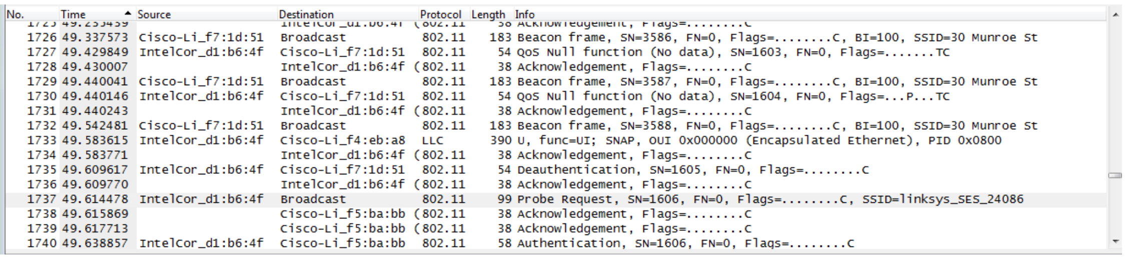
Lab 6

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

Answer



No.	Time	Source	Destination	Protocol	Length	Info
1725	49.235439		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 (	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 (	802.11	38	Acknowledgement, Flags=........C
1732	49.542481	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3588, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1733	49.583615	IntelCor_d1:b6:4f	Cisco-Li_f4:eb:a8	LLC	390	U, func=UI; SNAP, OUI 0x000000 (Encapsulated Ethernet), PID 0x0800
1734	49.583771		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 (	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 (	802.11	38	Acknowledgement, Flags=........C
1739	49.617713		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

They are Linksys_SES_24086 and 30 Munroe St.

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).

Answer

They are both 0.1024 s.

3. What (in hexadecimal notation) is the source MAC address on the beacon frame from 30 Munroe St? Recall from Figure 6.13 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).

Answer

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?

Answer

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

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

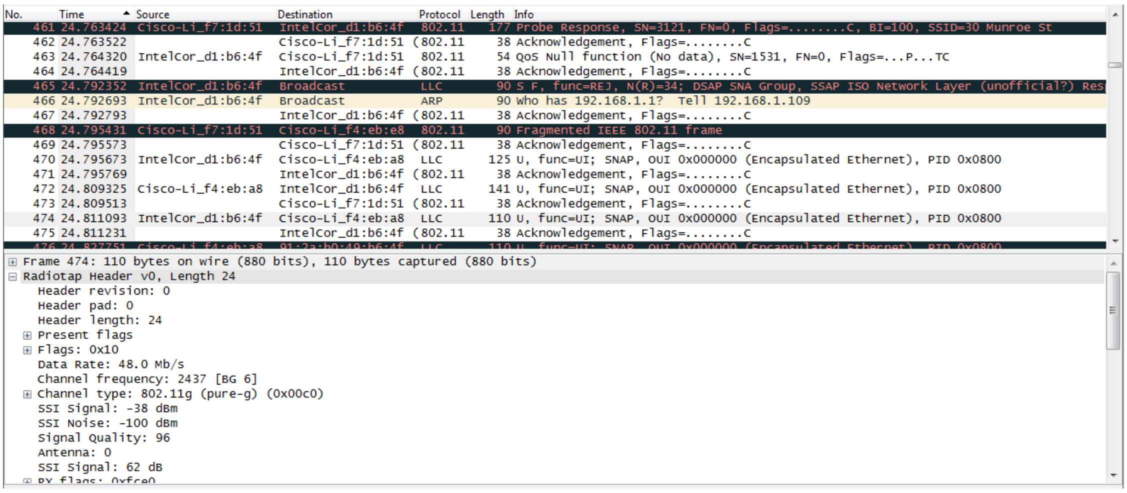
Answer

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

6. 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

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.



