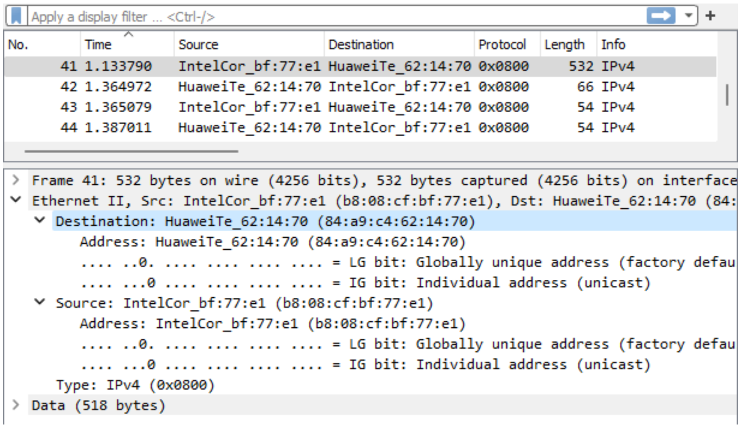
ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC & KỸ THUẬT MÁY TÍNH

**MẠNG MÁY TÍNH (CO3094)**

# Báo cáo Lab 6: Wireshark Lab – Ethernet and ARP

| | |
|---|---|
| Giảng viên: | Nguyễn Tấn Đạt |
| SV thực hiện: | Đinh Như Tân – 1915040 |

Tp. Hồ Chí Minh, Tháng 10/2021



```
Apply a display filter ... <Ctrl-/>
No.   Time       Source              Destination         Protocol  Length  Info
   41 1.133790   IntelCor_bf:77:e1   HuaweiTe_62:14:70   0x0800       532  IPv4
   42 1.364972   HuaweiTe_62:14:70   IntelCor_bf:77:e1   0x0800        66  IPv4
   43 1.365079   IntelCor_bf:77:e1   HuaweiTe_62:14:70   0x0800        54  IPv4
   44 1.387011   HuaweiTe_62:14:70   IntelCor_bf:77:e1   0x0800        54  IPv4
```

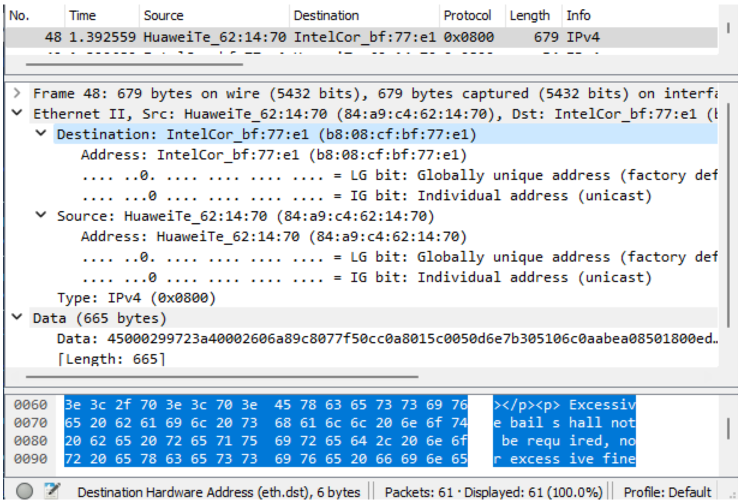
```
> Frame 41: 532 bytes on wire (4256 bits), 532 bytes captured (4256 bits) on interface
v Ethernet II, Src: IntelCor_bf:77:e1 (b8:08:cf:bf:77:e1), Dst: HuaweiTe_62:14:70 (84:
  v Destination: HuaweiTe_62:14:70 (84:a9:c4:62:14:70)
      Address: HuaweiTe_62:14:70 (84:a9:c4:62:14:70)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory defau
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: IntelCor_bf:77:e1 (b8:08:cf:bf:77:e1)
      Address: IntelCor_bf:77:e1 (b8:08:cf:bf:77:e1)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory defau
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Data (518 bytes)
```

1. What is the 48-bit Ethernet address of your computer?
   *The Ethernet address of my computer is b8:08:cf:bf:77:e1*

2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]
   *The destination address 84:a9:c4:62:14:70 is not the Ethernet address of gaia.cs.umass.edu. It is the address of my HuaweiTe router, which is the link used to get off the subnet.*

3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
   *The hex value for the Frame type field is 0x0800. This corresponds to the IP protocol (the frame type filed indicates that the nest layer above IP – the layer to which the payload of ths Ethernet frame will be passed – is IP*

