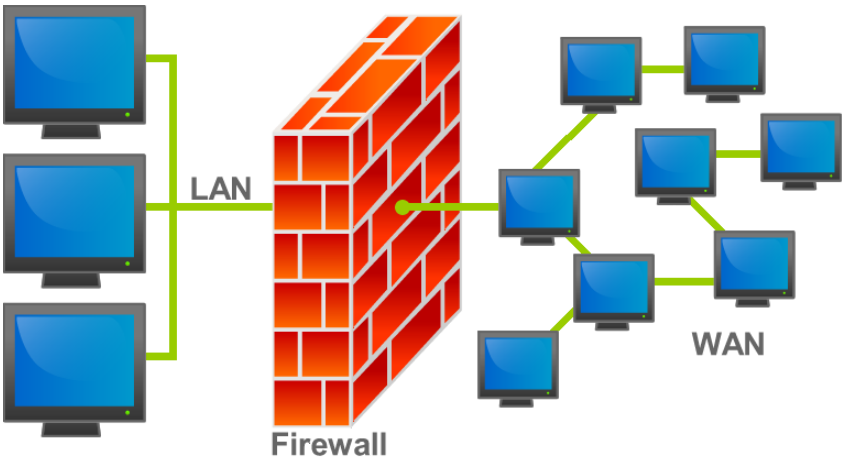
Table of Contents

Introduction to Firewall

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.

Depending on the organization's firewall policy, the firewall may completely disallow some traffic or all traffic, or it may perform verification on some or all of the traffic. There are two commonly used types of firewall policies:

- Whitelisting — The firewall denies all connections except for those specifically listed as acceptable.
- Blacklisting — The firewall allows all connections except those specifically listed as unacceptable.



Firewalls can be standalone systems or they can be included in other infrastructure devices, such as routers or servers.

Type of Firewall	Parameters / Purpose	Layer of Working	Protocols	Attacks
Packet-filtering firewall	Source & Destination IP Addresses Source & Destination Port Numbers Protocols	Layer 3 of OSI Model	ICMP ARP RARP BOOTP DHCP	DoS attacks

Stateful firewall	Source & Destination IP Addresses Source & Destination Port Numbers It has state table, dynamic memory.	Layer 4 of OSI Model	UDP ICMP	DDoS and Vulnerability attacks
Proxy firewall	Shielding and filtering mechanism between internal and external networks. Used for authentication schemes.	Application layer of OSI Model	DNS FTP HTTP ICMP SMTP	Vulnerability attacks
Web application firewall	Protects Web app by applying set of rules to HTTP conversation	Application layer of OSI Model	HTTP HTTPS	SQL injection attack XSS attack DDoS attacks

Components of Firewall

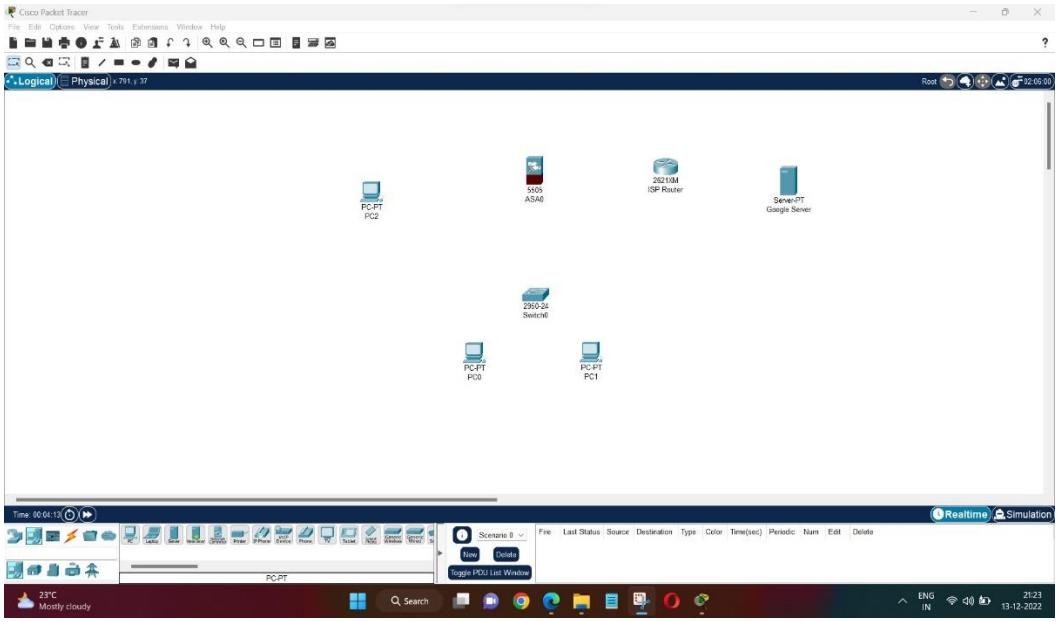
1. Perimeter router
   It is used to provide a link to the public networking system like the internet, or a distinctive organization. It performs the routing of data packets with the help of an appropriate routing protocol. It also provides the filtering of packets and addresses translations.
2. Firewall
   The provision of distinctive levels of security and supervises traffic among each level. Most of the firewalls are present near the router that provides security from external threats, but sometimes the firewall is present in the internal network to protect from internal attacks.
3. Virtual Private Network (VPN)
   Its function is to provide a secure connection among two machines or networks. It provides the secure remote access of the network, thereafter connecting two WAN networks on the same platform while not being physically connected.
4. Intrusion Detection System (IDS)
   It is used to identify, investigate, and resolve unauthorized attacks. A hacker can attack the network in various ways. It can execute a denial-of-service (DoS) attack or an attack from the backside of the network through some unauthorized access.

Firewall Configuration using CISCO Packet Tracer

Step 0 : Outlining the components and their connections

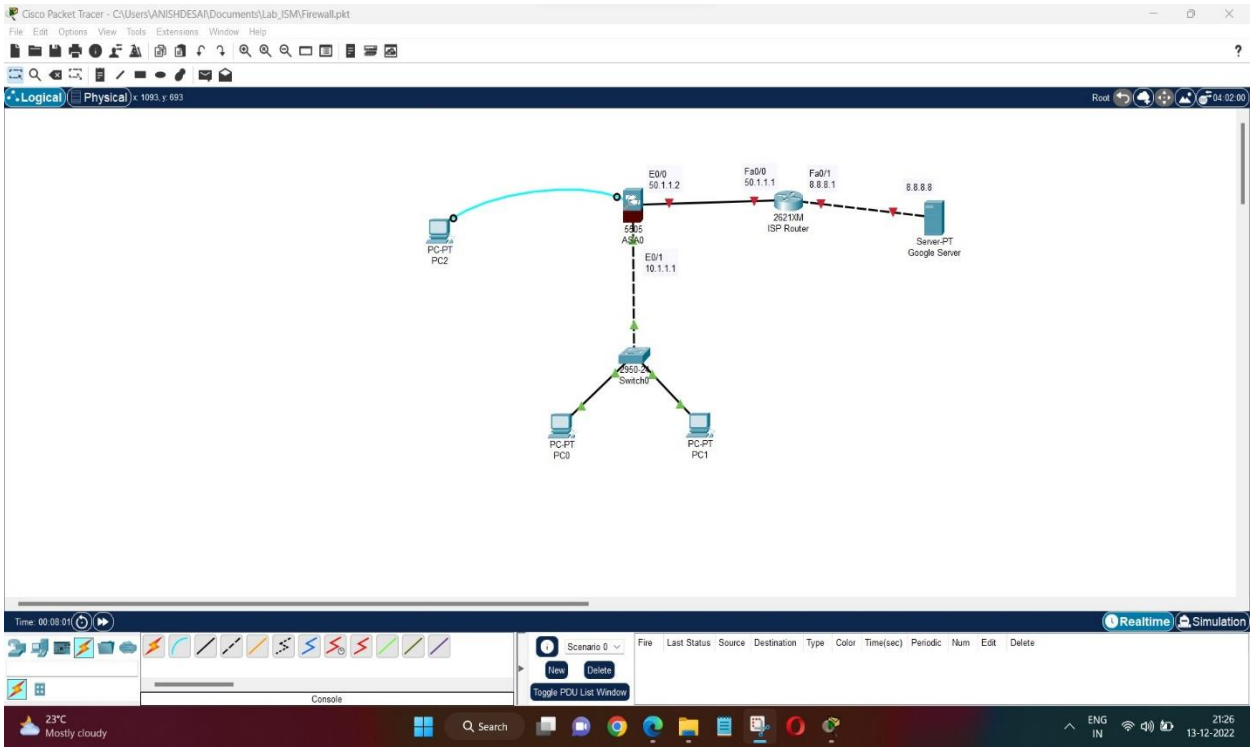
Components used include:

1. PCs – PC0, PC1 & PC2
2. Switch 2950-24T – Switch0
3. Firewall 5505 – ASA0
4. Router 2621XM – ISP Router
5. Server PT – Google Server



Step 1 : Making the topology

Component	Connected to	Via
PC0 – FA0	Switch0 – FA0/1	Copper Straight-through
PC1 – FA0	Switch0 – FA0/2	Copper Straight-through
Switch0 – FA0/3	ASA0 – Ethernet0/1	Copper Cross-Over
PC2 – RS232	ASA0 - Console	Console
ASA0 – Ethernet0/0	ISP Router – FA0/0	Copper Straight-through
ISP Router – FA0/1	Google Sever – FA0	Copper Cross-Over



Step 2 : Assigning IP Address to ASA and ISP Router

Following IP Address allocation is proposed:

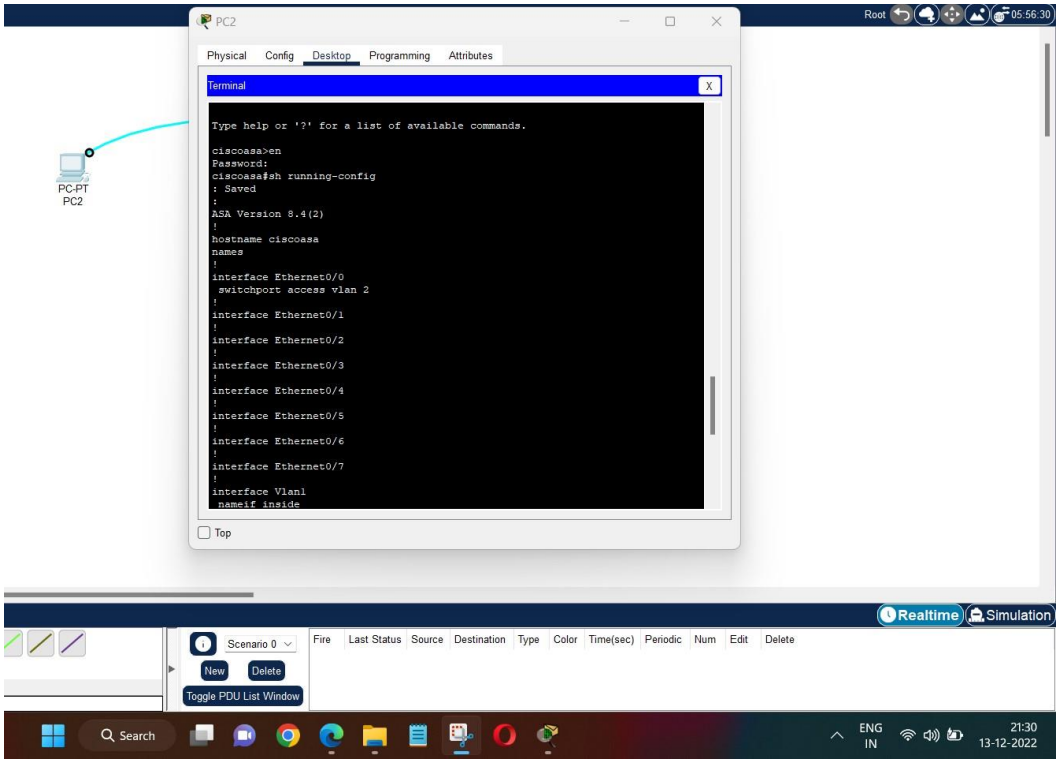
Device	Connection	IP Address
ASA0	Ethernet0/0	50.1.1.2
ISP Router	FA0/0	50.1.1.1
ISP Router	FA0/1	8.8.8.1
Google Server	FA0	8.8.8.8
ASA0	Ethernet0/1	10.1.1.1