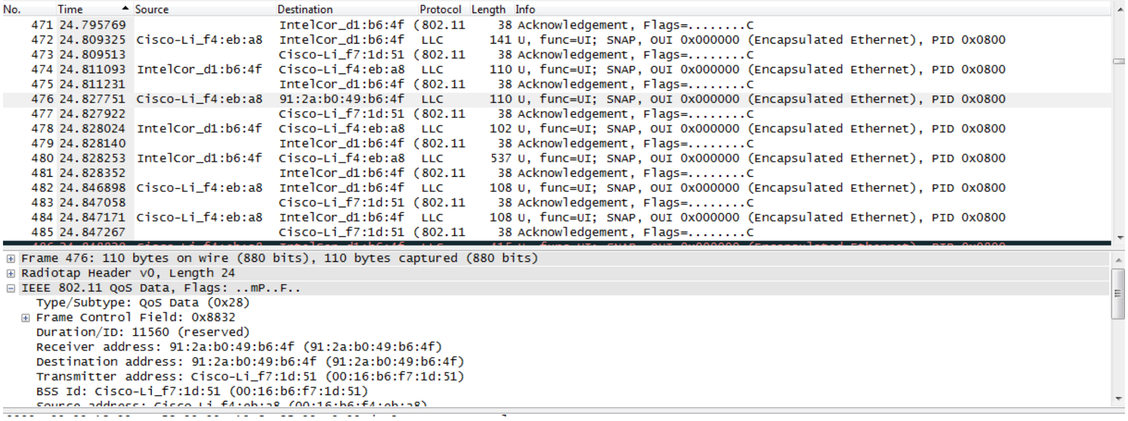
```
No.  Time        Source             Destination        Protocol Length Info
 461 24.763424  Cisco-Li_f7:1d:51  IntelCor_d1:b6:4f   802.11   177 Probe Response, SN=3121, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
 462 24.763522                     Cisco-Li_f7:1d:51  (802.11    38 Acknowledgement, Flags=........C
 463 24.764320  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51   802.11    54 QoS Null function (No data), SN=1531, FN=0, Flags=...P...TC
 464 24.764419                     IntelCor_d1:b6:4f  (802.11    38 Acknowledgement, Flags=........C
 465 24.792352  IntelCor_d1:b6:4f  Broadcast           LLC       90 S F, func=REJ, N(R)=34; DSAP SNA Group, SSAP ISO Network Layer (unofficial?) Res
 466 24.792693  IntelCor_d1:b6:4f  Broadcast           ARP       90 Who has 192.168.1.1?  Tell 192.168.1.109
 467 24.792793                     IntelCor_d1:b6:4f  (802.11    38 Acknowledgement, Flags=........C
 468 24.795431  Cisco-Li_f7:1d:51  Cisco-Li_f4:eb:e8   802.11    90 Fragmented IEEE 802.11 frame
 469 24.795573                     Cisco-Li_f7:1d:51  (802.11    38 Acknowledgement, Flags=........C
 470 24.795673  IntelCor_d1:b6:4f  Cisco-Li_f4:eb:a8   LLC      125 U, func=UI; SNAP, OUI 0x000000 (Encapsulated Ethernet), PID 0x0800
 471 24.795769                     IntelCor_d1:b6:4f  (802.11    38 Acknowledgement, Flags=........C
 472 24.809325  Cisco-Li_f4:eb:a8  IntelCor_d1:b6:4f   LLC      141 U, func=UI; SNAP, OUI 0x000000 (Encapsulated Ethernet), PID 0x0800
 473 24.809513                     Cisco-Li_f7:1d:51  (802.11    38 Acknowledgement, Flags=........C
 474 24.811093  IntelCor_d1:b6:4f  Cisco-Li_f4:eb:a8   LLC      110 U, func=UI; SNAP, OUI 0x000000 (Encapsulated Ethernet), PID 0x0800
 475 24.811231                     IntelCor_d1:b6:4f  (802.11    38 Acknowledgement, Flags=........C
 476 24.827751  Cisco-Li_f4:eb:a8  91:2a:b0:49:b6:4f   LLC      110 U, func=UI; SNAP, OUI 0x000000 (Encapsulated Ethernet), PID 0x0800

⊞ Frame 474: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
⊟ Radiotap Header v0, Length 24
    Header revision: 0
    Header pad: 0
    Header length: 24
  ⊞ Present flags
  ⊞ Flags: 0x10
    Data Rate: 48.0 Mb/s
    Channel frequency: 2437 [BG 6]
  ⊞ Channel type: 802.11g (pure-g) (0x00c0)
    SSI Signal: -38 dBm
    SSI Noise: -100 dBm
    Signal Quality: 96
    Antenna: 0
    SSI Signal: 62 dB
  ⊞ RX flags: 0xfce0
```

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.

