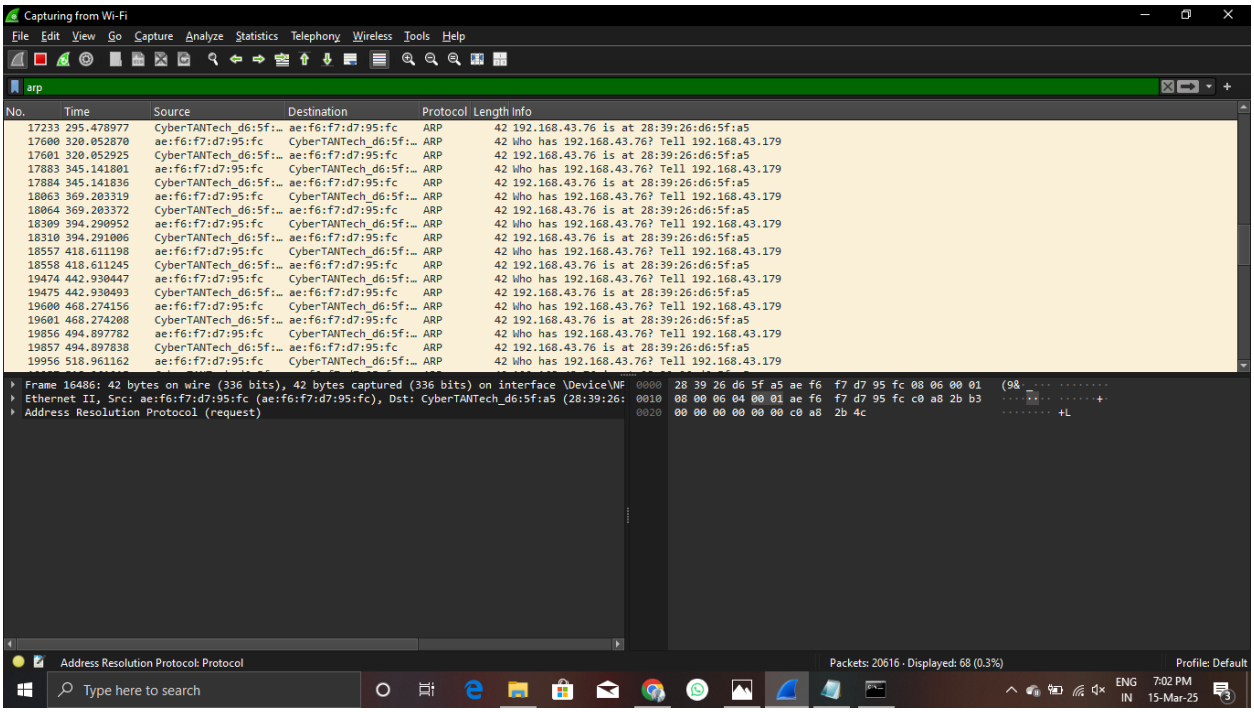
Network Training Assignment 5&6

- Yuvan Shankar

Problem1:



The sender's MAC address (ae:f6:f7:d7:95:fc) belongs to the device making the ARP request.

The sender's IP address (192.168.43.179) indicates the device that is looking for the MAC address of 192.168.43.76.

The target MAC address is 00:00:00:00:00:00 because the sender does not yet know it.

The target IP address is 192.168.43.76, meaning the sender wants to communicate with this device.

The ARP request is broadcasted to all devices on the local network to resolve the MAC address of 192.168.43.76.

If 192.168.43.76 is active, it will reply with an ARP reply containing its MAC address.

Once the ARP reply is received, 192.168.43.179 can directly communicate with 192.168.43.76 using its MAC address.

This process enables devices in a local network to discover each other's MAC addresses for direct communication.

Problem2:

ARP spoofing is an attack where a malicious device sends fake ARP replies on a network.

The attacker associates their MAC address with the IP of a legitimate device, like the gateway.

Victim devices update their ARP cache with the attacker's MAC instead of the real one.

Traffic meant for the legitimate device is sent to the attacker instead.

The attacker can intercept, modify, or drop packets (Man-in-the-Middle attack).

