ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC BÁCH KHOA

KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH

BÁO CÁO

MẠNG MÁY TÍNH THỰC HÀNH (CO3094)

LAB 7

GV hướng dẫn: Bùi Xuân Giang

SV thực hiện: Trịnh Thị Mỹ Lệ

Thành phố Hồ Chí Minh, Tháng 4 năm 2025

1. Question 1

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

Answer: SSIDs are 30 Munroe St and linsys_SES_24086

2. Question 2

Question: 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?

Answer: They are both 0.1024s

3. Question 3

Question: What (in hexadecimal notation) is the source MAC address on the beacon frame from 30 Munroe St?

Answer: The source MAC on the beacon feacom frame from 30 Munroe is 00:16:b6:f7:1d:51

4. Question 4

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

Answer: The destination MAC is for broadcast. The destination MAC is ff:ff:ff:ff:ff:ff

5. Question 5

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

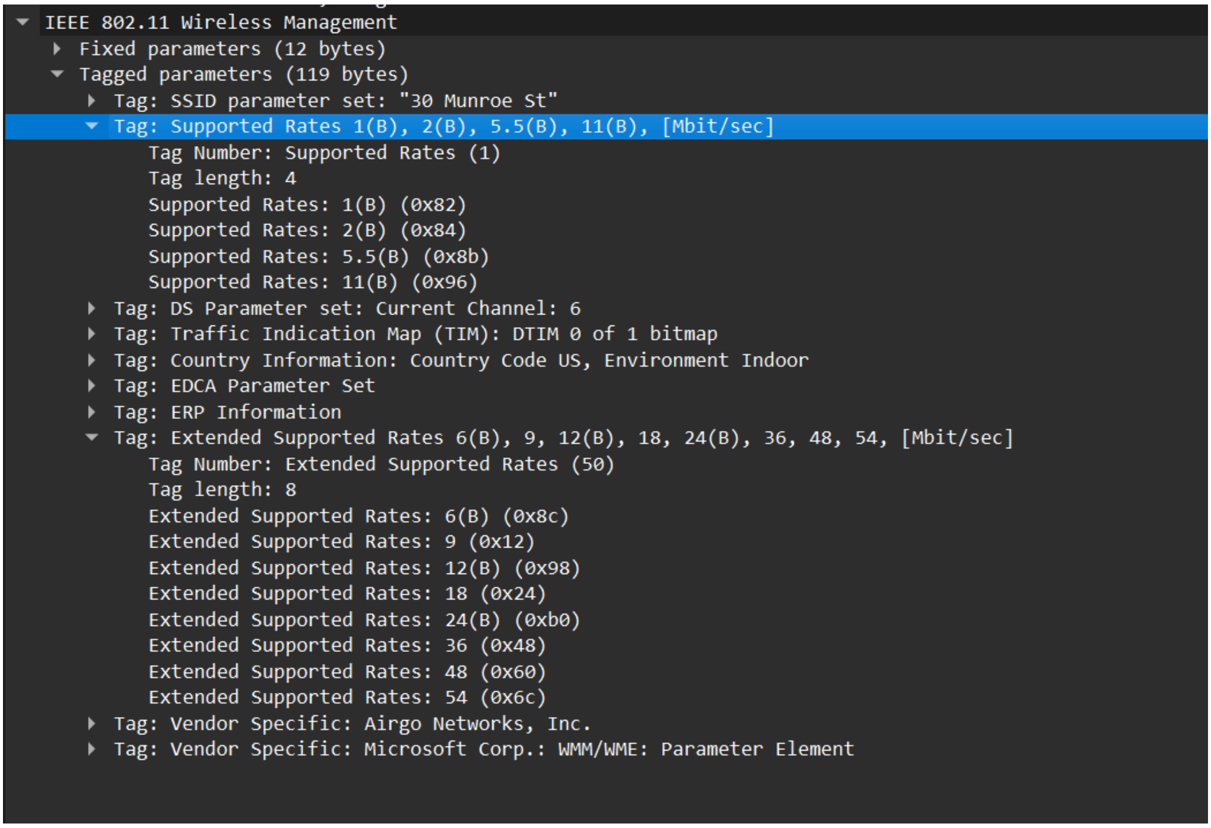
Answer: The MAC BSS is on the beacon frame from 30 Munroe St is 00:16:b6:f7:1d:51

6. Question 6

Question: 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?