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.



```
No.   Time       Source            Destination       Protocol Length Info
  471 24.795769                    IntelCor_d1:b6:4f (802.11    38 Acknowledgement, Flags=........C
  472 24.809325 Cisco-Li_f4:eb:a8  IntelCor_d1:b6:4f  LLC      141 U, func=UI; SNAP, OUI 0x000000 (Encapsulated Ethernet), PID 0x0800
  473 24.809513                    Cisco-Li_f7:1d:51 (802.11    38 Acknowledgement, Flags=........C
  474 24.811093 IntelCor_d1:b6:4f  Cisco-Li_f4:eb:a8  LLC      110 U, func=UI; SNAP, OUI 0x000000 (Encapsulated Ethernet), PID 0x0800
  475 24.811231                    IntelCor_d1:b6:4f (802.11    38 Acknowledgement, Flags=........C
  476 24.827751 Cisco-Li_f4:eb:a8  91:2a:b0:49:b6:4f  LLC      110 U, func=UI; SNAP, OUI 0x000000 (Encapsulated Ethernet), PID 0x0800
  477 24.827922                    Cisco-Li_f7:1d:51 (802.11    38 Acknowledgement, Flags=........C
  478 24.828024 IntelCor_d1:b6:4f  Cisco-Li_f4:eb:a8  LLC      102 U, func=UI; SNAP, OUI 0x000000 (Encapsulated Ethernet), PID 0x0800
  479 24.828140                    IntelCor_d1:b6:4f (802.11    38 Acknowledgement, Flags=........C
  480 24.828253 IntelCor_d1:b6:4f  Cisco-Li_f4:eb:a8  LLC      537 U, func=UI; SNAP, OUI 0x000000 (Encapsulated Ethernet), PID 0x0800
  481 24.828352                    IntelCor_d1:b6:4f (802.11    38 Acknowledgement, Flags=........C
  482 24.846898 Cisco-Li_f4:eb:a8  IntelCor_d1:b6:4f  LLC      108 U, func=UI; SNAP, OUI 0x000000 (Encapsulated Ethernet), PID 0x0800
  483 24.847058                    Cisco-Li_f7:1d:51 (802.11    38 Acknowledgement, Flags=........C
  484 24.847171 Cisco-Li_f4:eb:a8  IntelCor_d1:b6:4f  LLC      108 U, func=UI; SNAP, OUI 0x000000 (Encapsulated Ethernet), PID 0x0800
  485 24.847267                    Cisco-Li_f7:1d:51 (802.11    38 Acknowledgement, Flags=........C
```

```
⊞ Frame 476: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
⊞ Radiotap Header v0, Length 24
⊟ IEEE 802.11 QoS Data, Flags: ..mP..F..
    Type/Subtype: QoS Data (0x28)
  ⊞ Frame Control Field: 0x8832
    Duration/ID: 11560 (reserved)
    Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Destination 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)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
```

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? (Hint: review Figure 5.19 in the text if you are unsure of how to answer this question, or the corresponding part of the previous question. It's particularly important that you understand this).

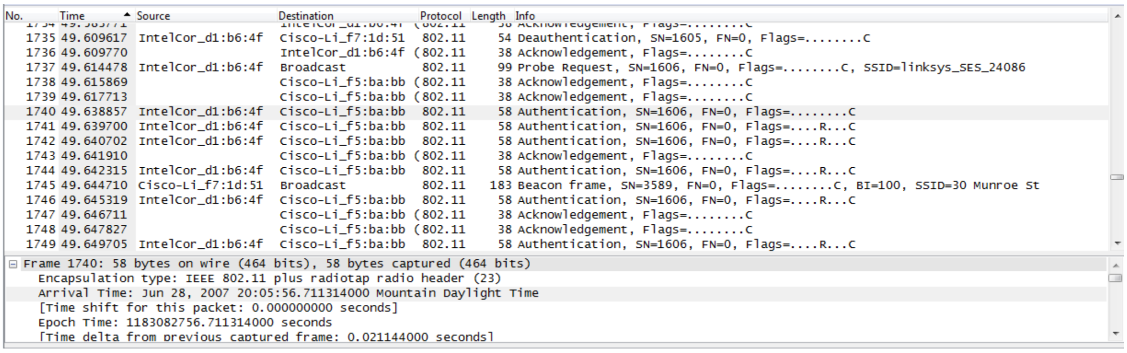
Answer

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. 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



```
No.  Time       Source             Destination          Protocol Length Info
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 (  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 (  802.11    38 Acknowledgement, Flags=........C
1739 49.617713                     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                     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
1745 49.644710  Cisco-Li_f7:1d:51  Broadcast            802.11   183 Beacon frame, SN=3589, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1746 49.645319  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb    802.11    58 Authentication, SN=1606, FN=0, Flags=....R...C
1747 49.646711                     Cisco-Li_f5:ba:bb (  802.11    38 Acknowledgement, Flags=........C
1748 49.647827                     Cisco-Li_f5:ba:bb (  802.11    38 Acknowledgement, Flags=........C
1749 49.649705  IntelCor_d1:b6:4f  Cisco-Li_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 28, 2007 20:05:56.711314000 Mountain Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1183082756.711314000 seconds
    [Time delta from previous captured frame: 0.021144000 seconds]
```