Problem3:

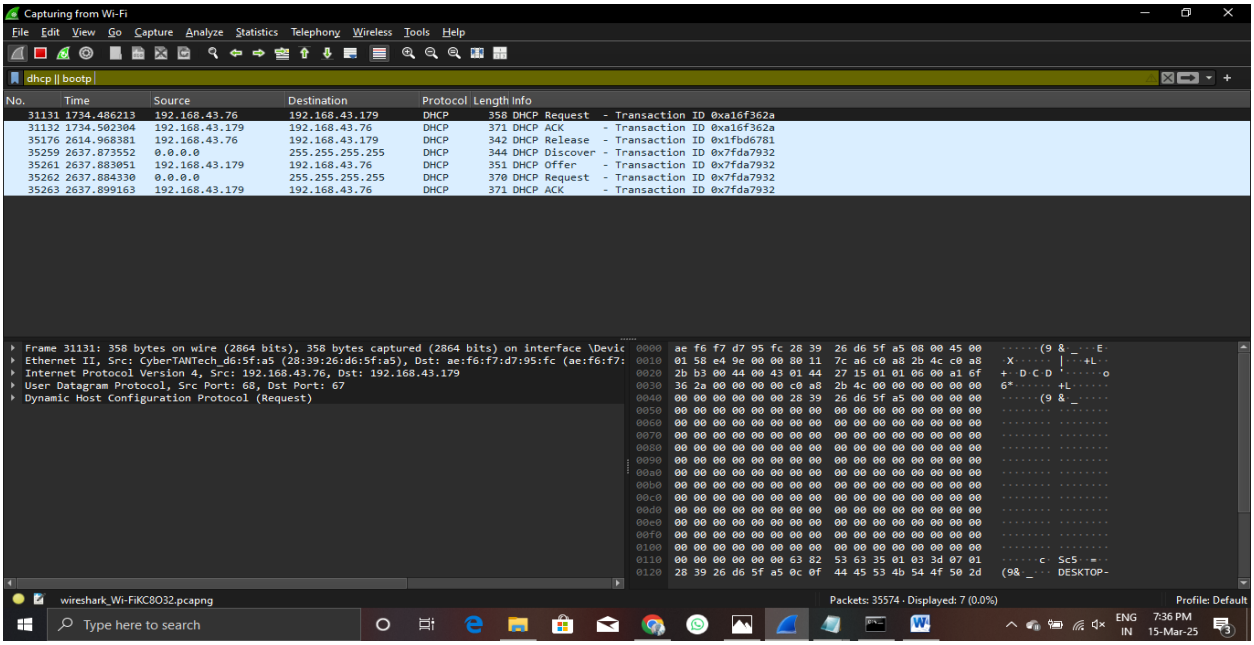
```
ubuntu@ubuntu1804:/etc/netplan$ sudo nano 01-network-manager-all.yaml
ubuntu@ubuntu1804:/etc/netplan$ sudo netplan apply
ubuntu@ubuntu1804:/etc/netplan$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.100  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fd00::a47b:ef2b:3e3e:6030  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::4c32:42ef:d617:52c6  prefixlen 64  scopeid 0x20<link>
        inet6 fd00::a00:27ff:fecb:3a16  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:cb:3a:16  txqueuelen 1000  (Ethernet)
        RX packets 23  bytes 2622 (2.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 256  bytes 28009 (28.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 430  bytes 33965 (33.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 430  bytes 33965 (33.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ubuntu@ubuntu1804:/etc/netplan$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:cb:3a:16 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fd00::a47b:ef2b:3e3e:6030/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86365sec preferred_lft 14365sec
    inet6 fd00::a00:27ff:fecb:3a16/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86365sec preferred_lft 14365sec
    inet6 fe80::4c32:42ef:d617:52c6/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
ubuntu@ubuntu1804:/etc/netplan$ ping 8.8.8.8
connect: Network is unreachable
ubuntu@ubuntu1804:/etc/netplan$ sudo nano 01-network-manager-all.yaml
ubuntu@ubuntu1804:/etc/netplan$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=0.046 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.084 ms
64 bytes from 192.168.1.100: icmp_seq=3 ttl=64 time=0.086 ms
64 bytes from 192.168.1.100: icmp_seq=4 ttl=64 time=0.078 ms
64 bytes from 192.168.1.100: icmp_seq=5 ttl=64 time=0.086 ms
```

As here in VM only Ethernet interface is available and I am connected to wifi, so I just ping locally the static ip and shown results.

