Data Communications Assignment 2

Stefan Mahabeer Ahmed

21359035

May 2019

ELement 1

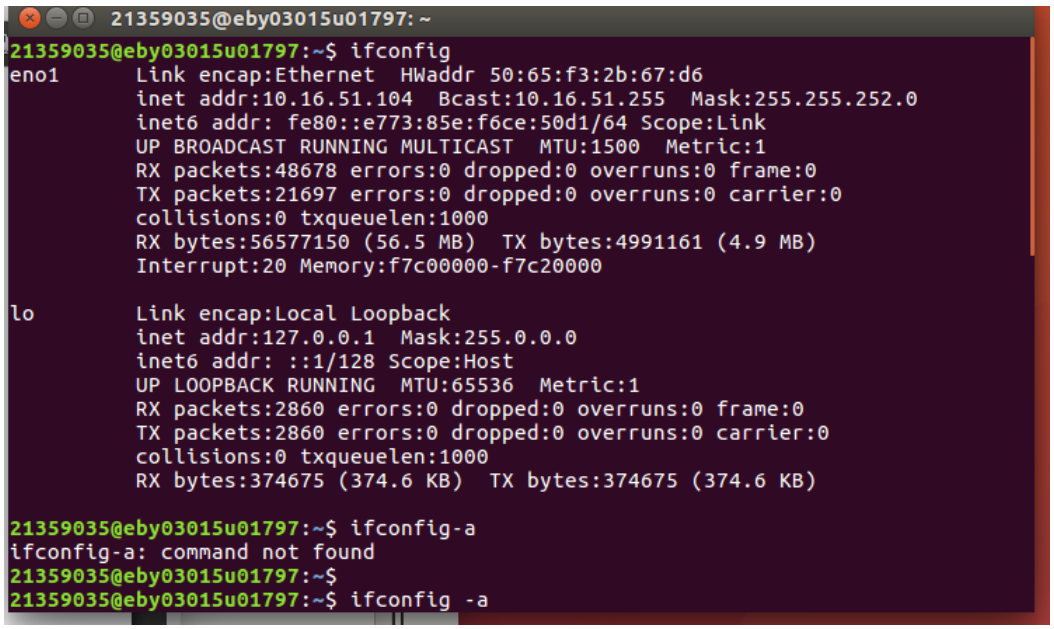
This element is about network interfaces which are how the devices are connected to a network, whether they are wired or wireless.

Network interfaces can be detected by using prompts on a computer when the devices which have the interface are connected to a network. There are certain lines of prompts to use to pick up interfaces and have details of them displayed on the computer screen. This section focuses on typing these prompts as commands to find details of available network interfaces.

1.

A1. find out the MAC address and the allocated IP address for the

active network interfaces.



The MAC address is for the active network interface eno1 is 50:65:f3:2b:67:d6 as this is given as the HW address of the interface.

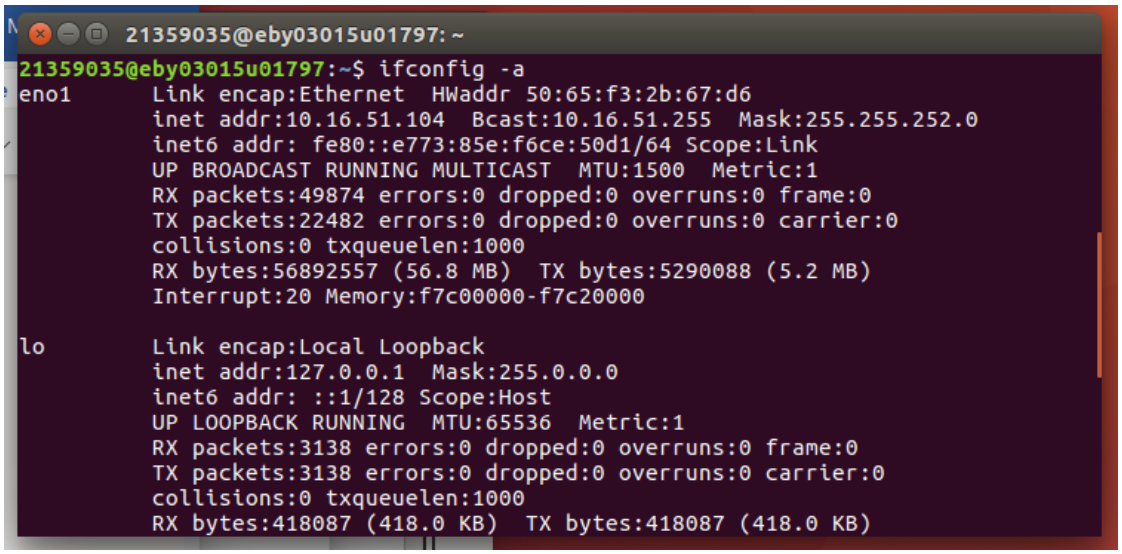
It's broadcast address might also count as the MAC address which is 10.16.51.255.

The allocated IP(Internet Protocol) address for eno1 is the inet address 10.16.51.104 since this is address is just numbers which an IP address usually consists of.

The inet6 address fe80::e773:85e:f6ce:50d1/64 may count as the allocated IP address although the allocated address is usually the first one.

The active network interface lo which is a loopback interface has a Mask address 255.0.0.0 which might also count as a MAC address.

The allocated IP address for lo is the inet address 127.0.0.1 since this is only numbers which an IP address usually consists of.



A2: Do you have a loopback interface being showed? If it is, explain

what are loopback interfaces and how they are used

The interface lo is a loopback interface which is being showed. A loopback interface is used to see whether or not a network can send or receive data.i.e. in the form of packets using the protocols TCP and IP between devices such as a computer and a server. Loopbacks are also used to test how well the connection between a computer i.e. client and a server is such as when the client communicates with the server to request a web page.

A3:

UP : This keyword when used in the prompt line is used to activate a network interface which is not yet activated or ready for communication.

BROADCAST: This keyword is used for setting a broadcast address to an interface. The address is used as an address of a network so that any device connected to the network receives data in the form of datagrams.

MULTICAST: This is a semantic used by devices that connect devices to a network known as a router. It is used to by a router to route data to other routers on a network to make themselves known to each other on the network. MULTICAST is used to route packets of data to many devices or even many packets to many devices.

MTU: This is the maximum transmission unit used for setting a size limit of packets of data before they are transmitted through an interface at any specific time. It is linked to the Ethernet card.

A6:

A routing table lists the details of data packets being sent and received and where they will be routed to.

Element 2

Intro

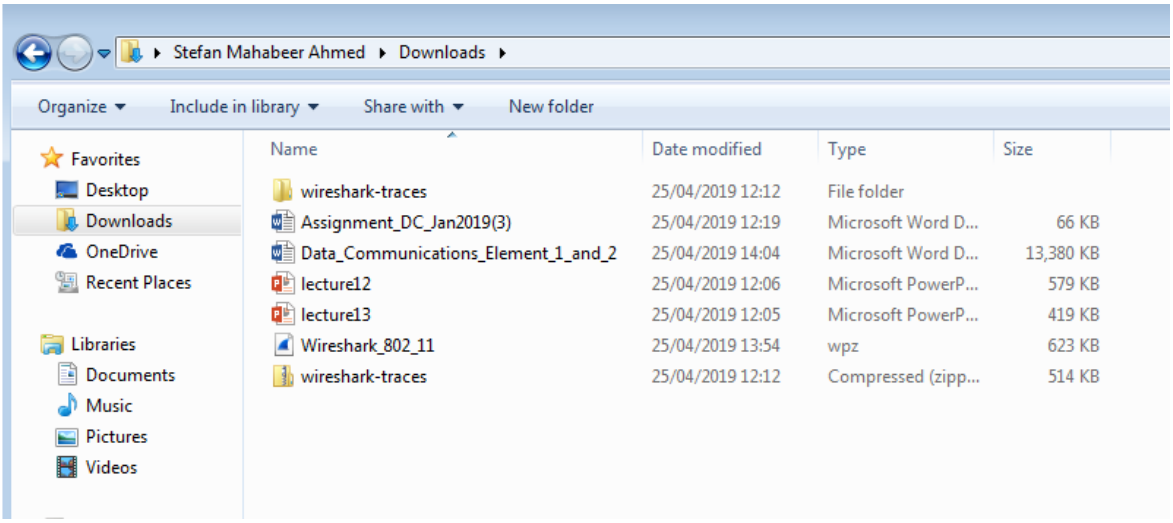
This element of the assignment is about wireless network connections. Devices connected as a network or to a network wirelessly.ie. without wires. We have the wired network connections where devices are connected using wires and cables such as an Ethernet cable (that looks and works just like a telephone cable) as a network or to a network. This section focuses on wireless network connections working too with wired connections where devices such as computers, mobile phones and servers connect to larger networks through transmitters, devices known as access points and stations known as base stations.

There is the local area network(LAN) being wireless known as 802.11 wireless LAN. This is used for wireless network connectivity and works by sending data to and from devices and access points for wireless connections. Data being sent is in the form of packets and data frames. There are also protocols used to send data between devices. A device has communicate with a station known as an access point and a router to connect to a larger network such as the internet.

