TRƯỜNG ĐẠI HỌC BÁCH KHOA

ĐẠI HỌC QUỐC GIA TP HỒ CHÍ MINH

HOMEWORK

MẠNG MÁY TÍNH (THỰC HÀNH) – LAB 7

Giảng viên hướng dẫn: Ths. Bùi Xuân Giang

Sinh viên thực hiện: Trần Minh Tân

Mã số sinh viên: 2012018

Lớp: L10.

Thành phố Hồ Chí Minh – 2022

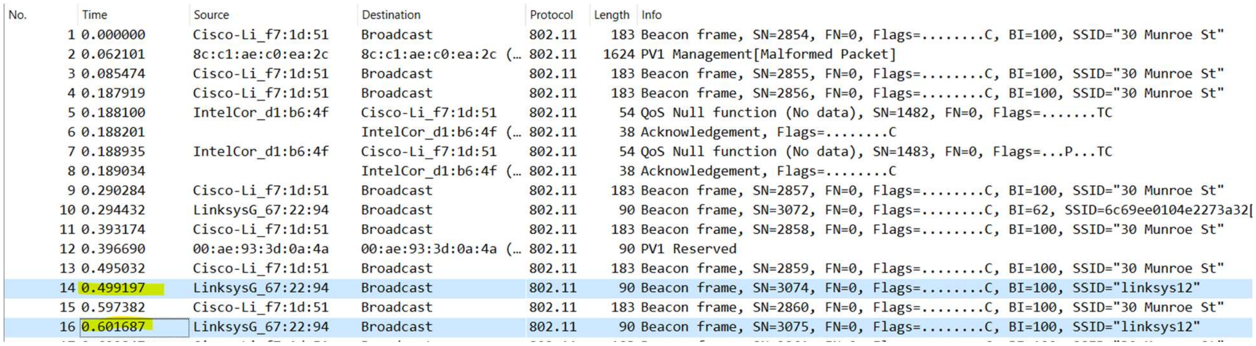
PART 2. Beacon Frames

1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?

They are “30 Munroe St” and “linksys12”.

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).

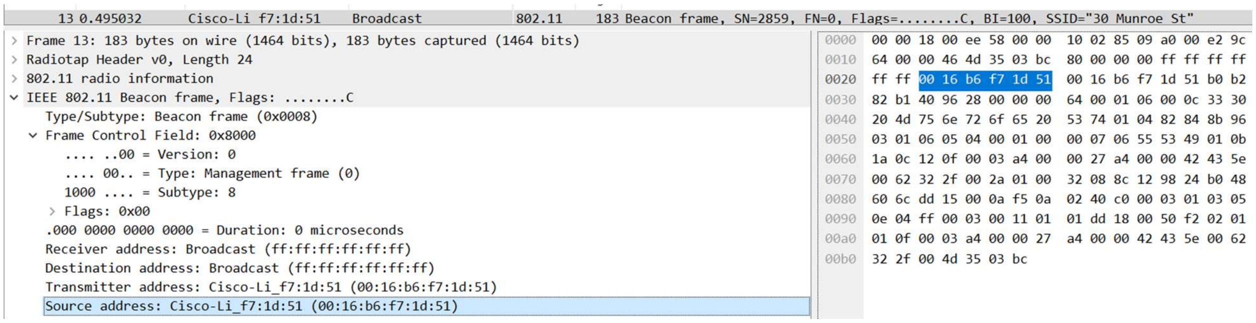
They are both 0.601687 – 0.499197 = 0.10249



```
No.  Time      Source             Destination         Protocol Length Info
   1 0.000000  Cisco-Li_f7:1d:51  Broadcast           802.11     183 Beacon frame, SN=2854, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   2 0.062101  8c:c1:ae:c0:ea:2c  8c:c1:ae:c0:ea:2c (… 802.11    1624 PV1 Management[Malformed Packet]
   3 0.085474  Cisco-Li_f7:1d:51  Broadcast           802.11     183 Beacon frame, SN=2855, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   4 0.187919  Cisco-Li_f7:1d:51  Broadcast           802.11     183 Beacon frame, SN=2856, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
   5 0.188100  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51   802.11      54 QoS Null function (No data), SN=1482, FN=0, Flags=.......TC
   6 0.188201                     IntelCor_d1:b6:4f (… 802.11      38 Acknowledgement, Flags=........C
   7 0.188935  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51   802.11      54 QoS Null function (No data), SN=1483, FN=0, Flags=...P...TC
   8 0.189034                     IntelCor_d1:b6:4f (… 802.11      38 Acknowledgement, Flags=........C
   9 0.290284  Cisco-Li_f7:1d:51  Broadcast           802.11     183 Beacon frame, SN=2857, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  10 0.294432  LinksysG_67:22:94  Broadcast           802.11      90 Beacon frame, SN=3072, FN=0, Flags=........C, BI=62, SSID=6c69ee0104e2273a32[
  11 0.393174  Cisco-Li_f7:1d:51  Broadcast           802.11     183 Beacon frame, SN=2858, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  12 0.396690  00:ae:93:3d:0a:4a  00:ae:93:3d:0a:4a (… 802.11      90 PV1 Reserved
  13 0.495032  Cisco-Li_f7:1d:51  Broadcast           802.11     183 Beacon frame, SN=2859, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  14 0.499197  LinksysG_67:22:94  Broadcast           802.11      90 Beacon frame, SN=3074, FN=0, Flags=........C, BI=100, SSID="linksys12"
  15 0.597382  Cisco-Li_f7:1d:51  Broadcast           802.11     183 Beacon frame, SN=2860, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
  16 0.601687  LinksysG_67:22:94  Broadcast           802.11      90 Beacon frame, SN=3075, FN=0, Flags=........C, BI=100, SSID="linksys12"
```

