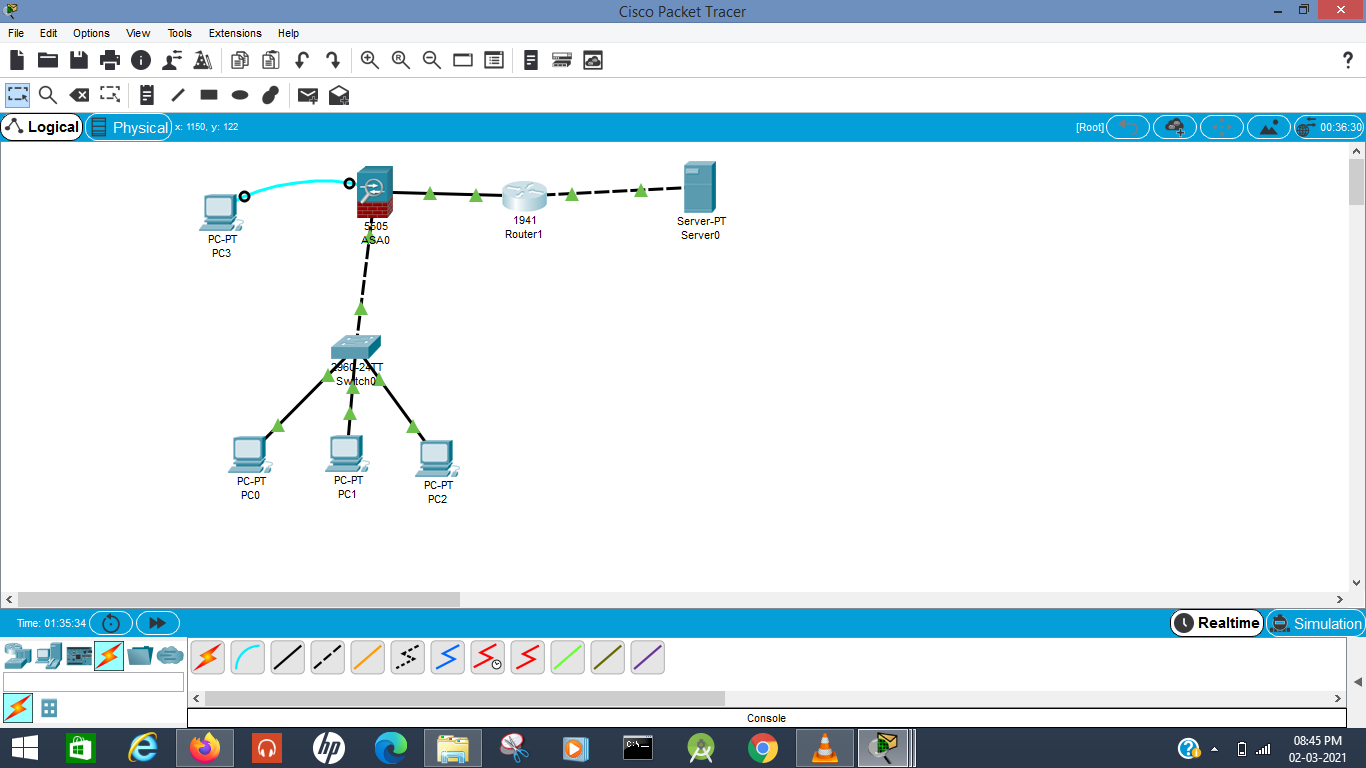
**NAME: RESHMA.P**

**REG NO: 17MIS1009**

LAB-3: FIREWALL

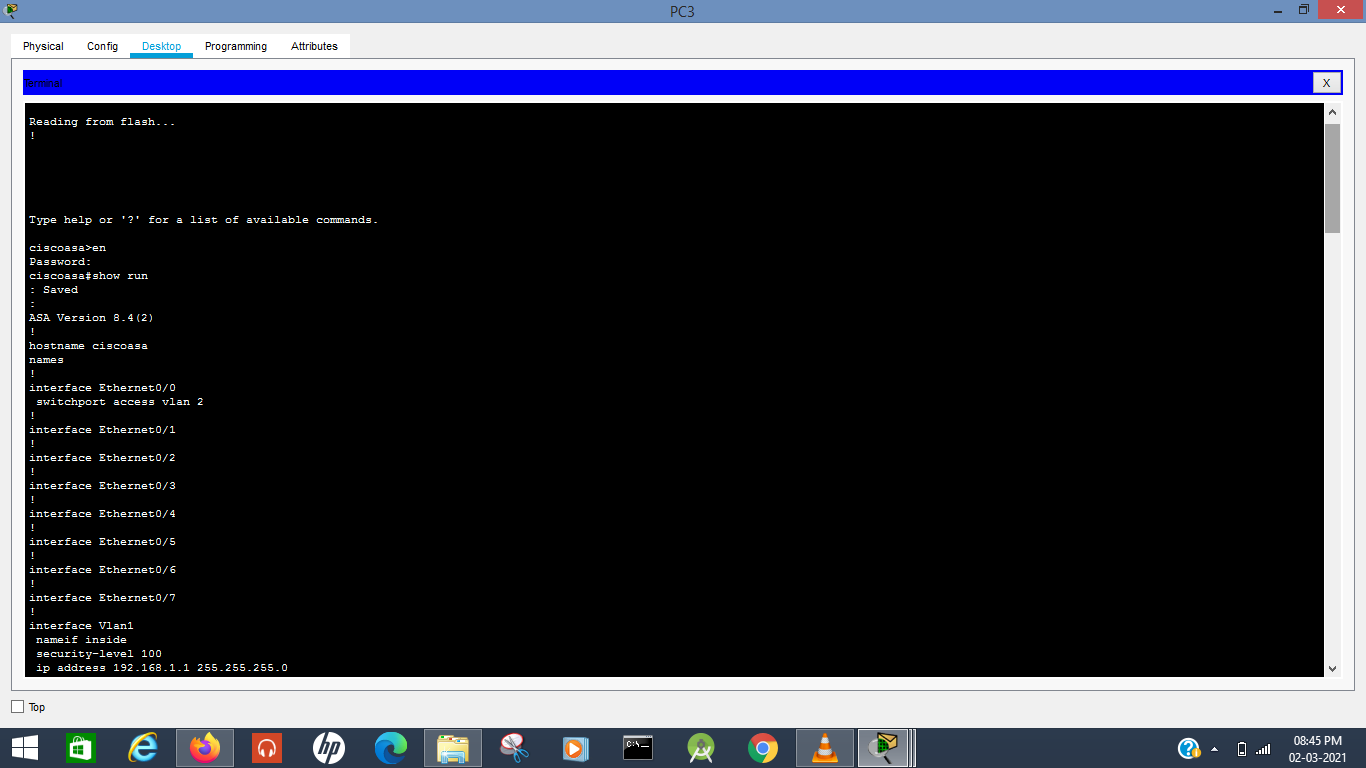
**Step-1: Network Topology**



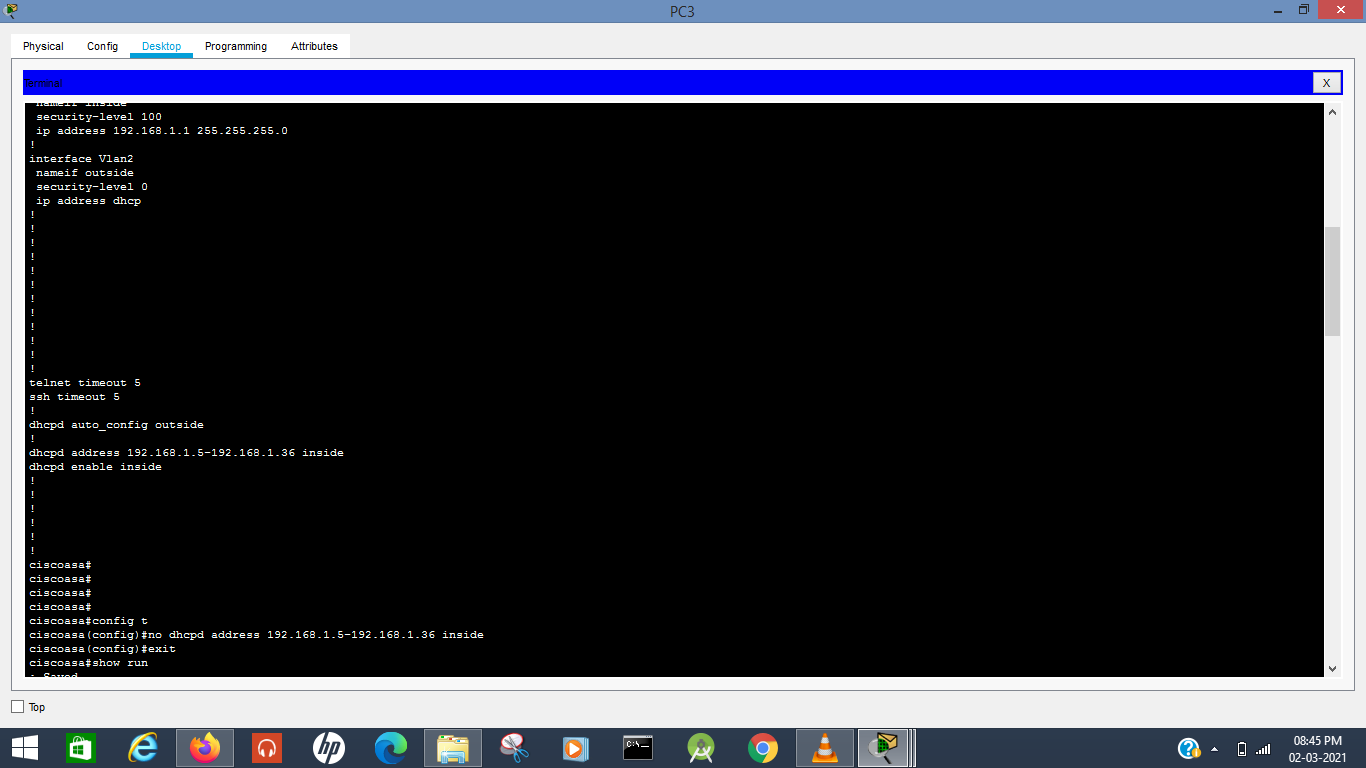
**Step-2: Configuration of ip**

**i)Configuration of asa firewall**

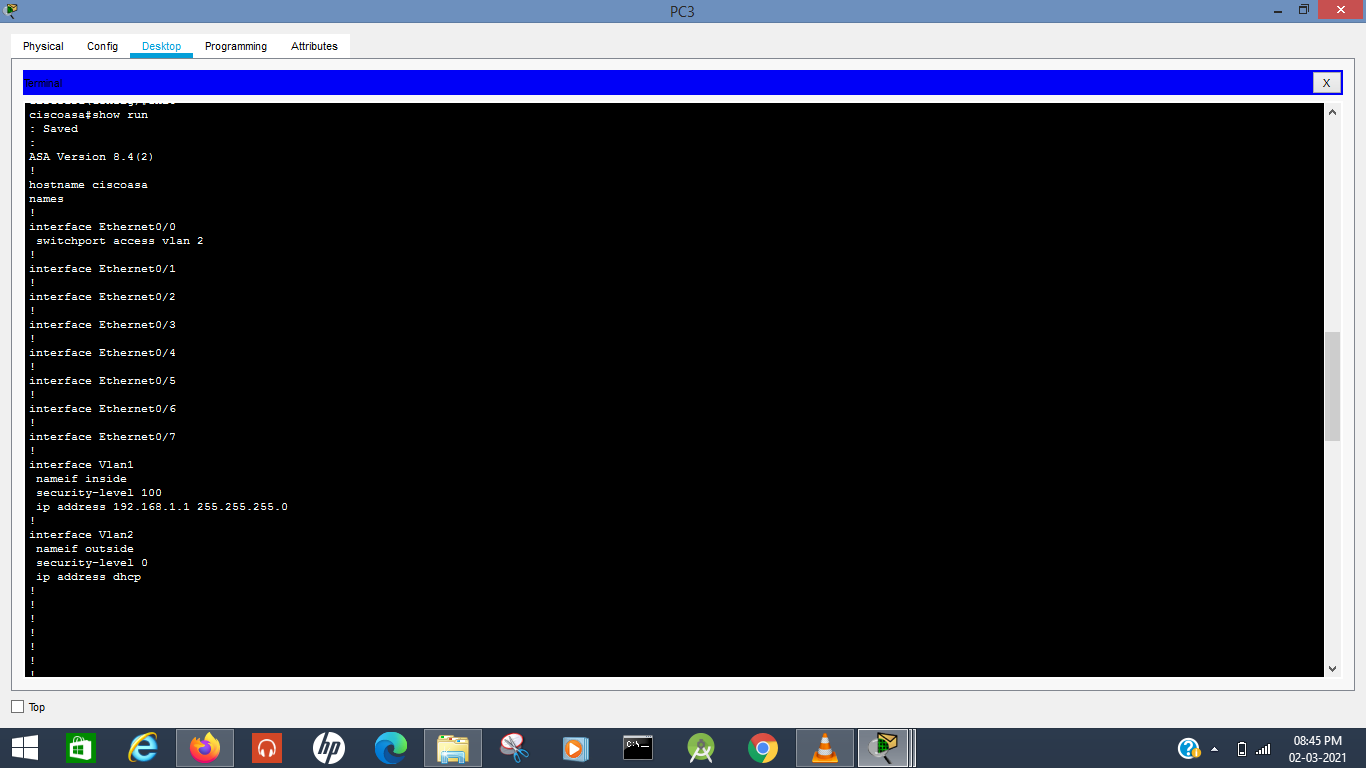