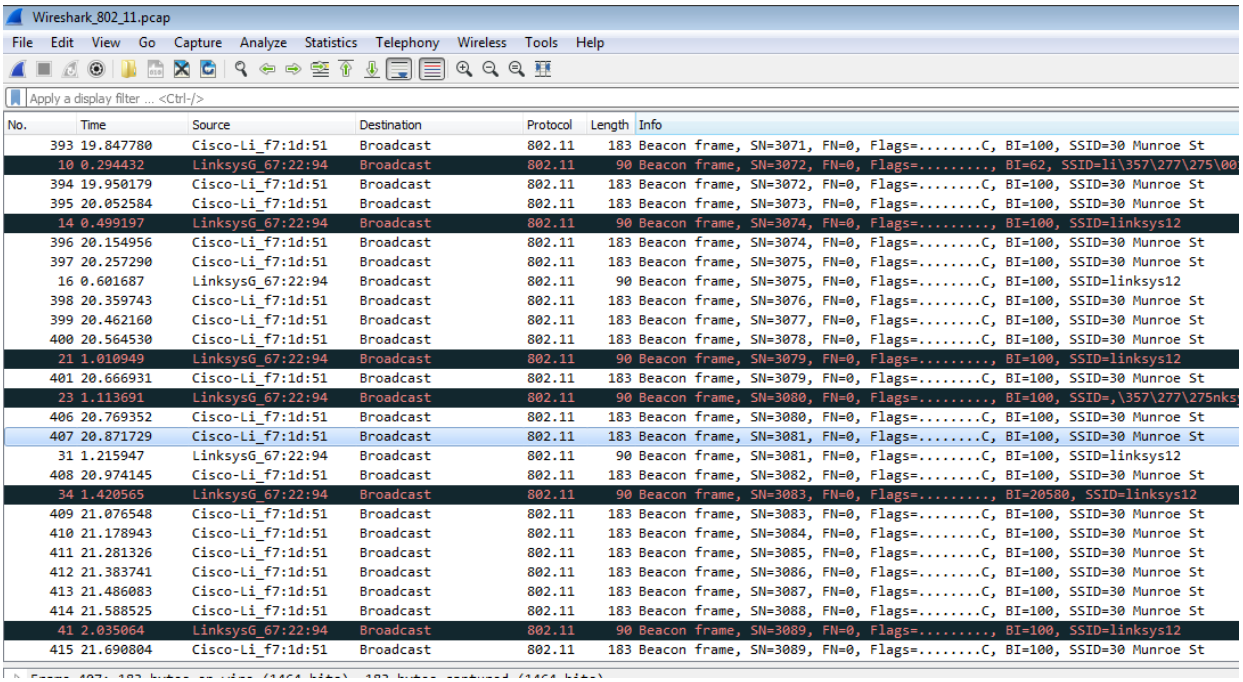
Devices such as computers, mobile phones and servers connect to larger networks such as the internet through access points, stations or base stations and routers. This involves them picking up data from the access points(AP's) or stations and data being sent back and forth between the two. Data being sent back and forth is in the form of frames and protocols being used for the sending.

This section focuses on using the packet sniffing tool Wireshark on the computer to capture data packets during a live wireless network connection and study the captured packets by opening them. The packets captured contain data frames such as beacon frames with details of protocols, addresses, transmission and other necessary information.

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



First the downloaded trace file captured using Wireshark packet sniffing tool and Airpcap is in stored in the downloads folder and opened from there.



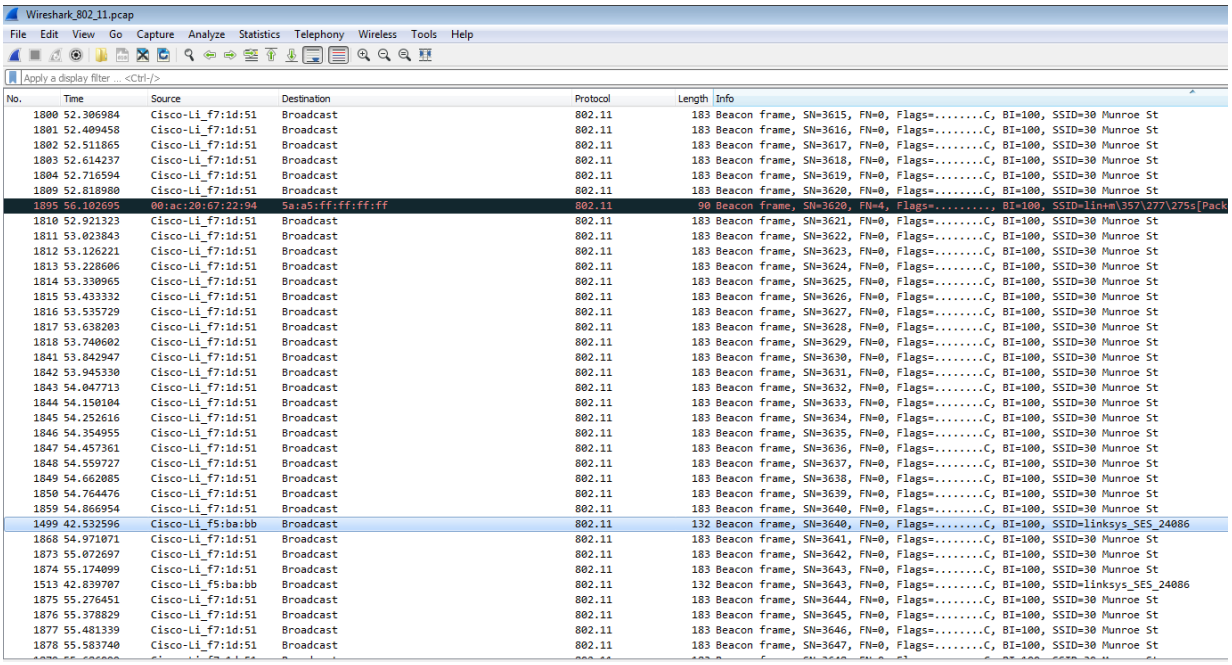
Here is the trace file of all the packets that were captured from the wireless network connection. The packets are mostly shown as frames between the devices sending the data. Infact data being sent to and from devices and access points, is in the form off frames know as beacon frames shown in this trace.

No.	Time	Source	Destination	Protocol	Length	Info
393	19.847780	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3071, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
10	0.294432	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3072, FN=0, Flags=........, BI=62, SSID=li\357\277\275\00
394	19.950179	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3072, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
395	20.052584	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3073, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
14	0.499197	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3074, FN=0, Flags=........, BI=100, SSID=linksys12
396	20.154956	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3074, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
397	20.257290	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3075, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
16	0.601687	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3075, FN=0, Flags=........C, BI=100, SSID=linksys12
398	20.359743	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3076, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
399	20.462160	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3077, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
400	20.564530	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3078, 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=........, BI=100, SSID=linksys12
401	20.666931	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3079, 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=........, BI=100, SSID=,\357\277\275nks
406	20.769352	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3080, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
407	20.871729	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3081, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
31	1.215947	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3081, FN=0, Flags=........C, BI=100, SSID=linksys12
408	20.974145	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3082, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
34	1.420565	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3083, FN=0, Flags=........, BI=20580, SSID=linksys12
409	21.076548	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3083, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
410	21.178943	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3084, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
411	21.281326	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3085, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
412	21.383741	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3086, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
413	21.486083	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3087, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
414	21.588525	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3088, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
41	2.035064	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3089, FN=0, Flags=........, BI=100, SSID=linksys12
415	21.690804	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3089, FN=0, Flags=........C, BI=100, SSID=30 Munroe St

The SSID's of the two access points sending out most of the beacon frames to show they exist are 30 Munroe Street and *Linksys_SES_24086*.

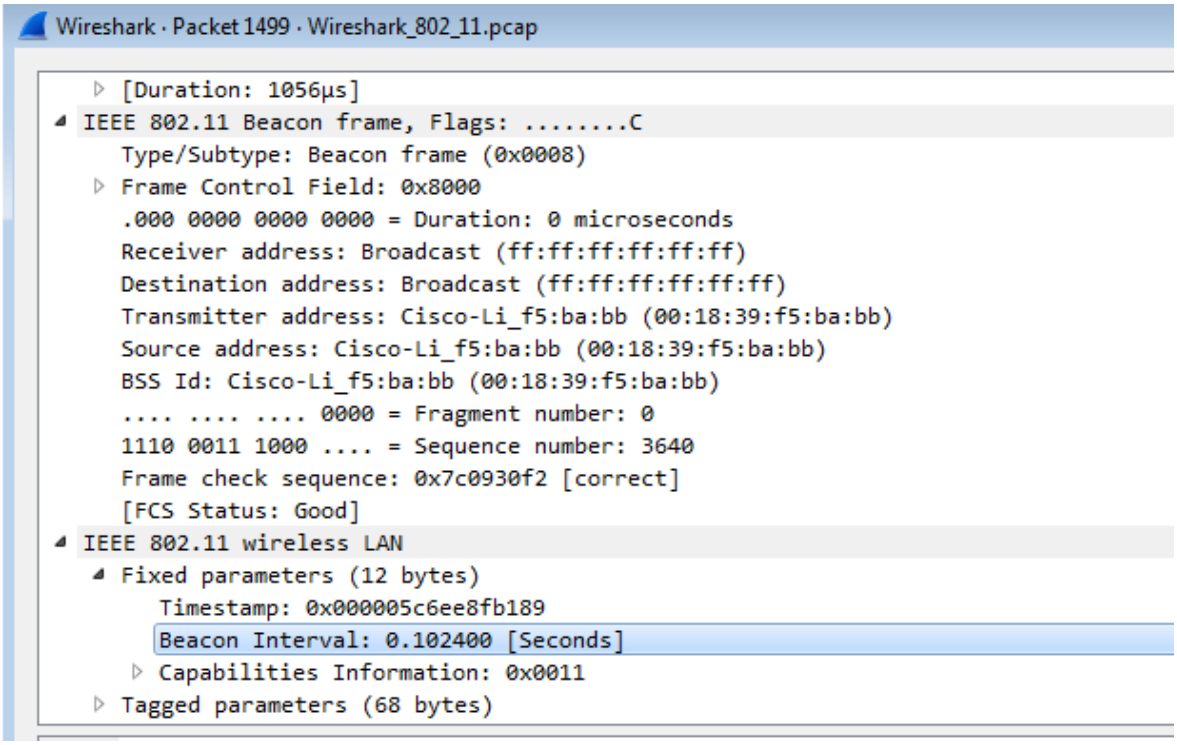
SSID stands for service set identifier – an identifier given to an access point or wireless station to identify it when it shows that it exists and connected to devices such as a computer or mobile phone to connect these devices to a network such as the internet.

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).



