Lab5 - Ethernet and ARP

Jiaxi Zhang

May 7, 2025

1 HTTP GET Packet

The below four questions are based on the HTTP GET packet captured by Wireshark and the screenshot is a printout of the packet.

1.1 The 48-bit Ethernet address of my computer

c6:19:77:e6:6b:1a

1.2 The 48-bit Ethernet address of the destination

00:00:5e:00:01:32. And this is not the MAC address of gaia.cs.umass.edu. It is a Virtual Router Redundancy Protocol address, which is used by my local router, and then forwards the request to gaia.

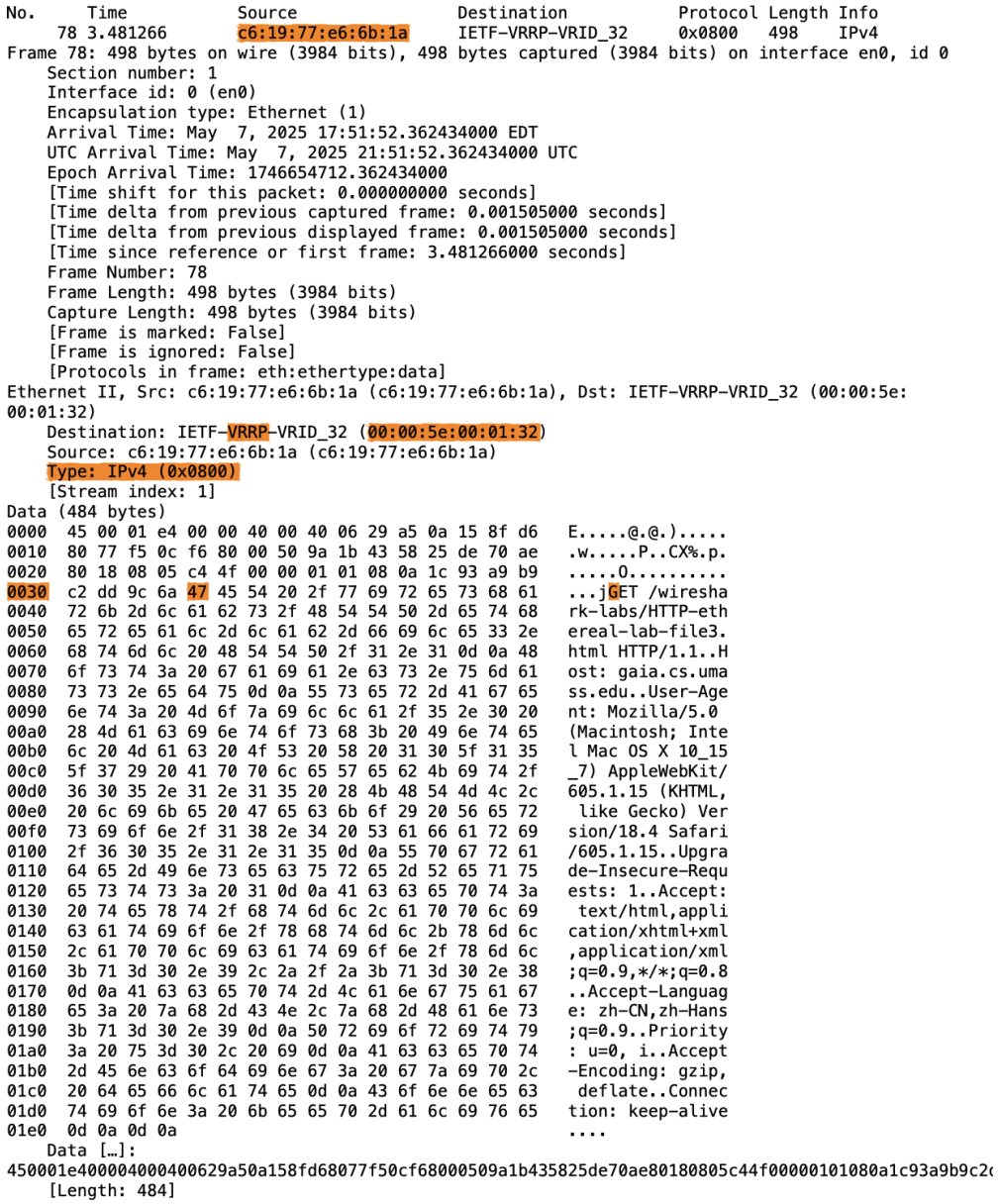

Figure 1: Question1-4 Screenshot

1.3 Hexadecimal value for the two-byte Frame type field

0x0800. It indicates that the upper-layer protocol is IPv4.

