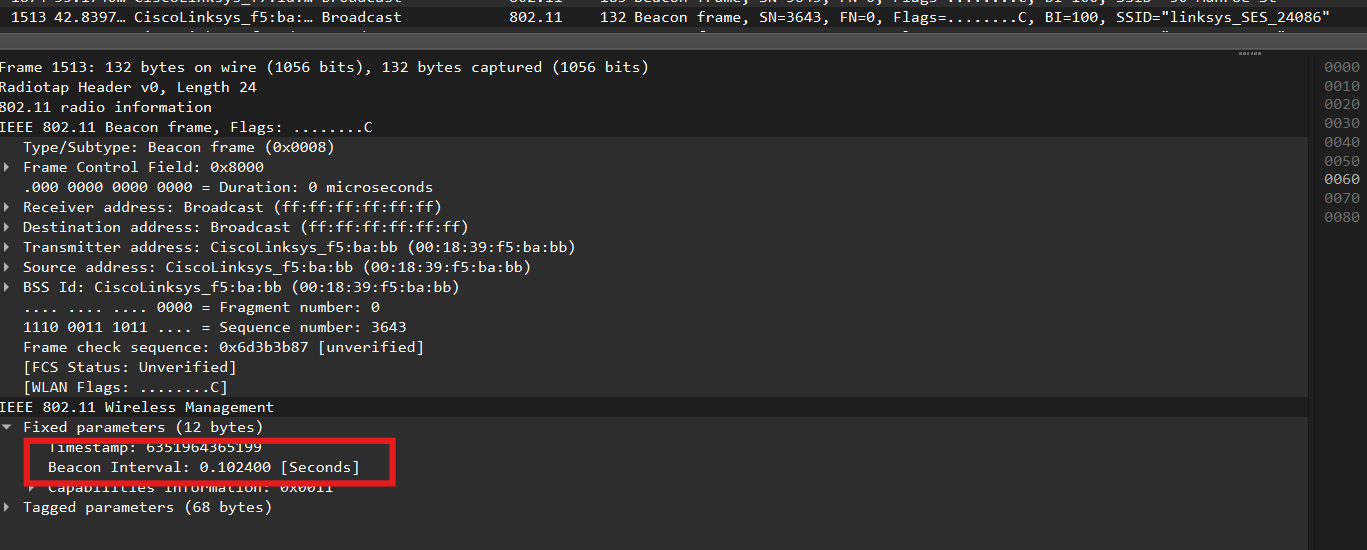
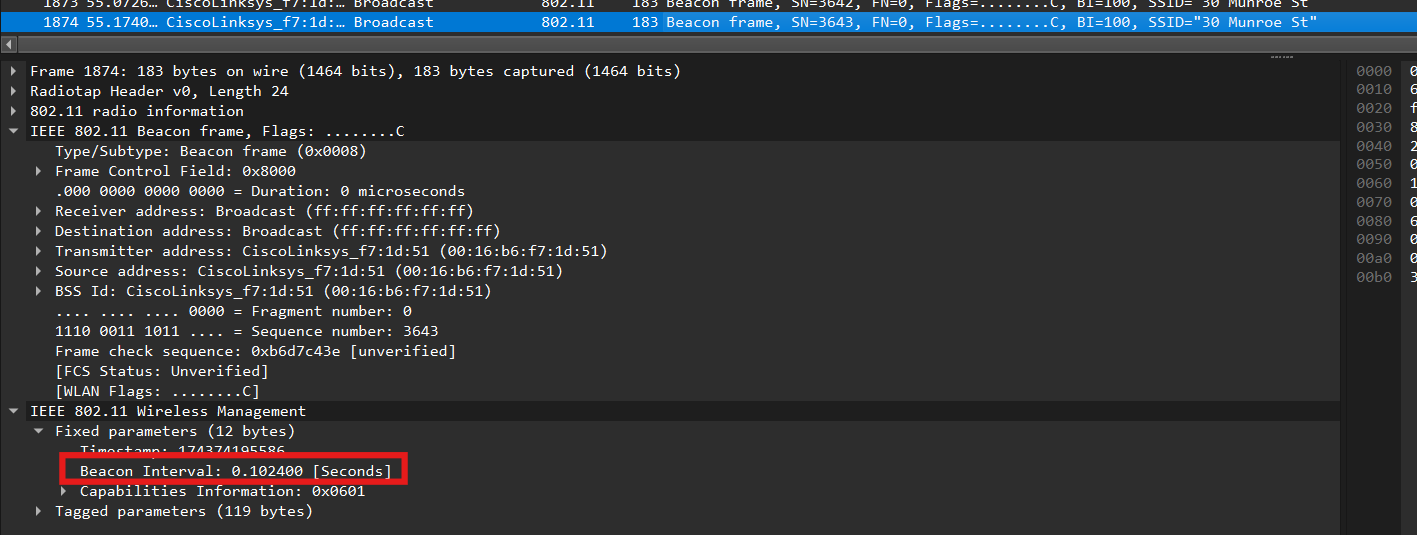
1. Through the command wlan.fc.type\_subtype == 0x08, we can filter SSIDs as follows: “30 Munroe St”, “linksys\_SES\_24086”, “linksys12”, “linksys1R”,…