Answer:

- support rates 1.0 / 2.0 / 5.5 / 11.0 Mbps
- extended rates 6.0 / 9.0 / 12.0 / 18.0/ 24.0/ 36.0/ 48.0/ 54.0 Mbps

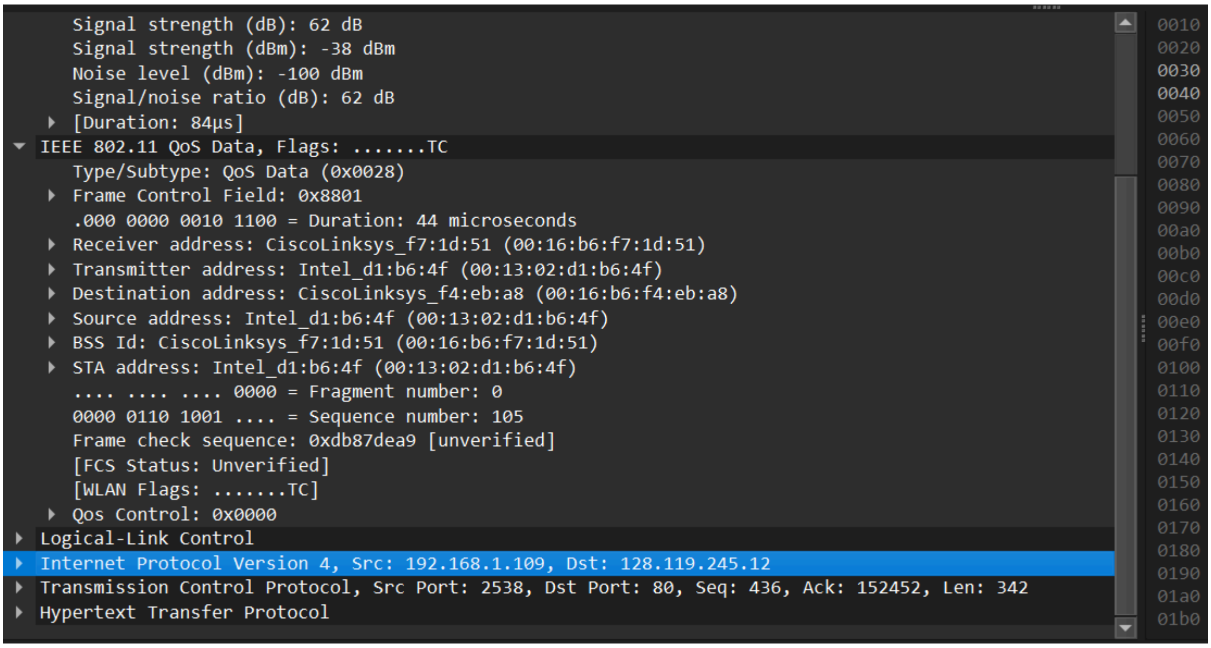


```
▾ IEEE 802.11 Wireless Management
   ▸ Fixed parameters (12 bytes)
   ▾ Tagged parameters (119 bytes)
      ▸ Tag: SSID parameter set: "30 Munroe St"
      ▾ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
           Tag Number: Supported Rates (1)
           Tag length: 4
           Supported 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 1 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, [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)
      ▸ Tag: Vendor Specific: Airgo Networks, Inc.
      ▸ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

7. Question 7

Question: 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.

Answer: Those MAC addresses are BSSid, source address and destination. 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. 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.