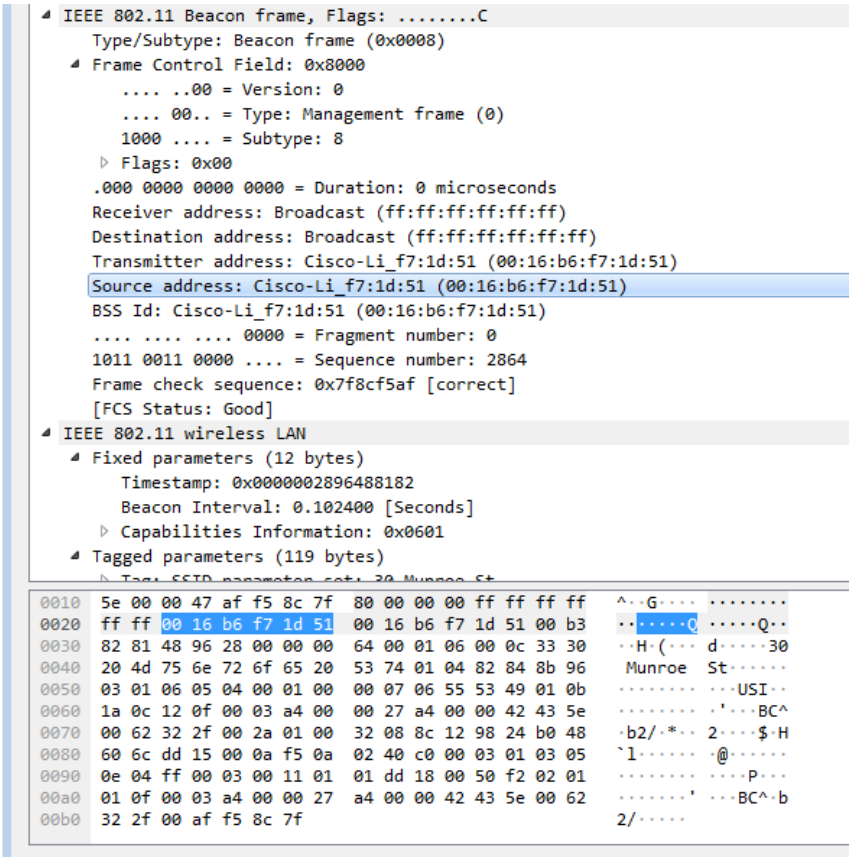
No.	Time	Source	Destination	Protocol	Length	Info
1800	52.306984	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3615, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1801	52.409458	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3616, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1802	52.511865	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3617, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1803	52.614237	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3618, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1804	52.716594	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3619, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1809	52.818980	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3620, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1895	56.102695	00:ac:20:67:22:94	5a:a5:ff:ff:ff:ff	802.11	90	Beacon frame, SN=3620, FN=4, Flags=........, BI=100, SSID=lin+m\357\277\275s[Pack
1810	52.921323	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3621, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1811	53.023843	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3622, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1812	53.126221	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3623, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1813	53.228606	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3624, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1814	53.330965	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3625, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1815	53.433332	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3626, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1816	53.535729	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3627, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1817	53.638203	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3628, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1818	53.740602	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3629, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1841	53.842947	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3630, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1842	53.945330	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3631, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1843	54.047713	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3632, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1844	54.150104	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3633, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1845	54.252616	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3634, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1846	54.354955	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3635, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1847	54.457361	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3636, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1848	54.559727	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3637, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1849	54.662085	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3638, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1850	54.764476	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3639, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1859	54.866954	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3640, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1499	42.532596	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3640, FN=0, Flags=........C, BI=100, SSID=linksys_SES_24086
1868	54.971071	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3641, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1873	55.072697	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3642, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1874	55.174099	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3643, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1513	42.839707	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3643, FN=0, Flags=........C, BI=100, SSID=linksys_SES_24086
1875	55.276451	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3644, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1876	55.378829	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3645, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1877	55.481339	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3646, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
1878	55.583740	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3647, FN=0, Flags=........C, BI=100, SSID=30 Munroe St

So here the data has been transmitted in the form of frames which are beacon frames between the access points which takes an amount of time.



The time interval of the transmission of the beacon frames - the linkisys_ses_24086 acCess point from the 30 munroe st access point is 0.102400 seconds. Shown above is this interval itself in the beacon frame in the 802.11 wireless LAN (local area network) section listed as a fixed parameter.

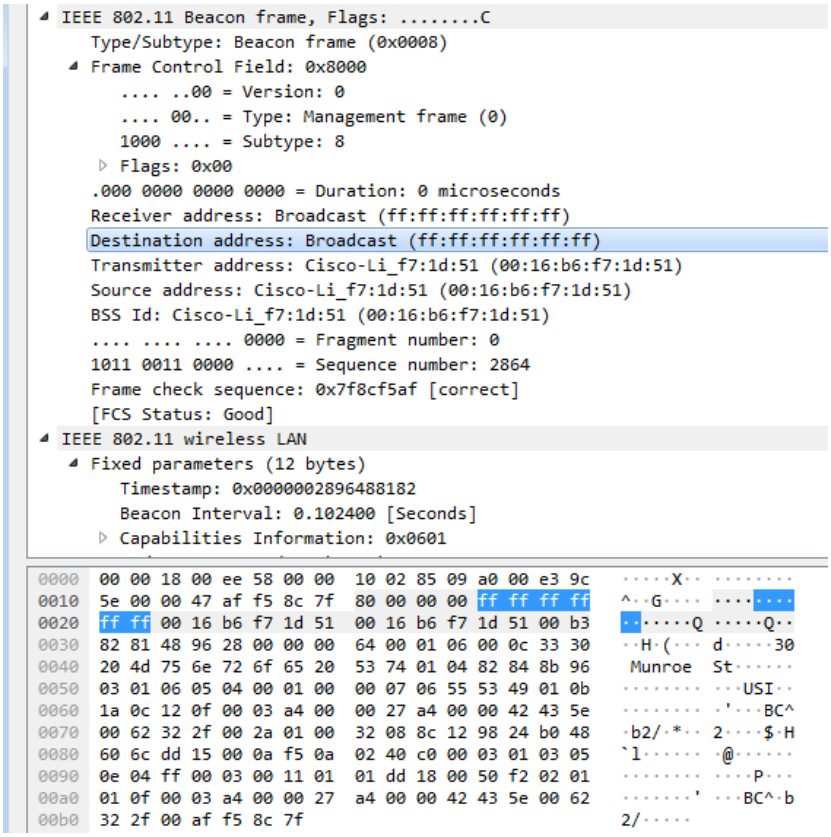
3.What (in hexadecimal notation) is the source MAC address on the beacon frame from 30 Munroe St? Recall from Figure 7.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE 802.11 standards document (cited above).



The source MAC address on the beacon frame from 30 Munroe St is 00 16 b6 f7 1d 51 in hexadecimal notation. The address is listed in the beacon frame in brackets and at the bottom of the window which shows all the captured packet data in hexadecimal and ascii.

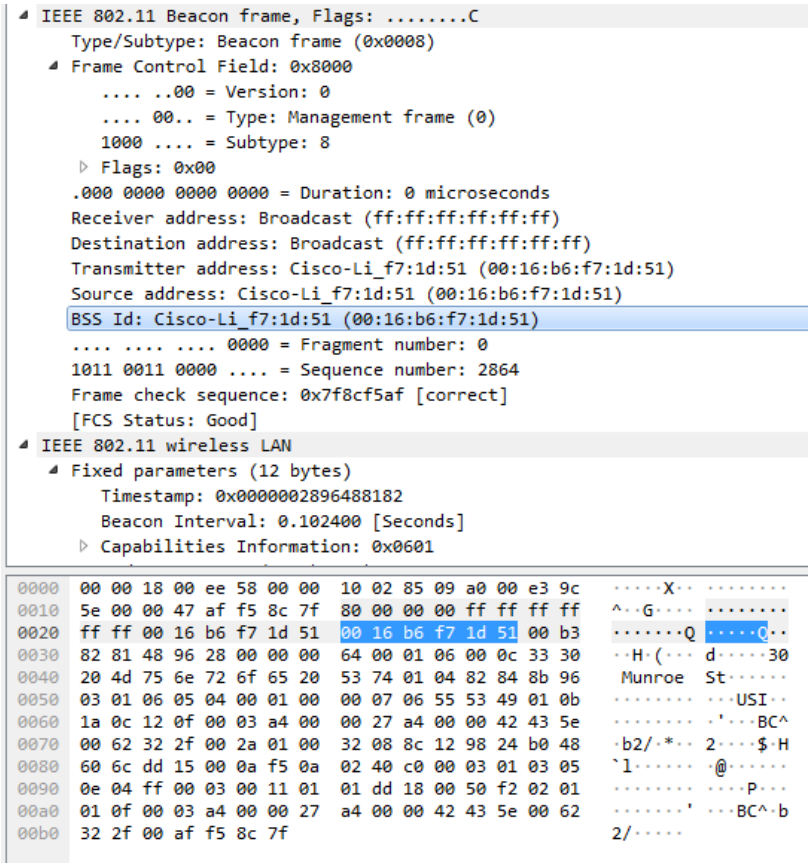
Here a MAC address is used. This address like the internet protocol(IP address) identifies devices used for connections in a network that use a protocol known as medium access control. Hence the MAC address is the medium access control address of the device being used for connection.

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 in hexadecimal notation is ff ff ff ff ff ff shown in the beacon frame as a broadcast and at the bottom of the window where the captured packet data is shown in hexadecimal and asccii notation. As it is a broadcast address it is only a pair of letter f's in this notation. This is an Ethernet broadcast.i.e.it was broadcast through the interface of an Ethernet connection.

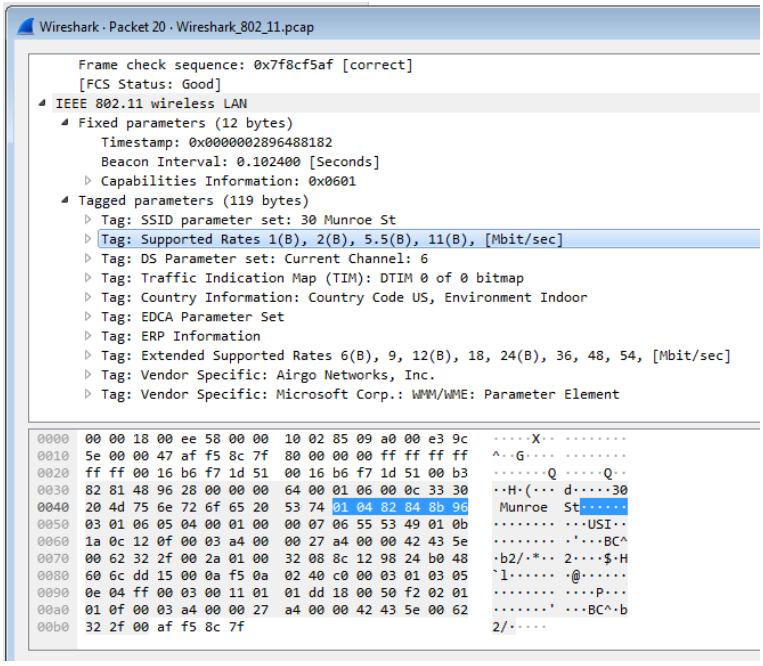
5. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from 30 Munroe St?