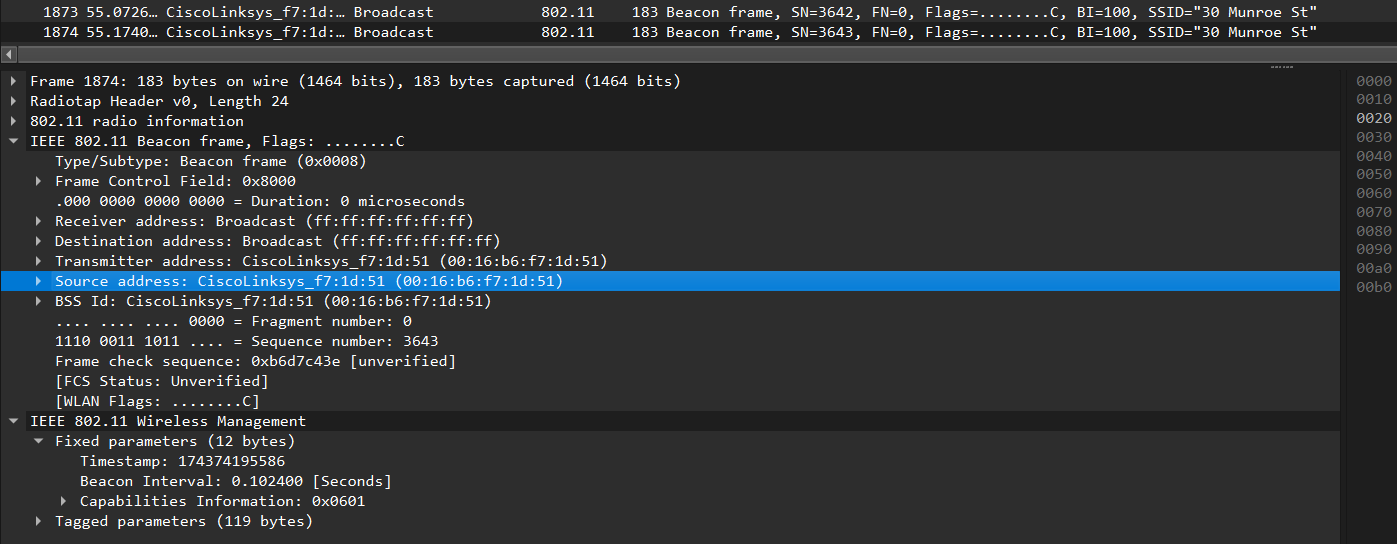
“30 Munroe St” can be found that detects the most beacon frames, but there are very few so I would expect “linksys\_SES\_24086”.

1. Cả hai đều là 0.102400 seconds





3.



Src MAC: 00:16:b6:f7:1d:51

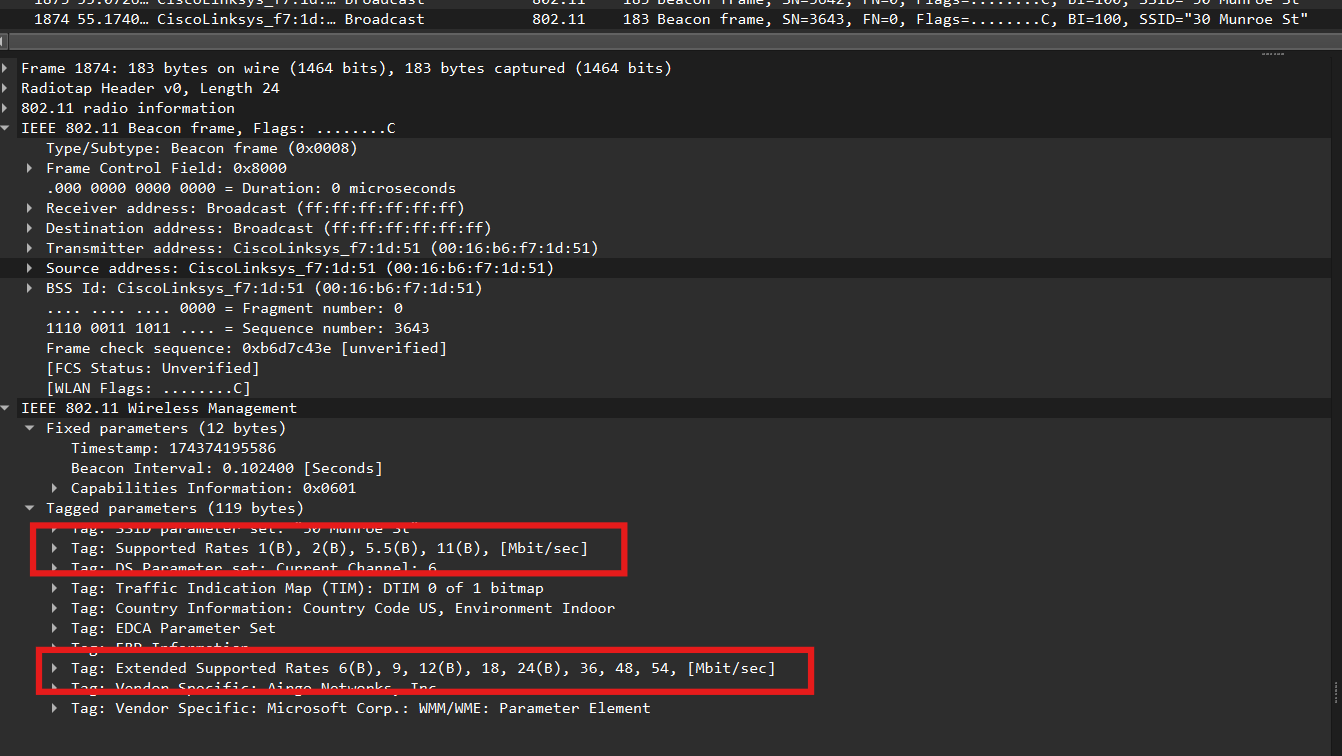
4.

