SIKSHA 'O' ANUSANDHAN
DEEMED TO BE UNIVERSITY

Admission Batch: 2022 **Session: Odd-2024**

Laboratory Record

Computer Networking: Concepts (CSE 3751)

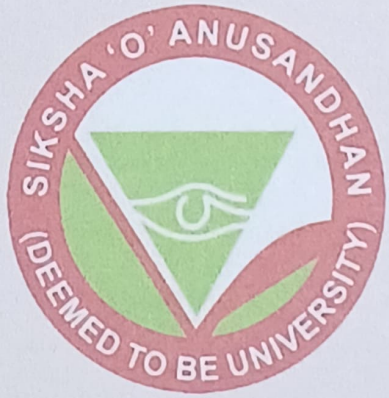
Submitted by

Name: **E. Jagadeeswar Patro**

Registration No.: **2241016309**

Branch: Computer Science & Engineering

Semester: 5th Section: 2241044



Department of Computer Science & Engineering

Faculty of Engineering & Technology (ITER)

Jagamohan Nagar, Jagamara, Bhubaneswar, Odisha - 751030

Contents

Experiment 1

Aim: Study on network elements, IP address, Subnet mask and network simulator(s).

Objective 1: An overview on network elements (i.e. switch, hub, router, bridge, repeater, access point).

→ Switch - a device working at the data link layer that is used to segment networks into different subnetworks of LAN segments. It is responsible for filtering & forwarding the packets between LAN segments.

→ Hub - a device working at physical layer & is used to connect computers together. It has multiple ports that are used to connect multiple out-devices. A hub sends incoming data to all destinations.

→ Router - It is a device working at network layer that handles different protocols. It is responsible for ~~handling~~ forwarding data from one network to another.

→ Bridge - works at datalink layer & links two networks together. It can handle networks that follows same protocol.

→ Repeater - amplifies & restores signals for long distance transmission.

→ Access Point - A wireless network device that acts other wireless network device to connect to a wired network. It is used to extend the wireless coverage of an existing network.

Objective 2: Overview on different classes of IP addressing, subnet mask & gateway:

(a) Class-A → in format a.b.c.d, the variation of the bits lies inbetween 0-127 with the category of subnet mask 255.0.0.0 where a is indicating the network ID and b, c, d are indicating host ID. This class is for larger network.

(b) Class B → it varies from 128 - 191 with subnet mask 255.255.0.0 where a, b are network IDs & c, d are host IDs. Used for medium size networks.

(c) Class C → it is used for small networks where the first 24 bits are network ID & the last 8 bits is host ID. The format of subnet mask is 255.255.255.0. The values vary from 192 - 255.

Objective 3: Introduction to Cisco Packet Tracer (CPT) tool to configure network.

→ CPT is a cross platform visual simulation tool designed by Cisco Systems that allows users to create network topologies & simulate them.

→ It helps practicing simple & complex networks through simulation.

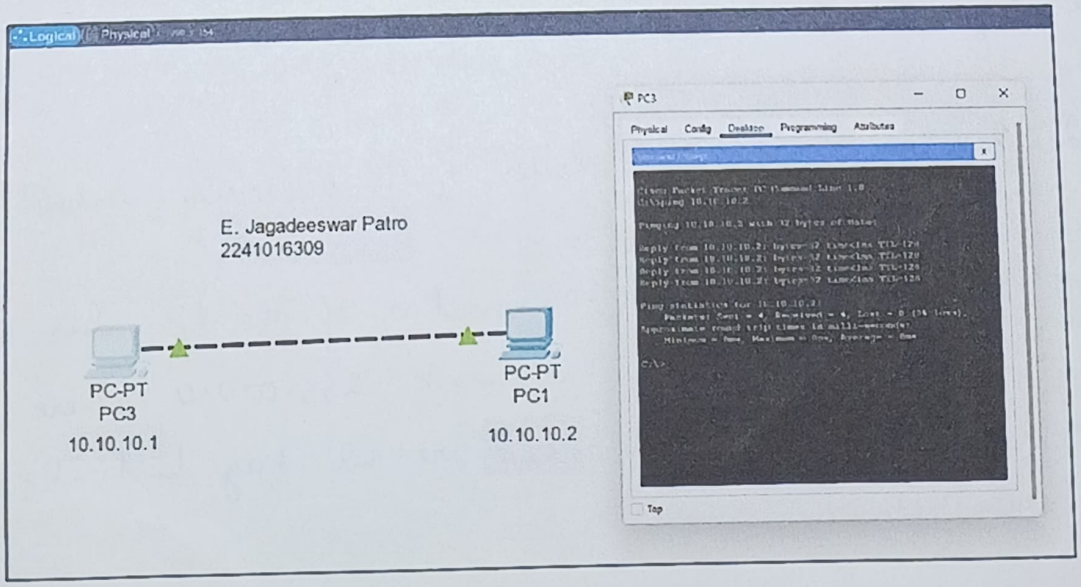
→ It offers effective, interactive environment for learning networking concepts and protocols.

→ Users can build, configure & troubleshoot networks using virtual equipment & simulated connections with or without multiple users.

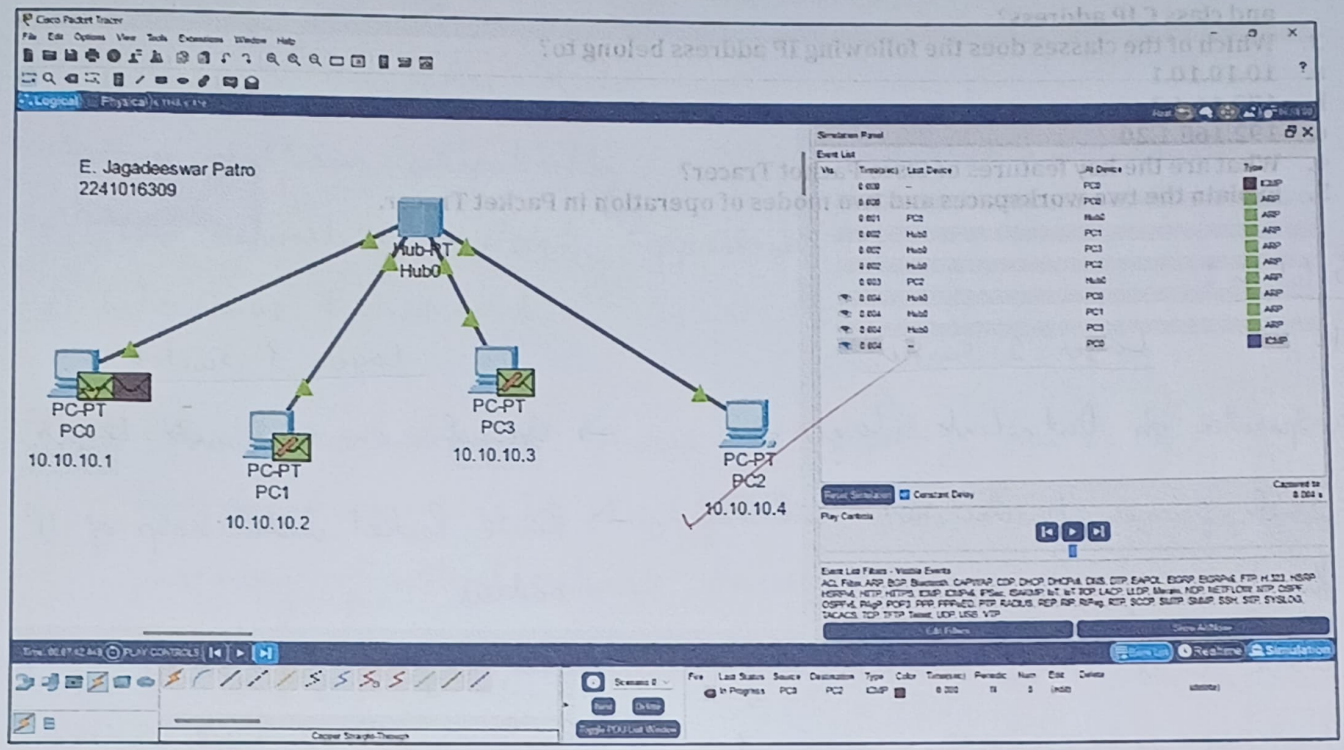
Objective 4: Making connection between two hosts PCs & analysing the communication using ping command.

Observation:

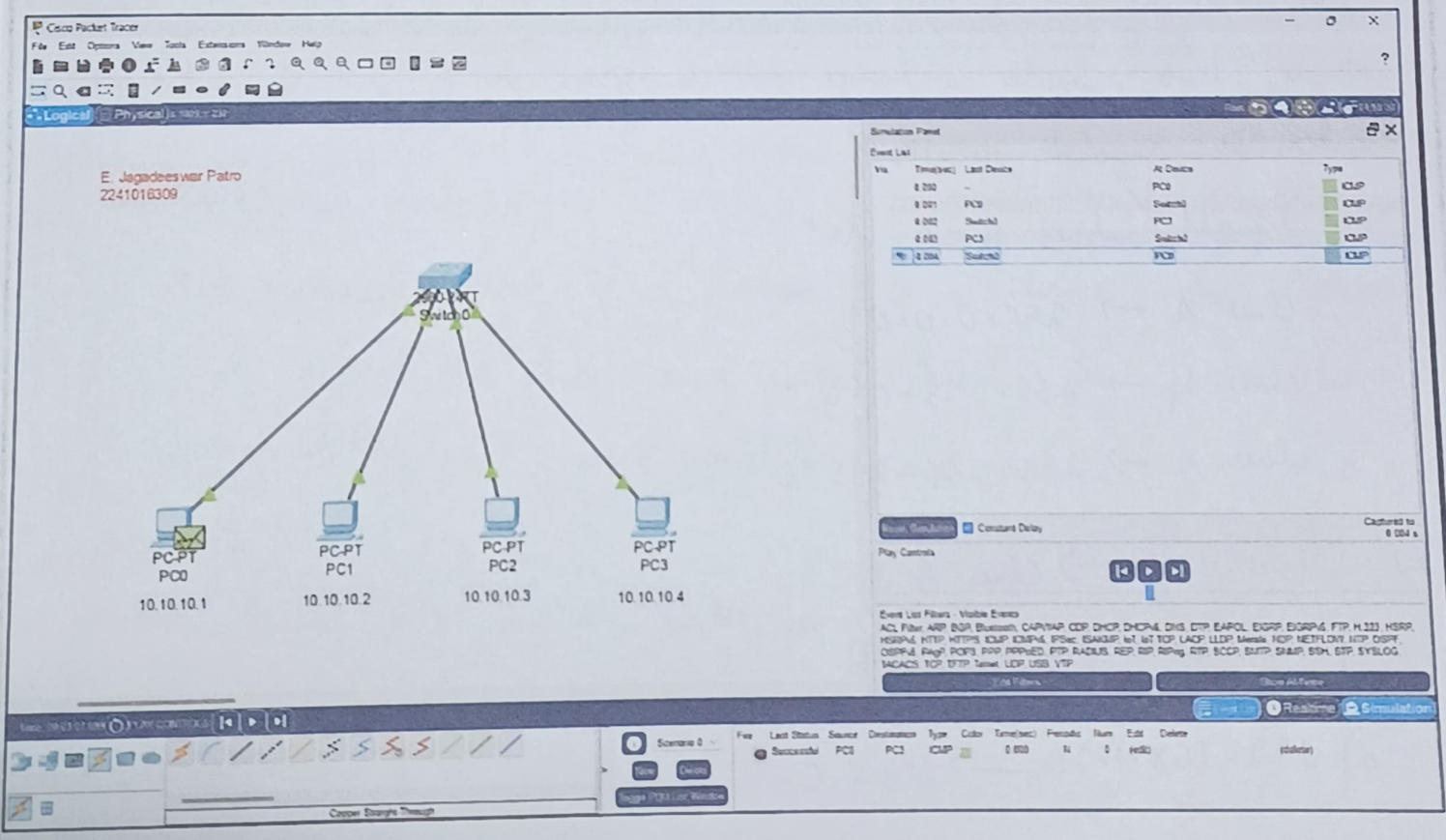
(i) End to End Connection:



ii) Communication through Hub:



(iii) Communication through Switch:



Exercises:

1. **Differentiate layer 2 and layer 3 switches.**
2. **Compare and contrast IPv4 and IPv6 addresses. What are the default subnet mask for class A, class B and class C IP address?**
3. **Which of the classes does the following IP address belong to?**

a. **10.10.10.1**
b. **172.16.4.3**
c. **192.168.1.20**

4. **What are the key features of Cisco Packet Tracer?**
5. **Explain the two workspaces and two modes of operation in Packet Tracer.**

Solution:

1.

Layer 2 switch	Layer 3 switch
→ Operates on Data Link layer	→ Operates on Network layer.
→ Sends frames to destination on the basis of MAC address.	→ Route Packet with help of IP address.
→ Work with MAC address only	→ Can perform functioning of both 2 layer & 3 layer switch.
→ Used to reduce traffic on local network	→ Used to implement Virtual LAN.

2) The IPv4 is a 32-bit address, whereas IPv6 is a 128-bit hexadecimal address. IPv6 provides a large address space & it contains a simple header as compared to IPv4.

The default subnet masks are:

class A → 255.0.0.0

class B → 255.255.0.0

class C → 255.255.255.0

3) a) 10.10.10.1 → Class A

b) 172.16.4.3 → Class B

c) 192.168.1.20 → Class C

4) Key features of CISCO packet Tracer are:

i) Visualizing Networks

ii) Real time & simulation Modes

iii) Cross platform compatibility

iv) Most networking protocols supported

v) Interactive Environment.

5) (i) → The logical workspace shows the topology built by the user through diagrams. It displays the connections, placement and clustering of virtual network devices.

→ The physical workspace shows us the physical implementation of the logical network.

(ii) CPT has two operating modes for visualizing a network's behaviour:

→ Real-time mode:

The network behaves like real devices, with immediate responses to all network activities.

→ Simulation mode:

The networks runs at a slower pace, allowing you to observe and inspect the paths that packets take. When you switch to simulation mode, the simulation Panel appears.

Conclusion:

Network devices like switch, router, hubs, bridges, repeaters and acces points play essential roles in assuring efficient communication within and between networks. Switch manages traffic within a local network while router handles communication between different networks.

Experiment - 2

Aim: Implementation of basic Ethernet using Cisco Packet Tracer to understand and make IP, TCP and UDP Header Analysis.

Objectives:

1. An overview on headers (i.e Ethernet, IP, TCP & UDP), ICMP, FTP and TFTP
2. Configuration of an Ethernet using the network devices in Cisco Packet Tracer.
3. Simulating the Ethernet by transmitting ICMP, FTP and TFTP messages between two end devices
4. Understanding and analysing different fields of IP, TCP & UDP headers after simulation.

Theory:

Objective 1:

→ Ethernet – a widely used technology for wired LAN which uses frames to encapsulate data, containing MAC address for source and destination. It supports speeds upto 100 GBPS.

→ IP – Internet Protocol responsible for addressing & routing. It's of two types:
IPv4 (32-bit)
IPv6 (128-bit)

→ TCP – Transmission Control Protocol ensures reliable, ordered & error checked delivery of data between applications.

→ UDP – User Datagram Protocol allows low-latency connectionless communication. – commonly used for streaming media and video conferencing.

→ ICMP – Internet Control Message Protocol operates at network layer for troubleshooting and monitoring network connectivity.

→ FTP – File Transfer Protocol is used for authentication & can operate in active or passive data.

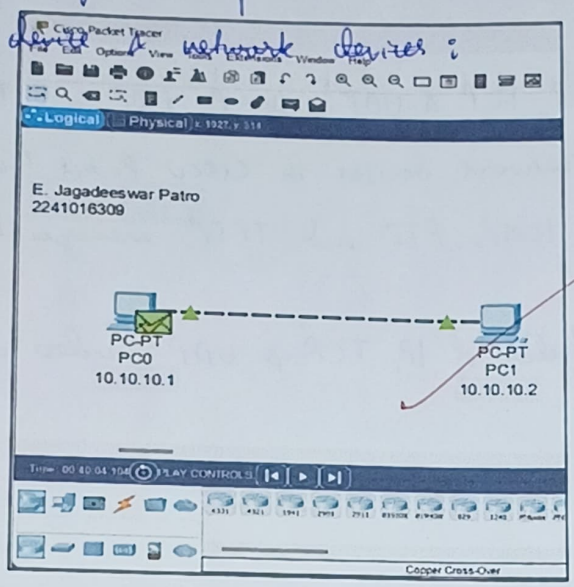
→ TFTP – Trivial File Transfer Protocol is a simpler version of FTP for transferring files with minimal overhead.

