Aim of the experiment: Study on network elements, IP address, Subnet mask, and network Simulators)

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

Theory :-

a.) Switch :- It connects multiple devices on a network by receiving data and using filtering and forwarding to send the data to the intended destination device

b.) Hub :- A device that extends the reach of a network by regenerating the electrical signal. It also receives data on one port and then sends it out to all other active ports

c.) Router :- A network layer device that forwards data packets between networks. It interconnects two or more computer networks, and selectively interchanges packets of data between them.

d.) Bridge :- It is a network device that connects multiple subnetworks to create a signal network. It provides interconnection with other computer networks that use the same protocol.

e.) Repeater :- A device that regenerates weak signals to extend the distance a signal can travel.

f.) Access point :- It is a networking device that connects wireless devices to a wired network.

Objective 2 :→ An overview on different classes of IP addressing Subnet mask, and gate way.

Theory :-

⇒ **IP address** :- A unique 32-bit address used to identify devices on a network.

Classes of IP addressing :-

→ **Class A** :- Supports 16 million hosts on each of 127 networks
Address Range :- 1.0.0.1 to 126.255.255.254

→ **Class B** :- Supports 65,000 hosts on each of 16,000 networks
Address Range :- 128.1.0.1 to 191.255.255.254

→ **Class C** :- Supports 254 hosts on each of 2 million networks
Address Range :- 192.0.1.1 to 223.255.254.254

→ **Class D** :- Reserved for multicast groups.
Address Range :- 224.0.0.0 to 239.255.255.255

→ **Class E** :- Reserved for Experimental purposes
Address Range :- 240.0.0.0 to 254.255.255.254

⇒ **Subnet mask** :- It is a 32 bit binary number that separates an IP address into two parts: the network and the host

→ **Default Subnet Mask** :-
Class A :- 255.0.0.0 **Class C** :- 255.255.255.0
Class B :- 255.255.0.0

⇒ **Gateway :-** It is a device on node that connects disparate networks by translating communications from one protocol to another.

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

Theory :-

1.) CPT is a crossplatform visual simulation Tool that allows users to create network topologies and simulate modern computer networks

2.) This tools provides a network simulation to pratice simple and complex networks

3.) It helps user to create a network with an almost unlimited no. of network devices, encouraging practice, discovery and troubleshooting.

Objective 4 :-→ Making connection between two host PCs (end devices) and analysing the communication using ping command.

Theory :-

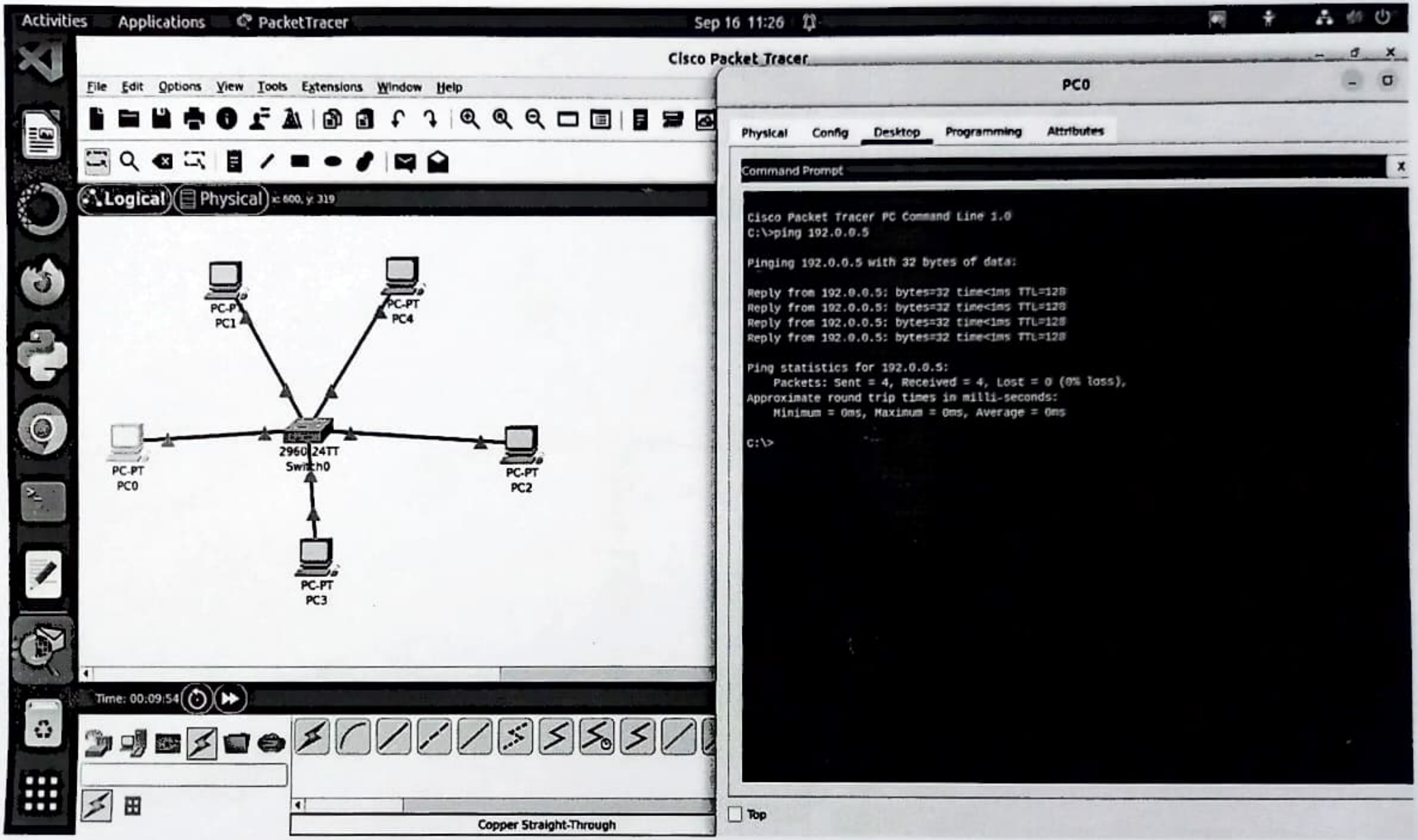
Ping :- The ping command is a network utility used to test the connectivity between two devices on a network. It helps to determine whether a particular host is reachable and measures the round-trip time of the messages.

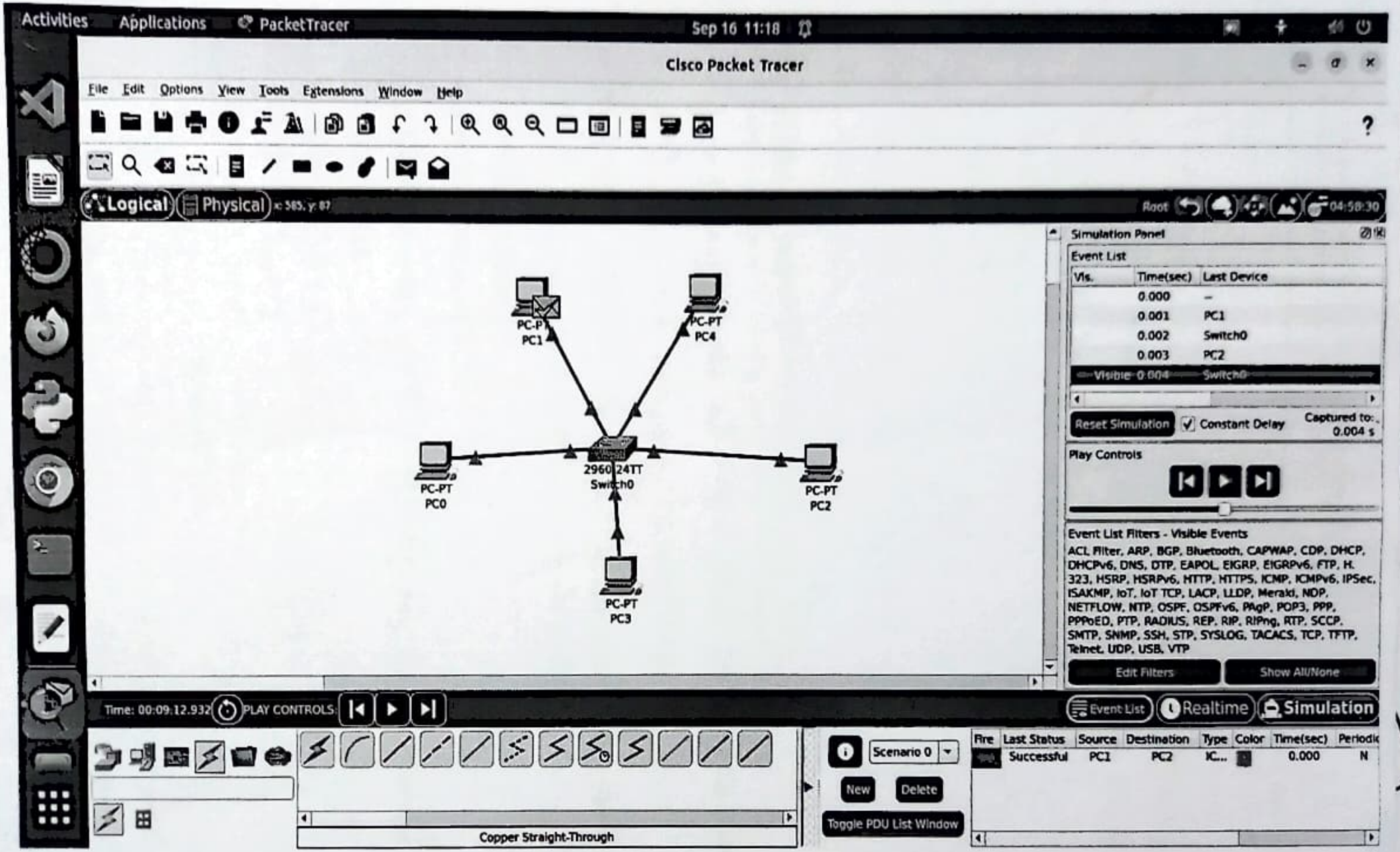
Example :- Ping 192.0.0.5

The output includes i) the no. of bytes sent to the destination IP address with TTL (Time to live), which shows the no. of hops the packet has taken to reach its destination ~~and how of~~

2.) The no. of packets sent and received with percentage of packet loss. If Packet sent and received successfully then there is 0% of Packet loss.
3.) Approximate round trip times in milli-seconds.

Observations :-


Activities
Applications
PacketTracer
Sep 16 11:26
Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical
Physical
x: 600, y: 319
PC-PT PC1
PC-PT PC4
PC-PT PC0
2960-24TT Switch0
PC-PT PC2
PC-PT PC3
Time: 00:09:54
Copper Straight-Through
PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.0.0.5
Pinging 192.0.0.5 with 32 bytes of data:
Reply from 192.0.0.5: bytes=32 time<1ms TTL=128
Reply from 192.0.0.5: bytes=32 time<1ms TTL=128
Reply from 192.0.0.5: bytes=32 time<1ms TTL=128
Reply from 192.0.0.5: bytes=32 time<1ms TTL=128
Ping statistics for 192.0.0.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top


Activities
Applications
PacketTracer
Sep 16 11:18
Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical
Physical
Root
PC-PT PC1
PC-PT PC4
PC-PT PC0
2960-24TT Switch0
PC-PT PC2
PC-PT PC3
Simulation Panel
Event List
Vis. Time(sec) Last Device
0.000 –
0.001 PC1
0.002 Switch0
0.003 PC2
Visible 0.004 Switch0
Reset Simulation
Constant Delay
Captured to: 0.004 s
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
Time: 00:09:12.932
PLAY CONTROLS
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic
Successful PC1 PC2 IC... 0.000 N
Copper Straight-Through

Analysis:-

In this Experiment, a simple network was designed using Cisco Packet Tracer, consisting of five PCs connected through a Switch. The PCs have the following Ip addresses:

→ PC0: 192.0.0.5
→ PC1: 192.0.0.4
→ PC2: 192.0.0.3
→ PC3: 192.0.0.2
→ PC4: 192.0.0.1

1) Ping test between PC3 and PC1:

⇒ A ping test was conducted from PC3 to PC1 (IP: 192.0.0.4) to check network connectivity.

⇒ The ping test results, displayed in the command prompt on PC3, show successful communication:

→ Packets sent: 4
→ Packets received: 4
→ NO packet loss (0% loss), indicating reliable communication

⇒ Round-trip times:

→ minimum: 0ms
→ maximum: 3ms
→ Average: 0ms

2.) Packet Transmission Analysis :-

⇒ The packet is successfully routed through the Switch in the Simulation mode. It confirms the successful Exchange between PC1 and PC3

Conclusions :-

The network simulation in Cisco Packet Tracer was successful in demonstrating connectivity and packet forwarding between PCs through a switch. The use of ping command that all devices could communicate within the same subnet without any pack loss.

Exercises:-

1.) Differentiate layer 2 & layer 3 switches.

