Wireshark Experiment – 03

IEEE 802.11 WiFi Protocol

Name: Pratik P Patil
USN: 02FE21BEC063
Roll No: 53
Div: A

IEEE 802.11 WiFi Protocol

The 802.11 protocol is a set of standards developed by the Institute of Electrical and Electronics Engineers (IEEE) for wireless local area networking (WLAN). It defines how wireless devices, such as laptops, smartphones, and other equipment, communicate over a wireless network using radio waves. This protocol operates primarily in the 2.4 GHz and 5 GHz frequency bands, although newer versions also use 6 GHz, providing different speeds, ranges, and capabilities.

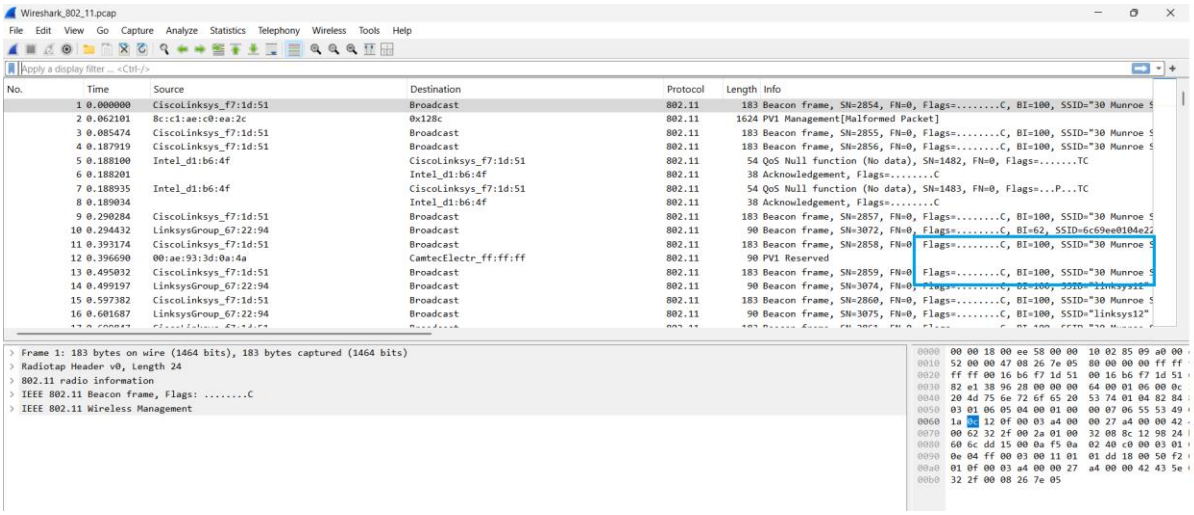
Definition

802.11 refers to a family of specifications for wireless networking, more commonly known as Wi-Fi. It defines the medium access control (MAC) and physical layer (PHY) protocols to enable reliable and efficient wireless communication. Different versions of the protocol, such as 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax, offer various levels of performance and are backward compatible

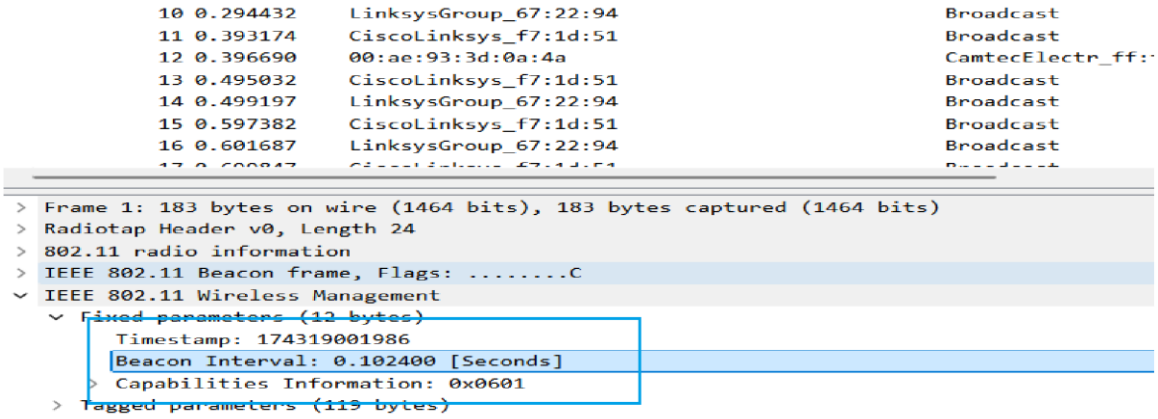
802.11 Protocol Versions

• 802.11a: Operates at 5 GHz with data rates up to 54 Mbps.
• 802.11b: Operates at 2.4 GHz with data rates up to 11 Mbps.
• 802.11g: Operates at 2.4 GHz with data rates up to 54 Mbps.
• 802.11n: Operates at both 2.4 GHz and 5 GHz with data rates up to 600 Mbps using multiple input multiple output (MIMO) technology.
• 802.11ac: Operates at 5 GHz with data rates up to 1.3 Gbps and uses wider channels and MIMO.
• 802.11ax (Wi-Fi 6): Operates in 2.4, 5, and 6 GHz bands with data rates up to 9.6 Gbps, offering better performance in dense environments through technologies like Orthogonal Frequency-Division Multiple Access (OFDMA).

