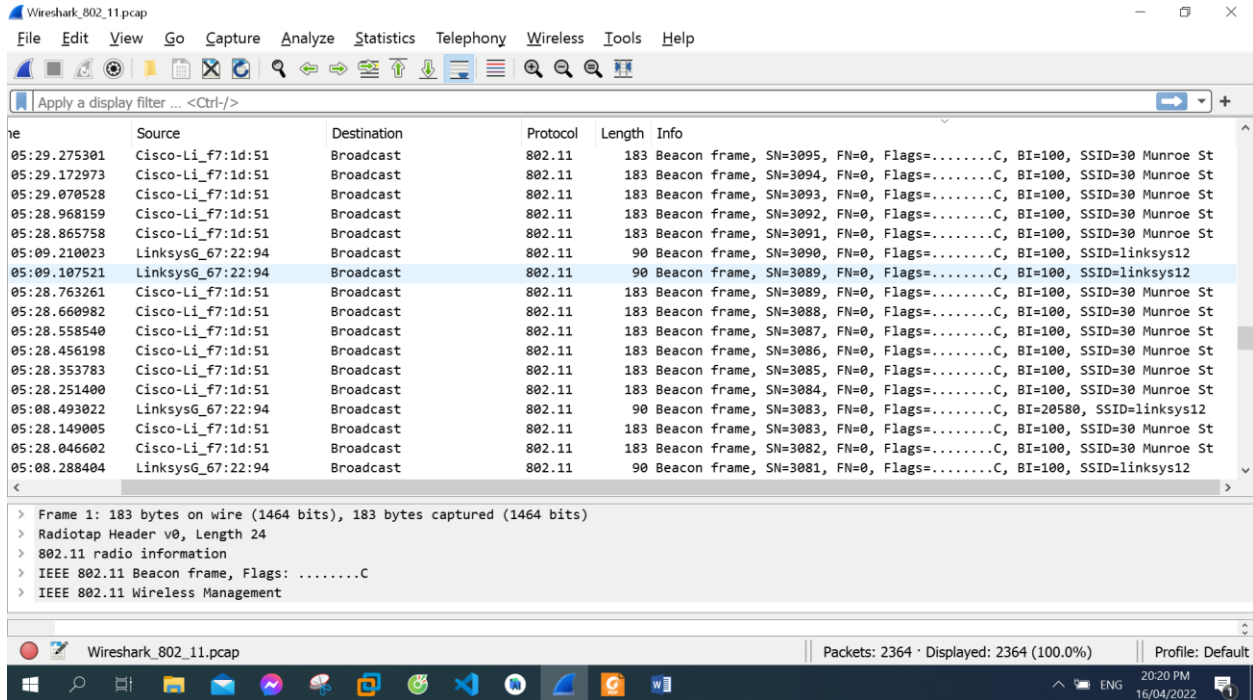


LAB 7: 802.11 WiFi

Name: Hồ Đức Trí

Student No: 1912288

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



“30 Munroe St” and “linksys12” are the SSIDs of the two access points that are issuing most of the beacon frames in this trace

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).

Wireshark_802.11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Time	Source	Destination	Protocol	Length	Info
05:29.275301	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3095, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
05:29.172973	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3094, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
05:29.070528	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3093, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
05:28.968159	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3092, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
05:28.865758	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3091, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
05:09.210023	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3090, FN=0, Flags=.....C, BI=100, SSID=linksys12
05:09.107521	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3089, FN=0, Flags=.....C, BI=100, SSID=linksys12
05:28.763261	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3089, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
05:28.660982	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3088, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
05:28.558540	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3087, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
05:28.456198	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3086, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
05:28.353783	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3085, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

> Frame 41: 90 bytes on wire (720 bits), 90 bytes captured (720 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: 9534923469437
 - Beacon Interval: 0.102400 [Seconds]
 - Capabilities Information: 0x0011
- Tagged parameters (26 bytes)

Wireshark_802.11.pcap | Packets: 2364 · Displayed: 2364 (100.0%) | Profile: Default

