P.HARINI
SEC 7
2300033404

NPS-LAB EXPERIMENT-9

Configuration of Network address translation in Cisco packet tracer and verify the configuration.

1. Network Setup (Assume the setup has a router with two interfaces):

- Inside Network (e.g., 192.168.1.0/24 on GigabitEthernet0/0)
- Outside Network (connected to ISP or another router with public IP, e.g., 203.0.113.1/30 on GigabitEthernet0/1)

2. Configure NAT on the Router

1. Access the Router CLI:
    - Click the router, go to the CLI tab.
2. Enter Global Configuration Mode:

    enable
    configure terminal

3. Assign IP Addresses to Interfaces:
    - Inside Interface (connected to the LAN):

        interface GigabitEthernet0/0
        ip address 192.168.1.1 255.255.255.0
        ip nat inside
        no shutdown
        exit

    - Outside Interface (connected to ISP or another router with a public IP):

        interface GigabitEthernet0/1
        ip address 203.0.113.2 255.255.255.252
        ip nat outside

no shutdown
exit

4. Configure an Access Control List (ACL):
   - This defines the private IP range to be translated.

   access-list 1 permit 192.168.1.0 0.0.0.255

5. Configure NAT Overload (PAT):
   - Use the outside interface's IP address for NAT overload.

   ip nat inside source list 1 interface GigabitEthernet0/1 overload

6. Exit to Save:

   exit

3. Verify NAT Configuration

1. View NAT Translations:
   - Ping a device in the outside network (e.g., ISP router's IP).
   - Check active NAT translations.

   show ip nat translations

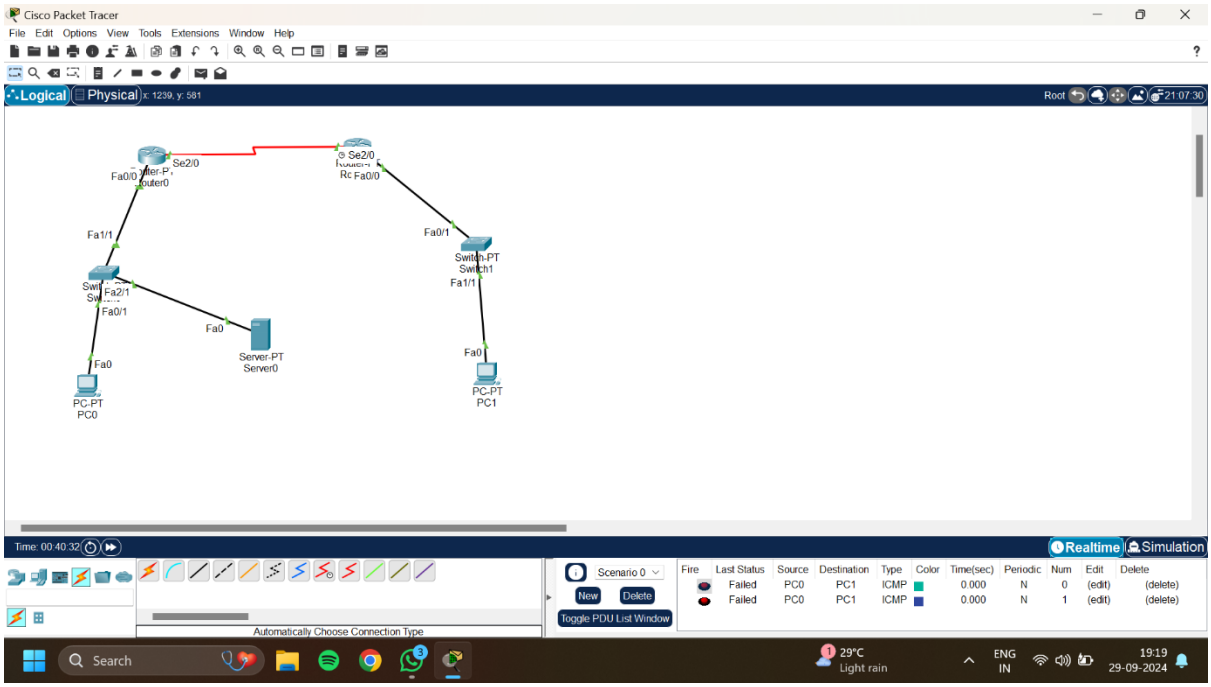
2. Verify NAT Statistics:

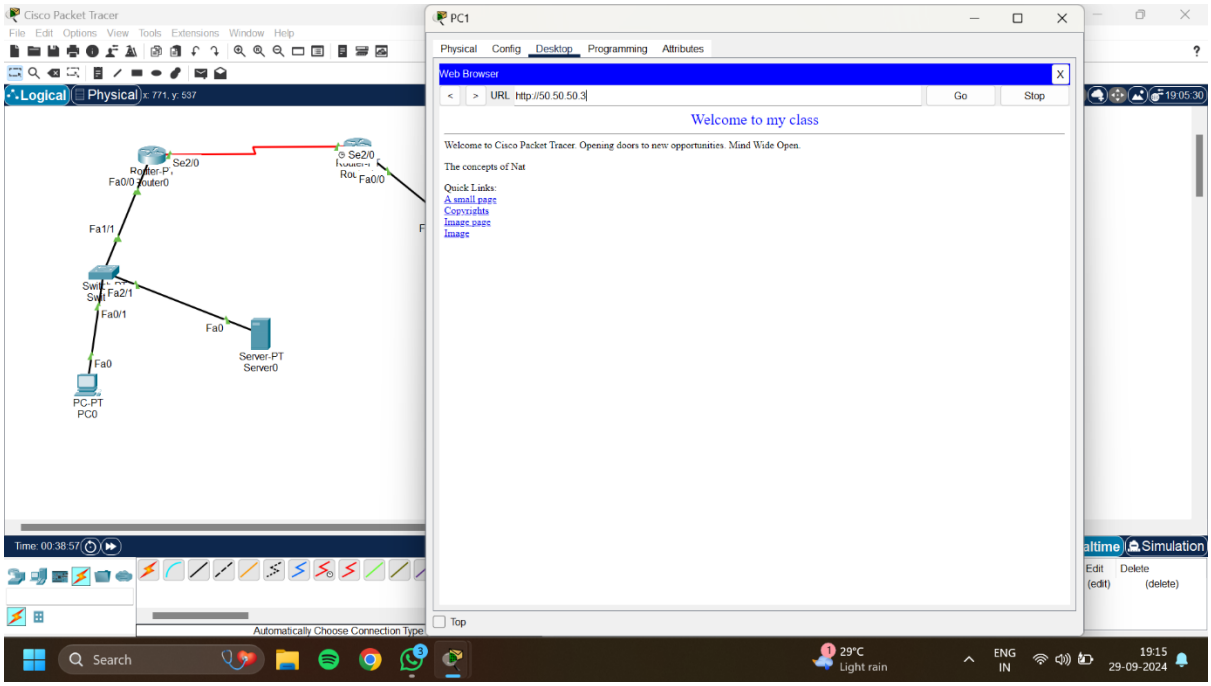
   show ip nat statistics

3. Test Connectivity with Ping:
   - On a PC in the inside network, ping an outside address (e.g., ping 8.8.8.8).
   - Successful replies indicate NAT is working.

Each ping test from the internal network should show active NAT translations and confirm successful NAT configuration.

P.HARINI
SEC 7
2300033404





P.HARINI
SEC 7
2300033404