Experiment - 4

Date: 6/8/25

Configure Dynamic NAT in Cisco Packet Tracer

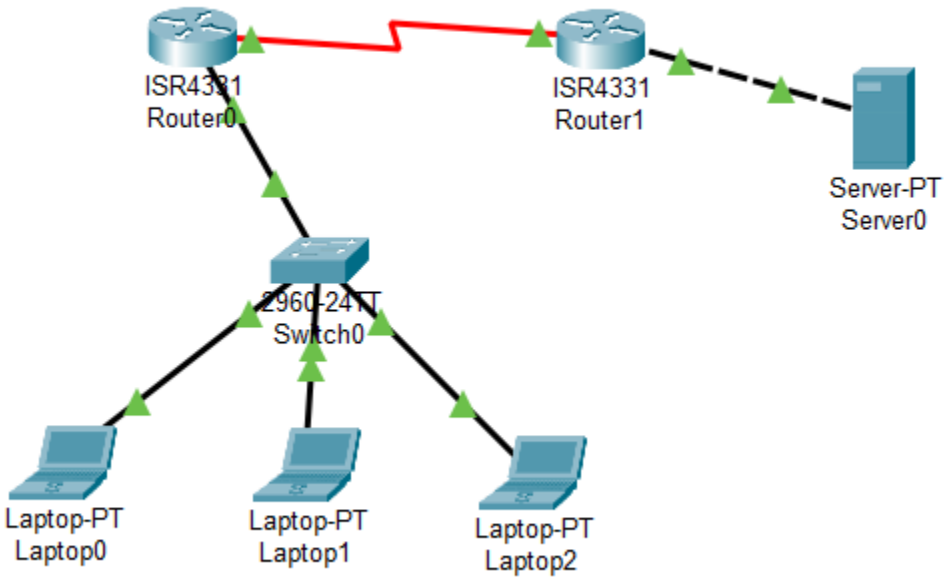
Aim:

To configure Dynamic Network Address Translation (NAT) in Cisco Packet Tracer and verify the translation of private IP addresses into public IP addresses for internet access.

Procedure:

1. Step-1: Build the network topology in Cisco Packet Tracer with at least 3 PCs, one Router, and one Server/Cloud.
2. Step-2: Assign IP addresses to all PCs in the private range (e.g., 192.168.1.0/24).
3. Step-3: Assign IP addresses to router interfaces – one in the LAN side and another in the public side.
4. Step-4: Configure a pool of public IP addresses on the router to be used for Dynamic NAT.
   Commands:
   Router> enable
   Router# configure terminal
   Router(config)# ip nat pool MYPOOL 200.0.0.10 200.0.0.20 netmask 255.255.255.0
5. Step-5: Define an access control list (ACL) to permit the private IP range for NAT translation.
   Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
6. Step-6: Bind the ACL to the NAT pool.
   Router(config)# ip nat inside source list 1 pool MYPOOL
7. Step-7: Configure router interfaces for NAT roles:
   Router(config)# interface fa0/0
   Router(config-if)# ip nat inside
   Router(config-if)# exit
   Router(config)# interface fa0/1
   Router(config-if)# ip nat outside
   Router(config-if)# exit
8. Step-8: Save configuration using the command:
   Router# write memory
9. Step-9: Test connectivity.
   From PC1, PC2, and PC3 ping the Server (public IP).
10. Step-10: Verify NAT operation.
    Router# show ip nat translations
    Router# show running-config

Output:



After performing the configuration, the PCs in the private network were able to access the public network.

The following outputs were observed:
1. Successful ping replies from PCs to the public server.
2. 'show ip nat translations' displayed the dynamic mapping of private IP addresses to public IP addresses.
3. 'show running-config' verified the NAT pool and access-list configuration.

Sample output of 'show ip nat translations':

Pro	Inside global	Inside local	Outside local	Outside global
icmp	200.0.0.10:2	192.168.1.10:2	200.0.0.100:2	200.0.0.100:2
icmp	200.0.0.11:3	192.168.1.11:3	200.0.0.100:3	200.0.0.100:3

Result:

Thus, Dynamic NAT was successfully configured on the router. Multiple private IP addresses were translated to a pool of public IPs, allowing secure communication between the internal network and external network.