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).

Source MAC address: (00:16:b6:f7:1d:51)



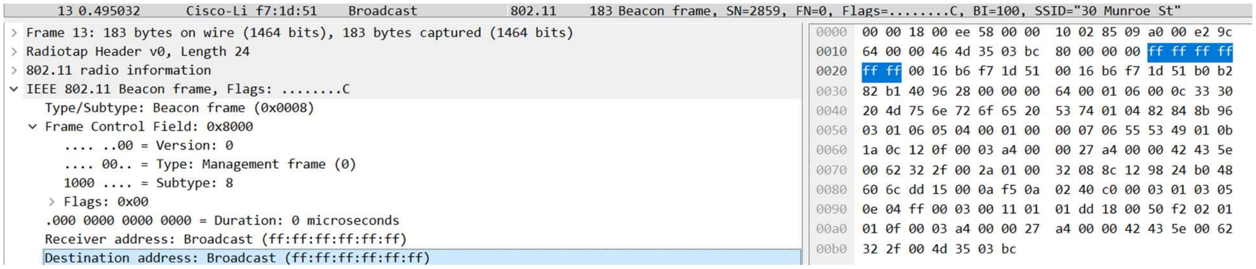
```
  13 0.495032   Cisco-Li f7:1d:51   Broadcast   802.11   183 Beacon frame, SN=2859, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"

> Frame 13: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  v Frame Control Field: 0x8000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1000 .... = Subtype: 8
    > Flags: 0x00
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
```

```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e2 9c
0010  64 00 00 46 4d 35 03 bc  80 00 00 00 ff ff ff ff
0020  ff ff 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 b0 b2
0030  82 b1 40 96 28 00 00 00  64 00 01 06 00 0c 33 30
0040  20 4d 75 6e 72 6f 65 20  53 74 01 04 82 84 8b 96
0050  03 01 06 05 04 00 01 00  00 07 06 55 53 49 01 0b
0060  1a 0c 12 0f 00 03 a4 00  00 27 a4 00 00 42 43 5e
0070  00 62 32 2f 00 2a 01 00  32 08 8c 12 98 24 b0 48
0080  60 6c dd 15 00 0a f5 0a  02 40 c0 00 03 01 03 05
0090  0e 04 ff 00 03 00 11 01  01 dd 18 00 50 f2 02 01
00a0  01 0f 00 03 a4 00 00 27  a4 00 00 42 43 5e 00 62
00b0  32 2f 00 4d 35 03 bc
```