Ans → Layer 2 switches operate at the Data link layer and use MAC addresses for forwarding.

→ Layer 3 switches operate at the network layer and forward traffic using IP addresses

2.) Compare and constrast IPv4 and IPv6 addresses. What are the default subnet mask for class A, class B and class C IP addresses?

Ans → IPv4:- Address length :- 32 bit, written in decimal

→ IPv6:- Address Length:- 128 bit, written in Hexadecimal

→ Default Subnet Masks:-

class A :- 255.0.0.0
class B :- 255.255.0.0
class C :- 255.255.255.0

3.) Which of the ~~following~~ classes does the following IP address belong to?

a.) 10.10.10.1 – Class A

b.) 172.16.4.3 – class B

c.) 192.168.1.20 - Class C

4.) What are the key features of Cisco Packet Tracer?

Ans → Simulation of both simple and complex networks
→ Offers both physical and logical views of network design
→ Supports various Cisco devices for configuration
→ Allow real-time and simulation modes.

5.) Explain the two workspaces and two modes of operation in packet Tracer.

Ans i) Workspaces:-

→ Logical workspace:- It shows the logical network topology that is built by the user. It displays the connecting, placing and clustering of virtual network devices.

→ Physical workspace:- We can see the physical implementation of the logical network.

ii) Modes:-

→ Real time modes:- The network behaves like real devices, with immediate responses to all network activities.

Name: Rit Manichandan Regd. Number: 2241008005

→ Simulation mode :- The network 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.

Experiment - 9

Aim :-

Implementation of basic Ethernet using Cisco packet Tracer to understand and make IP, TCP and UDP header analysis.

Objective - 1

An overview on headers (i.e Ethernet, IP, TCP and UDP), ICMP. FTP and TFTP.

Ethernet :-

→ A widely used technology for called Local Area networks.
→ Uses frames to encapsulate data, containing MAC addresses for source and destination.
→ Supports Speed 10 MBPS to 100 GBPS.

IP :-

→ Internet protocol responsible for addressing and routing packets of data across networks.
→ It's basically two types. IPV4 (32-bit address)
IPV6 (128-bit address)

TCP :-

→ TCP Stands for Transmission Control Protocol.
→ TCP ensures reliable, ordered and errors checked delivery of data between applications.

UDP :-

→ UDP Stands for User Datagram protocol.
→ The purpose of UDP to allows low-latency, connectionless communication.
→ Common uses of UDP is Streaming media and online gaming.

ICMP :-

→ ICMP stands for Internet Control Message protocol.
→ operates at the network layer, primarily for control messages.
→ Used for Troubleshooting and monitoring network connectivity.

FTP :-

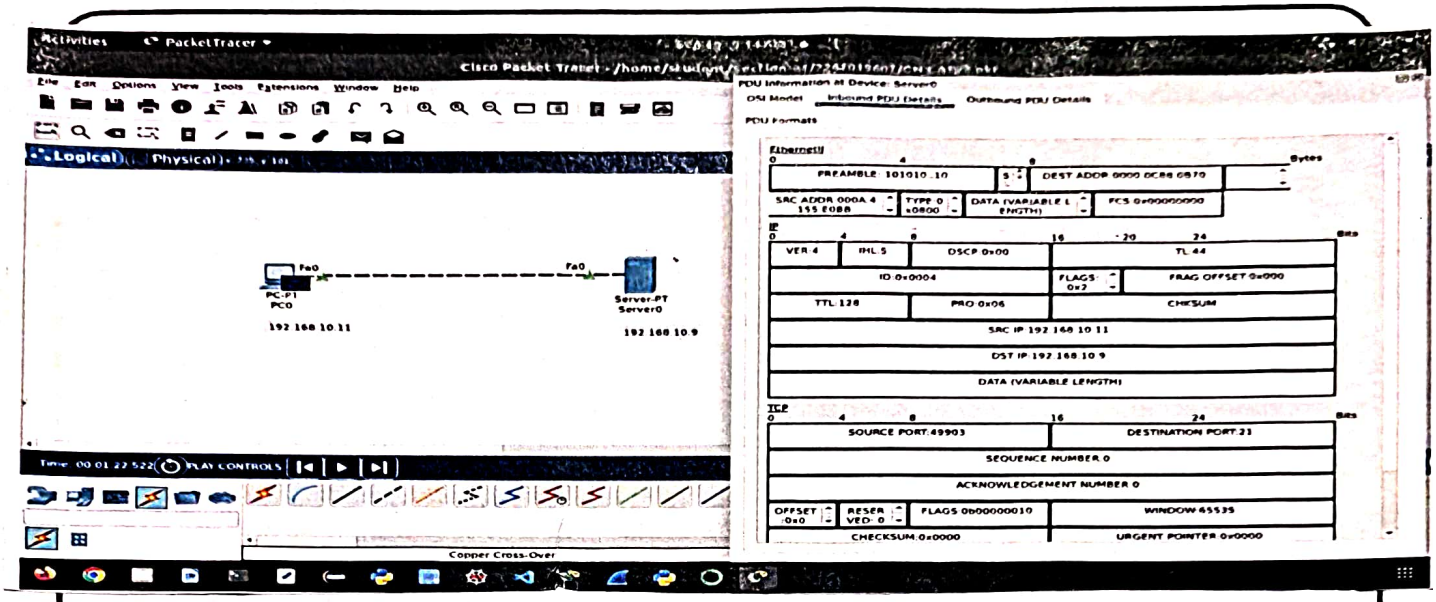
→ FTP stands for File Transfer protocol.
→ Supports authentication and can operate in active or passive modes.
→ Uses for uploading and downloading files from web servers.

TFTP :-

→ TFTP stands for Trivial File Transfer protocol.
→ Purpose is a simple version of FTP for transferring files with minimal overhead.
→ common uses booting devices over a network and transferring firmwares or configuration files.

Observation - 9

Configuration of an ethernet using the network devices in Cisco packet Tracer.



Objective-3 :-

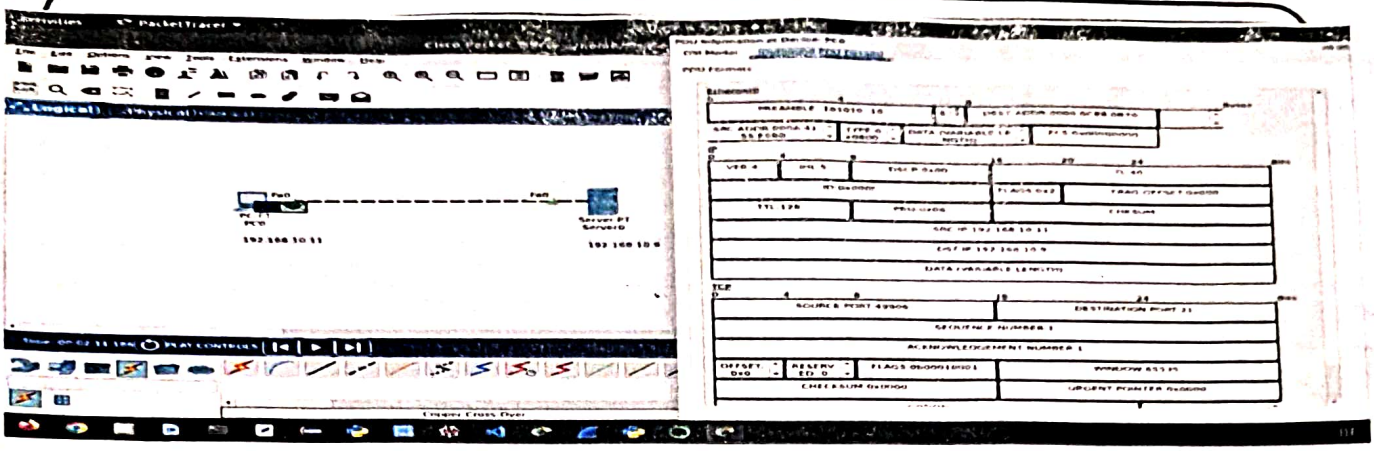
Simulating the Ethernet by transmitting ICMP, FTP and TFTP messages between two end devices.

→ ICMP stands for Internet Control Message protocol is primarily used for network diagnostics and error reporting.

→ FTP stands for File Transfer protocol used to transfer files between a client and a server over a TCP/IP network.

→ TFTP stands for Trivial File Transfer protocol is a simplified version of FTP, designed for transferring files without authentications.

→ Configuring ethernet using cisco packet Tracer allows users to simulate a real world networking environment by transmitting ICMP, FTP and TFTP messages between end device.



Objective - 4

Understanding and analysing different fields of IP, TCP and UDP headers after simulations.

After simulating data transmission using these protocols,

→ Packet Inspection: Use packet tracers simulation mode or connect to capture packets. This allows you to view the headers in real time.

→ For IP headers, check the source and destination IP addresses to verify routing and connectivity.

→ For TCP headers, analyze the sequence and acknowledgement numbers to understand the flow of data and ensure reliable delivery.

→ For protocol identification use the protocol field in the IP header to determine if the data using TCP or UDP, which impacts how data is managed and transmitted.

→ This knowledge is foundational for anyone working in networking and network administration.

Conclusion :-

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

Exercise

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

Ans Given that, IP header = 100

the offset is measured in 8-byte blocks.

So, Bytes = 100 x 8 = 800 bytes.

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

Ans Given, IP packets: 0100 0010

Here, the first 4 bits represent the corresponds to version 4 (0100) that IP version IPv4.

→ Fore header length: 0010 represent the header length in 32-bit words.

0010 = 2

Header Length = 2 x 4 = 8 bytes.

3. A TCP header in hexadecimal format is given as below.
0532 0017 00000001 00000000 5002 07FF
00000000.

(a) What is the source port number?

The First 16-bits (4-hexadecimal) digits are,

$0532 = 2 \times 16^0 + 3 \times 16^1 + 5 \times 16^2 + 0 \times 16^3$

$= 2 + 48 + 1280$

$= 1330$

(b) What is the destination port number?

Here, next 16-bits are,

$0017 = 7 \times 16^0 + 1 \times 16^1 + 0 \times 16^2 + 0 \times 16^3$

$= 7 + 16 + 0 + 0$

$= 23$

(c) What is the Length of the header?

Here, Header = 5002

1st hex digit = 5 = (0101)

Header length = $5 \times 4 = 20$ bytes.

(d) What is the window size?

Window size found in the next 16-bits after header length.

$07FF = F \times 16^0 + F \times 16^1 + 7 \times 16^2 + 0 \times 16^3$

$= 15 \times 16^0 + 15 \times 16 + 7 \times 256 + 0$

$= 15 + 240 + 1792$

$= 2047$

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

(a) Source port number?

The 1st 16 bit digit are: 06 32

$0632 = 2 \times 16^0 + 3 \times 16^1 + 6 \times 16^2 + 0$

$= 2 + 48 + 1536$

$= 1586$

(b) Destination port number?

Next 16-bit after source port are: 000D

$000D = D \times 16^0 + 0 + 0 + 0$

$= 13 \times 1$

$= 13$

(c) Length of User Datagram?

The next 16-bites are 001C.

$001C = C \times 16^0 + 1 \times 16^1 + 0 + 0$

$= 12 + 16$

$= 28$

(d) Length of the data.

Length of data = Total Length - Header Length

For UDP header length = 8 bytes.

Total length of UDP = 28 bytes.

So, Length of data = 28 bytes - 8 bytes

= 20 bytes.

EXPERIMENT 3

AIM :-
Implementation of network topologies using Cisco Packet Tracer

OBJECTIVE 1 : An overview on network topologies

- Star topology : In this topology, all the devices are connected to a single hub/switch through a cable. This hub/switch is the central node and all other node are connected to the central node.
- Bus topology : It is a network type in which every computer and network devices is connected to a single cable. This is a bidirectional topology.
- Ring topology : In a ring topology, it forms a ring connecting devices with exactly two neighbouring devices. A no. of repeate are used for ring topology with a large no. of nodes, because if someone wants to send some data to the last node in a ring topology with 100 nodes, then data has to pass through 99 nodes to reach the 100th node.
- Mesh topology : Every device on this topology is connected to every other devices on the ~~Internet~~ network. This is like a hive connection. The total no. of connections that can be set-up between devices ~~in~~ is given by the formula a $n(n-1)/2$.

OBJECTIVE 2 : Constructing and simulating a network based on star topology to analyse performance scalability and fault tolerance.