1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace? The two access points that are issuing most of the beacon frames have an SSID of “30 Munroe St” and “linsys_SES_24086”

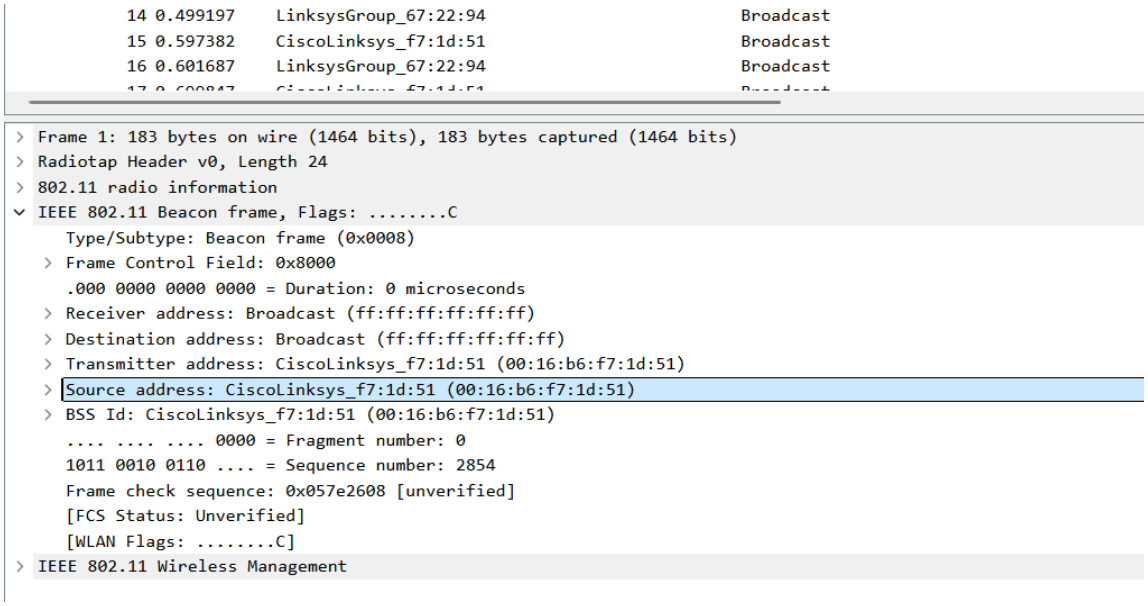


2. What are the intervals of time between the transmissions of the beacon frames the linksys_ses_24086 access point? From the 30 Munroe St. access point?
   The beacon interval for both access points in reported in the Beacon Interval of the 802.11 wireless LAN Management frame as .1024 seconds (i.e., just over 100 milliseconds).



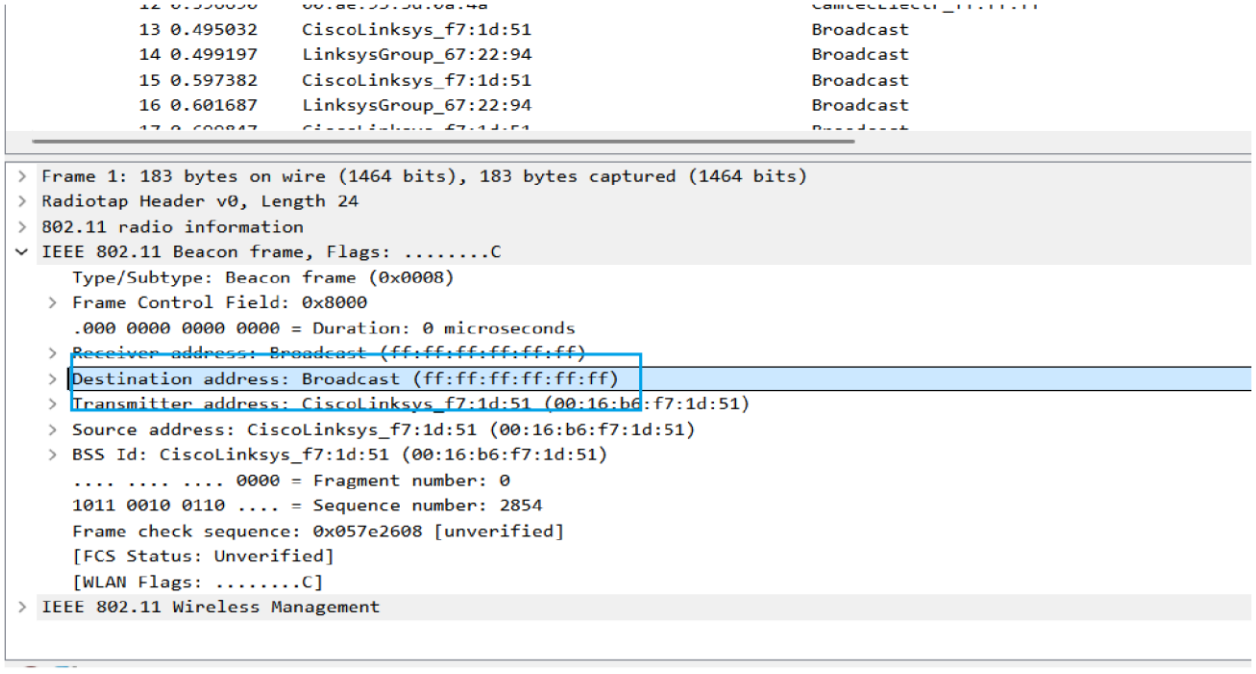
3. What (in hexadecimal notation) is the source MAC address on the beacon frame from 30 Munroe St? Recallfrom Figure 6.13 in the text that the source, destination, and BSS are three addresses used in an 802.11frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE 802.11 standards document (cited above).