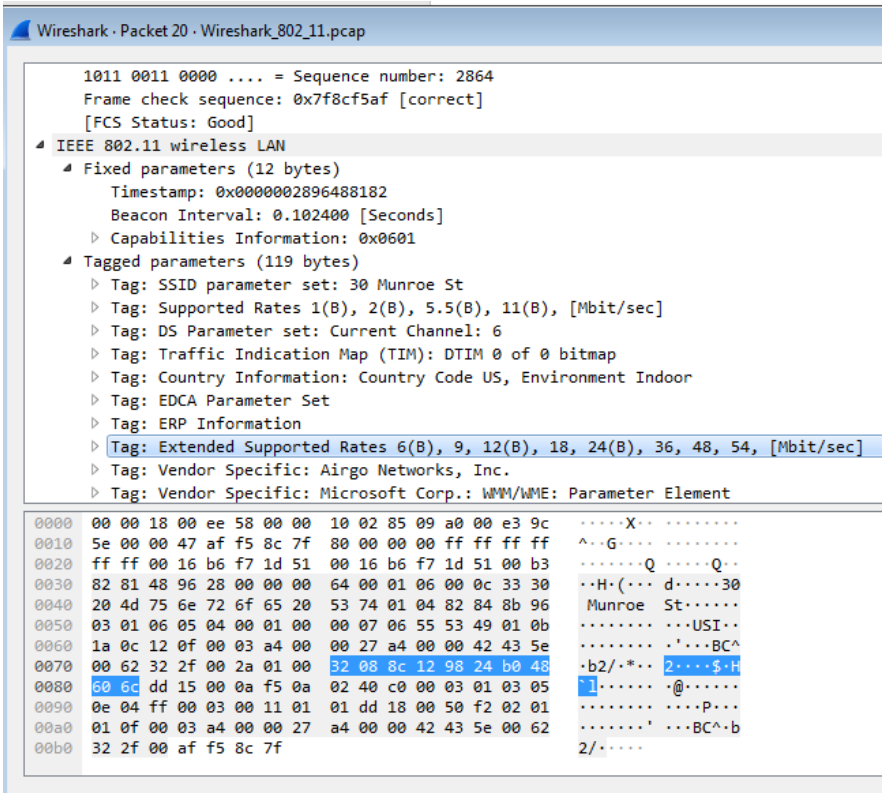
The BSS id is the id of the basic service set which is one set of devices connected to a network through an access point or wireless station.

The MAC BSS id on the beacon frame from 30 Munroe St is 00 16 b6 f7 1d 51 in hexadecimal notation as shown in the frame and at the bottom of the window where captured packet data is shown in hexadecimal and Ascii notation.

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?

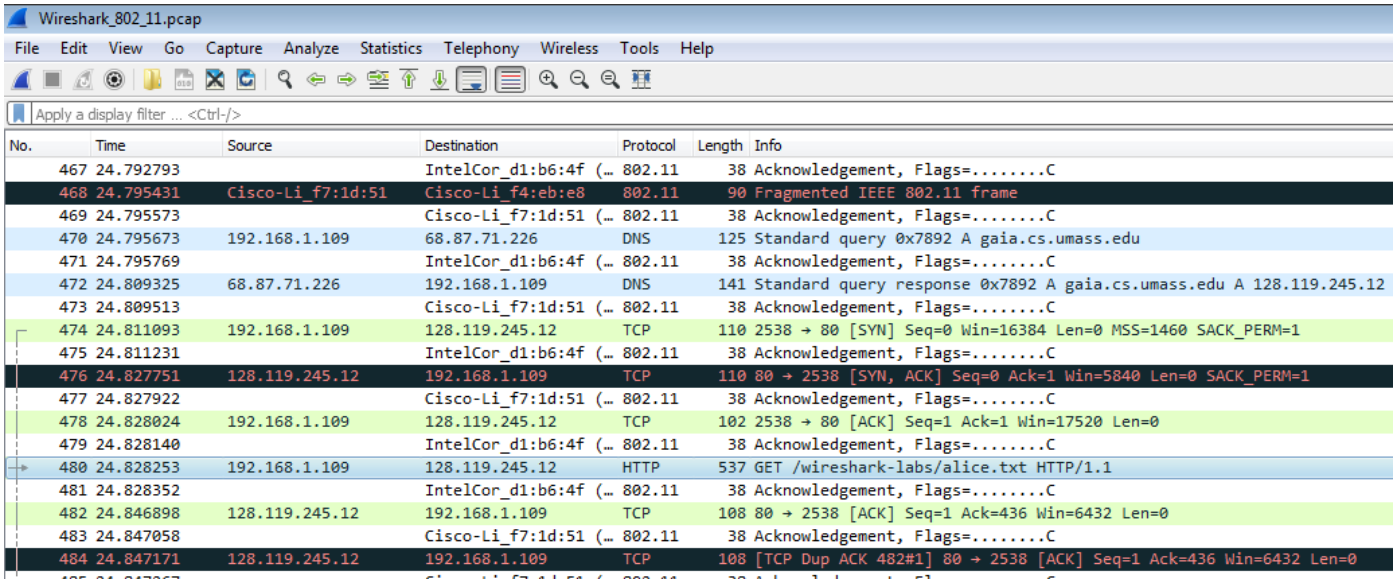


The supported data rates are parameters in this captured beacon frame. The four data rates are 1, 2, 5.5 and 11 Mbits/sec.

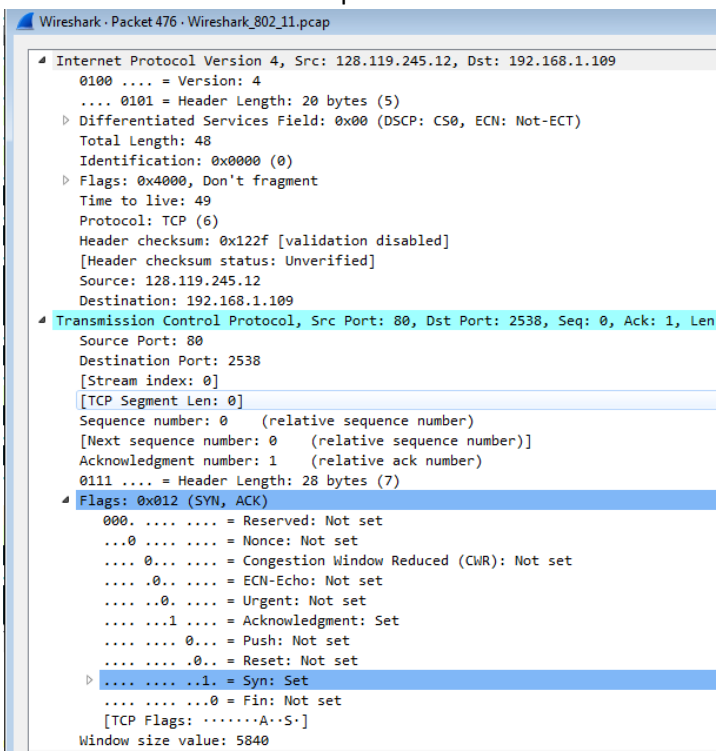


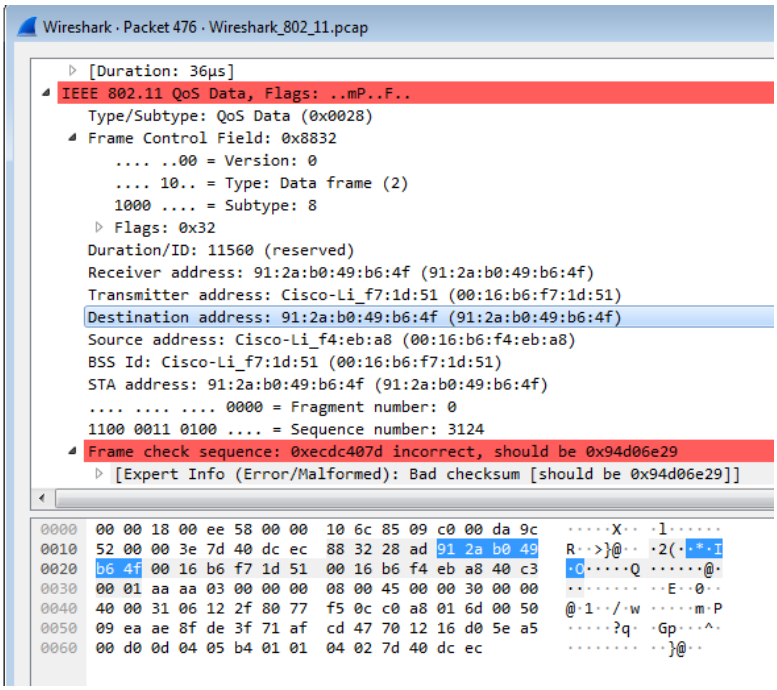
Eight extra support data rates are 6, 9, 12 ,18, 24, 36, 48 and 54 Mbits/sec.

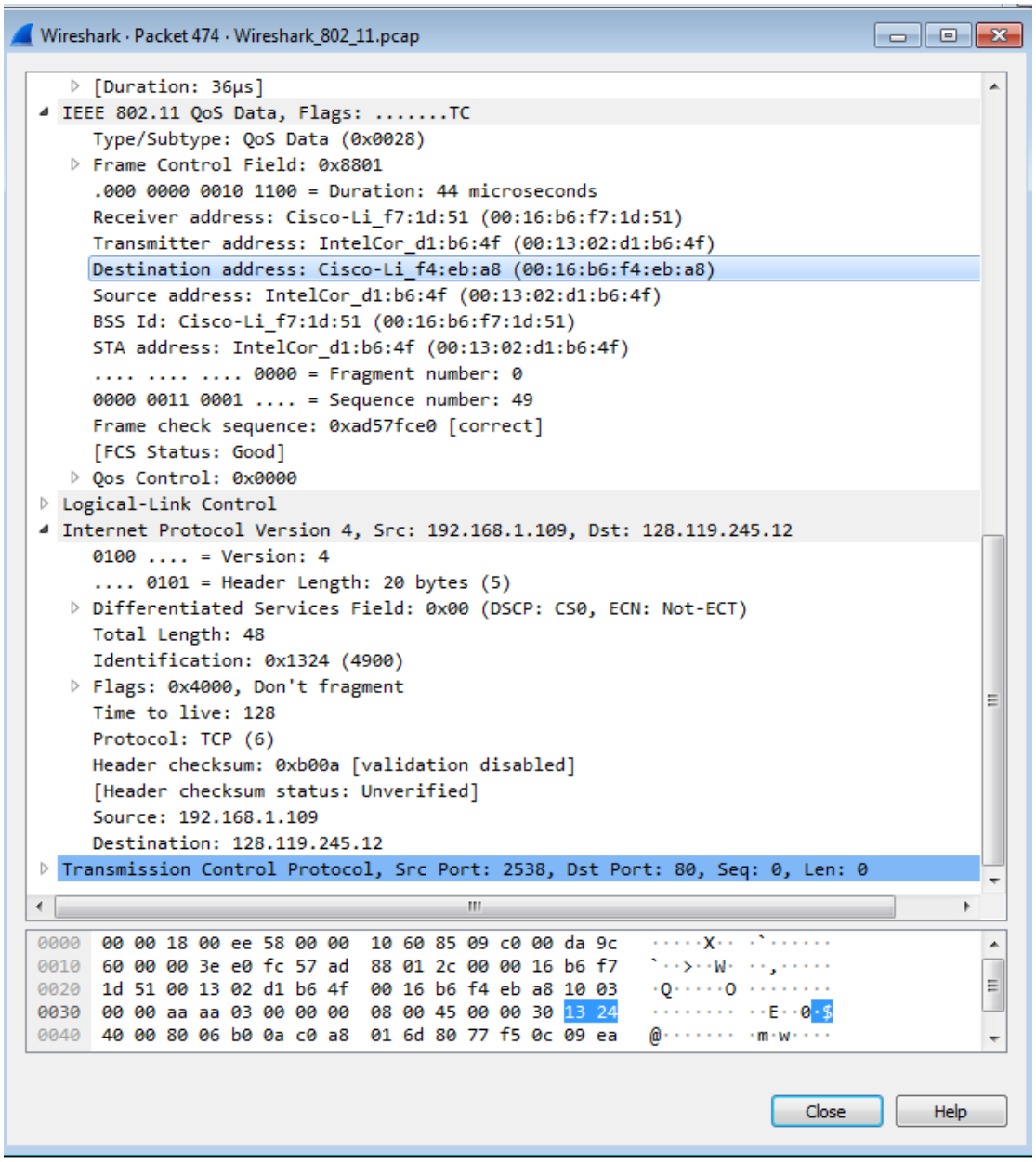
7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)?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

