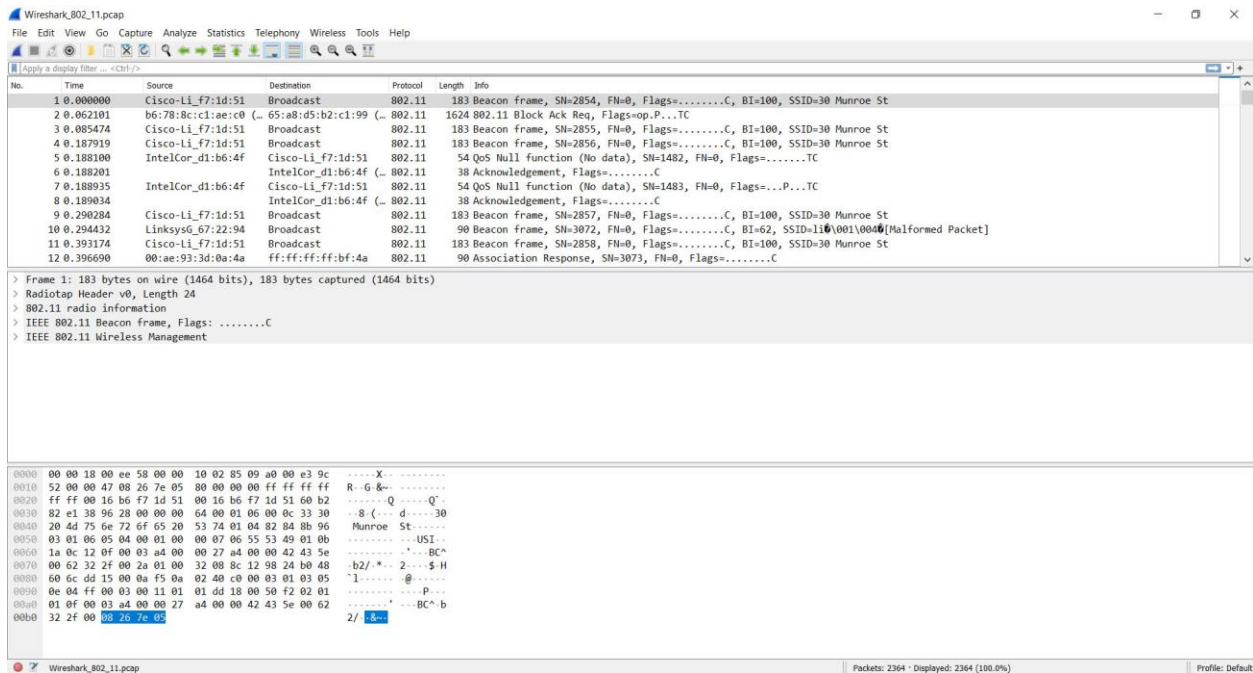


CO513 - Lab 07

Wireless Wireshark Lab - 802.11

E/16/039

Balasuriya B.M.N.U



Bacon Files

Exercise 1

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

SSID = 30 Munroe st and SSID = Linksys 12

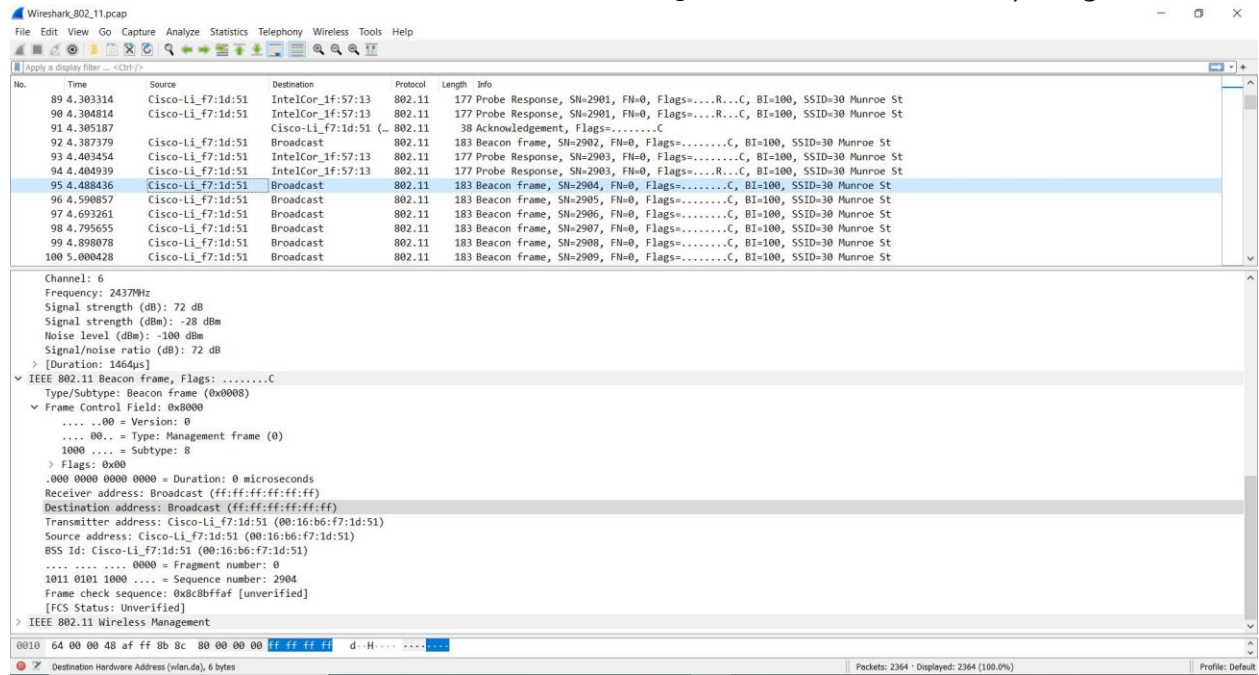
No.	Time	Source	Destination	Protocol	Length	Info
16	0.601687	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3075, FN=0, Flags=.....C, BI=100, SSID=linksys12
17	0.699847	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2861, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
18	0.802226	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2862, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
19	0.904619	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2863, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
20	1.007015	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2864, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
21	1.010949	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3079, FN=0, Flags=.....C, BI=100, SSID=linksys12
22	1.109406	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2865, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
23	1.113691	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3080, FN=0, Flags=.....C, BI=100, SSID=linksys
24	1.211843	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2866, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
25	1.211992	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1484, FN=0, Flags=.....TC
26	1.212089	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
27	1.212185	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=2867, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

- What are the intervals of time between the transmissions of the beacon frames and 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 both are **0.1024 seconds**.

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

The source MAC on the beacon feacom frame from 30 Munroe is **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 shown here as broadcast. Therefore the destination mac address is **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 is **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?

Four data rates are,
1.0Mb/s, 2.0Mb/s, 5.5Mb/s, 11.0Mb/s.

