Ex.No: 1 Date :	**Study of Network Tool – Packet Tracer**
Registration Number:	99220041160
Name:	CHINTAPALLI PAVAN KUMAR
Section & Slot	S23 & Slot-1

Objectives:

To introduce, explore and get familiar with using Cisco Packet Tracer simulator program to implement the different lab exercises of the networking course.

Introduction:

Packet Tracer https:/www.netacad.com/courses/packet-tracer is a network design, simulation and modelling tool that allows you to develop your skill set in networking, cybersecurity, and the Internet of Things (IoT). It allows you to model complex systems without the need for dedicated equipment. Using Packet Tracer, you can create detailed projects by creating Network topologies or create a virtual environment of your existing network with this software

Requirements:

1. You must enroll in and go through the free course Introduction to Packet Tracer provided by Cisco Networking Academy (Netacad) through the following link: https://www.netacad.com/portal/web/self-enroll/m/course-262199

   This is a free course to help you understand and work with Packet Tracer. It is short and helpful one, so please make sure you get benefit from it.

2. You must download and install Cisco Packet Tracer version 7.3.1 (8.2.1 is the recent version) on your computer.
3. To start the Packet Tracer simulator, you will be asked to log in to your Cisco account (which you have created earlier) for verification. (else you may use guest login)

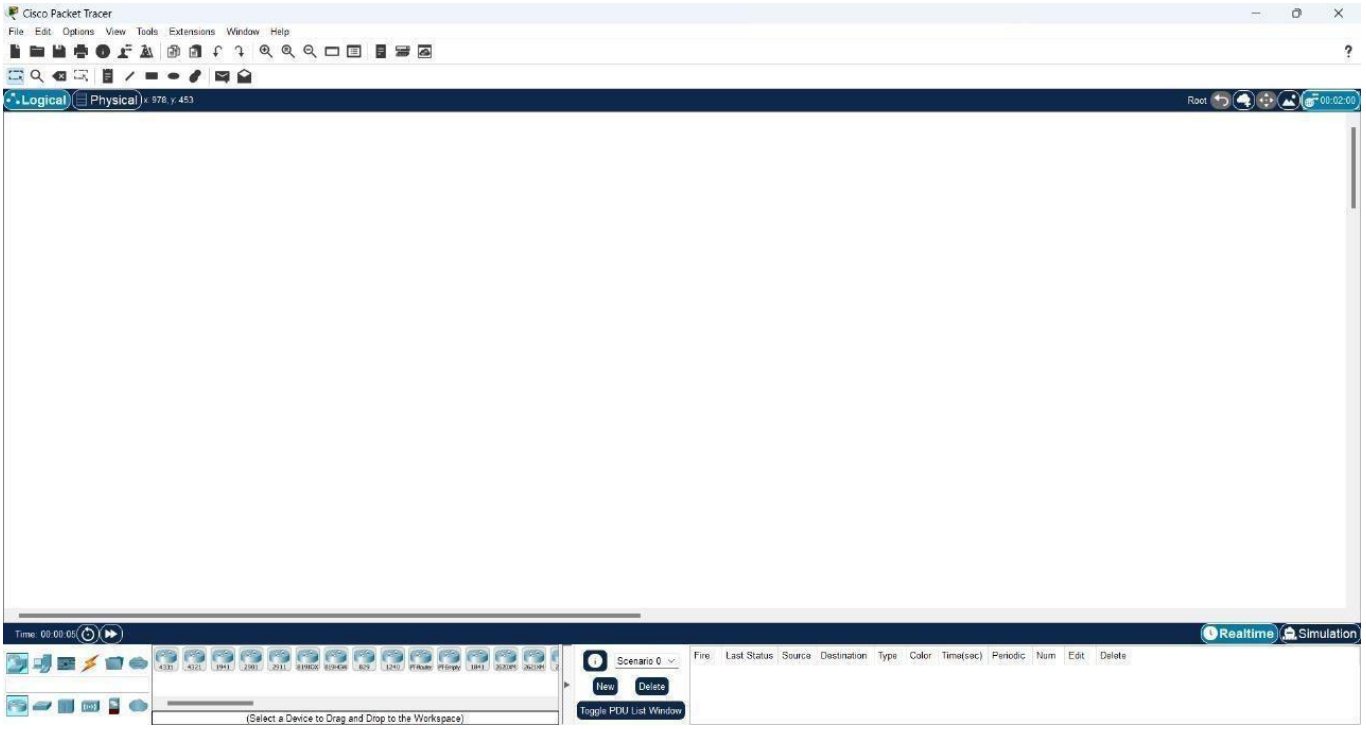
In this Lab:

1- You will download and install Packet Tracer version 8.2.1

2- You will explore the Packet Tracer User Interface and functions.

3- You will create a simple network topology Interface overview

INTERFACE OVERVIEW:



The components of the Packet Tracer interface are as follows:

Area 1: Menu bar – This is a common menu found in all software applications; it is used to open, save, print, change preferences, and so on.

Area 2: Main toolbar – This bar provides shortcut icons to menu options that are commonly accessed, such as open, save, zoom, undo, and redo, and on the right-hand side is an icon for entering network information for the current network.

Area 3: Logical/Physical workspace tabs – These tabs allow you to toggle betweenthe **Logical** and **Physical** work areas.

Area 4: Workspace – This is the area where topologies are created and simulations are displayed.

Area 5: Common tools bar – This toolbar provides controls for manipulating topologies, such as select, move layout, place note, delete, inspect, resize shape, and add simple/complex PDU.

Area 6: Realtime/Simulation tabs – These tabs are used to toggle between the real and simulation modes. Buttons are also provided to control the time, and to capture the packets.

Area 7: Network component box – This component contains all of the network and end devices available with Packet Tracer, and is further divided into two areas:

Area 7a: Device-type selection box – This area contains device categories

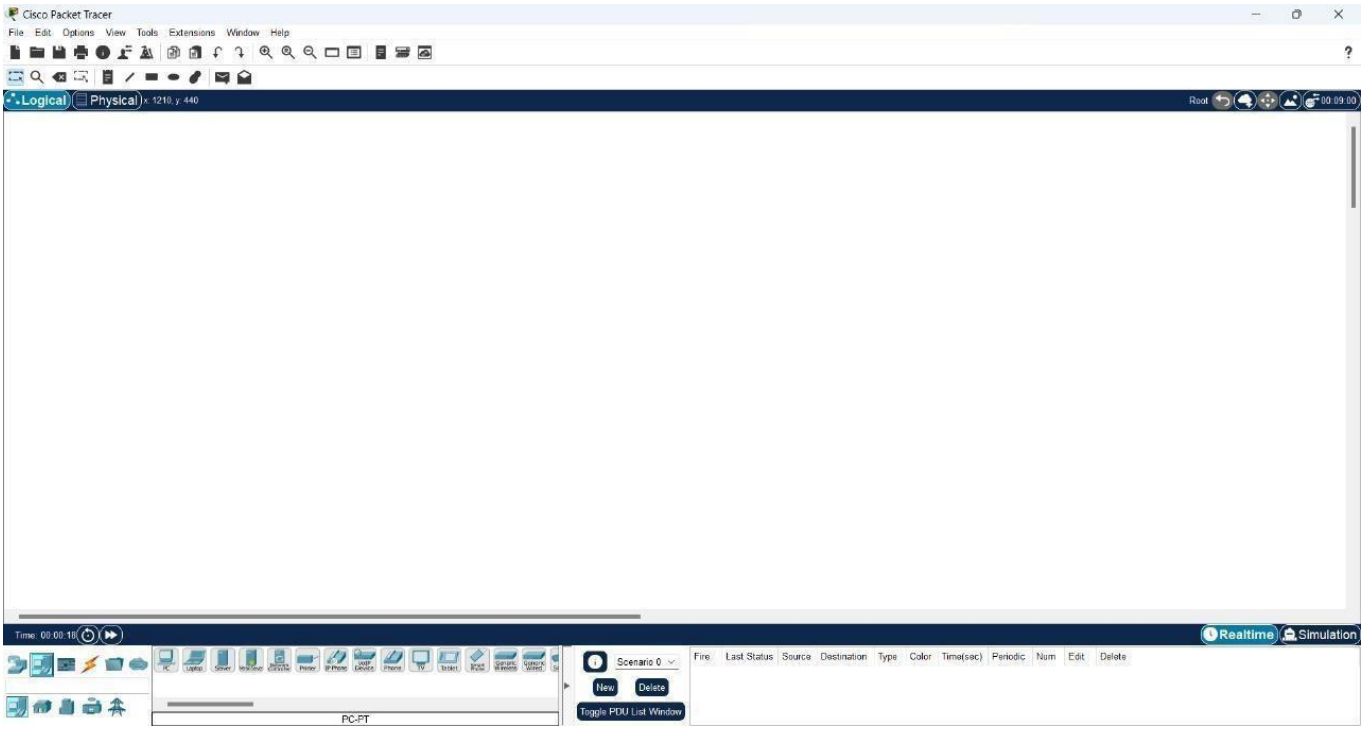
Area 7b: Device-specific selection box – When a device category is selected, this selection boxdisplays the different device models within that category

Area 8: User-created packet box – Users can create highly-customized packets to test their topologyfrom this area, and the results are displayed as a list.

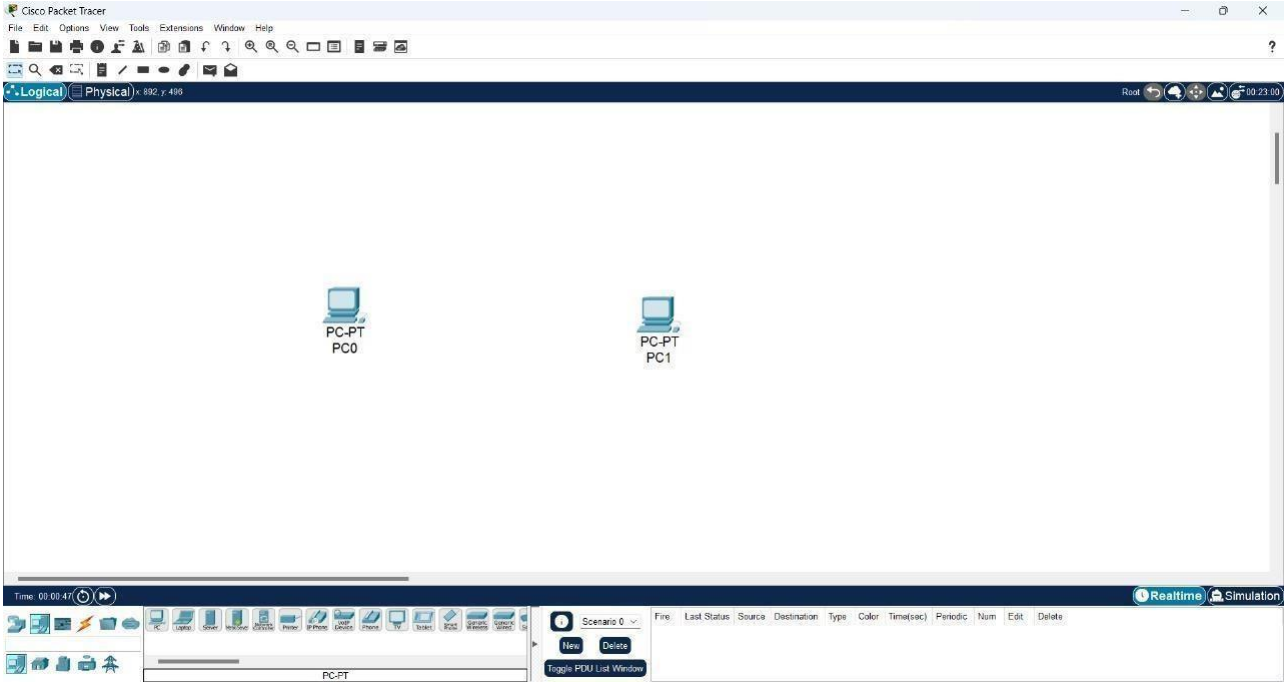
Make sure you are familiar with these names, because moving forward we will be referring to them frequently.

Creating a simple topology

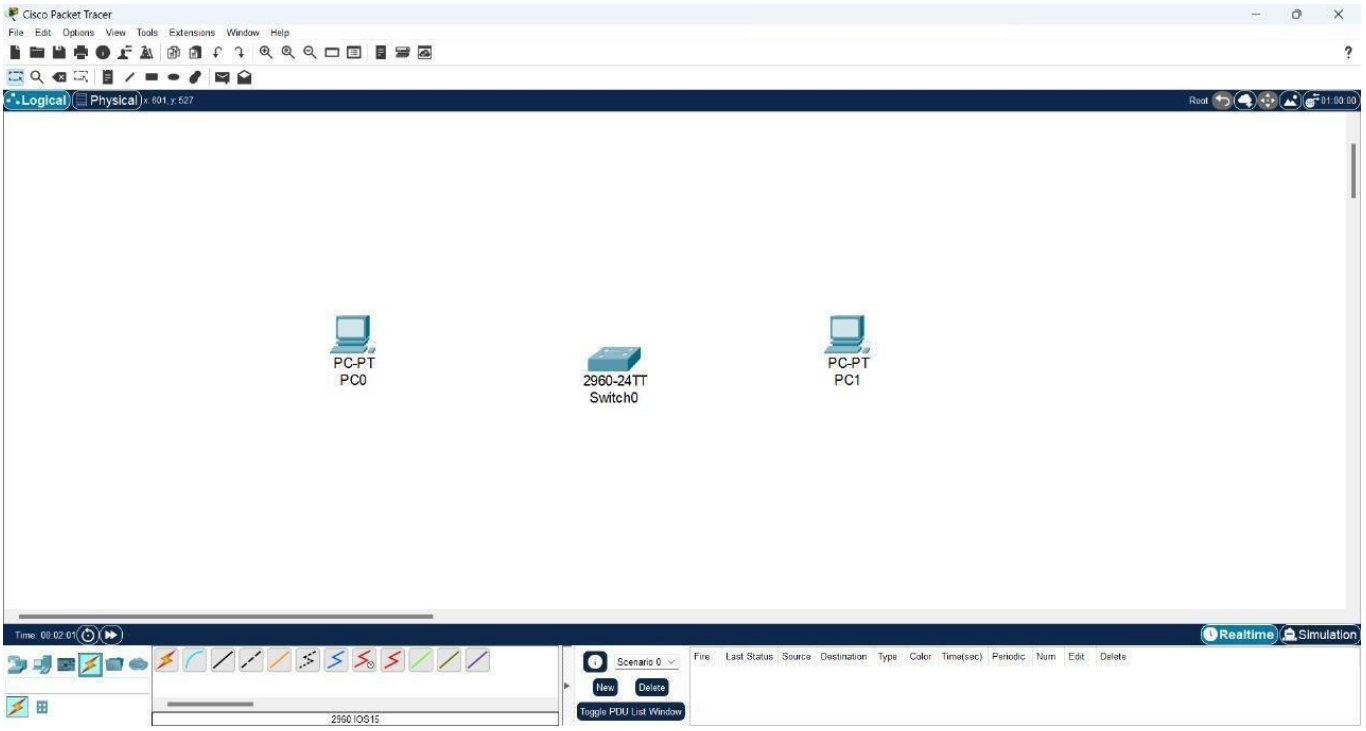
1. Open the *cisco packet tracer* application
2. Simple Network Installation Preparation in this example is to use 2 workstations (PCs) and 1 switch. Each node is connected to the cable.



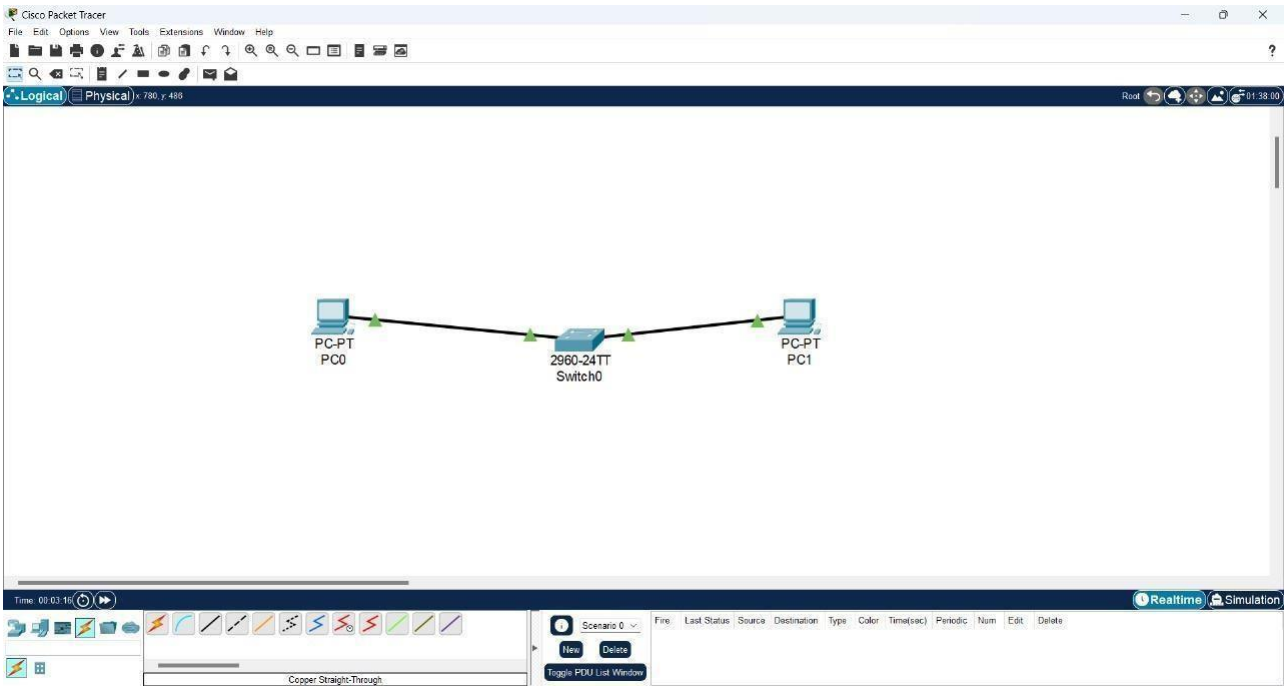
3. Select the icon of the PC that sits in the left corner and then put on display
4. Place the 2 pieces on the PC display



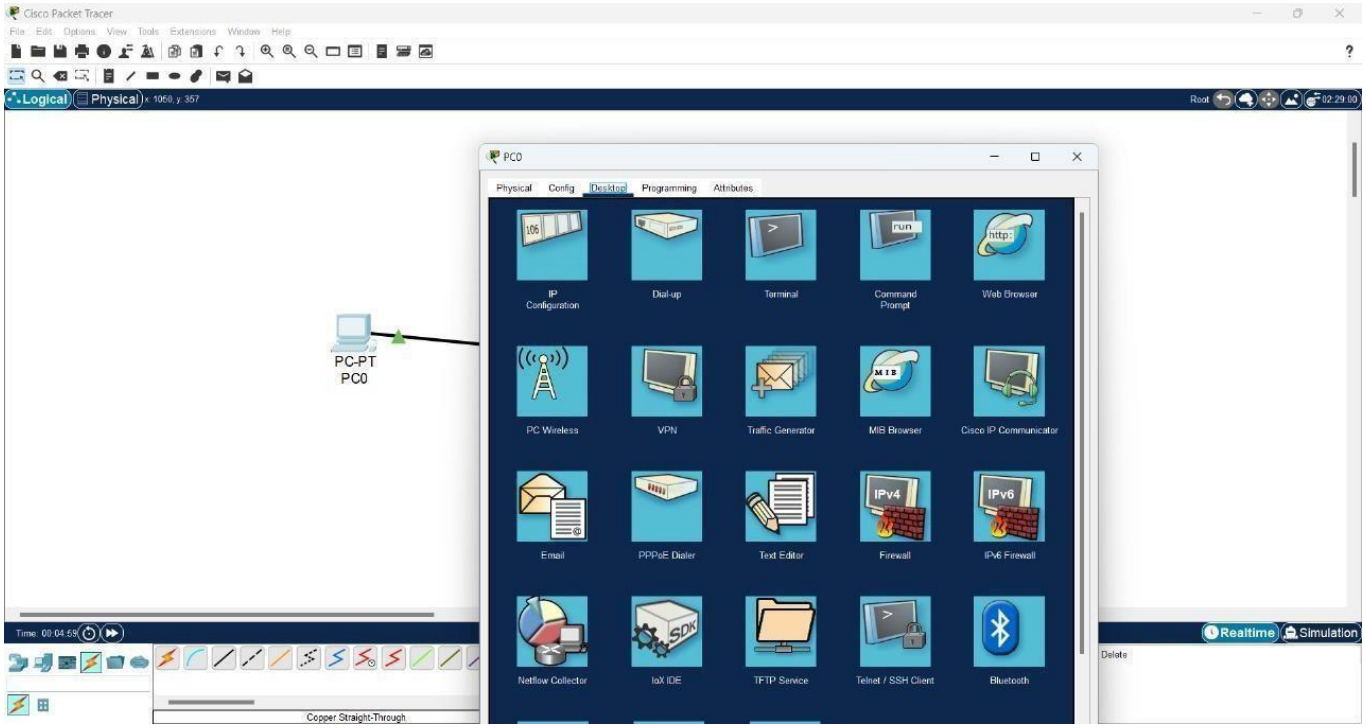
5. Next select switch and put on display

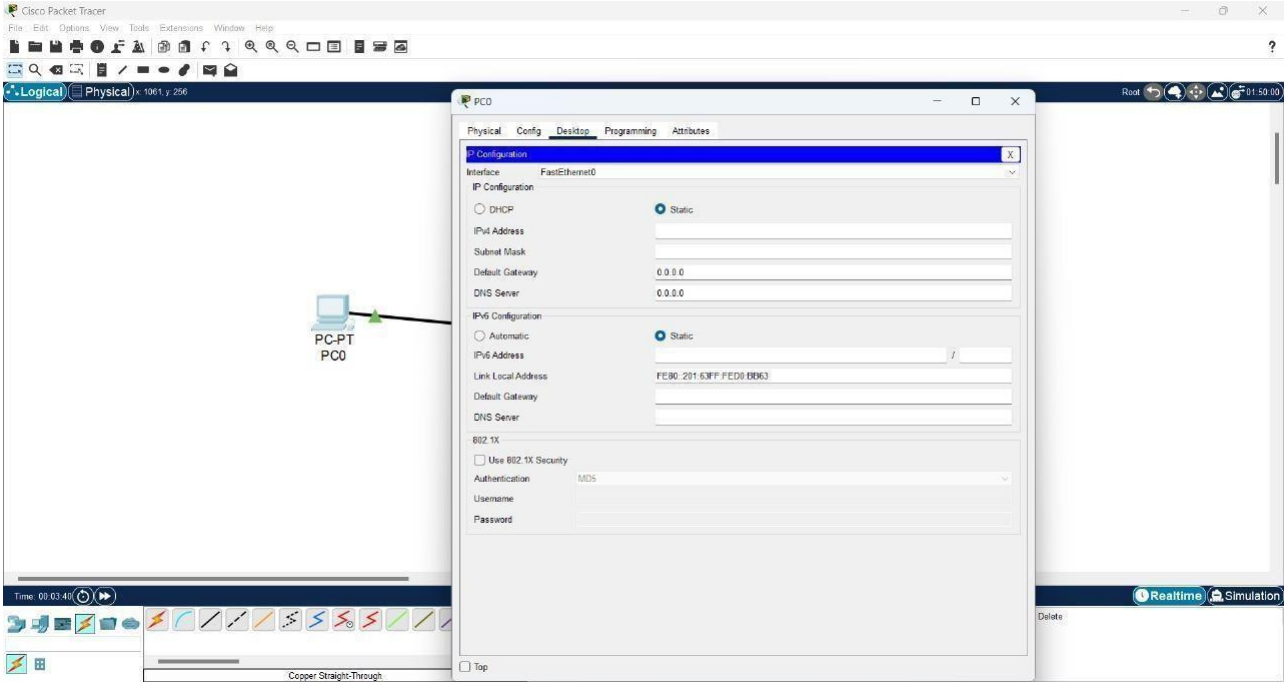


6. The process of wiring to connect 2 PC, select the straight cable, create an image such as this, when the wires yet is green then the PC yet connect

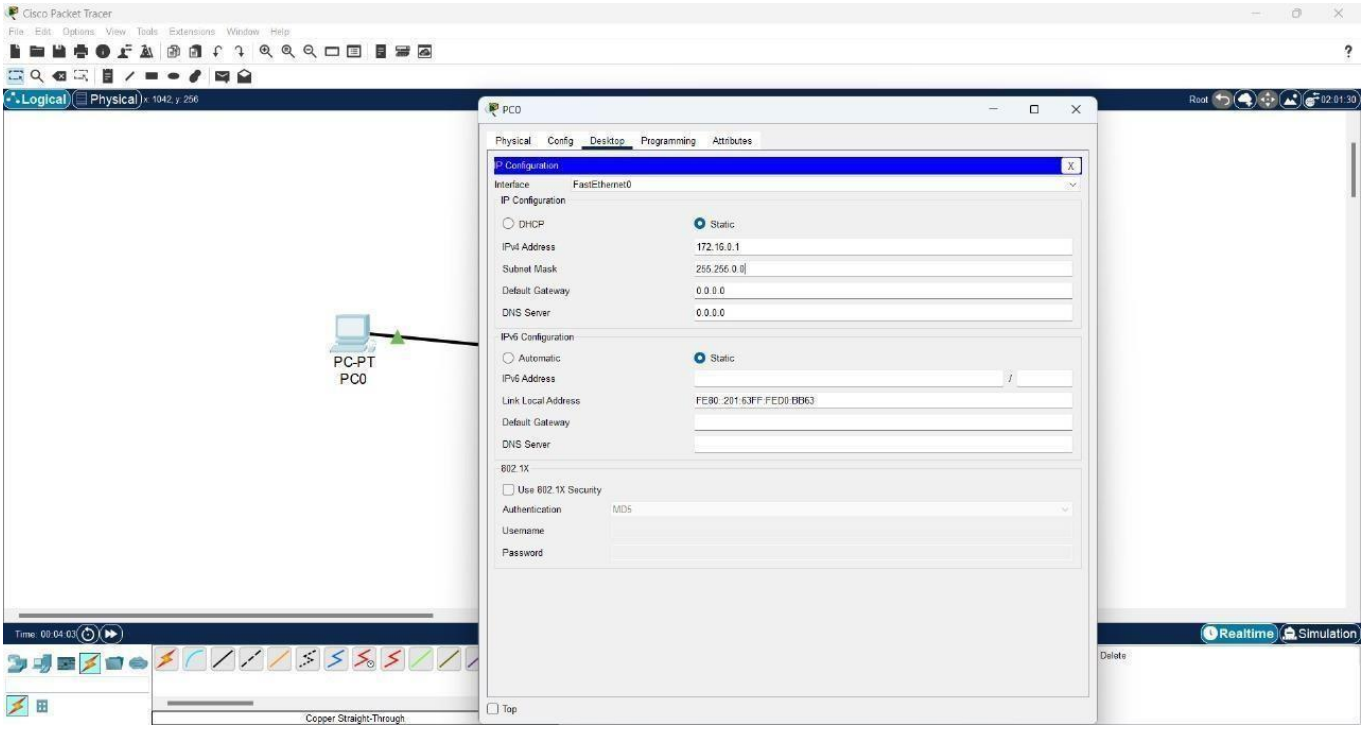


7. And then do the configuration IP address host **PC0** by means of double-click image **PC0**, then click the tab of the Desktop and choose menu section the IP Configuration so that the display is visible on the picture below This

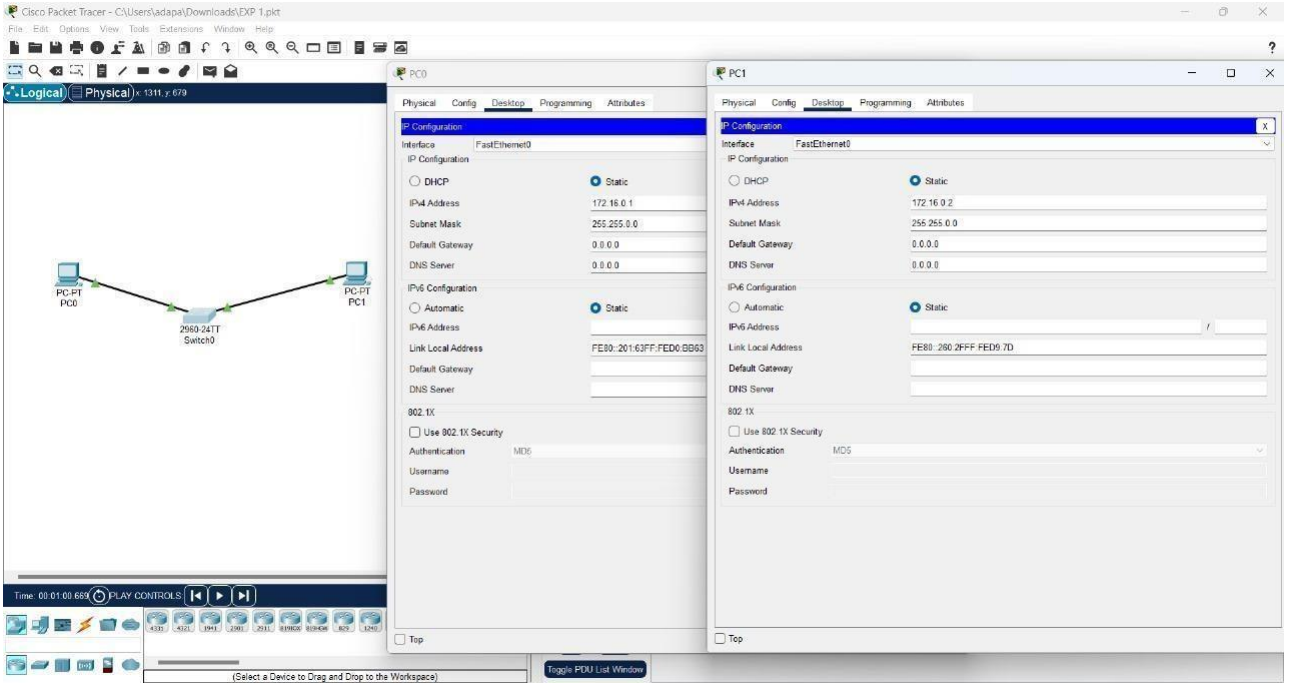




8. Add the IP Address **172.16.0.1** and Subnetmask will come out automatically

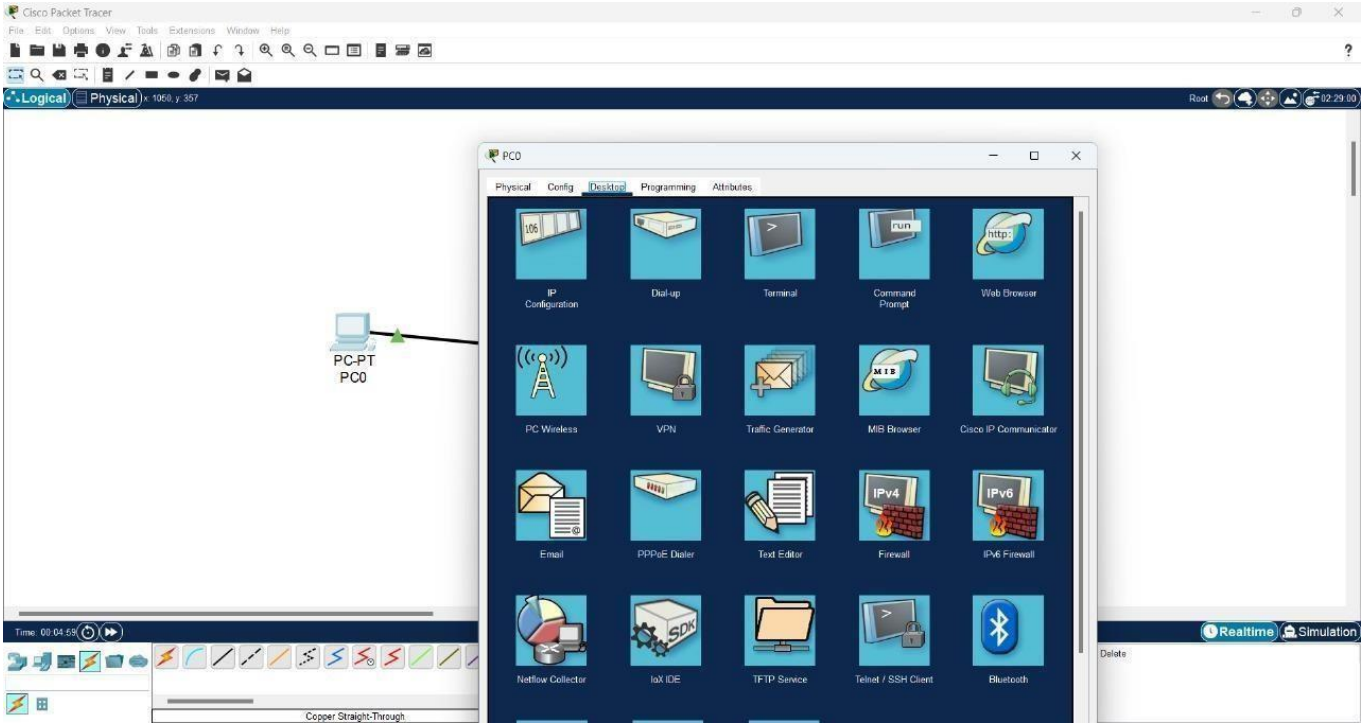


9. Do the same on the workstation configuration is as follows: each PC with a different ip address

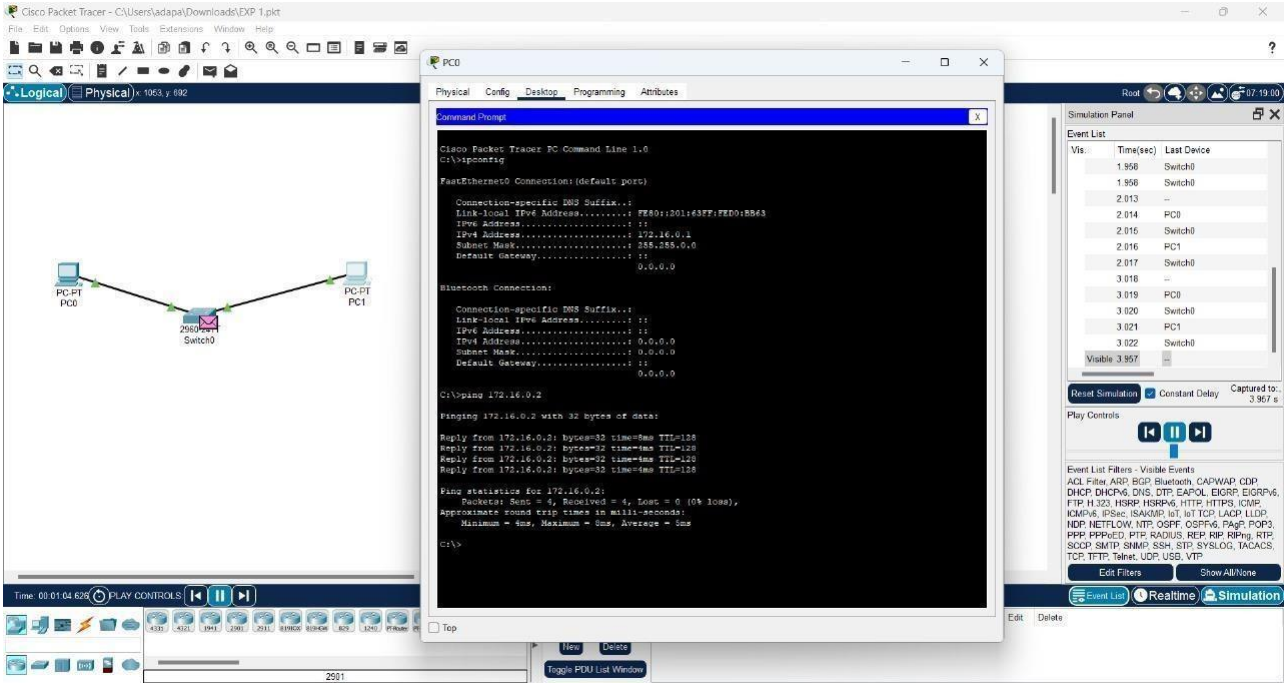


PING

10. To test the connection between the two nodes using the "ping" utility. To start the ping from **PC0 PC1** headed, double-click the **PC0** making it appear properties window for **PC0**, then select the tab of the **Desktop**, then select the **menu Command Prompt** so that it appears look like Figure below.



11. **.**Do a "ping" by way of typing: ping [ip_address_target] to do ping towards **PC1** which has IP address 172.16.0.2 is by way of type in: **ping 172.16.0.2 .** If the configuration you do is correct then the produced output like this:



CONCLUSION

From the results of experiments conducted, it can be concluded that:

1. The new **PC0** and **PC1** workstations can be connected if both workstation IP addresses have been well configured and correct.
2. To test connectivity between nodes can use the "ping" command

Rubrics for Experiment Assessment:

Rubrics	Good	Normal	Poor	Marks
Creation of Topology (4)	Created the topology, Identify the proper devices and making the connections **(4)**	Created the topology, Identify the proper devices, making the connectionsBut missing some features **(3)**	Created wrong topology, Failed to Identify the proper devices and making connections **(1)**	
Verify the connectivity (4)	Verified the connectivity in all the levels **(4)**	Verified the connectivity at some levels (only some nodes) **(2)**	Verified the connectivity is not done. **(1)**	
Timely Completion (2)	Completed the lab before the allotted time **(2)**	Completed the lab after the deadline **(1)**	Did not submitted before grading **(0)**	
			Total	

Ex.No: 02	Study of Network Devices
Date :	
Registration Number:	99220041065
Name:	DESU SIVA NAGA SATYA SAI
Section & Slot:	S12 & Slot-03

Objective(s):

To understand working principle of network devices Hub, Switch, Routers and configure the following using Cisco Packet Tracer

a) Building a Peer-to-Peer Network.

Design a Peer-to-peer network with minimum of 3 PC's and verify the connectivity from both the ends using Packet Tracer.

b). Design a Simple LAN Network

Create a Simple LAN deign with 1 switch, 4 PC's, 2 laptops and verify the connections from all the ends using Packet Tracer.

Introduction:

Study of following Network Devices in Detail

- Repeater
- Hub
- Switch
- Bridge
- Router
- Gate Way

Theoretical Background:

To know more about the above network devices, Refer textbook for detailed explanation.

a) Building a Peer-to-Peer Network with at least three hosts

Objective(s):

Design a Peer-to-peer network with minimum of 3 PC's and verify the connectivity from both the ends using Packet Tracer.

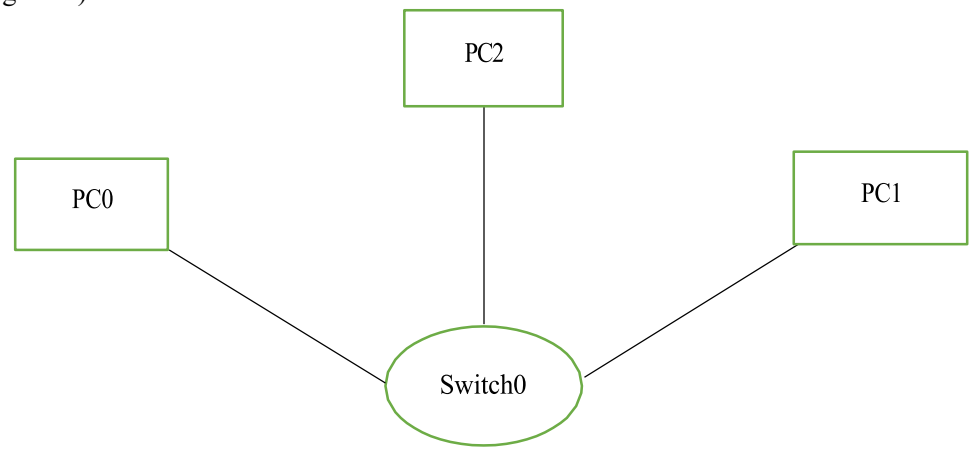
Theoretical Background:

In Peer-to-Peer architecture every node is connected to other node directly for exchanging information instead of connected to central server Every computer node is referred as peer and they do the job of client as well as server both. Every peer provides services to other peers as well as uses services provided by other peers.

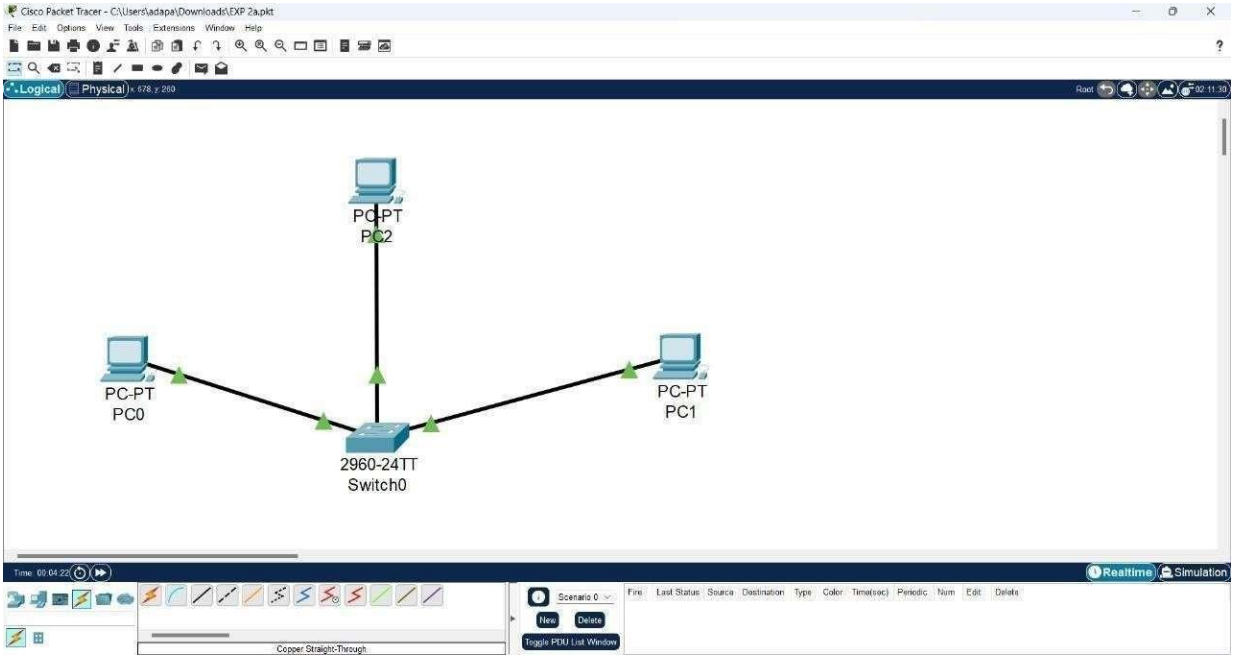
1. Device Requirements:

1. PC0
2. PC1
3. PC2
4. Switch0
5. Copper Straight-Through

2. Network Diagram for your experiment (draw the diagram either hand drawing/ms paint or any other drawing tools)



3. Network Diagram (packet tracer diagram before configuration):



4. Configuration details:

Device Name	Interface Name	IP Address	Subnet mask
PC0	Fa0	172.16.0.1	255.255.0.0
PC1	Fa0	172.16.0.2	255.255.0.0
PC2	Fa0	172.16.0.3	255.255.0.0
Switch0	Fa0		

5. Commands used in each of the diagram (if any):

    1. ipconfig
    2. ping <Ip_address>

6. Output Diagram (Minimum 3 screenshot):

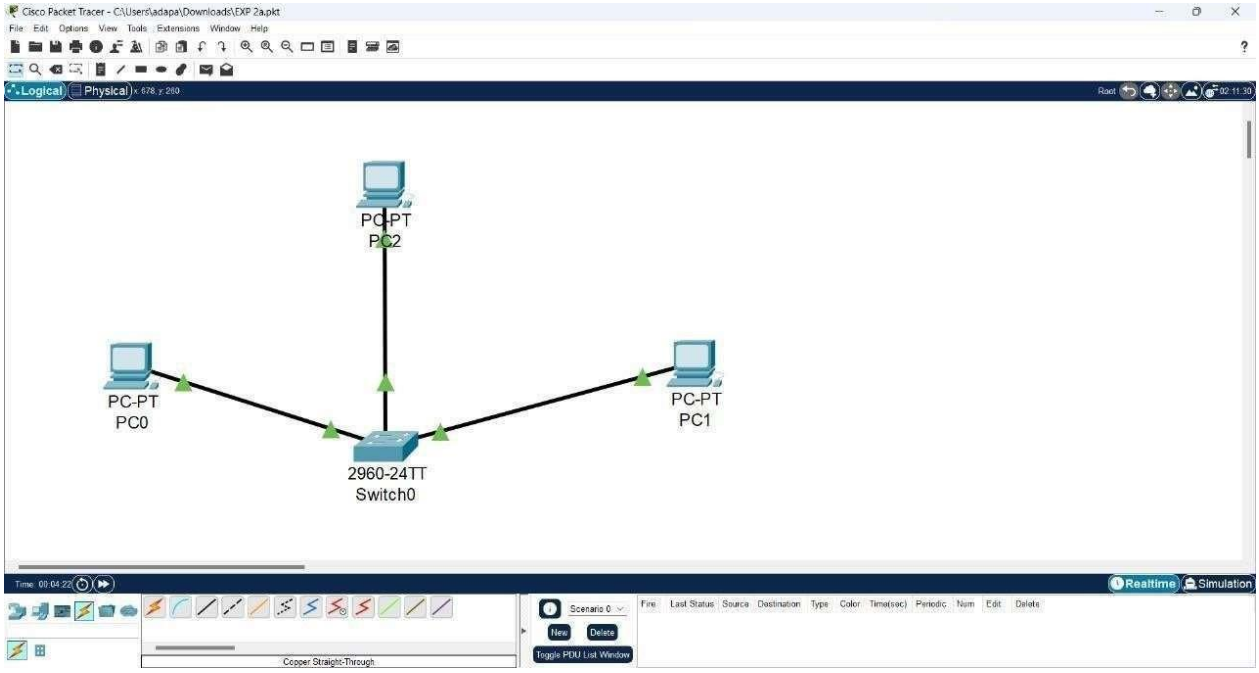
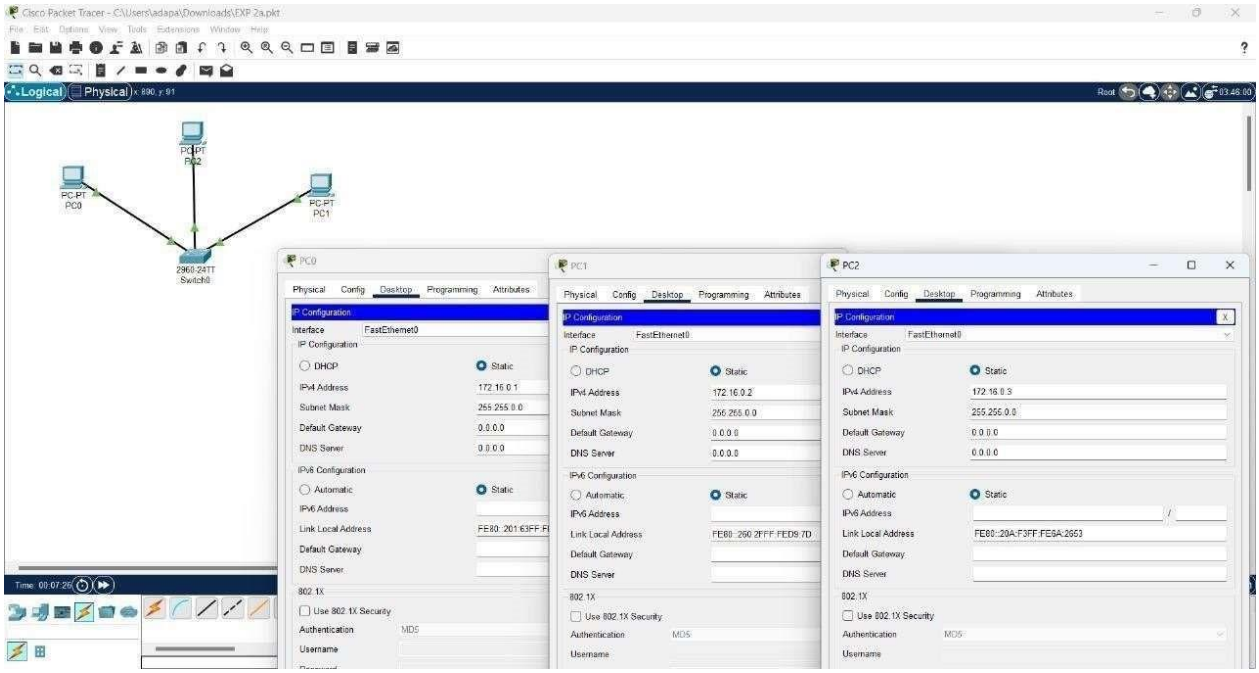


FIG: Network Diagram



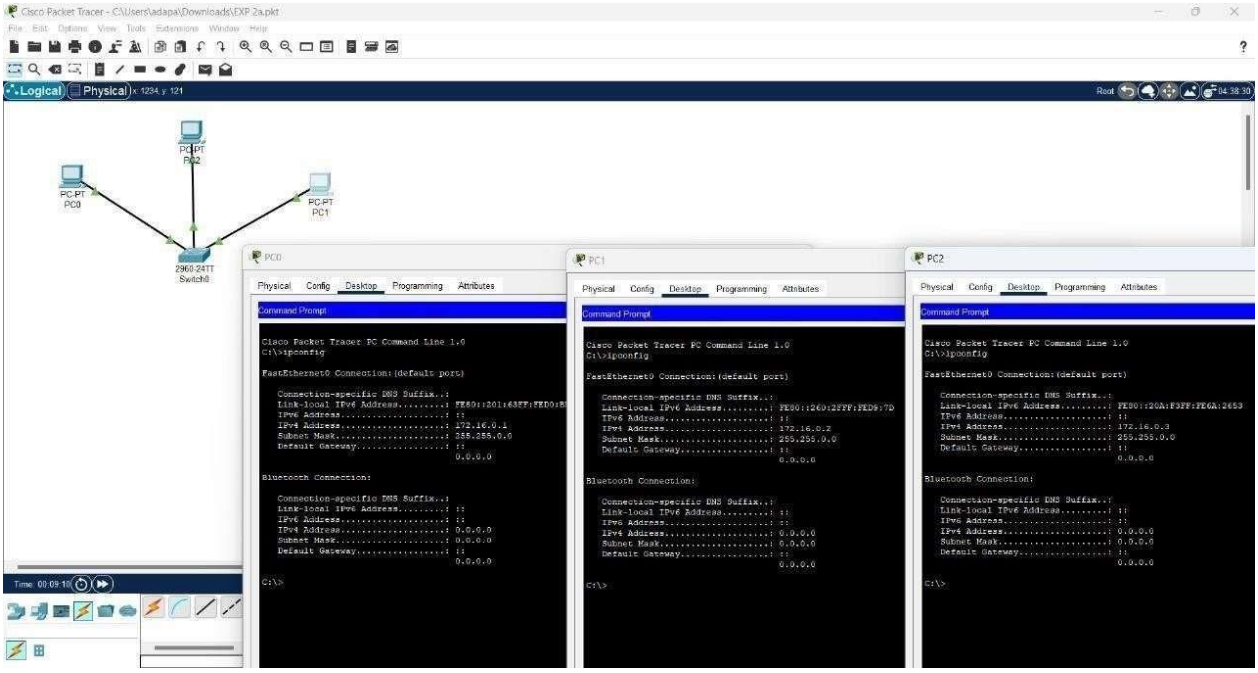


FIG: ASSIGNING IP ADDRESS

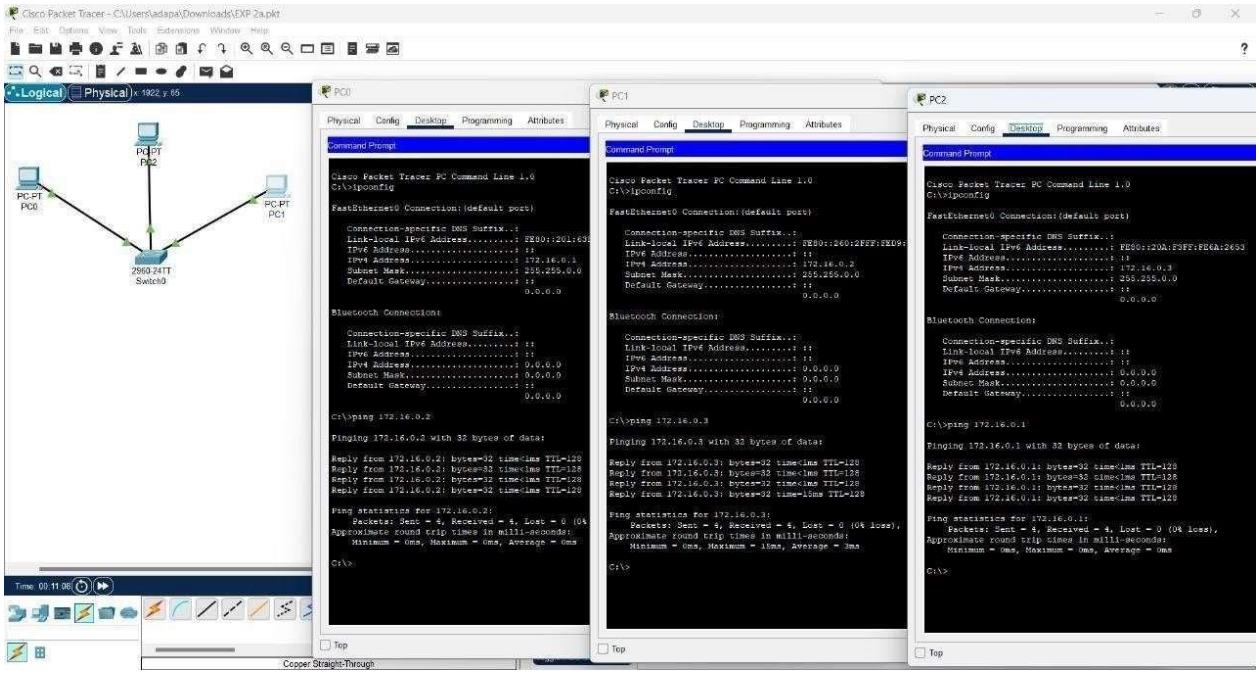
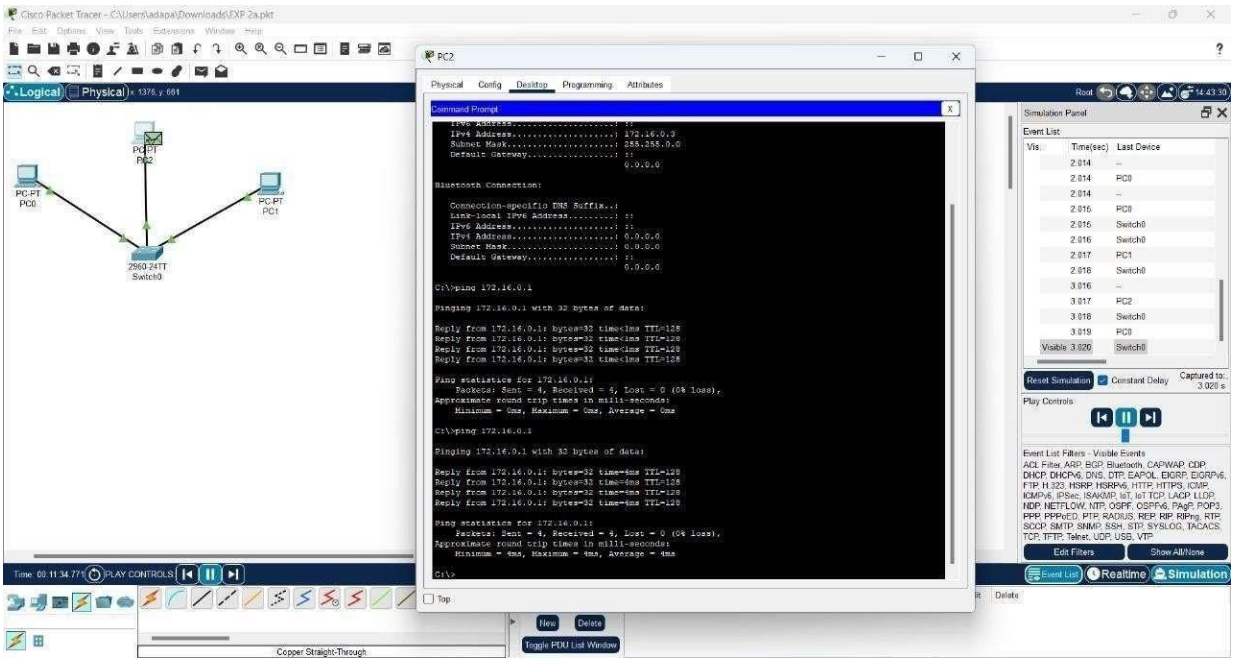


FIG: PING



CONCLUSION (provide conclusion about this experiment):

Successfully designed a Peer-to-peer network with 3 PC's and verified the connectivity from both the ends using Packet Tracer.

Rubrics for Experiment Assessment:

Rubrics	Good	Normal	Poor	Marks
Creation of Topology (4)	Created the topology, Identify the proper devices and making the connections (4)	Created the topology, Identify the proper devices, making the connections But missing some features (3)	Created wrong topology, Failed to Identify the proper devices and making connections (1)	
Verify the connectivity (4)	Verified the connectivity in all the levels (4)	Verified the connectivity at some levels (only some nodes) (2)	Verified the connectivity is not done. (1)	
Timely Completion (2)	Completed the lab before the allotted time (2)	Completed the lab after the deadline (1)	Did not submitted before grading (0)	
			Total	

b). Design a Simple LAN Network.

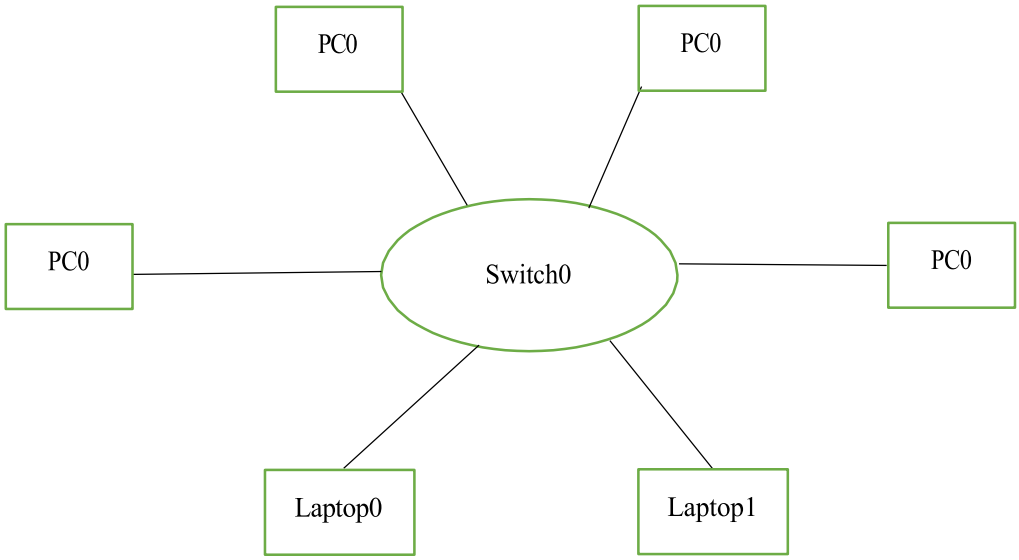
Objective(s):

Create a Simple LAN design with minimum of 1 switch, 4 PC's, 2 laptops and verify the connections from all the ends using Packet Tracer.

