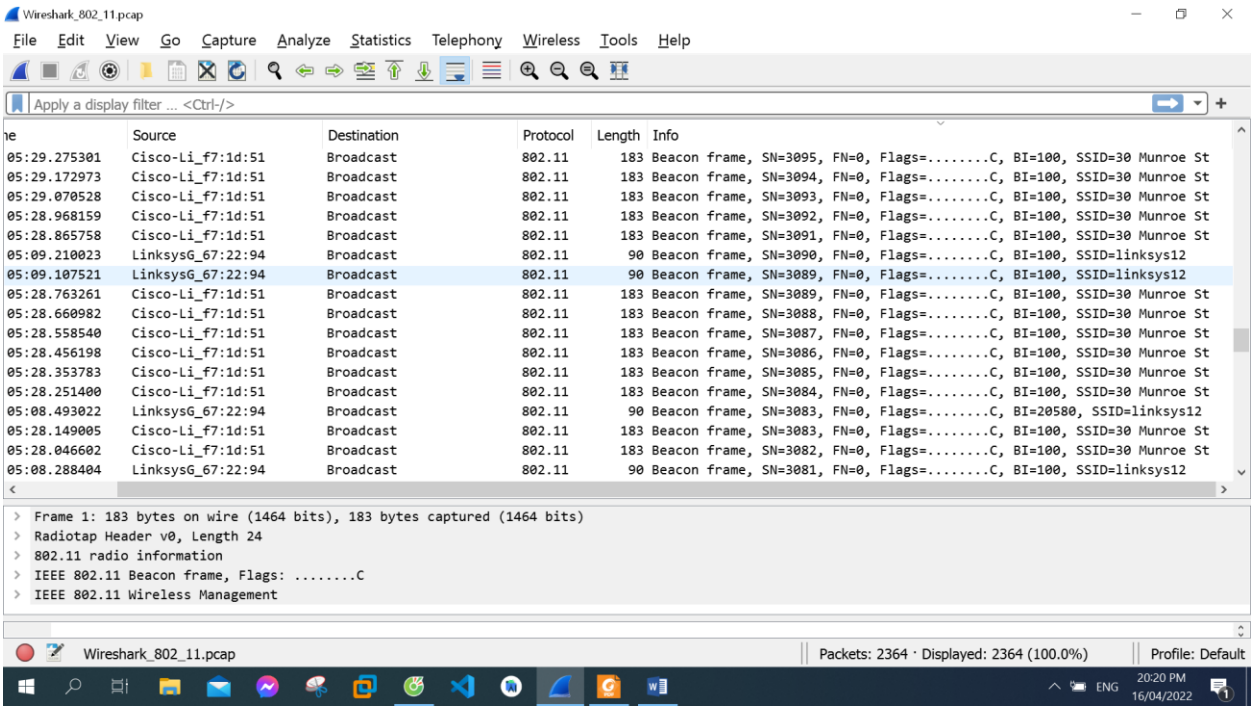
# LAB 7: 802.11 WiFi

**Name: Hồ Đức Trí**

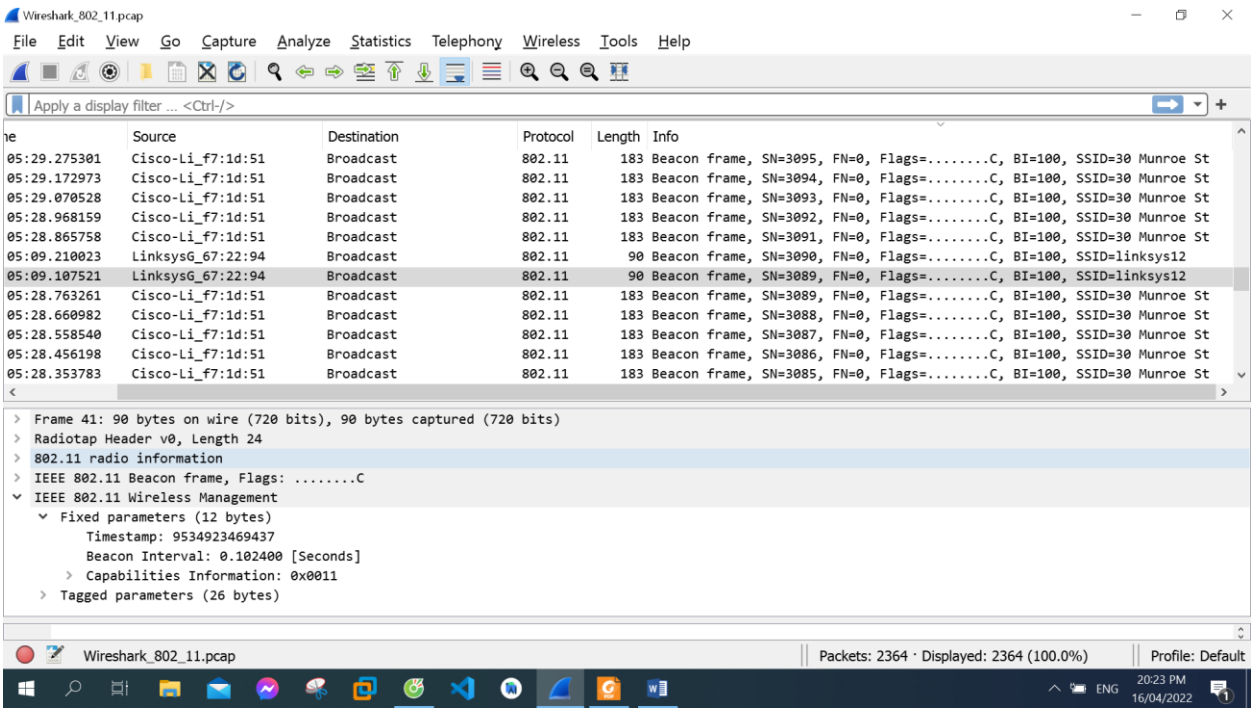