```
    Signal strength (dB): 62 dB
    Signal strength (dBm): -38 dBm
    Noise level (dBm): -100 dBm
    Signal/noise ratio (dB): 62 dB
  ▸ [Duration: 84µs]
▾ 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: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
  ▸ Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
  ▸ 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: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
  ▸ STA address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    .... .... .... 0000 = Fragment number: 0
    0000 0110 1001 .... = Sequence number: 105
    Frame check sequence: 0xdb87dea9 [unverified]
    [FCS Status: Unverified]
    [WLAN Flags: .......TC]
  ▸ Qos Control: 0x0000
▸ Logical-Link Control
▸ Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
▸ Transmission Control Protocol, Src Port: 2538, Dst Port: 80, Seq: 436, Ack: 152452, Len: 342
▸ Hypertext Transfer Protocol
```

```
0010
0020
0030
0040
0050
0060
0070
0080
0090
00a0
00b0
00c0
00d0
00e0
00f0
0100
0110
0120
0130
0140
0150
0160
0170
0180
0190
01a0
01b0
```

8. Question 8

Question: 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?

Answer: Three MAC address fields in the 802.11 frame are BSS id: 00:16:b6:f7:1d:51, Destination: 00:13:02:d1:b6:4f and source address: 00:16:b6:f4:eb:a8. The MAC corresponds to the host is 00:13:02:d1:b6:4f (destination). The MAC corresponds to the first hop is 00:16:b6:f4:eb:a8 (Source). The sender MAC address in the frame does not correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram, because the TCP SYNACK's IP address is 128:199:245:12 but the destination IP address is 192.168.1.109

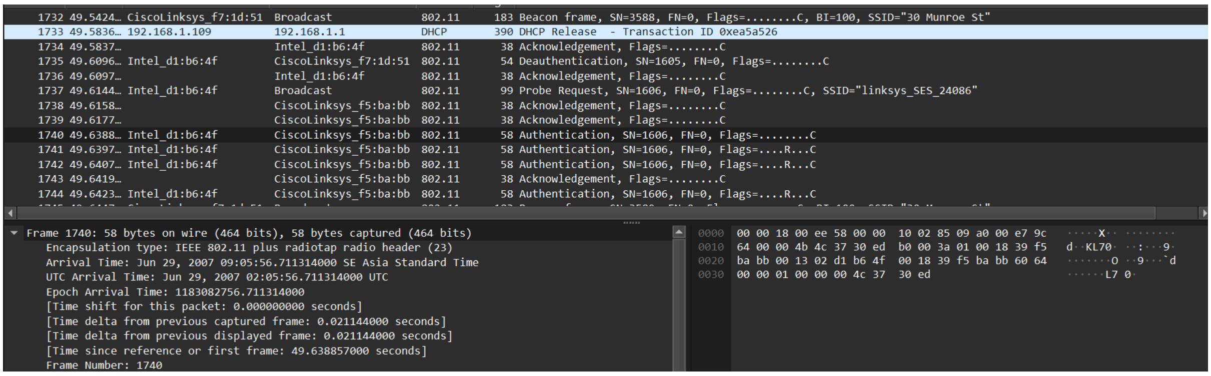
9. Question 9

Question: 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?

Answer:

1. A DHCP is sent to 192.168.1.1

2. The host sends a DEAUTHENTICATION frame after 0.02s



```
1732 49.5424… CiscoLinksys_f7:1d:51  Broadcast              802.11     183 Beacon frame, SN=3588, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
1733 49.5836… 192.168.1.109          192.168.1.1            DHCP       390 DHCP Release  - Transaction ID 0xea5a526
1734 49.5837…                        Intel_d1:b6:4f         802.11      38 Acknowledgement, Flags=........C
1735 49.6096… Intel_d1:b6:4f         CiscoLinksys_f7:1d:51  802.11      54 Deauthentication, SN=1605, FN=0, Flags=........C
1736 49.6097…                        Intel_d1:b6:4f         802.11      38 Acknowledgement, Flags=........C
1737 49.6144… Intel_d1:b6:4f         Broadcast              802.11      99 Probe Request, SN=1606, FN=0, Flags=........C, SSID="linksys_SES_24086"
1738 49.6158…                        CiscoLinksys_f5:ba:bb  802.11      38 Acknowledgement, Flags=........C
1739 49.6177…                        CiscoLinksys_f5:ba:bb  802.11      38 Acknowledgement, Flags=........C
1740 49.6388… Intel_d1:b6:4f         CiscoLinksys_f5:ba:bb  802.11      58 Authentication, SN=1606, FN=0, Flags=........C
1741 49.6397… Intel_d1:b6:4f         CiscoLinksys_f5:ba:bb  802.11      58 Authentication, SN=1606, FN=0, Flags=....R...C
1742 49.6407… Intel_d1:b6:4f         CiscoLinksys_f5:ba:bb  802.11      58 Authentication, SN=1606, FN=0, Flags=....R...C
1743 49.6419…                        CiscoLinksys_f5:ba:bb  802.11      38 Acknowledgement, Flags=........C
1744 49.6423… Intel_d1:b6:4f         CiscoLinksys_f5:ba:bb  802.11      58 Authentication, SN=1606, FN=0, Flags=....R...C

