Networking Training Program

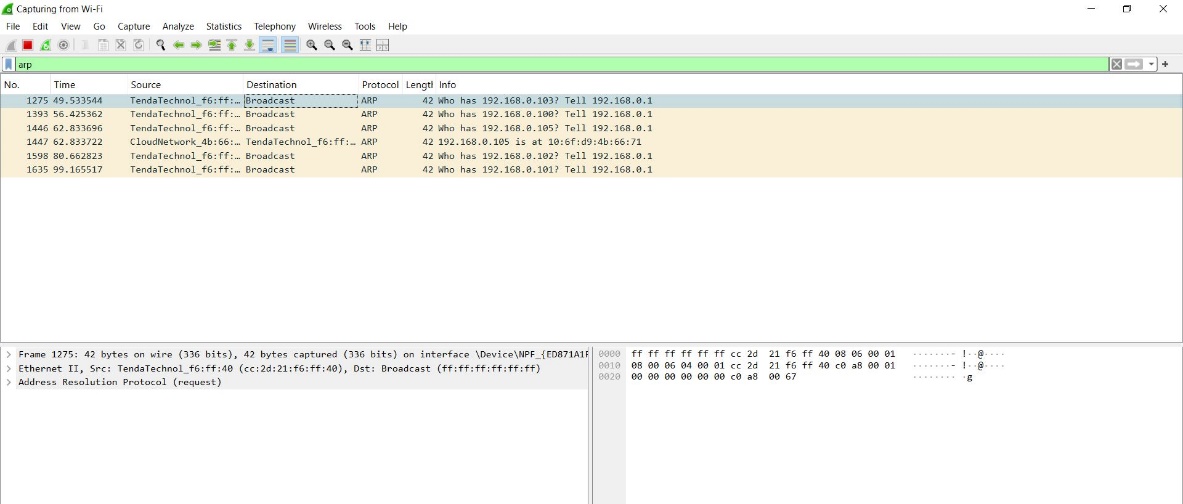
Module 05

Assignment Questions for Layer-03

Name: Gowtham S

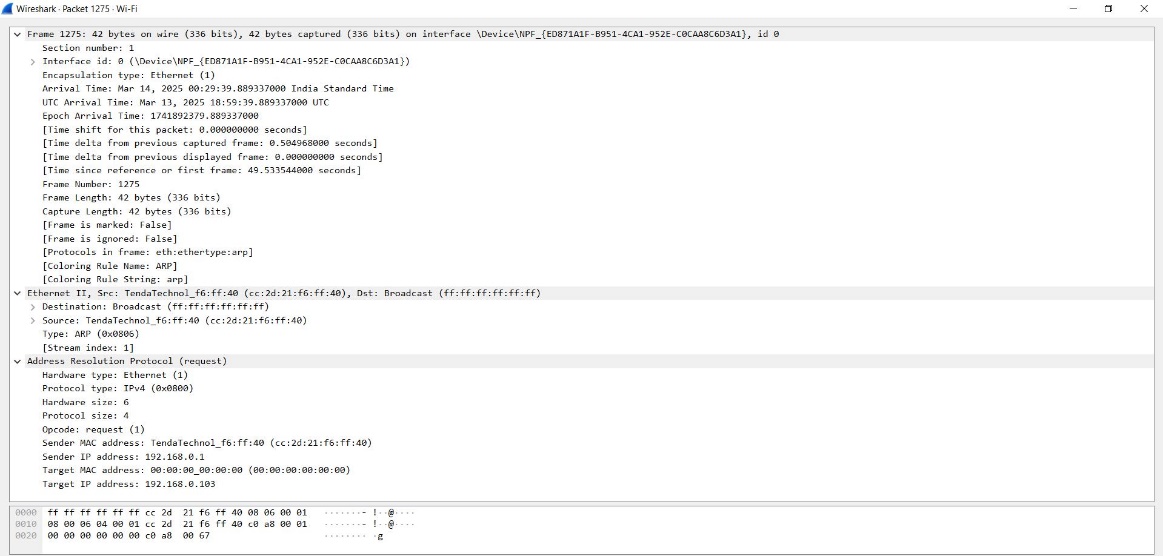
College: Kumaraguru College of Technology

1) Capture and analyse ARP packets using Wireshark. Inspect the ARP request and reply frames, and discuss the role of the sender's IP and MAC address in these packets.



Open Wireshark and capture packets through Wifi and use filter “ arp “ to capture only arp packets.

I have captured these packets by “ping google.com” command.