20:23 PM 16/04/2022

Wireshark_802.11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Time	Source	Destination	Protocol	Length	Info
05:29.275301	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3095, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
05:29.172973	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3094, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
05:29.070528	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3093, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
05:28.968159	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3092, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
05:28.865758	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3091, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
05:09.210023	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3090, FN=0, Flags=.....C, BI=100, SSID=linksys12
05:09.107521	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3089, FN=0, Flags=.....C, BI=100, SSID=linksys12
05:28.763261	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3089, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
05:28.660982	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3088, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
05:28.558540	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3087, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
05:28.456198	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3086, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
05:28.353783	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3085, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

> Frame 415: 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

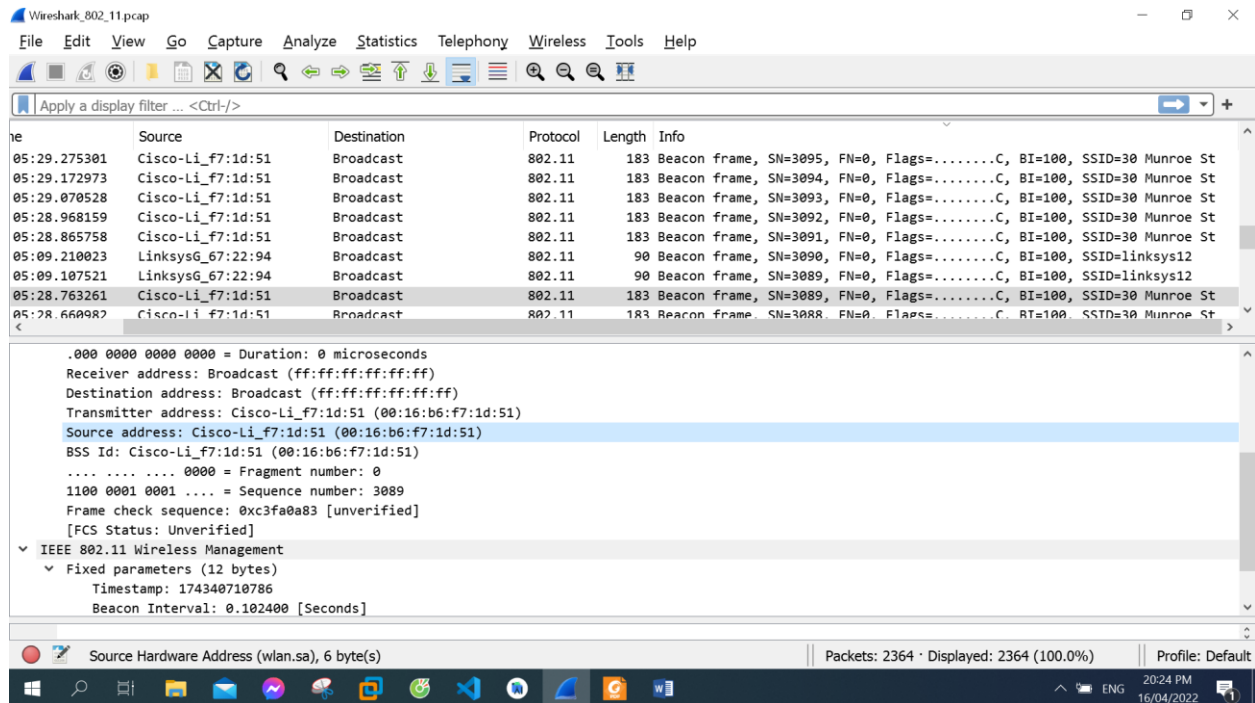
- Fixed parameters (12 bytes)
 - Timestamp: 174340710786
 - Beacon Interval: 0.102400 [Seconds]
 - Capabilities Information: 0x0011
- Tagged parameters (119 bytes)

Wireshark_802.11.pcap | Packets: 2364 · Displayed: 2364 (100.0%) | Profile: Default

