Networking Training Program (Module 3 & 4)
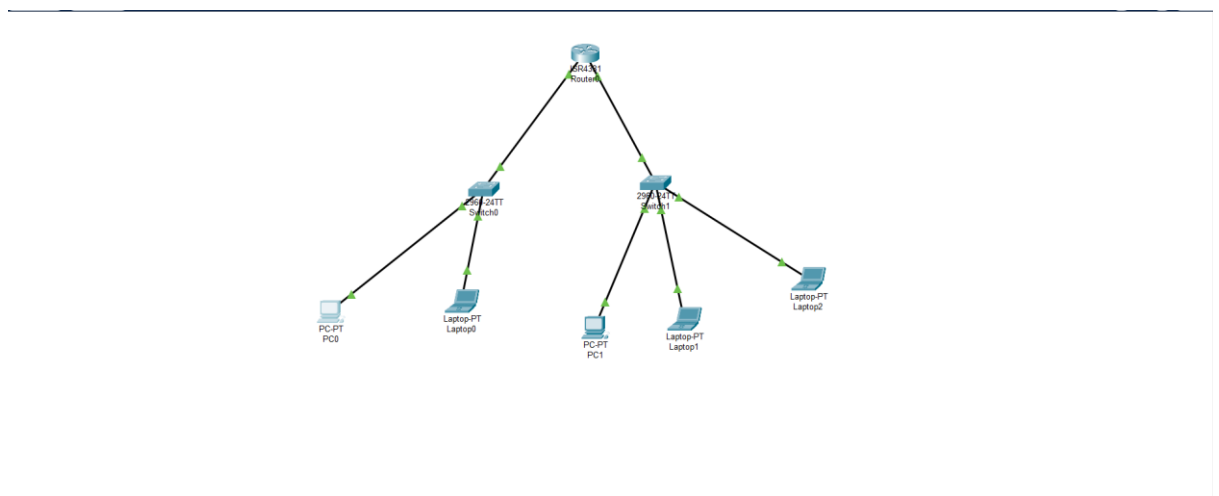
1.) Simulate a small network with switches and multiple devices. Use ping to generate traffic and observe the MAC address table of the switch. Capture packets using Wireshark to analyze Ethernet frames and MAC addressing.

This is the simulated network in Cisco Packet Tracer.

