### Implement ACLs to restrict traffic based on source and destination ports. Test rules by simulating legitimate and unauthorized traffic.

* Configure a standard Access Control List (ACL) on a router to permit traffic from a specific IP range. Test connectivity to verify the ACL is working as intended.

### Create an extended ACL to block specific applications, such as HTTP or FTP traffic. Test the ACL rules by attempting to access blocked services.

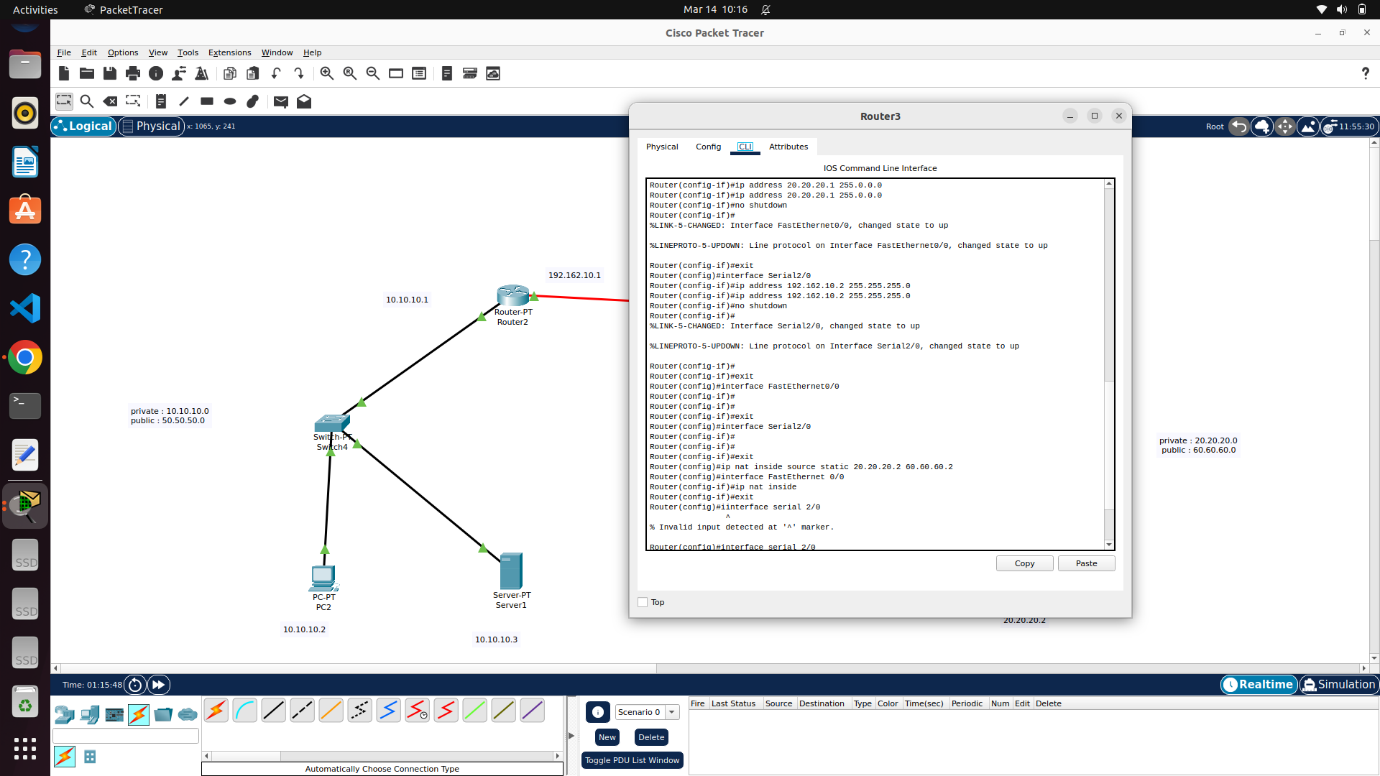
### Try Static NAT, Dynamic NAT and PAT to translate IPs.

STATIC NAT IMPLEMENTATION IN CISCO PACKET TRACER :

Two different networks are made to communicate with each other in this setup:

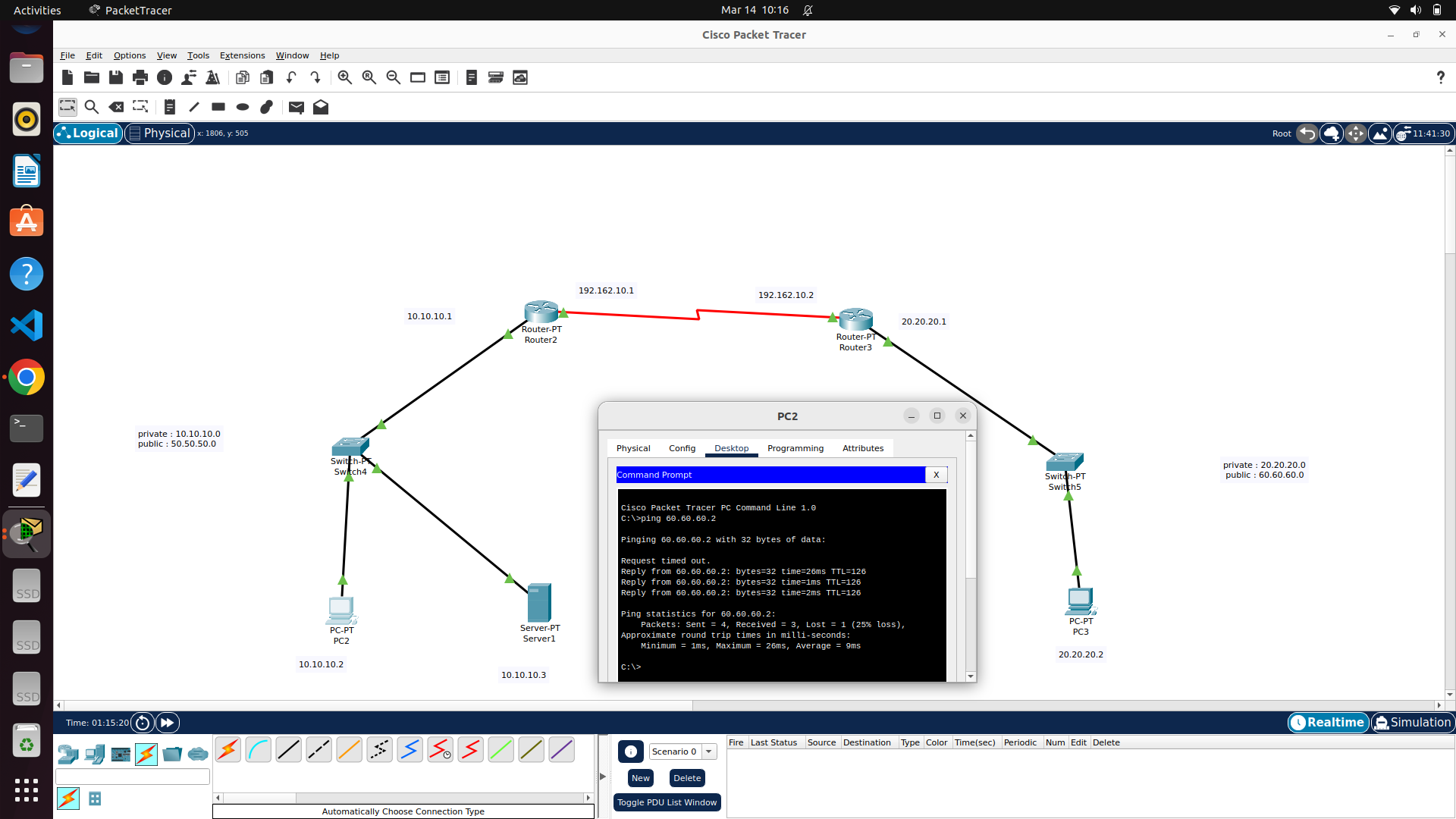
1. Private network with network address – 10.10.10.0/8 with PC of IP – 10.10.10.2/8 and Server of IP – 10.10.10.3/8 [this network is translated to 50.50.50.0/8 by NAT accordingly PC will be represented as 50.50.50.2/8 and Server as 50.50.50.3/8]

Sample router configuration is shown below with constructed network.



(Here, in right side network, consisting of single PC, though 20.20.20.0/8 is not coming under private IP, just for security reasons or to isolate, it also got translated to other public IP – 60.60.60.0/8)