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



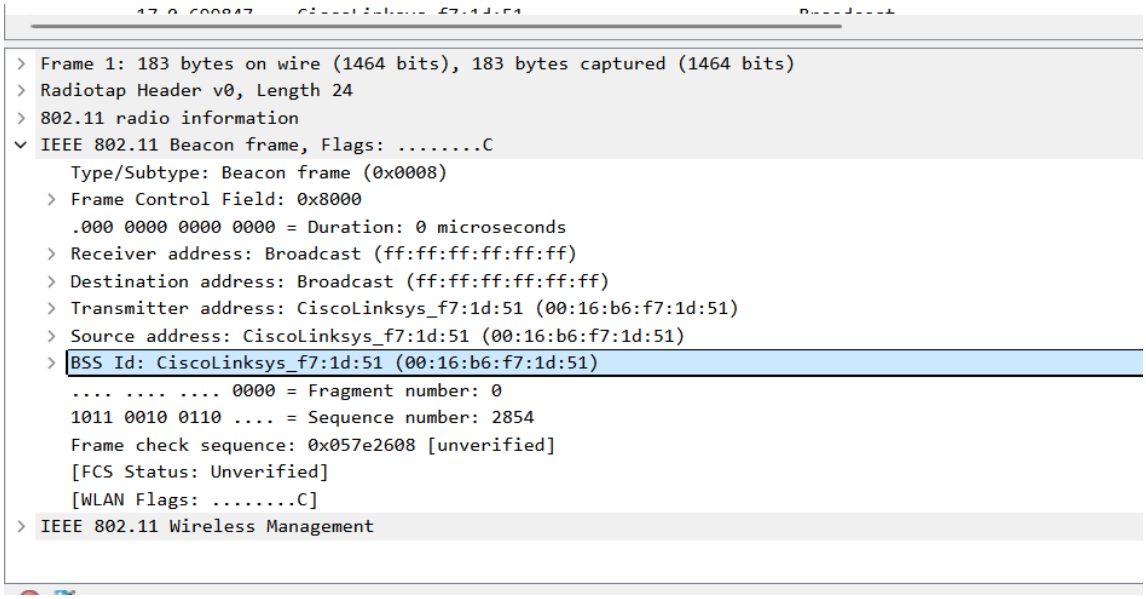
4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St?

Ans : The destination MAC address on the 30 Munroe St, beacon frame isff:ff:ff:ff:ff:ff, i.e., the Ethernet broadcast address.



