CSE3502

INFORMATION SECURITY MANAGEMENT

Prof. Ayesha S.

LABORATORY MANUAL

LAB- 7

Submitted by

Harshit Maheshwari – 19BCE1040

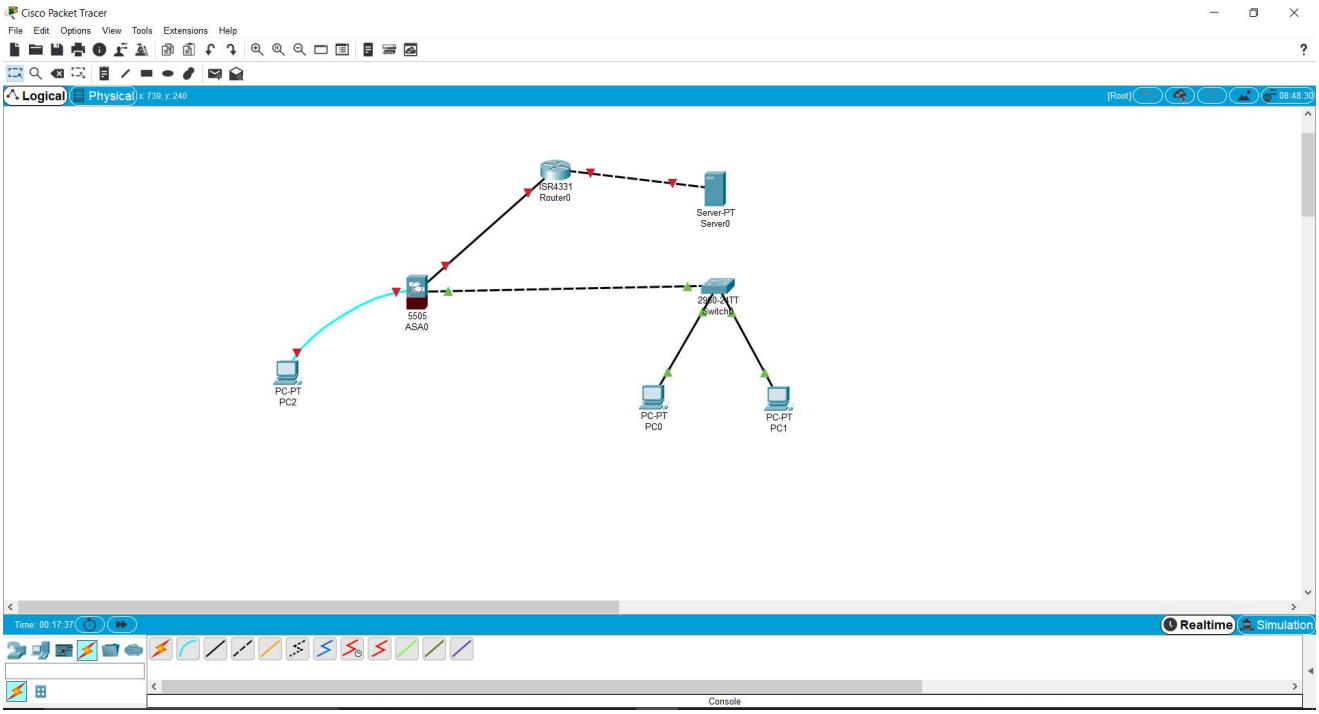
VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

