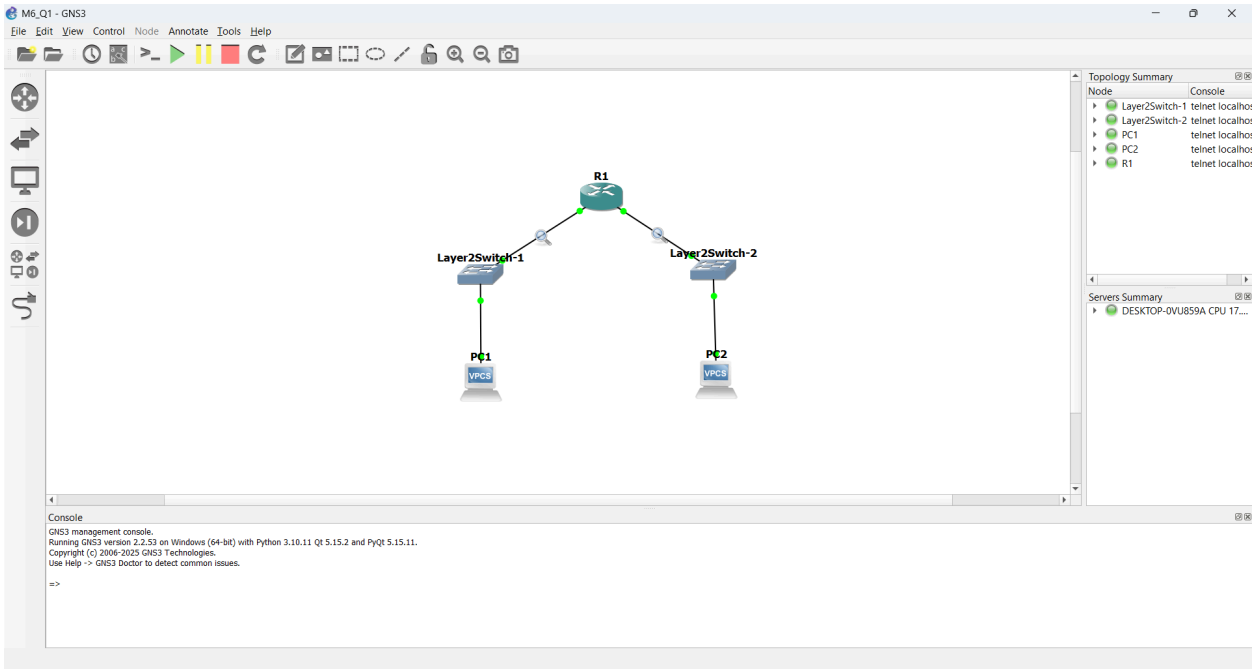
Networking Assessment 4 - Module 6

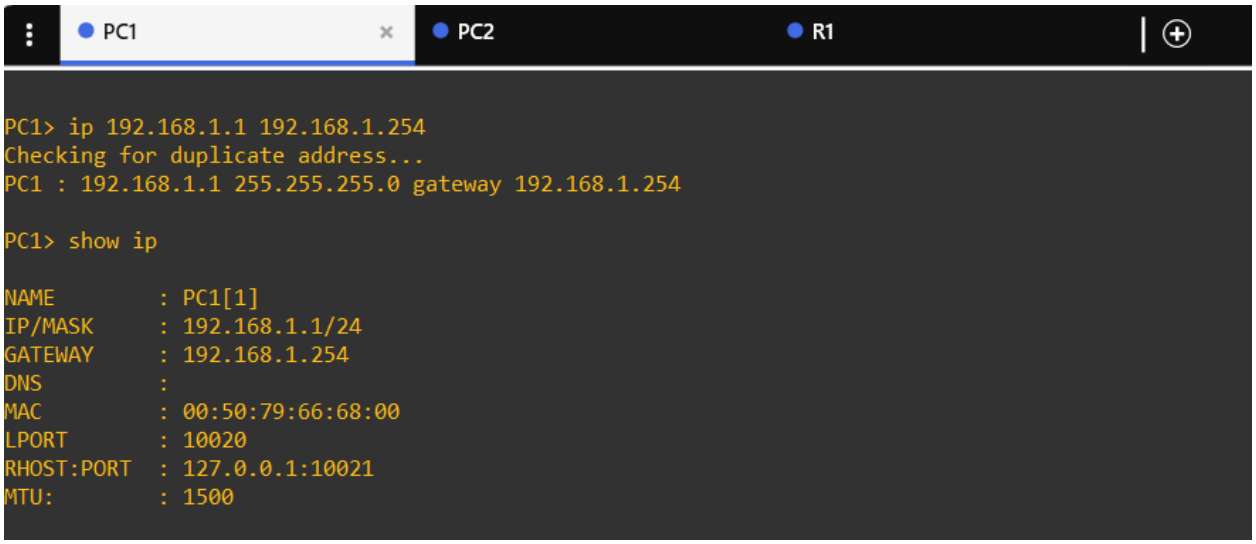
Name	T K Gowtham
Email ID	gowthamkamalasekar@gmail.com
College	VIT Chennai

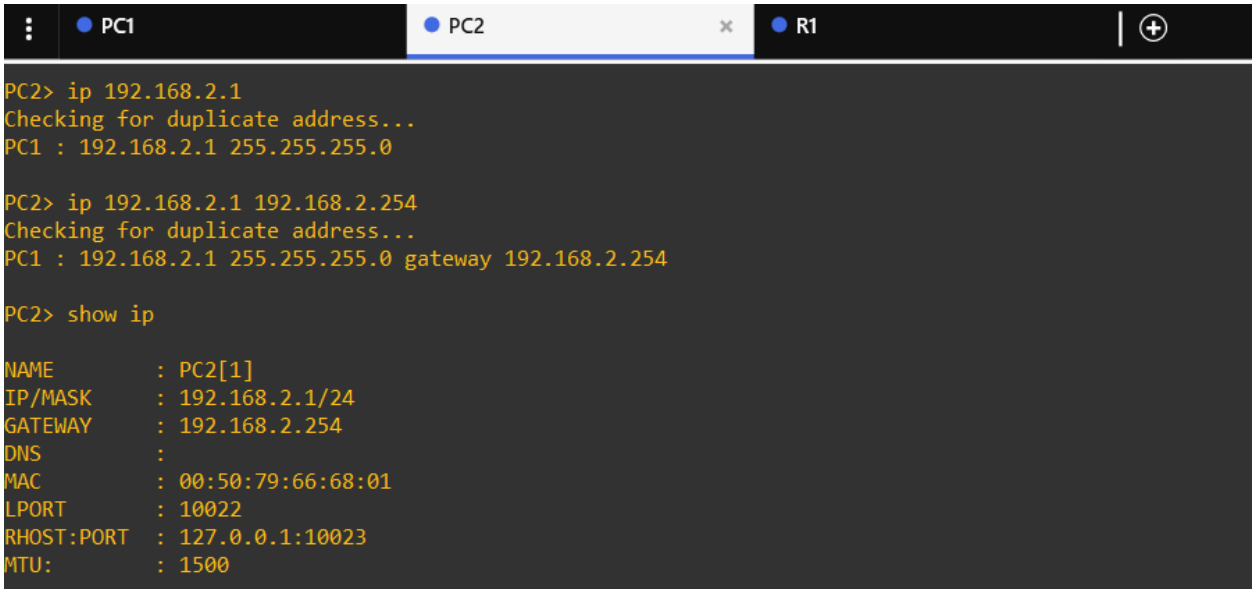
1. Capture and analyze ARP packets using Wireshark. Inspect the ARP request and reply frames when your device attempts to find the router's MAC address. Discuss the importance of ARP in packet forwarding.

Configure the Network topology in GNS3 as given below, in the Switch make sure to add two ports :

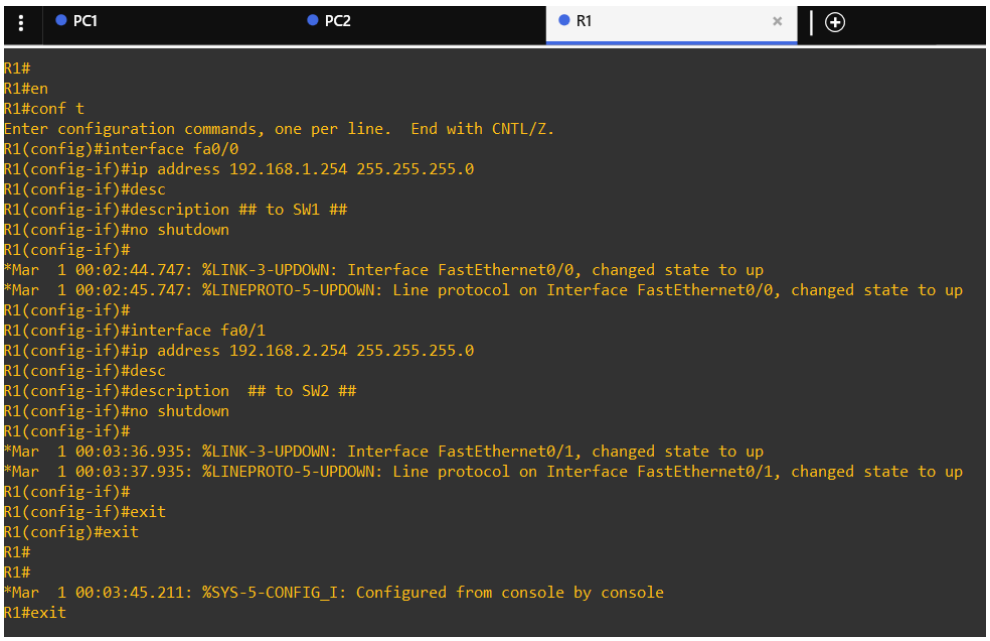


Configure the IP address and default gateway of PC1 and PC2 :

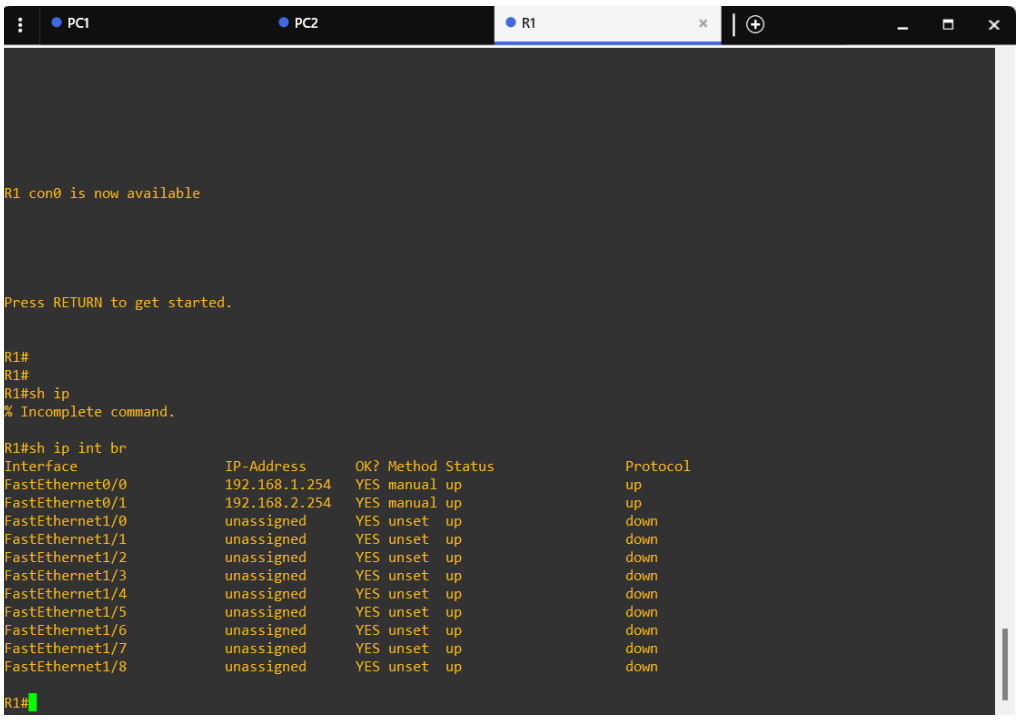




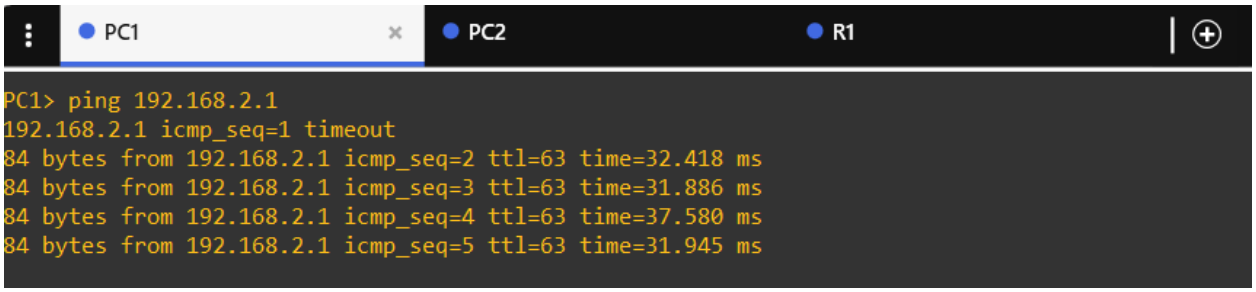
Configure the Router with IP address of each of its interfaces with IP address which will de the default gateway :