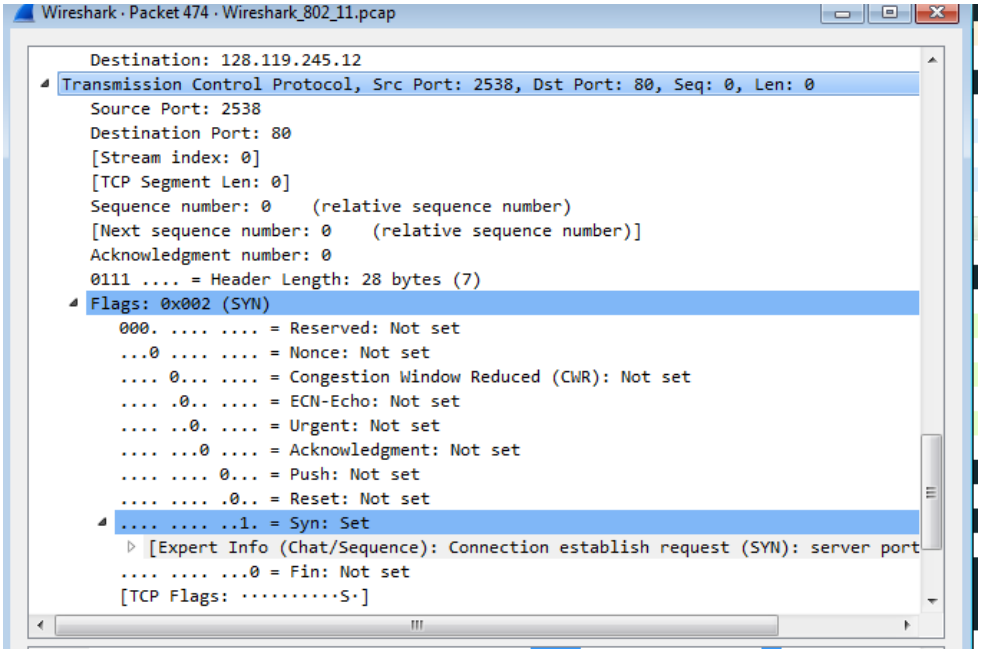


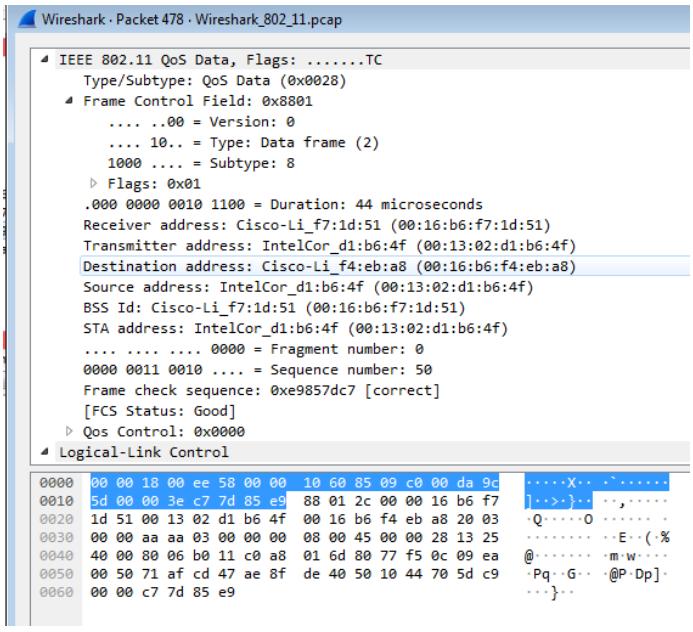
The frame that used the transport control protocol TCP, which has the SYN segment for this first TCP session starts from packet no.474 as shown in the screenshot above.

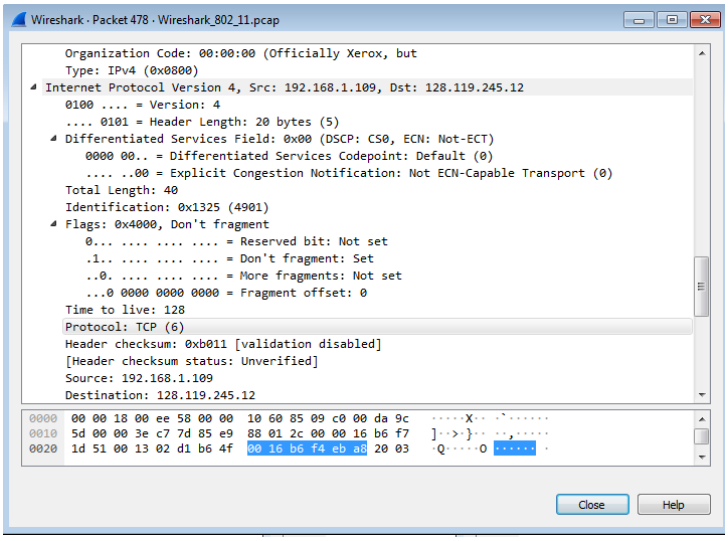



Wireshark · Packet 476 · Wireshark_802_11.pcap
[Duration: 36µs]
IEEE 802.11 QoS Data, Flags: ..mP..F..
Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8832
.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
Flags: 0x32
Duration/ID: 11560 (reserved)
Receiver address: 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)
Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
.... 0000 = Fragment number: 0
1100 0011 0100 .... = Sequence number: 3124
Frame check sequence: 0xecdc407d incorrect, should be 0x94d06e29
[Expert Info (Error/Malformed): Bad checksum [should be 0x94d06e29]]
0000 00 00 18 00 ee 58 00 00 10 6c 85 09 c0 00 da 9c
0010 52 00 00 3e 7d 40 dc ec 88 32 28 ad 91 2a b0 49
0020 b6 4f 00 16 b6 f7 1d 51 00 16 b6 f4 eb a8 40 c3
0030 00 01 aa aa 03 00 00 00 08 00 45 00 00 30 00 00
0040 40 00 31 06 12 2f 80 77 f5 0c c0 a8 01 6d 00 50
0050 09 ea ae 8f de 3f 71 af cd 47 70 12 16 d0 5e a5
0060 00 d0 0d 04 05 b4 01 01 04 02 7d 40 dc ec


Wireshark · Packet 474 · Wireshark_802_11.pcap
[Duration: 36µs]
IEEE 802.11 QoS Data, Flags: ....TC
Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8801
.000 0000 0010 1100 = Duration: 44 microseconds
Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
.... 0000 = Fragment number: 0
0000 0011 0001 .... = Sequence number: 49
Frame check sequence: 0xad57fce0 [correct]
[FCS Status: Good]
Qos Control: 0x0000
Logical-Link Control
Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 48
Identification: 0x1324 (4900)
Flags: 0x4000, Don't fragment
Time to live: 128
Protocol: TCP (6)
Header checksum: 0xb00a [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.109
Destination: 128.119.245.12
Transmission Control Protocol, Src Port: 2538, Dst Port: 80, Seq: 0, Len: 0
0000 00 00 18 00 ee 58 00 00 10 60 85 09 c0 00 da 9c
0010 60 00 00 3e e0 fc 57 ad 88 01 2c 00 00 16 b6 f7
0020 1d 51 00 13 02 d1 b6 4f 00 16 b6 f4 eb a8 10 03
0030 00 00 aa aa 03 00 00 00 08 00 45 00 00 30 13 24
0040 40 00 80 06 b0 0a c0 a8 01 6d 80 77 f5 0c 09 ea
Close
Help


Wireshark · Packet 474 · Wireshark_802_11.pcap
Destination: 128.119.245.12
Transmission Control Protocol, Src Port: 2538, Dst Port: 80, Seq: 0, Len: 0
Source Port: 2538
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 0
0111 .... = Header Length: 28 bytes (7)
Flags: 0x002 (SYN)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....1. = Syn: Set
[Expert Info (Chat/Sequence): Connection establish request (SYN): server port
....0 = Fin: Not set
[TCP Flags: ··········S·]

