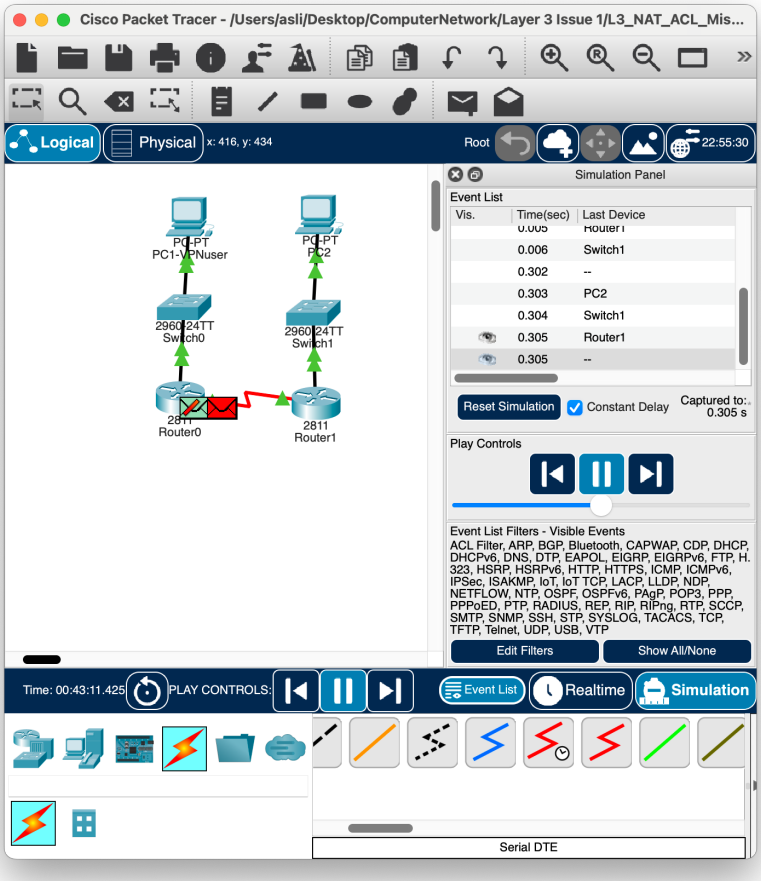
L3 - VPN Lobby Join Failure Due to NAT and Port Forwarding Restrictions Explanation

A developer working on a host-client multiplayer game reported the following issue: when one of the players connects to the game using a VPN, the other players cannot join the lobby. This situation is typically caused by NAT restrictions and lack of port forwarding on the VPN user's network. Although all users are authenticated and technically connected to the internet, only the host cannot receive incoming connections from peers.



Connection Attempt:

Player 1 (with VPN) hosts the lobby → success

Player 2 attempts to join → connection times out

Ping and telnet to the VPN host fail, even though the host's IP is assigned correctly

After simulating the scenario in Cisco Packet Tracer, it was observed that Router1 (the NAT router behind VPN) did not allow incoming packets to reach the internal host (PC1) due to missing port forwarding rules.

Troubleshooting Steps:

- Confirmed PC1 (VPN host) had IP 192.168.10.10
- Confirmed PC2 (client) tried to access 10.0.0.1:7777 (Router1's external IP)

- Added static port forwarding (PAT) on Router1 to map UDP & TCP 7777 to internal PC1
- Verified ACL permissions to allow external traffic on 7777
- Re-tested connection using telnet 10.0.0.1 7777

The issue lies strictly within OSI Layer 3 – Network Layer, as NAT, PAT, and ACL configurations determine packet forwarding rules across subnets. Even when all IP-level configurations are correct, communication fails if NAT blocks or misroutes the traffic.