**a)remove default dchp**

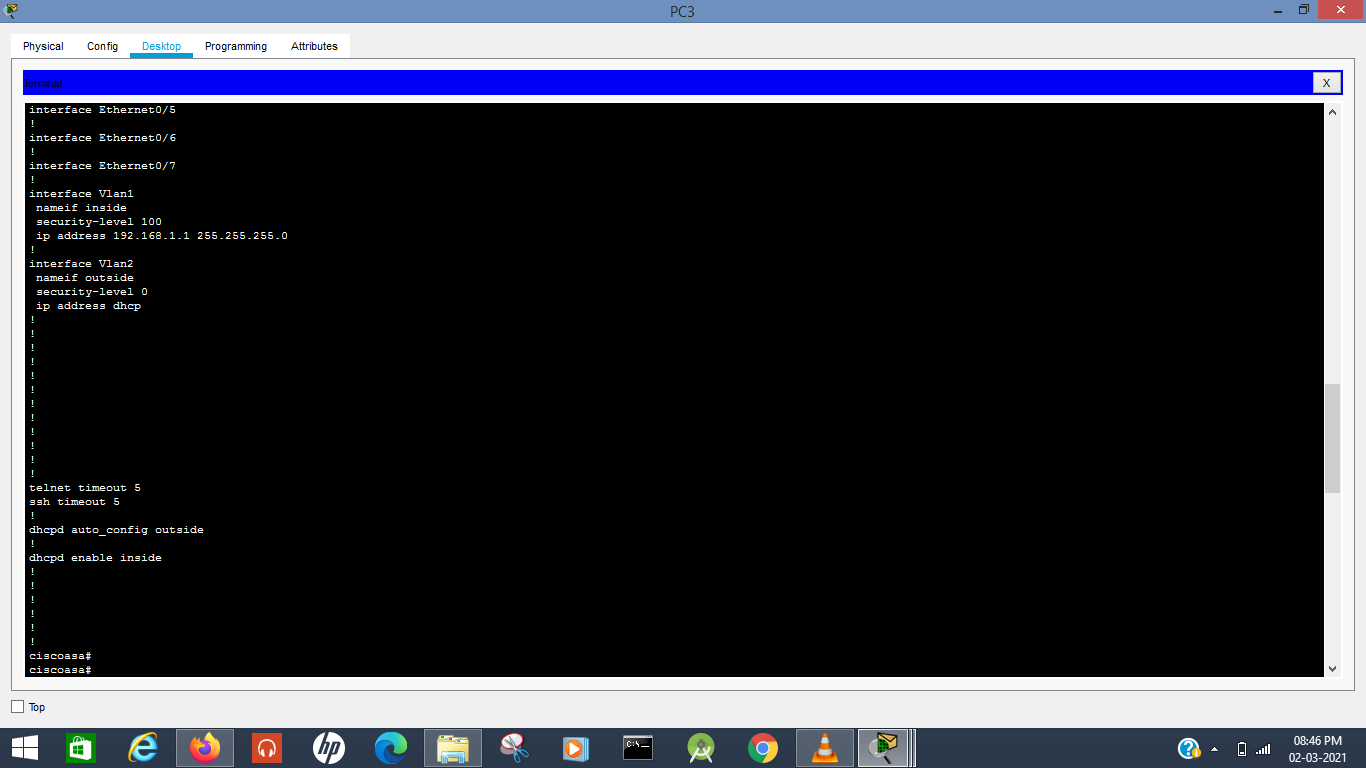
****

Delete previous dhpc address

****

Previous dhpc successfully deleted

****

****

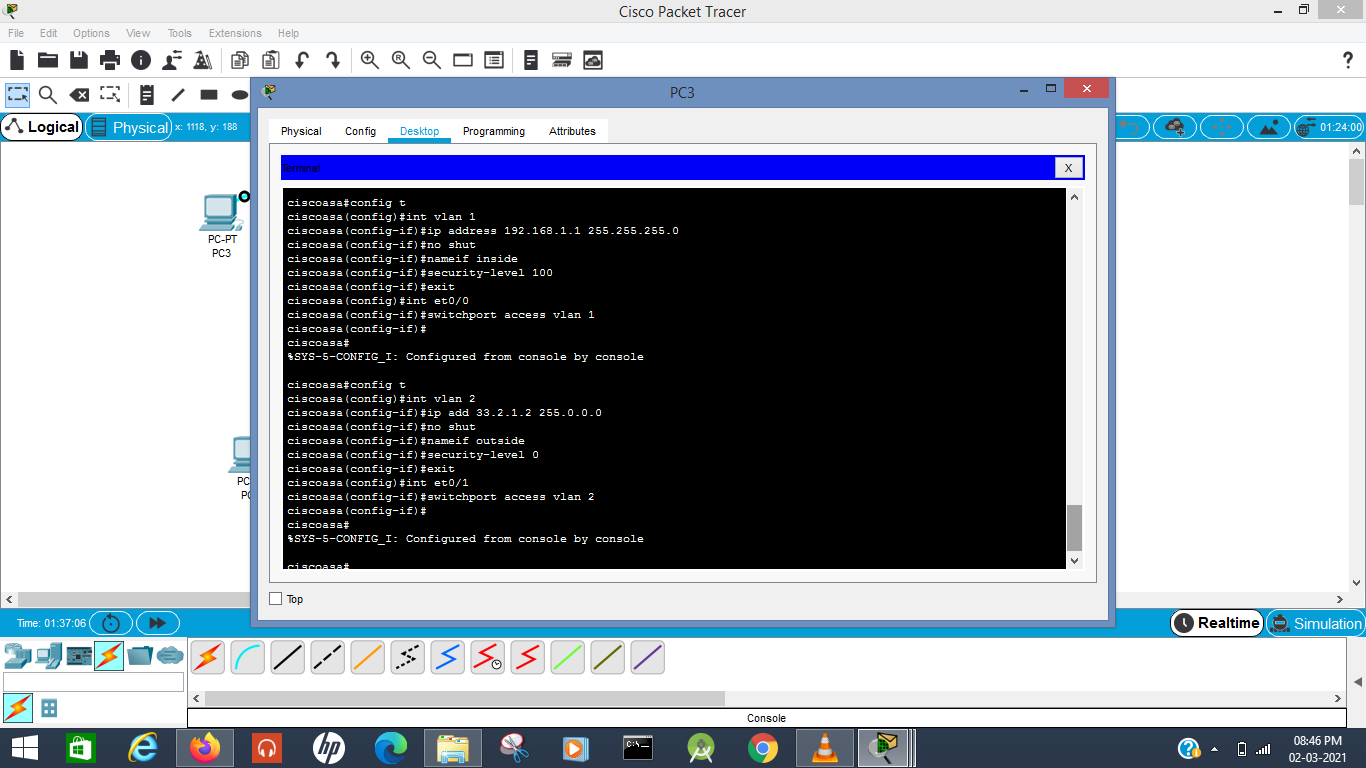
**Command Explanation:**

Use the machine connected to the ASA, and go to its terminal.

* En
* (no password by default, so just hit [enter])
* show run
  + It might have some preconfigured IPs set up already, so we need to check first.
  + Interface vlan might have shit in it, and the dhcp is enabled on the firewall by default so we need to remove those default settings
* config t
* no dhcpd [whatever dhcp address it had as default]
  + Removes the dhcp config
* ctrl+c

**b)configure vlan 1 and vlan 2**

Configure vlan 1 and vlan 2. This will override previous vlan1 and vlan2 configuration prefixed in cisco packet tracer