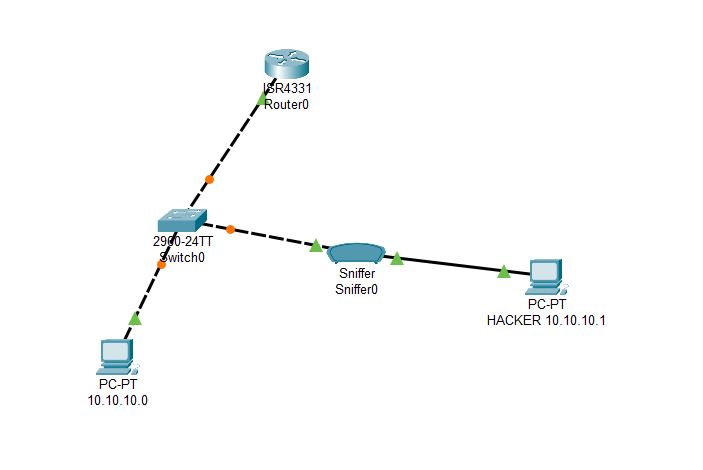
Now inside the captured packet we can see the ARP frame structure with all attributes.

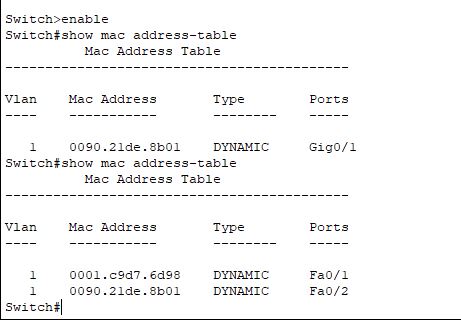
Role of the sender's IP and MAC address in these packets:

* The sender's IP in the ARP request identifies the device making the request.
* The sender’s IP in the ARP reply confirms the identity of the responding device.
* The sender's MAC in the ARP request helps other devices recognize the requester's identity.
* The responder provides its MAC in the ARP reply, allowing direct communication.

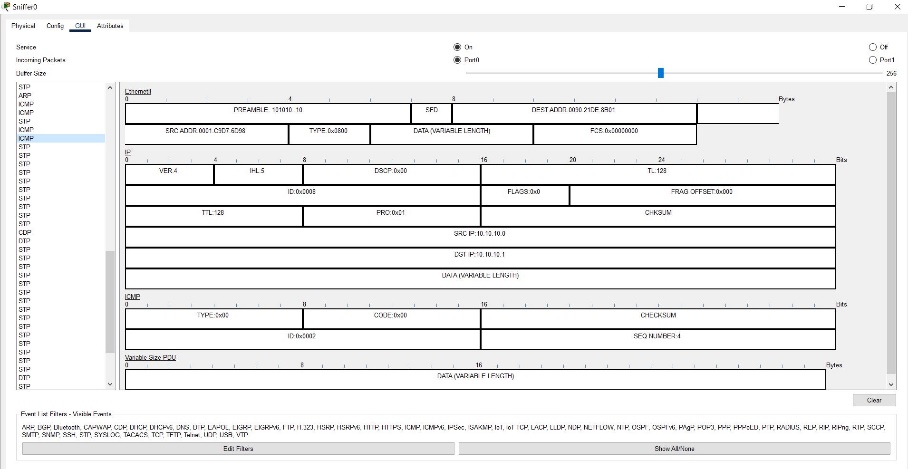
2) Using Packet Tracer, simulate an ARP spoofing attack. Analyze the behavior of devices on the network when they receive a malicious ARP response.

Ans: ARP spoofing is nothing but Middle men attack while the packet is transmitting from source to destination, this attack demo has been performed in CISCO packet tracer tool.

  
This is network to perform ARP spoofing.



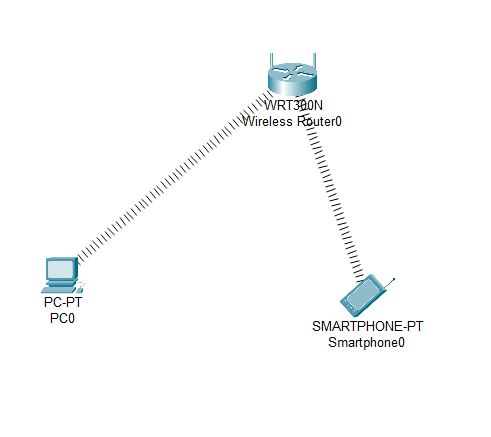
This is MAC address table of switch in that network there we can see that MAC address is spoofed that is MAC address of router is manually replaced in Hacker PC.