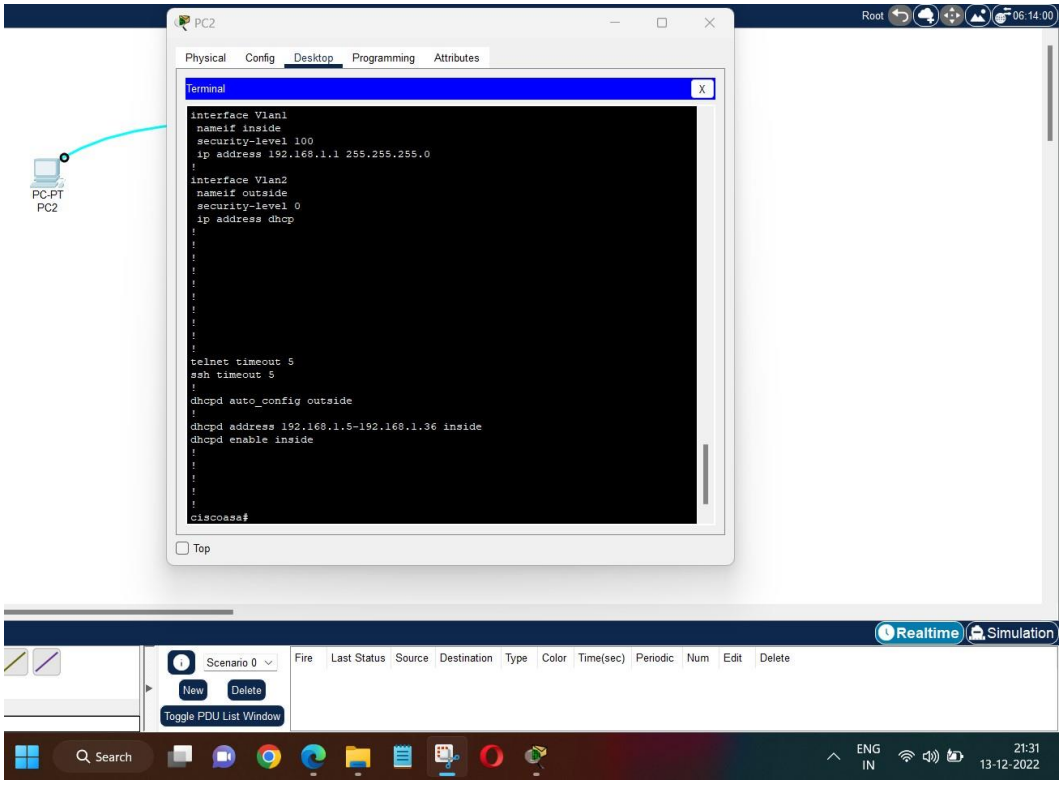
We will configure the firewall using the Command Line Terminal of PC2.

For this, *Click on PC2 → Desktop → Terminal*

To enable and check the basic pre-configuration of firewall, use the commands:

en
sh running-config



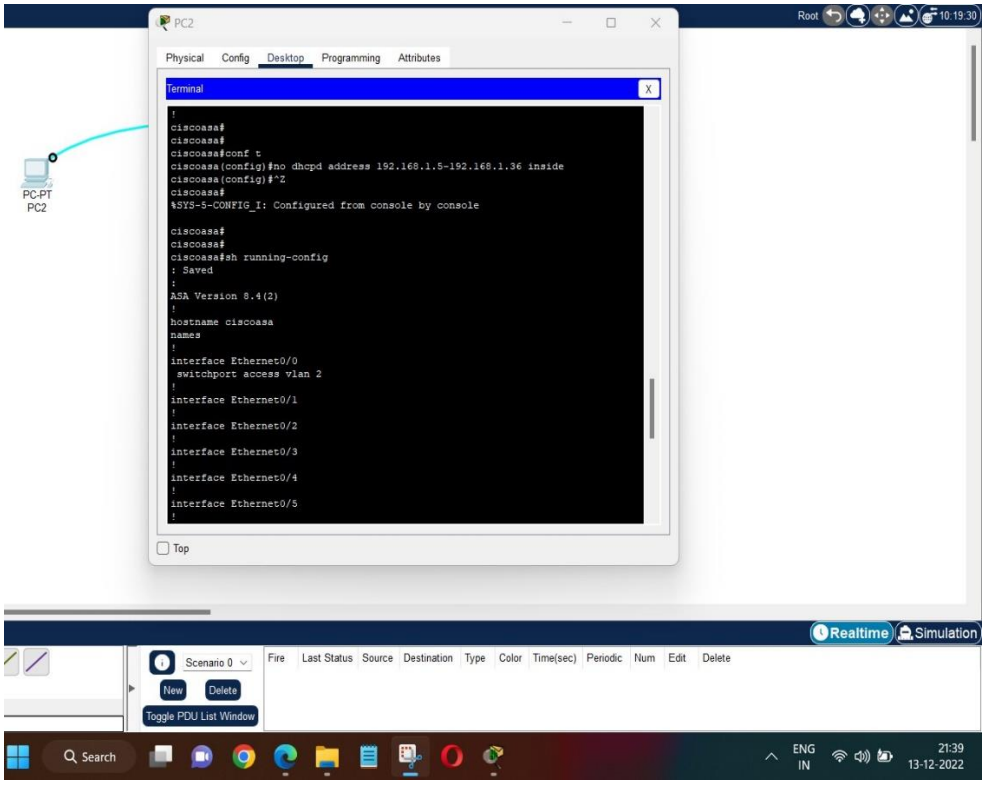


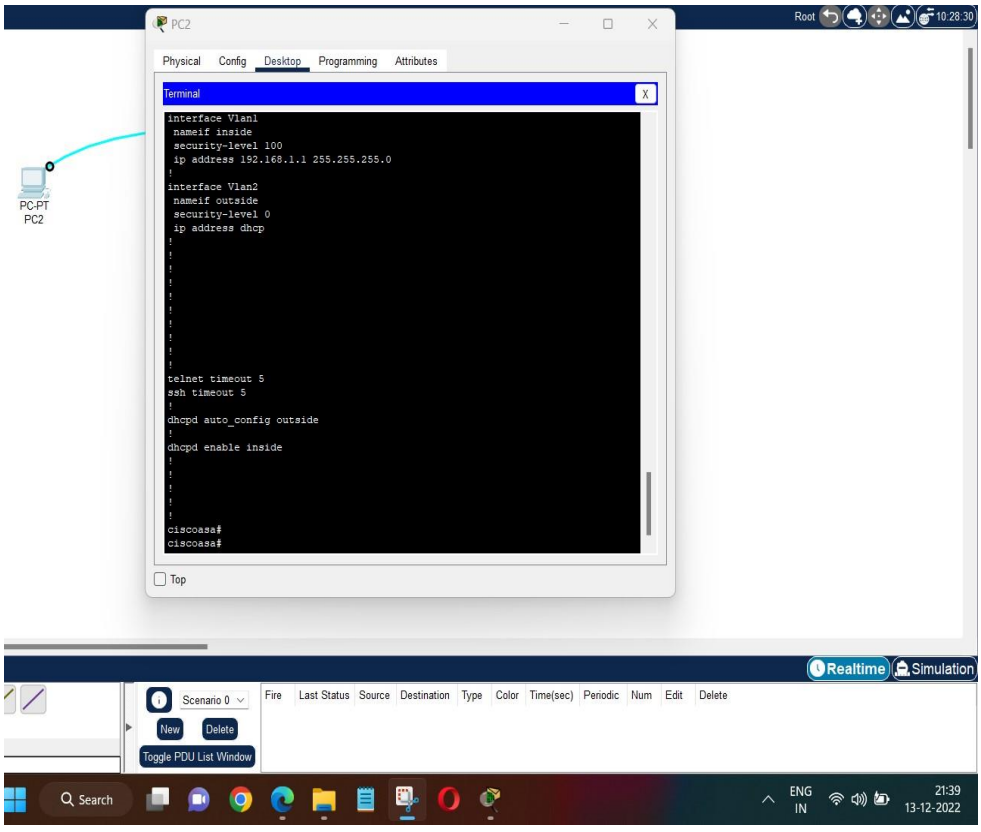
Remove default configuration settings :

conf t

no dhcpd address 192.168.1.5-192.168.1.36 inside (Removed DHCPD Address)

sh running-config





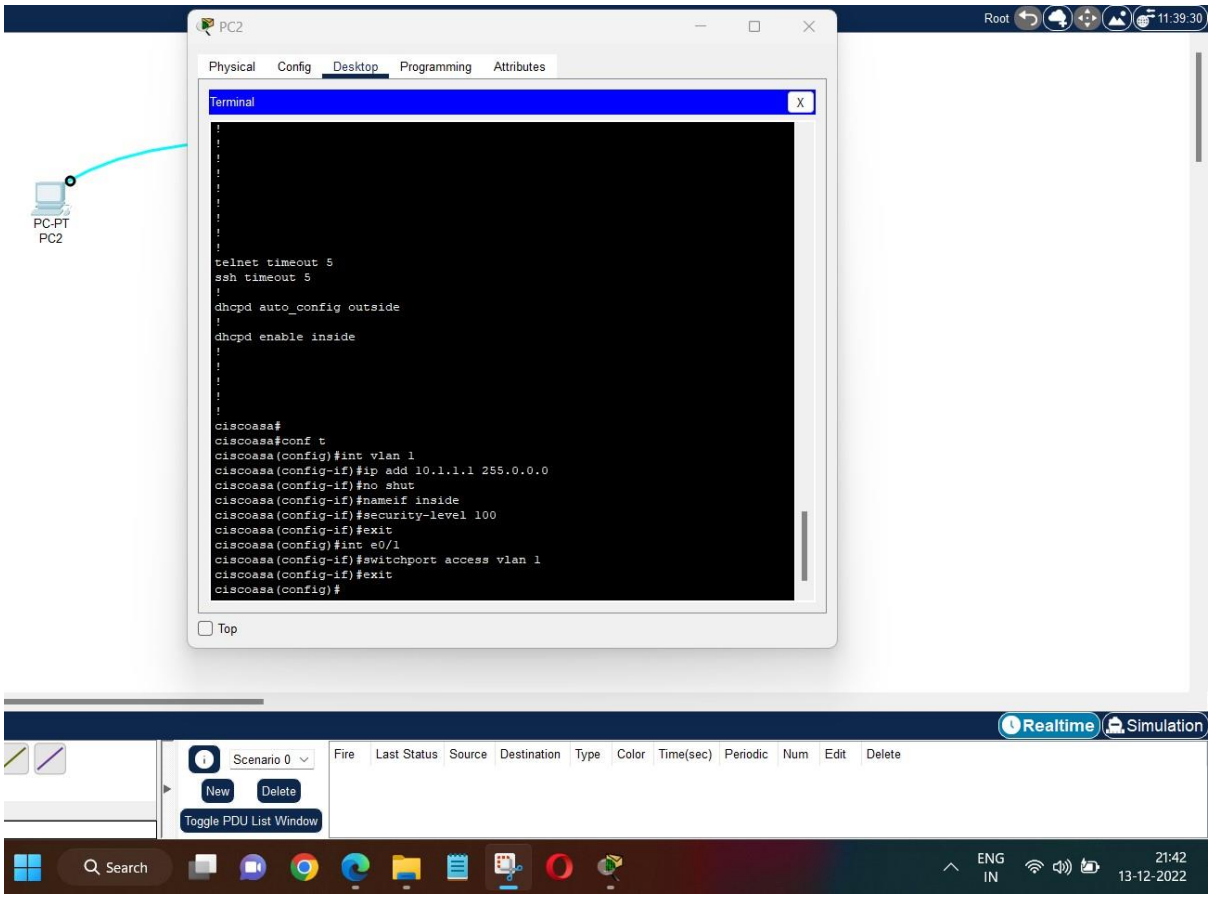
Step 3 : Setting Inside and Outside on ASA Firewall

Rather than removing the default IP Addresses, we can set a new IP Address so that the previous one will automatically get removed.