****

**Command Explanation:**

**Inside**

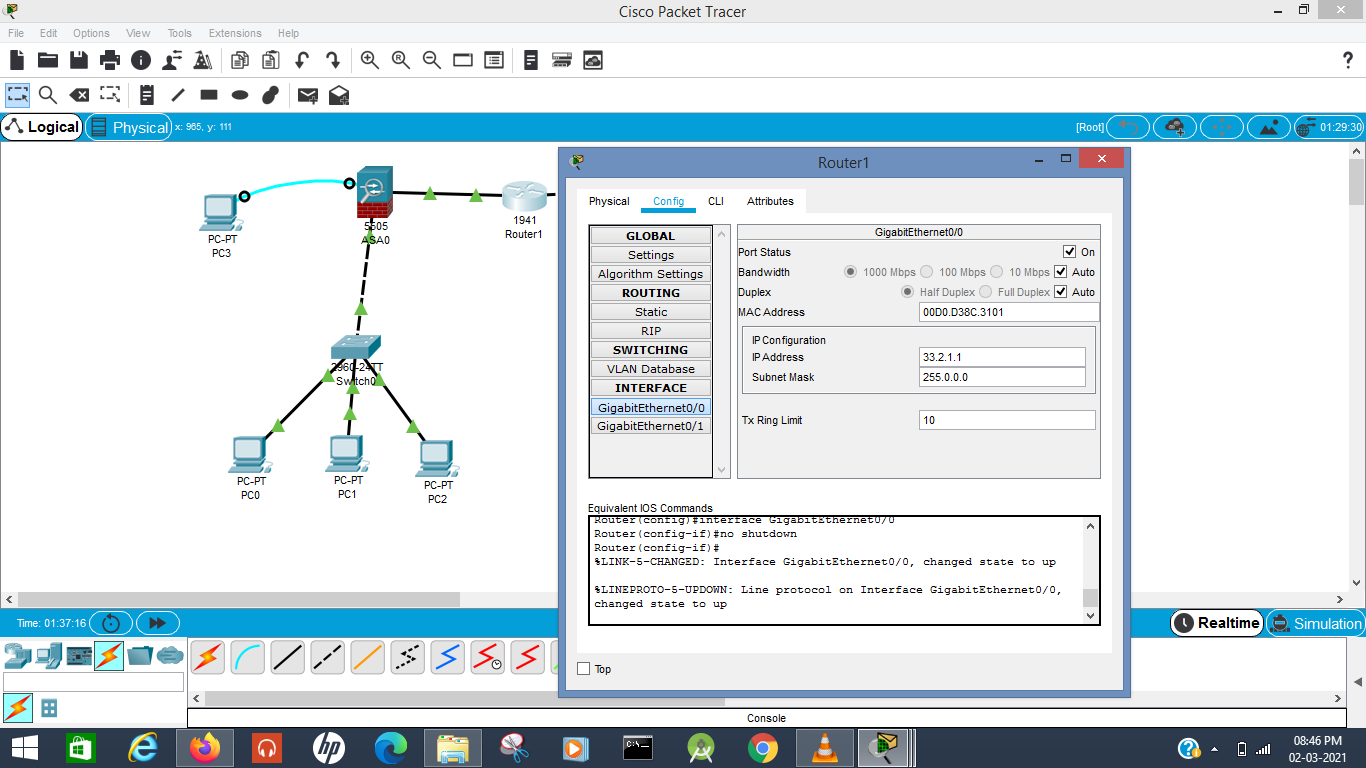
* config t
* int vlan 1
  + In the int (interface) vlan1 (where the preconfigured IPs were seen when we did show run)
* ip add [our inside ip] [our mask] (here, 192.168.1.1 255.255.255.0 for inside / private network)
* no shut
* nameif inside
* security-level 0
* exit
* int [what physical port is connected for our inside firewall] (here, et0/0)
* switchport access vlan 1
  + So whatever setting we did in vlan 1 (setting IP, security level 100, renaming to inside) is now working on that et0/0 port
* exit
* Ctrl+c

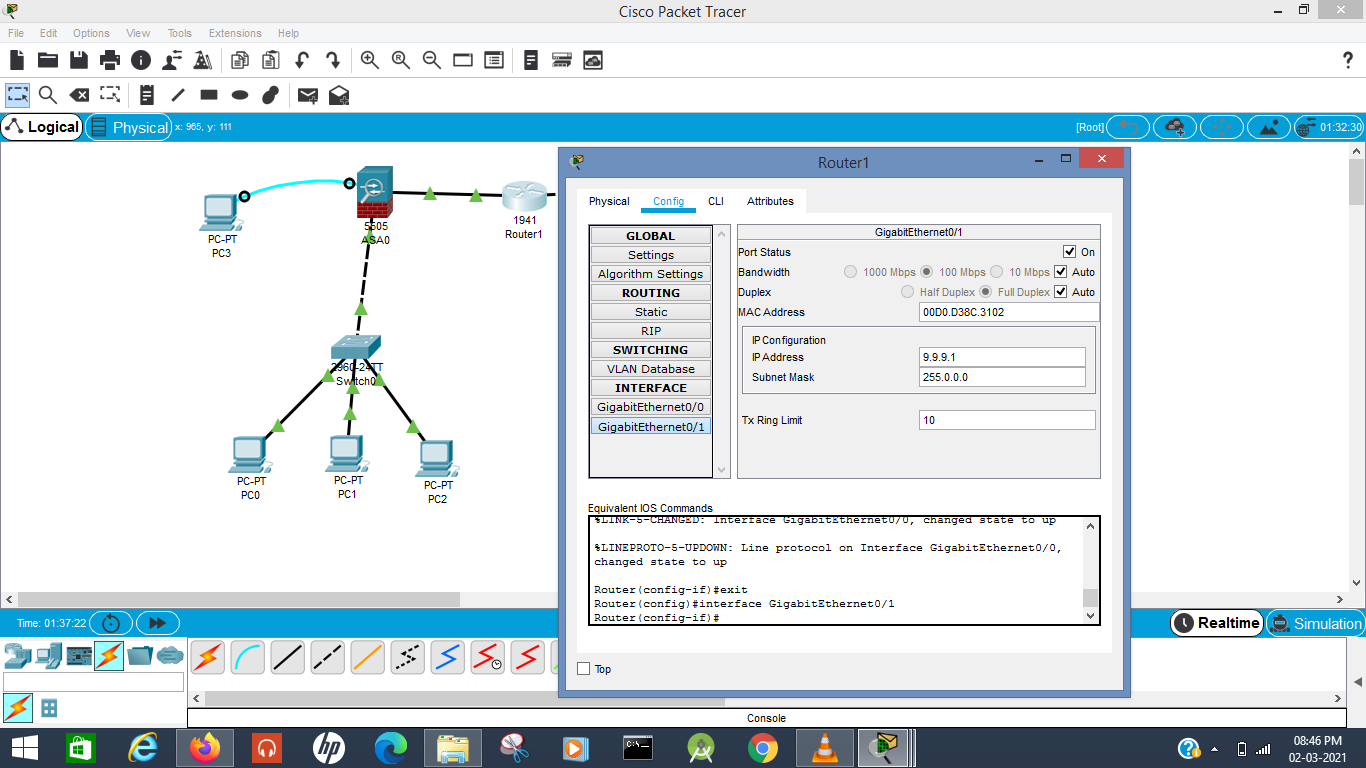
**Outside**

* Config t
* Int vlan 2
* Ip add [our outside ip] [our mask] (here, 33.2.1.2 255.0.0.0 for outside / public network)
* No shut
* Nameif outside
* Security-level 100
* Exit
* Int [what physical port is connected for our outside firewall] (here, et0/1)
* Switchport access vlan 2
* Exit
* Ctrl + c