- At first I tried to ping a network with only switches and end devices but I couldn't as to use ping we need to have ip address assigned to the device.
- I created an extended network with the router but have not created a default gateway.
- Therefore ping with the same network works but with another network fails and this will we illustrated in the below snapshot
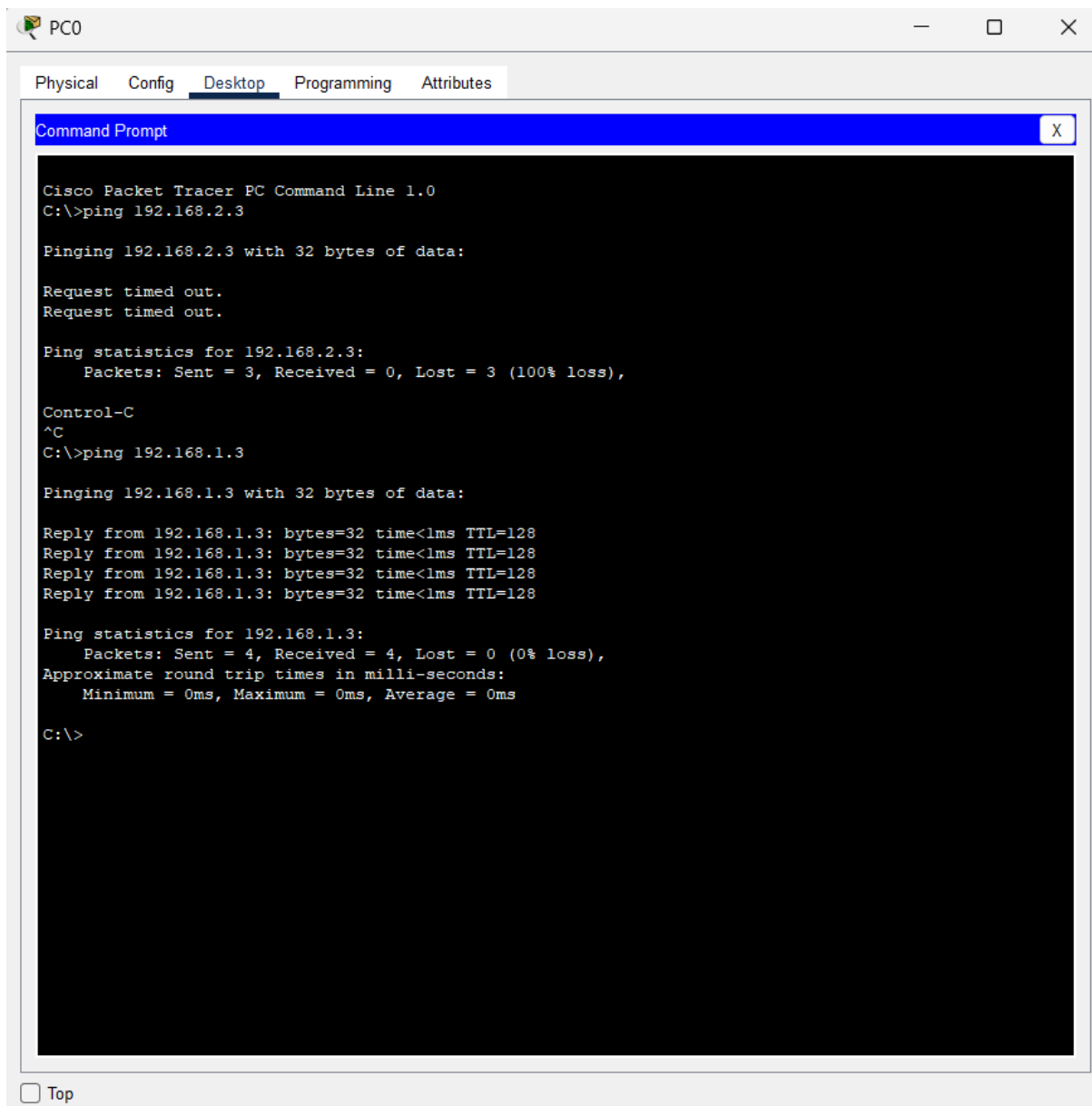
- Now the MAC address table of the switch will be displayed below
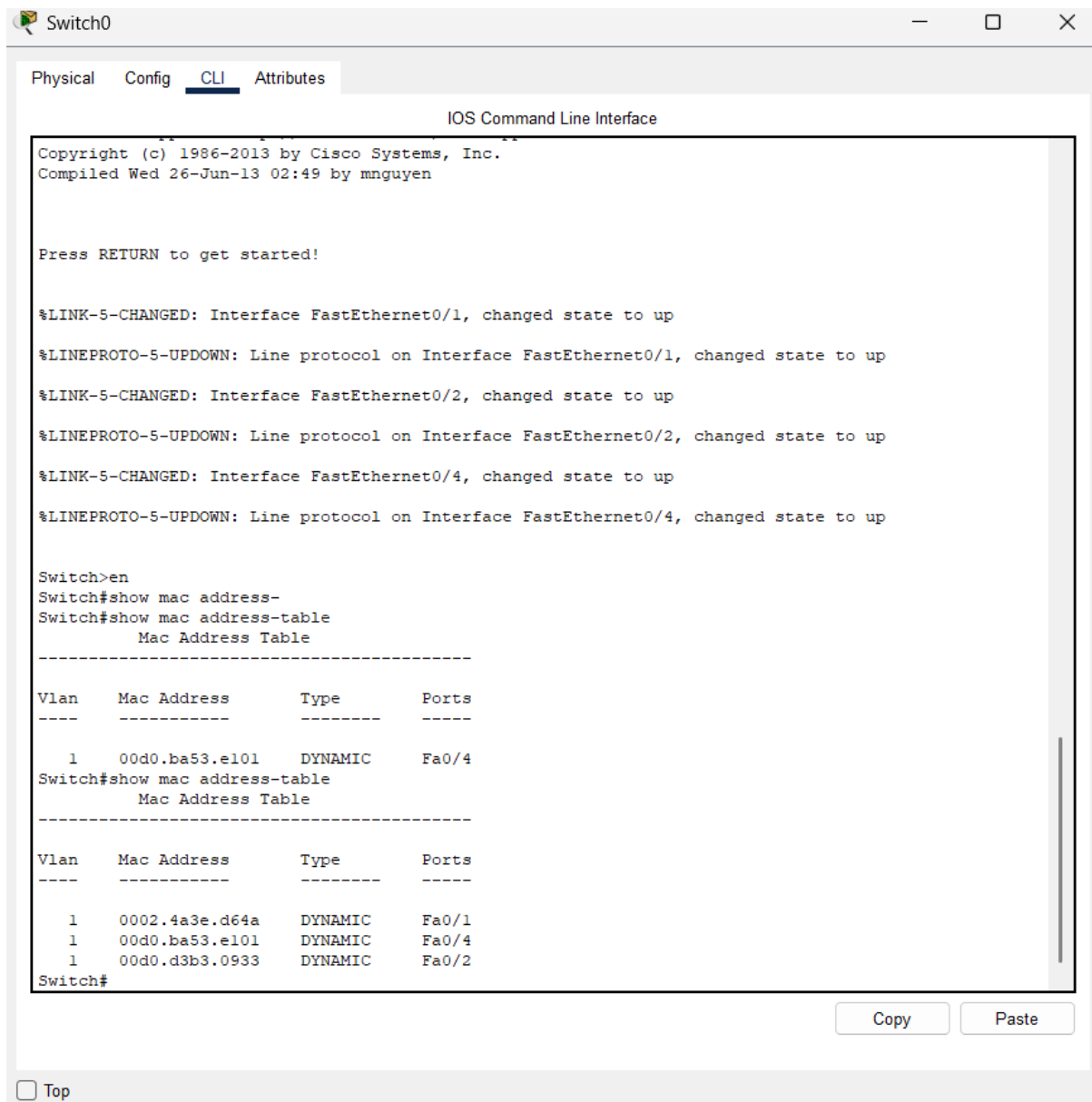
- As you can see at first when we used ping from only one device only that device's address has been noted in the mac address because of DMAC setup.
- The switch learns the MAC dynamically when packets flow through them.
- Every time it notes the source MAC's port Number. If Destination MAC is not present in the table. Then, it floods the packet through all it's port
- After transferring packets through all the ports the MAC table is updated and at the end it has it's completed MAC table.