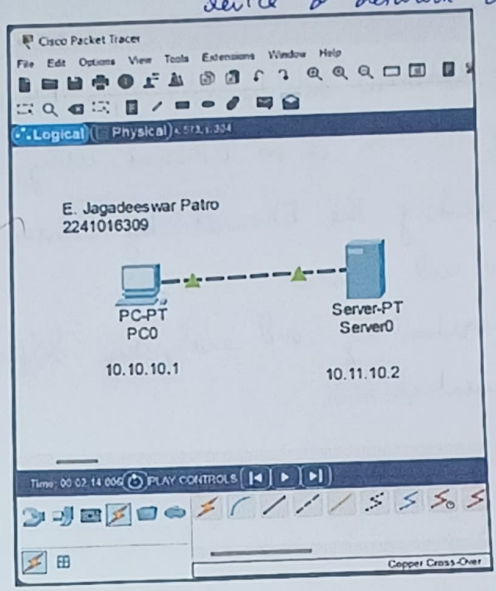
=) Objective 2 :

observation :

Configuration of ethernet between two end devices and between an end device & network device

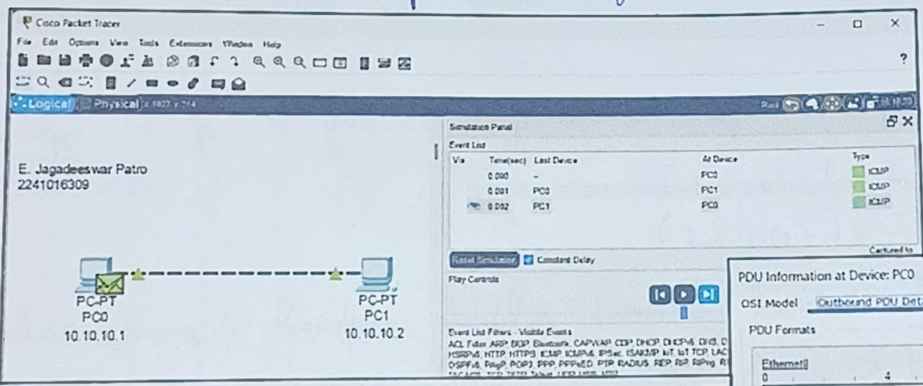
end device & network devices :



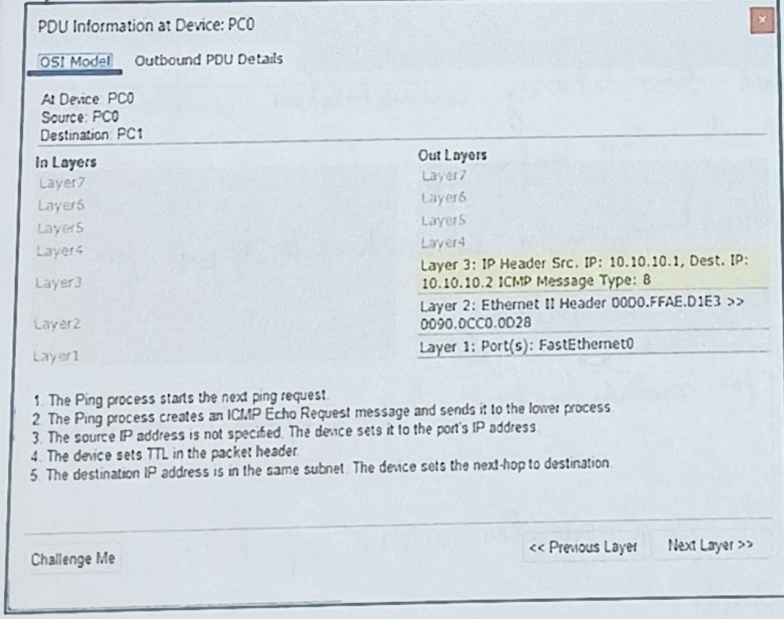


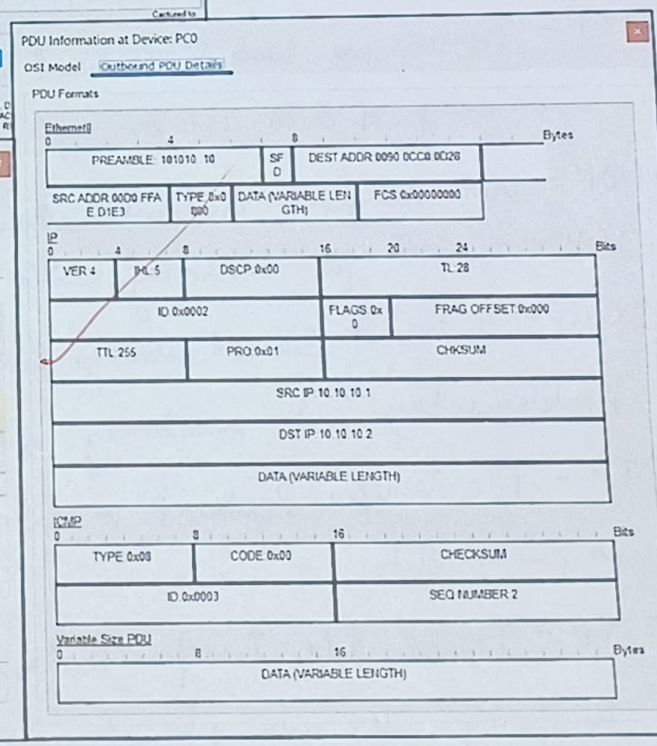
=) Objective 3 :

Observation : Simulation of ICMP message transmission



(Message ready for transmission)





(Message after Transmission)

PDU Information at Device: PC1

OSI Model | Inbound PDU Details | Outbound PDU Details

At Device: PC1
Source: PC0
Destination: PC1

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 10.10.10.1, Dest. IP: 10.10.10.2 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 10.10.10.2, Dest. IP: 10.10.10.1 ICMP Message Type: 0
Layer 2: Ethernet II Header 00D0.FFAE.D1E3 >> 0090.0CC0.0D28	Layer 2: Ethernet II Header 0090.0CC0.0D28 >> 00D0.FFAE.D1E3
Layer 1: Port FastEthernet0	Layer 1: Port(s): FastEthernet0

1. FastEthernet0 receives the frame.

PDU Information at Device: PC1

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	Bytes
PREAMBLE: 101010..10		DEST ADDR 00D0.FFAE.D1E3	
SRC ADDR 0090.0CC0.0D28	TYPE 0x0800	DATA (VARIABLE LENGTH)	FCS 0x00000000

IP

0	4	8	16	20	24	Bits
VER 4	IHL 5	DSCP 0x00	TL 28			
ID 0x0002			FLAGS 0x0	FRAG OFFSET 0x000		
TTL 128	PRO 0x01	CHKSUM				
SRC IP 10.10.10.2						
DST IP 10.10.10.1						
DATA (VARIABLE LENGTH)						

ICMP

0	8	16	Bits
TYPE 0x00	CODE 0x00	CHECKSUM	
ID 0x0003		SEQ NUMBER 2	

Variable Size PDU

0	8	16	Bytes
DATA (VARIABLE LENGTH)			

PDU Information at Device: PC1

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	Bytes
PREAMBLE: 101010..10		DEST ADDR 0090.0CC0.0D28	
SRC ADDR 00D0.FFAE.D1E3	TYPE 0x0800	DATA (VARIABLE LENGTH)	FCS 0x00000000

IP

0	4	8	16	20	24	Bits
VER 4	IHL 5	DSCP 0x00	TL 28			
ID 0x0002			FLAGS 0x0	FRAG OFFSET 0x000		
TTL 255	PRO 0x01	CHKSUM				
SRC IP 10.10.10.1						
DST IP 10.10.10.2						
DATA (VARIABLE LENGTH)						

ICMP

0	8	16	Bits
TYPE 0x08	CODE 0x00	CHECKSUM	
ID 0x0003		SEQ NUMBER 2	

Variable Size PDU

0	8	16	Bytes
DATA (VARIABLE LENGTH)			

(Acknowledgement Recieved)

PDU Information at Device: PC0

OSI Model | Inbound PDU Details

At Device: PC0
Source: PC0
Destination: PC1

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 10.10.10.2, Dest. IP: 10.10.10.1 ICMP Message Type: 0	Layer3
Layer 2: Ethernet II Header 0090.0CC0.0D28 >> 00D0.FFAE.D1E3	Layer2
Layer 1: Port FastEthernet0	Layer1

1. FastEthernet0 receives the frame.

PDU Information at Device: PC0

OSI Model | Inbound PDU Details

PDU Formats

Ethernet II

0	4	8	Bytes
PREAMBLE: 101010..10	SFD	DEST ADDR 00D0.FFAE.D1E3	
SRC ADDR 0090.0CC0.0D28	TYPE 0x0800	DATA (VARIABLE LENGTH)	FCS 0x00000000

IP

0	4	8	16	20	24	Bits
VER 4	IHL 5	DSCP 0x00	TL 28			
ID 0x0002			FLAGS 0x0	FRAG OFFSET 0x000		
TTL 128	PRO 0x01	CHKSUM				
SRC IP 10.10.10.2						
DST IP 10.10.10.1						
DATA (VARIABLE LENGTH)						

ICMP

0	8	16	Bits
TYPE 0x00	CODE 0x00	CHECKSUM	
ID 0x0003		SEQ NUMBER 2	

Variable Size PDU

0	8	16	Bytes
DATA (VARIABLE LENGTH)			

Objective 4 :

After simulating transmission through TCP & UDP protocols,

-> Packet Inspection is used to view header in real time.

-> Source & destination IP address is checked for IP header.

-> By analyzing the sequence and acknowledgement numbers in the TCP header, reliable flow of data can be observed.

-> Protocol field in the IP header is used to determine if the data using TCP or UDP is transmitted.

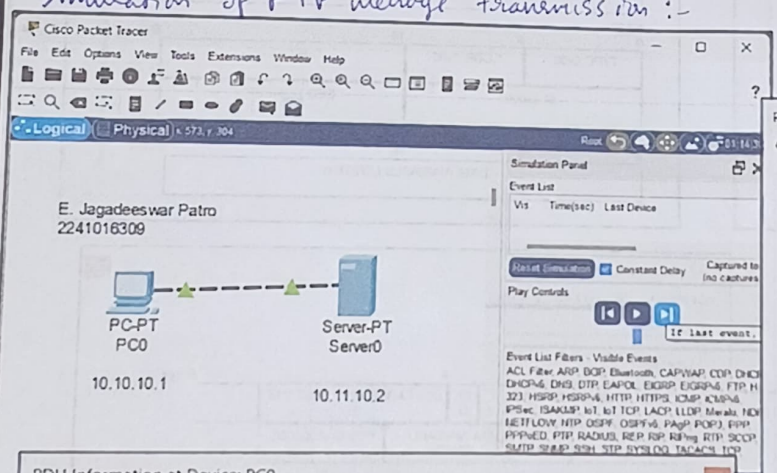
Observation :-

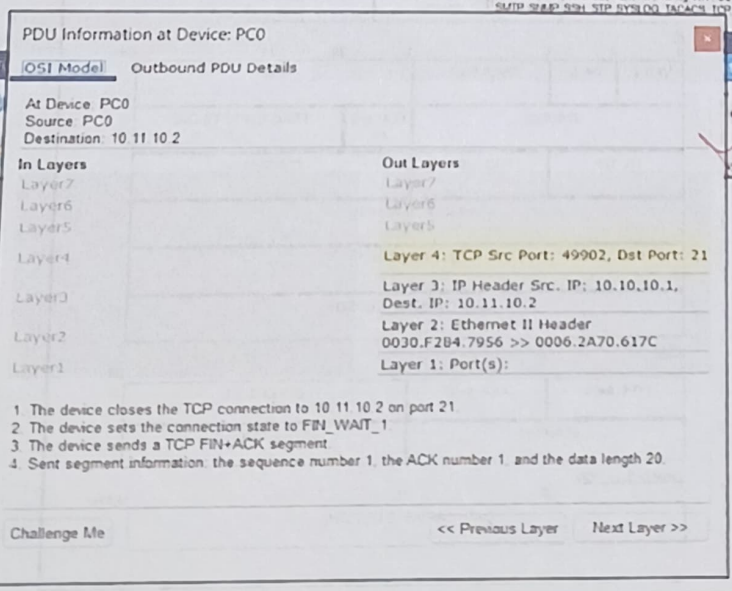
=> TCP :-

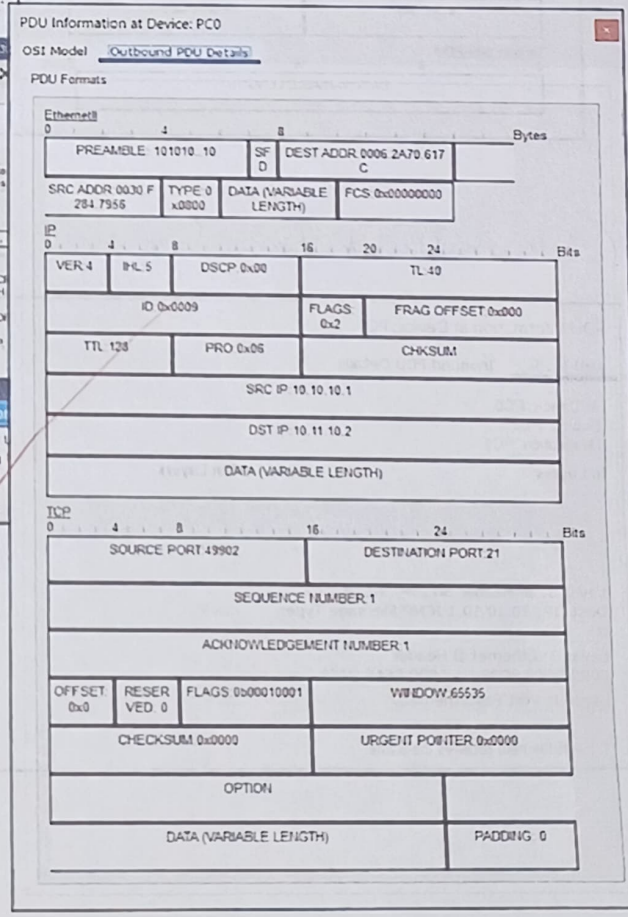
(Packet Transmission through TCP)

Outbound PDU :

Simulation of FTP message transmission :-







PDU Information at Device: PC0

OSI Model | Inbound PDU Details | Outbound PDU Details

At Device: PC0
Source: PC0
Destination: 10.11.10.2

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer 4: TCP Src Port: 21, Dst Port: 49902	Layer 4: TCP Src Port: 49902, Dst Port: 21
Layer 3: IP Header Src. IP: 10.11.10.2, Dest. IP: 10.10.10.1	Layer 3: IP Header Src. IP: 10.10.10.1, Dest. IP: 10.11.10.2
Layer 2: Ethernet II Header 0006.2A70.617C >> 0030.F284.7956	Layer 2: Ethernet II Header 0030.F284.7956 >> 0006.2A70.617C
Layer 1: Port FastEthernet0	Layer 1: Port(s): FastEthernet0

1 FastEthernet0 receives the frame

Challenge Me | << Previous Layer | Next Layer >>

PDU Information at Device: PC0

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	Bytes
PREAMBLE: 101010...10	SFD	DEST ADDR: 0006.2A70.617C	
SRC ADDR: 0030.F284.7956	TYPE: 0x0800	DATA (VARIABLE LENGTH)	FCS: 0x00000000

IP

0	4	8	16	20	24	Bits
VER: 4	IHL: 5	DSCP: 0x00	TL: 40			
ID: 0x0000			FLAGS: 0x2	FRAG OFFSET: 0x000		
TTL: 128	PRO: 0x06	CHKSUM				
SRC IP: 10.10.10.1						
DST IP: 10.11.10.2						
DATA (VARIABLE LENGTH)						

TCP

0	4	8	16	24	Bits
SOURCE PORT: 49902			DESTINATION PORT: 21		
SEQUENCE NUMBER: 1					
ACKNOWLEDGEMENT NUMBER: 1					
OFFSET: 0x0	RESERVED: 0	FLAGS: 0b00010000	WINDOW: 65535		
CHECKSUM: 0x0000			URGENT POINTER: 0x0000		
OPTION					
DATA (VARIABLE LENGTH)			PADDING: 0		

PDU Information at Device: PC0

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	Bytes
PREAMBLE: 101010...10	SFD	DEST ADDR: 0030.F284.7956	
SRC ADDR: 0006.2A70.617C	TYPE: 0x0800	DATA (VARIABLE LENGTH)	FCS: 0x00000000

IP

0	4	8	16	20	24	Bits
VER: 4	IHL: 5	DSCP: 0x00	TL: 44			
ID: 0x0007			FLAGS: 0x2	FRAG OFFSET: 0x000		
TTL: 128	PRO: 0x06	CHKSUM				
SRC IP: 10.11.10.2						
DST IP: 10.10.10.1						
DATA (VARIABLE LENGTH)						

TCP

0	4	8	16	24	Bits
SOURCE PORT: 21			DESTINATION PORT: 49902		
SEQUENCE NUMBER: 0					
ACKNOWLEDGEMENT NUMBER: 1					
OFFSET: 0x0	RESERVED: 0	FLAGS: 0b00010010	WINDOW: 16384		
CHECKSUM: 0x0000			URGENT POINTER: 0x0000		
OPTION					
DATA (VARIABLE LENGTH)			PADDING: 0		

PDU Information at Device: Server0

OSI Model | Inbound PDU Details

At Device: Server0
Source: PC0
Destination: 10.11.10.2

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer 4: TCP Src Port: 59001, Dst Port: 21	Layer4
Layer 3: IP Header Src. IP: 10.10.10.1,	Layer3
Layer 2: Ethernet II Header 0060.2F4C.	Layer2
Layer 1: Port FastEthernet0	Layer1

1 FastEthernet0 receives the frame

Challenge Me | << Previous Layer | Next Layer >>

PDU Information at Device: Server0

OSI Model | Inbound PDU Details

PDU Formats

Ethernet II

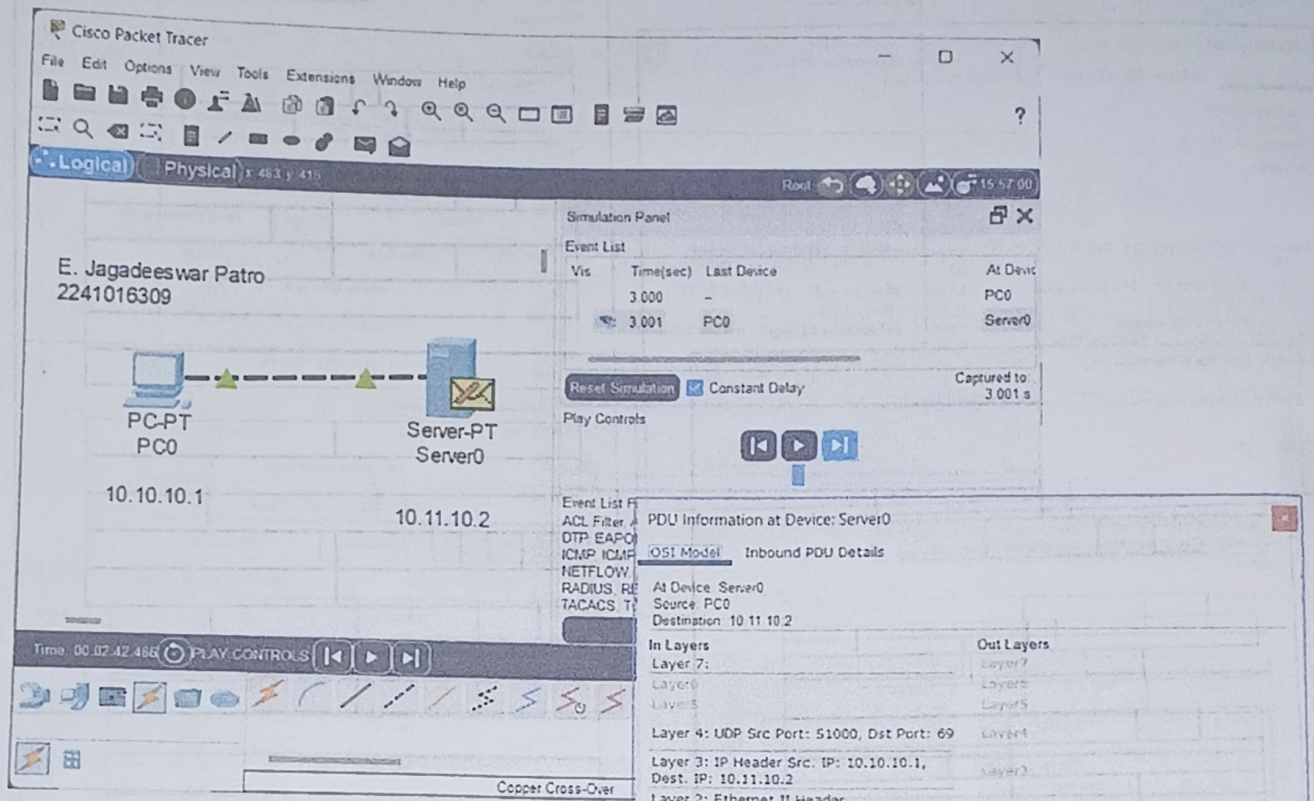
0	4	8	Bytes
PREAMBLE: 101010...10	SFD	DEST ADDR: 00D0.D326.E85E	
SRC ADDR: 0060.2F4C.1D9D	TYPE: 0x0800	DATA (VARIABLE LENGTH)	FCS: 0x00000000