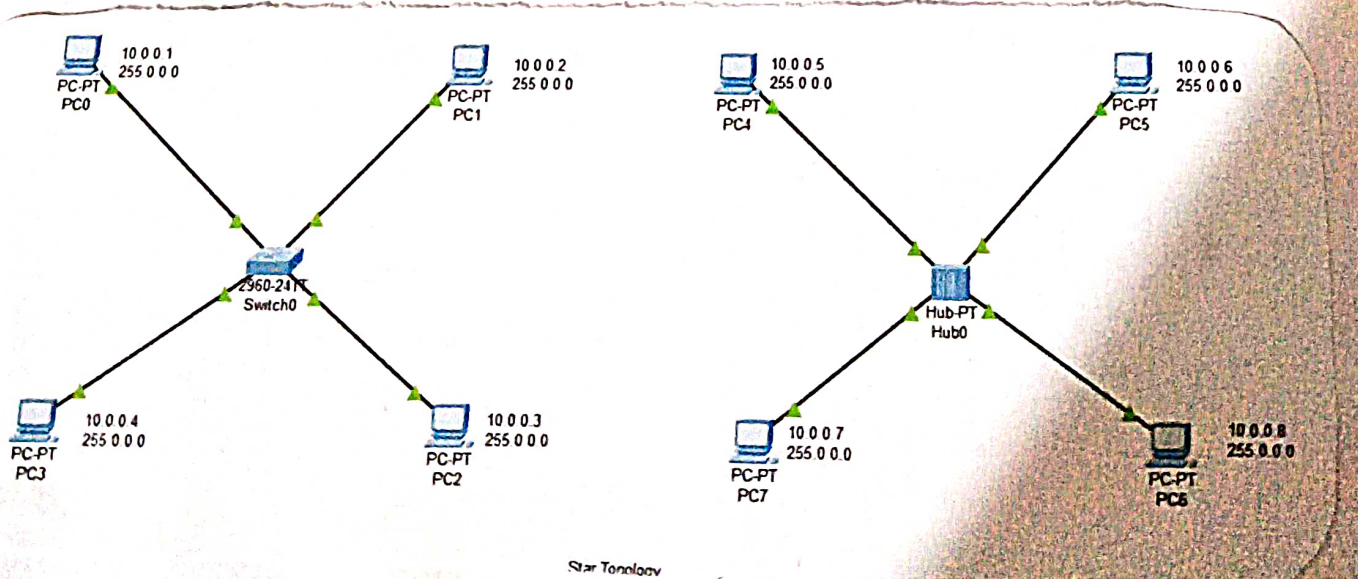


Fig : construction

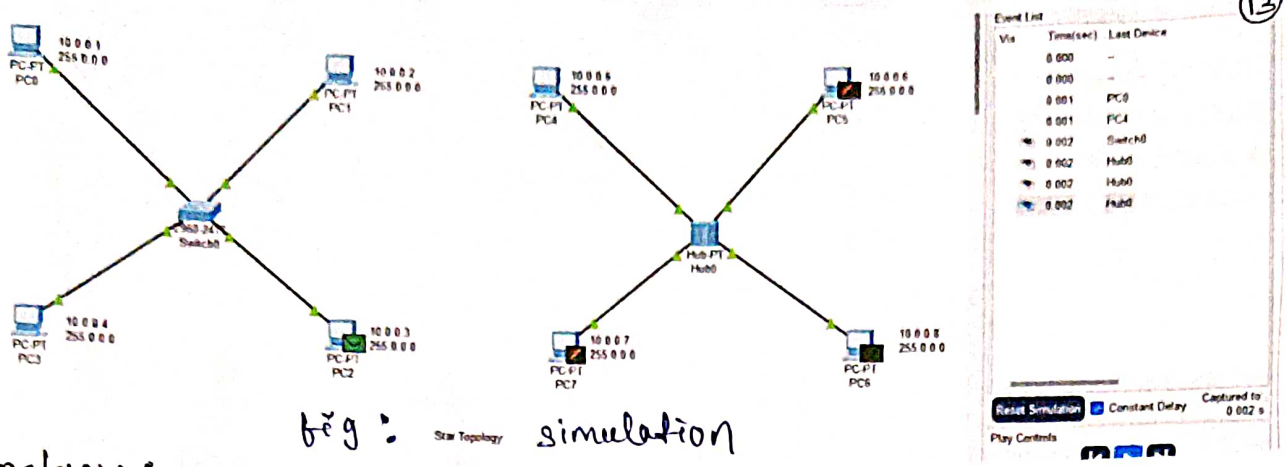


fig: Star Topology simulation

Analysis:

- Performance: With a central switch, data is quickly routed to connect device.
- Scalability: easily scalable by adding more devices to the switch.
- Fault tolerance: If one PC's connection fails, the rest of the network remain operational.

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

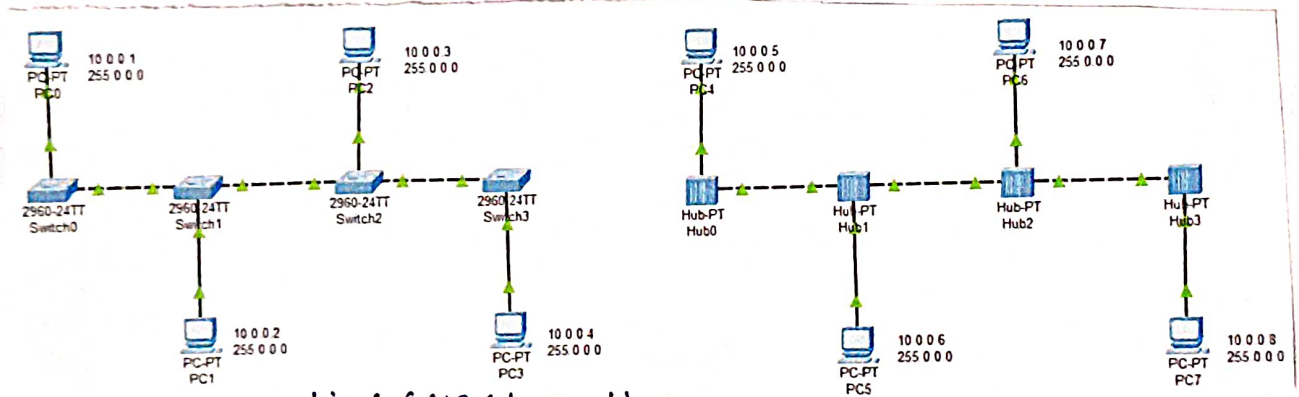


fig: construction

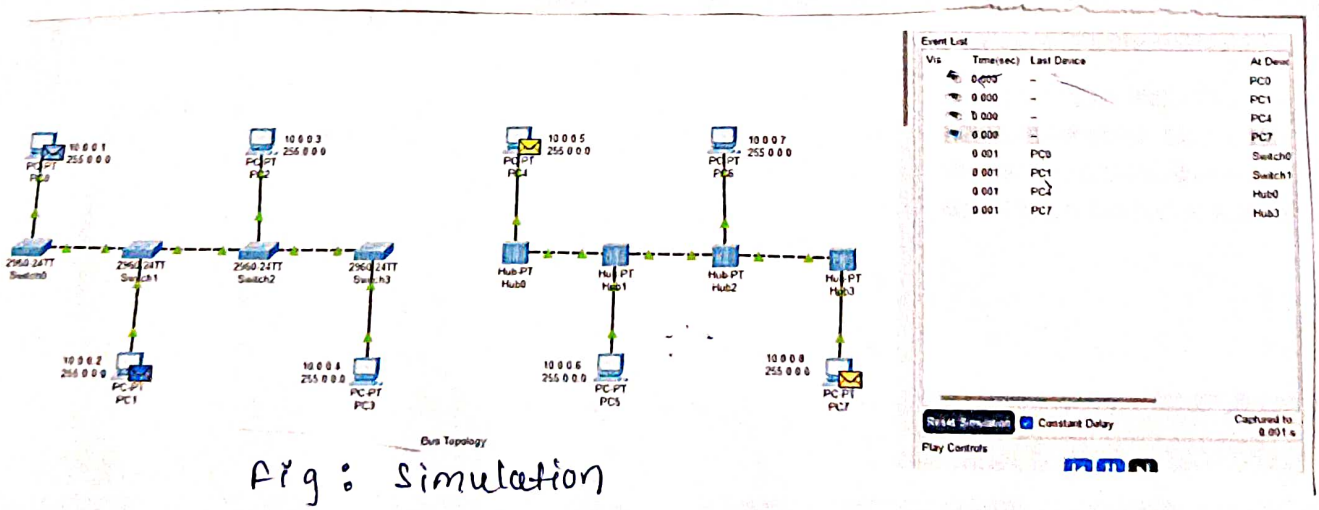


Fig: simulation

Analysis:

- Performance: As more PCs are added, performance decreases since all the devices share the same communication line
- Scalability: has limited scalability due to signal degradation.
- Fault tolerance: Failure in backbone cable can cause network failure

OBJECTIVE 4: Constructing and simulating a network based on ring topology to analyze the performance scalability and fault tolerance. (14)

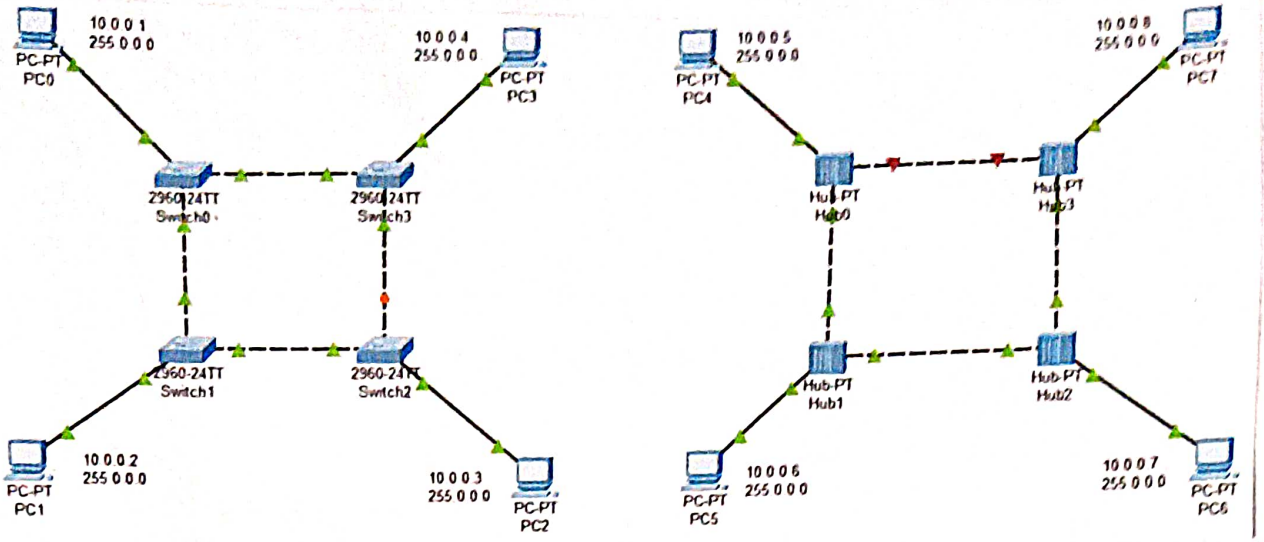


fig: construction

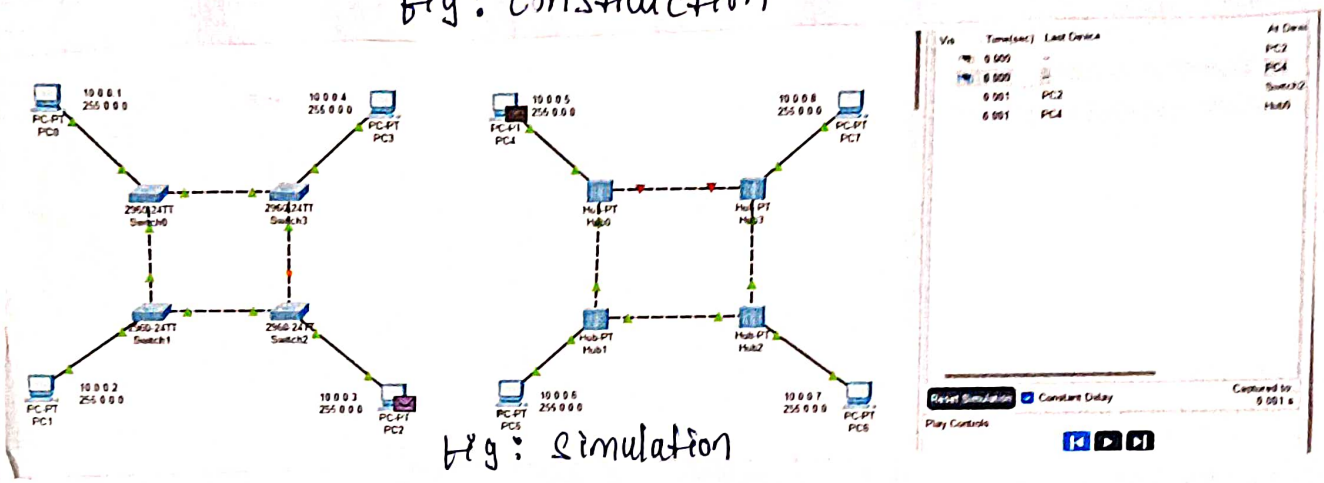


fig: simulation

Analysis :-

- Performance : data travels through each node, so performance can slow down in large rings.
- Scalability : Adding new devices require the network to be broken re connected.
- Fault tolerance : failure of one link disrupts the entire network unless ~~a~~ dual network rings are used.