3rd March 2022

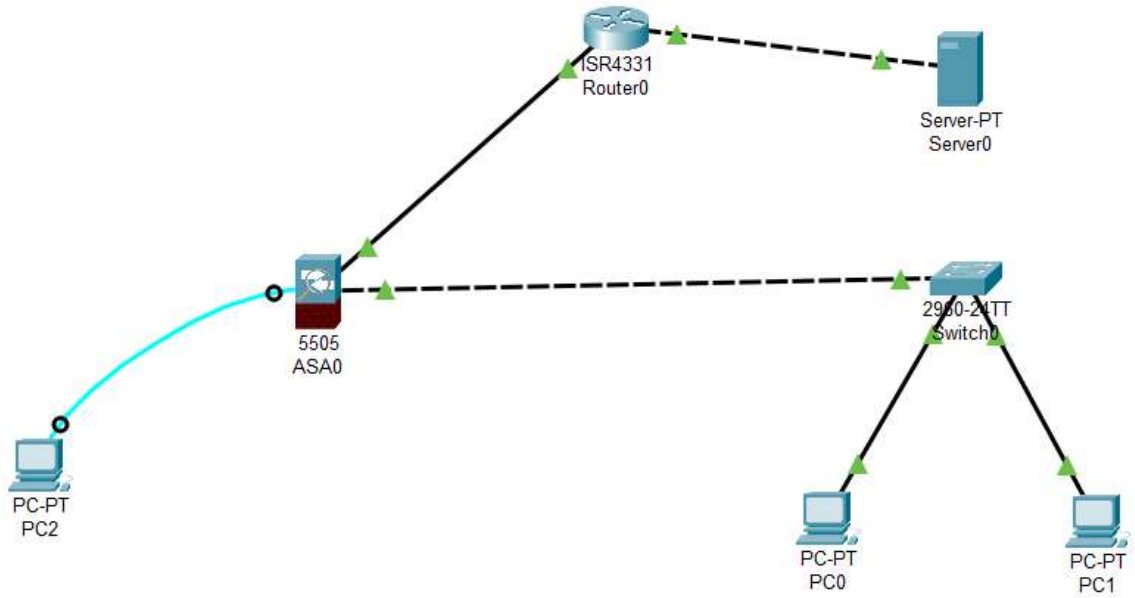
AIM- Create a network topology with a CISCO ASA Firewall, Router, Switch, 3 PCs and a Server. Here, a PC is to be connected with ASA Firewall and two PCs are to be connected with switch. Do the following: 1. Create two VLANs 2. Configure the Router, Server and Firewall. 3. Ensure the firewall functionality by demonstrating the packet transmission between the PCs and Server. 4. Apply NAT 5. Use DHCP and ICMP protocols 6. Ping the connected PCsNAT Configuration

PROCEDURE:

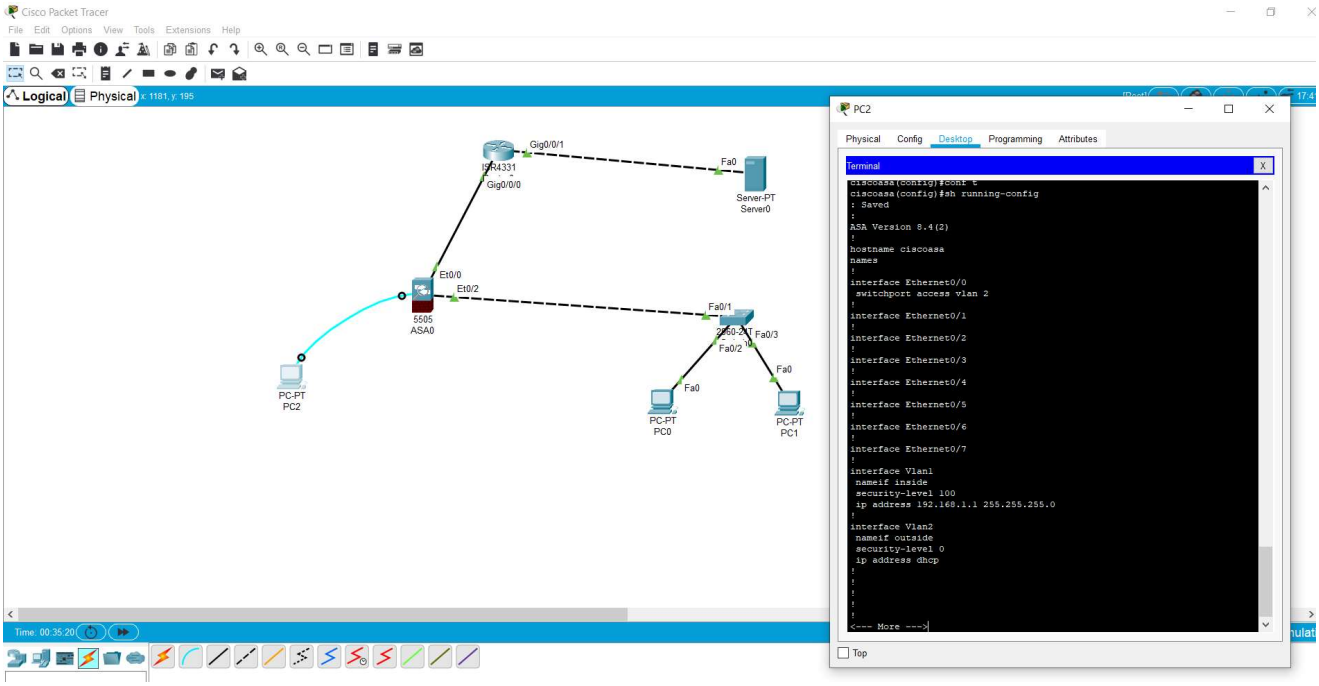
Step 1- Create a Topology



Step 2- Turn on the router



Step 3- Configuring 1 st VLAN with firewall.



```
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
!
!
!
!
```

```
ciscoasa(config)#no dhcpd address 192.168.1.5-192.168.1.36 inside
ciscoasa(config)#
```

