ACCESS CONTROL LIST :

1. An Access Control List (ACL) is a set of rules that controls traffic flow in a network by permitting or denying packets based on IP addresses, protocols, and port numbers. ACLs are used primarily in routers and firewalls to enforce security policies.
2. Stateless filtering examines each packet individually, without considering previous packets. It operates based on predefined rules such as source/destination IP, port, and protocol. Decisions are made only based on packet headers, not connection states.
3. Stateful filtering tracks active connections and remembers session states. It dynamically allows return traffic only for established connections. It makes decisions on packets based on previous conversations and selectively allow packets if not belonging to particular session unless explicitly permitted.
4. Types of ACL:

* Standard ACL -> filters only based on IP address (1-99 access list number range)
* Extended ACL -> filters based on multiple parameters: src/dest IP, protocol, port numbers.
* Dynamic ACL -> Grants temporary access based on authentication. It requires logging in.
* Reflexive ACL -> it is the stateful ACL implementation.
* Time based ACL -> Controls access based on time and date.

NAT – NETWORK ADDRESS TRANSLATION:

1. It is used to map private to public IP to enable devices using private IP access external network and vice-versa.
2. It is implemented in routers since it is the default gateway for private IP devices.
3. Operates on network layer and edits the packets before accessing external network.
4. There are three types of NAT possible :

* Static NAT – one to one mapping of unique private IP to unique public IP.
* Dynamic NAT – maintains pool of public IPs that router dynamically chooses from for private IP devices to get internet access.
* Port Address Translation – also called as NAT overload which uses essentially one public IP but distinguishes different private ip requests by allocating unique ports. It is more popular in modern day networking due to the conservation of public IPs.

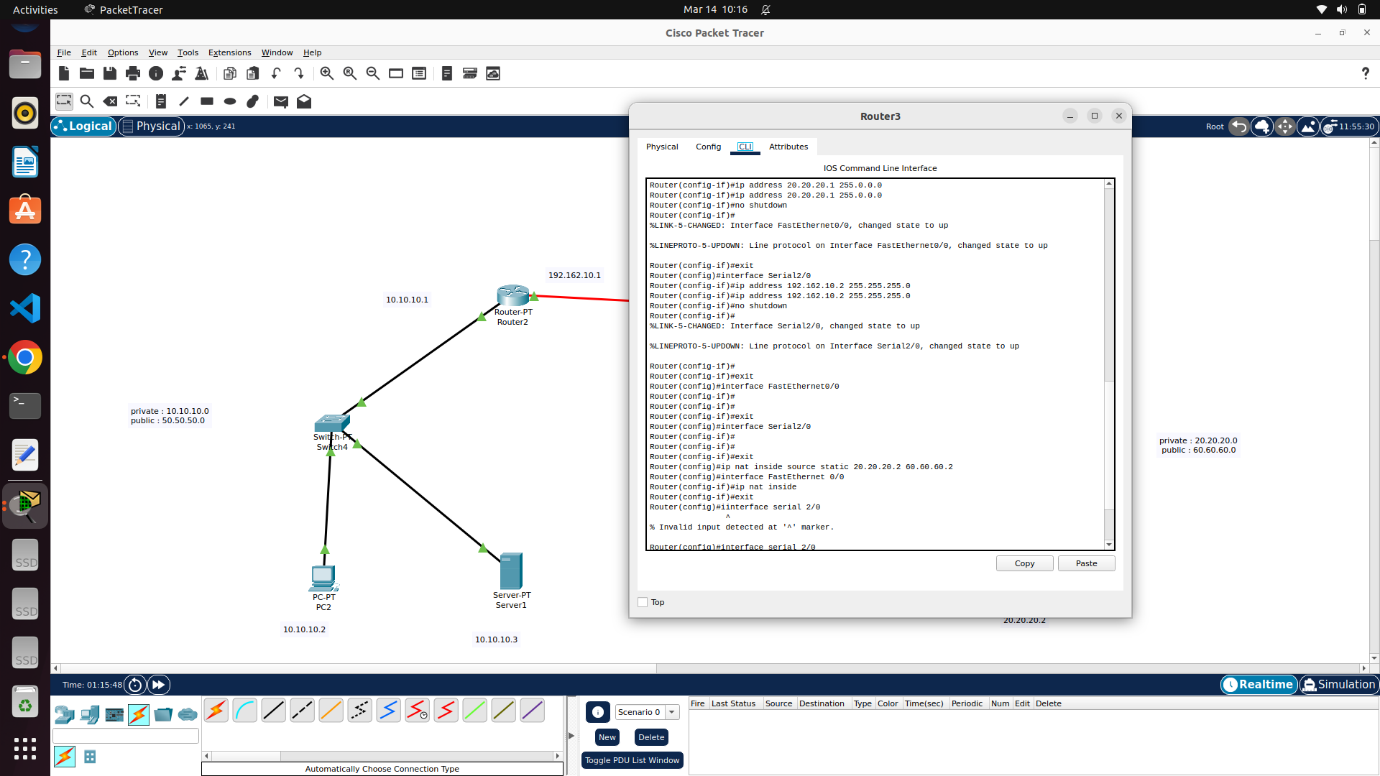
STATIC NAT IMPLEMENTATION IN CISCO PACKET TRACER :

SCENARIO CONSIDERED :