IP

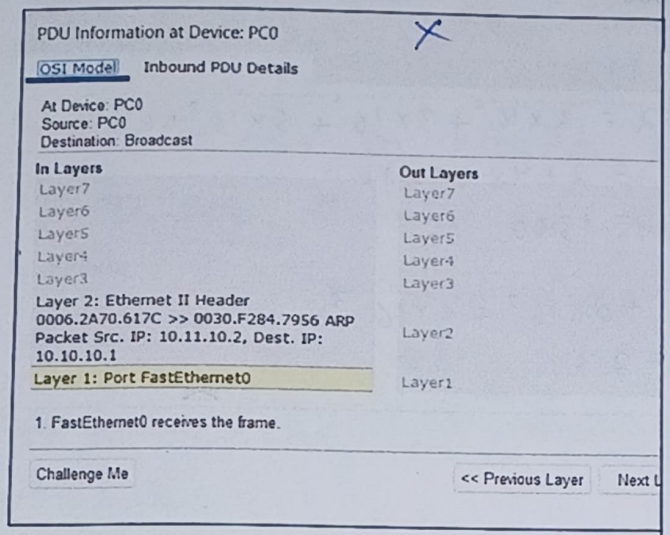
0	4	8	16	20	24	Bits
VER: 4	IHL: 5	DSCP: 0x00	TL: 40			
ID: 0x0005			FLAGS: 0x2	FRAG OFFSET: 0x000		
TTL: 128	PRO: 0x06	CHKSUM				
SRC IP: 10.10.10.1						
DST IP: 10.11.10.2						
DATA (VARIABLE LENGTH)						

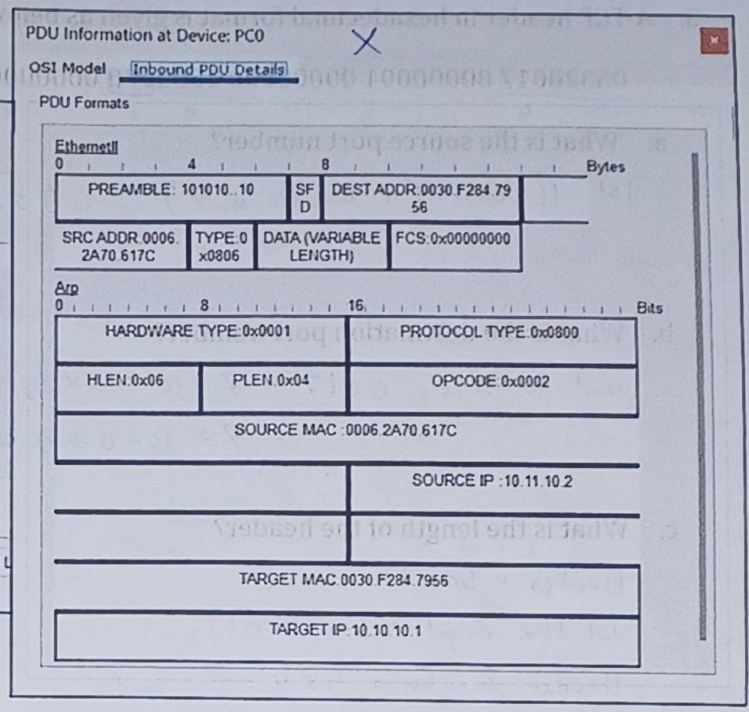
TCP

0	4	8	16	24	Bits
SOURCE PORT: 59001			DESTINATION PORT: 21		
SEQUENCE NUMBER: 1					
ACKNOWLEDGEMENT NUMBER: 1					
OFFSET: 0x0	RESERVED: 0	FLAGS: 0b00001000	WINDOW: 65535		
CHECKSUM: 0x0000			URGENT POINTER: 0x0000		
OPTION					
DATA (VARIABLE LENGTH)			PADDING: 0		


Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical Physical
E. Jagadeeswar Patro
2241016309
PC-PT
PC0
10.10.10.1
Server-PT
Server0
10.11.10.2
Simulation Panel
Event List
Vis Time(sec) Last Device At Devic
3.000 - PC0
3.001 PC0 Server0
Reset Simulation
Constant Delay
Captured to: 3.001 s
Play Controls
Time: 00:02:42.466
PLAY CONTROLS
Copper Cross-Over
PDU Information at Device: Server0
OSI Model
Inbound PDU Details
At Device: Server0
Source: PC0
Destination: 10.11.10.2
In Layers
Out Layers
Layer 7:
Layer 4: UDP Src Port: 51000, Dst Port: 69
Layer 3: IP Header Src. IP: 10.10.10.1, Dest. IP: 10.11.10.2
Layer 2: Ethernet II Header 0030.F284.7956 >> 0006.2A70.617C
Layer 1: Port FastEthernet0
1 FastEthernet0 receives the frame
Challenge Me
<< Previous Layer
Next Layer >>
PDU Information at Device: Server0
OSI Model
Inbound PDU Details
PDU Formats
Ethernet II
0 4 8
Bytes
PREAMBLE 10101010 10
SFD
DEST ADDR 0006.2A70.617C
SRC ADDR 0030.F284.7956
TYPE 0x0800
DATA (VARIABLE LENGTH)
FCS 0x00000000
IP
0 4 8 16 20 24
Bits
VER 4
IHL 5
DSCP 0x00
TL 28
ID 0x000a
FLAGS 0x0
FRAG OFFSET 0x000
TTL 32
PRO 0x11
CHKSUM
SRC IP 10.10.10.1
DST IP 10.11.10.2
DATA (VARIABLE LENGTH)
UDP
0 16
Bits
SOURCE PORT 51000
DESTINATION PORT 69
LENGTH 0x0008
CHECKSUM 0
DATA (VARIABLE LENGTH)
Variable Size PDU
0 8 16
Bytes
DATA (VARIABLE LENGTH)

Acknowledgment (Inbound PDU:)





Conclusion:

Implementing basic ethernet using CPT provides practical experience in configuring network devices and understanding communication protocols. This hands on approach enables detailed analysis of IP, TCP, UDP headers, enhancing knowledge of data transmission and error handling.

Exercises:

1. Given the value available in "fragment offset" field of IP header is 100. what is the number of bytes ahead of this fragment?

IP header = 100

offset measured in 8-byte blocks.

∴ Bytes = 100 × 8 = 800 bytes.

2. An IP packet has arrived with the first 8 bits as 01000010. What is the version and the header length?

IP Packet = 0100 0010

↓ version = 4

↓ header length = 2 = 2×4 (∵ scaling) = 8 bytes.

Name: E. Jagadeeswar Patro

Regd. Number: 2241016309

3. A TCP header in hexadecimal format is given as below.

05320017 00000001 00000000 50020 7ff 00000000
a b c d

a. What is the source port number?

1st 16-bits (4-hexadecimal) : $0532 = 2\times16^0 + 3\times16^1 + 5\times16^2 + 0\times16^3$
$= 2 + 48 + 1280$
$= 1330$

b. What is the destination port number?

next 16-bits, $0017 = 7\times16^0 + 1\times16^1 + 0\times16^2 + 0\times16^3$
$= 7 + 16 + 0 + 0 = 23$

c. What is the length of the header?

Header = 5002
1st hex digit = $5 = (0101)_2$
Header length = $5 \times 4 = 20$ bytes

d. What is the window size?

$07ff = f\times16^0 + f\times16^1 + f\times16^2 + 0\times16^3$
$= 15\times16^0 + 15\times16 + 15\times256 + 0$
$= 2047$

4. Given a UDP header in hexadecimal format 06 32 00 0D 00 1C E2 17. Find the following:

a. Source port number.

$0632 = 2\times16^0 + 3\times16^1 + 6\times16^2 + 0$
$= 1586$

b. Destination port number.

$000D = D\times16^0 + 0 + 0 + 0$
$= 13$

c. Length of user datagram.

$001C = C\times16^0 + 1\times16^1 + 0 + 0$
$= 28$

d. Length of the data.

Data Length = Total length − Header length
for UDP, HL = 8 bytes, TL = 28 bytes
∴ Length of Data = 28 − 8 = 20 bytes

Ashan 4/10/24

EXPERIMENT 3

Aim: Implementation of Network Topologies using Cisco Packet Tracer.

Objectives:

1- An overview on network topologies (star, bus, ring and mesh)

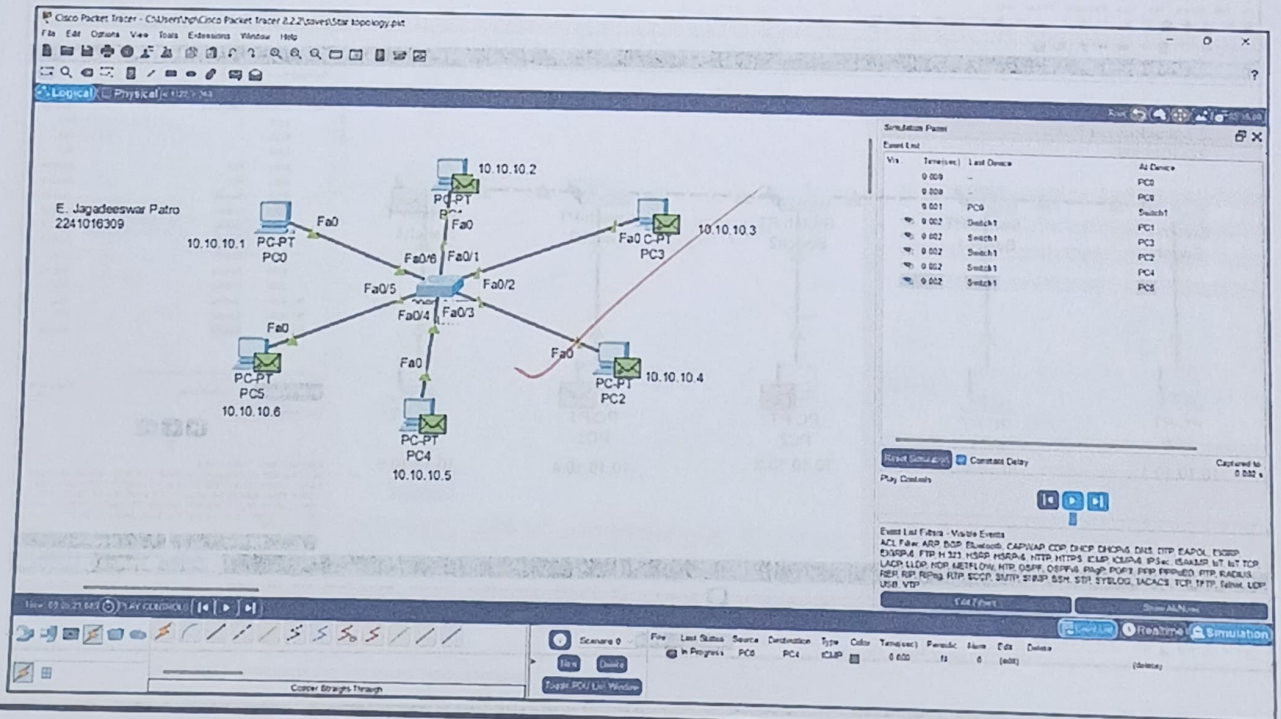
Star topology - all devices are connected to a single hub/switch through a cable. This hub/switch is the central node and all other nodes are connected to central node.

Bus Topology - Every computer & network device is connected to a single cable. This a bidirectional topology.

Ring Topology - a bus topology in a closed loop format allowing clock-wise / anti-clock wise communication. sending and recieving data in every direction occurs with the help of Token.

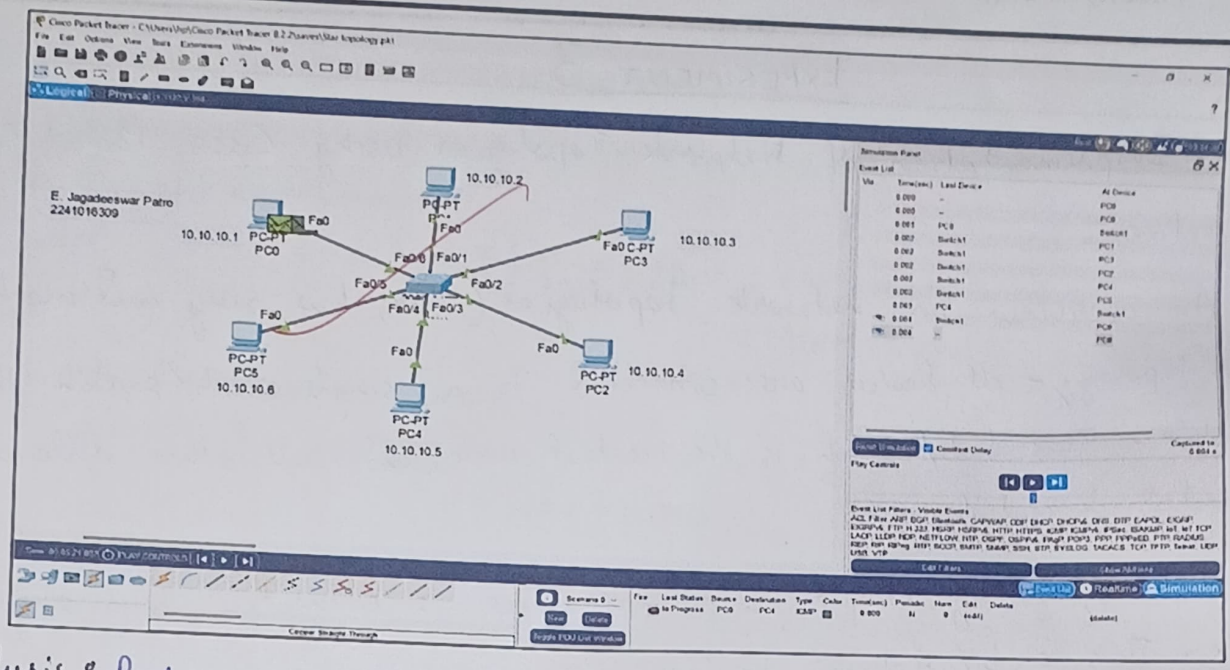
Mesh Topology - every node is directly connected to all other nodes making a hive network. Total no. of connections is given by $N(N-1)/2$.

2- Constructing & simulating a network based on star topology to analyse the performance, scalability & fault tolerance.



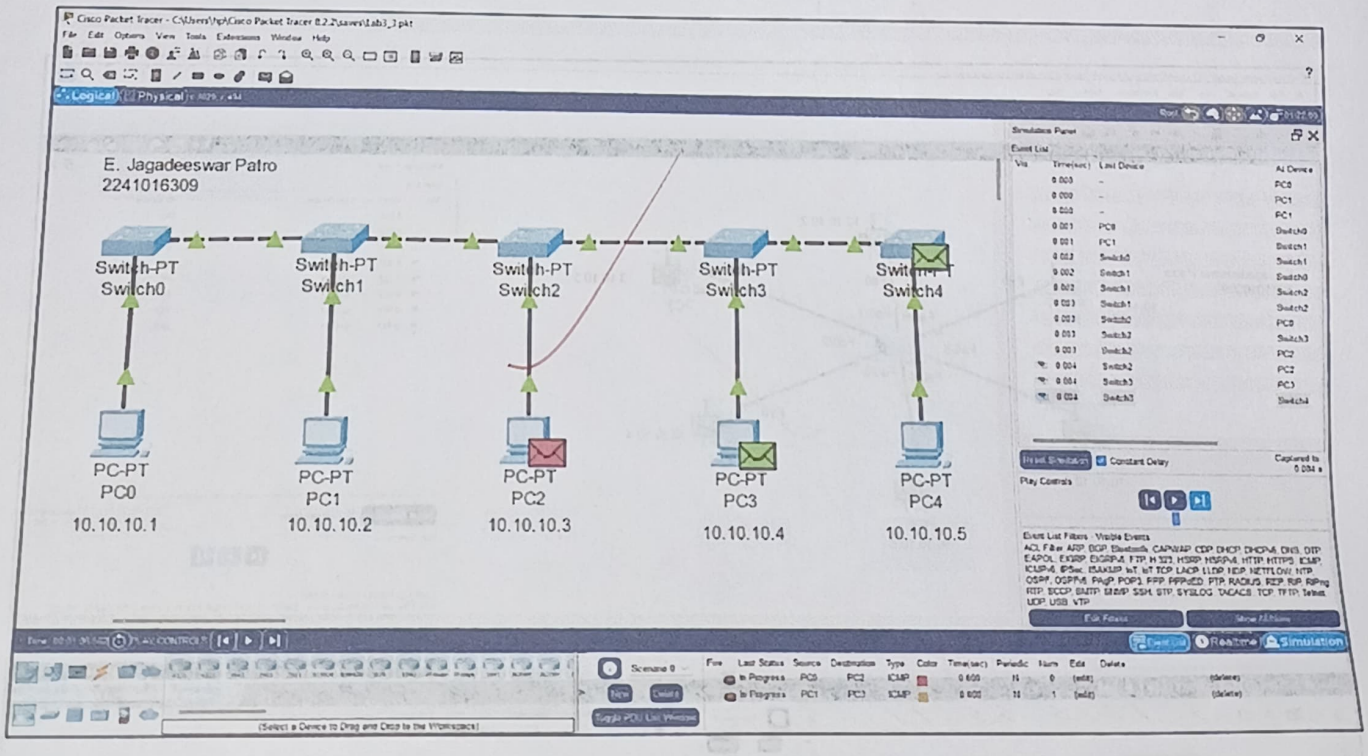
Name: E. Jagadeeswar Patro

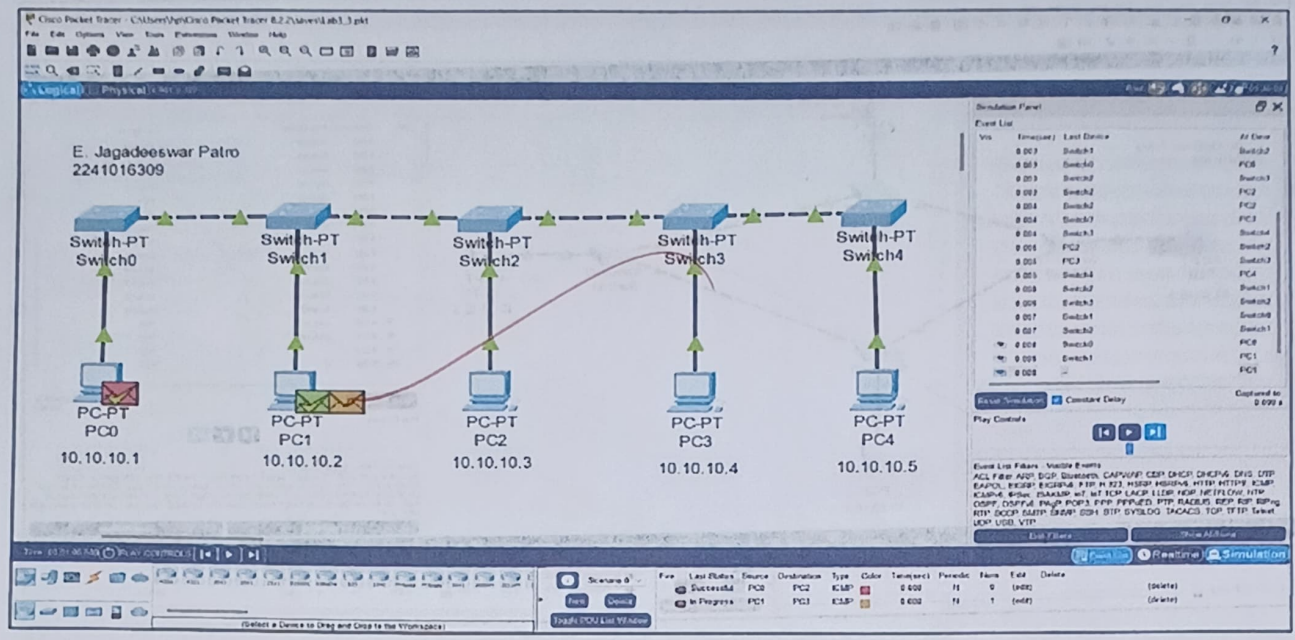
Regd. Number: 2241016309



Analysis:
Performance – with a central switch, data is quickly routed to correct device.
Scalability – easily scalable by adding more devices to the switch.
Fault Tolerance – If one computer's connection fails, the rest of the network remains operational.