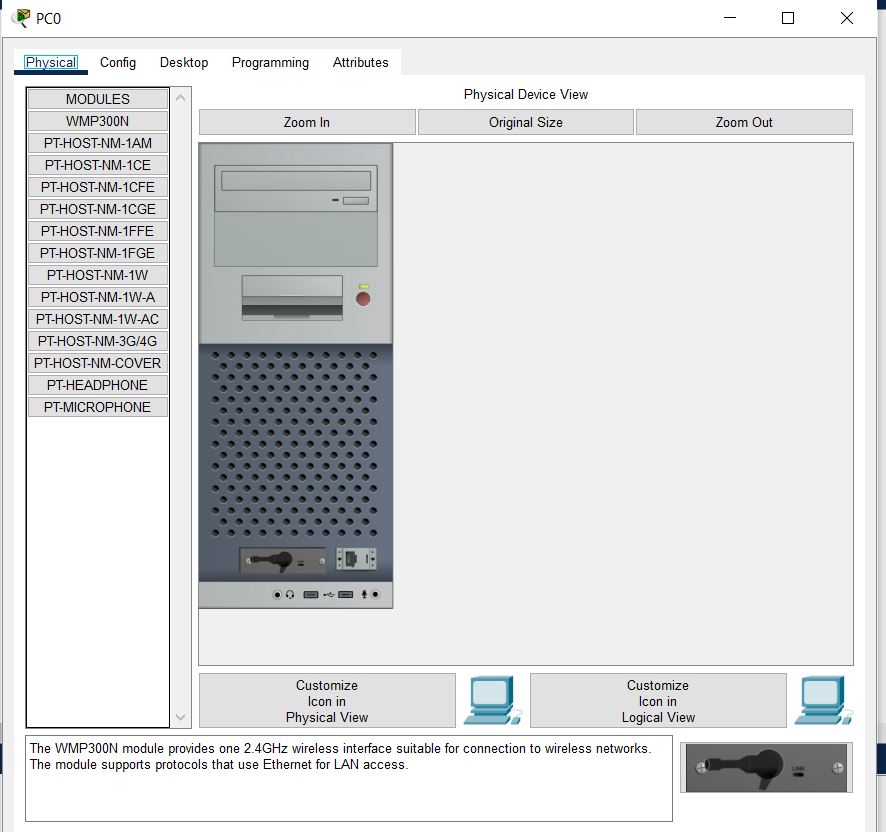
In this network spoofer is used to see whether hacker is receiving a packet from PC0or not and we proved that he received from above frame structure image which is captured by network spoofer of Hacker.

In this way ARP spoofing can be performed.

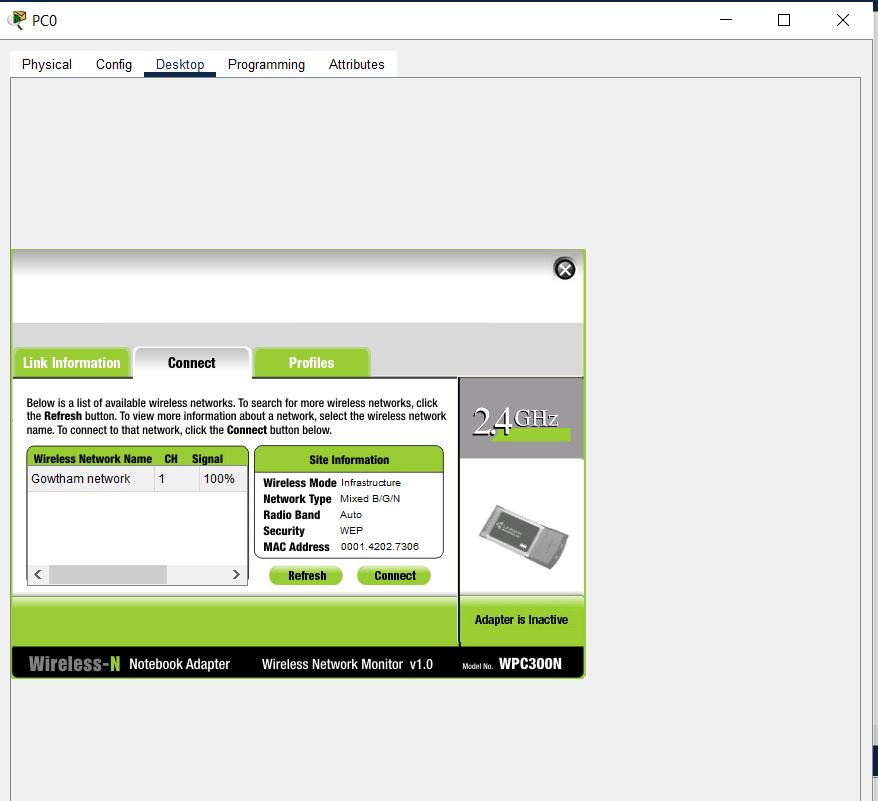
3) Manually configure static IPs on the client devices(like Pc or your mobile phone) and verify connectivity using ping.