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

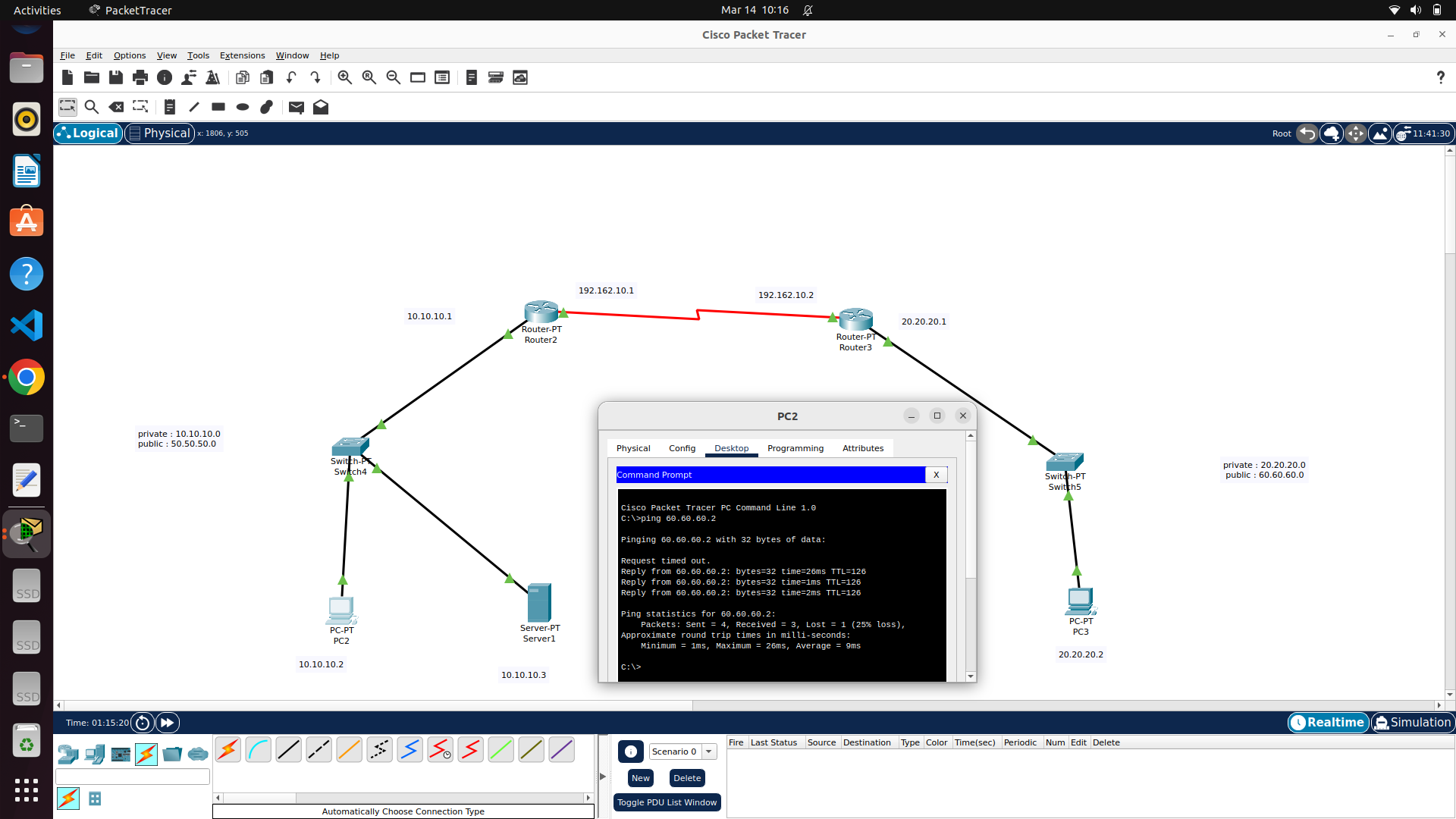
1. Private network with network address – 10.10.10.0/8 with PC of IP – 10.10.10.2/8 and Server of IP – 10.10.10.3/8 [this network is translated to 50.50.50.0/8 by NAT accordingly PC will be represented as 50.50.50.2/8 and Server as 50.50.50.3/8]

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 :

