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 (Network Address Translation).

IPv4 Addressing →

IPv4 is a 32-bit address system with unique identifiers for networked devices, categorized as:

i) Public Addresses: Globally routable; assigned by ISPs for internet-accessible devices.

ii) Private Addresses: Used within local networks; not routable on the internet.

Ranges include →

a) Class A → 10.0.0.0 - 10.255.255.255

b) Class B → 172.16.0.0 – 172.31.255.255

c) Class C → 192.168.0.0 – 192.168.255.255

iii) Classful Addressing → Divided into classes A, B, C, D (multicast) and E (experimental). Replaced by CIDR for efficient address usage.

Network Address Translation (NAT) →

NAT modifies IP addresses in packets, enabling private network devices to access the internet using fewer public IPs. Types include:

i) Static NAT → Maps one private IP to one public IP.

ii) Dynamic NAT → Uses a pool of public IPs for mapping.

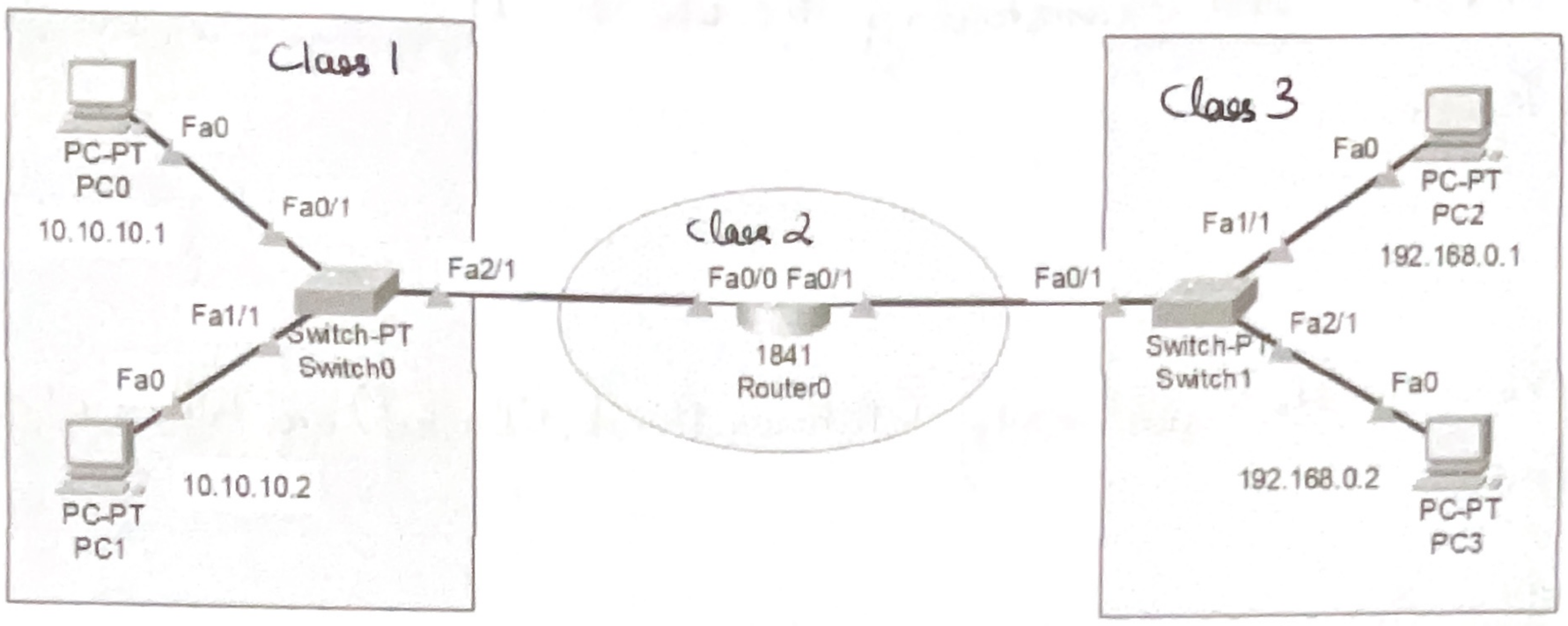
iii) PAT (NAT overload): Maps multiple private IPs to one public IP using port numbers.

Benefits: Conserves public IPs, enhancing security, and supports private networks.