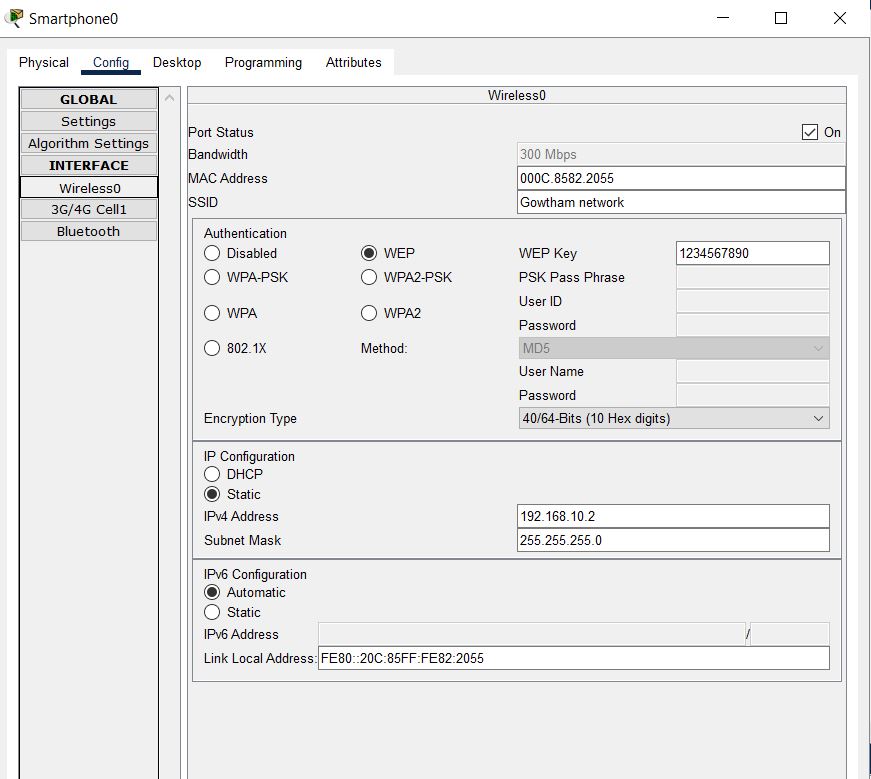
Now I have manually connected one PC and smartphone to wireless router.



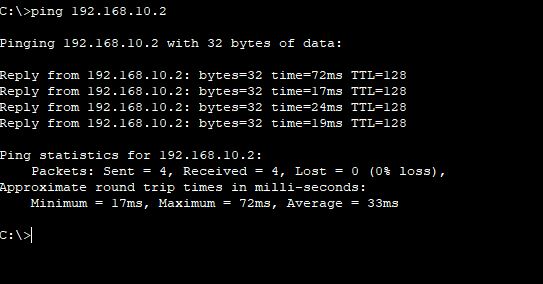
In pc physical setup we need to plug in WMP 300N to support wireless router connection.



Now PC has been successfully connected to wireless router.