Dst MAC: ff:ff:ff:ff:ff:ff

5.

MAC BSS Id: 00:16:b6:f7:1d:51

6.

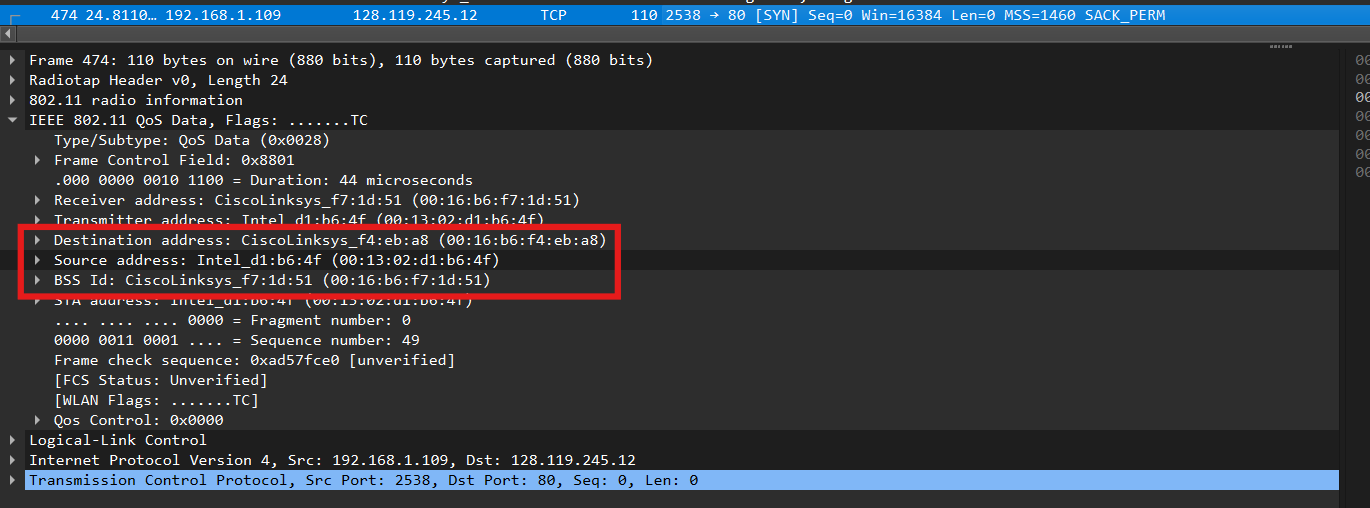


Four supported data rates: 1, 2, 5.5, 11 (Mbit/sec)

Eight extended supported rates: 6, 9, 12, 18, 24, 36, 48, 54 (Mbit/sec)

7.

The 802.11 frame containing the SYN TCP segment for this first TCP session is packet number474, at time t = 24.811093