**Student No: 1912288**

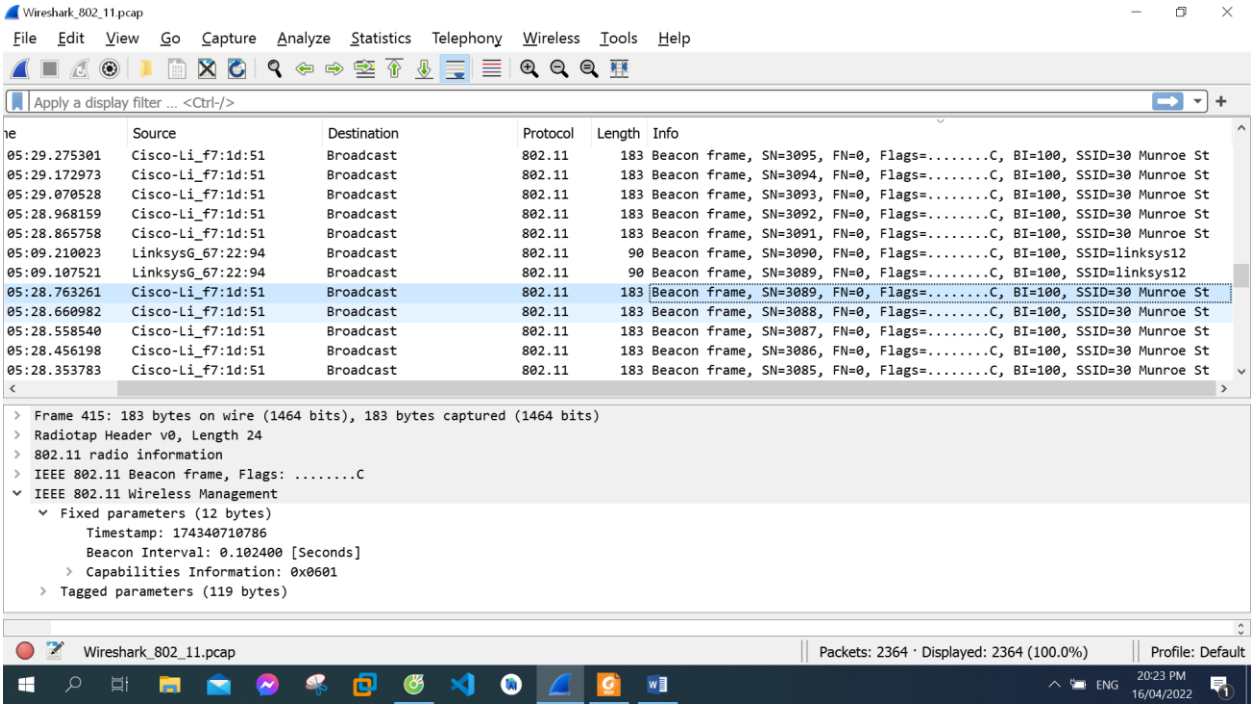
1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?