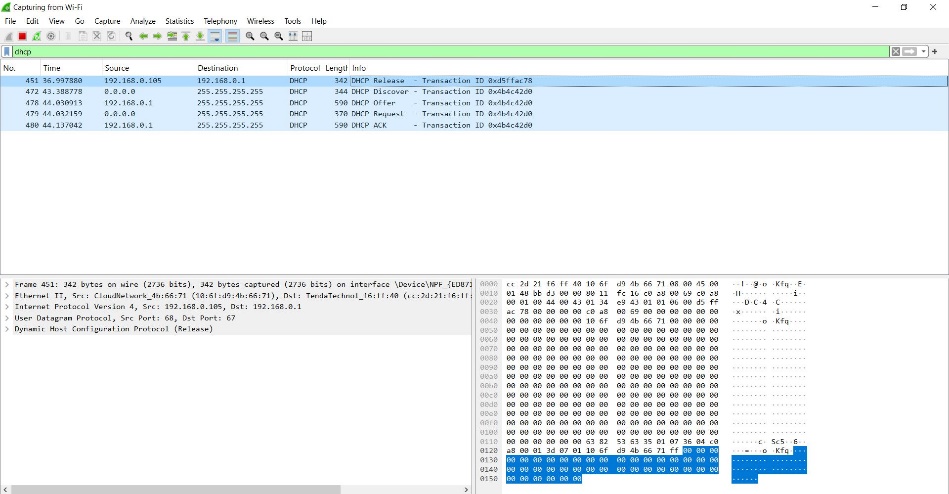


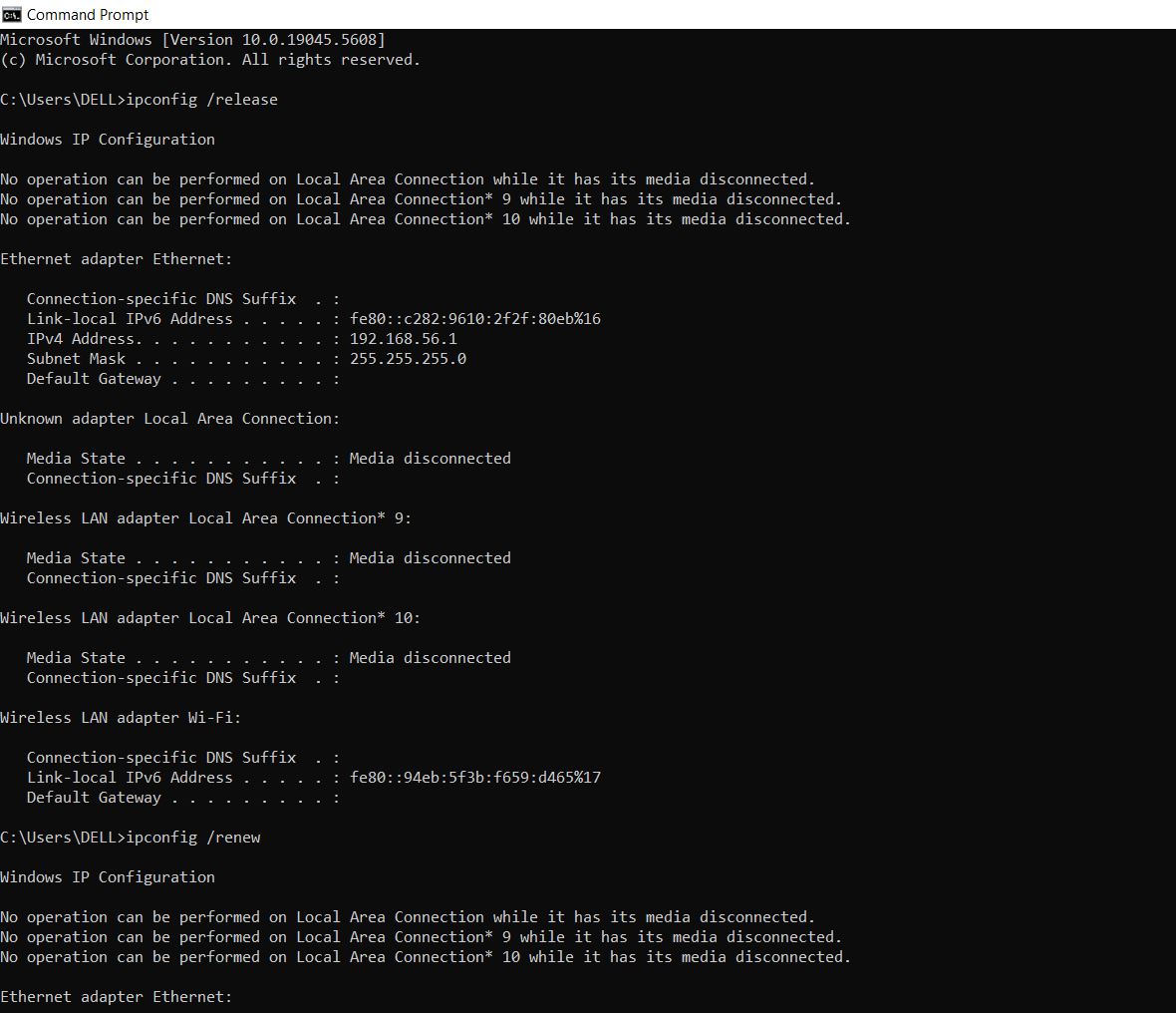
Smart phone manual IP config and wireless config has been done and now smartphone has been connected to wireless router.

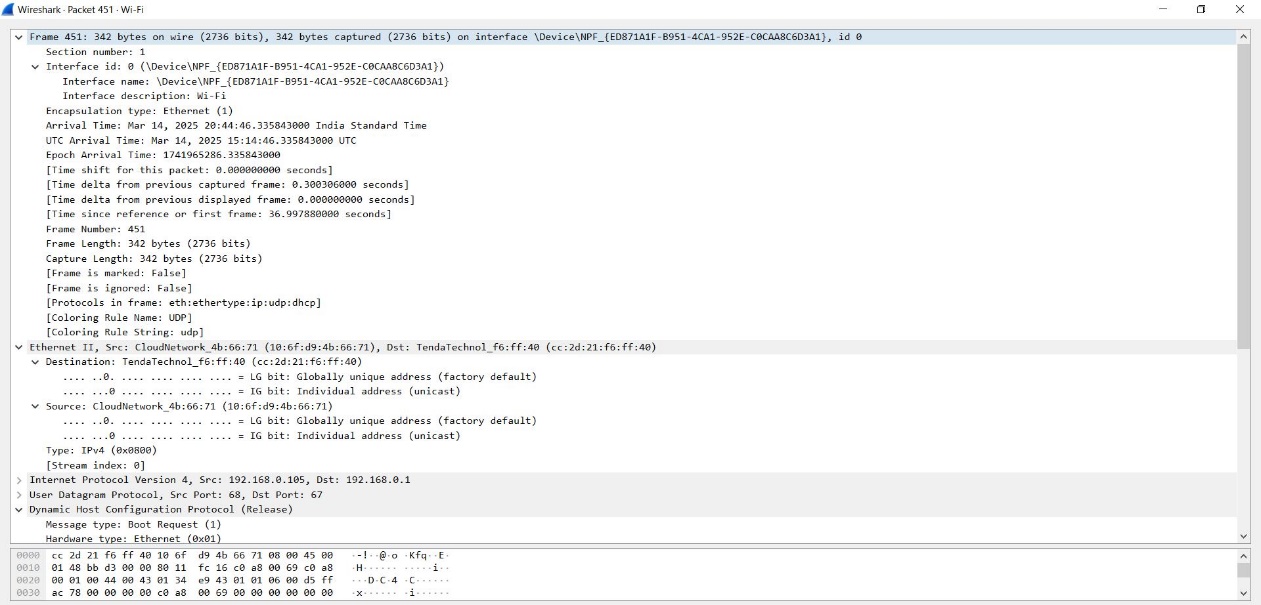


Now I ping smartphone IP from PC and ping has been successful.

