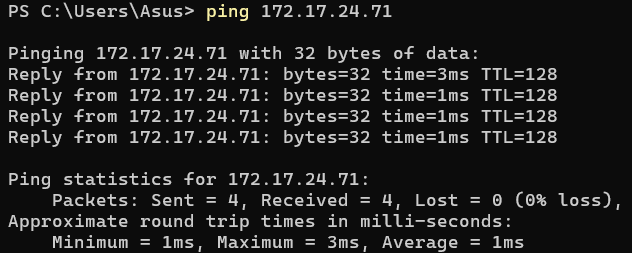
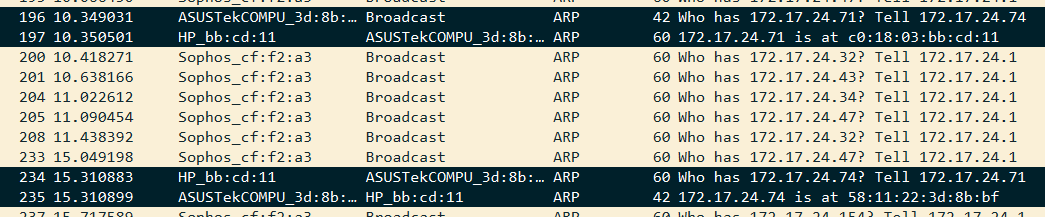
**Q1. Capture and analyze ARP packets using Wireshark. Inspect the ARP request and reply frames, and discuss the role of the sender's IP and MAC address in these packets.**