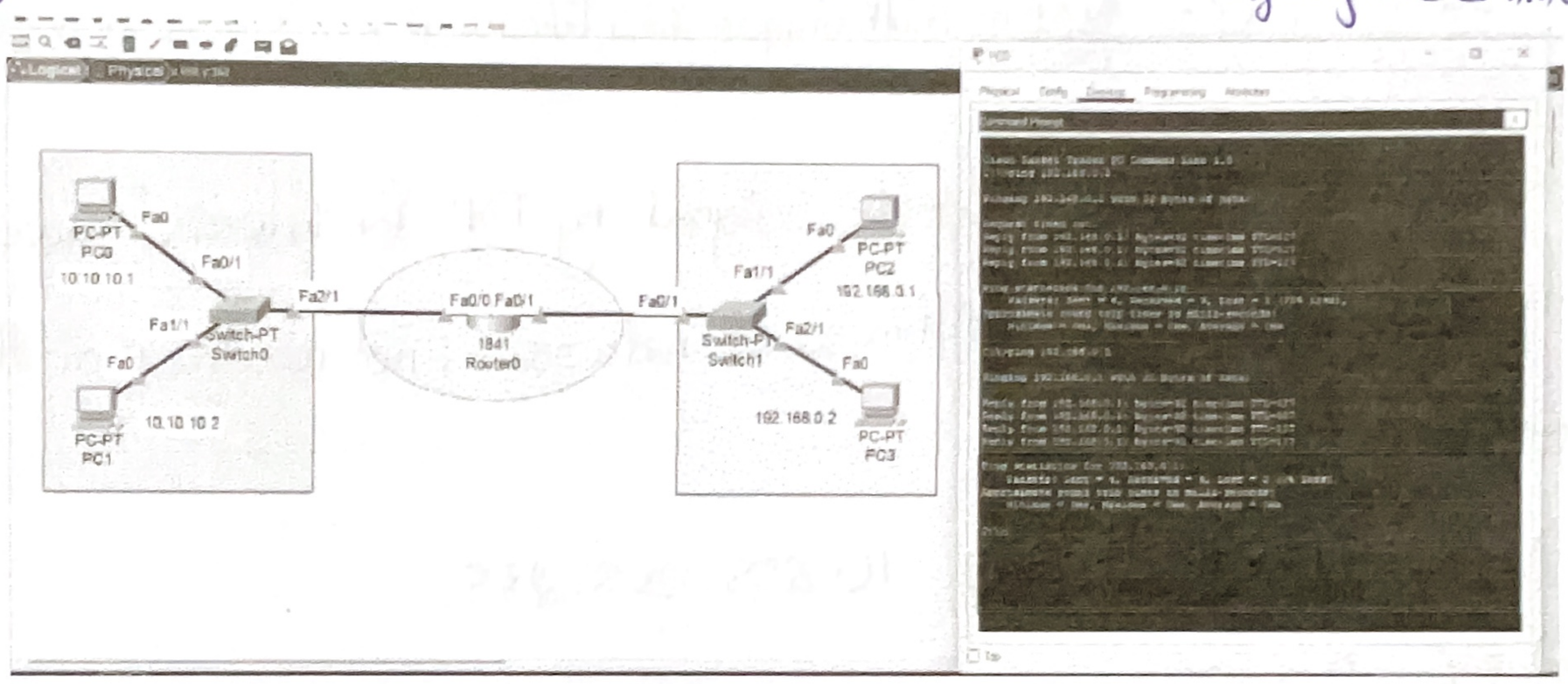
Limitations: Adds latency and breaks some applications' connectivity.

NAT ensures IPv4 sustainability, but IPv6 is reducing its necessity.