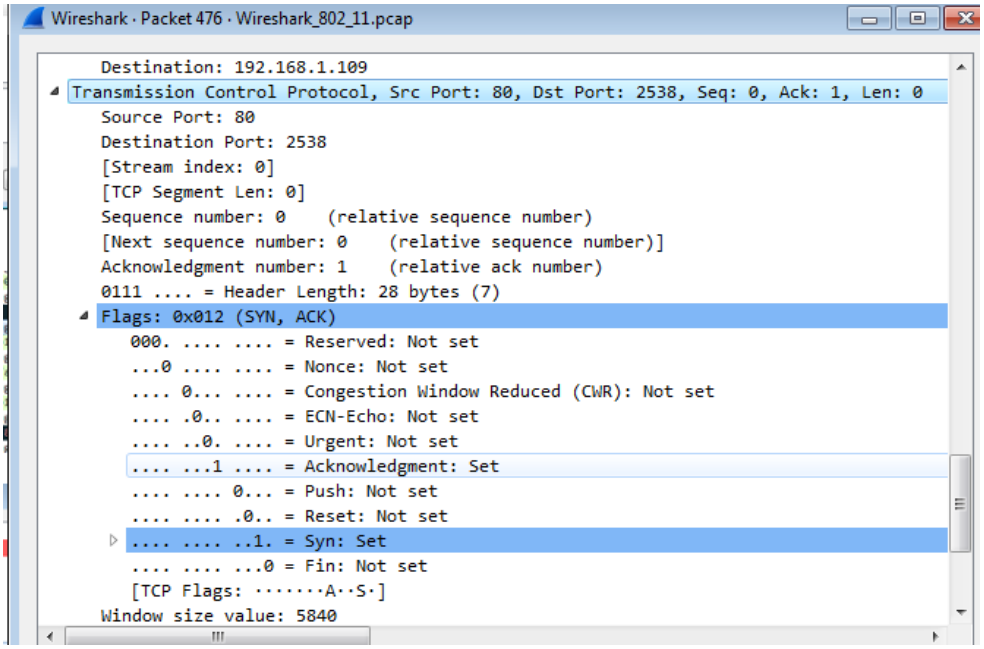

Wireshark · Packet 478 · Wireshark_802_11.pcap
IEEE 802.11 QoS Data, Flags: ....TC
Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8801
.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
Flags: 0x01
.000 0000 0010 1100 = Duration: 44 microseconds
Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
.... 0000 = Fragment number: 0
0000 0011 0010 .... = Sequence number: 50
Frame check sequence: 0xe9857dc7 [correct]
[FCS Status: Good]
Qos Control: 0x0000
Logical-Link Control
0000 00 00 18 00 ee 58 00 00 10 60 85 09 c0 00 da 9c
0010 5d 00 00 3e c7 7d 85 e9 88 01 2c 00 00 16 b6 f7
0020 1d 51 00 13 02 d1 b6 4f 00 16 b6 f4 eb a8 20 03
0030 00 00 aa aa 03 00 00 00 08 00 45 00 00 28 13 25
0040 40 00 80 06 b0 11 c0 a8 01 6d 80 77 f5 0c 09 ea
0050 00 50 71 af cd 47 ae 8f de 40 50 10 44 70 5d c9
0060 00 00 c7 7d 85 e9

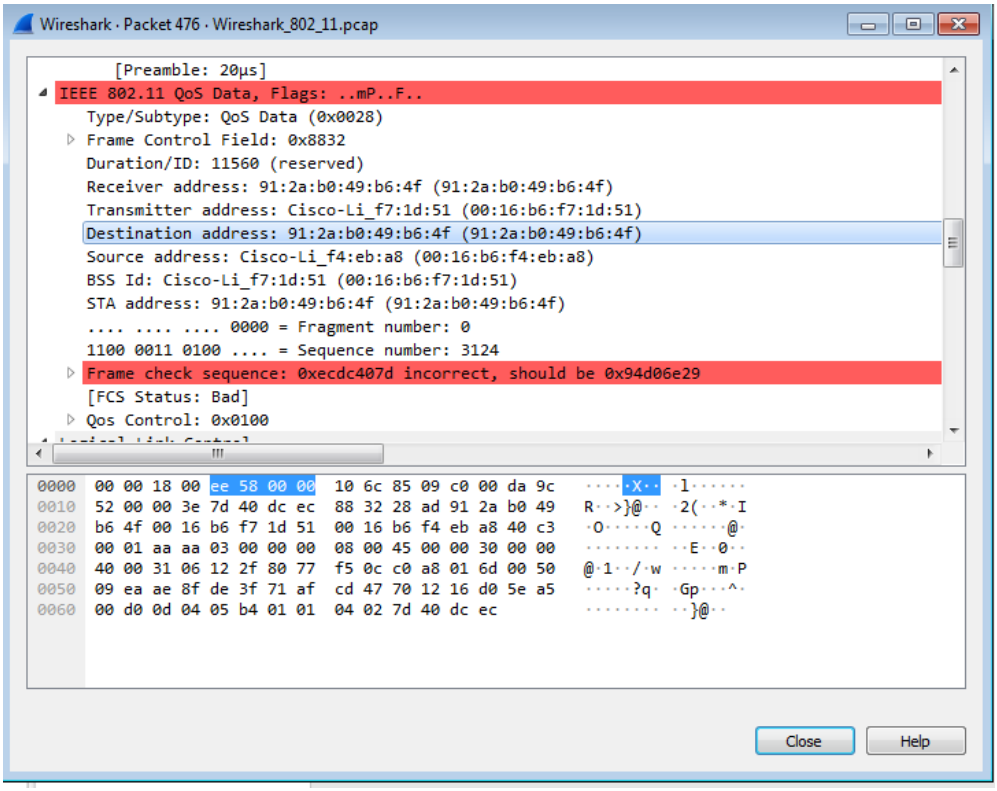


8. Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram? (Hint: review Figure 6.19 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).

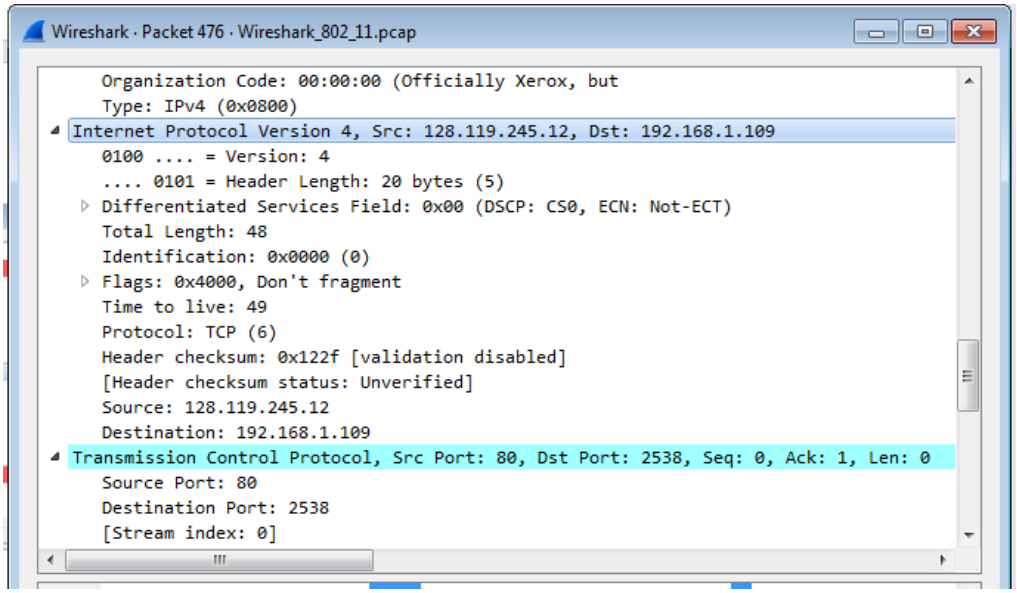
474	24.811093	192.168.1.109	128.119.245.12	TCP	110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
475	24.811231		IntelCor_d1:b6:4f (…	802.11	38 Acknowledgement, Flags=........C
476	24.827751	128.119.245.12	192.168.1.109	TCP	110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1
477	24.827922		Cisco-Li_f7:1d:51 (…	802.11	38 Acknowledgement, Flags=........C
478	24.828024	192.168.1.109	128.119.245.12	TCP	102 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
479	24.828140		IntelCor_d1:b6:4f (…	802.11	38 Acknowledgement, Flags=........C
480	24.828253	192.168.1.109	128.119.245.12	HTTP	537 GET /wireshark-labs/alice.txt HTTP/1.1
481	24.828352		IntelCor_d1:b6:4f (…	802.11	38 Acknowledgement, Flags=........C
482	24.846898	128.119.245.12	192.168.1.109	TCP	108 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
483	24.847058		Cisco-Li_f7:1d:51 (…	802.11	38 Acknowledgement, Flags=........C
484	24.847171	128.119.245.12	192.168.1.109	TCP	108 [TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
485	24.847267		Cisco-Li f7:1d:51 (…	802.11	38 Acknowledgement, Flags=........C

In the shot above the frame containing the SYNACK segment for this TCP session is captured at t=24.827751.





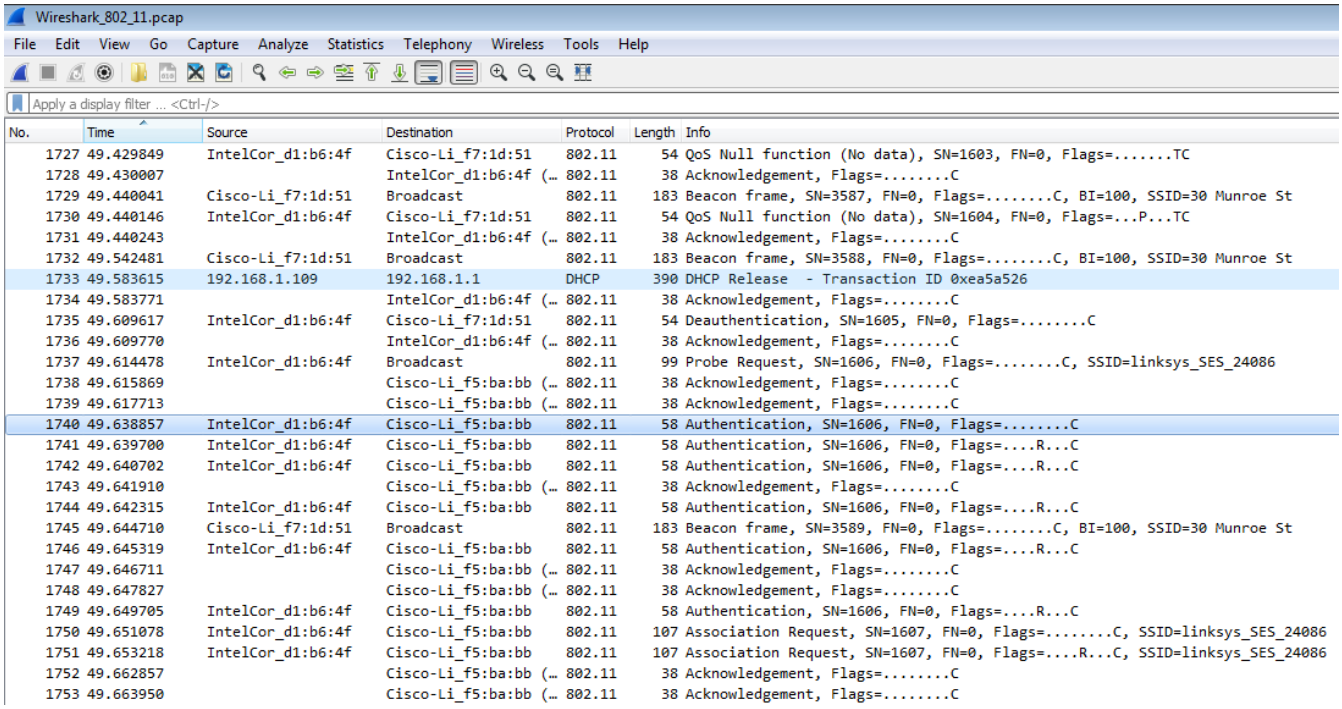
The three MAC address fields are the Source address, BSS Id and the Destination address. Source Address is the address of the sender which is MAC address 00:16:b6:f4:eb:a8 which corresponds to the host. The MAC address of the destination is 91:2a:b0:49:b6:4f. The MAC address of the BSS id is 00:16:b6:f7:1d:51.