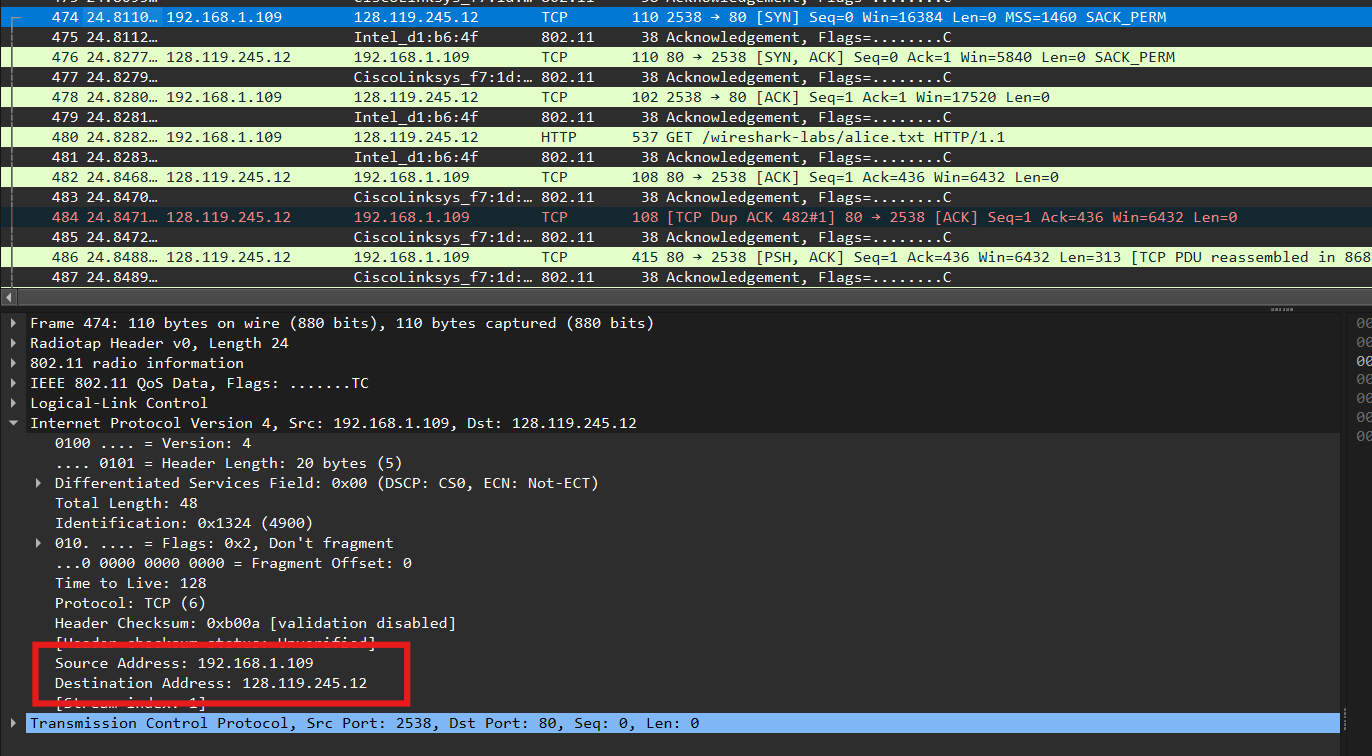


Three MAC address fields in the 802.11 frame:

+ 00:16:b6:f4:eb:a8  The MAC address for Destination corresponds to first-hop router

+ 00:13:02:d1:b6:4f  The MAC address for the host sending the TCP SYN corresponds to wireless host

+ 00:16:b6:f7:1d:51  The MAC address for the BSS corresponds to access point

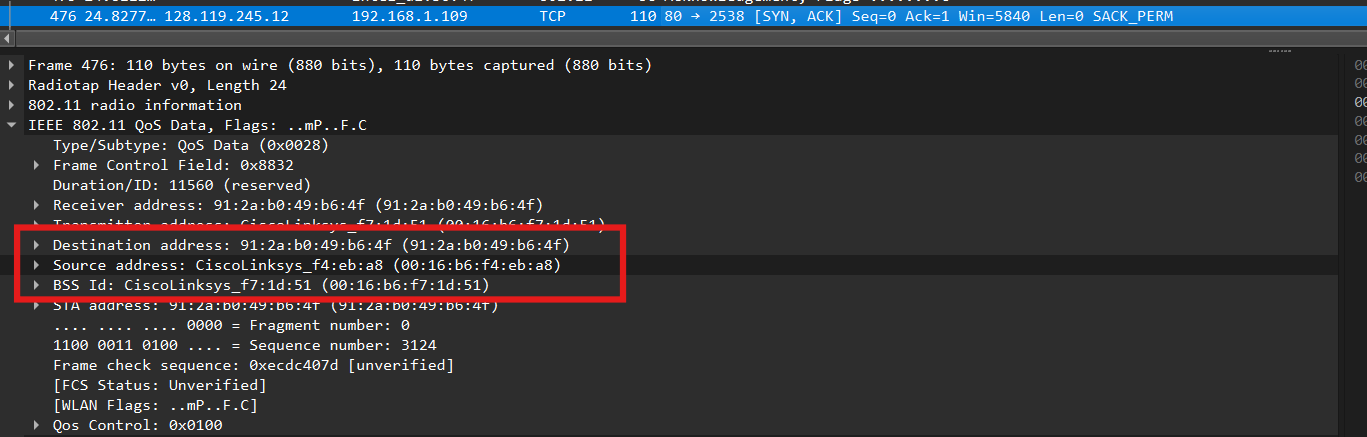


The IP address of the wireless host sending this TCP segment is 192.168.1.109 (NATedaddress)

The destination IP address is 128.119.245.12. This destination IP address corresponds to the server gaia.cs.umass.edu (Note that: the destination MAC address containing the SYNcorresponds to first-hop router, while the destination IP address corresponds to the server).Because this is the SYN message between the host and the server so the destination IPaddress is meant to direct the packet to the Server (not any network devices)

8.