Port works in two scenarios – either inside where interface connects to private network or outside where interface connects to the public network.

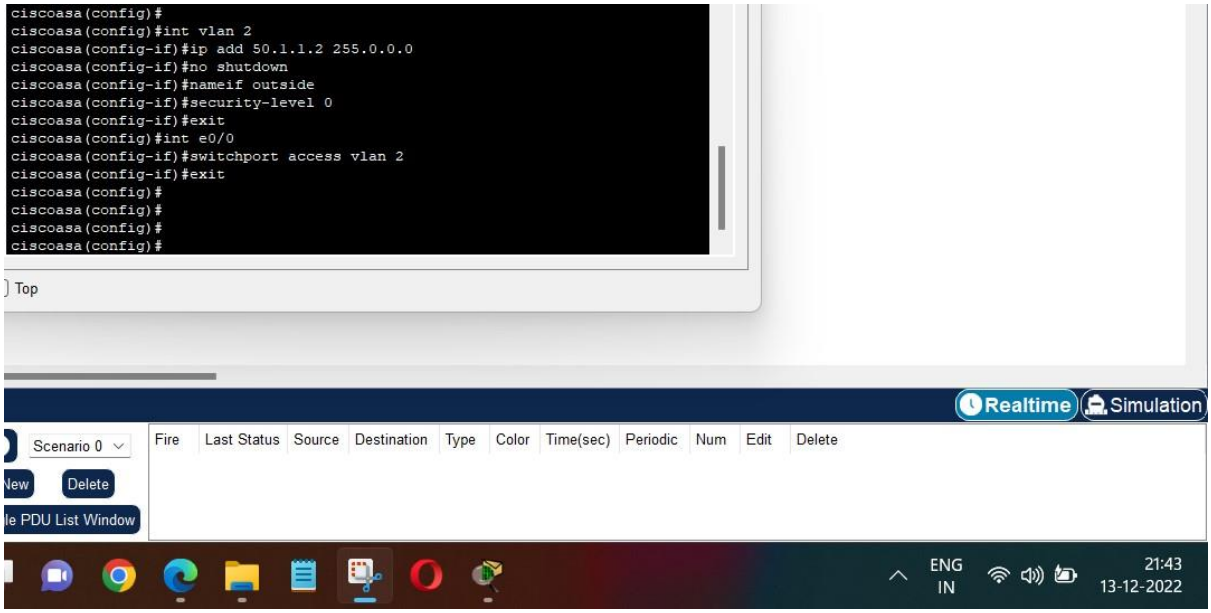
Setting IP Address and Security level of vlan1 (inside) using CLI of PC2

conf t
int vlan 1
ip add 10.1.1.1 255.0.0.0
no shut
nameif inside
security-level 100 (Between 0 and 100 – low to high security)
exit
int e0/1
switchport access vlan 1
exit



Setting IP Address and Security level of vlan2 (outside) using CLI of PC2

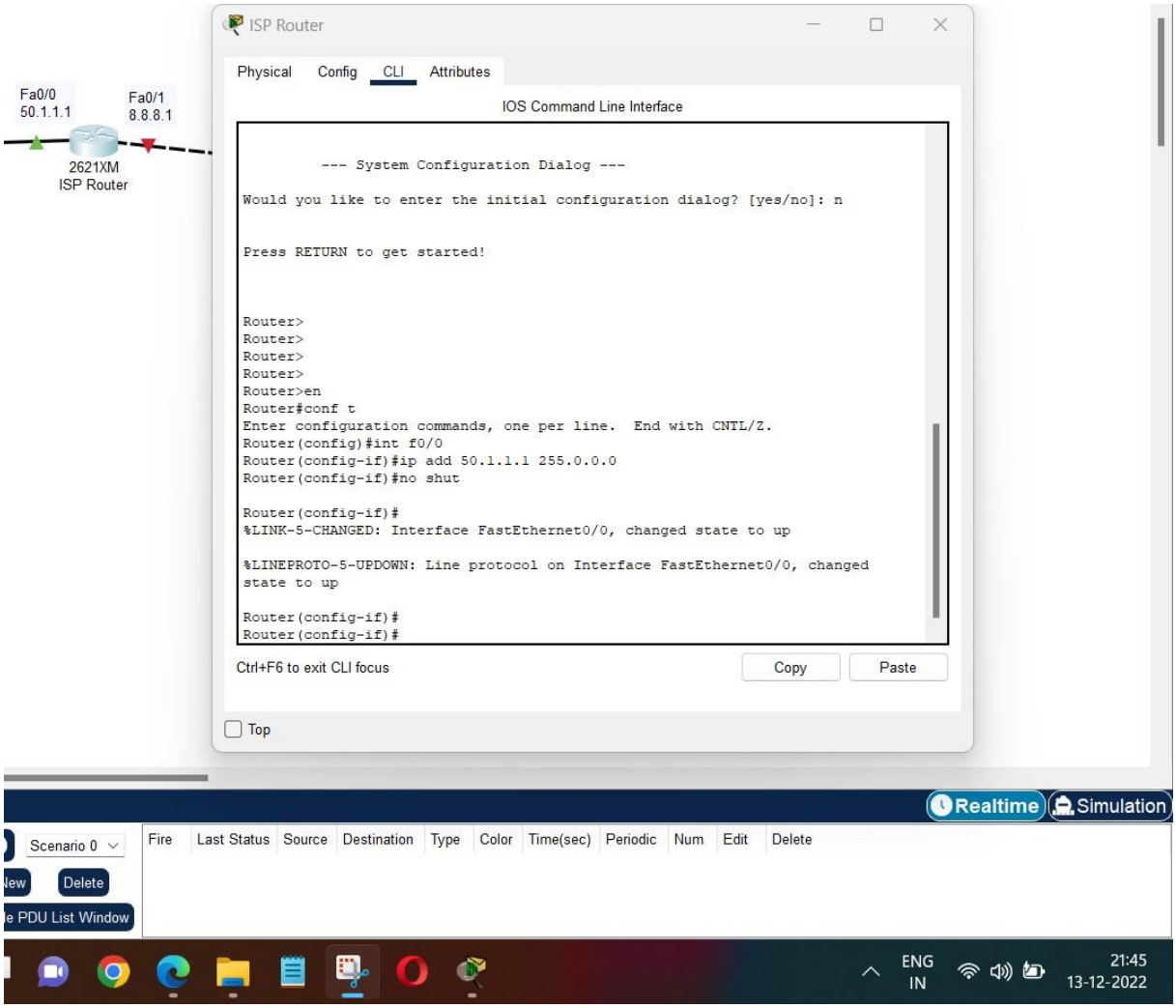
conf t
int vlan 1
ip add 50.1.1.2 255.0.0.0
no shut
nameif outside
security-level 0 (Between 0 and 100 – low to high security)
exit
int e0/0
switchport access vlan 2
exit



Setting IP Address of ISP Router

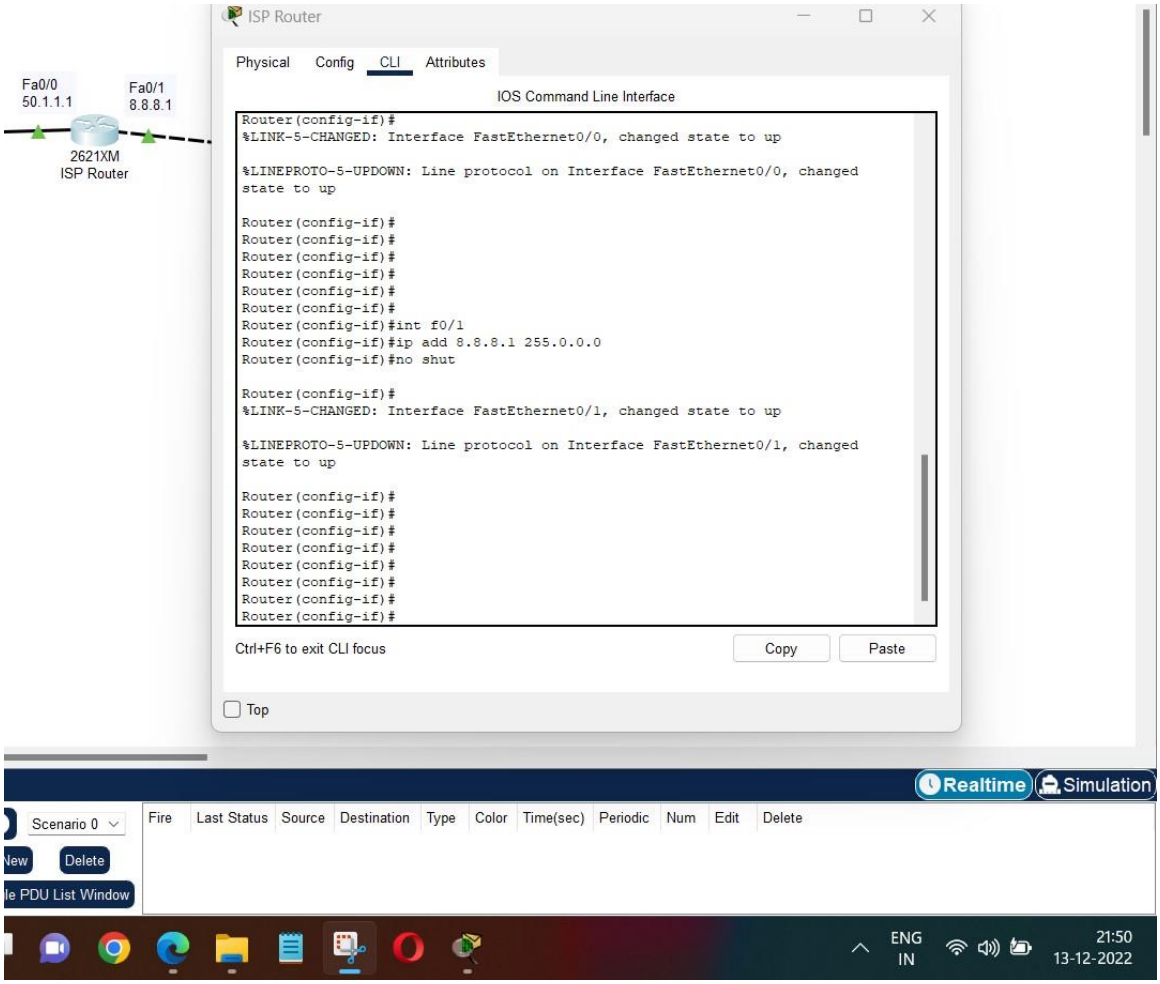
Enable the configuration and then set the IP Address by configuring the FA0/0 interface of the ISP Router.