The IP address of the sender is of the server, holding the live copy of the gaia.cs.umass.edu web page, which is 128.119.245.12. The sender MAC address does not correspond to the IP address of the sender.

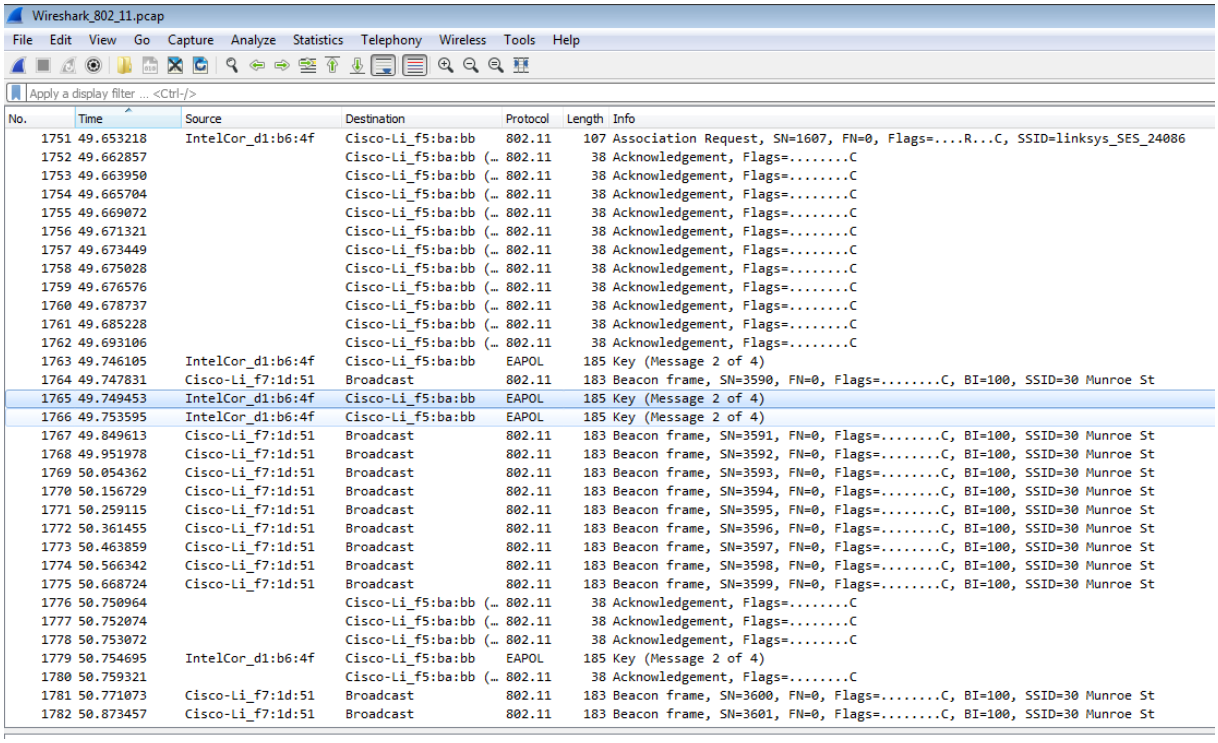
9. What two actions are taken (i.e., frames are sent) by the host in the trace just after t=49, to end the association with the 30 Munroe St AP that was initially in place when trace collection began? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification, is there another frame that you might have expected to see, but don't see here?

10.



No.	Time	Source	Destination	Protocol	Length	Info
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	192.168.1.109	192.168.1.1	DHCP	390	DHCP Release - Transaction ID 0xea5a526
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
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
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
1752	49.662857		Cisco-Li_f5:ba:bb (…	802.11	38	Acknowledgement, Flags=........C
1753	49.663950		Cisco-Li_f5:ba:bb (…	802.11	38	Acknowledgement, Flags=........C

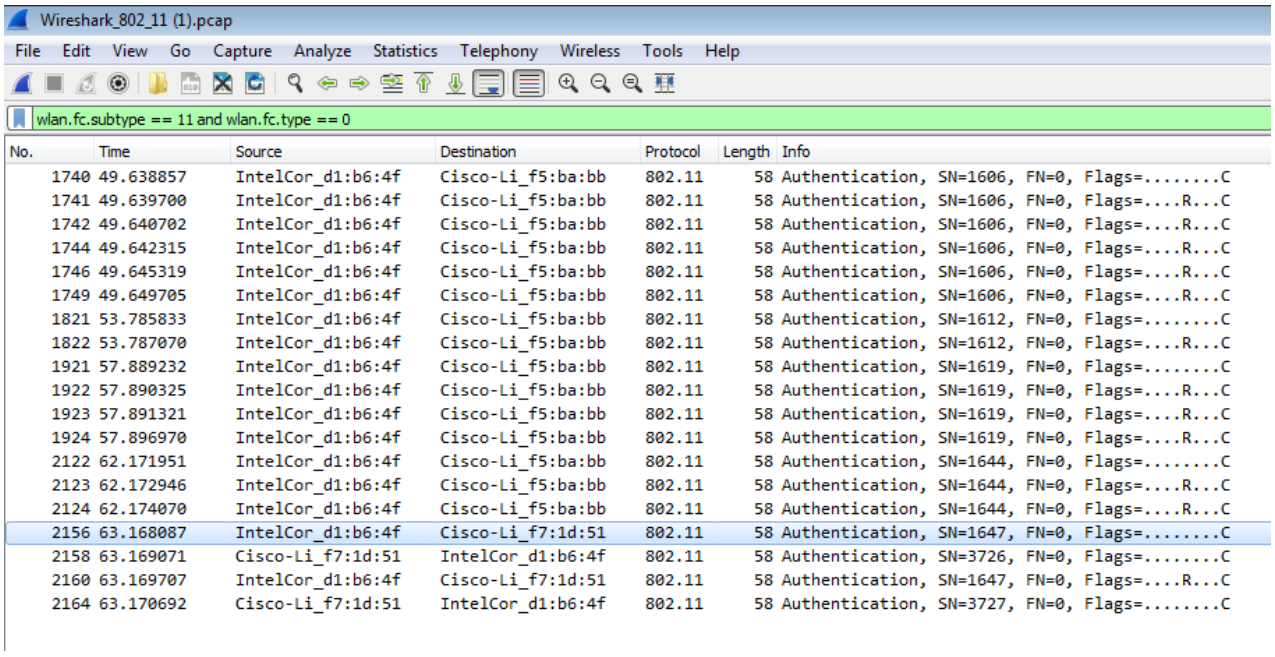
11. Does the host want the authentication to require a key or be open?



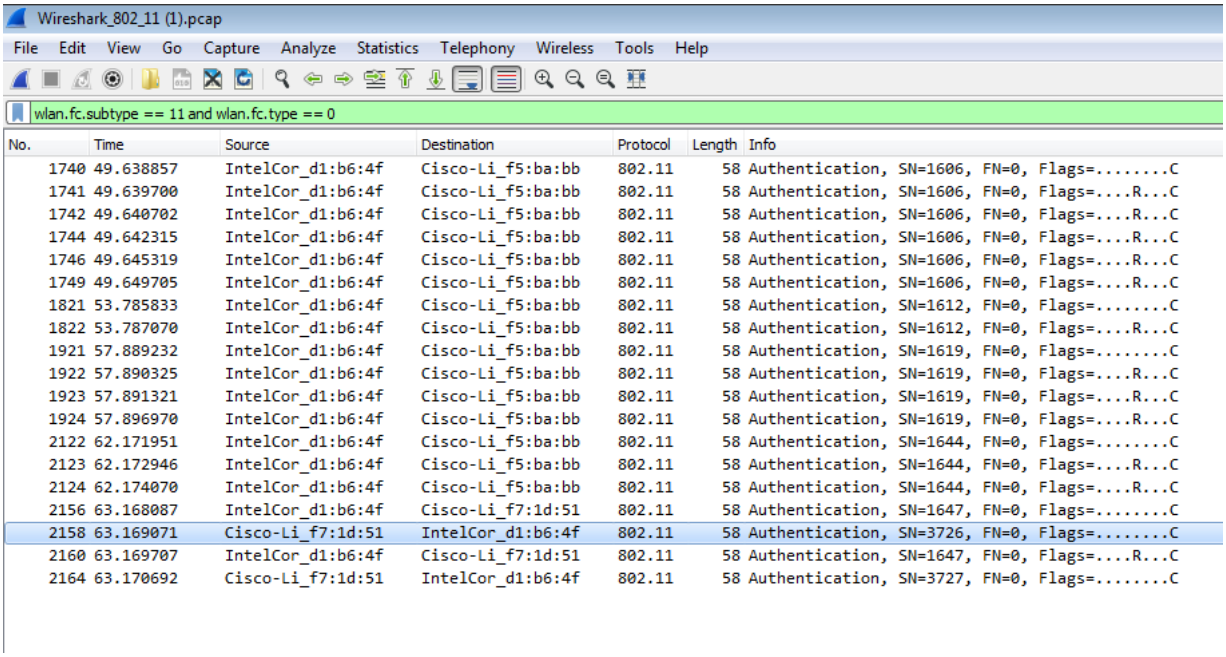
There are several key messages after the association so yes the host does want an authentication to have a key.

12. I have looked through the trace from between t=49.638857 and t= 53 and I do not see a reply authentication from linkys_24086 AP .

13.

