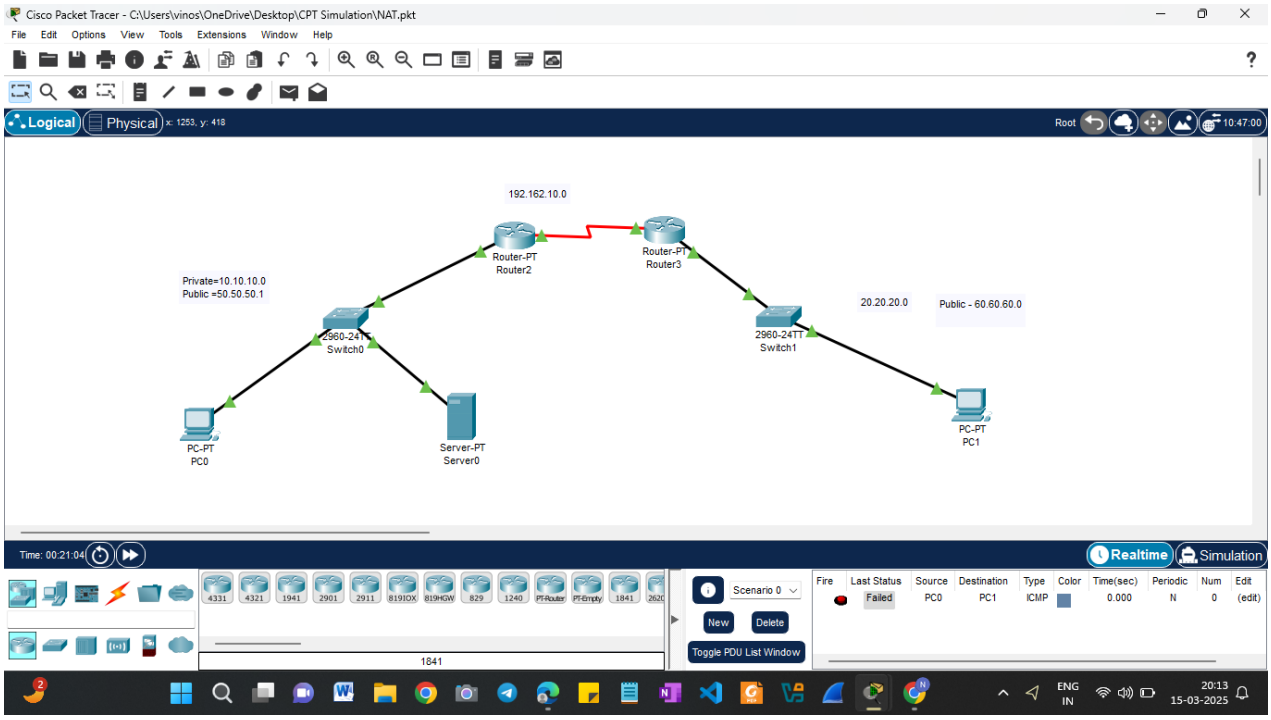
Q7) In Cisco Packet Tracer, create a small network with multiple devices (e.g., 2 PCs and a router). Use private IP addresses (e.g., 192.168.1.x) on the PCs and configure the router to perform NAT to allow the PCs to access the internet.

Task: Test the NAT configuration by pinging an external IP address from the PCs and capture the traffic using Wireshark.

What is the source IP address before and after NAT?



- **Before NAT:** The PC uses **192.168.1.10**, which is a private IP, and cannot be routed on the internet.
- **After NAT:** The router translates this private IP to its **public IP (203.0.113.1)** before forwarding the packet to the destination.
- **Return Traffic:** When the reply comes from **8.8.8.8**, the router reverses the NAT translation and sends the packet back to **192.168.1.10**.
- **NAT Overload (PAT)** ensures multiple internal devices can share the same public IP by tracking sessions using port numbers.