Setting Security Level as 100 means Insite traffic incoming as this is a Local Area Network.

```
% Incomplete command.
ciscoasa(config)#int vlan 1
ciscoasa(config-if)#ip add 10.1.1.1 255.0.0.0
ciscoasa(config-if)#no shut
ciscoasa(config-if)#nameif inside
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#exit
ciscoasa(config)#
```

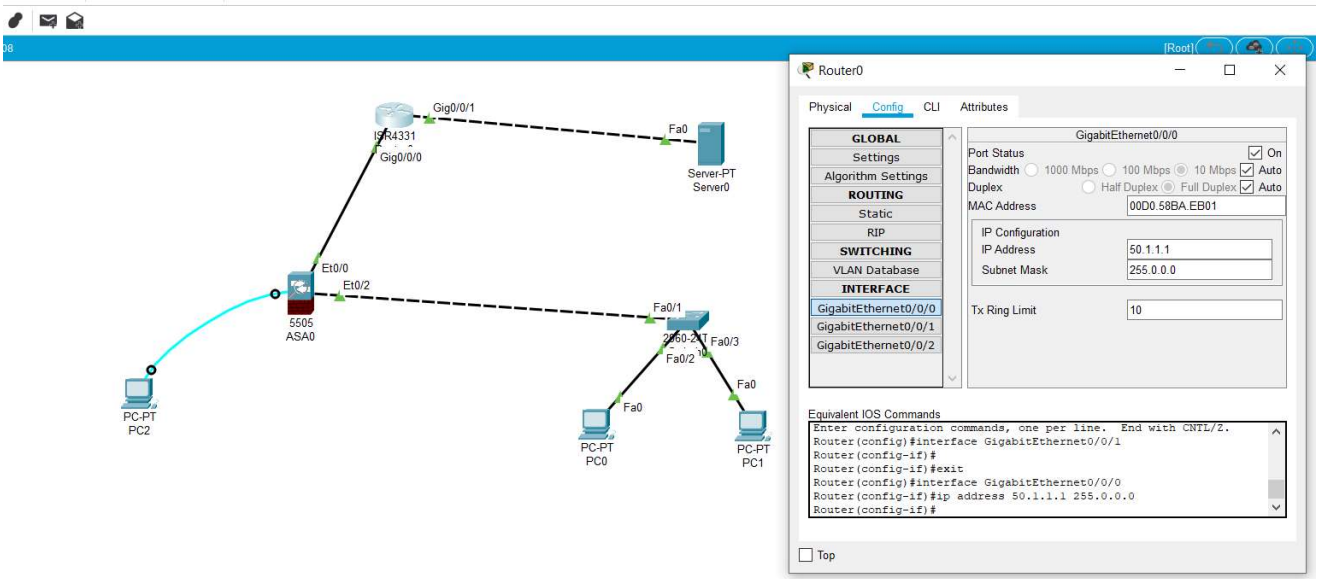
Step 4- Configuring 2nd VLAN with firewall.