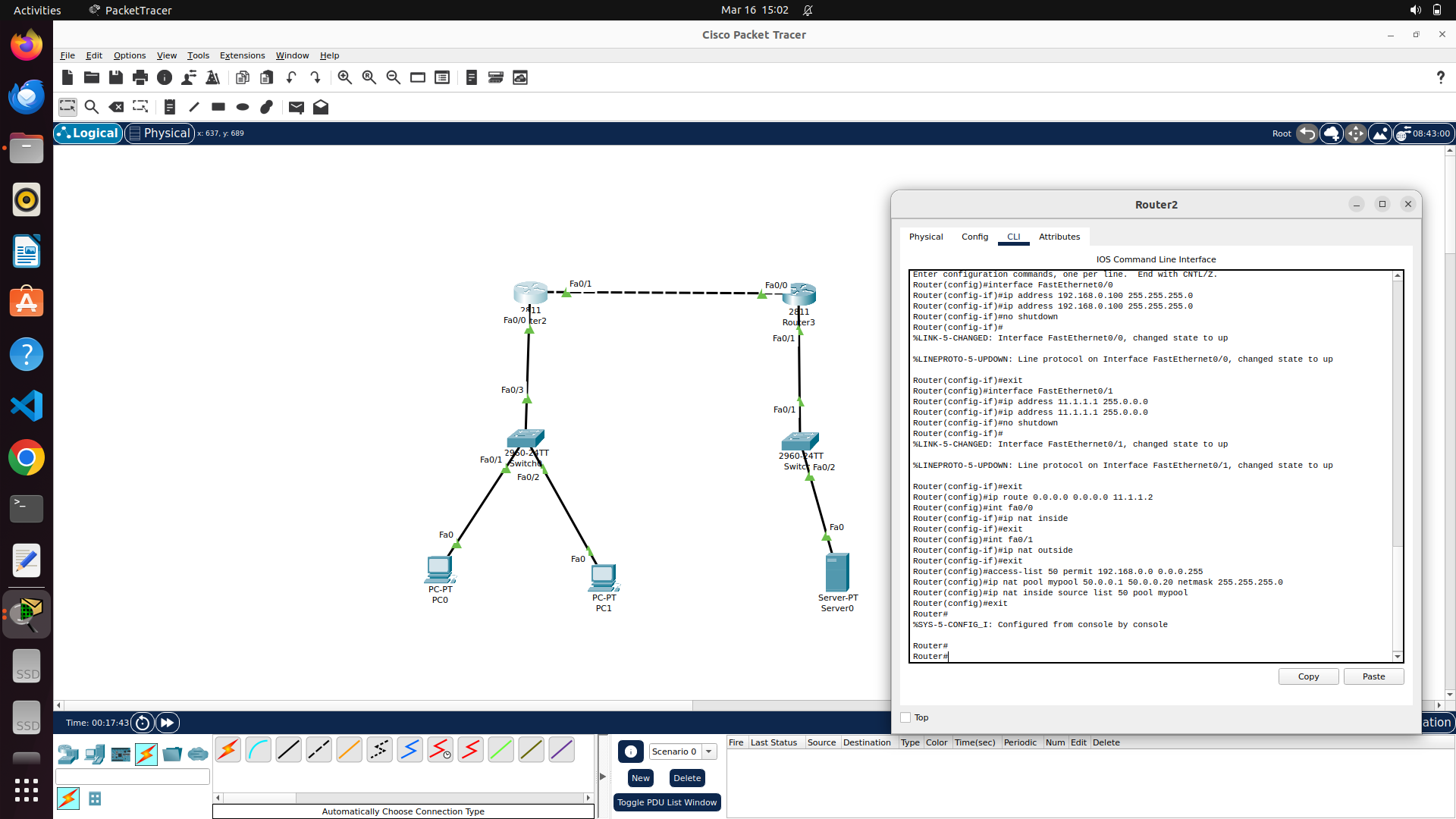


DYNAMIC NAT DEMONSTRATION :

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



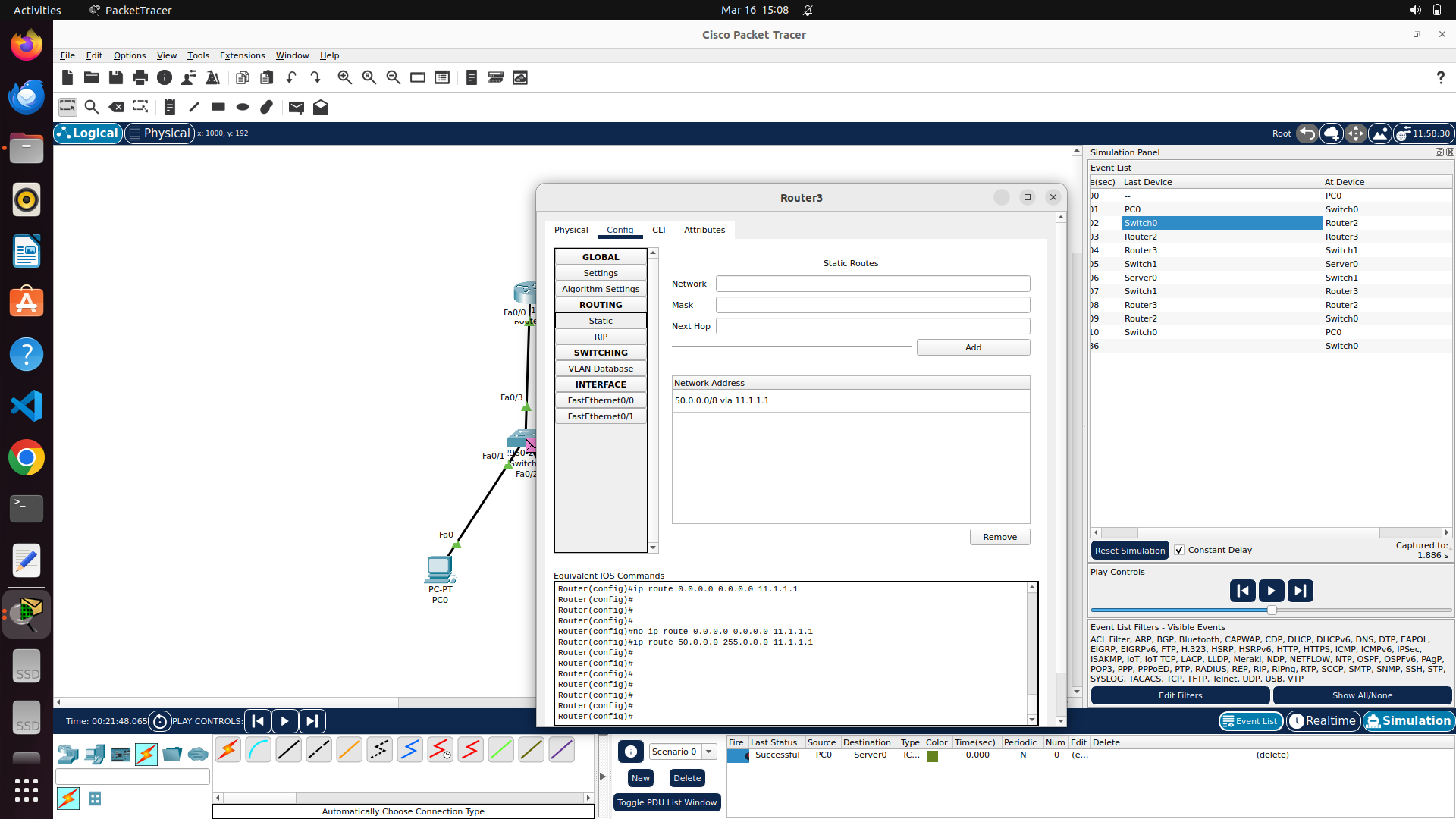
Here, after defining (assigning IP, subnet mask and turning it UP) router’s interface (router-2), each interface should be specified whether it is inside or outside the private network.