**Source : Laptop IP - 172.17.24.74**

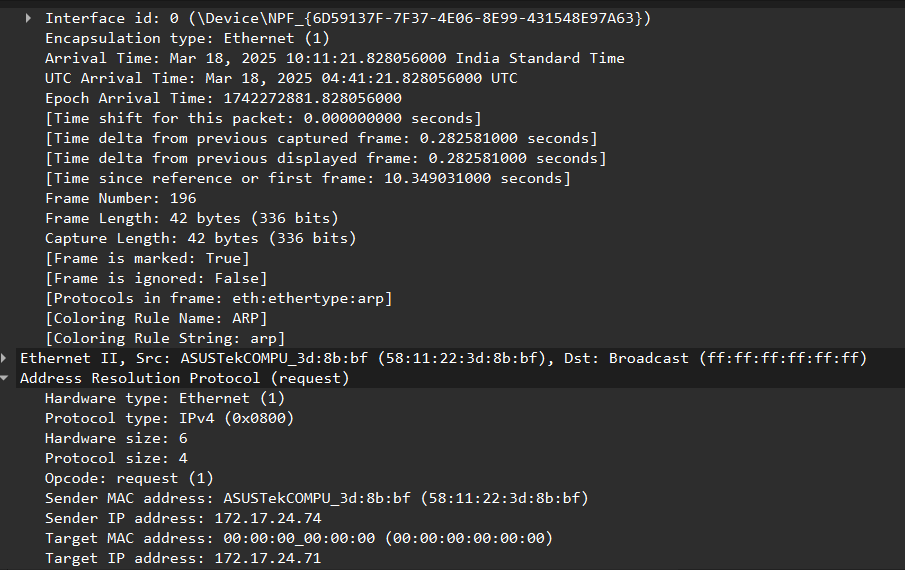
**Ping to 172.17.24.71 system in LAN**



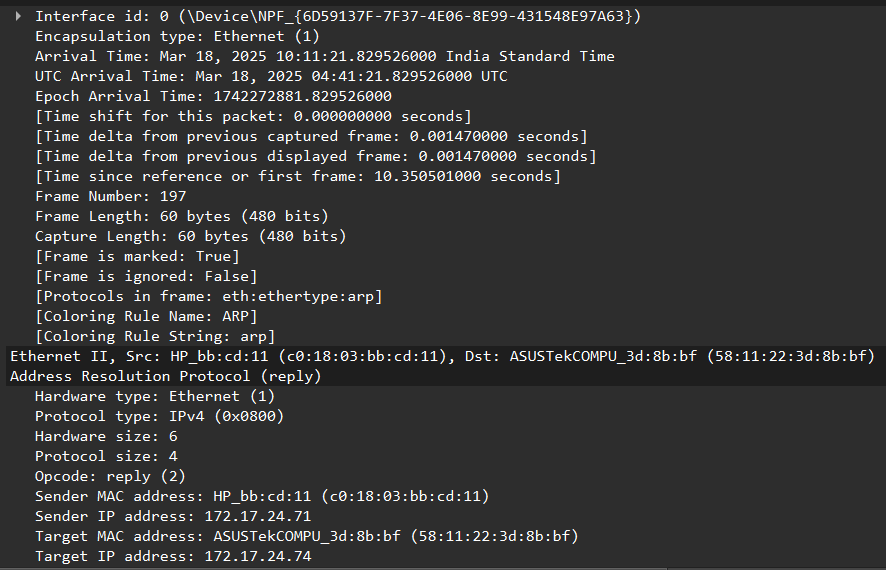
**Network Traffic in wireshark**



**ARP request packet** :



**ARP reply packet** :



**1. ARP Request Frame Structure**

**An ARP Request is broadcasted in the network to find the MAC address corresponding to a given IP address.**

* **Sender MAC Address: The MAC address of the device sending the request.**
* **Sender IP Address: The IP address of the sender requesting the MAC.**
* **Target MAC Address: Set to 00:00:00:00:00:00 (unknown).**
* **Target IP Address: The IP address whose MAC address is being requested.**
* **Destination MAC Address: FF:FF:FF:FF:FF:FF (broadcast).**

#### **2. ARP Reply Frame Structure**

**An ARP Reply is a unicast response from the requested device providing its MAC address.**

* **Sender MAC Address: The MAC address of the device responding.**
* **Sender IP Address: The IP address of the device responding.**
* **Target MAC Address: The MAC address of the requesting device.**
* **Target IP Address: The IP address of the requesting device.**
* **Destination MAC Address: MAC address of the request sender (unicast).**

### **Role of Sender's IP and MAC Address**

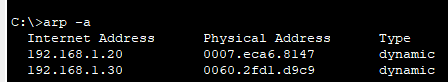
1. **In ARP Request:**
   * **The sender's IP address is used so that the recipient knows who is making the request.**
   * **The sender's MAC address is included so that the recipient can send the ARP Reply directly back.**
2. **In ARP Reply:**
   * **The sender's IP and MAC address provide the requested mapping.**
   * **The requester's MAC address ensures the reply reaches the correct device.**

**Q2.Using Packet Tracer, simulate an ARP spoofing attack. Analyze the behavior of devices on the network when they receive a malicious ARP response.**

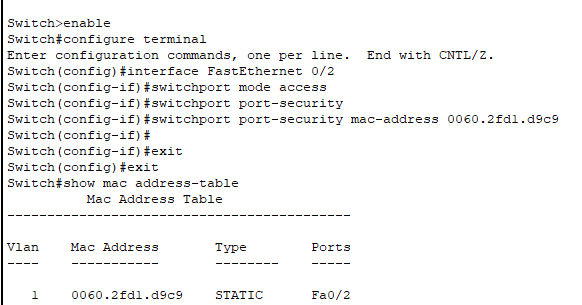
**PC-1:** 192.168.1.10

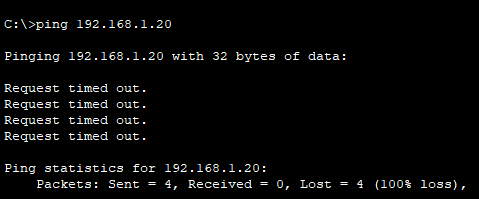
**PC-2:** 192.168.1.20

**PC-3 (Attacker):** 192.168.1.30



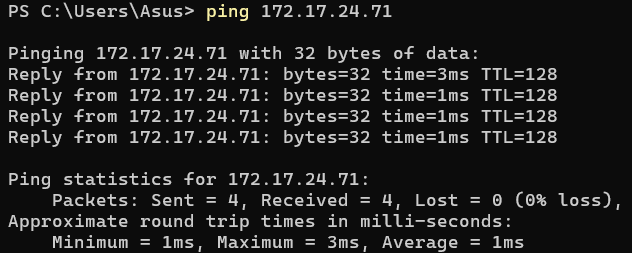
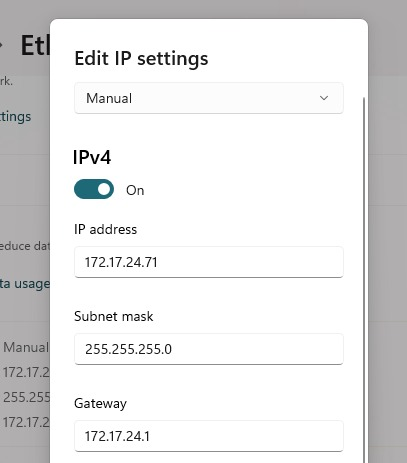
Changed the MAC address of PC2 with MAC address of PC3



Ping from PC1 , PC2 can’t be reached as PC2 and PC3 has same MAC address  
  


**Q3.Manually configure static IPs on the client devices(like Pc or your mobile phone) and verify connectivity using ping.**

**Configure a PC with IP : 172.17.24.71 with 255.255.255.0**



**Q4.Use Wireshark to capture DHCP Discover, Offer, Request, and Acknowledge messages and explain the process.**

Laptop IP : 192.168.104.159

Router IP : 192.168.104.131

The **DORA** process is a four-step mechanism used by the **Dynamic Host Configuration Protocol (DHCP)** to assign an IP address dynamically to a client.

