**Module 6 - questions - Layer 03**   
  
**1) Capture and analyze ARP packets using Wireshark. Inspect the ARP request and reply frames when your device attempts to find the router's MAC address.**

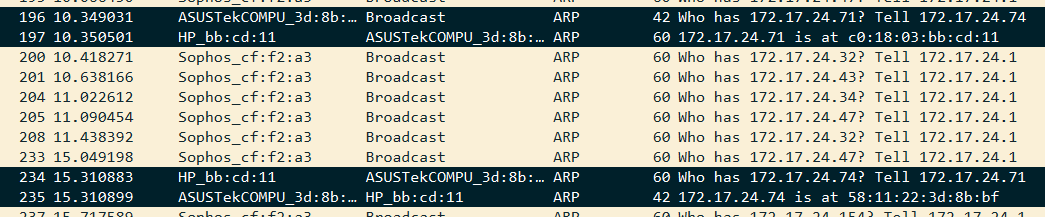
**Discuss the importance of ARP in packet forwarding.**

**Address Resolution Protocol (ARP)** is essential for packet forwarding in IPv4 networks because it maps **IP addresses to MAC addresses**, allowing communication between devices on a local network.

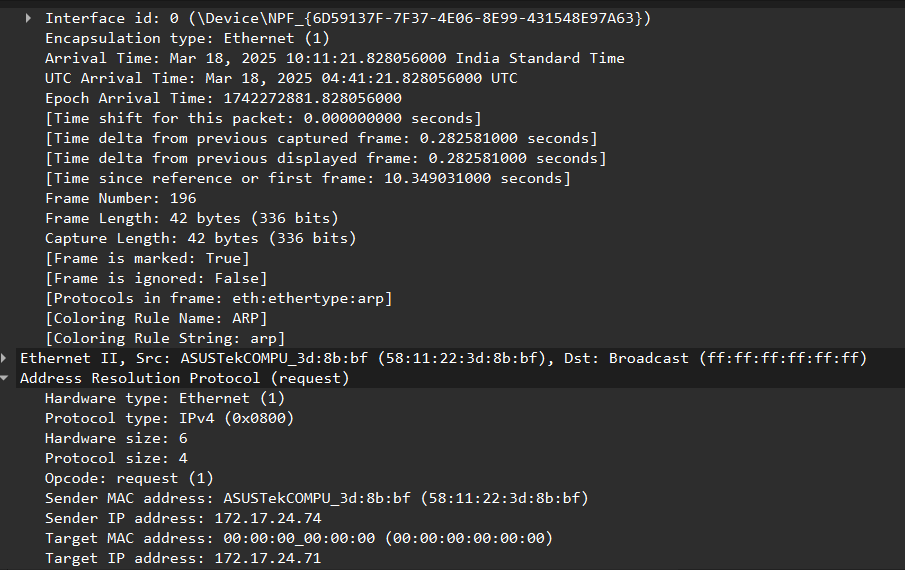
#### **Role of ARP in Packet Forwarding:**

1. **IP-to-MAC Address Resolution:**
   * When a device wants to send a packet, it knows the destination **IP address** but needs the corresponding **MAC address** for local delivery.
   * ARP helps resolve this by sending an **ARP request** and receiving an **ARP reply**.
2. **Ensures Local Network Communication:**
   * ARP is necessary for devices to communicate within a **subnet**, as data link layer (Layer 2) transmission requires MAC addresses.
3. **Facilitates Routing to Other Networks:**
   * If the destination is outside the subnet, the packet is sent to the **default gateway (router)**.
   * The router's MAC address is resolved using ARP to ensure correct forwarding.
4. **Optimizes Network Performance:**
   * ARP cache stores recently resolved addresses, reducing network overhead and latency.