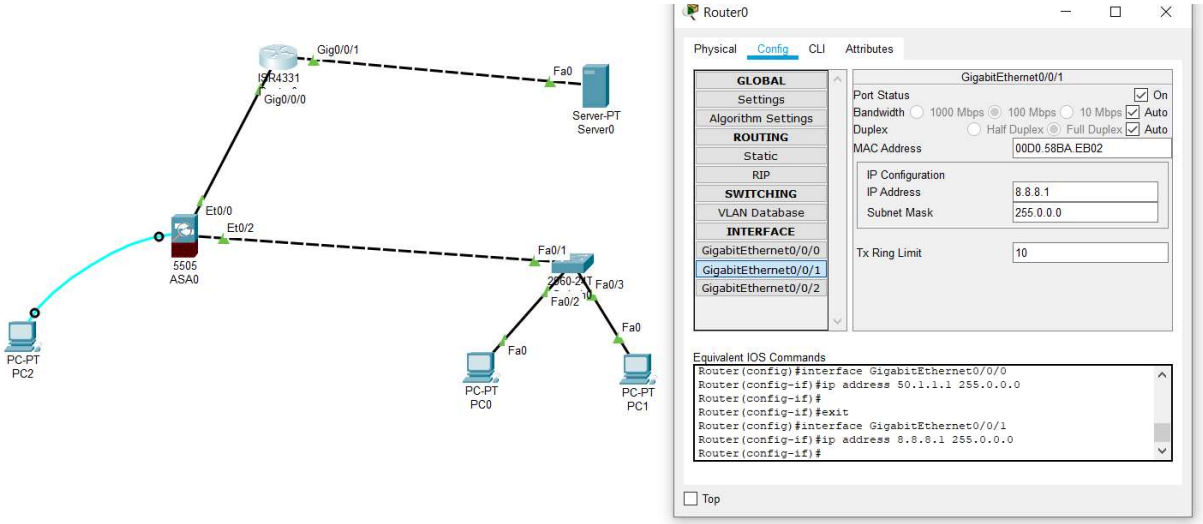
0 Security in Firewall means Outside traffic

```
ciscoasa(config-if)#
ciscoasa(config-if)#
ciscoasa(config-if)#int e0/2
ciscoasa(config-if)#switchport access vlan 1
ciscoasa(config-if)#exit
ciscoasa(config)#v
               ^
% Invalid input detected at '^' marker.

ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#int vlan 2
ciscoasa(config-if)#ip add 50.1.1.2 255.0.0.0
ciscoasa(config-if)#no shut
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#exit
ciscoasa(config)#intint e0/0
                  ^
% Invalid input detected at '^' marker.

ciscoasa(config)#int e0/0
ciscoasa(config-if)#switchport access vlan 2
ciscoasa(config-if)#
```

