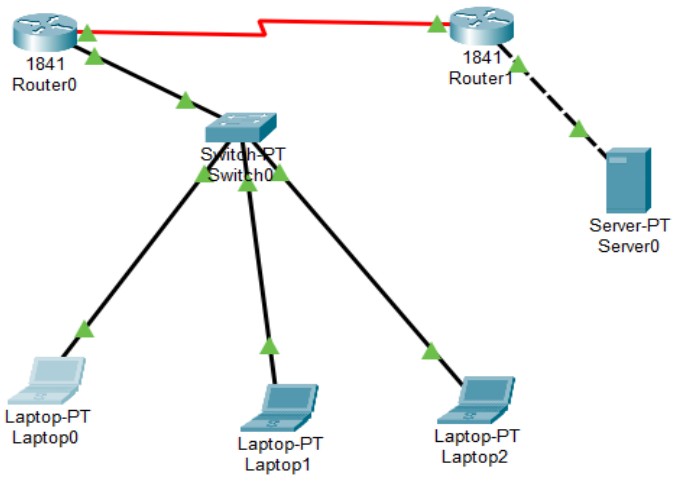
Experiment -4 **Date:18/8/2025**

Configure Dynamic NAT in Cisco Packet Tracer

AIM: To configure, manage, verify and debug dynamic NAT step by step with packet tracer.

Dynamic NAT configuration (creating an access list of IP addresses which need translation, creating a pool of available IP address, mapping access list with pool and defining inside and outside interfaces)



Initial IP Configuration:

DEVICE/INTERFACE	IP ADDRESS	CONNECTED WITH
Laptop0	10.0.0.10/8	Fa0/0 of R0
Laptop1	10.0.0.20/8	Fa0/0 of R0
Laptop2	10.0.0.30/8	Fa0/0 of Ro
Server0	192.168.1.10/24	Fa0/0 of R1
Serial 0/0/0 of R1	100.0.0.1/8	Serial 0/0/0 of R2
Serial 0/0/0 of R2	100.0.0.2/8	Serial 0/0/0 of R2

To configure IP address in Router1 click Router1 and select CLI and press Enter key.

Run following commands to set IP address and hostname.

```
R1#en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int FastEthernet 0/0
R1(config-if)#ip address 10.0.0.1 255.0.0.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#int Serial 0/0/0
R1(config-if)#ip address 100.0.0.1 255.0.0.0
R1(config-if)#clock rate 64000
R1(config-if)#bandwidth 64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

Same way accesses the command prompt of R2 and run following commands to set IP address and hostname.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#int FastEthernet 0/0
R2(config-if)#ip address 192.168.1.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#int Serial 0/0/0
R2(config-if)#ip address 100.0.0.2 255.0.0.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
```

Configure Dynamic NAT

Dynamic NAT configuration requires four steps: -

1. Create an access list of IP addresses which need translation

2. Create a pool of all IP address which are available for translation Map access list with pool

3. Define inside and outside interfaces

4. In first step we will create a standard access list which defines which inside local addresses are permitted to map with inside global address.

To create a standard numbered ACL following global configuration mode command is used:-

Router(config)# access-list ACL_Identifier_number permit/deny matching-parameters

Let's create a standard access list which allows two hosts and denies one host.

R1(config)#access-list 1 permit 10.0.0.10 0.0.0.0

R1(config)#access-list 1 permit 10.0.0.20 0.0.0.0

R1(config)#access-list 1 deny any

In second step we define a pool of inside global addresses which are available for translation. Following command is used to define the NAT pool.

Router(config)#ip nat pool [Pool Name] [Start IP address] [End IP address] netmask [Subnet mask]

Let's create a pool named ccna with an IP range of two addresses.

R1(config)#ip nat pool ccna 50.0.0.1 50.0.0.2 netmask 255.0.0.0

This pool consists two class A IP address 50.0.0.1 and 50.0.0.2.

In third step we map access list with pool. Following command will map the access list with pool and configure the dynamic NAT.