You can view the IP address configured as given below :

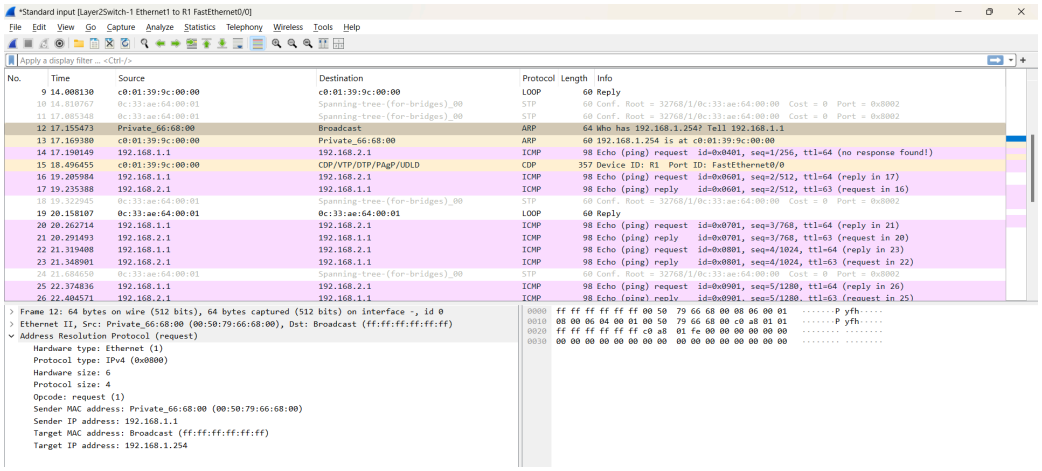


Ping from PC1 to PC2:

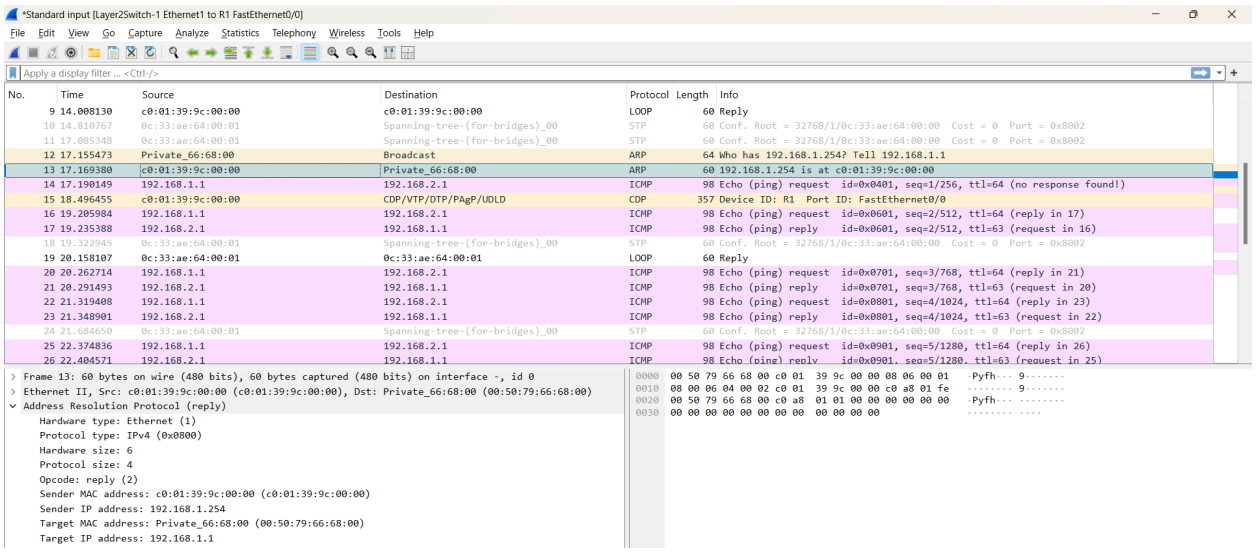


You will able to see the ARP request from PC1 side, between Switch 1 and Router that PC1 is requesting for Routers MAC address.

Request :

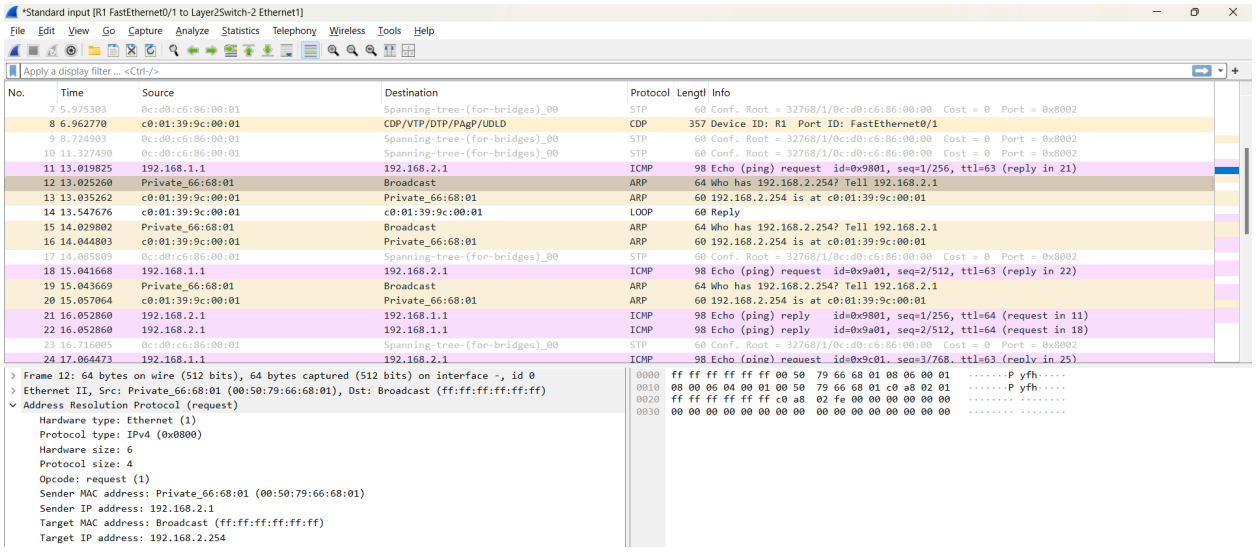


Reply :

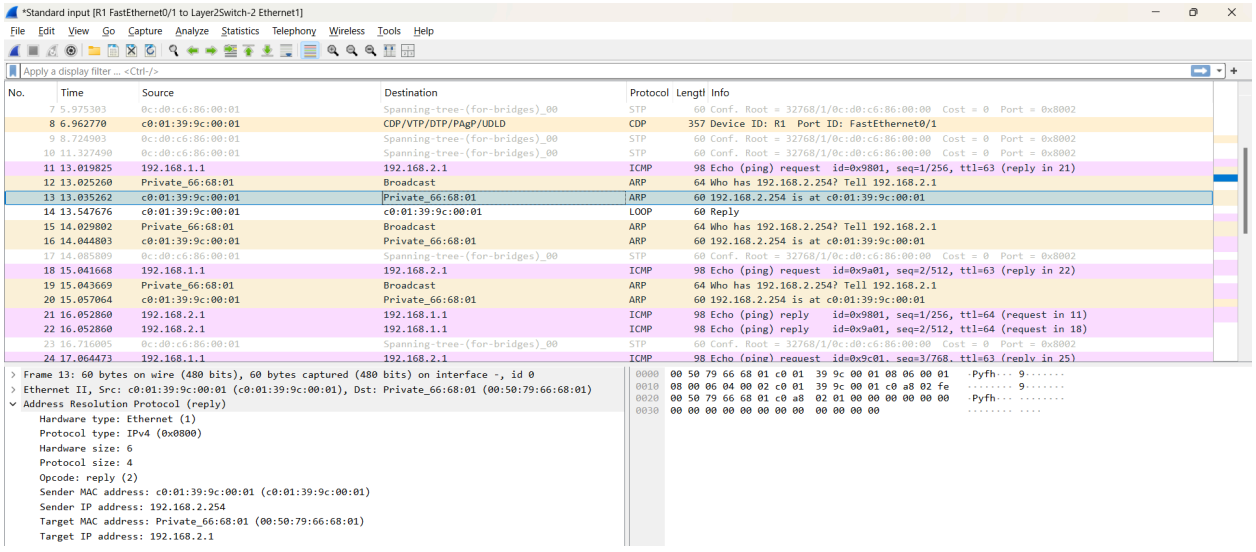


Similarly, between Switch 2 and Router, PC2 is requesting and getting reply for Router's MAC Address

Request :

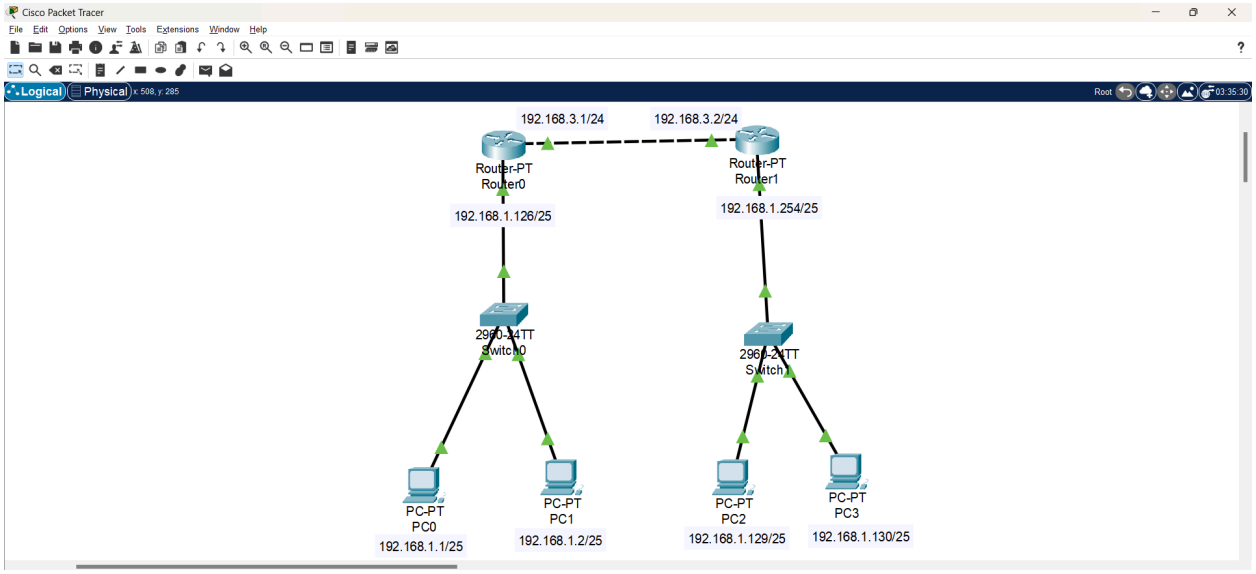


Reply:

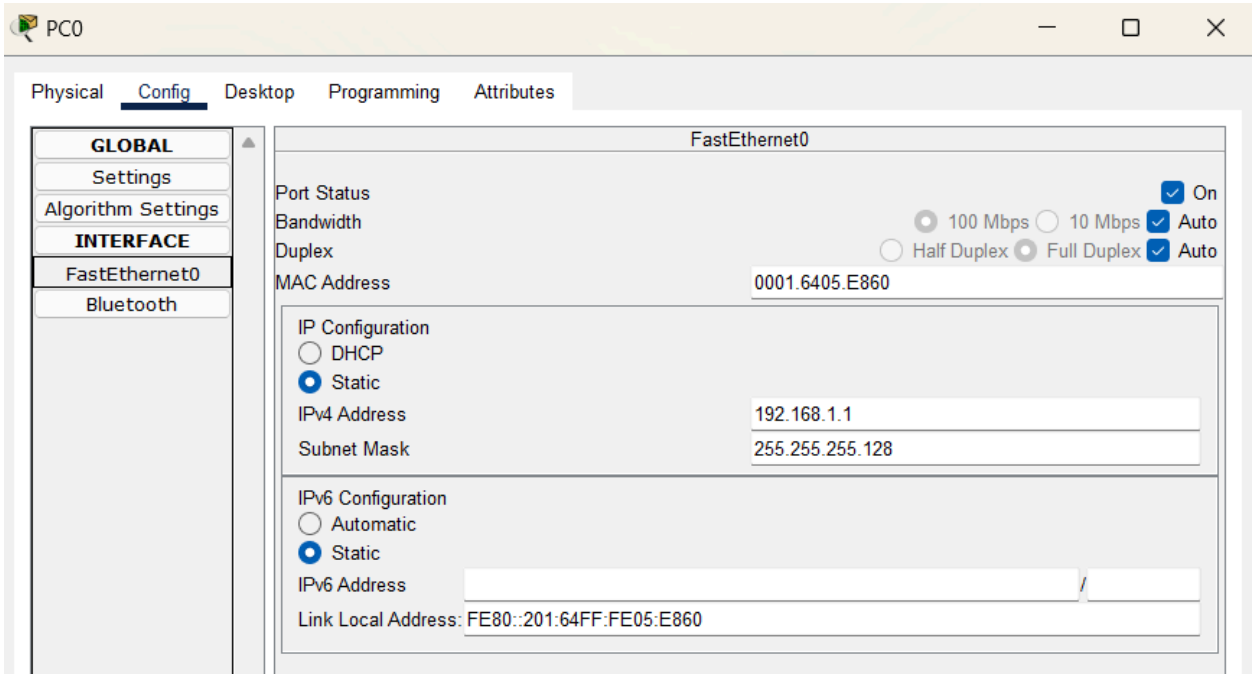


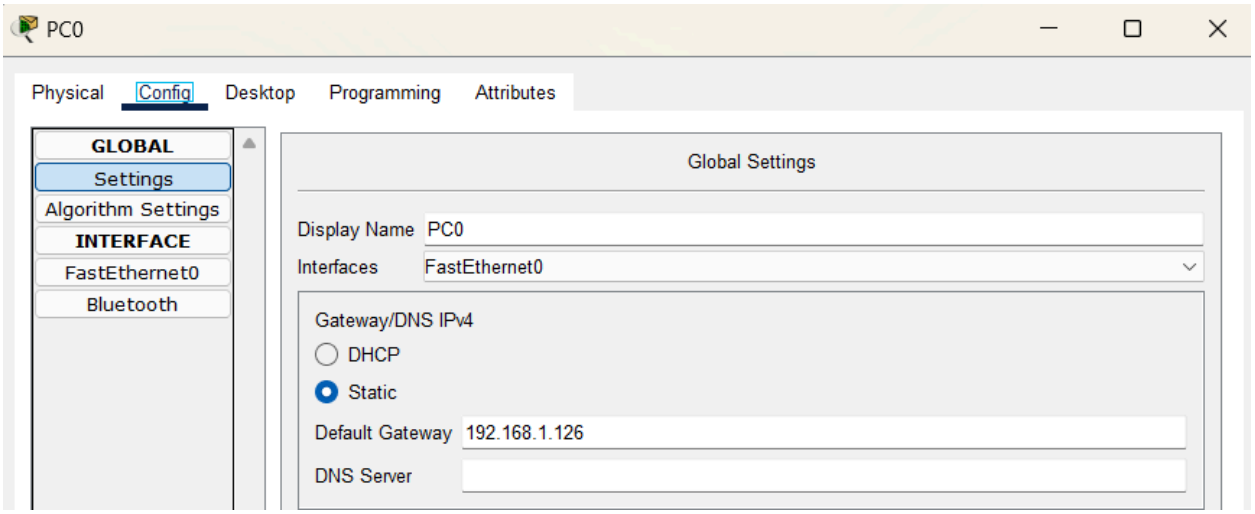
2. Manually configure static routes on a router to direct packets to different subnets. Use the ip route command and verify connectivity using ping and traceroute.

Configure the Network Topology in Cisco Packet Tracer :

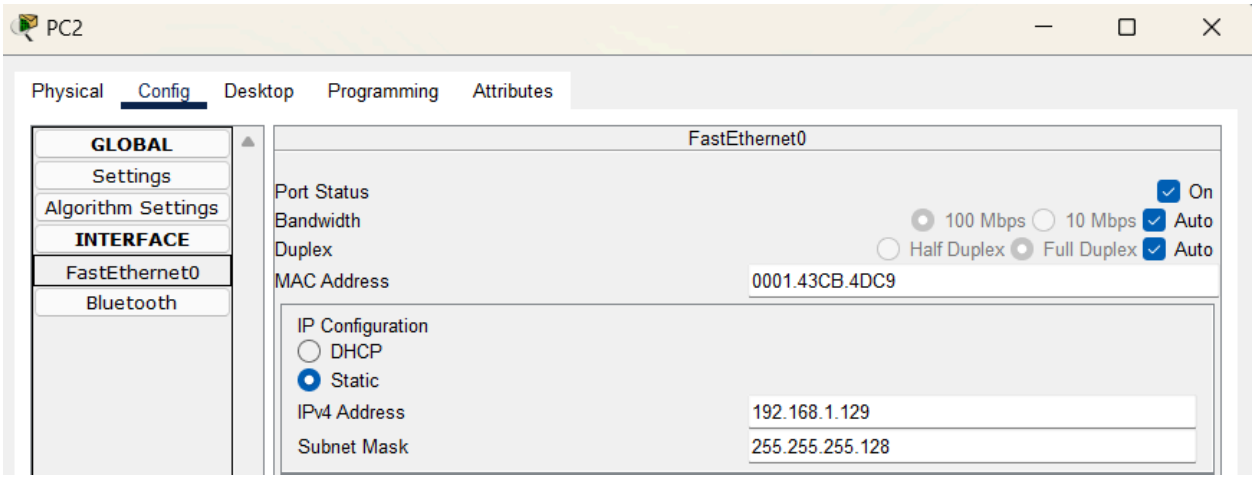


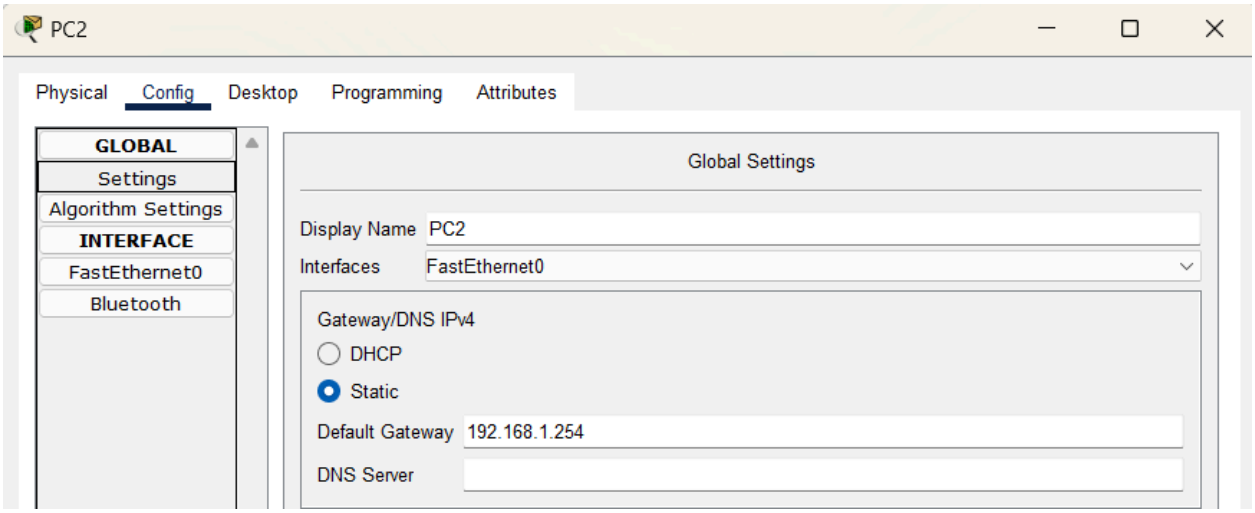
Configure PC0 (and similarly for PC1) with IP address, Subnet mask and default gateway. We have divided the 192.168.1.0/24 into 2 subnets.



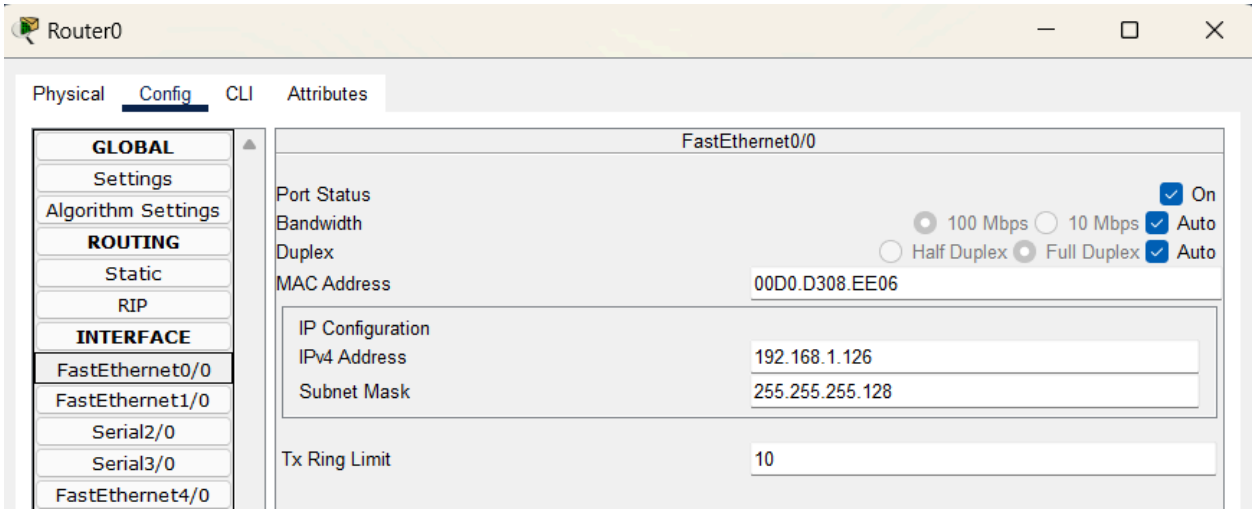


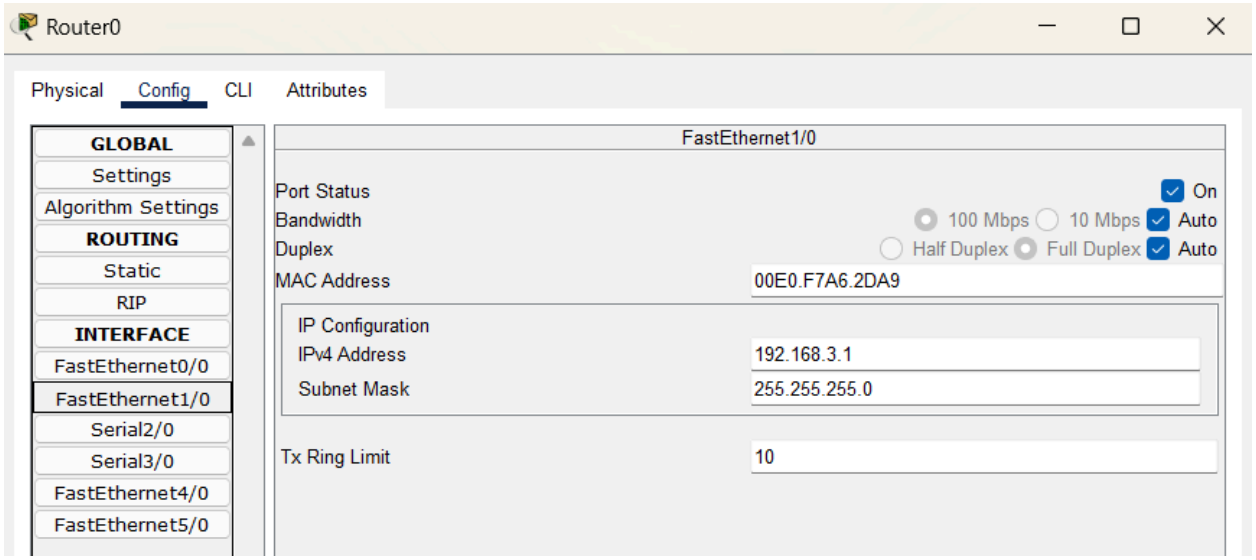
Use the second subnet and configure PC2 (similarly for PC3) with IP address, subnet mask and default gateway :