Frame 1740: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
    Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
    Arrival Time: Jun 29, 2007 09:05:56.711314000 SE Asia Standard Time
    UTC Arrival Time: Jun 29, 2007 02:05:56.711314000 UTC
    Epoch Arrival Time: 1183082756.711314000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.021144000 seconds]
    [Time delta from previous displayed frame: 0.021144000 seconds]
    [Time since reference or first frame: 49.638857000 seconds]
    Frame Number: 1740

0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e7 9c   ·····X·· ········
0010  64 00 00 4b 4c 37 30 ed  b0 00 3a 01 00 18 39 f5   d··KL70· ··:···9·
0020  ba bb 00 13 02 d1 b6 4f  00 18 39 f5 ba bb 60 64   ·······O ··9···`d
0030  00 00 01 00 00 00 4c 37  30 ed                     ······L7 0·
```

10. Question 10

Question: 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?

Answer: There are 17 AUTHENTICATION messages from the wireless host to the linksys_ses_24086 AP

11. Question 11

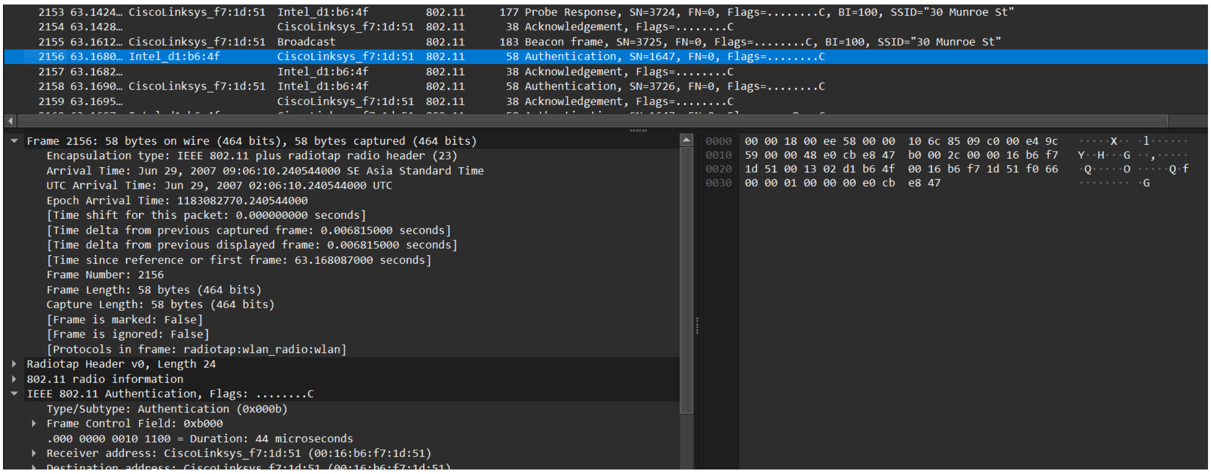
Question: Does the host want the authentication to require a key or be open?

Answer: Yes

12. Question 12

Question: Do you see a reply AUTHENTICATION from the linksys_ses_24086 AP in the trace?

Answer: No, there is no reply