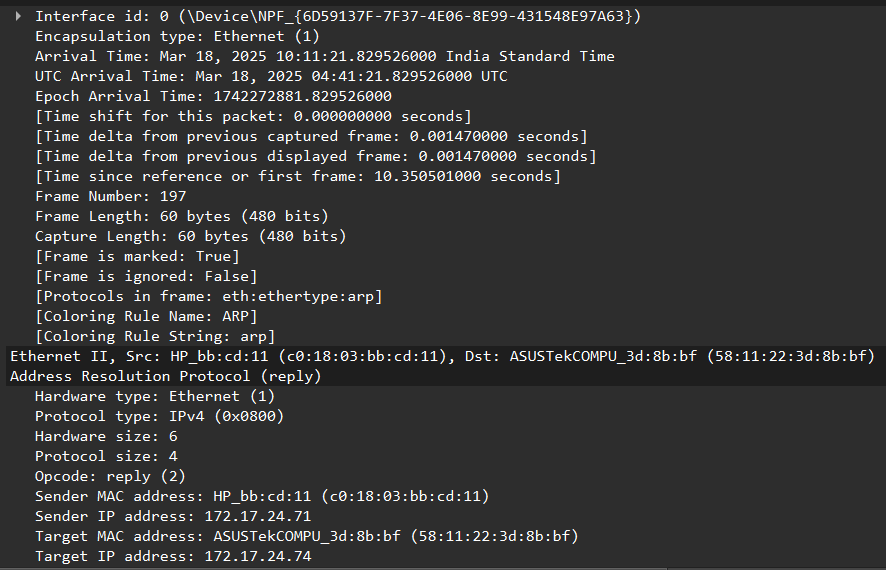
**Network packets in Wireshark**



**Request packet**

****

**Reply packet**



**2) Manually configure static routes on a router to direct packets to different subnets.**

**Use the ip route command and verify connectivity using ping and traceroute.**

**Check Existing Routes** Open Command Prompt as Administrator and run:  
route print

**Add a Static Route to a Specific Subnet**  
route add 192.168.2.0 mask 255.255.255.0 192.168.1.1 metric 1

* 192.168.2.0: Destination subnet.
* 255.255.255.0: Subnet mask.
* 192.168.1.1: Next-hop router.
* metric 1: Priority of the route (lower is preferred).

**Verify the Newly Added Route**  
route print

**Test Connectivity Using ping**  
ping 192.168.2.1

* Ensures the destination subnet is reachable.

**Trace the Route Using tracert**  
tracert 192.168.2.1

* Displays the hops taken to reach the destination.

Terminal Output:

C:\Windows\System32>route print

===========================================================================

Interface List

13...58 11 22 3d 8b bf ......Realtek PCIe GbE Family Controller

21...b6 8c 9d 8e 1e a5 ......Microsoft Wi-Fi Direct Virtual Adapter

8...b6 8c 9d 8e 1e b5 ......Microsoft Wi-Fi Direct Virtual Adapter #2

18...94 78 e4 3f 6b cc ......MediaTek Wi-Fi 6 MT7921 Wireless LAN Card

1...........................Software Loopback Interface 1

23...00 15 5d 42 2b 53 ......Hyper-V Virtual Ethernet Adapter

===========================================================================

IPv4 Route Table

===========================================================================

Active Routes:

Network Destination Netmask Gateway Interface Metric

0.0.0.0 0.0.0.0 192.168.104.131 192.168.104.102 50

127.0.0.0 255.0.0.0 On-link 127.0.0.1 331

127.0.0.1 255.255.255.255 On-link 127.0.0.1 331

127.255.255.255 255.255.255.255 On-link 127.0.0.1 331

172.18.176.0 255.255.240.0 On-link 172.18.176.1 5256

172.18.176.1 255.255.255.255 On-link 172.18.176.1 5256

172.18.191.255 255.255.255.255 On-link 172.18.176.1 5256

192.168.104.0 255.255.255.0 On-link 192.168.104.102 306

192.168.104.102 255.255.255.255 On-link 192.168.104.102 306

192.168.104.255 255.255.255.255 On-link 192.168.104.102 306

224.0.0.0 240.0.0.0 On-link 127.0.0.1 331

224.0.0.0 240.0.0.0 On-link 172.18.176.1 5256

224.0.0.0 240.0.0.0 On-link 192.168.104.102 306

255.255.255.255 255.255.255.255 On-link 127.0.0.1 331

255.255.255.255 255.255.255.255 On-link 172.18.176.1 5256

255.255.255.255 255.255.255.255 On-link 192.168.104.102 306

===========================================================================

Persistent Routes:

Network Address Netmask Gateway Address Metric

0.0.0.0 0.0.0.0 172.17.24.1 Default

===========================================================================

IPv6 Route Table

===========================================================================

Active Routes:

If Metric Network Destination Gateway

18 66 ::/0 fe80::83f:5ff:feff:2e16

1 331 ::1/128 On-link

18 66 2409:40f4:1014:7b60::/64 On-link

18 306 2409:40f4:1014:7b60:40c7:e111:b0bc:b855/128

On-link

18 306 2409:40f4:1014:7b60:c8d2:d784:f44f:77eb/128

On-link

23 5256 fe80::/64 On-link

18 306 fe80::/64 On-link

18 306 fe80::50a0:c6f4:5c54:f44d/128

On-link

23 5256 fe80::bea1:39d:bccc:1c75/128

On-link

1 331 ff00::/8 On-link

23 5256 ff00::/8 On-link

18 306 ff00::/8 On-link

===========================================================================

Persistent Routes:

None

C:\Windows\System32>route add 192.168.2.0 mask 255.255.255.0 192.168.1.1 metric 1

OK!

C:\Windows\System32>route print

===========================================================================

Interface List

13...58 11 22 3d 8b bf ......Realtek PCIe GbE Family Controller

21...b6 8c 9d 8e 1e a5 ......Microsoft Wi-Fi Direct Virtual Adapter

8...b6 8c 9d 8e 1e b5 ......Microsoft Wi-Fi Direct Virtual Adapter #2

18...94 78 e4 3f 6b cc ......MediaTek Wi-Fi 6 MT7921 Wireless LAN Card

1...........................Software Loopback Interface 1

23...00 15 5d 42 2b 53 ......Hyper-V Virtual Ethernet Adapter

===========================================================================

IPv4 Route Table

===========================================================================

Active Routes:

Network Destination Netmask Gateway Interface Metric

0.0.0.0 0.0.0.0 192.168.104.131 192.168.104.102 50

127.0.0.0 255.0.0.0 On-link 127.0.0.1 331

127.0.0.1 255.255.255.255 On-link 127.0.0.1 331

127.255.255.255 255.255.255.255 On-link 127.0.0.1 331

172.18.176.0 255.255.240.0 On-link 172.18.176.1 5256

172.18.176.1 255.255.255.255 On-link 172.18.176.1 5256

172.18.191.255 255.255.255.255 On-link 172.18.176.1 5256

192.168.2.0 255.255.255.0 192.168.1.1 192.168.104.102 51

192.168.104.0 255.255.255.0 On-link 192.168.104.102 306

192.168.104.102 255.255.255.255 On-link 192.168.104.102 306

192.168.104.255 255.255.255.255 On-link 192.168.104.102 306

224.0.0.0 240.0.0.0 On-link 127.0.0.1 331

224.0.0.0 240.0.0.0 On-link 172.18.176.1 5256

224.0.0.0 240.0.0.0 On-link 192.168.104.102 306

255.255.255.255 255.255.255.255 On-link 127.0.0.1 331

255.255.255.255 255.255.255.255 On-link 172.18.176.1 5256

255.255.255.255 255.255.255.255 On-link 192.168.104.102 306

===========================================================================

Persistent Routes:

Network Address Netmask Gateway Address Metric

0.0.0.0 0.0.0.0 172.17.24.1 Default

===========================================================================

IPv6 Route Table

===========================================================================

Active Routes:

If Metric Network Destination Gateway

18 66 ::/0 fe80::83f:5ff:feff:2e16

1 331 ::1/128 On-link

18 66 2409:40f4:1014:7b60::/64 On-link

18 306 2409:40f4:1014:7b60:40c7:e111:b0bc:b855/128

On-link

18 306 2409:40f4:1014:7b60:c8d2:d784:f44f:77eb/128

On-link

23 5256 fe80::/64 On-link

18 306 fe80::/64 On-link

18 306 fe80::50a0:c6f4:5c54:f44d/128

On-link

23 5256 fe80::bea1:39d:bccc:1c75/128

On-link

1 331 ff00::/8 On-link

23 5256 ff00::/8 On-link

18 306 ff00::/8 On-link

===========================================================================

Persistent Routes:

None

C:\Windows\System32>route -p add 192.168.2.0 mask 255.255.255.0 192.168.1.1 metric 1

OK!