3- Constructing & simulating a network based on bus topology to analyze the performance, scalability and fault tolerance.

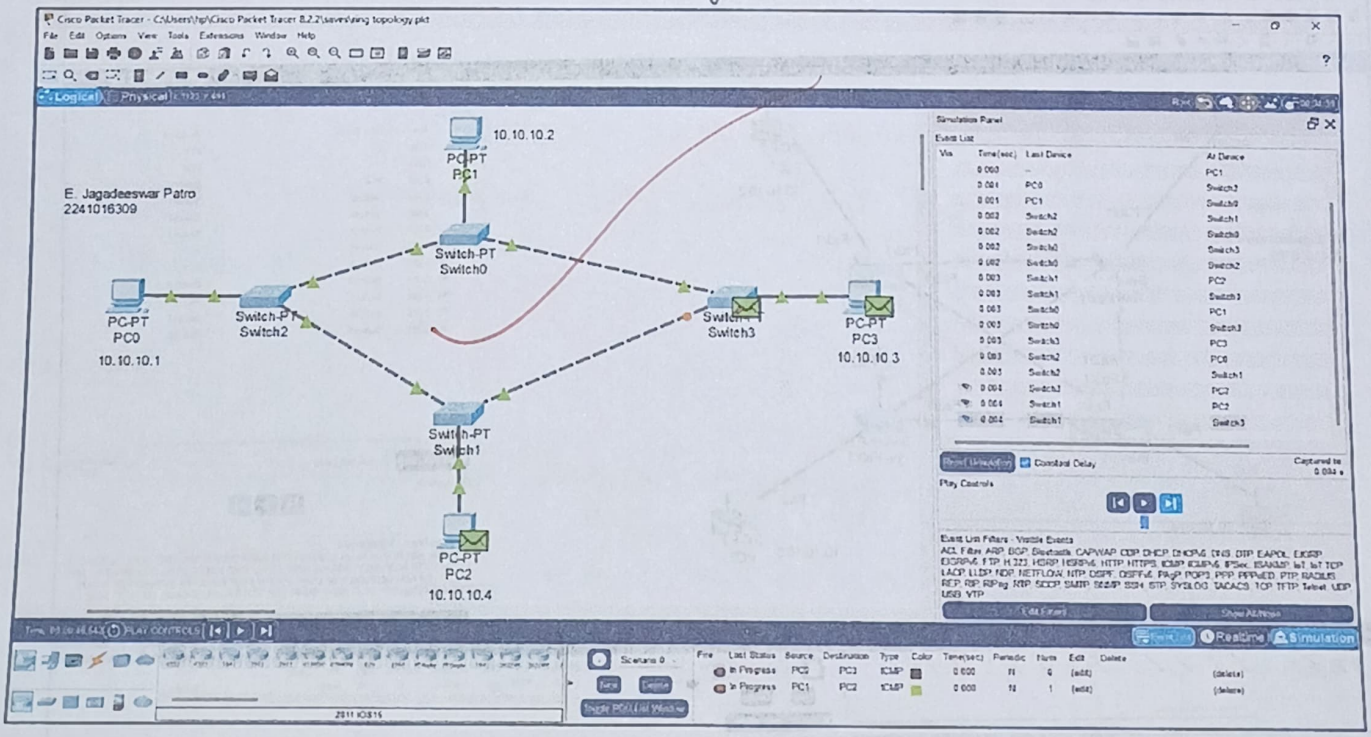


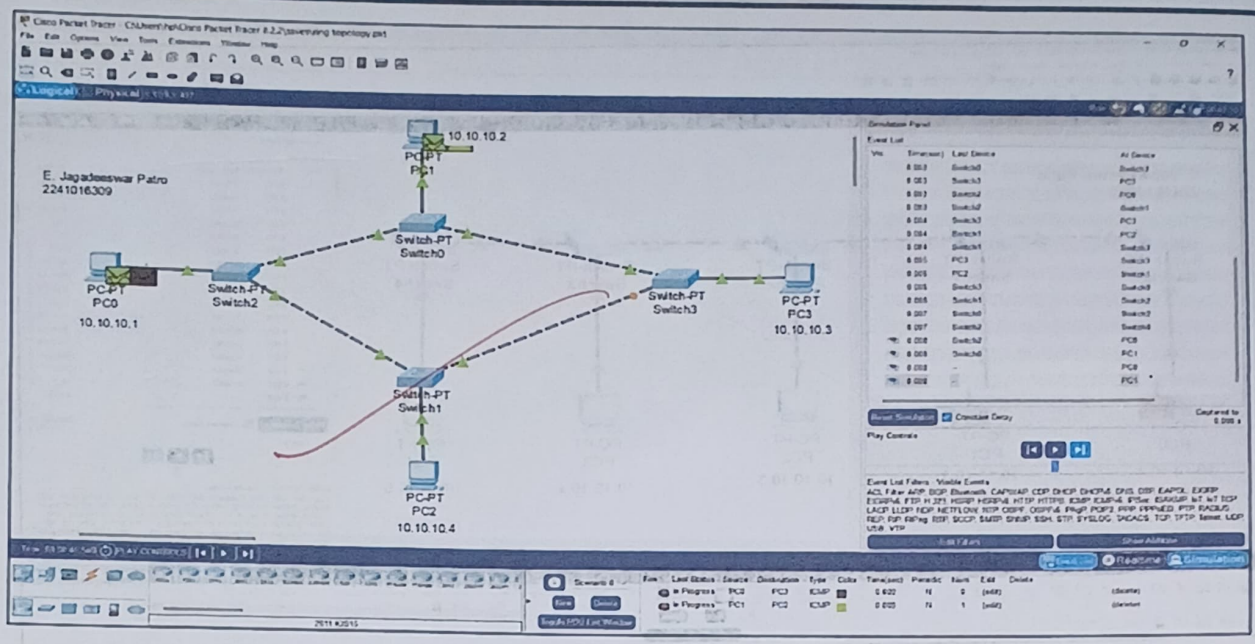


Analysis :-

- Performance : As more computers are added, performance decreases.
- Scalability : has limited scalability due to signal degradation.
- Fault Tolerance : Failure in backbone cable can cause network failure in entirety.

Obj 4 - Constructing and simulating a network based on ring topology to analyze the performance, scalability and fault tolerance.

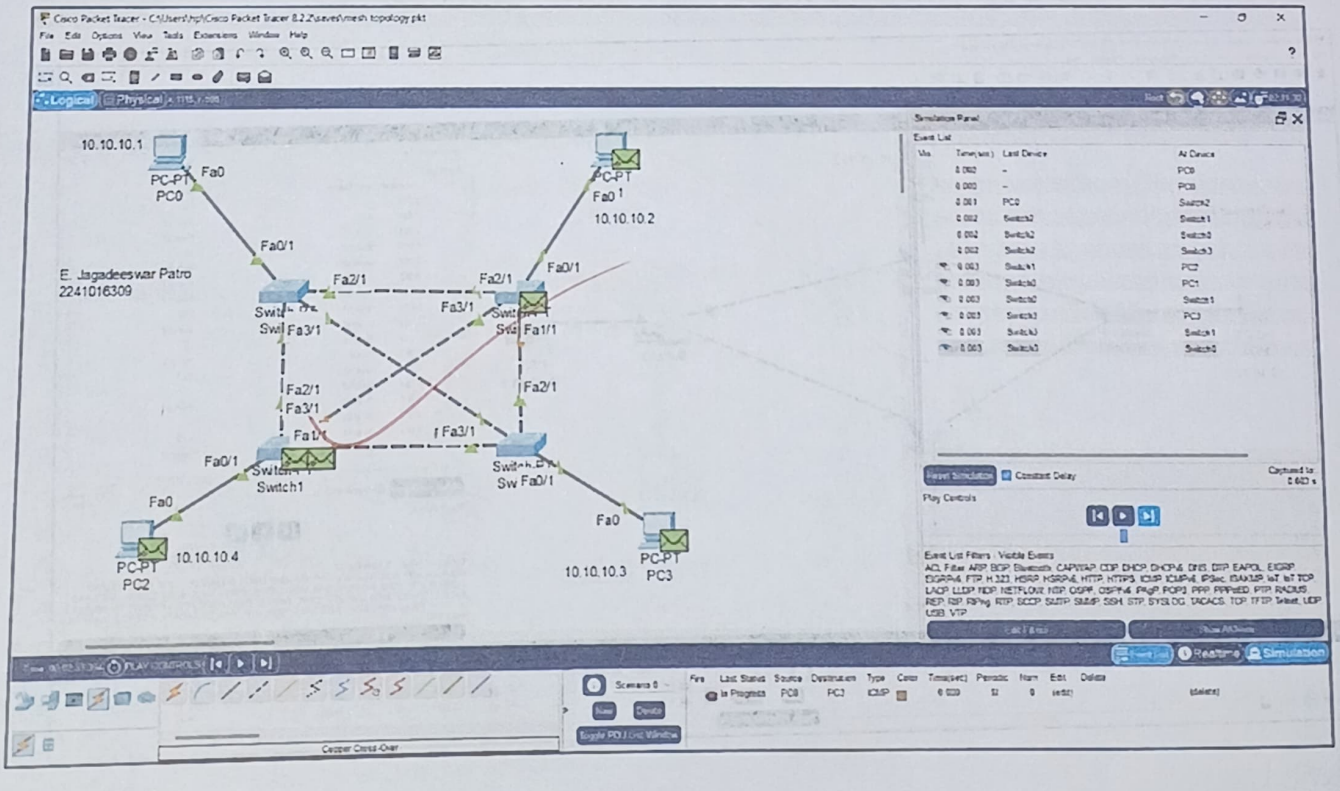


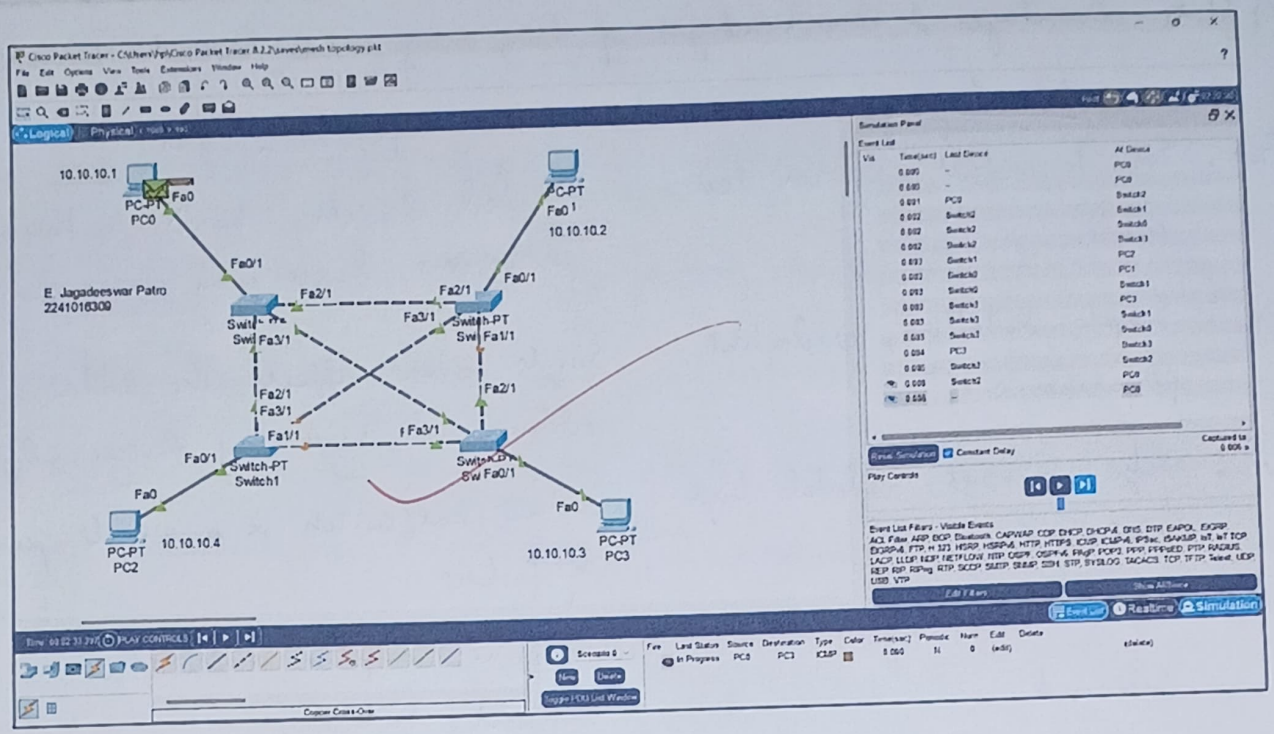


Analysis :-

- Performance - Data travels through each node making it slow.
- Scalability - Adding new devices require the network to be broken reconnected.
- Fault Tolerance - Failure of one link disrupts entire network unless dual rings used.

5 - Constructing and simulating a network based on mesh topology to analyze performance, scalability and fault tolerance.





Analysis :-

→ Performance : offers high performance with redundancy.

→ Scalability : It becomes difficult to manage as the number of devices increases.

→ Fault Tolerance : very high fault tolerance since each device has multiple links.

Conclusion :

Through this experiment, we have implemented and simulated various connections to analyze and understand the functioning of various network topologies.

Exercise :

1) Differentiate physical & logical topology -

Physical topology describes the actual layout of devices, cables, and network hardware. Whereas logical topology describes how data flows across the network, regardless of its physical layout.

2) State advantages & disadvantages of bus, ring, star & mesh technologies.

	Advantages	Disadvantages
Bus:	Easy to install, requires less cable.	limited devices, hard to troubleshoot performance drops with more devices
Ring:	Simple dataflow, predictive performance	Single failure affects the entire network adding and removing devices is difficult
Star:	easy to manage, scalable, high performance	central hub/switch is a single point of failure.
Mesh:	high redundancy, fault tolerant.	expensive, complex installation, difficult to scale

3) Briefly explain various factors for selecting a proper network topology.

-> cost - budget constraints may limit choice of topology.

-> Scalability - some topologies like star are easier to scale & some such as mesh are difficult.

-> Performance - networks require high throughput & low latency. Star & mesh benefit from this.

-> Fault Tolerance - Mesh topology offers high fault tolerance whereas bus & ring can break with single failure.

-> Maintainence - star is easier to maintain than ring or mesh topology.

4) For five devices in a network, what is the number of cable links require in a mesh ring, bus, and star topology?

-> Mesh: $\frac{n(n-1)}{2} = \frac{5(5-1)}{2} = 10$ Cable links.

→Ring : Always n links = 5 links

→Bus : 1 backbone link shared by all end device

→Star : n links ; one per device to central switch = 5 links.

5) How does bus arbitration work in network topology ?

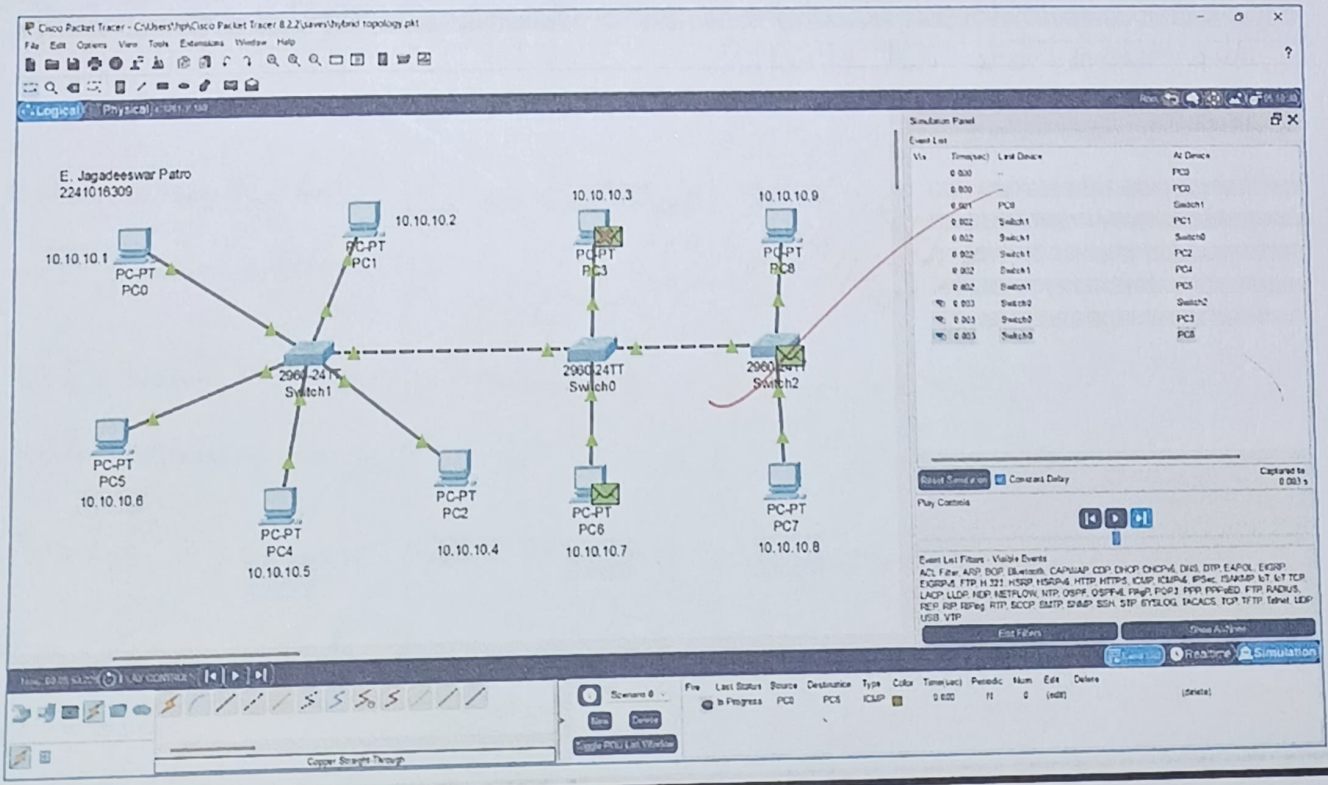
Bus arbitration is the method by which multiple devices share a common communication line. A control mechanism ensures that only one device transmits at a time, preventing data collision.