Now let us see the capturing of ethernet frames using wireshark

- Below picture is the capturing of ARP packet. Ethernet frame is encapsulated into an arp packet and therefore we can see the MAC address from the below packet capture.
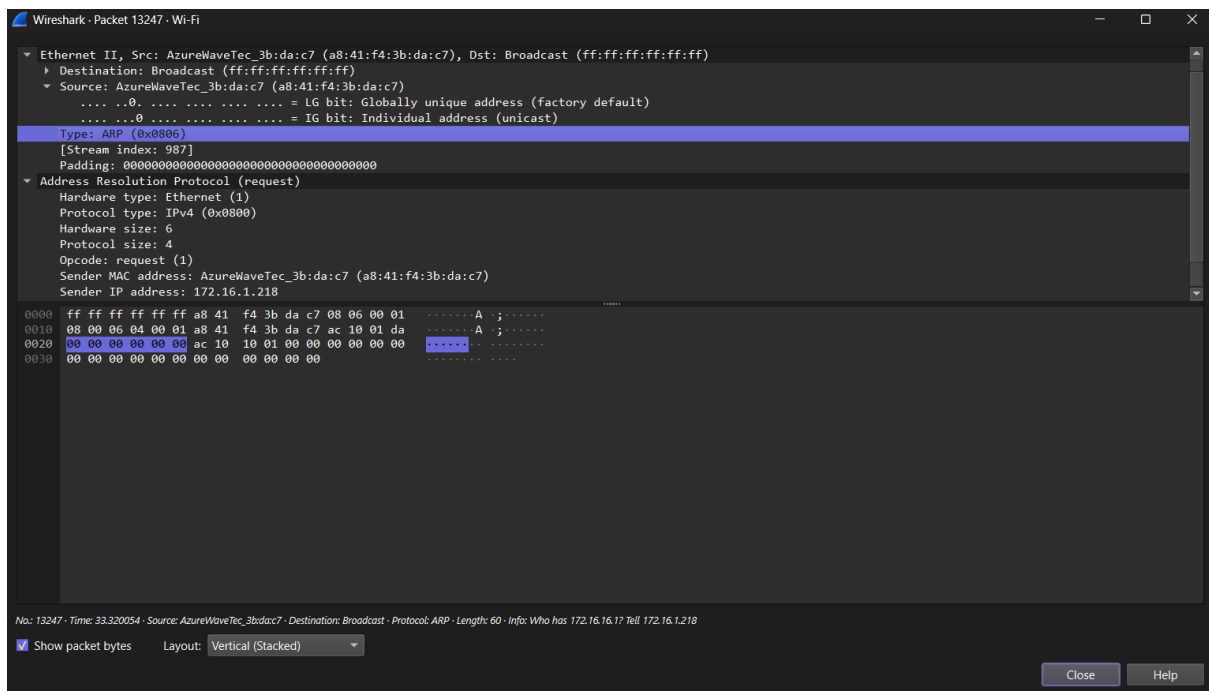
- This is a broadcast packet which has only target IP but not MAC address. Then the corresponding device will send an ARP response.