Extended supported rates are,
6.0Mb/s, 9.0Mb/s, 12.0Mb/s, 18.0Mb/s, 24.0Mb/s, 36.0Mb/s, 48.0Mb/s, 54.0Mb/s

```
> 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 1 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: Vendor Specific: Airgo Networks, Inc.
  > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

Data Transfer

Exercise 2

7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt).

7.1. What are three MAC address fields in the 802.11 frame?

BSS Id, source address and destination address

7.2. Which MAC address in this frame corresponds to the wireless host(in Hexadecimal Representation)?

00:13:02:d1:b6:4f

7.3. Which MAC address in this frame corresponds to the access point ?

00:16:b6:f4:eb:a8

7.4. Which MAC address in this frame corresponds to the first-hop router?

00:16:b6:j7:1d:51

7.5. What is the IP address of the wireless host sending this TCP segment?

192.168.1.109

7.6. What is the destination IP address?

128.199.245.12.

7.7. Does this destination IP address correspond to the host, access point, first-hop router, or some other network-attached device? Explain.

The destination MAC address of the frame, 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.

8.1. What are three MAC address fields in the 802.11 frame?

BSS id: 00:16:b6:f7:1d:51

Destination: 00:13:02:d1:b6:4f

source address: 00:16:b6:f4:eb:a8.

8.2. Which MAC address in this frame corresponds to the host?

The destination address, 00:13:02:d1:b6:4f

8.3. Which MAC address in this frame corresponds to the access point?

00:16:b6:f4:eb:a8

8.4. Which MAC address in this frame corresponds to the first-hop router?

00:16:b6:f4:eb:a8

8.5. 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?

the IP address of the device that sent the TCP segment is different from the MAC address of the host used in the frame that sends the TCP SYN. The host wireless interface is behaving as if it has two interface addresses

Association and Disassociation

Exercise 3

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?

At t = 49.583615 a DHCP release is sent by the host to the DHCP server (whose IP address is 192.168.1.1) in the network that the host is leaving. At t = 49.609617, the host sends a DEAUTHENTICATION frame

No.	Time	Source	Destination	Protocol	Length	Info
1708	48.825688	Cisco-Li-f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3580, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1709	48.826189	IntelCor_d1:b6:4f	Cisco-Li-f7:1d:51	802.11	54	QoS Null function (No data), SN=1598, FN=0, Flags=...P...TC
1710	48.826299	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
1711	48.928080	Cisco-Li-f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3581, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1712	49.000125	IntelCor_d1:b6:4f	Cisco-Li-f7:1d:51	802.11	54	QoS Null function (No data), SN=1599, FN=0, Flags=.....TC
1713	49.020257	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
1714	49.020356	128.119.101.5	192.168.1.109	TCP	108	80 → 2543 [SYN, PSH, ECH, NS] Seq=2758133200 Win=7504[Malformed Packet]
1715	49.020948	192.168.1.109	128.119.101.5	TCP	102	2543 → 80 [ACK] Seq=1 Ack=1 Win=16132 Len=0
1716	49.021047	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
1717	49.030423	Cisco-Li-f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3583, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1718	49.132768	Cisco-Li-f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3584, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1719	49.132804	IntelCor_d1:b6:4f	Cisco-Li-f7:1d:51	802.11	54	QoS Null function (No data), SN=1600, FN=0, Flags=...P...TC
1720	49.132981	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
1721	49.224975	IntelCor_d1:b6:4f	Cisco-Li-f7:1d:51	802.11	54	QoS Null function (No data), SN=1601, FN=0, Flags=.....TC
1722	49.225104	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
1723	49.235239	Cisco-Li-f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3585, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1724	49.235340	IntelCor_d1:b6:4f	Cisco-Li-f7:1d:51	802.11	54	QoS Null function (No data), SN=1602, FN=0, Flags=...P...TC
1725	49.235439	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
1726	49.337573	Cisco-Li-f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3586, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1727	49.429849	IntelCor_d1:b6:4f	Cisco-Li-f7:1d:51	802.11	54	QoS Null function (No data), SN=1603, FN=0, Flags=.....TC
1728	49.430007	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
1729	49.440041	Cisco-Li-f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3587, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1730	49.440146	IntelCor_d1:b6:4f	Cisco-Li-f7:1d:51	802.11	54	QoS Null function (No data), SN=1604, FN=0, Flags=...P...TC
1731	49.440243	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
1732	49.542481	IntelCor_d1:b6:4f	Broadcast	802.11	183	Beacon frame, SN=3588, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
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	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
1735	49.609617	IntelCor_d1:b6:4f	Cisco-Li-f7:1d:51	802.11	54	Deauthentication, SN=1605, FN=0, Flags=.....C
1736	49.609770	IntelCor_d1:b6:4f	IntelCor_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, SSID=linksys_SES_24086
1738	49.615869	Cisco-Li-f5:ba:bb	Cisco-Li-f5:ba:bb	802.11	38	Acknowledgement, Flags=.....C
1739	49.617713	Cisco-Li-f5:ba:bb	Cisco-Li-f5:ba:bb	802.11	38	Acknowledgement, 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
1743	49.641910	IntelCor_d1:b6:4f	Cisco-Li-f5:ba:bb	802.11	38	Acknowledgement, Flags=.....C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li-f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=...R...C

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? .

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

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

Yes

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

NO, we cannot see any reply authentication.

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 is there an AUTHENTICATION frame from the host to 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.)

The image shows a Wireshark packet capture of a wireless network. The filter applied is 'wlan.addr == IntelCor_d1:b6:4f'. The packet list shows several deauthentication frames from IntelCor_d1:b6:4f to Cisco-Li_f5:ba:bb. A probe request and response are visible for 30 Munroe St. An authentication frame is sent from IntelCor_d1:b6:4f to IntelCor_d1:b6:4f at t=63.168087. This is followed by an acknowledgment from IntelCor_d1:b6:4f to IntelCor_d1:b6:4f at t=63.169071. The packet details pane shows the authentication frame structure: IEEE 802.11 Authentication, Flags:C, Fixed parameters (6 bytes), Authentication Algorithm: Open System (0), Authentication SEQ: 0x0001, Status code: Successful (0x0000).