4) Use Wireshark to capture DHCP Discover, Offer, Request, and Acknowledge messages and explain the process.

  
DHCP packet captured in Wireshark by triggering it using ipconfig /release and ipconfig/ renew command.



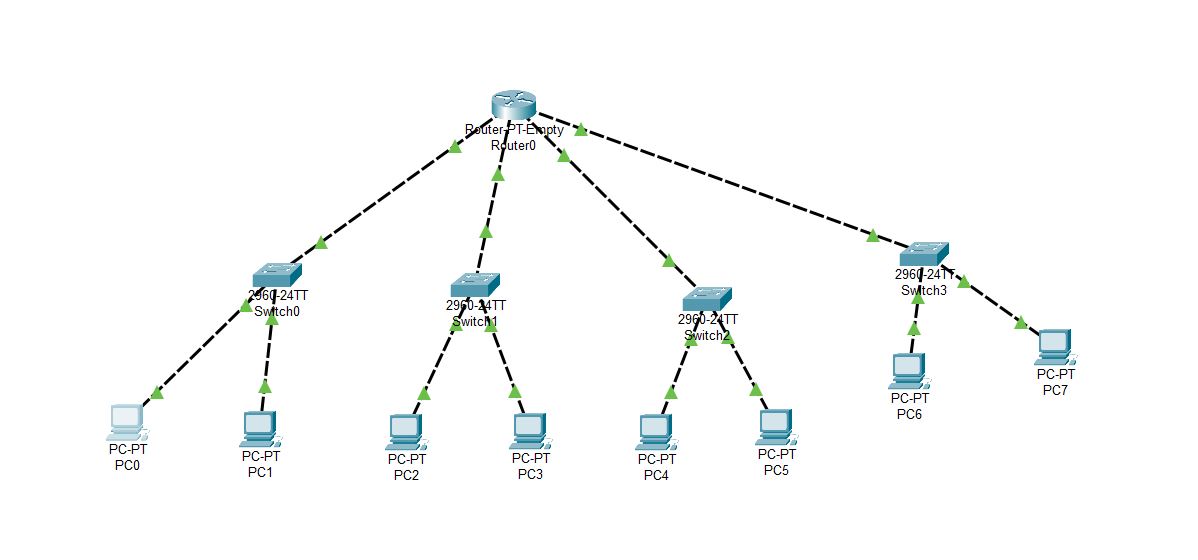


DHCP frame structure is captured in Wireshark.

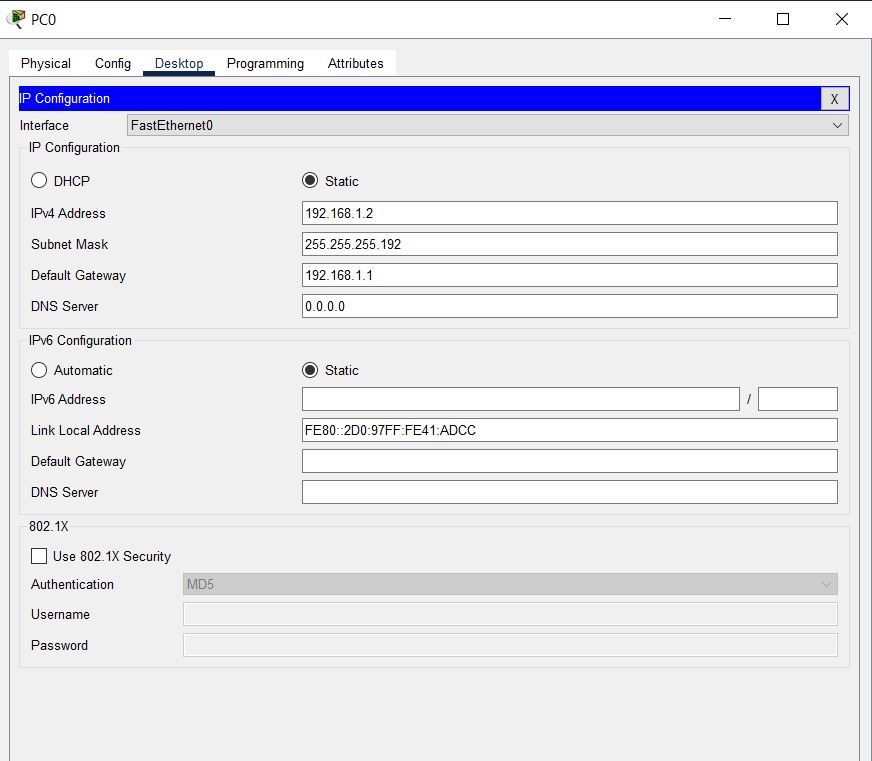
5) Given an IP address range of 192.168.1.0/24, divide the network into 4 subnets.

Task: Manually calculate the new subnet mask and the range of valid IP addresses for each subnet.