Problem4:



The client, without an IP, sends a DHCP Discover message as a broadcast (0.0.0.0 → 255.255.255.255), asking for an IP address.

The DHCP server (192.168.43.179) responds with a DHCP Offer, offering an available IP (192.168.43.76) along with subnet mask, gateway, and DNS info.

The client sends a DHCP Request, confirming it wants to use the offered IP, broadcasting this request so other DHCP servers know it has made a choice.

The DHCP server sends a DHCP Acknowledge (ACK) to finalize the process, officially assigning 192.168.43.76 to the client with lease and configuration details.

The client can now communicate on the network using the assigned IP.

If multiple DHCP servers reply, the client selects one and ignores others.

If no DHCP server is available, the client may assign itself an APIPA (169.254.X.X).

This process is essential for automatic IP assignment.

Problem5:

Subnet 1:

Network: 192.168.1.0/26 First usable: 192.168.1.1 Last usable: 192.168.1.62 Broadcast: 192.168.1.63

Subnet 2:

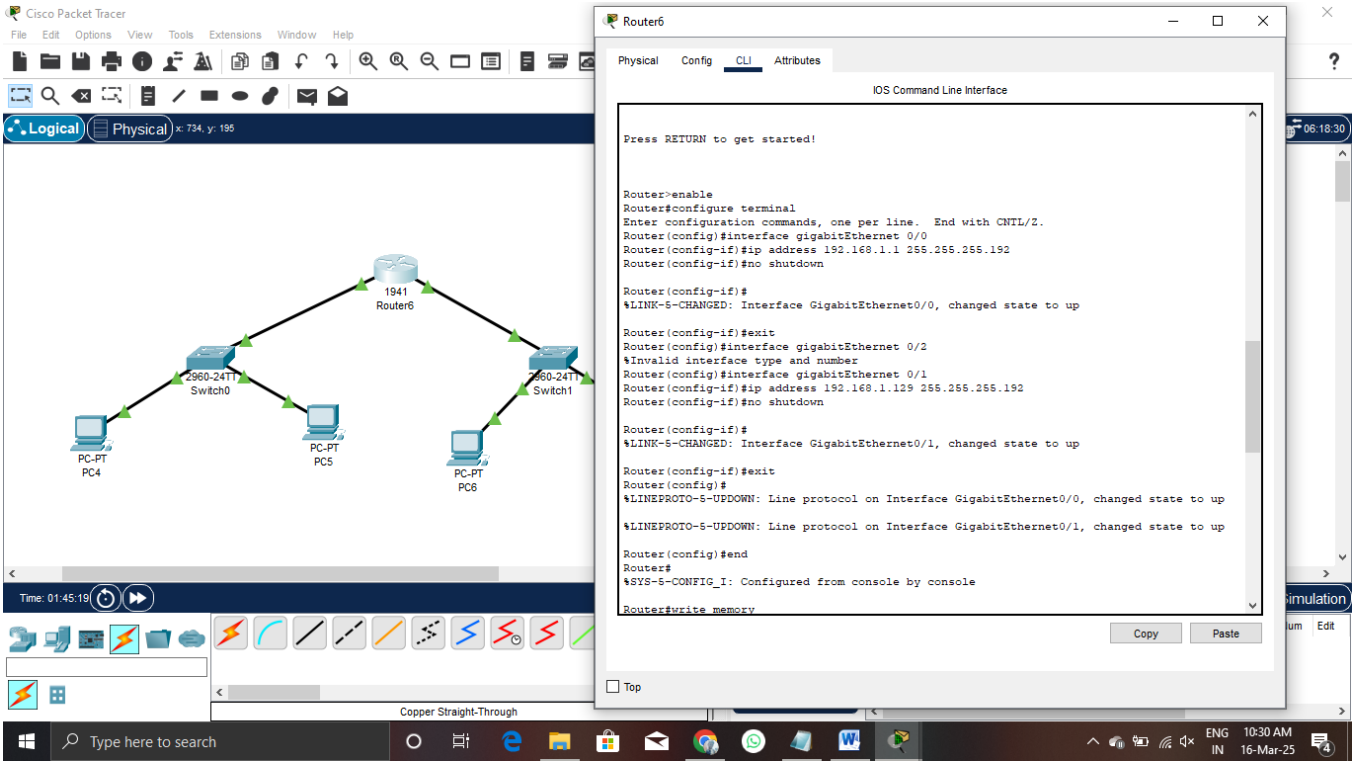
Network: 192.168.1.64/26 First usable: 192.168.1.65 Last usable: 192.168.1.126 Broadcast: 192.168.1.127