No.	Time	Source	Destination	Protocol	Length	Info
2147	63.087480	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54	Deauthentication, SN=1646, FN=0, Flags=....R...C
2148	63.090971	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54	Deauthentication, SN=1646, FN=0, Flags=....R...C
2149	63.094985	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54	Deauthentication, SN=1646, FN=0, Flags=....R...C
2150	63.116231	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54	Deauthentication, SN=1646, FN=0, Flags=....R...C
2151	63.135362	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54	Deauthentication, SN=1646, FN=0, Flags=....R...C
2152	63.140106	IntelCor_d1:b6:4f	Broadcast	802.11	94	Probe Request, SN=1647, FN=0, Flags=.....C, SSID=30 Munroe St
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=30 Munroe St
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	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
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	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 Munroe St
2163	63.170008	IntelCor_d1:b6:4f	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
2166	63.192101	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C

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.

14. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to be associated with an AP.

14.1. At what time is there an ASSOCIATE REQUEST from host to the 30 Munroe St AP?

At t = 63.169910 seconds

14.2. 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.)

Replied at t = 63.192101 s

The image shows a Wireshark packet capture of an 802.11 wireless LAN management frame. The packet list shows a sequence of Association Request frames from IntelCor_d1:b6:4f to Cisco-Li_f5:ba:bb. The selected packet is an Association Request frame at time 63.169910 seconds. The packet details pane shows the frame structure: Radiotap Header, IEEE 802.11 radio information, IEEE 802.11 Association Request, and IEEE 802.11 Wireless Management. The Wireless Management section is expanded, showing Fixed parameters (Capabilities Information) and Tagged parameters (SSID, Supported Rates, and Vendor Specific). The packet bytes pane shows the raw data of the frame.

No.	Time	Source	Destination	Protocol	Length	Info
1750	49.651078	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=.....C, SSID=linksys_SES_24086
1751	49.653219	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=.....C, SSID=linksys_SES_24086
1824	53.789944	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=.....C, SSID=linksys_SES_24086
1825	53.790943	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=.....C, SSID=linksys_SES_24086
1827	53.793568	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=.....C, SSID=linksys_SES_24086
1926	57.903699	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086
1927	57.904945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086
1932	57.911195	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086
1933	57.915945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086
1934	57.924199	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086
1935	57.936216	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086
1937	57.939196	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086
2126	62.176945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1645, FN=0, Flags=.....C, SSID=linksys_SES_24086
2127	62.178194	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1645, FN=0, Flags=.....C, SSID=linksys_SES_24086
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
2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C

15. To answer this question, you will need to look into the parameters fields of the 802.11 wireless LAN management frame.

15.1. What transmission rates is the host willing to use?

15.2. What transmission rates is the AP willing to use?

The possible rates that willing to use both host and AP are 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, 54 Mbps.

Other Frame types

Exercise 4

16. Our trace contains a number of PROBE REQUEST and PROBE RESPONSE frames.

16.1. What are the sender, receiver and BSS ID MAC addresses in these frames?

Probe request:

Source: 00:12:fo: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

No.	Time	Source	Destination	Protocol	Length	Info
2014	60.191465	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3693, FH=0, Flags=.....C, BI=100, SSID=30 Munroe St
2015	60.248091	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	52	Null function (No data), SN=1626, FH=0, Flags=...P...TC
2016	60.249322	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	52	Null function (No data), SN=1626, FH=0, Flags=...PR...TC
2017	60.250820	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	52	Null function (No data), SN=1626, FH=0, Flags=...PR...TC
2018	60.256570	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=3694, FH=0, Flags=.....C, BI=100, SSID=30 Munroe St
2019	60.258070	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=3694, FH=0, Flags=.....R...C, BI=100, SSID=30 Munroe St
2020	60.259945	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=3694, FH=0, Flags=.....R...C, BI=100, SSID=30 Munroe St
2021	60.280076	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=3695, FH=0, Flags=.....C, BI=100, SSID=30 Munroe St
2022	60.284196	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	52	Null function (No data), SN=1627, FH=0, Flags=.....TC
2023	60.285195	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	52	Null function (No data), SN=1627, FH=0, Flags=.....R...TC
2024	60.286695	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	52	Null function (No data), SN=1627, FH=0, Flags=.....R...TC
2025	60.287944	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	52	Null function (No data), SN=1627, FH=0, Flags=.....R...TC
2026	60.292694	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	52	Null function (No data), SN=1627, FH=0, Flags=.....R...TC
2027	60.294447	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3696, FH=0, Flags=.....C, BI=100, SSID=30 Munroe St
2028	60.300320	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	52	Null function (No data), SN=1627, FH=0, Flags=.....R...TC

> Frame 2018: 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_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 0110 1110 = Sequence number: 3694

Frame check sequence: 0x89d81da4 [unverified]

[FCS Status: Unverified]

> IEEE 802.11 Wireless Management

16.2. What is the purpose of these two types of frames?

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