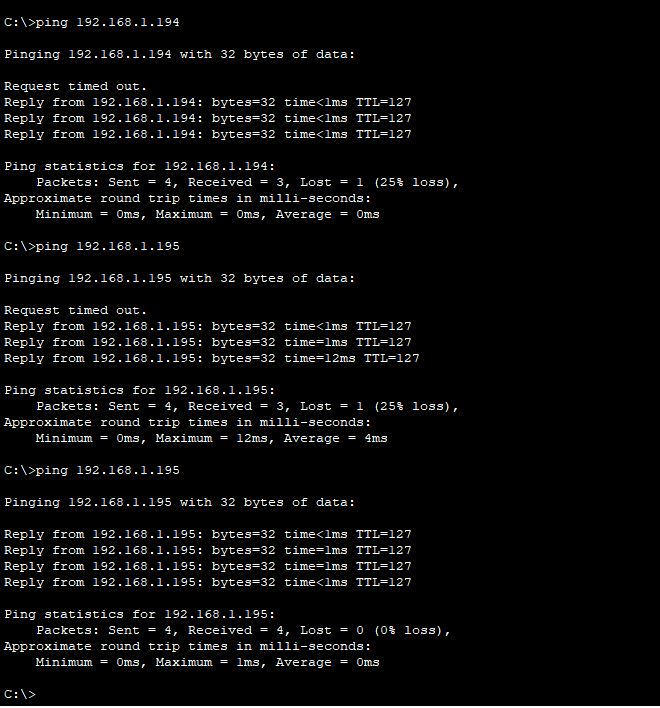
Assign IP addresses from these subnets to devices in Cisco Packet Tracer and verify connectivity using ping between them.



Subnetting LAN network with single router connected to 4 switch.



IP configuration of PC in subnetting network



Ping successful throughout the network with subnetting.

6) You are given three IP addresses: 10.1.1.1, 172.16.5.10, and 192.168.1.5.

Task: Identify the class of each IP address (Class A, B, or C). What is the default subnet mask for each class?

Provide the range of IP addresses for each class.

Ans : 10.1.1.1 → Class A, Default Subnet: 255.0.0.0

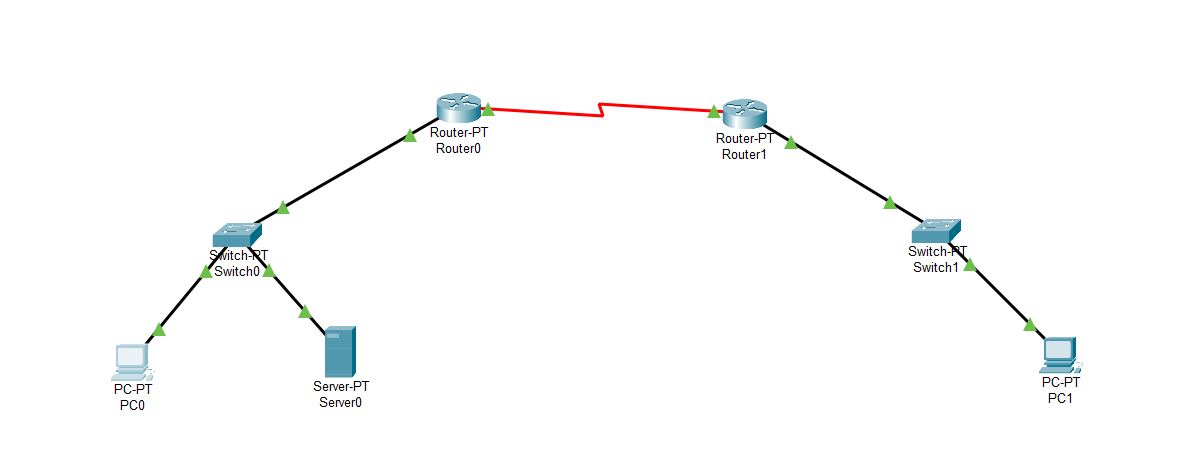
172.16.5.10 → Class B, Default Subnet: 255.255.0.0