C:\Windows\System32>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 192.168.2.1:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\System32>tracert 192.168.2.1

Tracing route to 192.168.2.1 over a maximum of 30 hops

1 2 ms 2 ms 2 ms 192.168.104.131

2 \* \* \* Request timed out.

3 \* \* \* Request timed out.

4 \* \* \* Request timed out.

5 42 ms 23 ms 22 ms ^C

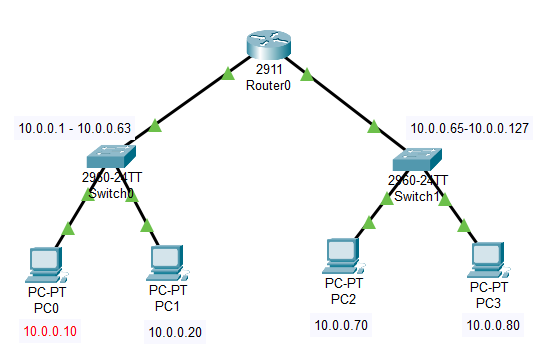
**3).Given a network address of 10.0.0.0/24, divide it into 4 equal subnets.**

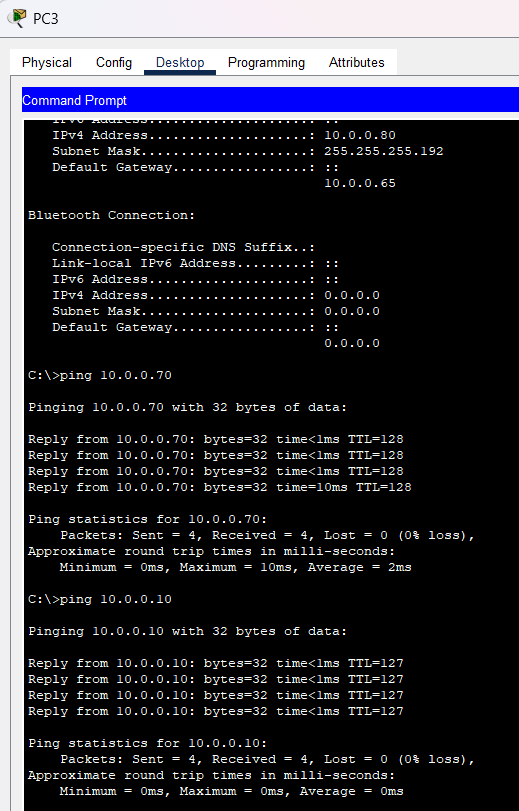
**Calculate the new subnet mask.**

**Determine the valid host range for each subnet.**

* Given network: 10.0.0.0/24
* /24 means **255.255.255.0**, providing **256** IP addresses (0-255).
* To divide into **4 equal subnets**, we need **2 extra bits** for subnetting:
  + New subnet mask = **/26** → **255.255.255.192**
  + Each subnet has **64** IPs (including network & broadcast).

| **Subnet** | **Network Address** | **First Host** | **Last Host** | **Broadcast Address** |
| --- | --- | --- | --- | --- |
| 1 | 10.0.0.0/26 | 10.0.0.1 | 10.0.0.62 | 10.0.0.63 |
| 2 | 10.0.0.64/26 | 10.0.0.65 | 10.0.0.126 | 10.0.0.127 |
| 3 | 10.0.0.128/26 | 10.0.0.129 | 10.0.0.190 | 10.0.0.191 |
| 4 | 10.0.0.192/26 | 10.0.0.193 | 10.0.0.254 | 10.0.0.255 |