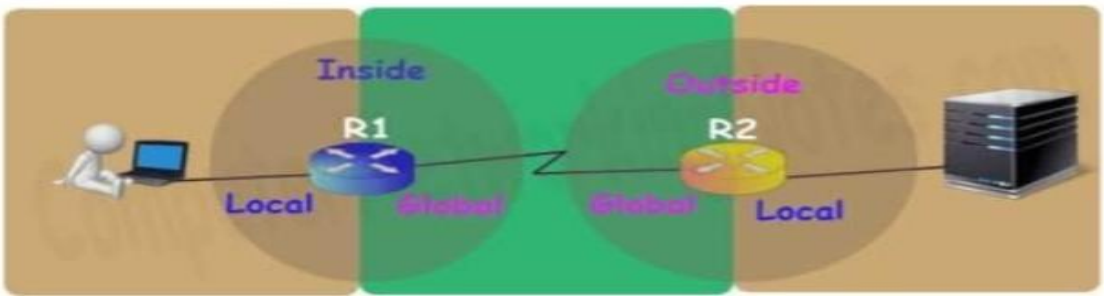
Router(config)#ip nat inside source list [access list name or number] pool [pool name]

To configure a dynamic NAT with these options we will use following command.

R1(config)#ip nat inside source list 1 pool ccna

Finally we have to define which interface is connected with local network and which interface is connected with global network.

- To define an inside local we use following command, Router(config-if)#ip nat inside
- Following command defines inside global, Router(config-if)#ip nat outside



R1 Dynamic NAT Configuration

```
R1(config)#access-list 1 permit 10.0.0.10 0.0.0.0
R1(config)#access-list 1 permit 10.0.0.20 0.0.0.0
R1(config)#access-list 1 deny any
R1(config)#ip nat pool ccna 50.0.0.1 50.0.0.2 netmask 255.0.0.0
R1(config)#ip nat inside source list 1 pool ccna
R1(config)#ip nat inside
% Incomplete command.
R1(config)#int FastEthernet 0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#int Serial 0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
```

On R2 we can keep standard configuration or can configure dynamic NAT as we just did in R1 or can configure static NAT

Configure static NAT on R2.

```
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip nat inside source static 192.168.1.10 200.0.0.10
R2(config)#int Serial 0/0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#int FastEthernet 0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#
```

Before we test this lab we need to configure the IP routing. IP routing is the process which allows router to route the packet between different networks.

Configure static routing in R1

R1(config)#ip route 200.0.0.0 255.255.255.0 100.0.0.2

Configure static routing in R2

R2(config)#ip route 50.0.0.0 255.0.0.0 100.0.0.1

Testing Dynamic NAT Configuration

We configured dynamic NAT on R1for 10.0.0.10 and 10.0.0.20 and static NAT on R2 for 192.168.1.10.

Device	Inside Local IP address	Inside Global IP address
Laptop0	10.0.0.10	50.0.0.10
Laptop1	10.0.0.20	50.0.0.2
Server	192.168.1.10	200.0.0.10

To test this setup click Laptop0 and Desktop and click Command Prompt.

Run ipconfig command.

Run ping 200.0.0.10 command.

Run ping 192.168.1.10 command.

```
C:\>ping 200.0.0.10

Pinging 200.0.0.10 with 32 bytes of data:

Request timed out.
Reply from 200.0.0.10: bytes=32 time=17ms TTL=126
Reply from 200.0.0.10: bytes=32 time=1ms TTL=126
Reply from 200.0.0.10: bytes=32 time=13ms TTL=126

Ping statistics for 200.0.0.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 17ms, Average = 10ms

C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
R1#show ip access-lists 1
Standard IP access list 1
    permit host 10.0.0.10
    permit host 10.0.0.20
    deny any
```

Basically it is access list which filters the traffic. NAT does not filter any traffic it only translate the address.

NAT translation on router R2.

```
R2#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
---  200.0.0.10        192.168.1.10       ---                ---
```

RESULT:

Thus, created an access list of IP addresses which need translation, created a pool of available IP address, mapping access list with pool is done successfully and the dynamic NAT is configured in cisco packet tracer.