2.) Capture and analyze Ethernet frames using Wireshark. Inspect the structure of the frame, including destination and source MAC addresses, Ethertype, payload, and FCS. Use GNS3 or Packet Tracer to simulate network traffic.
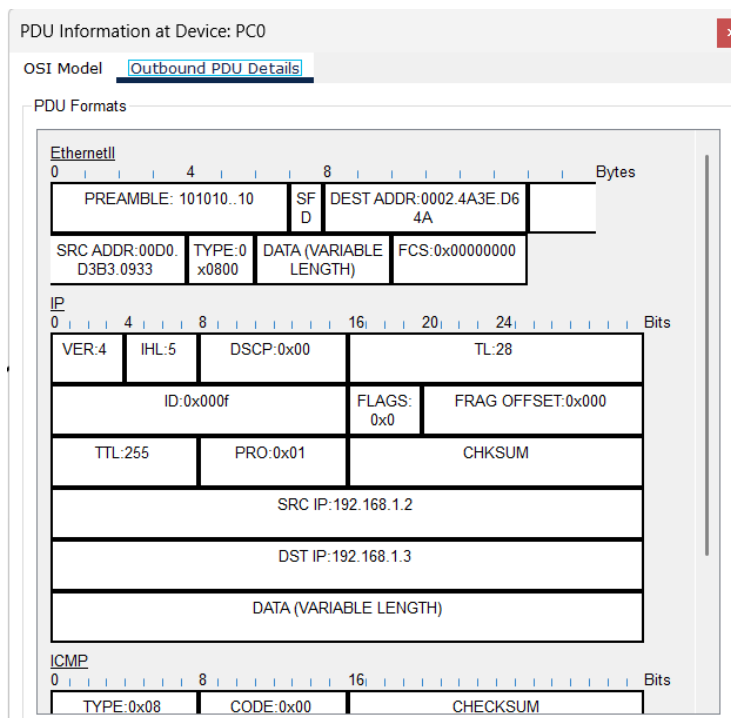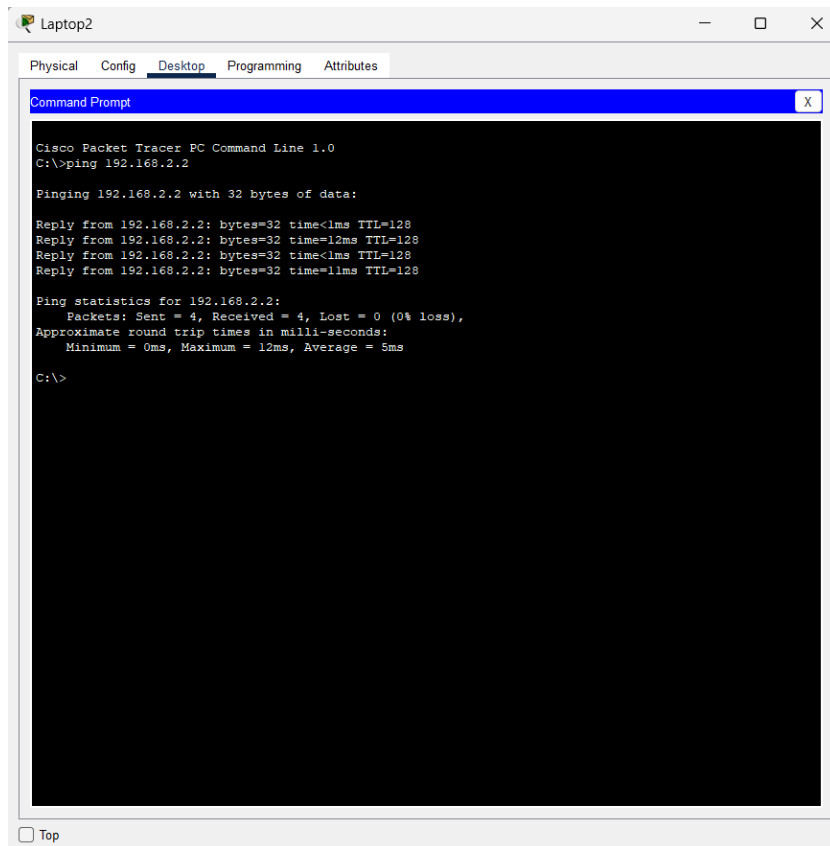