1.4 Byte Number

The 'G' is the 53th byte from the very start of the Ethernet frame. We can find from the screenshot that for each line, there are 16 bytes, and the line for 'G' appears starts from '0030', which is the 48th byte. In the

ASCII code, 'G' is 0x47, and we can find it in the 53rd byte with an offset of 52.

2 HTTP 200 OK Packet

The below four questions are based on the HTTP 200 OK packet captured by Wireshark and the screenshot is a printout of the packet.

```
No.     Time           Source                Destination           Protocol Length Info
    116 3.498177       Cisco_c4:c7:82        c6:19:77:e6:6b:1a     0x0800   1354   IPv4
Frame 116: 1354 bytes on wire (10832 bits), 1354 bytes captured (10832 bits) on interface en0, id
0
    Section number: 1
    Interface id: 0 (en0)
    Encapsulation type: Ethernet (1)
    Arrival Time: May  7, 2025 17:51:52.379345000 EDT
    UTC Arrival Time: May  7, 2025 21:51:52.379345000 UTC
    Epoch Arrival Time: 1746654712.379345000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.001746000 seconds]
    [Time delta from previous displayed frame: 0.001746000 seconds]
    [Time since reference or first frame: 3.498177000 seconds]
    Frame Number: 116
    Frame Length: 1354 bytes (10832 bits)
    Capture Length: 1354 bytes (10832 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:data]
Ethernet II, Src: Cisco_c4:c7:82 (f0:4a:02:c4:c7:82), Dst: c6:19:77:e6:6b:1a (c6:19:77:e6:6b:1a)
    Destination: c6:19:77:e6:6b:1a (c6:19:77:e6:6b:1a)
    Source: Cisco_c4:c7:82 (f0:4a:02:c4:c7:82)
    Type: IPv4 (0x0800)
    [Stream index: 0]
Data (1340 bytes)
0000  45 00 05 3c ec 3b 40 00 26 06 54 11 80 77 f5 0c   E..<.;@.&.T..w..
0010  0a 15 8f d6 00 50 f6 80 25 de 70 ae 9a 1b 45 08   .....P..%.p...E.
0020  80 10 00 eb 85 0b 00 00 01 01 08 0a c2 dd 9c 94   ................
0030  1c 93 a9 b9 48 54 54 50 2f 31 2e 31 20 32 30 30   ....HTTP/1.1 200
0040  20 4f 4b 0d 0a 44 61 74 65 3a 20 57 65 64 2c 20    OK..Date: Wed,
0050  30 37 20 4d 61 79 20 32 30 32 35 20 32 31 3a 35   07 May 2025 21:5
0060  31 3a 35 32 20 47 4d 54 0d 0a 53 65 72 76 65 72   1:52 GMT..Server
0070  3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 20 28   : Apache/2.4.6 (
0080  43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 4c 2f   CentOS) OpenSSL/
0090  31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 50 2f   1.0.2k-fips PHP/
```

Figure 2: Question5-8 Screenshot

2.1 The 48-bit Ethernet address of source

f0:4a:02:c4:c7:82. It is neither the MAC address of gaia.cs.umass.edu nor my computer. But rather the default gateway or router (Cisco device in this situation) that forwarded the response from gaia.cs.umass.edu.

2.2 The 48-bit Ethernet address of destination

c6:19:77:e6:6b:1a. It is the MAC address of my computer.

2.3 Hexadecimal value for the two-byte Frame type field

0x0800. It indicates that the upper-layer protocol is IPv4.

2.4 Byte Number

The 'O' is the 66th byte from the very start of the Ethernet frame. We can find from the screenshot that for each line, there are 16 bytes, and the line for 'O' appears starts from '0040', which is the 64th byte. In the ASCII code, 'O' is 0x4F, and we can find it in the 66th byte with an offset of 65.

3 ARP cache

3.1 Contents of ARP Cache

Below is the output of the `arp -a` command on my computer, which displays the current contents of the ARP cache:

```
arp -a

1536-gw.net.nyu.edu (10.21.128.1) at 0:0:5e:0:1:32 on en0 ifscope [ethernet]
10-21-143-214.dynapool.wireless.nyu.edu (10.21.143.214) at c6:19:77:e6:6b:1a on en0
    ifscope permanent [ethernet]
1536-bcast.net.nyu.edu (10.21.255.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (169.254.169.254) at f0:4a:2:c4:b9:c2 on en0 [ethernet]
mdns.mcast.net (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
```

Meaning of Each Column

- **Hostname**: If resolvable, this is the DNS name associated with the IP address (eg `1536-gw.net.nyu.edu`).
- **IP Address**: The IP address for which the ARP entry maps a MAC address(eg. `10.21.128.1`)
- **MAC Address**: The Ethernet hardware address (e.g., `00:00:5e:0:1:32`).