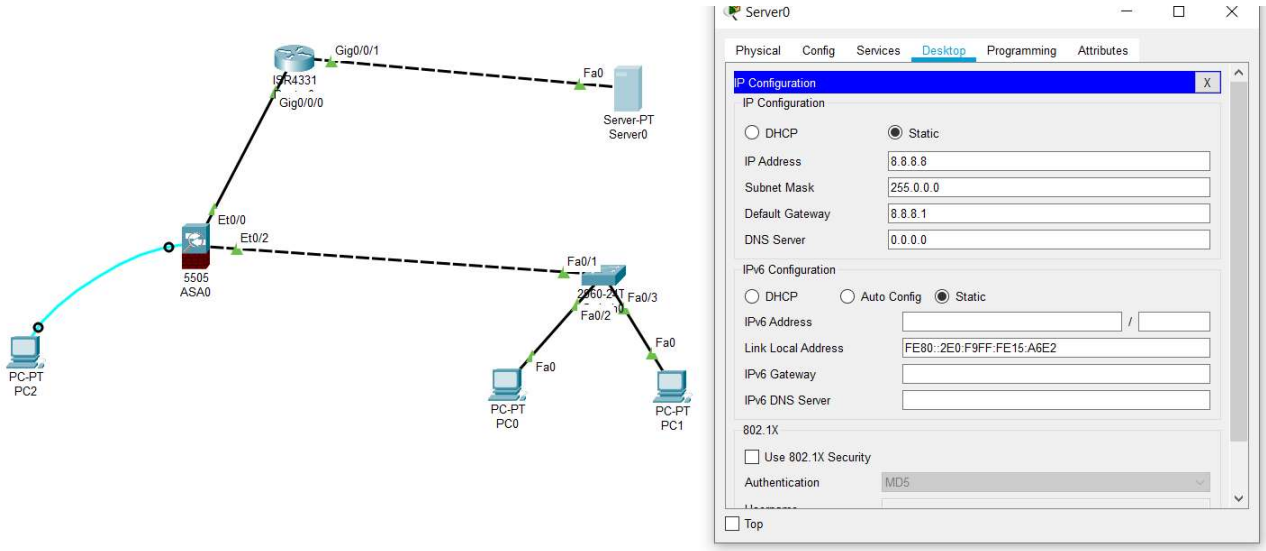
Top

Step 5- Setting the IP Address on Router

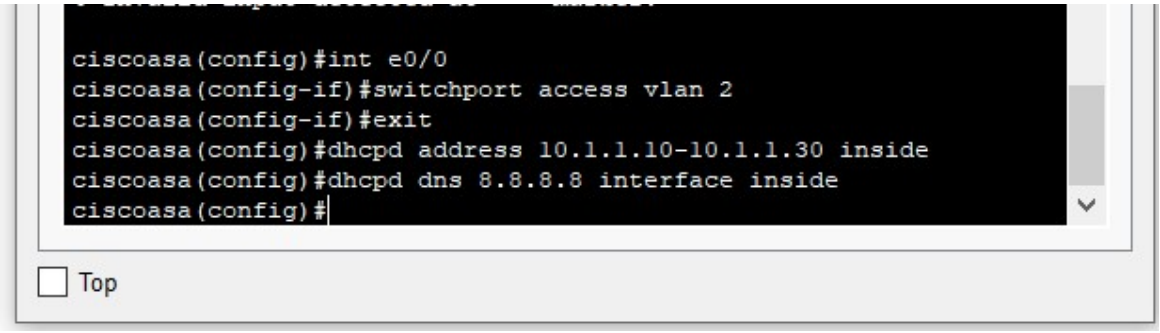




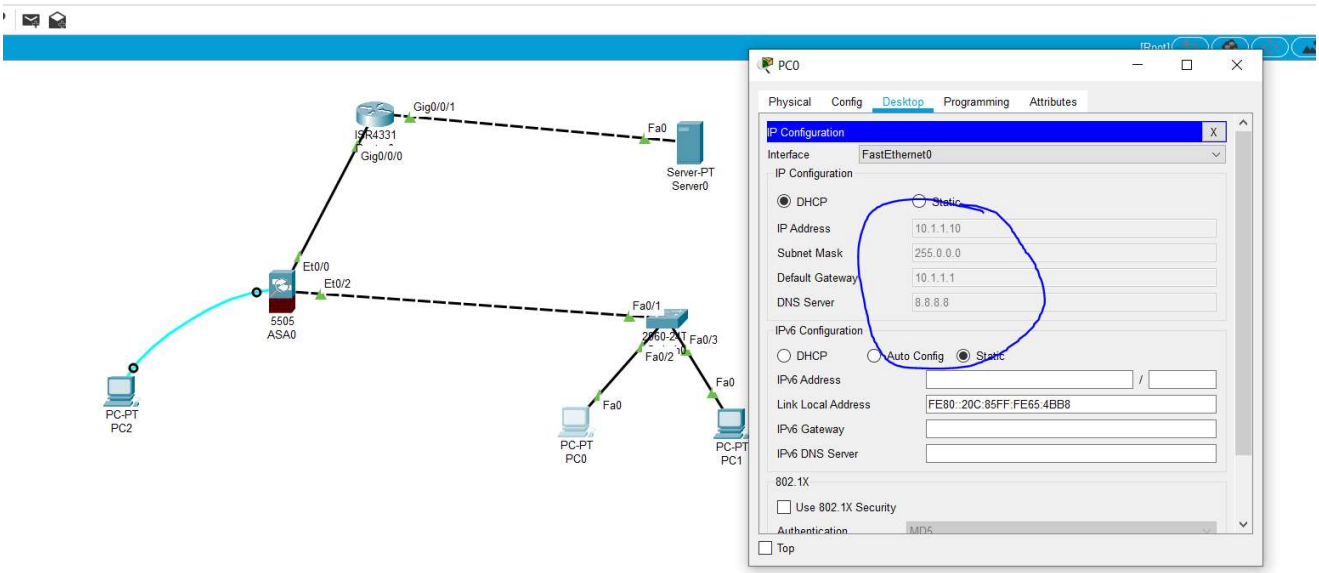
Step 6- Setting the IP Address on the Server