- From the network simulated in the 1st question using Cisco Packet Tracer the outbound PDU Details were captured.
- From this we can understand each header of ethernet frame

- It has preamble, SFD, Dest addr, source MAC addr, type is 0x0800 which signifies an IPV4 packet and then we also have the Frame Check Sequence (FCS).

3.) Configure static IP addresses, modify MAC addresses, and verify network connectivity using ping and ifconfig commands.

- Using the same network in question 1, The static ip configuration settings are displayed below
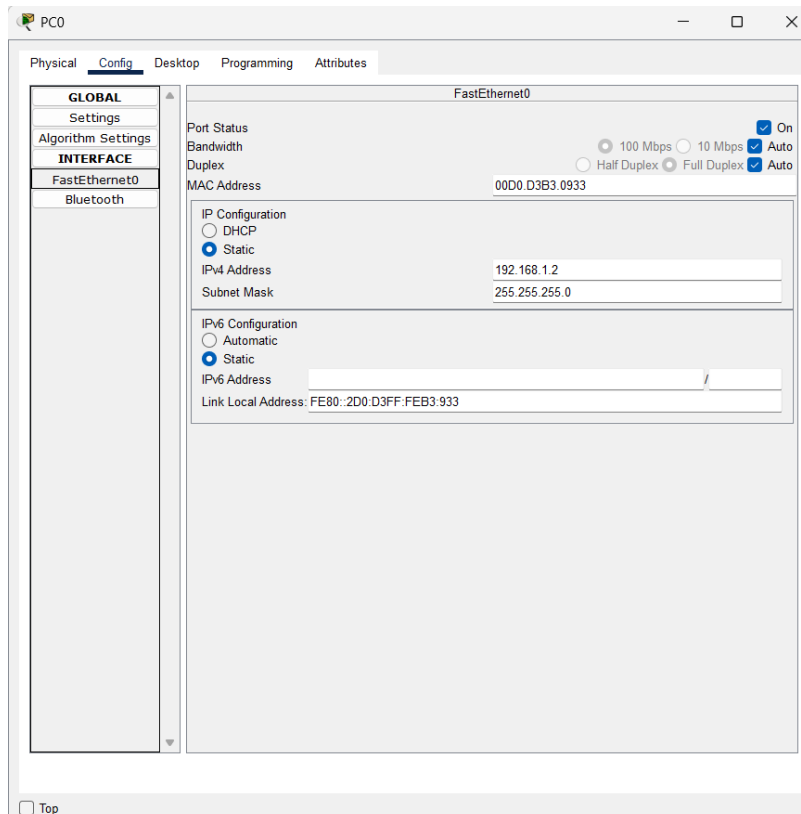
- It is not possible to modify the MAC address of a device. In real time if that has to be possible then the Network Interface card has to be changed. Only then MAC address of a device changes.
- Ifconfig command can be used in a Linux machine to identify the ipaddress of each interface and also some basic information about it like broadcast multicast status, MTU,amount of transmitted packets and received packets etc.
- Below is an example of checking connectivity using ping.

```
Laptop2                                              —  □  X

Physical   Config   Desktop   Programming   Attributes

Command Prompt                                              X

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time=12ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time=11ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 5ms

C:\>

□ Top
```
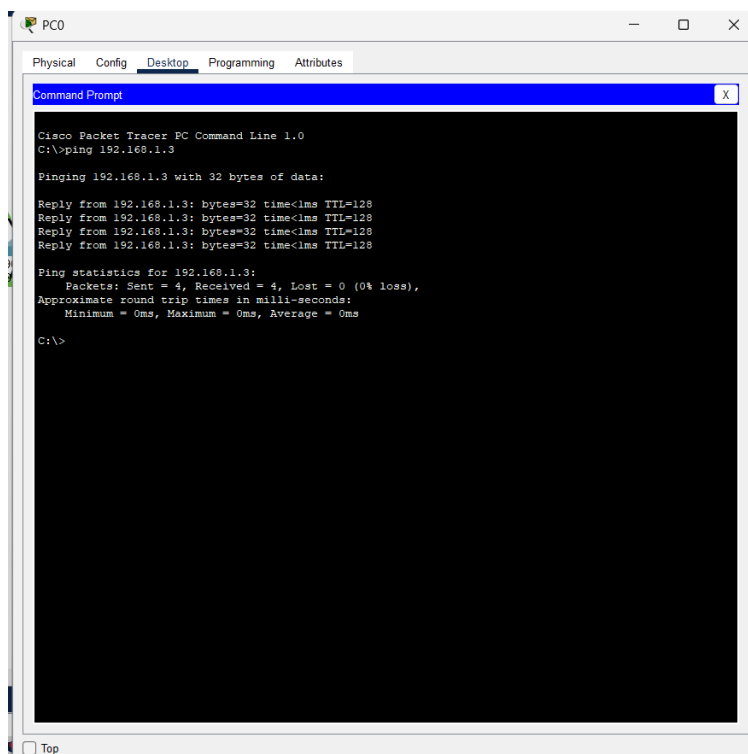
4.) Troubleshoot Ethernet Communication with ping and traceroute -> Using cisco packet tracer:

- Below is the network simulated in Cisco Packet Tracer.
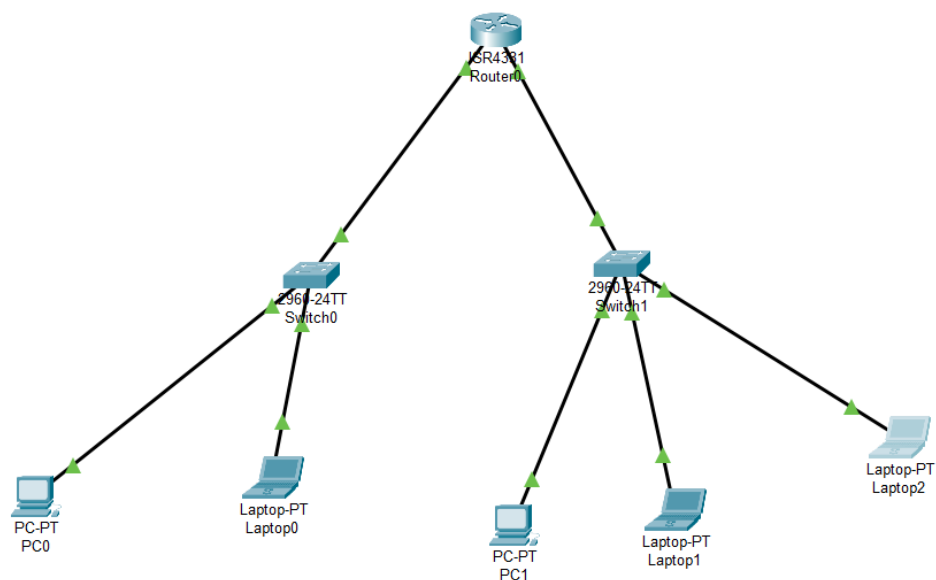
Now let me create a ping between PC0 and Laptop0

As you can see the ping is successful and therefore there is an active connection between PC0 which is 192.168.1.2 and Laptop0 which is 192.168.1.3