The 802.11 frame containing the SYNACK segment for this TCP session is packet number 476,at time t = 24.827751

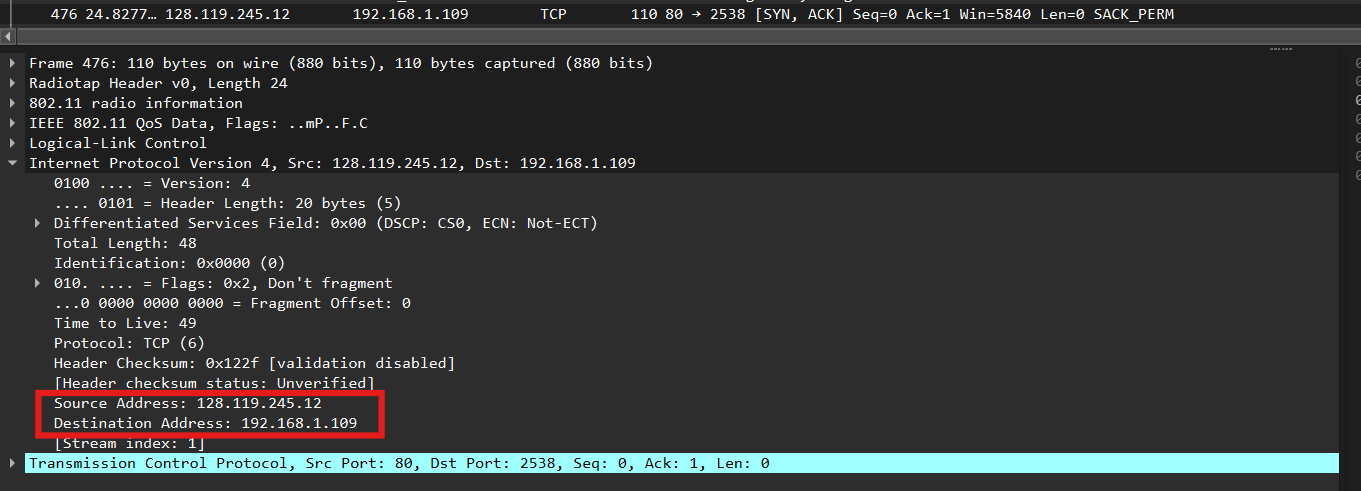


Three MAC address fields in the 802.11 frame are:

+ 91:2a:b0:49:b6:4f The MAC address for destination corresponds to the host

+ 00:16:b6:f4:eb:a8 The MAC address for the source (the sender of 802.11 frame containing TCP SYNACK segment) corresponds to the first-hop router

+ 00:16:b6:f7:1d:51 The MAC address for BSS corresponds to the access point



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 IPaddress is 128:199:245:12 but the destination IP address is 192.168.1.109.

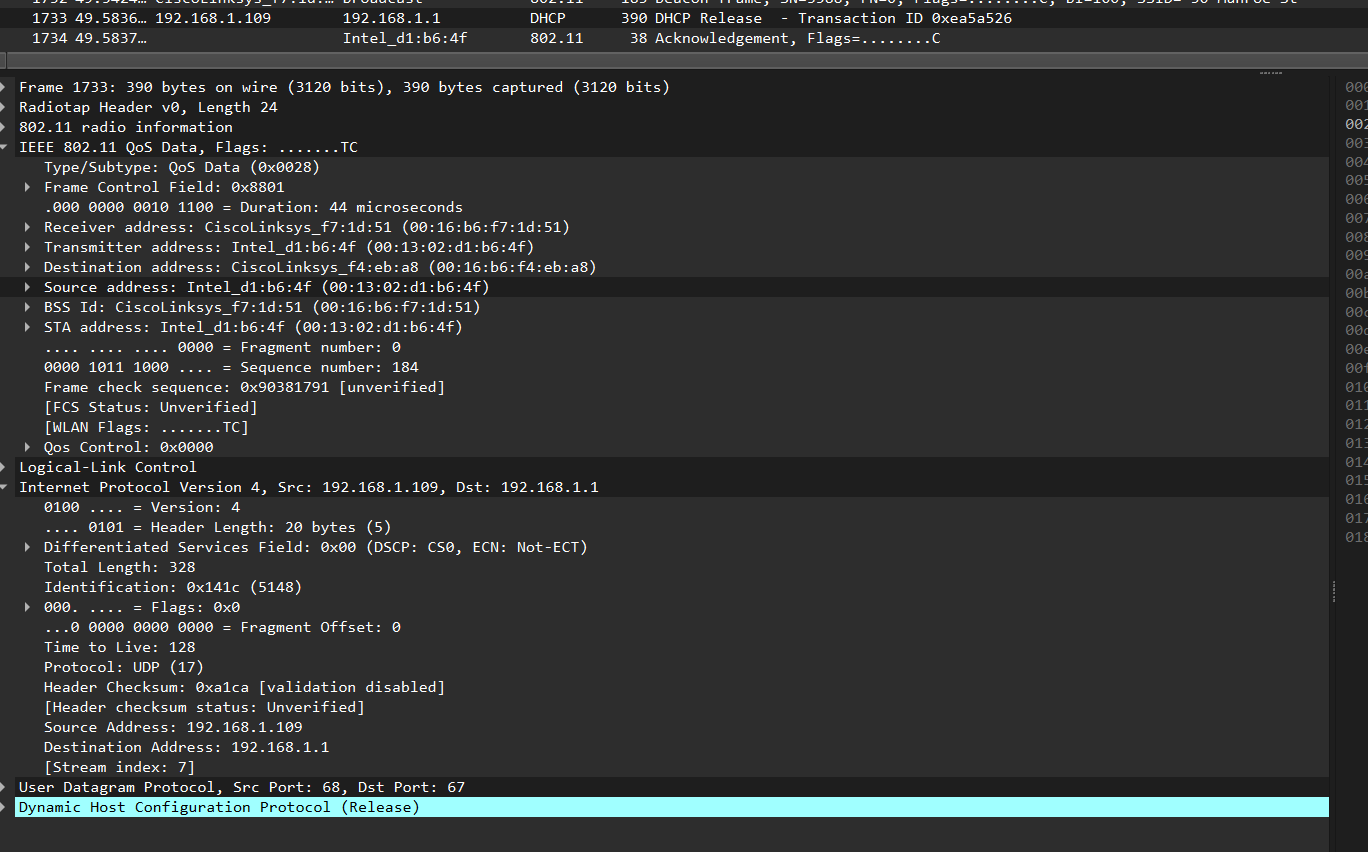
9.