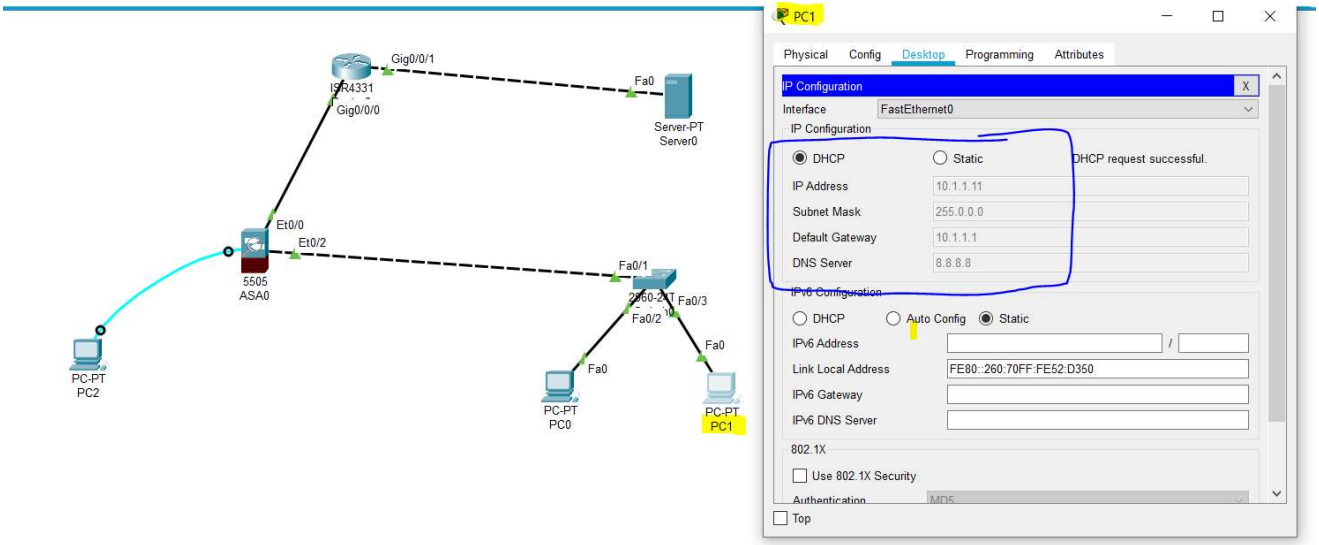


Step 6- Setting DHCPD range for Firewall via the PC-2 and the DNS IP

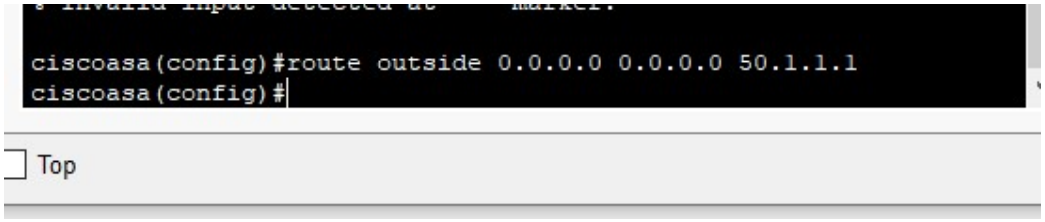


Step 6- Checking the DNS on the PC's:

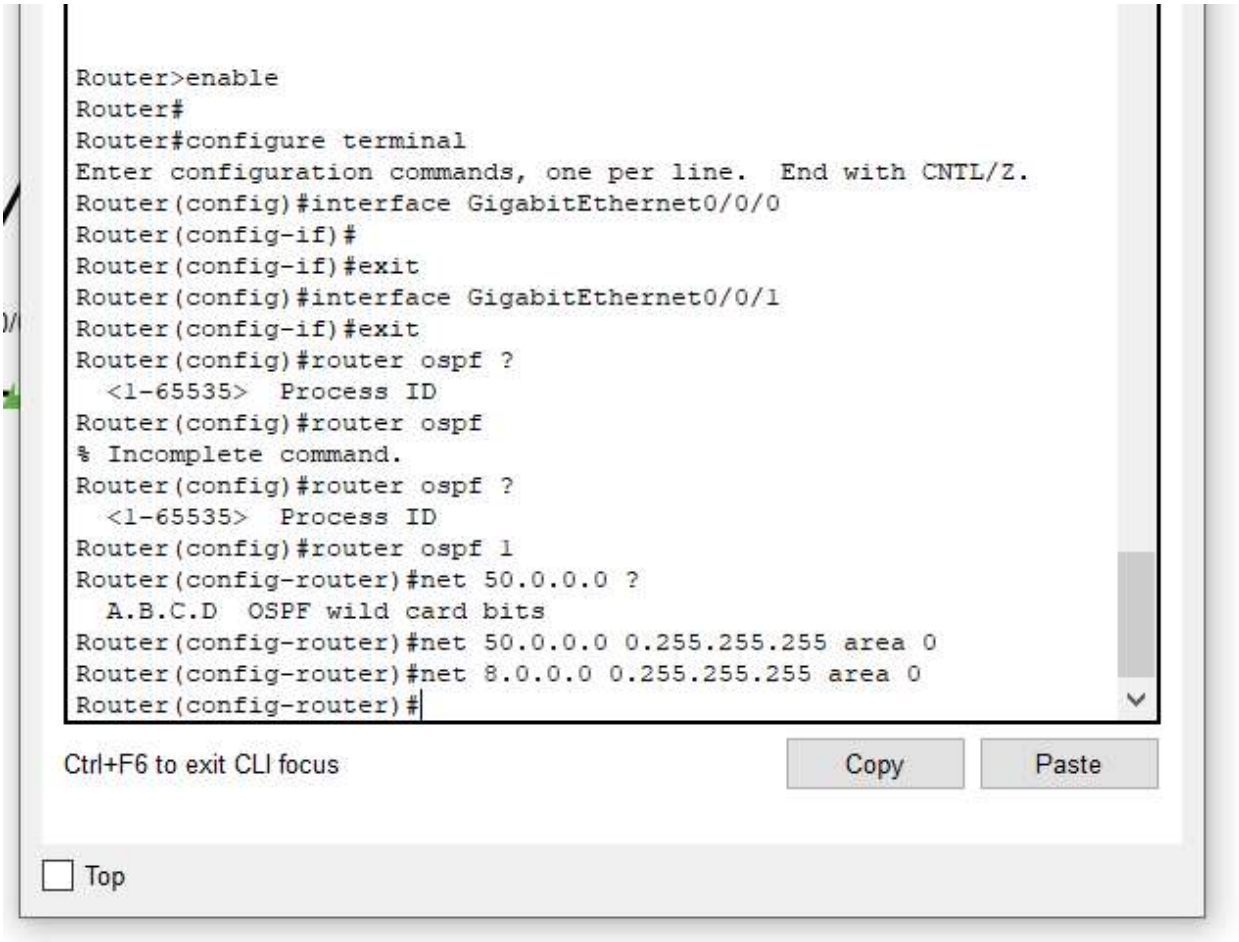




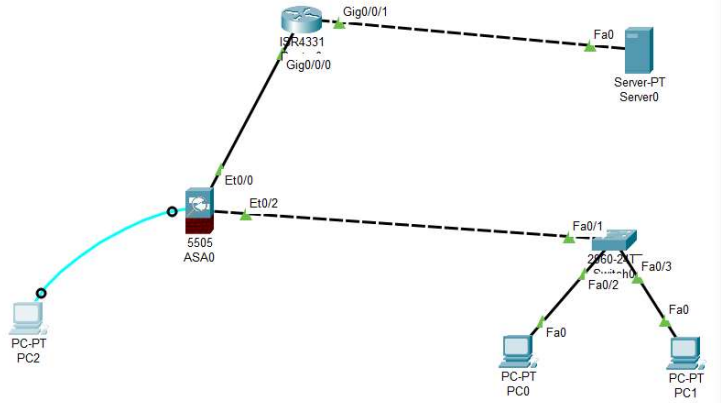
Step 7- Configuring Default Route on ASA

