Computer Networks 1

Lab 6

Wireshark Lab: Ethernet and ARP v8.0

Student Name: **Nguyễn Quý Hải**

Student No.: **2052974**

I. Objectives

In this lab, we'll investigate the Ethernet protocol and the ARP protocol

II. Content

1. Capturing and analyzing Ethernet frames

- Q1: What is the 48-bit Ethernet address of your computer?

  Answer: It is a4:97:b1:e3:90:0b

- Q2. 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.]

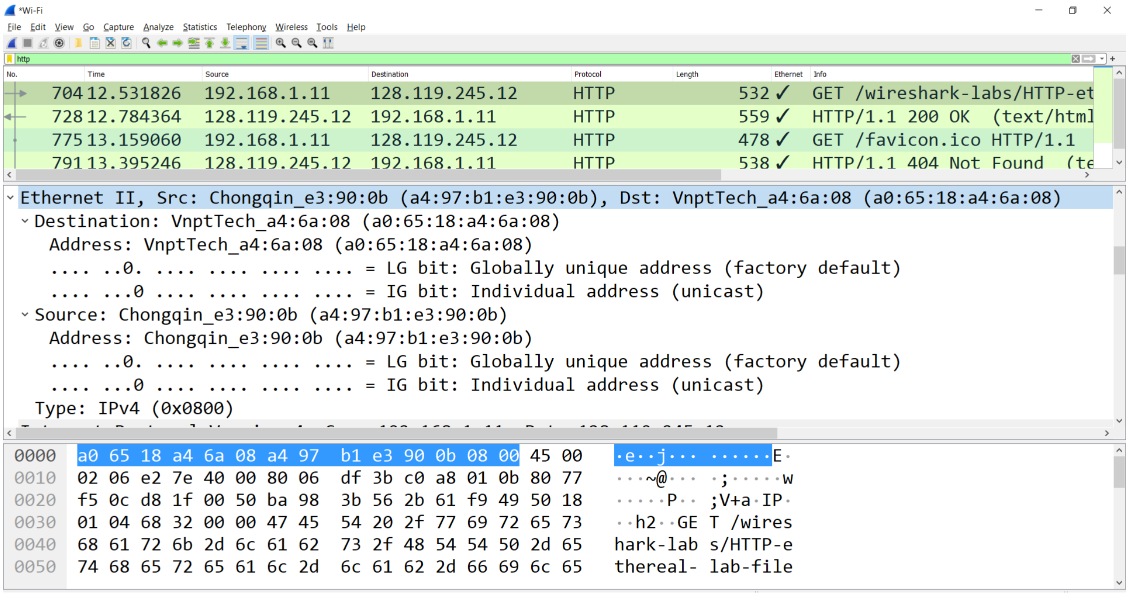
  Answer: It is a0:65:18:a4:6a:08 and it is not the Ethernet address of gaia.cs.umass.edu. It is just a address of router name VnptTech

- Q3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

  Answer: Type: IPv4 (0x0800). This corresponds to Internet protocol.

- Q4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?