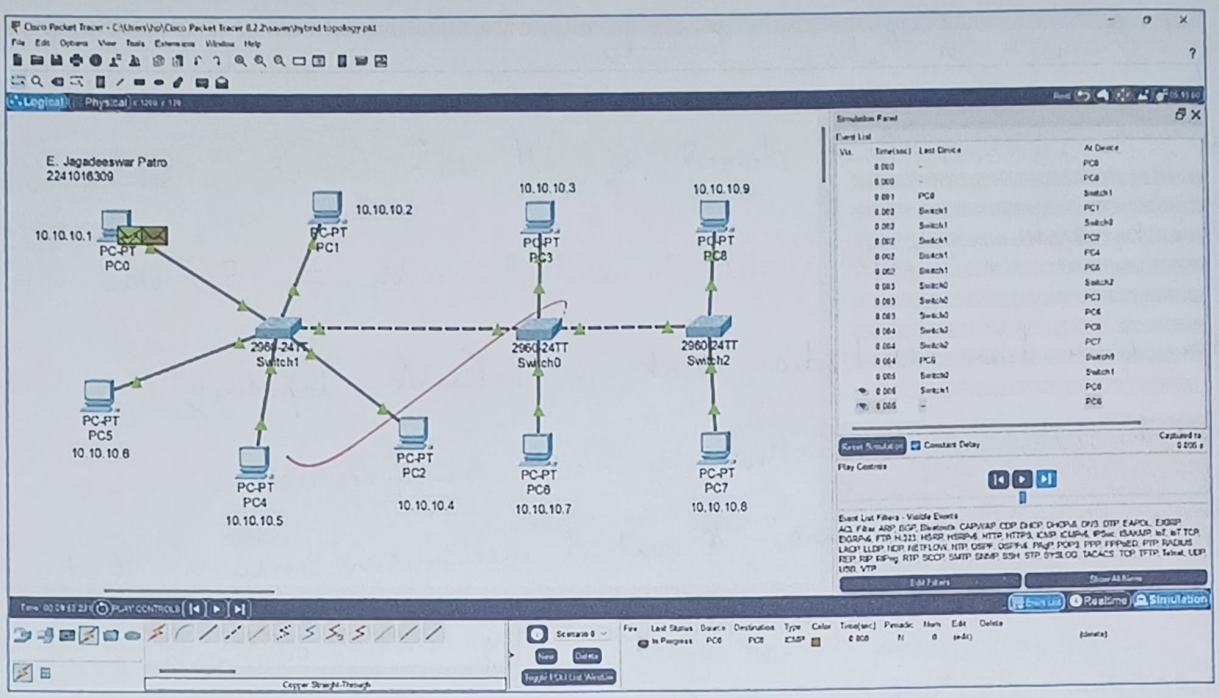
Common bus arbitration methods include :

- CSMA/CD – Carrier Sense Multiple Access with Collision Detection.
- Token passing

Extra Objective :

Constructing and simulating a network based on hybrid topology to analyze performance, scalability and fault tolerance.





Analysis :

↳ Performance : optimized for specific needs such as, it can implement star to improve fault tolerance and mesh to improve data routing efficiency.

↳ Scalability : it can scale and adapt without major changes.

↳ Fault Tolerance : It is highly reliable as if one part fails, rest of the nodes are not affected.

18/10/24

Name: E. Jagadeeswar Patro

Regd. Number: 2241016309

Experiment 4

Aim: Implementation and understanding the use of IPv4 Addressing, NAT with Cisco Packet Tracer

Objectives:

1) An overview on IPv4 addressing (Public, Private, Classful) and NAT.

↳ Public IPv4 addresses are globally unique, used to identify devices accessible over the internet. They are routable on the internet & are assigned by IANA or regional registries.

Range: 0.0.0.0 to 255.255.255.255 (excluding private ranges)

↳ Private IPv4 addresses are used within local network for devices without internet connectivity. They allow internal communication without consuming public IP space.

Reserved ranges:

A: 10.0.0.1 – 10.255.255.255

B: 172.16.0.1 – 172.31.255.255

C: 192.168.0.1 – 192.168.255.255

↳ Classful Addressing – IPv4 addresses are classified into 5 types - A, B, C, D, E every class is associated with the default subnet mask which defines the network and the host portion. These are further categorised into public and private addressing.

↳ NAT (Network Address Translator) is an IP service allowing translation of private addresses to public. It's necessary for inter-network communication. It helps to conserve public IP addresses & provides additional security. It also allows multiple devices on a local network to share single public IP address.

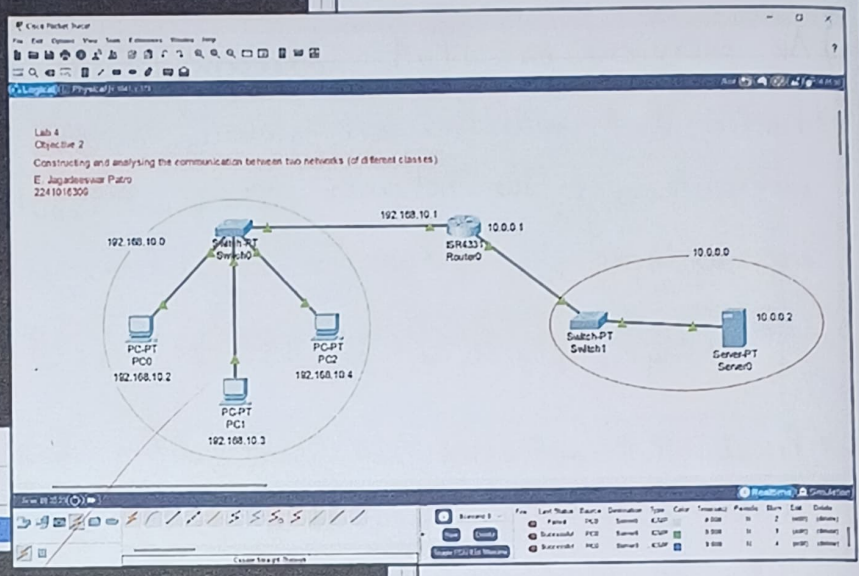
2) Constructing and analysing the communication between two networks (of different classes).

PC0

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time<1ms TTL=127
Reply from 10.0.0.2: bytes=32 time=28ms TTL=127
Reply from 10.0.0.2: bytes=32 time<1ms TTL=127
Reply from 10.0.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 28ms, Average = 7ms

C:\>
```

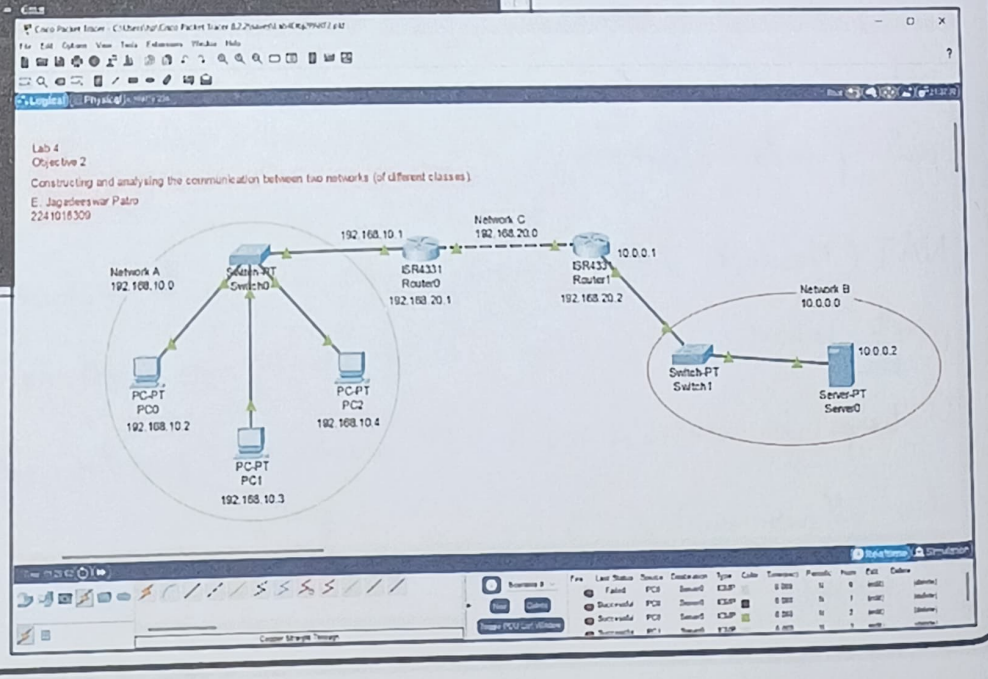


PC0

Physical Config Desktop Programming Attributes

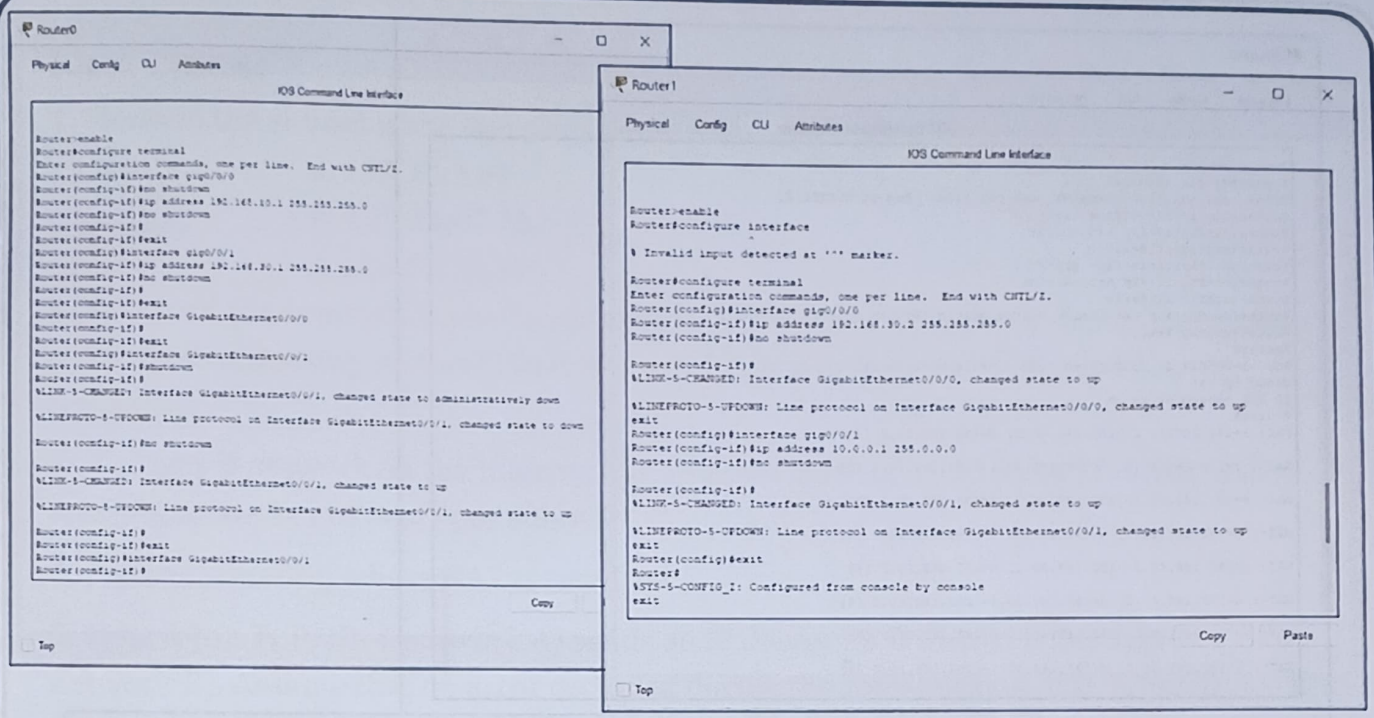
Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time<1ms TTL=127
Reply from 10.0.0.2: bytes=32 time=28ms TTL=127
Reply from 10.0.0.2: bytes=32 time<1ms TTL=127
Reply from 10.0.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 28ms, Average = 7ms

C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=27ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 27ms, Average = 6ms

C:\>
```

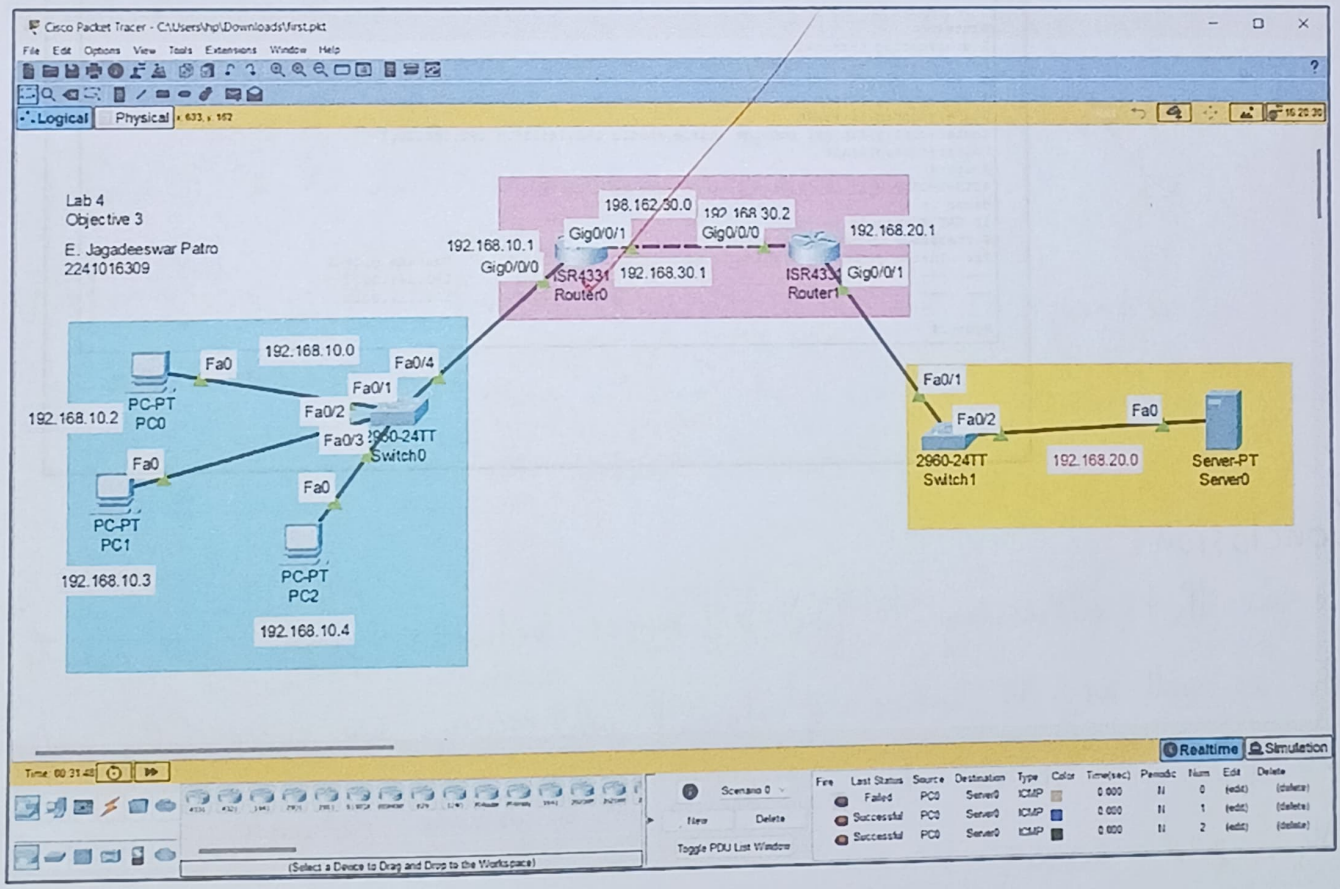


Name: E. Jagadeeswar Patro

Regd. Number: 2241016309



3) Configuring and implementing NAT using a router to analyze the comm. between PCs (in a private network) and a public server.



Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gig0/0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface gig0/0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip nat inside source static 192.168.10.2 192.168.30.1
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
debug ip nat
IP NAT debugging is on
Router#
NAT: s=192.168.10.2->192.168.30.1, d=192.168.20.2 [4]

NAT*: s=192.168.20.2, d=192.168.30.1->192.168.10.2 [2]

NAT: s=192.168.10.2->192.168.30.1, d=192.168.20.2 [5]

NAT*: s=192.168.20.2, d=192.168.30.1->192.168.10.2 [3]

NAT: s=192.168.10.2->192.168.30.1, d=192.168.20.2 [6]

NAT*: s=192.168.20.2, d=192.168.30.1->192.168.10.2 [4]

NAT: s=192.168.10.2->192.168.30.1, d=192.168.20.2 [7]

NAT*: s=192.168.20.2, d=192.168.30.1->192.168.10.2 [5]
```

Top

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>en
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gig0/0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip nat outside source static 192.168.30.2 192.168.20.2
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
debug ip nat
IP NAT debugging is on
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  ---               ---                192.168.30.2       192.168.20.2
---  ---               ---                192.168.20.2       192.168.30.2

Router#
```

Copy Paste

Top

Conclusion:

We use IPv4 addressing to find differences between public and private IPs as well as the basics of classful addressing. We successfully configured NAT on a router allowing devices in a private network to communicate with a public server.

Exercises:

1. Mention the subnet mask and class of the following IPv4 addresses:

a. 172.14.9.64
b. 129.34.67.25
c. 185.56.32.87

2. What are the commands used to determine the current IP address configurations on a Windows operating system? What is the difference between ipconfig and ifconfig commands?

3. If a class B network on the Internet has a subnet mask of 255.255.248.0, what is the maximum number of hosts per subnet?