- Now the default gateway is configured to be the router link that is 192.168.1.1 similarly on the other side of the network 192.168.2.1.
- Let us try to traceroute from this network to that network.
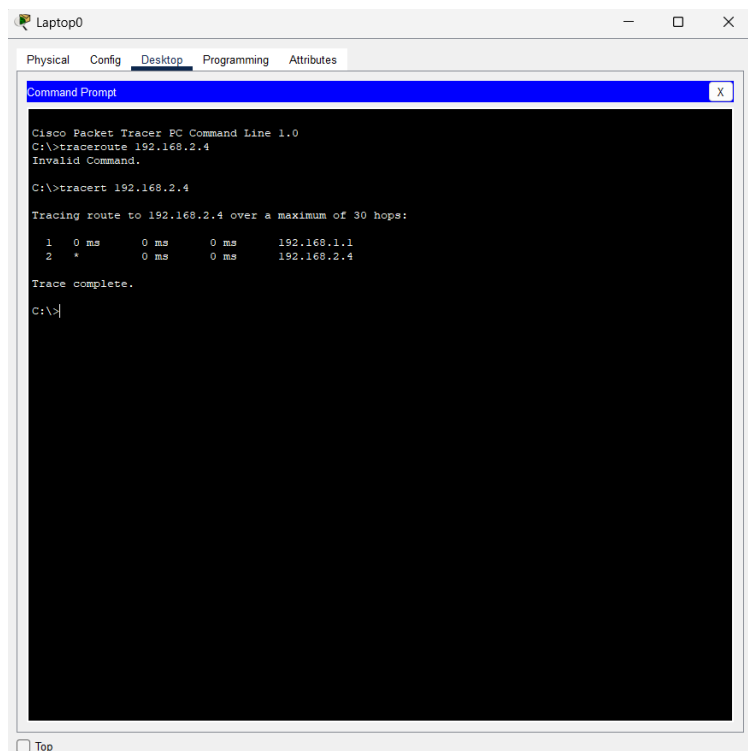
We used the command tracert to find the hops between the transimitter and receiver. As you can see, it takes only 2 hops to reach the receiver PC.

5.) Create a simple LAN setup with two Linux machines connected via a switch.
- Below is a simple example where 2 pcs are connected using a switch in Cisco Packet Tracer.
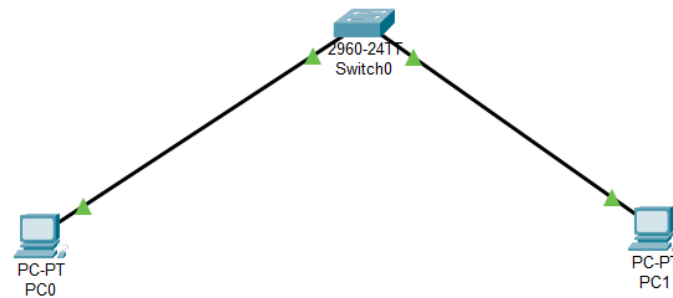
6.) Ping from one machine to the other. If it fails, use ifconfig to ensure the IP addresses are configured correctly.

In the same network configured in Question 5, the PC0 and PC1 were pinged and shown that it is connected.

If they were not connected, we could've used GNS3 and simulate the same using linux machines and there we can use ifconfig to debug the issues.
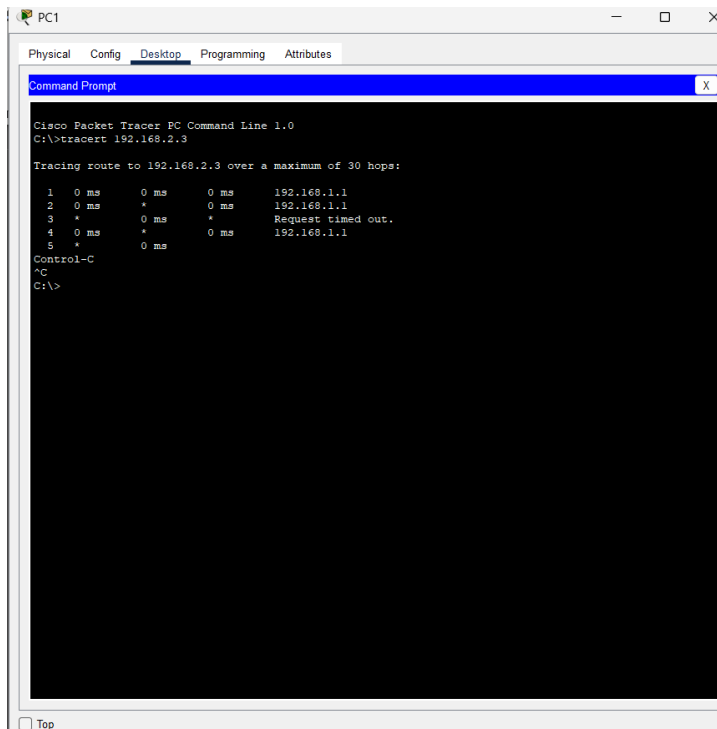
7.) Use traceroute to identify where the packets are being dropped if the ping fails.