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

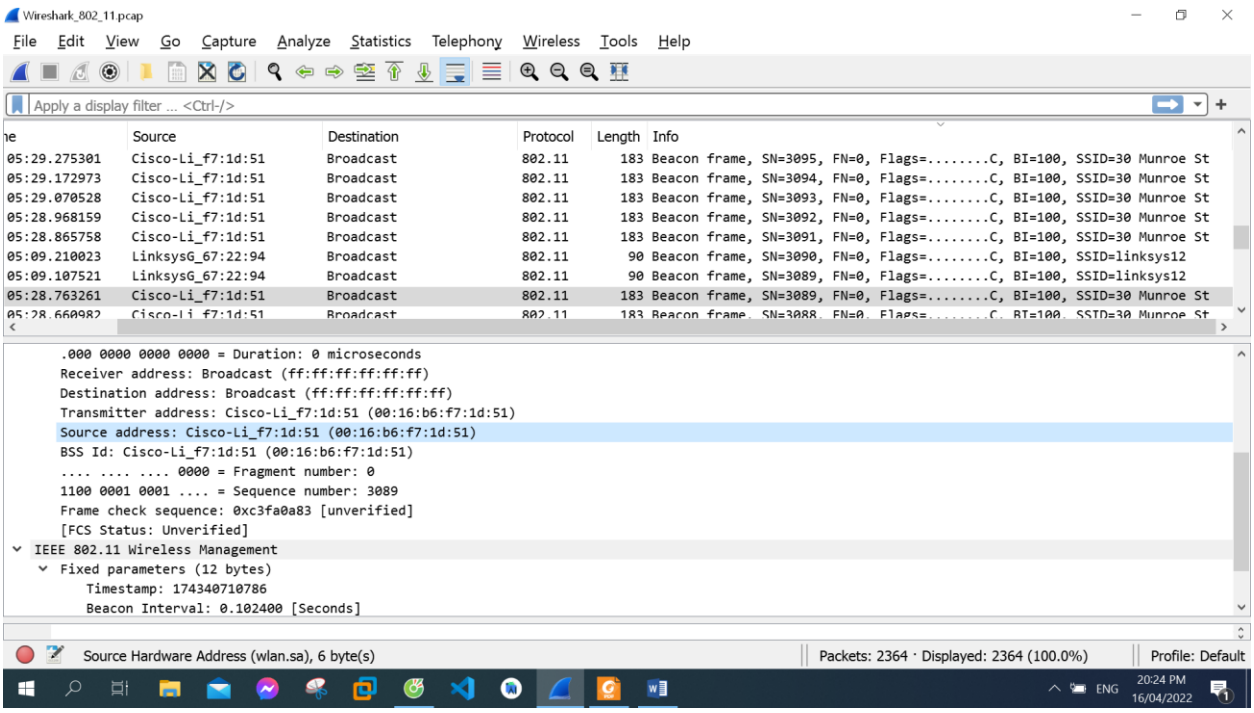
2. What are the intervals of time between the transmissions of the beacon frames the linksys_ses_24086 access point? From the 30 Munroe St. access point? (Hint: this interval of time is contained in the beacon frame itself).