**ii) router**

Set ip and subnest mask for et0/0 and et0/1 for router

****

****

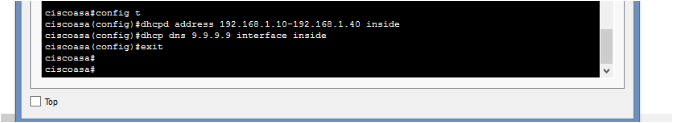
**Equivalent Commands in cli and it’s explanation:**

Go to the CLI

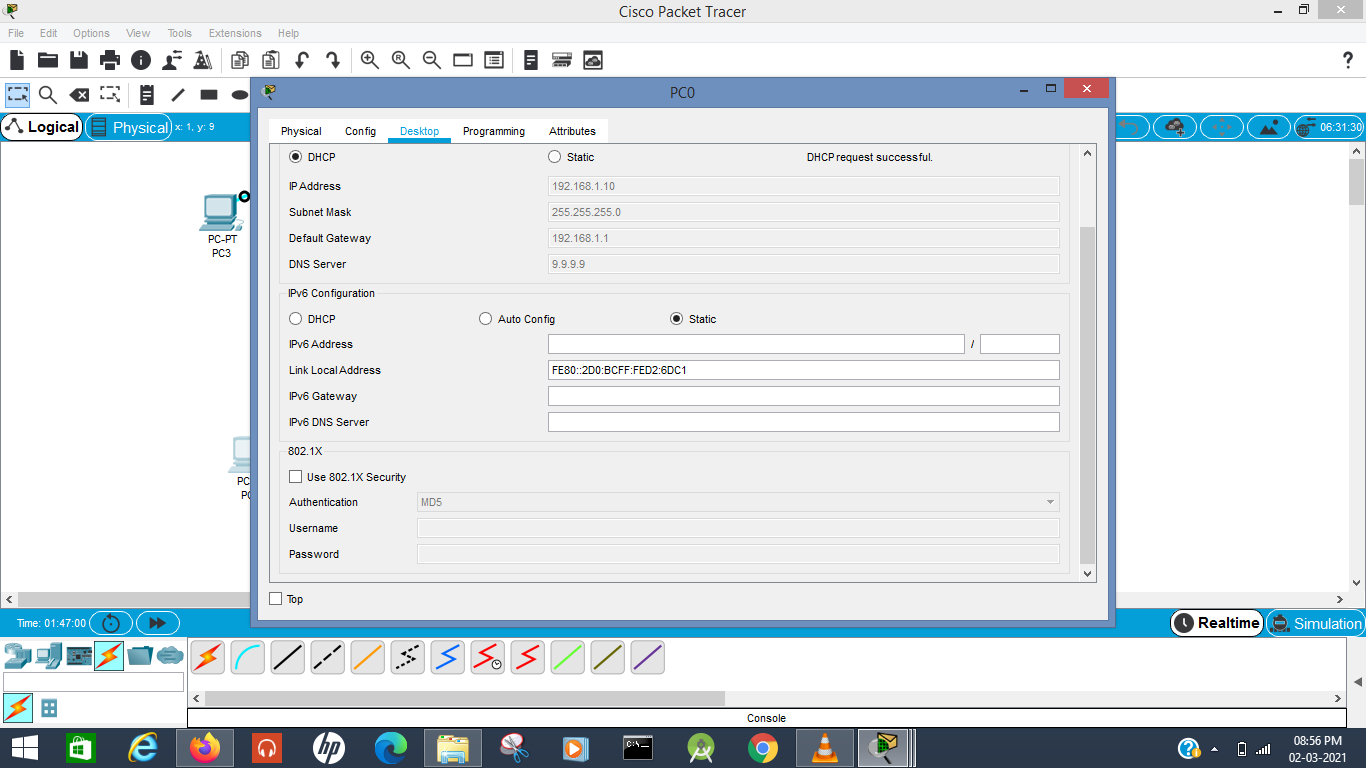
* En
* Int gig0/0
* Ip add [router in ip] (here, 33.2.1.1 255.0.0.0)
* No shut
* Exit
* Int gig0/1
* Ip add [router out ip] (here, 9.9.9.1)
* No shut
* Ctrl+c