#### **1. Discover (D)**

* The client (new device) broadcasts a **DHCPDISCOVER** message to find available DHCP servers.
* Source IP: 0.0.0.0 (since the client has no IP yet).
* Destination IP: 255.255.255.255 (broadcast).

#### **2. Offer (O)**

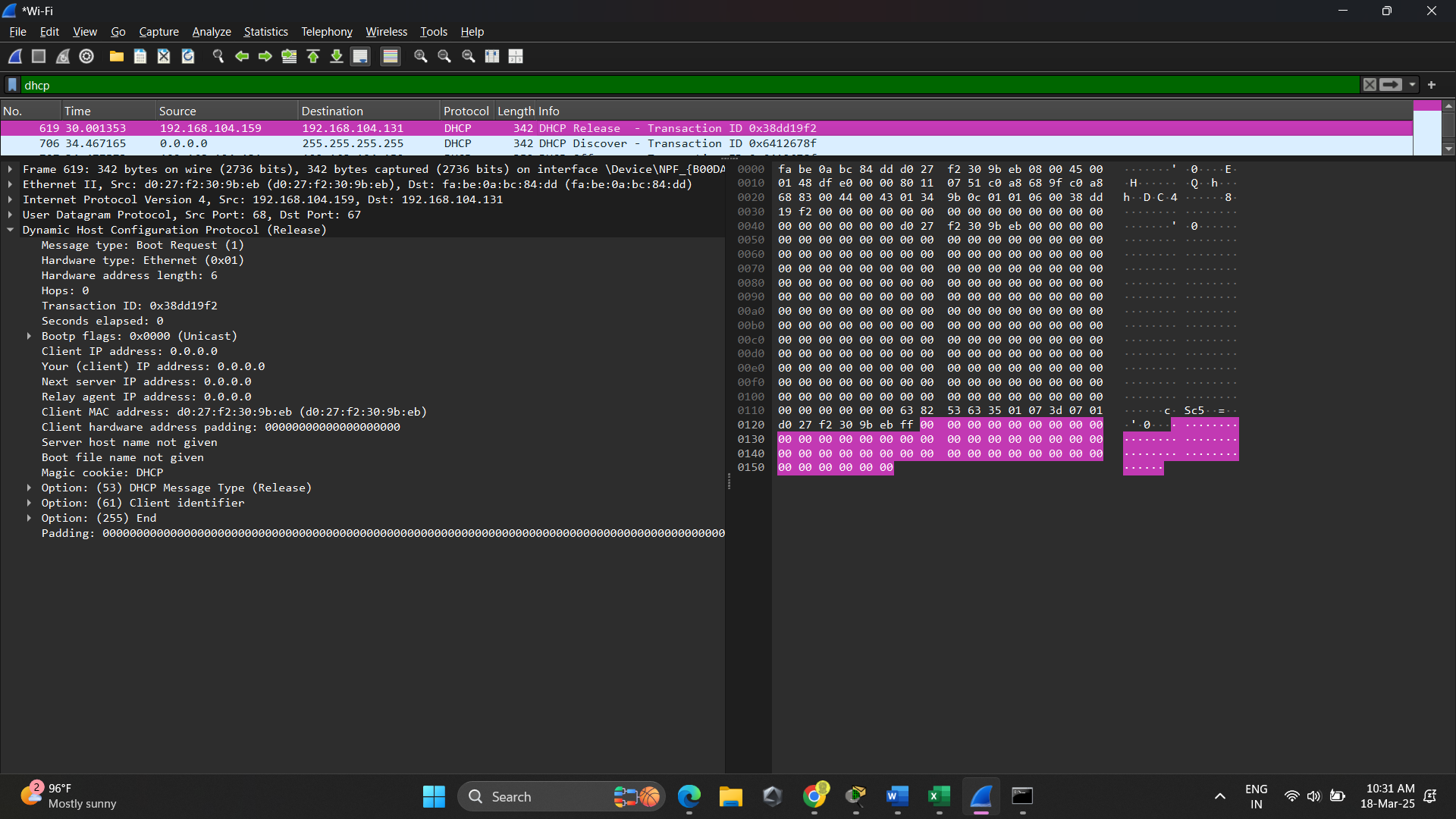
* A DHCP server responds with a **DHCPOFFER**, proposing an available IP address.
* The offer includes:
  + Available IP address.
  + Subnet mask, gateway, and lease duration.
  + Server's IP address.