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

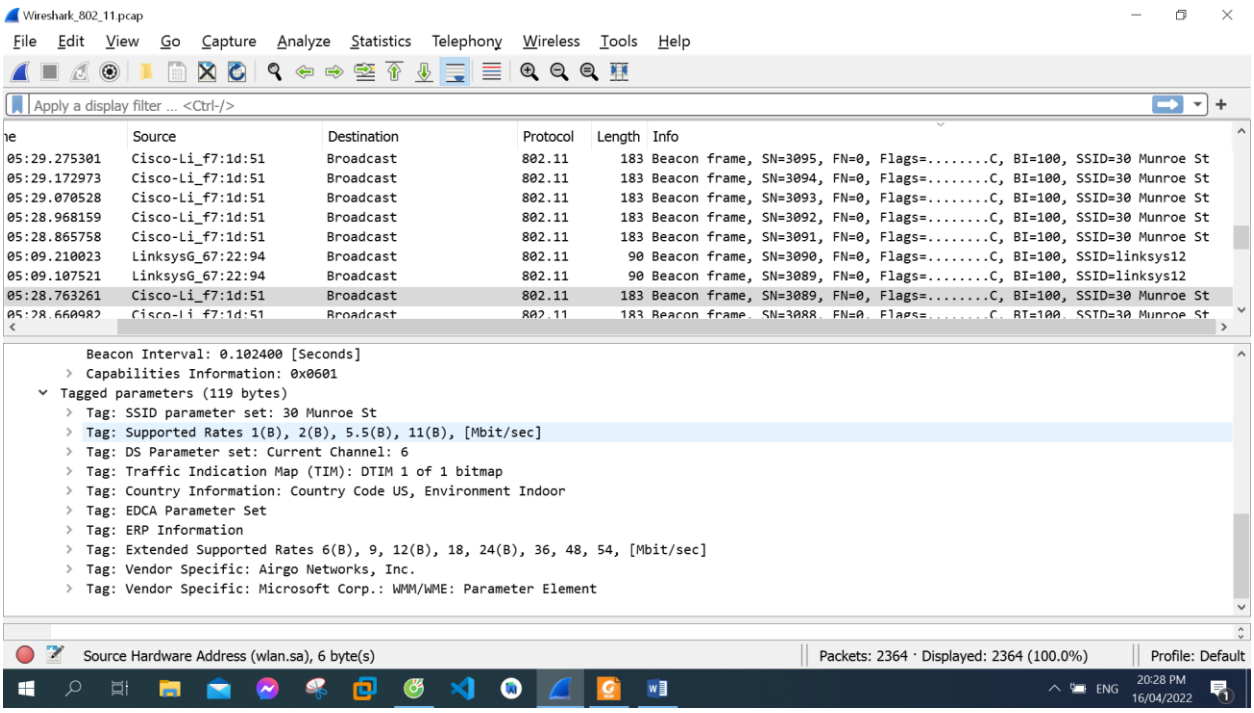
4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St?

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?

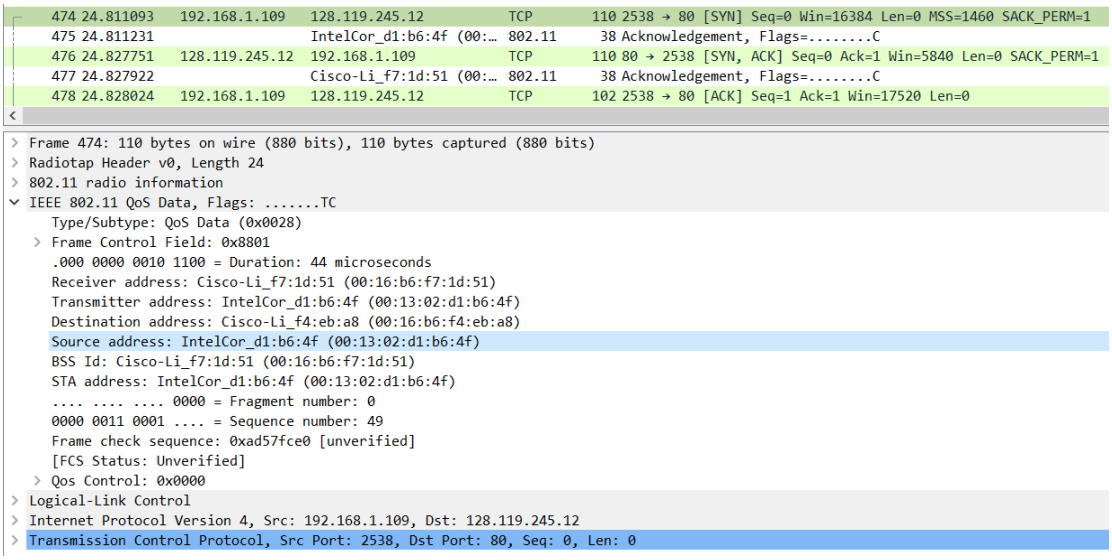
The MAC BSS id on the beacon frame from 30 Munroe St: 00:16:b6:f7:1d:51

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.