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

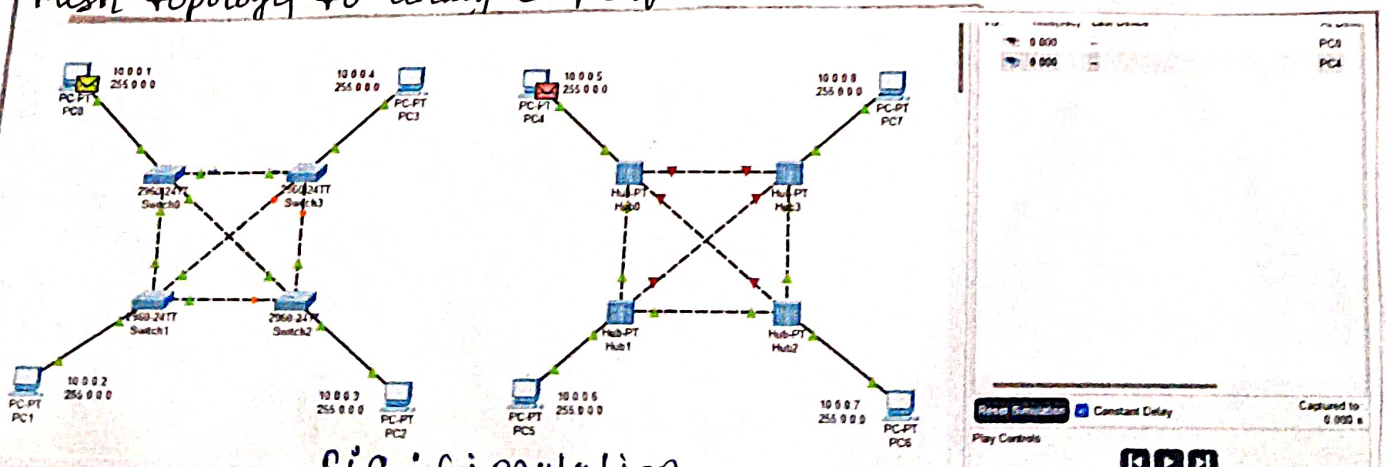


fig : simulation

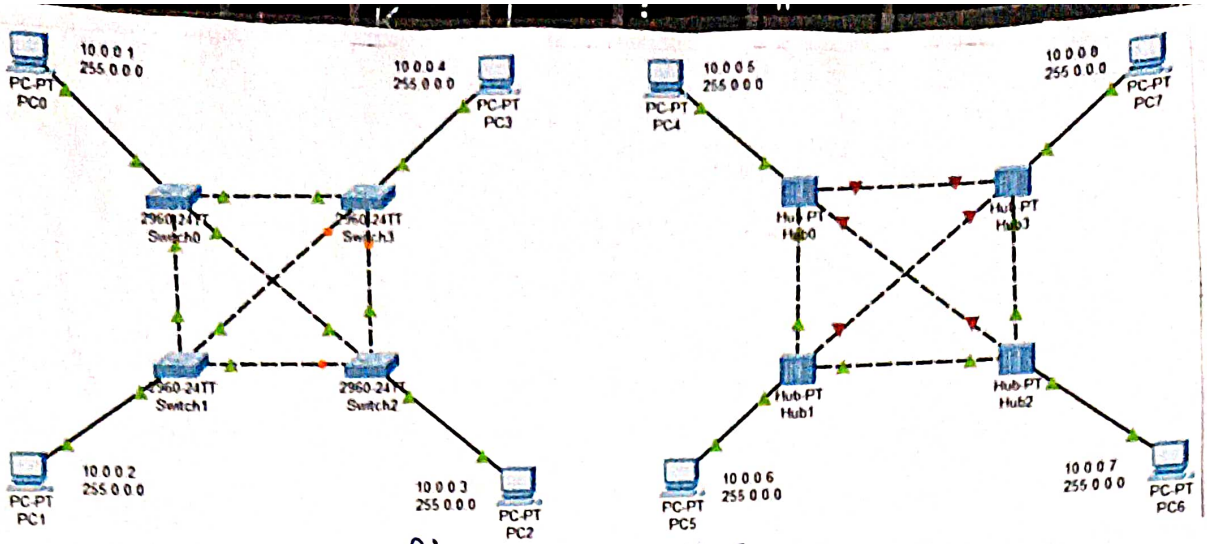


Fig: construction

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.

EXERCISES :-

1. Differentiate physical and 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 and disadvantages of bus, ring, star and mesh topologies.

Topology	Advantages	Disadvantages
Bus	Easy to install, requires less cable	Limited devices, hard to troubleshoot, performance drops with more devices
Ring	simple data flow, predictable 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 tolerance	expensive, complex installation, difficult to scale

3. Briefly explain various factors for selecting a proper network topology. (16)

Factors are:

- Cost: budget constraints may limit the choice of topology
- Scalability: some topologies like star or mesh are more scalable thus more preferred than bus or ring.
- Performance: networks requires high throughput and low latency may benefit from star and mesh.
- Fault Tolerance: Mesh topology offers high fault tolerance, while bus and ring are vulnerable to single points of failure.
- Ease of maintenance: Star is easier to maintain the ring or mesh tplgy

4. For 5 devices in a network, what is the number of cables links required 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: one backbone link shared by all end devices

Star: n links; one per device to central switch

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

Submitted By:-

Annanya Devi

22410042224

Sec 6

27/9/24

Assignment - 4

Aim :- Implementation and understanding of the use of IPV4 adressing, NAT with CISCO packet tracer.

Objective_1 :- An overview of IPV4 adressing (Public, Private Classful) and NAT (Network Address Translation).

IPV4 is the 4th version of the internet protocol (IP), providing a system for identifying devices on a network using a 32-bit adress space.

→ Public IPV4 adress :-
-) globally unique & can be routed on the internet.
-) Assigned by IANA.
-) Example : 8.8.8.8 (google DNS)

→ Private IPV4 adress :-
-) used for communication within a private network.
-) not routable on internet & must use NAT to access external networks.
-) these adresses allow devices in a local network to communicate with each other using public IP adress.

→ Classful IPV4 adress :-
-) IPV4 adresses are initially classified into 5 classes (A, B, C, D, E), based on the number of network & hosts supported.

→ Adress Translation (NAT) :-
-) A method that allows multiple devices on a local network to share single IP (public) for accessing

Name _____ Regd. Number: _____

the internet.

•) There are 3 types of NAT :-

i) static NAT → maps a single private IP adress to a single public IP adress.

ii) Dynamic NAT → maps multiple private IP adresses to a single public IP adress from a pool • on FCFS basis.

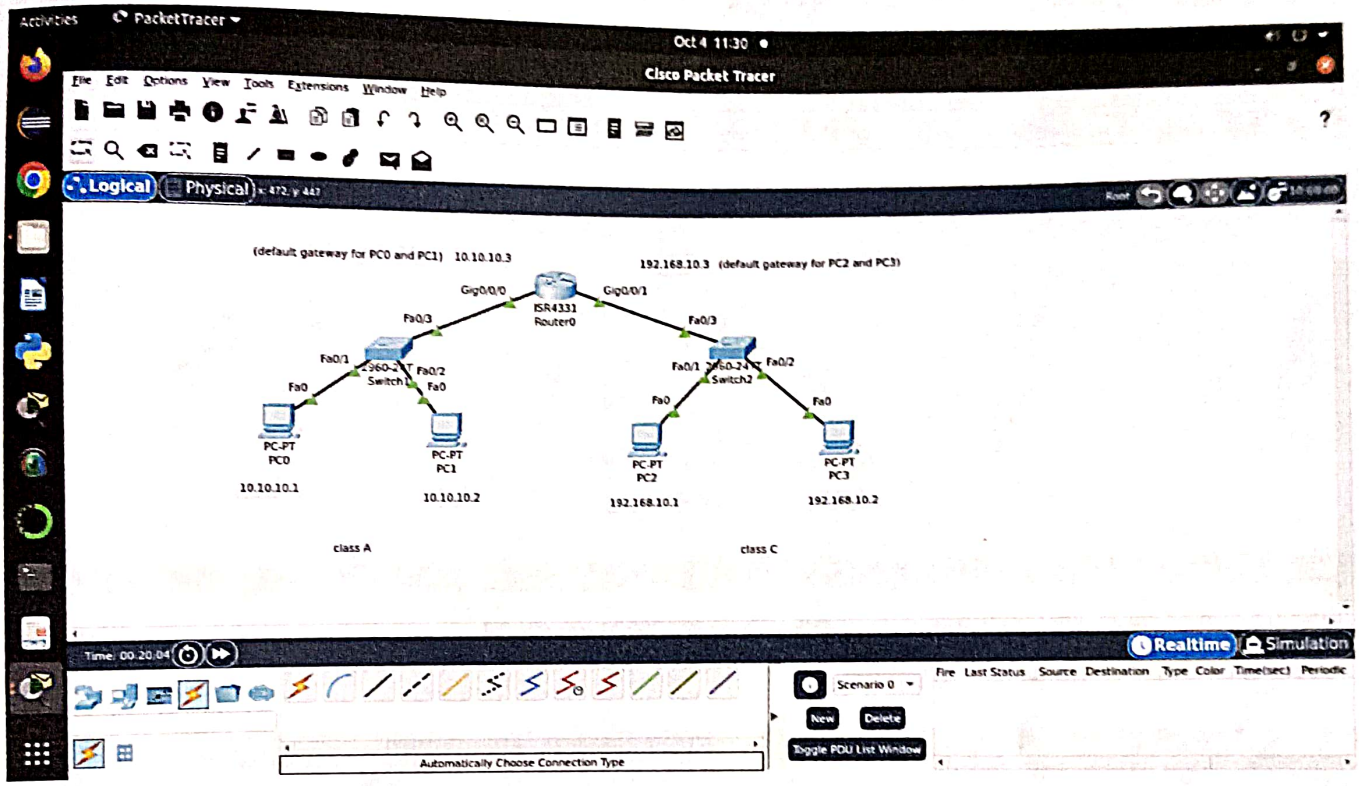
iii) Post adress translation (PAT) → maps private IP adresses to a single public adress by using different ports.
aka (NAT Overloading)

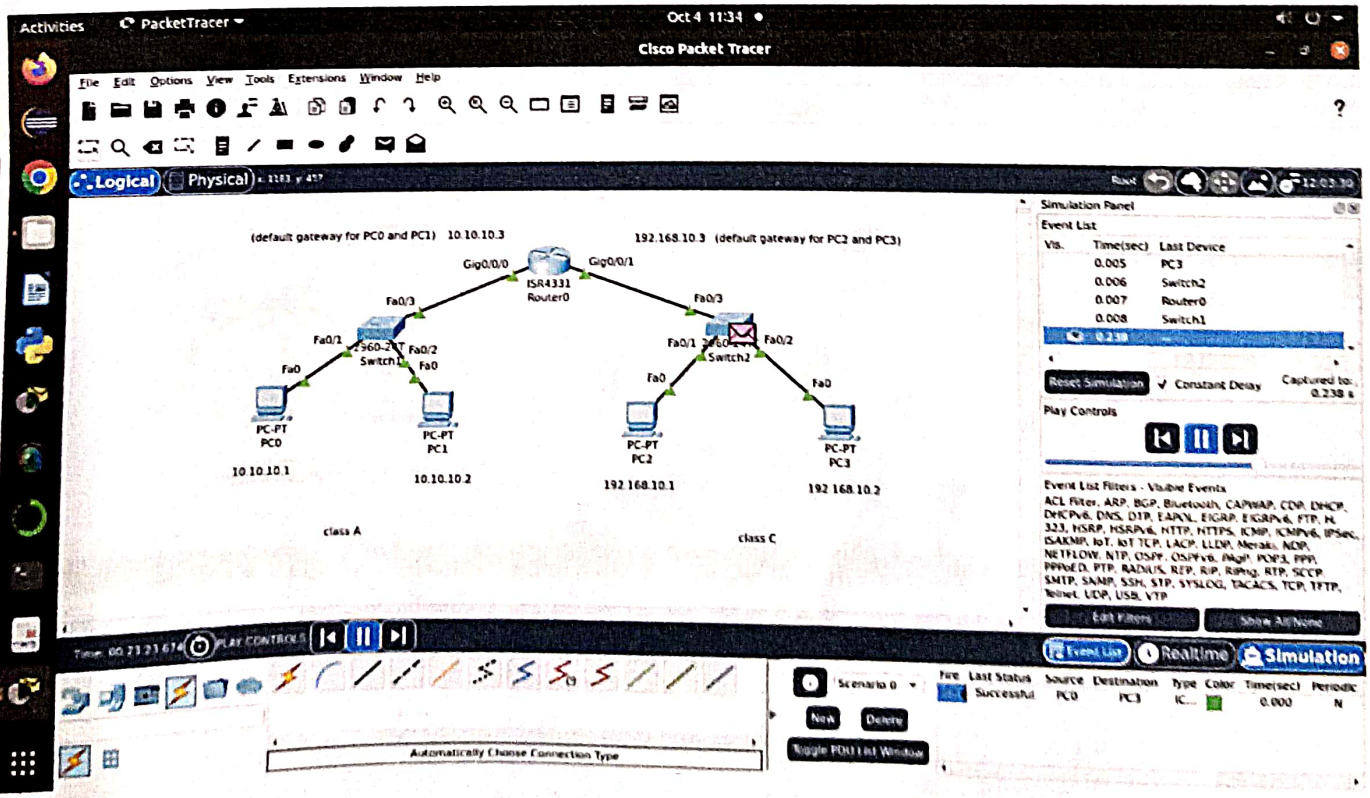
Objective-2 :- Constructing & analysing the communication between 2 networks (of different classes).