20:23 PM 16/04/2022

They are both 0.102400 seconds

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



The source MAC address on the beacon frame from 30 Munroe St: 00:16:b6:f7:1d:51

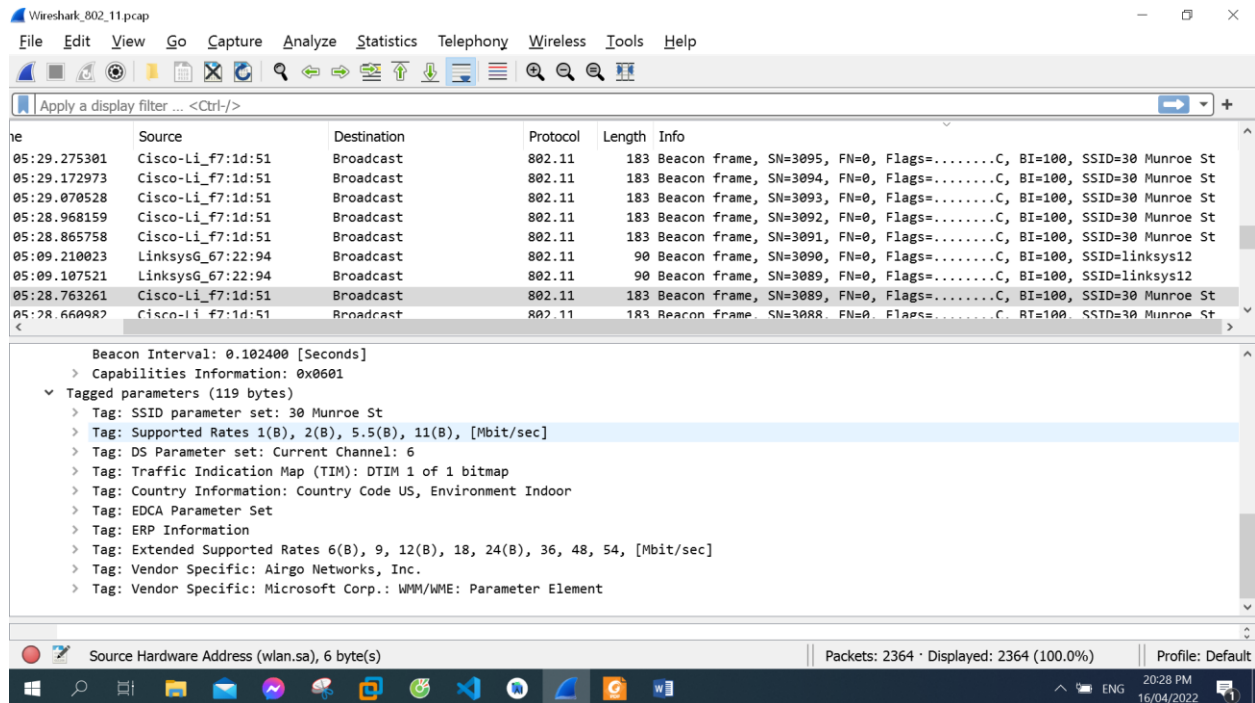
4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St?

The destination MAC address on the beacon frame from 30 Munroe St: ff:ff:ff:ff:ff:ff

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

The MAC BSS id on the beacon frame from 30 Munroe St: 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?



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

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	24.811093	192.168.1.109	128.119.245.12	TCP	110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
475	24.811231		IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)	802.11	38 Acknowledgement, Flags=.....C
476	24.827751	128.119.245.12	192.168.1.109	TCP	110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1
477	24.827922		Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)	802.11	38 Acknowledgement, Flags=.....C
478	24.828024	192.168.1.109	128.119.245.12	TCP	102 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0


```

> 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
  > 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: 0, Len: 0

```

Those MAC addresses are BSS ID, source and destination.

The MAC address in this frame corresponds to the wireless host: 00:13:02:d1:b6:4f

The MAC address in this frame corresponds to the access point: 00:16:b6:f4:eb:a8

The MAC address in this frame corresponds to the first-hop router: 00:16:b6:f7:1d:51

The IP address of the wireless host sending this TCP segment: 192.168.1.109

The destination IP address: 128.199.245.12

This corresponds to the server `gaia.cs.umass.edu`. The destination MAC address of the frame containing the SYN is different from the destination IP address of the IP packet contained within this frame

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?

476	24.827751	128.119.245.12	192.168.1.109	TCP	110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1
477	24.827922		Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)	802.11	38 Acknowledgement, Flags=.....C
478	24.828024	192.168.1.109	128.119.245.12	TCP	102 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
479	24.828140		IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)	802.11	38 Acknowledgement, Flags=.....C
480	24.828253	192.168.1.109	128.119.245.12	HTTP	537 GET /wireshark-labs/alice.txt HTTP/1.1

```

<
> 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: 0xecd407d [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, Len: 0

```

Those MAC addresses are BSSid, source address and destination.