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

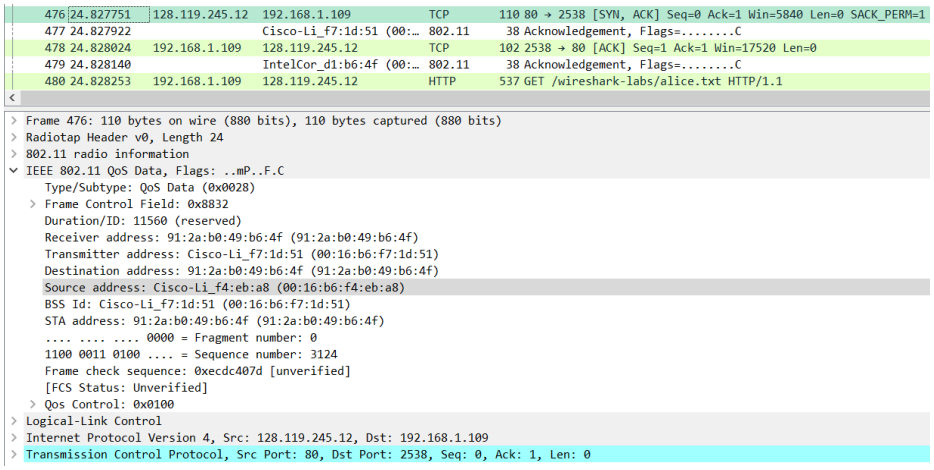
The MAC address in this frame corresponds to the first-hop router: 00:16:b6:f7:1d:51

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?




Those MAC addresses are BSSid, source address and destination.

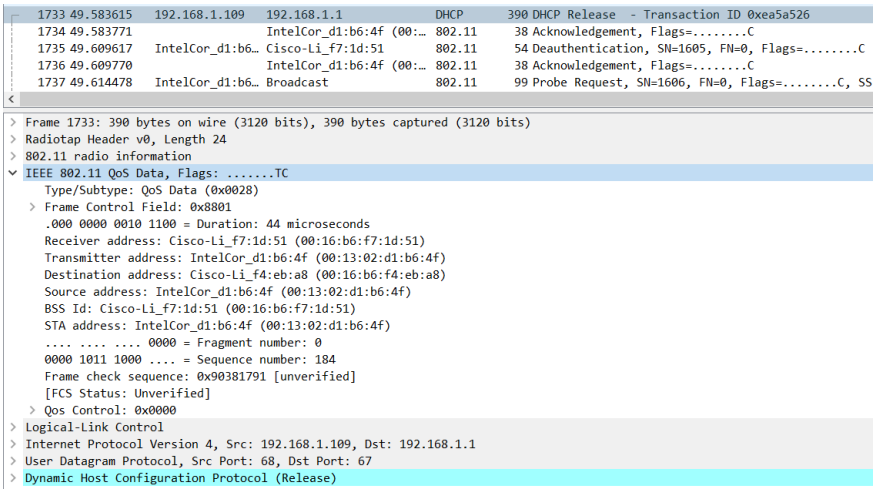
The MAC address in this frame corresponds to the host: 91:2a:b0:49:b6:4f.