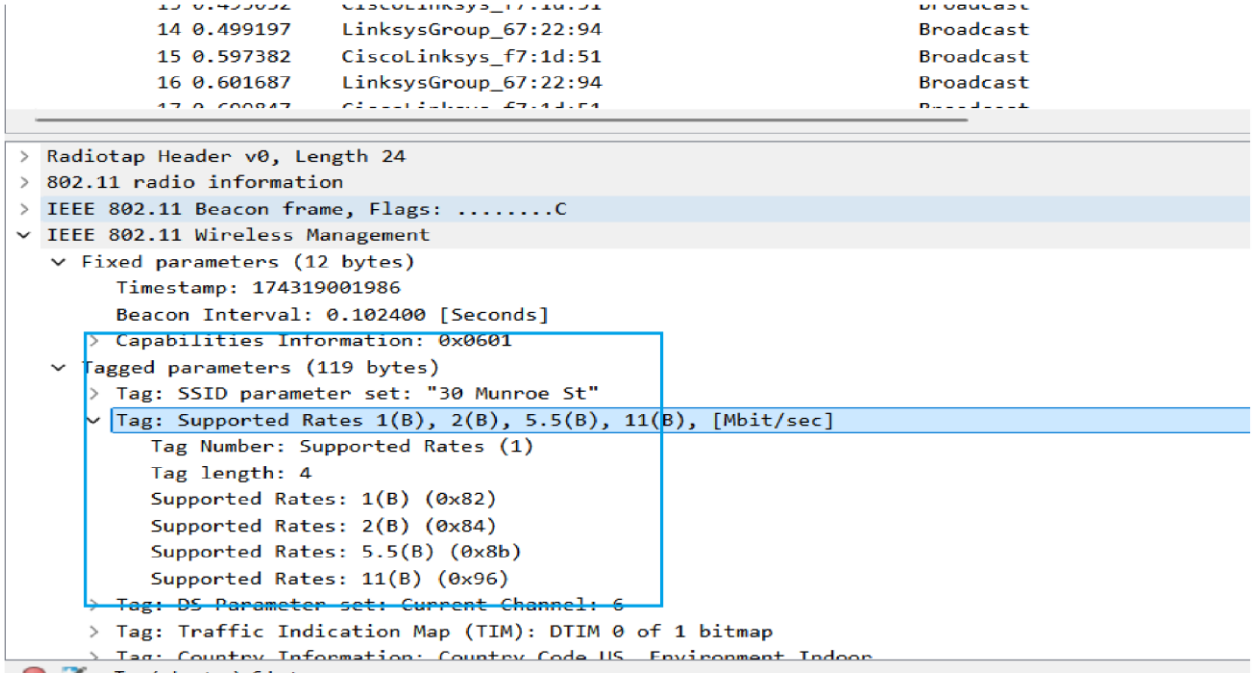
5. What (in hexadecimal notation) is the MAC BSS IS on the beacon frame from 30 Munroe St?

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



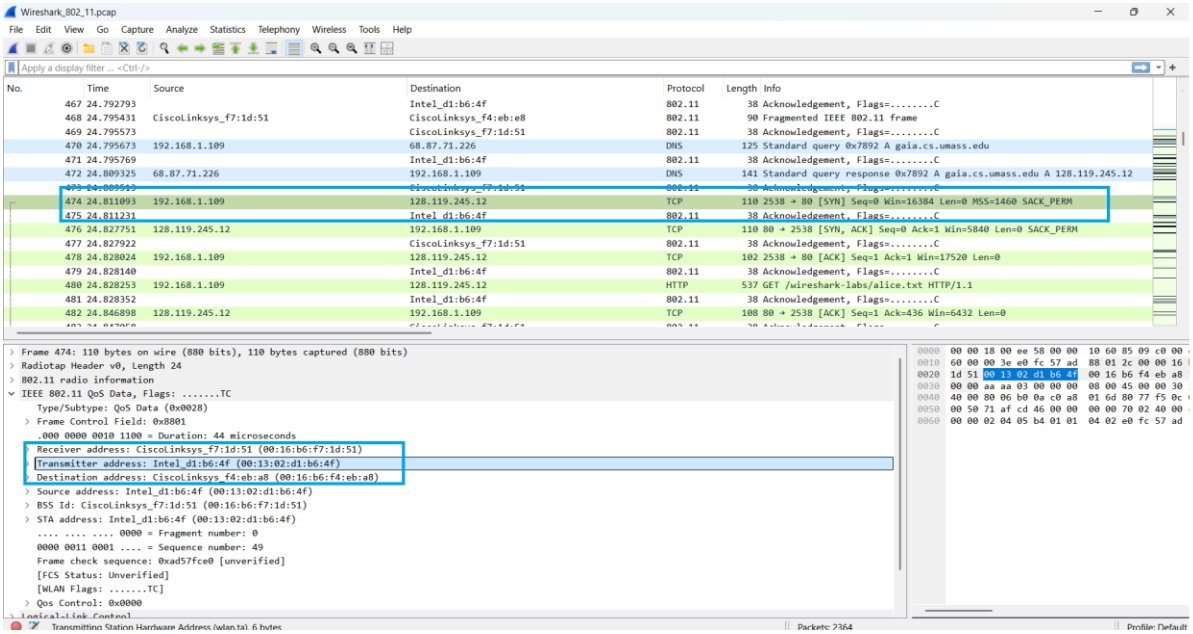
6. The beacon frames from the 30 Munroe St access point advertise that the access point can support four data rates and eight additional “extended supported rates.” What are these rates?

Ans : The support rates are 1.0, 2.0, 5.5, 11.0 Mbps. The extended rates are 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0
and 54.0 Mbps