**RESULT :**

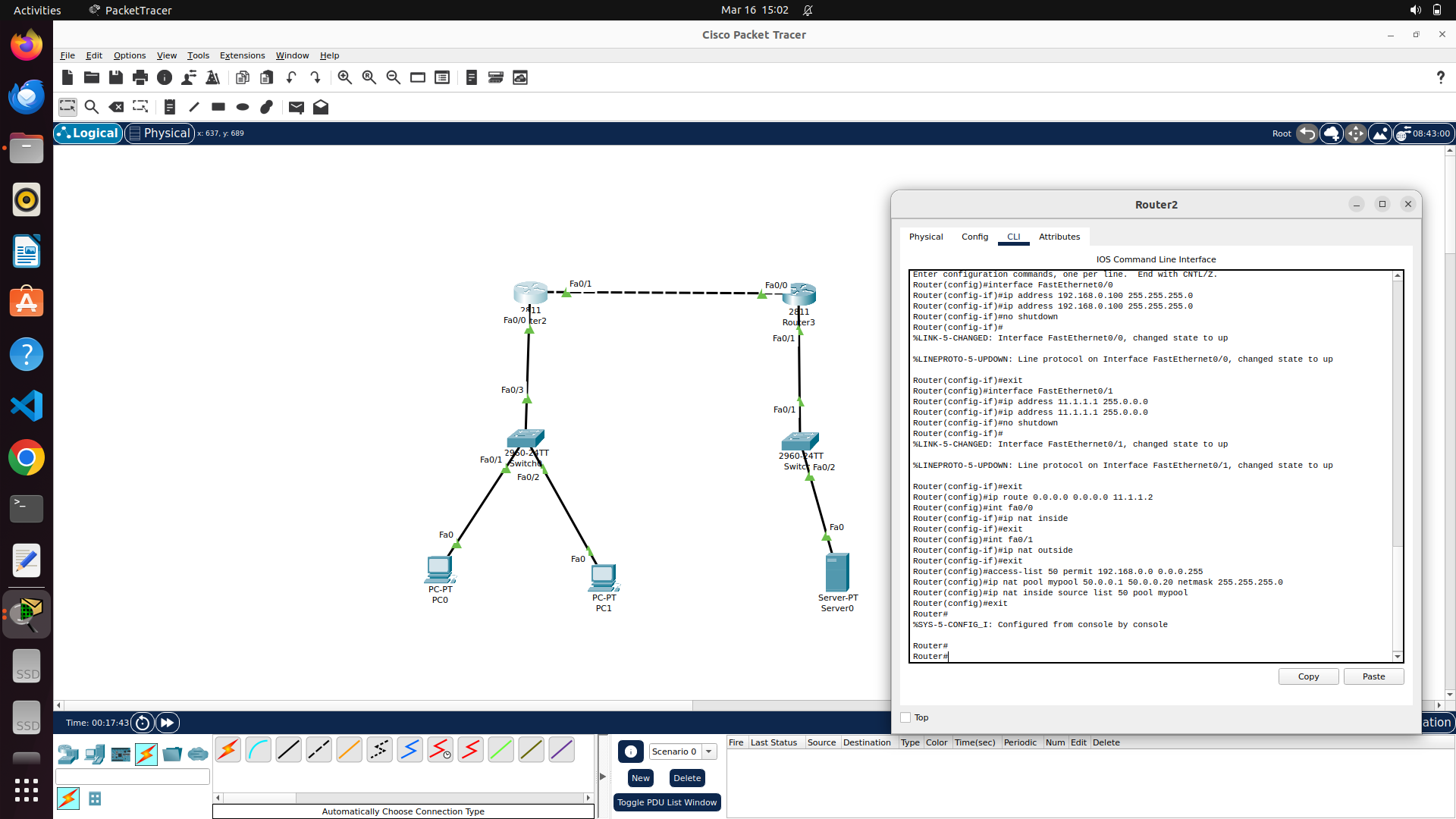


DYNAMIC NAT DEMONSTRATION :

The below image has a private network (192.168.0.0/24) with two PC’s (pc0- 192.168.0.2 and pc1 – 192.168.0.3/24) connected to switch and a router 2 here manages this private network and acts as default gateway with IP 192.168.0.1/24

Router 2 also gets connected with router 3 (default gateway for public network with server) via 11.1.1.0/30 network.

Server is configured with IP – 200.0.0.1/24 (public IP) via switch in 200.0.0.0/24 network to router3



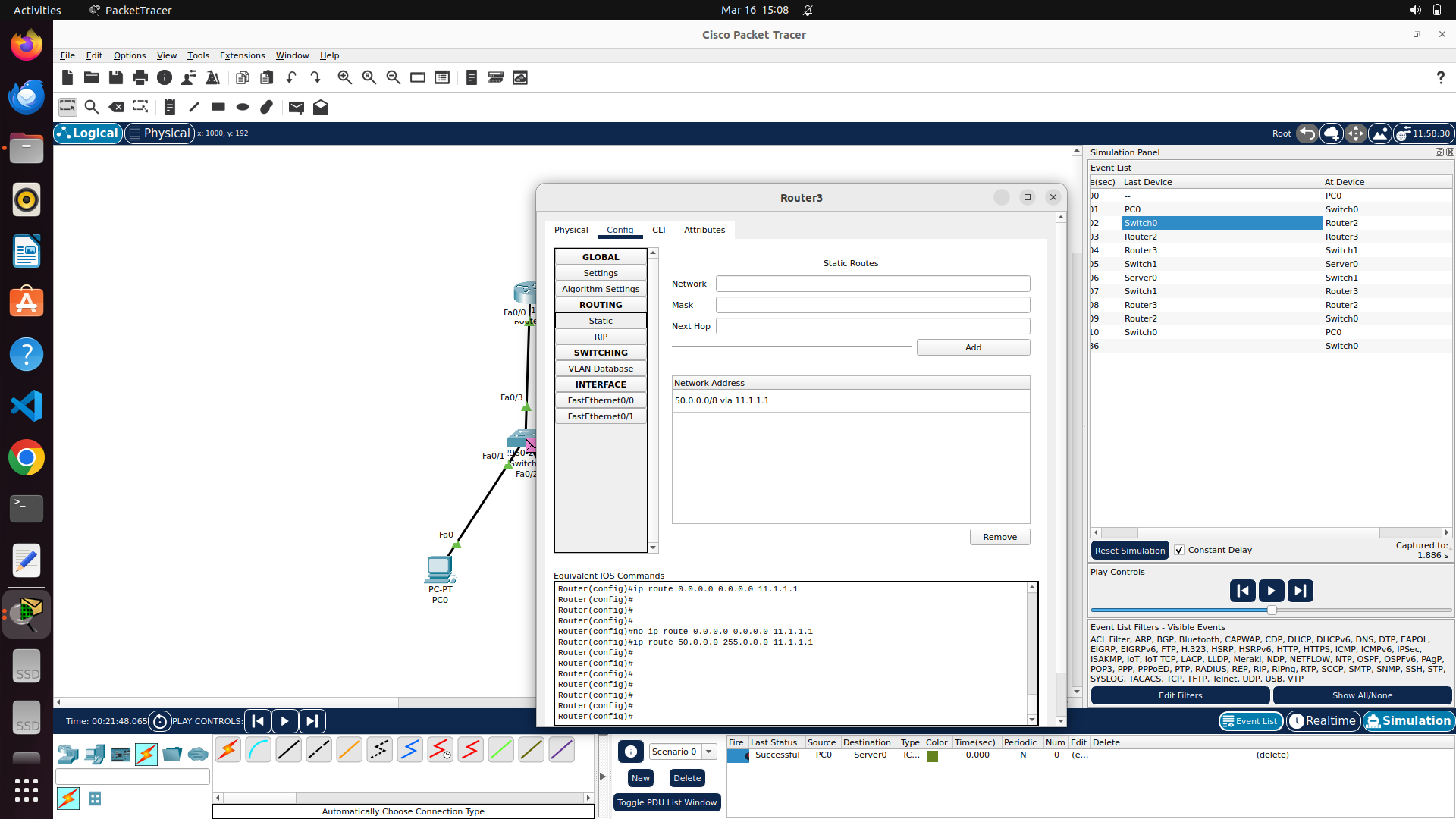
Here, after defining (assigning IP, subnet mask and turning it UP) router’s interface (router-2), each interface should be specified whether it is inside or outside the private network.