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

Destination MAC address is ff:ff:ff:ff:ff:ff

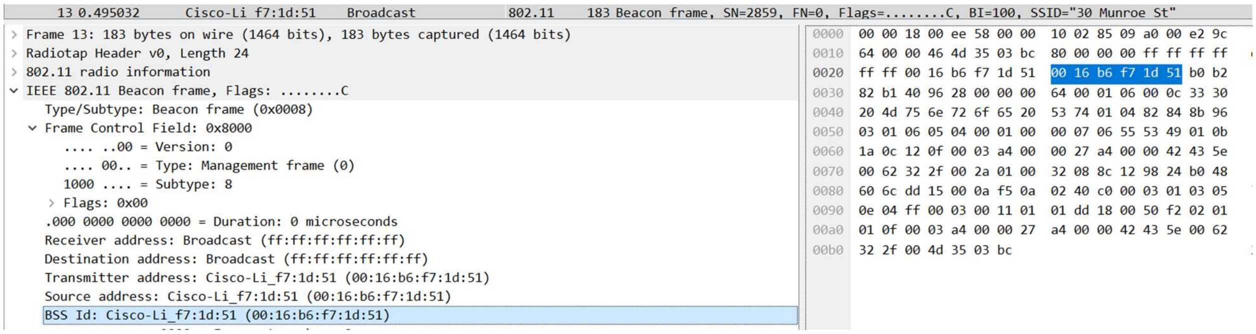


```
    13 0.495032      Cisco-Li_f7:1d:51     Broadcast          802.11     183 Beacon frame, SN=2859, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
> Frame 13: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  v Frame Control Field: 0x8000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1000 .... = Subtype: 8
    > Flags: 0x00
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
```

```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e2 9c
0010  64 00 00 46 4d 35 03 bc  80 00 00 00 ff ff ff ff
0020  ff ff 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 b0 b2
0030  82 b1 40 96 28 00 00 00  64 00 01 06 00 0c 33 30
0040  20 4d 75 6e 72 6f 65 20  53 74 01 04 82 84 8b 96
0050  03 01 06 05 04 00 01 00  00 07 06 55 53 49 01 0b
0060  1a 0c 12 0f 00 03 a4 00  00 27 a4 00 00 42 43 5e
0070  00 62 32 2f 00 2a 01 00  32 08 8c 12 98 24 b0 48
0080  60 6c dd 15 00 0a f5 0a  02 40 c0 00 03 01 03 05
0090  0e 04 ff 00 03 00 11 01  01 dd 18 00 50 f2 02 01
00a0  01 0f 00 03 a4 00 00 27  a4 00 00 42 43 5e 00 62
00b0  32 2f 00 4d 35 03 bc
```

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

The MAC BSS id is 00:16:b6:f7:1d:51



```
    13 0.495032      Cisco-Li_f7:1d:51     Broadcast          802.11     183 Beacon frame, SN=2859, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
> Frame 13: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  v Frame Control Field: 0x8000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1000 .... = Subtype: 8
    > Flags: 0x00
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
```

```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e2 9c
0010  64 00 00 46 4d 35 03 bc  80 00 00 00 ff ff ff ff
0020  ff ff 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 b0 b2
0030  82 b1 40 96 28 00 00 00  64 00 01 06 00 0c 33 30
0040  20 4d 75 6e 72 6f 65 20  53 74 01 04 82 84 8b 96
0050  03 01 06 05 04 00 01 00  00 07 06 55 53 49 01 0b
0060  1a 0c 12 0f 00 03 a4 00  00 27 a4 00 00 42 43 5e
0070  00 62 32 2f 00 2a 01 00  32 08 8c 12 98 24 b0 48
0080  60 6c dd 15 00 0a f5 0a  02 40 c0 00 03 01 03 05
0090  0e 04 ff 00 03 00 11 01  01 dd 18 00 50 f2 02 01
00a0  01 0f 00 03 a4 00 00 27  a4 00 00 42 43 5e 00 62
00b0  32 2f 00 4d 35 03 bc
```

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?

The eight additional "extended supported rates" are 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0 Mbps and four data rates are 1.0, 2.0, 5.5, 11.0 Mbps.