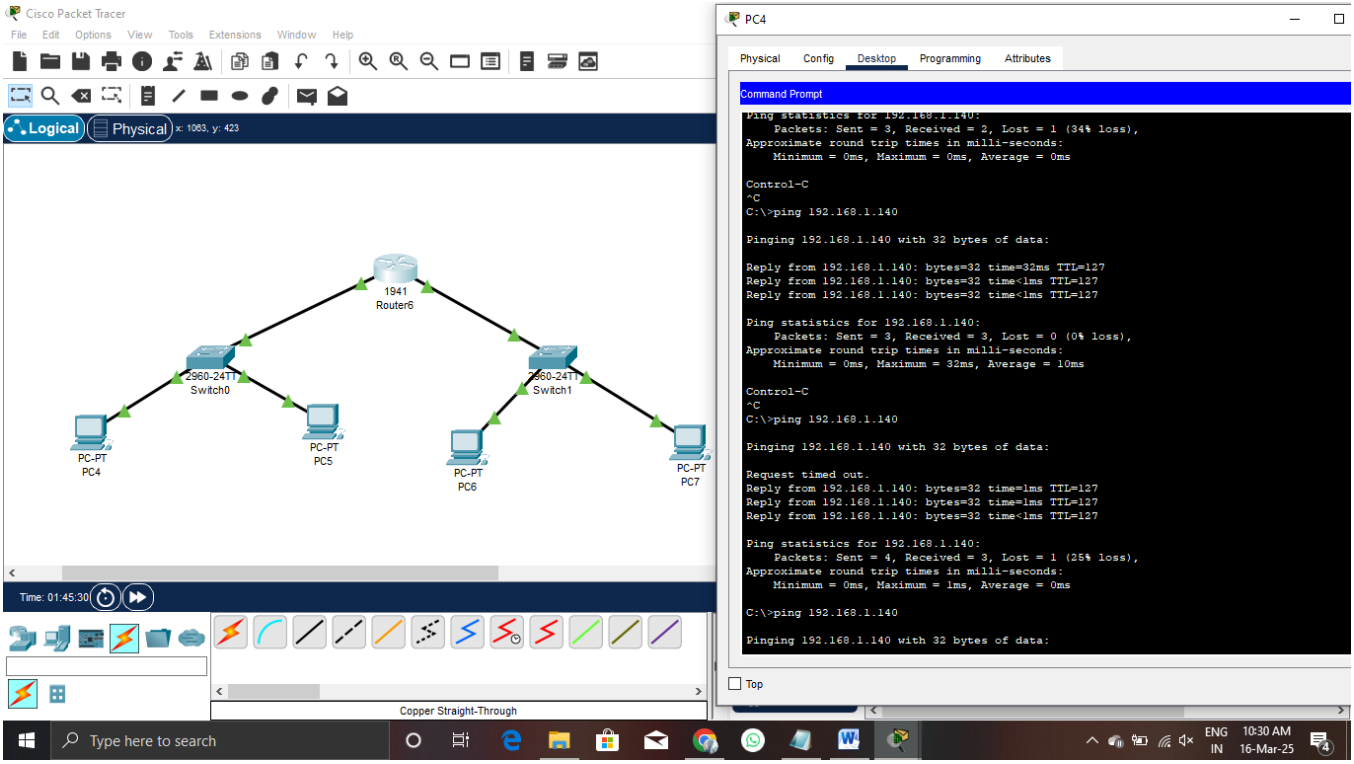
Subnet 3:

Network: 192.168.1.128/26 First usable: 192.168.1.129 Last usable: 192.168.1.190 Broadcast: 192.168.1.191

Subnet 4:

Network: 192.168.1.192/26 First usable: 192.168.1.193 Last usable: 192.168.1.254 Broadcast: 192.168.1.255





Problem6:

IP Address: 10.1.1.1

Class: A

Default Subnet Mask: 255.0.0.0

Class A Range: 10.0.0.0 - 10.255.255.255

First Octet Range: 1 - 126

IP Address: 172.16.5.10

Class: B

Default Subnet Mask: 255.255.0.0

Class B Range: 172.16.0.0 - 172.31.255.255

First Octet Range: 128 - 191

IP Address: 192.168.1.5

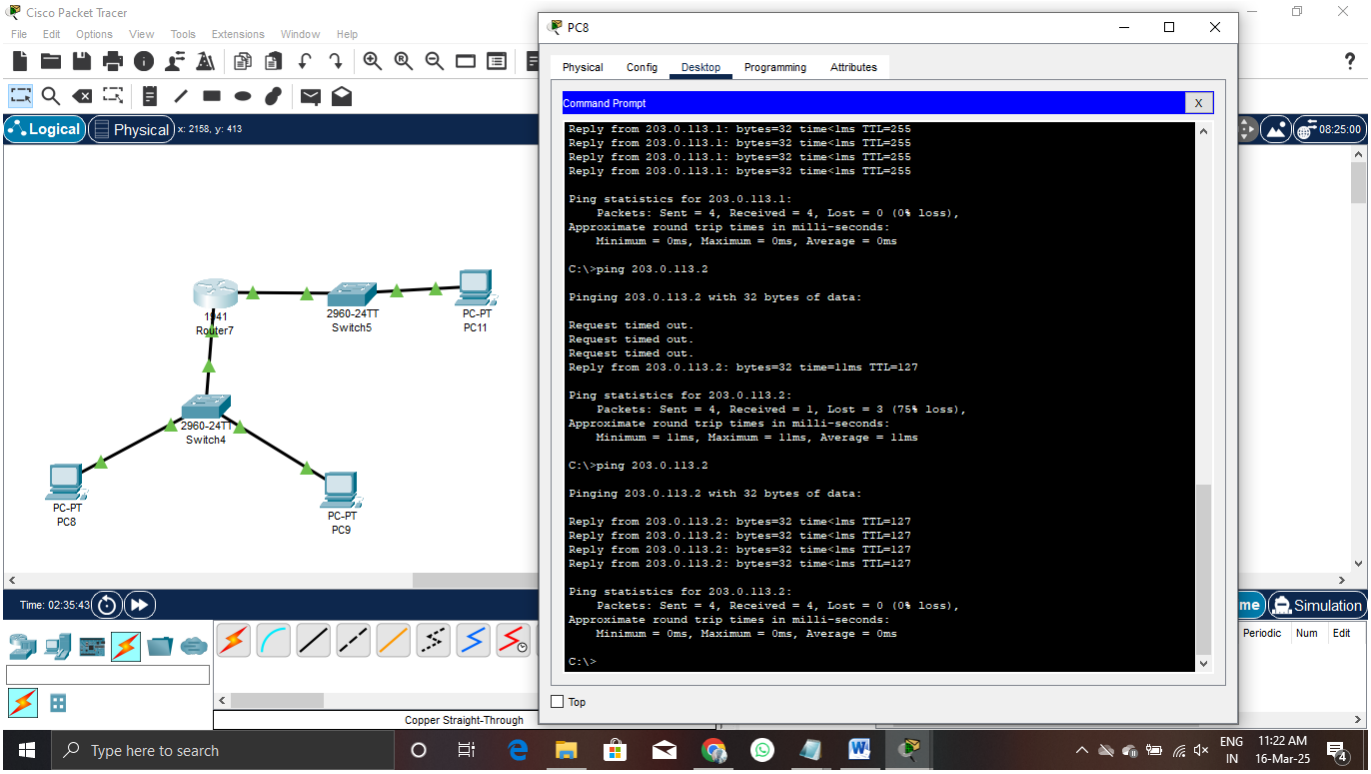
Class: C

