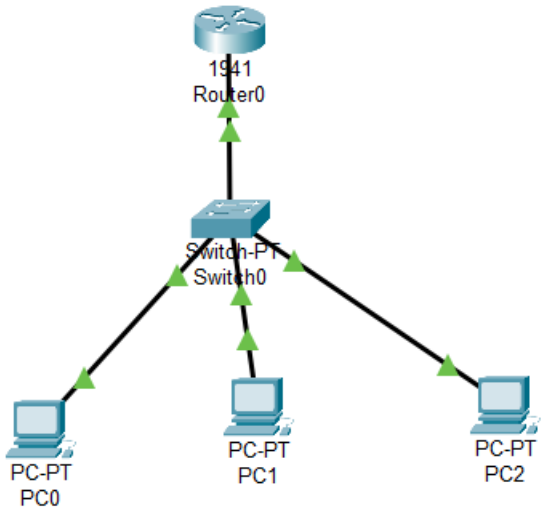
2. **Using Packet Tracer, simulate an ARP spoofing attack. Analyze the behavior of devices on the network when they receive a malicious ARP response.**

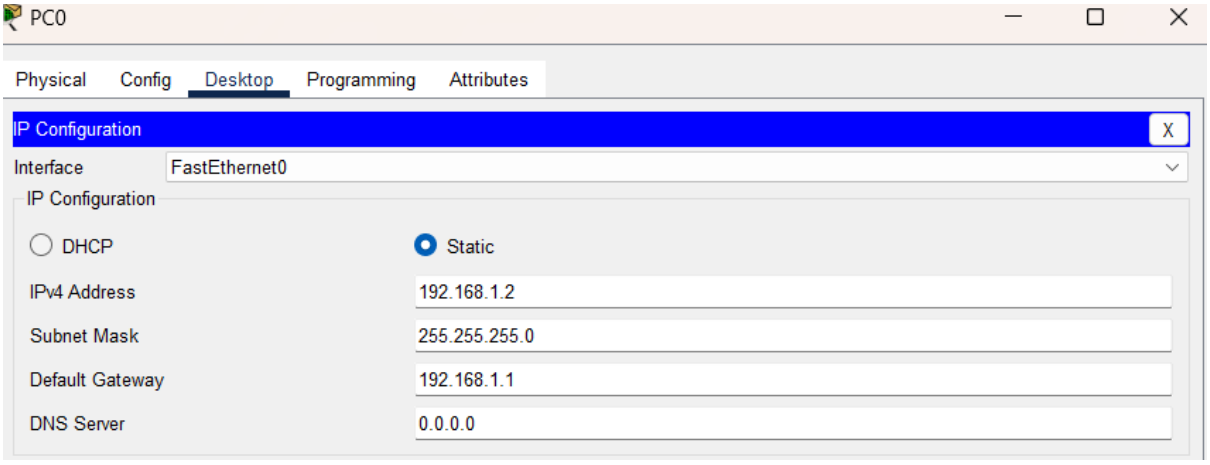
Process that I followed :

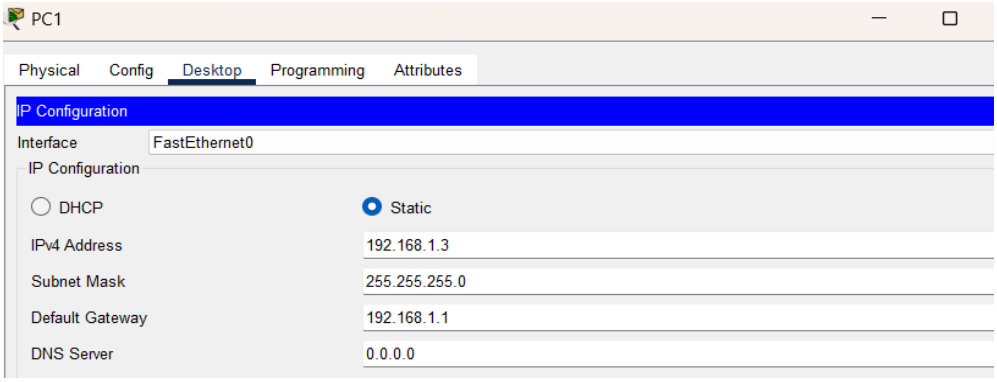
- Connected three PCS where two are normal pc and one is attacker pc
- Which are connected to switch
- Changed the ARP table in the victim pc .
- In cisco packet tracer the command
- Arp -s <victim ip address> <attackers mac address>
- Is not working . so I decided to change the mac address in the victims pcmanuaaly to attackers mac address

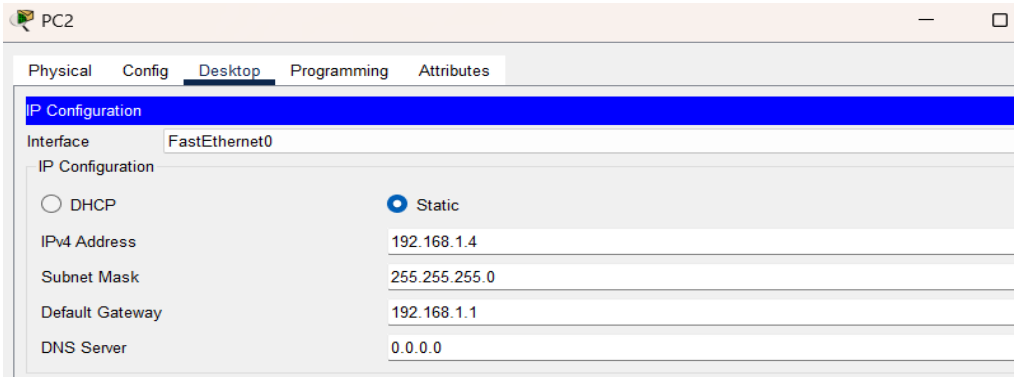
Network topology :