en
conf t
int f0/0
ip add 50.1.1.1 255.0.0.0
no shut
exit

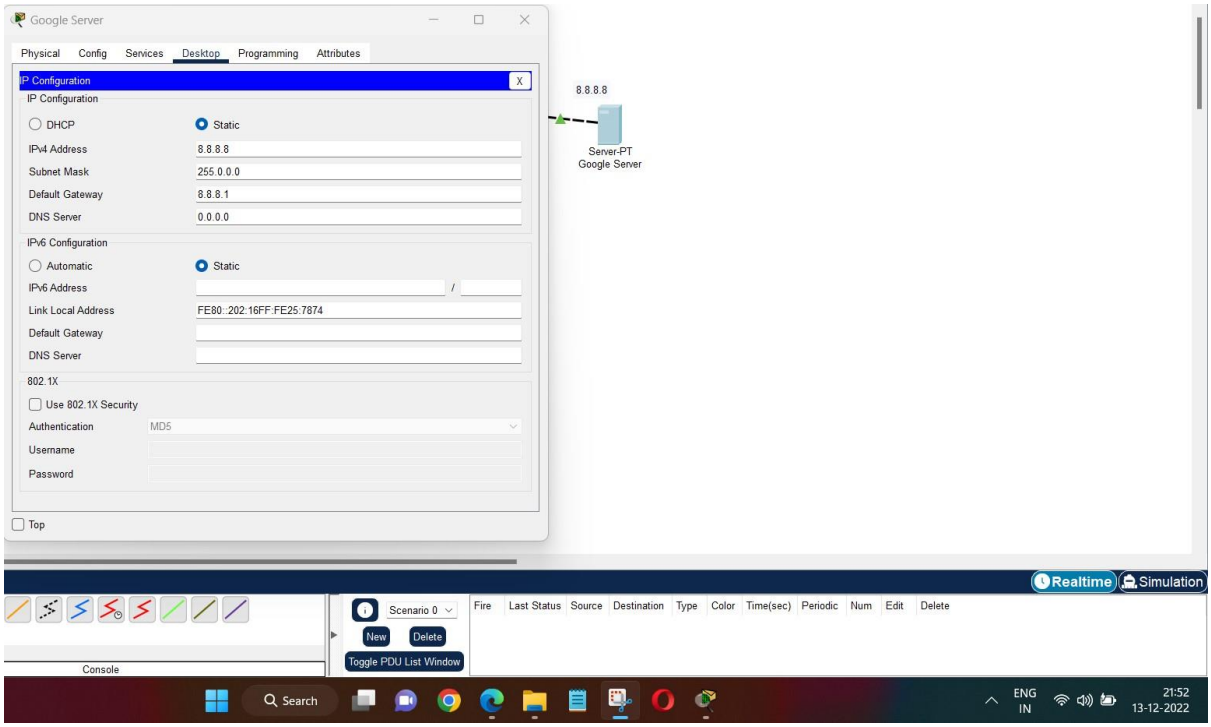


Enable the configuration and then set the IP Address by configuring the FA0/1 interface of the ISP Router.

int f0/1
ip add 8.8.8.1 255.0.0.0
no shut
exit



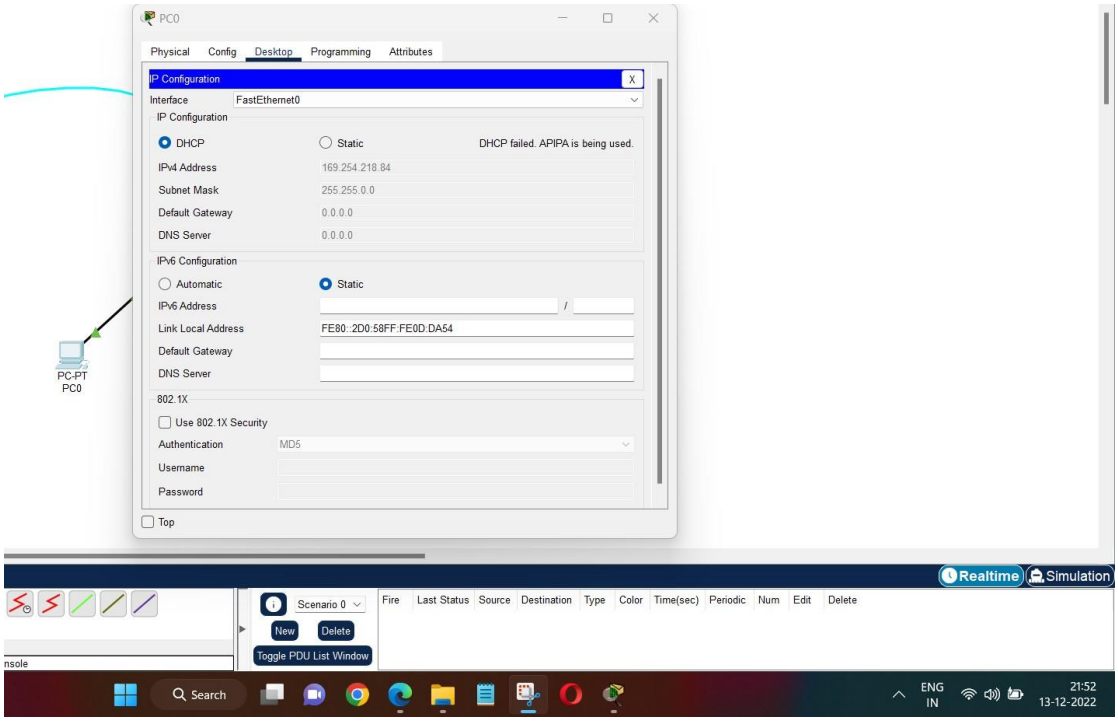
Set the IP Address by configuring the FA0 interface of the Google Server



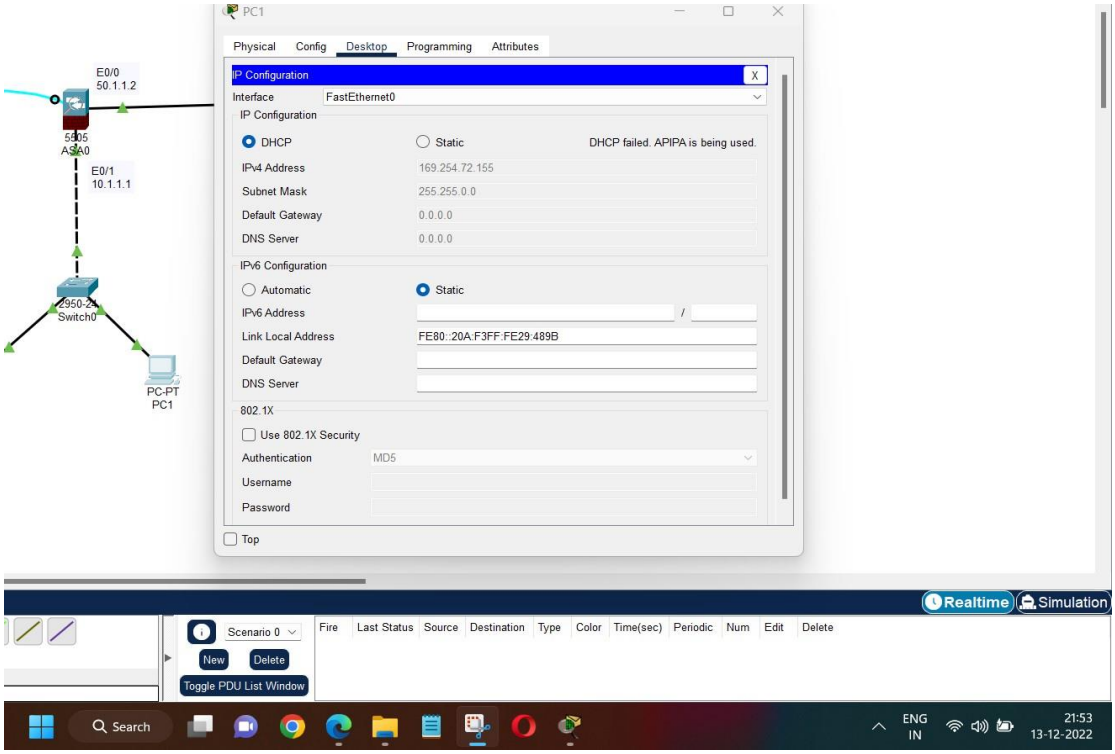
Step 4 : Configuration of DHCP Server and DNS IP on ASA

The PCs connected to the interface would automatically be allotted IP Addresses by the firewall.

Set IP Configuration of PC0 from Static to DHCP



Set IP Configuration of PC1 from Static to DHCP

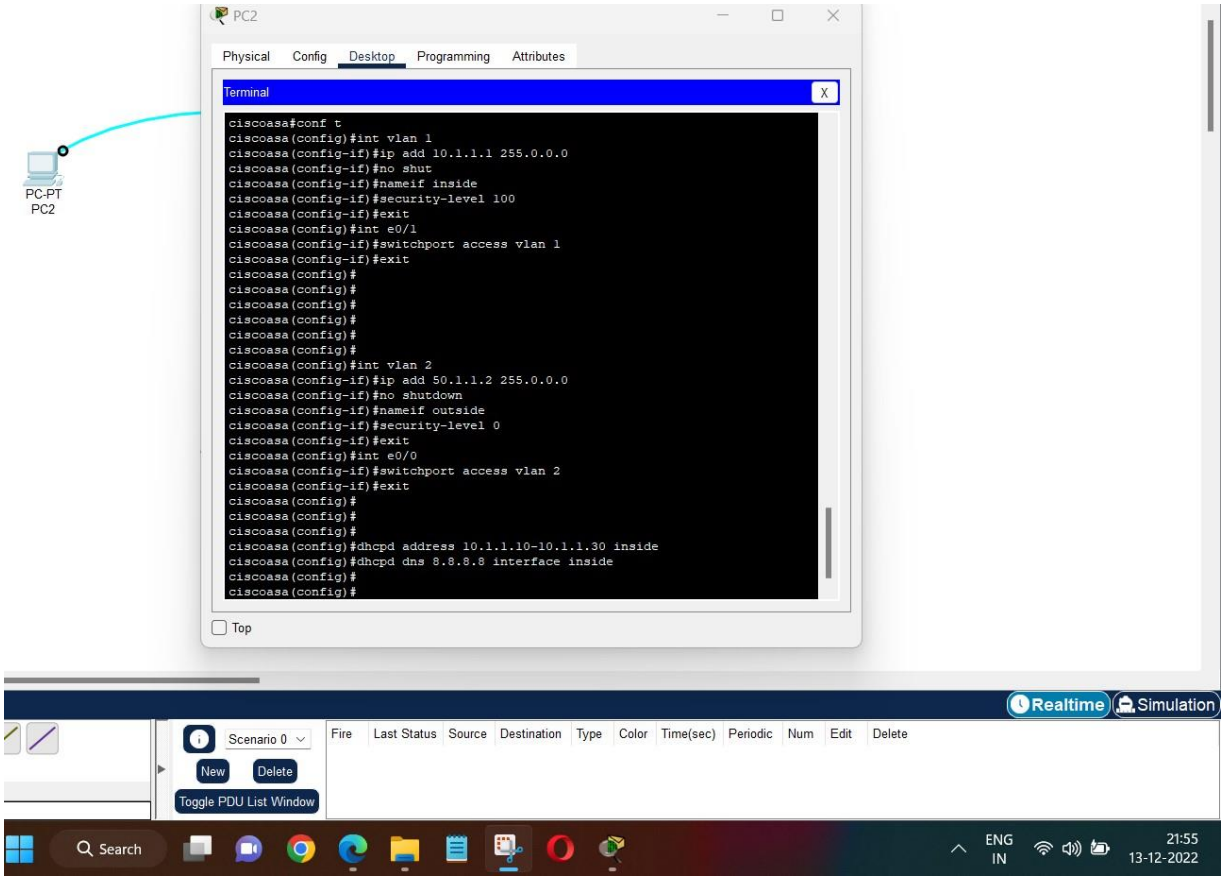


The DHCP addresses won't be provided as of now.