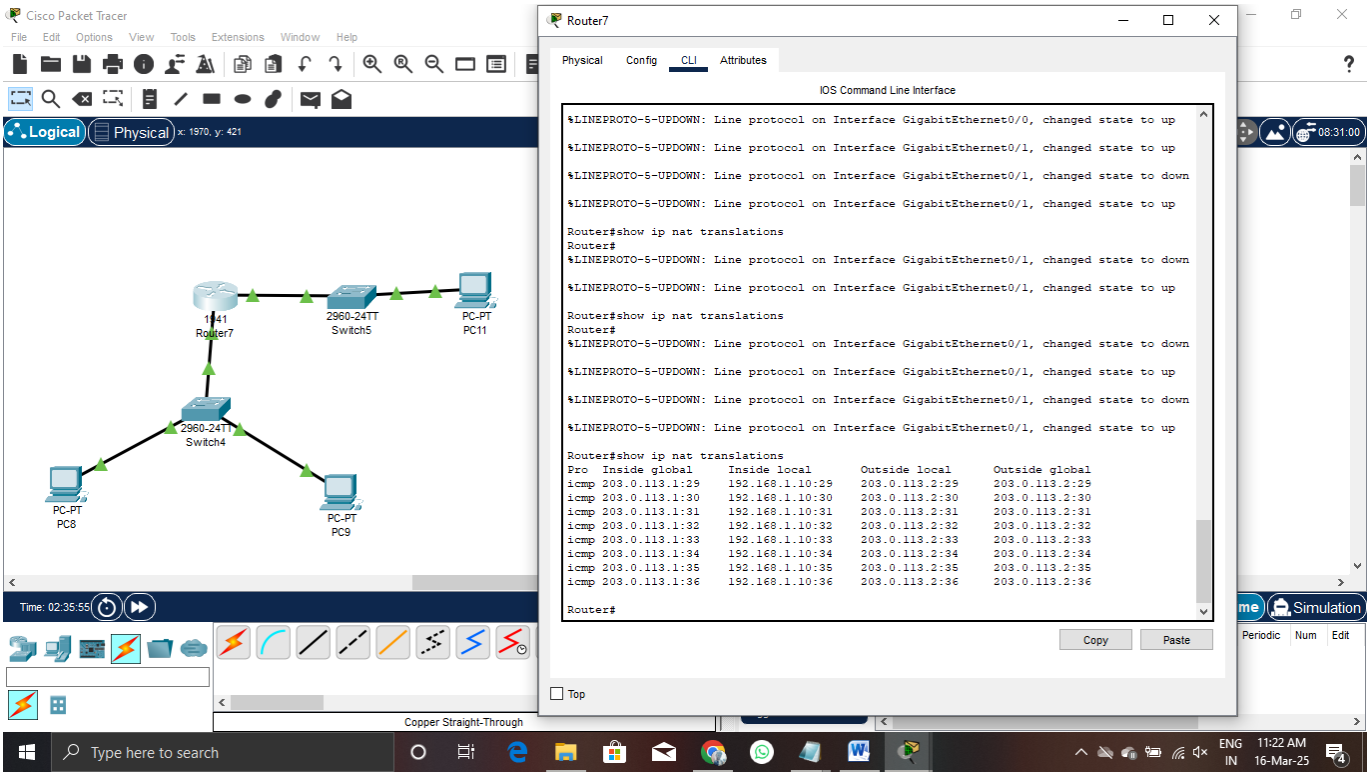
Default Subnet Mask: 255.255.255.0

Class C Range: 192.168.0.0 - 192.168.255.255

First Octet Range: 192 - 223

Problem7:





Before NAT:

Source IP in the packet is 192.168.1.10 (Private IP).

Router performs NAT and replaces the source IP.

After NAT:

Source IP becomes 203.0.113.1 (Public IP of the router).