4. List the situation where NAT is required.

5. Host A (on TCP/IPv4 network A) sends an IP datagram D to host B (also on TCP/IPv4 network B). Assume that no error occurred during the transmission of D. When D reaches B, what are the IP header field(s) that may be different from that of the original datagram D?

Solution:

class subnet

1) a) 172.14.9.64 → Class B, 255.255.0.0

b) 129.34.67.25 → Class B, 255.255.0.0

c) 185.56.32.87 → Class B, 255.255.0.0

2) 'ipconfig' is used to display the current network configuration on a windows machine. 'ipconfig/all' can be used for a more detailed info. including MAC address, DNS server & DHCP settings.

'ipconfig' is run on windows machine whereas 'ifconfig' is run on a linux/unix machine.

3) 255.255.248.0 → in binary : 11111111.11111111.11111000.00000000

∴ N/w bits = 21 & Host bits = 32 − 21 = 11

Maximum hosts = $2^{11} - 2$ = 2046 hosts.

4) NAT is required:

a) IPv4 address shortage

b) Private N/w communication

c) security

d) Port forwarding

e) Multiple device accessing the internet

f) simplified address management.

5) When IP datagram D reaches host B, the following IP header field may be different:

(i) Time to live (TTL): Decreases by 1 at each hop

(ii) Header checksum: Recalculated at each hop

(iii) source IP address: May change if NAT used.

(iv) Destination IP address: Generally remains unchanged unless NAT is involved.

S. Tabor

Experiment - 5

Aim: Implementation and understanding the use of DNAT and PAT with Cisco Packet Tracer.

Objectives:

1) An overview on DAT and PAT

→ DAT: Dynamic Network Address Translation

↳ It dynamically assigns a public IP address from a pool of public IP address to devices in a private network, whenever they initiate outbound traffic.

↳ The addresses are returned to the pool when the session ends.

↳ Enables multiple devices to access without requiring unique public IPs.

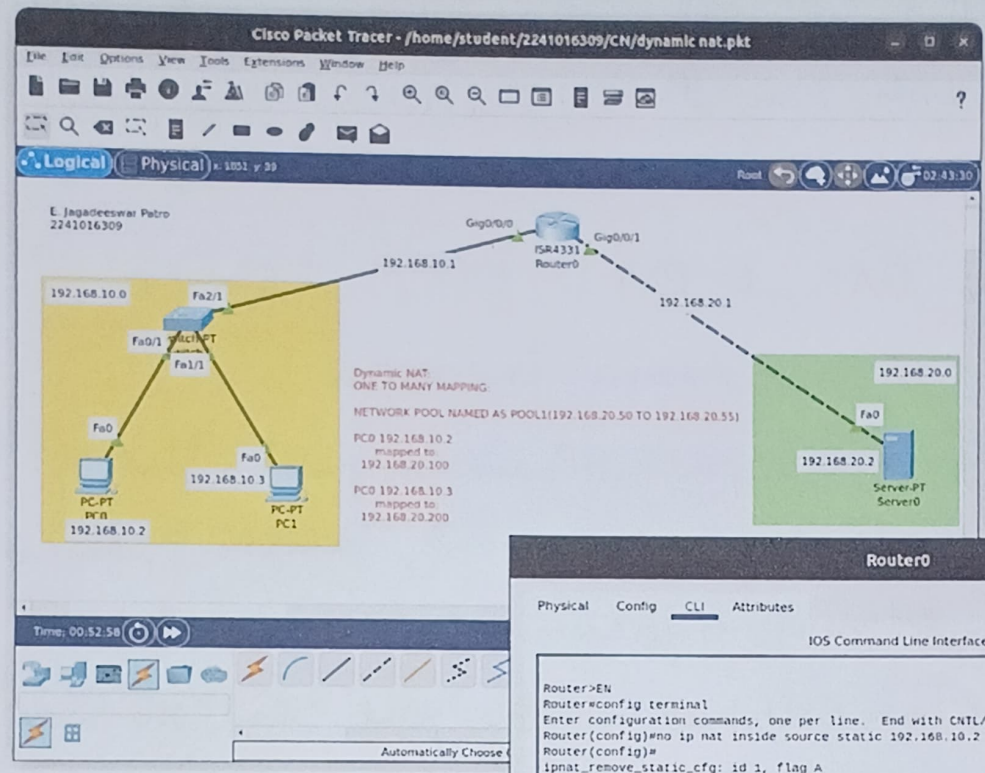
→ PAT: Port Address Translation

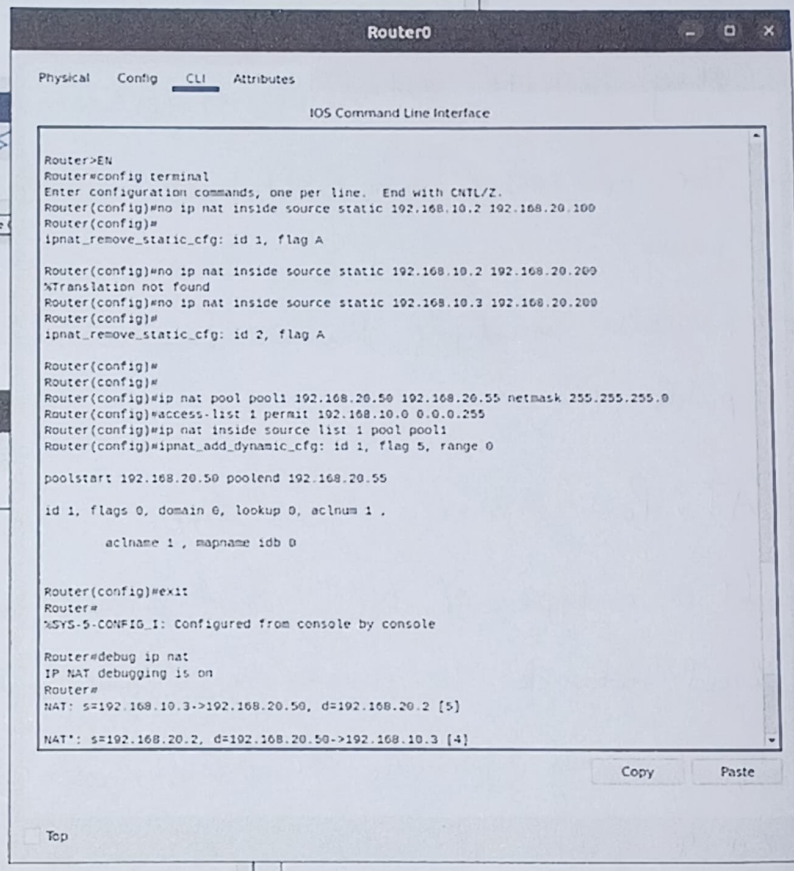
↳ It is a type of NAT that allows multiple devices on a local network to share a single public IP address. It works by mapping private IP address and their port numbers to a single public IP address with unique port numbers.

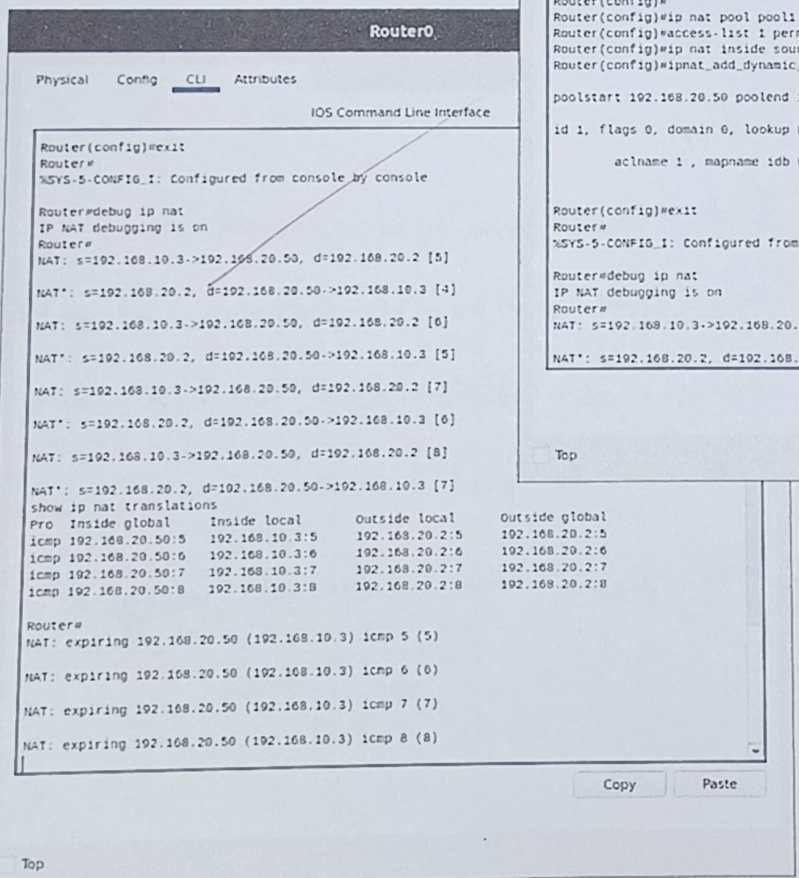
↳ Enables multiple devices to access the internet using a single public IP.

↳ Conserves IPv4 Addresses.

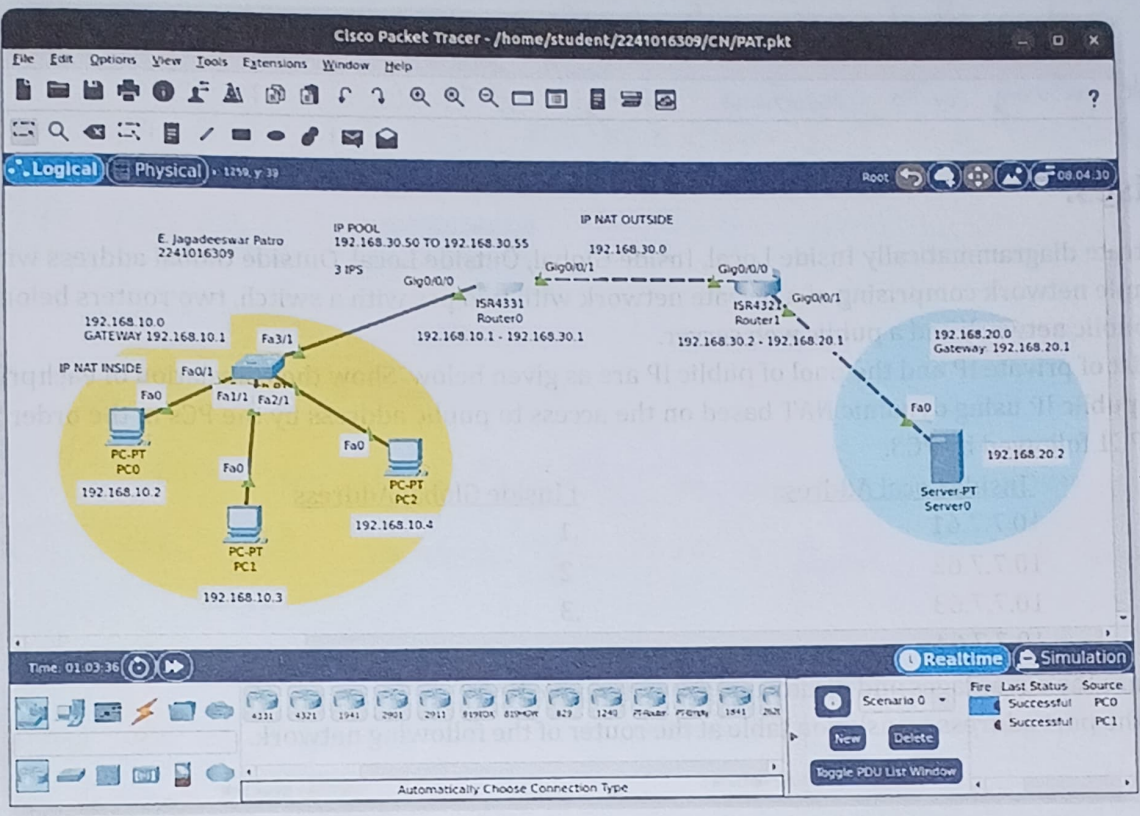
2) Configuring and implementing DAT using a router to analyse the communication between PCs (in a private network) and Public Server

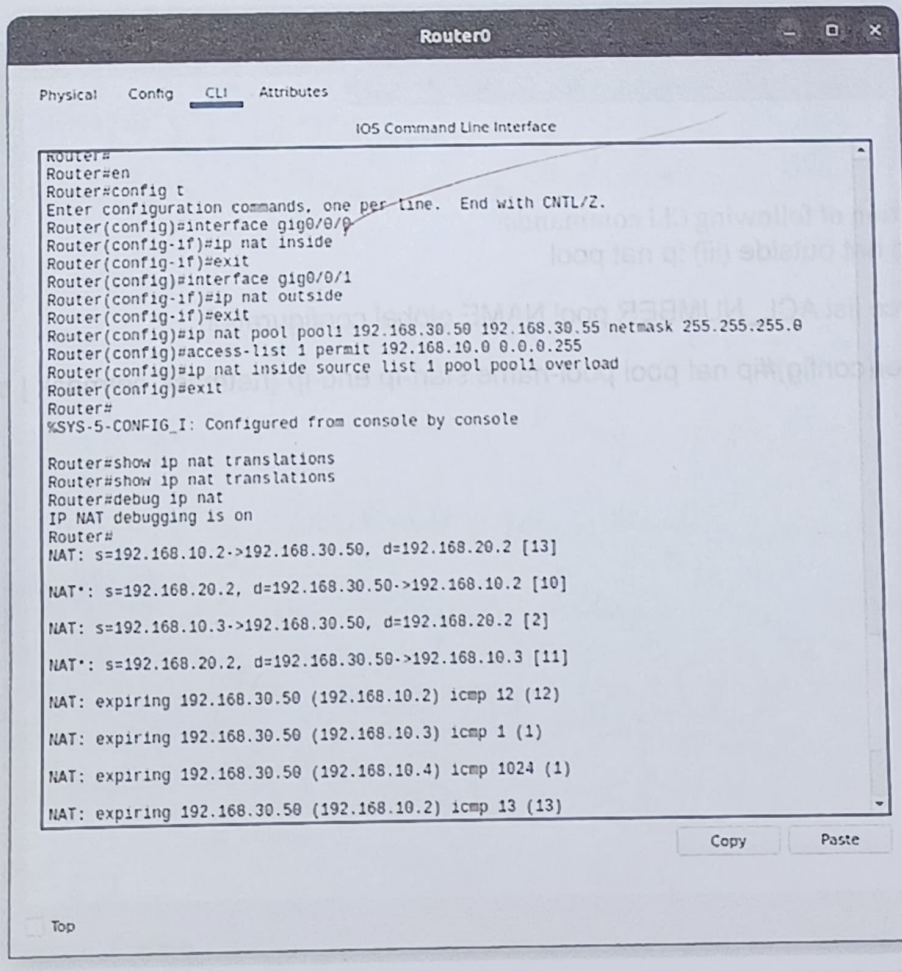






3) Configuring and implementing PAT using a router to analyze the communication between PCs (in a private network) and a PC in public n/w.





Conclusion :

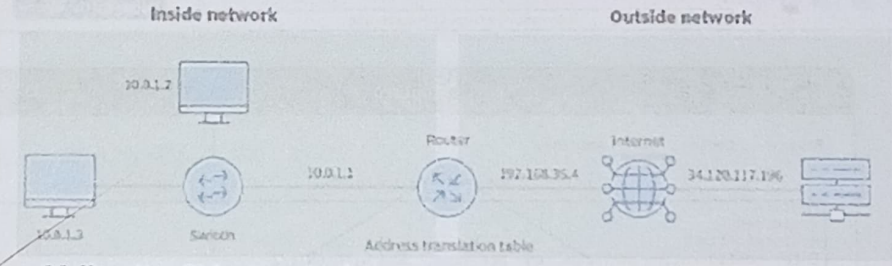
Use of DNAT and PAT was understood and implemented on a newly constructed & configured topology consisting of private & public network along with routers using CPT.

Exercises:

1. Illustrate diagrammatically Inside Local, Inside Global, Outside Local, Outside Global address with an example network comprising of a private network with two pcs with a switch, two routers belonging to a public network and a public web server.
2. The list of private IP and the pool of public IP are as given below. Show the translation of eachprivate IP to public IP using dynamic NAT based on the access to public address by the PCs in the order PC2, PC4, PC1 followed by PC3.

Inside Local Address	f Inside Global Address
l0.7.7.61	.1
l0.7.7.62	.2
l0.7.7.63	.3
l0.7.7.64	

3. What are the advantages and disadvantages of dynamic NAT?
4. Show the port address translation table at the router of the following network.



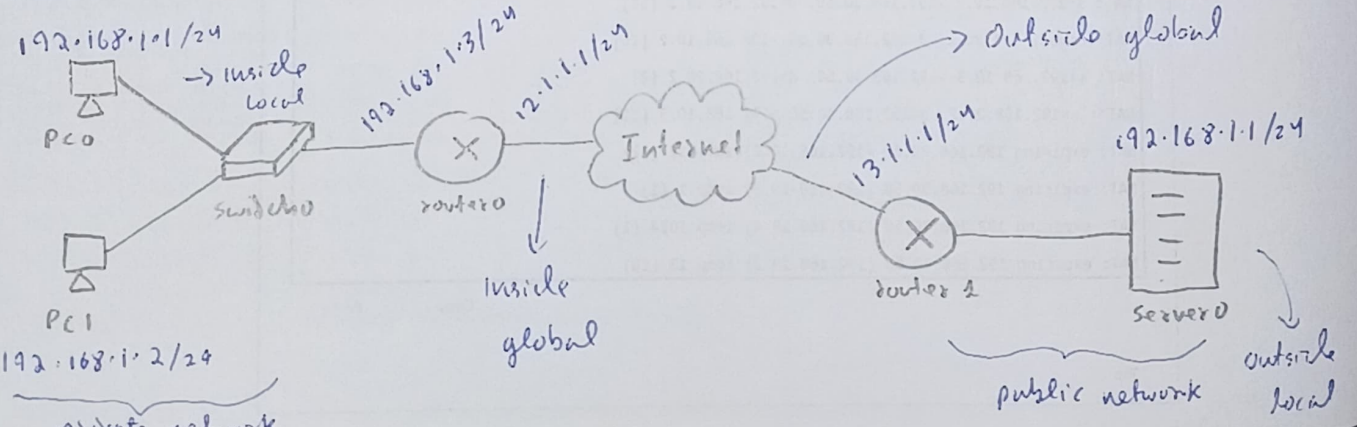
5. Describe the function of following CLI commands:

(i) ip nat inside (ii) ip nat outside (iii) ip nat pool

(iv) ip nat inside source list ACL_NUMBER pool NAME global configuration

(v) router(config)#ip nat pool pool-name start-ip end-ip {netmask netmask | prefix-length prefix-length}

Solution :



2) i) PC_2 (10.7.7.62) Accesses first

Allocated inside global IP: 55.4.4.1

ii) PC_4 (10.7.7.64) Accesses next

Allocated inside global IP: 55.4.4.2

iii) PC1 (10.7.7.61) Access next

Allocated inside global IP: 55.4.4.3

iv) PC_3 (10.7.7.63) Access last

waits for PC_2, PC_4, PC_1 to complete their access & return the pools. whichever global IP is freed 1st will be used.

