- ping commands were successful, confirming bidirectional peer communication.

Experiment 8

Title: Examine Network Address Translation (NAT)

1. Introduction

Network Address Translation (NAT) is a method used in networking to map private (local) IP addresses to a public IP address before transferring the information over the internet. It allows multiple devices in a private network to access the internet using a single public IP address, helping to conserve IPv4 addresses and providing security.

2. Objectives

- To understand the purpose and functionality of NAT.
- To configure and examine NAT in a simulated environment using Cisco Packet Tracer.
- To observe the translation of private IP addresses to public IP addresses.

3. Types of NAT

Type	Description
Static NAT	Maps one private IP address to one public IP address permanently.
Dynamic NAT	Maps private IPs to public IPs from a pool, temporarily.

PAT (Port Address Translation)	Also known as **NAT Overload**. Multiple private IPs share one public IP using different port numbers. Most commonly used type of NAT.

---

4. Tools Required

- Cisco Packet Tracer software
- 1 Router
- 1 Switch
- 2 PCs (in private LAN)
- 1 Server (to simulate the public internet)
- Copper straight-through cables

---

5. Network Topology

[PC0] [PC1]

\ /

[Switch]------[Router]------[Web Server (Public IP)]

NAT Enabled

---

6. IP Addressing Scheme

Device	Interface	IP Address	Subnet Mask
PC0	NIC	192.168.1.2	255.255.255.0
PC1	NIC	192.168.1.3	255.255.255.0
Router LAN	FastEthernet0/0	192.168.1.1	255.255.255.0

Router WAN	FastEthernet0/1	200.1.1.1	255.255.255.0
Server	NIC	200.1.1.2	255.255.255.0

7. NAT Configuration (PAT - NAT Overload)

Step 1: Assign IP addresses (PCs, Router, Server)

- Use **IP Configuration** for PCs and Server.
- Use **CLI** on the router for interface setup:

```
Router> enable
Router# configure terminal

Router(config)# interface FastEthernet0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit

Router(config)# interface FastEthernet0/1
Router(config-if)# ip address 200.1.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
```

Step 2: Configure NAT Overload (PAT)

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# ip nat inside source list 1 interface FastEthernet0/1 overload
Router(config)# interface FastEthernet0/0
Router(config-if)# ip nat inside
```

```
Router(config-if)# exit
Router(config)# interface FastEthernet0/1
Router(config-if)# ip nat outside
Router(config-if)# exit
```

8. Testing NAT

1. Open PC0 and PC1 command prompt.
2. Type: ping 200.1.1.2 (IP of web server)
3. Successful ping replies confirm NAT is working.
4. On router, use:

```
Router# show ip nat translations
```

→ Displays active NAT mappings from private to public IP addresses.

Experiment 9

Simulate the Implementation of Various Routing Protocols (Using Cisco Packet Tracer)

1. Introduction

Routing protocols are essential in dynamic networks to ensure that routers can automatically discover and maintain optimal paths for data transmission. These protocols help routers communicate with each other to update and maintain routing tables. In this simulation, we implement and compare different routing protocols using **Cisco Packet Tracer**.

2. Objectives

- To understand and simulate the working of various routing protocols.
- To configure routers using **static**, **RIP**, **EIGRP**, and **OSPF** protocols.
- To verify communication between networks using routing tables and ping tests.

3. Tools Required

- Cisco Packet Tracer software
- 3 Routers
- 3 Switches