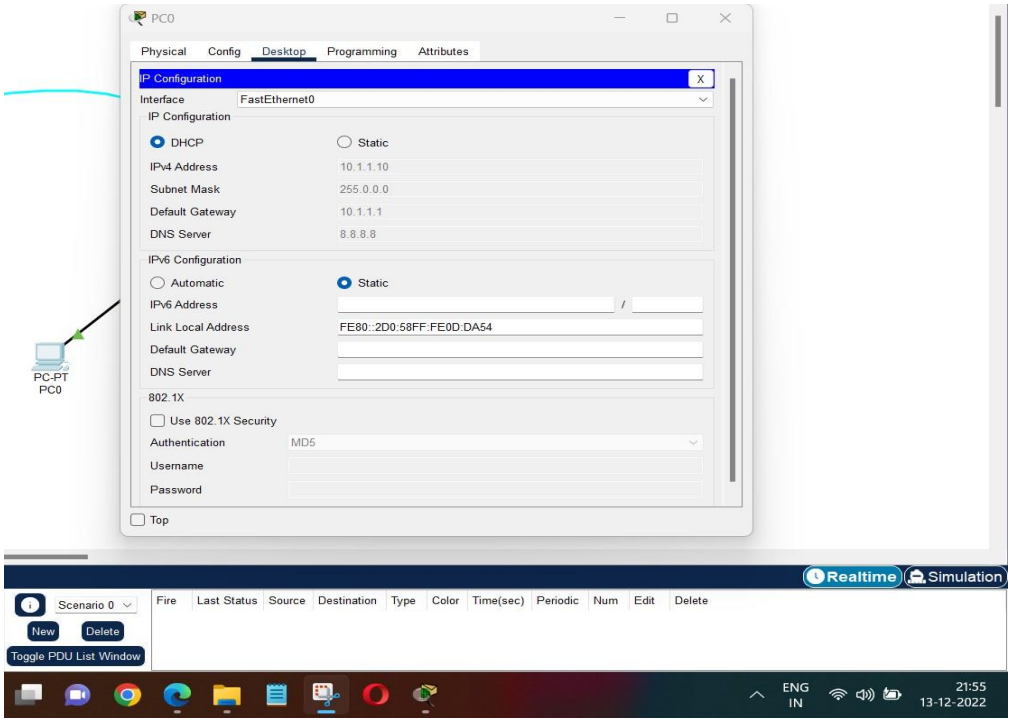
Setting DHCP Server and the DNS IP of firewall using CLI of PC2

Using global configuration mode:

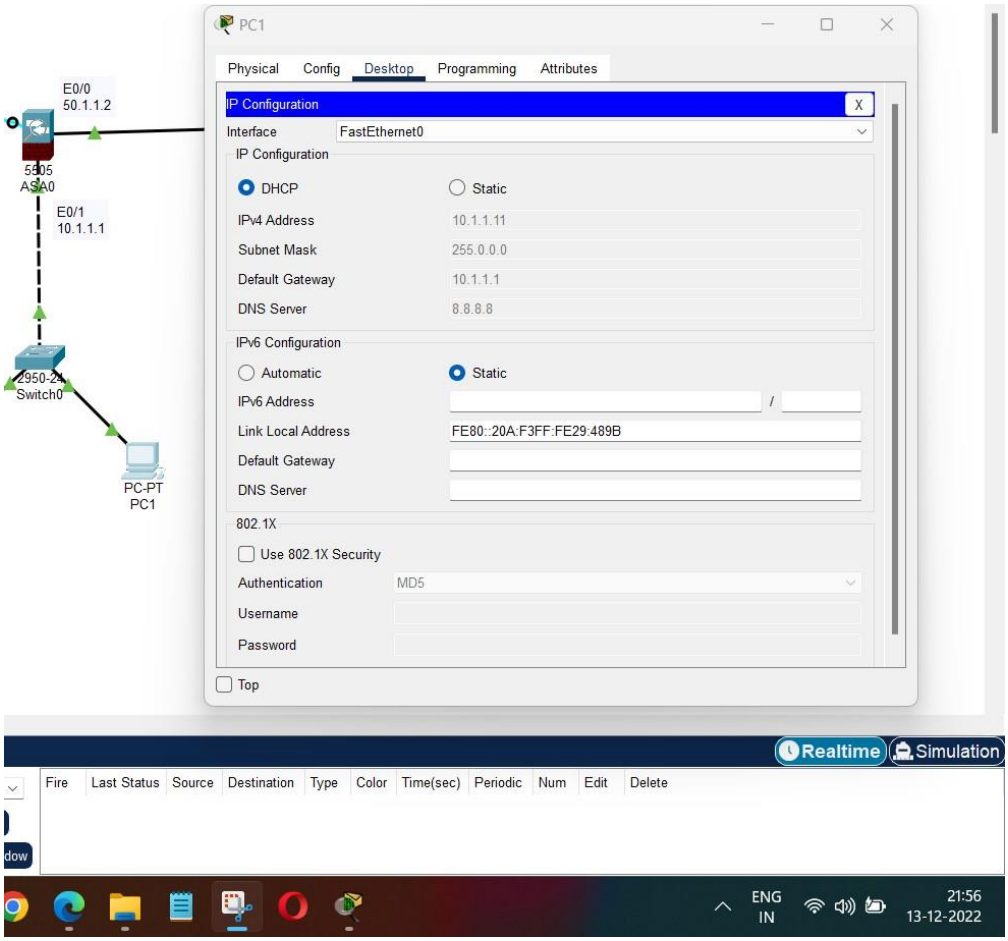
dhcpd address 10.1.1.10-10.1.1.30 inside (Specifying the DHCP range)
dhcpd dns 8.8.8.8 interface inside (Setting DNS IP)



DHCP Server providing IP Address to PC0



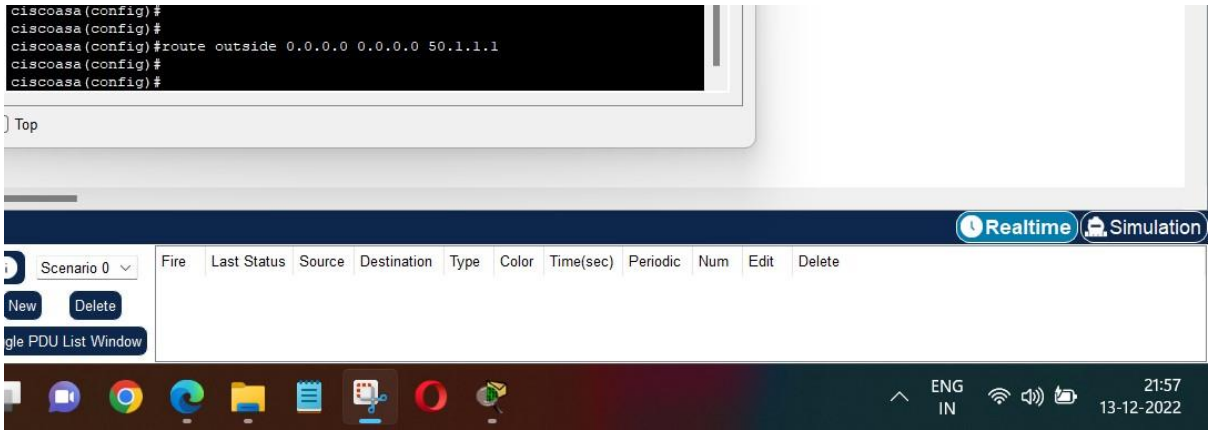
DHCP Server providing IP Address to PC1



Step 5 : Configuration of Default Route on ASA

To configure the default route on ASA using CLI Terminal of PC2

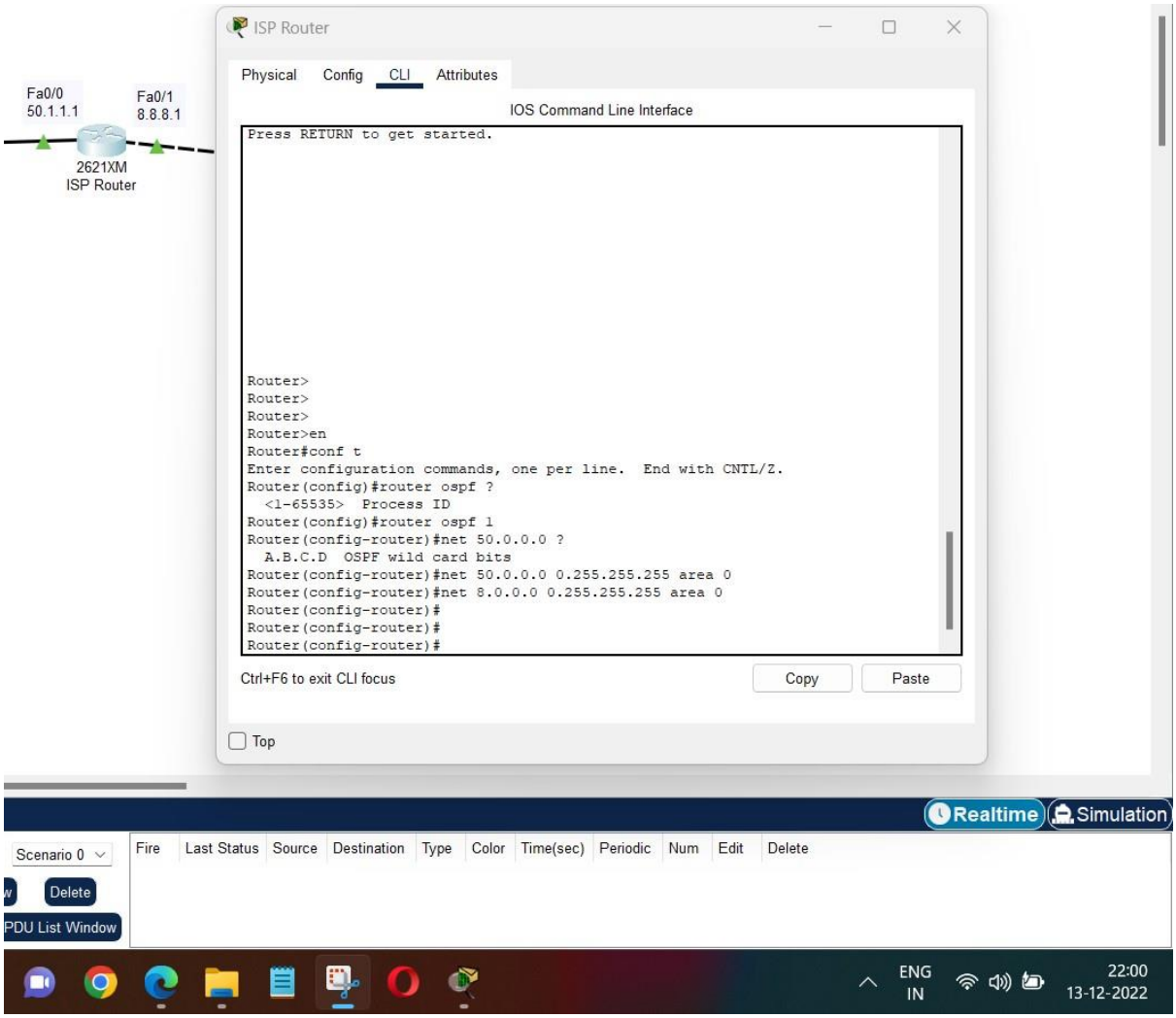
route outside 0.0.0.0 0.0.0.0 50.1.1.1 (IPAddress SubnetMask DefaultRoute)