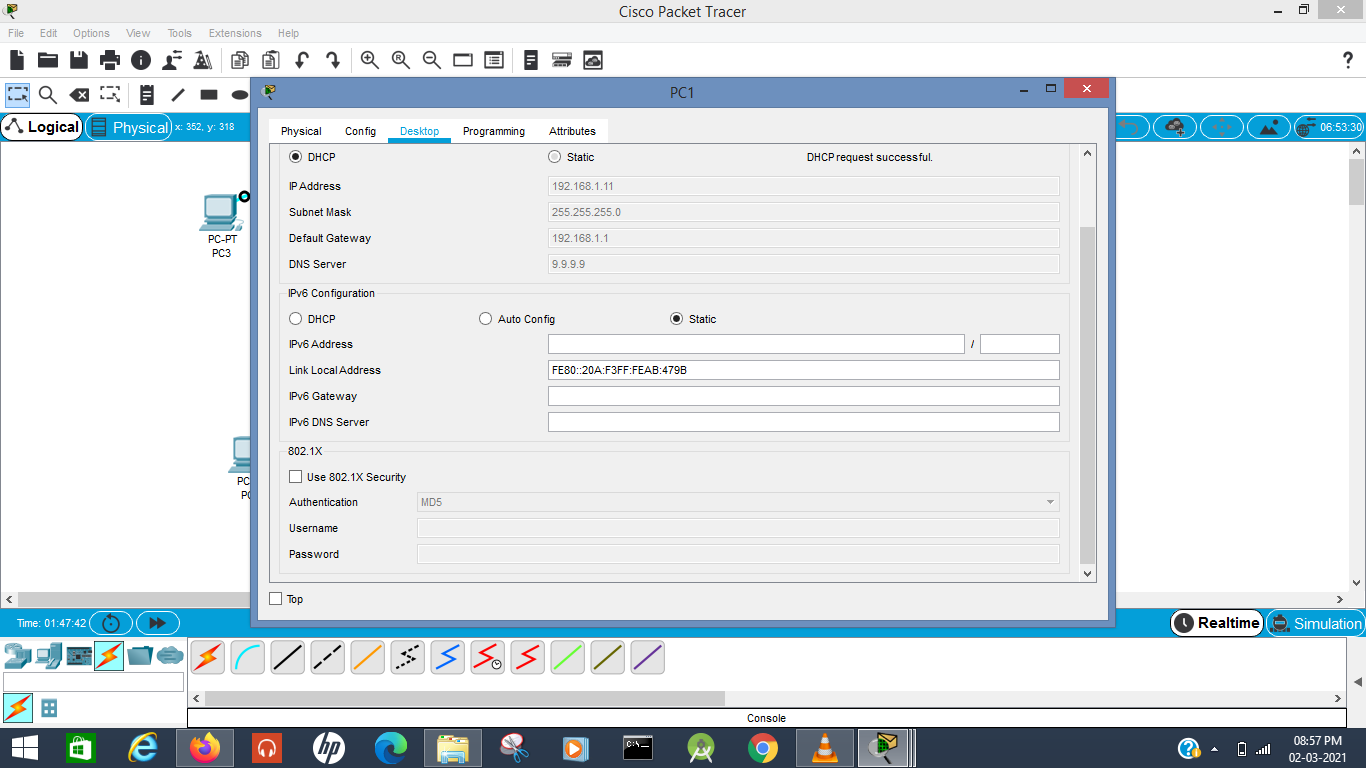
**Step 3: Set up DHCP and DNS Server on the ASA**

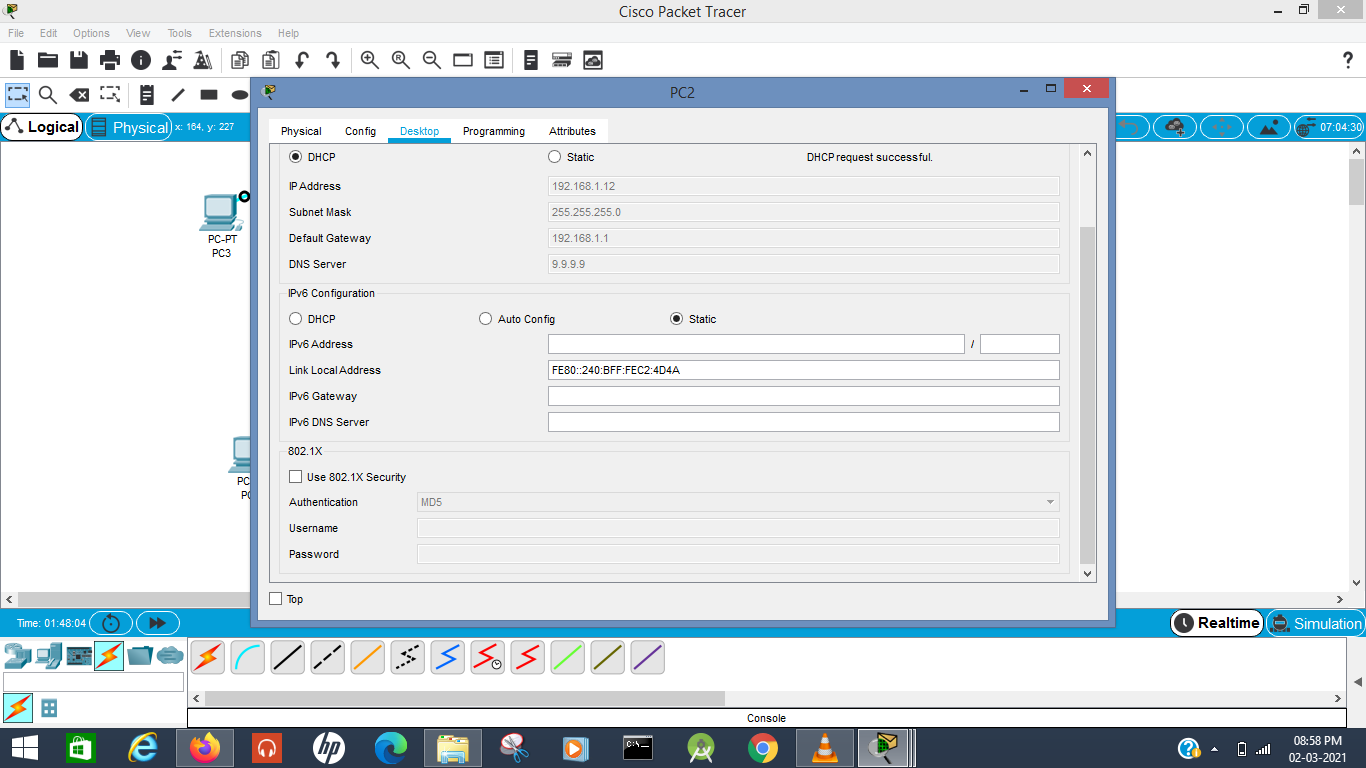
set up dhcp address and dns

****

now go to pc in network and in desktop choose dhcp







**Command Explanation:**

Open up Terminal on Server console

* Conf t
* Dhcpd address [inside ip range for network] (here, let's say 192.168.1.10-192.168.1.30) inside
  + The range depends on the number of computers you want in your network
  + 10 - 30 is the range we specified here
* Dhcpd dns 9.9.9.9 interface inside
  + Basically configuring the DNS Ip on the dhcp server
* exit