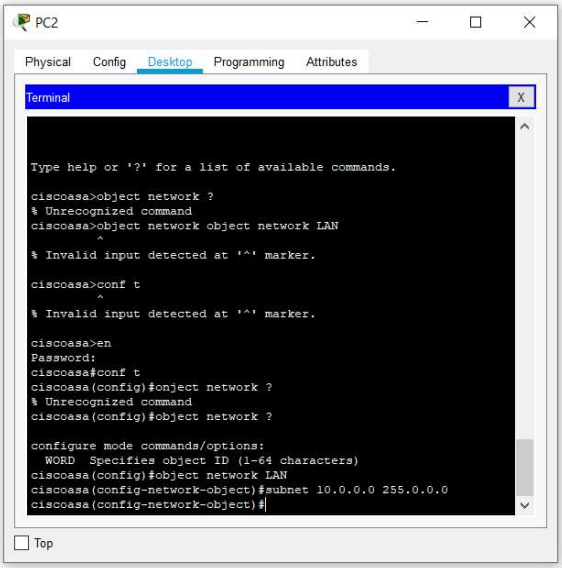


Step 8- Setting up OSPF on the Router

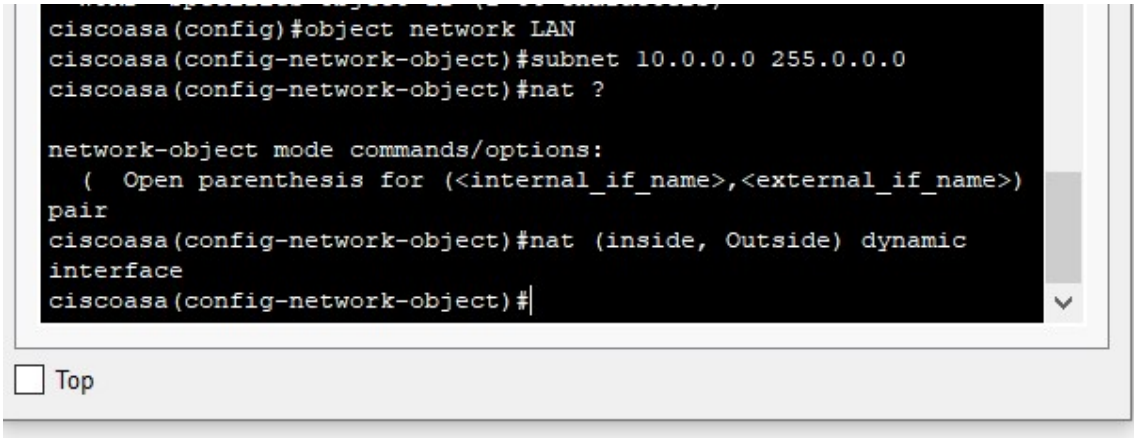


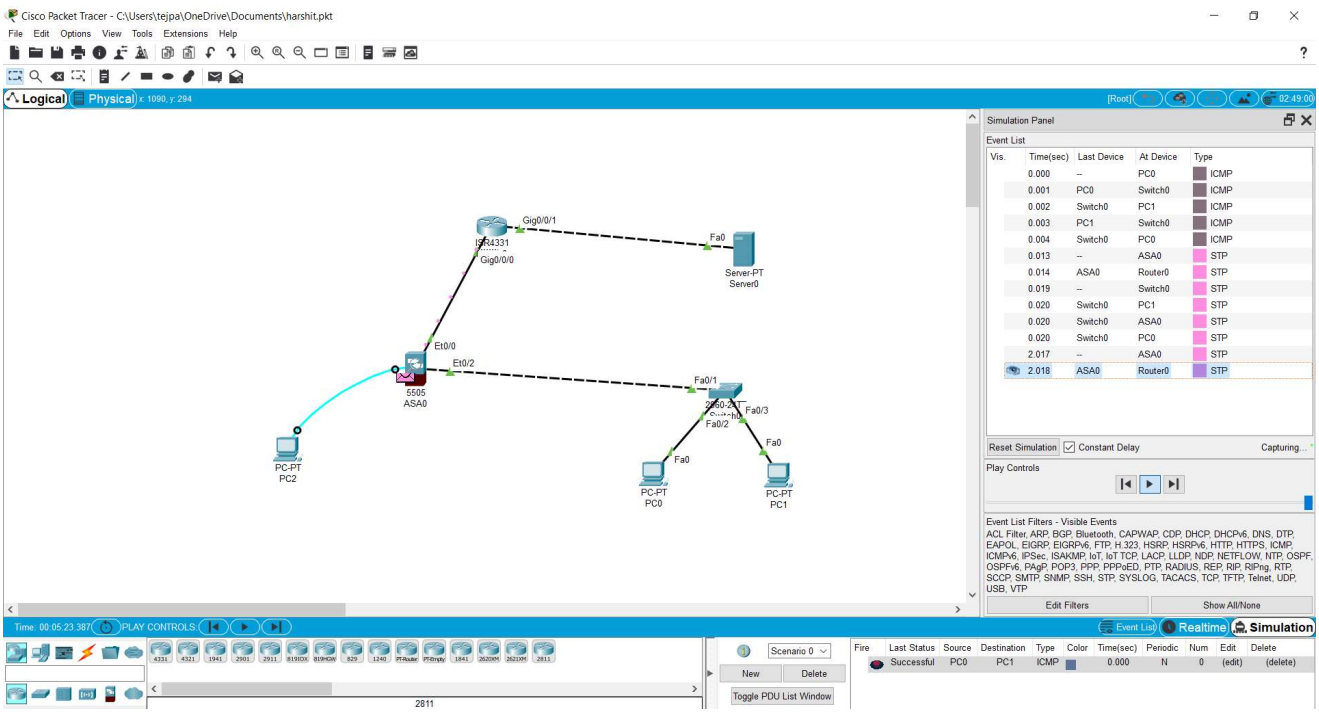
Step 9- Creating an object network





Step 10- Enable NAT on ASA





INFERENCE- We learned to configure ASA Firewall in Cisco Packety Tracer in this LAB