Pinged from 10.0.0.80 to device in same subnet (10.0.0.70) and device in different subnet(10.0.0.10)   
  


**4).You are given three IP addresses: 192.168.10.5, 172.20.15.1, and 8.8.8.8.**

**Identify the class of each IP address.**

**Determine if it is private or public.**

**Explain how NAT would handle a private IP when accessing the internet.**

### **Identifying IP Classes and Private/Public Status**

| **IP Address** | **Class** | **Private/Public** | **Private IP Range (If Applicable)** |
| --- | --- | --- | --- |
| 192.168.10.5 | **Class C** | **Private** | 192.168.0.0 – 192.168.255.255 |
| 172.20.15.1 | **Class B** | **Private** | 172.16.0.0 – 172.31.255.255 |
| 8.8.8.8 | **Class A** | **Public** | Not in private range (Google DNS) |

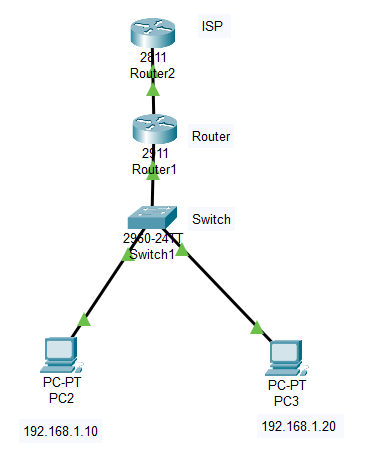
**How NAT Handles Private IP Addresses for Internet Access**

1. **Private IPs Cannot Directly Access the Internet**
   * Private IPs (like 192.168.x.x, 172.16.x.x - 172.31.x.x, and 10.x.x.x) are **not routable** over the internet.
   * They require **Network Address Translation (NAT)** to communicate with public servers.
2. **Role of NAT (Network Address Translation)**
   * NAT translates private IP addresses to a **public IP address** assigned by the ISP.
   * The router maintains a **NAT table** mapping private IPs to their assigned public IP.
   * When a response from the internet arrives, NAT forwards it to the corresponding private IP.
3. **Types of NAT**
   * **Static NAT** – Maps a private IP to a fixed public IP.
   * **Dynamic NAT** – Uses a pool of public IPs and assigns one dynamically.
   * **PAT (Port Address Translation)** – Multiple private IPs share a single public IP, distinguished by port numbers.
4. **Example of NAT in Action**
   * **Source IP before NAT:** 192.168.10.5 → Internet
   * **Router translates it:** 192.168.10.5 → 203.0.113.1 (public IP)
   * **Response from server (e.g., Google DNS 8.8.8.8) returns to 203.0.113.1.**
   * **Router forwards it back to 192.168.10.5 using NAT table mapping.**

**5).In Cisco Packet Tracer, configure NAT on a router to allow internal devices (192.168.1.x) to access the internet.**

**Test connectivity by pinging an external public IP.**

**Capture the traffic in Wireshark and analyze the source IP before and after NAT translation.**

**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)**

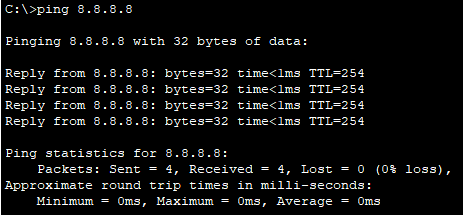
* **PC0: 192.168.1.10/24, Gateway: 192.168.1.1**
* **PC1: 192.168.1.20/24, Gateway: 192.168.1.1**

**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** |

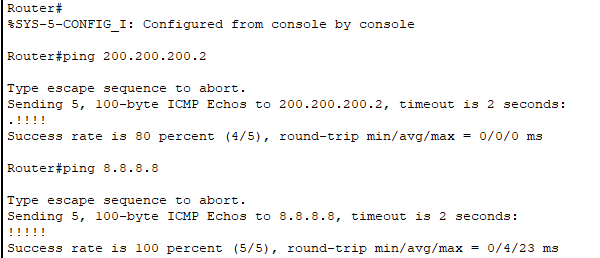
**Ping from PC0 to External IP**

**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**

****