#### **3. Request (R)**

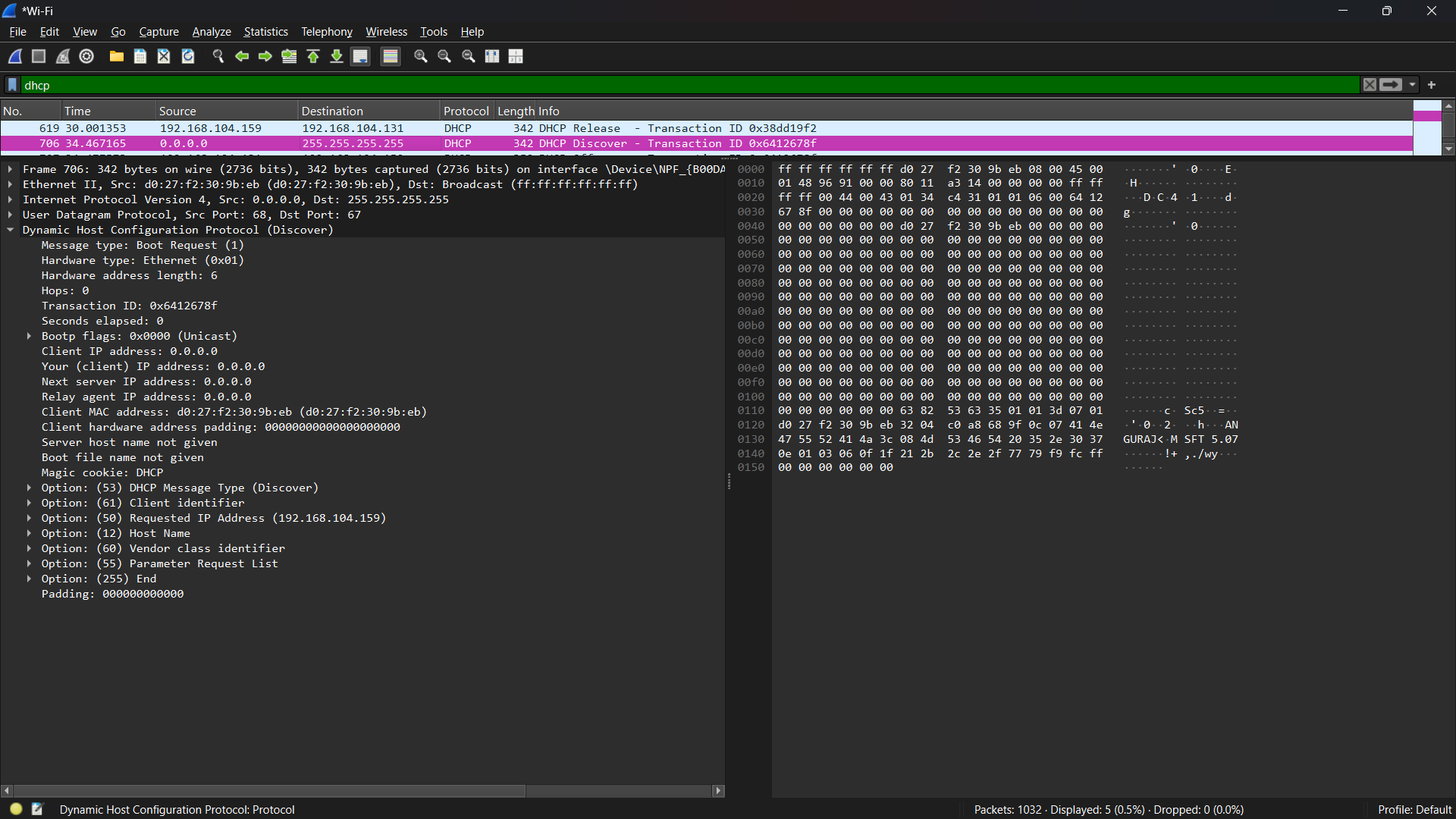
* The client responds with a **DHCPREQUEST** to accept the offered IP.
* The request is broadcasted, allowing other DHCP servers (if any) to know the client accepted this offer.