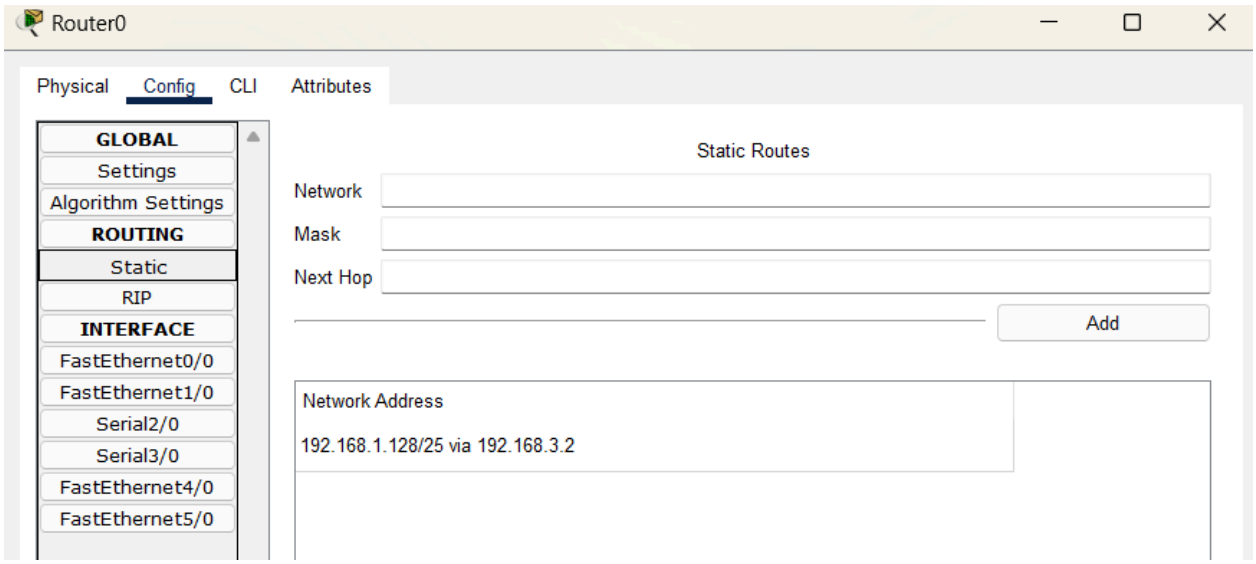


In the Router configure the Default gateway IP address with its IP addresses for respective interfaces :

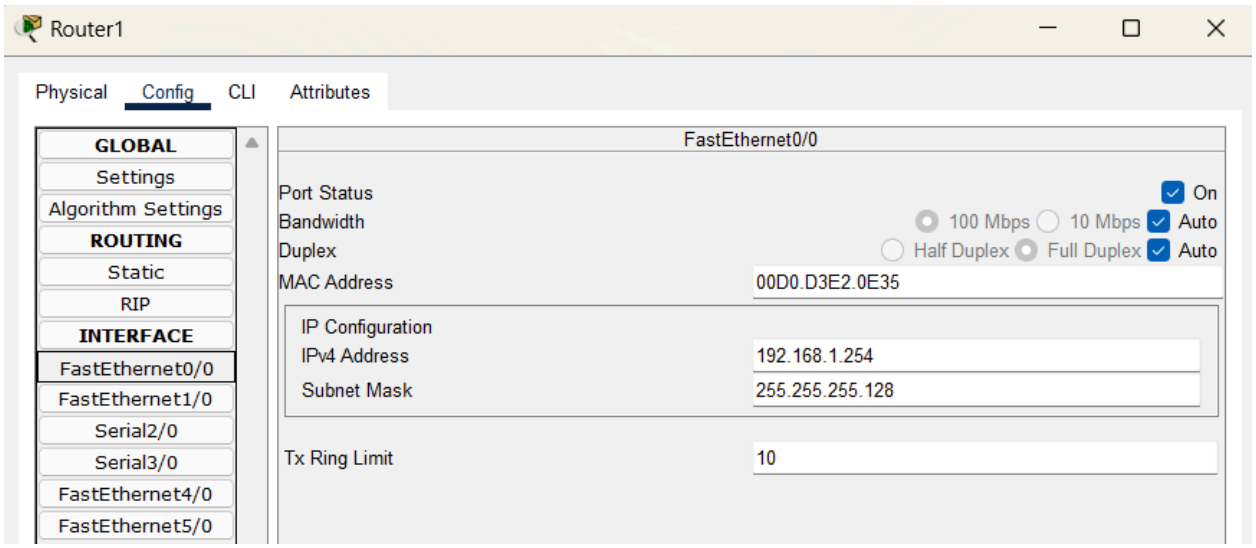


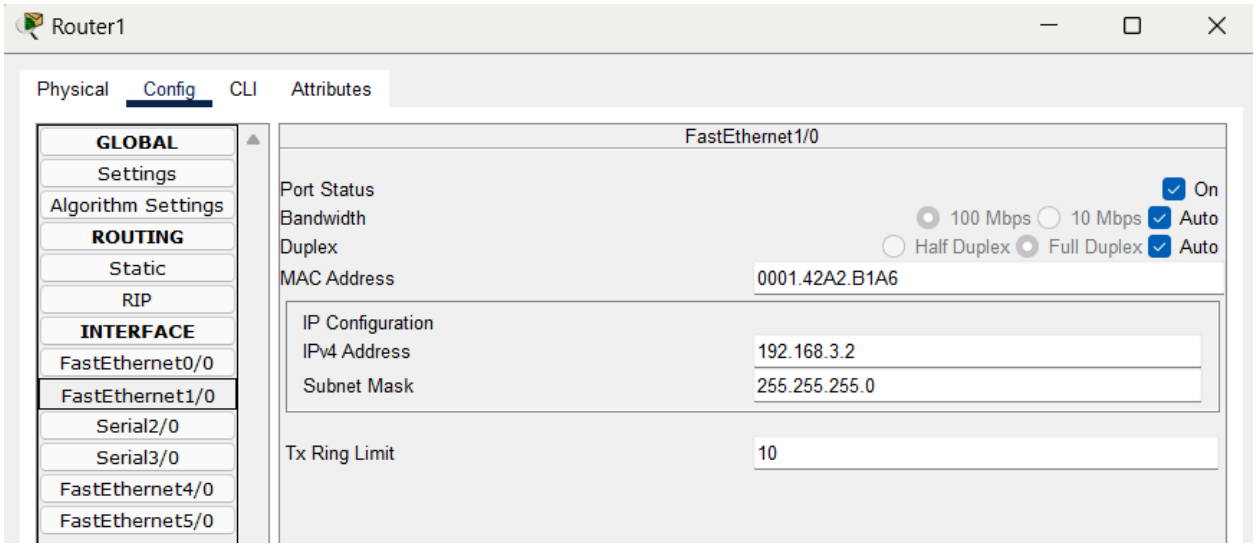


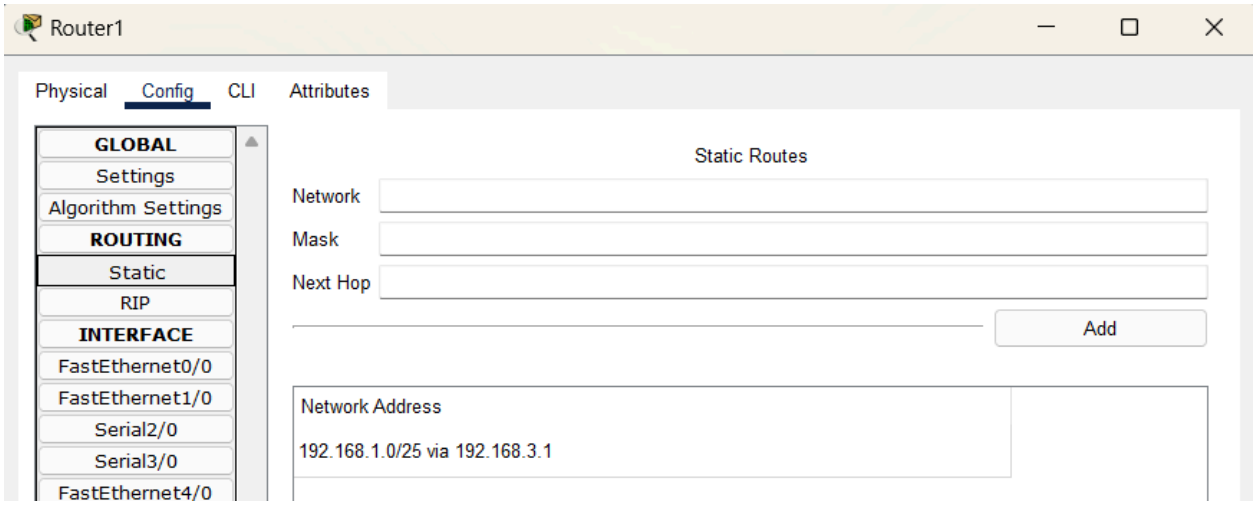
Add the static route for the packets to travel from Router 1 to Router 2 :