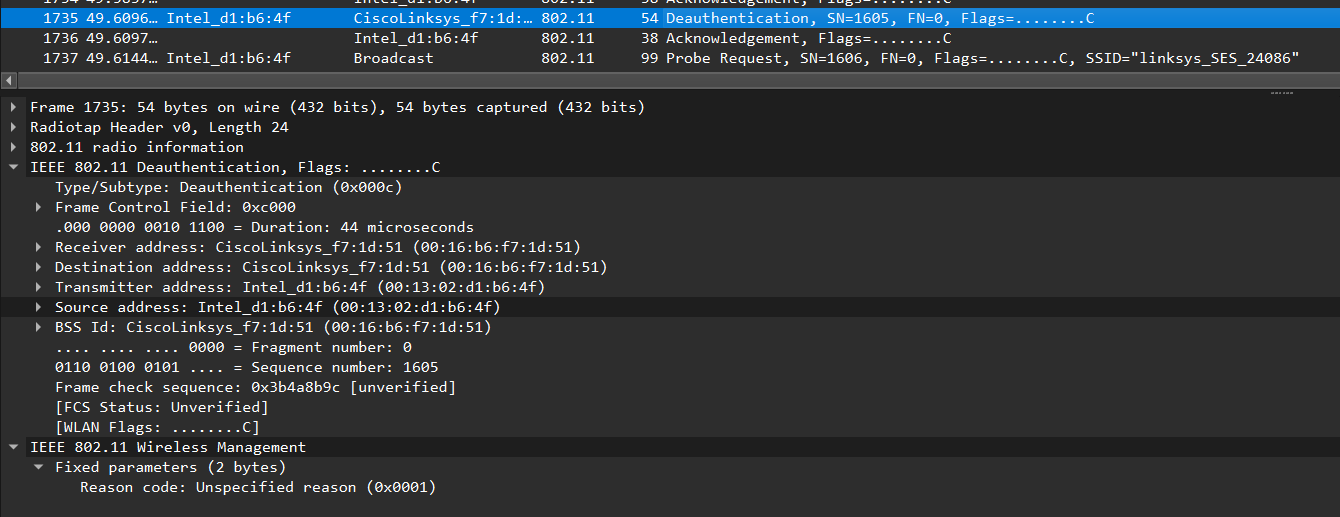
- Two actions taken by the host:

+ The host sends the DCHP release to return the IP Address to the DHCP server (IP address is192.168.1.1) at time t = 49.583615 (packet number 1733)

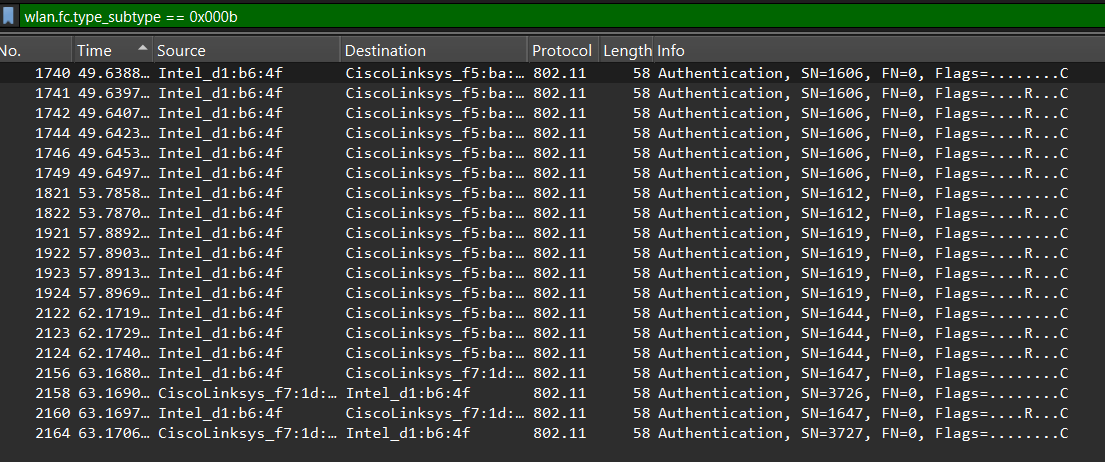
+ The host sends the Deauthentication frame to end the association with 30 Munroe ST at t =49.609617 (packet number 1735)

-Another frame that I expected to see is Disassociation request



10.