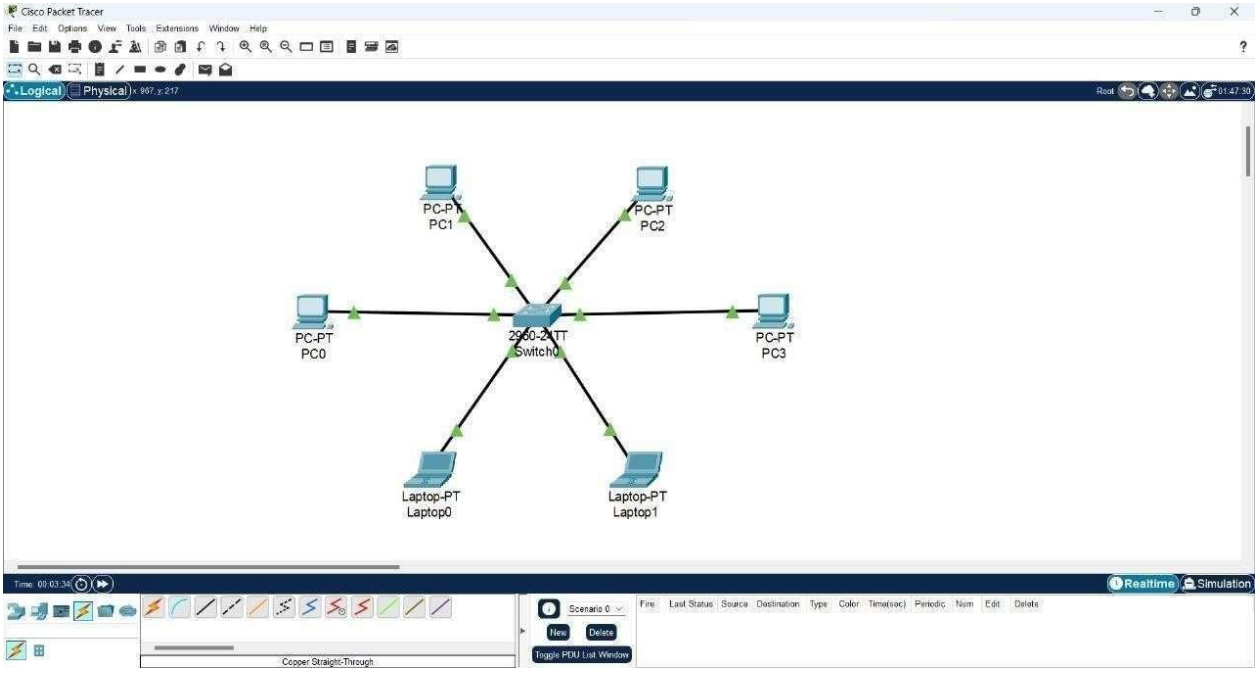
1. Device Requirements:

    1. PC-0
    2. PC-1
    3. PC-2
    4. PC-3
    5. Laptop0
    6. Laptop1
    7. Switch0
    8. Copper Straight-Through

2. Network Diagram for your experiment (draw the diagram either hand drawing/mspaint or any other drawing tools)



3. Network Diagram (packet tracer diagram before configuration):



4. Configuration details:

Device Name	Interface Name	IP Address	Subnet mask
PC0	Fa0	172.16.0.1	255.255.0.0
PC1	Fa0	172.16.0.2	255.255.0.0
PC2	Fa0	172.16.0.3	255.255.0.0
PC3	Fa0	172.16.0.4	255.255.0.0
Laptop0	Fa0	172.16.0.5	255.255.0.0
Laptop1	Fa0	172.16.0.6	255.255.0.0
Switch0	Fa0		

5. Commands used in each of the diagram (if any):

    1. ipconfig
    2. ping <ip_address>

6. Output Diagram (Minimum 3 screenshot):

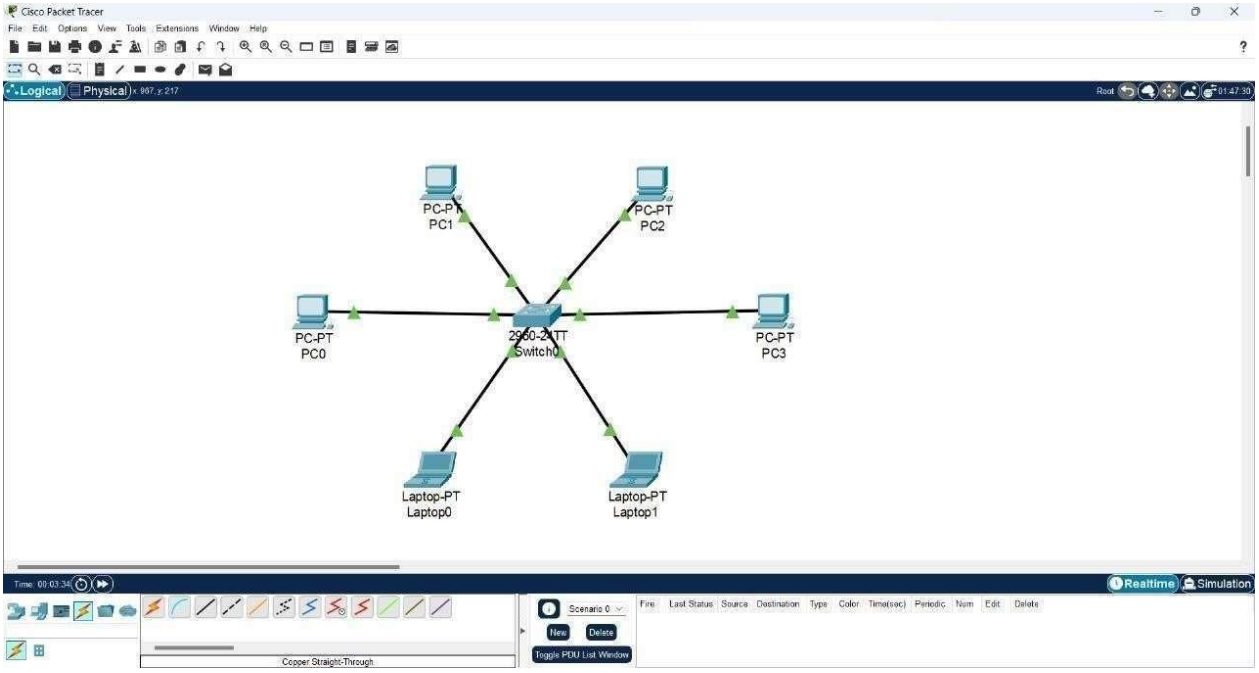
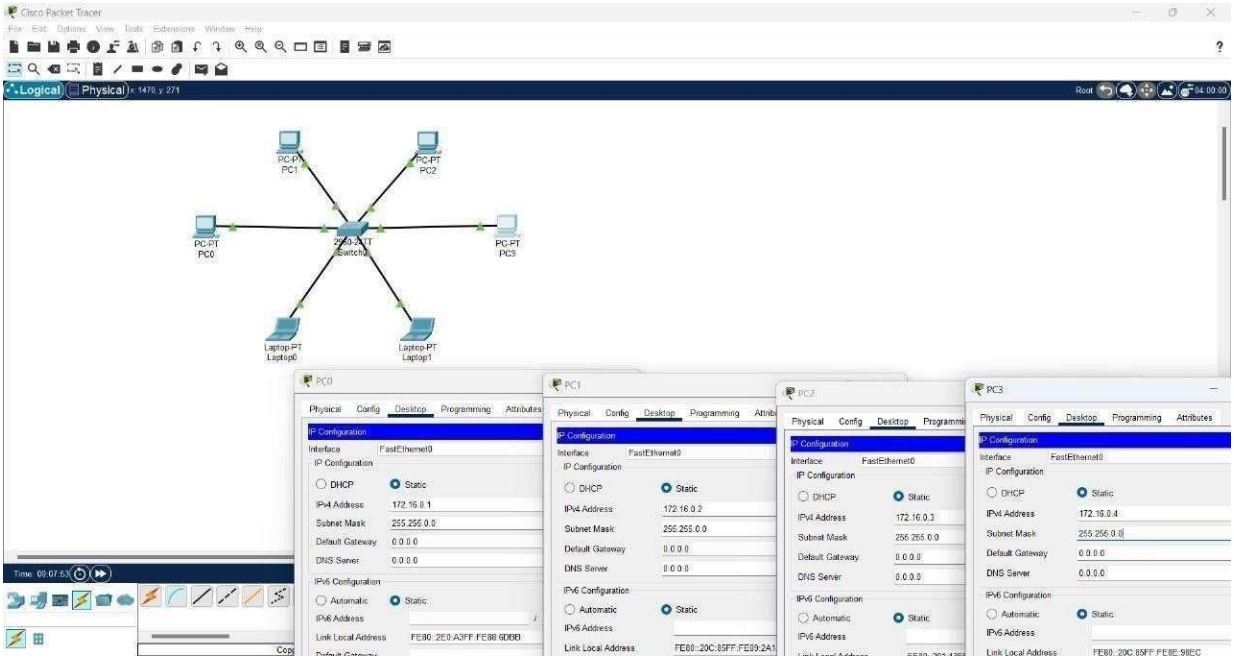


FIG: NETWORK DIAGRAM



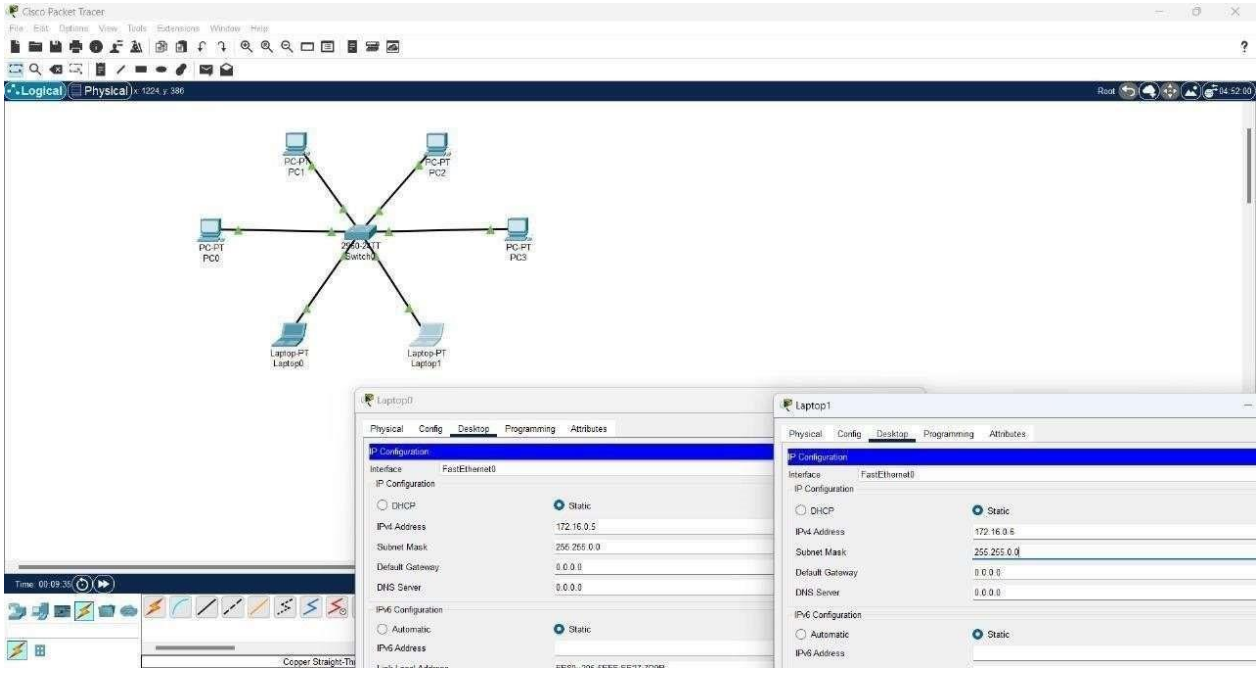


FIG: ASSIGNING IP ADDRESS

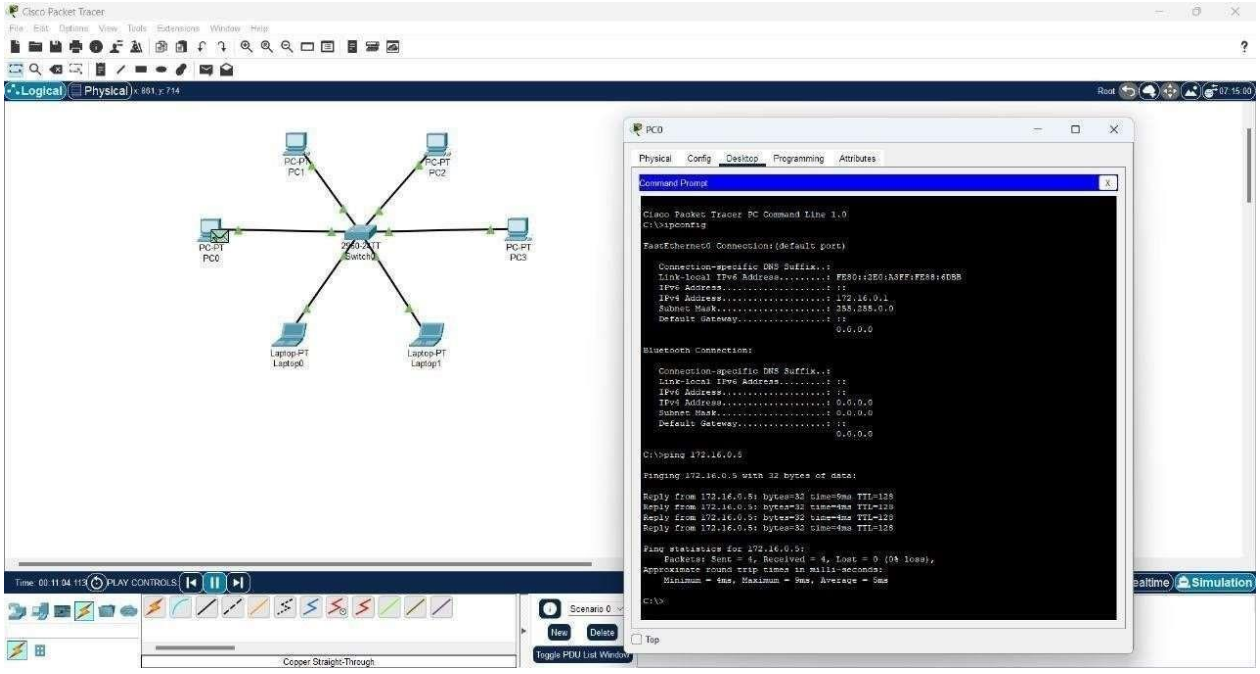
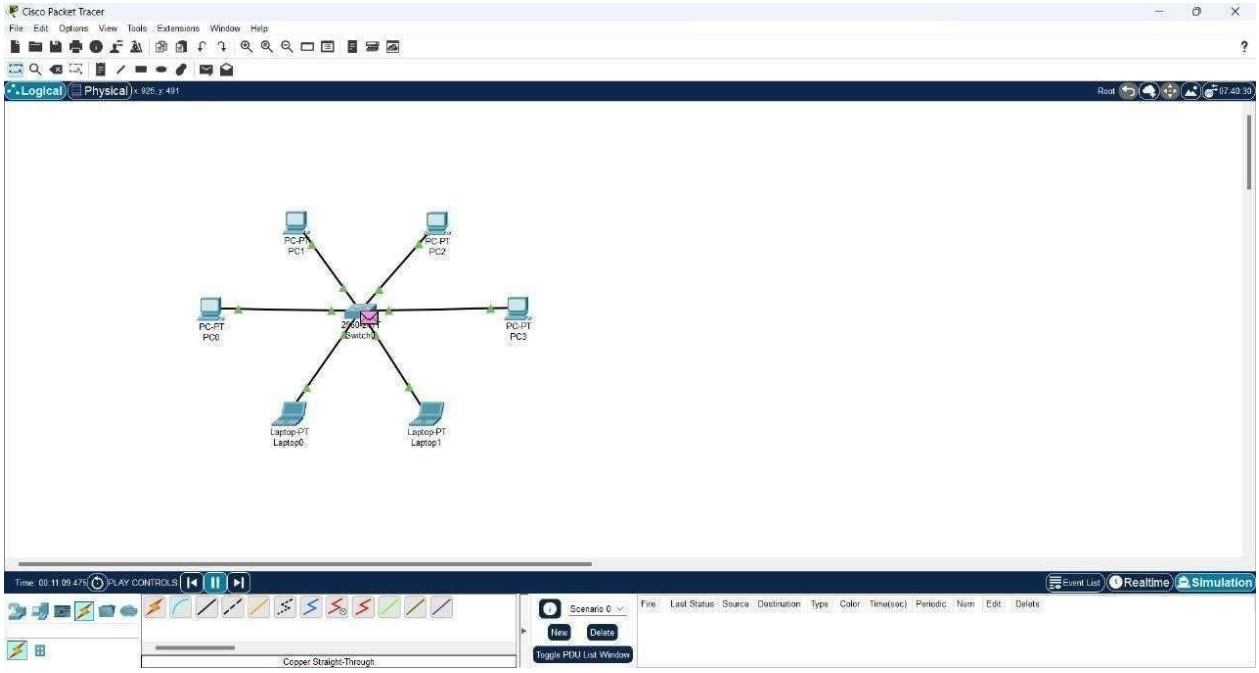


FIG: PING



CONCLUSION (provide conclusion about this experiment):

Successfully created a Simple LAN design with 1 switch, 4 PC's, 2 laptops and verified the connections from all the ends using Packet Tracer.

Rubrics for Experiment Assessment:

Rubrics	Good	Normal	Poor	Marks
Creation of Topology (4)	Created the topology, Identify the proper devices and making the connections (4)	Created the topology, Identify the proper devices, making the connections But missing some features (3)	Created wrong topology, Failed to Identify the proper devices and making connections (1)	
Verify the connectivity (4)	Verified the connectivity in all the levels (4)	Verified the connectivity at some levels (only some nodes) (2)	Verified the connectivity is not done. (1)	
Timely Completion (2)	Completed the lab before the allotted time (2)	Completed the lab after the deadline (1)	Did not submitted before grading (0)	
			Total	

Ex.No: 03	Study of Guided Media
Date :	
Registration Number:	99220041066
Name:	EMANI RAM MOHAN REDDY
Section & Slot:	S12 & Slot-03

Objective(s):
To Study of different types of Network cables and practically implement the Crossover wired and Straight through cable using Crimping Tool.

Components Required:
- CAT5, CAT6 Cable
- RJ45 Crimpable Connector
- Crimping tools
- Splicer

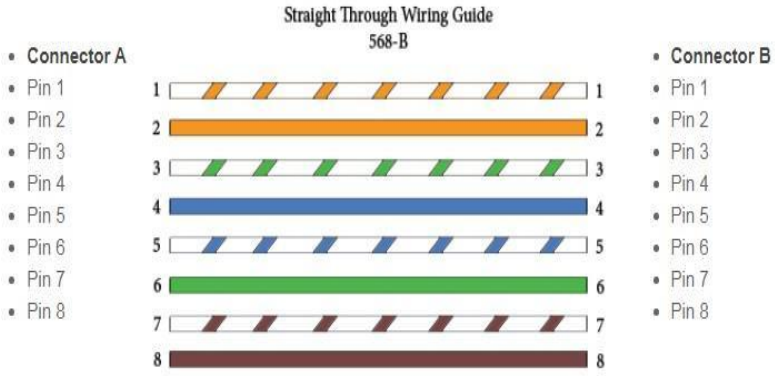
Description:
The Ethernet cables for connectivity in most office and home environments rely on twisted wire pairs within an overall cable - Cat 5, Cat 6 and Cat 7 all used this format.

Straight-Through Wired Cables

Straight-Through refers to cables that have the pin assignments on each end of the cable. In other words, Pin 1 connector A goes to Pin 1 on connector B, Pin 2 to Pin 2, etc. Straight-Through wired cables are most commonly used to connect a host to a client. When we talk about cat5e patch cables, the Straight-Through wired cat5e patch cable is used to connect computers, printers, and other network client devices to the router switch or hub (the host device in this instance).

Use straight-through cables for the following connections:

- Switch to a router Ethernet port
- Computer to switch
- Computer to hub



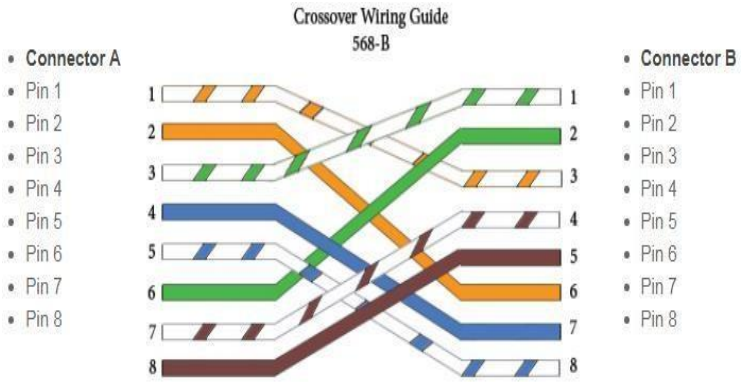
Crossover Wired Cables

Crossover wired cables (commonly called crossover cables) are very much like Straight-Through cables with the exception that TX and RX lines are crossed (they are at opposite positions on either end of the cable). Using the 568-B standard as an example below, you will see that Pin 1 on connector A goes to Pin 3 on connector B. Pin 2 on connector A goes to Pin 6 on connector B, etc. Crossover cables are most commonly used to connect two hosts directly. Examples would be connecting a computer directly to

another computer, connecting a switch directly to another switch, or connecting a router to a router. Note: While in the past, when connecting two host devices directly, a crossover cable was required. Nowadays, most devices have auto-sensing technology that detects the cable and device and crosses pairs when needed.

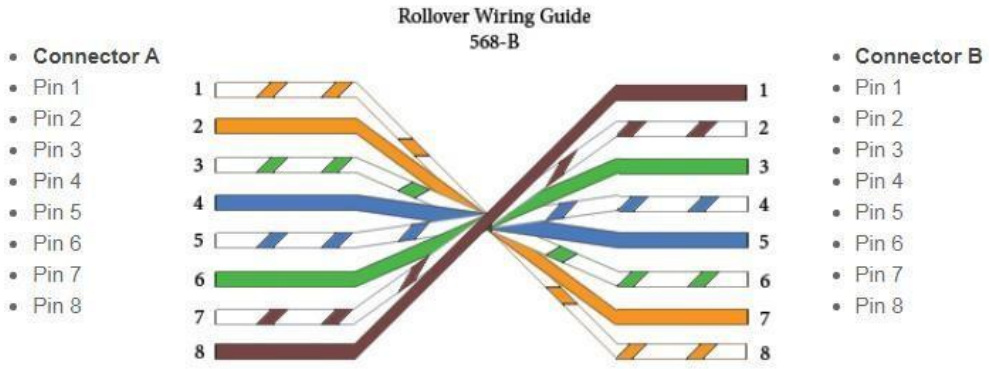
To summarize, crossover cables directly connect the following devices on a LAN:

- Switch to switch
- Switch to hub
- Hub to hub
- Computer to computer
- Computer to a router Ethernet port
- Router to router Ethernet port connection



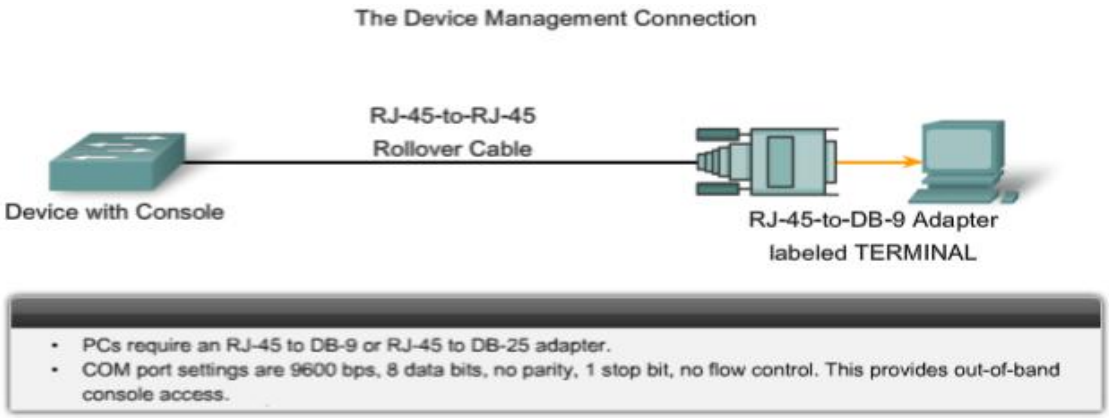
Rollover Wired Cables

Rollover wired cables, most commonly called rollover cables, have opposite Pin assignments on each end of the cable or, in other words, it is "rolled over." Pin 1 of connector A would be connected to Pin 8 of connector B. Pin 2 of connector A would be connected to Pin 7 of connector B and so on. Rollover cables, sometimes referred to as Yost cables are most commonly used to connect to a device's console port to make programming changes to the device. Unlike crossover and straight-wired cables, rollover cables are not intended to carry data but instead create an interface with the device.



Console Cables (RJ-45 to DB-9 Female). This cable is also known as Management Cable

The connection to the console is made by plugging the DB-9 connector into an available EIA/TIA 232 serial port on the computer. It is important to remember that if there is more than one serial port, note which port number is being used for the console connection. Once the serial connection to the computer is made, connect the RJ-45 end of the cable directly into the console interface on the router.



Video Reference:
Refer the following videos:

Categories of Cables: https://www.youtube.com/watch?v=_NX99ad2FUA

Crimpling : https://www.youtube.com/watch?v=8qTS2BiRZzU

Answer the following VIVA Questions:

1. Transmission media are directly controlled by **Physical** Layer.

2. What are the three major classes of Guided Media?
   - **Twisted Pair Cable**: Insulated copper wires twisted together, used in Ethernet and telecommunication.
   - **Coaxial Cable**: Central conductor with insulating layers, used in cable TV and broadband.
   - **Fiber Optic Cable**: Transmits data using light signals, ideal for high-speed and Long-distance Communication.

3. Why Cladding is used in Fiber Optics?
   - It ensures total internal reflection, keeping light signals confined within the core.
   - Minimizes dispersion and loss by maintaining the light's pathway.
   - Provides mechanical protection and preserves the integrity of the core.
   - Improves transmission efficiency and reduces interference.

4. List the Categories of UTP cables.
   - Category 1 (Cat 1): Used for voice communication (e.g., telephone lines).
   - Category 2 (Cat 2): Supports data up to 4 Mbps (obsolete).
   - Category 3 (Cat 3): Used in 10 Mbps Ethernet networks.
   - Category 4 (Cat 4): Supports data up to 16 Mbps (Token Ring networks).
   - Category 5 (Cat 5): Used in 100 Mbps Ethernet and 1 Gbps networks.
   - Category 5e (Cat 5e): Enhanced Cat 5 for reduced crosstalk; supports 1 Gbps.
   - Category 6 (Cat 6): Supports 10 Gbps over shorter distances, with improved performance.
   - Category 6a (Cat 6a): Augmented Cat 6, supports 10 Gbps over longer distances.
   - Category 7 (Cat 7): Shielded for higher performance; supports 10 Gbps.
   - Category 8 (Cat 8): Designed for 25/40 Gbps data centers

5. Mention the cause of attenuation and how will you measure it.
   Attenuation is caused by the reduction in signal strength during transmission due to:
   - Loss of energy as the signal interacts with the medium.
   - Dispersion of signal energy due to imperfections in the medium.
   - Signal leakage caused by bends in the transmission medium.
   - External electromagnetic noise affecting the signal.

   Measurement:

   $$\text{Attenuation (dB)} = 10 \times \log_{10}(P_{output}/P_{input})$$

6. What are the advantage s of Fiber Optics?
   - High Bandwidth
   - Long-Distance Transmission
   - Immunity to Electromagnetic Interference
   - Security
   - Lightweight and Durable.

7. What is meant by LOS?
   Line of Sight (LOS) refers to a direct, unobstructed path between the transmitting and receiving antennas in a communication system.
   - Essential for high-frequency signals like microwaves and infrared.
   - Obstructions like buildings, trees, or terrain can disrupt LOS communication.
   - Commonly used in satellite, radio, and point-to-point wireless systems

8. Mention the modes of propagation in unguided medium.
   - Ground Wave Propagation
   - Sky Wave Propagation
   - Space Wave Propagation

9. List out the connectors used in guided medium.
   - Twisted Pair Cable Connectors
   - Coaxial Cable Connectors
   - Fiber Optic Cable Connectors

10. Where you will use Straight through cable and Cross over cable?

    Straight-Through Cable
    - Connects a computer (or any device) to a network switch or router.
    - Connects a router to a modem for internet access.
    - For connecting a network switch to a hub.

    Cross-Over Cable
    - Directly connects two computers without a hub or switch.
    - For connecting two switches together.
    - Used when directly connecting two routers.
    - For connecting two hubs directly.

Rubrics for Experiment Assessment:

Description	Marks Weightage	Marks Scored
Build Straight through, Cross over, Roll over UTP cable	4	
Test the connectivity using small network	4	
Timely Completion	2	
Total Marks		

RESULT:

Thus the different types of network cables and the implementation of the crossover wired and straight-through cable using Crimping Tool was completed successfully.

Ex.No: 4 Date :	Configuration of Intra VLAN network
Registration Number:	99220041065
Name:	DESU SIVA NAGA SATYA SAI
Section & Slot	S12 & Slot-3

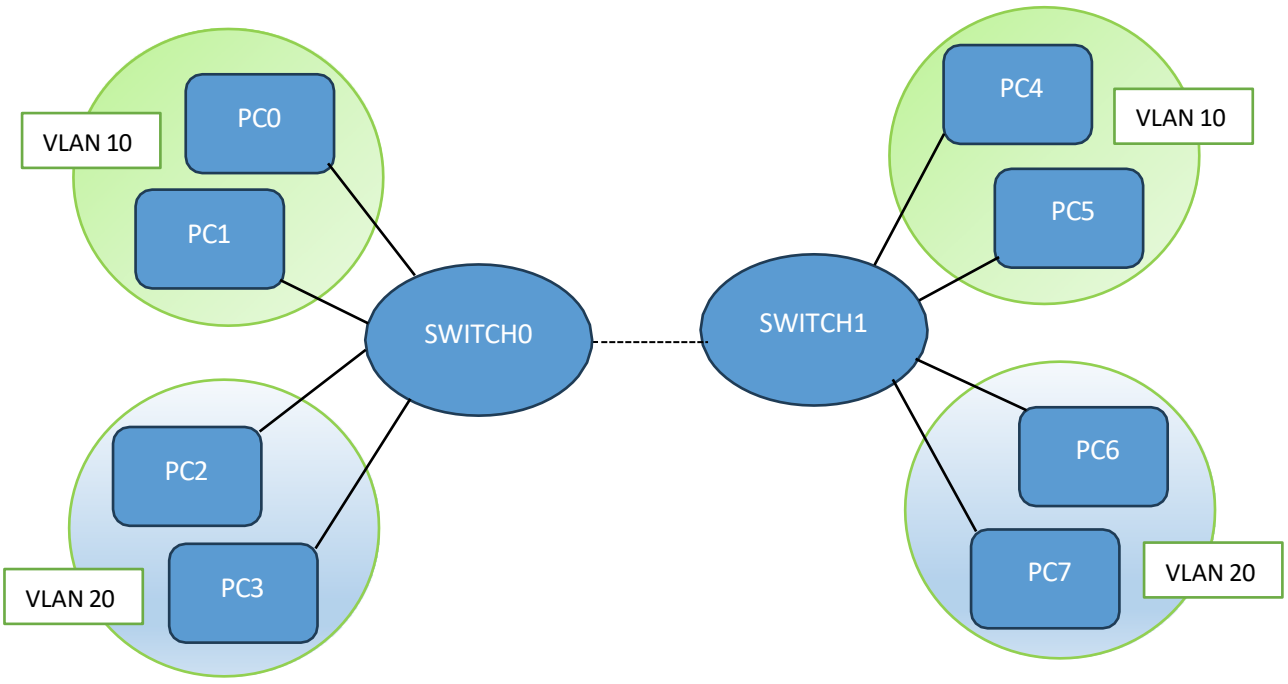
Objective(s):

To design and implement Intra VLAN using switch configuration

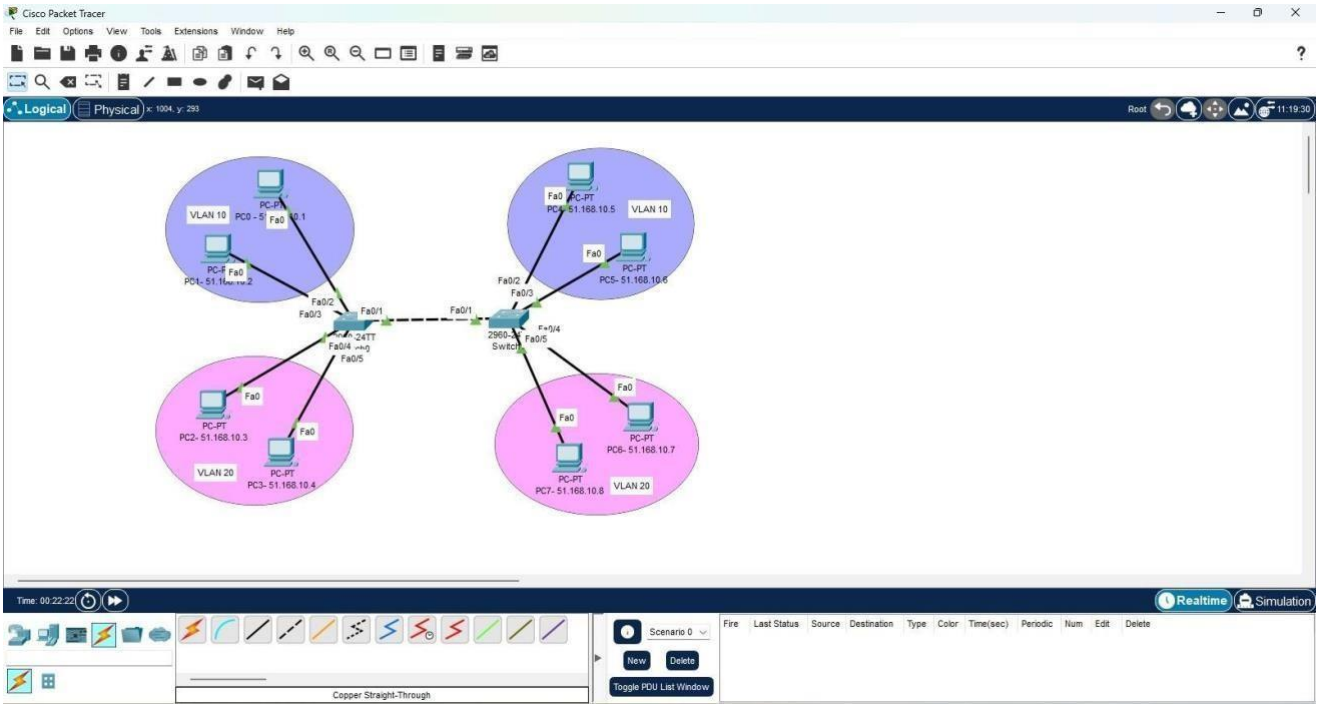
Introduction:

A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.VLANs define broadcast domains in a Layer 2 network. A broadcast domain is the set of all devices that will receive broadcast frames originating from any device within the set. Broadcast domains are typically bounded by routers because routers do not forward broadcast frames. Layer 2 switches create broadcast domains based on the configuration of the switch. Switches are multiport bridges that allow you to create multiple broadcast domains. Each broadcast domain is like a distinct virtual bridge within a switch. Design the above-mentioned topologies and verify the connectivity.

1. **Device Requirements:**
   1. PC's
   2. Switch (2960-24TT)
   3. Copper stand through cable
   4. Copper cross wire cable
2. **Network Diagram for your experiment:**



3. Network Diagram (Packet tracer diagram before configuration):



4. Configuration details:

Device Name	Interface Name	IP Address	Subnet mask
SWITCH0			
PC0	FastEtherent0/2	51.168.10.1	255.0.0.0
PC1	FastEtherent0/3	51.168.10.2	255.0.0.0
PC2	FastEtherent0/4	51.168.10.3	255.0.0.0
PC3	FastEtherent0/5	51.168.10.4	255.0.0.0
SWITCH1			
PC4	FastEtherent0/2	51.168.10.5	255.0.0.0
PC5	FastEtherent0/3	51.168.10.6	255.0.0.0
PC6	FastEtherent0/4	51.168.10.7	255.0.0.0
PC7	FastEtherent0/5	51.168.10.8	255.0.0.0

5. Describe step by step configuration steps properly

1. Create VLANs:

Switch0 & switch1:

- **VLAN 10**
  - enable
  - configure terminal
  - vlan 10
  - Show vlan
- **VLAN 20**
  - enable
  - configure terminal
  - vlan 20

2. Configure interfaces:

Switch0 & Switch1:

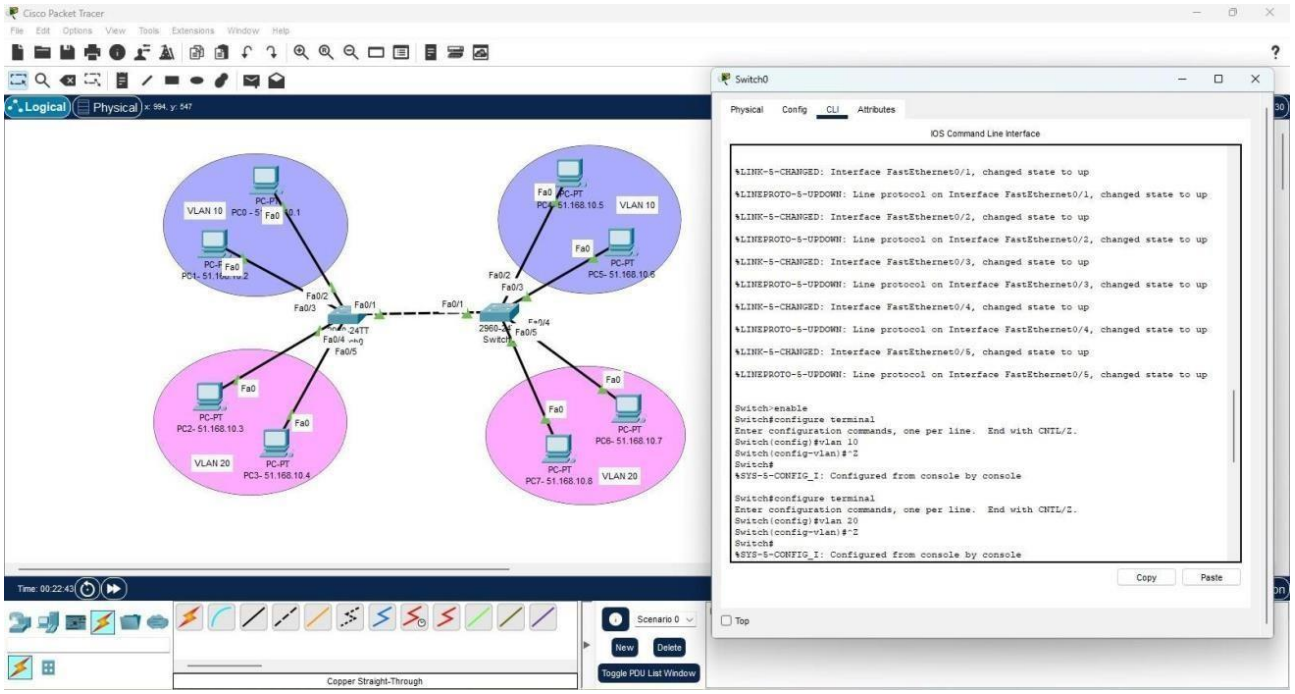
- **VLAN 10:**
  - interface fastethernet0/2
  - switchport mode access
  - switchport access vlan 10
  - interface fastethernet0/3
  - switchport mode access
  - switchport access vlan 10
- **VLAN 20:**
  - interface fastethernet0/4
  - switchport mode access
  - switchport access vlan 20
  - show vlan
  - ping <ip_address>
  - interface fastethernet0/5
  - switchport mode access
  - switchport access vlan 20

3. Configure trunking:

Switch0 & Switch1:

- Configure terminal
- Interface fastethernet0/1
- Switchport mode trunk
- Ping <ip_address>

6. Output Diagram:



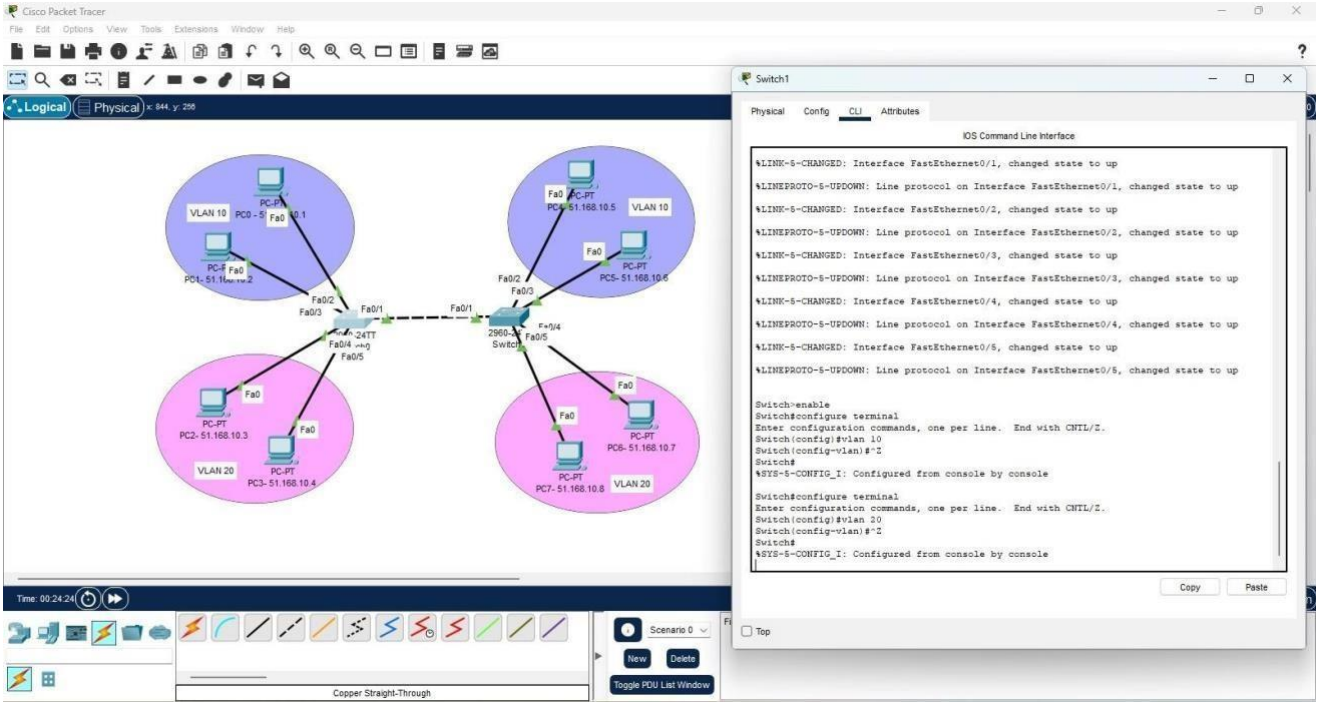
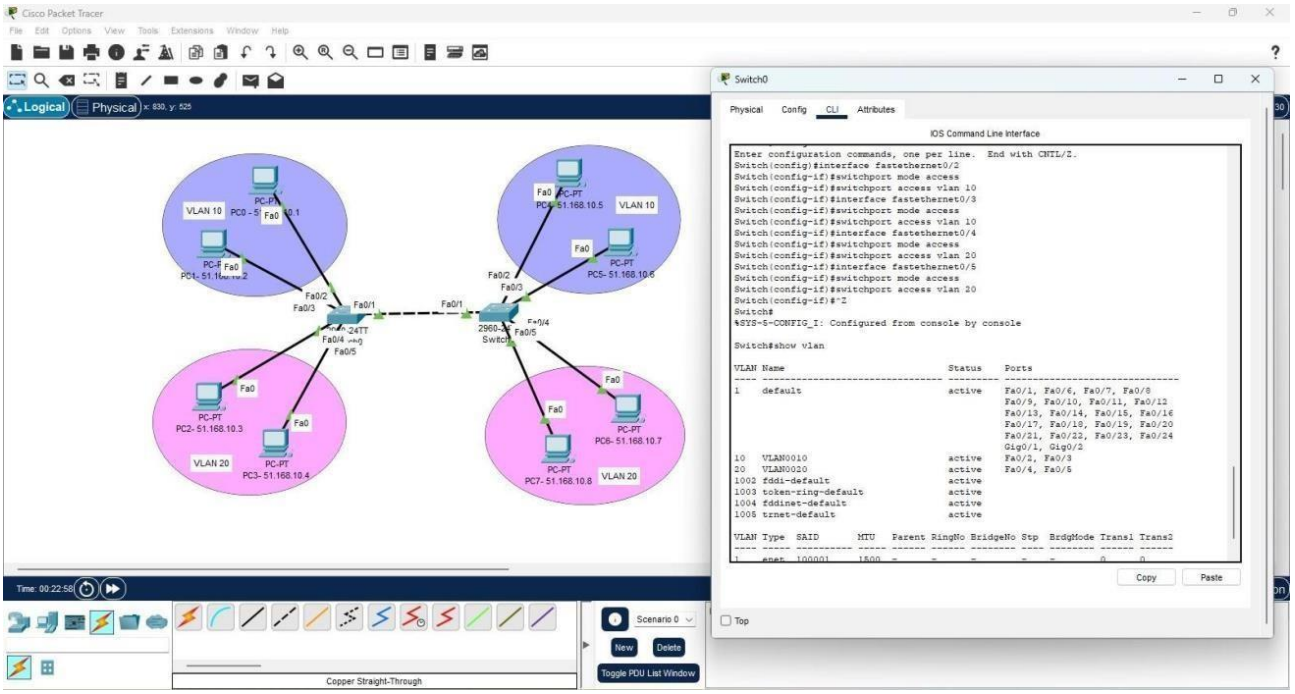


FIG: Creating VLAN'S



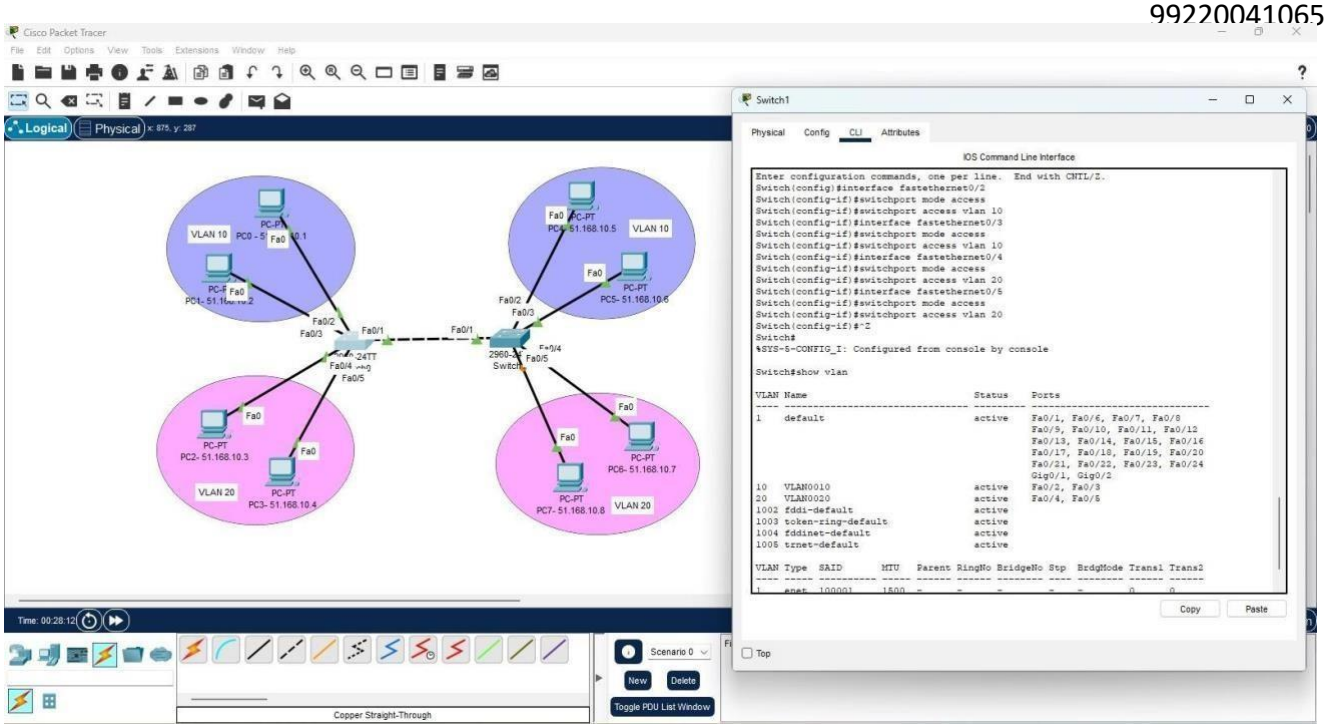


FIG: Configure interfaces

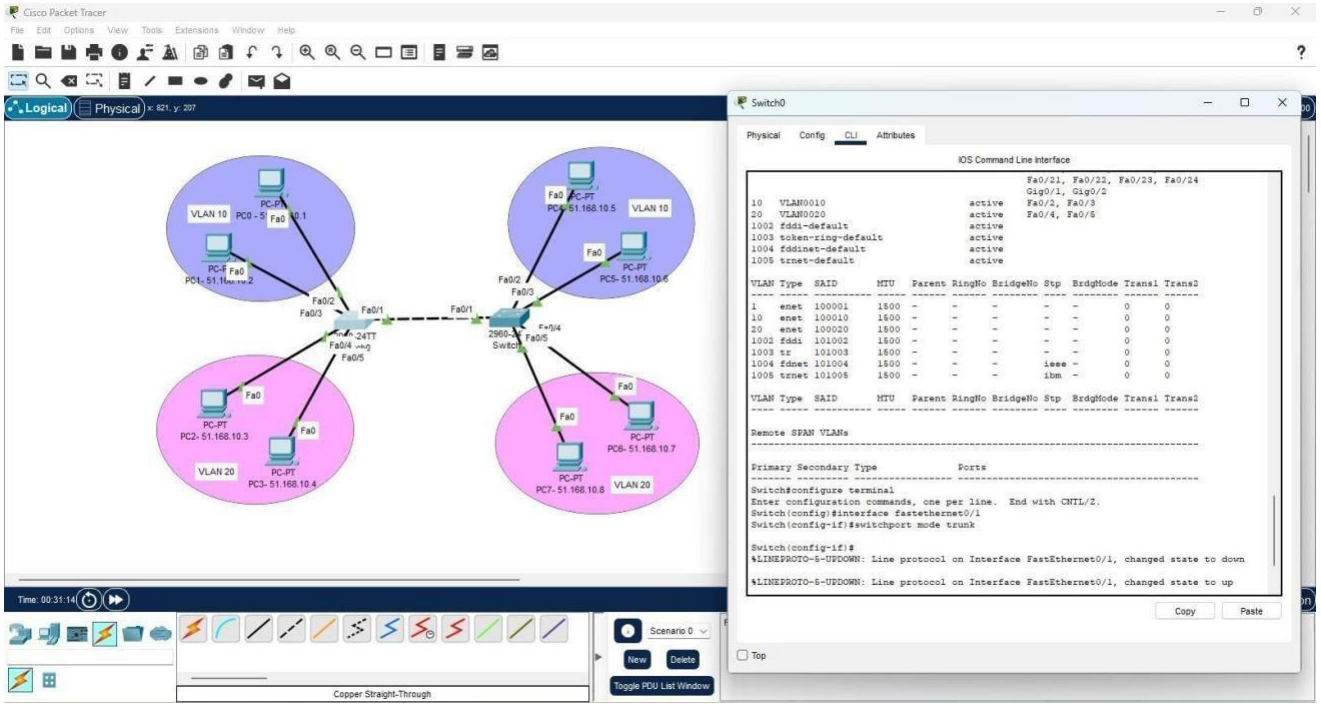
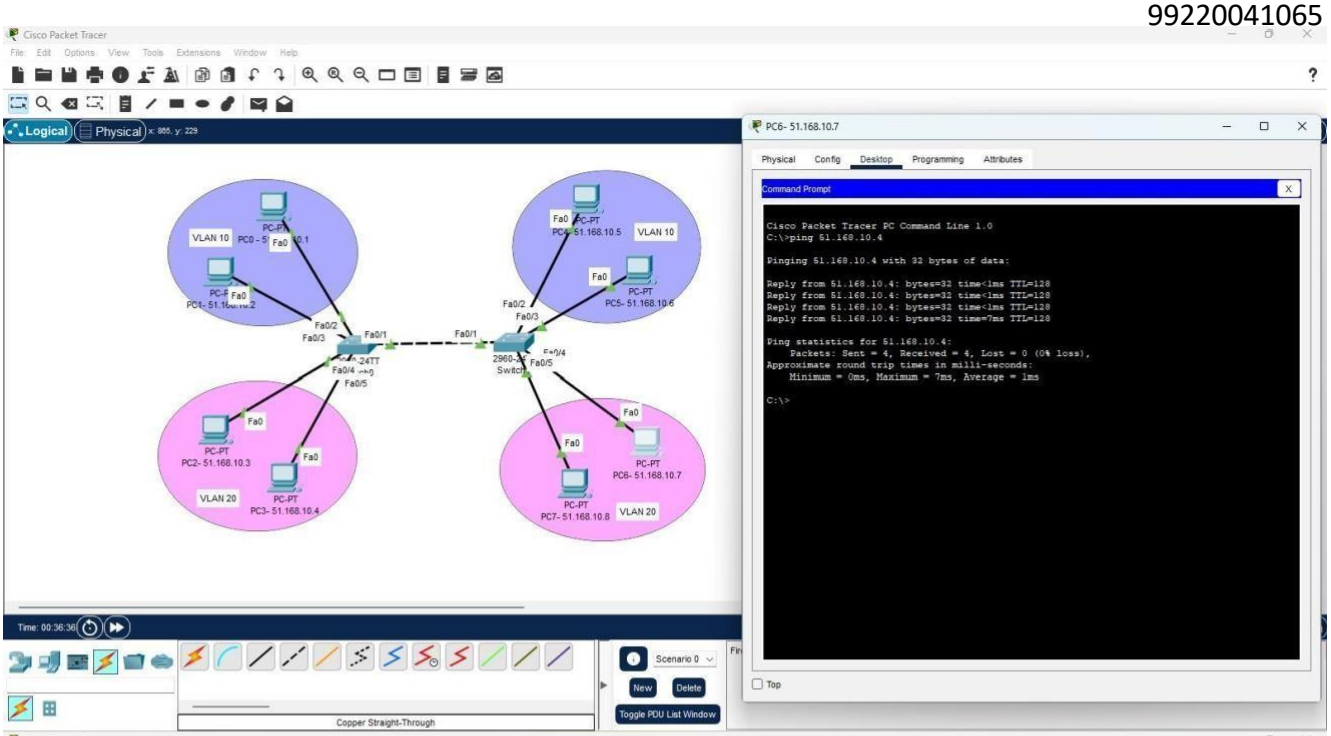
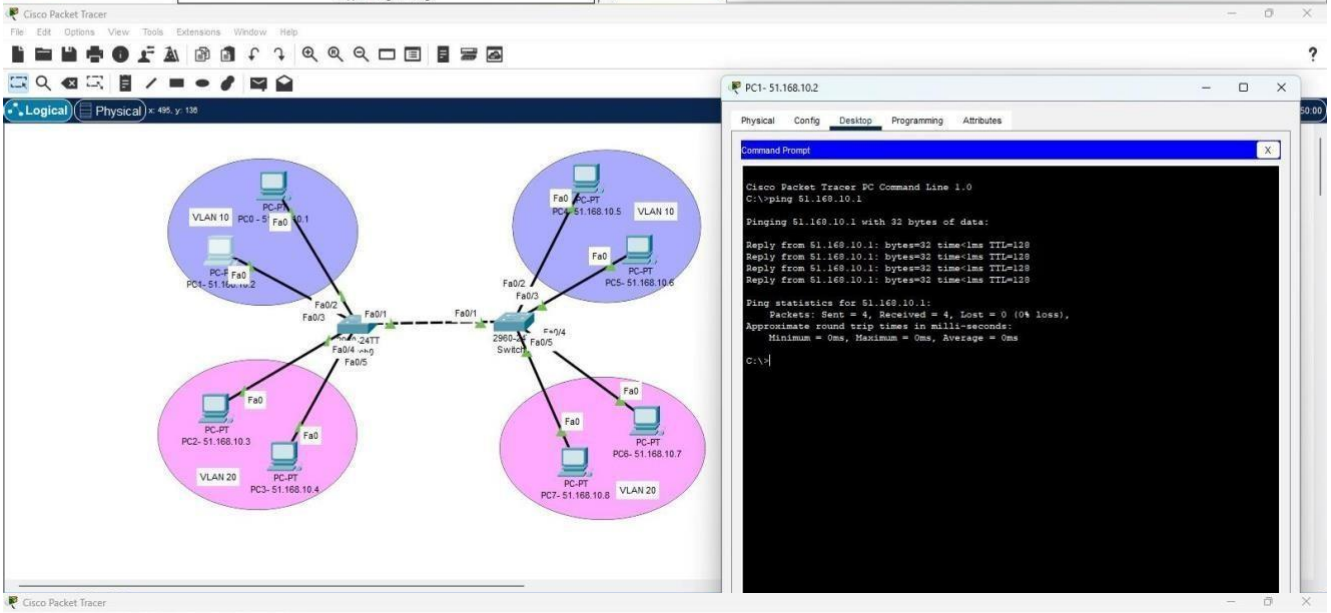
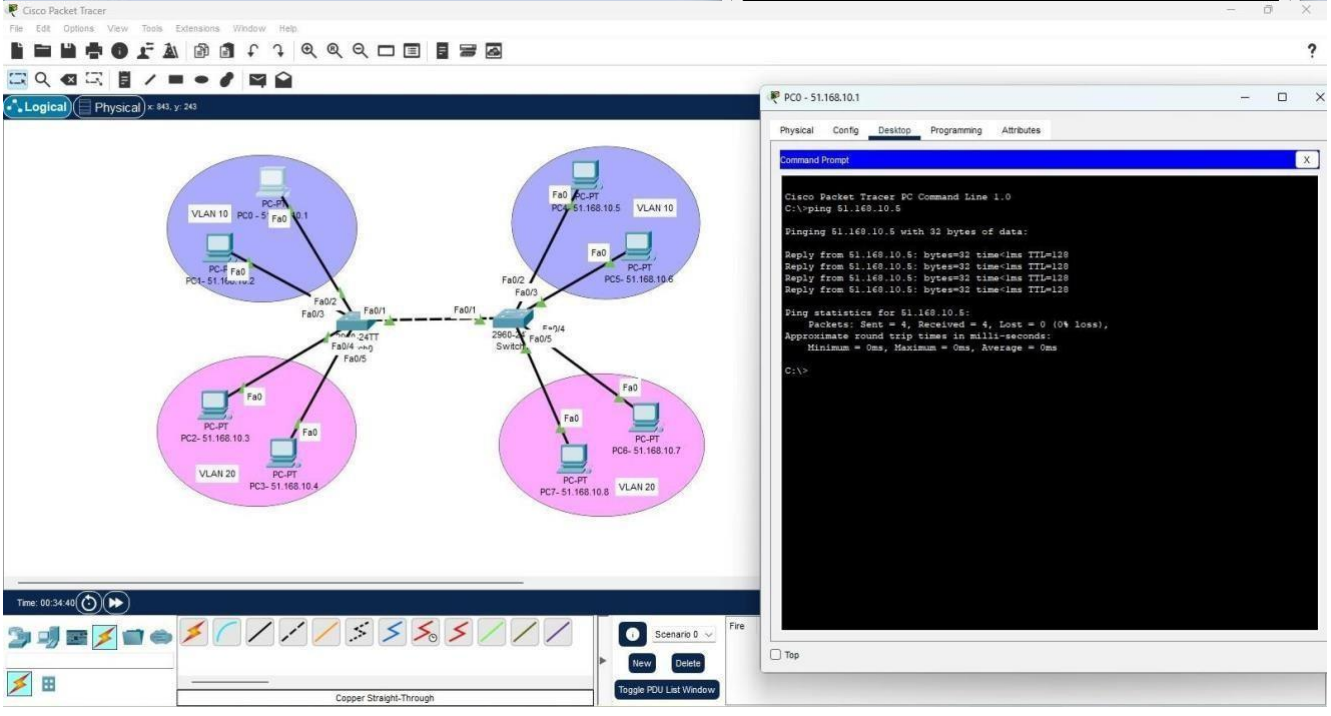


FIG: Configure trunking


Cisco Packet Tracer
Logical
Physical
PC6- 51.168.10.7
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 51.168.10.4
Pinging 51.168.10.4 with 32 bytes of data:
Reply from 51.168.10.4: bytes=32 time<1ms TTL=128
Reply from 51.168.10.4: bytes=32 time<1ms TTL=128
Reply from 51.168.10.4: bytes=32 time<1ms TTL=128
Reply from 51.168.10.4: bytes=32 time=7ms TTL=128
Ping statistics for 51.168.10.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 7ms, Average = 1ms
C:\>
VLAN 10
VLAN 20
PC-PT
PC2- 51.168.10.3
PC3- 51.168.10.4
PC5- 51.168.10.6
PC7- 51.168.10.8
Fa0
Fa0/1
Fa0/2
Fa0/3
Fa0/5
Switch
Time: 00:36:36
Copper Straight-Through
Scenario 0
New
Delete
Toggle PDU List Window
Top


Cisco Packet Tracer
Logical
Physical
PC1- 51.168.10.2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 51.168.10.1
Pinging 51.168.10.1 with 32 bytes of data:
Reply from 51.168.10.1: bytes=32 time<1ms TTL=128
Reply from 51.168.10.1: bytes=32 time<1ms TTL=128
Reply from 51.168.10.1: bytes=32 time<1ms TTL=128
Reply from 51.168.10.1: bytes=32 time<1ms TTL=128
Ping statistics for 51.168.10.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
VLAN 10
VLAN 20
PC-PT
PC2- 51.168.10.3
PC3- 51.168.10.4
PC5- 51.168.10.6
PC6- 51.168.10.7
PC7- 51.168.10.8
Fa0
Fa0/1
Fa0/2
Fa0/3
Fa0/5
Switch


Cisco Packet Tracer
Logical
Physical
PC0 - 51.168.10.1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 51.168.10.5
Pinging 51.168.10.5 with 32 bytes of data:
Reply from 51.168.10.5: bytes=32 time<1ms TTL=128
Reply from 51.168.10.5: bytes=32 time<1ms TTL=128
Reply from 51.168.10.5: bytes=32 time<1ms TTL=128
Reply from 51.168.10.5: bytes=32 time<1ms TTL=128
Ping statistics for 51.168.10.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
VLAN 10
VLAN 20
PC-PT
PC2- 51.168.10.3
PC3- 51.168.10.4
PC5- 51.168.10.6
PC6- 51.168.10.7
PC7- 51.168.10.8
Fa0
Fa0/1
Fa0/2
Fa0/3
Fa0/5
Switch
Time: 00:34:40
Copper Straight-Through
Scenario 0
New
Delete
Toggle PDU List Window
Top

CONCLUSION (provide a conclusion about this experiment):

Successfully designed and implemented Intra VLAN using switch configuration

Rubrics for Experiment Assessment:

Rubrics	Good	Normal	Poor	Marks
Creation of Topology (4)	Created the topology, identified the proper devices, and made the connections **(4).**	Created the topology, identified the proper devices, and made the connections. But missing some features **(3)**	Created the wrong topology, failed to identify the proper devices, and made connections **(1)**	
Verify the connectivity (4)	Verified the connectivity in all the levels **(4)**	Verified the connectivity at some levels (only some nodes) **(2)**	Verified the connectivity is not done. **(1)**	
Timely Completion (2)	Completed the lab before the allotted time **(2)**	Completed the lab after the deadline **(1)**	Did not submit before grading **(0)**	
			Total	

Ex No: 05 Date:	Study of Network Topologies
Register Number:	99220041065
Name:	DESU SIVA NAGA SATYA SAI
Section & Slot	S12 & Slot-03

Objective(s):

To design and implement network topologies using Cisco Packet Tracer

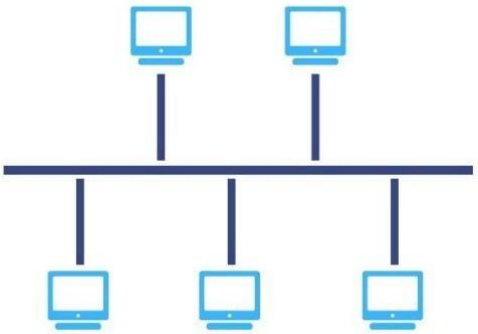
Introduction:

Network topology is the geometric representation of relationship of all the links connecting the devices or nodes. Network topology represent in two ways one is physical topology that define the way in which a network is physically laid out and other one is logical topology that defines how data actually flow through the network. In this lab, we will discuss how to design bus, star and mesh topology network and provide interfacing and simulation between end points using packet tracer software.