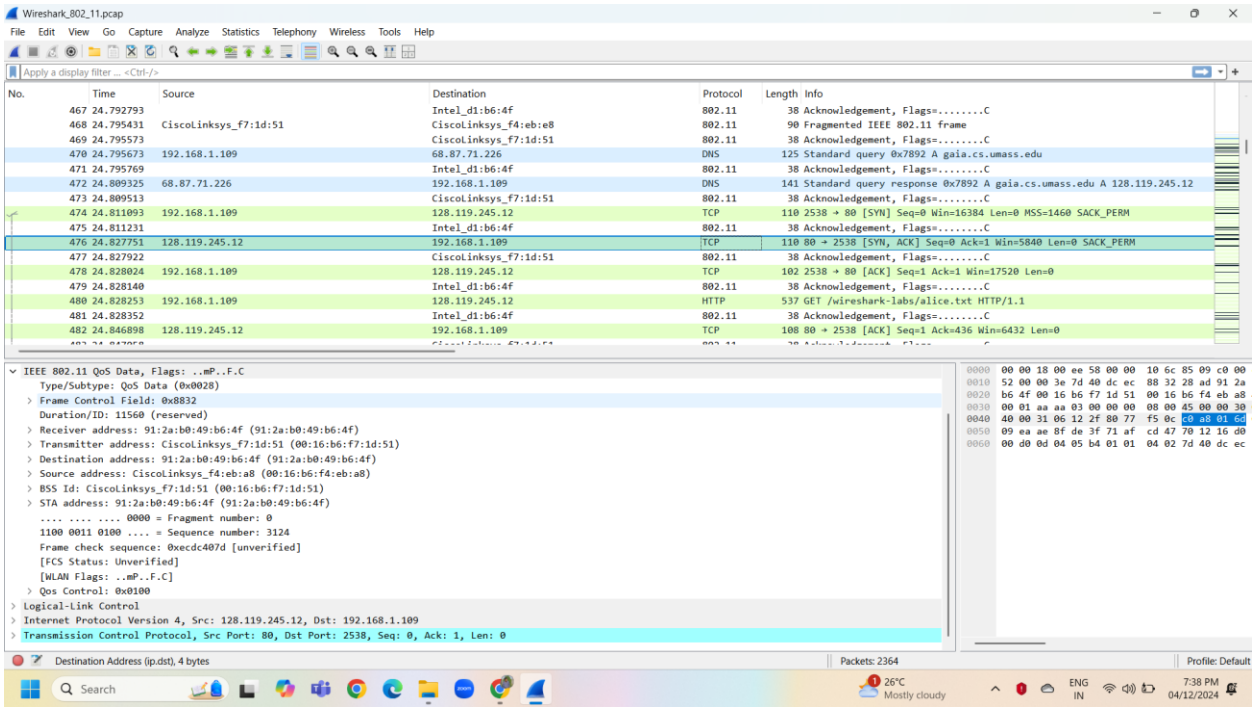


7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt).What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)? 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?

Ans : the TCP SYN is sent at t = 24.811093 seconds into the trace. The MAC address for the host sending the TCP SYN is 00:13:02:d1:b6:4f. The MAC address for the BSS is 00:16:b6:f7:1d:51. The IP address of the host sending the TCP SYN is 192.168.1.109.