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.

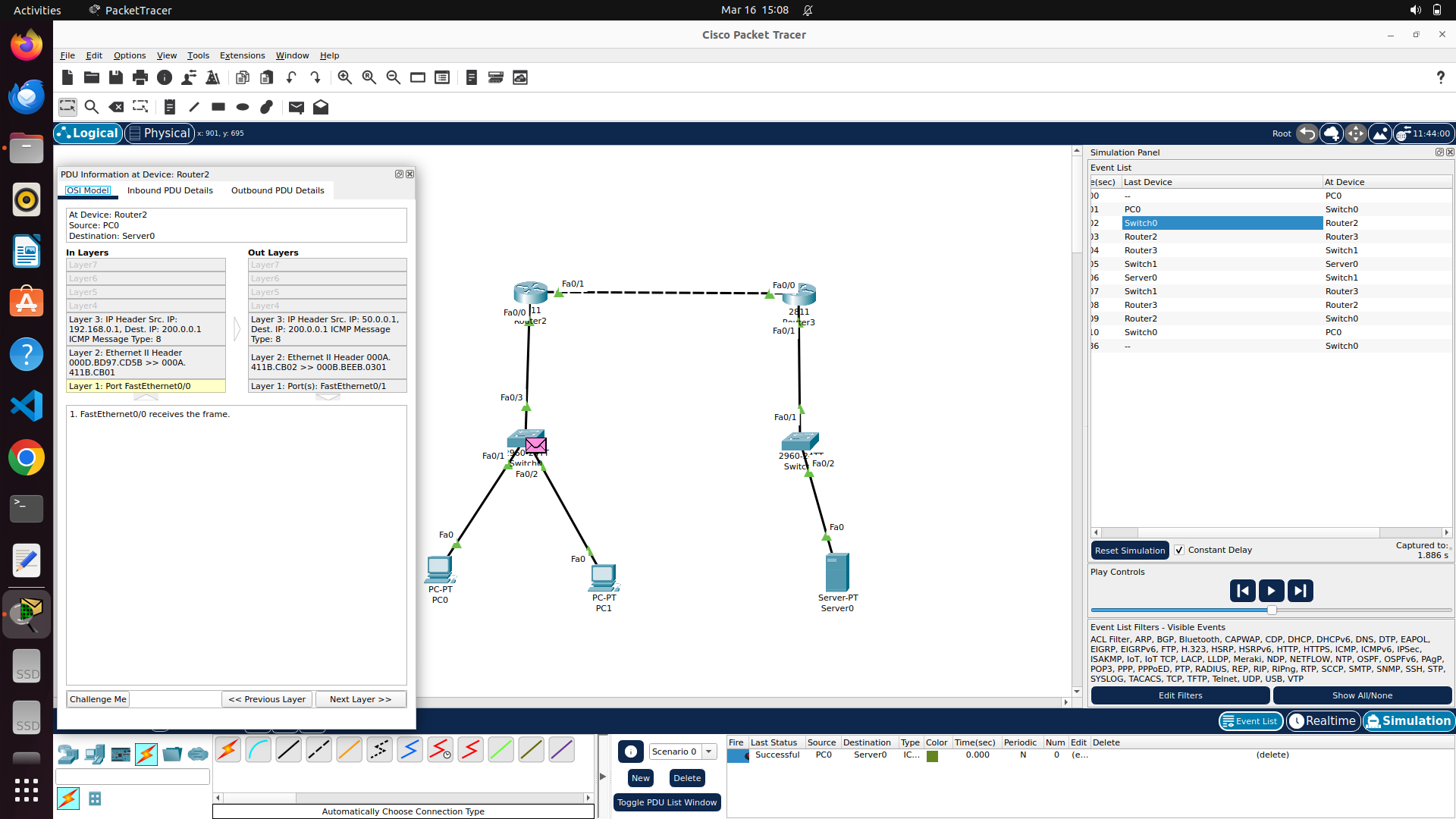
For routing table, here for router – 2 (governing private network) , is allowed for any traffic (actually , ping is the only traffic for this demonstration) to pass through router 3 (with server)