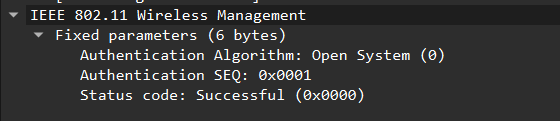
There are 15 AUTHENTICATION messages are sent from the wireless host to thelinksys\_ses\_24086 AP (which has a MAC address of Cisco\_Li\_f5:ba:bb) starting at around t=49. The below picture will show 15 AUTHENTICATION messages:



11.

The host wants the authentication to be open

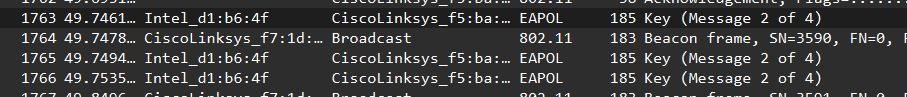
Because we look at “Authentication Algorithm” field, we can see that “Open System (0)”



12.

I can’t see any reply AUTHENTICATION from the linksys\_ses\_24086 AP in the trace.

Because the AP is set to require a key for authentication. This means it will not respond to open (unauthenticated) requests. You see other frames related to a secure handshake or encryption key exchange (EAPOL frames for WPA2/WPA3) instead.



13.

- At time t = 63.168087 (packet number 2156), there is a Authentication frame sent from thehost (00:13:02:d1:b6:4f ) to the AP (00:16:b7:f7:1d:51)

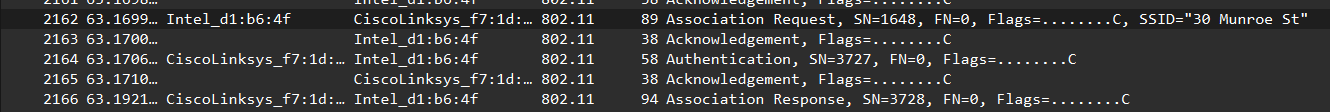
- At time t = 63.169071 (packet number 2158), there is an Authentication sent from the AP(00:16:b7:f7:1d:51) to the host (00:13:02:d1:b6:4f )



14.

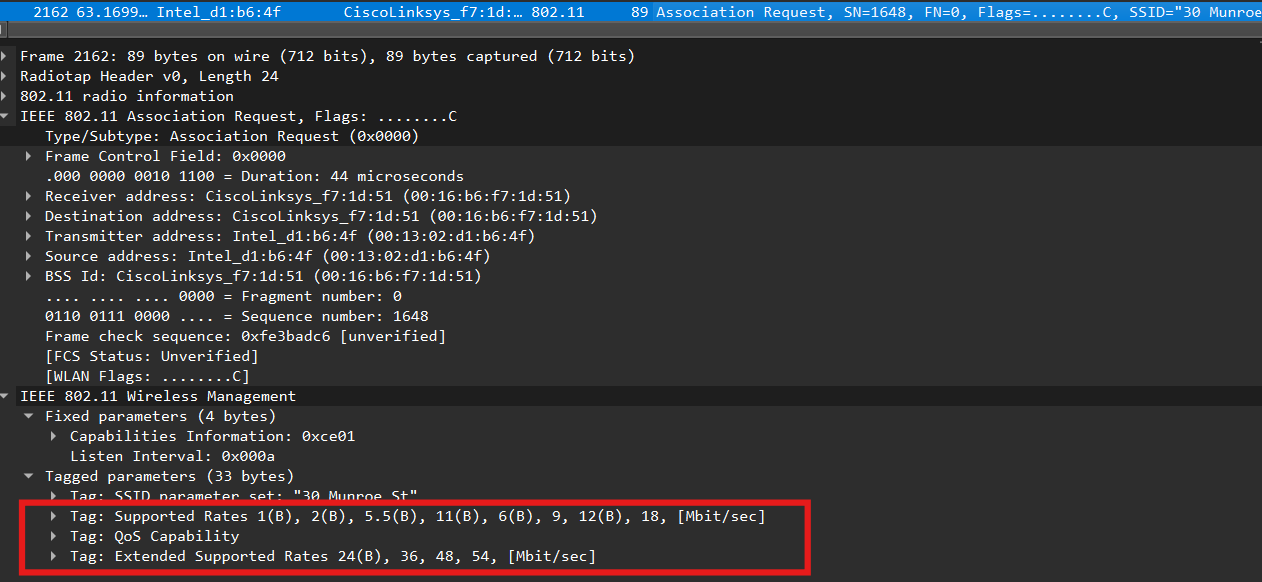
- At time t = 63.169910 (packet number 2162), there is a Association Request sent from thehost (00:13:02:d1:b6:4f ) to the AP (00:16:b7:f7:1d:51)

- At time t = 63.192101 (packet number 2166), there is an Association Response sent from theAP (00:16:b7:f7:1d:51) to the host (00:13:02:d1:b6:4f )