192.168.1.5 → Class C, Default Subnet: 255.255.255.0

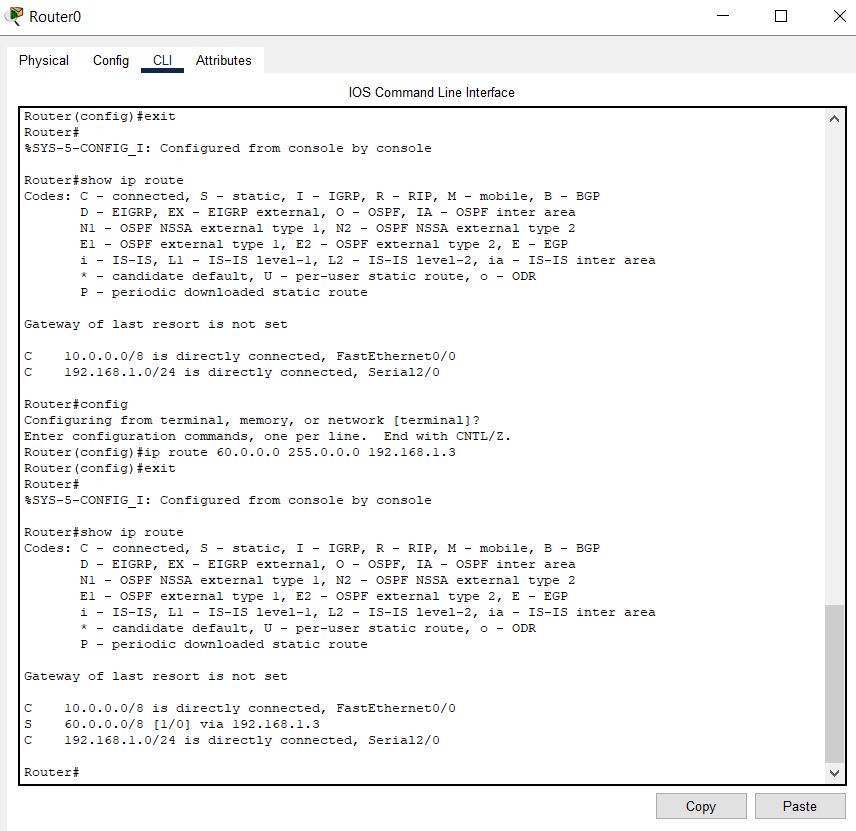
7) In Cisco Packet Tracer, create a small network with multiple devices (e.g., 2 PCs and a router). Use private IP addresses (e.g., 192.168.1.x) on the PCs and configure the router to perform NAT to allow the PCs to access the internet.

Task: Test the NAT configuration by pinging an external IP address from the PCs and capture the traffic using Wireshark.

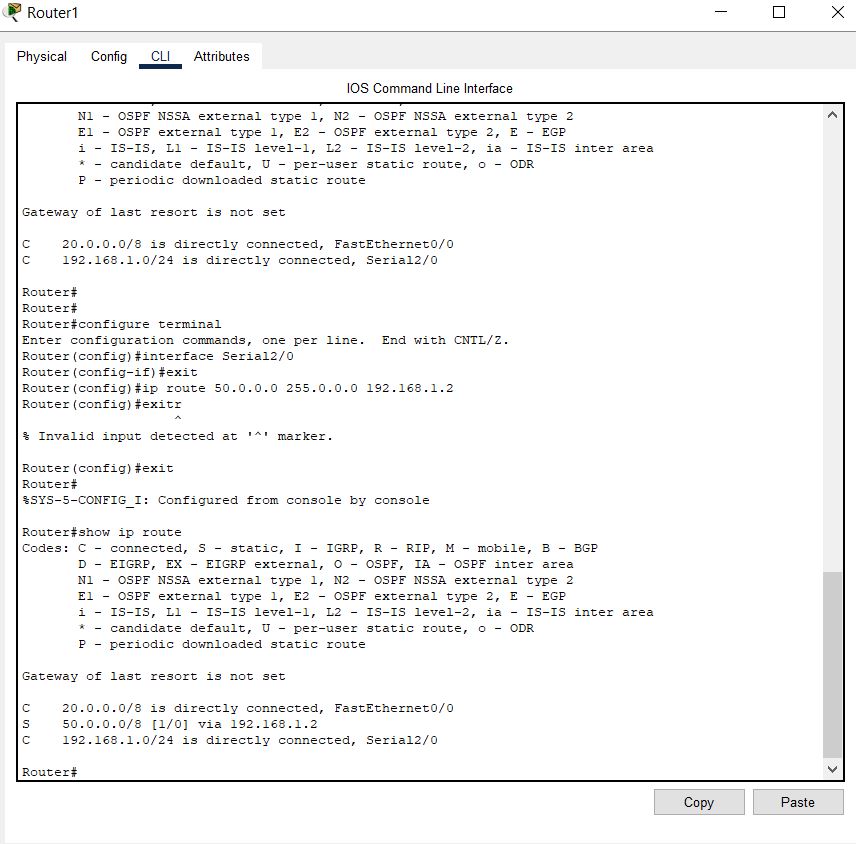
What is the source IP address before and after NAT?



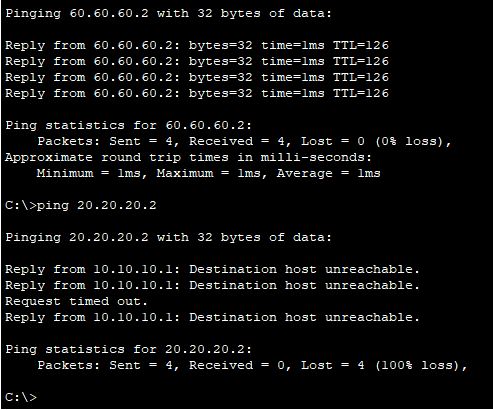
NAT demo network with 2 router and 2 switches connected.



Public IP route have been configured in router 0



Public IP route have been configured in router 1



Now Ping has been successful to public IP and host unreachable while trying with private IP in this way we can protect our private IP and this is simple static NAT implementation.