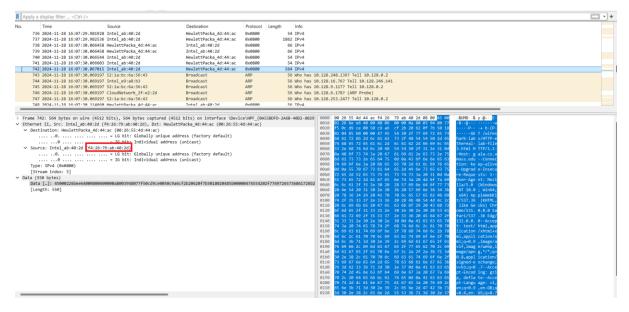
### 2252720 Võ Trúc Sơn lab7 Ethernet&ARP

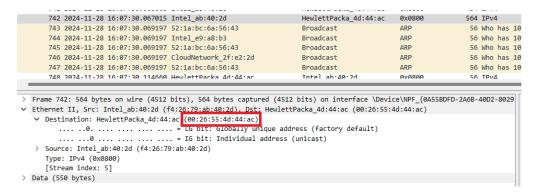
1. What is the 48-bit Ethernet address of your computer?

Answer: The source address is as picture follow



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.]

<u>Answer:</u> The destination address is in the picture as follow. This is not the address of *gaia.cs.umass.edu*. We can see in the picture that the Ethernet address is of "HewlettPacka 4d:44:ac".



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

Answer: The hexadecimal value is 0x0800. It is corresponded to the IPv4 protocol.

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

Answer: Calculation: 54 bytes

```
0000
      00 26 55 4d 44 ac f4 26
                                79 ab 40 2d 08 00 45 00
                                                             &UMD · · & y · @ - · · E
         26 be e6 40 00 80 06
                                00
                                   00 0a 80
                                                94 80
0010
0020
      f5
         0c
            d9
               ce 00 50 c9 a6
                                cf
                                    2b 20
                                          62 0f
                                                7b 50
                                                              ...p..
      02 04 85 b0 00 00 47
                            45
                                54 20 2f
                                             69 72 65
                                                             ·····GE T /wires
0030
                                          77
      68 61 72 6b 2d 6c 61 62
                                73 2f 48 54 54 50 2d
                                                      65
                                                            hark-lab s/HTTP-e
9949
      74 68 65 72 65 61 6c 2d
                                6c 61 62 2d 66 69 6c 65
                                                            thereal- lab-file
9959
9969
      33 2e 68 74 6d 6c 20 48
                                54 54 50
                                          2f
                                             31 2e 31
                                                            3.html H TTP/1.1
               73
      0a 48 6f
                  74 3a 20 67
                                 61
                                   69 61
                                          2e 63 73 2e
0070
                                                            ·Host: g aia.cs.ι
      6d
         61 73
               73
                  2e 65
                         64 75
                                0d
                                    0a 43 6f
                                             6e 6e 65
0880
                                                            mass.edu ∙∙Connec
0090
      74 69 6f
               6e 3a 20 6b 65
                                65 70 2d 61 6c 69 76
                                                       65
                                                            tion: ke ep-alive
      0d 0a 55 70 67 72 61 64
                                65 2d 49 6e 73 65 63
                                                             ··Upgrad e-Insecu
00a0
      72 65 2d 52 65 71 75 65
                                73 74 73 3a 20 31 0d
99b9
                                                            re-Reque sts: 1.
         73 65 72 2d 41 67 65
                                   74 3a
                                бе
                                          20 4d 6f
                                                      69
                                                            User-Age nt: Mozi
00c0
                  35 2e
                                                            lla/5.0
            61 2f
                         30 20
                                 28
                                   57
                                       69
                                          6e 64
                                                6f
00d0
         бс
                                                                      (Windows
00e0
        4e 54 20 31 30 2e 30
                                 3b 20 57
                                          69
                                             6e 36 34
                                                             NT 10.0 ; Win64:
      20 78 36 34 29 20 41 70
                                 70 6c 65 57 65 62 4b
aafa
                                                             x64) Ap pleWebKi
      74 2f 35 33 37 2e 33 36
                                 20 28 4b 48 54 4d 4c
0100
                                                             :/537.36
                                                                       (KHTML
```

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?

<u>Answer:</u> You can see the source address as follow. It probably not the address of my computer or *gaia.cs.umass.edu* but it is from HewlettPacka\_4d:44:ac

```
815 2024-11-28 16:07:30.366052 HewlettPacka_4d:44:ac
                                                                          Intel_ab:40:2d
                                                                                                   0x0800
       816 2024-11-28 16:07:30.366052 HewlettPacka 4d:44:ac
                                                                         Intel_ab:40:2d
                                                                                                   0x0800
                                                                                                                    1506 IPv4
       817 2024-11-28 16:07:30.366052 HewlettPacka_4d:44:ac
                                                                          Intel_ab:40:2d
                                                                                                   0x0800
       818 2024-11-28 16:07:30.366052 HewlettPacka 4d:44:ac
                                                                         Intel ab:40:2d
                                                                                                   0x0800
                                                                                                                    1506 IPv4
       819 2024-11-28 16:07:30.366052 HewlettPacka_4d:44:ac
                                                                         Intel ab:40:2d
                                                                                                                    559 IPv4
                                                                                                   0x0800
       820 2024-11-28 16:07:30.366098 Intel ab:40:2d
                                                                         HewlettPacka_4d:44:ac
                                                                                                   0x0800
                                                                                                                      56 Who has 10.128.0.2? Tell 10.128.7.182
       821 2024-11-28 16:07:30.375254 6e:df:4b:29:96:ea
                                                                         Broadcast
                                                                                                   ARP
       822 2024-11-28 16:07:30.376845 Intel_c1:58:36
                                                                                                                     56 ARP Announcement for 10.128.249.13
56 Who has 10.128.6.138? Tell 10.128.0.2
                                                                                                   ARP
       823 2024-11-28 16:07:30.376845 52:1a:bc:6a:56:43
                                                                         Broadcast
                                                                                                   ARP
       825 2024-11-28 16:07:30 376845 52:1a:hc:6a:56:43
                                                                         Broadcast
                                                                                                   ΔRP
                                                                                                                      56 Who has 10 128 7 367 Tell 10 128 0 2
> Frame 816: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface \Device\NPF {0A55BDFD-2A6B-40D2-8029-D8967079945C}, id 0
                                                      4d:44:ac), Dst: Intel_ab:40:2d (f4:26:79:ab:40:2d)
     Destination: Intel ab:40:2d (f4:26:79:ab:40:2d)
      Source: HewlettPacka_4d:44:ac (00:26:55:4d:44:ac)
      [Stream index: 5]
 Data (1492 bytes)
     Data [...]: 452005d4f82d40002f06ca3e8077f50c0a8003940050d9ce20620f7bc9a6d129501000edfe650000485454502f312e3120323030204f4b0d0a446174653a205468752c2032
      [Length: 1492]
```

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

<u>Answer:</u> You can see the destination address as follow. This is the Ethernet address of my computer.

```
815 2024-11-28 16:07:30.366052 HewlettPacka_4d:44:ac
                                                                          Intel_ab:40:2d
                                                                                                                      56 IPv4
       816 2024-11-28 16:07:30.366052 HewlettPacka 4d:44:ac
                                                                          Intel_ab:40:2d
                                                                                                    0x0800
                                                                                                                    1506 IPv4
       817 2024-11-28 16:07:30.366052 HewlettPacka 4d:44:ac
                                                                          Intel ab:40:2d
                                                                                                    0x0800
                                                                                                                    1506 IPv4
       818 2024-11-28 16:07:30.366052 HewlettPacka 4d:44:ac
                                                                          Intel ab:40:2d
                                                                                                    0x0800
                                                                                                                    1506 IPv4
                                                                                                                     559 IPv4
       819 2024-11-28 16:07:30.366052 HewlettPacka 4d:44:ac
                                                                          Intel ab:40:2d
                                                                                                    0x0800
       820 2024-11-28 16:07:30.366098 Intel_ab:40:2d
                                                                          HewlettPacka_4d:44:ac
                                                                                                    0x0800
                                                                                                                      54 IPv4
                                                                                                                      56 Who has 10.128.0.2? Tell 10.128.7.182
       821 2024-11-28 16:07:30.375254 6e:df:4b:29:96:ea
                                                                          Broadcast
                                                                                                    ARP
       822 2024-11-28 16:07:30.376845 Intel_c1:58:36
       823 2024-11-28 16:07:30.376845 52:1a:bc:6a:56:43
                                                                          Broadcast
                                                                                                    ARP
                                                                                                                      56 Who has 10.128.6.138? Tell 10.128.0.2
                                                                                                                      56 Who has 10.128.6.138? Tell 10.128.0.4
       824 2024-11-28 16:07:30.376845 c2:1d:36:6c:29:5f
                                                                          Broadcast
                                                                                                    ARP
       825 2024-11-28 16:07:30 376845 52:1a:bc:6a:56:43
                                                                          Renadrast
                                                                                                    ARP
                                                                                                                      56 Who has 18 128 7 362 Tell 18 128 8 2
> Frame 816: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface \Device\NPF_{0A55BDFD-2A68-4002-8029-D8967079945C}, id 0
                    : HewlettPacka 4d:44:ac (00:26:55:4d:44:ac), Dst: Intel_ab:40:2d (f4:26:79:ab:40:2d)
     Destination: Intel_ab:40:2d (f4:26:79:ab:40:2d)
Source: HewlettPacka_4d:44:ac (00:26:55:4d:44:ac)
      [Stream index: 5]
V Data (1492 bytes)
     Data [_]: 452005d4f82d40002f06ca3e8077f50c0a8003940050d9ce20620f7bc9a6d129501000edfe650000485454502f312e3120323030204f4b0d0a446174653a205468752c2032
```

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

Answer: This is the hexadecimal value, correspond to Ipv4.

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?

Answer: it's 54 bytes.

```
55 4d 44 ac 08 00 45 20
                                                            &y ⋅@ - ⋅ & UMD · ⋅ ⋅ E
9999
      f4 26 79 ab 40 2d 00 26
                                                            ···-@·/· ·>·w···
               2d 40 00 2f
                                ca 3e 80
                                            f5
                                                0c
0020
      03 94 00 50 d9 ce 20 62
                                0f 7b c9 a6 d1 29 50 10
      00 ed fe 65 00 00 48 54
                                54 50 2f 31 2e 31 20 32
0030
                                                            ···e··HT TP/1.1 2
      30 30 20 4f 4b 0d 0a 44
                                61 74 65 3a 20 54 68 75
                                                           00 OK··D ate: Thu
0040
0050
      2c 20 32 38 20 4e 6f 76
                                20 32 30 32 34
                                               20 30 39
                                                            , 28 Nov
                                                                     2024 09
0060
      3a 30 36 3a 33 37 20 47
                                4d 54 0d 0a 53 65
                                                   72
                                                           :06:37 G MT · · Ser\
      65 72 3a
                                68 65 2f
0070
               20 41 70 61 63
                                         32
                                             2e
                                                34
                                                   2e
                                                            er: Apac he/2.4.6
                                                            (CentOS ) OpenSS
      20 28 43 65 6e 74 4f 53
                                29 20 4f
                                         70 65
0880
                                                бе
0090
      4c 2f 31 2e 30 2e 32 6b
                                2d 66 69 70 73
                                                20 50 48
                                                            L/1.0.2k -fips PH
      50 2f 37 2e 34 2e 33 33
                                20 6d 6f 64 5f
                                                70 65 72
                                                           P/7.4.33 mod per
00a0
      6c 2f 32 2e 30 2e 31 31
                                20 50 65 72 6c 2f 76 35
                                                           1/2.0.11 Perl/v5
aaba
00c0
      2e 31 36 2e 33 0d 0a 4c
                                61 73 74 2d 4d 6f 64 69
                                                            .16.3⋅⋅L ast-Modi
         69 65 64 3a 20 54 68
                                75 2c
                                      20
                                         32 38
                                                           fied: Th u, 28 No
aada
                                                20
```

9. Write down the contents of your computer's ARP cache. What is the meaning of each column value?

```
C:\Users\rkvdg>arp -a
Interface: 172.16.57.99 --- 0x8
                        Physical Address
  Internet Address
                                               Type
                                               dynamic
  172.16.56.1
                        70-01-b5-af-d1-d6
  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
                                               static
C:\Users\rkvdg> arp -d *
C:\Users\rkvdg>
```

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

```
AmbitMicrosy_a9:3d:_ Broadcast
                                                                           42 Who has 192.168.1.1? Tell 192.168.1.105
      2 0.001018
                     LinksysGroup_da:af:_ AmbitMicrosy_a9:3d:_ ARP
                                                                           60 192.168.1.1 is at 00:06:25:da:af:73
      3 0.001028
                     AmbitMicrosy_a9:3d:.. LinksysGroup_da:af:.. 0x0800
                                                                           62 IPv4
      4 2.962850
                     AmbitMicrosy_a9:3d:__LinksysGroup_da:af:__0x08000
                                                                          62 IPv4
      5 8.971488
                     AmbitMicrosy_a9:3d:.. LinksysGroup_da:af:.. 0x0800
                                                                          62 IPv4
      6 13.542974
                    CnetTechnolo_73:8d:_ Broadcast
                                                                          60 Who has 192.168.1.117? Tell 192.168.1.104
      7 17.444423
                     AmbitMicrosy_a9:3d:.. LinksysGroup_da:af:.. 0x0800
                                                                           62 IPv4
      8 17,465902
                     LinksysGroup_da:af:.. AmbitMicrosy_a9:3d:.. 0x0800
                                                                          62 IPv4
      9 17,465927
                   AmbitMicrosy_a9:3d:.. LinksysGroup_da:af:.. 0x0800
                                                                          54 IPv4
     10 17,466468
                     AmbitMicrosy_a9:3d:__LinksysGroup_da:af:__0x0800
                                                                        686 IPv4
     11 17,494766
                     LinksysGroup_da:af:... AmbitMicrosy_a9:3d:.. 0x0800
                                                                          60 IPv4
     12 17.498935
                     LinksysGroup_da:af:.. AmbitMicrosy_a9:3d:.. 0x0800
                                                                        1514 IPv4
     13 17,500025
                     LinksysGroup_da:af:.. AmbitMicrosy_a9:3d:.. 0x0800
                                                                        1514 IPv4
                   AmbitMicrosy_a9:3d:.. LinksysGroup_da:af:.. 0x0800
     14 17,500069
                                                                          54 TPv4
                    LinksysGroup_da:af:.. AmbitMicrosy_a9:3d:.. 0x0800 1514 IPv4
     15 17.527057
     16 17,527422
                     LinksysGroup_da:af:.. AmbitMicrosy_a9:3d:.. 0x0800
                                                                         489 IPv4
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
  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)
    Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
> Address Resolution Protocol (request)
```

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

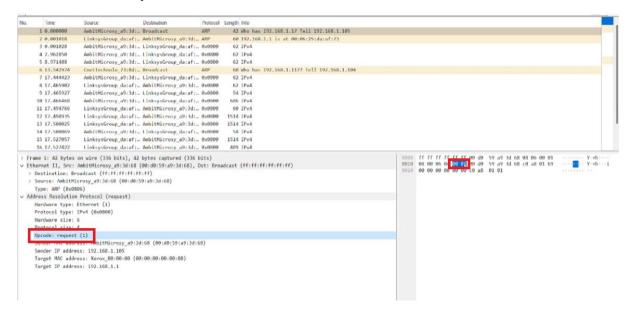
```
Type: ARP (0x0806)
```

12. 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.

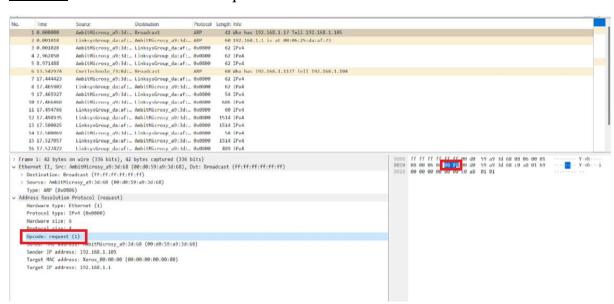
a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

## Answer: 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 request is made?

Answer: That is 00 01. It is a request

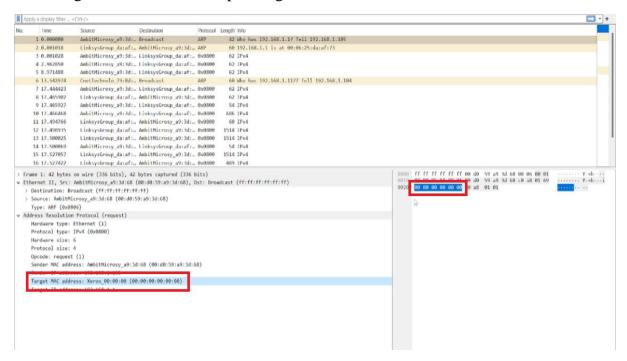


c) Does the ARP message contain the IP address of the sender?

Answer: Yes, you can see the source which is my computer IP address.

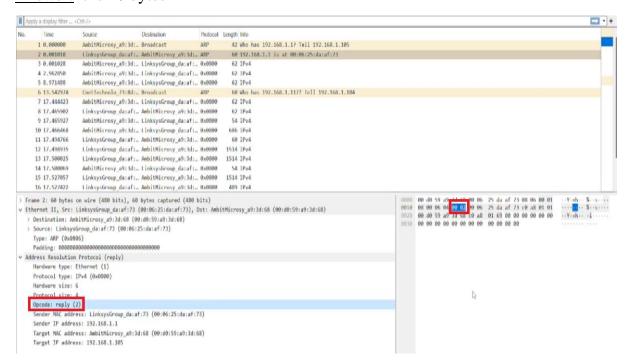
d) Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?

<u>Answer:</u> We can conclude that ARP packet structure conclude many fields and the ARP hardware address is specifically where the ARP request indicates the ethernet address that correspond to the IP address being queried. This field is basically of 6 bytes and is used to specify the hardware address of the target machine for which the ARP request is seeking to resolve the corresponding IP address.



- 13. 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

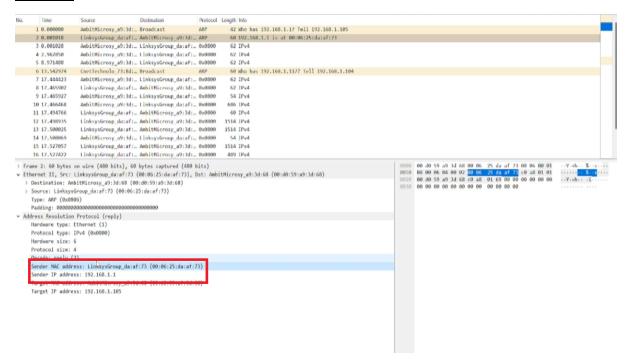


b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

Answer: The opcode value is 00 02.

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: the answer is as follow.



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

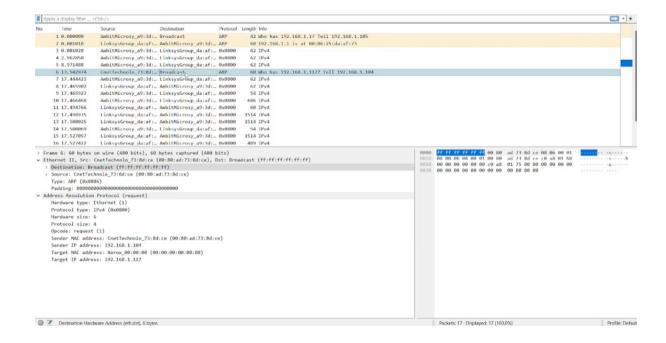
Answer: the answer is as follow.

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

#### 15. 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: the destination is broadcast so it don't know who has the IP to reply



### 2252720 Võ Trúc Sơn lab8

- 1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?
- Beacon frames are the special files that contain the information of the appearance of the Internet such as SSID, security and other things
- SSIDs is the name of the Internet
- From:

# CiscoLinksys\_f7:1d:...

▶ Tag: SSID parameter set: "30 Munroe St"

- From:

# LinksysGroup\_67:22:...

```
▼ Tagged parameters (26 bytes)
▼ Tag: SSID parameter set: 6c69ee0104e2273a32
Tag Number: SSID parameter set (0)
Tag length: 9
SSID: 6c69ee0104e2273a32
```

2. What are the intervals of time between the transmissions of the beacon frames the

linksys\_ses\_24086 access point? From the 30 Munroe St. access point? (Hint: this

interval of time is contained in the beacon frame itself)

- From 30 Munroe St:

```
Fixed parameters (12 bytes)
Timestamp: 174319001986
Beacon Interval: 0.102400 [Seconds]
```

- From linksys\_ses\_24086:

```
Fixed parameters (12 bytes)
Timestamp: 11529295568209666840
Beacon Interval: 0.063488 [Seconds]
```

3. What (in hexadecimal notation) is the source MAC address on the beacon frame from 30 Munroe St? Recall from Figure 7.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed

discussion of the 802.11 frame structure, see section 7 in the IEEE 802.11 standards document (cited above).

- MAC address is below:

# BSS Id: CiscoLinksys\_f7:1d:51 (00:16:b6:f7:1d:51)

4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from *30 Munroe St*??

# Destination address: Broadcast (ff:ff:ff:ff:ff)

5. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from *30* 

Munroe St?

# BSS Id: CiscoLinksys\_f7:1d:51 (00:16:b6:f7:1d:51)

- 6. The beacon frames from the 30 Munroe St access point advertise that the access point can support four data rates and eight additional "extended supported rates." What are these rates?
- "Support rate": usually is the standard rate that each AP supports

```
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
   Tag Number: Supported Rates (1)
   Tag length: 4
   Supported Rates: 1(B) (0x82)
   Supported Rates: 2(B) (0x84)
   Supported Rates: 5.5(B) (0x8b)
   Supported Rates: 11(B) (0x96)
```

- "Extended supported rates": is the higher rate that the AP can run if it is supported.

```
▼ Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag Number: Extended Supported Rates (50)
    Tag length: 8
    Extended Supported Rates: 6(B) (0x8c)
    Extended Supported Rates: 9 (0x12)
    Extended Supported Rates: 12(B) (0x98)
    Extended Supported Rates: 18 (0x24)
    Extended Supported Rates: 24(B) (0xb0)
    Extended Supported Rates: 36 (0x48)
    Extended Supported Rates: 48 (0x60)
    Extended Supported Rates: 54 (0x6c)
```

7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session

(that downloads alice.txt). What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)? To the access point? To the first-hop router? What is the IP address of the wireless host sending this TCP segment? What is the destination IP address? Does this destination IP address correspond to the host, access point, first-hop router, or some other network-attached device? Explain

474 24.81 192.168.1.109 128.119.245.12 TCP 110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK\_PER

- Three 3 MAC addresses are:
- Destination address: CiscoLinksys\_f4:eb:a8 (00:16:b6:f4:eb:a8)
- Source address: Intel\_d1:b6:4f (00:13:02:d1:b6:4f)
- BSS Id: CiscoLinksvs f7:1d:51 (00:16:b6:f7:1d:51)
  - The MAC address of wireless host is Source address.
  - The MAC address of access point is BSSID
  - The MAC address of first-hop router is Destination address
  - IP address of wireless host:

#### Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12

- Destination IP address: 128.119.245.12
- This destination IP address is involving to the host which contains the information of the text, it is not an address of other devices listed.
- 8. Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram? (Hint: review Figure 6.19 in the text if you are unsure of how to answer this question, or the corresponding part of the previous question. It's particularly important that you understand this).

476 24.82 128.119.245.12 192.168.1.109 TCP 110 80 -> 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK\_PER

Three 3 MAC addresses are:

```
Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
Source address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)

BSS Id: CiscoLinksys f7:1d:51 (00:16:b6:f7:1d:51)
```

- The MAC address of wireless host is Source address.
- The MAC address of access point is BSSID

- The MAC address of first-hop router is Destination address
- IP address of wireless host:

#### Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.109

- Destination IP address: 192.168.1.109
- No, if there is the AP taking the role of intermediate the MAC address will be of the AP, but the destination IP address is from the host
- 9. What two actions are taken (i.e., frames are sent) by the host in the trace just after
  - t=49, to end the association with the 30 Munroe St AP that was initially in place when trace collection began? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification, is there another frame that you might have expected to see, but don't see here?
- These two frames are:

```
1733 49.58 192.168.1.109 192.168.1.1 DHCP 390 DHCP Release - Transaction ID 0xea5a526

1735 49.60 Intel_d1:b6:4f CiscoLinksys_f7:1d:... 802.11 54 Deauthentication, SN=1605, FN=0, Flags=......C
```

- I am waiting for the frame disassociation, but in this case because the host or the AP chooses the way that disconnects directly and fast, so they choose the frame "de-authentication" instead of "disassociation"
- 10. Examine the trace file and look for AUTHENICATION frames sent from the host to an AP and vice versa. How many AUTHENTICATION messages are sent from the wireless host to the linksys\_ses\_24086 AP (which has a MAC address of Cisco\_Li\_f5:ba:bb) starting at around t=49?

```
CiscoLinksys f5:ba:... 802.11
1740 49.63
             Intel d1:b6:4f
                                                                      58 Authentication, SN=1606, FN=0, Flags=......
             Intel_d1:b6:4f
1741 49.63
                                    CiscoLinksys_f5:ba:... 802.11
                                                                      58 Authentication, SN=1606, FN=0, Flags=....R...C
             Intel_d1:b6:4f
                                   CiscoLinksys_f5:ba:... 802.11
                                                                      58 Authentication, SN=1606, FN=0, Flags=....R..
1742 49.64
          Intel_d1:b6:4f
                                                        58 Authentication, SN=1606, FN=0,
                                                                                          .....C, BI=100, SSID="30 Munroe
1749 49.64 Intel d1:b6:4f
                                   CiscoLinksys_f5:ba:... 802.11
                                                                     58 Authentication, SN=1606, FN=0, Flags=....R...C
```

- There are 6
- 11. Does the host want the authentication to require a key or be open?

# Authentication Algorithm: Open System (0)

- It requires open
- 12. Do you see a reply AUTHENTICATION from the linksys\_ses\_24086 AP in the trace?
- No, I do not

13. Now let's consider what happens as the host gives up trying to associate with the *linksys\_ses\_24086* AP and now tries to associate with the *30 Munroe St* AP. Look

for AUTHENICATION frames sent from the host to and AP and vice versa. At what times are there an AUTHENTICATION frame from the host to the 30 Munroe St. AP, and when is there a reply AUTHENTICATION sent from that AP

to the host in reply? (Note that you can use the filter expression "wlan.fc.subtype == 11 and wlan.fc.type == 0 and wlan.addr == IntelCor\_d1:b6:4f" to display only the AUTHENTICATION frames in this trace for this wireless host.)

- Time sending AUTHENTICATION: 49.64

1749 49.64 Intel\_d1:b6:4f CiscoLinksys\_f5:ba:... 802.11 58 Authentication, SN=1606, FN=0, Flags=....R...C

- Time receiving AUTHENTICATION: 63.16

2158 63.16 CiscoLinksys f7:1d:... Intel d1:b6:4f 802.11 58 Authentication, SN=3726, FN=0, Flags=......C

14. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associated with an AP. At what time is there an ASSOCIATE REQUEST from host to the 30 Munroe St AP? When is the corresponding ASSOCIATE REPLY sent? (Note that you can use the filter expression "wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == IntelCor\_d1:b6:4f" to display only the ASSOCIATE REOUEST and ASSOCIATE RESPONSE frames for this trace.)

```
2126 62.17 Intel_d1:b6:4f CiscoLinksys_f5:ba:... 802.11 107 Association Request, SN=1645, FN=0, Flags=......C, SSID="linksys_SES_24086"

2127 62.17 Intel_d1:b6:4f CiscoLinksys_f5:ba:... 802.11 107 Association Request, SN=1645, FN=0, Flags=.....C, SSID="linksys_SES_24086"

2162 63.16 Intel_d1:b6:4f CiscoLinksys_f7:1d:... 802.11 89 Association Request, SN=1648, FN=0, Flags=......C, SSID="30 Munroe St"

2166 63.19 CiscoLinksys_f7:1d:... Intel_d1:b6:4f 802.11 94 Association Response, SN=3728, FN=0, Flags=......C
```

- Time sending ASSOCIATE REQUEST: 62.17
- Time receiving ASSOCIATE REPLY: 63.19
- 15. What transmission rates is the host willing to use? The AP? To answer this question, you will need to look into the parameters fields of the 802.11 wireless LAN management frame
- From the host:

```
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
Tag Number: Supported Rates (1)
Tag length: 4
Supported Rates: 1(B) (0x82)
Supported Rates: 2(B) (0x84)
Supported Rates: 5.5(B) (0x8b)
Supported Rates: 11(B) (0x96)
```

- The AP:

```
▼ Tagged parameters (36 bytes)
▼ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
Tag Number: Supported Rates (1)
Tag length: 4
Supported Rates: 1(B) (0x82)
Supported Rates: 2(B) (0x84)
Supported Rates: 5.5(B) (0x8b)
Supported Rates: 11(B) (0x96)
```

- 16. What are the sender, receiver and BSS ID MAC addresses in these frames? What is the purpose of these two types of frames? (To answer this last question, you'll need to dig into the online references cited earlier in this lab).
- Sender, Receiver and BSS ID MAC addresses:

```
Receiver address: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)

Destination address: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)

Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)

Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)

BSS Id: CiscoLinksys f5:ba:bb (00:18:39:f5:ba:bb)
```

```
Proceiver address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
Destination address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
```

- The associative frame used to create the connection.
- Beacon frame used to announce the availability of the Internet and information for host to decide to connect