify PCs can Ping each other



8. Interconnect the switches



   a. Verify PCs can Ping each other

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time=12ms TTL=128
Reply from 192.168.0.2: bytes=32 time=15ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 6ms

C:\>
```

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**]

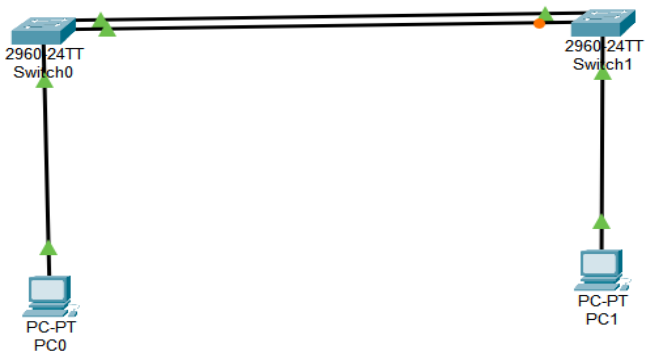
```
Switch1#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0030.f225.c002    DYNAMIC      Fa0/2
Switch1#show
```

```
Switch>en
Switch#show mac address-table dynamic
          Mac Address Table
-----------------------------------------------

Vlan     Mac Address         Type         Ports
----     -----------         --------     -----

   1     000a.f3b8.8302      DYNAMIC       Fa0/2
Switch#
```

Port FastEthernet 02 on both switch1 and switch2 mapping the mad address from end devices.

10. Add an additional link between Switch1 and Switch2

    a. Explain what should happen in this case [**5 points**]



    b. Verify the switches resolved the problem above, indicate how you can determine this in the Cisco switch (*hint: Spanning-tree blocked*) [**5 points**]

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**]

Report Questions

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

   A MAC Address is a 12 digit, hexadecimal number consists of 48 bits. A Mac address is divided into two parts. The first six digits represented the OUI (Organisational unique identifier) and the last six digitas represent the NIC(Network Interface Controller).

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

Switches are slightly faster in the LAN Network because they are wired connections which helps in eliminating the Network Congestion as faced by Router/Modem.

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

   Address Resolution protocol working in the Network Layer of the OSI Model helps in finding the MAC address of the device given the IP address

   How it works :

   In the network layer when the source wants to find out the MAC address of the destination device it first looks for the MAC address in the ARP table. If present there then it will use the MAC address from there for communication. If the MAC addr is not found in the ARP table then the source device will generate an ARP Request message. In the request message the source puts its own MAC address, its IP address, destination IP address and the destination MAC address is left blank.

   When the source receives the ARP reply it comes to know about the destination MAC address and it also updates its ARP cache. Now the packets can be sent as the source knows destination MAC address.

   The ARP Source message is "Broadcast" whereas ARP Reply message is "Unicast"

Total Score = _____/121