Step 6 : Configuration of OSPF on ISP Router

Configure OSPF or any dynamic routing protocol by enabling global configuration mode

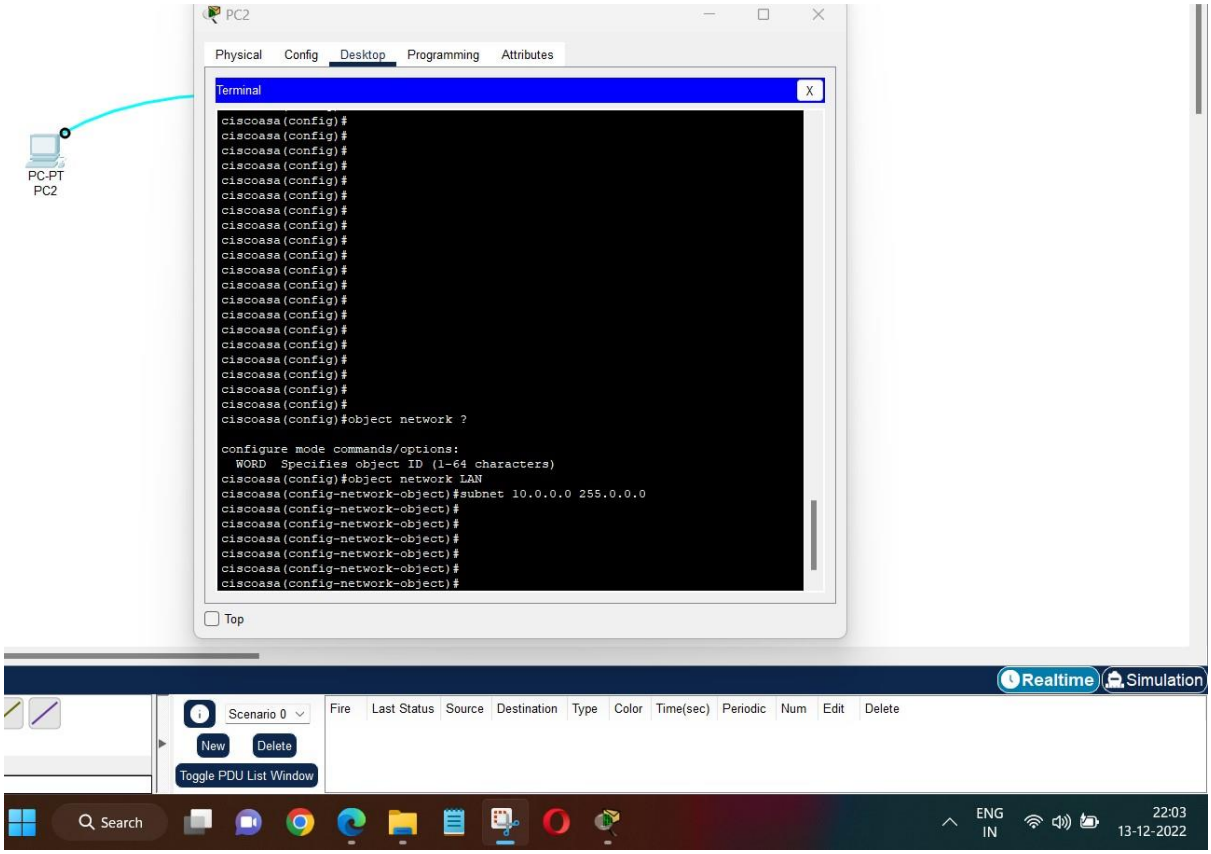
en
conf t
router ospf ?
router ospf 1 (Process ID)
net 50.0.0.0 ?
(Networks directly connected with the router)
net 50.0.0.0 0.255.255.255 area 0
net 8.0.0.0 0.255.255.255 area 0



Step 7 : Creation of Object Network and Enable NAT on ASA

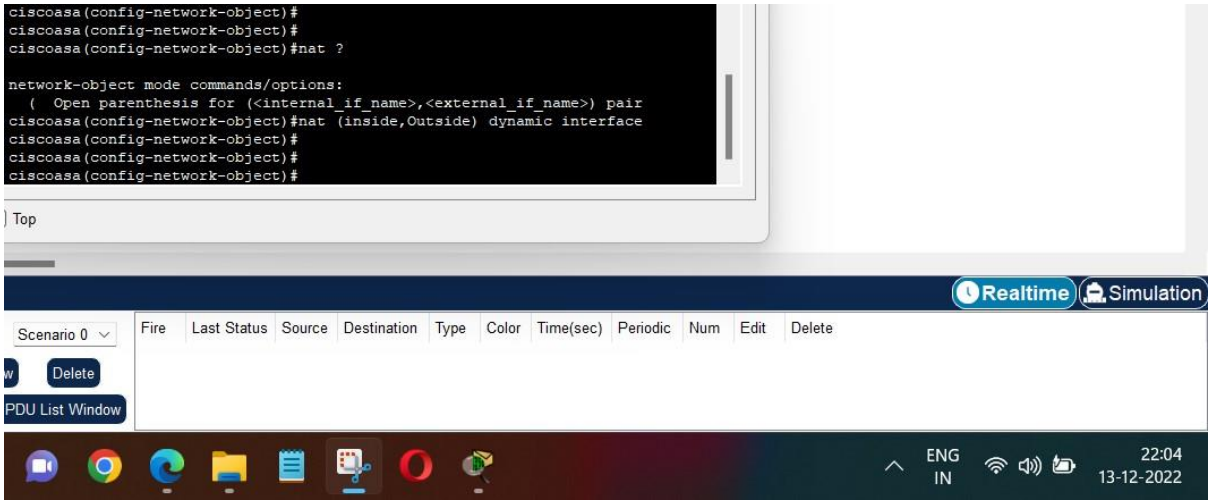
Create object network using CLI Terminal of PC2

object network ?
object network LAN
subnet 10.0.0.0 255.0.0.0



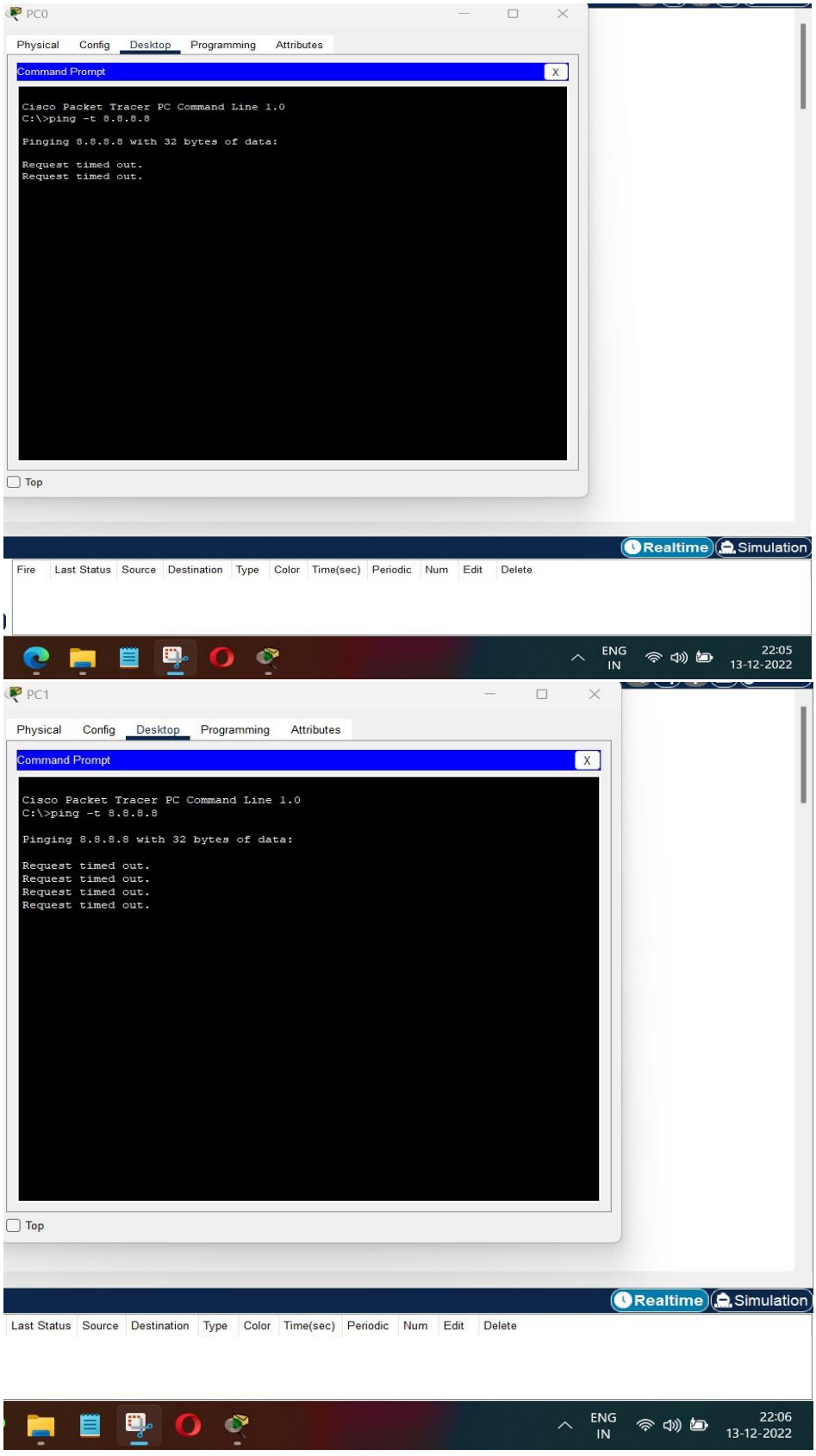
Enabling NAT on ASA

nat ?
nat (inside,Outside) dynamic interface



Checking Communication

Now, if we try to ping Google Server using Command prompt of PC0 and PC1, we aren't able to get a response.