```
2153 63.1424… CiscoLinksys_f7:1d:51 Intel_d1:b6:4f         802.11    177 Probe Response, SN=3724, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2154 63.1428…                       CiscoLinksys_f7:1d:51  802.11     38 Acknowledgement, Flags=........C
2155 63.1612… CiscoLinksys_f7:1d:51 Broadcast              802.11    183 Beacon frame, SN=3725, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2156 63.1680… Intel_d1:b6:4f        CiscoLinksys_f7:1d:51  802.11     58 Authentication, SN=1647, FN=0, Flags=........C
2157 63.1682…                       Intel_d1:b6:4f         802.11     38 Acknowledgement, Flags=........C
2158 63.1690… CiscoLinksys_f7:1d:51 Intel_d1:b6:4f         802.11     58 Authentication, SN=3726, FN=0, Flags=........C
2159 63.1695…                       CiscoLinksys_f7:1d:51  802.11     38 Acknowledgement, Flags=........C
```

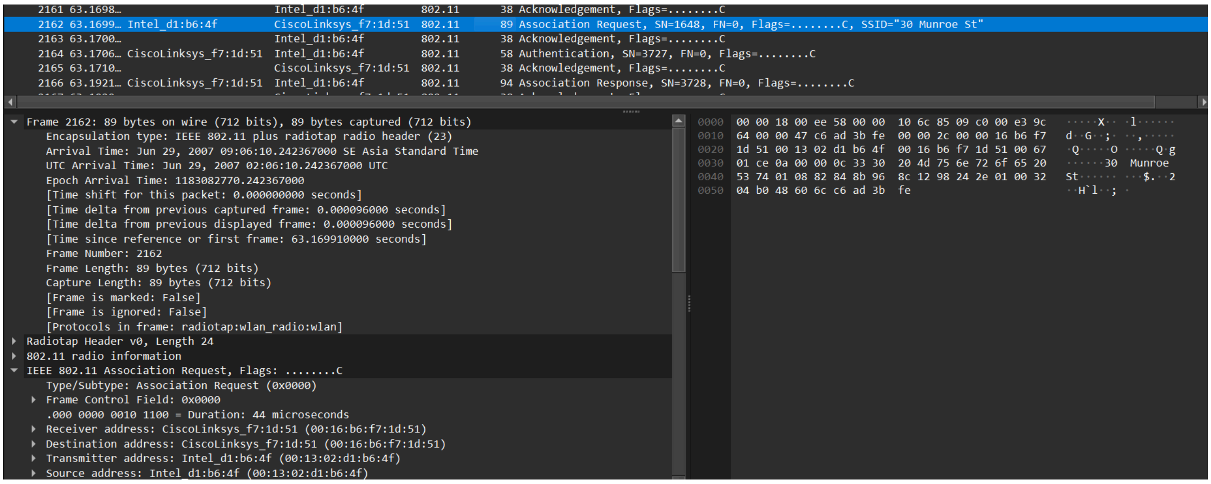
```
Frame 2156: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
   Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
   Arrival Time: Jun 29, 2007 09:06:10.240544000 SE Asia Standard Time
   UTC Arrival Time: Jun 29, 2007 02:06:10.240544000 UTC
   Epoch Arrival Time: 1183082770.240544000
   [Time shift for this packet: 0.000000000 seconds]
   [Time delta from previous captured frame: 0.006815000 seconds]
   [Time delta from previous displayed frame: 0.006815000 seconds]
   [Time since reference or first frame: 63.168087000 seconds]
   Frame Number: 2156
   Frame Length: 58 bytes (464 bits)
   Capture Length: 58 bytes (464 bits)
   [Frame is marked: False]
   [Frame is ignored: False]
   [Protocols in frame: radiotap:wlan_radio:wlan]
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Authentication, Flags: ........C
   Type/Subtype: Authentication (0x000b)
   Frame Control Field: 0xb000
   .000 0000 0010 1100 = Duration: 44 microseconds
   Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
```