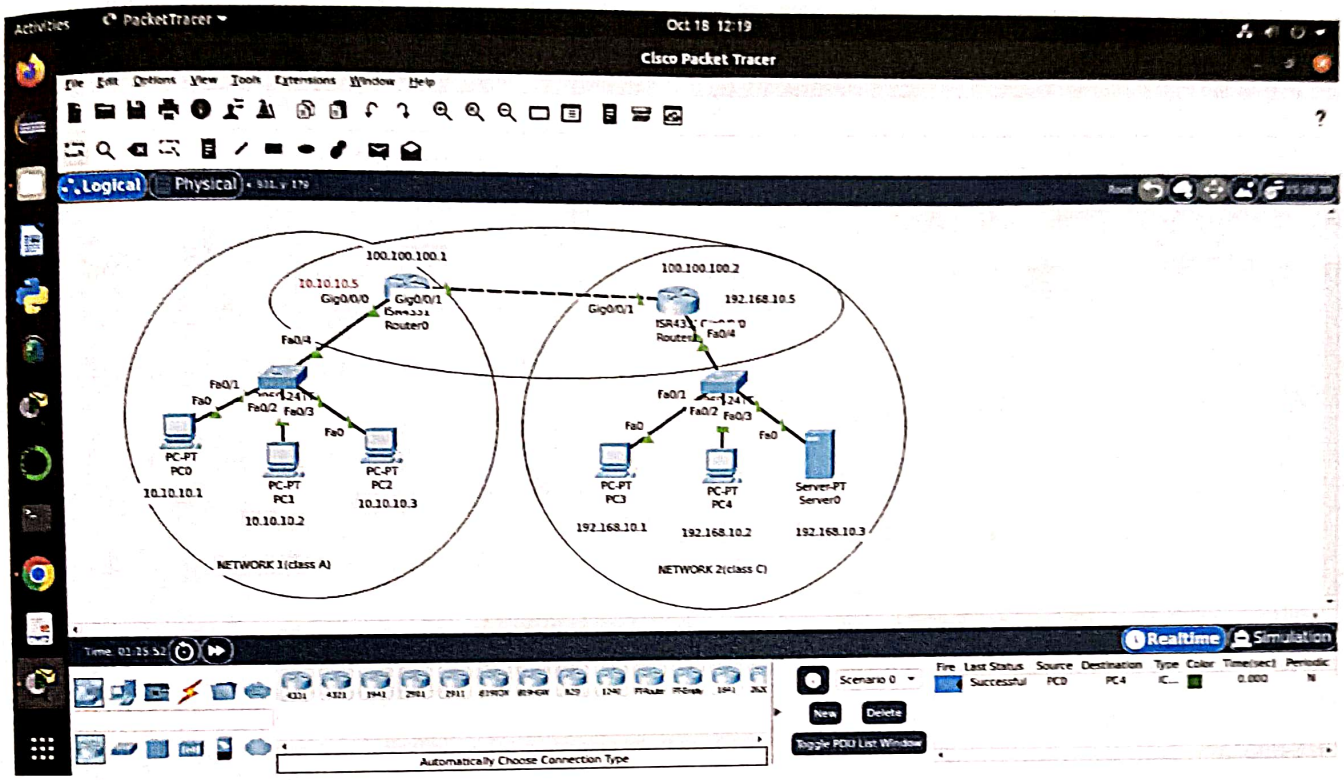
Constructing 2 networks, one with class A & other with class C IP adress & communicate via default gateway 120.10.10.3

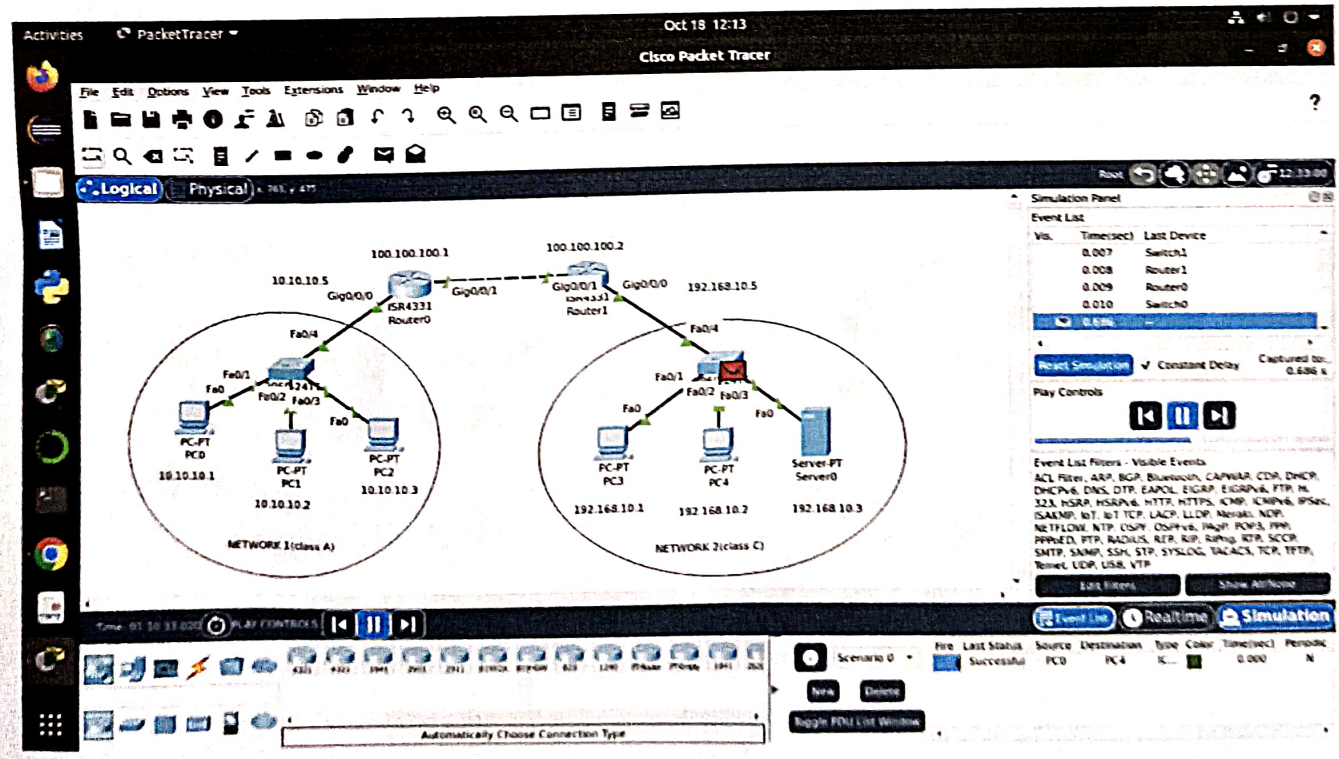
Objective-3 :- Configuring & implementing NAT using a router to analyse the communication between PC's (in a private network) of a public server.

Configuring 2 networks having class A & class C IP adress & communicating them using router.


Activities
PacketTracer
Oct 4 11:30
Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical
Physical
(default gateway for PC0 and PC1) 10.10.10.3
192.168.10.3 (default gateway for PC2 and PC3)
Gig0/0/0
Gig0/0/1
ISR4331
Router0
Fa0/3
Fa0/1
Fa0/2
Switch
Switch2
Fa0
PC-PT
PC0
PC1
PC2
PC3
10.10.10.1
10.10.10.2
192.168.10.1
192.168.10.2
class A
class C
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic
Automatically Choose Connection Type


Activities
PacketTracer
Oct 4 11:34
Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical
Physical
(default gateway for PC0 and PC1) 10.10.10.3
192.168.10.3 (default gateway for PC2 and PC3)
Gig0/0/0
Gig0/0/1
ISR4331
Router0
Fa0/3
Fa0/1
Fa0/2
Switch
Switch2
Fa0
PC-PT
PC0
PC1
PC2
PC3
10.10.10.1
10.10.10.2
192.168.10.1
192.168.10.2
class A
class C
Simulation Panel
Event List
Vis. Time(sec) Last Device
0.005 PC3
0.006 Switch2
0.007 Router0
0.008 Switch1
Reset Simulation
Constant Delay
Play Controls
Event List Filters - Visible Events
Edit Filters
Show All/None
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic
Successful PC0 PC3
Automatically Choose Connection Type


Activities
PacketTracer
Oct 18 12:19
Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical
Physical
100.100.100.1
10.10.10.5
Gig0/0/0
Gig0/0/1
Router0
100.100.100.2
Gig0/0/1
192.168.10.5
Fa0/4
Fa0/1
Fa0
Fa0/2
Fa0/3
PC-PT PC0
10.10.10.1
PC-PT PC1
10.10.10.2
PC-PT PC2
10.10.10.3
NETWORK 1(class A)
PC-PT PC3
192.168.10.1
PC-PT PC4
192.168.10.2
Server-PT Server0
192.168.10.3
NETWORK 2(class C)
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic
Successful PC0 PC4
Automatically Choose Connection Type


Activities
PacketTracer
Oct 18 12:13
Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical
Physical
100.100.100.1
10.10.10.5
Gig0/0/0
ISR4331
Router0
Gig0/0/1
100.100.100.2
Gig0/0/1
Router1
Gig0/0/0
192.168.10.5
Fa0/4
Fa0/1
Fa0
Fa0/2
Fa0/3
PC-PT PC0
10.10.10.1
PC-PT PC1
10.10.10.2
PC-PT PC2
10.10.10.3
NETWORK 1(class A)
PC-PT PC3
192.168.10.1
PC-PT PC4
192.168.10.2
Server-PT Server0
192.168.10.3
NETWORK 2(class C)
Simulation Panel
Event List
Vis. Time(sec) Last Device
0.007 Switch1
0.008 Router1
0.009 Router0
0.010 Switch0
Reset Simulation
Constant Delay
Play Controls
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type

Exercise

1) Mention the subnet mask & class of the following IPV4 adresses :-

ⓐ 172.14.9.64
ⓑ 129.34.67.25
ⓒ 185.56.32.87

All the above adresses fall within the range of class B (128.0.0.0 to 191.255.255.255). They all have subnet mask of 255.255.0.0.

2) What are the components used to determine the current IP adress configuration on a windows OS ? Whats the diff. bet" 'IP config' and 'if config' commands ?

"Ipconfig" command is used to determine the current IP adress configuration on a windows OS.

"Ipconfig" command	"ifconfig" command
• Used on windows OS.	• Used on unix systems.
• Primarily displays the networks, including subnet mask & default gateways.	• Displays & configures network interface (similar to IP config but with more control & options).

3) If a class B network has a subnet mask of 255.255.248.0, what is the maximum no. of hosts per subnet ?

[P.T.O]

Name:_____ Regd. Number:_____

255.255.248.0

11111111.11111111.11111000.00000000

Here 21 bits from left are for network and rest 11 for host.

Hosts per subnet = $2^{11} - 2 = 2046$

4) List the situation where NAT is required.

Situations :-

i) Connecting private networks to the internet.
ii) Overcoming IPV4 adress exhaustion.
iii) Network security
iv) Managing networks
v) Connecting multiple subnets with overlapping IPs.
vi) Virtual Private Networks (VPN)
vii) Connecting to cloud services.

5) Host A (on TCP/IPV4 network A) sends an IP datagram D to host B (also TCP/IPV4 network B). Assume that no error occured during the transfer.
i- IP header fields that may be different from that of the original datagram, 'D'.

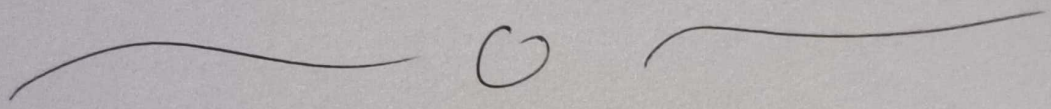
Ans.

When an IP datagram is transmitted from host A to host B over a TCP/IPV4 network, following fields of IP header may change :-

•) TTL (Time To Live)

•) Header Check Sum

TTL value decrements by 1 after each hop and since TTL changes, Check Sum must be also be recalculated after each hop.