  Answer: It is 52 bytes


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

No.	Time	Source	Destination	Protocol	Length	Ethernet	Info
704	12.531826	192.168.1.11	128.119.245.12	HTTP	532	✓	GET /wireshark-labs/HTTP-et
728	12.784364	128.119.245.12	192.168.1.11	HTTP	559	✓	HTTP/1.1 200 OK (text/html
775	13.159060	192.168.1.11	128.119.245.12	HTTP	478	✓	GET /favicon.ico HTTP/1.1
791	13.395246	128.119.245.12	192.168.1.11	HTTP	538	✓	HTTP/1.1 404 Not Found (te

```
˅ Ethernet II, Src: Chongqin_e3:90:0b (a4:97:b1:e3:90:0b), Dst: VnptTech_a4:6a:08 (a0:65:18:a4:6a:08)
  ˅ Destination: VnptTech_a4:6a:08 (a0:65:18:a4:6a:08)
      Address: VnptTech_a4:6a:08 (a0:65:18:a4:6a:08)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ˅ Source: Chongqin_e3:90:0b (a4:97:b1:e3:90:0b)
      Address: Chongqin_e3:90:0b (a4:97:b1:e3:90:0b)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

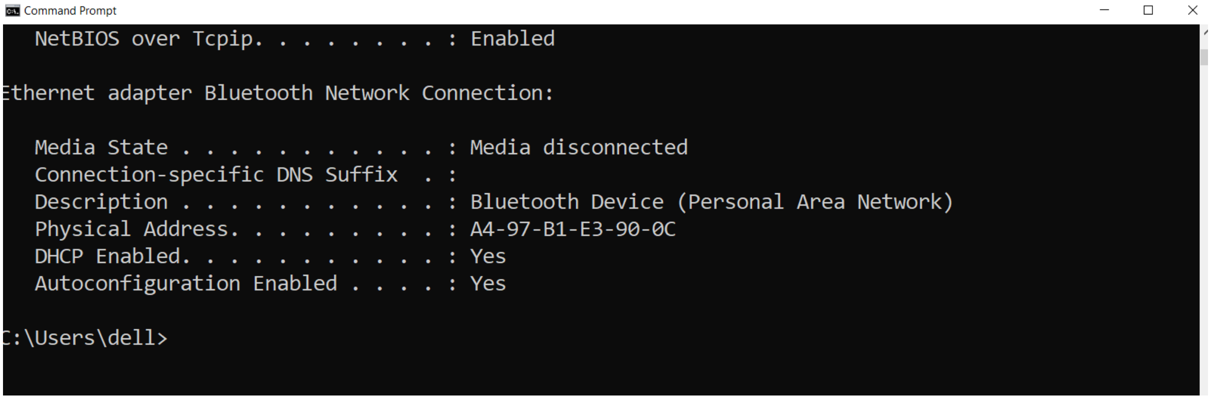
```
0000  a0 65 18 a4 6a 08 a4 97  b1 e3 90 0b 08 00 45 00   ·e··j··· ······E·
0010  02 06 e2 7e 40 00 80 06  df 3b c0 a8 01 0b 80 77   ···~@··· ·;·····w
0020  f5 0c d8 1f 00 50 ba 98  3b 56 2b 61 f9 49 50 18   ·····P·· ;V+a·IP·
0030  01 04 68 32 00 00 47 45  54 20 2f 77 69 72 65 73   ··h2··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 65   hark-lab s/HTTP-e
0050  74 68 65 72 65 61 6c 2d  6c 61 62 2d 66 69 6c 65   thereal- lab-file
```

- Q5: 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?

  <u>Answer</u>: It is a0:65:18:a4:6a:08, it is not the address of my computer or of gaia.cs.umass.edu. The name of the device has this as its Ethernet address is VnptTech router

- Q6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

  <u>Answer</u>: It is <u>a4:97:b1:e3:90:0b</u>**.** It is address of my computer



```
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : A4-97-B1-E3-90-0C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

C:\Users\dell>
```

- Q7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

  <u>Answer</u>: the hex value of this field is 0x0800. It corresponds to the IP protocol.

- Q8. How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appears in the Ethernet frame?

  <u>Answer</u>: It is 52 bytes

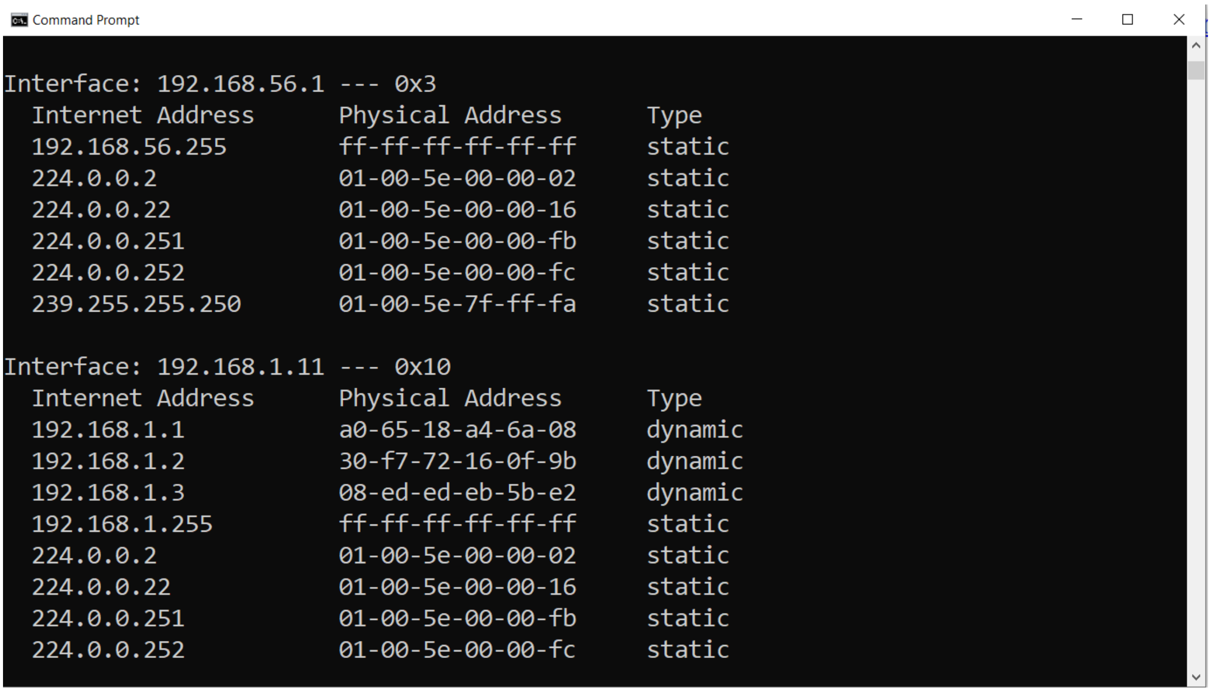
2. The Address Resolution Protocol

ARP Caching

- Q9: Write down the contents of your computer’s ARP cache. What is the meaning of each column value?

Answer:

● Internet Address:	IP address
● Physical Address:	The MAC address
● Type:	The protocol type



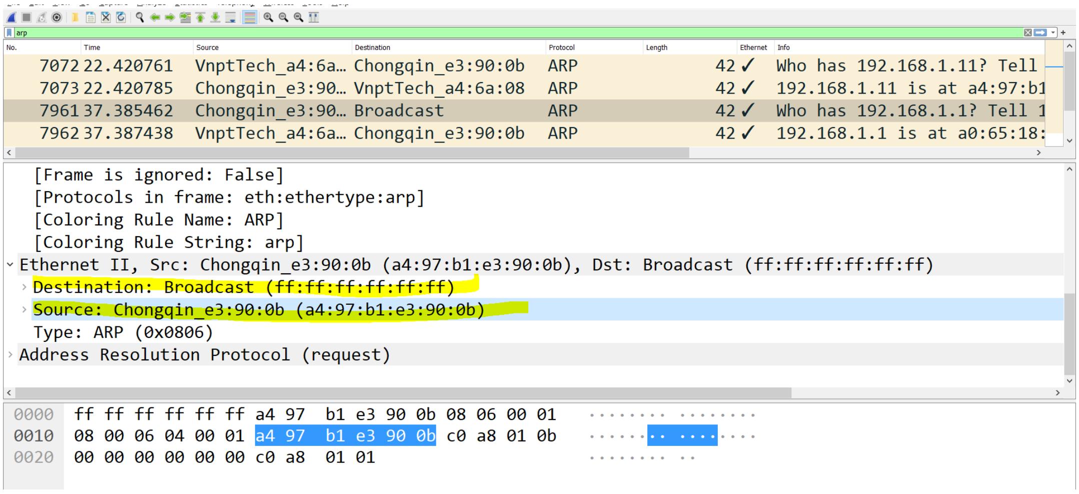
```
Interface: 192.168.56.1 --- 0x3
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.1.11 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           a0-65-18-a4-6a-08     dynamic
  192.168.1.2           30-f7-72-16-0f-9b     dynamic
  192.168.1.3           08-ed-ed-eb-5b-e2     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     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
```

Observing ARP in action

- Q10: . What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

Answer: Ethernet II, Src: Chongqin_e3:90:0b (a4:97:b1:e3:90:0b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)



arp

```
No.   Time       Source             Destination          Protocol  Length  Ethernet  Info
7072 22.420761   VnptTech_a4:6a…   Chongqin_e3:90:0b    ARP           42 ✓  Who has 192.168.1.11? Tell
7073 22.420785   Chongqin_e3:90…   VnptTech_a4:6a:08    ARP           42 ✓  192.168.1.11 is at a4:97:b1
7961 37.385462   Chongqin_e3:90…   Broadcast            ARP           42 ✓  Who has 192.168.1.1? Tell 1
7962 37.387438   VnptTech_a4:6a…   Chongqin_e3:90:0b    ARP           42 ✓  192.168.1.1 is at a0:65:18:
```

```
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
  Ethernet II, Src: Chongqin_e3:90:0b (a4:97:b1:e3:90:0b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: Chongqin_e3:90:0b (a4:97:b1:e3:90:0b)
    Type: ARP (0x0806)
  Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff a4 97  b1 e3 90 0b 08 06 00 01   ········ ········
0010  08 00 06 04 00 01 a4 97  b1 e3 90 0b c0 a8 01 0b   ········ ········
0020  00 00 00 00 00 00 c0 a8  01 01                     ········ ··
```

- Q11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

  Answer: The hex value for the two byte Ethernet frame is ARP (0x0806), the corresponding upper layer protocol is ARP.

- Q12. Download the ARP specification from ftp://ftp.rfc-editor.org/in-notes/std/std37.txt. A readable, detailed discussion of ARP is also at http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.

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

    Answer: 10 bytes (6 bytes hardware + 4 bytes protocol)

  - b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

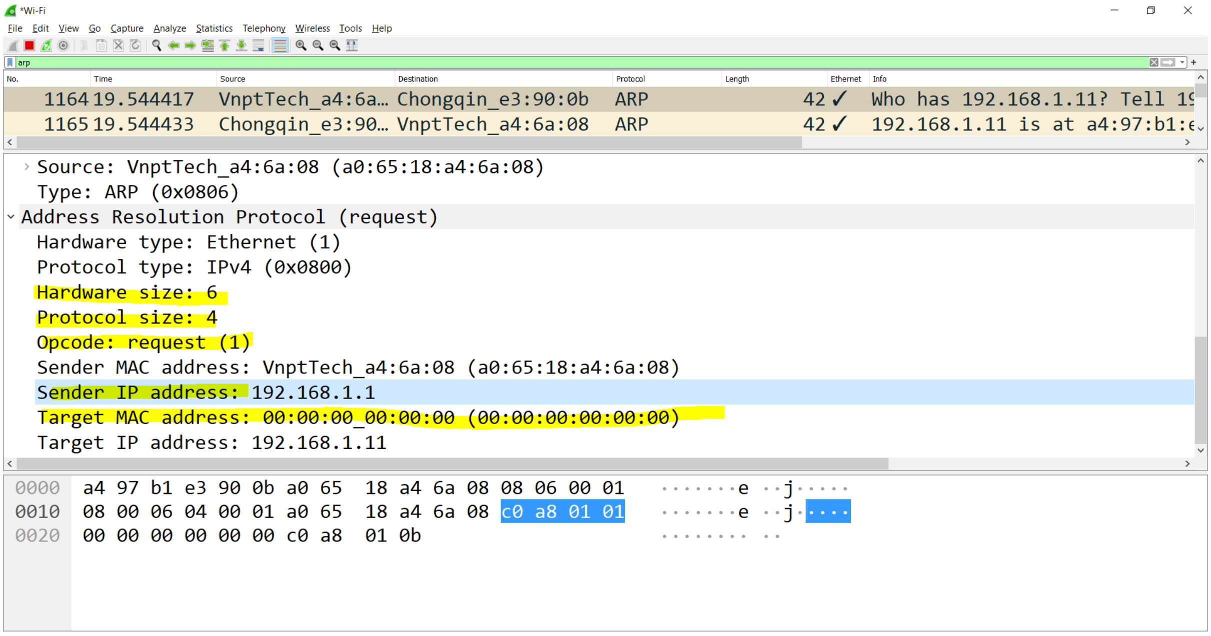
    Answer: It is 1 (request)

  - c) Does the ARP message contain the IP address of the sender?

    Answer: Yes, it is 192.168.1.1

  - d) Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?

    Answer: 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.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

```
No.   Time       Source              Destination         Protocol  Length  Ethernet  Info
1164 19.544417   VnptTech_a4:6a…  Chongqin_e3:90:0b   ARP                  42 ✓    Who has 192.168.1.11? Tell 19
1165 19.544433   Chongqin_e3:90…  VnptTech_a4:6a:08   ARP                  42 ✓    192.168.1.11 is at a4:97:b1:e
```

```
  › Source: VnptTech_a4:6a:08 (a0:65:18:a4:6a:08)
    Type: ARP (0x0806)
˅ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: VnptTech_a4:6a:08 (a0:65:18:a4:6a:08)
    Sender IP address: 192.168.1.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.11
```

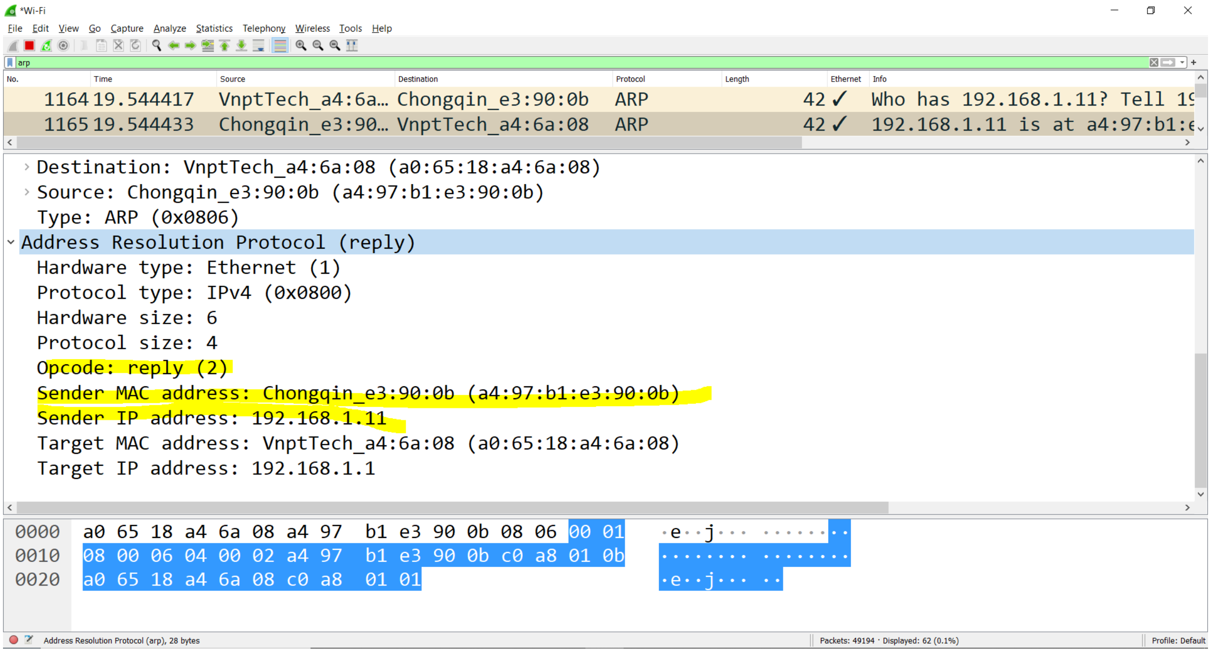
```
0000  a4 97 b1 e3 90 0b a0 65  18 a4 6a 08 08 06 00 01   ·······e ··j·····
0010  08 00 06 04 00 01 a0 65  18 a4 6a 08 c0 a8 01 01   ·······e ··j·····
0020  00 00 00 00 00 00 c0 a8  01 0b                     ········ ··
```

- Q13. Now find the ARP reply that was sent in response to the ARP request.
    - a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

      Answer: It is 20 bytes
    - b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

      Answer: 2 (reply)
    - c) 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?

      Answer: Sender IP address: 192.168.1.11 and Sender MAC address: a4:97:b1:e3:90:0b does the “answer” to the earlier ARP request


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

No.	Time	Source	Destination	Protocol	Length	Ethernet	Info
1164	19.544417	VnptTech_a4:6a…	Chongqin_e3:90:0b	ARP	42	✓	Who has 192.168.1.11? Tell 19
1165	19.544433	Chongqin_e3:90…	VnptTech_a4:6a:08	ARP	42	✓	192.168.1.11 is at a4:97:b1:e

```
  › Destination: VnptTech_a4:6a:08 (a0:65:18:a4:6a:08)
  › Source: Chongqin_e3:90:0b (a4:97:b1:e3:90:0b)
    Type: ARP (0x0806)
⌄ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Chongqin_e3:90:0b (a4:97:b1:e3:90:0b)
    Sender IP address: 192.168.1.11
    Target MAC address: VnptTech_a4:6a:08 (a0:65:18:a4:6a:08)
    Target IP address: 192.168.1.1
```

```
0000  a0 65 18 a4 6a 08 a4 97  b1 e3 90 0b 08 06 00 01   ·e··j··· ········
0010  08 00 06 04 00 02 a4 97  b1 e3 90 0b c0 a8 01 0b   ········ ········
0020  a0 65 18 a4 6a 08 c0 a8  01 01                     ·e··j··· ··
```

Address Resolution Protocol (arp), 28 bytes | Packets: 49194 · Displayed: 62 (0.1%) | Profile: Default

- Q14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

  Answer: Source: a4:97:b1;e3:90:0b Destination: a0:65:18:a4:6a:08

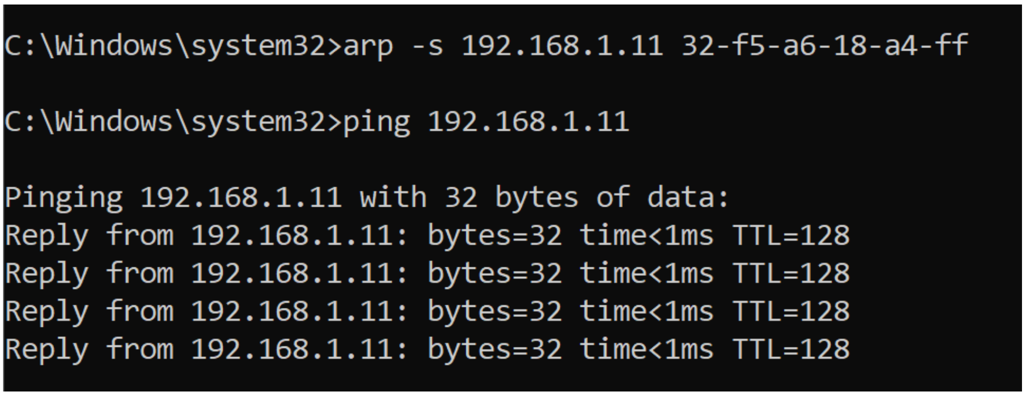
- Q15. Open the ethernet-ethereal-trace-1 trace file in http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But there is yet another computer on this network, as indicated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?

  Answer: Because the ARP request is broadcast, but the ARP reply is not broadcast. The reply will be sent to the computer who made the request directly.

3. Extra Credit

- EX-1. The arp command: arp -s InetAddr EtherAddr allows you to manually add an entry to the ARP cache that resolves the IP address InetAddr to the physical address EtherAddr. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for that remote interface?

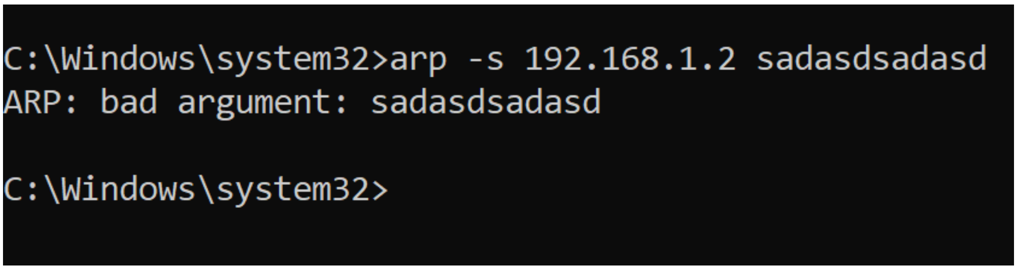
  Answer: I don't see any problems in this case even though I've tried to change the static and dynamic one. Ping requests still happen normally. Just 1 thing we need to consider: Be careful of bad arguments. It will block the assign.



```
C:\Windows\system32>arp -s 192.168.1.11 32-f5-a6-18-a4-ff

C:\Windows\system32>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
```



```
C:\Windows\system32>arp -s 192.168.1.2 sadasdsadasd
ARP: bad argument: sadasdsadasd

C:\Windows\system32>
```

- EX-2. What is the default amount of time that an entry remains in your ARP cache before being removed. You can determine this empirically (by monitoring the cache contents) or by looking this up in your operation system documentation. Indicate how/where you determined this value.

  Answer: There is no clear answer for this question. Some sources said the default amount of time is 4 hours and other references showed that it is 6 hours. But in general, we can configure it!