```
0000  00 00 18 00 ee 58 00 00  10 6c 85 09 c0 00 e4 9c   ·····X·· ·l······
0010  59 00 00 48 e0 cb e8 47  b0 00 2c 00 00 16 b6 f7   Y··H···G ··,·····
0020  1d 51 00 13 02 d1 b6 4f  00 16 b6 f7 1d 51 f0 66   ·Q·····O ·····Q·f
0030  00 00 01 00 00 00 e0 cb  e8 47                     ········ ·G
```

13. Question 13

Question: 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?

Answer: There is an AUTHENTICATION frame from 00:13:02:d1:b6:4f to 00:16:b7:f7:1d:51 when t = 63.168087. The AUTHENTICATION sent back at t = 63.169071



```
2161 63.1698…                       Intel_d1:b6:4f         802.11     38 Acknowledgement, Flags=........C
2162 63.1699… Intel_d1:b6:4f        CiscoLinksys_f7:1d:51  802.11     89 Association Request, SN=1648, FN=0, Flags=........C, SSID="30 Munroe St"
2163 63.1700…                       Intel_d1:b6:4f         802.11     38 Acknowledgement, Flags=........C
2164 63.1706… CiscoLinksys_f7:1d:51 Intel_d1:b6:4f         802.11     58 Authentication, SN=3727, FN=0, Flags=........C
2165 63.1710…                       CiscoLinksys_f7:1d:51  802.11     38 Acknowledgement, Flags=........C
2166 63.1921… CiscoLinksys_f7:1d:51 Intel_d1:b6:4f         802.11     94 Association Response, SN=3728, FN=0, Flags=........C
```

```
Frame 2162: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
   Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
   Arrival Time: Jun 29, 2007 09:06:10.242367000 SE Asia Standard Time
   UTC Arrival Time: Jun 29, 2007 02:06:10.242367000 UTC
   Epoch Arrival Time: 1183082770.242367000
   [Time shift for this packet: 0.000000000 seconds]
   [Time delta from previous captured frame: 0.000096000 seconds]
   [Time delta from previous displayed frame: 0.000096000 seconds]
   [Time since reference or first frame: 63.169910000 seconds]
   Frame Number: 2162
   Frame Length: 89 bytes (712 bits)
   Capture Length: 89 bytes (712 bits)
   [Frame is marked: False]
   [Frame is ignored: False]
   [Protocols in frame: radiotap:wlan_radio:wlan]
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Association Request, Flags: ........C
   Type/Subtype: Association Request (0x0000)
   Frame Control Field: 0x0000
   .000 0000 0010 1100 = Duration: 44 microseconds
   Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
   Destination address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
   Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
   Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
```

```
0000  00 00 18 00 ee 58 00 00  10 6c 85 09 c0 00 e3 9c   ·····X·· ·l······
0010  64 00 00 47 c6 ad 3b fe  00 00 2c 00 00 16 b6 f7   d··G··;· ··,·····
0020  1d 51 00 13 02 d1 b6 4f  00 16 b6 f7 1d 51 00 67   ·Q·····O ·····Q·g
0030  01 ce 0a 00 00 0c 33 30  20 4d 75 6e 72 6f 65 20   ······30  Munroe
0040  53 74 01 08 82 84 8b 96  8c 12 98 24 2e 01 00 32   St······ ···$.··2
0050  04 b0 48 60 6c c6 ad 3b  fe                        ··H`l··; ·
```

14. Question 14

Question: 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?

Answer: ASSOCIATE REQUEST from host to the 30 Munroe St AP at t = 63.169910 and replied at t = 63.192101

15. Question 15

Question: What transmission rates is the host willing to use?

Answer: The possible rates are 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, 54 Mbps

16. Question 16

Question: What are the sender, receiver and BSS ID MAC addresses in these frames? What is the purpose of these two types of frames?

Answer: Probe request: Source: 00:12:f0:1f:57:13, destination: ff:ff:ff:ff:ff:ff, BSSID: ff:ff:ff:ff:ff:ff Probe response: Source: 00:16:b6:f7:1d:51, destination: 00:16:b6:f7:1d:51, BSSID: 00:16:b6:f7:1d:51 The probe request is a broadcast to scan for an access point from the host. The probe response is used to response the host from the access point