- **Interface**: The network interface through which the ARP entry applies (in this case, `en0`).
- **Flags**: Includes whether the entry is dynamically learned or permanent, and the link layer type, which is typically `[ethernet]`.

4 Observe ARP In Action

I tried http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-lab-file3.html which is instructed in the lab manual. However, even though with all the caches cleared, I still cannot observe the ARP packets in the Wireshark capture. So I choose to use the given file in the lab manual for the following questions.

4.1 Request

```
No.     Time           Source                Destination           Protocol Length Info
      1 0.000000       AmbitMicrosy_a9:3d:68 Broadcast             ARP      42     Who has
192.168.1.1? Tell 192.168.1.105
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 28, 2004 13:19:20.157130000 EDT
    UTC Arrival Time: Aug 28, 2004 17:19:20.157130000 UTC
    Epoch Arrival Time: 1093713560.157130000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    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: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the
factory default)
        .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
    Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    [Stream index: 0]
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
    Sender IP address: 192.168.1.105
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.1
```

Figure 3: Question5-8 Screenshot

4.2 Hexadecimal values for the source and destination addresses

In the first ARP packet containing ARP Request, Source MAC: 00:d0:59:a9:3d:68, and Destination MAC: ff:ff:ff:ff:ff:ff

4.3 Frame type field and upper-layer protocol

Type: 0x0806, Upper-layer protocol: ARP

4.3.1 How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

According to the RFC 826, the ARP opcode field is located at byte 21 in the ARP packet because there are 14 bytes of Ethernet header and 6 bytes of ARP header before the opcode field.

4.3.2 the value of the opcode field

The value of the opcode field is 1. We can find in the screenshot that "Opcode: request (1)"

4.3.3 whether containing the sender's IP address

Yes, it contains the sender's IP address. We can find in the screenshot that "Sender IP address: 192.168.1.105"

4.3.4 Where in the ARP request does the "question" appear?

The "question" appears in the "Target MAC address" field. Since the sender does not know the MAC address of the target, it is set to 00:00:00:00:00:00.

4.4 Response

```
No.     Time           Source                Destination           Protocol Length Info
      2 0.001018       LinksysGroup_da:af:73 AmbitMicrosy_a9:3d:68 ARP      60     192.168.1.1 is
at 00:06:25:da:af:73
Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 28, 2004 13:19:20.158148000 EDT
    UTC Arrival Time: Aug 28, 2004 17:19:20.158148000 UTC
    Epoch Arrival Time: 1093713560.158148000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.001018000 seconds]
    [Time delta from previous displayed frame: 0.001018000 seconds]
    [Time since reference or first frame: 0.001018000 seconds]
    Frame Number: 2
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 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: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: AmbitMicrosy_a9:3d:68
(00:d0:59:a9:3d:68)
```

```
    Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    [Stream index: 1]
    Padding: 000000000000000000000000000000000000
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: LinksysGroup_da:af:73 (00:06:25:da:af:73)
    Sender IP address: 192.168.1.1
    Target MAC address: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
    Target IP address: 192.168.1.105
```

Figure 4: Question5-8 Screenshot

4.4.1 How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

According to the RFC 826, the ARP opcode field is located at byte 21 in the ARP packet. The same as the ARP request.

4.4.2 the value of the opcode field

The value of the opcode field is 2. We can find in the screenshot that "Opcode: reply (2)"

4.4.3 Where in the ARP message does the “answer” to the earlier ARP request appear?

The ”answer” appears in the ”Sender MAC address” field and ”Sender IP address” field. Sender MAC address: LinksysGroup_da:af:73 (00:06:25:da:af:73) Sender IP address: 192.168.1.1

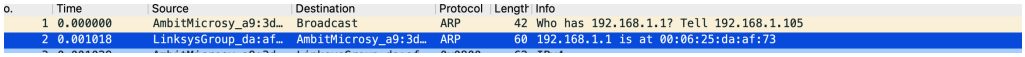

Figure 5: Question5-8 Screenshot

4.5 Hexadecimal values for the source and destination addresses

Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68) Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)

4.6 The reason for not getting the ARP response

There is no ARP reply to the request in packet 6 because the host with IP address 192.168.1.117 might be either not active on the network at the time, or was configured not to respond to ARP requests.

5 Extra Credit

5.1

If I entered the correct IP address, but the wrong Ethernet address for that remote interface when manually adding an entry, the ARP cache would not be able to resolve the IP address to the correct MAC address. It will be successful in adding the entry to the ARP cache, but the entry will not be useful for communication and the target host will not be reachable.