4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?
   *The ASCII "G" appears 52 bytes from the start of the Ethernet frame. There are 14 B Ethernet frame, and then 20 bytes of IP header followed by 20 bytes of TCP header before the HTTP data is encountered.*
   *Here is a screenshot of the Ethernet frame containing the HTTP OK response:*



```
No.   Time       Source              Destination         Protocol  Length  Info
   48 1.392559   HuaweiTe_62:14:70   IntelCor_bf:77:e1   0x0800       679  IPv4
```

```
> Frame 48: 679 bytes on wire (5432 bits), 679 bytes captured (5432 bits) on interfa
v Ethernet II, Src: HuaweiTe_62:14:70 (84:a9:c4:62:14:70), Dst: IntelCor_bf:77:e1 (b
  v Destination: IntelCor_bf:77:e1 (b8:08:cf:bf:77:e1)
      Address: IntelCor_bf:77:e1 (b8:08:cf:bf:77:e1)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory def
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: HuaweiTe_62:14:70 (84:a9:c4:62:14:70)
      Address: HuaweiTe_62:14:70 (84:a9:c4:62:14:70)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory def
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
v Data (665 bytes)
    Data: 45000299723a40002606a89c8077f50cc0a8015c0050d6e7b305106c0aabea08501800ed…
    [Length: 665]
```

```
0060  3e 3c 2f 70 3e 3c 70 3e  45 78 63 65 73 73 69 76   ></p><p> Excessiv
0070  65 20 62 61 69 6c 20 73  68 61 6c 6c 20 6e 6f 74   e bail s hall not
0080  20 62 65 20 72 65 71 75  69 72 65 64 2c 20 6e 6f    be requ ired, no
0090  72 20 65 78 63 65 73 73  69 76 65 20 66 69 6e 65   r excess ive fine
```

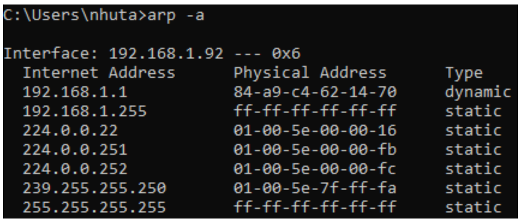
Destination Hardware Address (eth.dst), 6 bytes
Packets: 61 · Displayed: 61 (100.0%)
Profile: Default

5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?
   *The source address 84:a9:c4:62:14:70 is neither the Ethernet address of gaia.cs.umass.edu nor the address of my computer. It is the address of my HuaweiTe router, which is the link used to get onto my subnet.*

6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?
   *The destination address b8:08:cf:bf:77:e1 is the address of my computer*

7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
   *The hex value for the Frame type field is 0x0800. This value corresponds to the IP protocol (see also answer to 3. above)*

8. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" (i.e., the HTTP response code) appear in the Ethernet frame?
   *The ASCII "O" appears 52 bytes from the start of the Ethernet frame. Again, there are 14 bytes of Ethernet frame, and then 20 bytes of IP header followed by 20 bytes of TCP header before the HTTP data is encountered.*

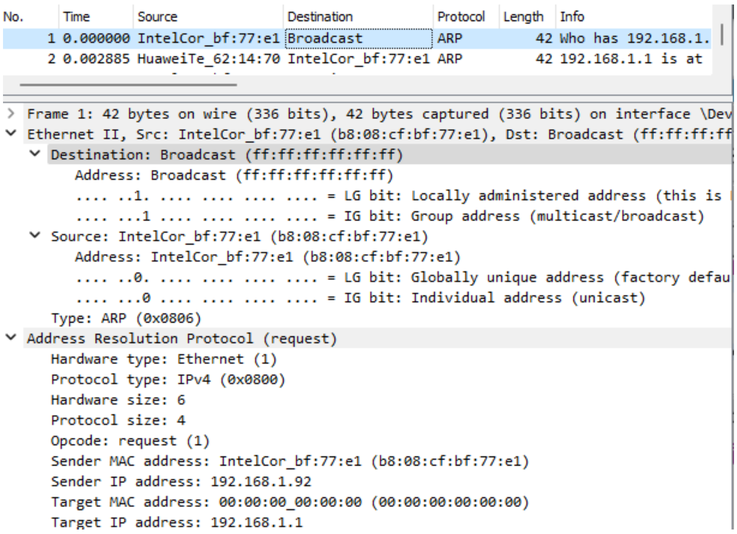


```
C:\Users\nhuta>arp -a

Interface: 192.168.1.92 --- 0x6
  Internet Address      Physical Address      Type
  192.168.1.1           84-a9-c4-62-14-70     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

9. Write down the contents of your computer's ARP cache. What is the meaning of each column value?
   *The Internet Address column contains the IP address, the Physical Address column contains the MAC address, and the type indicates the protocol type.*

   *Here is a screenshot showing the ARP request message:*