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

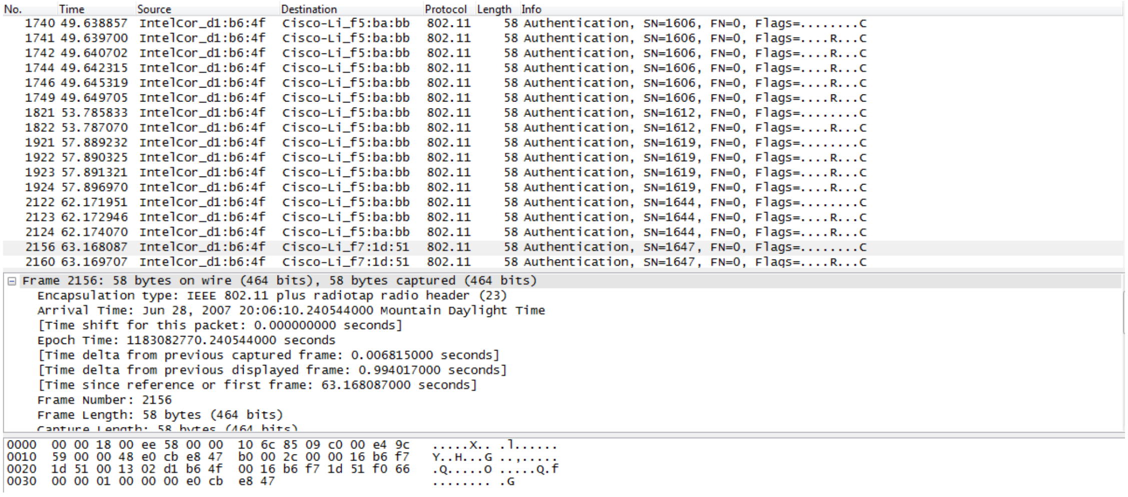
Answer

Yes.

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

Answer

No, there is no reply.



```
No.  Time       Source             Destination        Protocol Length Info
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=........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=........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=........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=........C
2160 63.169707  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51  802.11    58 Authentication, SN=1647, FN=0, Flags=....R...C
```

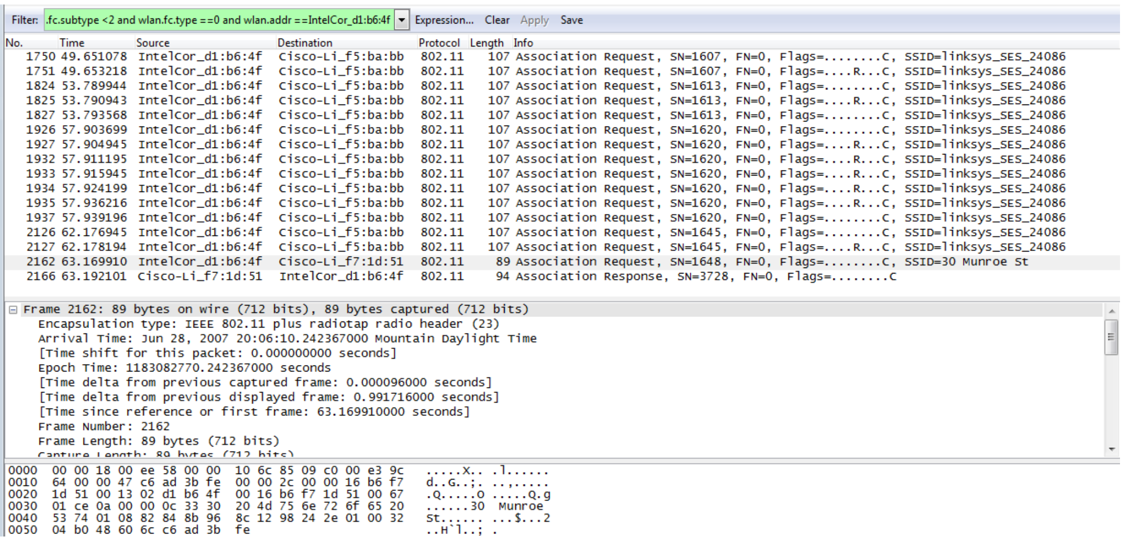
```
⊟ Frame 2156: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
    Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
    Arrival Time: Jun 28, 2007 20:06:10.240544000 Mountain Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1183082770.240544000 seconds
    [Time delta from previous captured frame: 0.006815000 seconds]
    [Time delta from previous displayed frame: 0.994017000 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)
```

```
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. 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.)

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.



Filter: .fc.subtype <2 and wlan.fc.type ==0 and wlan.addr ==IntelCor_d1:b6:4f

```
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 49.653218  IntelCor_d1:b6:4f   Cisco-Li_f5:ba:bb   802.11    107 Association Request, SN=1607, FN=0, Flags=....R...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=....R...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=....R...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=....R...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=....R...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=....R...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=....R...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=....R...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
```

```
⊟ 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 28, 2007 20:06:10.242367000 Mountain Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1183082770.242367000 seconds
    [Time delta from previous captured frame: 0.000096000 seconds]
    [Time delta from previous displayed frame: 0.991716000 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)
```

```
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. 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.)

Answer

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

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.

Answer

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

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).

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.