#### **4. Acknowledge (A)**

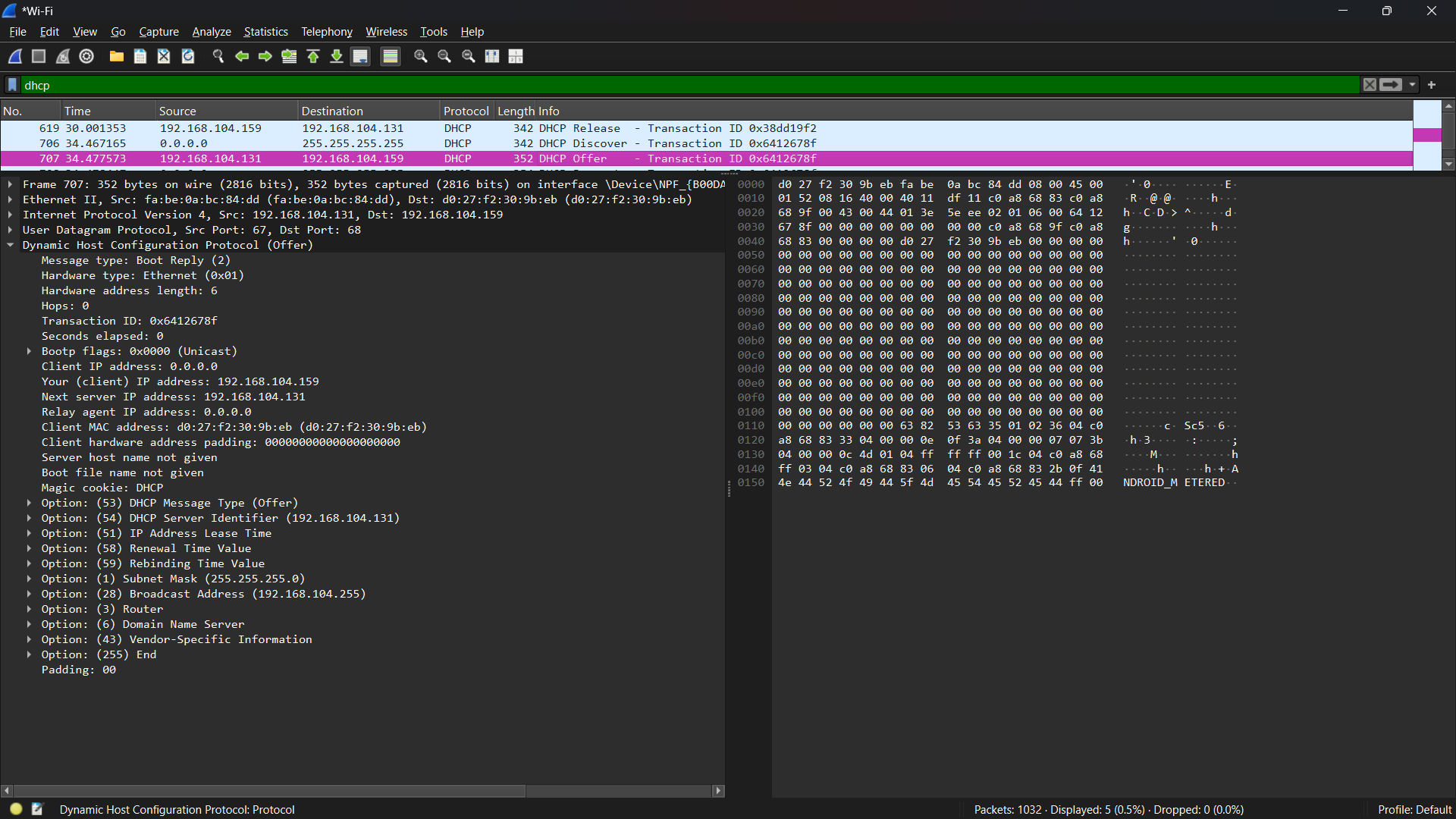
* The DHCP server sends a **DHCPACK** message, confirming the lease.
* The client configures the assigned IP and network settings.