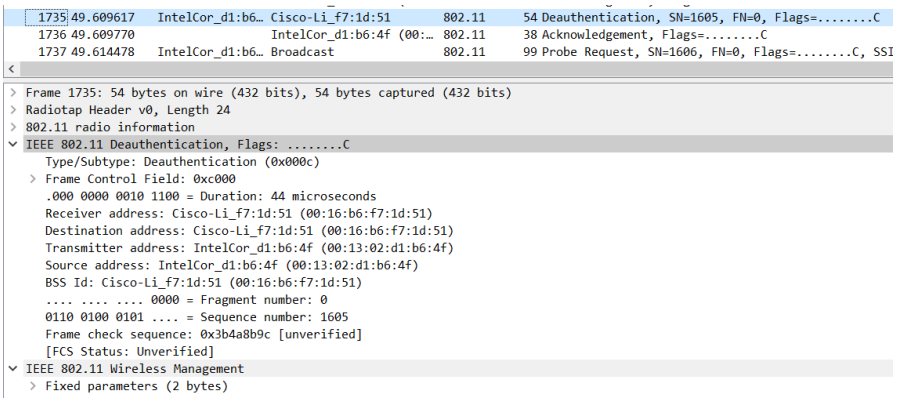
The MAC address in this frame corresponds to the access point: 00:16:b6:f7:1d:51.

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?






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 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?

| | | | | | | |
|---|---|---|---|---|---|---|
| 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=........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 |
| 2158 | 63.169071 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 58 | Authentication, SN=3726, FN=0, Flags=........C |
| 2164 | 63.170692 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 58 | Authentication, SN=3727, FN=0, Flags=........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.

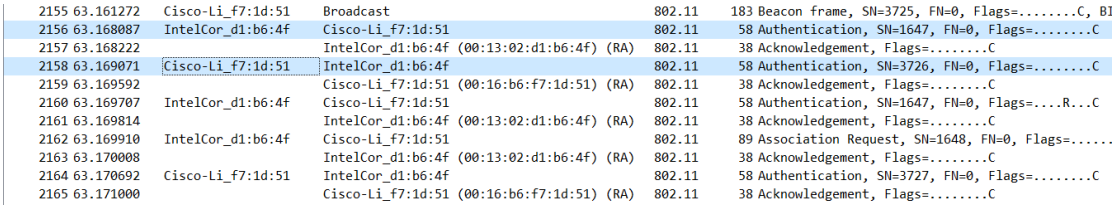
11. Does the host want the authentication to require a key or be open?

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 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?

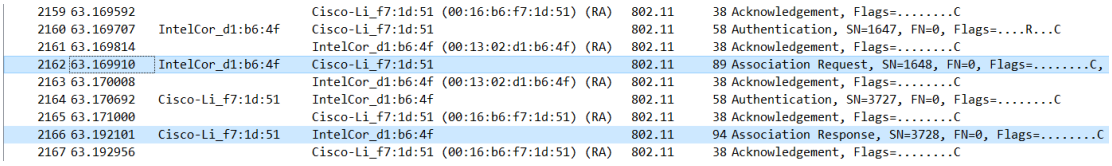


| | | | | | | |
|---|---|---|---|---|---|---|
| 2155 | 63.161272 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3725, FN=0, Flags=........C, BI |
| 2156 | 63.168087 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 58 | Authentication, SN=1647, FN=0, Flags=........C |
| 2157 | 63.168222 | | IntelCor_d1:b6:4f (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=..... |
| 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?