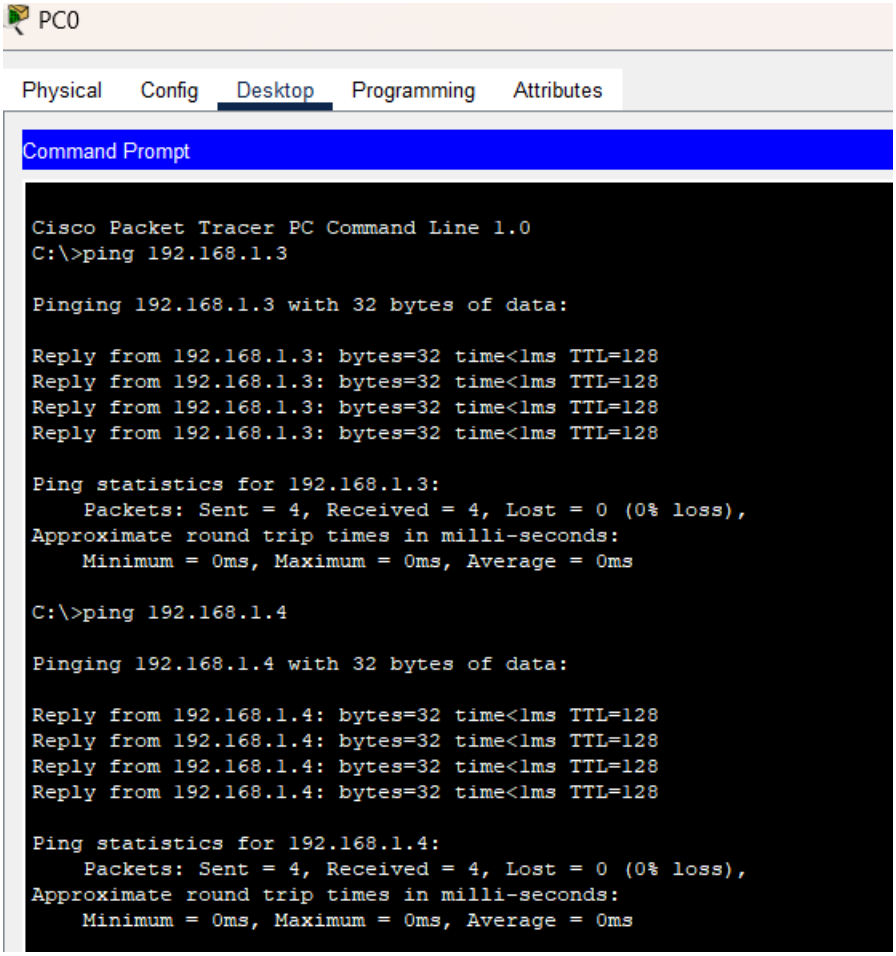
Configuring ip address in PC :







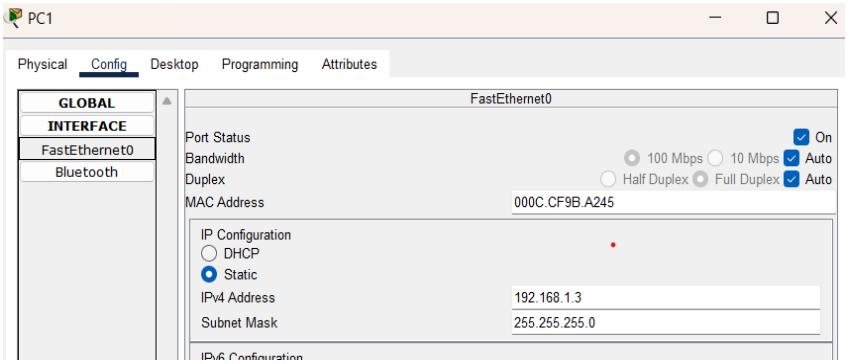
Pinging to other devices in pc0:



ARP table before spoofing :

```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.3           00d0.d33e.98d5        dynamic
  192.168.1.4           000c.cf9b.a245        dynamic
```

Changing PC1 MAC ADDRESS to attackers mac address:



Pinging from pc0 to pc1 after changing pc2 mac address:

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

ARP table after spoofing :

```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.3           000c.cf9b.a245        dynamic
  192.168.1.4           000c.cf9b.a245        dynamic
```

Behaviour of Devices after receving malicious arp response :

- ARP spoofing is a serious attack where the Attacker tricks the Victim PC into associating the Router's IP address with the Attacker's MAC address.
- This causes the Victim PC to send all traffic meant for the Router to the Attacker instead.
- The Attacker can then intercept, modify, or drop packets, leading to data theft, communication disruption, or other malicious activities.
- By using preventive measures like static ARP entries, DAI, and encryption, you can protect your network from ARP spoofing attacks.