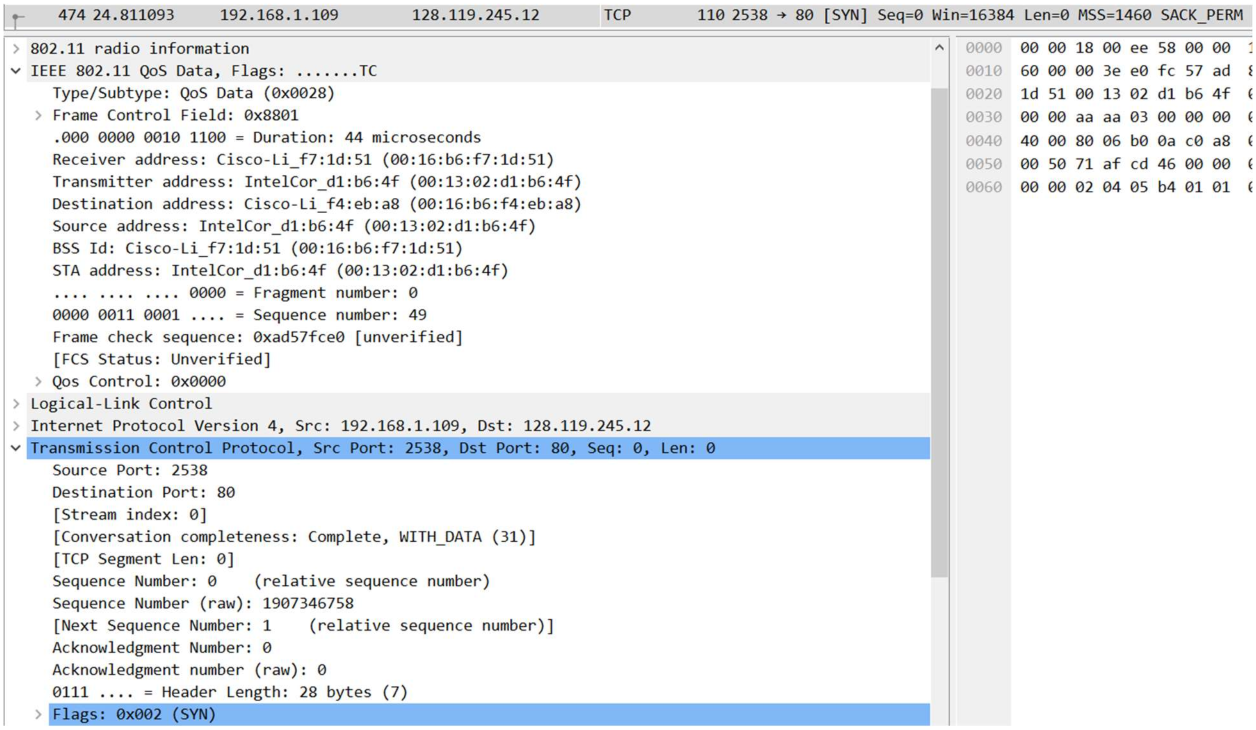
PART 3. Data Transfer

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.

Solution:

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?



```
474 24.811093     192.168.1.109        128.119.245.12       TCP       110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
```

```
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8801
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
    Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    .... .... .... 0000 = Fragment number: 0
    0000 0011 0001 .... = Sequence number: 49
    Frame check sequence: 0xad57fce0 [unverified]
    [FCS Status: Unverified]
  > Qos Control: 0x0000
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 2538, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 2538
    Destination Port: 80
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1907346758
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    0111 .... = Header Length: 28 bytes (7)
  > Flags: 0x002 (SYN)
```

```
0000  00 00 18 00 ee 58 00 00
0010  60 00 00 3e e0 fc 57 ad
0020  1d 51 00 13 02 d1 b6 4f
0030  00 00 aa aa 03 00 00 00
0040  40 00 80 06 b0 0a c0 a8
0050  00 50 71 af cd 46 00 00
0060  00 00 02 04 05 b4 01 01
```

This frame is at t = 24.811093.

Three MAC address fields in the 802.11 frame are BSS id, source address and destination.

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?

The MAC address corresponds to the wireless host is 00:13:02:d1:b6:4f.

Corresponding to the first hop router is 00:16:b6:f4:eb:a8.

Corresponding to the wireless host sending this TCP segment is 00:16:b6:f7:1d:51.

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.

The corresponding IP of the wireless host is 192.168.1.109.

The destination IP is 128.199.245.12 and this IP is corresponds to the host.