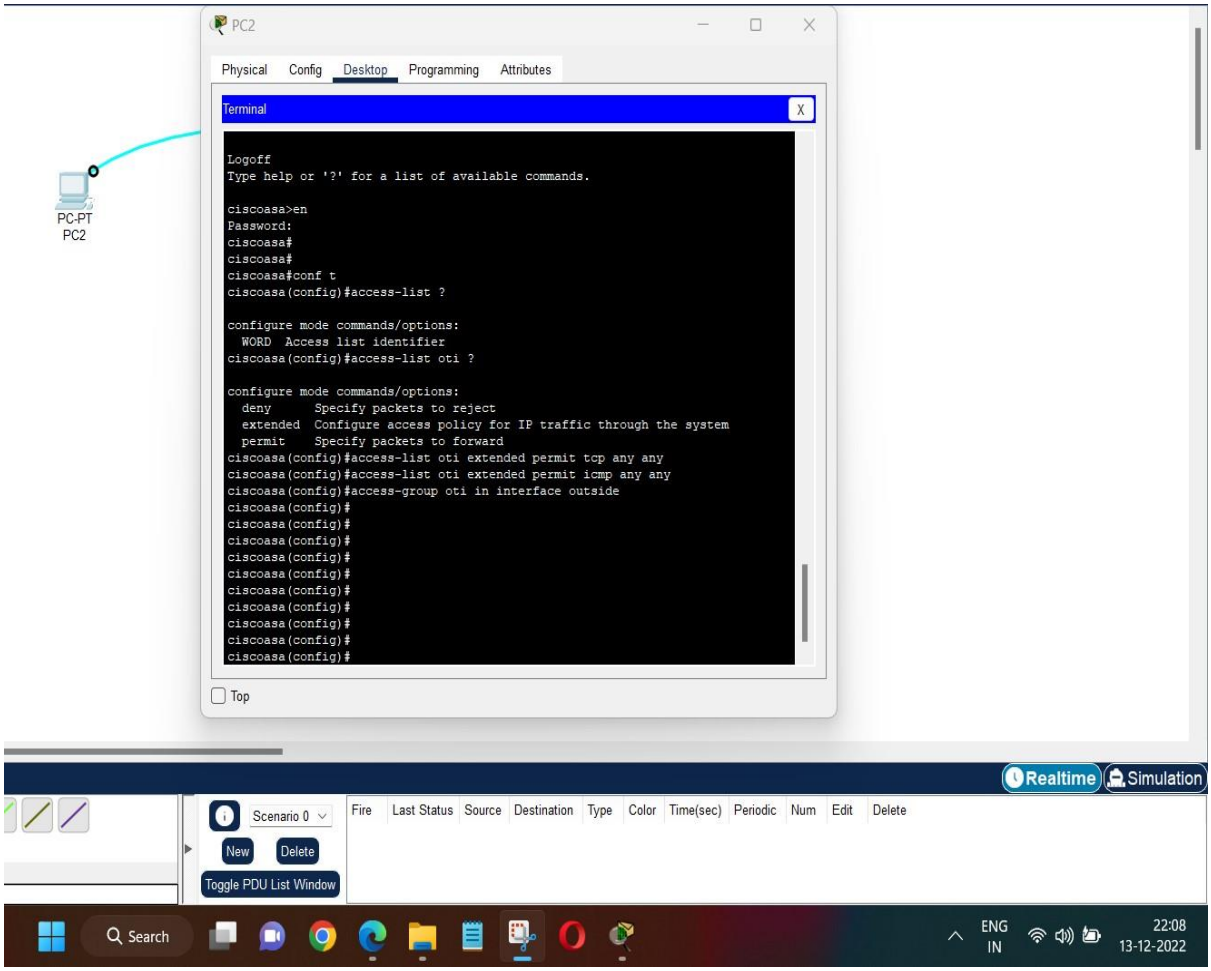


To solve this issue, we will have to configure and create ACL on ASA.

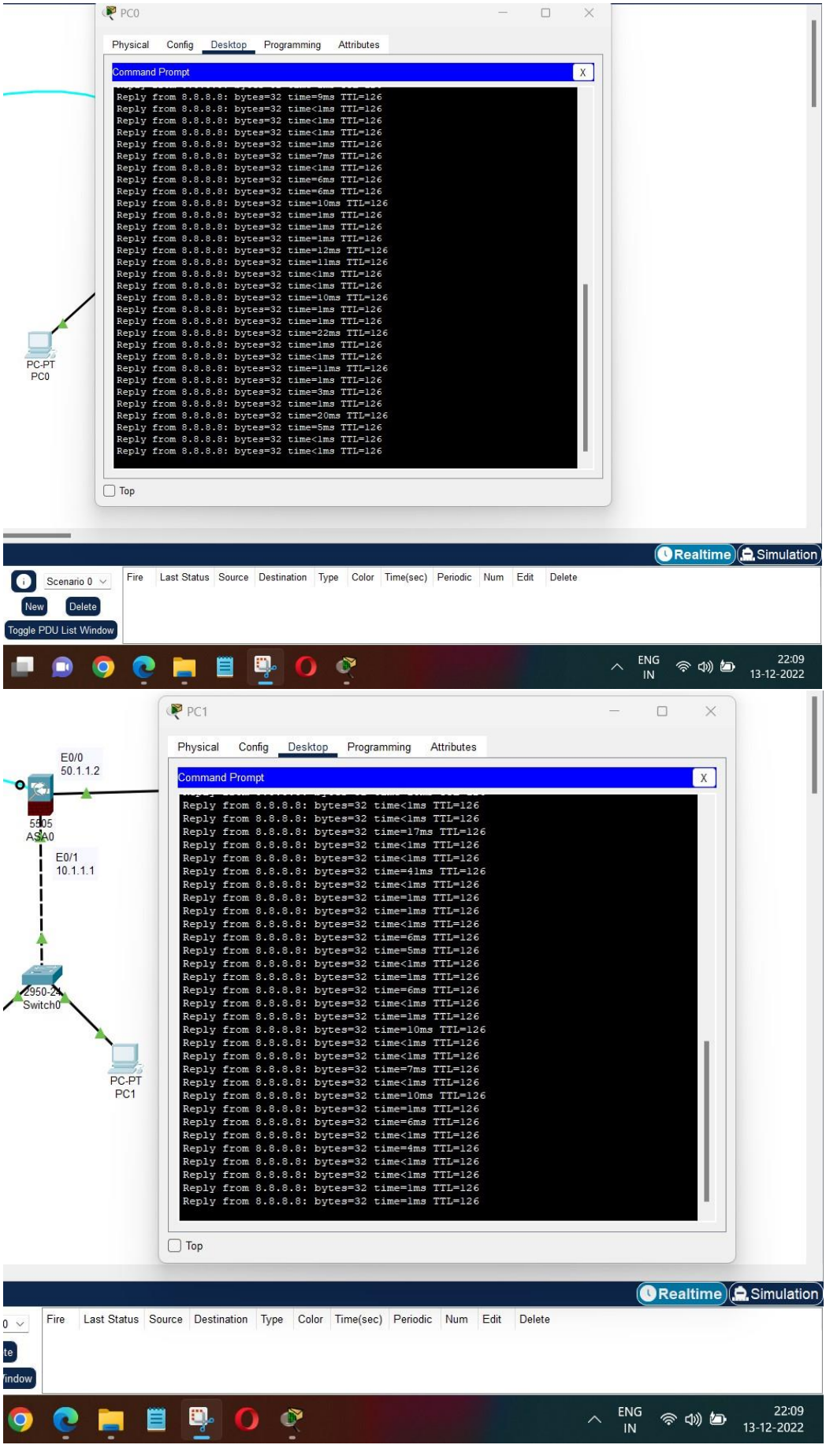
Step 8 : Create ACL on ASA

Using CLI Terminal of PC2 and enabling global configuration

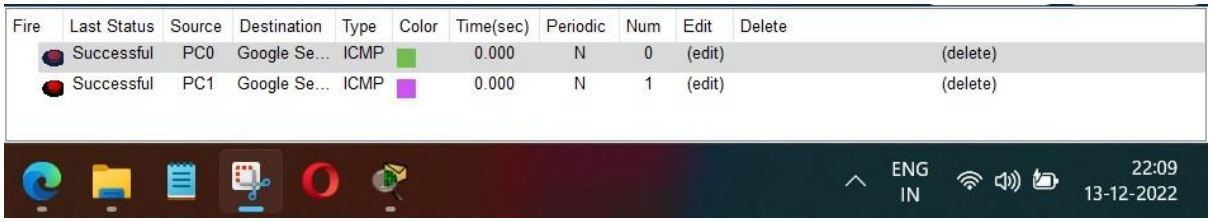
conf t
access-list ?
access-list oti ?
access-list oti extended permit tcp any any (From any source to any destination)
access-list oti extended permit icmp any any
access-group oti in interface outside



The request-response mechanism is now perfectly working between the Google Server and the PCs 0 & 1 as the firewall allows the communication.


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Reply from 8.8.8.8: bytes=32 time=9ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=7ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=6ms TTL=126
Reply from 8.8.8.8: bytes=32 time=6ms TTL=126
Reply from 8.8.8.8: bytes=32 time=10ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=12ms TTL=126
Reply from 8.8.8.8: bytes=32 time=11ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=10ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=11ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=3ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=20ms TTL=126
Reply from 8.8.8.8: bytes=32 time=5ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Top
PC-PT
PC0
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
ENG
IN
22:09
13-12-2022
PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=17ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=41ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=6ms TTL=126
Reply from 8.8.8.8: bytes=32 time=5ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=6ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=10ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=7ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=10ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=6ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=4ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Top
E0/0
50.1.1.2
5505
ASA0
E0/1
10.1.1.1
2950-24
Switch0
PC-PT
PC1
Realtime
Simulation
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
ENG
IN
22:09
13-12-2022

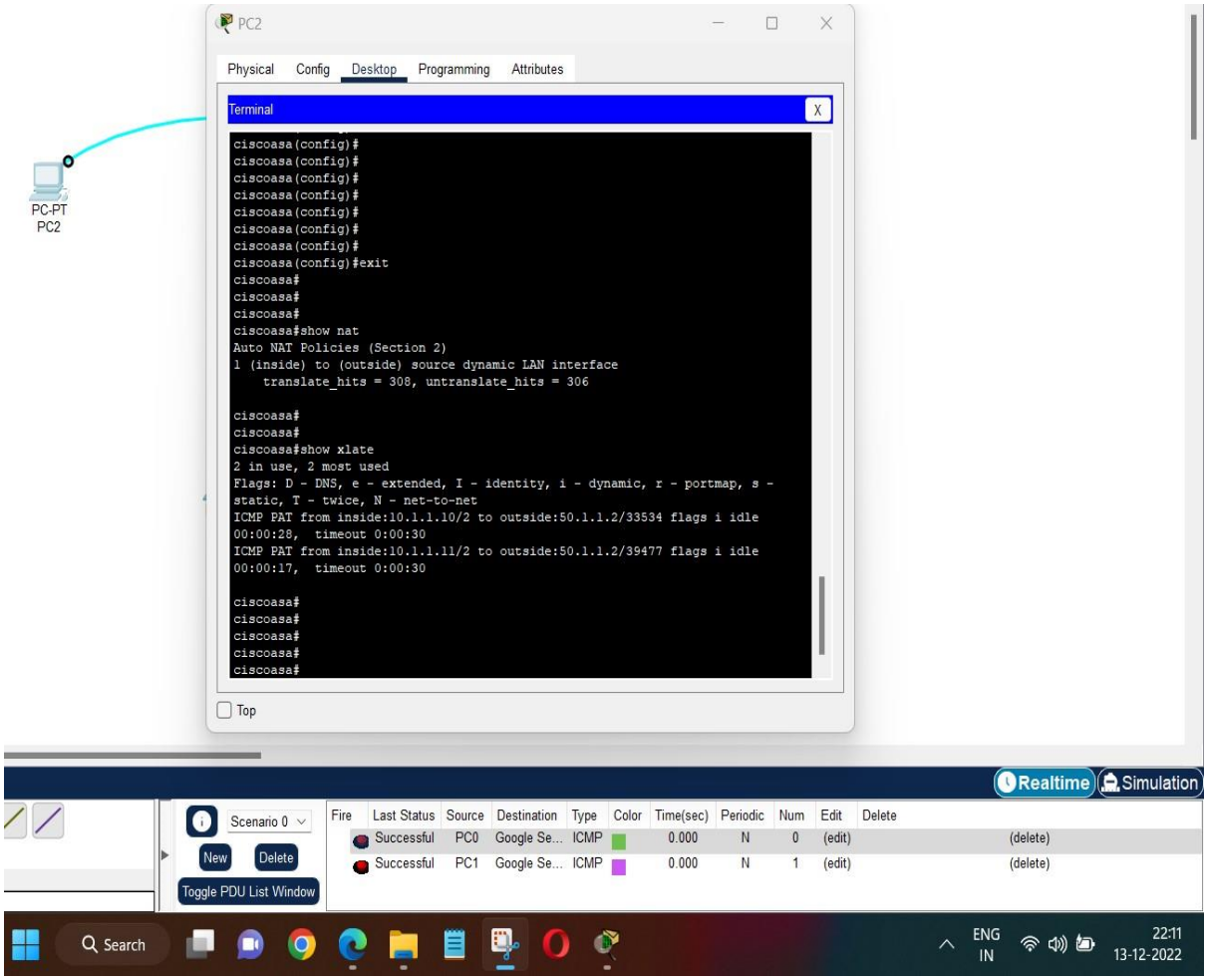
Simple PDUs successfully sent from PC0 and PC1 to Google Server.