Theoretical Background:

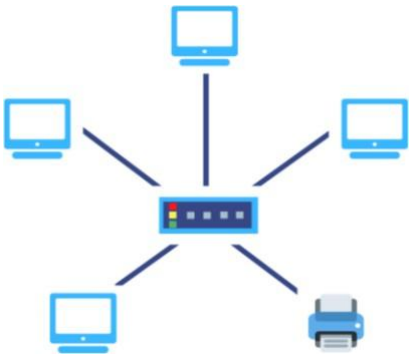
Bus Topology

In local area network, it is a single network cable runs in the building or campus and all nodes are connected along with this communication line with two endpoints called the bus or backbone. In other words, it is a multipoint data communication circuit that is easily control data flow between the computers because this configuration allows all stations to receive every transmission over the network. For bus topology we build network using three generic pc which are serially connected with three switches using copper straight through cable and switches are interconnected using copper cross over cable.

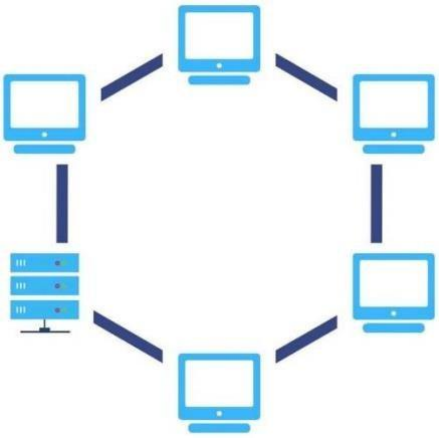


Star Topology

In star topology, all the cables run from the computers to a central location where they are all connected by a device called a hub. It is a concentrated network, where the end points are directly reachable from a central location when network is expanded. Ethernet 10 base T is a popular network based on the star topology. For star topology we build network using five generic pc which are centrally connected to single switch 2950-24 using copper straight through cable.



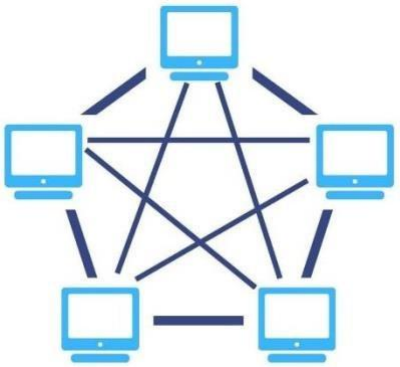
RING TOPOLOGY



As we mentioned earlier, the ring topology is similar to a daisy chain topology but with the loop closed so that the nodes are arranged in a ring or circle. Each node has exactly two peers and the data travels in one direction passing through each intermediate node on the ring until it reaches the destination node. Data can be made to pass in both directions by adding a second connection between the network nodes, creating a dual ring topology.

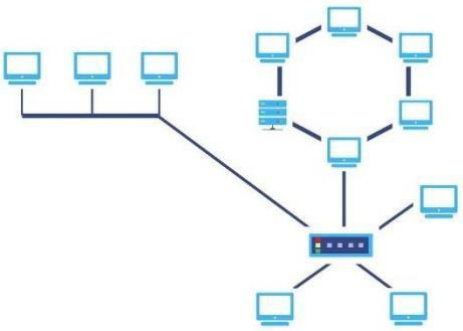
In a ring topology, an electrical "token" circulates around the network. Any node that wants to transmit data has to wait until it has possession of the token.

MESH TOPOLOGY



In mesh topology every device has a dedicated point to point link to every other device. The term dedicated stand for link carries traffic only between four devices it connects. It is a well-connected topology; in this, every node has a connection to every other node in the network. The cable requirements are high and it can include multiple topologies. Failure in one of the computers does not cause the network to break down, as they have alternative paths to other computers star topology, all the cables run from the computers to a central location.

Hybrid Topology



Hybrid topology combines two or more topologies. You can see in the above architecture in such a manner that the resulting network does not exhibit one of the standard topologies.

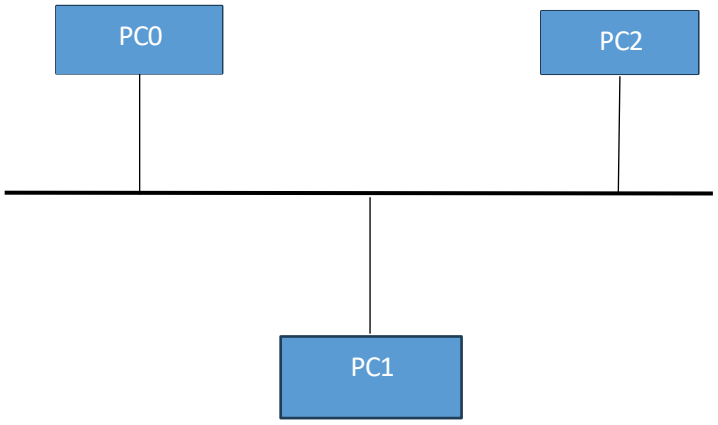
For example, as you can see in the above image that in an office in one department, Star and P2P topology is used. A hybrid topology is always produced when two different basic network topologies are connected.

Design the above mentioned topologies and verify the connectivity.

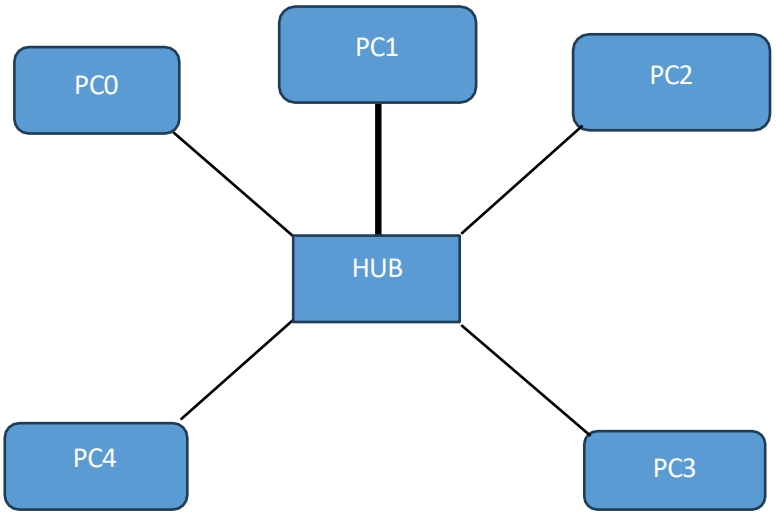
1. **Device Requirements:**
   1. PC's
   2. Switch (2950-24, 2960-24TT)
   3. Copper stand through cable
   4. Copper cross wire cable

2. **Network Diagram for your experiment (draw the diagram either hand drawing/ms paint or any other drawing tools)**

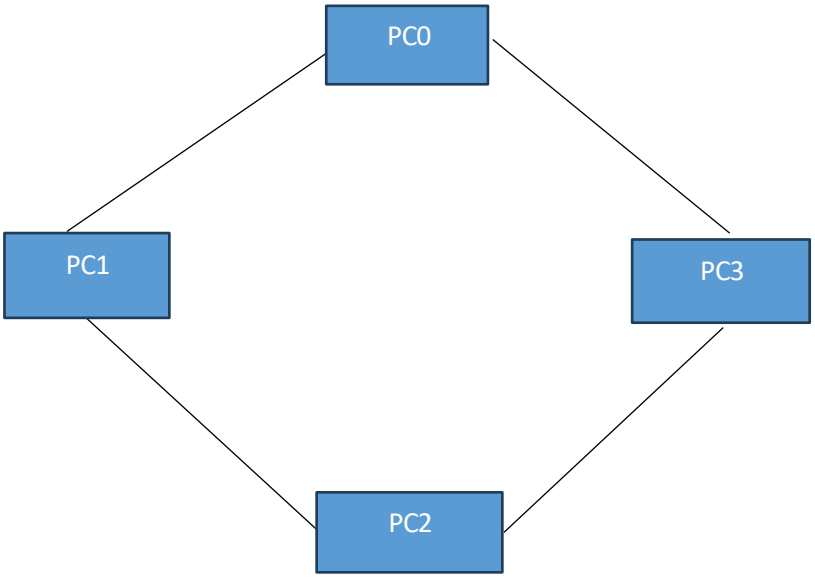
BUS TOPOLOGY:



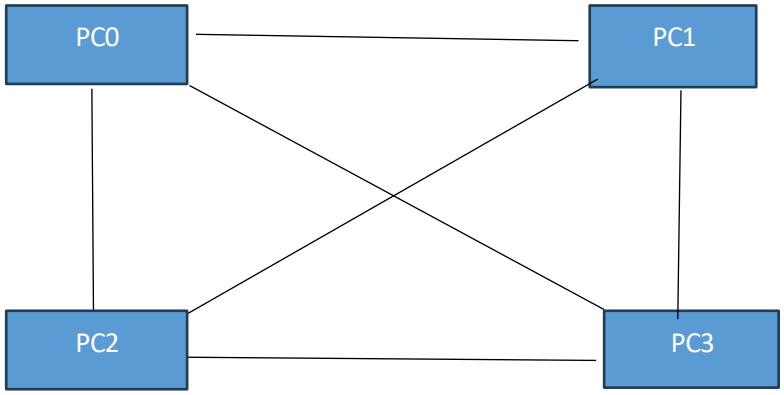
STAR TOPOLOGY:



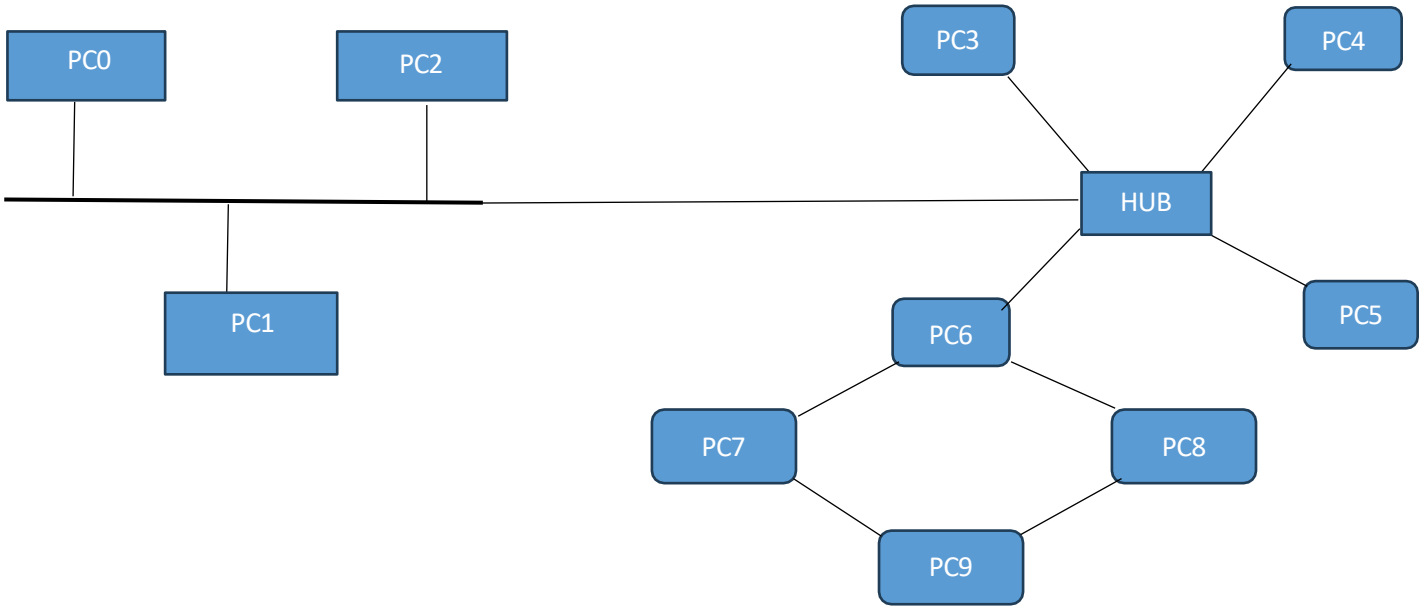
RING TOPOLOGY:



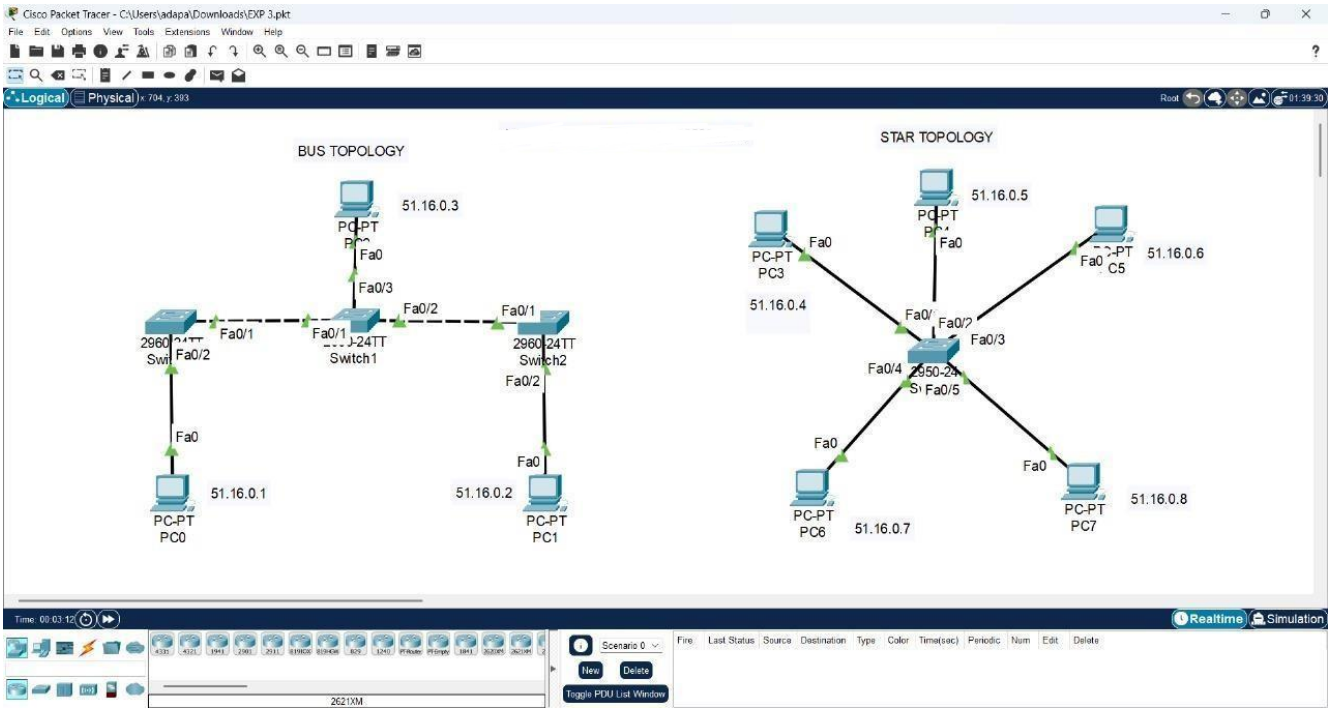
MESH TOPOLOGY:

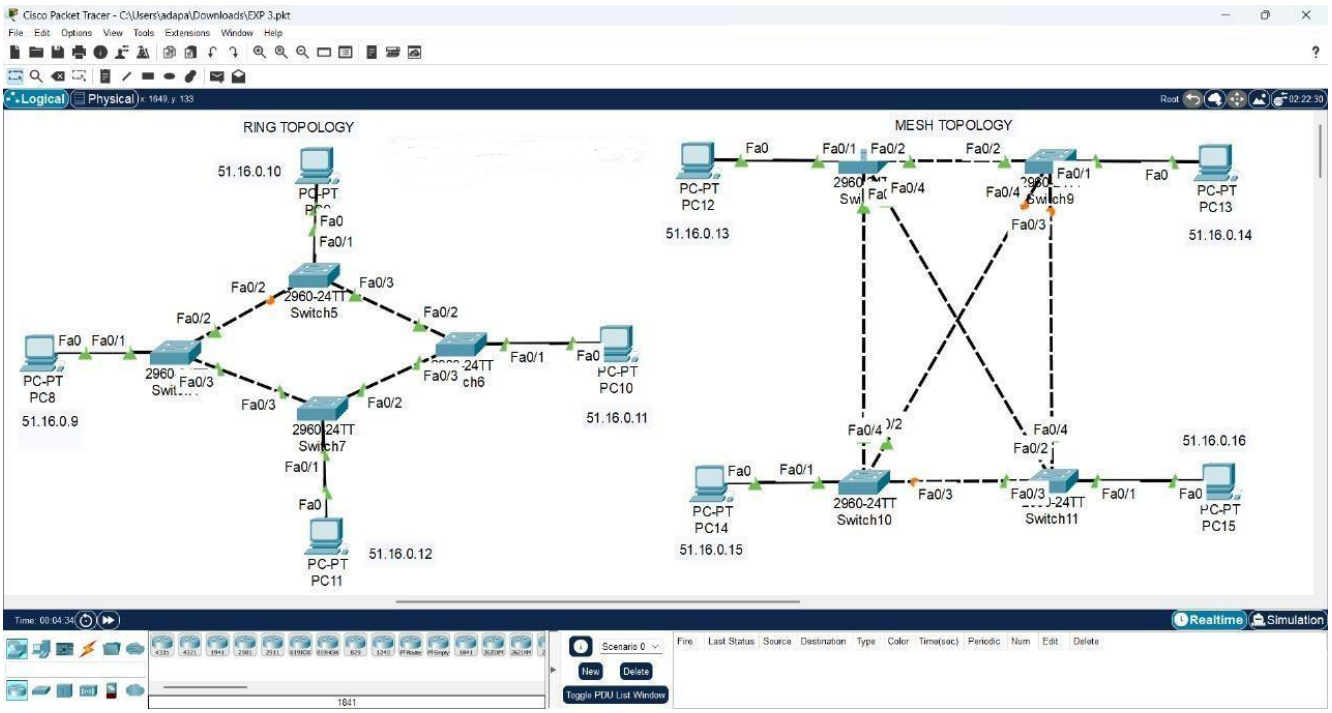


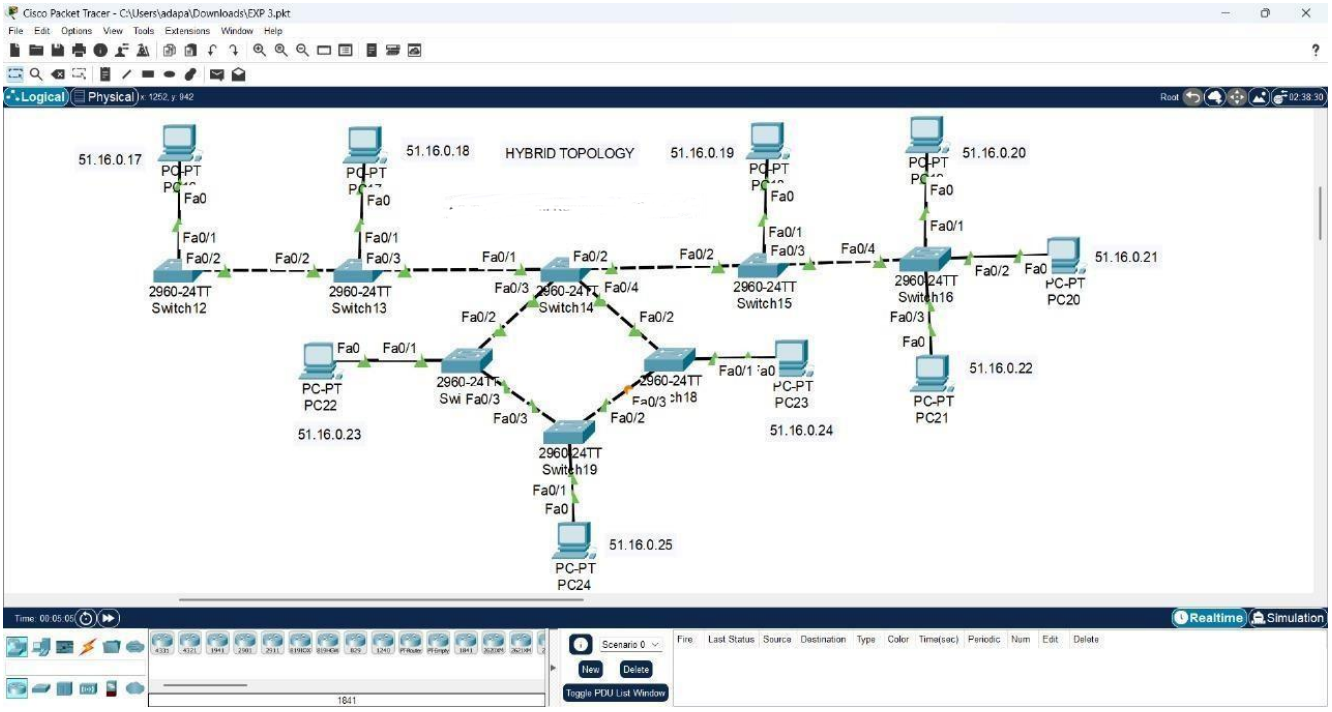
HYBRID TOPOLOGY:



3. Network Diagram:







4. Configuration details:

BUS TOPOLOGY:

Device Name	Interface Name	IP Address	Subnet mask
PC0	FastEtherent0/1	51.16.0.1	255.0.0.0
PC1	FastEtherent0/2	51.16.0.2	255.0.0.0
PC2	FastEtherent0/3	51.16.0.3	255.0.0.0

STAR TOPOLOGY:

Device Name	Interface Name	IP Address	Subnet mask
PC3	FastEtherent0/0	51.16.0.4	255.0.0.0
PC4	FastEtherent0/1	51.16.0.5	255.0.0.0
PC5	FastEtherent0/2	51.16.0.6	255.0.0.0
PC6	FastEtherent0/3	51.16.0.7	255.0.0.0
PC7	FastEtherent0/4	51.16.0.8	255.0.0.0

RING TOPOLOGY:

Device Name	Interface Name	IP Address	Subnet mask
PC8	FastEtherent0/0	51.16.0.9	255.0.0.0
PC9	FastEtherent0/1	51.16.0.10	255.0.0.0
PC10	FastEtherent0/2	51.16.0.11	255.0.0.0
PC11	FastEtherent0/3	51.16.0.12	255.0.0.0

MESH TOPOLOGY:

Device Name	Interface Name	IP Address	Subnet mask
PC12	FastEtherent0/0	51.16.0.13	255.0.0.0
PC13	FastEtherent0/1	51.16.0.14	255.0.0.0
PC14	FastEtherent0/2	51.16.0.15	255.0.0.0
PC15	FastEtherent0/3	51.16.0.16	255.0.0.0

HYBRID TOPOLOGY:

Device Name	Interface Name	IP Address	Subnet mask
PC16	FastEtherent0/0	51.16.0.17	255.0.0.0
PC17	FastEtherent0/1	51.16.0.18	255.0.0.0
PC18	FastEtherent0/2	51.16.0.19	255.0.0.0
PC19	FastEtherent0/3	51.16.0.20	255.0.0.0
PC20	FastEtherent0/4	51.16.0.21	255.0.0.0
PC21	FastEtherent0/5	51.16.0.22	255.0.0.0
PC22	FastEtherent0/6	51.16.0.23	255.0.0.0
PC23	FastEtherent0/7	51.16.0.24	255.0.0.0
PC24	FastEtherent0/8	51.16.0.25	255.0.0.0

5. Commands used in each of the diagram:

Ipconfig

Ping <IP_ADDRESS>

6. Output Diagram:

BUS TOPOLOGY:

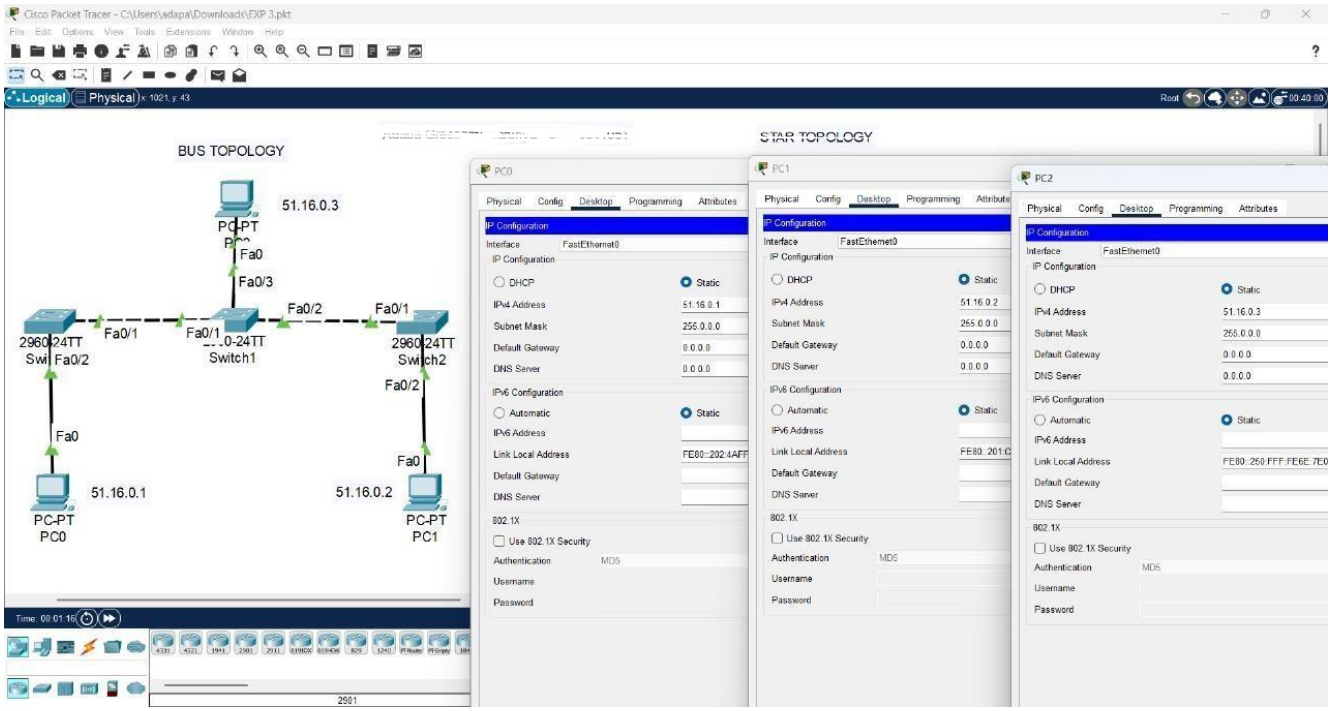


FIG: ASSIGNING IP ADDRESS

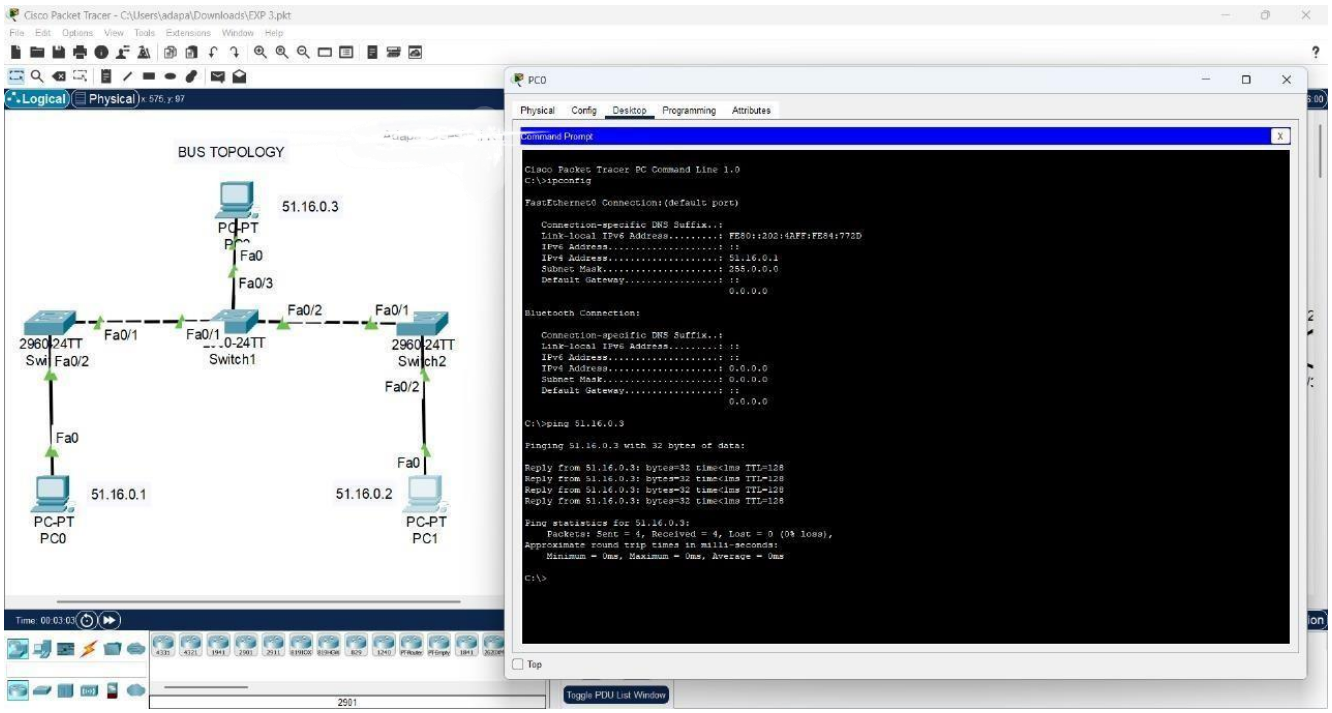


FIG: PING

STAR TOPOLOGY:

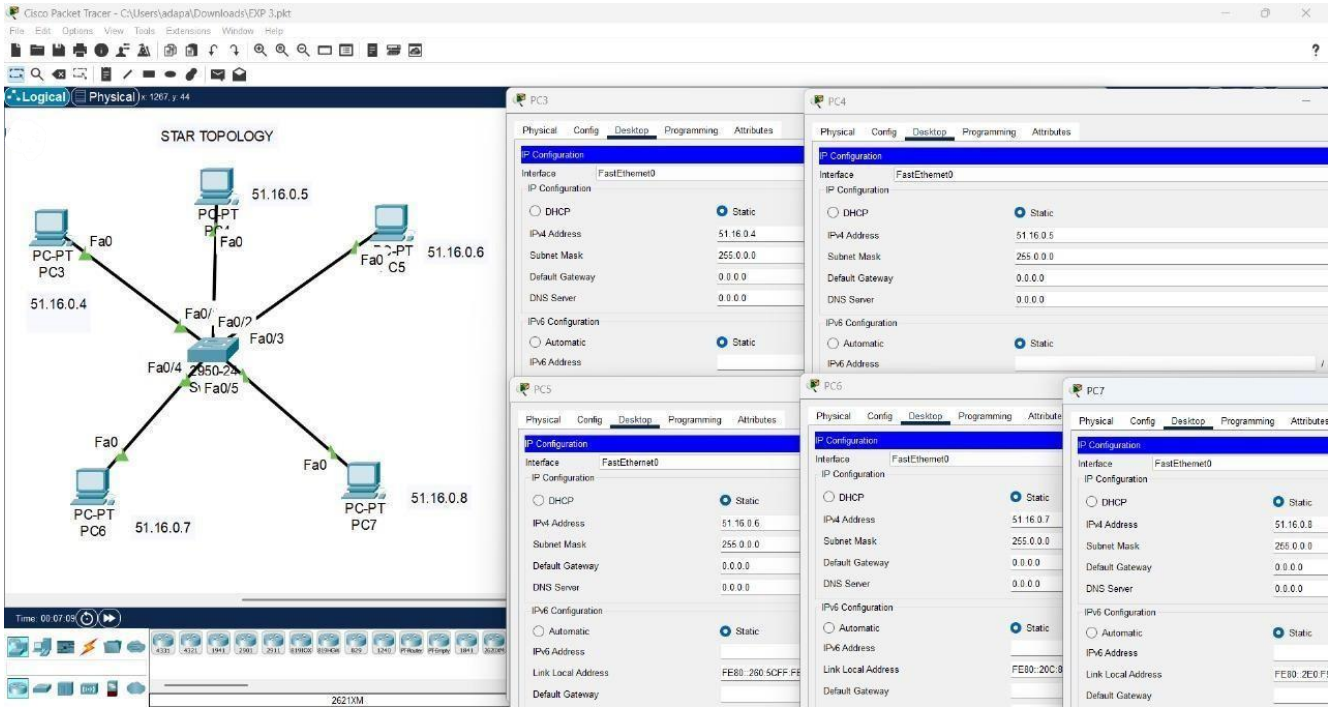


FIG: ASSIGNING IP ADDRESS

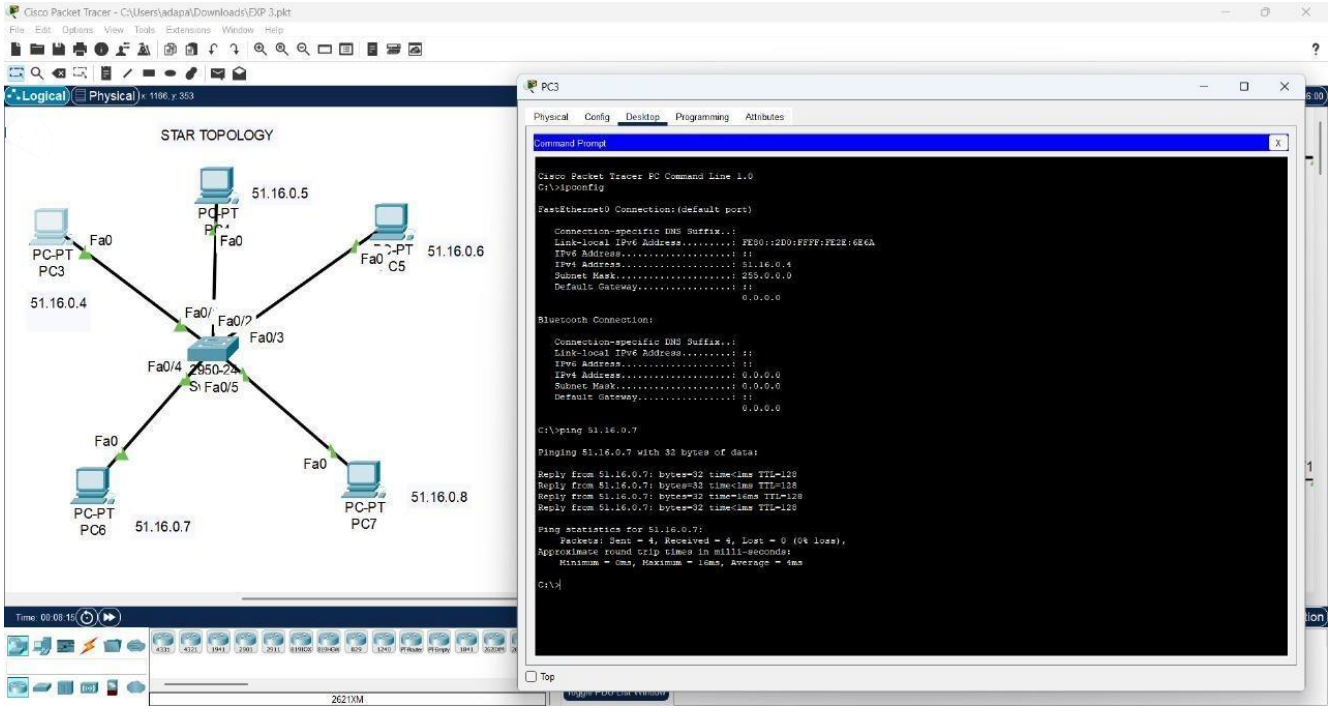


FIG: PING

RING TOPOLOGY:

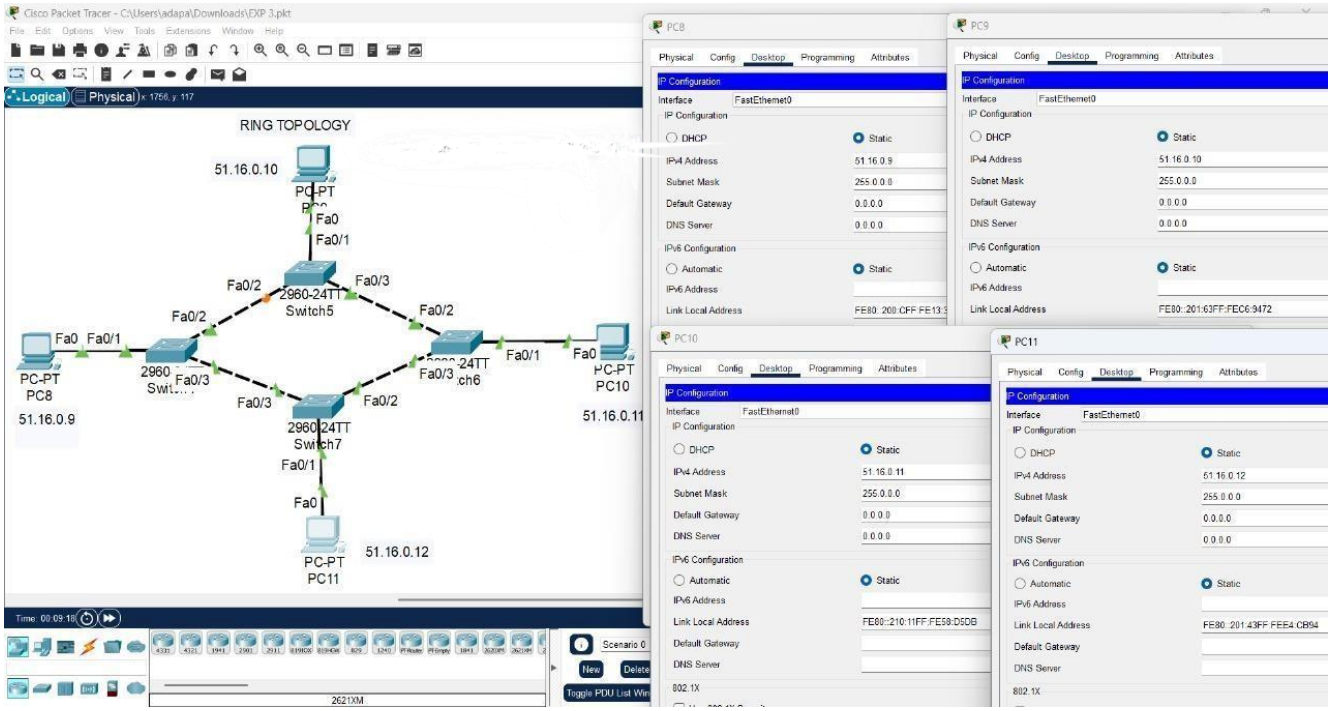


FIG: ASSIGNING IP ADDRESS

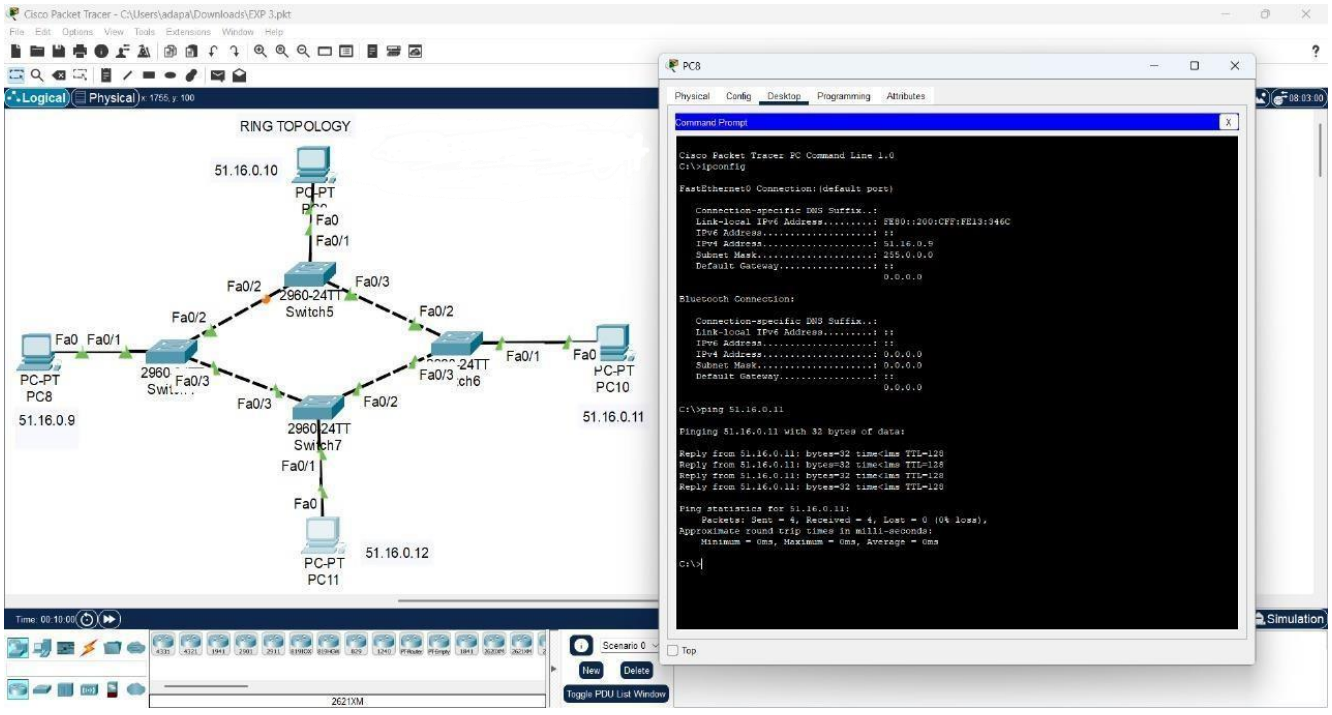


FIG: PING

MESH TOPOLOGY:

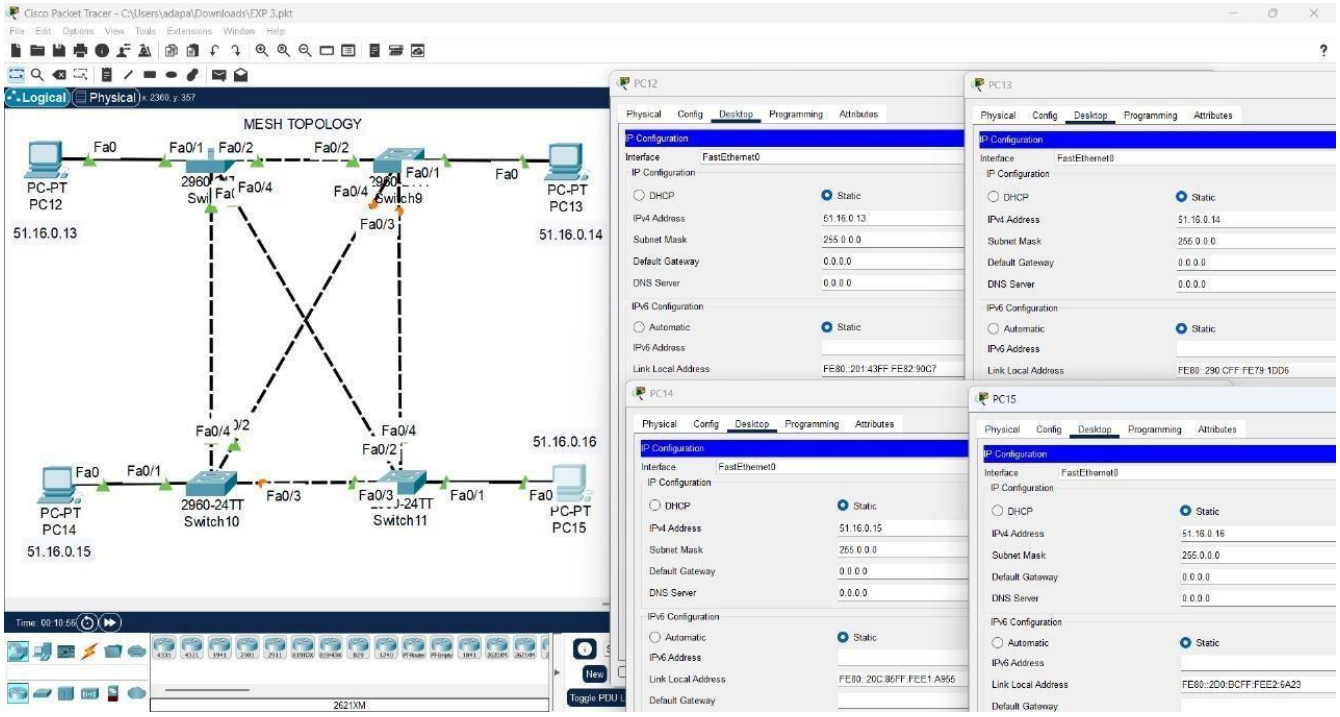


FIG: ASSIGNING IP ADDRESS

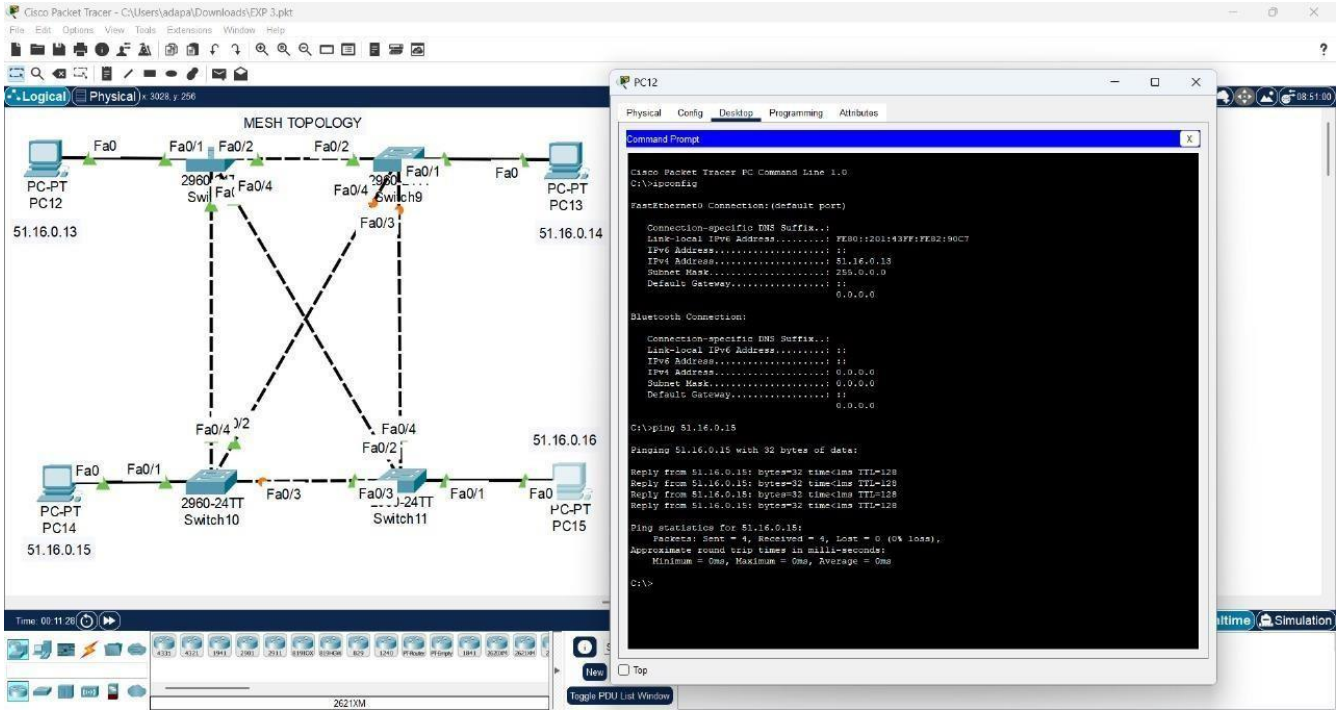


FIG: PING

HYBRID TOPOLOGY:

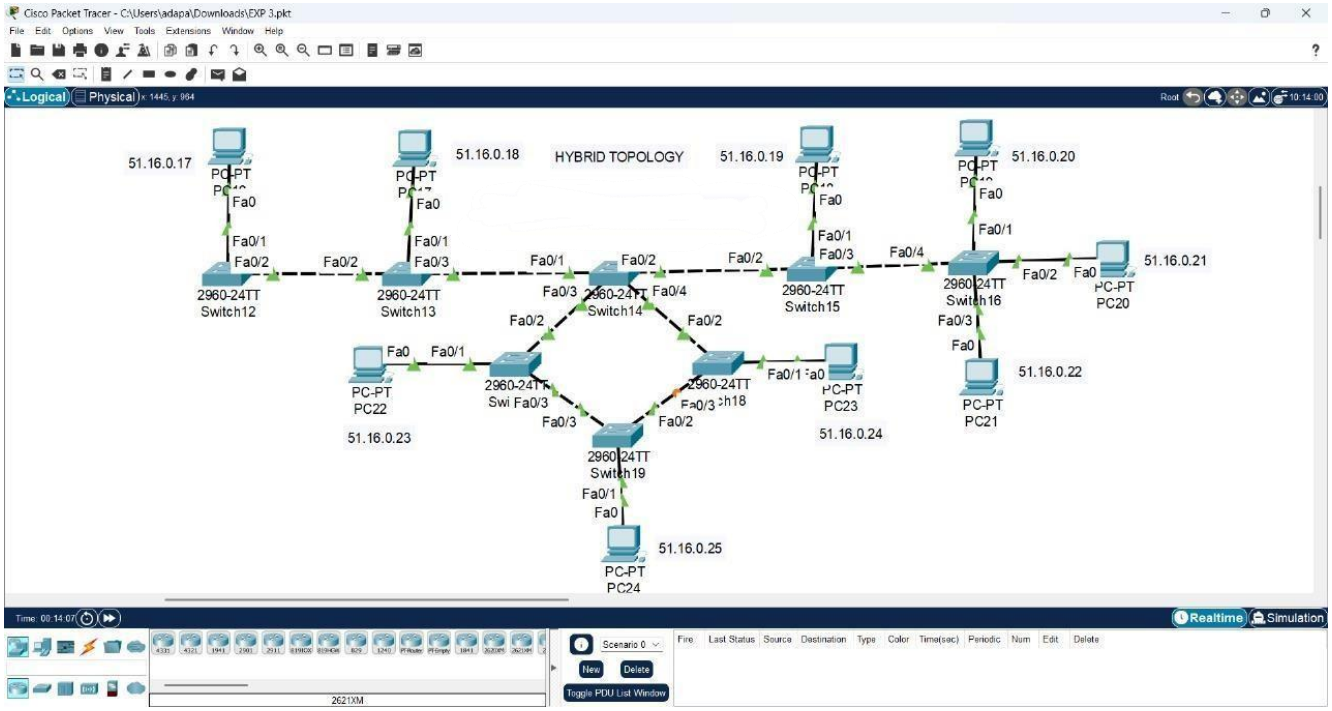


FIG: NETWORK DIAGRAM WITH ASSSIGNED IPADDRESSES

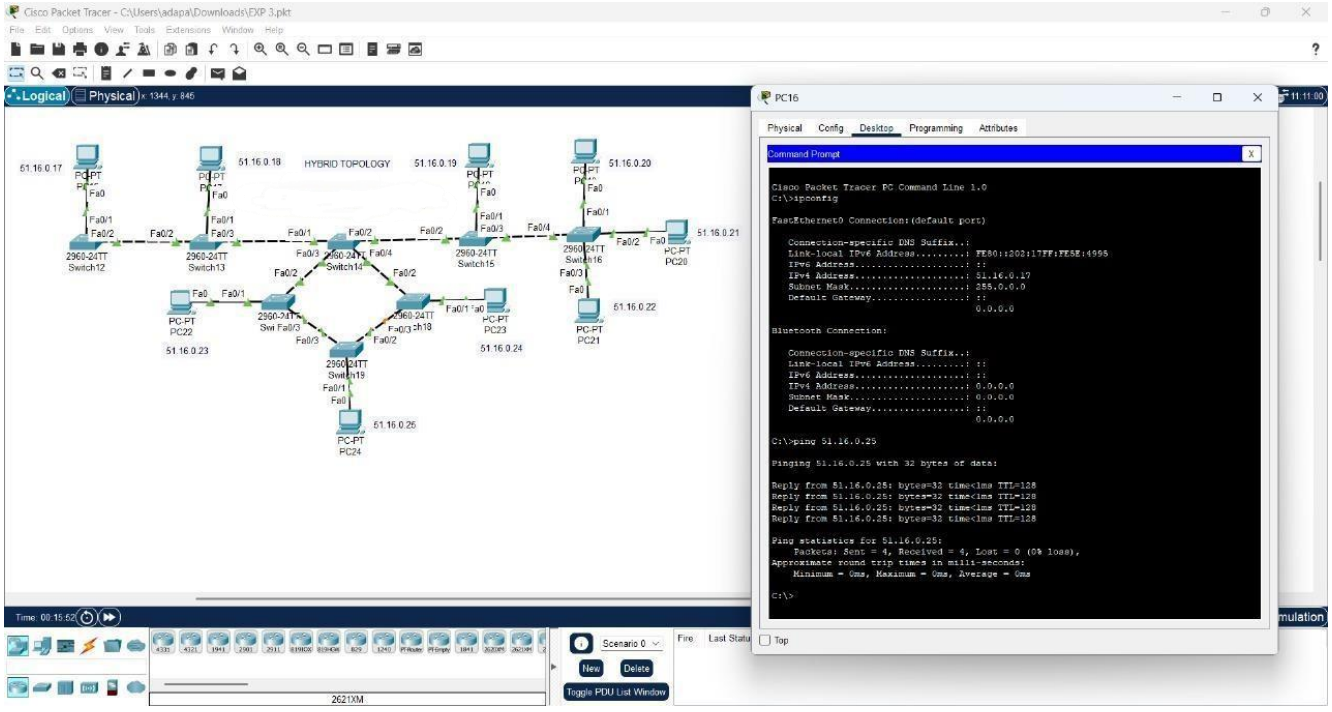


FIG: PING

CONCLUSION (provide conclusion about this experiment):

Successfully designed and implemented network topologies using Cisco Packet Tracer

Rubrics for Experiment Assessment:

Rubrics	Good	Normal	Poor	Marks
Creation of Topology (4)	Created the topology, Identify the proper devices and making the connections **(4)**	Created the topology, Identify the proper devices, making the connections But missing some features **(3)**	Created wrong topology, Failed to Identify the proper devices and making connections **(1)**	
Verify the connectivity (4)	Verified the connectivity in all the levels **(4)**	Verified the connectivity at some levels (only some nodes) **(2)**	Verified the connectivity is not done. **(1)**	
Timely Completion (2)	Completed the lab before the allotted time **(2)**	Completed the lab after the deadline **(1)**	Did not submitted before grading **(0)**	
			Total	

Register No:	**99220041065**
Name	**DESU SIVA NAGA SATYA SAI**
Section/Slot	**S12/Slot-03**
Ex.No:	**6a**
Date of Submission	
Name of the Experiment	**Configuration of Inter VLAN network using L3 switch**

Objective(s):

To design and implement Inter VLAN using switch configuration

Introduction:

Normally, Routers are used to divide the broadcast domain and switches (at layer 2) Operate in a single broadcast domain but Switches can also divide the broadcast domain by using the concept of **VLAN (Virtual LAN)**.

VLAN is the logical grouping of devices in the same or different broadcast domains. By default, all the switch ports are in VLAN 1. As the single broadcast domain is divided into multiple broadcast domains, Routers or layer 3 switches are used for intercommunication between the different VLANs.The process of intercommunication of the different Vlans is known as Inter Vlan Routing (IVR).

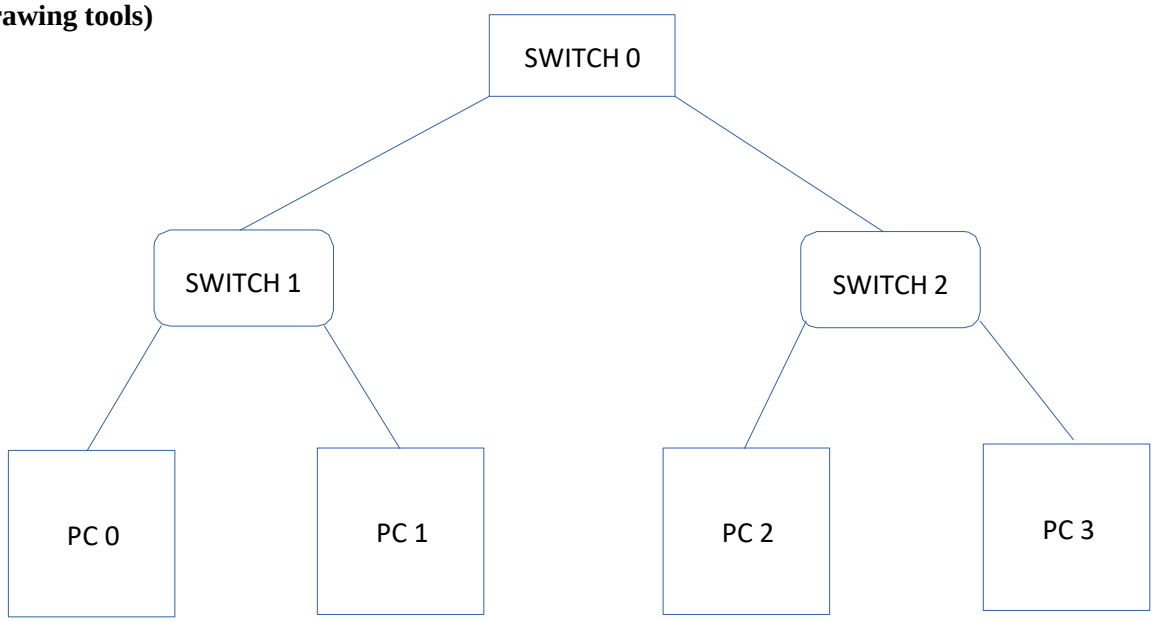
Suppose we have made 2 logical groups of devices (VLAN) named sales and finance. If a device in the sales department wants to communicate with a device in the finance department, inter-VLAN routing has to be performed. These can be performed by either router or layer 3 switches.