- Below is the simulated network for the question.
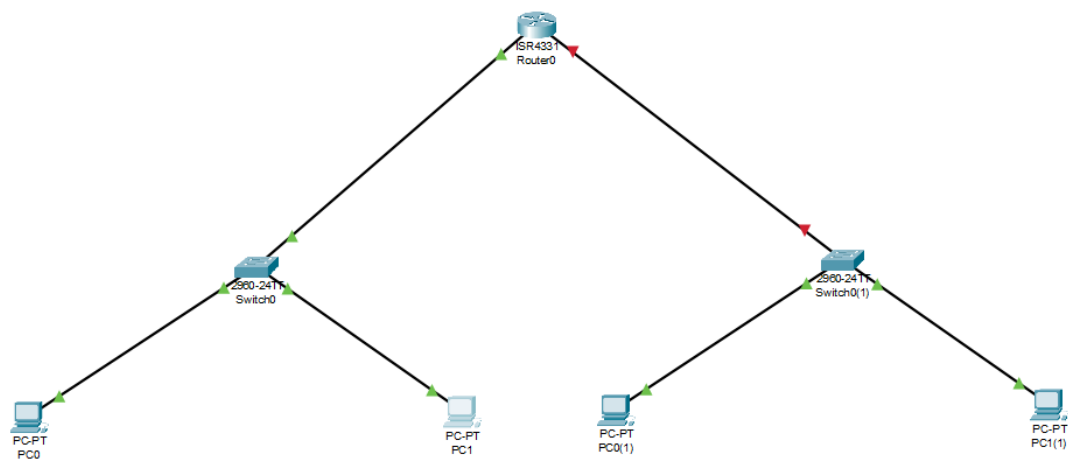
As you can see, a link in the router is switched off, and therefore there is no connectivity there which will be identified by the tracert command.

- We will ping from PC1 to PC1(1)

```
PC1                                                        –  □  ✕

Physical   Config   Desktop   Programming   Attributes

Command Prompt                                                   X

Cisco Packet Tracer PC Command Line 1.0
C:\>tracert 192.168.2.3

Tracing route to 192.168.2.3 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.1.1
  2    0 ms      *         0 ms      192.168.1.1
  3    *         0 ms      *         Request timed out.
  4    0 ms      *         0 ms      192.168.1.1
  5    *         0 ms
Control-C
^C
C:\>

□ Top
```

- From the output of the trace route command it is inferenced that the packets reach the default gateway(Router) 192.168.1.1 but then it doesn't know where to go, as the link is shut down.

8.) Research the Linux kernel's handling of Ethernet devices and network interfaces. Write a short report on how the Linux kernel supports Ethernet communication (referencing kernel.org documentation).

- Linux kernel handles the Ethernet Devices and network interfaces using drivers
- Each ethernet devices are referred to as network interfaces such as etho0, eth1..etc.

9.) Describe how you would configure a basic LAN interface using the ip command in Linux (kernel.org).

Using the ip command

- First you have to use ip link show, to see all the available interfaces, and then you can create or add a default gateway and routes to configure a basic LAN interface.

10.) Use Linux to view the MAC address table of a switch (if using a Linux-based network switch). Use the bridge or ip link commands to inspect the MAC table and demonstrate a basic switch's operation.

- In Cisco Packet Tracer You can inspect the MAC address using the command show mac address-table.
- In linux based switch you can use bridge fdb show command to inspect the MAC address of a table.