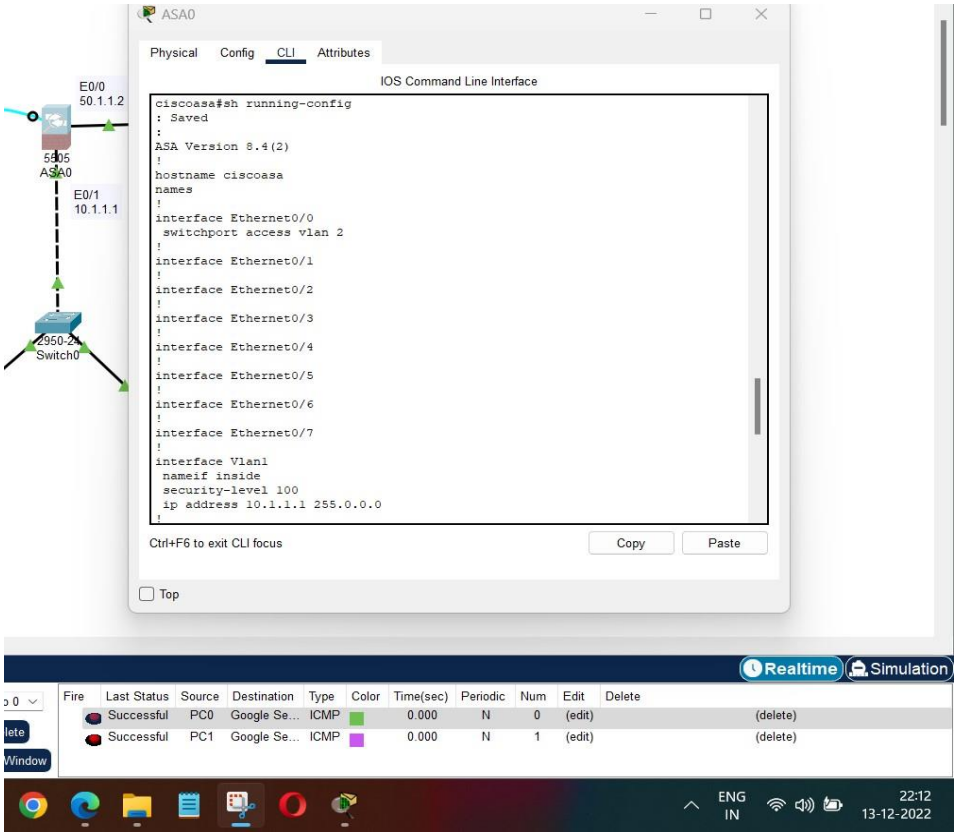
Step 9 : Verification

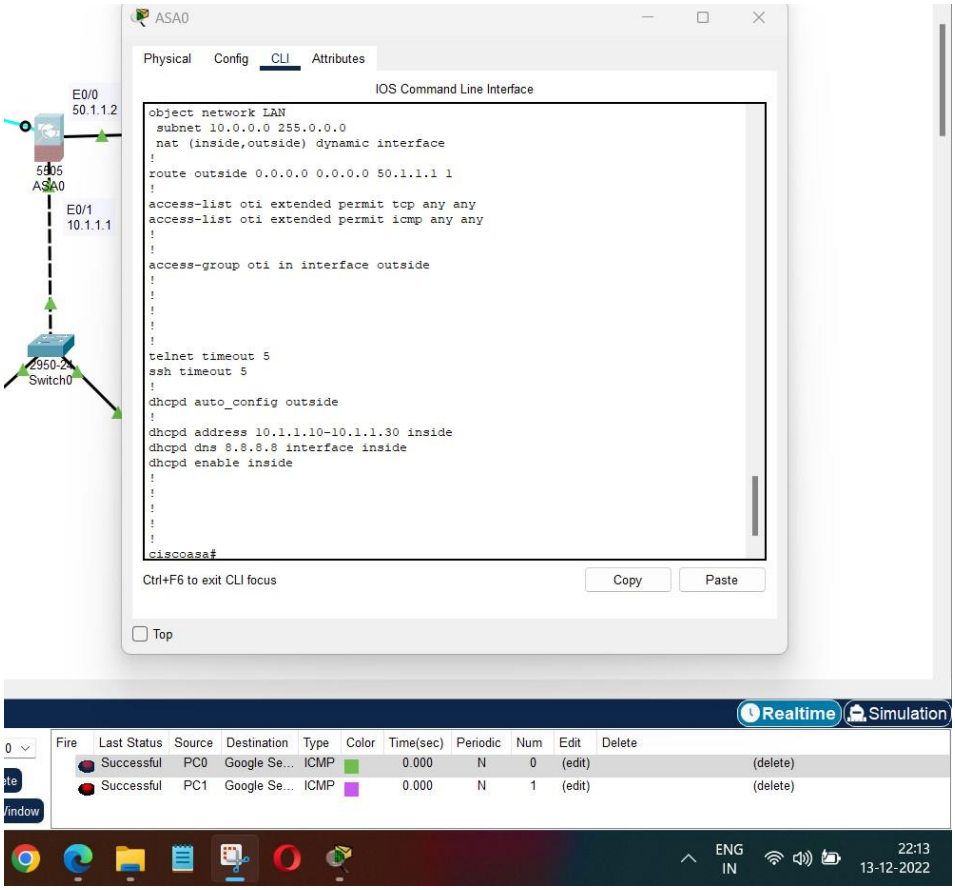
Using privilege mode of the firewall

show nat
show xlate

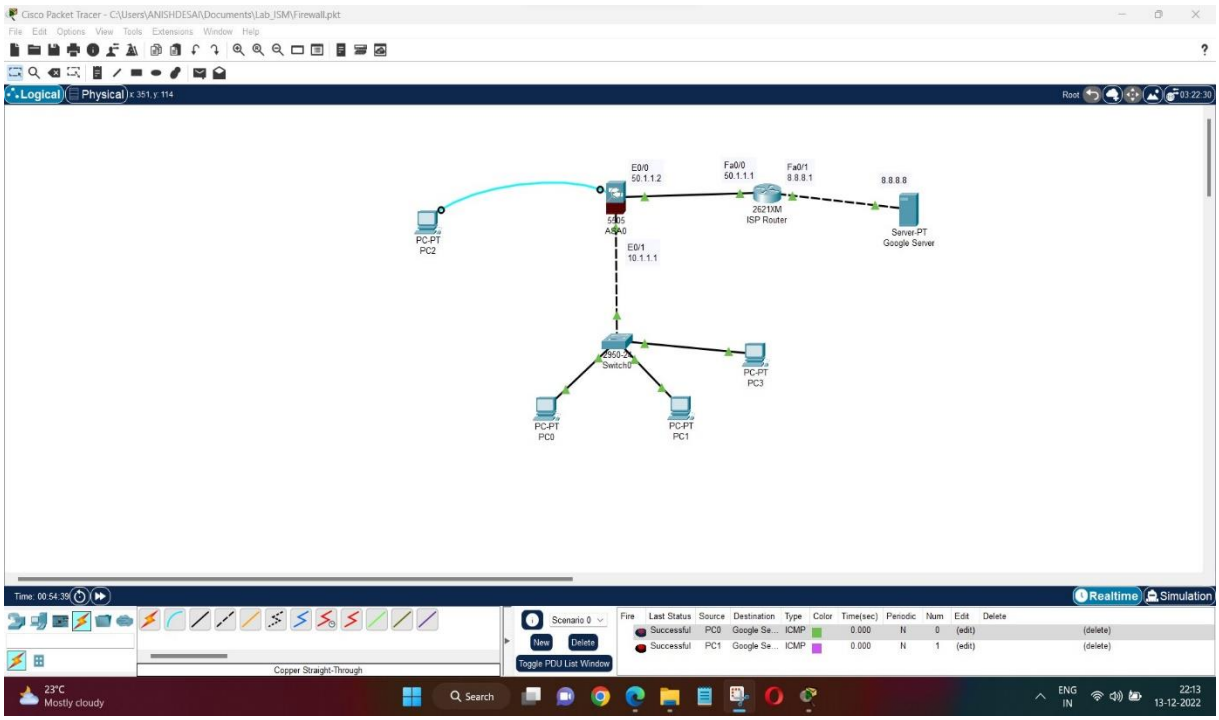


Using running configuration on CLI Terminal of ASA firewall

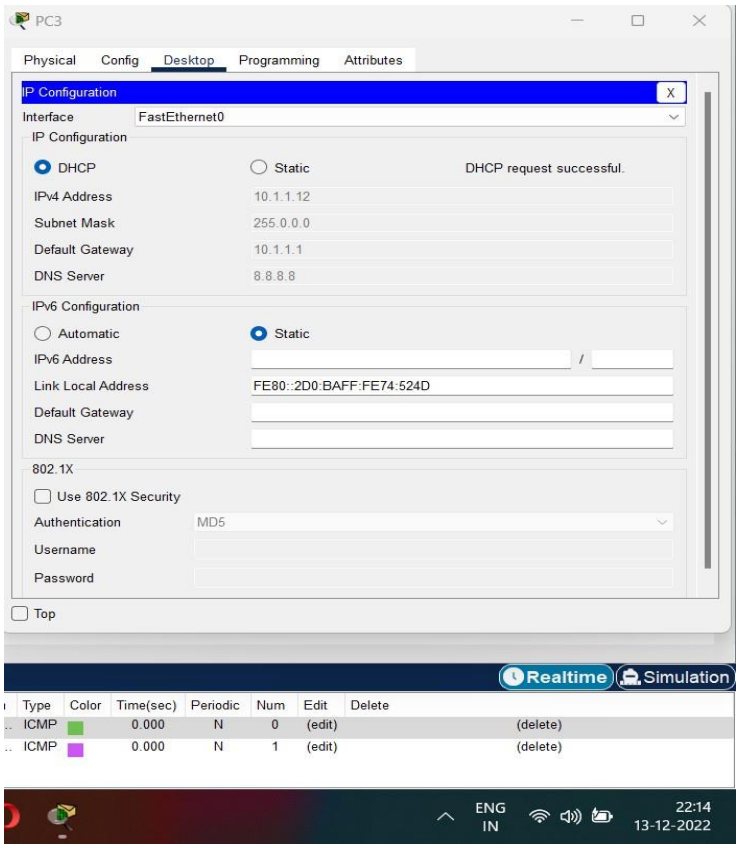




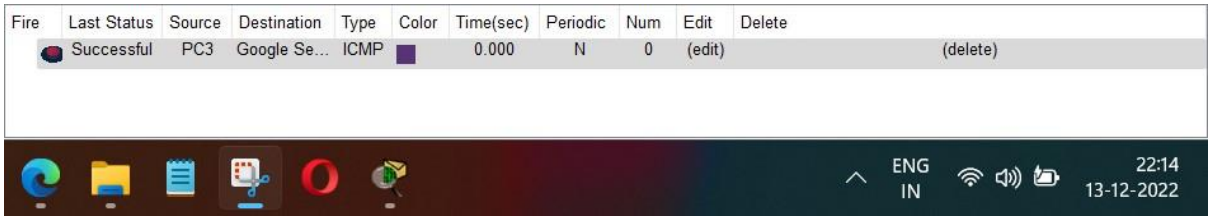
By adding third PC to inside network and initiating communication between that PC and the Google Server



IP Address successfully allocated to the added PC by the DHCP Server



Communication successful between the added PC and the Google Server



Conclusion :

We have therefore configured ASA firewall using CISCO Packet Tracer. We can add as many PCs and end-devices in the network and all will have access to the internet, in our case Google Server, via the firewall.

Note: The IP address range in the DHCP Server must be adjusted accordingly.