Switch Virtual Interface (SVI): SVI is a logical interface on a multilayer switch that provides layer 3 processing for packets to all switch ports associated with that VLAN. A single SVI can be created for a VLAN. SVI on the layer 3 switch provides both management and routing services while SVI on layer 2 switch provides only management services like creating VLANs or telnet/SSH services.

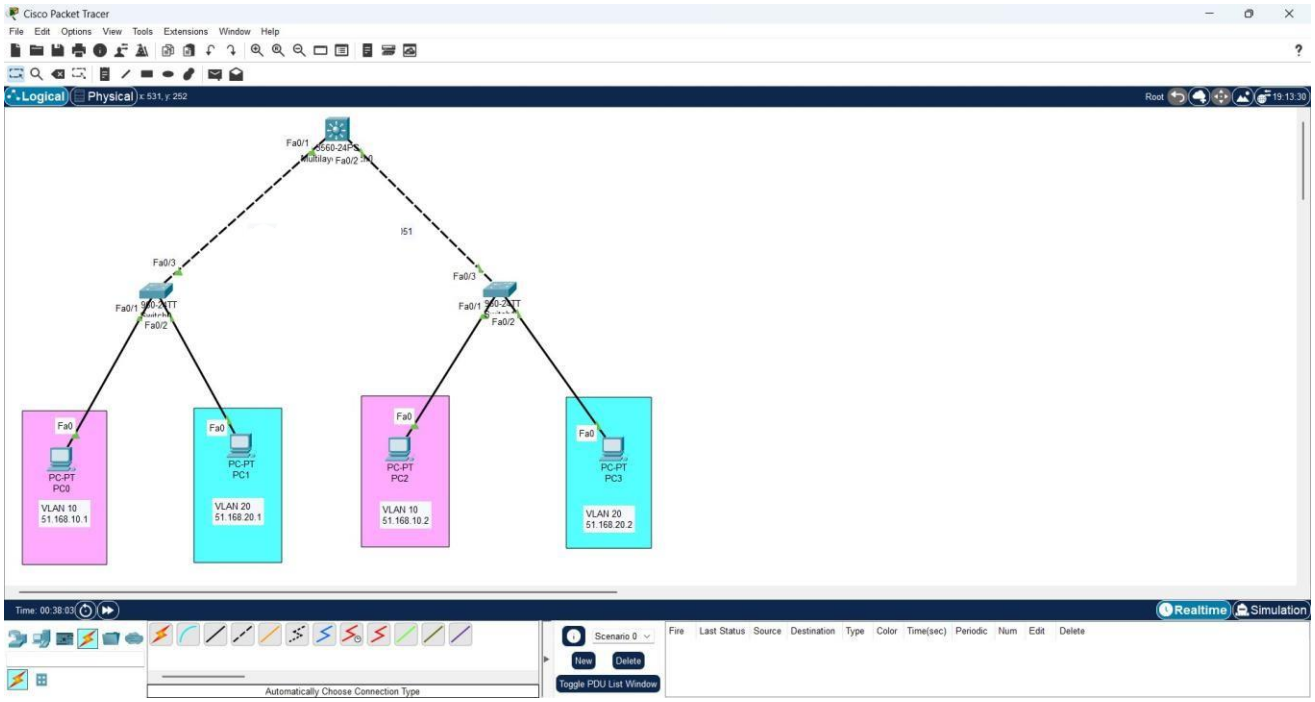
Process of Inter Vlan Routing by Layer 3 Switch: The SVI created for the respective VLAN acts as a default gateway for that VLAN just like the sub-interface of the router (in the process of Router On a stick). If the packet is to be delivered to different VLANs i.e inter VLAN Routing is to be performed on the layer 3 switch then first the packet is delivered to the layer 3 switch and then to the destination just like in the process of the router on a stick.

1. **Device Requirements:**
   1. PC's
   2. Switches(2960-24TT,3650-24PS)
   3. Copper stand through cable
   4. Copper cross wire cable

2. **Network Diagram for your experiment (draw the diagram either hand drawing/ms paint or any other drawing tools)**



3. **Network Diagram (Packet Tracer diagram before configuration):**



4. **Configuration details:**

Device Name	Interface Name	IP Address	Subnet mask
Multilayer SWITCH			
Switch 0			
PC0	fa0/1	51.168.10.1	255.0.0.0
PC1	fa0/2	51.168.10.2	255.0.0.0

Switch 1			
PC2	fa0/1	51.168.20.1	255.0.0.0
PC3	fa0/2	51.168.20.2	255.0.0.0

5. Describe step by step configuration steps properly:

1. Create VLANs:

Multilayer Switch0	**Switch0**	**Switch1**
enable	enable	enable
configure terminal	configure terminal	configure terminal
vlan 10	vlan 10	vlan 10
vlan 20	exit	exit
exit	vlan 20	vlan 20
	exit	exit

2. Configure interfaces:

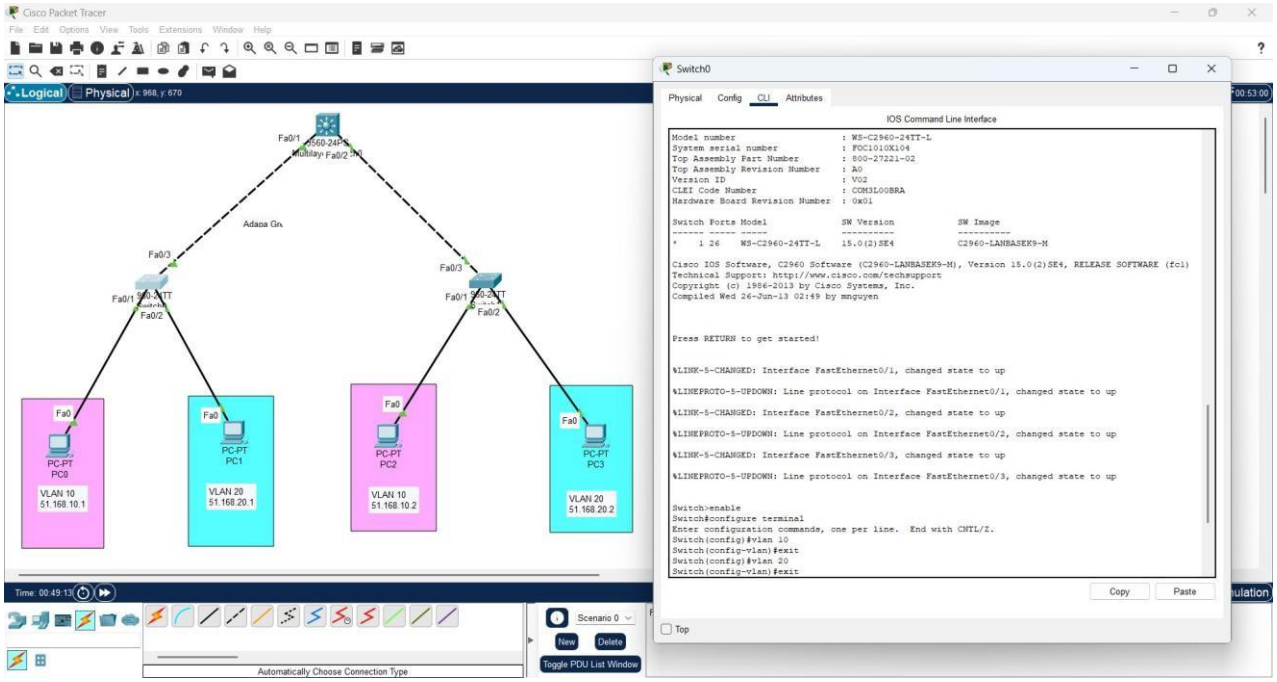
Switch0	**Switch1**
interface fastethernet0/1	interface fastethernet0/1
switchport mode access	switchport mode access
switchport access vlan 10	switchport access vlan 10
exit	exit
interface fastethernet0/2	interface fastethernet0/2
switchport mode access	switchport mode access
switchport access vlan 10	switchport access vlan 10
exit	exit

3. Configure trunking:

Multilayer switch0

interface ethernet0/1	interface vlan 10
switchport trunk encapsulation dot1q	ip address 51.168.10.100 255.255.255.0
switchport mode trunk	no shut
access	interface vlan 20
exit	ip address 51.168.20.100 255.255.255.0
ip routing	no shut

6. Output Diagram :



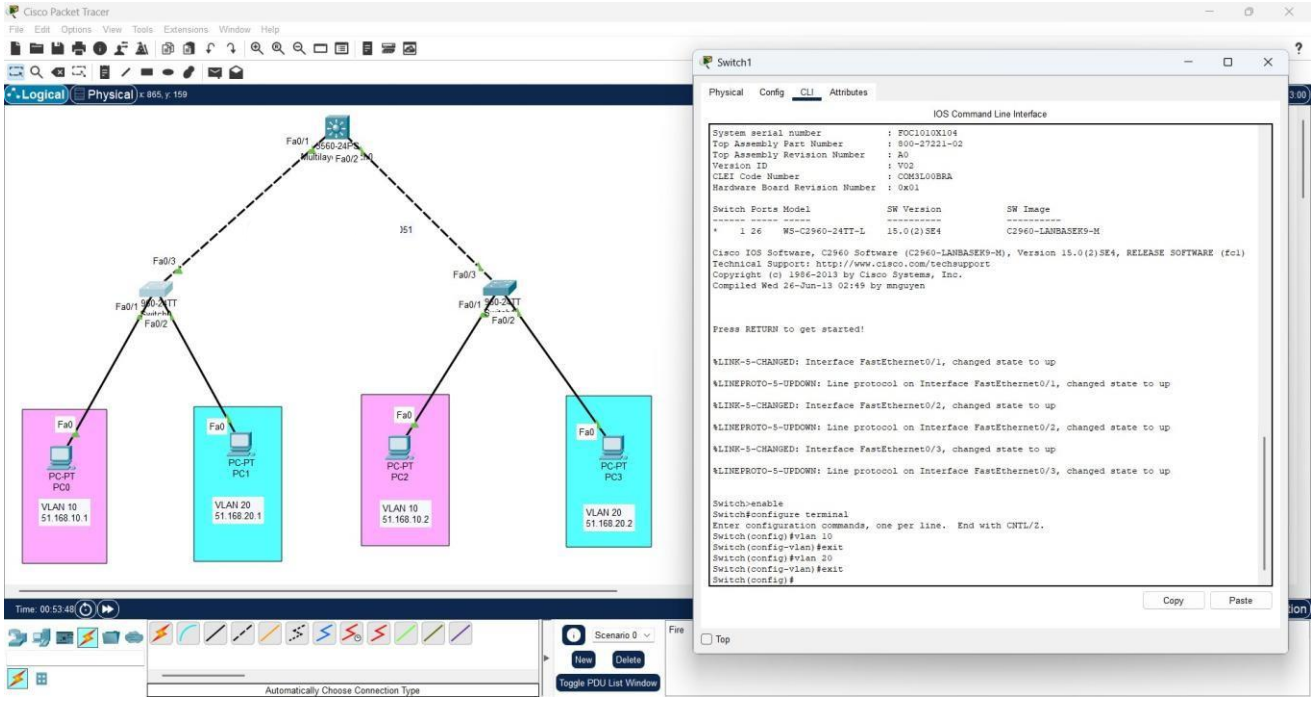
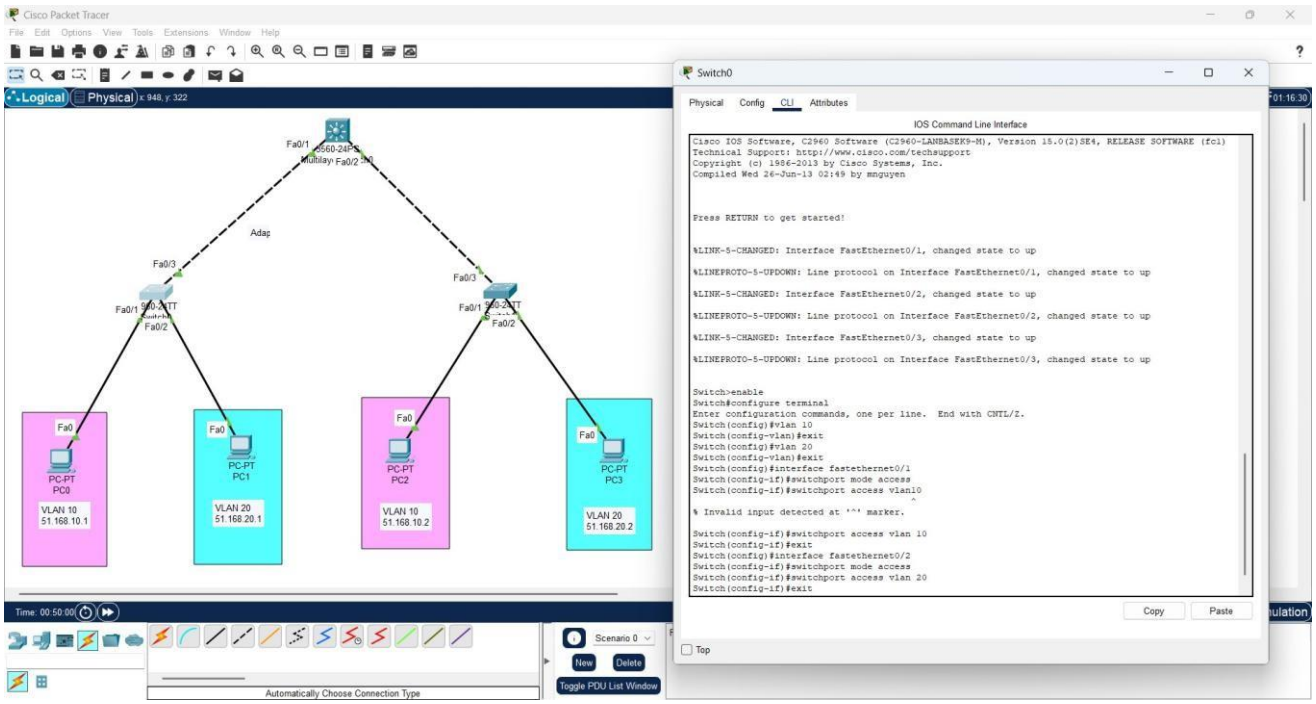


FIG: Creating VLAN'S in switch0 & switch1



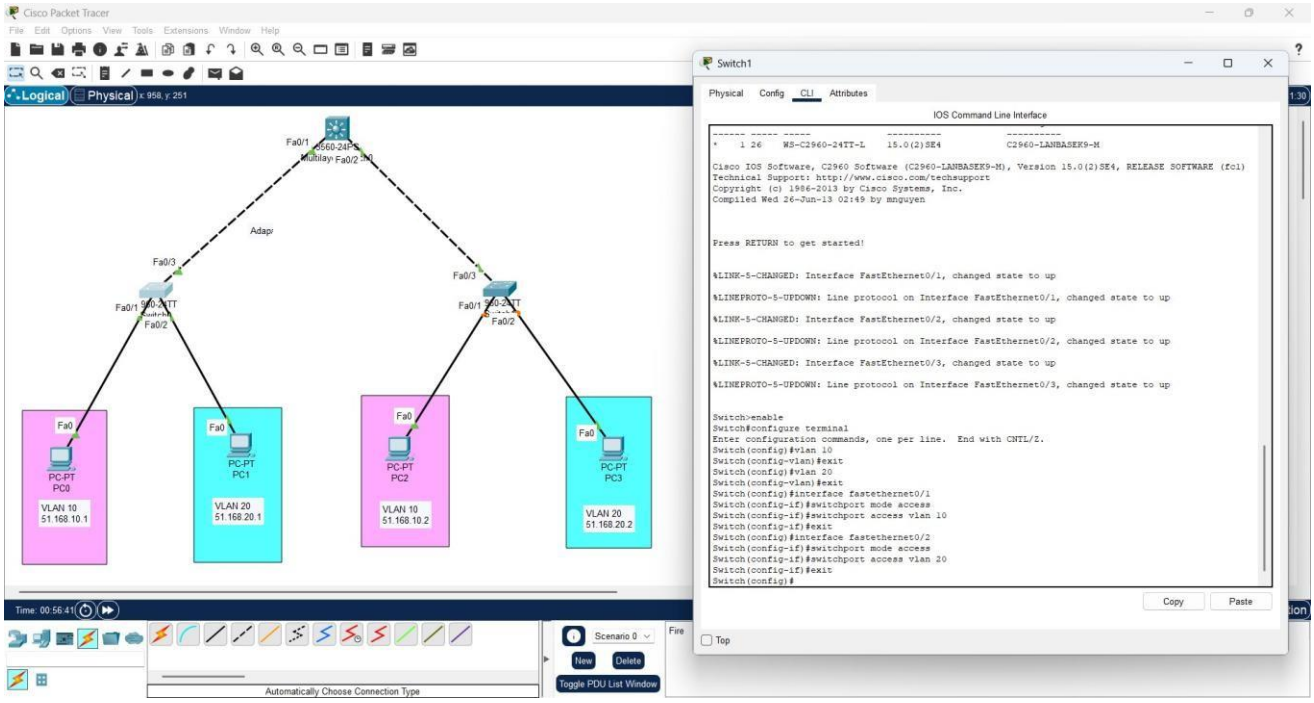
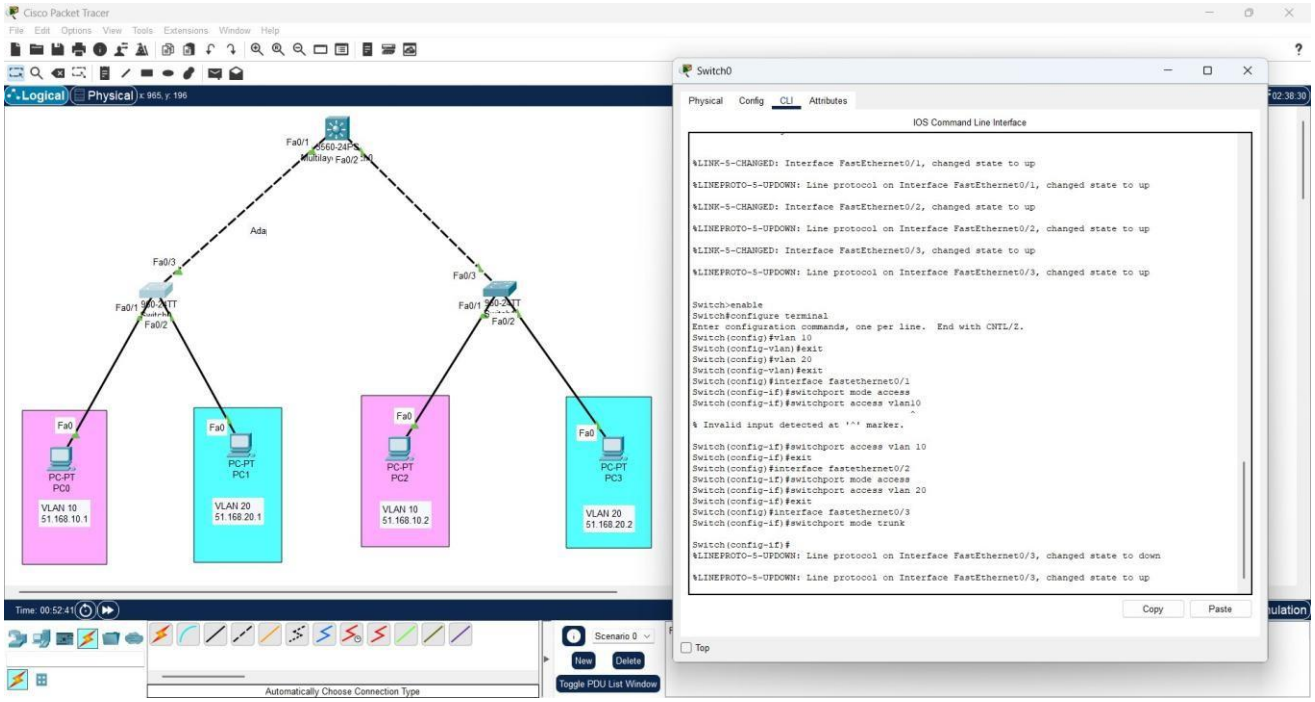


FIG: Configure interfaces in switch0 & switch1



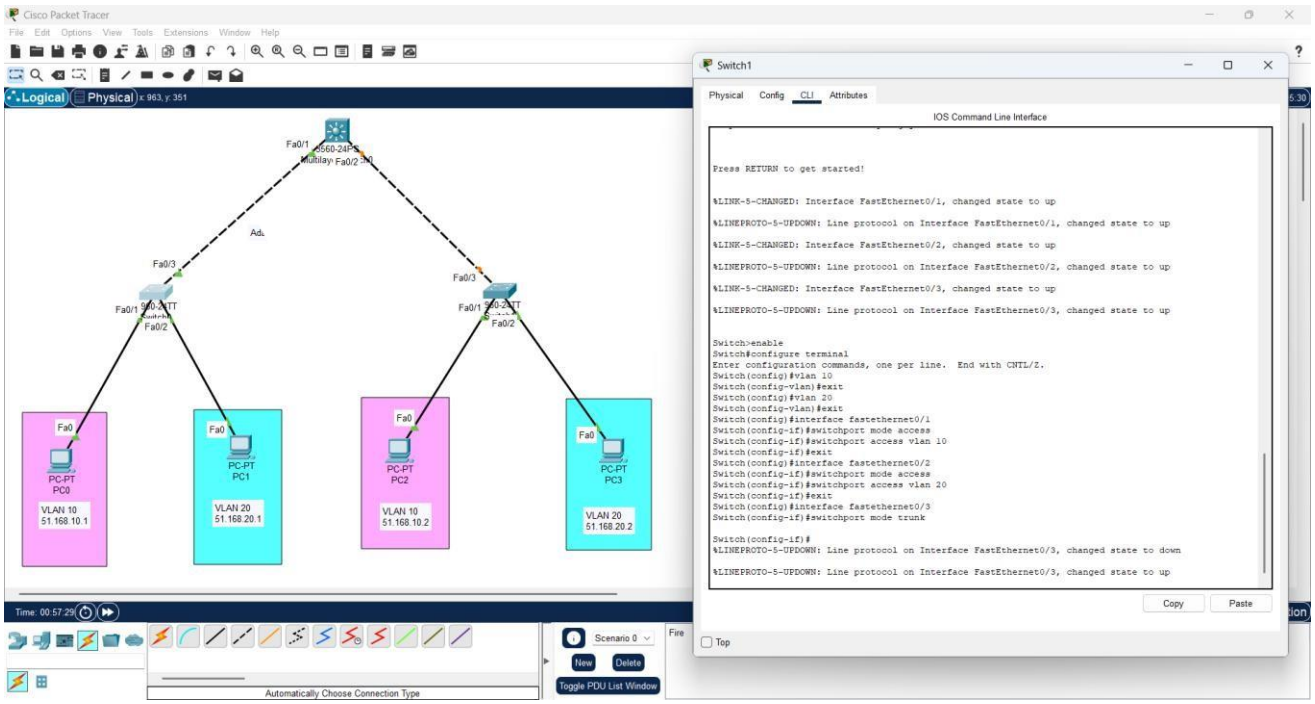


FIG: Configure trunking in switch0 & switch1

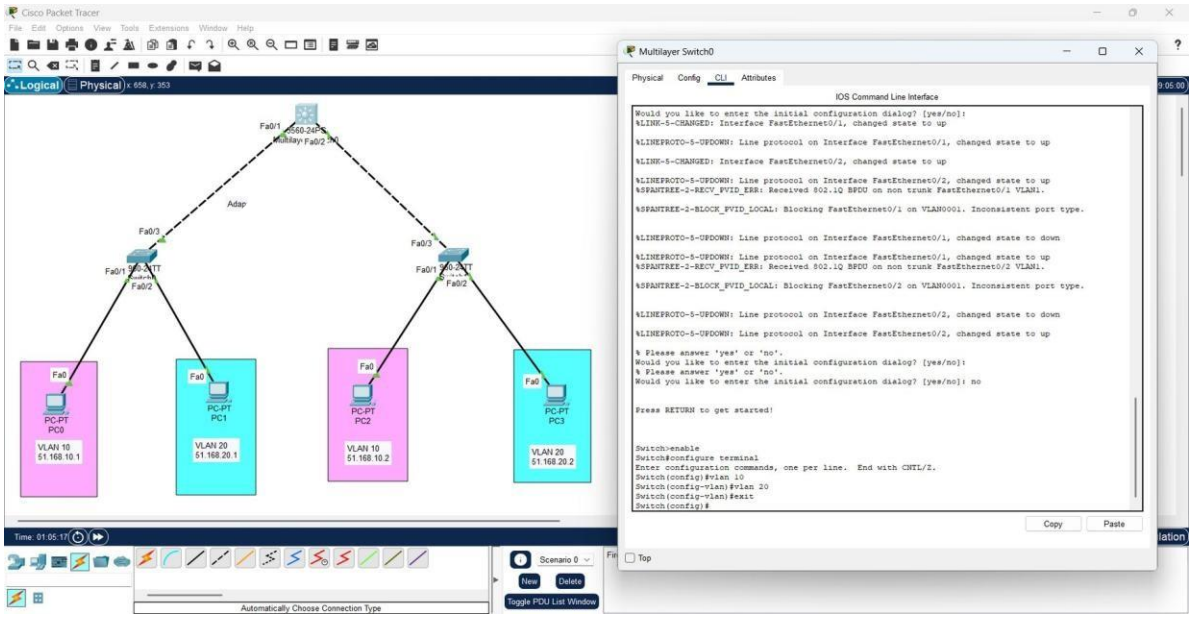


FIG:Creating Vlan's in multilayer switch0

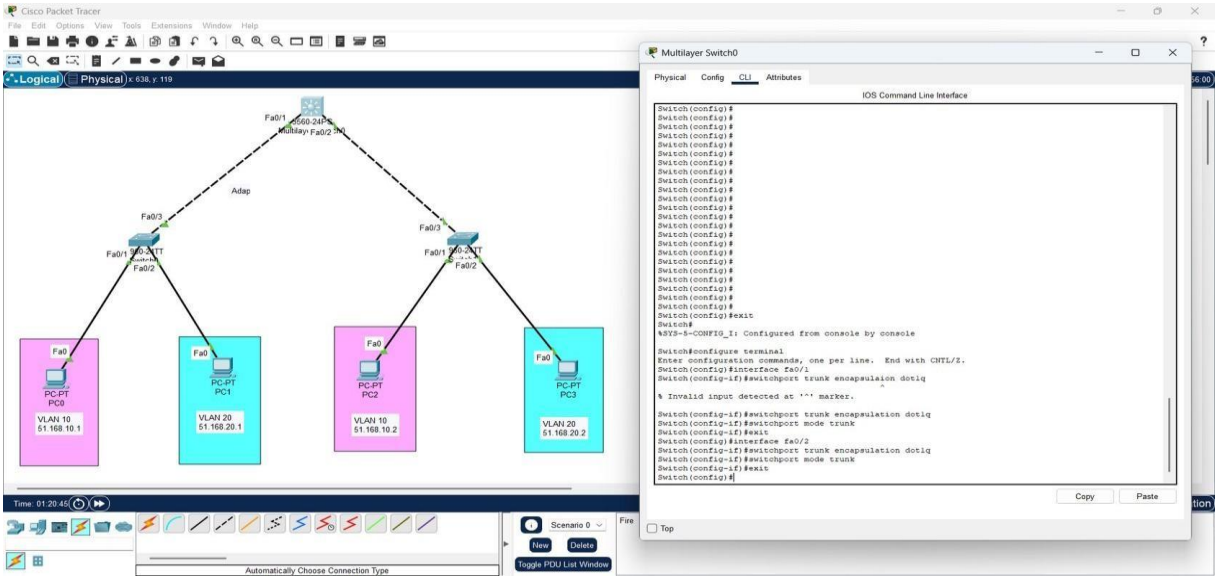


FIG: Configure interfaces in multilayer switch0

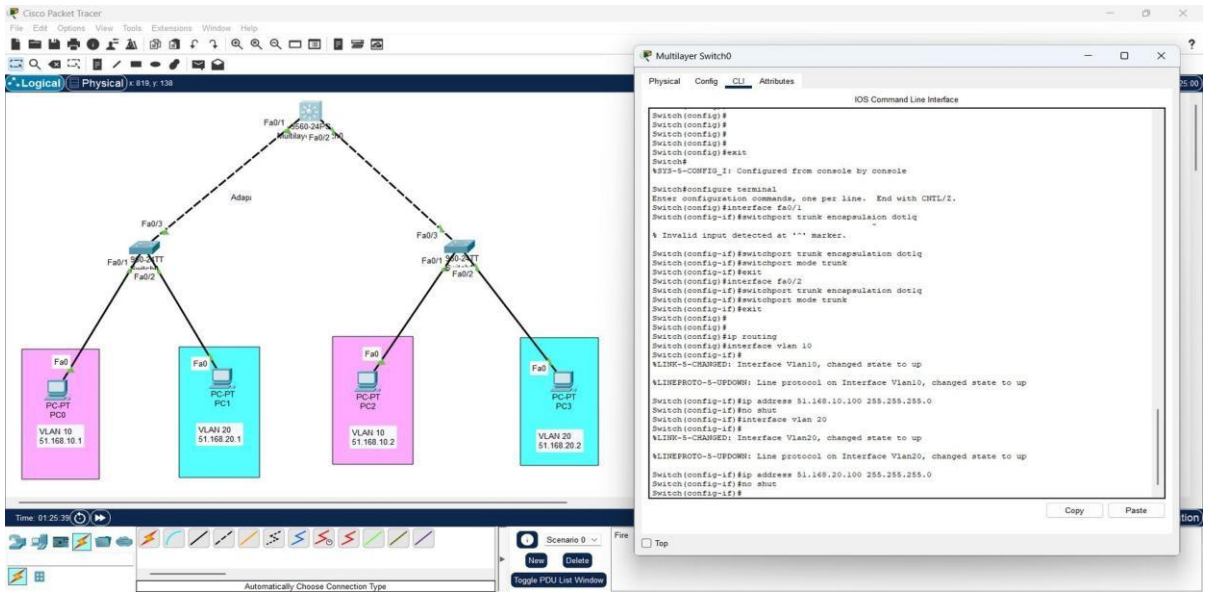
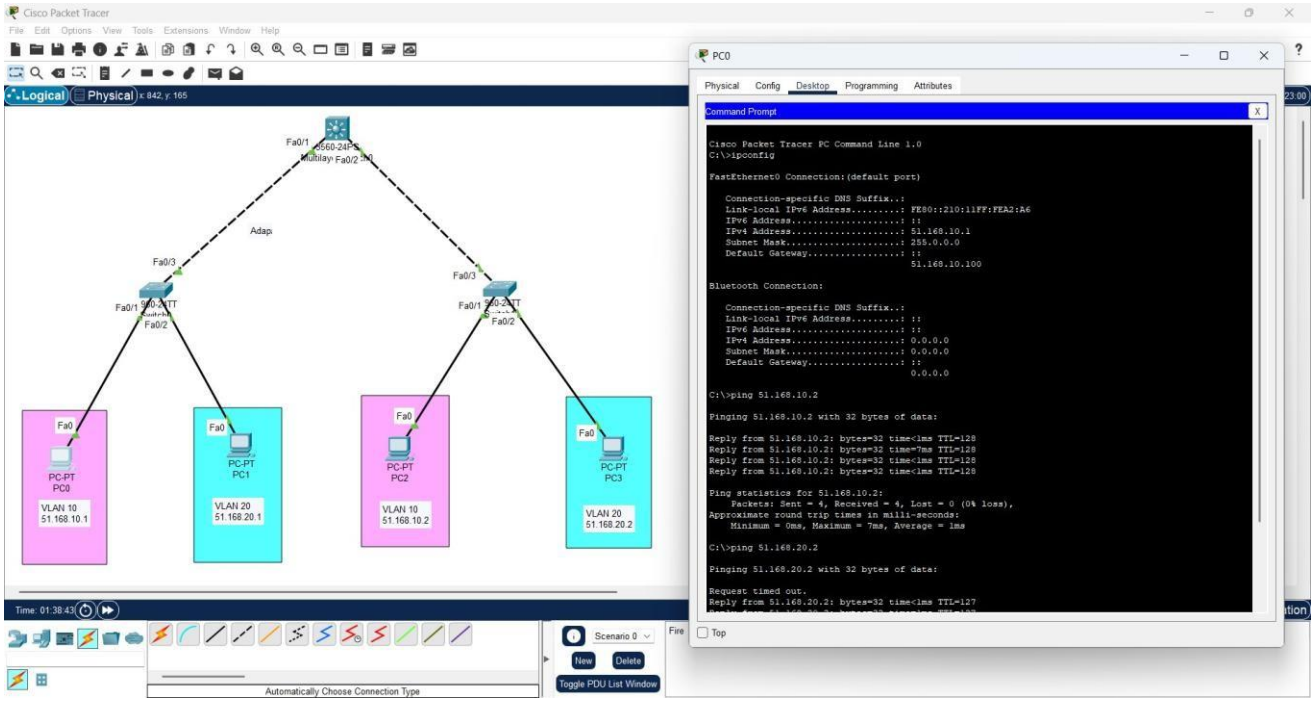


FIG: Configure trunking in multilayer switch0



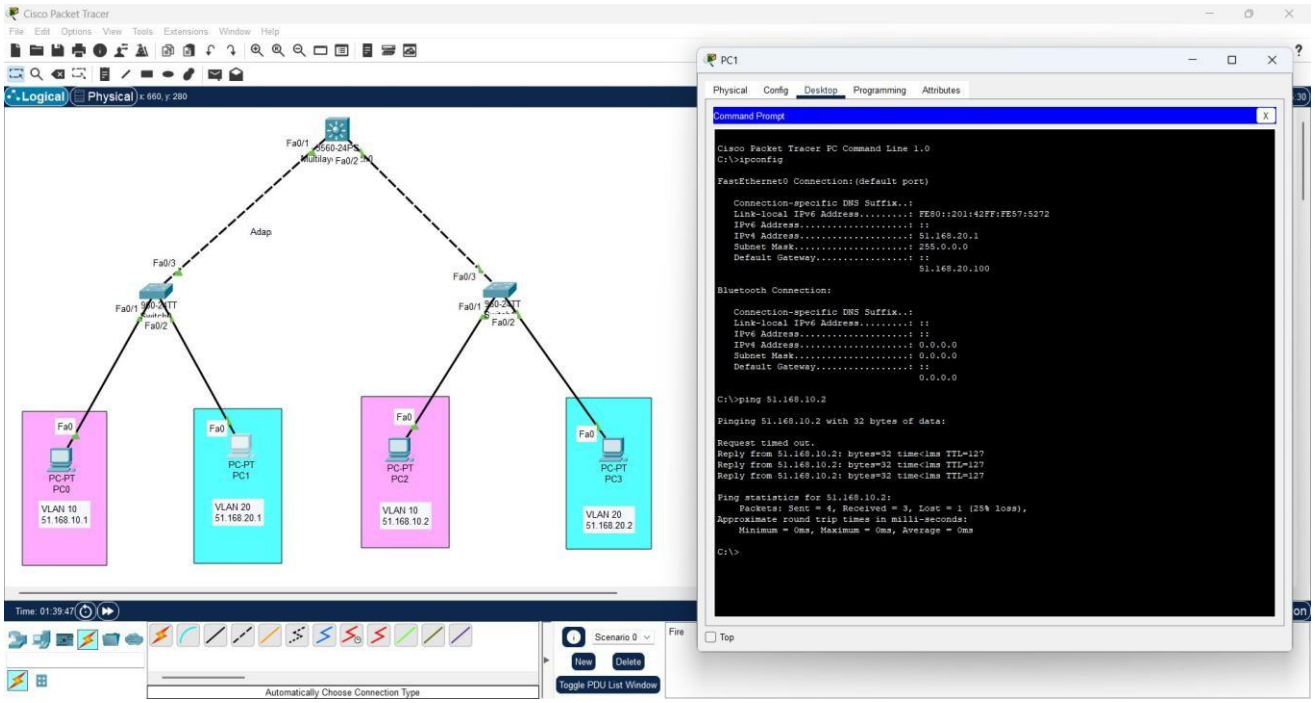


FIG: PING COMMAND

CONCLUSION :

Successfully designed and implemented Inter VLAN using switch configuration.

Rubrics for Experiment Assessment:

Rubrics	Good	Normal	Poor	Marks
Creation of Topology (4)	Created the topology, Identify the proper devices and making the connections **(4)**	Created the topology, Identify the proper devices, making the connections But missing some features **(3)**	Created wrong topology, Failed to Identify the proper devices and making connections **(1)**	
Verify the connectivity (4)	Verified the connectivity in all the levels **(4)**	Verified the connectivity at some levels (only some nodes) **(2)**	Verified the connectivity is not done. **(1)**	
Timely Completion (2)	Completed the lab before the allotted time **(2)**	Completed the lab after the deadline **(1)**	Did not submitted before grading **(0)**	
			Total	

Register No:	**99220041065**
Name	**DESU SIVA NAGA SATYA SAI**
Section/Slot	**S12 & Slot-03**
EXP NO:	**6b**
Date of Submission	
Name of the Experiment	**Configuration of Inter VLAN using Router**

Objective(s):

To design and implement Inter VLAN using switch configuration

Introduction:

'Router on a Stick' allows routing between VLANs with only one interface. Each VLAN represents a different Subnet. In general, routers can take traffic from only one subnet and transfer it to another subnet. And we can assign only one IP Address to a router interface. 'Router on a stick' allow us to create sub-interfaces, and assign IP Addresses to those sub-interfaces. To make it work, we have to create a truck connection between the switch and a router so that traffic from multiple VLANs can be sent to the router.

If we create a route between VLANs without the 'Router on a Stick' method, then we have to waste interfaces on the switches and routers. And if we enable routing between multiple VLANs then it will become practically inefficient as the switches and the routers will use those multiple interfaces.

Here we use an alternative method for allowing routing between VLANs. we are using two interfaces on both the router and a switch to allow routing between VLANs. We have not created sub-interface.

You can see that we have to use extra interfaces for each VLAN. So, it becomes practically non-efficient if we have multiple VLANs. Hence, 'Router on a Stick' is a perfect solution for routing between VLANs with just one router interface.

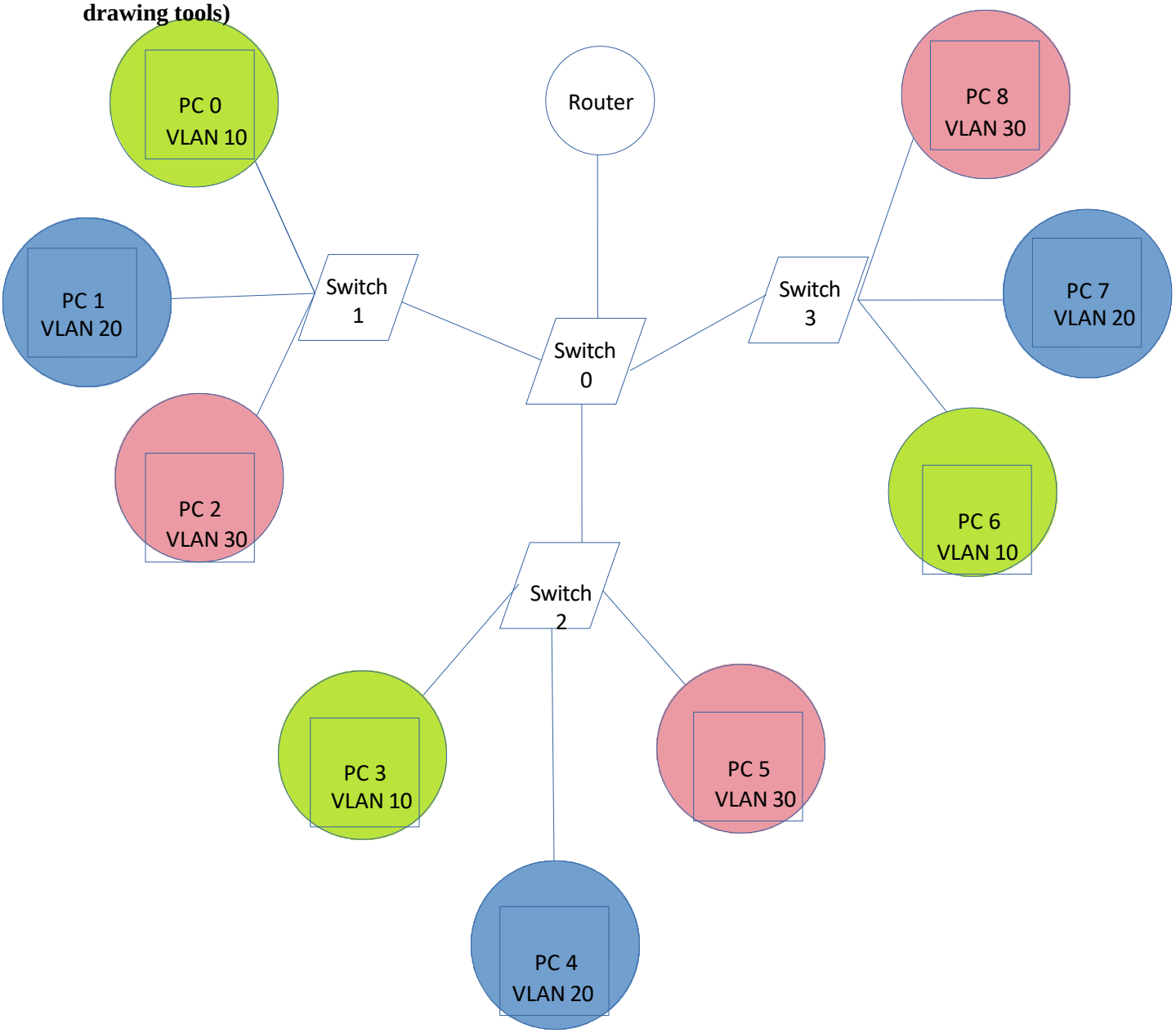
The more simple way to do routing between VLANs is by using a Layer 3 Switch. We just have to create virtual interfaces for each VLAN and assign them IP Addresses from the same network. A Layer 3 Switch will then enable routing between VLANs as it has routing capabilities as well. However, Layer 3 Switch is quite expensive so it might not be an affordable option for small office networks.

In the below lab, we will configure 'Router on a Stick' that would allow routing between the VLANs. Some of the important concepts in this lab are – to create sub-interfaces, use encapsulation dot1Q command to encapsulate the traffic, and mentioning the VLAN number to ascertain that for which VLAN the sub-interface should respond.

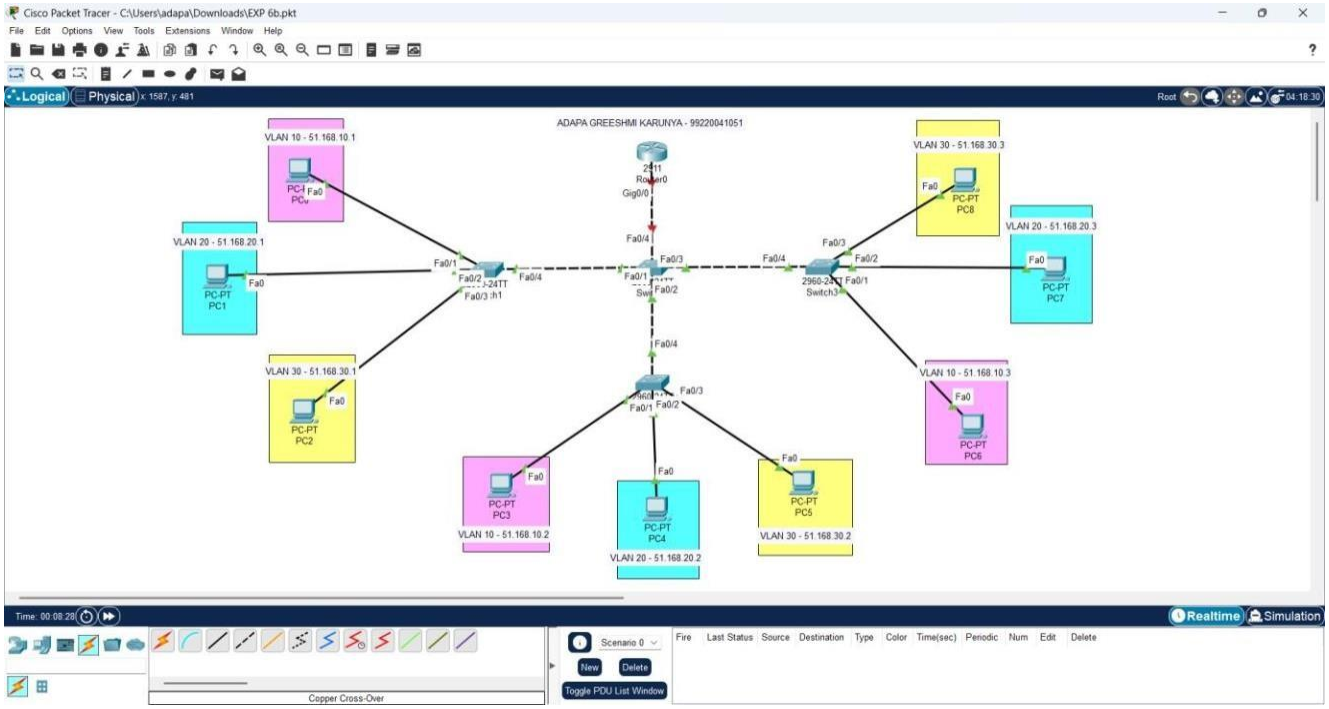
1. Device Requirements:

1. PC's
2. Switches
3. Router
4. Copper stand through cable
5. Copper cross wire cable

2. Network Diagram for your experiment (draw the diagram either hand drawing/ms paint or any other drawing tools)



3. Network Diagram (Packet tracer diagram before configuration):



4. Configuration details:

Device Name	Interface Name	IP Address	Subnet mask
Switch1			
PC0	fa0/1	51.168.10.1	255.255.255.0
PC1	fa0/2	51.168.10.2	255.255.255.0
PC2	fa0/3	51.168.10.3	255.255.255.0
Switch2			
PC3	fa0/1	51.168.20.1	255.255.255.0
PC4	fa0/2	51.168.20.2	255.255.255.0
PC5	fa0/3	51.168.20.3	255.255.255.0
Switch3			
PC6	fa0/1	51.168.30.1	255.255.255.0
PC7	fa0/2	51.168.30.2	255.255.255.0
PC8	fa0/3	51.168.30.3	255.255.255.0

5. Describe step by step configuration steps properly :

1. Creating VLAN'S :

IN – SWITCH0,SWITCH1,SWITCH2,SWITCH3

- enable
- configure terminal
- vlan10
- vlan20
- vlan 30
- exit
- show vlan

2. Configure interfaces:

IN – SWITCH1,SWITCH2,SWITCH3

• interface fa0/1	interface fa0/2	interface fa0/3
• switchport mode access	switchport mode access	switchport mode access
• switchport access vlan 10	switchport access vlan 20	switchport access vlan 30
• exit	exit	exit

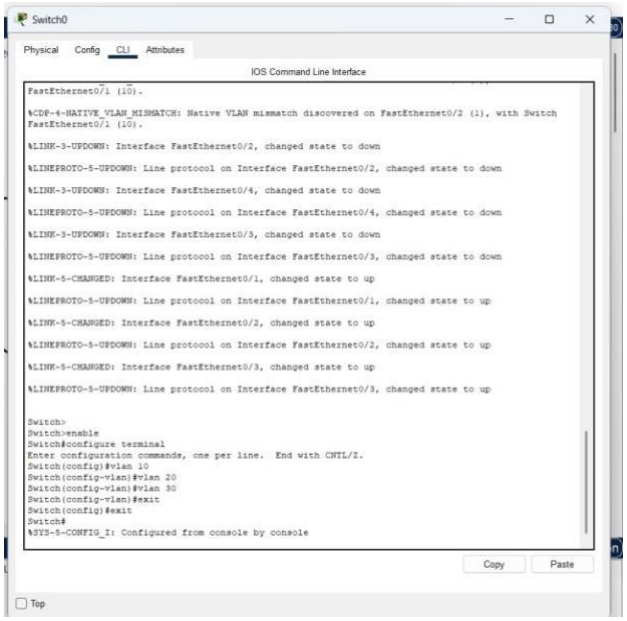
3. Configure trunking:

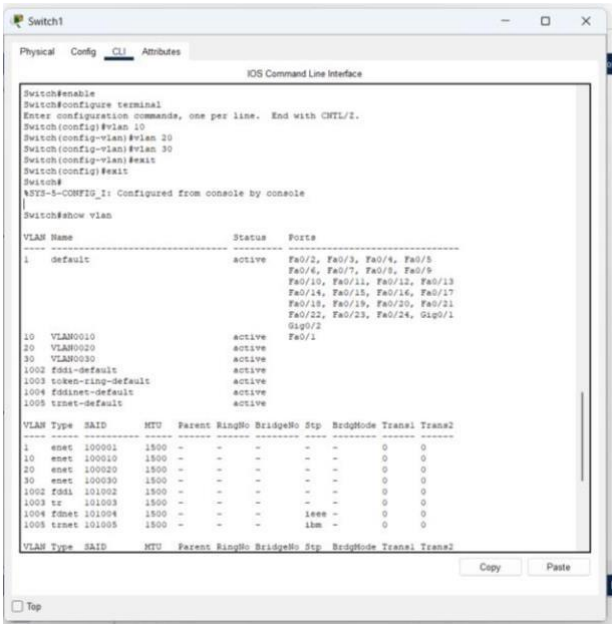
- **IN – SWITCH0:**
- interface range fa0/1-3
- switchport mode trunk
- exit
- show interfaces trunk
- **IN ROUTER:**

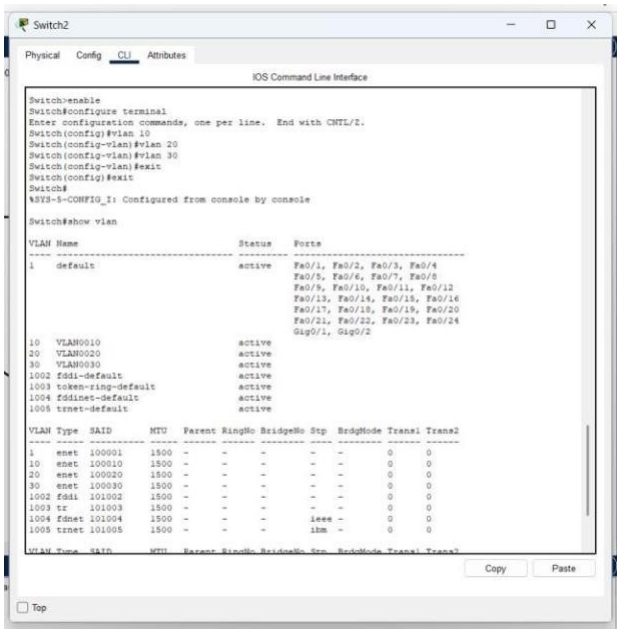
• interface gigabitEthernet 0/0.10	interface gigabitEthernet 0/0.20
• encapsulation dot1Q 10	encapsulation dot1Q 20
• ip address 51.168.10.100 255.255.255.0	ip address 51.168.20.100 255.255.255.0
• exit	exit

- interface gigabitEthernet 0/0.30
- encapsulation dot1Q 30
- ip address 51.168.30.100 255.255.255.0
- exit

6. Output Diagram :







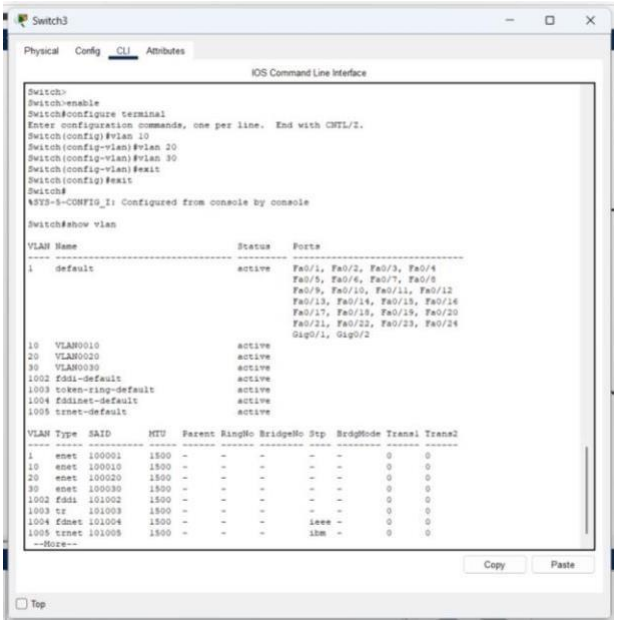
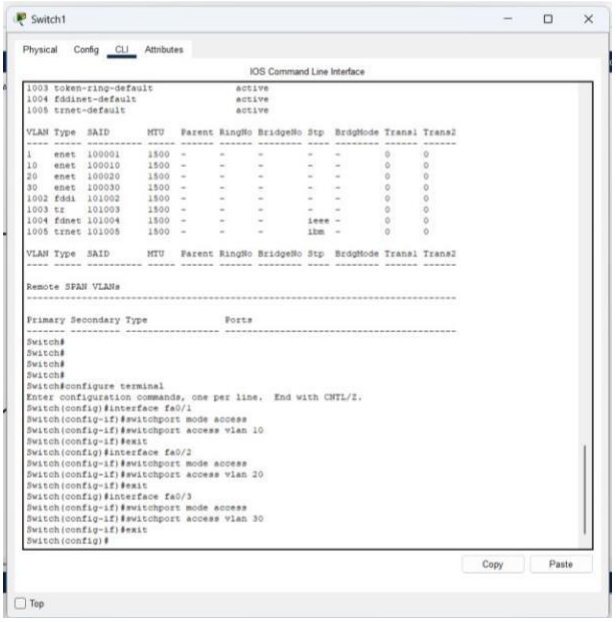
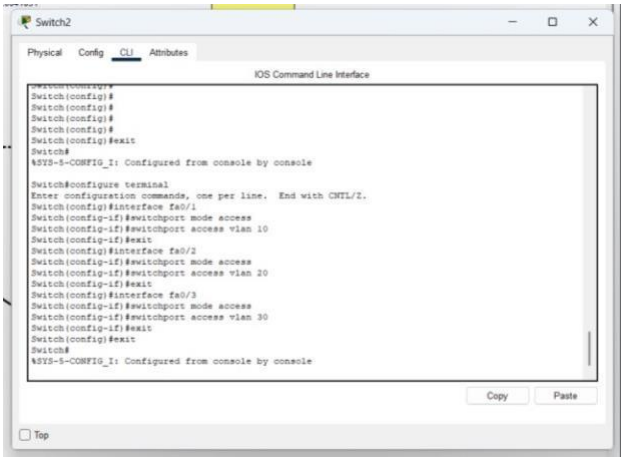


FIG: CREATING VLAN'S





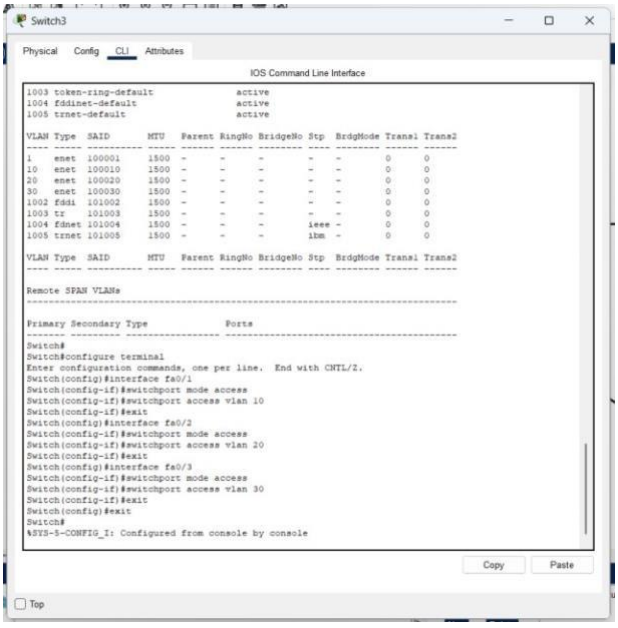
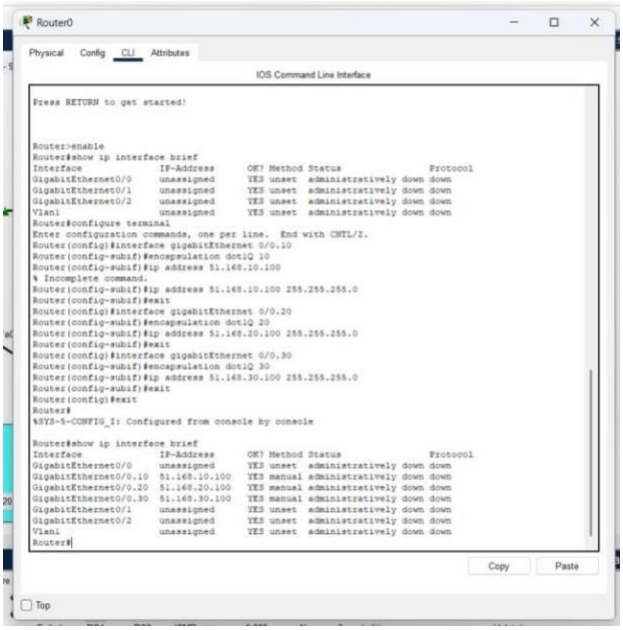
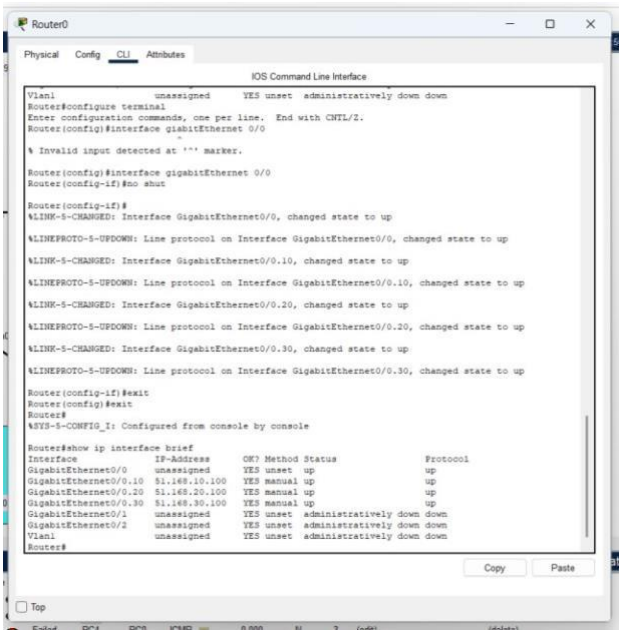
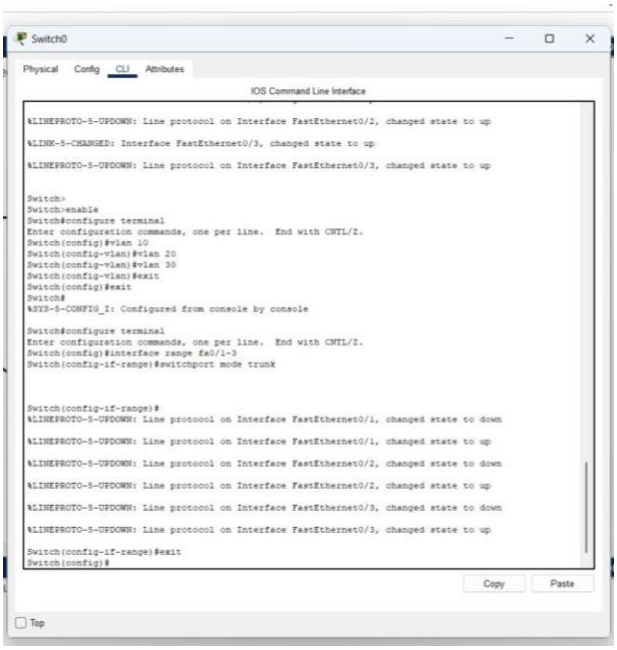


FIG: CONFIGURE INTERFACES







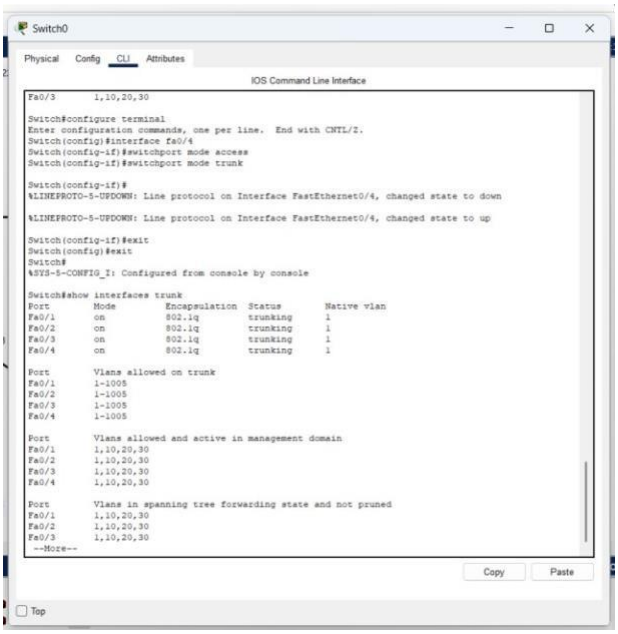


FIG: CONFIGURE TRUNKING

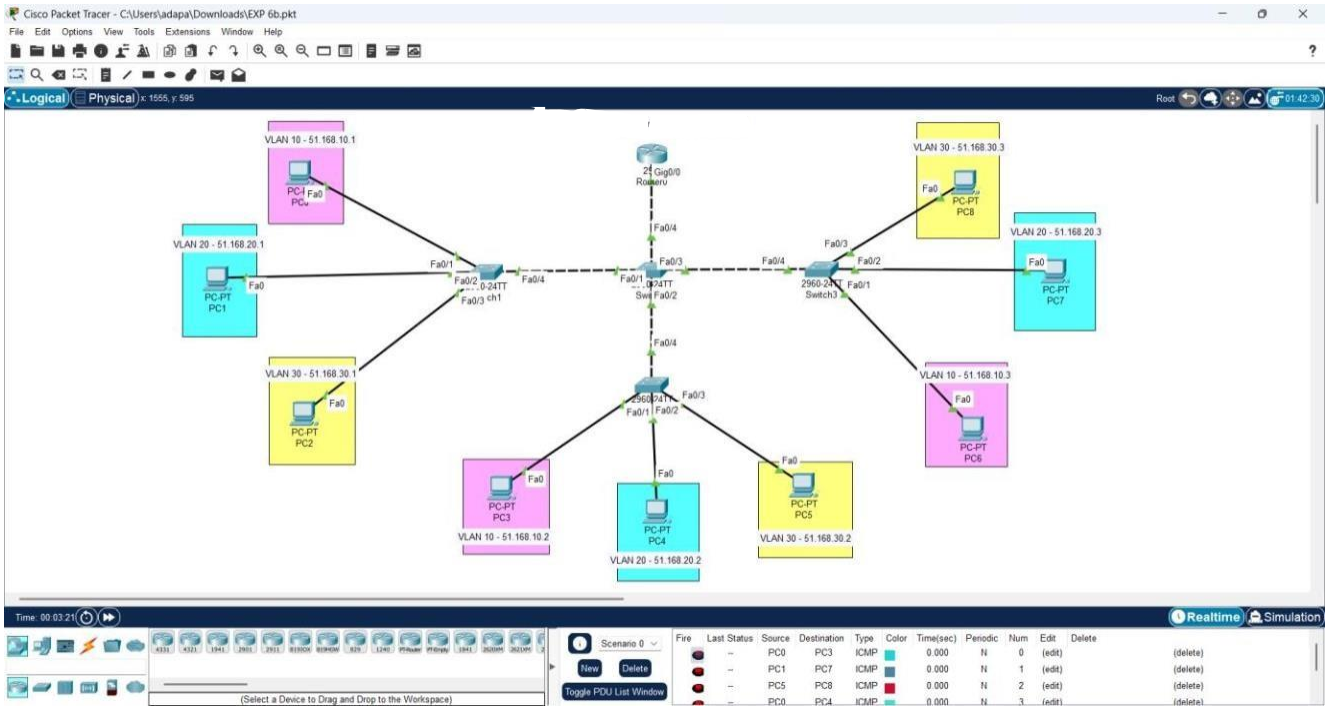


FIG: NETWORK DIAGRAM AFTER CONFIGURATION

CONCLUSION (provide conclusion about this experiment):

Successfully designed and implemented Inter VLAN using switch configuration.