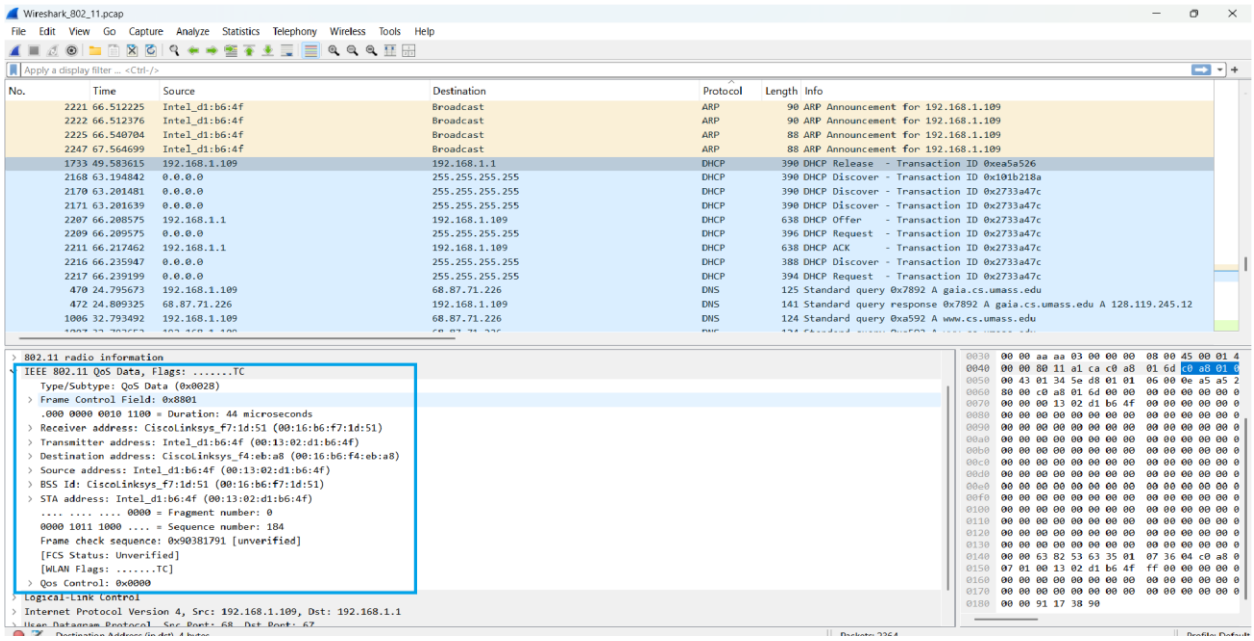


8. Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram



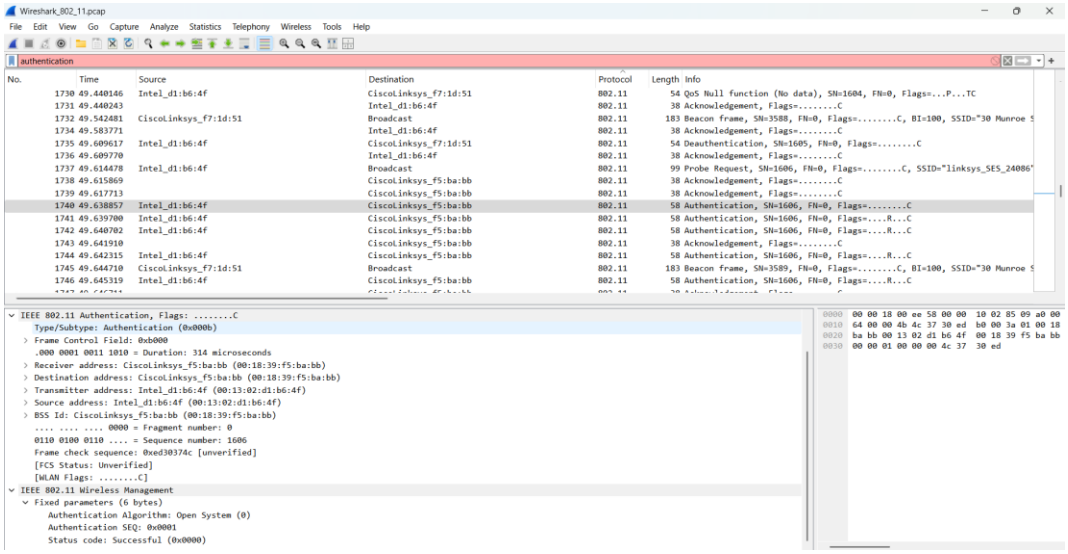
9. What two actions are taken (i.e., frames are sent) by the host in the trace just after t=49, to end the association with the 30 Munroe St AP that was initially in place when trace collection began

Ans: 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 (Frametype = 00 [Management], subframe type = 12[Deauthentication]).



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?

Ans : The first AUTHENTICATION from the host to the AP is at t = 49.638857.



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

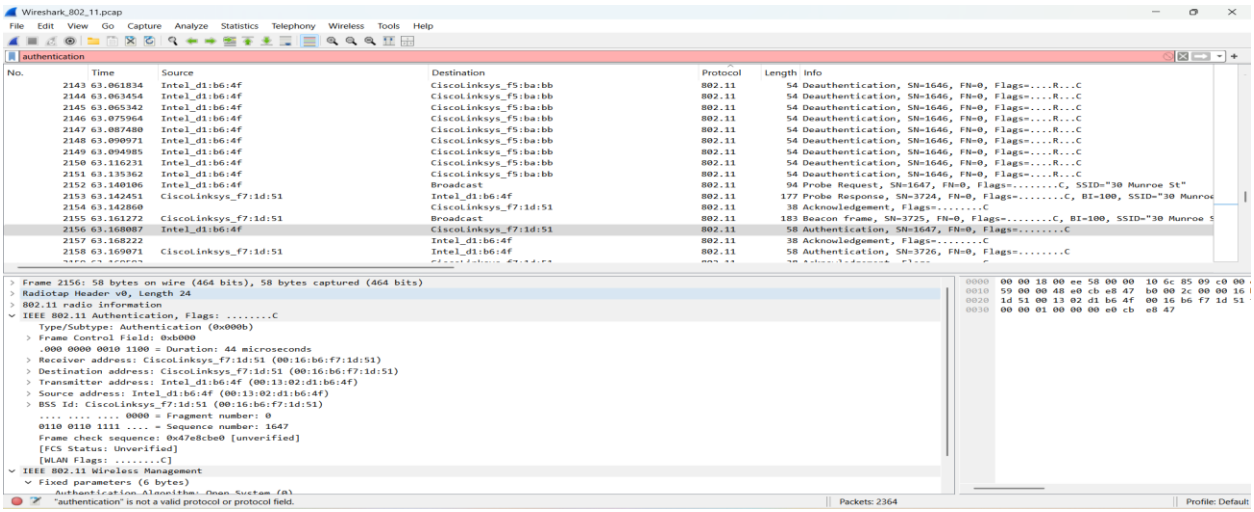
Ans : The host is requesting that the association be open .

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

Ans : I can’t find any reply from the AP. This is probably because the AP is configured to require a key when associating with that AP,so the AP is likely ignoring (i.e., not responding to) requests for open access.

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.

