NOTRE DAME UNIVERSITY
BANGLADESH

Computer Networks Lab Report-01

Course Code: CSE-3204
Course Title: Computer Networks Lab
Lab Task Topic: Configuration of Dynamic NAT

Submitted by:

Name: Istiak Alam
ID: 0692230005101005
Batch: CSE-20

Submission Date: May 7, 2025

Submitted to:

Dr. Fernaz Narin Nur
Adjunct Professor,
Notre Dame University Bangladesh

Objective

To implement and understand the working of **Dynamic NAT (Network Address Translation)** using Cisco Packet Tracer, allowing private IP addresses to access a public network by translating them dynamically to a public IP pool.

Tools Used

- Cisco Packet Tracer

- Routers (2x: Public Router & NAT Router)

- Switches (1 or more)

- End Devices (PC, Server)

- Copper Cross-Over & Serial DCE cables

Network Design Overview

Device	Interface	IP Address / Role
PC	NIC	192.168.30.2 (Internal User Device)
Public Router	Fa0/0	192.168.30.1 (Gateway to NAT Router)
Public Router	S2/0	20.0.0.2 (Link to NAT Router)
NAT Router	S2/0	20.0.0.1 (NAT Inside)
NAT Router	Fa0/0	10.0.0.1 (NAT Outside)
Server	NIC	10.0.0.100 (External Server)

Step by Step Configuration

0.1   PC Configuration

```
IP Address: 192.168.30.2, 192.168.30.3 & 192.168.30.4
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.30.1
```
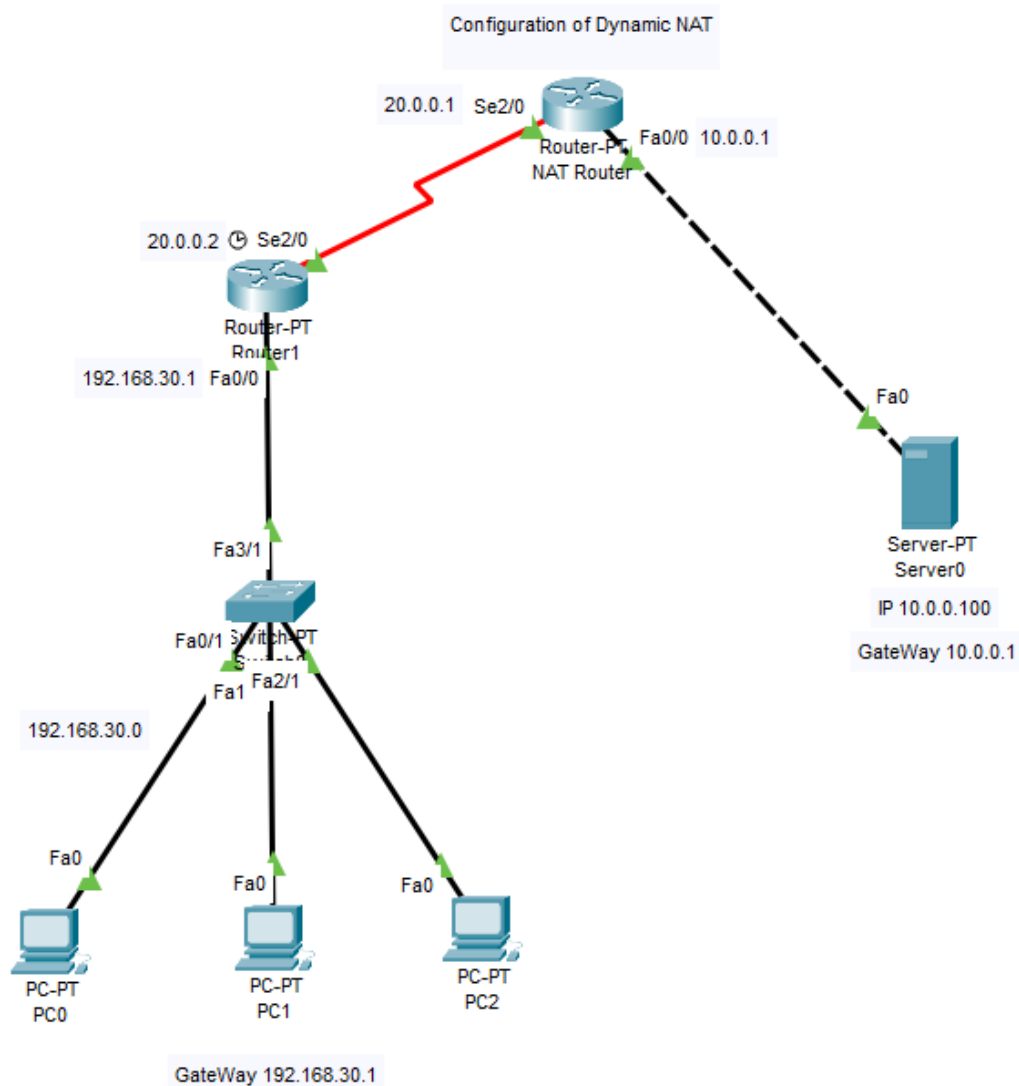
Network Topology in Packet Tracer :

Figure 1: Network Topology for Dynamic NAT Configuration

0.2 Public Router Configuration

```
enable
configure terminal

interface fa0/0
ip address 192.168.30.1 255.255.255.0
no shutdown
exit

interface s2/0
ip address 20.0.0.2 255.255.255.252
clock rate 64000
no shutdown
exit

ip route 0.0.0.0 0.0.0.0 20.0.0.1
```

0.3 NAT Router Configuration

```
enable
configure terminal

interface s2/0
ip address 20.0.0.1 255.255.255.252
ip nat inside
no shutdown
exit

interface fa0/0
ip address 10.0.0.1 255.255.255.0
ip nat outside
no shutdown
exit

ip nat pool DYN_POOL 10.0.0.20 10.0.0.30 netmask 255.255.255.0
access-list 1 permit 192.168.30.0 0.0.0.255
ip nat inside source list 1 pool DYN_POOL overload

ip route 192.168.30.0 255.255.255.0 20.0.0.2
```

0.4 Server Configuration

```
IP Address: 10.0.0.100
Subnet Mask: 255.255.255.0
Default Gateway: 10.0.0.1
```

Testing the Configuration

- From PC, run: `ping 10.0.0.100`

- On NAT Router, verify NAT translations:

  ```
  show ip nat translations
  ```

Output:

```
Pro   Inside Global      Inside Local      Outside Local      Outside Global
icmp 10.0.0.20:6        192.168.30.3:6      10.0.0.100:6        10.0.0.100:6
icmp 10.0.0.20:7        192.168.30.3:7      10.0.0.100:7        10.0.0.100:7
icmp 10.0.0.20:8        192.168.30.3:8      10.0.0.100:8        10.0.0.100:8
icmp 10.0.0.20:9        192.168.30.3:9      10.0.0.100:9        10.0.0.100:9
```

Conclusion

This lab successfully demonstrated how **Dynamic NAT** works in a network, allowing internal private IPs to dynamically be assigned public IPs from a pool when accessing an external network. The configuration ensures secure and controlled access between internal and external networks.