Experiment 4: Configure Dynamic NAT in Cisco Packet Tracer

Date: 6/8/25

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: Network Topology Setup**
   Construct the network topology in Cisco Packet Tracer, including at least three PCs, one router, and one server/cloud.
2. **Step 2: Private IP Addressing**
   Assign IP addresses to all PCs within the private range (e.g., 192.168.1.0/24).
3. **Step 3: Router Interface IP Addressing**
   Assign IP addresses to the router interfaces: one for the LAN side and one for the public side.

Step 4: Dynamic NAT Pool Configuration
Configure a pool of public IP addresses on the router for Dynamic NAT.

Commands:
Router> enable
Router# configure terminal

4. Router(config)# ip nat pool MYPOOL 200.0.0.10 200.0.0.20 netmask 255.255.255.0
5. **Step 5: Access Control List (ACL) Definition**
   Define an access control list (ACL) to permit the private IP range for NAT translation.

   Command:
   Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
6. **Step 6: ACL to NAT Pool Binding**
   Bind the configured ACL to the NAT pool.

   Command:
   Router(config)# ip nat inside source list 1 pool MYPOOL

Step 7: Router Interface NAT Role Configuration
Configure the router interfaces to assume their respective NAT roles (inside and outside).

Commands:
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

7. Router(config-if)# exit

8. **Step 8: Save Configuration**
   Save the current configuration using the command:

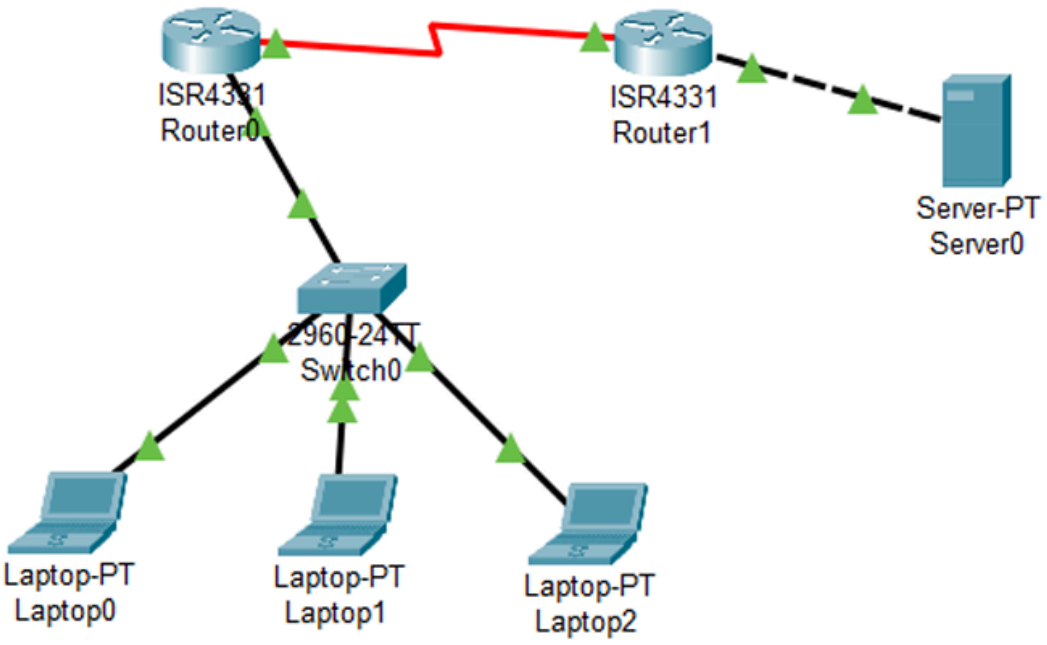
   Command:
   Router# write memory
9. **Step 9: Connectivity Test**
   Test connectivity by pinging the public server from PC1, PC2, and PC3.

Step 10: NAT Operation Verification
Verify the NAT operation using the following commands:

Commands:
Router# show ip nat translations

10. Router# show running-config

Output:

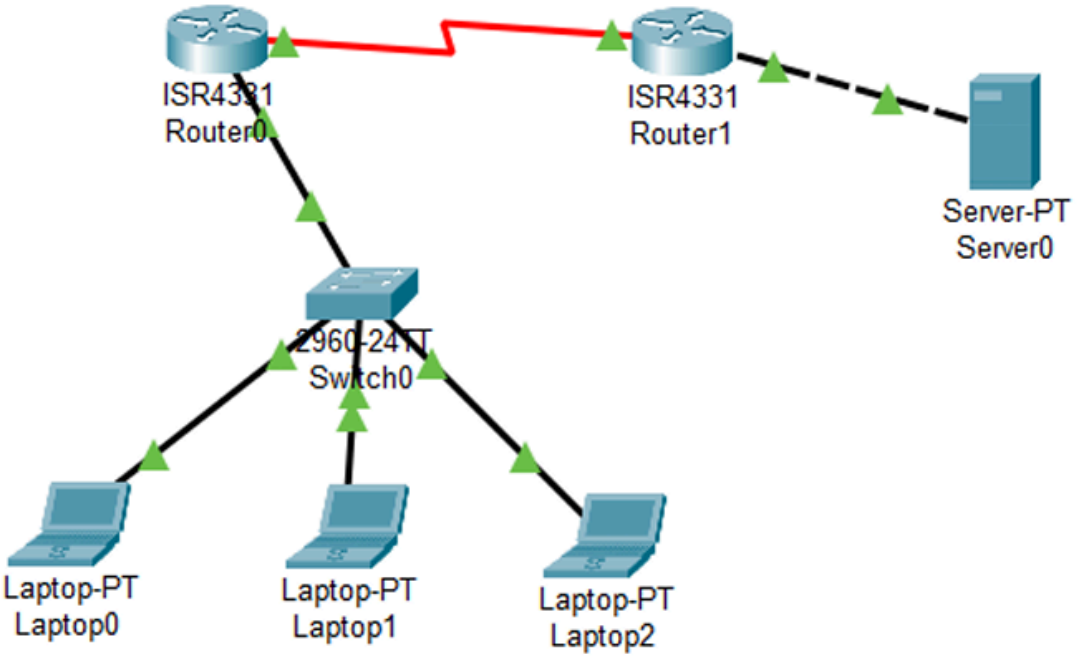


Following the configuration, the PCs within the private network successfully accessed the public network. The following observations were made:

1. Successful ping replies were received from the PCs to the public server.
2. The `show ip nat translations` command displayed the dynamic mapping of private IP addresses to public IP addresses.
3. The `show running-config` command confirmed the NAT pool and access-list configurations.

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:

Dynamic NAT was successfully configured on the router. This allowed multiple private IP addresses to be translated to a pool of public IPs, enabling secure communication between the internal and external networks.