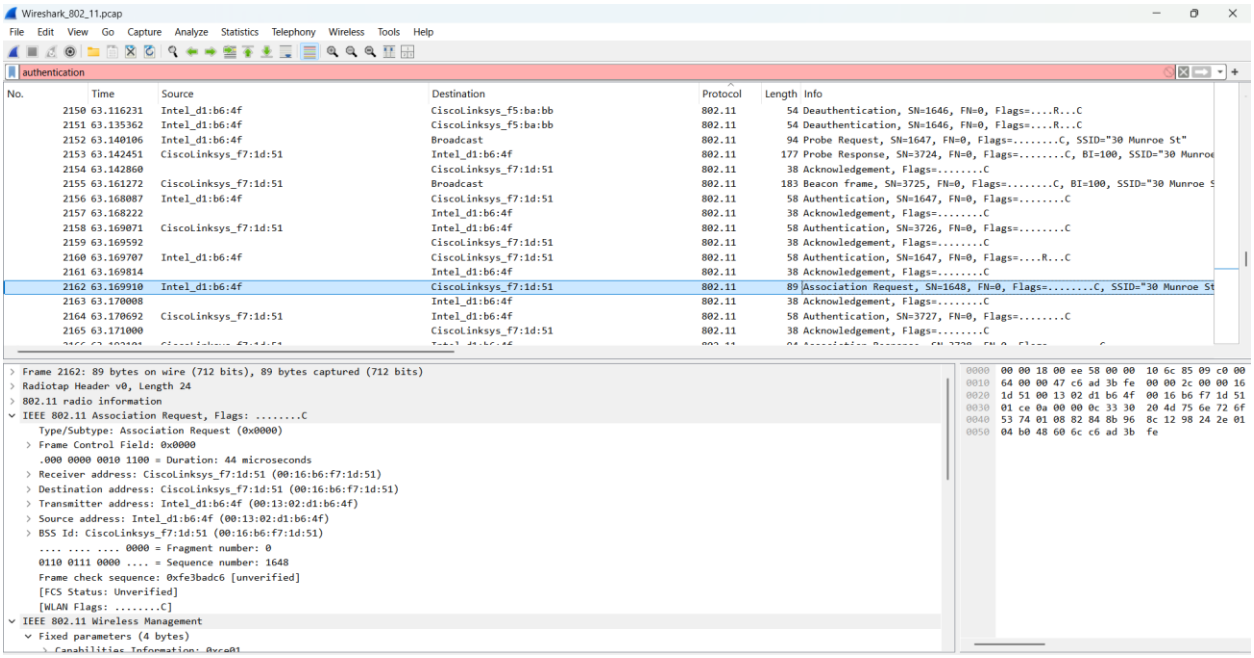
Ans :



At t = 63.168087 there is a AUTHENTICATION frame sent from 00:13:02: d1:b6:4f (the wireless host) to 00:16:b7:f7:1d:51 (the BSS). At t = 63.169071 there is an AUTHENTICATION from sent in the reverse direction from the BSS to the wireless host

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?

Ans : At t = 63.169910 there is a ASSOCIATE REQUEST frame sent from 00:13:02:d1:b6:4f (the wireless host) to 00:16:b7:f7:1d:51 (the BSS). At t = 63.192101 there is an ASSOCIATE RESPONSE from sent in the reverse direction from the BSS to the wireless host