Rubrics for Experiment Assessment:

Rubrics	Good	Normal	Poor	Marks
Creation of Topology (4)	Created the topology, Identify the proper devices and making the connections **(4)**	Created the topology, Identify the proper devices, making the connections But missing some features **(3)**	Created wrong topology, Failed to Identify the proper devices and making connections **(1)**	
Verify the connectivity (4)	Verified the connectivity in all the levels **(4)**	Verified the connectivity at some levels (only some nodes) **(2)**	Verified the connectivity is not done. **(1)**	
Timely Completion (2)	Completed the lab before the allotted time **(2)**	Completed the lab after the deadline **(1)**	Did not submitted before grading **(0)**	
			Total	

Register No:	**99220041762**
Name:	**G.ASISH**
Class/Section:	**S18/8301A**
Ex.No:	**9**
Name of the Experiment	DHCP CONFIGURATION
Google Drive link of the packet tracer file (give view permission):	**https://drive.google.com/drive/folders/1kZYMTJ0uZatmg4XpevUQnRGjCA_W4BOF**

Objective(s):

To design and implement DHCP configuration using packet tracer

Introduction:

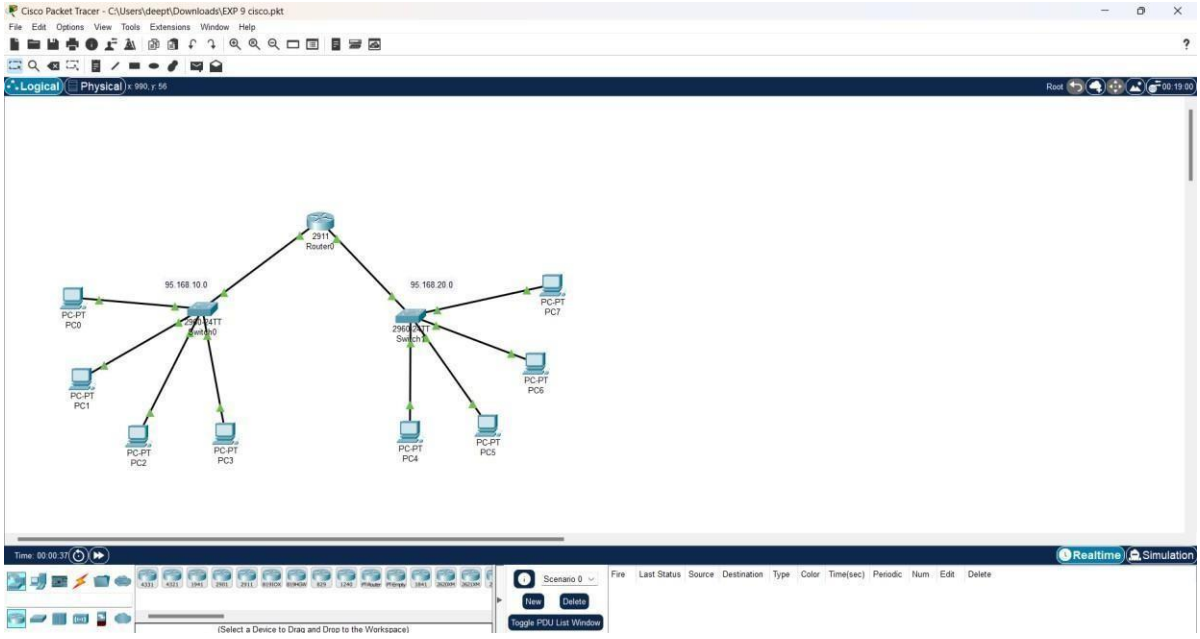
Dynamic Host Configuration Protocol or DHCP is a networking protocol that allows for the automatic assignment of IP addresses to devices in a network. You have probably seen DHCP in action at the most basic level when you connect your laptop to an ISP router (like MTN-HynetFlex) or your phone's hotspot. Every new device that joins the Wifi network will get a local IP address, usually in the range 192.168.0.* or 172.16.*.* where * is a number between 0 and 255.

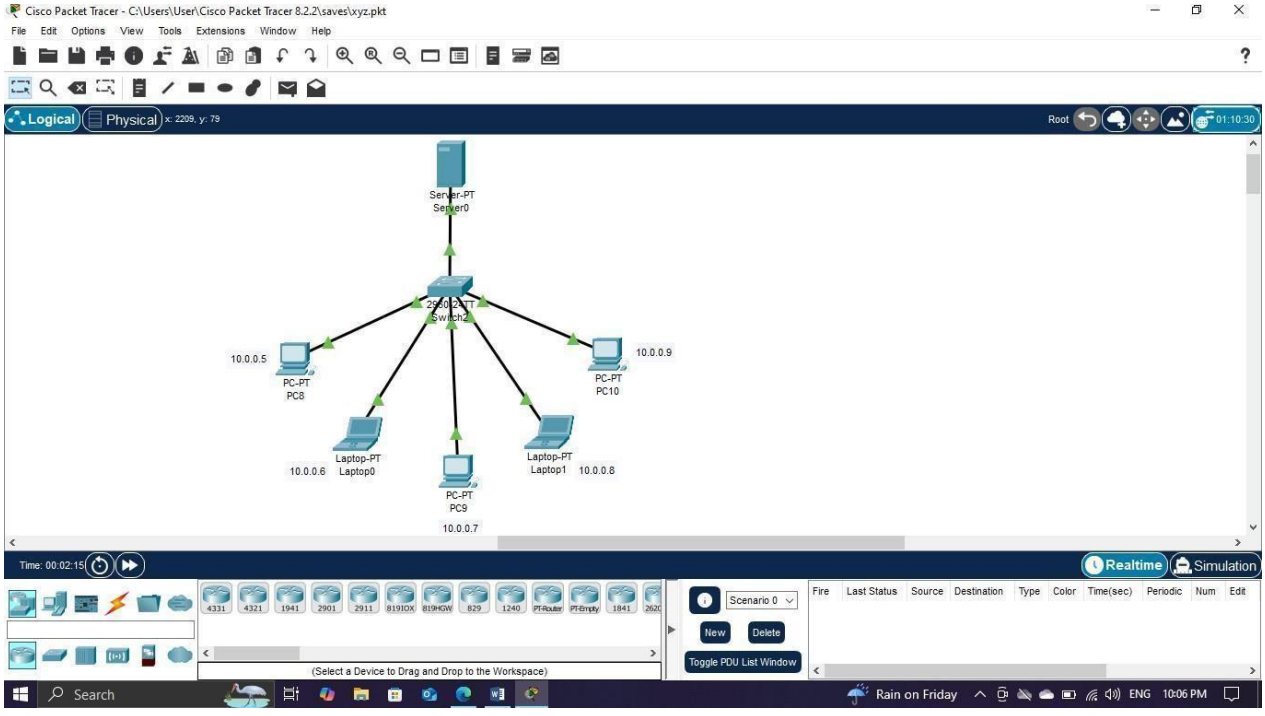
Without DHCP, these massive networks will require physical agents in call centers to manage who gets what IP address. While this is not only a hassle, it will be a huge cost to the service provider.

One easy way to practice a DHCP setup is in a local network simulation environment like Cisco Packet Tracer. This lab will discuss how to configure DHCP on a router for a simple 4-computer, two-switch network. The router will assign the IP addresses to the computers in each network so that inter-network communication can happen.

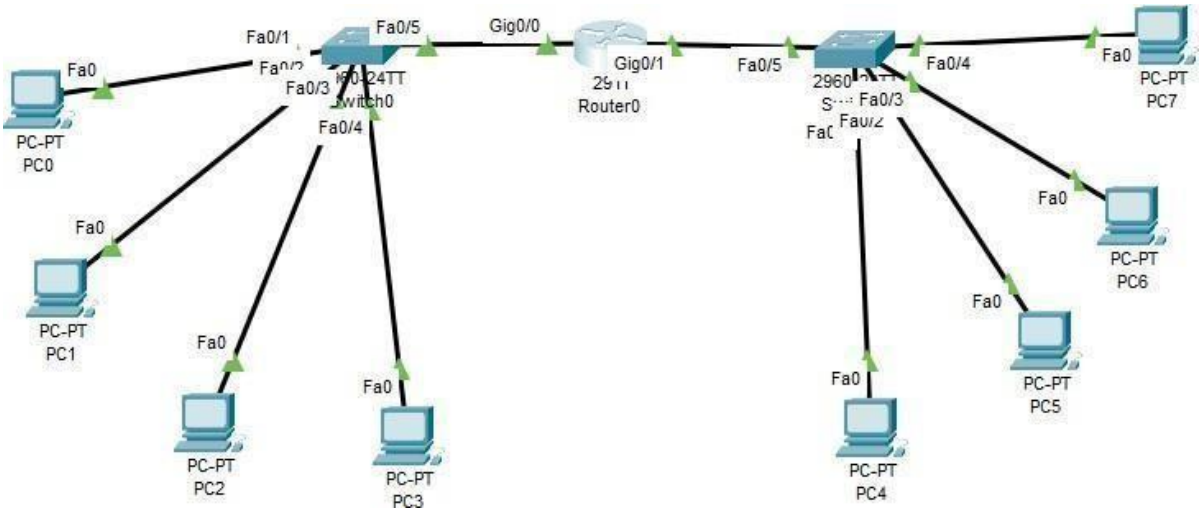
1. **Device Requirements:**
   1. PC’s
   2. Router
   3. Switches
   4. Connection wires

2. Network Diagram for your experiment (draw the diagram either hand drawing/ms paint or any other drawing tools)





3. Network Diagram (Packet tracer diagram before configuration):



4. Configuration details:

Device Name	Interface Name	IP Address	Subnet mask	Default Gateway
PC0	Fa 0 : Fa 0/1	47.0.0.1	255.0.0.0	47.168.10.1
PC1	Fa 0 : Fa 0/2	47.0.0.2	255.0.0.0	47.168.10.1
PC2	Fa 0 : Fa 0/3	47.0.0.9	255.0.0.0	47.168.10.1
PC3	Fa 0 : Fa 0/4	47.0.0.10	255.0.0.0	47.168.10.1
Switch0				
Router0				
PC4	Fa 0 : Fa 0/2	46.0.0.2	255.0.0.0	46.168.20.1
PC5	Fa 0 : Fa 0/3	46.0.0.3	255.0.0.0	46.168.20.1
PC6	Fa 0 : Fa 0/4	46.0.0.1	255.0.0.0	46.168.20.1
PC7	Fa 0 : Fa 0/5	46.0.0.4	255.0.0.0	46.168.20.1
Switch1				

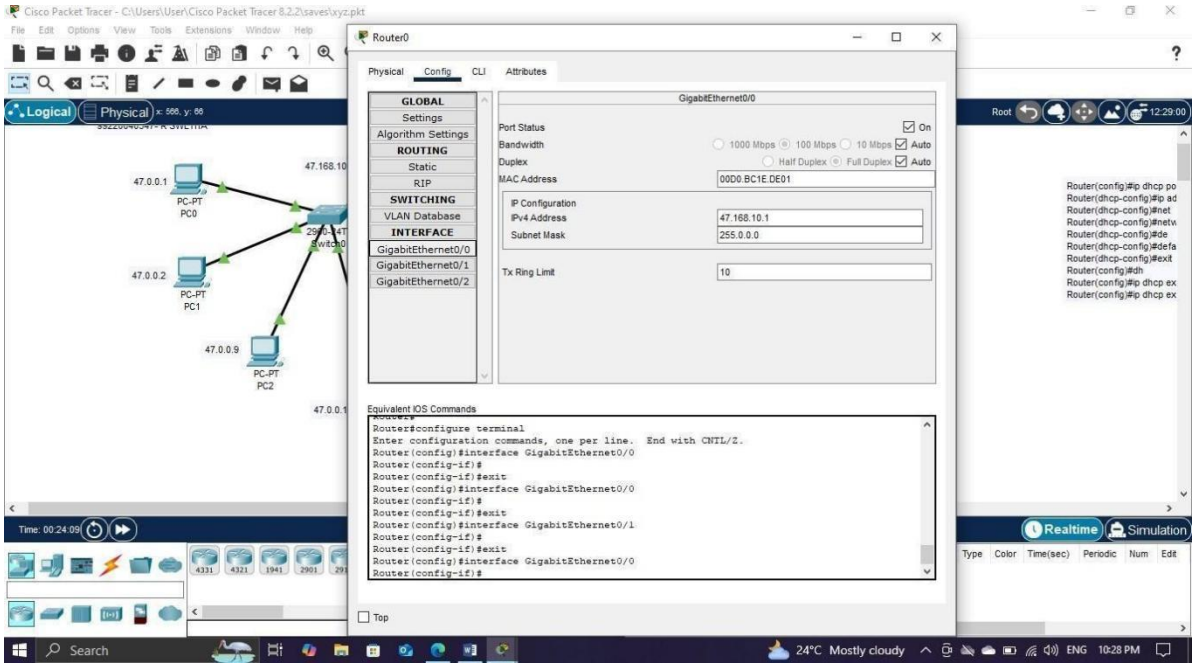
5. Describe step by step configuration steps properly (you may copy the commands used in the configuration tab and paste it.)

a. Allot IP Address to the interfaces connected to the switch (GigabitEthernet0/0, GigabitEthernet0/1)

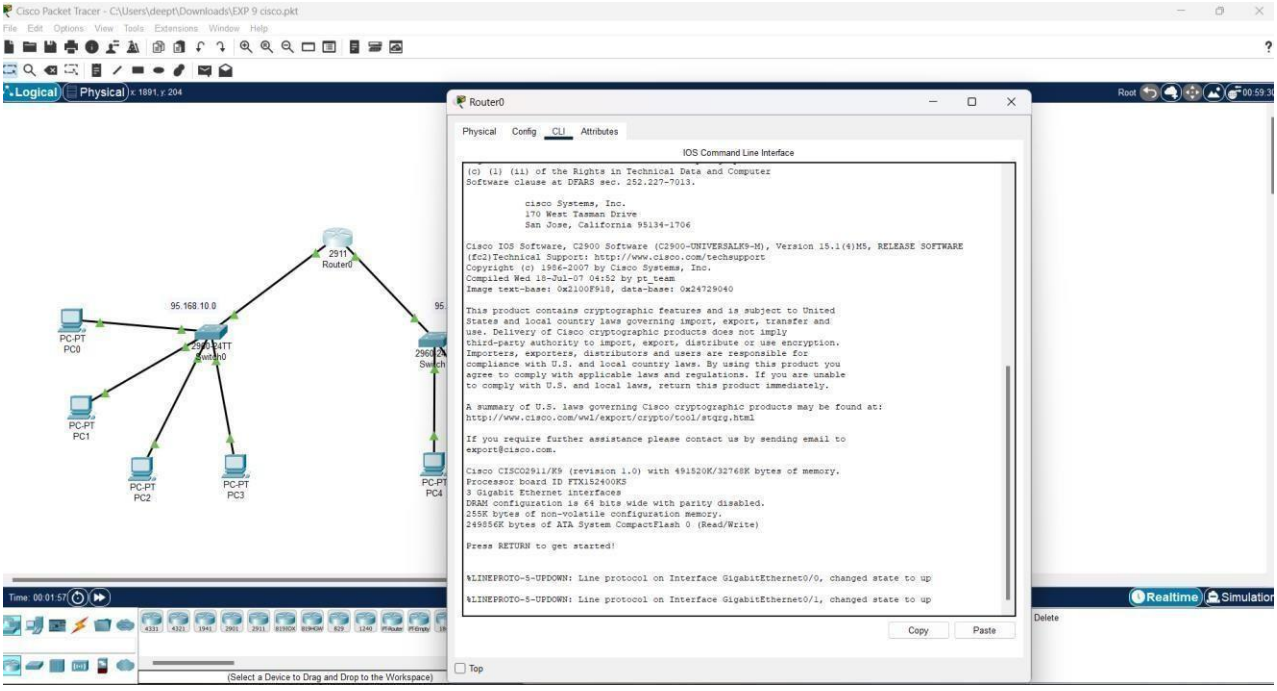
b. Router(config)#ip dhcp pool 10
Router(dhcp-config)#network 47.0.0.0 255.0.0.0
Router(dhcp-config)#default-router 47.168.10.1
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 47.168.10.3 47.168.10.8

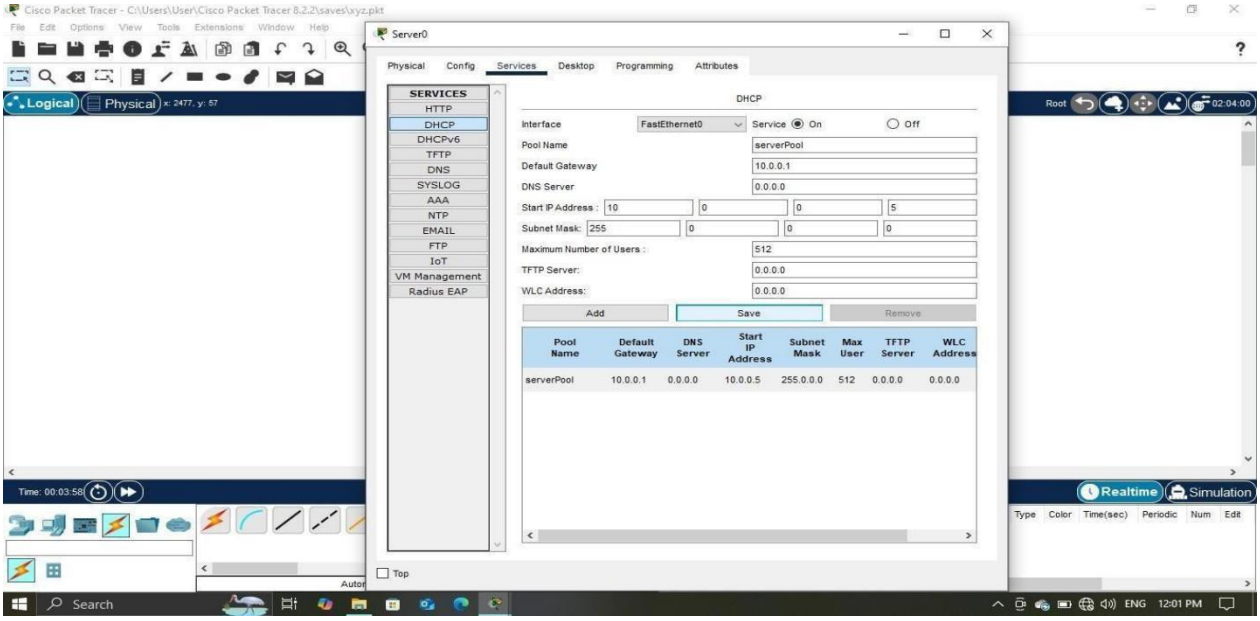
c. IP configure the PC's using dhcp

6. Output Diagram (Minimum 3 screenshot):



99220041762





Rubrics for Experiment Assessment:

Rubrics	Good	Normal	Poor	Marks
Creation of Topology (4)	Created the topology, identified the proper devices and made the connections **(4)**	Created the topology, Identify the proper devices, making the connections But missing some features **(3)**	Created wrong topology, Failed to Identify the proper devices and making connections **(1)**	
Verify the connectivity (4)	Verified the connectivity in all the levels **(4)**	Verified the connectivity at some levels (only some nodes) **(2)**	Verified the connectivity is not done. **(1)**	
Timely Completion (2)	Completed the lab before the allotted time **(2)**	Completed the lab after the deadline **(1)**	Did not submitted before grading **(0)**	
Total				

CONCLUSION (provide conclusion about this experiment):

Thus, the design and implementation of DHCP configuration using packet tracer is successfully implemented.

Register No:	**99220041762**
Name:	**G.ASISH**
Class/Section:	**S18/8301A**
Ex.No:	**8B**
Name of the Experiment	Distance Vector Routing
Google Drive link of the packet tracer file (give view permission):	**https://drive.google.com/drive/folders/1kZYMTJ0uZatmg4XpevUQnRGjCA_W4BOF**

Objective(s):

To design and implement Distance Vector routing using packet tracer

Introduction:

Distance-Vector routing protocols select the best path for data packets. Here distance is reference of hop in network. Distance-Vector protocols calculate the distance between source and destination on the basis of hop count. Suppose there are two path available for data packet from source and destination. Distance-Vector protocol select the path in which the number of hopes are less. RIP and IGRP are example of Distance-Vector routing protocol.

Distance vector routing protocols manage the selection of best path for data packets by routers. Routing table of all routers update by sharing the information on the network. The destination network path defines by hop count up to destination network. Distance vector routing protocols generally known as DVRP. Distance vector routing protocols is mostly used protocol in present scenario. DVRP sent the data packets over the internet protocol.

There are two terms in DVRP. The first term is distance and second is vector. Distance is number of hop or step to send the data packets up to destination network. Path selection for a data packet is depends on the hop count. **Minimum hope count path selected by the Distance vector routing protocols**. The term vector refers to the propagating of the packet on a given set of network nodes. Routers broadcast the information of remote network to next router. **Every router does the same thing so the routing table of all routers updated automatically**. All router informs about the connected networks to next router then router update its own routing table.

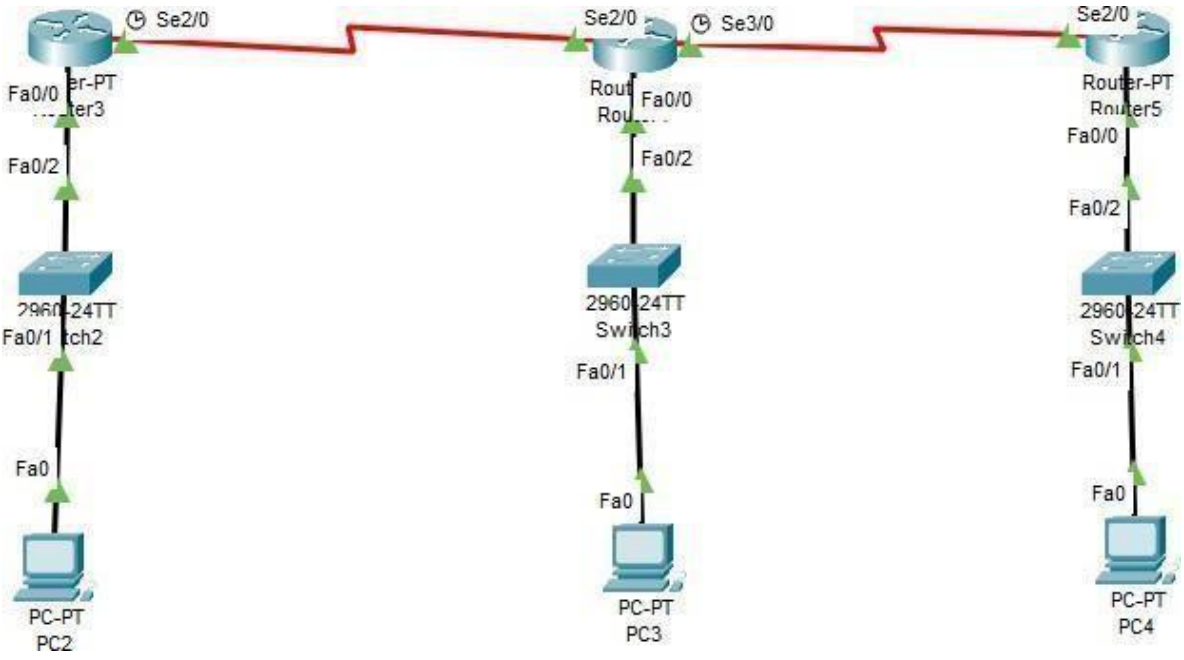
Network topology changes time to time. Adding or removing a router in a network is very common phenomena. **Any change in network should be updated in all router's routing table**. Doing this manually is very critical work. Distance vector routing protocols do this job automatically. The process of broadcasting any update in routing table and updation in all routing tables is known as convergence.

The algorithm distance vector routing protocol find the routes on a internetwork. The other algorithm used to select the best path for data packets is Link State routing protocols. DVRP algorithm allow routers to exchange the routing tables with each other. Each router received the routing table from neighbour router, update own routing table and share the updated table to next neighbour router. This process repeat after a fix predefined time interval. By repeating this process all devices connected in the network maintain the routing table which allow the flow of data packets efficiently.

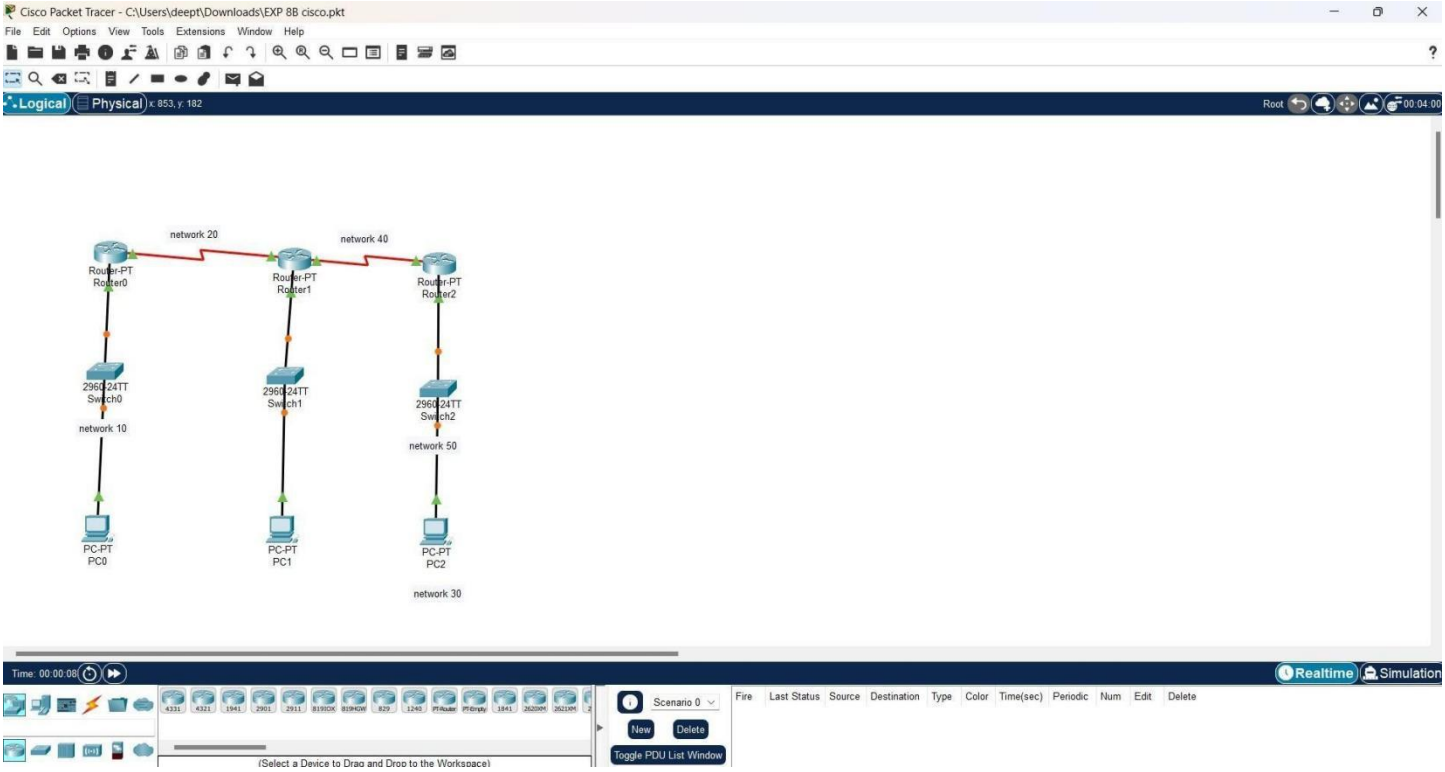
1. **Device Requirements:**
   1. PC's
   2. Switches

3. Router-PT
4. Connection wires

2. Network Diagram for your experiment (draw the diagram either hand drawing/ms paint or any other drawing tools)



3. Network Diagram (Packet tracer diagram before configuration):



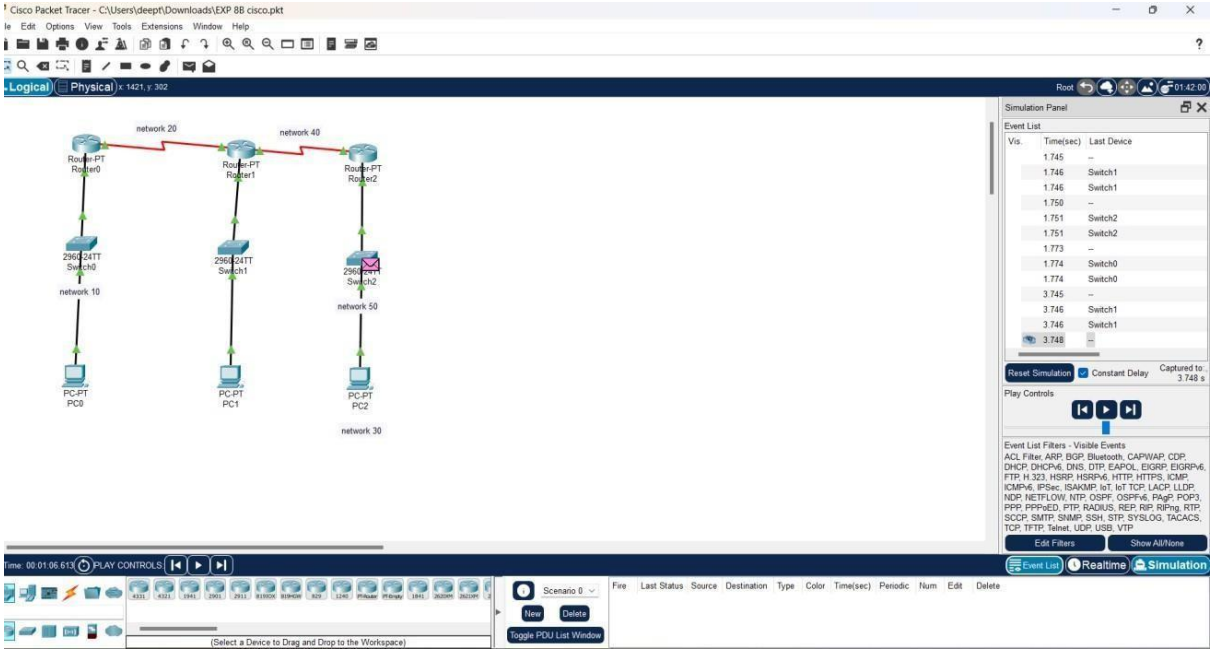
4. Configuration details:

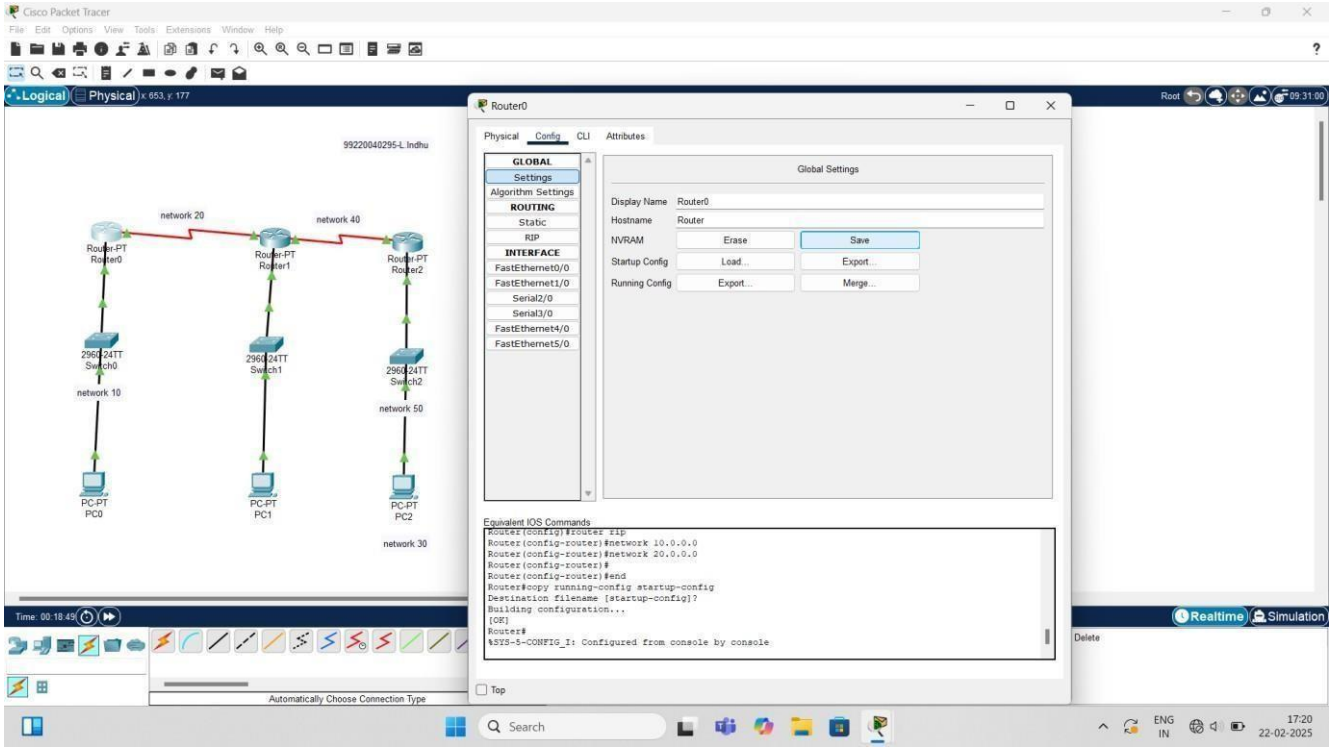
Device Name	Interface Name	IP Address	Subnet mask	Default Gateway
PC0	Fa0:Fa0/1	10.10.10.2	255.0.0.0	10.10.10.1
Switch0				
Router-PT0	Fa0/0:Fa0/2	10.10.10.1	255.0.0.0	
PC1	Fa0:Fa0/1	30.30.30.2	255.0.0.0	30.30.30.1
Switch1				
Router-PT1	Fa0/0:Fa0/2	30.30.30.1	255.0.0.0	
PC2	Fa0:Fa0/1	50.50.50.2	255.0.0.0	50.50.50.1
Switch2				
Router-PT2	Fa0/0:Fa0/2	50.50.50.1	255.0.0.0	

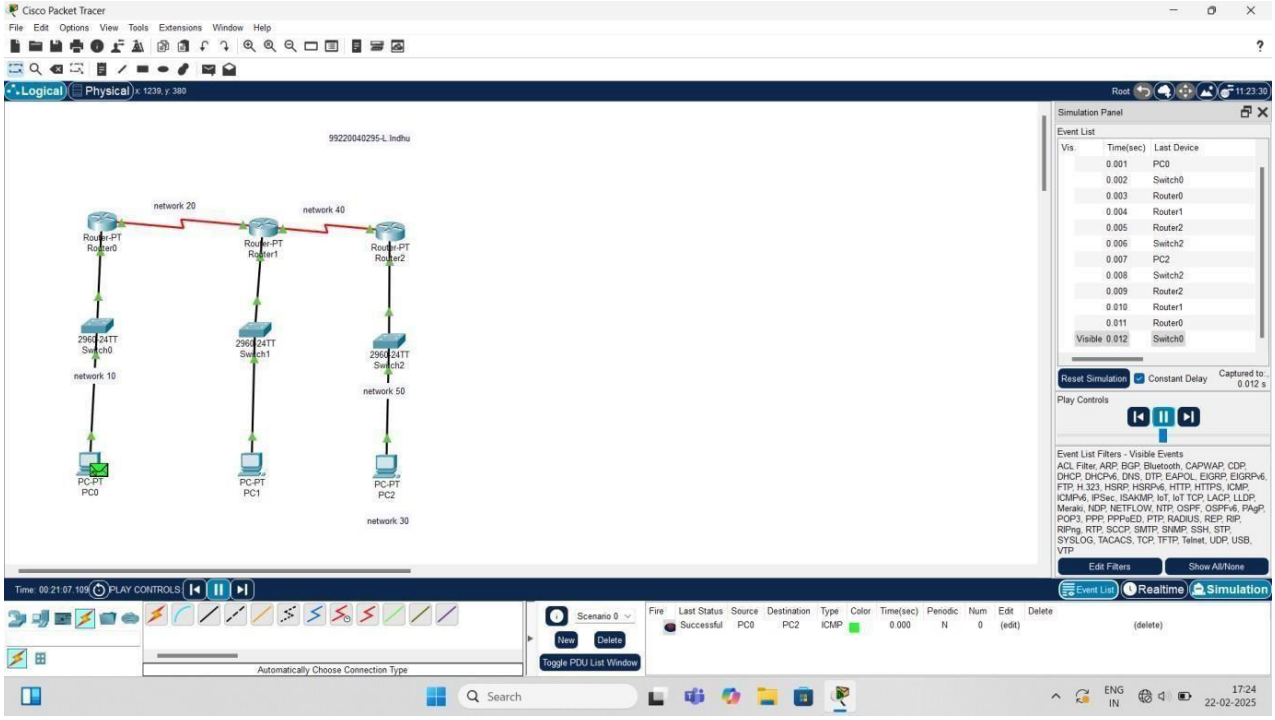
5. Describe step by step configuration steps properly (you may copy the commands used in the configuration tab and paste it.)

1. IP configuration of PC's
2. Set the clock rate for router as 64000 and the other router path is mentioned as NOT SET. Manually turn ON the port status.
3. Add the network using RIP and go to settings to SAVE the network.

6. Output Diagram (Minimum 3 screenshot):




Cisco Packet Tracer
Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Global Settings
Display Name Router0
Hostname Router
NVRAM Erase Save
Startup Config Load... Export...
Running Config Export... Merge...
Equivalent IOS Commands
Router(config)#router rip
Router(config-router)#network 10.0.0.0
Router(config-router)#network 20.0.0.0
Router(config-router)#
Router(config-router)#end
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
%SYS-5-CONFIG_I: Configured from console by console
99220040295-L Indhu
network 20
network 40
network 10
network 50
network 30
Router-PT Router0
Router-PT Router1
Router-PT Router2
2960-24TT Switch0
2960-24TT Switch1
2960-24TT Switch2
PC-PT PC0
PC-PT PC1
PC-PT PC2
Logical
Physical
Realtime
Simulation
Automatically Choose Connection Type


Cisco Packet Tracer
Logical
Physical
99220040295-L Indhu
network 20
network 40
network 10
network 50
network 30
Router-PT Router0
Router-PT Router1
Router-PT Router2
2960-24TT Switch0
2960-24TT Switch1
2960-24TT Switch2
PC-PT PC0
PC-PT PC1
PC-PT PC2
Simulation Panel
Event List
Vis. Time(sec) Last Device
0.001 PC0
0.002 Switch0
0.003 Router0
0.004 Router1
0.005 Router2
0.006 Switch2
0.007 PC2
0.008 Switch2
0.009 Router2
0.010 Router1
0.011 Router0
Visible 0.012 Switch0
Reset Simulation
Constant Delay
Play Controls
Event List Filters - Visible Events
Edit Filters
Show All/None
Realtime
Simulation
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
Successful PC0 PC2 ICMP 0.000 N 0 (edit) (delete)
Scenario 0
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type

7. Rubrics for Experiment Assessment:

Rubrics	Good	Normal	Poor	Marks
Creationof Topology (4)	Created the topology, identified the proper devices and made the connections **(4)**	Created the topology, Identify the proper devices, making the connections But missing some features **(2)**	Created wrong topology, Failed to Identify the proper devices and made connections **(1)**	
Verify the connectivity (4)	Verified the connectivity in all the levels **(4)**	Verified the connectivity at some levels (only some nodes) **(2)**	Verified the connectivity is not done. **(1)**	
Timely Completion (2)	Completed the lab before the allotted time **(2)**	Completed the lab after the deadline **(1)**	Did not submit before grading **(0)**	
			Total	

8. CONCLUSION (provide conclusion about this experiment):

Thus, the design and implementation of Distance Vector Routing using packet tracer is successfully implemented and connections are verified.

Register No:	**99220041762**
Name:	**G.ASISH**
Class/Section:	**S18/8301A**
Ex.No:	**8A**
Name of the Experiment	Link State Routing
Google Drive link of the packet tracer file (give view permission):	**https://drive.google.com/drive/folders/1kZYMTJ0uZatmg4XpevUQnRGjCA_W4BOF**

Objective(s):

To design and implement Link state routing using packet tracer

Introduction:

Link State Routing Protocols used to select the path for data packet in an internetwork. Link state routing protocols uses link state routers to share information of connected network devices. This is a learning process. By learning process each router maintain the routing table to select the shortest path for data packet transmission. Each router update the network topology to nearby router only. Link state routing protocols are also known as **shortest path first protocol.**

Link state protocols allow routers to share the information about network connected to it. This information passed to neighbour router only. An accurate information of network topology around the router updated in routing table. By help of the routing table better routing path selected by the router.

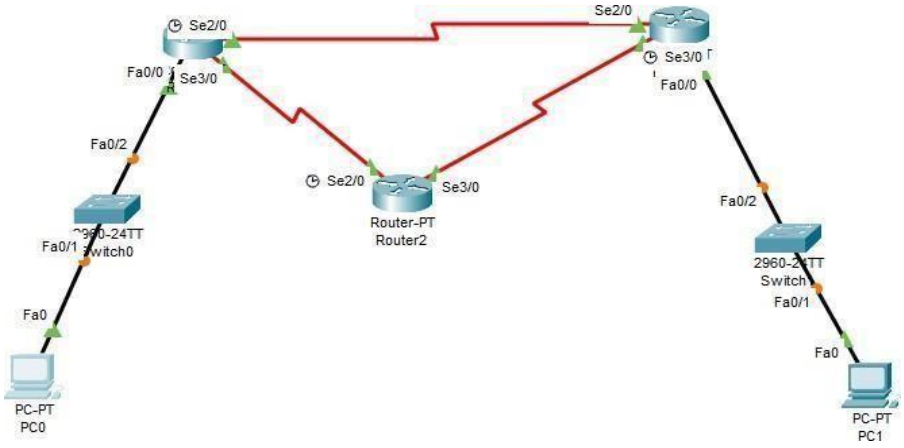
The information passes by router is known as link state advertisements (LSAs). In distance vector the information message passes in a fix time interval. Link state advertisements shared only when any changes done in the network topology. The bandwidth less consumed by link state routing protocol. The time of convergence is less than in distance vector protocol.

Function of link state routing protocol

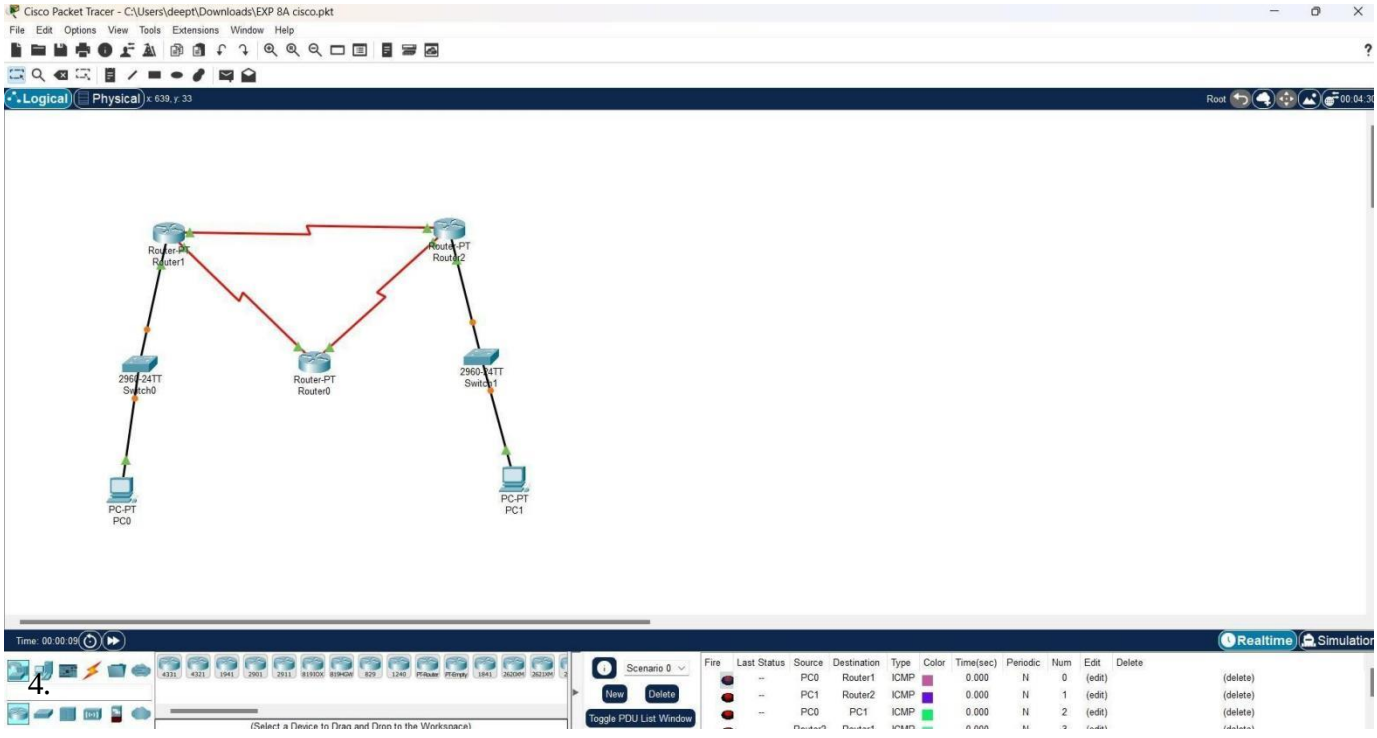
Important terms of link state routing protocol are link state packet, database, algorithm, routing table etc. Link state packets contains the routing information and sent to neighbour only when any changes occurs in connected network. Link state packets update the routing table in nearby routers. The informati on collected by link state packets stored in link state database.

1. **Device Requirements:**
   1. PC
   2. SWITCH
   3. ROUTER-PT
   4. Connection wires

2. **Network Diagram for your experiment (draw the diagram either hand drawing/ms paint or any other drawing tools)**



3. **Network Diagram (Packet tracer diagram before configuration):**



4.

5. **Configuration details:**

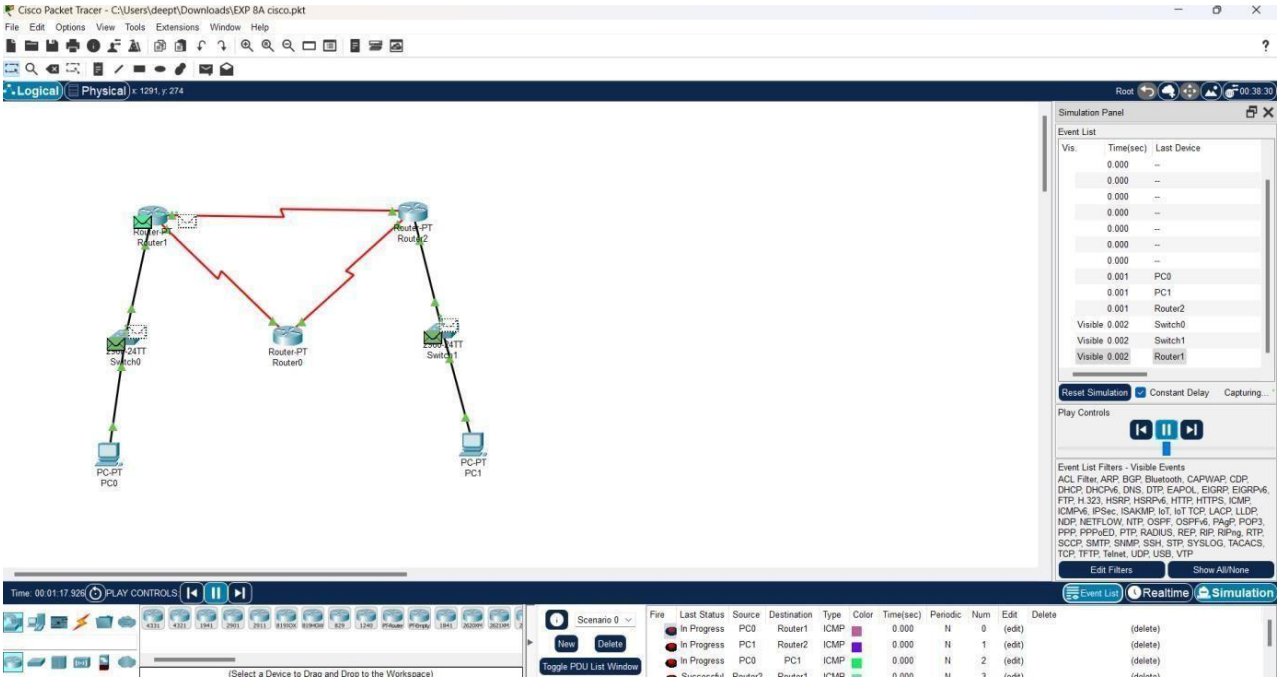
Device Name	Interface Name	IP Address	Subnet mask	Default Gateway
PC 0	Fa0 - fa0/1	10.10.10.2	255.0.0.0	10.10.10.0
PC 1	Fa0 - Fa0/2	50.50.50.2	255.0.0.0	50.50.50.1
SWITCH 0				
SWITCH 1				
ROUTER-PT 0				

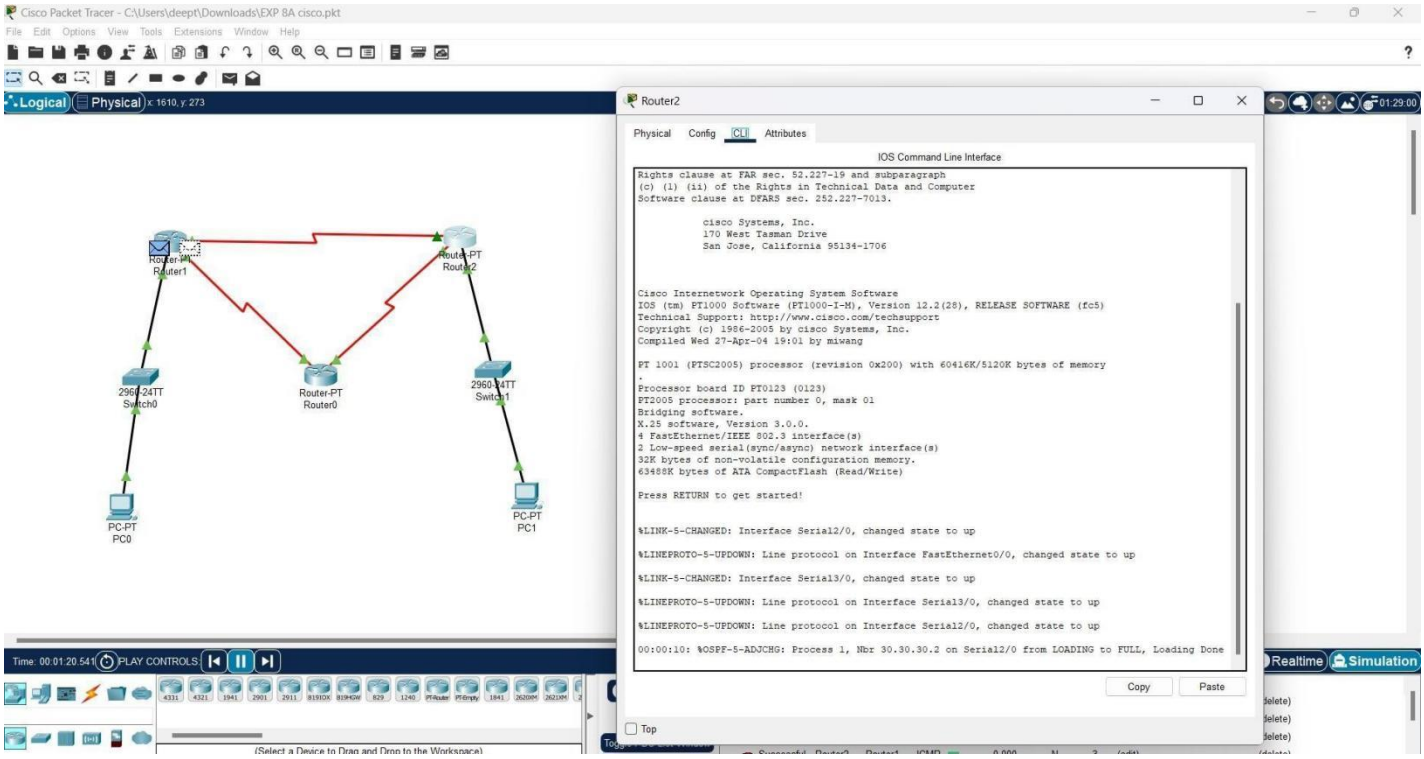
ROUTER-PT1				
ROUTER-PT 2				

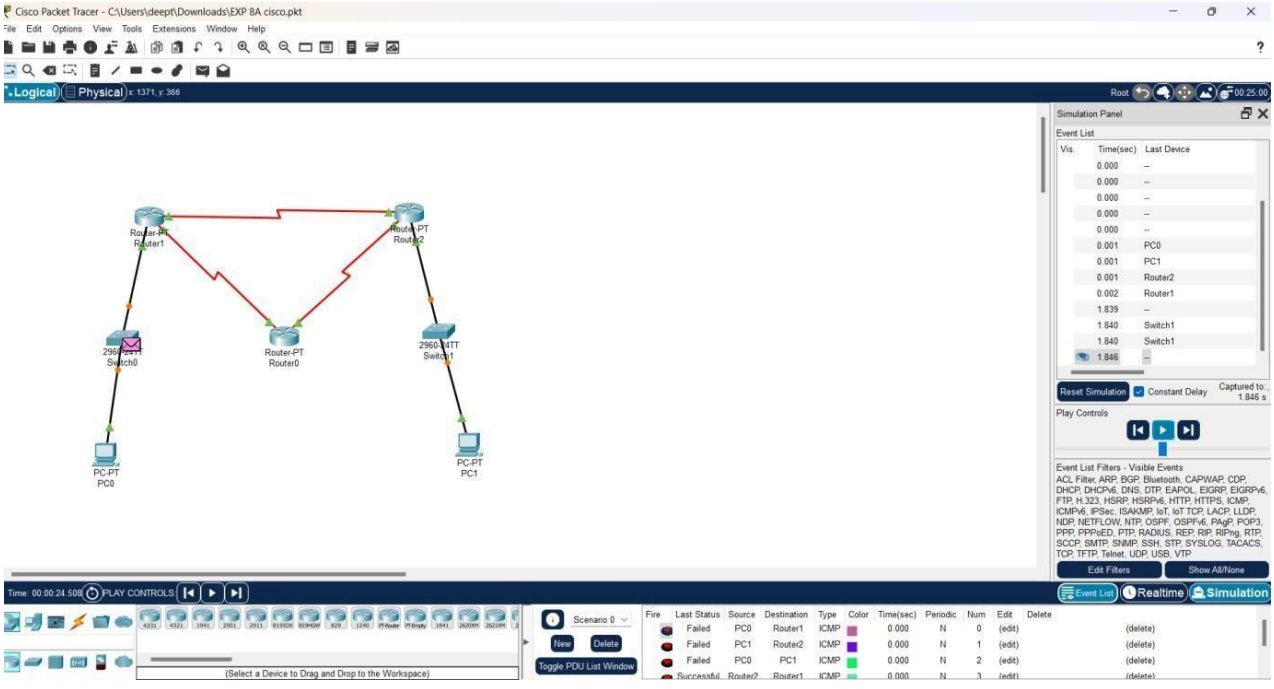
6. **Describe step by step configuration steps properly (you may copy the commands used in the configuration tab and paste it.)**

    1. IP configuration of PC's
    2. Set the clock rate for router as 64000 and the other router path is mentioned as NOT SET. Manually turn ON the port status.
    3. Router(config)#router ospf
       Router(config-router)#network 20.0.0.0 0.255.255.255 area 0
       Router(config-router)#network 40.0.0.0 0.255.255.255 area 0
       Router(config-router)#network 50.0.0.0 0.255.255.255 area 0
       Router(config-router)#exit

7. **Output Diagram (Minimum 3 screenshot):**




Cisco Packet Tracer - C:\Users\deept\Downloads\EXP 8A cisco.pkt
Router2
Physical
Config
CLI
Attributes
IOS Command Line Interface
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Cisco Internetwork Operating System Software
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)
Press RETURN to get started!
%LINK-5-CHANGED: Interface Serial2/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface Serial3/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 30.30.30.2 on Serial2/0 from LOADING to FULL, Loading Done
Copy
Paste
Top
Router-PT Router1
Router-PT Router2
2960-24TT Switch0
Router-PT Router0
2960-24TT Switch1
PC-PT PC0
PC-PT PC1
Logical
Physical
Realtime
Simulation


Cisco Packet Tracer - C:\Users\deept\Downloads\EXP 8A cisco.pkt
Logical
Physical
Simulation Panel
Event List
Vis.
Time(sec)
Last Device
Reset Simulation
Constant Delay
Play Controls
Event List Filters - Visible Events
Edit Filters
Show All/None
Router-PT Router1
Router-PT Router2
Router-PT Router0
2960-24TT Switch1
PC-PT PC0
PC-PT PC1
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
Realtime
Simulation

Rubrics for Experiment Assessment:

Rubrics	Good	Normal	Poor	Marks
Creationof Topology (4)	Created the topology, identified the proper devices and made the connections **(4)**	Created the topology, Identify the proper devices, making the connections But missing some features **(2)**	Created wrong topology, Failed to Identify the proper devices and made connections **(1)**	
Verify the connectivity (4)	Verified the connectivity in all the levels **(4)**	Verified the connectivity at some levels (only some nodes) **(2)**	Verified the connectivity is not done. **(1)**	
Timely Completion (2)	Completed the lab before the allotted time **(2)**	Completed the lab after the deadline **(1)**	Did not submit before grading **(0)**	
			Total	

CONCLUSION (provide conclusion about this experiment):
Thus, the design and implementation of Link state routing using packet tracer is successfully implemented and connections are verified.