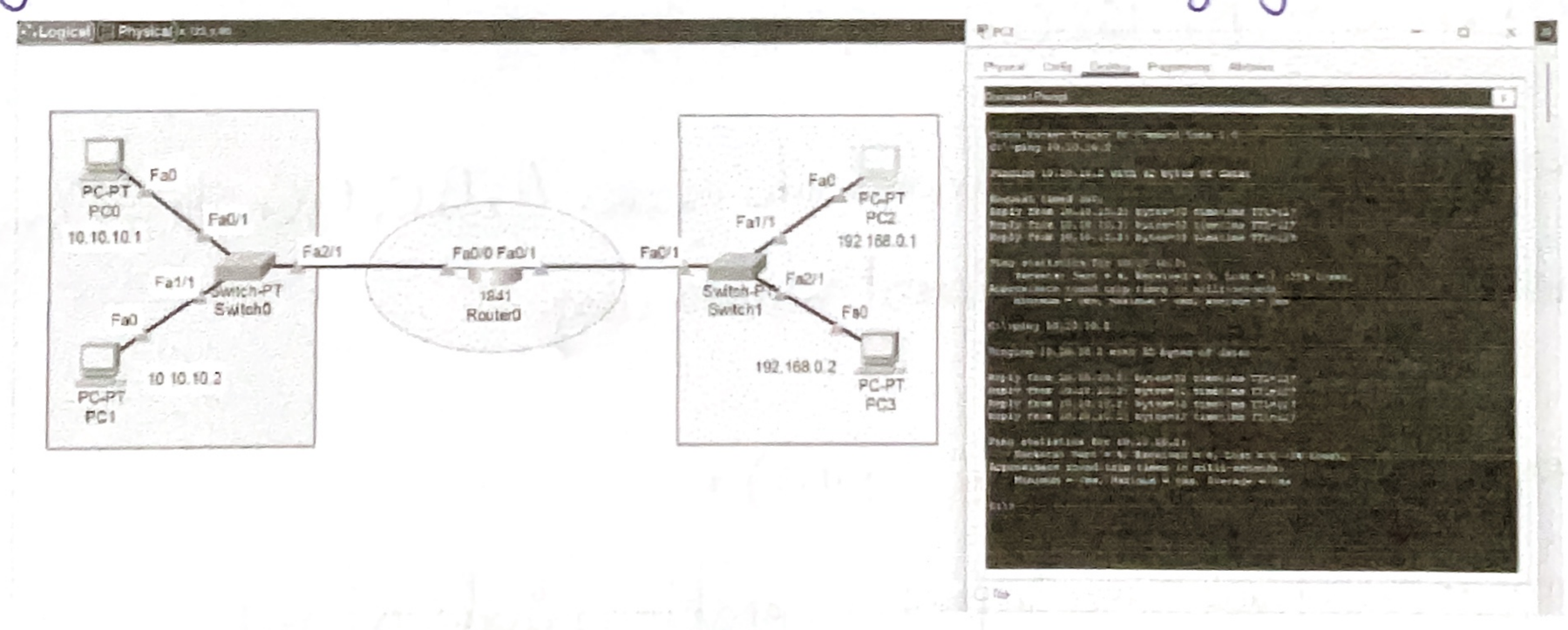
Objective 2 → Constructing and analyzing the communication between two networks (of different classes).



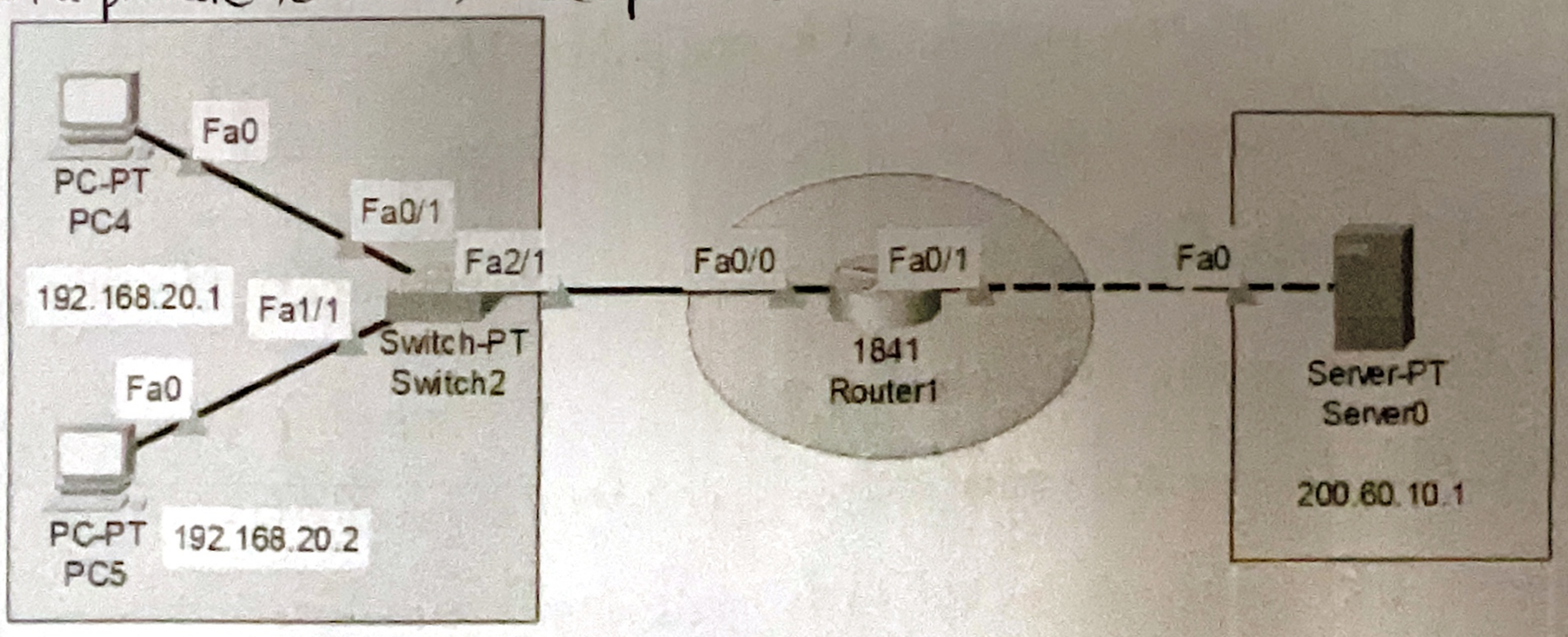
Step 1 → Ping from PC0(10.10.10.1) to PC2(192.168.0.1) and analyzing the communication.