Submitted by:-

Computer Networking: Concepts

(CSE 3751)

Experiment 5

Aim:

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

Objectives:

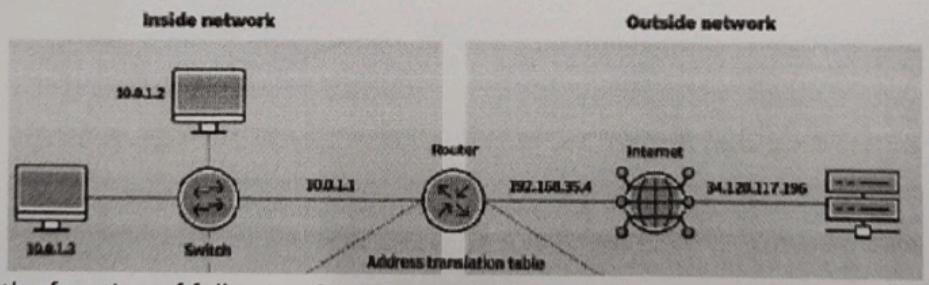
1. An overview on DAT (Dynamic Network Address Translation) and PAT (Port Address Translation).
2. Configuring and implementing DAT using a router to analyse the communication between PCs (in a private network) and public server.
3. Configuring and implementing PAT using a router to analyse the communication between PCs (in a private network) and a PCs in a public network.

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 each private 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.

List of Inside Local Address	Pool of Inside Global Address
PC1 : 10.7.7.61	55.4.4.1
PC2 : 10.7.7.62	55.4.4.2
PC3 : 10.7.7.63	55.4.4.3
PC4 : 10.7.7.64	

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

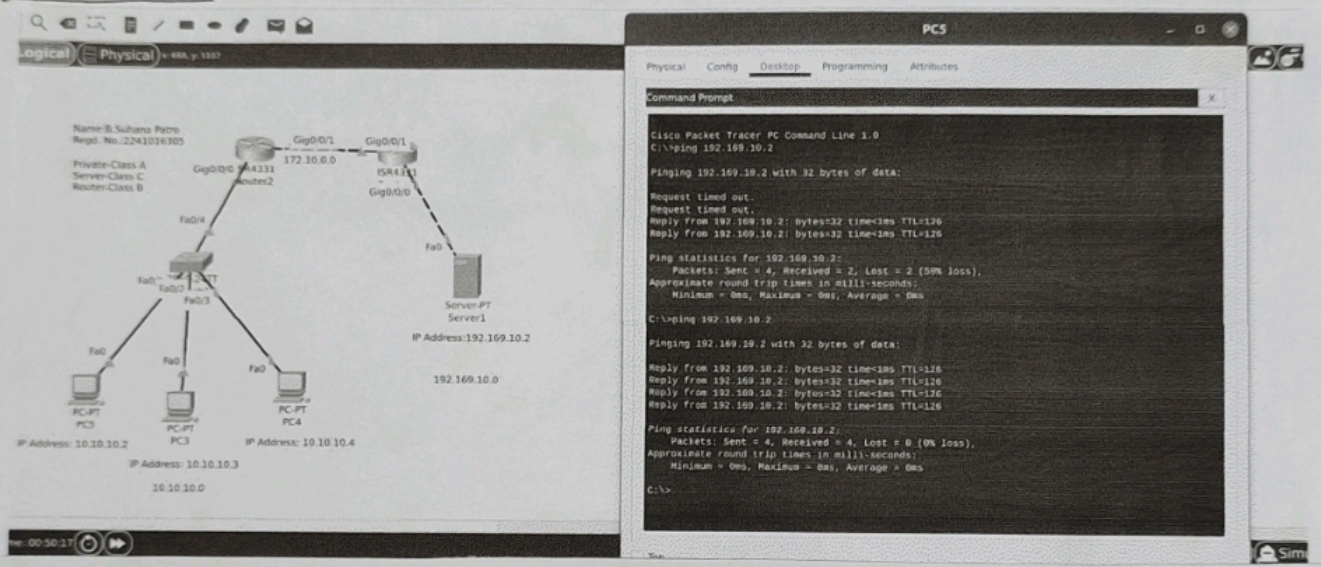
   (v) router(config)#ip nat pool pool-name start-ip end-ip {netmask netmask | prefix-length prefix-length}

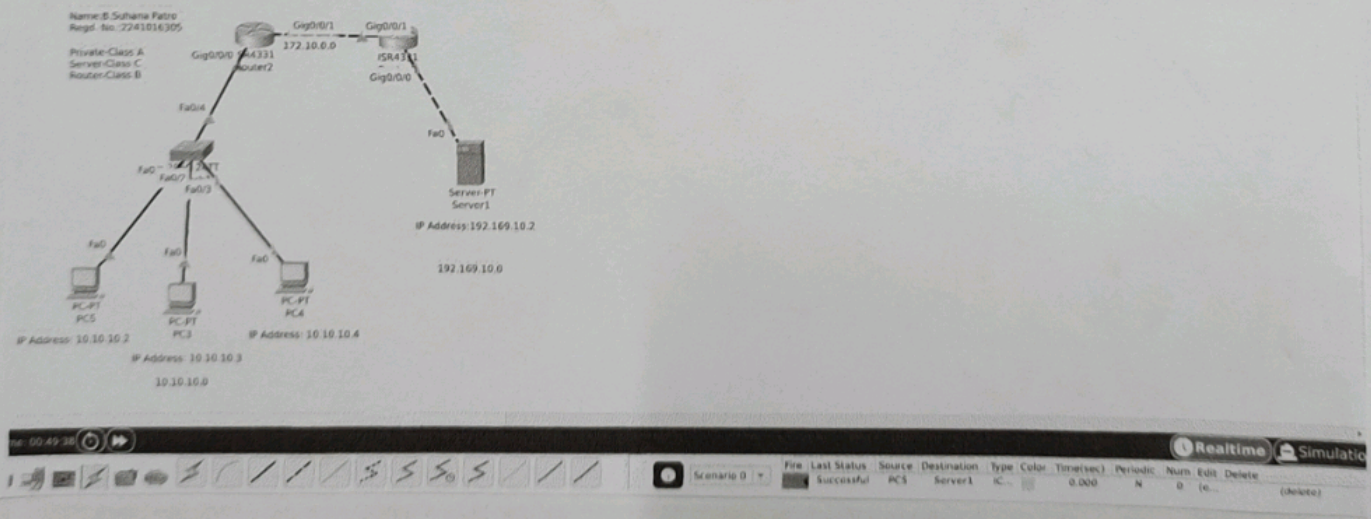
OBJECTIVE-1:

DAT (Dynamic Network Address Translation): DAT dynamically assigns private IPs to public IPs from a pool. Each mapping lasts for the duration of a session. It requires multiple public IPs & is suitable for medium to large networks. It provides a level of flexibility for handling varying connection demands.

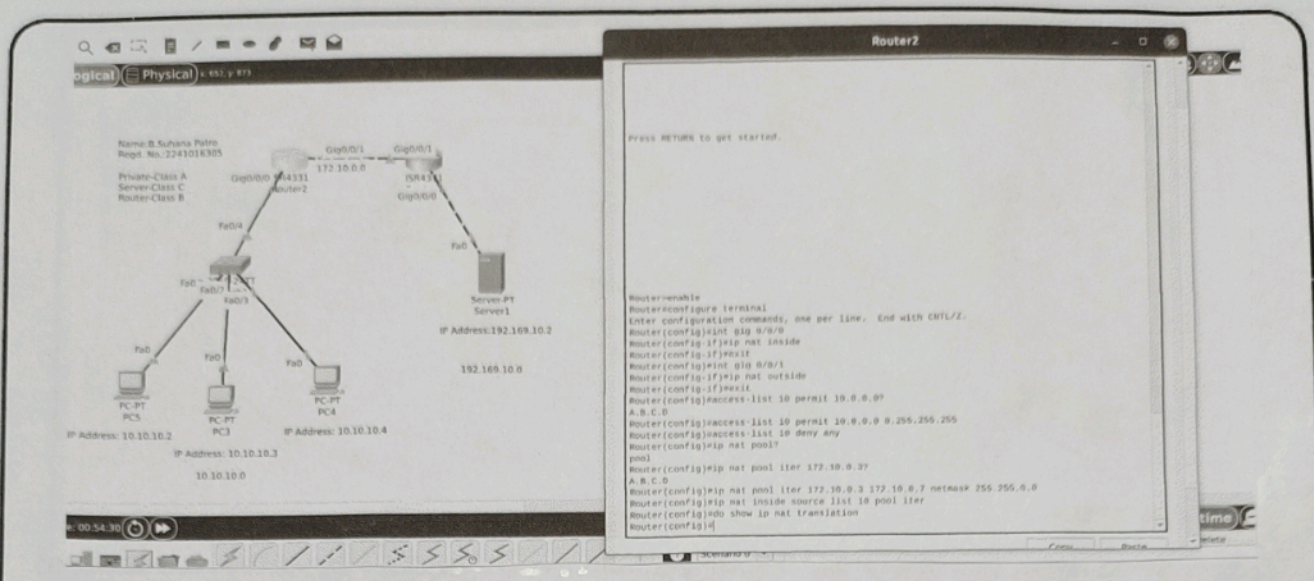
PAT (Port Address Translation): PAT allows multiple private IPs to share a single public IP by assigning unique port numbers to each session. It efficiently conserves public IPs and is commonly used in home and small business networks. It increases security by hiding internal IP addresses and simple to configure and is cost-effective.

OBJECTIVE-2:

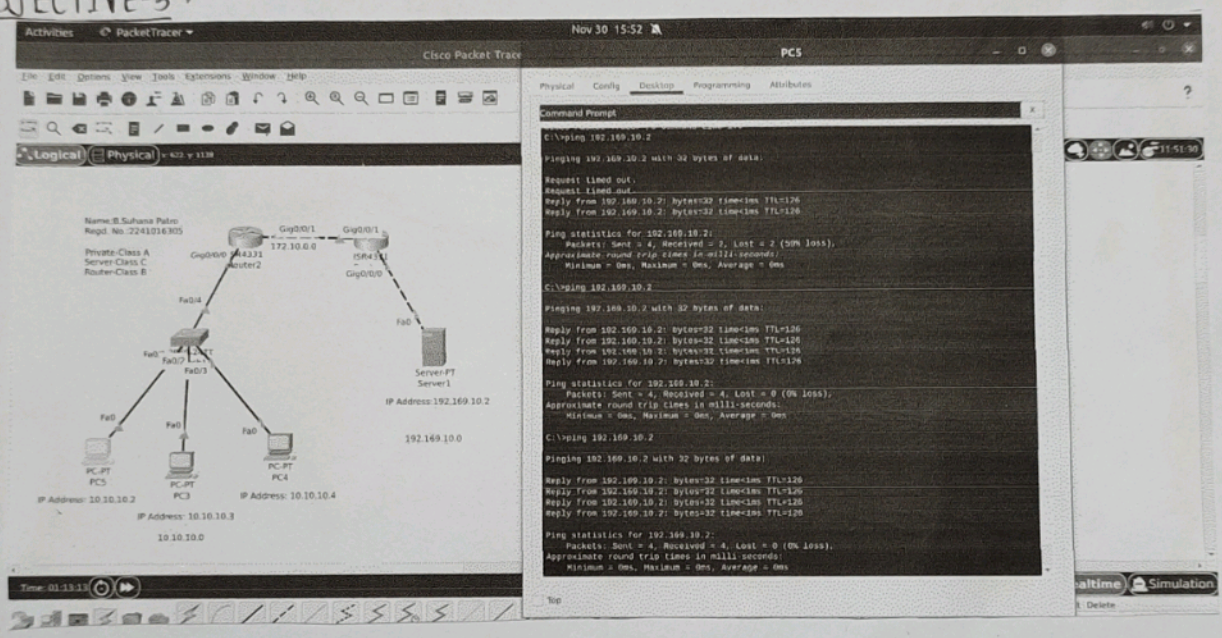


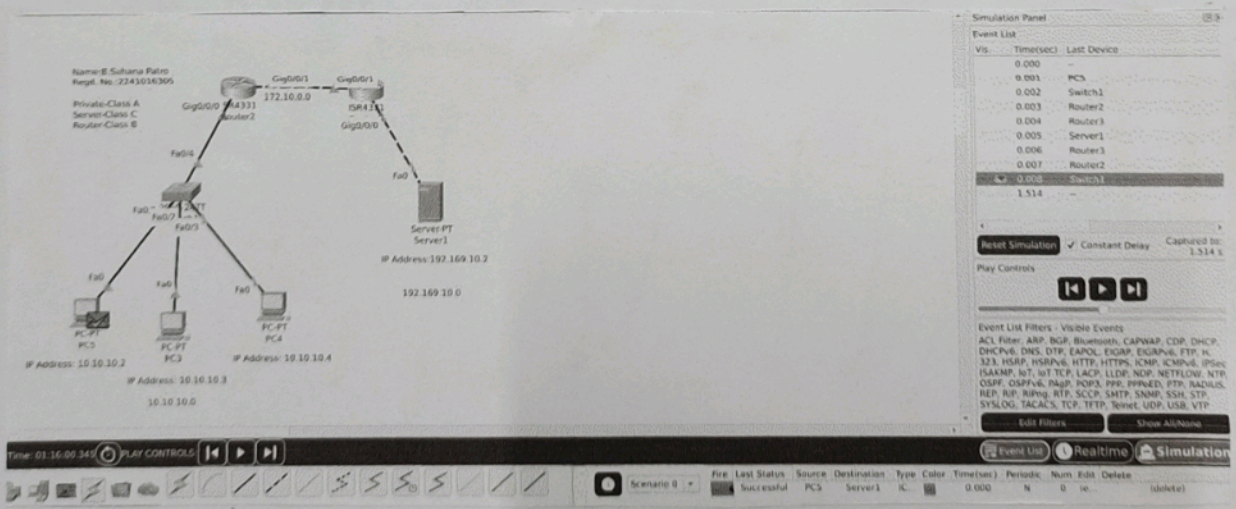


Name:_____ Regd. Number:_____

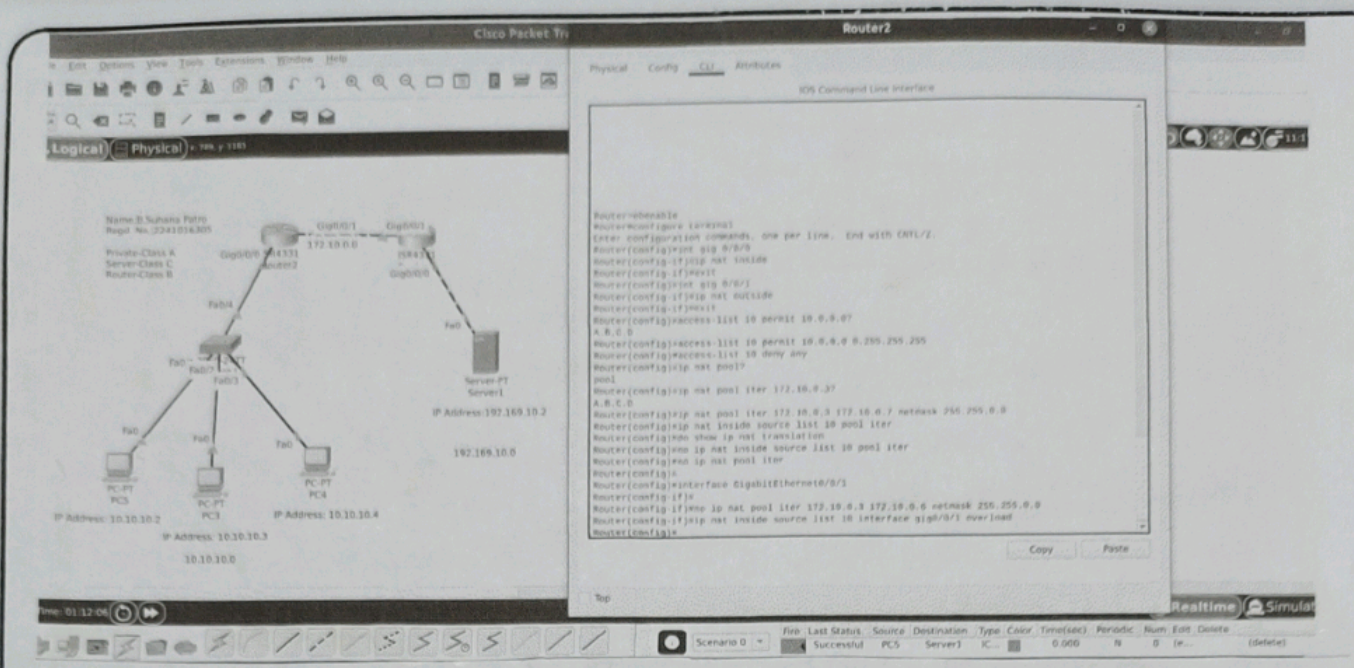


OBJECTIVE-3 :





Name:——————— Regd. Number:———————

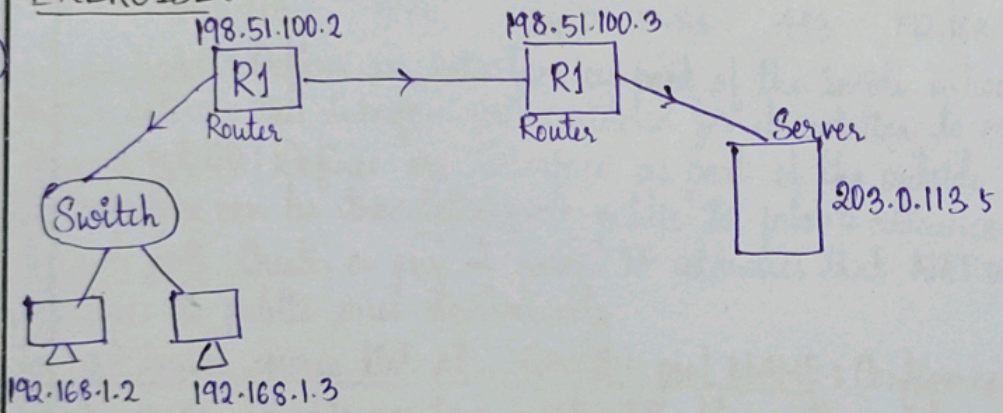


CONCLUSION:

Use of DAT & PAT was understood & implemented on newly constructed & configured topology consisting of private & public network along with routers using CPT or Cisco Packet Tracer.

EXERCISE:

1)



Inside Local: Private IP Addresses of two PCs (192.168.1.2, 192.168.1.3)
Inside Global: Public IP assigned by Router R1 (198.51.100.2)
Outside Global: Public IP of the web server (203.0.113.5)

2) NAT mapping Table:

PC	Inside Local (Private IP)	Inside Global (Public IP)
PC2	10.7.7.62	55.4.4.1
PC4	10.7.7.64	55.4.4.2
PC1	10.7.7.61	55.4.4.3
PC3	10.7.7.63	No IP available

PC2 is assigned the first available public IP (55.4.4.1) then PC4 then PC1 is assigned

Name:_____ Regd. Number:_____

PC3 can't be assigned a public IP address because all public IPs are in use. It must wait until a public ID is freed.

3) Advantages:
i) Efficient use of public IPs by allocating them only when needed
ii) Hides internal IPs for added security.
iii) Reduces IP conflicts with temporary mapping.
iv) Allows multiple devices to access the internet without needing a one-to-one public IP allocation

Disadvantages:
i) Limited by the size of the public IP pool.
ii) Complex to manage due to IP pool configuration.
iii) Connections may fail if public IPs are exhausted
iv) It doesn't allow multiple device to share single public IPs, leading to potential IP wastage.

4) Inside Network:
- 10.0.1.2 is sending a request to an external IP 34.120.117.196 on port 80.
- 10.0.1.3 is sending a request to same external IP 34.120.117.196 on port 443.

Outside Network:
- The router has a public IP of 192.168.35.4 for external communication.

PAT Table:

Internal IP	Internal Port	External IP	External Port	Public IP	Public Port
10.0.1.2	50000	34.120.117.196	80	192.168.35.4	60000
10.0.1.3	50001	34.120.117.196	443	192.168.35.4	60001

5) i) ip nat inside: Defines an interface as part of the inside network for NAT configuration. Packets entering this interface are considered for translation to external addresses.
ii) ip nat outside: Defines an interface as part of the outside network. Packets entering the interface can be translated from public to private addresses.
iii) ip nat pool: Creates a pool of public IP addresses that NAT can use to map private addresses to public ones dynamically.
iv) ip nat inside source list ACL_NUMBER pool NAME: Configures NAT to translate the inside source IP addresses to a public IP address from a specified pool.
v) ip nat pool pool-name start-ip end-ip {netmask netmask | prefix-length prefix-length}: Defines a NAT pool with a range of public IP addresses, specifying either a subnet mask or a prefix length for the pool.

Name:_____ Regd. Number:_____

Aim of the experiment:

Implementing & understanding the use of subnetting & VLSM.

Objectives:

i) An overview on classless IPv4 addressing, CIDR notation, subnetting & VLSM in comp. NW.

ii) → classless IPv4 addressing: It uses subnetting property to reduce the load on router & can faster routing. It reduces the un necessary use of IPv4 addr.

→ CIDR notation: It is a method for allocating IP addr to devices on a N/W which improves the efficiency of data routing. It uses VLSM to divide IP addr into subnets.

→ Subnetting & VLSM: it is a networking technique that allows network engineers to use different subnet mask for different subnets in a network. This will more efficient use of IP addr, Less network congestion, Different from fixed length subnet masks.

iii) Implementing subnetting techniques to divide a NW into smaller subnets and analyting the communication b/w PCs in both inter / intra N/W.

iv) NW subnet configuration:

→ IP addr segmentation:

(a) Divide NW addr space into subnet masking.

(b) create multiple subnets with predefined addr range.

(c) Implement CIDR notation.

Exercise:

Express the following classful ip add^{n} in CIDR notation.

192.34.1.9 → 192.34.1.9/24

10.10.10.1 → 10.10.10.1/8

129.10.14.15 → 129.10.14.15/16

Given ip add^{n} of a device = 192.168.10.126 /25 find subnet mask & nw id.

192.168.10.126

255.255.255.128 → subnet mask

&

192.168.10.0 → nw id

& nw id 200.1.2.0 is divided into 3 subnets find no of hosts per subnet. Also for all subnet find (a) subnet add^{n} (b) first host (c) last host (d) Broadcast add^{n}.

Total add^{n}able host = 256

Host per subnet = 84

subnet-1: 200.1.2.0 (nw id)

200.1.2.1 (first host id)

200.1.2.84 (last " ")

200.1.2.85 (Broadcast add^{n})

subnet-2: 200.1.2.86 (nw id)

200.1.2.87 (first host id)

200.1.2.170 (last host id)

200.1.2.171 (Bc. add^{n})

→ subnet parameters:

(a) Define subnet size based on device count

(b) Establish subnet mask.

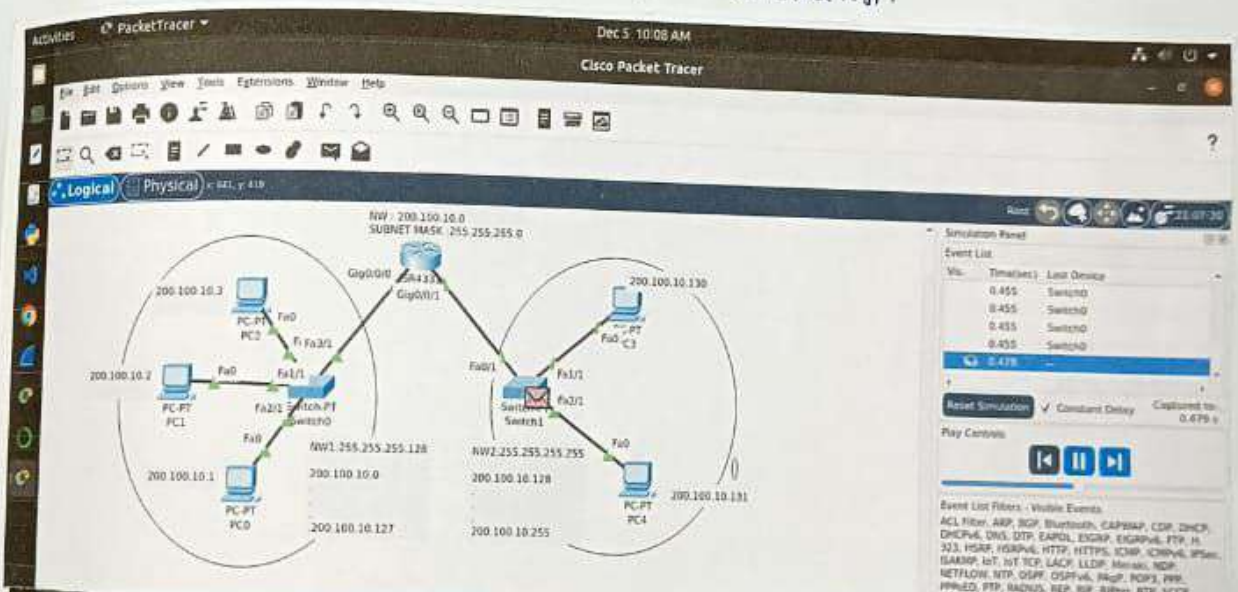
(c) Allocate unique network ID for each subnet