Register No:	**99220041762**
Name:	**G.ASISH**
Class/Section:	**S18**
Ex.No:	**7b**
Date of Submission	
Name of the Experiment	**Configuration of Address Resolution protocol**
Google Drive link of the packet tracer file (give view permission):	**https://drive.google.com/drive/folders/1kZYMTJ0uZatmg4XpevUQnRGjCA_W4BOF**

Objective(s):

To design and implement Address Resolution Protocol using packet tracer

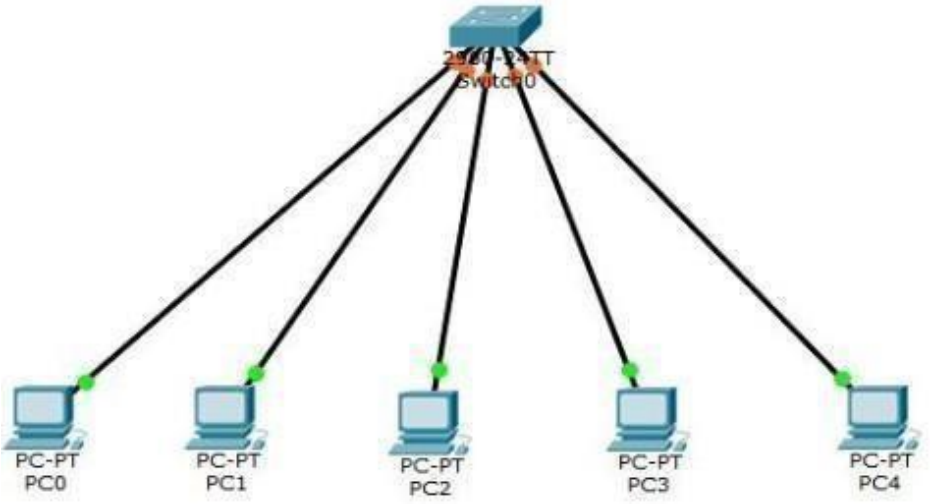
Introduction:

ARP (Address Resolution Protocol) is a network protocol used to find out the hardware (MAC) address of a device from an IP address. It is used when a device wants to communicate with some other device on a local network (for example on an Ethernet network that requires physical addresses to be known before sending packets). The sending device uses ARP to translate IP addresses to MAC addresses. The device sends an ARP request message containing the IP address of the receiving device. All devices on a local network segment see the message, but only the device that has that IP address responds with the ARP reply message containing its MAC address. The sending device now has enough information to send the packet to the receiving device.

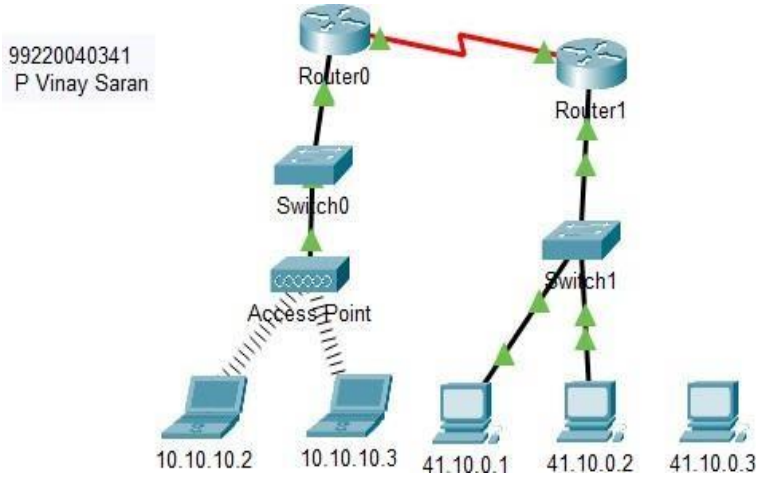
1. **Device Requirements:**
   1. Switch
   2. Laptop
   3. PC'S
   4. Copper Cross-Over

2. **Network Diagram for your experiment (draw the diagram either hand drawing/ms paint or any other drawing tools)**

99220041762



3. **Network Diagram (Packet tracer diagram before configuration):**



4. **Configuration details:**

Device Name	Interface Name	IP Address	Subnet mask
PC0	Fa0/1	41.10.0.1	255.255.255.0
PC0	Fa0/2	41.10.0.2	255.255.255.0
PC0	Fa0/3	41.10.0.3	255.255.255.0
laptop	Fa0/4	10.10.10.2	255.255.255.0
laptop	Fa0/5	10.10.10.3	255.255.255.0

Switch0			

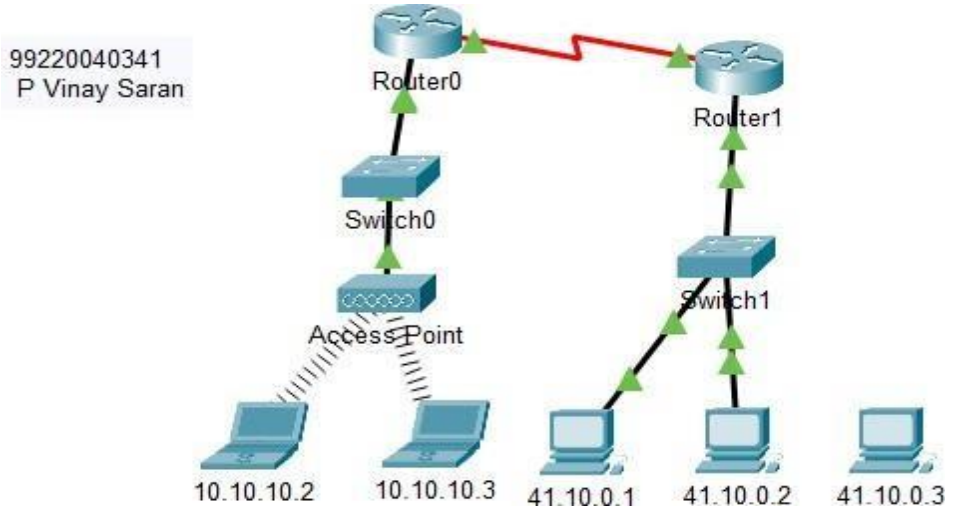
5. **Describe step by step configuration steps properly (you may copy the commands used in the configuration tab and paste it.)**

Ipconfig Ping

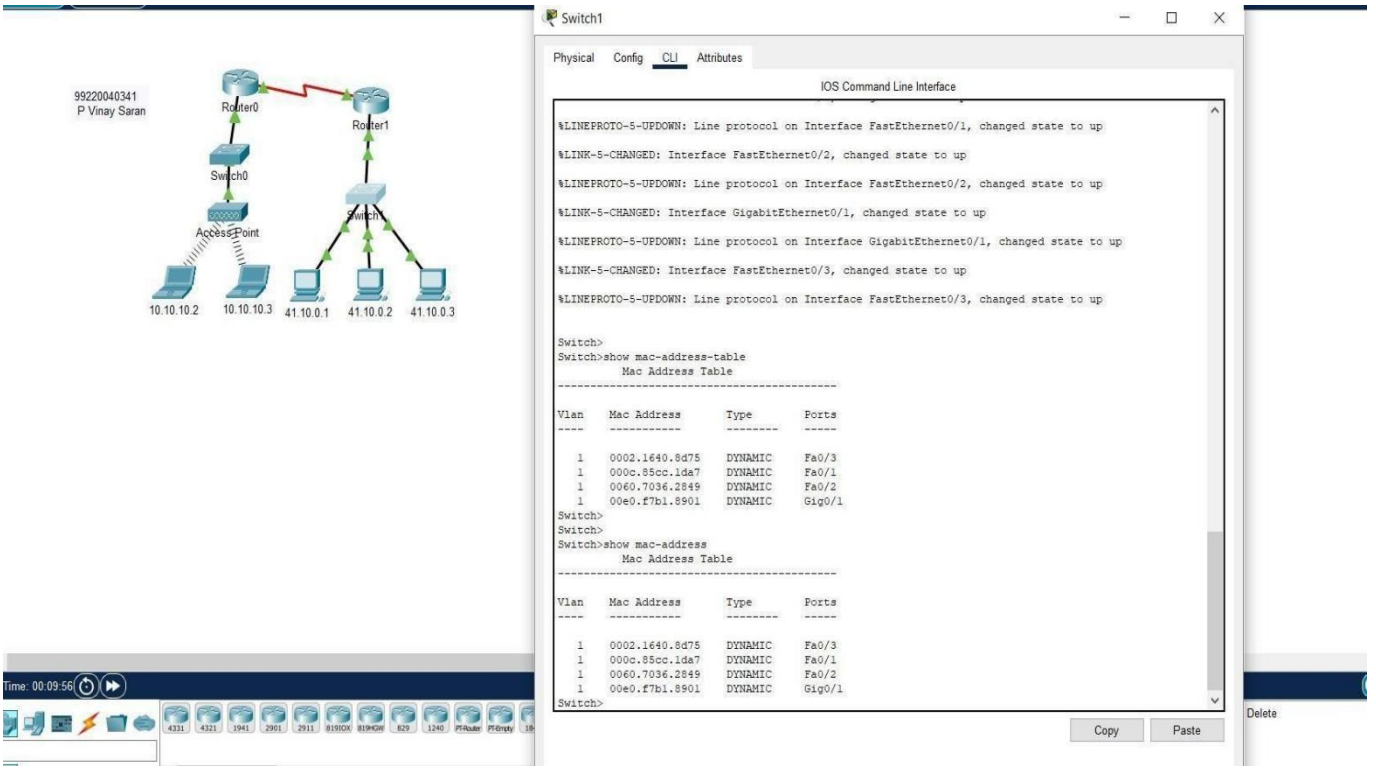
ip_address arp -

a arp -d

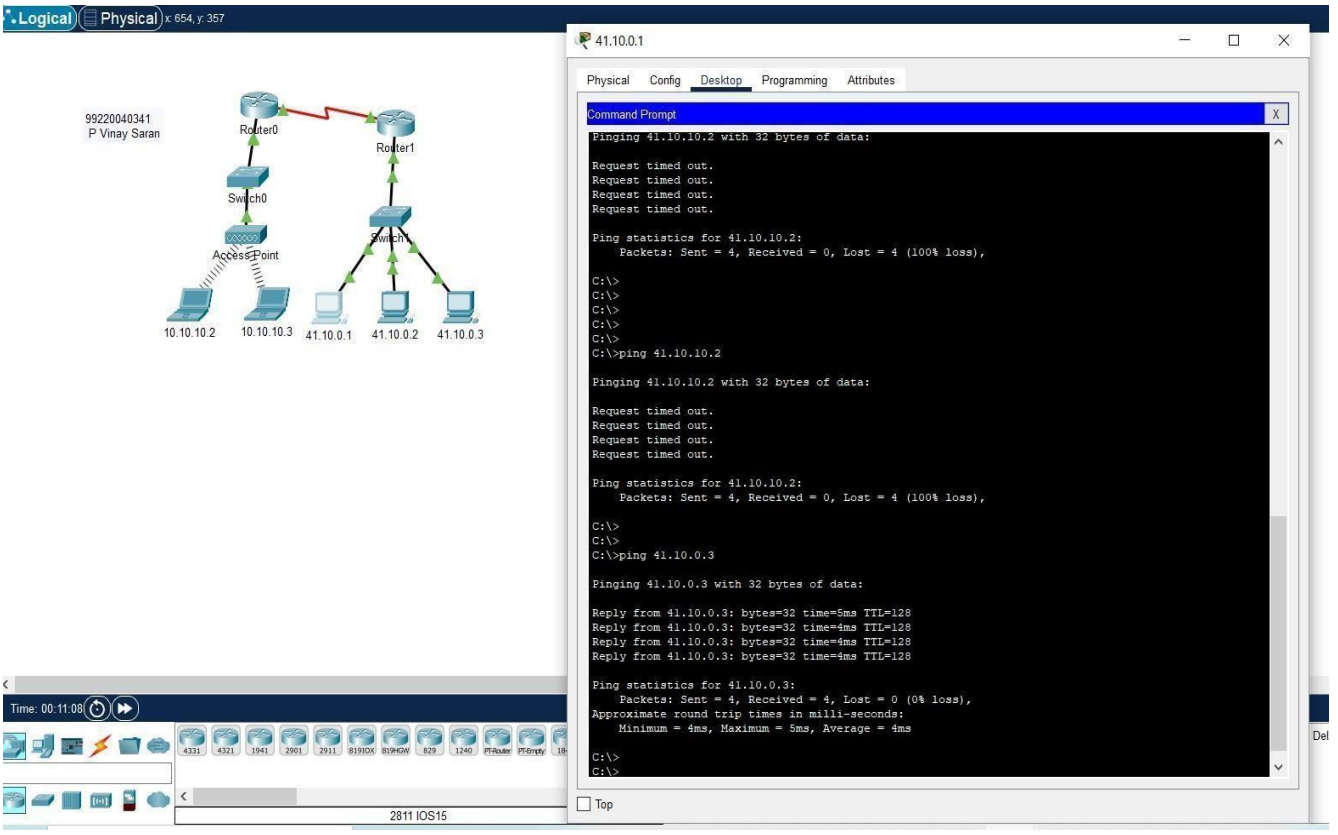
6. **Output Diagram (Minimum 3 screenshot):**



99220041762



99220041762



CONCLUSION (provide conclusion about this experiment):

Rubrics for Experiment Assessment:

Rubrics	Good	Normal	Poor	Marks
Creation of Topology (4)	Created the topology, Identify the proper devices and making the connections **(4)**	Created the topology, Identify the proper devices, making the connections But missing some features **(3)**	Created wrong topology, Failed to Identify the proper devices and making connections **(1)**	
Verify the connectivity (4)	Verified the connectivity in all the levels **(4)**	Verified the connectivity at some levels (only some nodes) **(2)**	Verified the connectivity is not done. **(1)**	
Timely Completion (2)	Completed the lab before the allotted time **(2)**	Completed the lab after the deadline **(1)**	Did not submitted before grading **(0)**	
			Total	

Register No:	**99220041762**
Name:	**G.ASISH**
Class/Section:	**S18**
Ex.No:	**7a**
Date of Submission	
Name of the Experiment	**Spanning Tree Protocol Configuration**
Google Drive link of the packet tracer file (give view permission):	**https://drive.google.com/drive/folders/1kZYMTJ0uZatmg4XpevUQnRGjCA_W4BOF**

Objective(s):

To design and implement spanning tree configuration using packet tracer

Introduction:

In a typical network topology, we have redundant connections between switches. Redundant connections play a very crucial role as it eliminates the single point of failure in the network. However, redundant connections create loop in the network. And to prevent those loops in networks the Spanning Tree Protocol chooses the best link while blocking the redundant links.

Root Bridge is the most important switch in a Spanning Tree Network. And all the other switches choose the best way to reach a Root Bridge and block the redundant links. Therefore, it is very important to choose the best switch in the network as a Root Bridge.

Root is selected on the basis of a Bridge ID. So, whichever switch will have the lowest Bridge ID, that very switch will be selected as a Root Bridge. Basically, Bridge ID is made up of a priority number and the MAC Address. And by default, all switches have the same priority number – 32768 to be precise – so the Spanning Tree relies on a MAC address for the selection of Root Bridge. But the problem is that by default any switch which has the lowest Bridge ID can be automatically selected as a Root Bridge. And if that switch is slow then it will slow down the entire network because its network traffic will pass through that switch. Hence, it is very important that every Spanning Tree Network has the best Switch as a root.

By default, the Spanning Tree is enabled on the switches so if we create a redundant connection on switches then the Spanning Tree Protocol will automatically come into action to prevent a loop in the network. Therefore, for maximum optimization it is very important to select the right switch as a Root Bridge.

We cannot however, change the MAC address of a switch so we will have to change the priority number of switches to influence the selection of a Root Bridge.

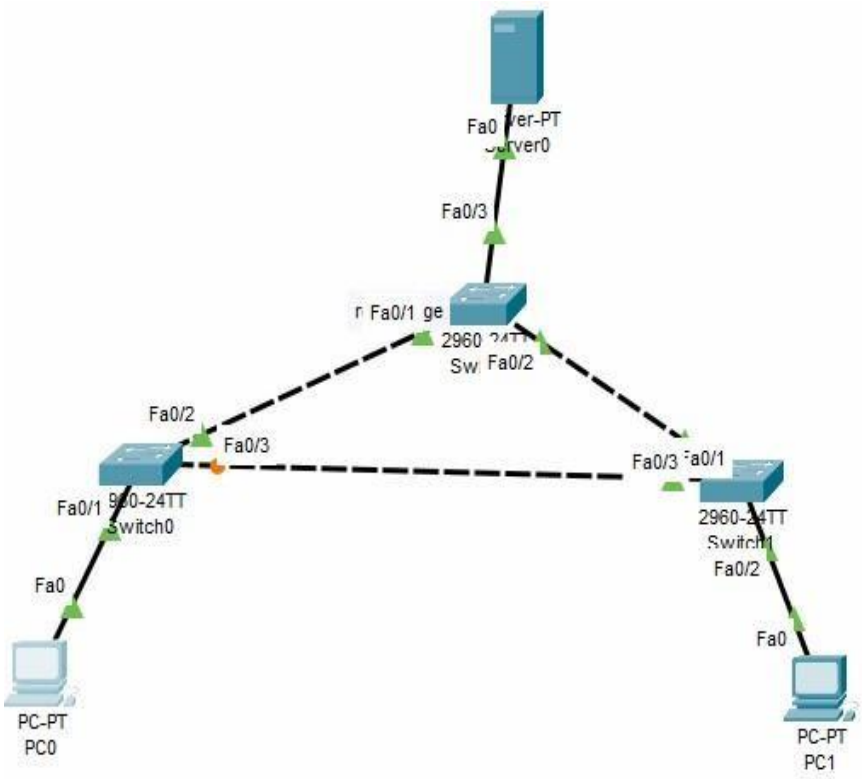
In this lab, we will try changing the priority of a switch to be able to select the switch of our choice as a Root Bridge. Root Bridge is selected as per the VLAN number so we have to mention that for which VLAN, the switch is a root. We will also enable a newer version of the Spanning Tree which is a Rapid Spanning Tree.

1. **Device Requirements:**
   1. SWITCH 0

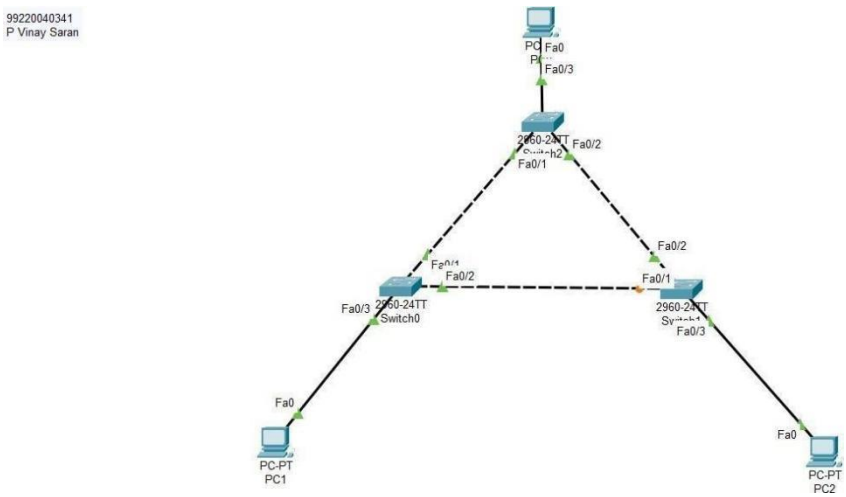
99220041762

2. SWITCH 1
3. SWITCH 2
4. PC 0
5. PC 1
6. PC 2

2. Network Diagram for your experiment (draw the diagram either hand drawing/ms paint or any other drawing tools)



3. Network Diagram (Packet tracer diagram before configuration):



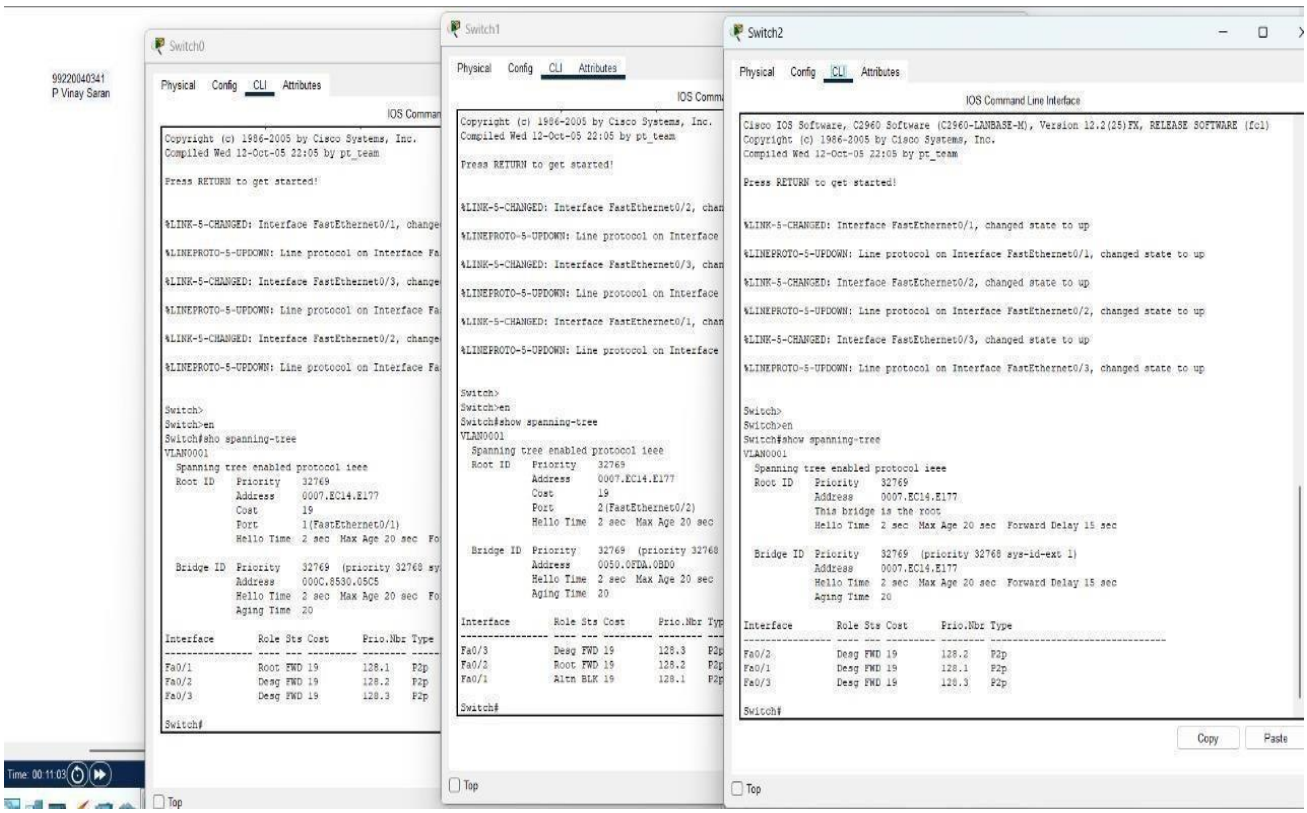
99220041762

4. **Configuration details:**

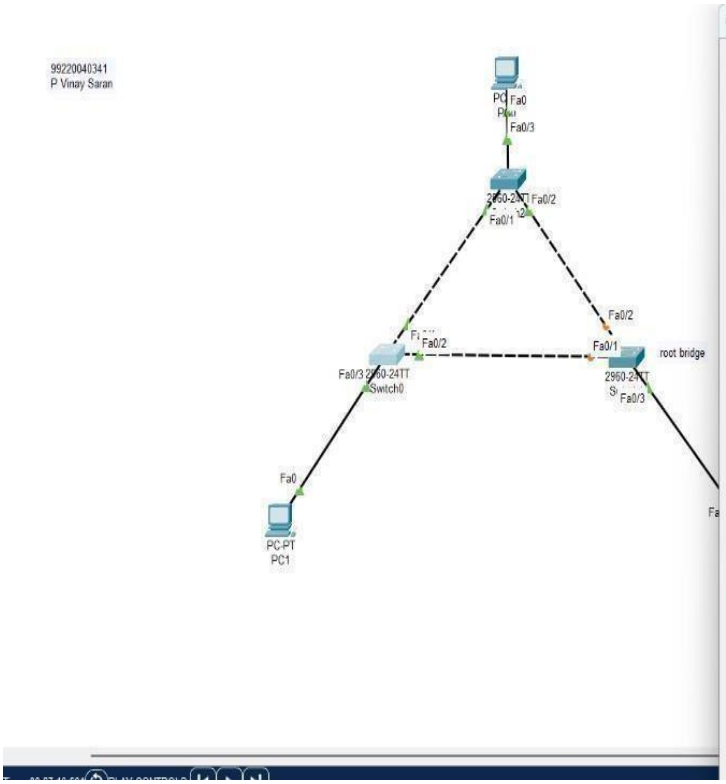
Device Name	Interface Name	IP Address	Subnet mask
PC 0	Fa0/1-3	41.168.10.1	255.0.0.0
PC 1	Fa0/1-3	41.168.10.2	255.0.0.0
PC 2	Fa0/1-3	41.168.10.3	255.0.0.0

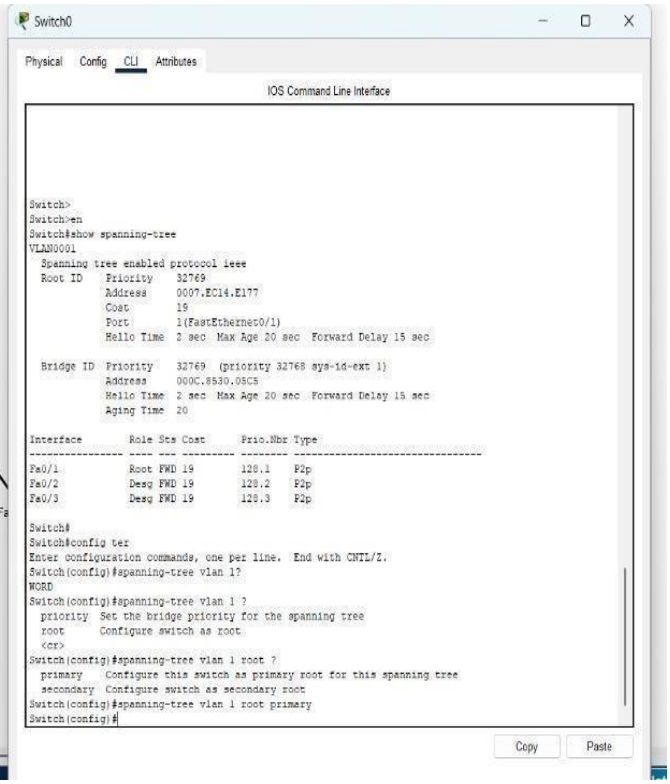
5. **Describe step by step configuration steps properly (you may copy the commands used in the configuration tab and paste it.)**
    1. **Create VLANs**
    2. **Configure interfaces**
    3. **Configure trunking**

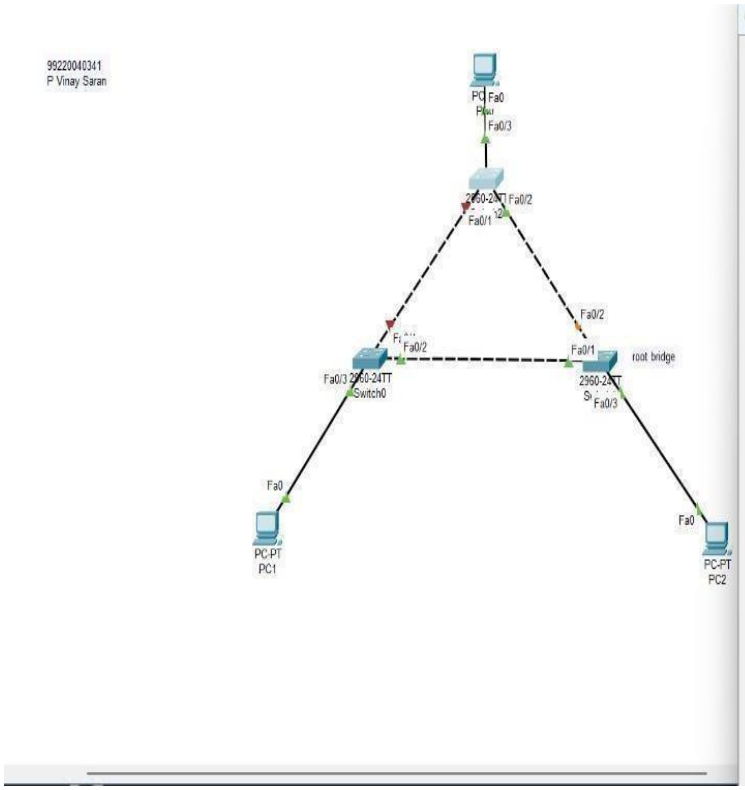
6. **Output Diagram (Minimum 3 screenshot):**

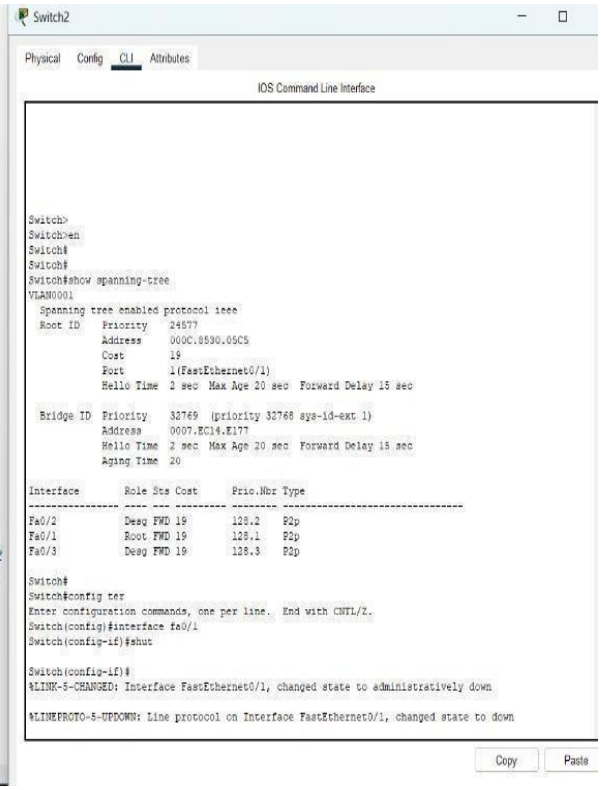


99220041762

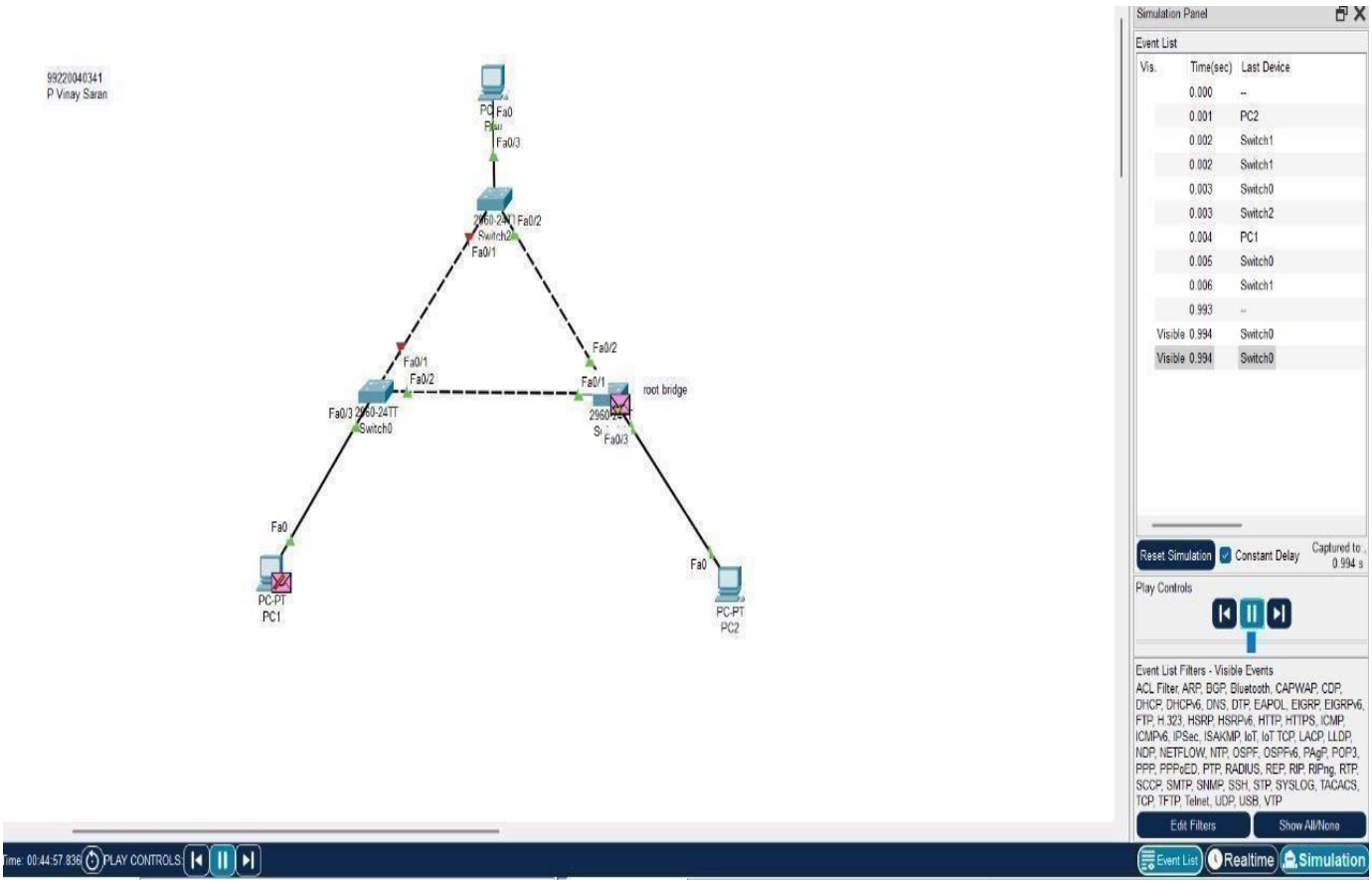








99220041762



CONCLUSION (provide conclusion about this experiment):

Rubrics for Experiment Assessment:

Rubrics	Good	Normal	Poor	Marks
Creation of Topology (4)	Created the topology, Identify the proper devices and making the connections **(4)**	Created the topology, Identify the proper devices, making the connections But missing some features **(3)**	Created wrong topology, Failed to Identify the proper devices and making connections **(1)**	
Verify the connectivity (4)	Verified the connectivity in all the levels **(4)**	Verified the connectivity at some levels (only some nodes) **(2)**	Verified the connectivity is not done. **(1)**	
Timely Completion (2)	Completed the lab before the allotted time **(2)**	Completed the lab after the deadline **(1)**	Did not submitted before grading **(0)**	
			Total	

Register No:	**99220041762**
Name:	**G.Asish**
Class/Section:	**8301A/S18**
Ex. No:	**10**
Name of the Experiment	**Capture and Analyze TCP and IP packets**
Google Drive link of the packet tracer file (give view permission):	https://drive.google.com/drive/folders/1kZYMTJ0uZatmg4XpevUQnRGjCA_W4BOF

Objective(s): To capture and analyze TCP and IP packet using Wireshark. **Introduction**

Packet Analysis is a technique used to intercept data in information security, where many of the tools that are used to secure the network can also be used by attackers to exploit and compromise the same network. The core objective of sniffing is to steal data, such as sensitive information, email text, etc., or sniff the traffic that is being transmitted between two parties.

Packet Analysis involves intercepting network traffic between two target network nodes and capturing network packets exchanged between nodes. A packet sniffer is referred to as a network monitor that is used legitimately by a network administrator to monitor the network for vulnerabilities by capturing the network traffic and should there be any issues, proceeds to troubleshoot the same. Similarly, sniffing tools can be used by attackers in promiscuous mode to capture and analyze all the network traffic. Once attackers have captured the network traffic they can analyze the packets and view the user name and password information in a given network as this information is transmitted in a cleartext format. An attacker can easily intrude into a network using this login information and compromise other systems on the network.

Hence, it is very crucial for an Information Security Auditor or a Penetration Tester to be familiar with network traffic analyzers and he or she should be able to maintain and monitor a network to detect rogue packet sniffers, MAC attacks, DHCP attacks, ARP poisoning, spoofing, or DNS poisoning, and know the types of information that can be detected from the captured data and use the information to keep the network running smoothly.

Exercise:

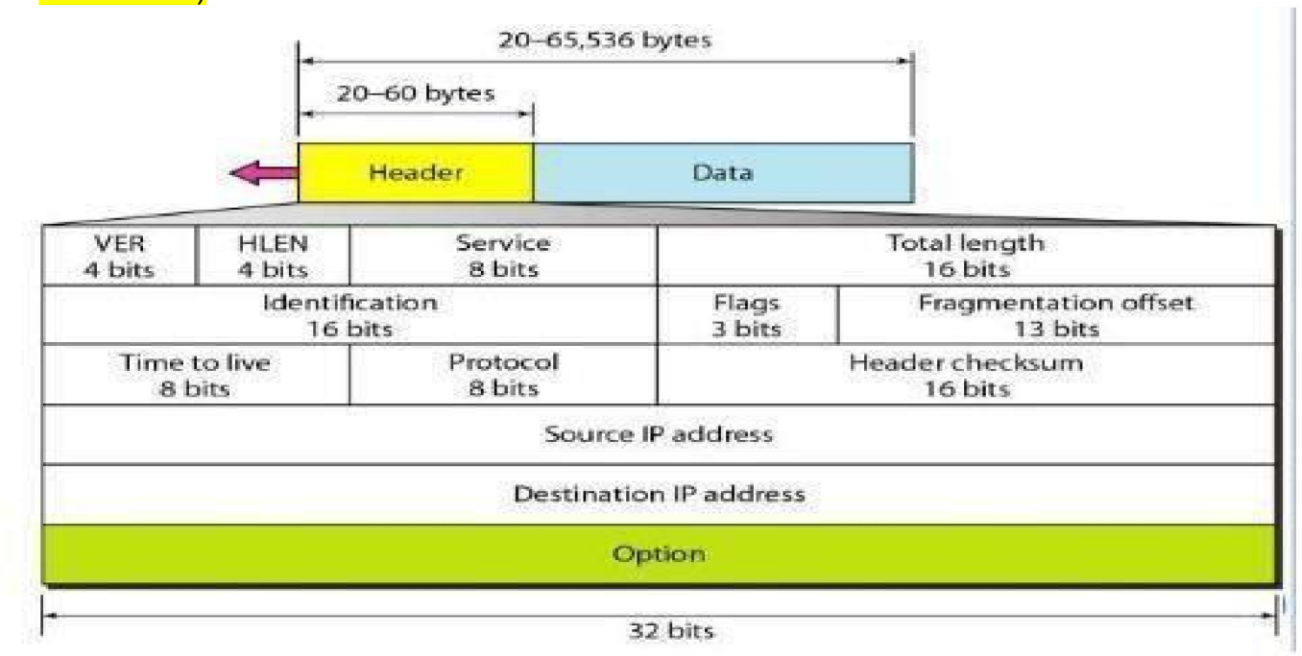
1. Visit any one website by opening a browser and fill your machine details (attach relevant screenshots).

Parameter	Value
Your Machine IP Address.	10.1.10.139
Your Machine MAC Address	50-5A-65-8F-24-97
Default Gateway address	10.1.0.1
Website URL	https://www.kalasalingam.ac.in
Website IP Address	18.67.161.45

2. Fill the following IP packet details:

Field Name	Field Length (no of bits)	Field value
Destination MAC address	48 bits	c8-4f-86-fc-00-0f
Source MAC address	48 bits	50-5A-65-8F-24-97
Destination IP address	32 bits	18.67.161.45
Source IP Address	32 bits	10.1.10.139
Destination TCP port	16 bits	59960
Source TCP port	16 bits	443

3. Fill the details as per the IP frame format .(highlight the details for each of the output and paste screenshot)

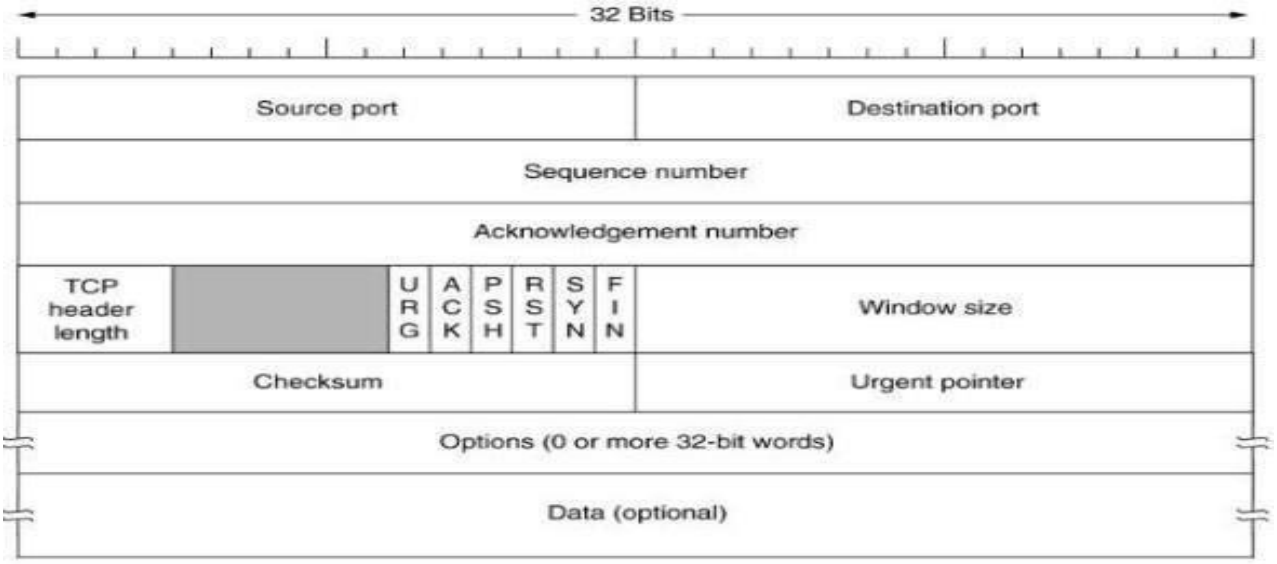


Field Name	**Field Value (# of bits)**	**Field Value (Either Binary or Hex Value)**
Version	4	0100
Header Length	4	0101
Type of service	8	0x00
Datagram Length	16	05c8(52)
16 bit Identifier	16	0x446c
Flags	3	010
13-bit Fragment offset	13	0 0000 0000 0000
Time-to-live	8	fa(250)
Upper layer protocol	8	6
Header Checksum	16	0xaec7
32 bit Source Address	32	18.67.161.45
32 bit destination address	32	10.1.10.139

Options (if any)	-	-
Date	-	08-03-2025

99220041762

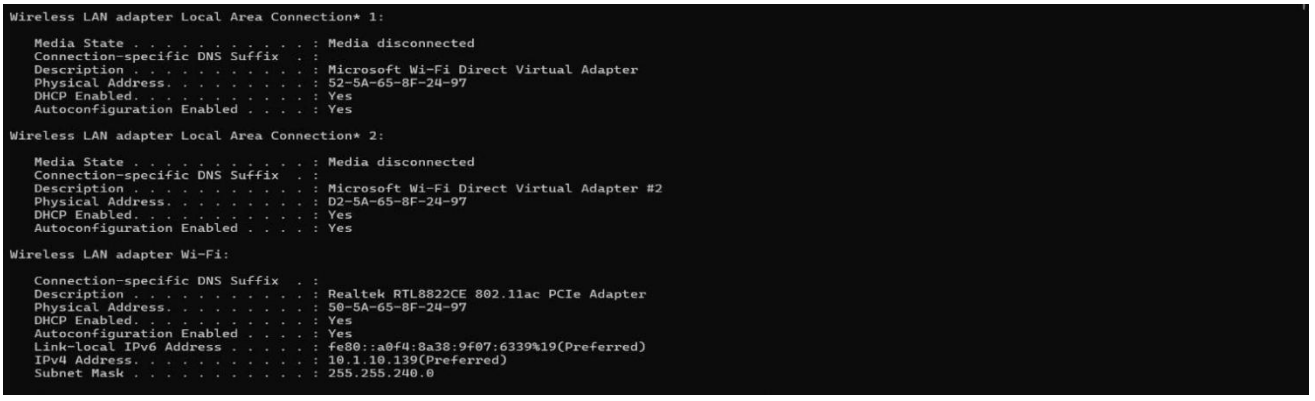
TCPHeader Format:

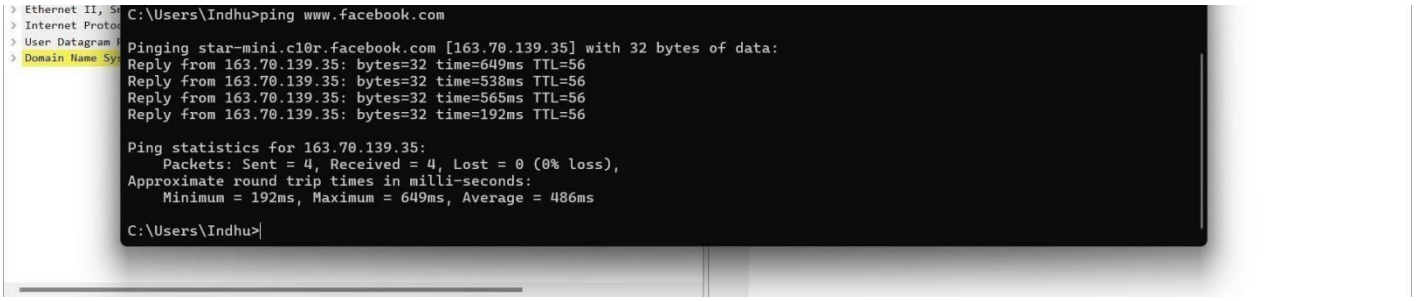


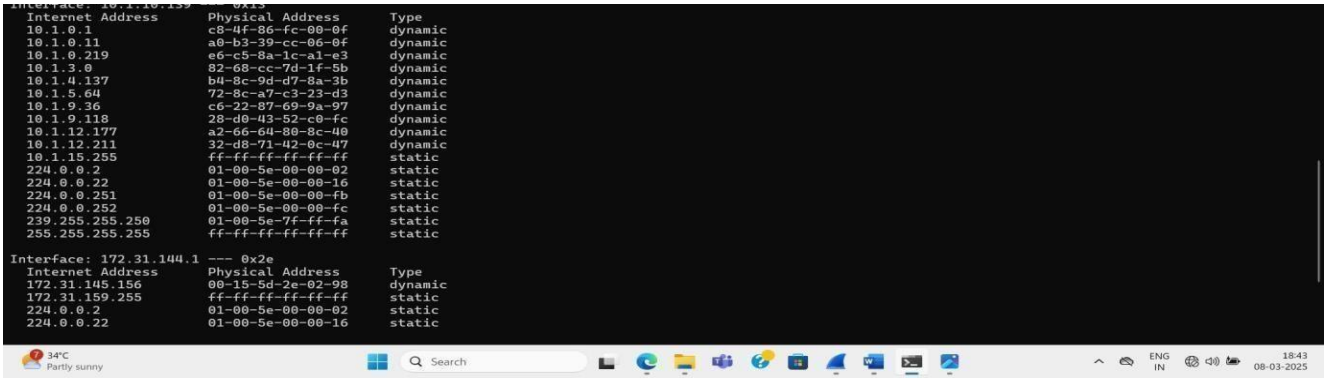
TCP Header.

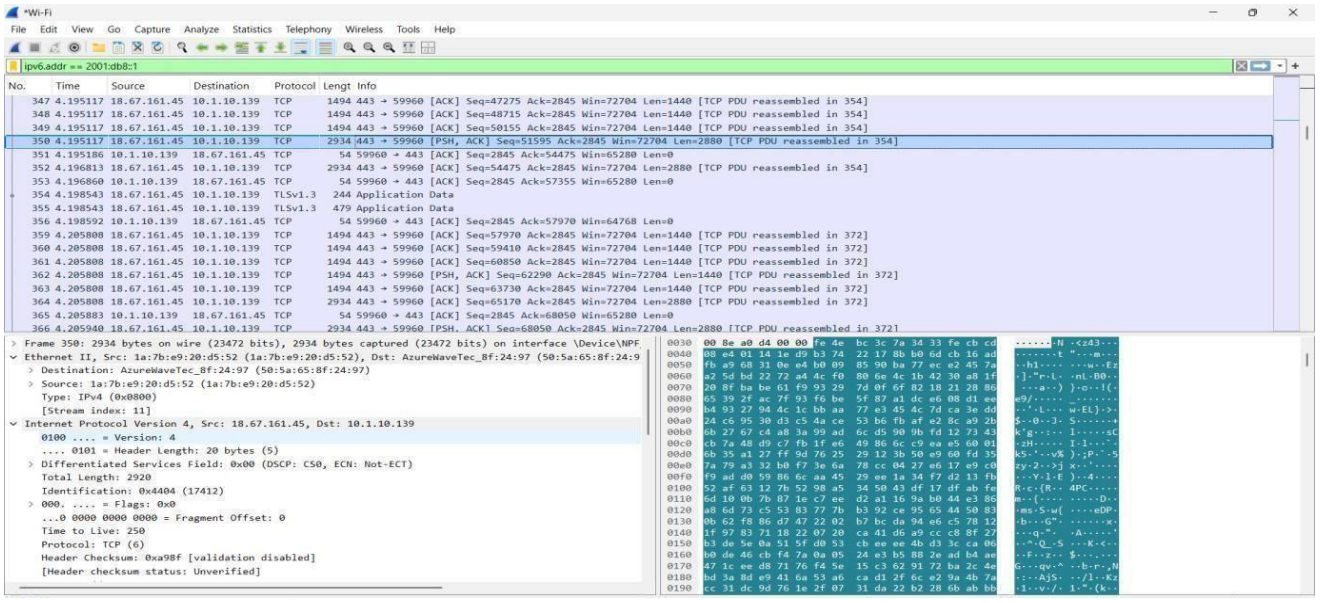
Field Name	Field Value (# of bits)	Field Value (Either Binary or Hex Value)
Source Port	16 bits	443
Destination Port	16 bits	59960
Sequence No.	32 bits	51595
Acknowledgement No	32 bits	2845
Header Length	4 bits	5
FLSGS (URG,PSH,ACK,RST,SYN,FIN)	6 bits	011000
Receive Window Size	16 bits	72704
Checksum	16 bits	0xa0d4
Urgent Pointer	6 bits	0
Options	-	-
Data	--	-

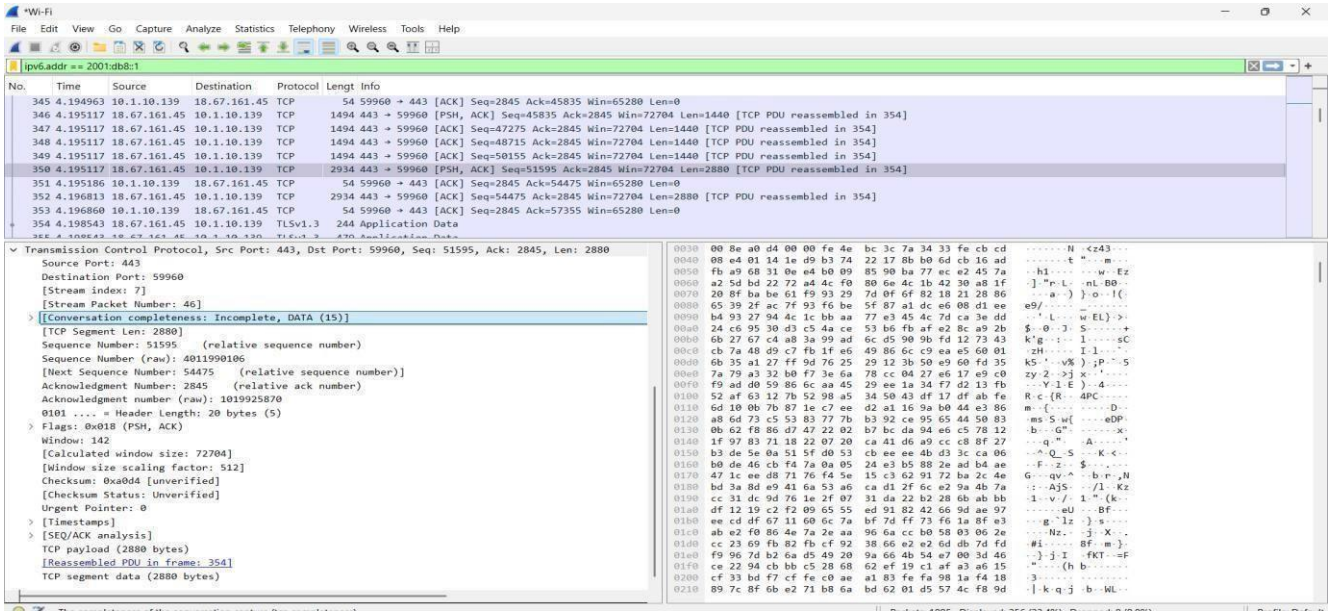
Paste the screenshot and highlight the above details:

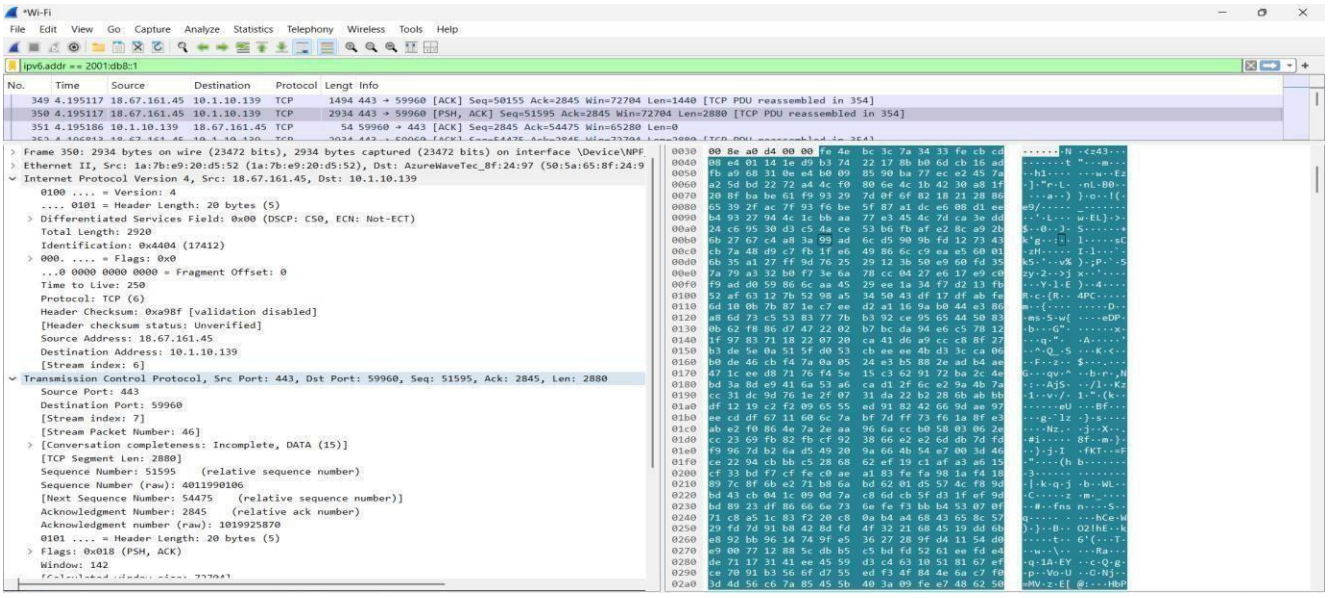



C:\Users\Indhu>ping www.facebook.com
Pinging star-mini.c10r.facebook.com [163.70.139.35] with 32 bytes of data:
Reply from 163.70.139.35: bytes=32 time=649ms TTL=56
Reply from 163.70.139.35: bytes=32 time=538ms TTL=56
Reply from 163.70.139.35: bytes=32 time=565ms TTL=56
Reply from 163.70.139.35: bytes=32 time=192ms TTL=56
Ping statistics for 163.70.139.35:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 192ms, Maximum = 649ms, Average = 486ms
C:\Users\Indhu>


Internet Address Physical Address Type
10.1.0.1 c8-4f-86-fc-00-0f dynamic
10.1.0.11 a0-b3-39-cc-06-0f dynamic
10.1.0.219 e6-c5-8a-1c-a1-e3 dynamic
10.1.1.8 82-68-cc-7d-1f-5b dynamic
10.1.4.137 b4-8c-9d-d7-8a-3b dynamic
10.1.5.64 72-8c-a7-c3-23-d3 dynamic
10.1.9.36 c6-22-87-69-9a-97 dynamic
10.1.9.118 28-d0-43-52-c0-fc dynamic
10.1.12.177 a2-66-64-80-8c-40 dynamic
10.1.12.211 32-d8-71-42-0c-47 dynamic
10.1.15.255 ff-ff-ff-ff-ff-ff static
224.0.0.2 01-00-5e-00-00-02 static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static
Interface: 172.31.144.1 --- 0x2e
Internet Address Physical Address Type
172.31.145.156 00-15-5d-2e-02-98 dynamic
172.31.159.255 ff-ff-ff-ff-ff-ff static
224.0.0.2 01-00-5e-00-00-02 static
224.0.0.22 01-00-5e-00-00-16 static
34°C
Partly sunny
Search
ENG
IN
18:43
08-03-2025


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ipv6.addr == 2001:db8::1
No. Time Source Destination Protocol Lengt Info
347 4.195117 18.67.161.45 10.1.10.139 TCP 1494 443 → 59960 [ACK] Seq=47275 Ack=2845 Win=72704 Len=1440 [TCP PDU reassembled in 354]
348 4.195117 18.67.161.45 10.1.10.139 TCP 1494 443 → 59960 [ACK] Seq=48715 Ack=2845 Win=72704 Len=1440 [TCP PDU reassembled in 354]
349 4.195117 18.67.161.45 10.1.10.139 TCP 1494 443 → 59960 [ACK] Seq=50155 Ack=2845 Win=72704 Len=1440 [TCP PDU reassembled in 354]
350 4.195117 18.67.161.45 10.1.10.139 TCP 2934 443 → 59960 [PSH, ACK] Seq=51595 Ack=2845 Win=72704 Len=2880 [TCP PDU reassembled in 354]
351 4.195186 10.1.10.139 18.67.161.45 TCP 54 59960 → 443 [ACK] Seq=2845 Ack=54475 Win=65280 Len=0
352 4.196813 18.67.161.45 10.1.10.139 TCP 2934 443 → 59960 [ACK] Seq=54475 Ack=2845 Win=72704 Len=2880 [TCP PDU reassembled in 354]
353 4.196860 10.1.10.139 18.67.161.45 TCP 54 59960 → 443 [ACK] Seq=2845 Ack=57355 Win=65280 Len=0
354 4.198543 18.67.161.45 10.1.10.139 TLSv1.3 244 Application Data
355 4.198543 18.67.161.45 10.1.10.139 TLSv1.3 479 Application Data
356 4.198592 10.1.10.139 18.67.161.45 TCP 54 59960 → 443 [ACK] Seq=2845 Ack=57970 Win=64768 Len=0
359 4.205808 18.67.161.45 10.1.10.139 TCP 1494 443 → 59960 [ACK] Seq=57970 Ack=2845 Win=72704 Len=1440 [TCP PDU reassembled in 372]
360 4.205808 18.67.161.45 10.1.10.139 TCP 1494 443 → 59960 [ACK] Seq=59410 Ack=2845 Win=72704 Len=1440 [TCP PDU reassembled in 372]
361 4.205808 18.67.161.45 10.1.10.139 TCP 1494 443 → 59960 [ACK] Seq=60850 Ack=2845 Win=72704 Len=1440 [TCP PDU reassembled in 372]
362 4.205808 18.67.161.45 10.1.10.139 TCP 1494 443 → 59960 [PSH, ACK] Seq=62290 Ack=2845 Win=72704 Len=1440 [TCP PDU reassembled in 372]
363 4.205808 18.67.161.45 10.1.10.139 TCP 1494 443 → 59960 [ACK] Seq=63730 Ack=2845 Win=72704 Len=1440 [TCP PDU reassembled in 372]
364 4.205808 18.67.161.45 10.1.10.139 TCP 2934 443 → 59960 [ACK] Seq=65170 Ack=2845 Win=72704 Len=2880 [TCP PDU reassembled in 372]
365 4.205883 10.1.10.139 18.67.161.45 TCP 54 59960 → 443 [ACK] Seq=2845 Ack=68050 Win=65280 Len=0
366 4.205940 18.67.161.45 10.1.10.139 TCP 2934 443 → 59960 [PSH, ACK] Seq=68050 Ack=2845 Win=72704 Len=2880 [TCP PDU reassembled in 372]
Frame 350: 2934 bytes on wire (23472 bits), 2934 bytes captured (23472 bits) on interface \Device\NPF
Ethernet II, Src: 1a:7b:e9:20:d5:52 (1a:7b:e9:20:d5:52), Dst: AzureWaveTec_8f:24:97 (50:5a:65:8f:24:9
Destination: AzureWaveTec_8f:24:97 (50:5a:65:8f:24:97)
Source: 1a:7b:e9:20:d5:52 (1a:7b:e9:20:d5:52)
Type: IPv4 (0x0800)
[Stream index: 11]
Internet Protocol Version 4, Src: 18.67.161.45, Dst: 10.1.10.139
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 2920
Identification: 0x4404 (17412)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 250
Protocol: TCP (6)
Header Checksum: 0xa98f [validation disabled]
[Header checksum status: Unverified]





Rubrics for Wireshark labs:

Rubrics	Excellent	Fair	Poor	Marks
Understanding (2)	Understand the Concept very well. (2)	Understand the Concept (1)	Poor Understand the Concept (0)	
Usage of filters (3)	Identified and applied the filter correctly (3)	Identified the filter, but not applied correctly (2-1)	Couldn't identify and apply the filter. Just captured the packets (1)	
Attach relevant Screenshots (3)	clearly Highlighted the answers and attached the screenshots (3)	attached the screenshots, but not highlighted. (2-1)	Did not attach the screenshots (0)	
On time Submission (2)	Early or on time submission (2)	Submitted after deadline (1)	Did not Submit (0)	
			Total	

CONCLUSION:

Thus, the Capture and Analyze TCP and IP packets has implemented successfully by using WIRESHARK.