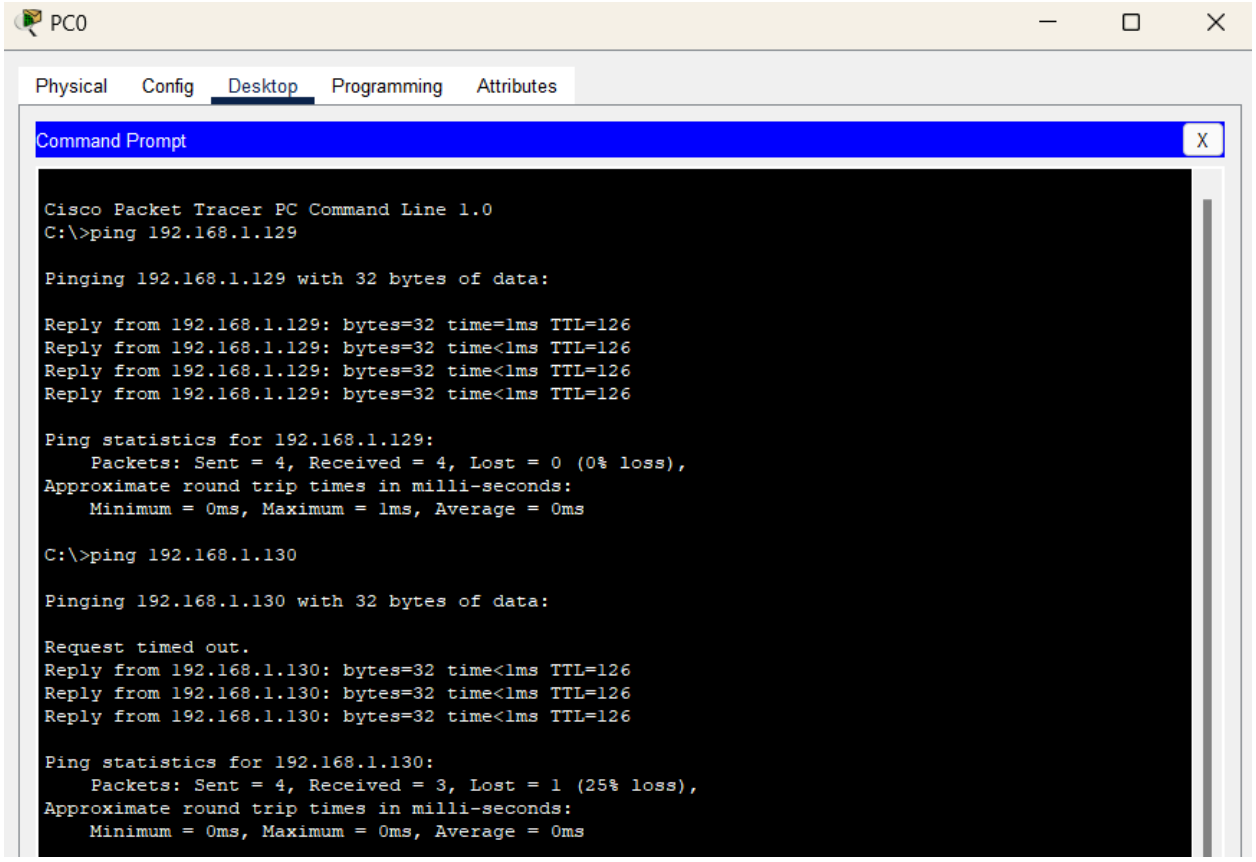
Similarly configure Router 2 with IP address for its Interfaces and also add the static route for it send packets from Router 1 to Router 2 :



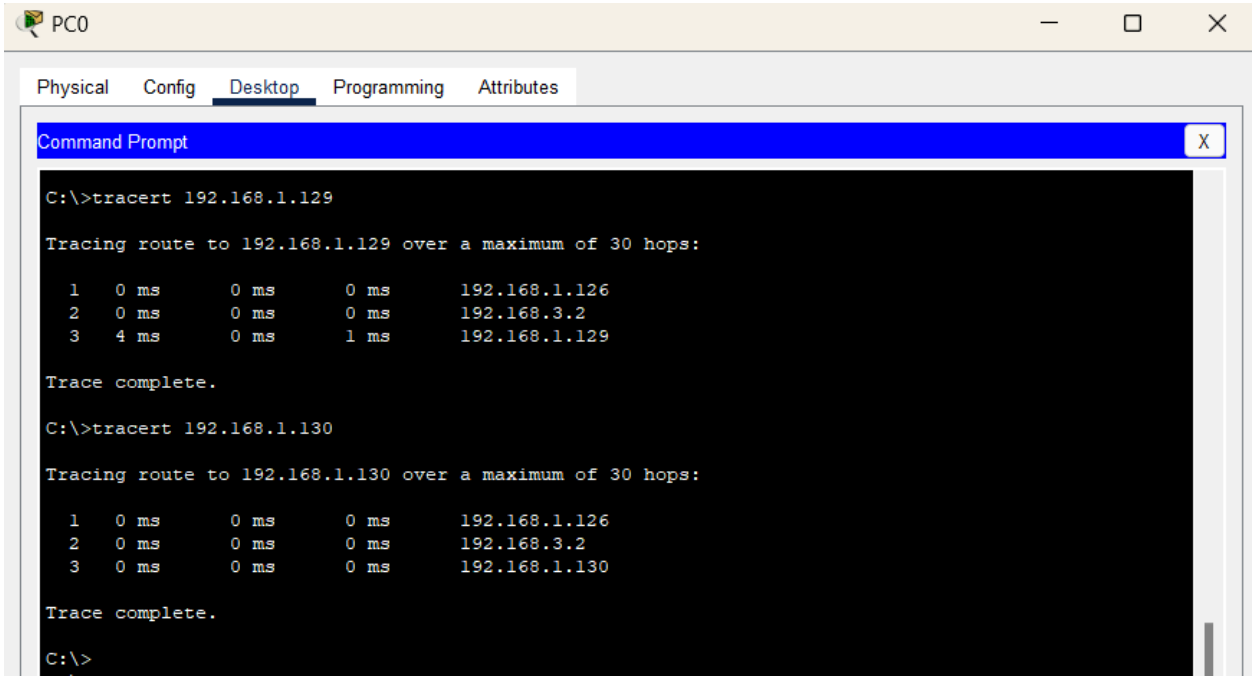

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
FastEthernet1/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.42A2.B1A6
IP Configuration
IPv4 Address
192.168.3.2
Subnet Mask
255.255.255.0
Tx Ring Limit
10


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
Static Routes
Network
Mask
Next Hop
Add
Network Address
192.168.1.0/25 via 192.168.3.1

Now Ping from PC0 to PC2 and PC 0 to PC3, we that it successfully sends the packets :



Similarly, use tracert for trace route the PC 0 to PC2 and PC 0 to PC3 and we see the routes :



3. Given a network address of 10.0.0.0/24, divide it into 4 equal subnets. Calculate the new subnet mask. Determine the valid host range for each subnet. Assign IP addresses to devices in Packet Tracer and verify connectivity.

Dividing the 10.0.0.0/24 into 4 equal subnets :

10.0.0.00000000/26 → 10.0.0.0/26

10.0.0.01000000/26 → 10.0.0.64/26

10.0.0.10000000/26 → 10.0.0.128/26

10.0.0.11000000/26 → 10.0.0.192/26

Ranges and Usable valid host of the subnets :

1. 10.0.0.0/26 → 10.0.0.63/26

   Valid Host are 10.0.0.1/26 → 10.0.0.62/26

2. 10.0.0.64/26 → 10.0.0.127/26

   Valid hosts are 10.0.0.65/26 → 10.0.0.126/26

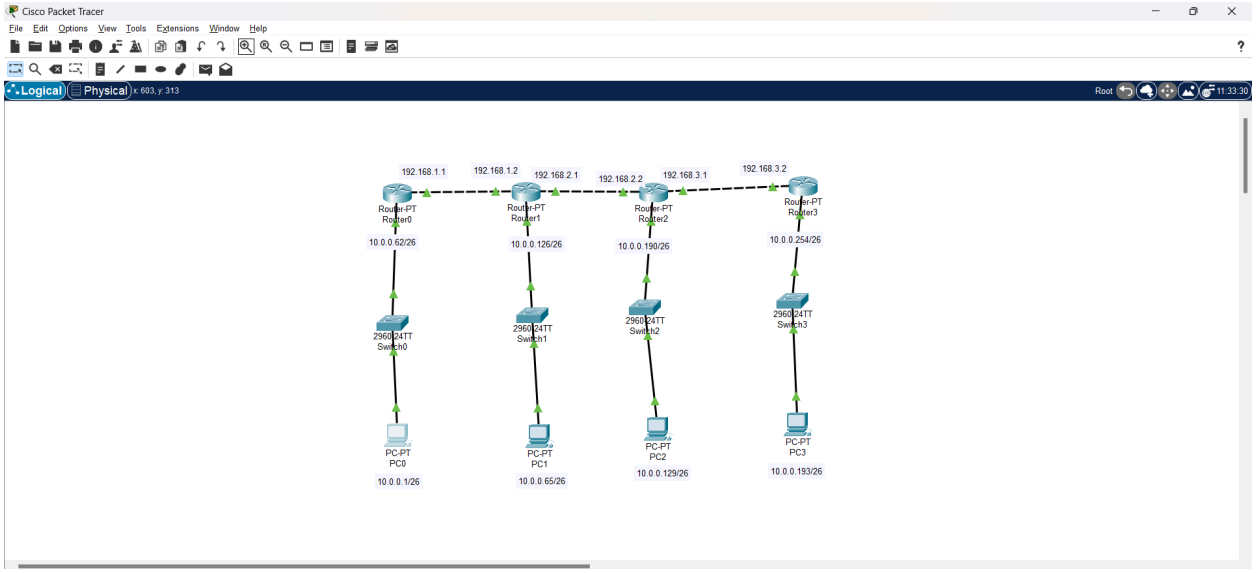
3. 10.0.0.128/26 → 10.0.0.191/26

   Valid hosts are 10.0.0.129/26 → 10.0.0.190/26

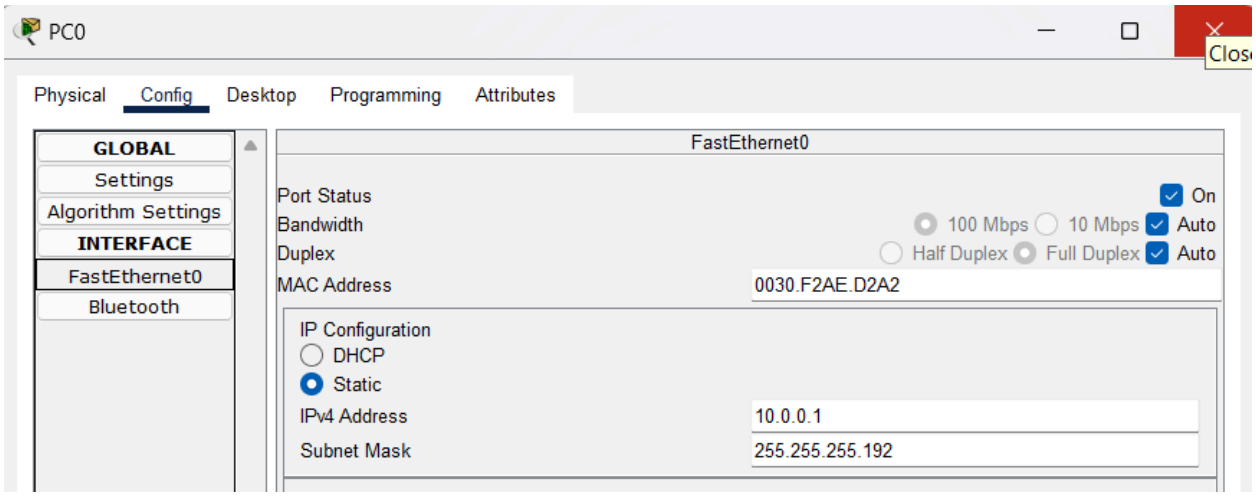
4. 10.0.0.192/26 → 10.0.0.255/26

   Valid hosts are 10.0.0.193/26 → 10.0.0.254/26

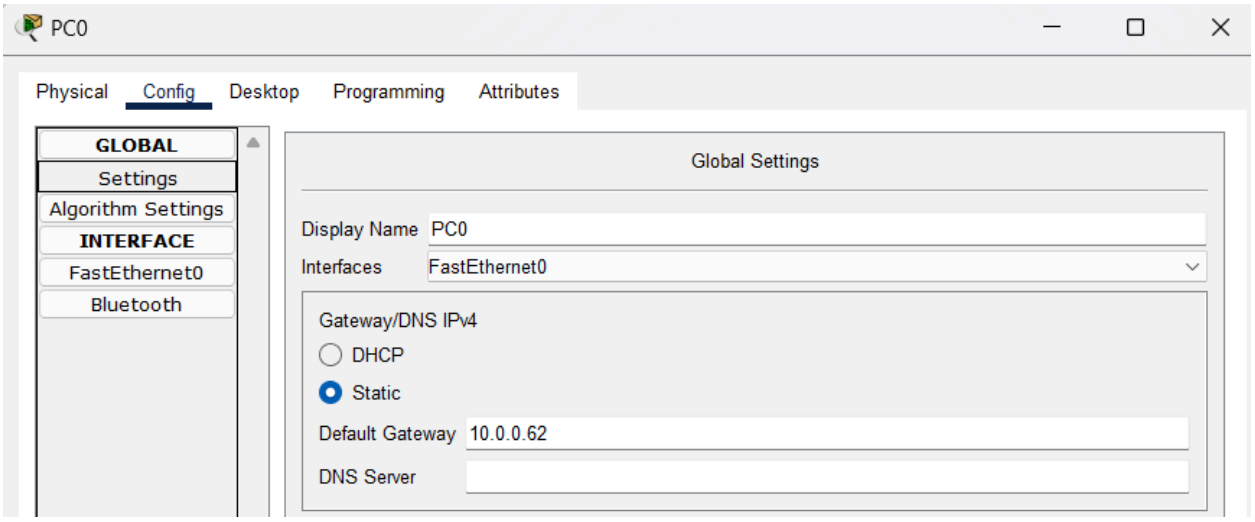
Now configure the Network topology as given below in the Cisco Packet Tracer :



