

Q1. 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.

```
Command Prompt

Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::5684:b125:9f2:3f3e%10
IPv4 Address. . . . . : 192.168.224.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : 
IPv6 Address. . . . . : 2401:4900:67a5:7997:2f83:add8:7543:4e41
Temporary IPv6 Address. . . . . : 2401:4900:67a5:7997:7080:43d2:1a42:72a4
Link-local IPv6 Address . . . . . : fe80::c6d3:c85d:d9bd:d131%3
IPv4 Address. . . . . : 192.168.195.162
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::8092:3bff:fe97:e4e6%3
                             192.168.195.37

C:\Users\brindha>ping 192.168.195.37

Pinging 192.168.195.37 with 32 bytes of data:
Reply from 192.168.195.37: bytes=32 time=10ms TTL=64
Reply from 192.168.195.37: bytes=32 time=4ms TTL=64
Reply from 192.168.195.37: bytes=32 time=5ms TTL=64
Reply from 192.168.195.37: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.195.37:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 10ms, Average = 5ms
```

Wireshark Analysis

The image shows a Wireshark packet capture analysis of ARP traffic. The packet list on the left shows several ARP requests and replies between 192.168.195.162 and 192.168.195.37. The selected packet (No. 60) is an ARP request from 82:92:3b:97:e4:e6 to 82:92:3b:97:e4:e6. The packet details pane shows the Ethernet II header and the ARP request structure. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
60	20.848106	82:92:3b:97:e4:e6	AzureWaveTec_9b:22:92	ARP	42	Who has 192.168.195.162? Tell 192.168.195.37
61	20.848159	AzureWaveTec_9b:22:92	82:92:3b:97:e4:e6	ARP	42	192.168.195.162 is at cc:47:40:9b:22:92
147	43.682406	82:92:3b:97:e4:e6	AzureWaveTec_9b:22:92	ARP	42	Who has 192.168.195.162? Tell 192.168.195.37
148	43.682455	AzureWaveTec_9b:22:92	82:92:3b:97:e4:e6	ARP	42	192.168.195.162 is at cc:47:40:9b:22:92
307	95.394275	82:92:3b:97:e4:e6	AzureWaveTec_9b:22:92	ARP	42	Who has 192.168.195.162? Tell 192.168.195.37
308	95.394352	AzureWaveTec_9b:22:92	82:92:3b:97:e4:e6	ARP	42	192.168.195.162 is at cc:47:40:9b:22:92
354	117.790007	82:92:3b:97:e4:e6	AzureWaveTec_9b:22:92	ARP	42	Who has 192.168.195.162? Tell 192.168.195.37

Wireshark - Packet 60 - Wi-Fi

Frame 60: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{03EF3B24-15EB-4AC0-BFD3-9400B0EA8DEB}, id 0

Section number: 1

Interface id: 0 (\Device\NPF_{03EF3B24-15EB-4AC0-BFD3-9400B0EA8DEB})

Encapsulation type: Ethernet (1)

Arrival Time: Mar 14, 2025 18:54:29.715602000 India Standard Time

UTC Arrival Time: Mar 14, 2025 13:24:29.715602000 UTC

Epoch Arrival Time: 1741958669.715602000

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 4.089573000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 20.848106000 seconds]

Frame Number: 60

Frame Length: 42 bytes (336 bits)

Capture Length: 42 bytes (336 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:arp]

[Coloring Rule Name: ARP]

[Coloring Rule String: arp]

Ethernet II, Src: 82:92:3b:97:e4:e6 (82:92:3b:97:e4:e6), Dst: AzureWaveTec_9b:22:92 (cc:47:40:9b:22:92)

Destination: AzureWaveTec_9b:22:92 (cc:47:40:9b:22:92)

Source: 82:92:3b:97:e4:e6 (82:92:3b:97:e4:e6)

Type: ARP (0x0806)

[Stream index: 0]

Address Resolution Protocol (request)

0000 cc 47 40 9b 22 92 82 92 3b 97 e4 e6 08 06 00 01 -GG-.....

0010 08 00 06 04 00 01 82 92 3b 97 e4 e6 c0 a8 c3 25 -.....%..%

ARP Request

Source MAC Address: 82:92:3b:97:e4:e6

Destination MAC Address: cc:47:40:9b:22:92

Protocol: ARP (0x0806)

ARP Reply

Source MAC Address: cc:47:40:9b:22:92

Destination MAC Address: 82:92:3b:97:e4:e6

Packet forwarding

This ARP exchange allows a device to find out the MAC address linked to an IP address before sending any data.

192.168.195.37 is the default gateway, then the system now knows how to send packets outside the local network.

This process is essential for packet forwarding, as without knowing the MAC address, the device wouldn't be able to communicate.

Packet forwarding ensures data reaches the right device