The MAC address in this frame corresponds to the host: 91:2a:b0:49:b6:4f.

The MAC address in this frame corresponds to the access point: 00:16:b6:f7:1d:51.

The MAC address in this frame corresponds to the first-hop router: 00:16:b6:f4:eb:a8.

No, 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. 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? Looking at the 802.11 specification, is there another frame that you might have expected to see, but don't see here?

1733	49.583615	192.168.1.109	192.168.1.1	DHCP	390 DHCP Release - Transaction ID 0xea5a526
1734	49.583771		IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)	802.11	38 Acknowledgement, Flags=.....C
1735	49.609617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)	802.11	54 Deauthentication, SN=1605, FN=0, Flags=.....C
1736	49.609770		IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)	802.11	38 Acknowledgement, Flags=.....C
1737	49.614478	IntelCor_d1:b6:4f	Broadcast	802.11	99 Probe Request, SN=1606, FN=0, Flags=.....C, SS

```

<
> Frame 1733: 390 bytes on wire (3120 bits), 390 bytes captured (3120 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 1011 1000 .... = Sequence number: 184
    Frame check sequence: 0x90381791 [unverified]
    [FCS Status: Unverified]
  > QoS Control: 0x0000
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.1.109, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Release)

```


1735	49.609617	IntelCor_d1:b6:...	Cisco-Li_f7:1d:51	802.11	54 Deauthentication, SN=1605, FN=0, Flags=.....C
1736	49.609770	IntelCor_d1:b6:4f (00:...	IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)	802.11	38 Acknowledgement, Flags=.....C
1737	49.614478	IntelCor_d1:b6:...	Broadcast	802.11	99 Probe Request, SN=1606, FN=0, Flags=.....C, SSI

>	Frame 1735: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
>	Radiotap Header v0, Length 24
>	802.11 radio information
>	IEEE 802.11 Deauthentication, Flags:C
>	Type/Subtype: Deauthentication (0x000c)
>	Frame Control Field: 0xc000
>	.000 0000 0010 1100 = Duration: 44 microseconds
>	Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
>	Destination address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
>	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: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
> 0000 = Fragment number: 0
>	0110 0100 0101 = Sequence number: 1605
>	Frame check sequence: 0xb4a8b9c [unverified]
>	[FCS Status: Unverified]
>	IEEE 802.11 Wireless Management
>	Fixed parameters (2 bytes)

At t = 49.583615 a DHCP release is sent by the host to the DHCP server in the network that the host is leaving.

At t = 49.609617, the host sends a DEAUTHENTICATION frame.

One might have expected to see a DISASSOCIATION request to have been sent

10. Examine the trace file and look for AUTHENTICATION 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?

2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94 Association Response, SN=3728, FN=0, Flags=.....C
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=.....C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=.....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=.....R...C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=.....R...C
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=.....R...C
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=.....R...C
1821	53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1612, FN=0, Flags=.....R...C
1822	53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1612, FN=0, Flags=.....R...C
1921	57.889232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1619, FN=0, Flags=.....R...C
1922	57.890325	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1619, FN=0, Flags=.....R...C
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1619, FN=0, Flags=.....R...C
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1619, FN=0, Flags=.....R...C
2122	62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1644, FN=0, Flags=.....R...C
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1644, FN=0, Flags=.....R...C
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1644, FN=0, Flags=.....R...C
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58 Authentication, SN=1647, FN=0, Flags=.....R...C
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58 Authentication, SN=1647, FN=0, Flags=.....R...C
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58 Authentication, SN=3726, FN=0, Flags=.....R...C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58 Authentication, SN=3727, FN=0, Flags=.....R...C
1	0.000000	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100,

There are 15 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.

11. Does the host want the authentication to require a key or be open?

The host is requesting that the association be open

12. Do you see a reply AUTHENTICATION from the linksys_ses_24086 AP in the trace?

No, I do not see any reply AUTHENTICATION from the linksys_ses_24086 AP

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 AUTHENTICATION 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?