Register No:	**99220041762**
Name:	**G.Asish**
Class/Section:	**8301A/S18**
Ex.No:	**11**
Name of the Experiment	Capture and analyze the TCP 3 way handshake
Google Drive link of the packet tracer file (give view permission):	https://drive.google.com/drive/folders/1kZYMTJ0uZatmg4XpevUQnRGjCA_W4BOF

Objective(s):

To capture and analyse TCP 3-way handshake packet using Wireshark.

Introduction:

TCP or Transmission Control Protocol is one of the most important protocols or standards for enabling communication possible amongst devices present over a particular network. It has algorithms that solve complex errors arising in packet communications, i.e. corrupted packets, invalid packets, duplicates, etc. Since it is used with IP(Internet Protocol), many times it is also referred to as TCP/IP. In order to start a communication, the TCP first establishes a connection using the three-way- handshake. TCP's efficiency over other protocols lies in its error detecting and correction attribute. Not only this, it organizes packets and segments larger data into a number of packets without disrupting the integrity of the data.

So now we are a bit familiar with TCP, let's look at how we can analyze TCP using Wireshark, which is the most widely used protocol analyzer in the world.

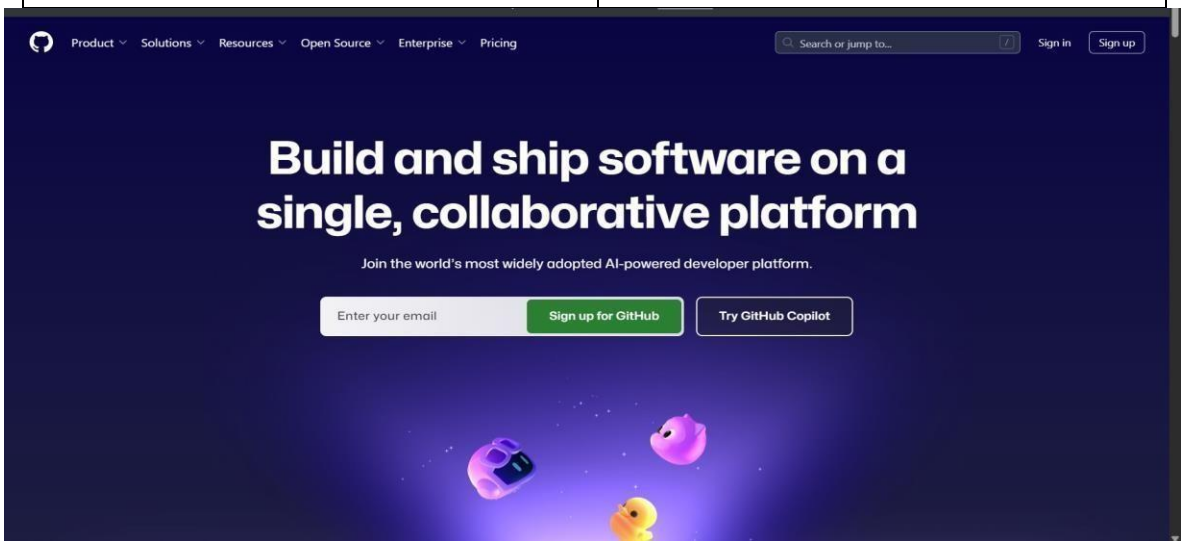
Here you will have the list of TCP packets. The first three packets of this list are part of the three-way handshake mechanism of TCP to establish a connection. Let's get a basic knowledge of this mechanism which happens in the following 3 steps:

- A synchronization packet (SYN) is sent by your local host IP to the server it desires to connect to.
- The server reciprocates by sending an acknowledgment packet (ACK) to the local host signaling that it has received the SYN request of the host IP to connect and also sends a synchronization packet (SYN) to the local host to confirm the connection. So this one is basically an SYN+ACK packet.
- The host answers this request by sending the ACK on receiving the SYN of the server.

1. Visit any one website by opening a browser fill your machine details(attach relevant screenshots)

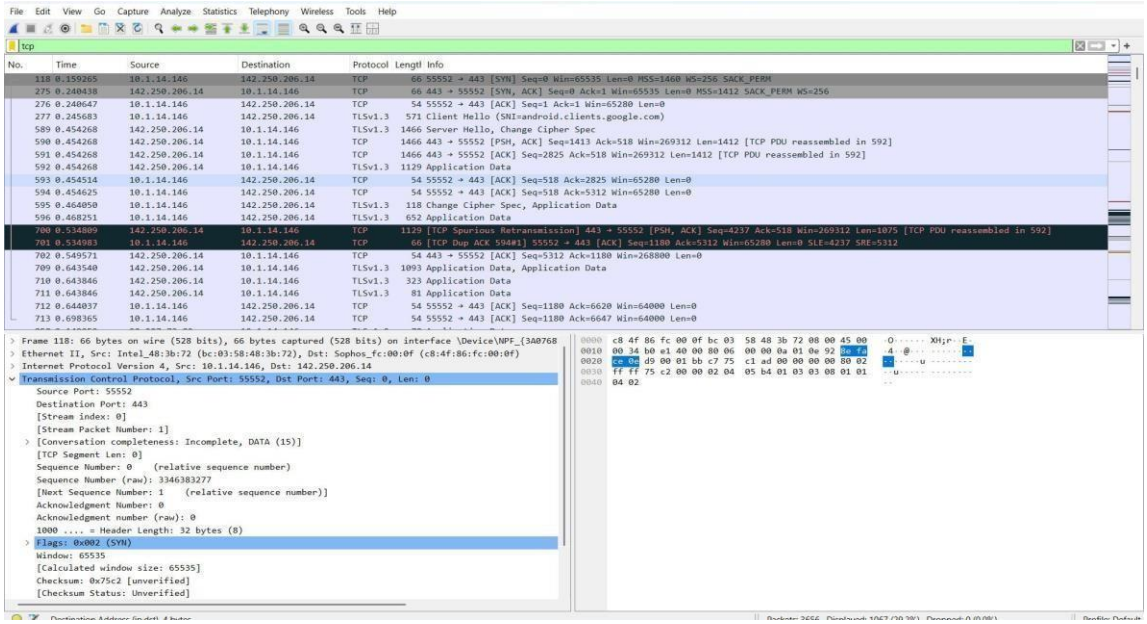
Parameter	Value
Your Machine IP Address.	10.1.14.146
Your Machine MAC Address	BC-03-58-48-3B-72
Default Gateway address	10.1.0.1

Website URL	https://github.com/
Website IP Address	142.250.206.14



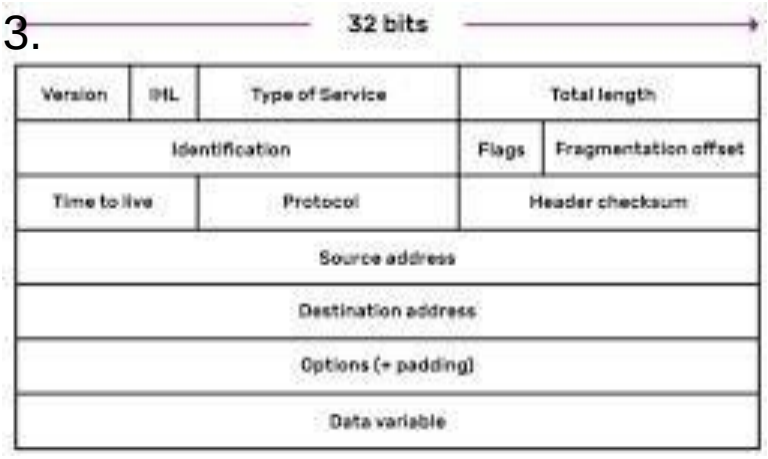
2. Fill the following details:

Field Name	Field Length (no of bits)	Field value
Destination MAC address	48	C8:4F:86:FC:00:0F
Source MAC address	48	BC-03-58-48-3B-72
Destination IP address	32	142.250.206.14
Source IP Address .	32	10.1.14.146
Destination TCP port	16	443
Source TCP port	16	55552



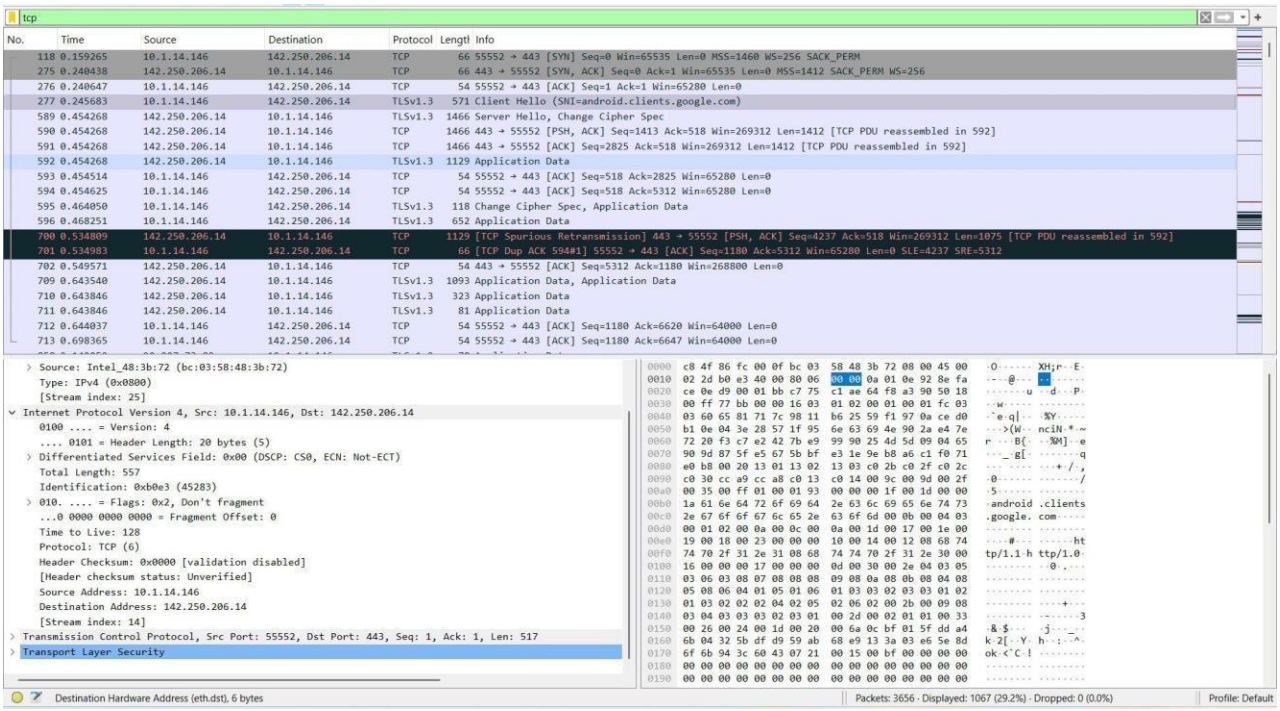
3. Fill the details as per the IP frame format .(highlight the details for each of the output and paste screenshot)

3.



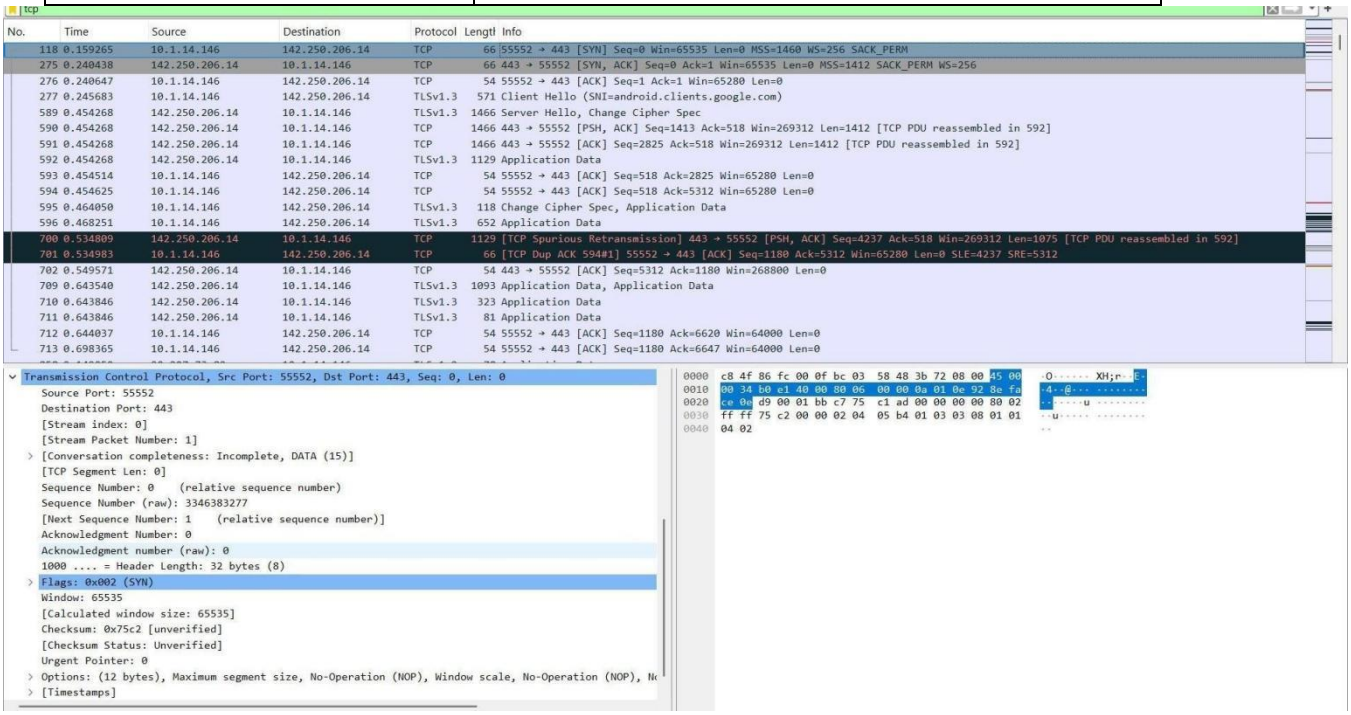
IPV4	20	TOS	557
0xb0e3		0x2	0
128	Tcp	0x0000	
10.1.14.146			
142.250.206.14			
Options (+ Padding)			

4. Using the Wireshark capture of the first TCP session startup (SYN bit set to 1), fill in information about the TCP header. (paste screenshot for each of the output). Capture the packet and analyze it.



5. Fill in the following information regarding the SYN message.(highlight the details for each of the output and paste screenshot)

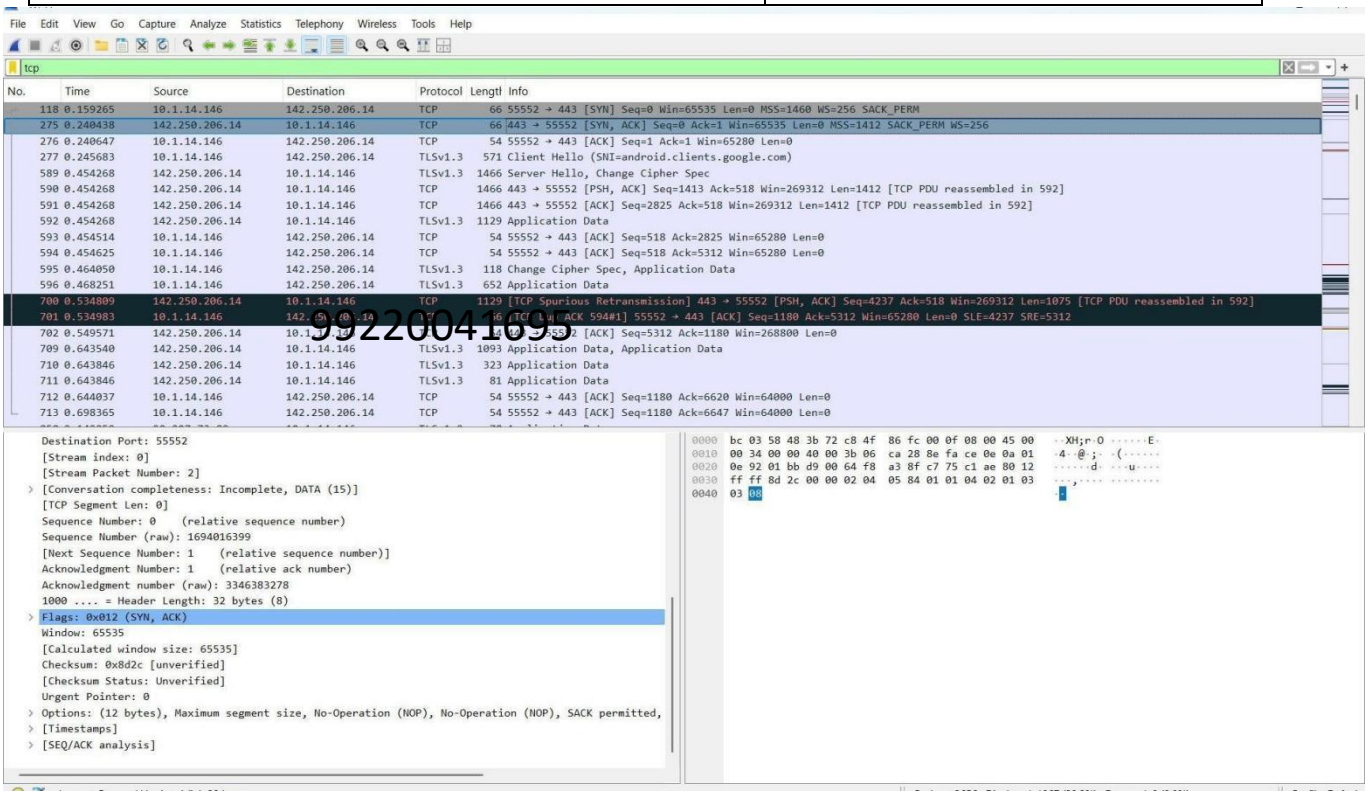
Source IP address	10.1.14.146
Destination IP address	142.250.206.14
Source port number	55552
Destination port number	443
Sequence number	0
Acknowledgement number	0
Flags	0x002
Header length	32bytes
Window size	65535
Checksum	0x75c2



6. Fill in the following information regarding the SYN-ACK message .(highlight the details for each of the output and paste screenshot)

Source IP address	142.250.206.14
Destination IP address	10.1.14.146
Source port number	443

Destination port number	55552
Sequence number	0
Acknowledgement number	1
Header length	20 bytes
Window size	65535
Flags	0x012
Checksum	0x8d2c

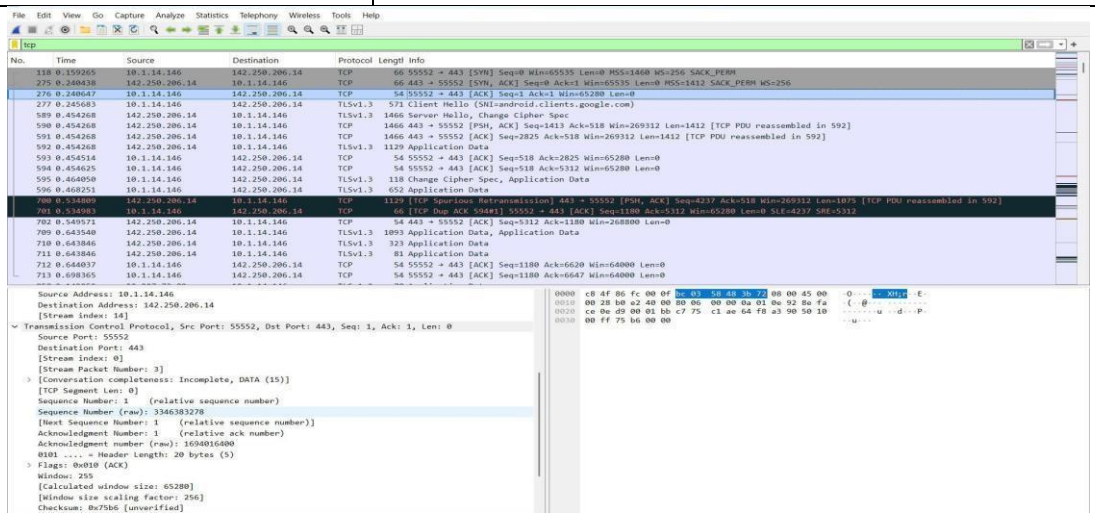


7. Fill in the following information regarding the ACK message. .(highlight the details for each of the output and paste screenshot)

99220041762

Source IP address	10.1.14.146
Destination IP address	142.250.206.14
Source port number	55552
Destination port number	443
Sequence number	1

Acknowledgement number	1
Header length	20
Window size	65280
Flags	0x010
Checksum	0x75b6



Rubrics for Wireshark labs: (To be Filled by the Class Teacher)

Rubrics	Excellent	Fair	Poor	Marks
Understanding (2)	Understand the Concept very well. (2)	Understand the Concept (1)	Poor Understand the Concept (0)	
Usage of filters (3)	Identified and applied the filter correctly (3)	Identified the filter, but not applied correctly (2-1)	Couldn't identify and apply the filter. Just captured the packets (1)	
Attach relevant Screenshots (3)	clearly Highlighted the answers and attached the screenshots (3)	attached the screenshots, but not highlighted. (2-1)	Did not attach the screenshots (0)	
On time Submission (2)	Early or on time submission (2)	Submitted after deadline (1)	Did not Submit (0)	
			Total	

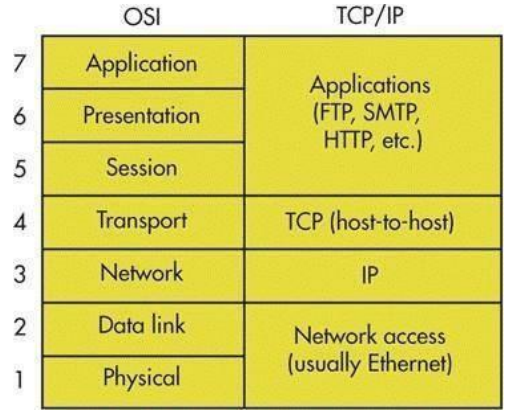
Register No:	**99220041762**
Name:	**G.Asish**
Class/Section:	**8301A/S18**
Ex.No:	**12**
Name of the Experiment	**Capture and analyze the HTTP protocol**
Google Drive link of the packet tracer file (give view permission):	https://drive.google.com/drive/folders/1kZYMTJ0uZatmg4XpevUQnRGjCA_W4BOF

Objective(s):

To capture and analyse TCP and IP packet using Wireshark.

Introduction:

Full form of HTTP is HyperText Transfer Protocol. HTTP is an application layer protocol in ISO or TCP/IP model. See below picture to find out HTTP which resides under application layer.



HTTP is used by the World Wide Web (w.w.w) and it defines how messages are formatted and transmitted by browser. So HTTP define rules what action should be taken when a browser receives HTTP command. And also HTTP defines rules for transmitting HTTP command to get data from server.

For example, when you enter a url in browser (Internet explorer, Chrome, Firefox, Safari etc) it actually sends an HTTP command to server. And server replies with appropriate command.

HTTP Methods:

There are some set of methods for HTTP/1.1 (This is HTTP version) GET, HEAD, POST, PUT, DELETE, CONNECT, OPTION and TRACE.

We will not go in details of each method instead we will get to know about the methods which are seen quite often. Such as

GET: GET request asks data from web server. This is a main method used document retrival. We will see one practical example of this method.

POST: POST method is used when it's required to send some data to server.

HTTP is Wiresahark:

Let's try something practical to understand how HTTP works ?

So in this example we will download **"alice.txt" (Data file present in server)** from **"gaia.cs.umass.edu"** server.

Setps:

1. Open any URL http://gaia.cs.umass.edu/wireshark-labs/alice.txt 2.

Now we see the downloaded file in browser. Here is the screenshot

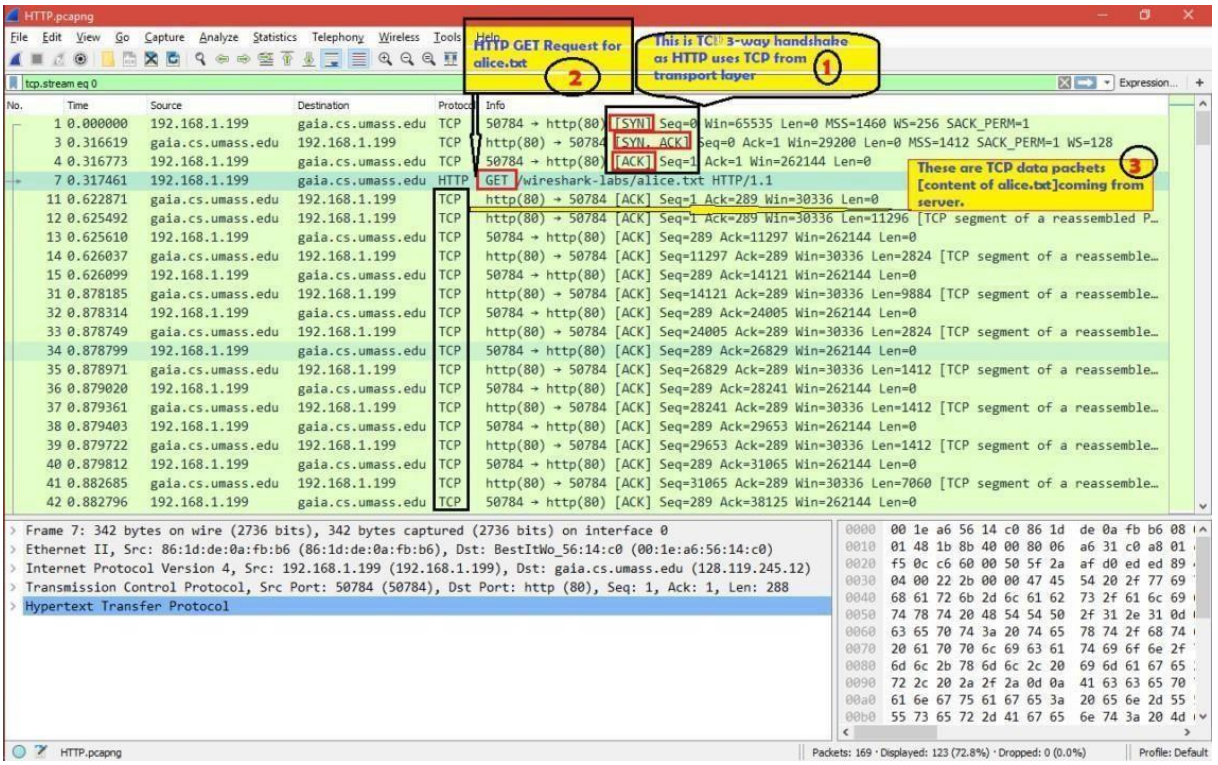
3. In parallel we have capture the packets in Wireshark.

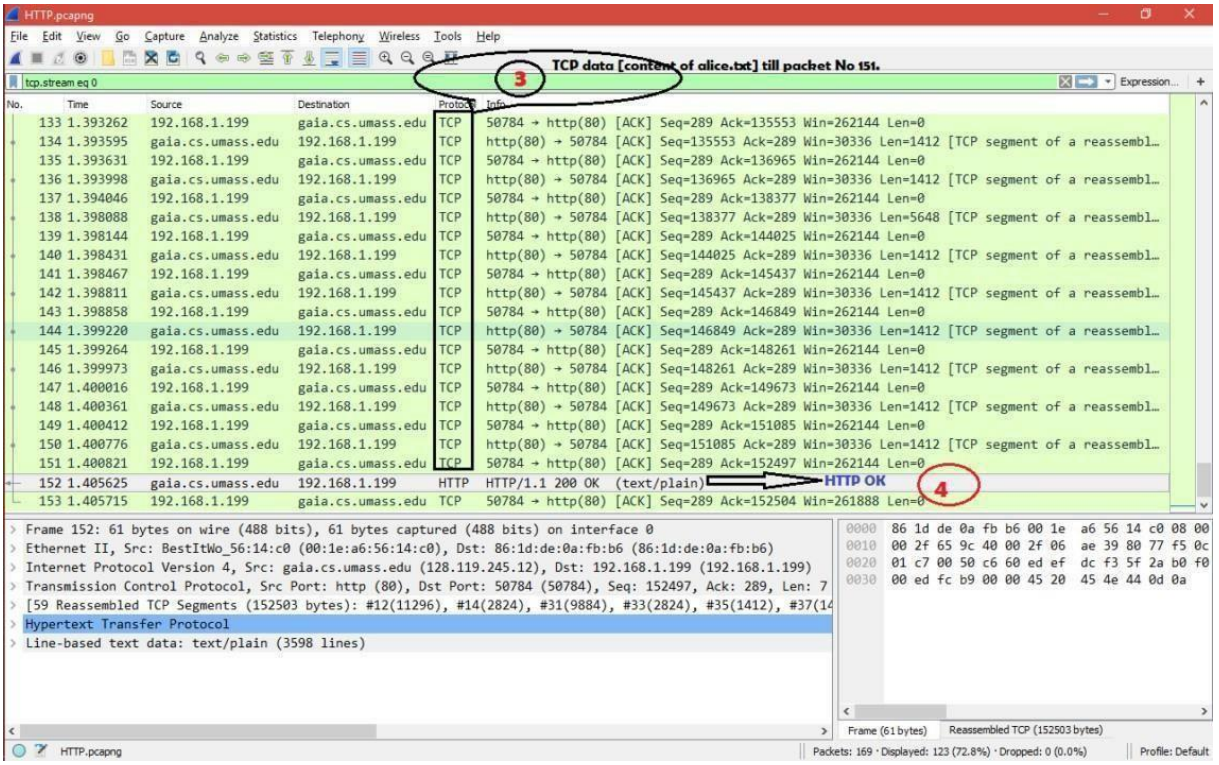
HTTP packets exchanges in Wireshark:

Before we go into HTTP we should know that HTTP uses port 80 and TCP as transport layer protocol [We will explain TCP in another topic discussion].

Now let's see what happens in network when we put that URL and press enter in browser. Here is the screenshot for

TCP 3-way handshake ——-> HTTP OK ——-> TCP Data [content of alice.txt] ——-> HTTP-OK





Now let's see what's there inside HTTP GET and HTTP OK packets. Note: We will explain TCP exchanges in another topic discussion. **HTTP GET:**

After TCP 3-way handshake [SYN, SYN+ACK and ACK packets] is done HTTP GET request is sent to the server and here are the important fields in the packet.

1. **Request Method: GET ==>** The packet is a HTTP GET .

2. **Request URI: /wireshark-labs/alice.txt** ==> The client is asking for file alice.txt present under /Wireshark-labs

3. **Request version:** HTTP/1.1 ==> It's HTTP version 1.1

4. **Accept: text/html, application/xhtml+xml, image/jxr, */* ==>** Tells server about the type of file it [client side browser] can accept. Here the client is expecting alice.txt which is text type.

5. **Accept-Language: en-US ==>** Accepted language standard.

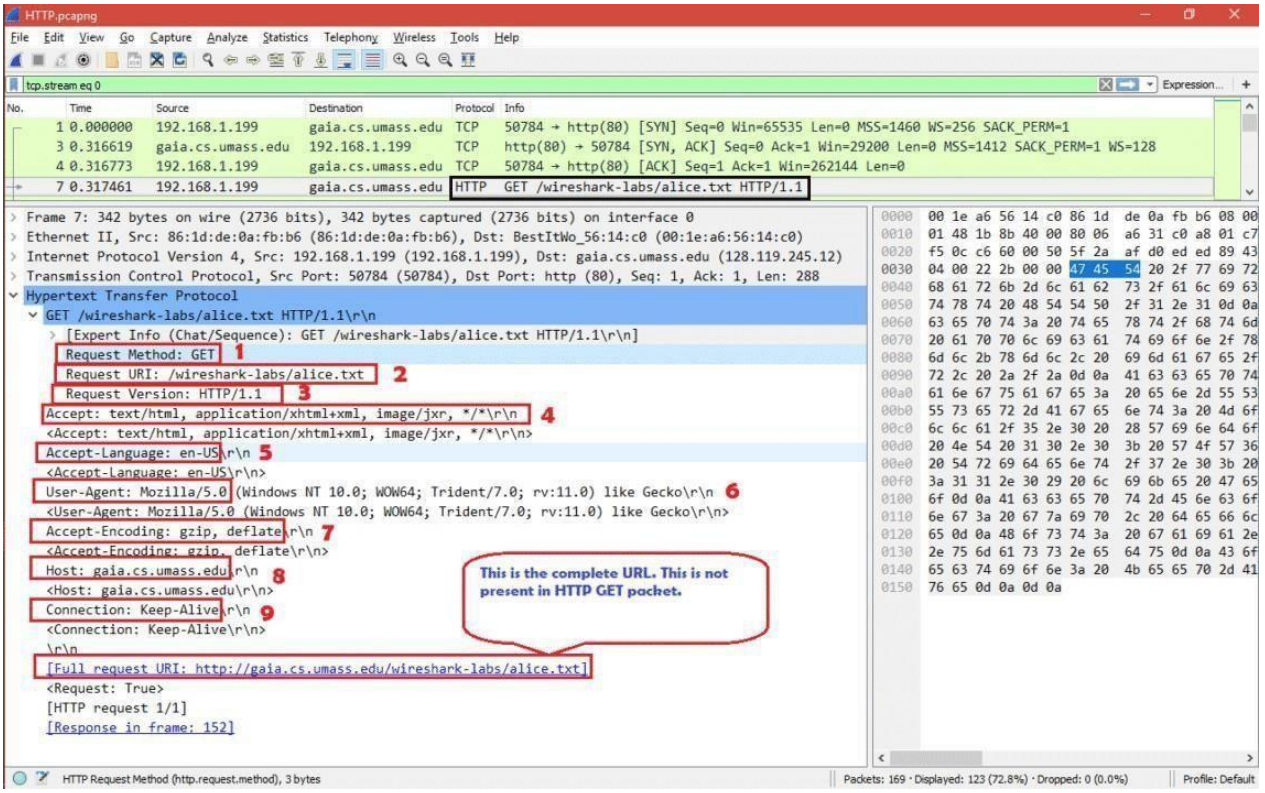
6. **User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko ==>** Client side browser type. Even if we used internet explorer but we see it always/maximum time says Mozilla

7. **Accept-Encoding: gzip, deflate** ==> Accepted encoding in client side.

8. **Host: gaia.cs.umass.edu** ==> This is the web server name where client is sending HTTP GET request.

9.Connection: Keep-Alive ==> Connection controls whether the network connection stays open after the current transaction finishes. Connection type is keep alive.

Here is the screenshot for HTTP-GET packet fields



HTTP OK:

After TCP data [content of alice.txt] is sent successfully HTTP OK is sent to the client and here are the important fields in the packet.

1. **Response Version: HTTP/1.1 ==>** Here server also in HTTP version 1.1

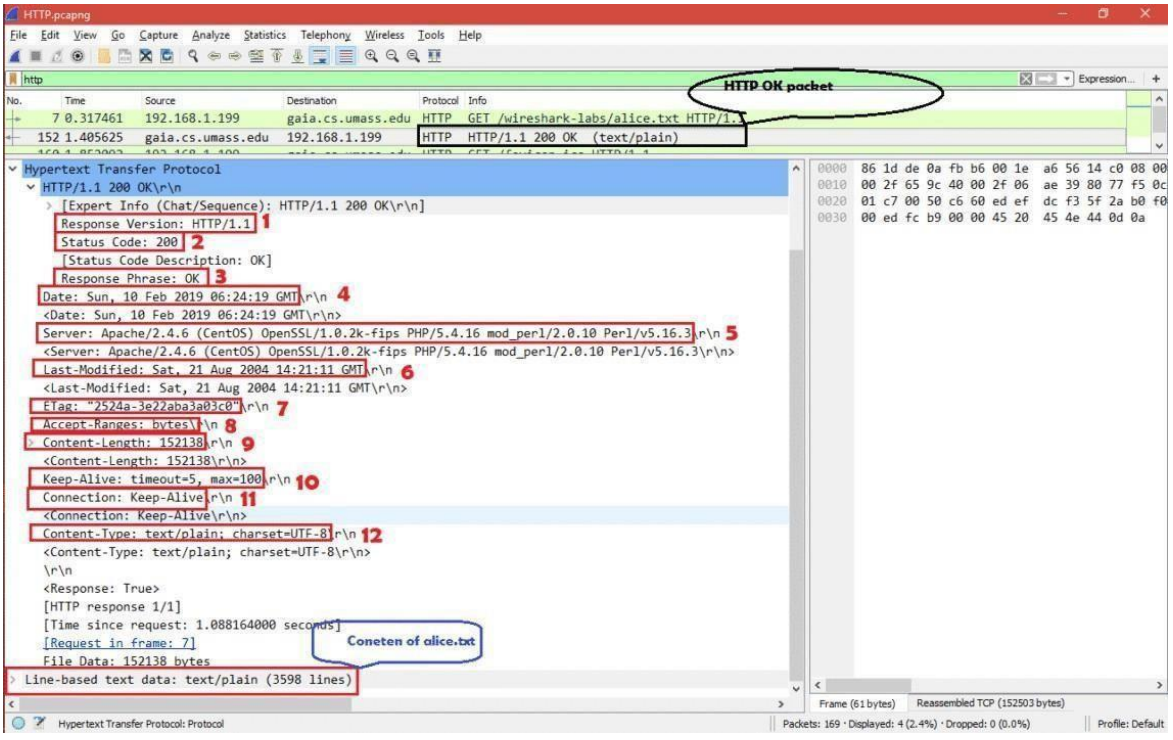
2. **Status Code: 200** ==> Status code sent by server.

3. **Response Phrase: OK** ==> Response phrase sent by server.

So the from 2 and 3 we get 200 OK which means the request [HTTP GET] has succeeded.

4. **Date: Sun, 10 Feb 2019 06:24:19 GMT** ==> Current date , time in GMT when HTTP GET was received by server.
5. **Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3** ==> Server details and configurations versions.
6. **Last-Modified**: **Sat, 21 Aug 2004 14:21:11 GMT** ==> Last modified date and time for the file "alice.txt".
7. **ETag: "2524a-3e22aba3a03c0" ==>** The ETag indicates the content is not changed to assist caching and improve performance. Or if the content has changed, etags are useful to help prevent simultaneous updates of a resource from overwriting each other.
8. **Accept-Ranges: bytes ==>** Byte is the unit used in server for content.
9. **Content-Length: 152138 ==>** This is the total length of the alice.txt in bytes.
10. **Keep-Alive: timeout=5, max=100** ==> Keep alive parameters.
11. **Connection: Keep-Alive** ==> Connection controls whether the network connection stays open after the current transaction finishes. Connection type is keep alive.
12. **Content-Type: text/plain; charset=UTF-8 ==>** The content [alice.txt] type is text and charset standard is UTF-8.

Here is the screenshot for different fields of HTTP OK packet.



So now we know what happens when we request for any file that is present in web server.

Conclusion:

HTTP is simple application protocol that we use every day in our life. But it's not secure so HTTPS has been implemented. That "S" stands for secure. That's why you so maximum web server name start with http***s://[websitename]***. This means all communication between you and server are encrypted. We will have separate discussion on this HTTPS in future.

99220041762

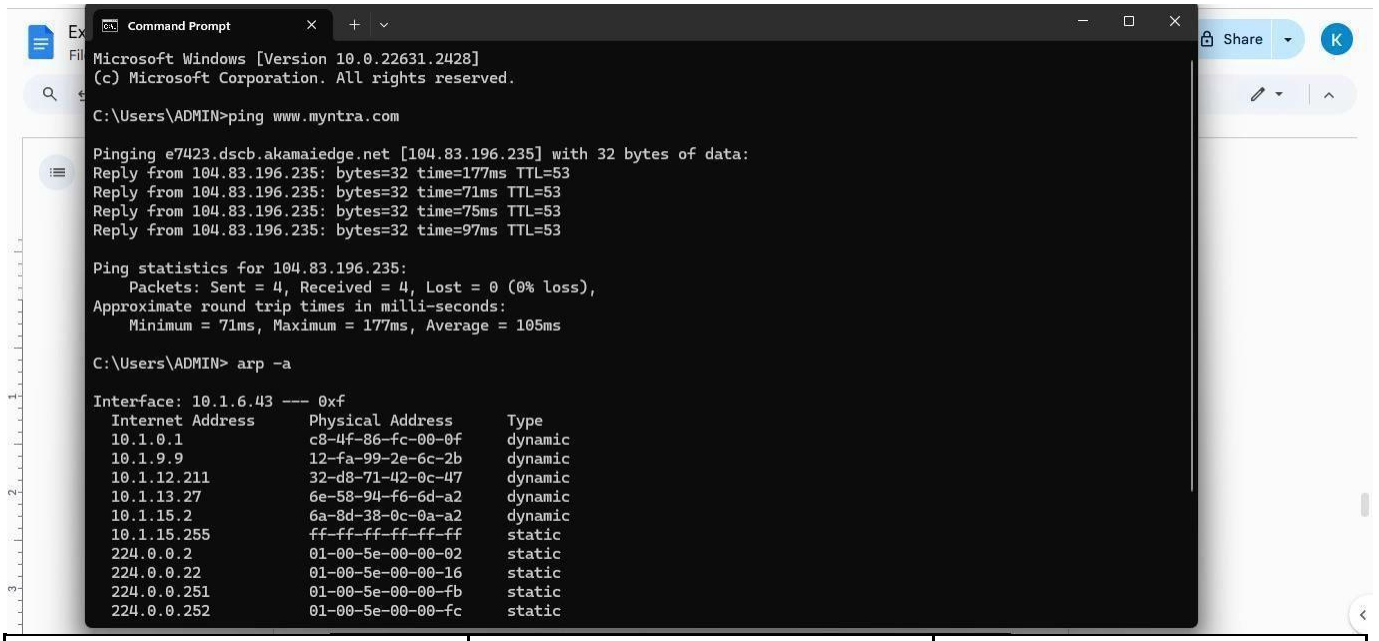
Exercise:

Analyze the HTTP protocol usingWireshark by visiting any URL.

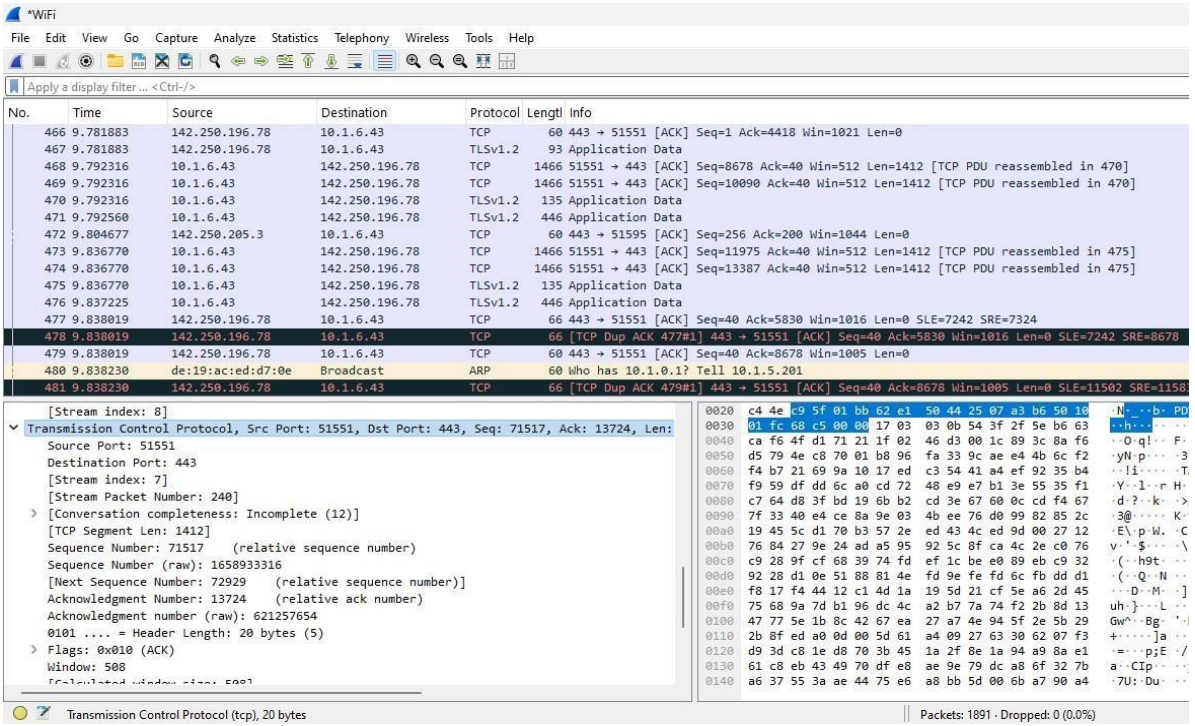
1. Visitany one website by opening a browser fill your machine details (attach relevant screenshots).

Parameter	Value
Your MachineIP Address.	192.168.213.64
Your MachineMACAddress	CC-47-40-59-DC-B8
Default Gateway address	192.168.213.158
WebsiteURL	www.myntra.com
WebsiteIP Address	104.83.196.235

2. Fill the TCP connection segment details:



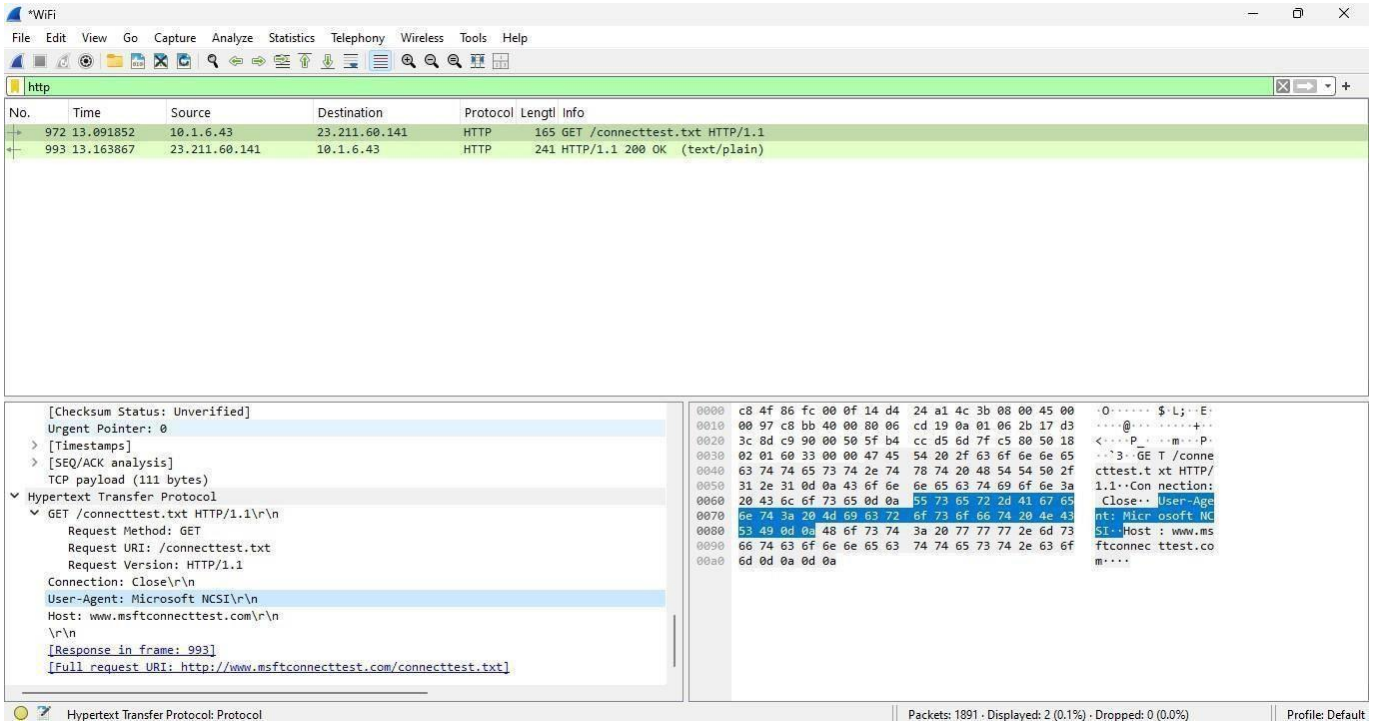
Field Name	Field Length (no of bits)	Field value
DestinationMAC address	48	C8:4f:86:fc:00:10
Source MAC address	48	CC-47-40-59-DC-B8
Destination IP address	32	104.83.196.235
Source IP Address	32	192.168.213.64
Destination TCP port	16	51551
Source TCP port	16	443



3. HTTP Request Message Details.

Field Name	Field Length (# of Bits)	Field Value (Binary or Hexa value)
Method	24	GET
Host	104	www.msftconnecttest.com
Accept	304	
User-Agent	144	Microsoft NCSI
Accept-Language	40	
Accept-Encoding	24	
Connection	80	Close

Paste the HTTP Response Screenshot:



Paste the Wireshark File with view permission:

https://drive.google.com/drive/folders/1ps1OS8kWsComBI4n6erG2VDeZSZanCar

Conclusion: The above experiment has been executed and successfully implememted.

Google Drive

Link:https://drive.google.com/drive/folders/1vhp9EeJq7i0LwOYGriXuL6Bz_maqpT ok

RubricsRubricsfor Wireshark	labs: (To Excellentbe Filled by the Cl	ss Teacher)Fair	Poor	Marks
Understanding (2)	Understand the Concept very well. (2)	Understand the Concept (1)	Poor Understand the Concept (0)	
Usage of filters (3)	Identified and applied the filter correctly (3)	Identified the filter, but not applied correctly (2-1)	Couldn't identify and apply the filter. Just captured the packets (1)	
Attach relevant Screenshots (3)	clearly Highlighted the answers and attached the screenshots (3)	attached the screenshots, but not highlighted. (2-1)	Did not attach the screenshots (0)	
On time Submission (2)	Early or on time submission (2)	Submitted after deadline (1)	Did not Submit (0)	
			Total	

Register No:	**99220041762**
Name:	**G.Asish**
Class/Section:	**8301A/S18**
Ex.No:	**13**
Name of the Experiment	**Capture and Anlyze ICMP packet**
Google Drive link of the packet tracer file (give view permission):	**https://drive.google.com/drive/folders/19Anx7mMIpy0ZHRjeJmOnOoTXjkDQ9Xpf**

Objective(s):

To capture and analyse ICMP Request Response packet using Wireshark.

Introduction:

The **I**nternet **C**ontrol **M**essage **P**rotocol (**ICMP**) is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information which indicates that a requested service is not available or that a host or router could not be reached.

It is layer 3 i.e. network layer protocol used by the ping command for sending a message through ICMP payload which is encapsulated with IP Header Packet. According to MTU the size of the ICMP packet cannot be greater than 1500 bytes.

ICMP packet at Network layer

IP header	ICMP header	ICMP payloadsize	MTU (1500)
20 bytes	8 bytes	1472 bytes (maximum)	20 + 8 + 1472 = 1500

ICMP packet at Data Link layer

Ethernetheader	IP header	ICMP header	ICMP payloadsize	MTU (1514)
14	20 bytes	8 bytes	1472 bytes (maximum)	14 + 20 + 8 + 1472 = 1514

ICMP Messagecode & Packet descriptionwith Wireshark

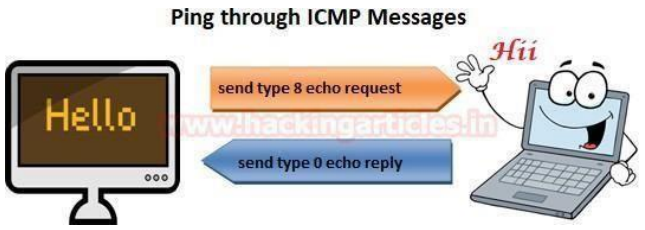
ICMP message contains two types of codes i.e. query and error.

Query: The query messages are the information we get from a router or another destination host.

For example, given below message types are some ICMP query codes:

- Type 0 = Echo Reply
- Type 8 = Echo Request
- Type 9 = Router Advertisement
- Type 10 = Router Solicitation
- Type 13 = Timestamp Request
- Type 14 = Timestamp Reply

A ping command sends an ICMP **echo request** to the target host. The target host responds with an **echo Reply** which means the target host is alive.

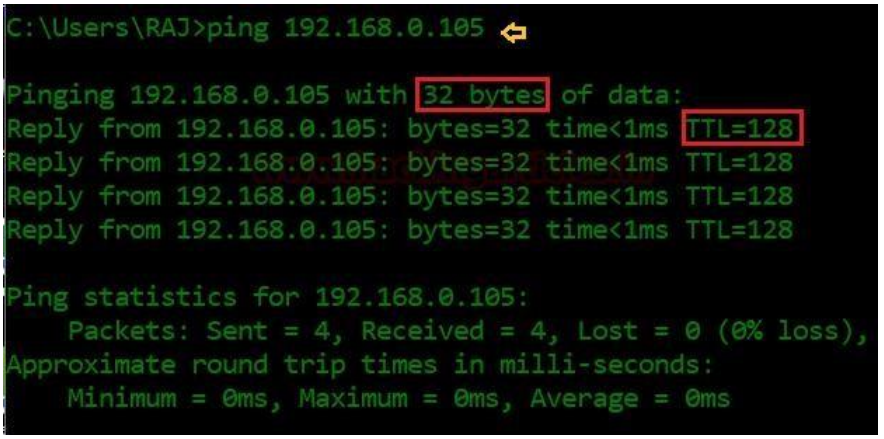


Here we are going to test how ping command helps in identifying an alive host by Pinging host IP.

```
ping 192.168.0.105
```

From the given below image you can see a reply from the host; now notice a few more things as given below:

- The default size of payload sent by source machine is 32 bytes (**request**)
- The same size of payload received by source machine is 32 bytes from Destination machine (**reply**) • **TTL= 128** which means host machine is windows system. • Total packets are **8**, 4 packets of the request and 4 of reply.

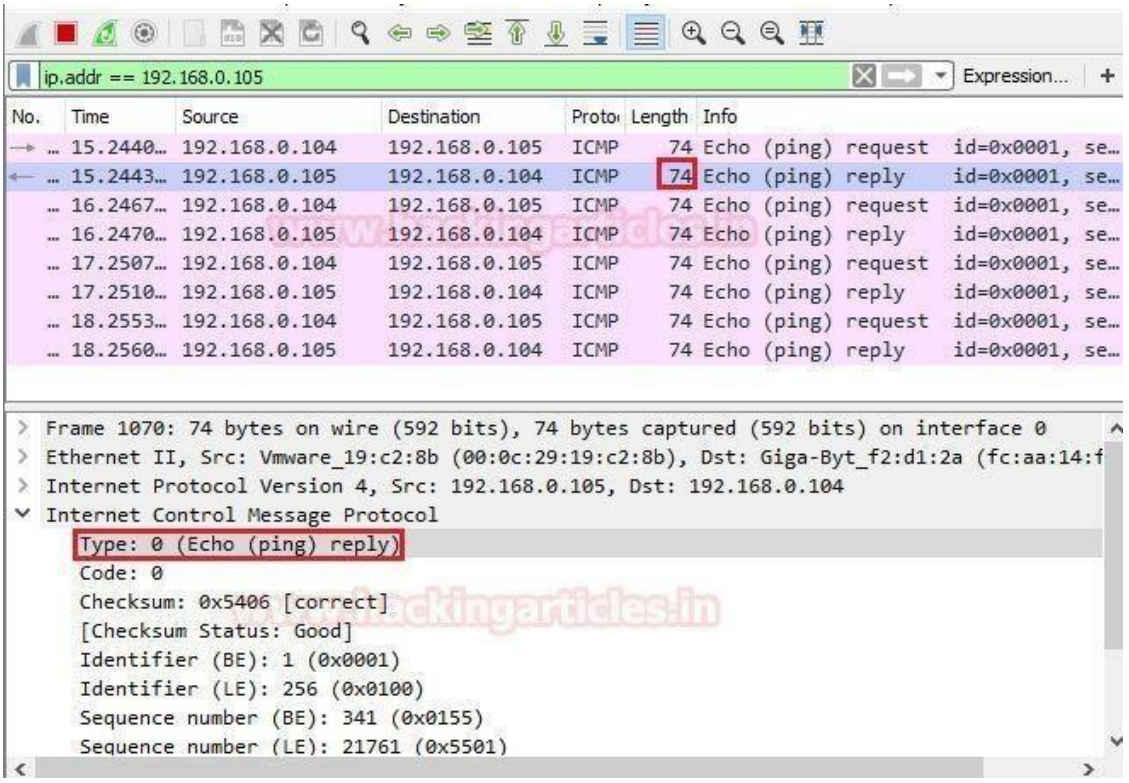


Look over the sequence of packet transfer between source and destination captured through Wireshark.

Total numbers of packet captured are 8, 4 for request and 4 for reply between the source and destination machine.

The 1st packet is sent by source machine is ICMP echo request and if you look by the given below image, you will observe highlighted text is showing ICMP query code: **type 8 echo ping request.**

Similarly given below image is showing details of **2nd** packet i.e. Echo reply, you can observe that the highlighted text is showing ICMP query code: **type 0 echo ping reply.**



Error: The error statement messages reports problem which a router or a destination host may generate.

For example: given below message types are some of the ICMP error codes:

- Type 3 = Destination Unreachable
- Type 4 = Source Quench
- Type 5 = Redirect
- Type 11 = Time Exceeded
- Type 12 = Parameter Problems

When we ping an IP sometimes we don't get echo ping reply from the host machine, instead of that, we get some reply such as **destination unreachable** or **time exceeded** this is known as **ICMP error reporting message**. There are so many reasons behind such kind of error message, possibly a host in a network is down or firewall is blocking your ping request.