```
No.   Time     Source              Destination         Protocol Length Info
    1 0.000000 IntelCor_bf:77:e1   Broadcast           ARP          42 Who has 192.168.1.
    2 0.002885 HuaweiTe_62:14:70   IntelCor_bf:77:e1   ARP          42 192.168.1.1 is at

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Dev
v Ethernet II, Src: IntelCor_bf:77:e1 (b8:08:cf:bf:77:e1), Dst: Broadcast (ff:ff:ff:ff
  v Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: IntelCor_bf:77:e1 (b8:08:cf:bf:77:e1)
      Address: IntelCor_bf:77:e1 (b8:08:cf:bf:77:e1)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory defau
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_bf:77:e1 (b8:08:cf:bf:77:e1)
    Sender IP address: 192.168.1.92
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.1
```

10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?
    *The hex value for the source address is b8:08:cf:bf:77:e1. The hex value for the destination address is ff:ff:ff:ff:ff:ff, the broadcast address.*

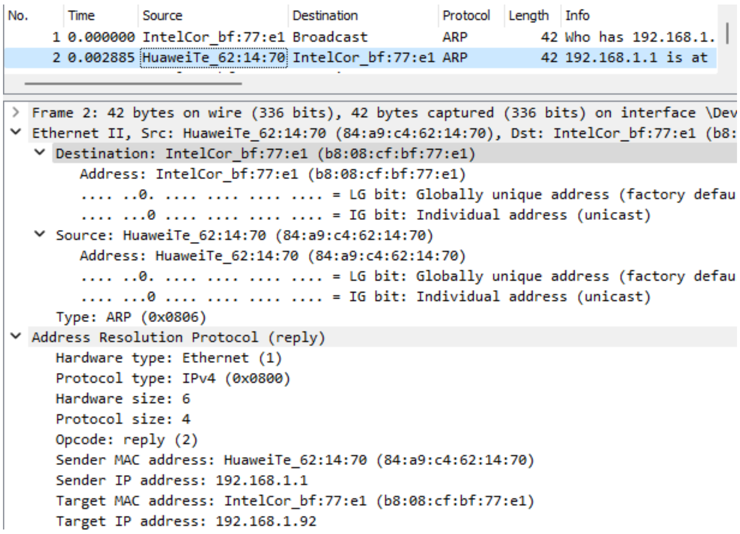
11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?
    *The hex value for the Ethernet Frame type field is 0x0806, for ARP.*

12. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin? What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which

an ARP request is made? Does the ARP message contain the IP address of the sender? Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?

- *The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.*
- *The hex value for opcode field withing the ARP-payload of the request is 0x0001, for request*
- *Yes, the ARP message containing the IP address 192.168.1.92 for the sender.*
- *The field "Target MAC address" is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address (192.168.1.1) is being queried.*

*Here is the screenshot for the ARP reply message:*



```
No.   Time       Source              Destination         Protocol  Length  Info
    1 0.000000   IntelCor_bf:77:e1   Broadcast           ARP           42  Who has 192.168.1.
    2 0.002885   HuaweiTe_62:14:70   IntelCor_bf:77:e1   ARP           42  192.168.1.1 is at

> Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Dev
v Ethernet II, Src: HuaweiTe_62:14:70 (84:a9:c4:62:14:70), Dst: IntelCor_bf:77:e1 (b8:
  v Destination: IntelCor_bf:77:e1 (b8:08:cf:bf:77:e1)
      Address: IntelCor_bf:77:e1 (b8:08:cf:bf:77:e1)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory defau
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: HuaweiTe_62:14:70 (84:a9:c4:62:14:70)
      Address: HuaweiTe_62:14:70 (84:a9:c4:62:14:70)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory defau
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: HuaweiTe_62:14:70 (84:a9:c4:62:14:70)
    Sender IP address: 192.168.1.1
    Target MAC address: IntelCor_bf:77:e1 (b8:08:cf:bf:77:e1)
    Target IP address: 192.168.1.92
```

13. Now find the ARP reply that was sent in response to the ARP request. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin? What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made? Where in the ARP message does the "answer" to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

    - *The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.*
    - *The hex value for opcode field withing the ARP-payload of the request is 0x0002, for reply.*
    - *The answer to the earlier ARP request appears in the"Sender MAC address" field, which contains the Ethernet address 84:a9:c4:62:14:70 for the sender with IP address 192.168.1.1.*

14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?
    *The hex value for the source address is 84:a9:c4:62:14:70 and for the destination is b8:08:cf:bf:77:e1.*

15. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?
    *There is no reply in this trace, because we are not at the machine that sent the request. The ARP request is broadcast, but the ARP reply is sent back directly to the sender's Ethernet address.*