Set DHCP on for the PCs and see if it works

**Step 4:Configure default route on ASA**

configure route



**Command Explanation:**

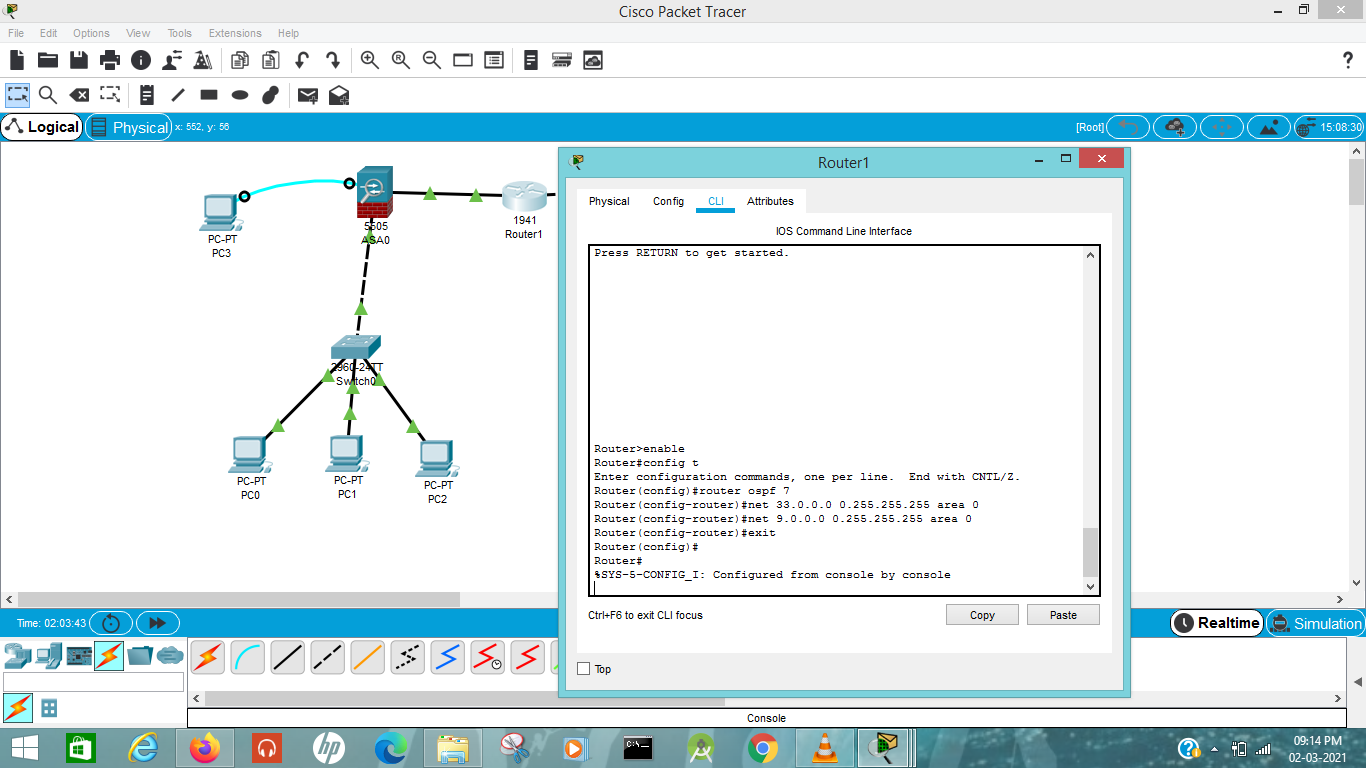
Just for easy traversal of packets without direction, we create a forwarding route.

Open up terminal again

* Config t
* Route outside 0.0.0.0 0.0.0.0 33.2.1.1
  + Any IP
  + Any subnet
  + 33.2.1.1 is the IP of the router

**Step 5: Configure Dynamic Route using OSPF Routing protocol**

Configure dynamic route



**Command Explanation:**

Go to router's CLI

* Config t
* Ospf 1
  + 1 - Process ID
* Net 33.0.0.0 0.255.255.255 area 0
  + Networks connected? 33 and 9
  + 0.255.255.255 means anything with 33.x.x.x IP is included
    - If it was 33.1.0.0 0.0.255.255, anything with 33.1.x.x IP is included
* Net 9.0.0.0 0.255.255.255 area 0

**Step 6: Configuring NAT**

Configure NAT



**Command Explanation:**

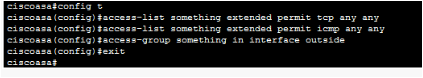
To make things easier to manage, we throw all our objects together into an object network and configure a way for the inside network to communicate with the outside using NAT

Terminal of the ASA:

* Config t
* Object network [name of object network]
* Subnet [subnet IP] [subnet mask]
  + Here, our private network runs on IP 192.168.1.0
  + So, our subnet can be 192.168.1.0 and the mask can be 255.255.255.0 or even 192.168.0.0 255.255.0.0 or even 192.0.0.0 255.0.0.0
* Nat (inside, outside) dynamic interface
  + NAT - Network Address Translation. Network address translation is a method of remapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. So, we basically connect the private and public ips.
* Exit

**Step 7: ACL on the firewall**

ACL on firewall



**Command Explanation:**

Terminal of ASA:

* Config t
* Access-list [nameoflist] extended permit tcp any any
  + Any source
  + Any destination
* Access-list [nameoflist] extended permit icmp any any
  + Allows icmp packets too
* Access-group [nameoflist] in interface outside
  + In for input traffic
  + Out for output traffic
  + Activates ACL and gives input traffic to the outside network

**Step 7: sending packets to check final result**

Send packet from pc0 to router, pc1 to router, pc2 to router ; if its successful then we got the desired result