2155 63.161272	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=3725, FN=0, Flags=.....C, BI
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	IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) (RA)	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 (00:16:b6:f7:1d:51) (RA)	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 (00:13:02:d1:b6:4f) (RA)	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
2163 63.170008		IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) (RA)	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 (00:16:b6:f7:1d:51) (RA)	802.11	38 Acknowledgement, Flags=.....C

At t = 63.168087 there is an AUTHENTICATION frame from the host to the 30 Munroe St. AP

At t = 63.169071 there is a reply AUTHENTICATION sent from that AP to the host in reply.

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?

2159 63.169592		Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51) (RA)	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 (00:13:02:d1:b6:4f) (RA)	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,
2163 63.170008		IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) (RA)	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 (00:16:b6:f7:1d:51) (RA)	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 (00:16:b6:f7:1d:51) (RA)	802.11	38 Acknowledgement, Flags=.....C

At t = 63.169910 there is an ASSOCIATE REQUEST from host to the 30 Munroe St AP.

At t = 63.192101 the corresponding ASSOCIATE REPLY is sent.

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.

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 Munroe St
2163 63.170008		IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) (RA)	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
> Frame 2162: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) > Radiotap Header v0, Length 24 > 802.11 radio information > IEEE 802.11 Association Request, Flags:C > IEEE 802.11 Wireless Management > Fixed parameters (4 bytes) > Tagged parameters (33 bytes) > Tag: SSID parameter set: 30 Munroe St > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec] > Tag: QoS Capability > Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]				

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 (00:16:b6:f7:1d:51) (RA)	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 (00:13:02:d1:b6:4f) (RA)	802.11	38 Acknowledgement, Flags=.....C
> Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) > Radiotap Header v0, Length 24 > 802.11 radio information > IEEE 802.11 Association Response, Flags:C > IEEE 802.11 Wireless Management > Fixed parameters (6 bytes) > Tagged parameters (36 bytes) > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec] > Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec] > Tag: EDCA Parameter Set				

In the ASSOCIATION REQUEST frame the supported rates are advertised as 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, and 54 Mbps.

The same rates are advertised in the ASSOCIATION RESPONSE.

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).

50 2.297613	IntelCor_1f:57:13	Broadcast	802.11	79 Probe Request, SN=576, FN=0, Flags=.....C, SSID=Home WIFI
51 2.300697	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
52 2.302191	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2878, FN=0, Flags=.....R...C, BI=100, SSID=30 Munroe St
53 2.304063	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2878, FN=0, Flags=.....R...C, BI=100, SSID=30 Munroe St
54 2.305562	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2878, FN=0, Flags=.....R...C, BI=100, SSID=30 Munroe St
> Frame 50: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) > Radiotap Header v0, Length 24 > 802.11 radio information > IEEE 802.11 Probe Request, Flags:C Type/Subtype: Probe Request (0x0004) > Frame Control Field: 0x4000 .0000 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_1f:57:13 (00:12:f0:1f:57:13) Source address: IntelCor_1f:57:13 (00:12:f0:1f:57:13) BSS Id: Broadcast (ff:ff:ff:ff:ff:ff) 0000 = Fragment number: 0 0010 0100 0000 = Sequence number: 576 Frame check sequence: 0xa373c5ff [unverified] [FCFS Status: Unverified] > IEEE 802.11 Wireless Management				

51	2.300697	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
52	2.302191	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
53	2.304063	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
54	2.305562	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
<					
> Frame 51: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)					
> Radiotap Header v0, Length 24					
> 802.11 radio information					
▼ IEEE 802.11 Probe Response, Flags:C					
Type/Subtype: Probe Response (0x0005)					
> Frame Control Field: 0x5000					
.000 0001 0011 1010 = Duration: 314 microseconds					
Receiver address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)					
Destination address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)					
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					
1011 0011 1110 = Sequence number: 2878					
Frame check sequence: 0x6ed851bb [unverified]					
[FCS Status: Unverified]					
> IEEE 802.11 Wireless Management					

PROBE REQUEST is sent with source 00:12:f0:1f:57:13, destination ff:ff:ff:ff:ff:ff, and a BSS ID MAC ff:ff:ff:ff:ff:f

PROBE RESPONSE is sent with source 00:16:b6:f7:1d:51, destination 00:12:f0:1f:57:13 and a BSS ID MAC 00:16:b6:f7:1d:51