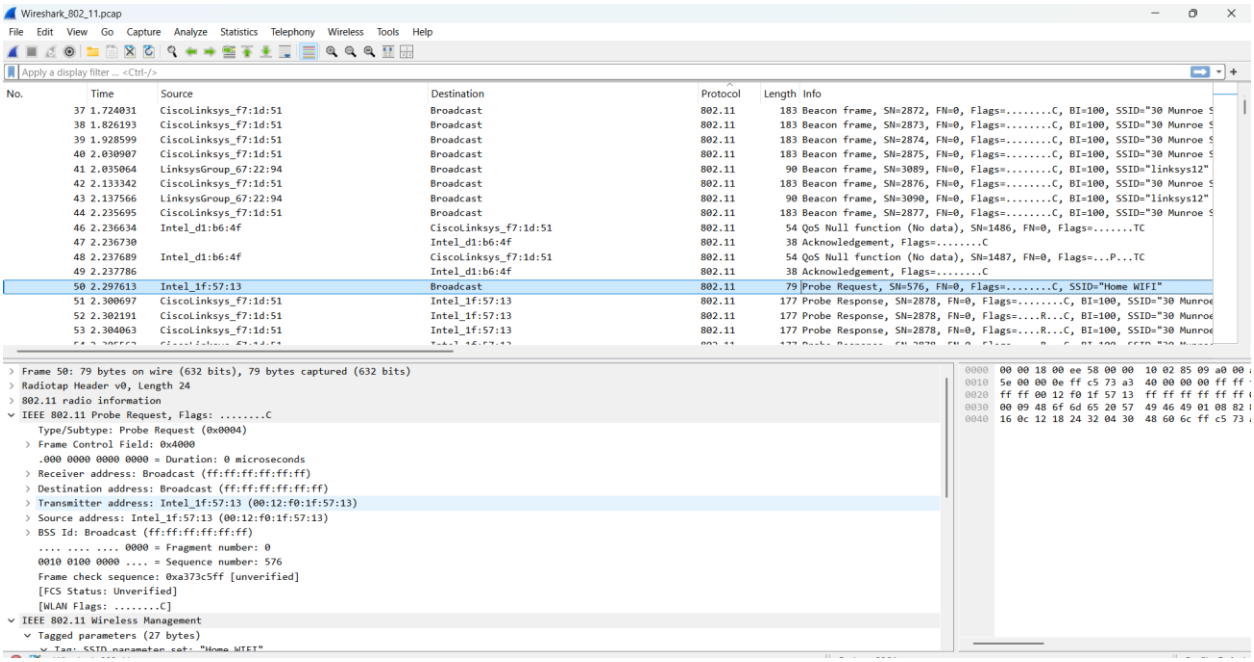


15. What transmission rates is the host willing to use? The AP? To answer this question, you will need to look into the parameters fields of the 802.11 wireless LAN management frame.

Ans : 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?

Ans : At t = 2.297613 there is a PROBE REQUEST sent with source 00:12:f0:1f:57:13, destination: ff:ff:ff:ff:ff:ff, and a BSSID of ff:ff:ff:ff:ff:ff. At t = 2.300697 there is a PROBE RESPONSE sent with source: 00:16:b6:f7:1d:51, destination and a BSSID of 00:16:b6:f7:1d:51


Wireshark_802_11.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
37 1.724031 CiscoLinksys_f7:1d:51 Broadcast 802.11 183 Beacon frame, SN=2872, FN=0, Flags=........C, BI=100, SSID="30 Munroe S
38 1.826193 CiscoLinksys_f7:1d:51 Broadcast 802.11 183 Beacon frame, SN=2873, FN=0, Flags=........C, BI=100, SSID="30 Munroe S
39 1.928599 CiscoLinksys_f7:1d:51 Broadcast 802.11 183 Beacon frame, SN=2874, FN=0, Flags=........C, BI=100, SSID="30 Munroe S
40 2.030907 CiscoLinksys_f7:1d:51 Broadcast 802.11 183 Beacon frame, SN=2875, FN=0, Flags=........C, BI=100, SSID="30 Munroe S
41 2.035064 LinksysGroup_67:22:94 Broadcast 802.11 90 Beacon frame, SN=3089, FN=0, Flags=........C, BI=100, SSID="linksys12"
42 2.133342 CiscoLinksys_f7:1d:51 Broadcast 802.11 183 Beacon frame, SN=2876, FN=0, Flags=........C, BI=100, SSID="30 Munroe S
43 2.137566 LinksysGroup_67:22:94 Broadcast 802.11 90 Beacon frame, SN=3090, FN=0, Flags=........C, BI=100, SSID="linksys12"
44 2.235695 CiscoLinksys_f7:1d:51 Broadcast 802.11 183 Beacon frame, SN=2877, FN=0, Flags=........C, BI=100, SSID="30 Munroe S
46 2.236634 Intel_d1:b6:4f CiscoLinksys_f7:1d:51 802.11 54 QoS Null function (No data), SN=1486, FN=0, Flags=.......TC
47 2.236730 Intel_d1:b6:4f 802.11 38 Acknowledgement, Flags=........C
48 2.237689 Intel_d1:b6:4f CiscoLinksys_f7:1d:51 802.11 54 QoS Null function (No data), SN=1487, FN=0, Flags=...P...TC
49 2.237786 Intel_d1:b6:4f 802.11 38 Acknowledgement, Flags=........C
50 2.297613 Intel_1f:57:13 Broadcast 802.11 79 Probe Request, SN=576, FN=0, Flags=........C, SSID="Home WIFI"
51 2.300697 CiscoLinksys_f7:1d:51 Intel_1f:57:13 802.11 177 Probe Response, SN=2878, FN=0, Flags=........C, BI=100, SSID="30 Munroe
52 2.302191 CiscoLinksys_f7:1d:51 Intel_1f:57:13 802.11 177 Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID="30 Munroe
53 2.304063 CiscoLinksys_f7:1d:51 Intel_1f:57:13 802.11 177 Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID="30 Munroe
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
.000 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: Intel_1f:57:13 (00:12:f0:1f:57:13)
Source address: Intel_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]
[FCS Status: Unverified]
[WLAN Flags: ....C]
IEEE 802.11 Wireless Management
Tagged parameters (27 bytes)
0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00
0010 5e 00 00 0e ff c5 73 a3 40 00 00 00 ff ff
0020 ff ff 00 12 f0 1f 57 13 ff ff ff ff ff ff
0030 00 09 48 6f 6d 65 20 57 49 46 49 01 08 82
0040 16 0c 12 18 24 32 04 30 48 60 6c ff c5 73