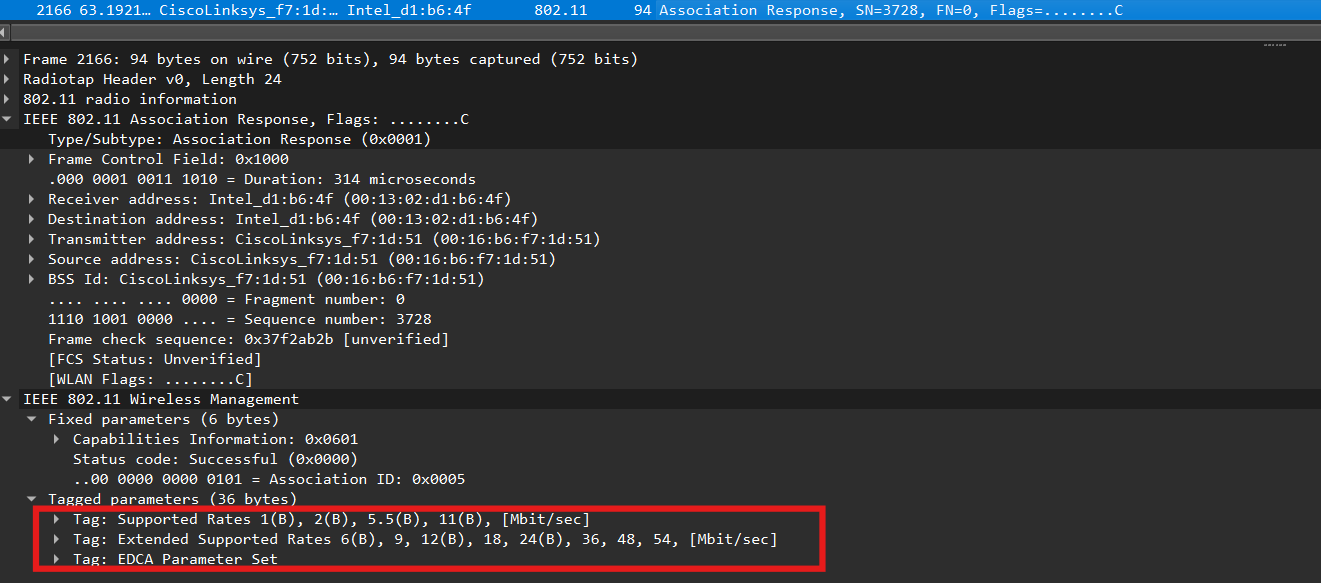


15.

- Transmission rates that the host (ASSOCIATION REQUEST) willing to use are 1, 2, 5.5, 11, 6, 9,12, 18, 24, 36, 48, 54 (Mbit/sec)

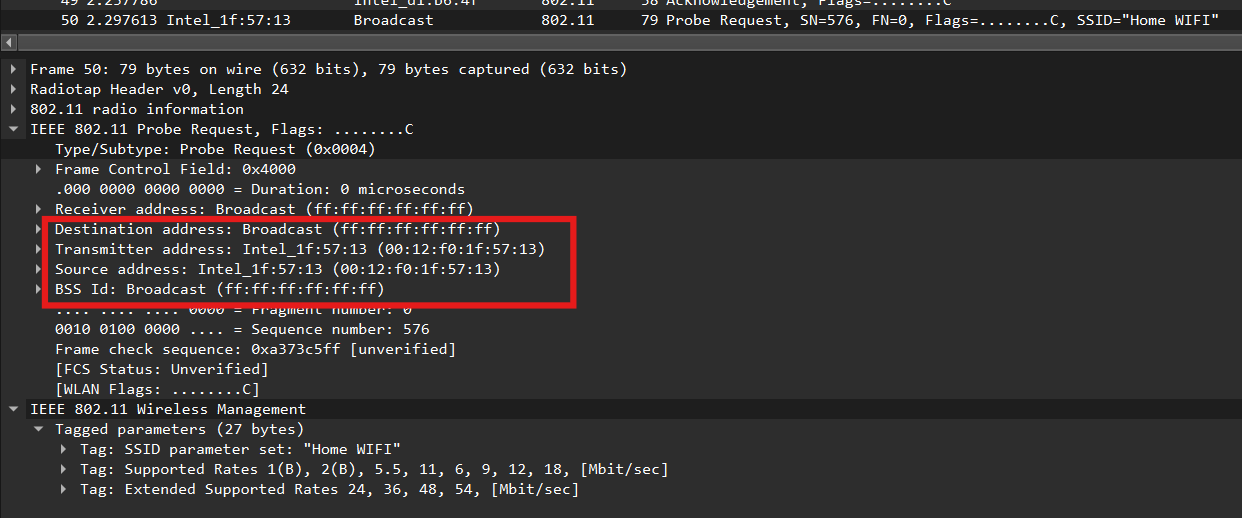


- Transmission rates that the AP (ASSOCIATION RESPONSE) willing to use are 1, 2, 5.5, 11, 6, 9,12, 18, 24, 36, 48, 54 (Mbit/sec)



16.

With packet number 50, at time t = 2.297613: we can find a PROBE REQUEST, which has sourceaddress 00:12:f0:1f:57:13, destination address ff:ff:ff:ff:ff:ff, and BSS ID ff:ff:ff:ff:ff:ff



With packet number 51, at time t =2.300697: we can find a PROBE RESPONSE, which has source address 00:16:b6:f7:1d:51, destination address 00:12:f0:1f:57:13, and BSS ID 00:16:b6:f7:1d:51