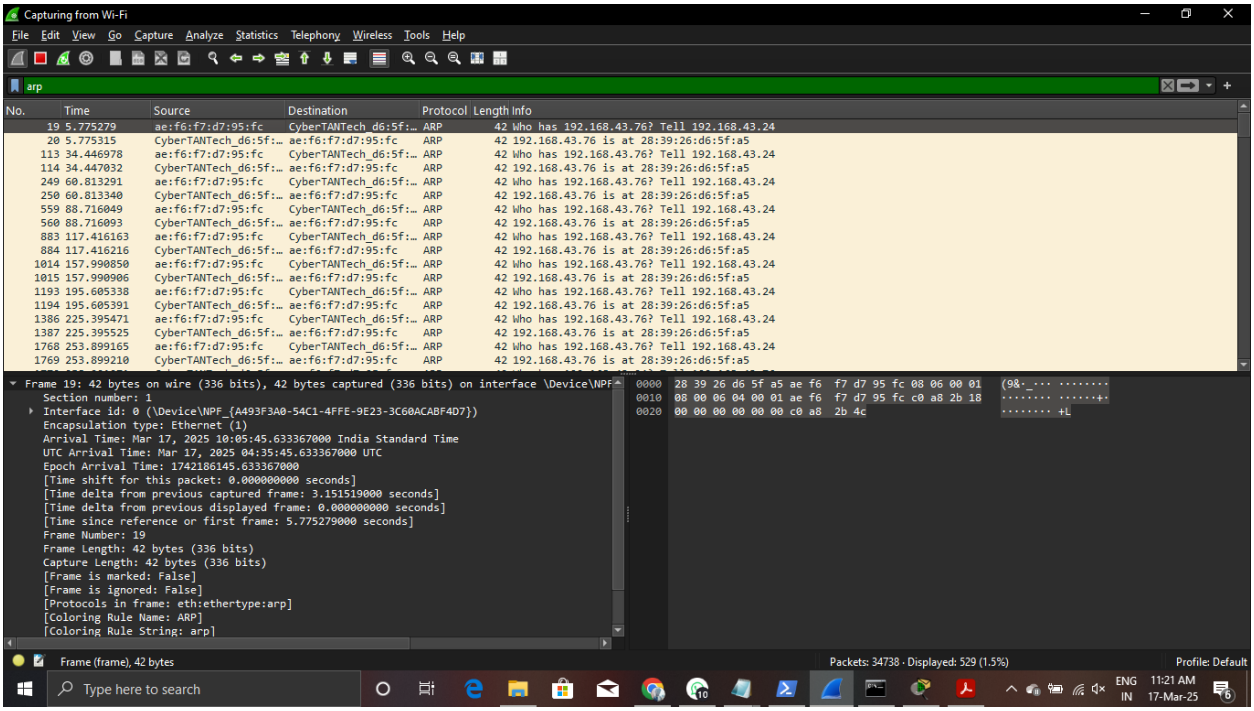
Packet reaches the destination 203.0.113.2.

Response from 203.0.113.2 is sent back to 203.0.113.1.

Router translates it back to 192.168.1.10 and forwards it to the PC.

PC receives the response, completing the communication.

Problem8:



Translates IP addresses to MAC addresses for communication within a local network.

Enables devices to find each other on the same subnet by resolving unknown MAC addresses.

Allows communication with the router by finding the MAC address of the default gateway.

Essential for Ethernet-based networks, where frames require destination MAC addresses.

Facilitates packet delivery within a LAN before forwarding to external networks.

Maintains an ARP cache to reduce repeated requests and improve efficiency.

Problem10:

Dividing into 4 equal subnets:

New subnet mask: /26 (255.255.255.192)

Each subnet has 64 addresses (2^6 = 64)

Valid host range (excluding network & broadcast addresses):

Subnet 1:

Network: 10.0.0.0/26

Valid hosts: 10.0.0.1 – 10.0.0.62

Broadcast: 10.0.0.63

Subnet 2:

Network: 10.0.0.64/26

Valid hosts: 10.0.0.65 – 10.0.0.126

Broadcast: 10.0.0.12

Subnet 3:

Network: 10.0.0.128/26

Valid hosts: 10.0.0.129 – 10.0.0.190

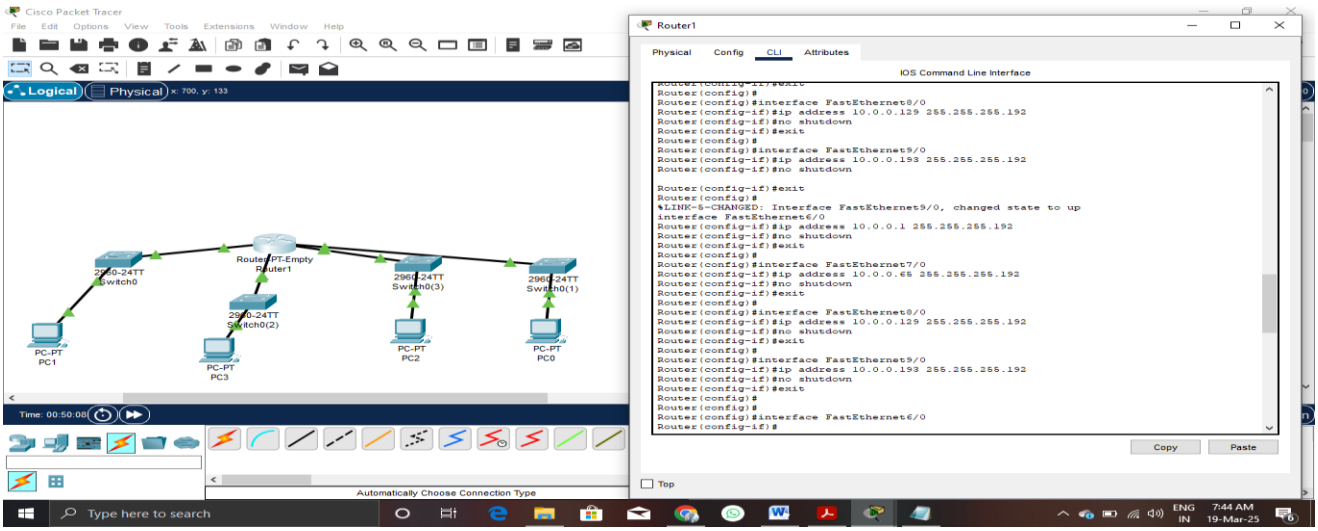
Broadcast: 10.0.0.191

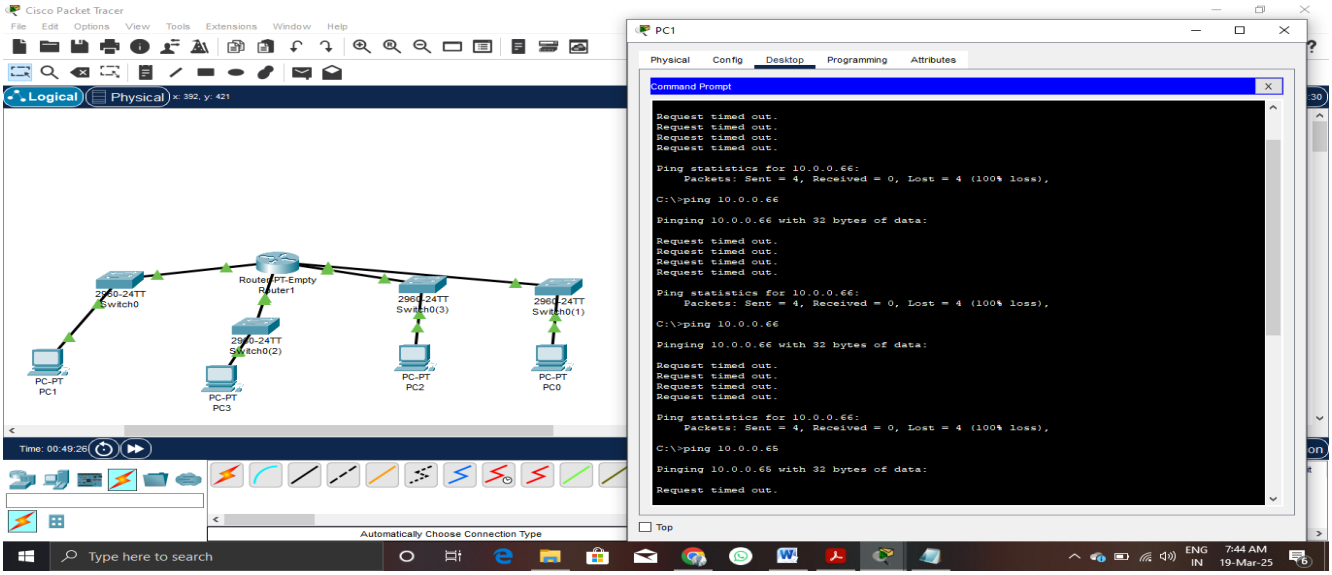
Subnet 4:

Network: 10.0.0.192/26

Valid hosts: 10.0.0.193 – 10.0.0.254

Broadcast: 10.0.0.255





Problem11:

- 192.168.10.5

  - Class C (Range: 192.0.0.0 – 223.255.255.255)

  - Private (192.168.x.x is reserved for private networks)

- 172.20.15.1

- Class B (Range: 128.0.0.0 – 191.255.255.255)

- Private (172.16.0.0 – 172.31.255.255 is reserved for private use)

- 8.8.8.8

- Class A (Range: 1.0.0.0 – 126.255.255.255)

- Public (Google's public DNS server)

Problem12: