Submission - LAB 5: Wireless 802.11

Please submit during this lab session or else at next week's lab session.

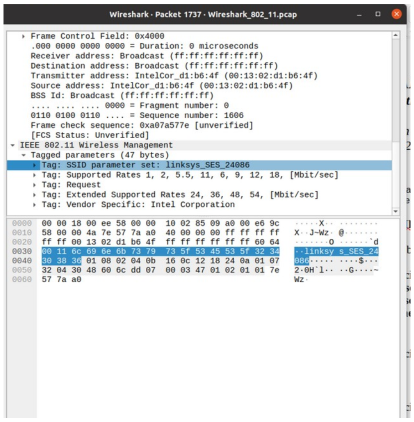
Student name: *Nathan Crowley* ***Student ID:*** *118429092*
Submission Date: *3/12/2020*

1. Beacon Frames

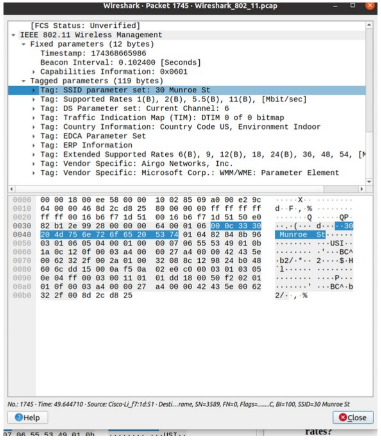
- Beacon frame contains network information needed by a station before it can transmit a frame. They are used for announcing the presence of devices in a WLAN as well as synchronization of devices and services.

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

   - Most of the beacon frames are being issued by linksys_SES_24086 and 30 Munroe St.



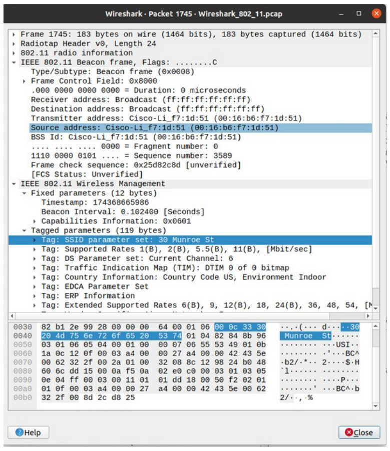
```
  ▸ Frame Control Field: 0x4000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    .... .... .... 0000 = Fragment number: 0
    0110 0100 0110 .... = Sequence number: 1606
    Frame check sequence: 0xa07a577e [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 Wireless Management
  ▾ Tagged parameters (47 bytes)
    ▸ Tag: SSID parameter set: linksys_SES_24086
    ▸ Tag: Supported Rates 1, 2, 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
    ▸ Tag: Request
    ▸ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▸ Tag: Vendor Specific: Intel Corporation

0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e6 9c   ·····X·· ········
0010  58 00 00 4a 7e 57 7a a0  40 00 00 00 ff ff ff ff   X··J~Wz· @·······
0020  ff ff 00 13 02 d1 b6 4f  ff ff ff ff ff ff 60 64   ·······O ······`d
0030  00 11 6c 69 6e 6b 73 79  73 5f 53 45 53 5f 32 34   ··linksy s_SES_24
0040  30 38 36 01 08 02 04 0b  16 0c 12 18 24 0a 01 07   086····· ····$···
0050  32 04 30 48 60 6c dd 07  00 03 47 01 02 01 01 7e   2·0H`l·· ··G····~
0060  57 7a a0                                           Wz·
```



```
    [FCS Status: Unverified]
▾ IEEE 802.11 Wireless Management
  ▾ Fixed parameters (12 bytes)
      Timestamp: 174368665986
      Beacon Interval: 0.102400 [Seconds]
    ▸ Capabilities Information: 0x0601
  ▾ Tagged parameters (119 bytes)
    ▸ Tag: SSID parameter set: 30 Munroe St
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 6
    ▸ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▸ Tag: Country Information: Country Code US, Environment Indoor
    ▸ Tag: EDCA Parameter Set
    ▸ Tag: ERP Information
    ▸ Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [M
    ▸ Tag: Vendor Specific: Airgo Networks, Inc.
    ▸ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e2 9c   ·····X·· ········
0010  64 00 00 46 8d 2c d8 25  80 00 00 00 ff ff ff ff   d··F·,·% ········
0020  ff ff 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 50 e0   ·······Q ·····QP·
0030  82 b1 2e 99 28 00 00 00  64 00 01 06 00 0c 33 30   ·..·(··· d·····30
0040  20 4d 75 6e 72 6f 65 20  53 74 01 04 82 84 8b 96    Munroe  St······
0050  03 01 06 05 04 00 01 00  00 07 06 55 53 49 01 0b   ········ ···USI··
0060  1a 0c 12 0f 00 03 a4 00  00 27 a4 00 00 42 43 5e   ········ ·'···BC^
0070  00 62 32 2f 00 2a 01 00  32 08 8c 12 98 24 b0 48   ·b2/·*·· 2····$·H
0080  60 6c dd 15 00 0a f5 0a  02 e0 c0 00 03 01 03 05   `l······ ········
0090  0e 04 ff 00 03 00 11 01  01 dd 18 00 50 f2 02 01   ········ ····P···
00a0  01 0f 00 03 a4 00 00 27  a4 00 00 42 43 5e 00 62   ·······' ···BC^·b
00b0  32 2f 00 8d 2c d8 25                               2/··,·%

No.: 1745 · Time: 49.644710 · Source: Cisco-Li_f7:1d:51 · Desti…rame, SN=3589, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
```

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

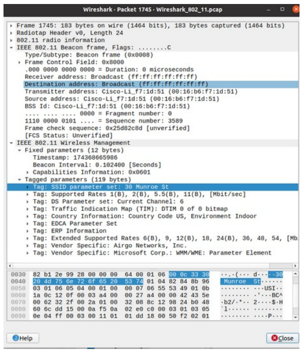
   - Source MAC addresses for the beacon frame from 30 Munroe St = 00:16:b6:f7:1d:51.



```
▸ Frame 1745: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
▸ Radiotap Header v0, Length 24
▸ 802.11 radio information
▾ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  ▸ Frame Control Field: 0x8000
    .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 = Fragment number: 0
    1110 0000 0101 .... = Sequence number: 3589
    Frame check sequence: 0x25d82c8d [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 Wireless Management
  ▾ Fixed parameters (12 bytes)
      Timestamp: 174368665986
      Beacon Interval: 0.102400 [Seconds]
    ▸ Capabilities Information: 0x0601
  ▾ Tagged parameters (119 bytes)
    ▸ Tag: SSID parameter set: 30 Munroe St
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 6
    ▸ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▸ Tag: Country Information: Country Code US, Environment Indoor
    ▸ Tag: EDCA Parameter Set
    ▸ Tag: ERP Information
    ▸ Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [M

0030  82 b1 2e 99 28 00 00 00  64 00 01 06 00 0c 33 30   ·..·(··· d·····30
0040  20 4d 75 6e 72 6f 65 20  53 74 01 04 82 84 8b 96    Munroe  St······
0050  03 01 06 05 04 00 01 00  00 07 06 55 53 49 01 0b   ········ ···USI··
0060  1a 0c 12 0f 00 03 a4 00  00 27 a4 00 00 42 43 5e   ········ ·'···BC^
0070  00 62 32 2f 00 2a 01 00  32 08 8c 12 98 24 b0 48   ·b2/·*·· 2····$·H
0080  60 6c dd 15 00 0a f5 0a  02 e0 c0 00 03 01 03 05   `l······ ········
0090  0e 04 ff 00 03 00 11 01  01 dd 18 00 50 f2 02 01   ········ ····P···
00a0  01 0f 00 03 a4 00 00 27  a4 00 00 42 43 5e 00 62   ·······' ···BC^·b
00b0  32 2f 00 8d 2c d8 25                               2/··,·%
```

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

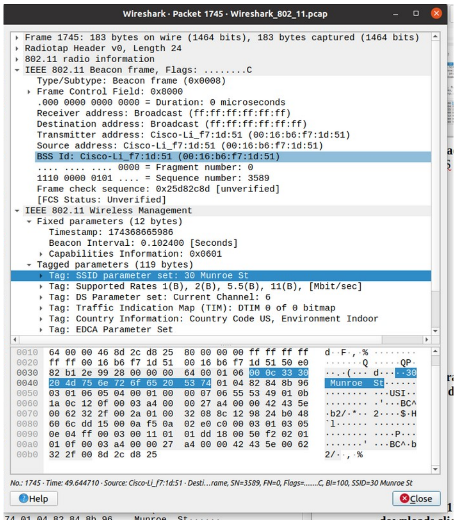
   - Destination MAC address for beacon frame from 30 Monroe St = ff:ff:ff:ff:ff:ff .



```
▸ Frame 1745: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
▸ Radiotap Header v0, Length 24
▸ 802.11 radio information
▾ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  ▸ Frame Control Field: 0x8000
    .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 = Fragment number: 0
    1110 0000 0101 .... = Sequence number: 3589
    Frame check sequence: 0x25d82c8d [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 Wireless Management
  ▾ Fixed parameters (12 bytes)
      Timestamp: 174368665986
      Beacon Interval: 0.102400 [Seconds]
    ▸ Capabilities Information: 0x0601
  ▾ Tagged parameters (119 bytes)
    ▸ Tag: SSID parameter set: 30 Munroe St
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 6
    ▸ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▸ Tag: Country Information: Country Code US, Environment Indoor
    ▸ Tag: EDCA Parameter Set
    ▸ Tag: ERP Information
    ▸ Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mb
    ▸ Tag: Vendor Specific: Airgo Networks, Inc.
    ▸ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

0030  82 b1 2e 99 28 00 00 00  64 00 01 06 00 0c 33 30   ···.(··· d·····30
0040  20 4d 75 6e 72 6f 65 20  53 74 01 04 82 84 8b 96    Munroe  St······
0050  03 01 06 05 04 00 01 00  00 07 06 55 53 49 01 0b   ········ ···USI··
0060  1a 0c 12 0f 00 03 a4 00  00 27 a4 00 00 42 43 5e   ········ ·'···BC^
0070  00 62 32 2f 00 2a 01 00  32 08 8c 12 98 24 b0 48   ·b2/·*·· 2····$·H
0080  60 6c dd 15 00 0a f5 0a  02 e0 c0 00 03 01 03 05   `l······ ········
0090  0e 04 ff 00 03 00 11 01  01 dd 18 00 50 f2 02 01   ········ ····P···
```

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

   - The BSS id for the beacon frame from 30 Munroe St = 00:16:b6:f7:1d:51.

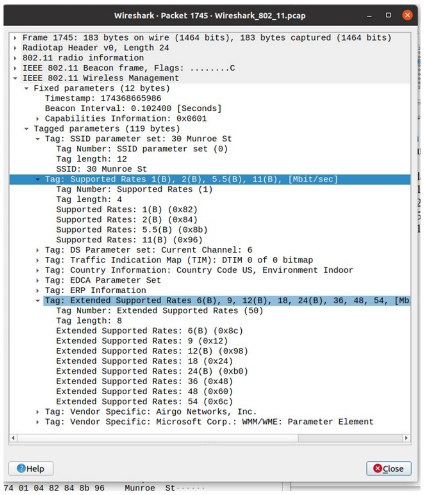


```
▸ Frame 1745: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
▸ Radiotap Header v0, Length 24
▸ 802.11 radio information
▾ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  ▸ Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    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 = Fragment number: 0
    1110 0000 0101 .... = Sequence number: 3589
    Frame check sequence: 0x25d82c8d [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 Wireless Management
  ▾ Fixed parameters (12 bytes)
      Timestamp: 174368665986
      Beacon Interval: 0.102400 [Seconds]
    ▸ Capabilities Information: 0x0601
  ▾ Tagged parameters (119 bytes)
    ▸ Tag: SSID parameter set: 30 Munroe St
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 6
    ▸ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▸ Tag: Country Information: Country Code US, Environment Indoor
    ▸ Tag: EDCA Parameter Set

0010  64 00 00 46 8d 2c d8 25  80 00 00 00 ff ff ff ff   d··F·,·% ········
0020  ff ff 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 50 e0   ·······Q ·····QP·
0030  82 b1 2e 99 28 00 00 00  64 00 01 06 00 0c 33 30   ···.(··· d·····30
0040  20 4d 75 6e 72 6f 65 20  53 74 01 04 82 84 8b 96    Munroe  St······
0050  03 01 06 05 04 00 01 00  00 07 06 55 53 49 01 0b   ········ ···USI··
0060  1a 0c 12 0f 00 03 a4 00  00 27 a4 00 00 42 43 5e   ········ ·'···BC^
0070  00 62 32 2f 00 2a 01 00  32 08 8c 12 98 24 b0 48   ·b2/·*·· 2····$·H
0080  60 6c dd 15 00 0a f5 0a  02 e0 c0 00 03 01 03 05   `l······ ········
0090  0e 04 ff 00 03 00 11 01  01 dd 18 00 50 f2 02 01   ········ ····P···
00a0  01 0f 00 03 a4 00 00 27  a4 00 00 42 43 5e 00 62   ·······' ···BC^·b
00b0  32 2f 00 8d 2c d8 25                               2/··,·%

No.: 1745 · Time: 49.644710 · Source: Cisco-Li_f7:1d:51 · Desti...rame, SN=3589, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
```

5. **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?**

   - Four data rates:
     1) 1(B) (0x82)
     2) 2(B) (0x84)
     3) 5.5(B) (0x8b)
     4) 11(B) (0x96)

   - Eight additional 'extended supported rates':
     1) 6(B)
     2) 9
     3) 12(B)
     4) 18
     5) 24(B)
     6) 36
     7) 48
     8) 54



```
▸ Frame 1745: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
▸ Radiotap Header v0, Length 24
▸ 802.11 radio information
▸ IEEE 802.11 Beacon frame, Flags: ........C
▾ IEEE 802.11 Wireless Management
  ▾ Fixed parameters (12 bytes)
      Timestamp: 174368665986
      Beacon Interval: 0.102400 [Seconds]
    ▸ Capabilities Information: 0x0601
  ▾ Tagged parameters (119 bytes)
    ▾ Tag: SSID parameter set: 30 Munroe St
        Tag Number: SSID parameter set (0)
        Tag length: 12
        SSID: 30 Munroe St
    ▾ 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)
    ▸ Tag: DS Parameter set: Current Channel: 6
    ▸ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▸ Tag: Country Information: Country Code US, Environment Indoor
    ▸ Tag: EDCA Parameter Set
    ▸ Tag: ERP Information
    ▾ Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mb
        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)
    ▸ Tag: Vendor Specific: Airgo Networks, Inc.
    ▸ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

2. Data Transfer

6. **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?**

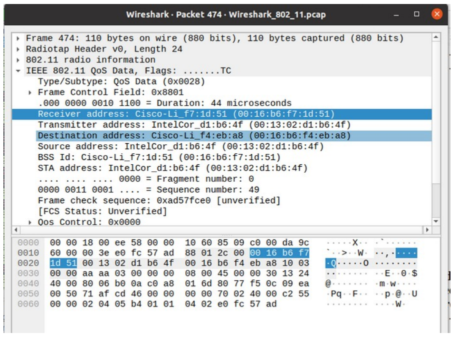
   - Three MAC address fields:

   1) Receiver address - 00:16:b6:f7:1d:51
   2) Transmitter address - 00:13:02:d1:b6:4f
   3) Destination address – 00:16:b6:f4:eb:a8

   - Wireless host address is the Transmitter address, **00:13:02:d1:b6:4f.**
   - Access point address is the Receiver address, **00:16:b6:f7:1d:51**.
   - First-hop router is the Destination address, **00:16:b6:f4:eb:a8**.

   - IP address of wireless host sending TCP segment = **192.168.1.109**
   - IP address of destination = **128.119.245.12**

SYN packet



Wireshark · Packet 474 · Wireshark_802_11.pcap

```
▸ Frame 474: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
▸ Radiotap Header v0, Length 24
▸ 802.11 radio information
▾ 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

0000  00 00 18 00 ee 58 00 00  10 60 85 09 c0 00 da 9c   ·····X·· ·`······
0010  60 00 00 3e e0 fc 57 ad  88 01 2c 00 00 16 b6 f7   `··>··W· ··,·····
0020  1d 51 00 13 02 d1 b6 4f  00 16 b6 f4 eb a8 10 03   ·Q·····O ········
0030  00 00 aa aa 03 00 00 00  08 00 45 00 00 30 13 24   ········ ··E··0·$
0040  40 00 80 06 b0 0a c0 a8  01 6d 80 77 f5 0c 09 ea   @······· ·m·w····
0050  00 50 71 af cd 46 00 00  00 00 70 02 40 00 c2 55   ·Pq··F·· ··p·@··U
0060  00 00 02 04 05 b4 01 01  04 02 e0 fc 57 ad         ········ ····W·
```

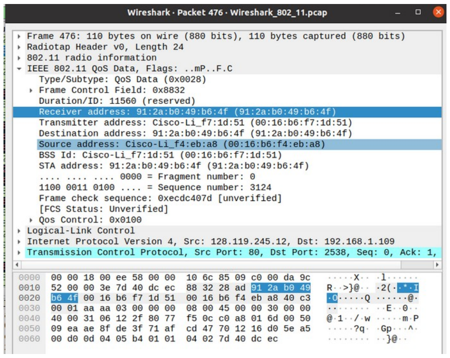
7. **Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router?**

   -Three MAC address fields:

   1) Receiver address - **91:2a:b0:49:b6:4f**
   2) Transmitter address **- 00:16:b6:f7:1d:51**
   3) Source address **– 00:16:b6:f4:eb:a8**

   - Wireless host address is the Transmitter address, **00:16:b6:f7:1d:51**
   - Access point address is the Receiver address, **91:2a:b0:49:b6:4f**
   - First-hop router is the Destination address, **00:16:b6:f4:eb:a8**

SYN-ACK packet



Wireshark · Packet 476 · Wireshark_802_11.pcap

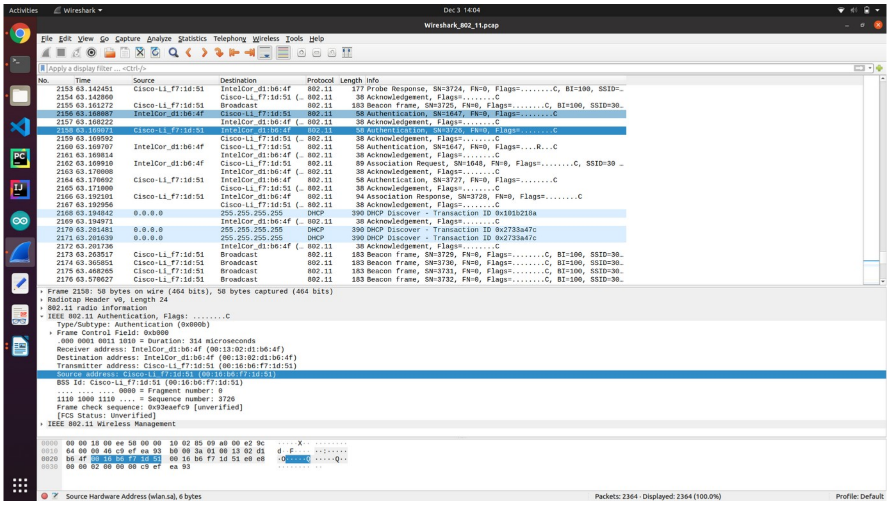
```
▸ Frame 476: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
▸ Radiotap Header v0, Length 24
▸ 802.11 radio information
▾ IEEE 802.11 QoS Data, Flags: ..mP..F.C
    Type/Subtype: QoS Data (0x0028)
  ▸ Frame Control Field: 0x8832
    Duration/ID: 11560 (reserved)
    Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    .... .... .... 0000 = Fragment number: 0
    1100 0011 0100 .... = Sequence number: 3124
    Frame check sequence: 0xecdc407d [unverified]
    [FCS Status: Unverified]
  ▸ Qos Control: 0x0100
▸ Logical-Link Control
▸ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.109
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 2538, Seq: 0, Ack: 1,

0000  00 00 18 00 ee 58 00 00  10 6c 85 09 c0 00 da 9c   ·····X·· ·l······
0010  52 00 00 3e 7d 40 dc ec  88 32 28 ad 91 2a b0 49   R··>}@·· ·2(··*·I
0020  b6 4f 00 16 b6 f7 1d 51  00 16 b6 f4 eb a8 40 c3   ·O·····Q ······@·
0030  00 01 aa aa 03 00 00 00  08 00 45 00 00 30 00 00   ········ ··E··0··
0040  40 00 31 06 12 2f 80 77  f5 0c c0 a8 01 6d 00 50   @·1··/·w ·····m·P
0050  09 ea ae 8f de 3f 71 af  cd 47 70 12 16 d0 5e a5   ·····?q· ·Gp···^·
0060  00 d0 0d 04 05 b4 01 01  04 02 7d 40 dc ec         ········ ··}@··
```

3. Association/Disassociation

8. **You can see The first AUTHENTICATION from the host to the AP is sent at t = 49.638857. There is not any reply from the *linksys_ses_24086* AP. This is probably because the AP is configured to require a key when associating with that AP, so the AP is likely ignoring (i.e., not responding to) requests for open access. 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 == 11and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the AUTHENTICATION frames in this trace for this wireless host.)**

   - There is an AUTHENTICATION frame sent from host (00:13:02:d1:b6:4f) to AP (00:16:b7:f7:1d:51) when the time is 63.168087. The AUTHENTICATION response is sent from AP to host at time 63.169071.

   Time taken to respond = 0.000984 seconds.


Activities
Wireshark
Dec 3 14:04
Wireshark_802_11.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.    Time       Source              Destination          Protocol Length Info
  2153 63.142451  Cisco-Li_f7:1d:51   IntelCor_d1:b6:4f      802.11   177 Probe Response, SN=3724, FN=0, Flags=........C, BI=100, SSID=…
  2154 63.142860                      Cisco-Li_f7:1d:51 (…   802.11    38 Acknowledgement, Flags=........C
  2155 63.161272  Cisco-Li_f7:1d:51   Broadcast              802.11   183 Beacon frame, SN=3725, FN=0, Flags=........C, BI=100, SSID=30…
  2156 63.168087  IntelCor_d1:b6:4f   Cisco-Li_f7:1d:51      802.11    58 Authentication, SN=1647, FN=0, Flags=........C
  2157 63.168222                      IntelCor_d1:b6:4f (…   802.11    38 Acknowledgement, Flags=........C
  2158 63.169071  Cisco-Li_f7:1d:51   IntelCor_d1:b6:4f      802.11    58 Authentication, SN=3726, FN=0, Flags=........C
  2159 63.169592                      Cisco-Li_f7:1d:51 (…   802.11    38 Acknowledgement, Flags=........C
  2160 63.169707  IntelCor_d1:b6:4f   Cisco-Li_f7:1d:51      802.11    58 Authentication, SN=1647, FN=0, Flags=....R...C
  2161 63.169814                      IntelCor_d1:b6:4f (…   802.11    38 Acknowledgement, Flags=........C
  2162 63.169910  IntelCor_d1:b6:4f   Cisco-Li_f7:1d:51      802.11    89 Association Request, SN=1648, FN=0, Flags=........C, SSID=30 …
  2163 63.170008                      IntelCor_d1:b6:4f (…   802.11    38 Acknowledgement, Flags=........C
  2164 63.170692  Cisco-Li_f7:1d:51   IntelCor_d1:b6:4f      802.11    58 Authentication, SN=3727, FN=0, Flags=........C
  2165 63.171000                      Cisco-Li_f7:1d:51 (…   802.11    38 Acknowledgement, Flags=........C
  2166 63.192101  Cisco-Li_f7:1d:51   IntelCor_d1:b6:4f      802.11    94 Association Response, SN=3728, FN=0, Flags=........C
  2167 63.192956                      Cisco-Li_f7:1d:51 (…   802.11    38 Acknowledgement, Flags=........C
  2168 63.194842  0.0.0.0             255.255.255.255        DHCP     390 DHCP Discover - Transaction ID 0x101b218a
  2169 63.194971                      IntelCor_d1:b6:4f (…   802.11    38 Acknowledgement, Flags=........C
  2170 63.201481  0.0.0.0             255.255.255.255        DHCP     390 DHCP Discover - Transaction ID 0x2733a47c
  2171 63.201639  0.0.0.0             255.255.255.255        DHCP     390 DHCP Discover - Transaction ID 0x2733a47c
  2172 63.201736                      IntelCor_d1:b6:4f (…   802.11    38 Acknowledgement, Flags=........C
  2173 63.263517  Cisco-Li_f7:1d:51   Broadcast              802.11   183 Beacon frame, SN=3729, FN=0, Flags=........C, BI=100, SSID=30…
  2174 63.365851  Cisco-Li_f7:1d:51   Broadcast              802.11   183 Beacon frame, SN=3730, FN=0, Flags=........C, BI=100, SSID=30…
  2175 63.468265  Cisco-Li_f7:1d:51   Broadcast              802.11   183 Beacon frame, SN=3731, FN=0, Flags=........C, BI=100, SSID=30…
  2176 63.570627  Cisco-Li_f7:1d:51   Broadcast              802.11   183 Beacon frame, SN=3732, FN=0, Flags=........C, BI=100, SSID=30…
```

```
▸ Frame 2158: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
▸ Radiotap Header v0, Length 24
▸ 802.11 radio information
▾ IEEE 802.11 Authentication, Flags: ........C
    Type/Subtype: Authentication (0x000b)
  ▸ Frame Control Field: 0xb000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    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 = Fragment number: 0
    1110 1000 1110 .... = Sequence number: 3726
    Frame check sequence: 0x93eaefc9 [unverified]
    [FCS Status: Unverified]
▸ IEEE 802.11 Wireless Management
```

```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e2 9c   ·····X·· ········
0010  64 00 00 46 c9 ef ea 93  b0 00 3a 01 00 13 02 d1   d··F···· ··:·····
0020  b6 4f 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 e0 e8   ·O·····Q ·····Q··
0030  00 00 02 00 00 00 c9 ef  ea 93                     ········ ··
```

Source Hardware Address (wlan.sa), 6 bytes   Packets: 2364 · Displayed: 2364 (100.0%)   Profile: Default

9. **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 REQUEST and ASSOCIATE RESPONSE frames for this trace.)**

   -

4. Other Frame types

10. **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 address = **00:12:f0:1f:57:13**
    - Receiver address = **ff:ff:ff:ff:ff:ff**
    - BSS Id addresses = **ff:ff:ff:ff:ff:ff**

    - The purpose of them two frame types is to broadcast a scan for an access point from the host. The response is used to respond to the host from the access point.