For the private network (marked “inside NAT”) is here defined with pool of IP (named mypool in picture above) with subnet mask for router to pick one dynamically. -> concept of Dynamic NAT

Here, simple (standard) ACL is applied (can be identified by its ACL number between 0-99 here, 50) just to limit PC0 to have IP translation thus restricting PC1 in communicating with external network.

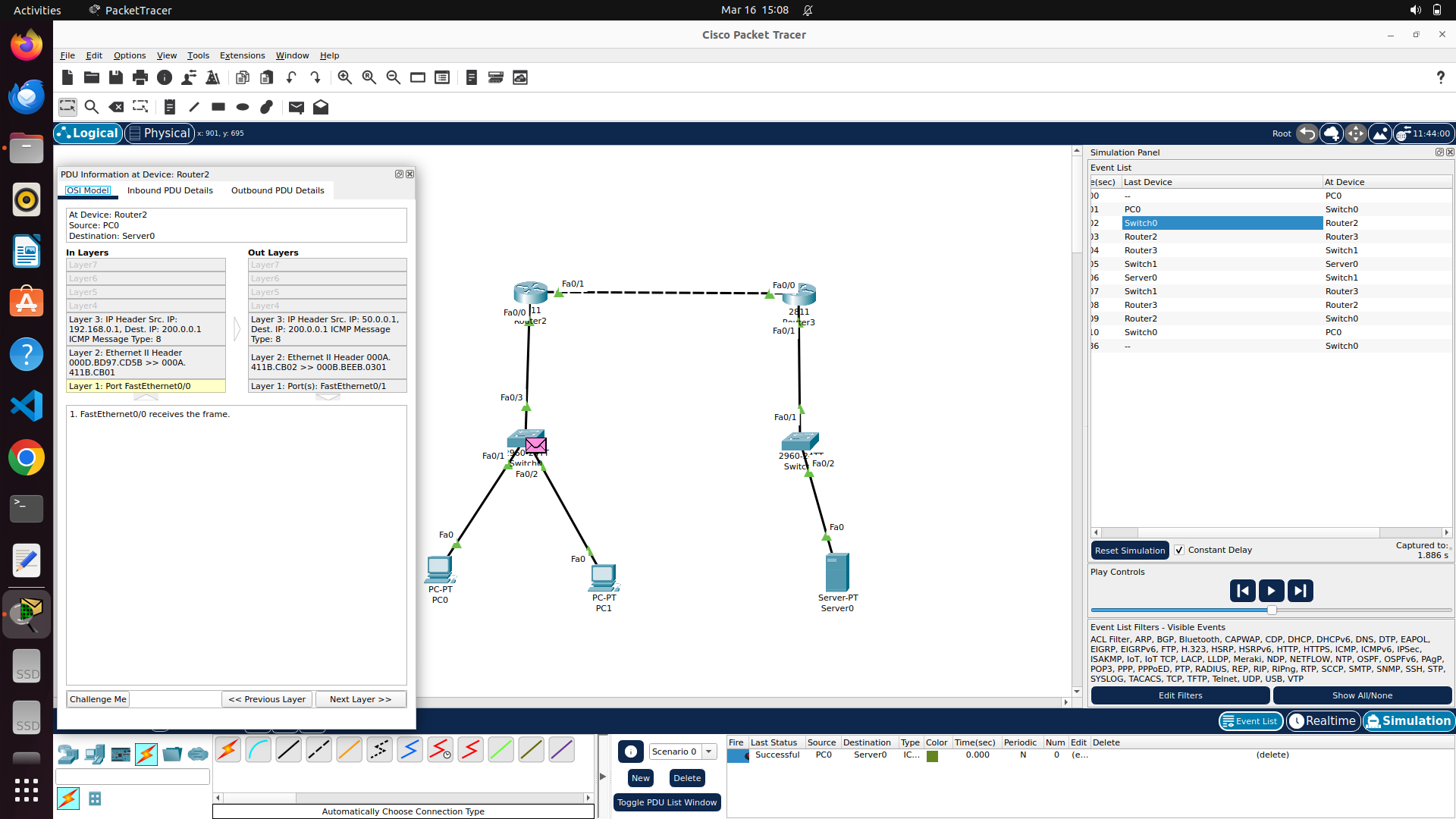
For routing table, here for router – 2 (governing private network) , is allowed for any traffic (actually , ping is the only traffic for this demonstration) to pass through router 3 (with server)