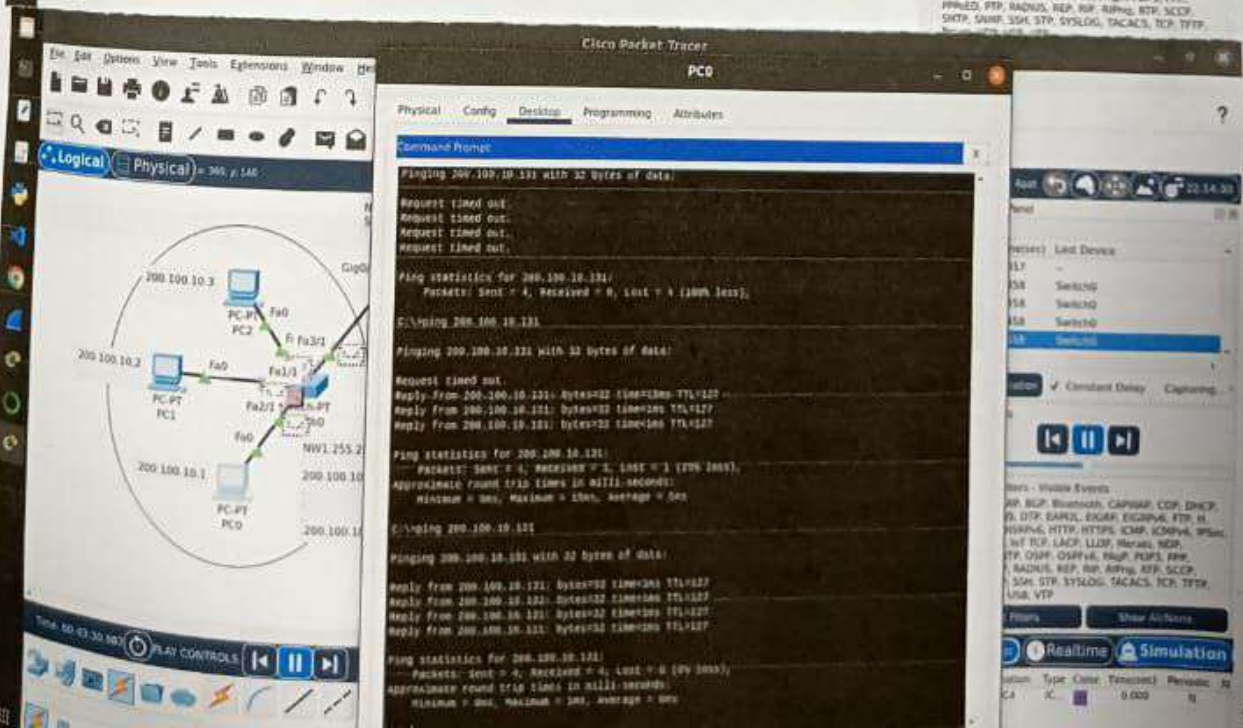
→ Intra subnet communication:

Device with in 1 subnet communicate via switch, minimal latency, high band width.

→ Inter subnet communication:

Device with in different subnet communicate via router, IP packet encapsulation & addr translation.

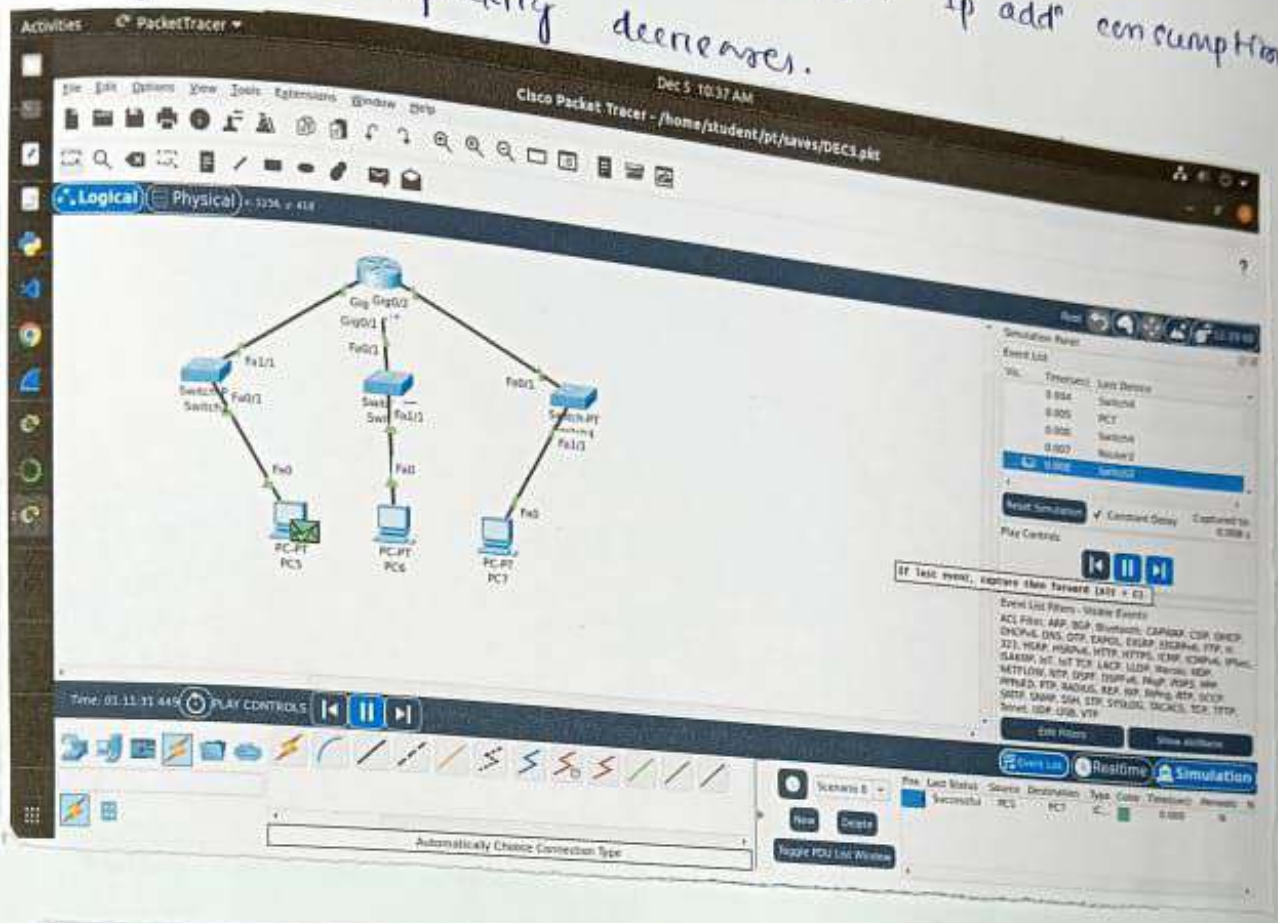


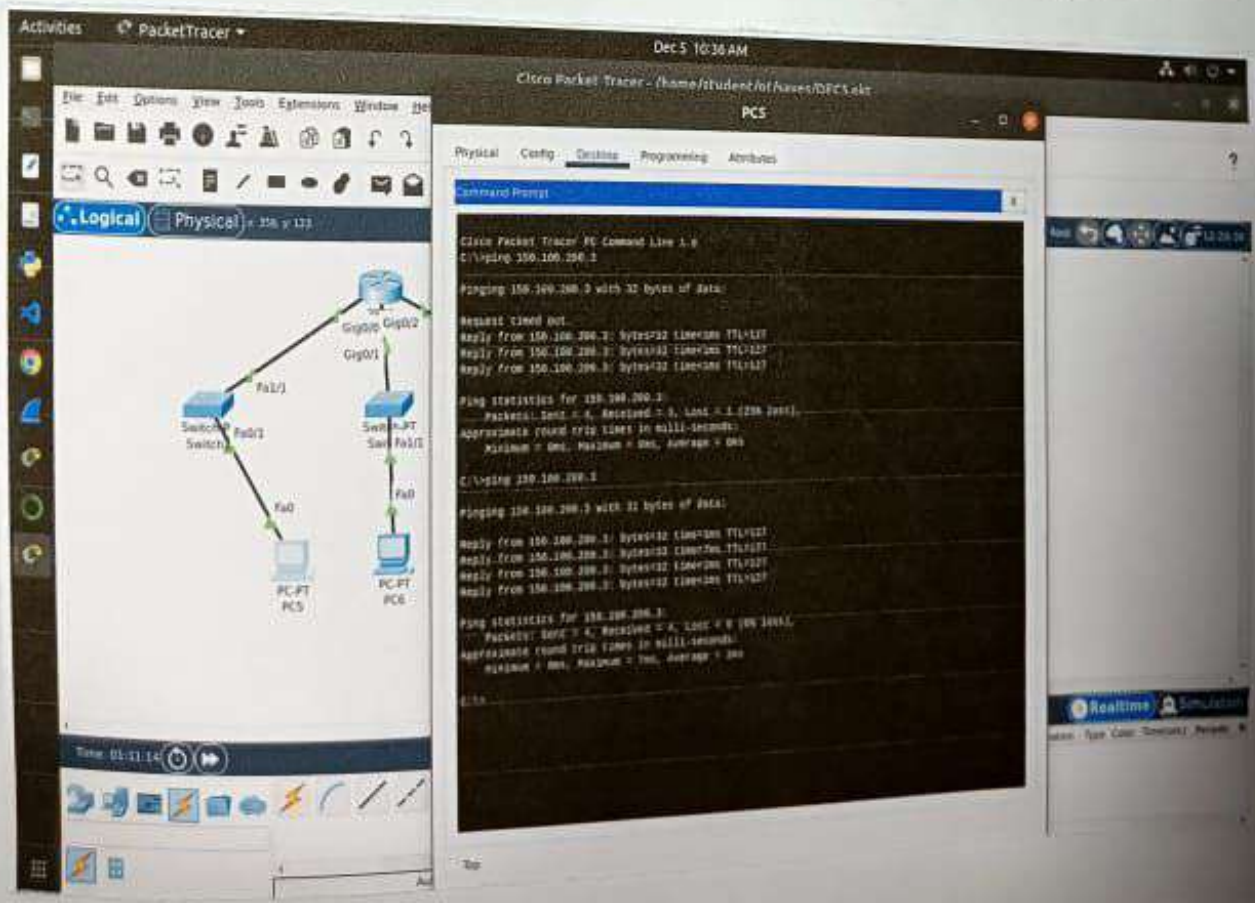


(TER)

Implementing VLSM technique to optimize IP addr allocn to PCs & interfaces in a given nw & analyzing the communicatn

VLSM will enable, precise nw segmentatn. Allows different nw site with in same network. Reduces IP addr consumptn. Routing table complexity decreases.





Subnet-3: 200.1.2.172 (nw id)

200.1.2.173 (First host)

200.1.2.254 (last ")

200.1.2.255 (BC. add^n)

4) Design a nw using VLSM for the following requirements with given 10.0.0.0/24. Assign Ip add^n accordingly: (a) nw A - 60 hosts, (b) nw B - 30 hosts, (c) nw C - 12 hosts, (d) nw D - 6 hosts.

Sol^n:

N/W A: 10.0.0.0/26

Rng: 10.0.0.1 - 10.0.0.60

N/W B: 10.0.0.64/27

Rng: 10.0.0.65 - 10.0.0.94

N/W C: 10.10.0.96/28

Rng: 10.10.0.97 - 10.10.0.110

N/W D: 10.10.0.112/29

Rng: 10.10.10.113 - 10.10.0.118

Department of Computer Science & Engineering
Faculty of Engineering & Technology (ITER)

EXPERIMENT - 7

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

OBJ-1 :~

Dynamic Host control Protocol (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.
Connection a TVs in 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:- Connects one laptop to another using Ethernet cable but there is no DHCP server (like router). Still Both laptos assign themselves APIPA address to share files directly with each other.

Name:_____ Regd. Number:_____

OBJ-2

FTP :~

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

- How it works ?
  - > Seting up connection
  - > Do Login
  - > Now, upload / download files
  - > Close the connection

TELNET :~

→ It is used to control another computer remotly over a network, similar to controlling a device using a command line.

- How it works ?
  - > Connection setup
  - > Do 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

Name:_____ Regd. Number:_____

Department of Computer Science & Engineering
Faculty of Engineering & Technology (ITER)

EXERCISE - 7

① What is DHCP Snooping ? What are the advantages of using DHCP in a network?

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

↳ ADVANTAGES :

① IP address is getting assigned automatically
② It ensure efficient use of IP address.
③ Scalability
.etc

② State the use of APIPA highlighting its advantages. what is the range of IP address for APIPA?. write APIA address generated for your address in this experiment?

Ans:-

Use of APIPA :

↳ It is used when a device canot get an IP address from a DHCP server. It assigns an IP address automatically. enabling devices to communicate within the same local network.

Advantages of APIPA :

① No need of manual configuration of IP addresses.
② Allow devices to communicate on the same network, even if DHCP is unavailable
③ Provides back up if DHCP fails.

Name:_____ Regd. Number:_____

You need to print out Q2

④ Compare FTP and TELNET protocols interms of functionality & security.

① Connection Type :

→ FTP uses Port 21 & Port 20
→ TELNET uses Port 23

② Data tranfer :

→ FTP transfers files, dictionaries
→ TELNET transfers text-based commands & outputs

③ Usage :

→ FTP is commonly used to upload & download files
→ whereas TELNET used to remotly 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)

Name:_____ Regd. Number:_____