3) Advantages:

-> Efficient use of Public IP address (allocated only when needed)

-> Hides private IP addresses, improving security.

-> Flexible and suitable for networks with variable external access needs.

-> Cost-effective by reducing the no. of public IPs required.

Disadvantages:

-> Limited by the size of the public IP, excess demands can cause failure

-> Temporary mappings lead to latency during setup

-> No persistent mapping, unreliable for inbound connection

-> scalability issues as the network increases.

4)

Private IP	Private Port	Global IP	Global Port
10.7.7.61	1028	55.4.4.1	5000
10.7.7.62	1026	55.4.4.2	5001

(5) i) ip nat inside : is used to configure an router's interface as an inside NAT interface. Identifies the interface as the private network.

ii) ip nat outside : configures an router's interface as outside NAT interface. Identifies the interface to be connected to the public network.

iii) ip nat pool :- Defines a pool of public IP address that the router can use for NAT translations.

iv) ip nat inside source list ACL_NUMBER pool NAME global configuration : configures DNAT by mapping the internal (Private) IP's specified in an ACL to a pool of public IPs.

v) router(config)# ip nat pool poolname startip endip {netmask netmask | prefix-length prefixlength}
↳ specifies the range of public IP addresses in a NAT pool for use in DNAT

13/12/24

Experiment - 6

Aim : Implementation and understanding the use of sub-netting, and VLSM (Variable Length Subnet Masking) with Cisco Packet Tracer.

Objectives :-

1) An overview on classless IPv4 addressing, CIDR notation, sub-netting and VLSM used in computer networking.

(i) Classless IPv4 addressing moves away from rigid classfull addressing.
↳ It allows flexible prefix lengths.

(ii) CIDR - Classless Inter-Domain Routing is a method for representing an IP address and its network mask in a compact way.
↳ combines IP addresses into blocks, reducing routing table size & enables efficient allocation and route summarization.

(iii) Sub-netting divides a network into smaller sub-networks.
↳ reduces network connections & improves the network.
↳ uses subnet masks.

(iv) VLSM - Variable Length Subnet Masking - assigns different subnet mask within a single network.
↳ Maximizes IP address utilization by reducing waste.
↳ Facilitates hierarchial and efficient routing.

2) Implementing the sub-netting technique to divide a network into smaller subnets (with predefined users) and analysing the communication between PCs in both intra and inter-subnets.

Network : 192.168.10.0

Subnet mask = 255 . 255 . 255 . 0

= 11111111 . 11111111 . 11111111 . 00000000

Subnets required = 3

New Subnet = 11111111 . 11111111 . 11111111 . 11000000

= 255 . 255 . 255 . 192

1st Subnet : 192 . 168 . 10 . 0 to 192 . 168 . 10 . 63

Network ID : 192 . 168 . 10 . 0

Usable range : 192 . 168 . 10 . 1 to 192 . 168 . 10 . 62

Gateway : 192 . 168 . 10 . 1

2nd Subnet : 192 . 168 . 10 . 64 to 192 . 168 . 10 . 127

Network ID : 192 . 168 . 10 . 64

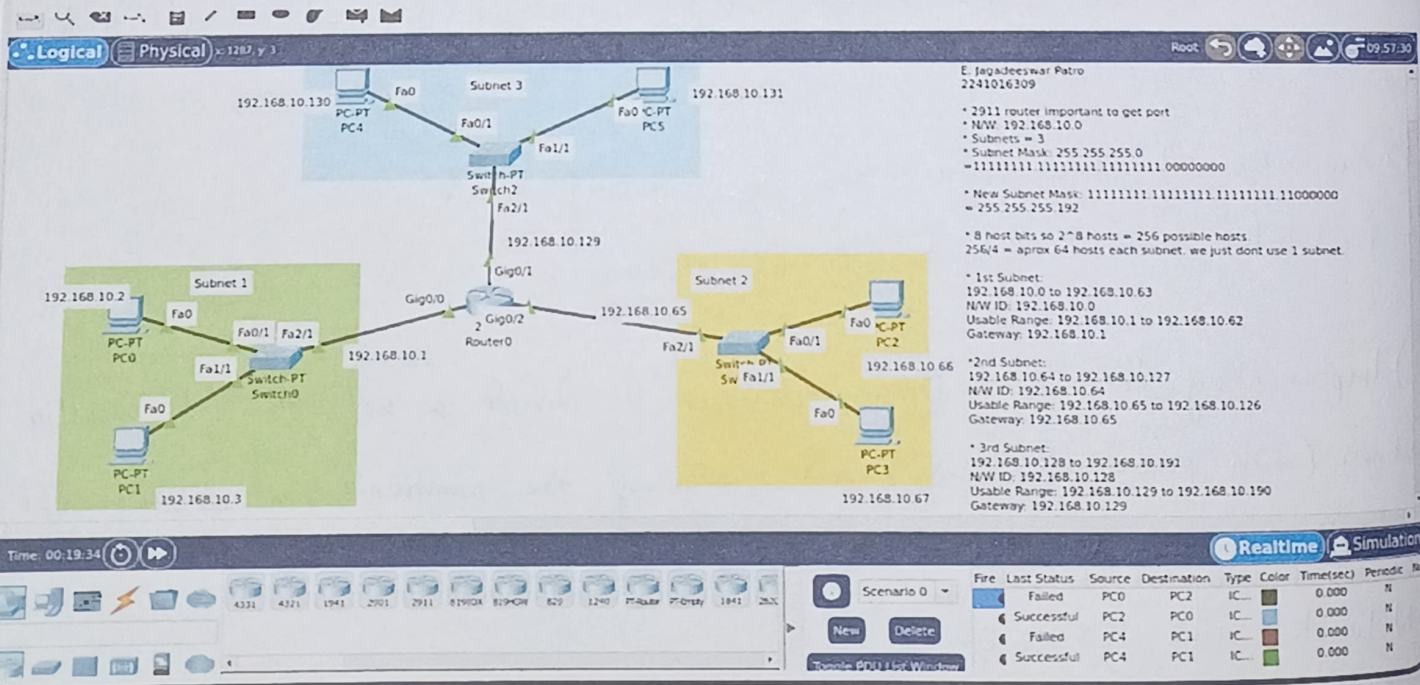
Usable range : 192 . 168 . 10 . 65 to 192 . 168 . 10 . 126

Gateway : 192 . 168 . 10 . 65

3rd Subnet : 192 . 168 . 10 . 128 to 192 . 168 . 10 . 191 , N/w ID : 192 . 168 . 10 . 128

Usable range : 192 . 168 . 10 . 129 to 192 . 168 . 10 . 190

Gateway : 192 . 168 . 10 . 129



3) Implementing the VLSM technique to optimize the IPv4 address allocations to PCs (belonging to subnets) and interfaces in a given network and analysing the communication between PCs in the network.

LAN with maximum hosts = LAN 1

= 70

$= (1000110)_2$ = 7 bits

∴ subnet generator = $2^7 = 128$

new subnet mask = 11111111 . 11111111 . 11111111 . 10000000 = /25

= 255 . 255 . 255 . 128

IP Range : 192 . 168 . 10 . 0 to 192 . 168 . 10 . 127

usable : 192 . 168 . 10 . 1 to 192 . 168 . 10 . 126

gateway : 192 . 168 . 10 . 1

LAN 2 : 45 hosts = $(101101)_2$ = 6 bits

subnet generator = $2^6 = 64$

New mask = 11111111 . 11111111 . 11111111 . 11000000 = /26

= 255 . 255 . 255 . 192

IP range = 192 . 168 . 10 . 128 to 192 . 168 . 10 . 191

usable : 192 . 168 . 10 . 129 to 192 . 168 . 10 . 190

Gateway = 192 . 168 . 10 . 129

LAN 3 : 17 hosts = $(10001)_2$ = 5 bits

Subnet generator = $2^5 = 32$

New mask = 11111111 . 11111111 . 11111111 . 11100000 = /27

= 255 . 255 . 255 . 224

IP range : 192 . 168 . 10 . 192 to 192 . 168 . 10 . 223

usable : 192 . 168 . 10 . 193 to 192 . 168 . 10 . 222

Gateway : 192 . 168 . 10 . 193

LAN 4 : 6 hosts = $(110)_2$ = 3 bits

Subnet generator = $2^3 = 8$

new mask = 11111111.11111111.11111111.11111000 = /29

= 255.255.255.248

IP range = 192.168.10.224 to 192.168.10.231

usable = 192.168.10.225 to 192.168.10.230

Gateway = 192.168.10.225

5th subnet : router to router

= 2 devices

= $(10)_2$ = 2 bits

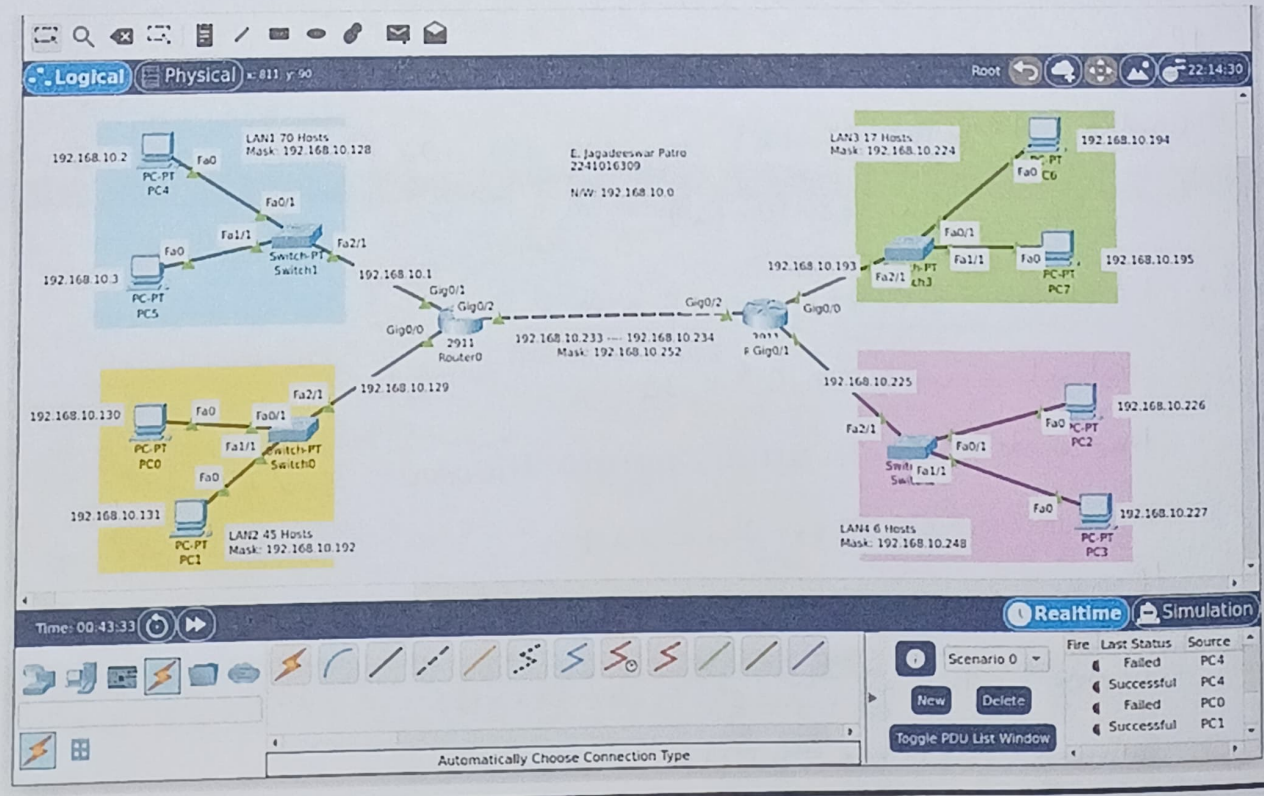
subnet generator = $2^2 = 4$

new mask = 11111111.11111111.11111111.11111100 = /30

= 255.255.255.252

IP range = 192.168.10.232 to 192.168.10.235

Usable = 192.168.10.233 & 192.168.10.234



Conclusion:

Subnetting and VLSM optimize IPv4 address usage and enhance network performance by dividing network and tailoring subnet sizes to host requirements. Using Cisco Packet Tracer these techniques were successfully implemented.

Exercises:

1. Express the following classful IP addresses in CIDR notation:
   a. 192.34.1.9
   b. 10.10.10.1
   c. 129.10.14.15
2. Given the IP address of a device as 192.168.10.126/25. Find the subnet mask and network ID in dotted decimal notation.
3. A network with ID 200.1.2.0 is divided into 3 subnets, find number of hosts per subnet. Also, for all the subnets, find-
   a. Subnet Address
   b. First Host ID
   c. Last Host ID
   d. Broadcast Address
4. Design a network using VLSM for the following requirements with the given network 10.0.0.0/24. Assign IP addresses accordingly: (a) Network A: 60 hosts (b) Network B: 30 hosts (c) Network C: 14 hosts (d) Network D: 6 hosts

Solution:

1) a) 192.34.1.9/24 (class C, 255.255.255.0)

b) 10.10.10.1/8 (class A, 255.0.0.0)

c) 129.10.14.15/16 (class B, 255.255.0.0)

2) Subnet mask: /25 -> 255.255.255.128

Network ID: 192.168.10.0

3) Network ID: 200.1.2.0/24

$24 \rightarrow 2^8 = 256$

=) 256/3 = 35.33, rounding up to nearest power of 2

= 128

~~∴ 128 - 2 = 126 hosts~~ New subnet mask = 255.255.255.192

$2^6 = 64$ hosts

∴ 64 hosts each subnet

Subnet 1: 200.1.2.0

to 200.1.2.63

First host ID = 200.1.2.1

Last host ID = 200.1.2.62

Broadcast address = 200.1.2.63

Subnet 2: 200.1.2.64 to 200.1.2.127

First host ID = 200.1.2.65

Last host ID = 200.1.2.126

Broadcast address = 200.1.2.127

Subnet 3: 200.1.2.128 to 200.1.2.191

First host ID = 200.1.2.129

Last host ID = 200.1.2.190

Broadcast address = 200.1.2.191

Q4) Network: 10.0.0.0/24

original mask = 255.255.255.0

Network with minimum hosts:

⇒ N/w A: 60 hosts = $(111100)_2$ = 6 bits

Subnet generator = $2^6 = 64$

new subnet mask = 11111111.11111111.11111111.11000000 = /26

= 255.255.255.192

IP range = 10.0.0.0 to 10.0.0.63

Unused IPs = 64 - (60 + 2) = 2

=) N/w B : 30 hosts = $(11110)_2$ = 5 bits

Subnet generates = $2^5 = 32$

new subnet mask = 11111111.11111111.11111111.11100000 = /27

= 255.255.255.224

IP Range : 10.0.0.64 to 10.0.0.95

unused = 32 − (30 + 2) = 0

=) N/w C : 14 hosts = $(1110)_2$ = 4 bits

Subnet generates = $2^4 = 16$

new subnet mask = 11111111.11111111.11111111.11110000 = /28

= 255.255.255.240

IP Range : 10.0.0.96 to 10.0.0.111

unused = 16 − (14 + 2) = 0

=) N/w D : 6 hosts = $(110)_2$ = 3 bits

subnet generates = $2^3 = 8$

New mask = 11111111.11111111.11111111.11111000 = /29

= 255.255.255.248

IP Range = 10.0.0.112 to 10.0.0.119

unused = 8 − (6 + 2) = 0

S. Jagadeeswar

Experiment - 7

Aim : Implementation of DHCP, APIPA and analysis of FTP & TELNET packets using Cisco Packet Tracer.

Objectives :-

1) Understanding the use of DHCP and APIPA.

=> Dynamic Host Control Protocal (DHCP) :-

DHCP is a network service that automatically assigns an IP address to the devices (like PCs, printers) when they connect to a network. Instead of manually setting an IP address, DHCP does it automatically.

Ex: when you connect your phone to wifi

connecting a TV to a router.

=> Automatic Private IP Addressing (APIPA) :-

APIPA is a backup system used when a device cannot get an IP address from the DHCP server. If no DHCP server is available, the device assigns itself an IP address from a specific range. This allows local communication with nearby devices but no access to the internet.

Ex: when you connect one laptop to another using Ethernet Cable but there is no DHCP server. Still both laptops assign themselves APIPA addresses to share files directly with each other.

2) An overview on message communication between two end hosts using FTP and TELNET packets.

File Transfer Protocol (FTP) :-

Used to transfer files, uploading / Downloading files between two devices. It requires login, then files are uploaded, downloaded or viewed using respective commands and permissions.

↳ How it works?

- Setting up connection
- Do login
- Upload / Download files
- Close the connection.

Teletype Network (TELNET) :-

It is used to control another computer remotely over a network. Similar to controlling a device using a command line.

↳ How it works?