For router-3, routing table is configured as follows:

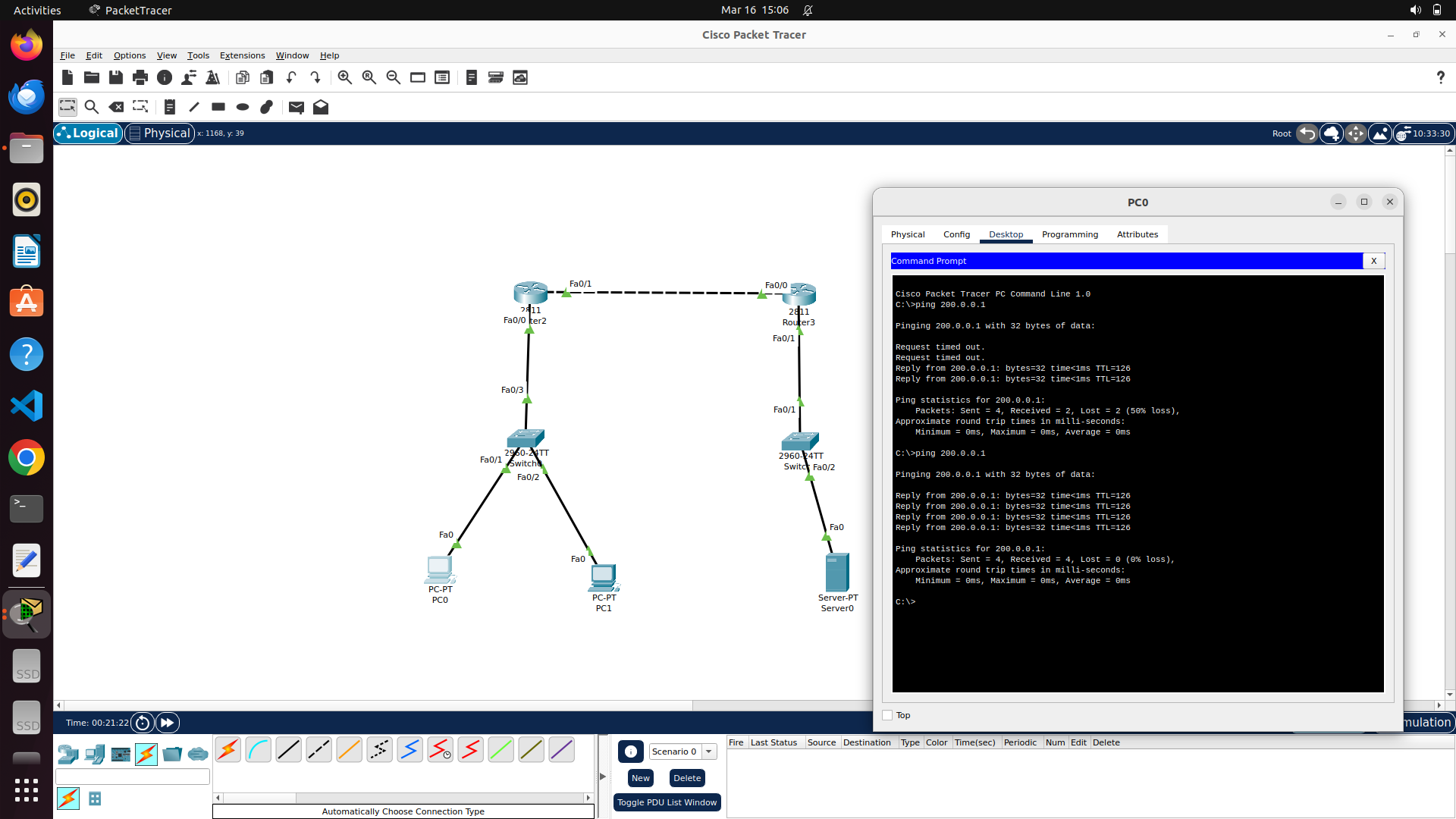


**RESULTS :**

In simulation mode, it is observed that, On router-2, NAT protocol worked which is evident in the left side panel, stating the packet arrived and dispatched to/from router-2 with change in source IP (edited by router as per NAT )

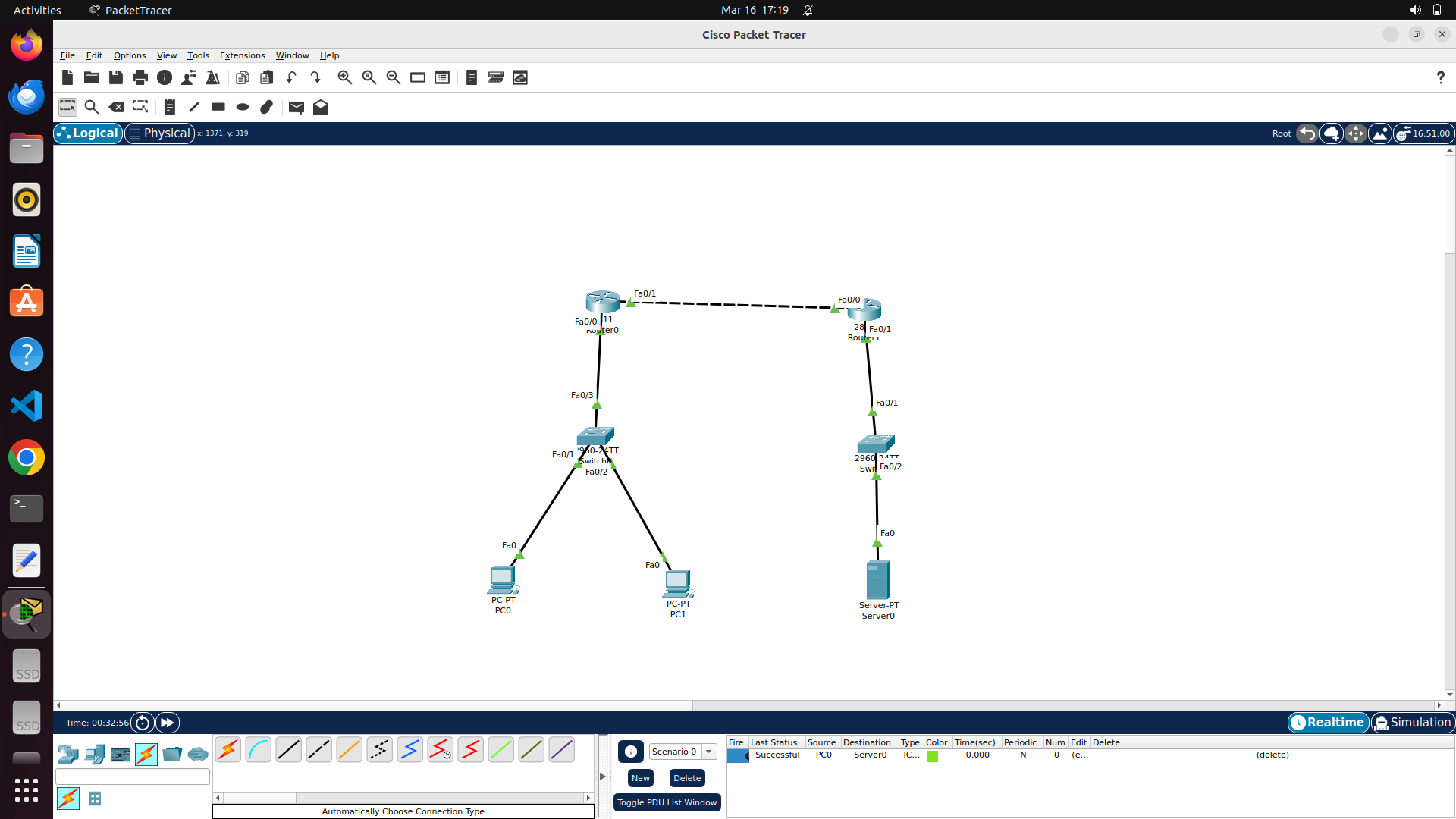


Here, PC0 was able to ping router-3 (200.0.0.1) -> default gateway of server.



DEMONSTRATION FOR PAT AND EXTENDED ACL IN CISCO PACKET TRACER :

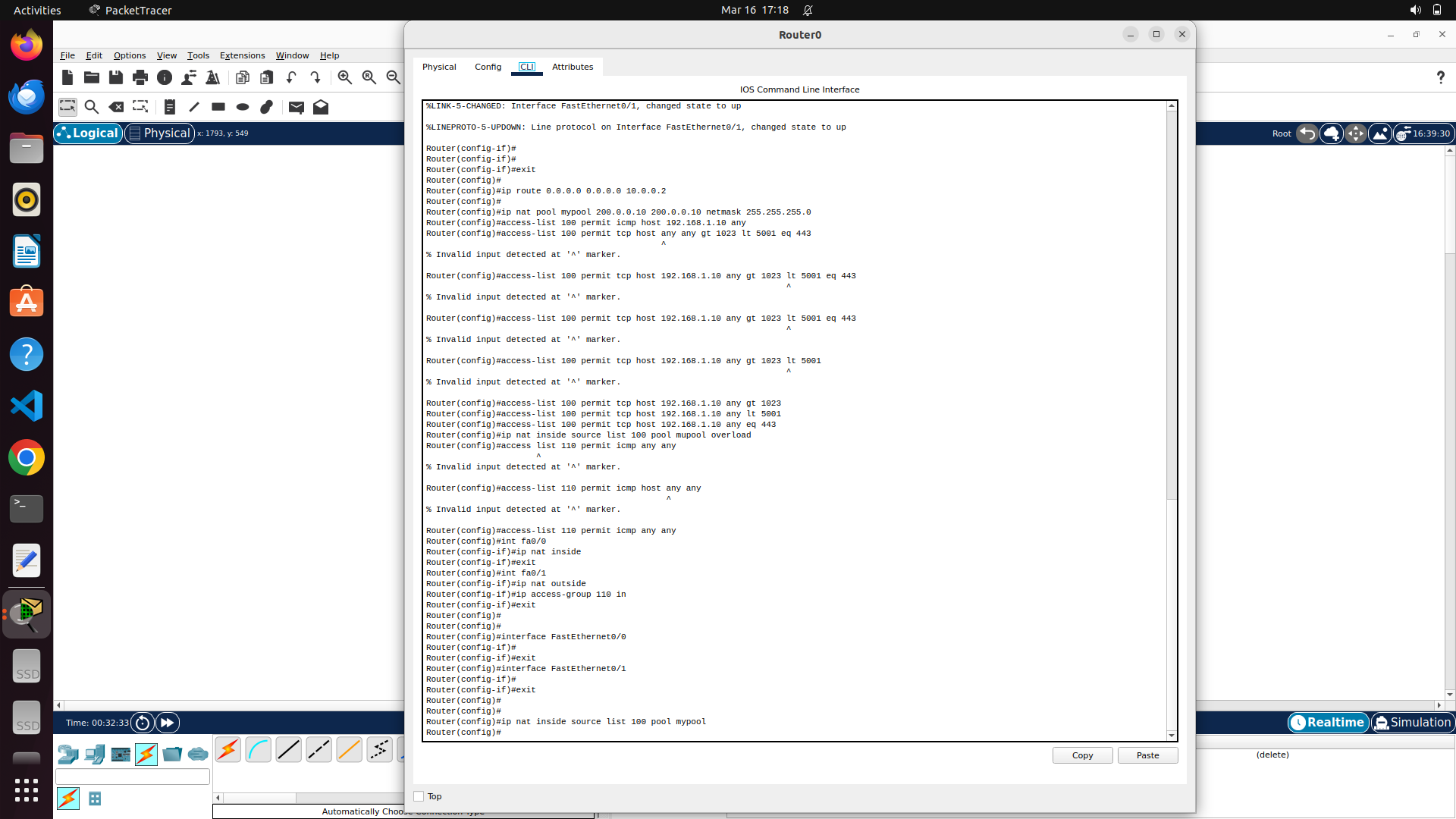
The following network is considered for this demonstration :



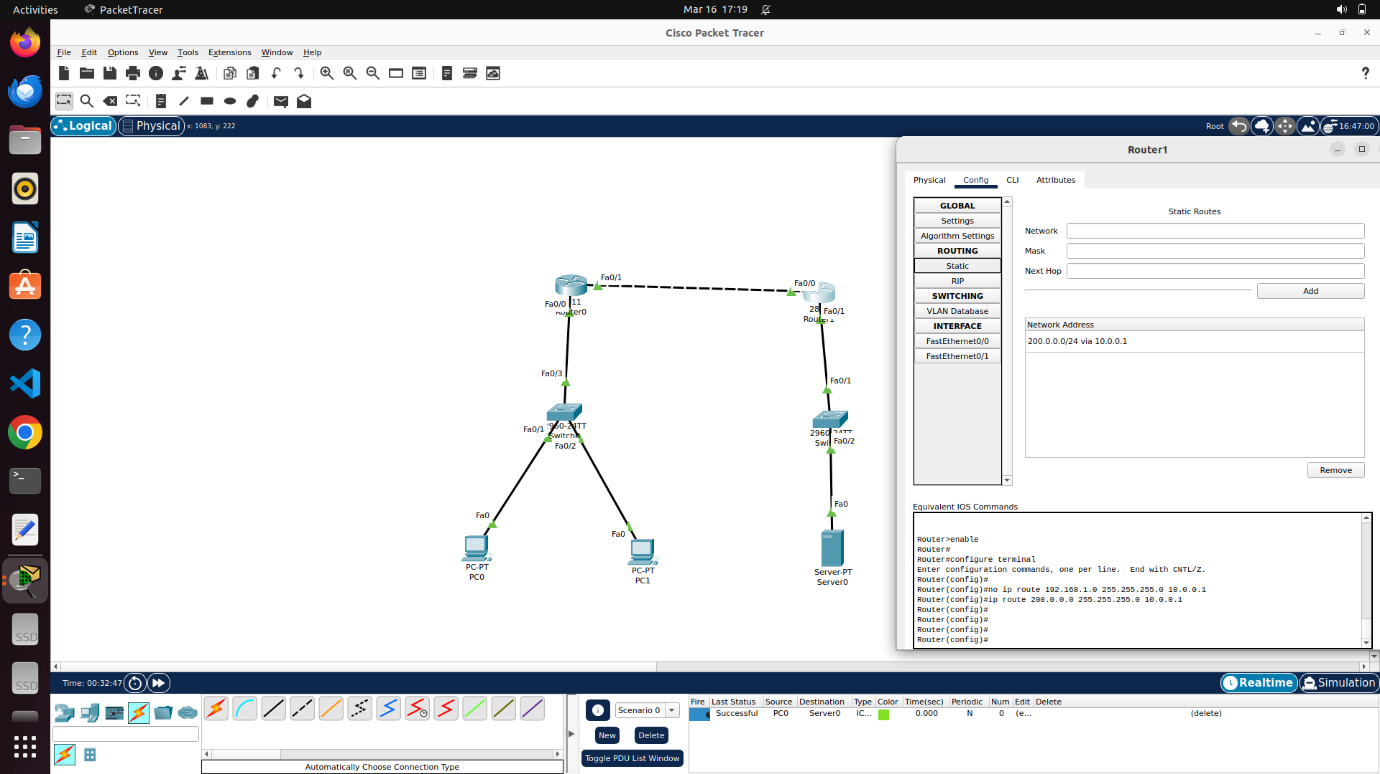
Here, 192.168.1.0/24 is taken as private network managed by router-0 in above image. 192.168.1.10/24 as IP for PC-0 and 192.168.1.20 as IP for PC-1 in private network.

Server is configured with IP – 193.0.0.2/24 with 193.0.0.0/24 as network ID .

Following image demonstrates the necessary configurations for router-0 to implement PAT with Extended ACL :

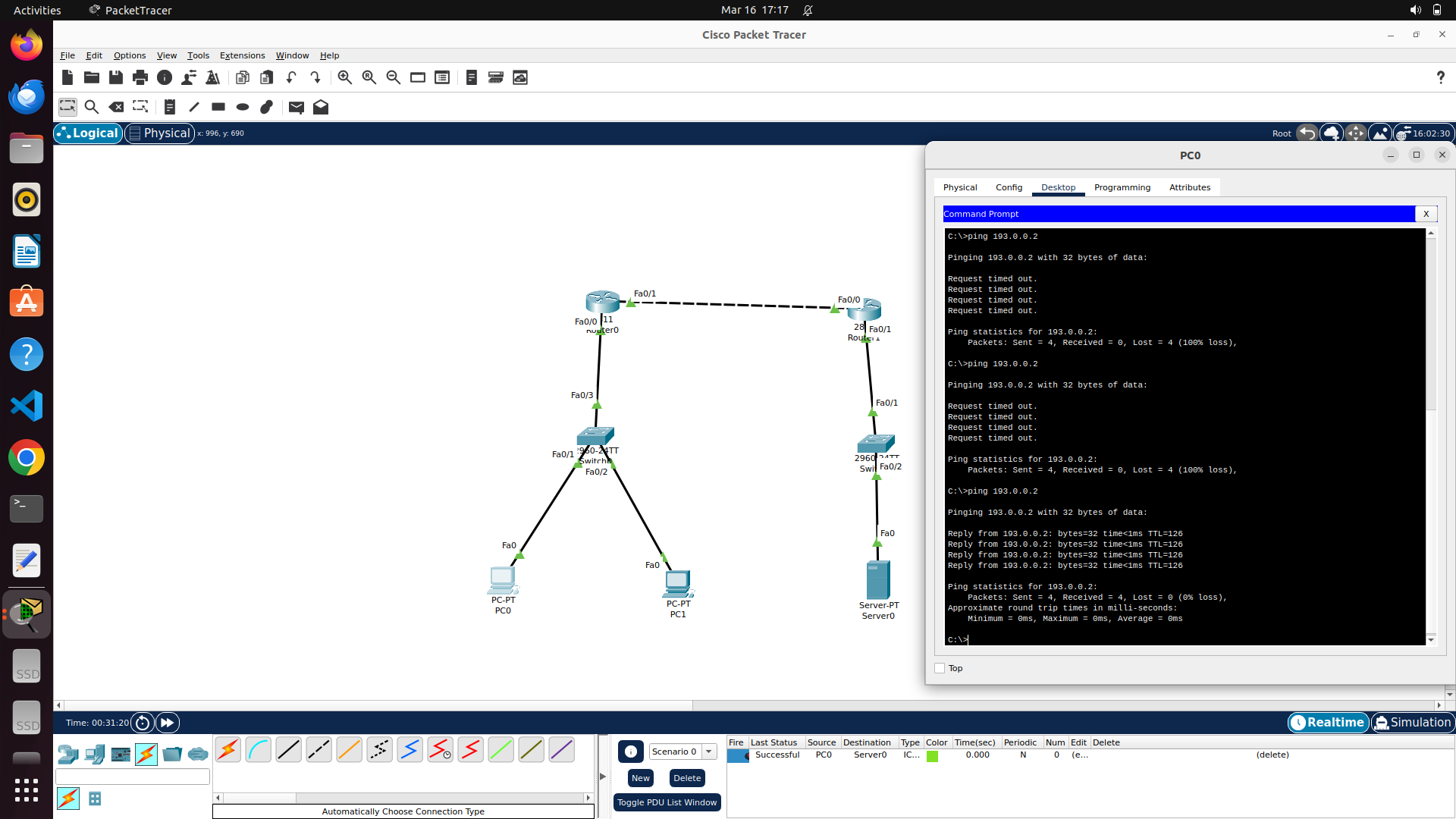


Following image shows the routing table of router-1 (with server) showing the public IP for network configured using pat in router-0



**RESULTS:**

Following image shows that PC-0 could ping the target server (as allowed in acl list rules)



Following image shows that PC-1 could not ping the target server as per acl rules (100):