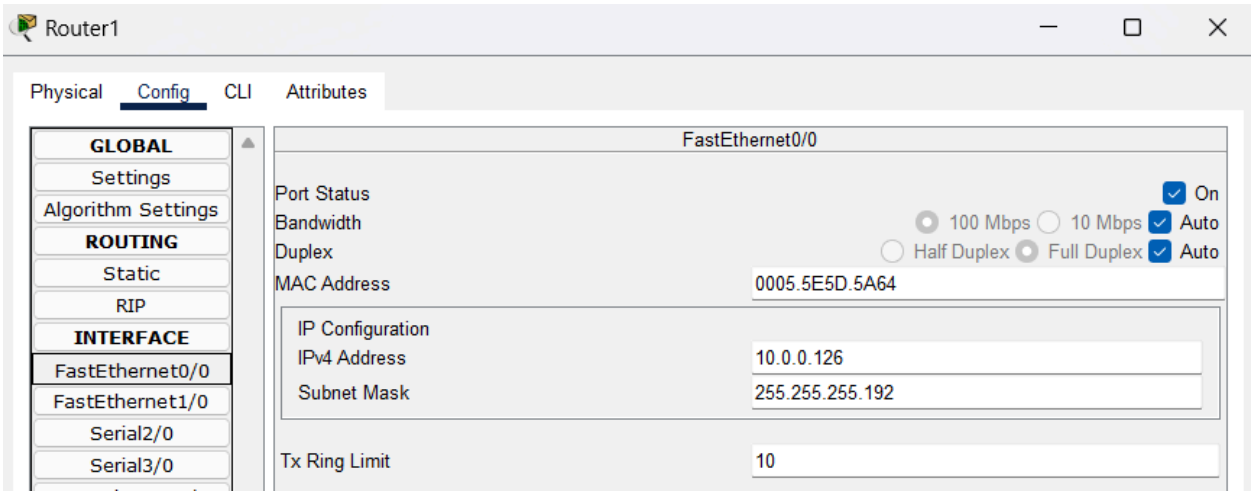
Configure the PC with IP address and Subnet mask as given below and do it for the other PCs as well similarly :



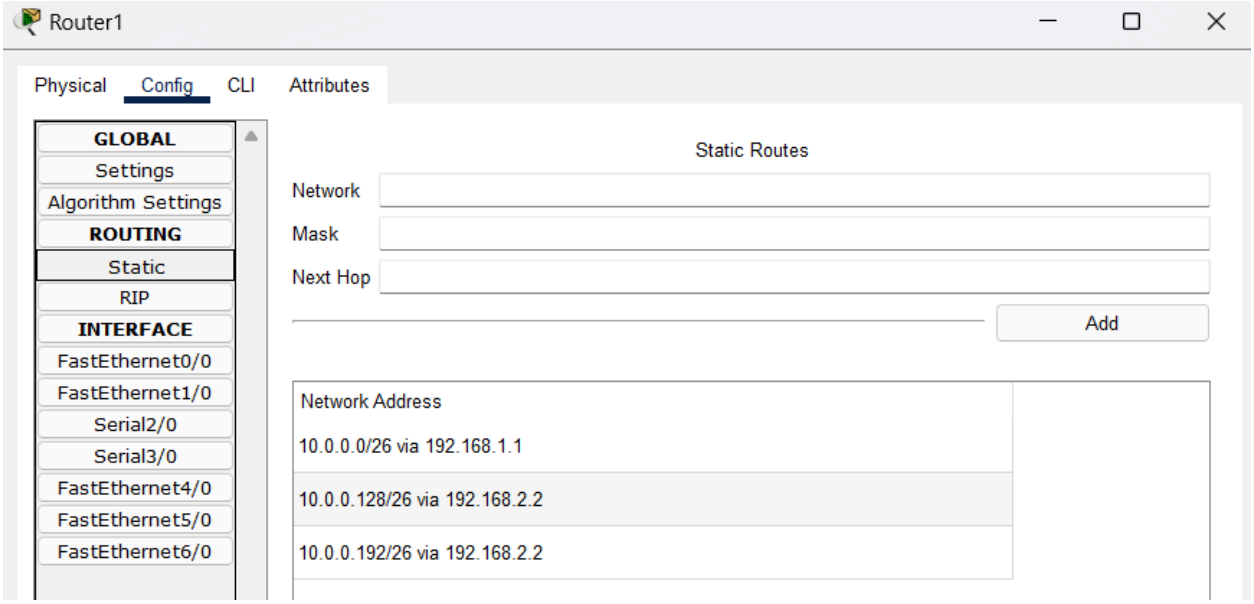
Configure the default gateway for every PC :



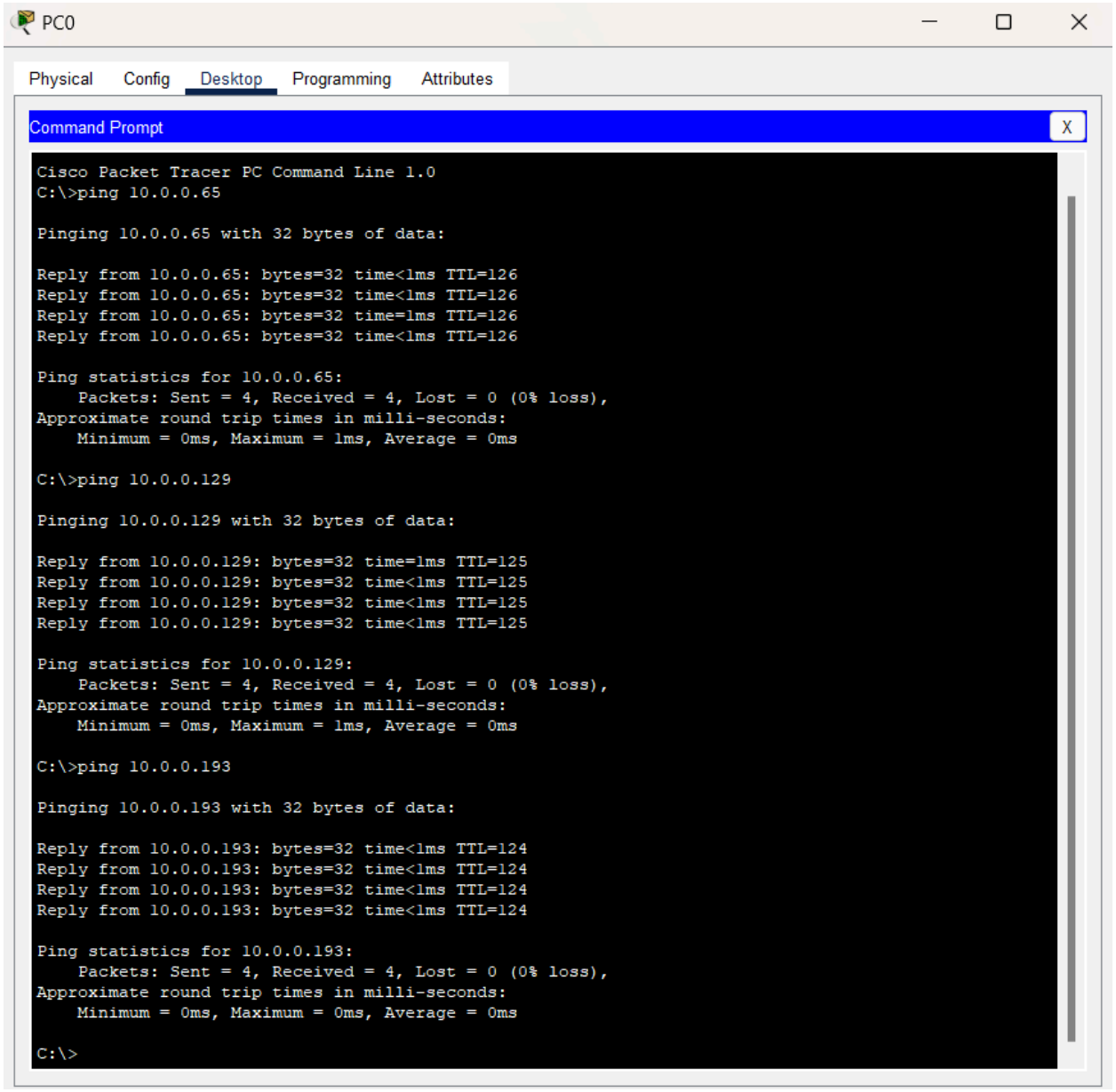
Go to each router and the IP address to its respective interfaces which will the default gateway to its respective networks :



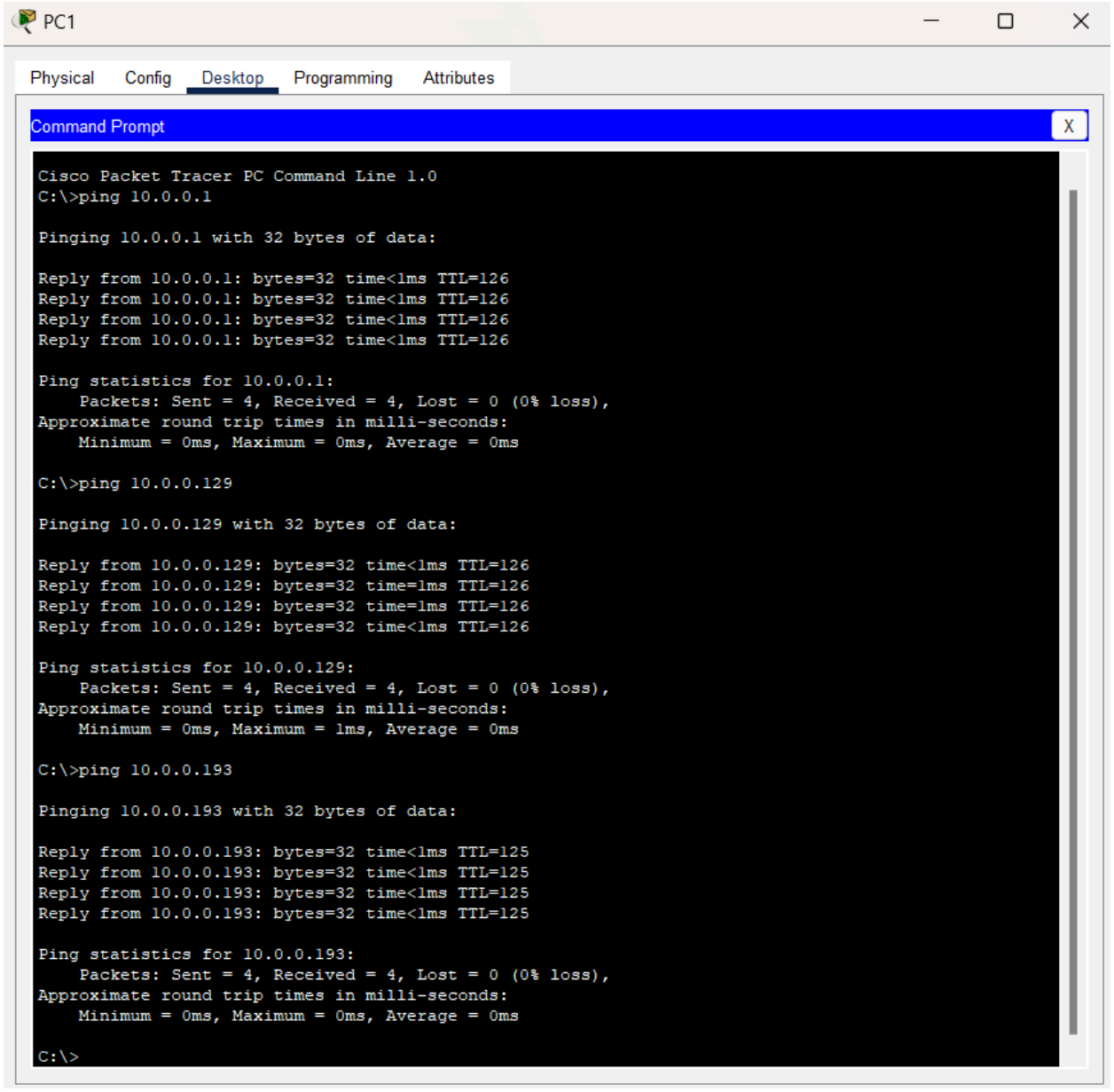
Add the Static routes the network has to reach by its Packets, and do it for all the unconnected networks to the router itself. Similarly do for all the Routers and given below is for Router1:



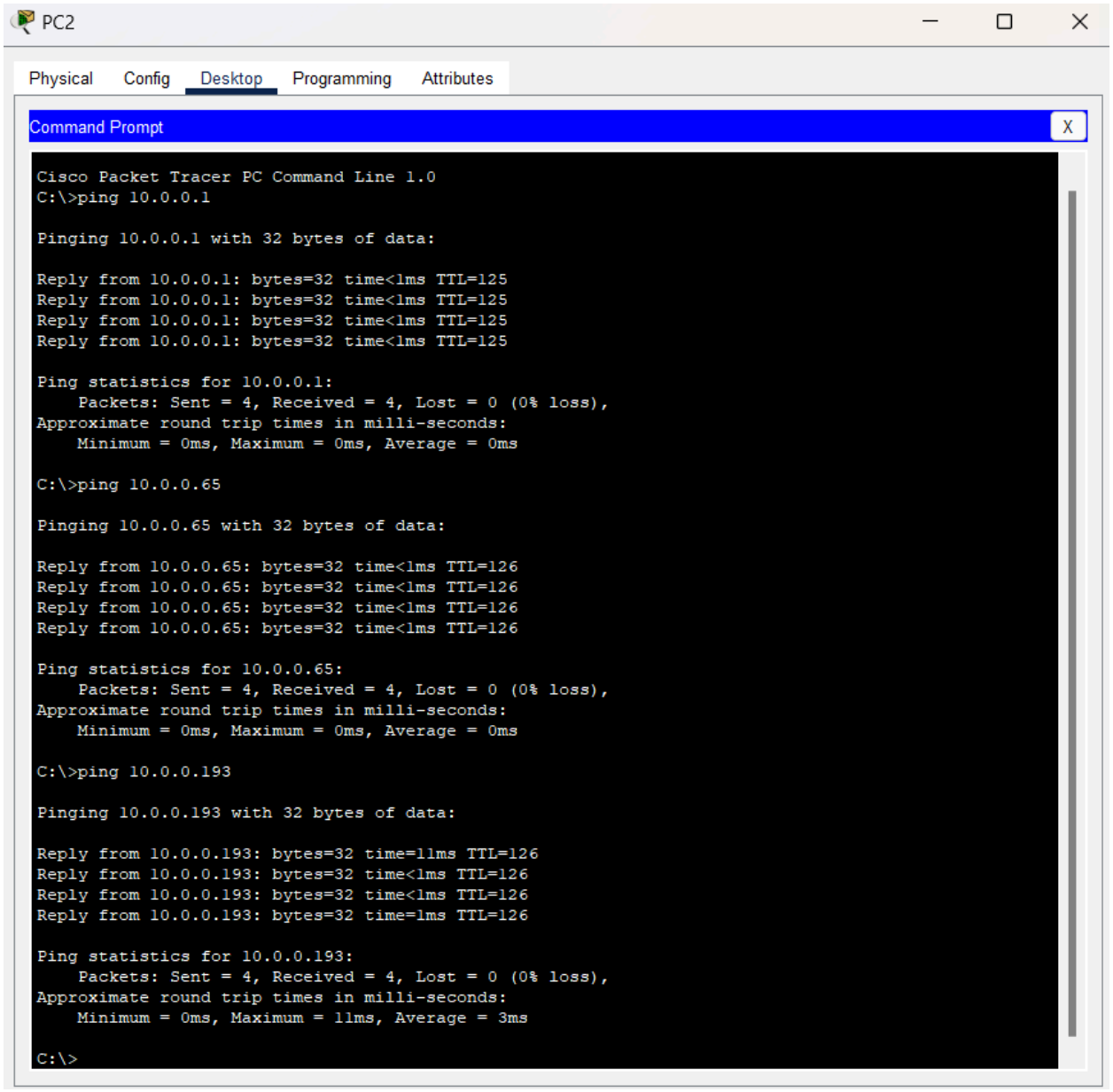
To verify the connectivity, lets Ping from PC0 to all the others PCs and we see that it is successfully pinging :



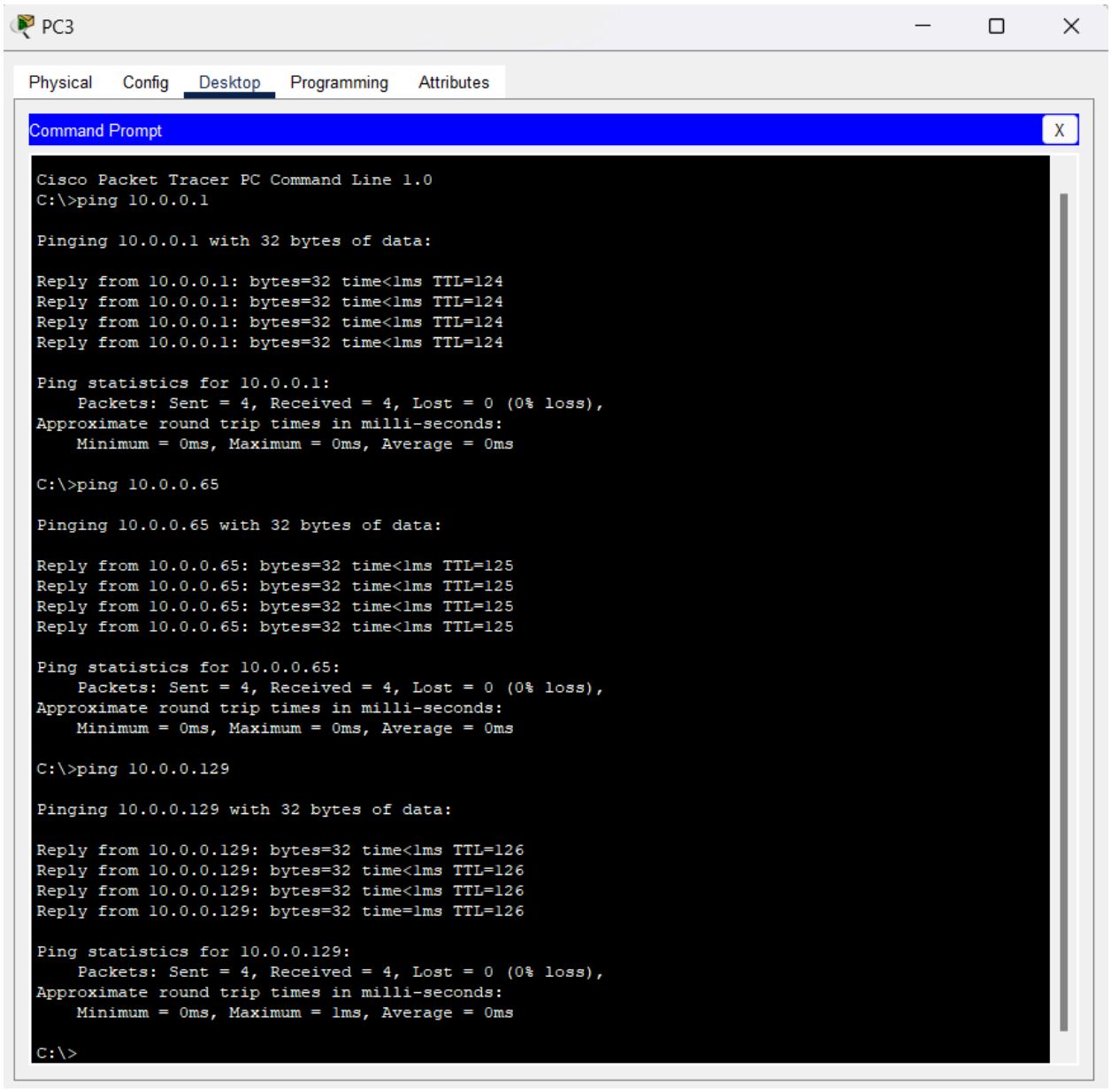
Similarly ping and check from PC1 :



Similarly ping and check from PC2 :



Similarly ping and check from PC3 :



4. You are given three IP addresses: 192.168.10.5, 172.20.15.1, and 8.8.8.8. Identify the class of each IP address. Determine if it is private or public. Explain how NAT would handle a private IP when accessing the internet.

Given IP Address	Class of IP Address	Private / Public IP Address
192.168.10.5	Class C	Private
172.20.15.1	Class B	Private
8.8.8.8	Class A	Public

Classful Addressing :

There are 5 classes of IP addressing, A to E. Where A to C are Unicast, D is Multicast, E is reserved.

0.0.0.0 → 127.255.255.255 → Class A

128.0.0.0 → 191.255.255.255 → Class B

192.0.0.0 → 223.255.255.255 → Class C

Private IP address :

These are reserved within private network usage and not accessible to the Internet. These fall in the range specified by RFC 1918 as given below :

10.0.0.0 → 10.255.255.255 (10.0.0.0/8)

172.16.0.0 → 172.31.255.255 (172.16.0.0/12)

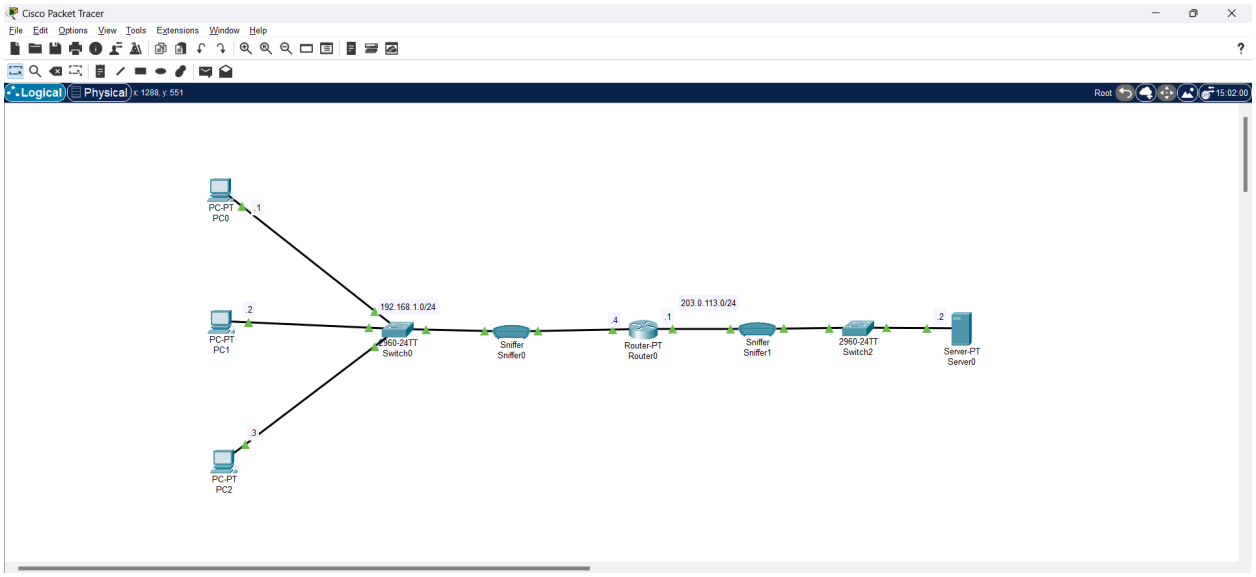
192.168.0.0 → 192.168.255.255 (192.168.0.0/16)