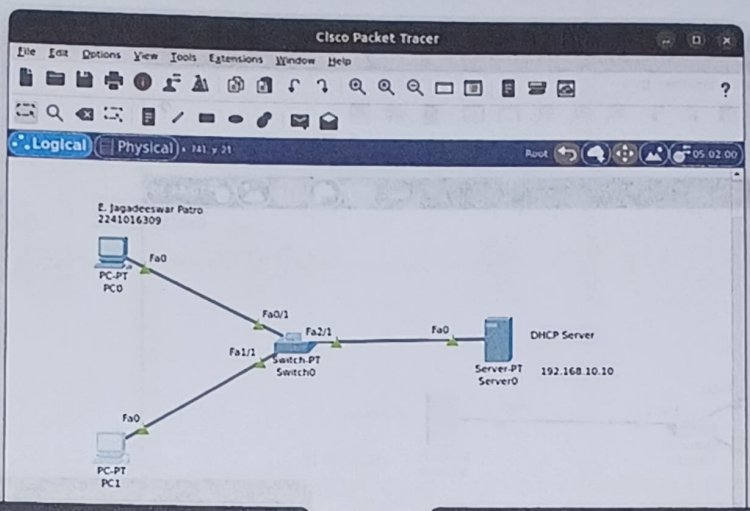
- Connection setup
- Login
- Remote control (commands are sent as packets)
- Closing the connection

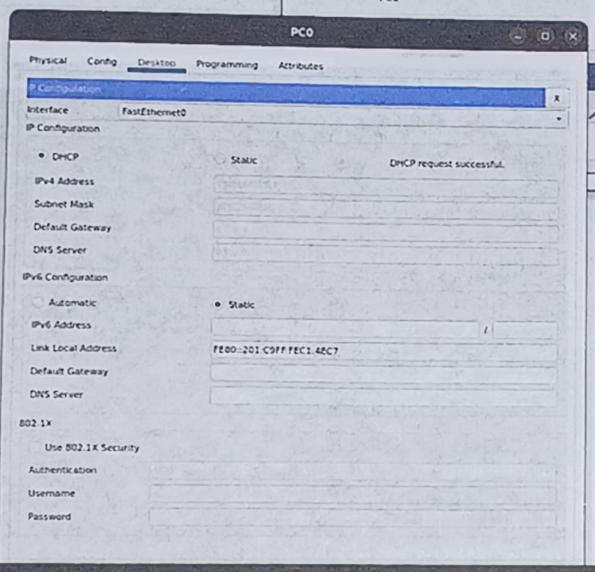
Examples:-

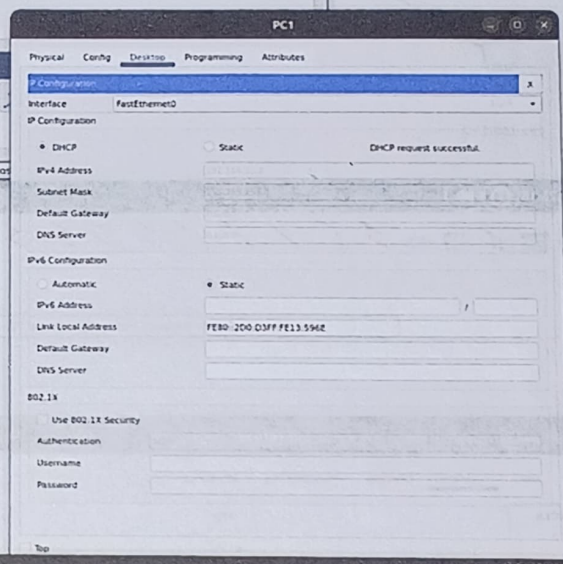
↳ FTP: Uploading a website to web server

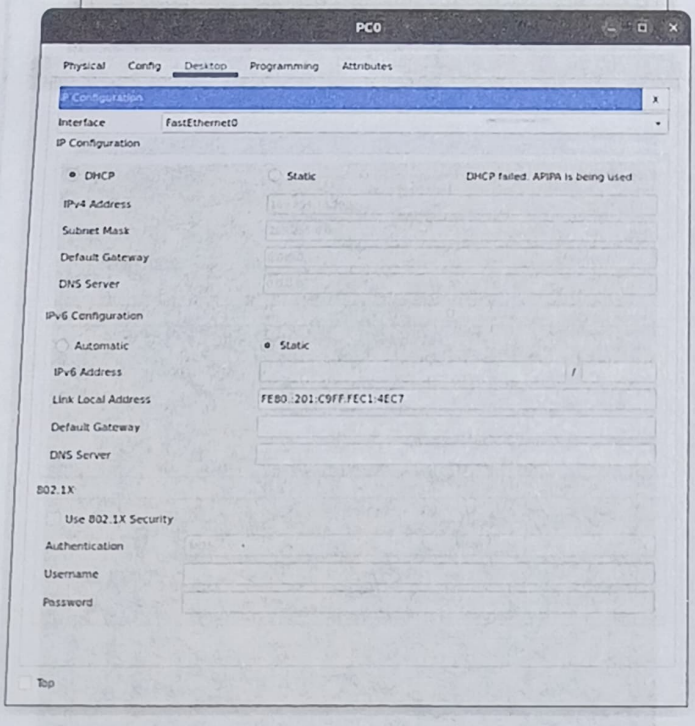
↳ TELNET: Managing a remote Linux server.

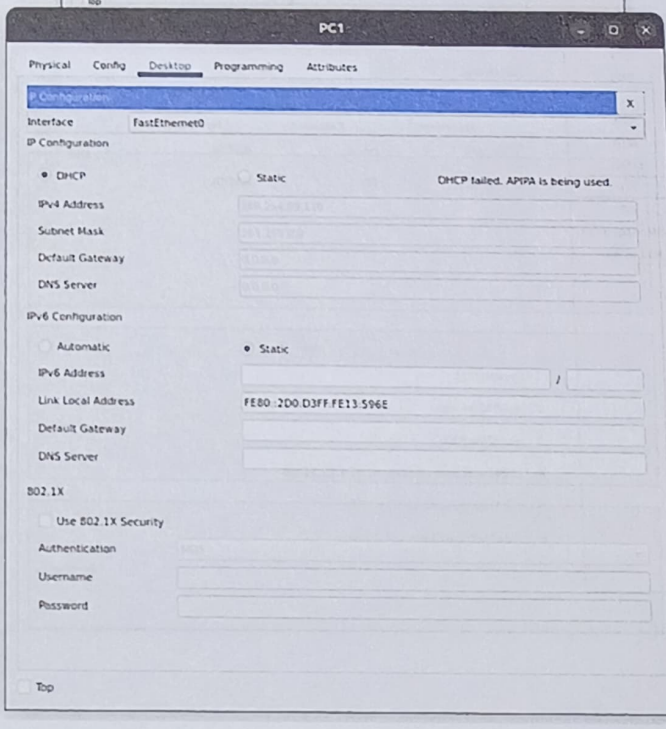
3) Implementing APIPA to generate and verify the IPv4 address for a PC connected to a network.





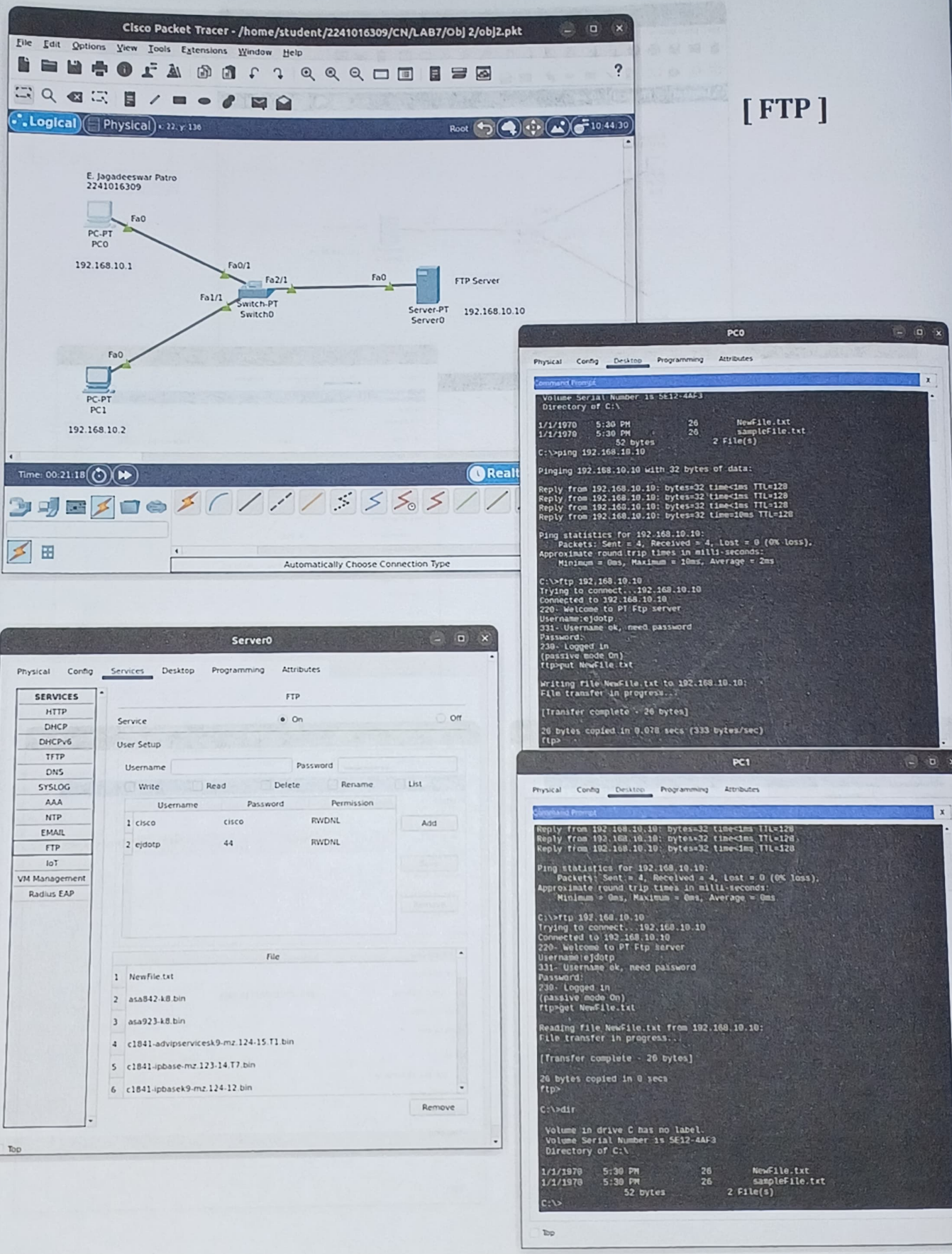


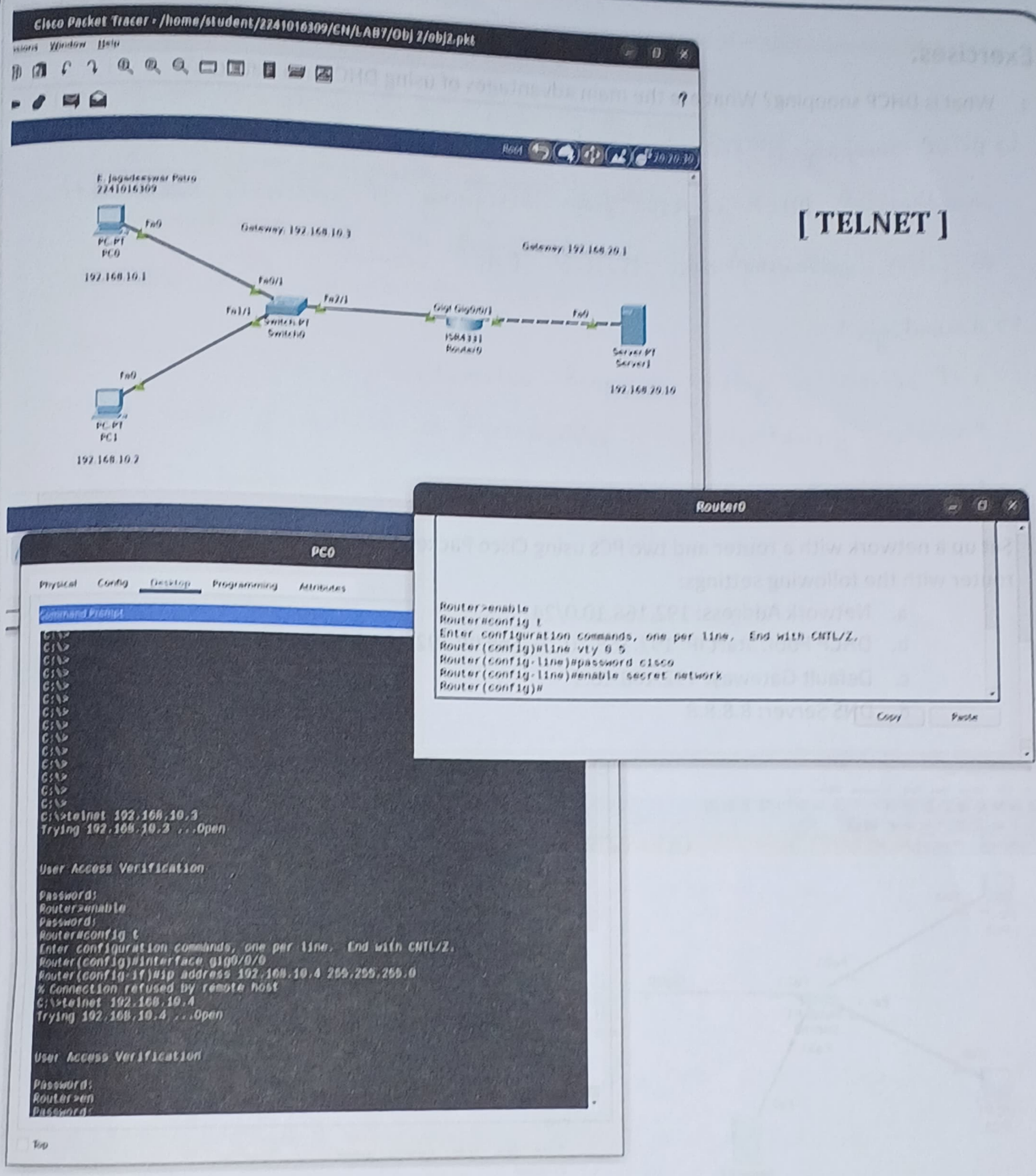




4) Configuring a client - server network and analysing the message communication between them using FTP and TELNET packets

[FTP]





[TELNET]

Conclusion:

The experiment successfully demonstrated DHCP and APIPA configuration, verified IPv4 assignment, and analyzed FTP and TELNET packet communication, enhancing understanding of network protocols and client-server interactions.

Exercises:

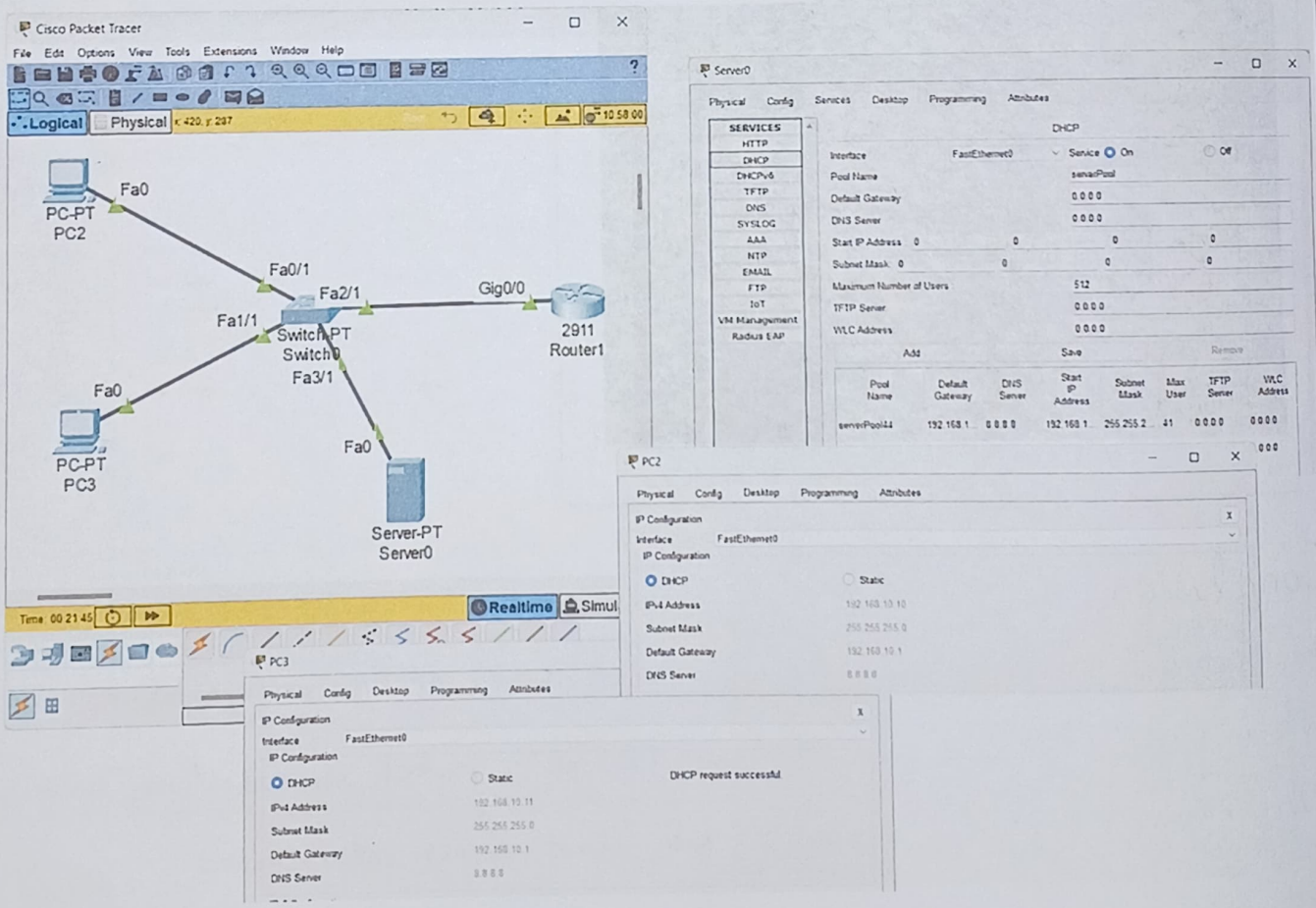
1. What is DHCP snooping? What are the main advantages of using DHCP in a network?

↳ DHCP Snooping is security feature used in networks to prevent unauthorized DHCP servers from assigning IP addresses. It acts as filter, allowing only trusted DHCP servers.

↳ Advantages:

- IP address is getting assigned automatically
- ensures efficient use of IP address.
- Scalability

2. Set up a network with a router and two PCs using Cisco Packet Tracer. Configure DHCP on the router with the following settings:
   a. Network Address: 192.168.10.0/24
   b. DHCP Pool: Start IP: 192.168.10.10, End IP: 192.168.10.50
   c. Default Gateway: 192.168.10.1
   d. DNS Server: 8.8.8.8



Name: E. Jagadeeswar Patro Regd. Number: 2241016309

3. State the use of APIPA highlighting its advantages. What is the range of IP addresses for APIPA? Write the APIA address generated for your device in this experiment.

↳ Uses of APIPA: it is used when a device cannot get an IP address from a DHCP server. It assigns an IP address automatically, enabling devices to communicate within the same local network.

↳ Advantages:

- No need of manual configuration of IP addresses.
- Allows devices to communicate on the same network, even if DHCP is unavailable. Provides backup if DHCP fails.

4. Compare FTP and TELNET protocols in terms of functionality and security.

↳ Connection Type:

FTP uses port 21 & 20 whereas TELNET uses port 23.

↳ Data Transfer:

FTP ~~was~~ transfers files, dictionaries whereas TELNET transfers text based commands & outputs.

↳ Usage:

FTP is commonly used to upload & download files whereas TELNET is used to remotely control/manage networks.

5. Mention true/false.
   a. FTP uses two TCP connections. (True)
   b. FTP sends exactly one file over the data connection (False)
   c. FTP server is stateless (False)
   d. Telnet is a general-purpose client-server program (True)
   e. Telnet can be used for file transfer (False)
   f. Telnet is used to establish a connection to TCP port number 23. (True)