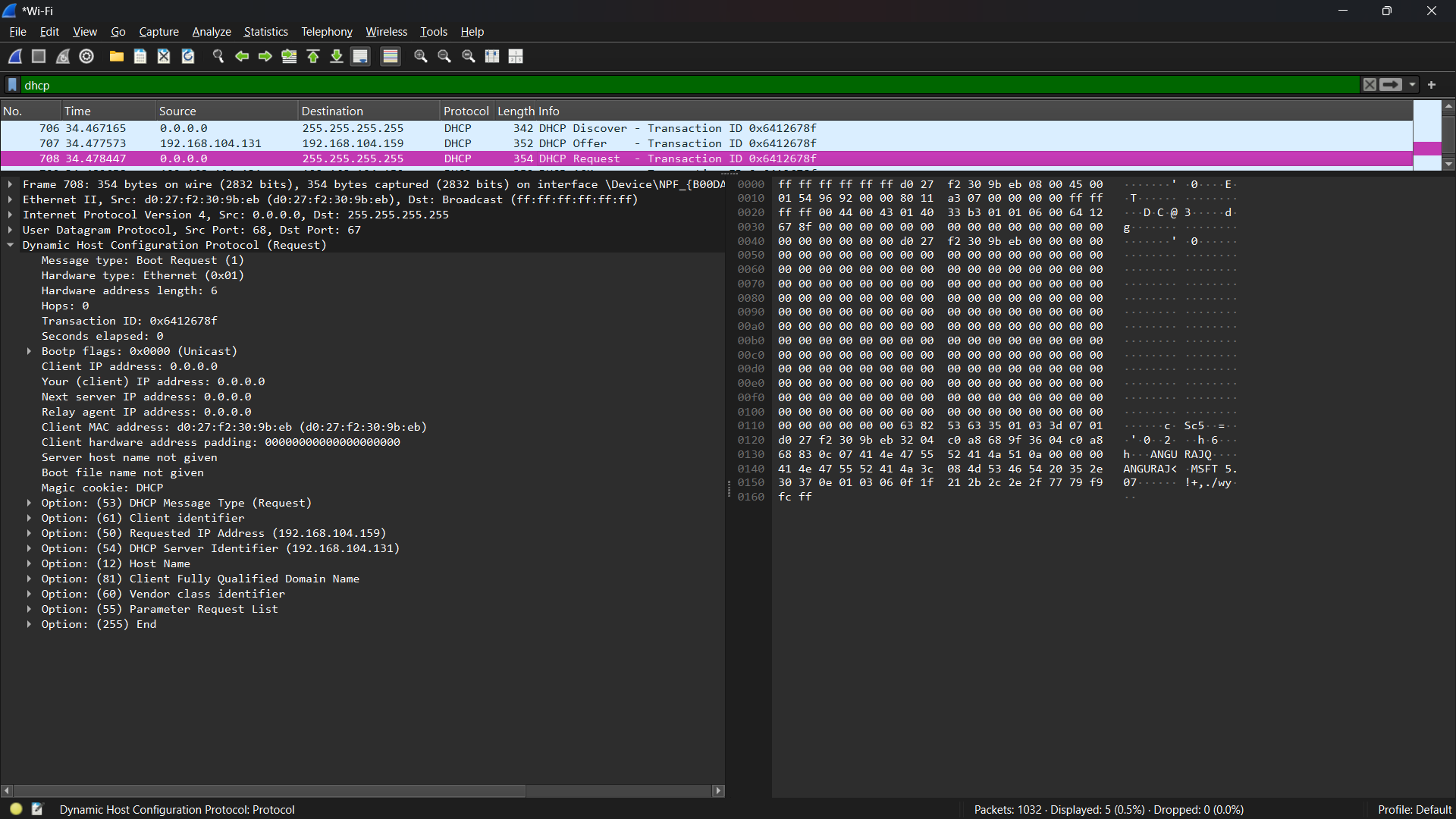
DORA Process in DHCP : Discover



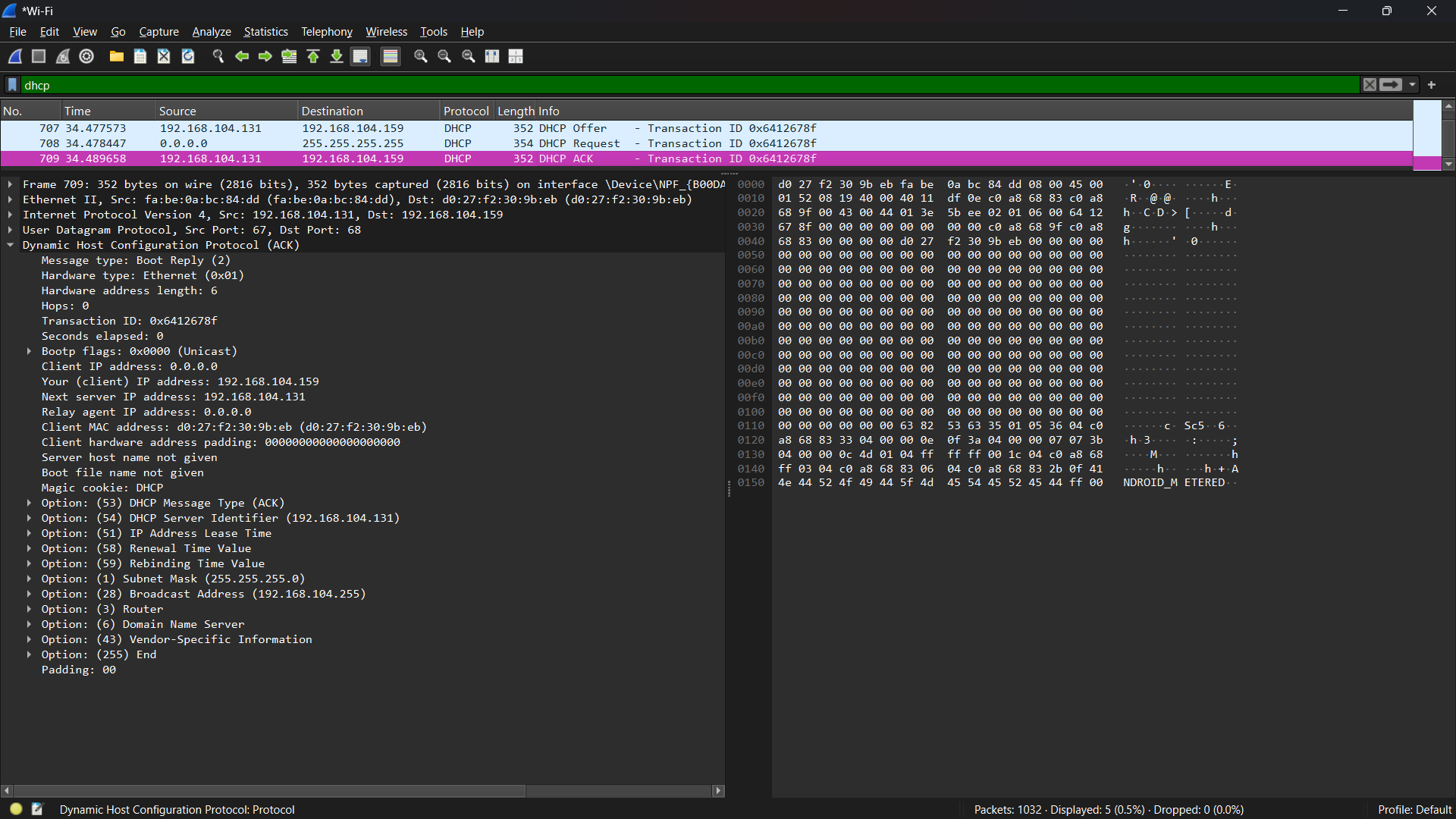
Offer :