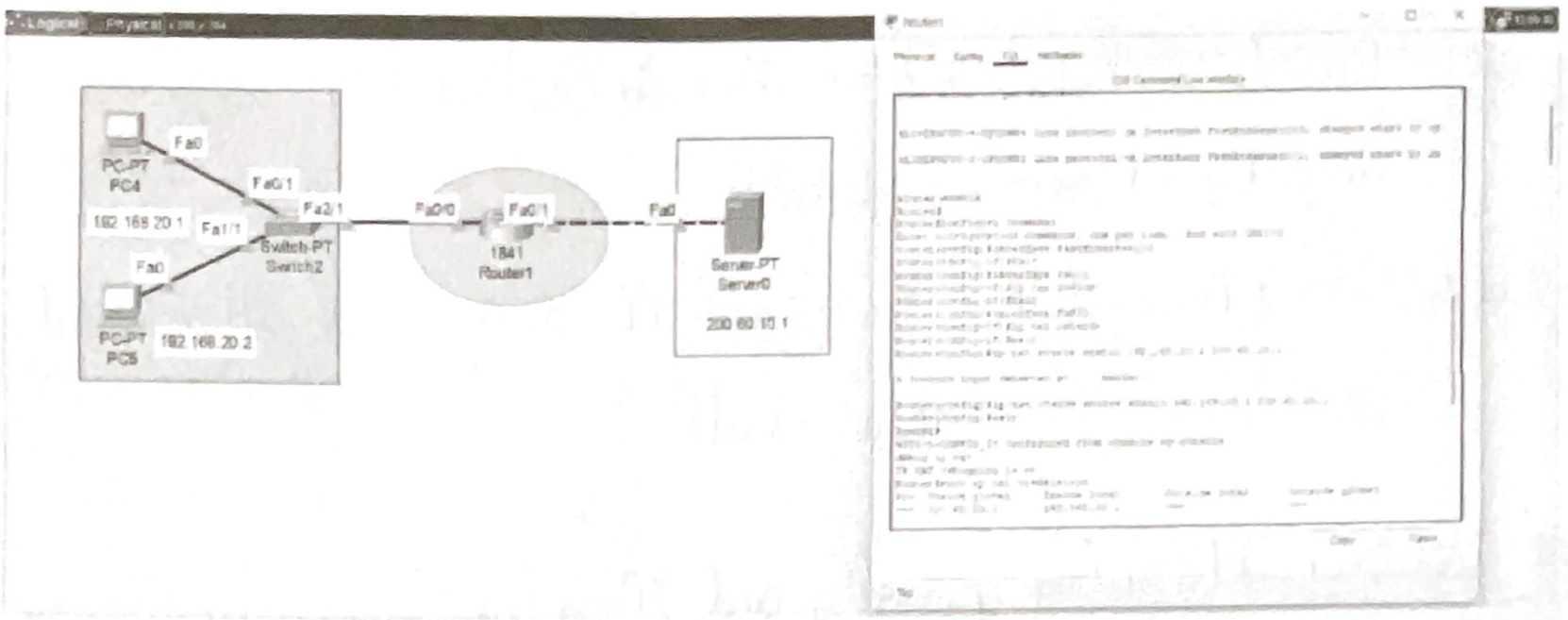
Step 2 → Ping from PC2(192.168.0.1) to PC0(10.10.10.1) and analyzing the communication.