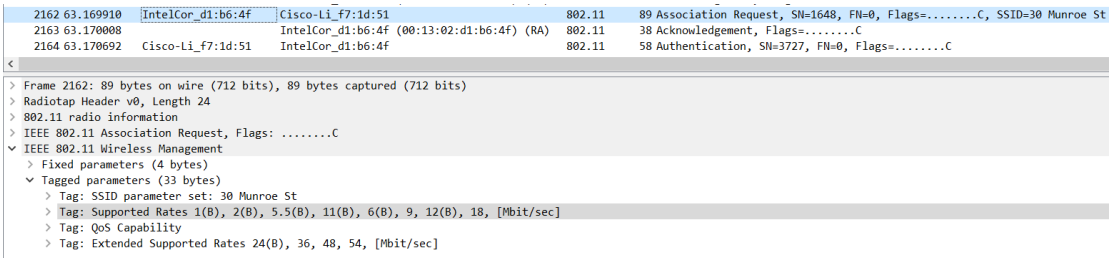


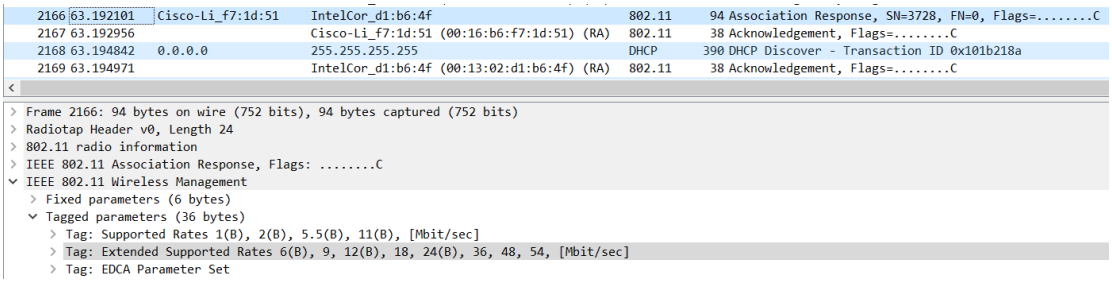
| | | | | | | |
|---|---|---|---|---|---|---|
| 2159 | 63.169592 | | Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51) (RA) | 802.11 | 38 | Acknowledgement, Flags=........C |
| 2160 | 63.169707 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 58 | Authentication, SN=1647, FN=0, Flags=....R...C |
| 2161 | 63.169814 | | 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.

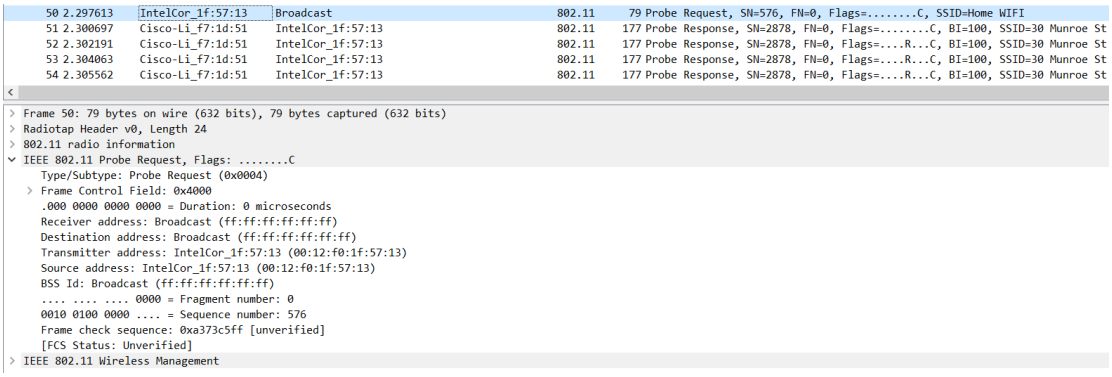


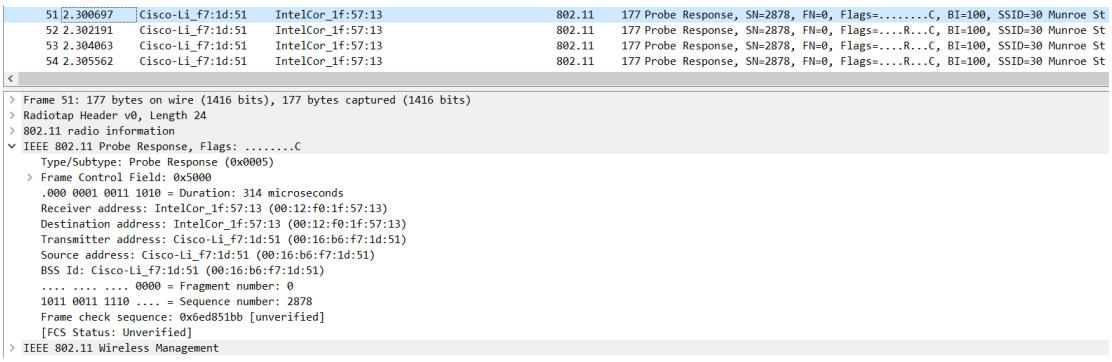




In the ASSOCIATION REQUEST frame the supported rates are advertised as 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, and 54 Mbps.

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).






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