Request :



Acknowledgement :



**Q5.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.**

**IP Address Range**: 192.168.1.0/24 – Class C

**Default Subnet Mask**: 255.255.255.0 for Class C

11111111. 11111111**.** 11111111.00000000

**Total Available Hosts**: 2^8 - 2 = 254 (since /24 means 8 bits for host IDs)

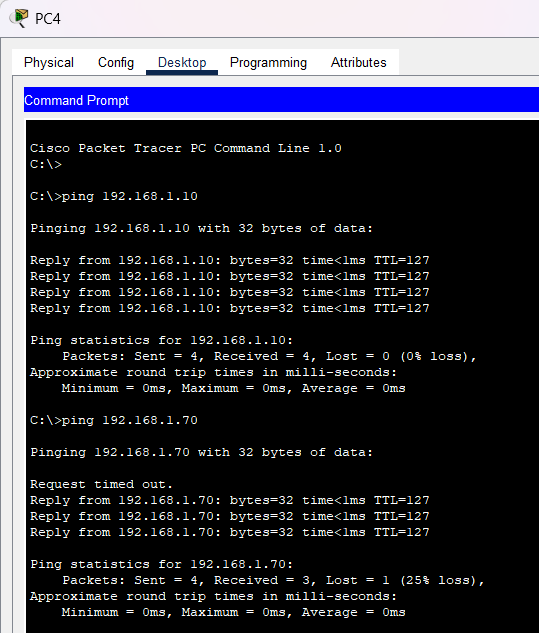
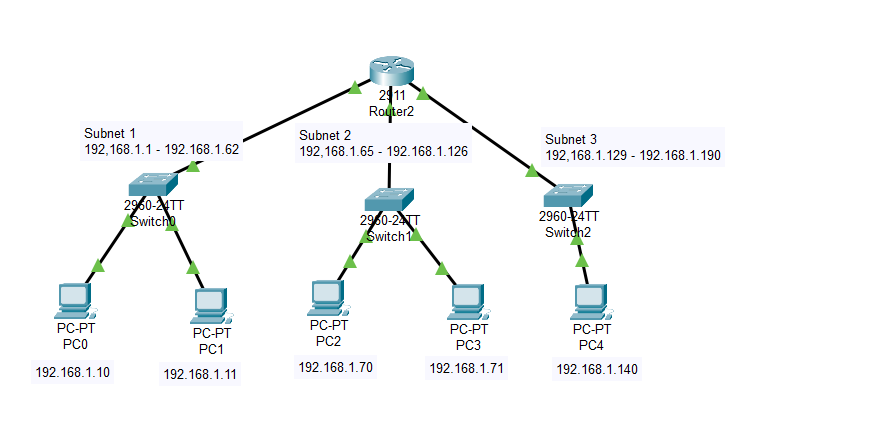
To divide 192.168.1.0/24 into **4 subnets**, we need to borrow **2 bits** from the **host portion**:

| **Before Subnetting** | **After Subnetting** |
| --- | --- |
| /24 → 255.255.255.0 | /26 → 255.255.255.192 |
| Hosts per subnet: 254 | Hosts per subnet: 2^6 - 2 = 62  111110 – 6 bits |