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



Sending messages using NAT commands at Router 0 from PC4 (192.168.20.1) to server and back to PC.



Conclusion →

The experiment demonstrated IPv4 addressing, subnetting, and NAT configuration using Cisco Packet Tracer. It highlighted how NAT facilities communication between private networks and public servers while reinforcing the role of subnetting and address translation in efficient network communication.

Exercises →

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

a) 172.14.9.64 →

Ans → • Class B (falls within 128.0.0.0 – 191.255.255.255)

• Default Subnet Mask → 255.255.0.0 (/16)

b) 129.34.67.25 →

Ans → • Class B (128.0.0.0 – 191.255.255.255)

• ~~Class~~ Default Subnet Mask → 255.255.0.0 (/16)

c) 185.56.32.87 →

Ans → • Class B

• Default Subnet Mask → 255.255.0.0

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?

Ans → Commands to Determine IP address Configurations in Windows →

Name: _____ Regd No: _____

i) ipconfig: Displays the IP address, subnet mask and default gateway for each network interface.

ii) ipconfig /all: Provides detailed information, including MAC addresses, DNS servers and DHCP ~~servers~~ details.

iii) Get-NetIPAddress (Powershell): Retrieves IP addresses of all network adapters using Powershell.

Difference between IR~~config~~ ipconfig and ifconfig:

Aspect	ipconfig	ifconfig
Platform	Windows OS	Linux and Unix-based systems
Function	Displays IP configuration details	Displays and configures network interfaces.
Scope	Primarily for viewing IP-related details	Can view, configure and manage interfaces.
Status	Actively used in Windows system	Depreceated in favour of ip commands in Linux.
Examples	ipconfig, ipconfig /release, ipconfig /renew	ifconfig, ifconfig eth0 up/down

3) If a class B network on the internet has a subnet mask of 255.255.248.0, what is the max^m number of host per subnet?

Ans→ 255.255.248.0 → 11111111.11111111.11111000.00000000 in binary

Here, the first 16 bits are network bits. The next 5 are subnet bits. The remaining 11 bits belong to the host bits.

So, the total no. of hosts per subnet = $2^n - 2$

$= 2^{11} - 2 = 2048 - 2$

$= \underline{\underline{2046}}$.

4) List the situation where NAT is required.

Ans → NAT (Network Address Translation) is required in the following situations →

i) Internet Access for private networks : Translates private IPs to public IPs for internet access.

ii) IP Address Conservation : Allows multiple devices to share a single public IP.

iii) Hiding Internal Network Topology → Masks internal IPs for security.

iv) Overlapping IP spaces → Resolves conflicts when networks have overlapping private IP ranges.

v) Load Balancing → Distributes traffic to multiple servers.

vi) VPN Connections → Ensures secure communication with remote networks.

vii) Port Forwarding → Routes external traffic to specific internal devices.

viii) ISP IPv4 management → Used by ISPs to manage address shortages (Carrier-Grade NAT).

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 errors 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?

Ans → When an IP datagram travels from host A to host B across a TCP/IPv4 network, the following IP header fields may differ in the datagram recieved by host B compared to the original datagram sent by host A:

i) Time to Live (TTL) → The TTL field decrements by 1 at each hop (router) along the path. If the packet passes through multiple hops, the TTL value will be lower at host B than when it left host A.

ii) Header Checksum → The IP header checksum is recalculated at each hop since the TTL changes. As a result, the checksum value will be different when the datagram reaches host B.

Other fields in the IP header (e.g., source IP address, destination IP address) remain unchanged during the transmission, provided no NAT or encapsulation occurs.

Name:_____ Regd No.:_____