NAT Address :

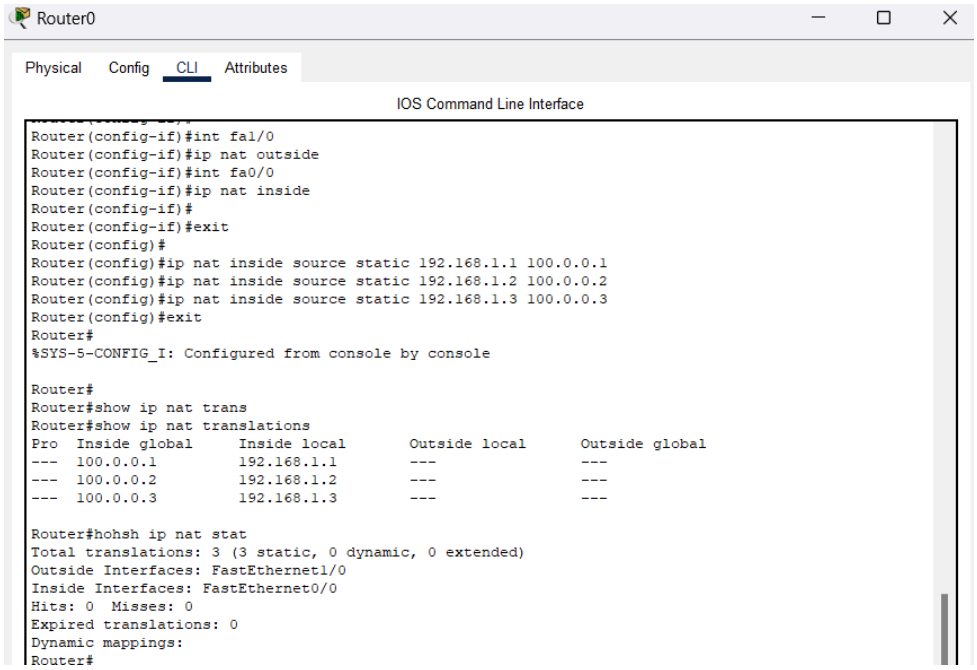
Network Address Translation is used to allow private IP addresses to communicate with the Internet using Public IP addresses. A device sends a Request to the Internet with a Private IP address and the router will convert it to a Public IP address of its own. When it gets a reply, the NAT in the router will convert it back to private IP and send it to the device.

5. In Cisco Packet Tracer, configure NAT on a router to allow internal devices (192.168.1.x) to access the internet. Test connectivity by pinging an external public IP. Capture the traffic in Wireshark and analyze the source IP before and after NAT translation.

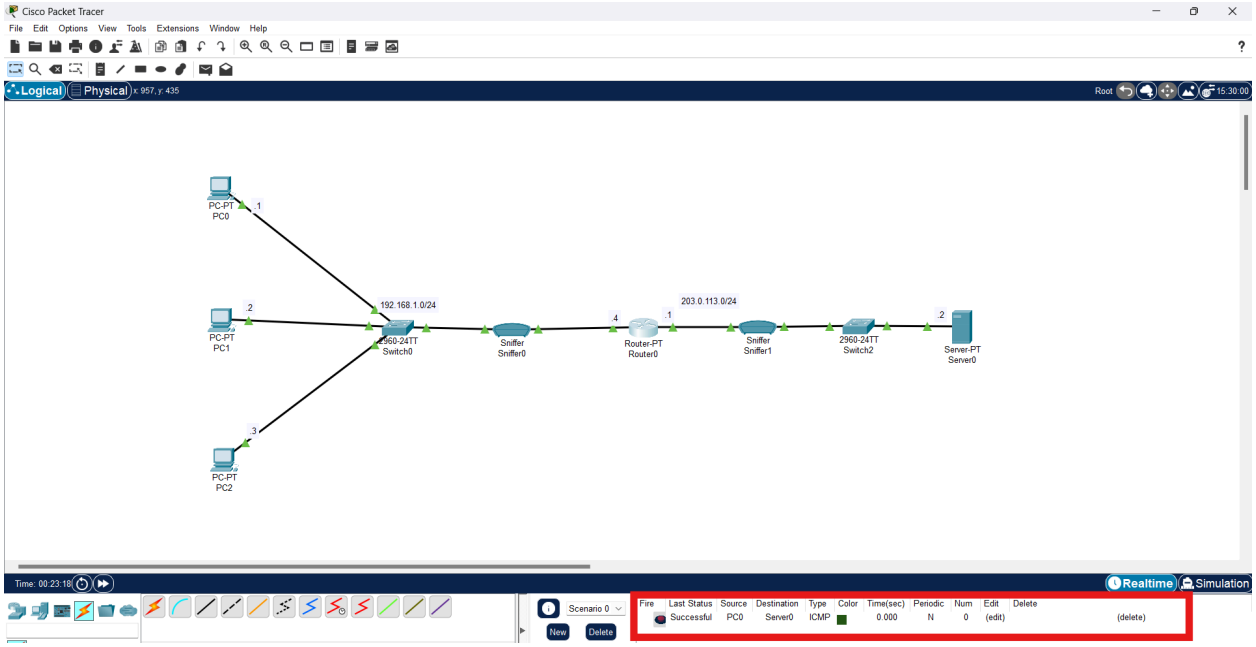
Configure the network topology in Cisco Packet Tracer :



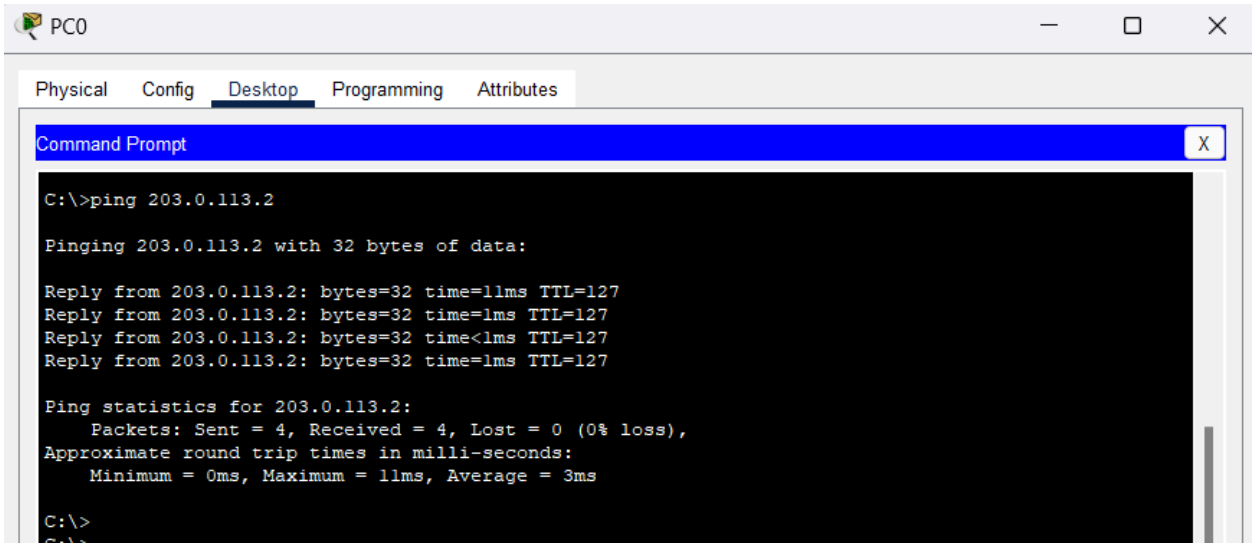
Configure the PC side (FastEthernet0/0) as Inside of NAT and Server Side (FastEthernet1/0) as Outside of NAT, followed by which add the static NAT source IP for each PC IP which will be converted to its NAT IP, then you will be able to see the NAT translations :



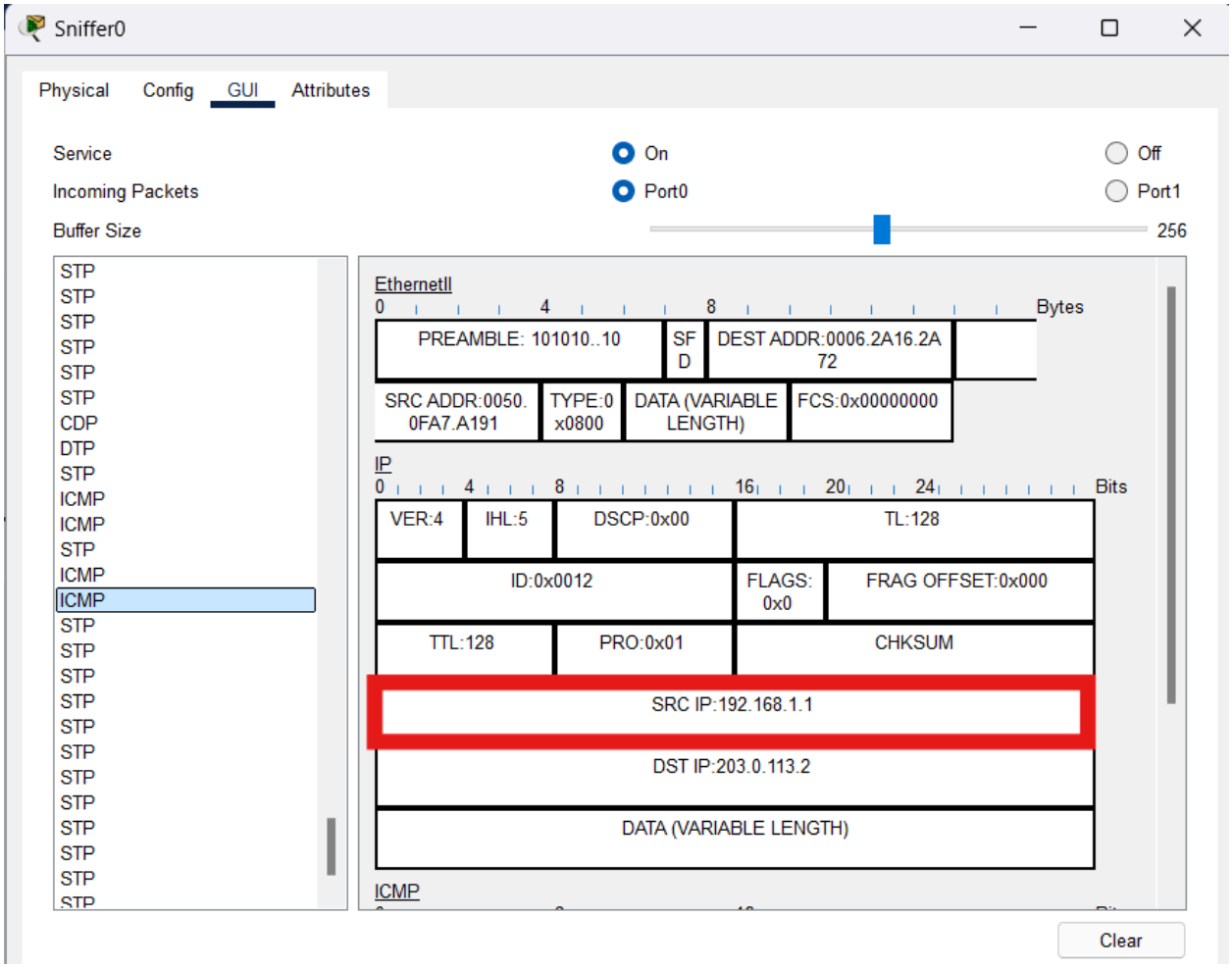
Let's check using PDU from PC1 to server and its successfully working :



Pinging from PC0 to server also we are able to see the successful connection with Server :



Since we don’t have Wireshark in Cisco Packet Tracer, as it is a simulation tool by itself, we can use the Sniffer device to view the Packets that are sent through the network and we see the ICMP packet in the NAT Inside, that the source IP is same as the PC’s IP :



Similarly, in the NAT outside, we are able to see that the Source IP has successfully changed by the NAT in the router as configured by the static NAT using the CLI, from the PC's IP to 100.0.0.1 which was configured. Hence the NAT translation is successful :