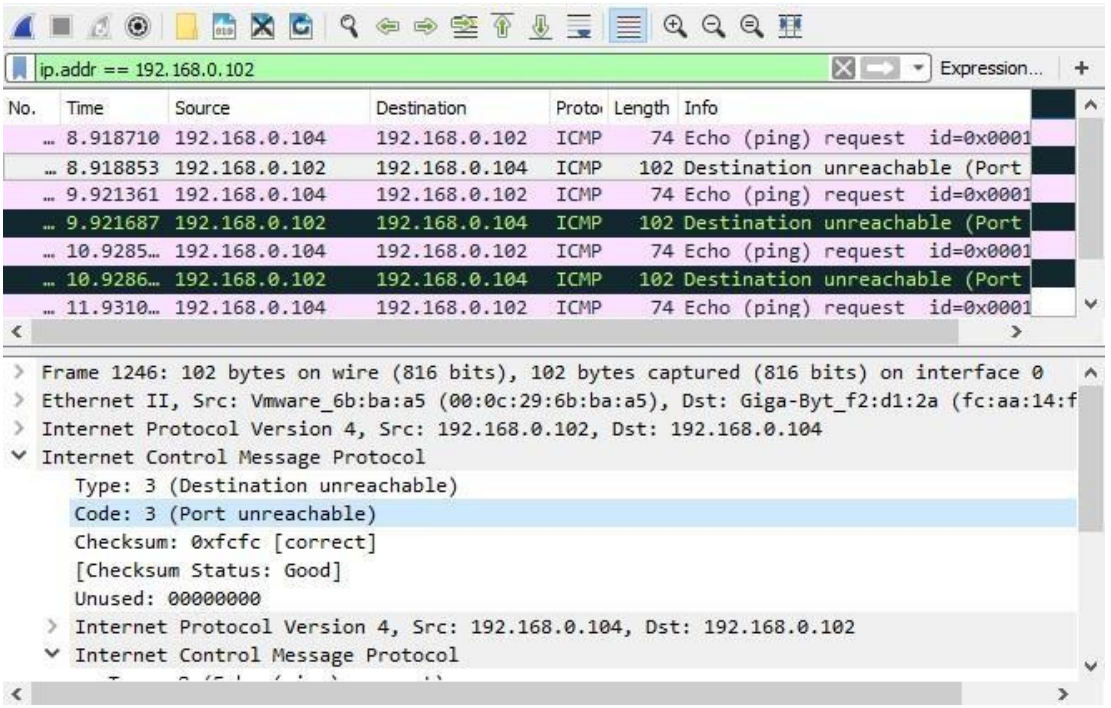
```
C:\Users\RAJ>ping 192.168.0.102

Pinging 192.168.0.102 with 32 bytes of data:
Reply from 192.168.0.102: Destination port unreachable.
Reply from 192.168.0.102: Destination port unreachable.
Reply from 192.168.0.102: Destination port unreachable.
Reply from 192.168.0.102: Destination port unreachable.

Ping statistics for 192.168.0.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

The **1st**packet sends by source machine is ICMP echo request and if you observe by the given below image the highlighted text is showing ICMP query code: **type 8 echo ping request.**

Similarly given below image is showing the detail of **2nd**packet i.e. Destination unreachable, you can observe that it is showing ICMP error code: **type 3.**



ping –a 192.168.0.105

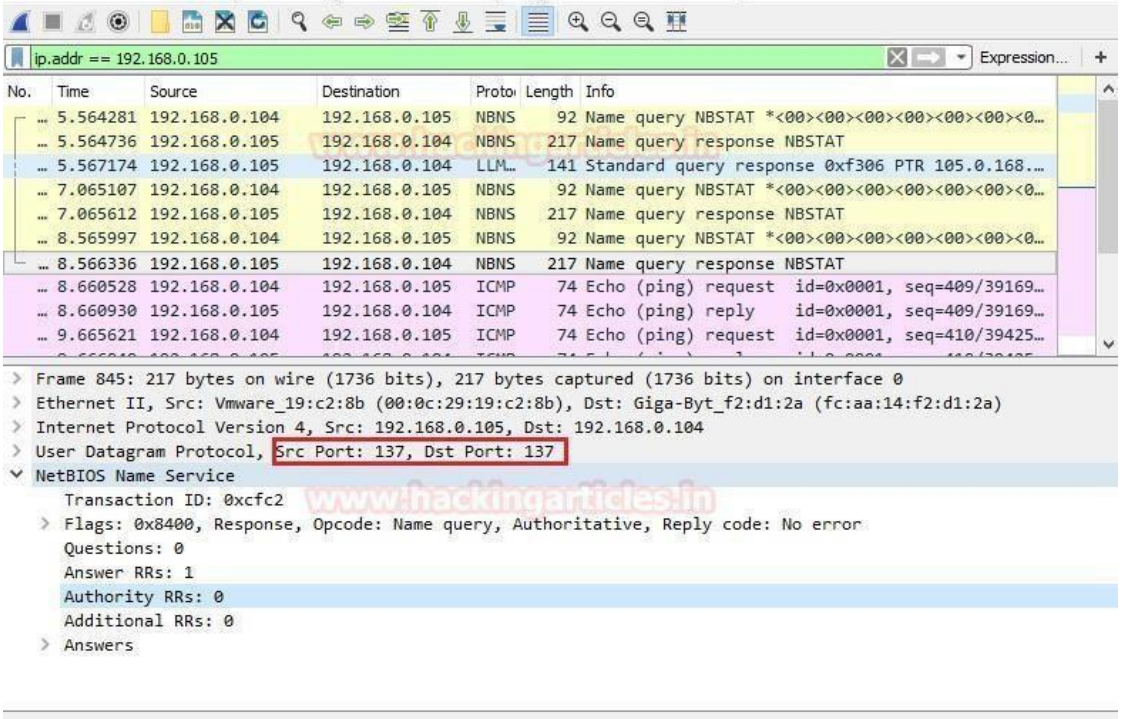
-a: Resolve IP addresses to host-name, identify's that reverse name resolution is carried out on the host IP address. If it is successful, ping shows the matching hostname.

```
C:\Users\RAJ>ping -a 192.168.0.105

Pinging WIN-1GKSSJ7D2AE [192.168.0.105] with 32 bytes of data:
Reply from 192.168.0.105: bytes=32 time<1ms TTL=128
Reply from 192.168.0.105: bytes=32 time<1ms TTL=128
Reply from 192.168.0.105: bytes=32 time<1ms TTL=128
Reply from 192.168.0.105: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.105:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

From the given below image, you can observe that instead of ICMP protocol the ping request has been sent through NBNS (NetBIOS Name Service) protocol through port 137 which is a UDP port.



By default, a ping sends 4 packets of the request and receives the same number of the packet as a reply from the host. You can increase or decrease this number of the packet by using given below command.

```
ping –n 2 192.168.0.105
```

-n: Number of echo requests to send

As we had set -n as 2 packets of request hence we got two packets as a reply.

```
C:\Users\RAJ>ping -n 2 192.168.0.105

Pinging 192.168.0.105 with 32 bytes of data:
Reply from 192.168.0.105: bytes=32 time<1ms TTL=128
Reply from 192.168.0.105: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.105:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Similarly, we can also set TTL (Time to Live) for echo request packet, by default 4 packet of request query are sent from source machine at the rate of 1 millisecond per packet. Suppose we want to give TTL between two packets, set -i as 5ms so that after the first packet is delivered the second packet is sent after

```
5pinmsg·–i 5 192.168.0.105
```

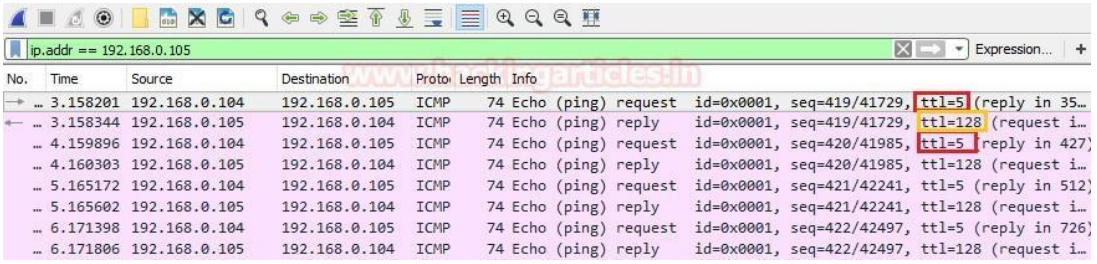
-i TTL: Time To Live

```
C:\Users\RAJ>ping -i 5 192.168.0.105

Pinging 192.168.0.105 with 32 bytes of data:
Reply from 192.168.0.105: bytes=32 time<1ms TTL=128
Reply from 192.168.0.105: bytes=32 time<1ms TTL=128
Reply from 192.168.0.105: bytes=32 time<1ms TTL=128
Reply from 192.168.0.105: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.105:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Let's verify TTL for a packet sent from source to destination through Wireshark. Now if you observe by the given below image you will notice that every echo ping request packet has TTL 5 but every echo reply has default TTL value i.e.128.



As we have discussed above default size of ICMP payload is 32 bytes and the maximum is 1472 if the size of the payload packet is greater than 1472 then packet gets fragmented into small packets.

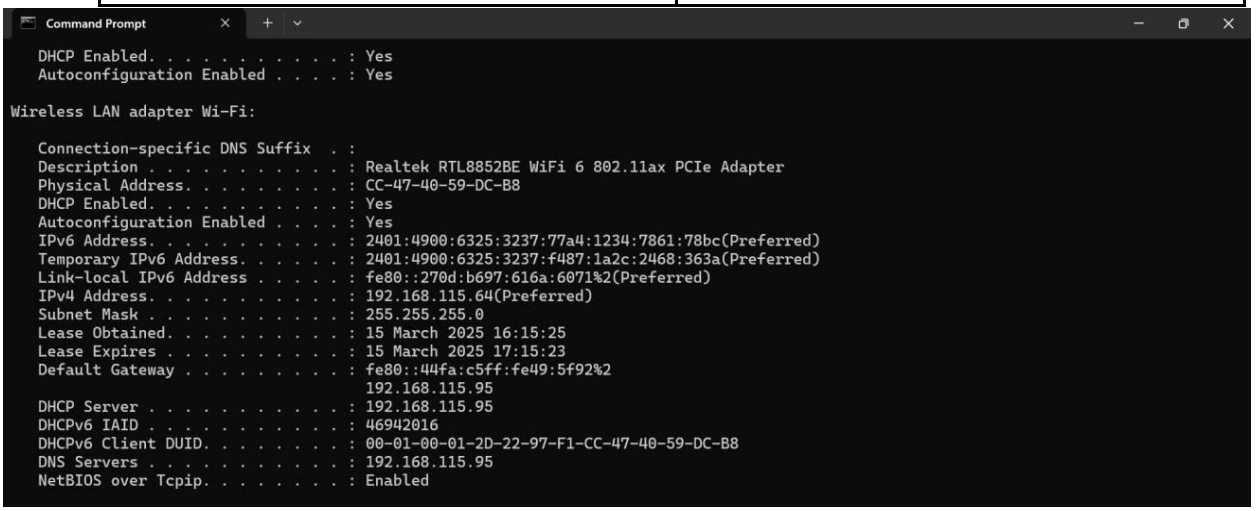
From the given below image, you can observe source has pinged the host which carries default 32 bytes size payload.

Now let check the information payload carries from source to destination using Wireshark. From the given below image, you can read that highlighted texts are alphabets that have been used as 32 bytes payload.

Exercise:

1. Use command prompt and fill the following details using ipconfig /all command. (highlight and paste screenshot for each of the output).

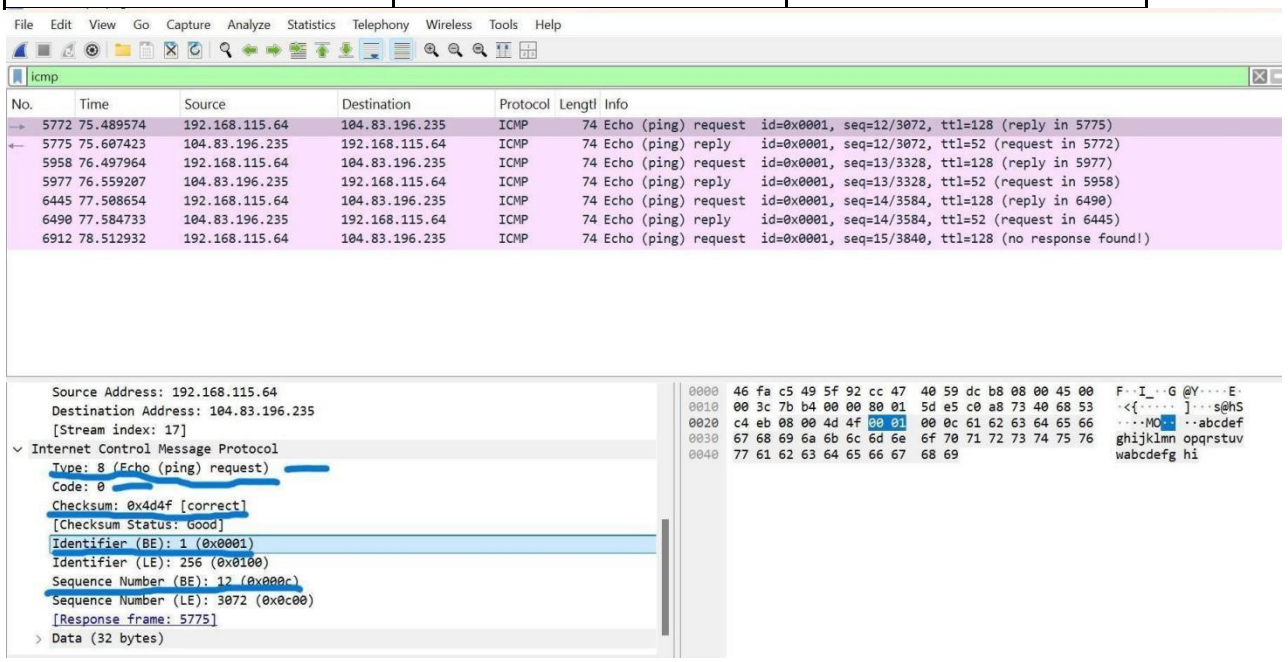
Parameter	Value
Your MachineIP Address.	192.168.115.64
Your MachineMAC Address	CC-47-40-59-DC-B8
Default Gateway address	192.168.115.95
DNS Server IP Address	192.168.115.95



2. Ping any website through command prompt and Fill the following details by applying the filter as **ICMP**: (highlight and paste screenshot for each of the output).

ICMP Request message:

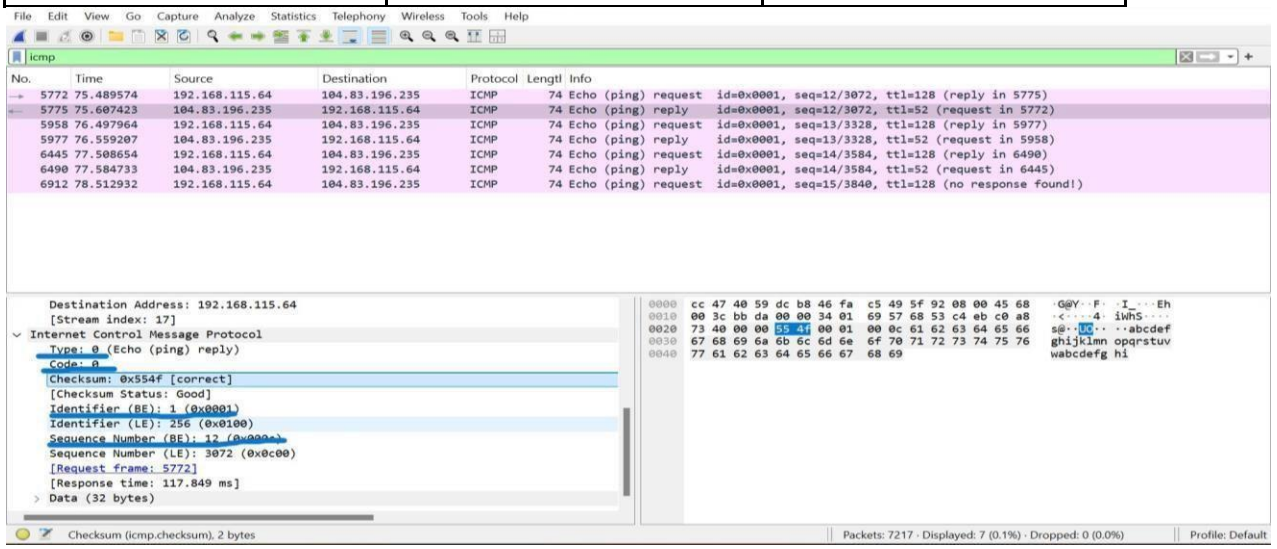
Field Name	Field Length (no of bits)	Fieldvalue
Type	8	8
Code	8	0
Checksum	16	0x4d4f
Identifier	16	1(0x0001)
Sequence Number	16	12(0x000c)



ICMP Reply message: (highlight and paste screenshot for each of the output).

Field Name	Field Length (no of bits)	Field value
Type	8	0
Code	8	0

Checksum	16	0x554f
Identifier	16	1(0x001)
Sequence Number	16	12(0x000c)



Conclusion: The above experiment has been executed and implemented successfully.

Rubrics for Wireshark labs: (To be Filled by the Class Teacher)

Rubrics	Excellent	Fair	Poor	Marks
Understanding (2)	Understand the Concept very well. (2)	Understand the Concept (1)	Poor Understand the Concept (0)	
Usage of filters (3)	Identified and applied the filter correctly (3)	Identified the filter, but not applied correctly (2-1)	Couldn't identify and apply the filter. Just captured the packets (1)	
Attach relevant Screenshots (3)	clearly Highlighted the answers and attached the screenshots (3)	attached the screenshots, but not highlighted. (2-1)	Did not attach the screenshots (0)	
On time Submission (2)	Early or on time submission (2)	Submitted after deadline (1)	Did not Submit (0)	
			Total	

Register No:	**99220041762**
Name:	**G.Asish**
Class/Section:	**8301A/S18**
Ex.No:	**14**
Name of the Experiment	**Capture and Analyze DNS packet**
Google Drive link of the packet tracer file (give view permission):	https://drive.google.com/drive/folders/1kZYMTJ0uZatmg4XpevUQnRGjCA_W4BOF

Objective(s):

To capture and analyse DNS Query Response packet using Wireshark.

Introduction: What is DNS?

The Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the internet or a private network.

To do DNS analysis in Wireshark, the nslookup command must be used.

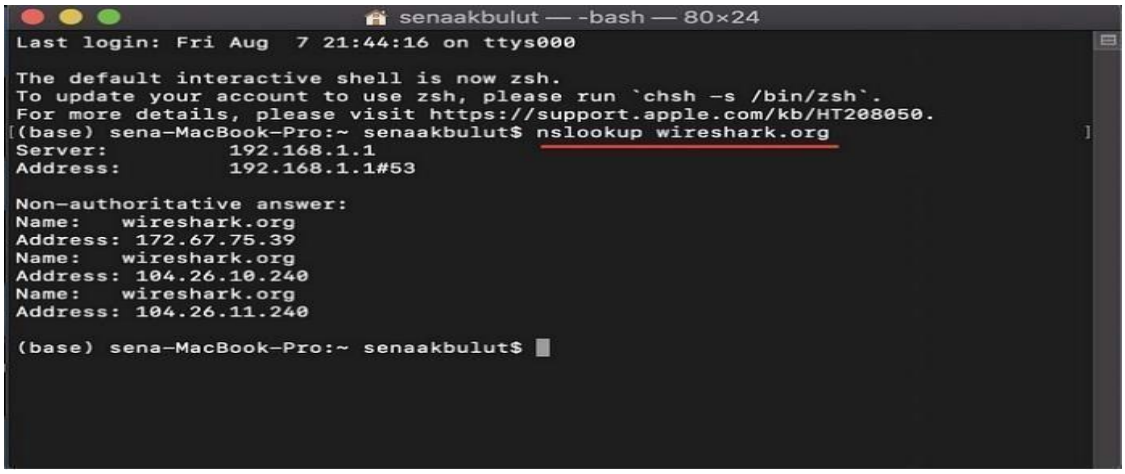
What is nslookup?

nslookup is a network administration command-line tool available in many computer operating system for querying the Domain Name System (DNS) to obtain a domain name or IP address mapping, or other DNS records.

Now that we have learned the meanings of these terms, let's examine the analysis steps in Wireshark.

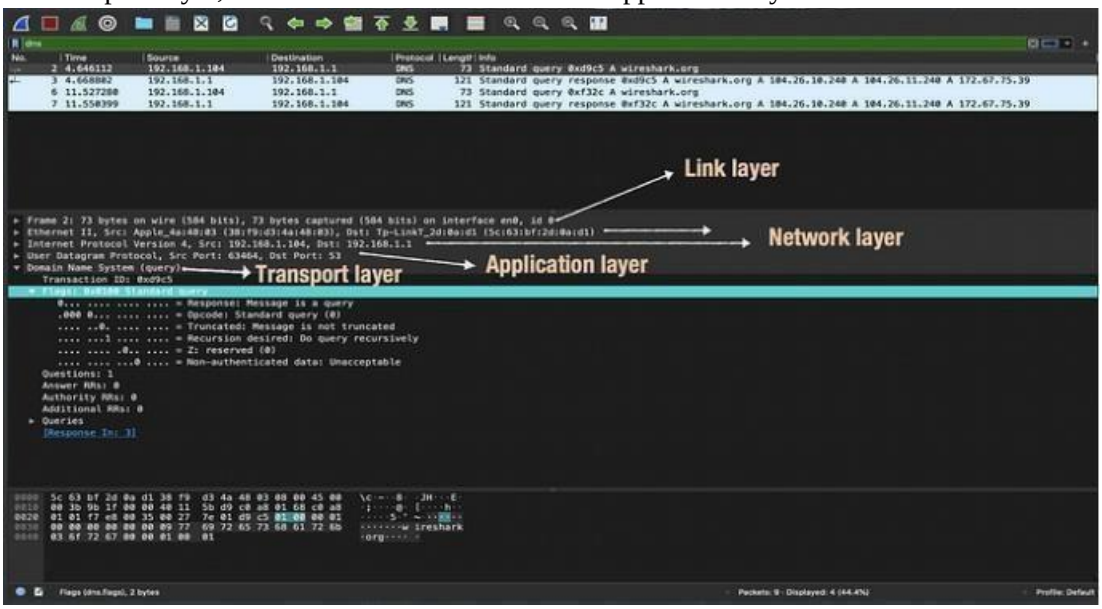
• To analyze it, I first ran the nslookup command for wireshark.org in the terminal and viewed the site's IP address and non-authoritative replies with the nslookup command.

nslookup wireshark.org



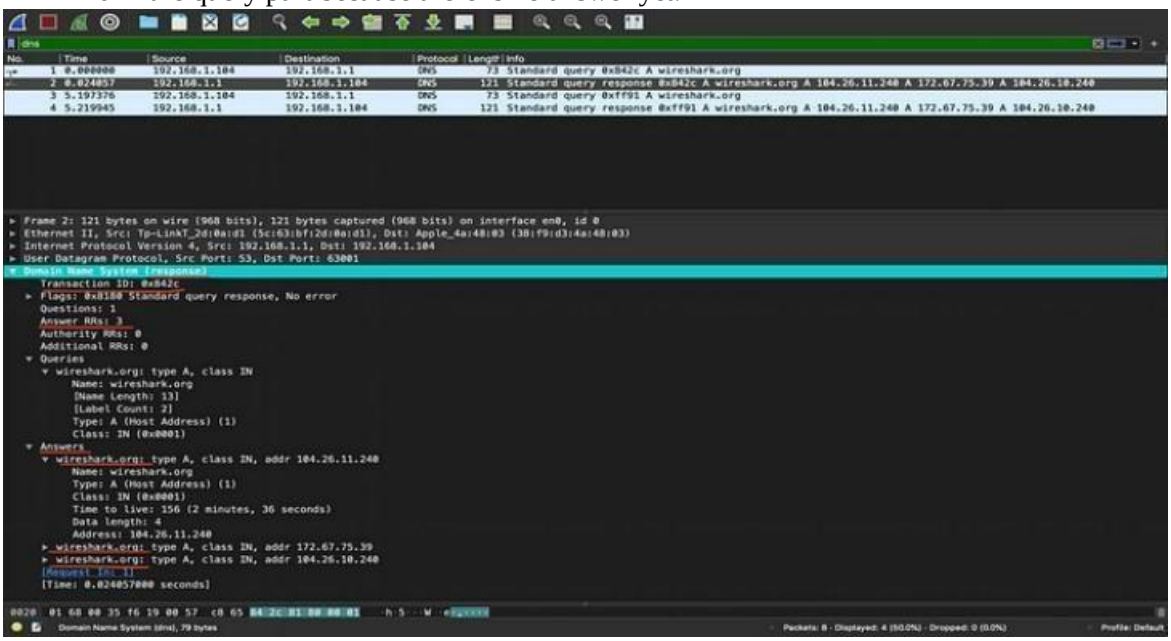
• Then when I ran the Wireshark traffic capture application and applied the DNS filter, the traffic I made in the terminal was displayed as follows.

When I looked at the first query, a small screen with information about the query appeared. The first feature here is below the link layer, the second and third is below the network layer, the fourth is below the transport layer, and the last feature is below the application layer.



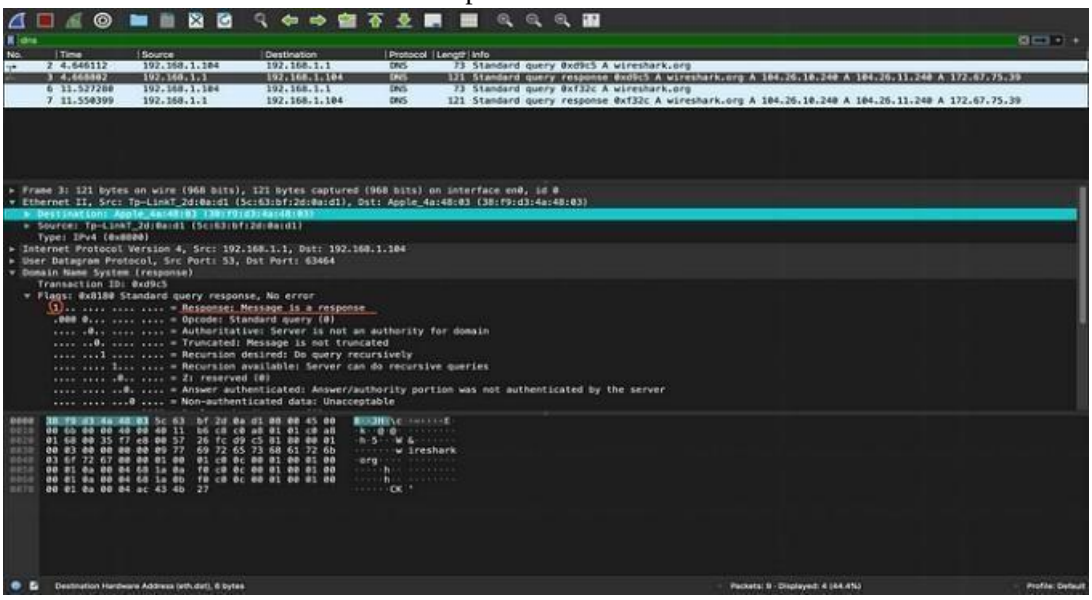
- When I came to response and when I opened the section that says domain name system, I saw sub-features named transaction id, flags and answers.

The Answer RRs part in the response section is as many as the answers we see in the terminal, so 3. The characteristics of the answers can also be examined in the lower part. The Answer RRs part is 0 in the query part because there is no answer yet.



- When we open the flags section, we see that it says 0 in query and 1 in response. This first flag bit indicates whether it is a query or a response.

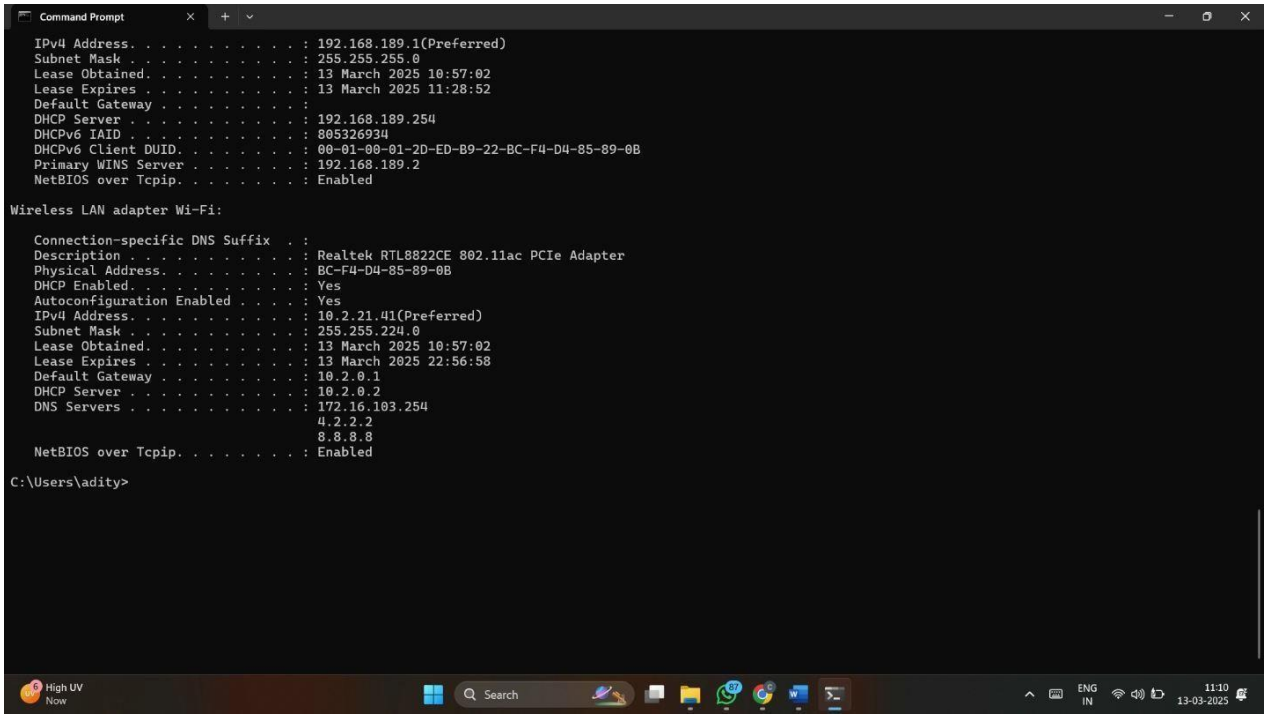
It also displays hexadecimal equivalents of destinations and sources. The first set of bits represents destination and the second set of bits represents source.



Exercise:

1. Use command prompt and fill the following details using ipconfig /all command. (highlight and paste screenshot for each of the output).

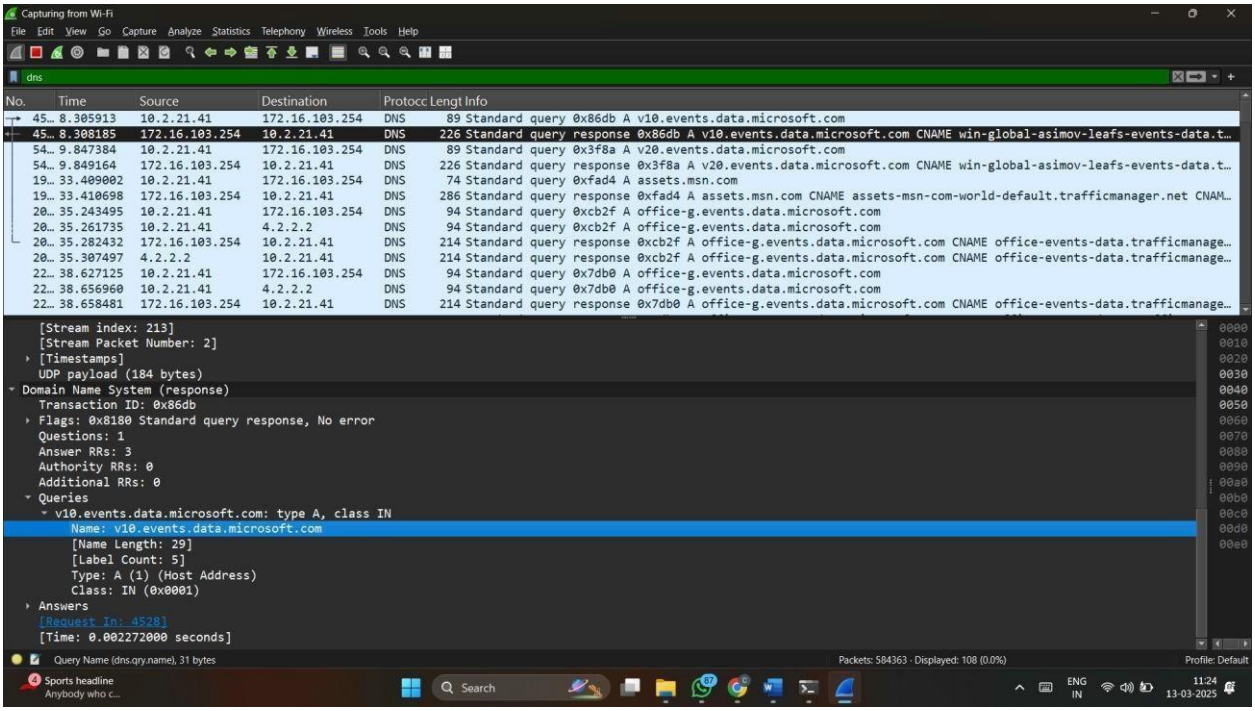
Parameter	**Value**
Your Machine IPAddress.	10.2.21.41
Your Machine MAC Address	BC-F4-D4-85-89-0B
Default Gateway address	10.2.0.1
DNS Server IPAddress	172.16.103.254



2. Ping any website through command prompt and Fill the following details by applying the filter as DNS: (highlight and paste screenshot for each of the output).

DNS Query message:

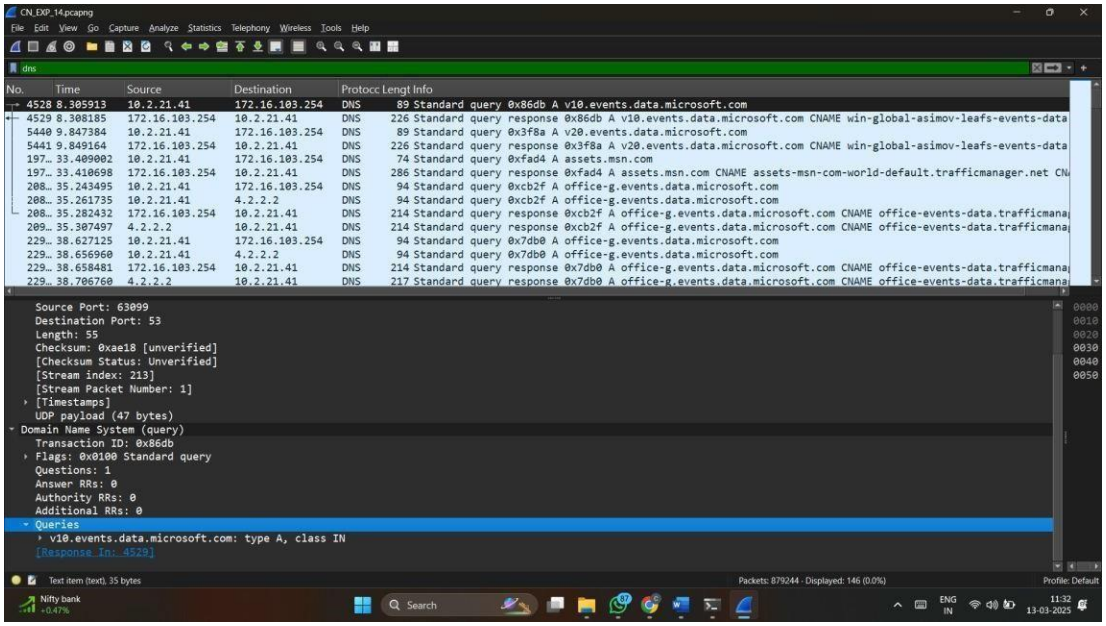
Field Name	**Field Length (no of bits)**	**Field value**
Destination MAC Address	48	C8:4f:86:fc:00:10
Source MAC Address	48	Bc:f4:d4:85:89:0b
Destination IPAddress	32	74.6.231.20
Source IPAddress	32	10.2.21.41
Destination UDP port	16	53
Source UDP port	16	63099
DNS Tx id	16	0x86db
DNS Flags	16	0x0100
DNS Questions	16	1
DNS Queries	variable	events.data.microsoft.com



3. DNS Response message: (highlight and paste screenshot for each of the output).

DNS Response message:

Field Name	**Field Length (no of bits)**	**Field value**
Destination MAC Address	48	C8:4f:86:fc:00:10
Source MAC Address	48	Bc:f4:d4:85:89:0b
Destination IPAddress	32	74.6.231.20
Source IPAddress	32	10.2.21.41
Destination UDP port	16	53
Source UDP port	16	63099
DNS Tx id	16	0x0xcb2f
DNS Flags	16	0x0100
DNS Questions	16	1
DNS Queries	Variable	Office-g.microsoft.com



Rubrics for Wireshark labs: (To be Filled by the Class Teacher)

Rubrics	Excellent	Fair	Poor	Marks
Understanding (2)	Understand the Concept very well. (2)	Understand the Concept (1)	Poor Understand the Concept (0)	
Usage of filters (3)	Identified and applied the filter correctly (3)	Identified the filter, but not applied correctly (2-1)	Couldn't identify and apply the filter. Just captured the packets (1)	
Attach relevant Screenshots (3)	clearly Highlighted the answers and attached the screenshots (3)	attached the screenshots, but not highlighted. (2-1)	Did not attach the screenshots (0)	
On time Submission (2)	Early or on time submission (2)	Submitted after deadline (1)	Did not Submit (0)	
Total				

Result: Thus the implementation of the DNS packet server has been successfully executed using cisco packet racer.

Register No:	**99220041762**
Name:	**G.Asish**
Class/Section:	**8301A/S18**
Ex.No:	**15**
Name of the Experiment	**FTP server Configuration**
Google Drive link of the packet tracer file (give view permission):	https://drive.google.com/drive/folders/1kZYMTJ0uZatmg4XpevUQnRGjCA_W4BOF

Objective(s): To design and implement FTP server configuration using packet tracer

Introduction:

The File Transfer Protocol is a standard network protocol used for the transfer of computer files between a client and server on a computer network. FTP is built on a client-server model architecture using separate control and data connections between the client and the server.

Let's now do FTP configuration in Packet Tracer

1) Open Cisco Packet Tracer and select 2 End Devices (PC device), 1 Switch, 1 Router, 1 Server.

2) Now Connect all the devices using the auto connection.

3) Then configure the IP addresses as per the diagram.

4) Now just wait for some time to let all the connection statu `C:\>ping 10.10.10.2`

5) Now we have achieved a connection where a class C IP address is being translated to class A IP Address.

6) Go to one of the PC devices and on Desktop tab select CMD.

7) Now we need to check the connection to the server by

`C:\>ftp 10.10.10.2`

8) If reply is coming then it means the server is properly configured and connected.

9) Go to the Server → Services → FTP.

10) Put on the FTP service and give username and password and click on ADD.

`ftp>put filenme.txt`

11) Come back to PC device and open the CMD and type

12) It will ask for username and password. Provide the username and password configured earlier.

13) Once the connection is established exit rom the CMD and go to Text Editor and make a new text file.

14) Save the new text file and return to cmd and type

`ftp>get filename.txt`

15) This will send the text file from the PC device (192.168.0.2) to Server (10.10.10.2).

16) Now to verify that the file has been transferred to the server, so type

17) You will see your Filename in the list.

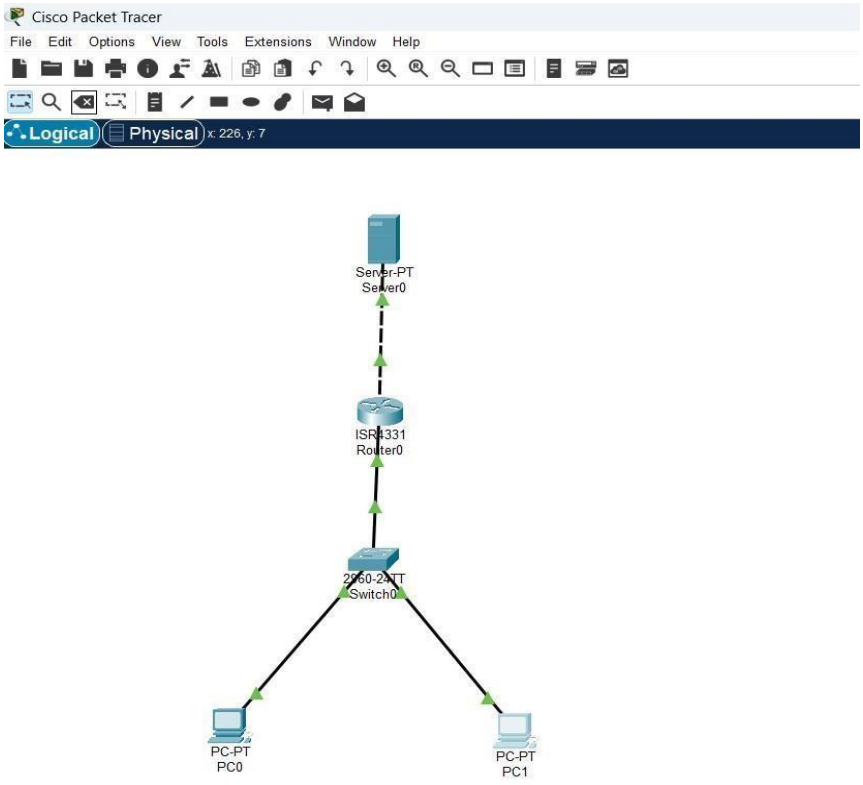
18) Now to get a file from server to PC type

19) Now exit from FTP type ctrl+C, then type dir to check that the file is there in the PC or not.

20) So we have successfully send and got a file from a server using FTP protocol.

1. **Device Requirements:**
   1. Router
   2. Server
   3. PC0
   4. PC1
   5. Switch 0
2. **Network Diagram for your experiment (draw the diagram either hand drawing/ms paint or any other drawing tools)**

3. **Network Diagram (Packet tracer diagram before configuration):**



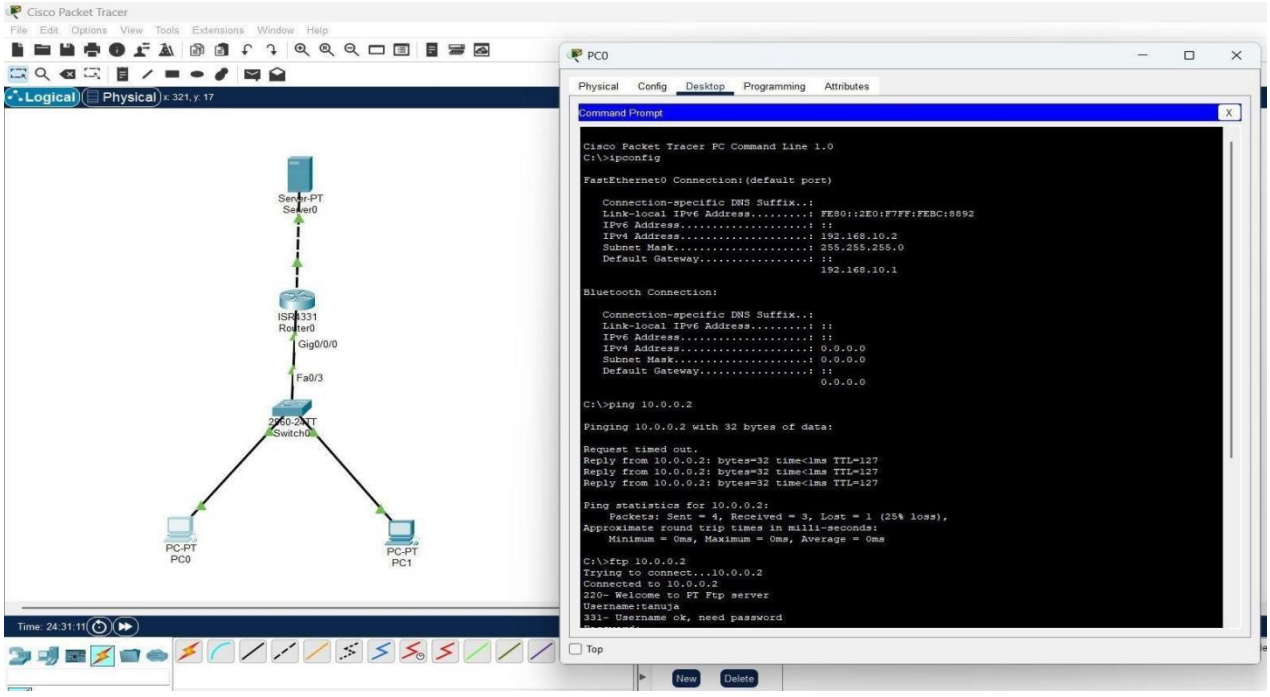
4. **Configuration details:**

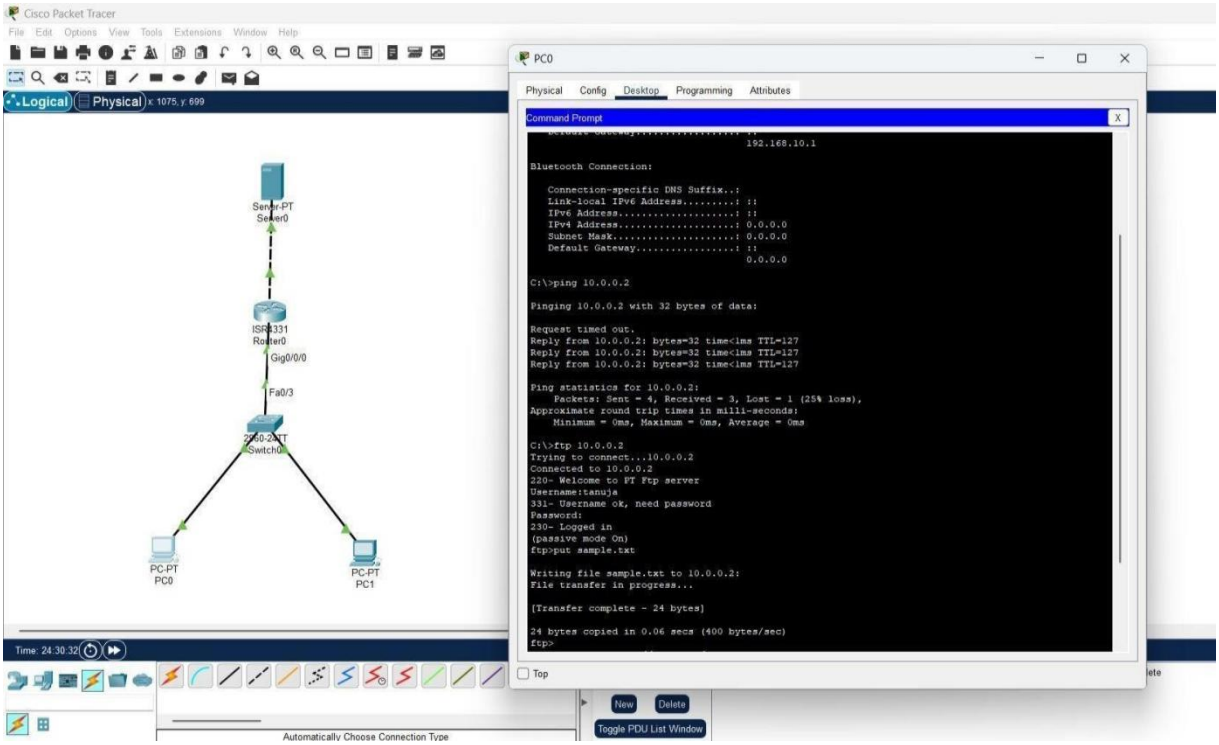
Device Name	Interface Name	IP Address	Subnet mask	Default Gateway
PC 0	Fa 0 – fa0/1	192.168.10.2	255.255.255.0	192.168.10.1
PC 1	Fa 0 – fa0/2	192.168.10.3	255.255.255.0	192.168.10.1

5. **Describe step by step configuration steps properly (you may copy the commands used in the configuration tab and paste it.)**

- ipconfig
- ping
- ftp
- put (to import)
- get (to download)

6. **Output Diagram (Minimum 3 screenshot):**





Rubrics for Experiment Assessment

Rubrics	Good	Normal	Poor	Marks
Creation of Topology (4)	Created the topology, Identify the proper devices and making the connections **(4)**	Created the topology, Identify the proper devices, making the connections But missing some features **(3)**	Created wrong topology, Failed to Identify the proper devices and making connections **(1)**	
Verify the connectivity (4)	Verified the connectivity in all the levels **(4)**	Verified the connectivity at some levels (only some nodes) **(2)**	Verified the connectivity is not done. **(1)**	
Timely Completion (2)	Completed the lab before the allotted time **(2)**	Completed the lab after the deadline **(1)**	Did not submitted before grading **(0)**	
			Total	

Result: Thus the implement of configuration of FTP service has been executed successfully in Cisco Packet .

Register No:	**99220041762**
Name:	**G.Asish**
Class/Section:	**8301A/S18**
Ex.No:	**16**
Name of the Experiment	**E-mail server Configuration**
Google Drive link of the packet tracer file (give view permission):	https://drive.google.com/drive/folders/1kZYMTJ0uZatmg4XpevUQnRGjCA_W4BOF

Objective(s):

To design and implement Email server configuration using packet tracer

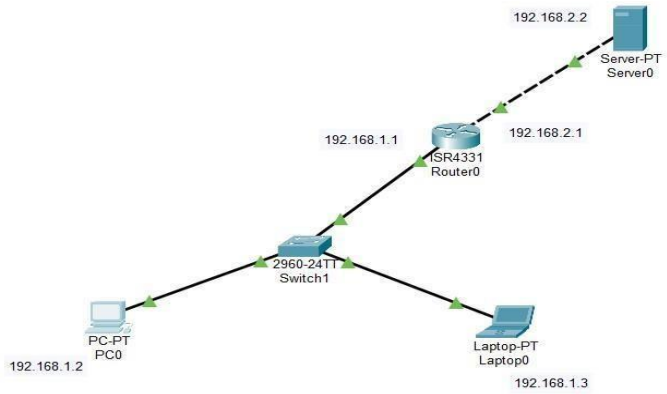
Introduction:

An email server, such as Gmail stores and sends email messages to email clients on request. We often send and receive emails on our mobile devices or computers. Have you ever imagined how this happens? Well, whenever you compose and send an email to another person, the message you send first goes to a mail server. It's the mail server which then sends the email when it is requested from the email client (e.g Gmail App) of the recipient's device.

So now, lets configure a mail server in Packet Tracer. And have in mind that although our main focus is configuring an email server, we'll still need services of a DNS server at one point.

1. **Device Requirements:**
    1. Server
    2. Router
    3. Switch
    4. PC0
2. **Network Diagram for your experiment (draw the diagram either hand drawing/ms paint or any other drawing tools)**

3. Network Diagram (Packet tracer diagram before configuration):



4. Configuration details:

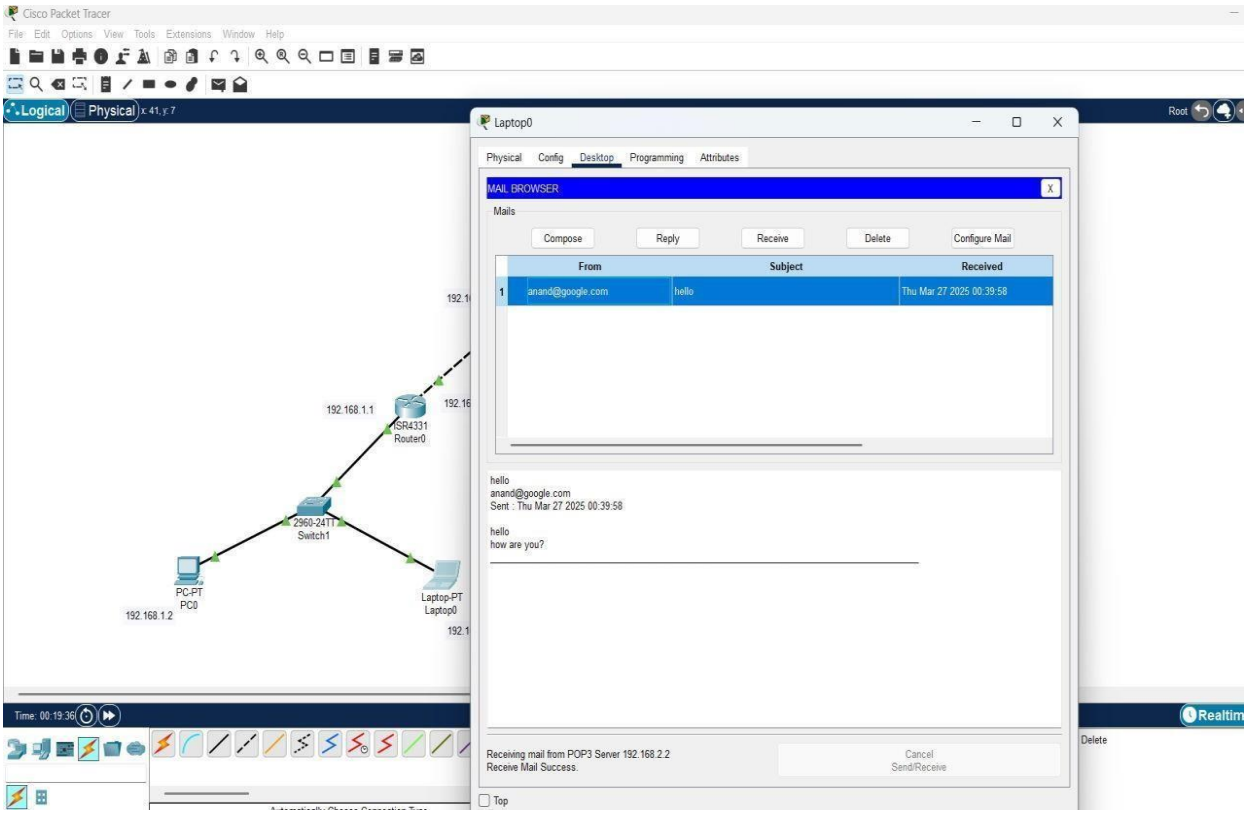
Device Name	Interface Name	IP Address	Subnet mask	Default Gateway
Router	Fa- 0 fa0/0	192.168.1.1	255.255.255.0	
Server	Fast Ethernet0	192.168.2.2	255.255.255.0	192.168.2.1
Switch				
Pc0	Fast Ethernet0	192.168.1.2	255.255.255.0	192.168.1.1
Laptop 0	Fast Ethernet0	192.168.1.3	255.255.255.0	192.168.1.1

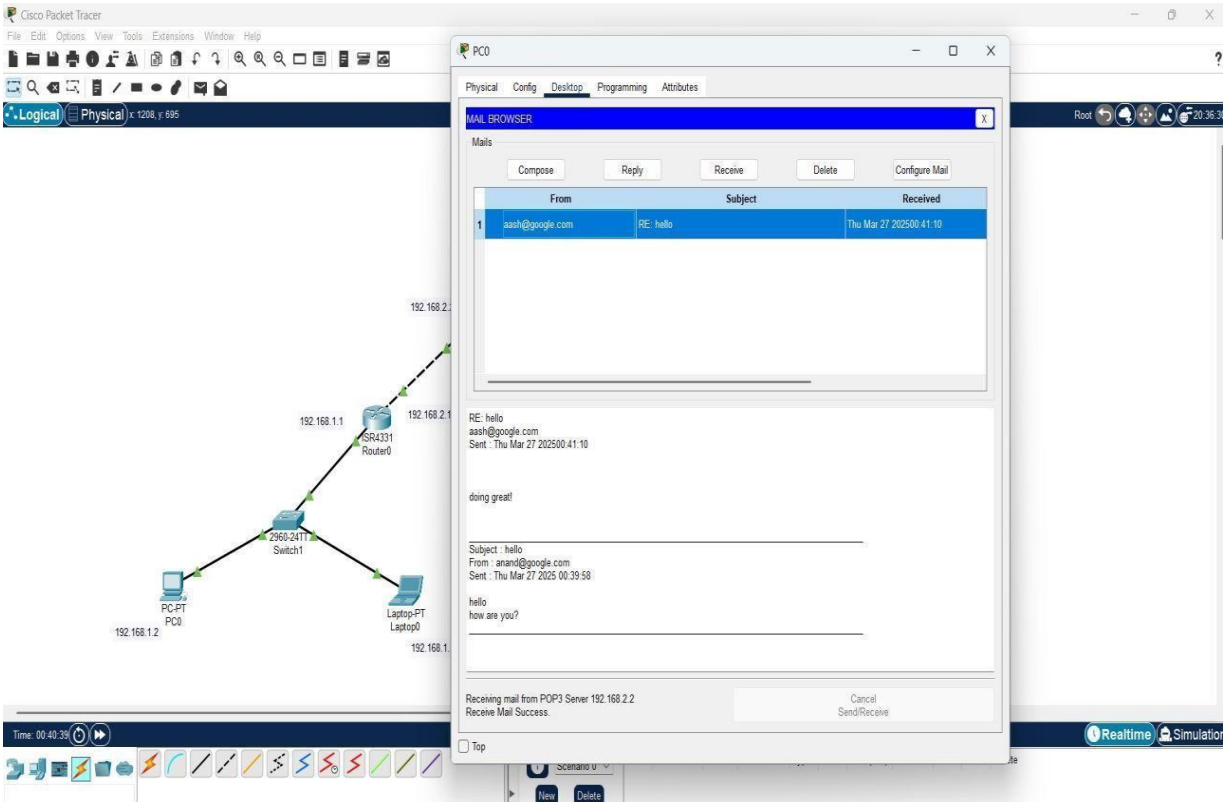
5. Describe step by step configuration steps properly (you may copy the commands used in the configuration tab and paste it.)

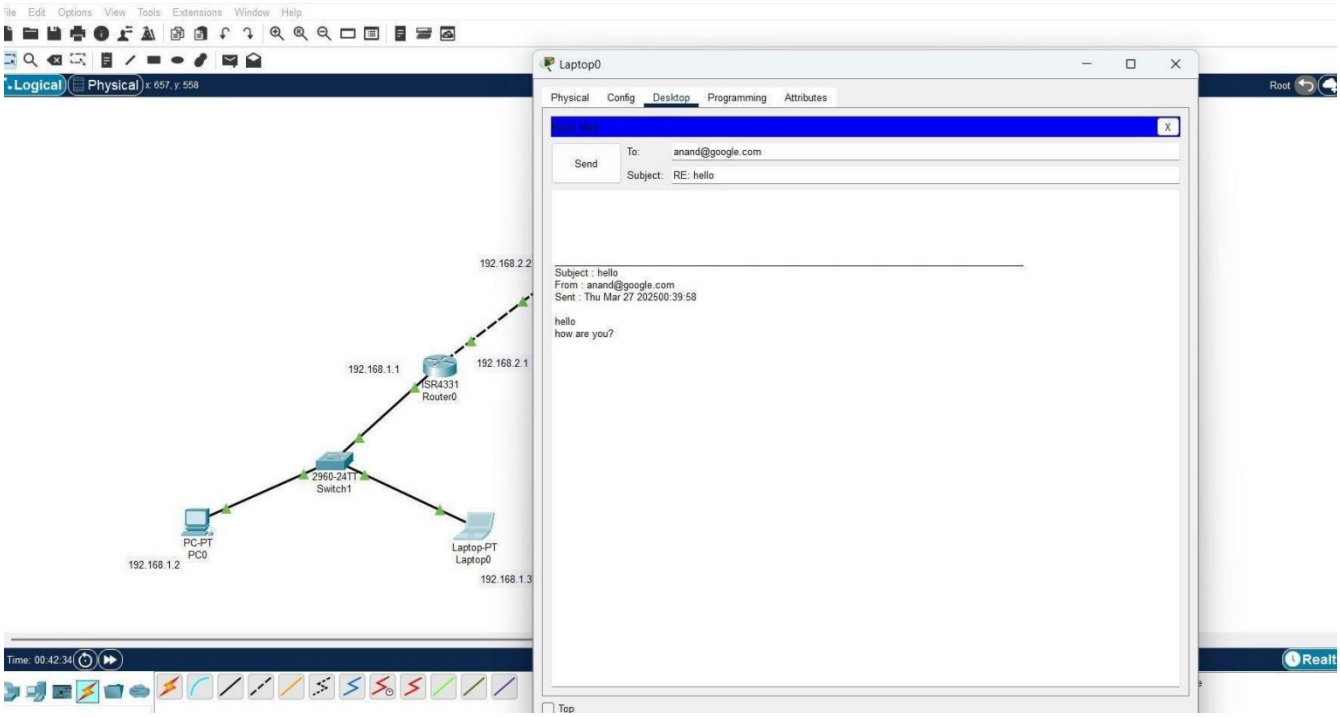
- **Create IP address**
- **Compose email through pc0**
- **Receive email through laptop**
- **Reply back for email received**

99220041762

6. Output Diagram (Minimum 3 screenshot):


Cisco Packet Tracer
Logical
Physical
Laptop0
Physical
Config
Desktop
Programming
Attributes
MAIL BROWSER
Mails
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
1
anand@google.com
hello
Thu Mar 27 2025 00:39:58
hello
anand@google.com
Sent : Thu Mar 27 2025 00:39:58
hello
how are you?
Receiving mail from POP3 Server 192.168.2.2
Receive Mail Success.
Cancel
Send/Receive
Top
192.168.1.1
ISR4331
Router0
2960-24TT
Switch1
PC-PT
PC0
192.168.1.2
Laptop-PT
Laptop0
Time: 00:19:36
Realtim
Delete


Cisco Packet Tracer
Logical
Physical
PC0
Physical
Config
Desktop
Programming
Attributes
MAIL BROWSER
Mails
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
1
aash@google.com
RE: hello
Thu Mar 27 202500:41:10
RE: hello
aash@google.com
Sent : Thu Mar 27 202500:41:10
doing great!
Subject : hello
From : anand@google.com
Sent : Thu Mar 27 2025 00:39:58
hello
how are you?
Receiving mail from POP3 Server 192.168.2.2
Receive Mail Success.
Cancel
Send/Receive
Top
192.168.1.1
ISR4331
Router0
2960-24TT
Switch1
PC-PT
PC0
192.168.1.2
Laptop-PT
Laptop0
Time: 00:40:39
Realtime
Simulation
New
Delete



Rubrics for ExperimentAssessment:

Rubrics	Good	Normal	Poor	Marks
Creation of Topology (4)	Created the topology, Identify the proper devices and making the connections **(4)**	Created the topology, Identify the proper devices, making the connections But missing some features **(3)**	Created wrong topology, Failed to Identify the proper devices and making connections **(1)**	
Verify the connectivity (4)	Verified the connectivity in all the levels **(4)**	Verified the connectivity at some levels (only some nodes) **(2)**	Verified the connectivity is not done. **(1)**	
Timely Completion (2)	Completed the lab before the allotted time **(2)**	Completed the lab after the deadline **(1)**	Did not submitted before grading **(0)**	
				Total

Result: Thus the implement of configuration of Email service has been executed successfully in Cisco Packet