**New Subnet** 11111111. 11111111. 11111111.11000000 – 255.255.255.192 or /26

**New Subnets and Address Ranges**

| **Subnet** | **Network Address** | **First Usable IP** | **Last Usable IP** | **Broadcast Address** |
| --- | --- | --- | --- | --- |
| **Subnet 1** | 192.168.1.0/26 | 192.168.1.1 | 192.168.1.62 | 192.168.1.63 |
| **Subnet 2** | 192.168.1.64/26 | 192.168.1.65 | 192.168.1.126 | 192.168.1.127 |
| **Subnet 3** | 192.168.1.128/26 | 192.168.1.129 | 192.168.1.190 | 192.168.1.191 |
| **Subnet 4** | 192.168.1.192/26 | 192.168.1.193 | 192.168.1.254 | 192.168.1.255 |



**Q6.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.**

| **Class** | **First Octet Range** | **Default Subnet Mask** | **IP Address Range** |
| --- | --- | --- | --- |
| Class A | 1 - 126 | 255.0.0.0 (/8) | 1.0.0.0 - 126.255.255.255 |
| Class B | 128 - 191 | 255.255.0.0 (/16) | 128.0.0.0 - 191.255.255.255 |
| Class C | 192 - 223 | 255.255.255.0 (/24) | 192.0.0.0 - 223.255.255.255 |
| Class D (Multicast) | 224 - 239 | N/A | 224.0.0.0 - 239.255.255.255 |
| Class E (Experimental) | 240 - 255 | N/A | 240.0.0.0 - 255.255.255.255 |

**10.1.1.1 → Class A** (Default Subnet Mask: 255.0.0.0)

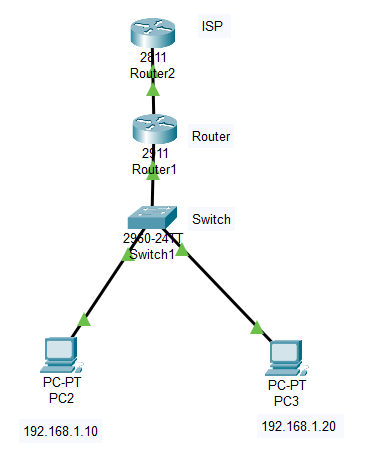
**172.16.5.10 → Class B** (Default Subnet Mask: 255.255.0.0)

**192.168.1.5 → Class C** (Default Subnet Mask: 255.255.255.0)

**Q7. 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?

**1. Network Setup**

**Devices Required**

* **Router0 (LAN Router)**
* **Router1 (ISP Router)**
* **Switch0**
* **PC0 and PC1**

**Connections**

* **Router0 (Gig0/0) → Switch0**
* **PC0 & PC1 → Switch0**
* **Router0 (Gig0/1) → Router1 (Gig0/0) (WAN link)**

**2. IP Configuration**

**PC0 & PC1 (Static IPs)**

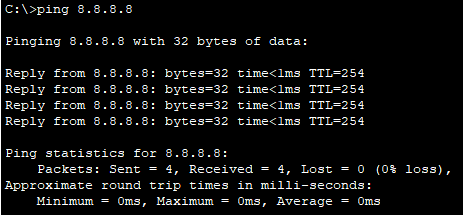
* **PC0: 192.168.1.10/24, Gateway: 192.168.1.1**
* **PC1: 192.168.1.20/24, Gateway: 192.168.1.1**

**interface Loopback0**

**ip address 8.8.8.8 255.255.255.255**

**exit**

**ip route 0.0.0.0 0.0.0.0 200.200.200.1**

****

**3. Configure NAT on Router0**

**access-list 1 permit 192.168.1.0 0.0.0.255**

**ip nat inside source list 1 interface GigabitEthernet0/1 overload**

**interface GigabitEthernet0/0**

**ip nat inside**

**exit**

**4. Testing Connectivity**

**Verify NAT Translations**

**show ip nat translations**

| **Protocol** | **Inside Local** | **Inside Global** | **Outside Local** | **Outside Global** |
| --- | --- | --- | --- | --- |
| **ICMP** | **192.168.1.10:1** | **200.200.200.1:1** | **8.8.8.8:1** | **8.8.8.8:1** |

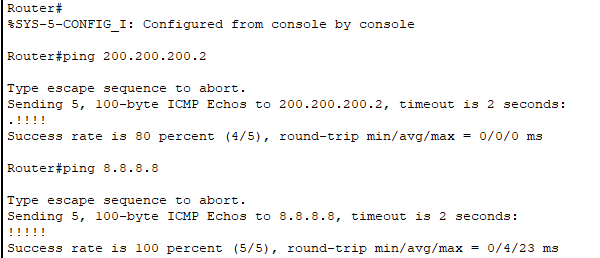
**Ping from PC0 to External IP**

**ping 8.8.8.8**

****

**5. Capture and Analyze Traffic**

1. **Start packet capture on Router0 (Gig0/1).**
2. **Ping 8.8.8.8 from PC0.**
3. **Analyze source IP change before and after NAT:**
   * **Before NAT: 192.168.1.10 → 8.8.8.8**
   * **After NAT: 200.200.200.1 → 8.8.8.8**

****