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

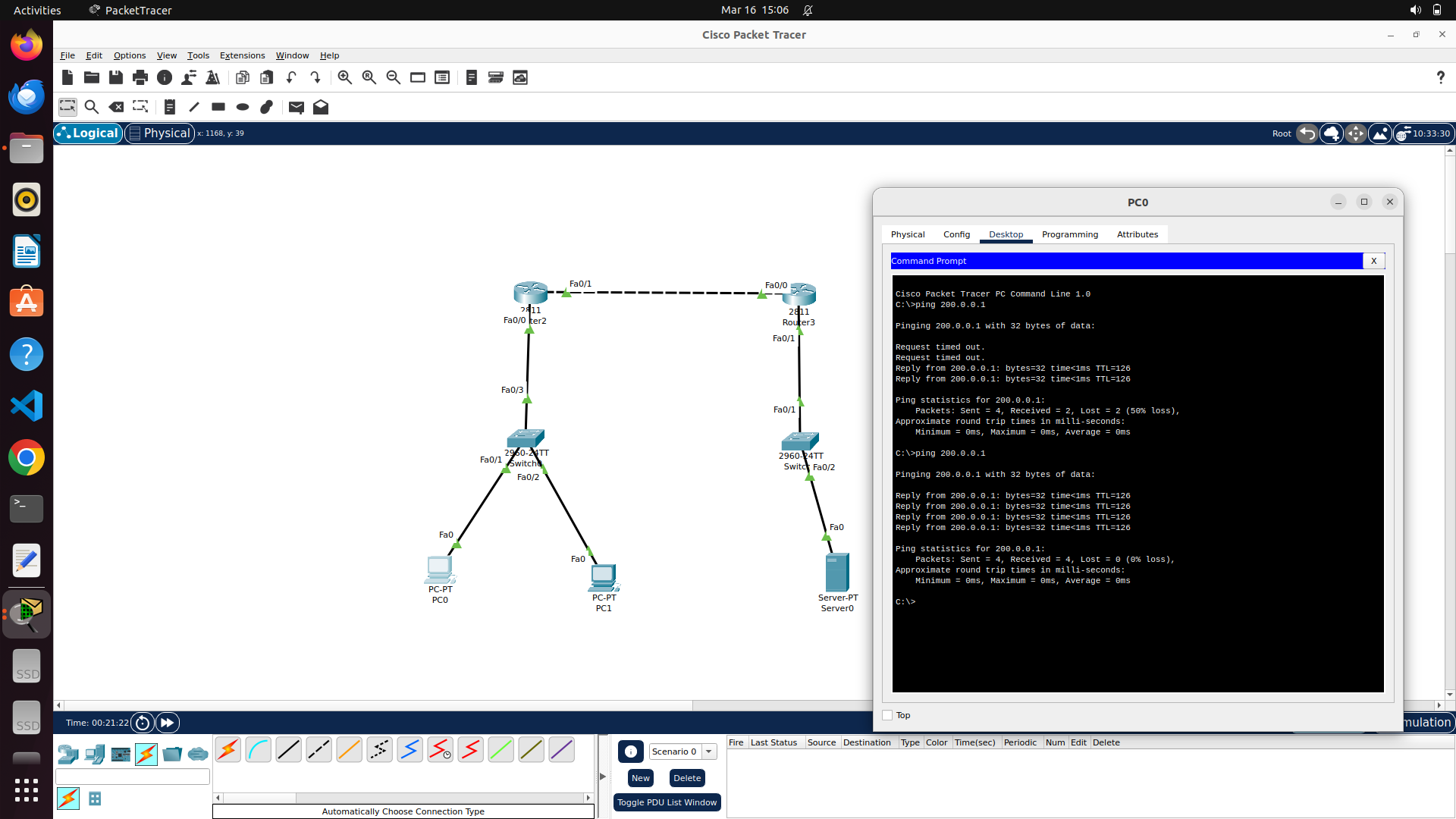


RESULTS :

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 )

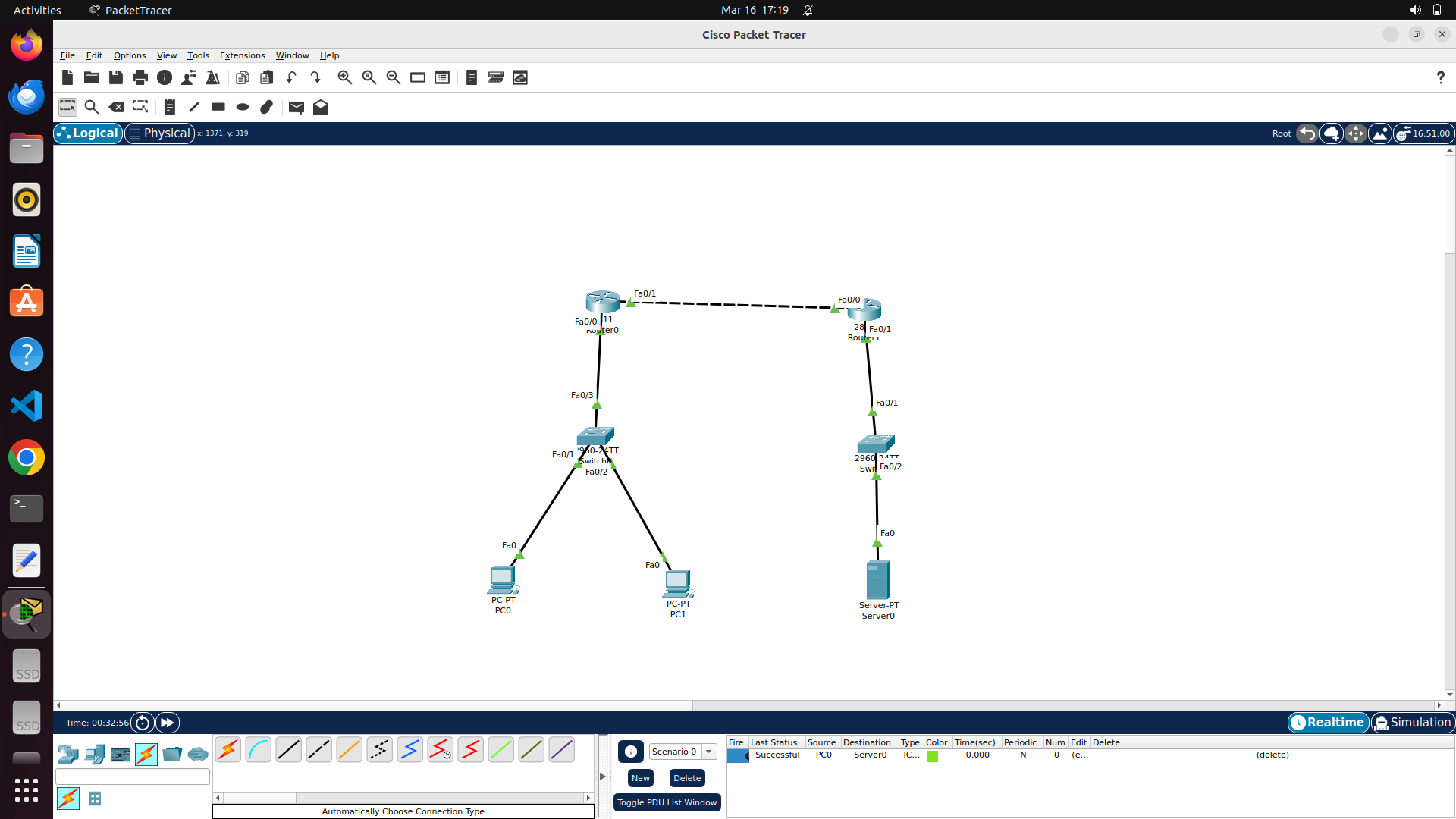


Here, PC0 was able to ping router-3 (200.0.0.1) -> default gateway of server.



DEMONSTRATION FOR PAT AND EXTENDED ACL IN CISCO PACKET TRACER :

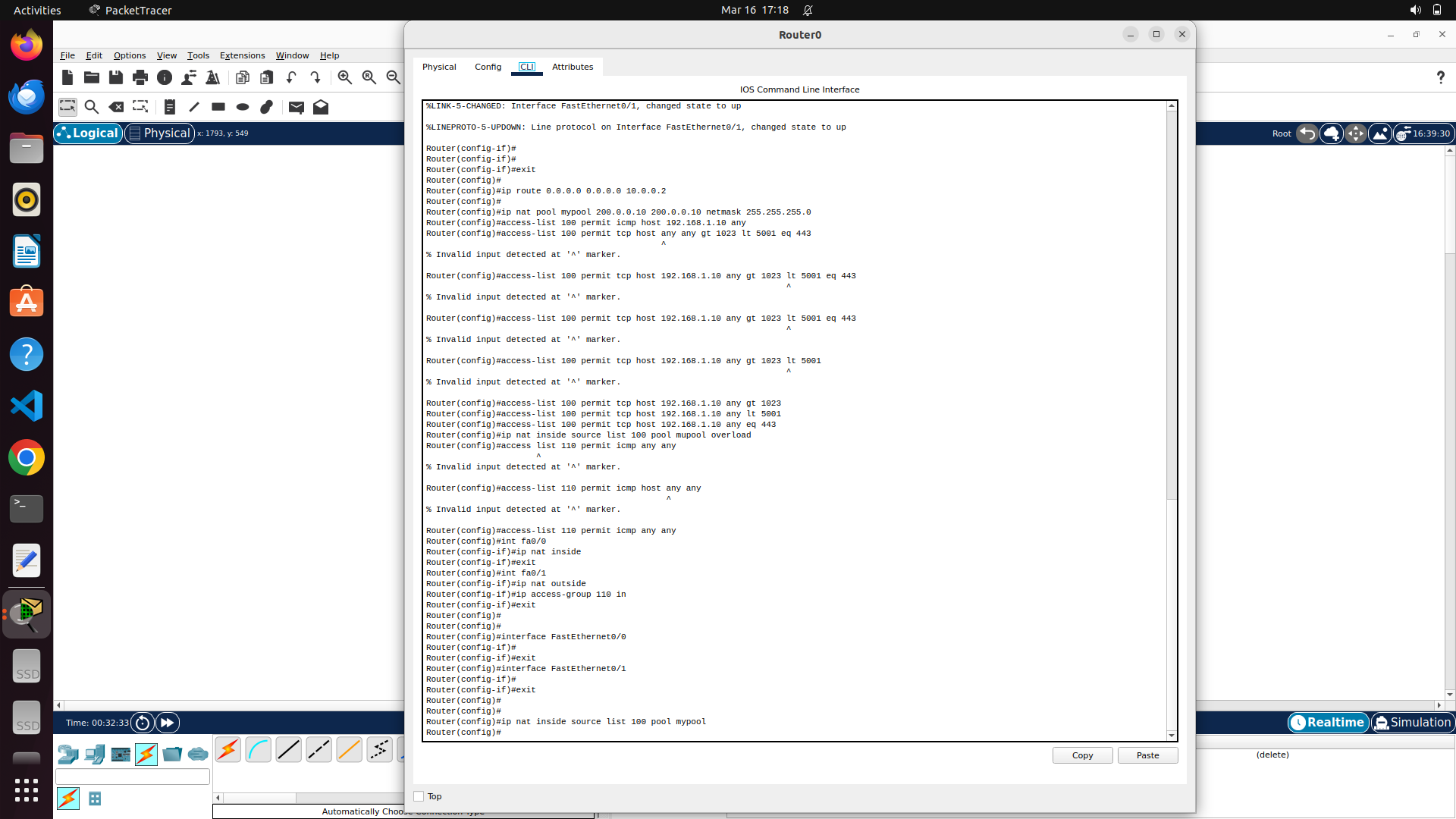
The following network is considered for this demonstration :



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 :



As usual, each interface for router to be configured with IP and subnet mask.

Followed by, developing router table (for simplicity, in router-0 , any traffic encountered is forwarded to server network – traffic controlled by private network ACL in router-0 as explained below)

In the above image, access control list 100 is used as extensive ACL in controlling the activities of private network. Here,

* PC-0 can only use ICMP (ping) by first rule.
* PC-0 can only use TCP connections to any dest host provided its port number ranges from 1023 (by second rule) to 5001 (by third rule) to destination port (443 – https) by fourth rule

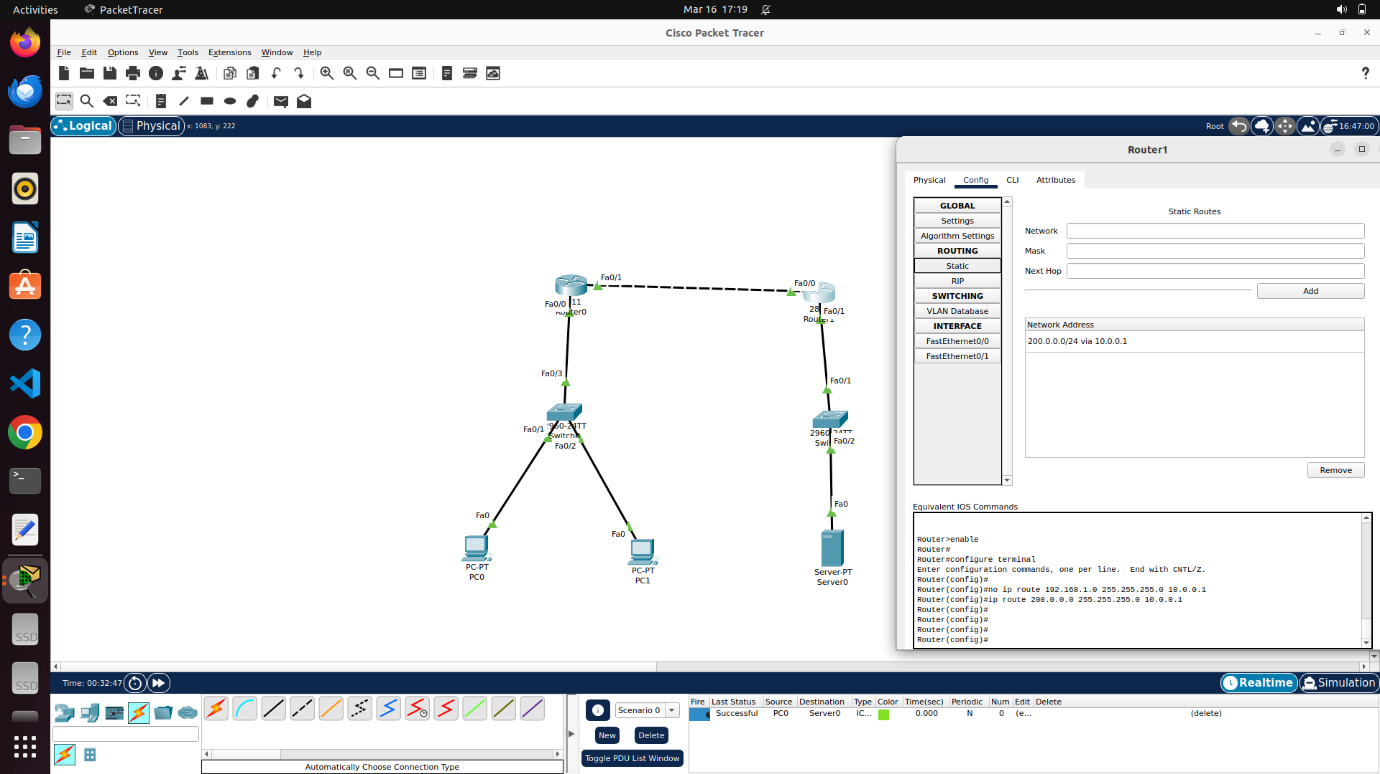
To use PAT , single public IP will be required. It can be taken from any interface using “interface” command or we can create a pool containing single IP in favour to this. Here, pool with single IP (200.0.0.10/24) is created using pool command with nat.

Access control list 110 in above image controls the incoming traffic from the router interface that connects next router by allowing only icmp packets.

Now, each interface should be marked either as inside NAT or outside NAT. if inside NAT, “ip nat inside source list <list number> pool <pool name> overload” command itself will be automatically assigned to outbound traffic from the interface which was marked “inside NAT”. here “OVERLOAD” keyword represents PAT.

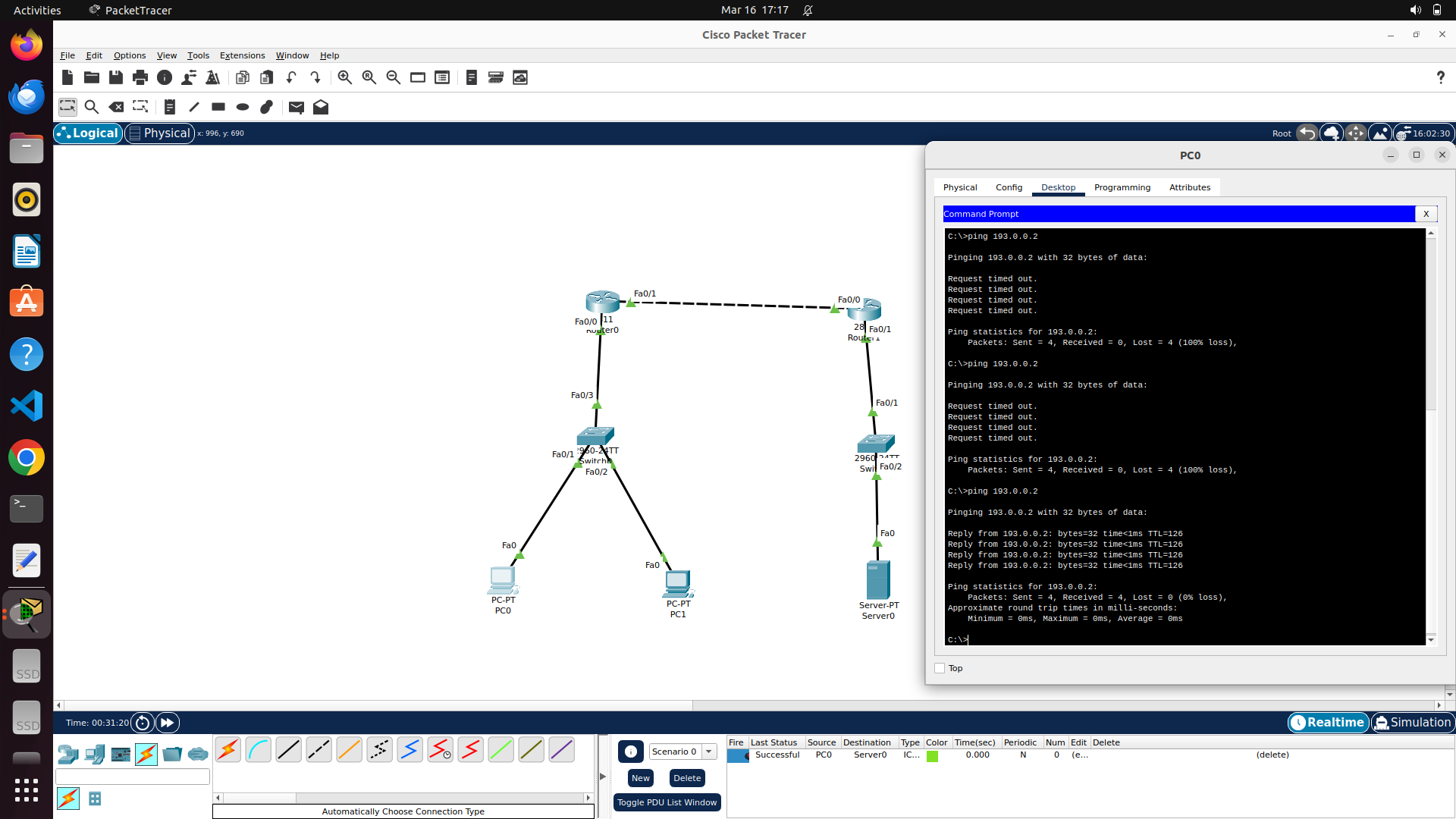
Access control list 110 should be deliberately applied on the outside interface as “ip access-group 110 <in/out>”.

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):