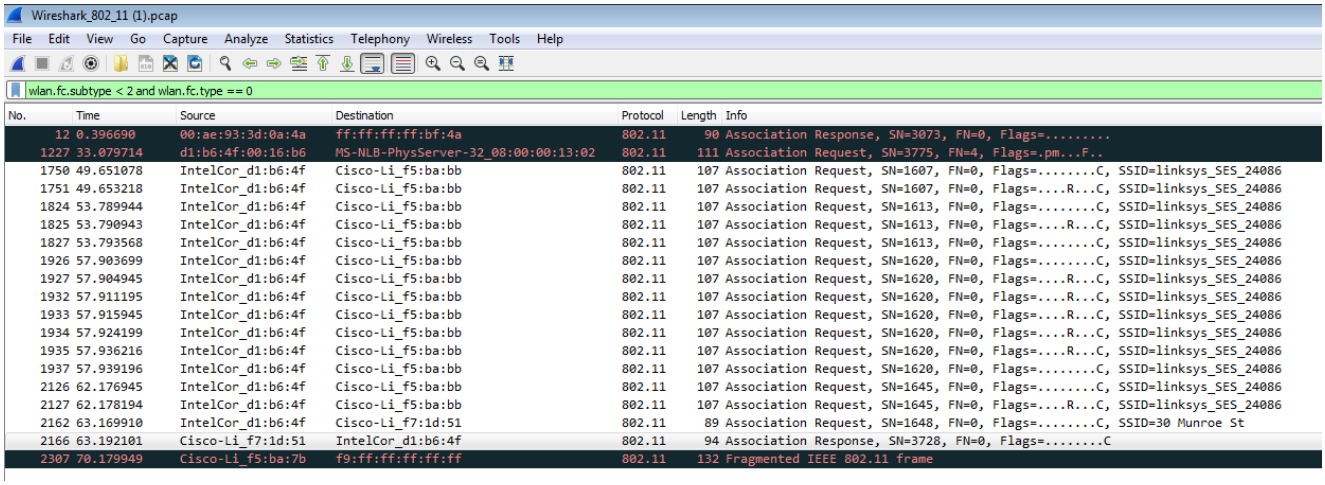


At the times 63.168087 an authentication frame is sent from the host to the Access Point and at 63.169071 an authentication reply frame is sent from that Access Point.

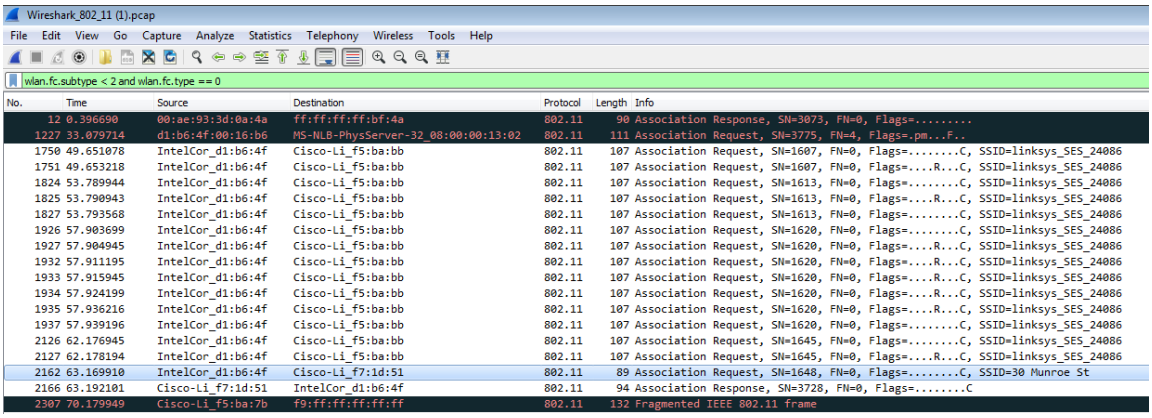


No.	Time	Source	Destination	Protocol	Length	Info
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=........C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	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
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
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=........C

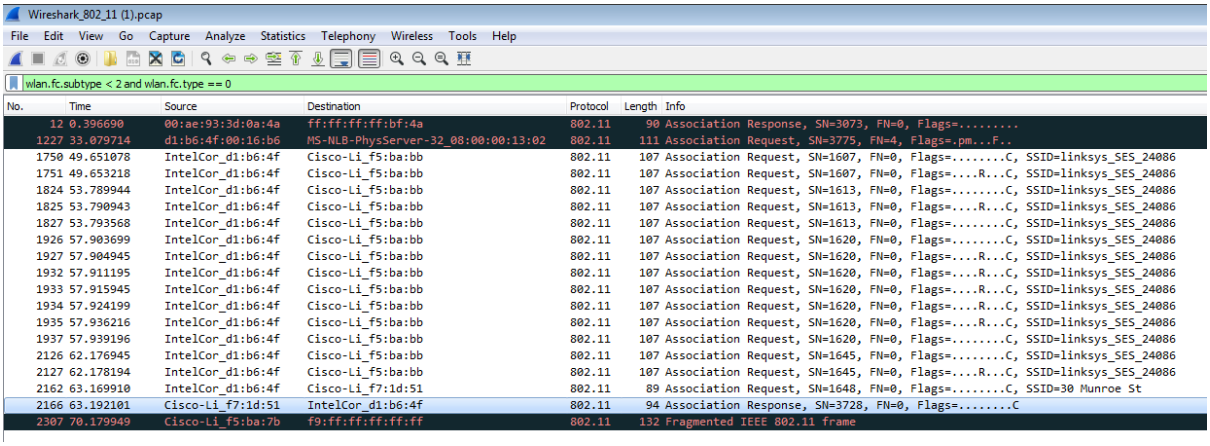
14.



No.	Time	Source	Destination	Protocol	Length	Info
12	0.396690	00:ae:93:3d:0a:4a	ff:ff:ff:ff:bf:4a	802.11	90	Association Response, SN=3073, FN=0, Flags=........
1227	33.079714	d1:b6:4f:00:16:b6	MS-NLB-PhysServer-32_08:00:00:13:02	802.11	111	Association Request, SN=3775, FN=4, Flags=.pm...F..
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
2307	70.179949	Cisco-Li_f5:ba:7b	f9:ff:ff:ff:ff:ff	802.11	132	Fragmented IEEE 802.11 frame

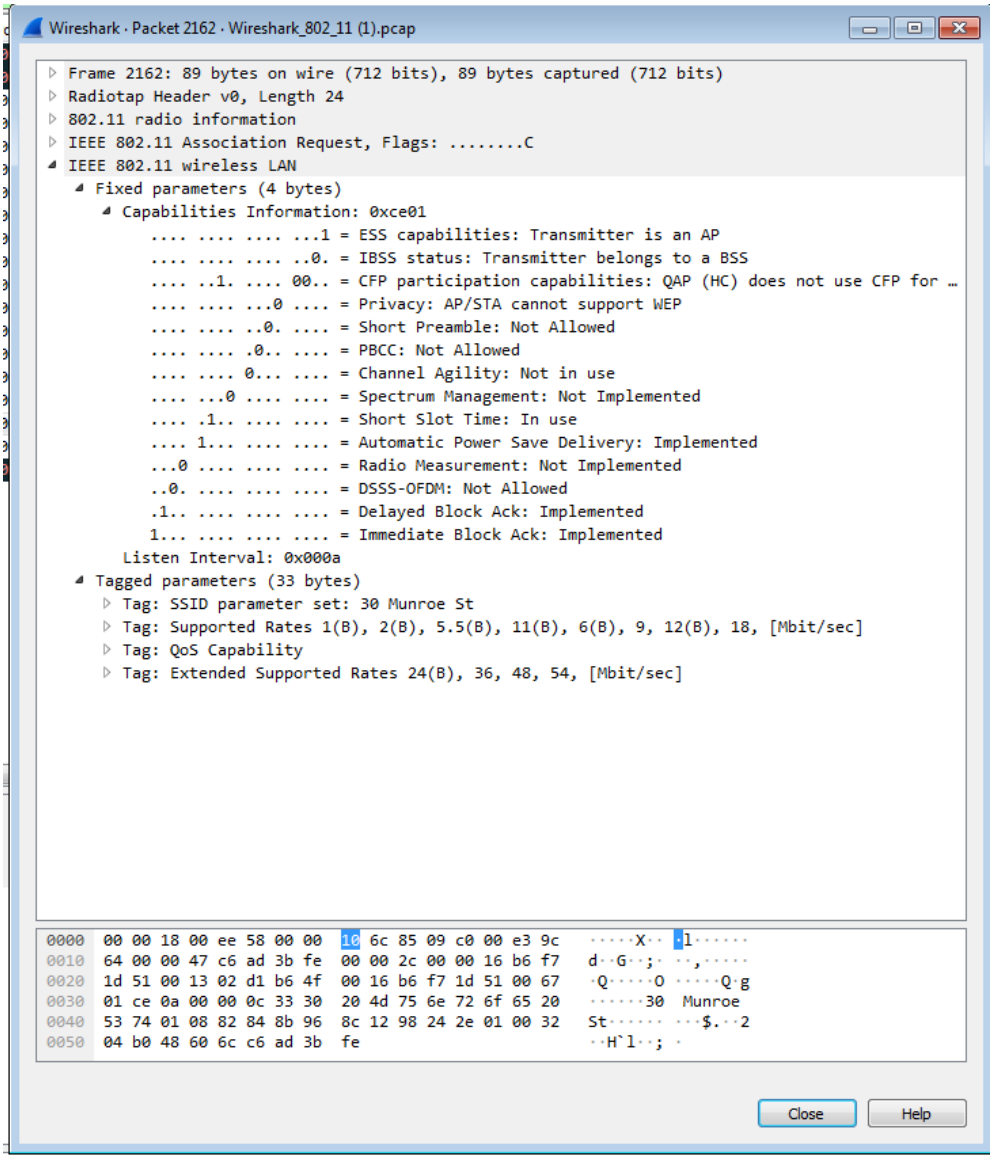


No.	Time	Source	Destination	Protocol	Length	Info
12	0.396690	00:ae:93:3d:0a:4a	ff:ff:ff:ff:bf:4a	802.11	90	Association Response, SN=3073, FN=0, Flags=........
1227	33.079714	d1:b6:4f:00:16:b6	MS-NLB-PhysServer-32_08:00:00:13:02	802.11	111	Association Request, SN=3775, FN=4, Flags=.pm...F..
1750	49.651078	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
2307	70.179949	Cisco-Li_f5:ba:7b	f9:ff:ff:ff:ff:ff	802.11	132	Fragmented IEEE 802.11 frame

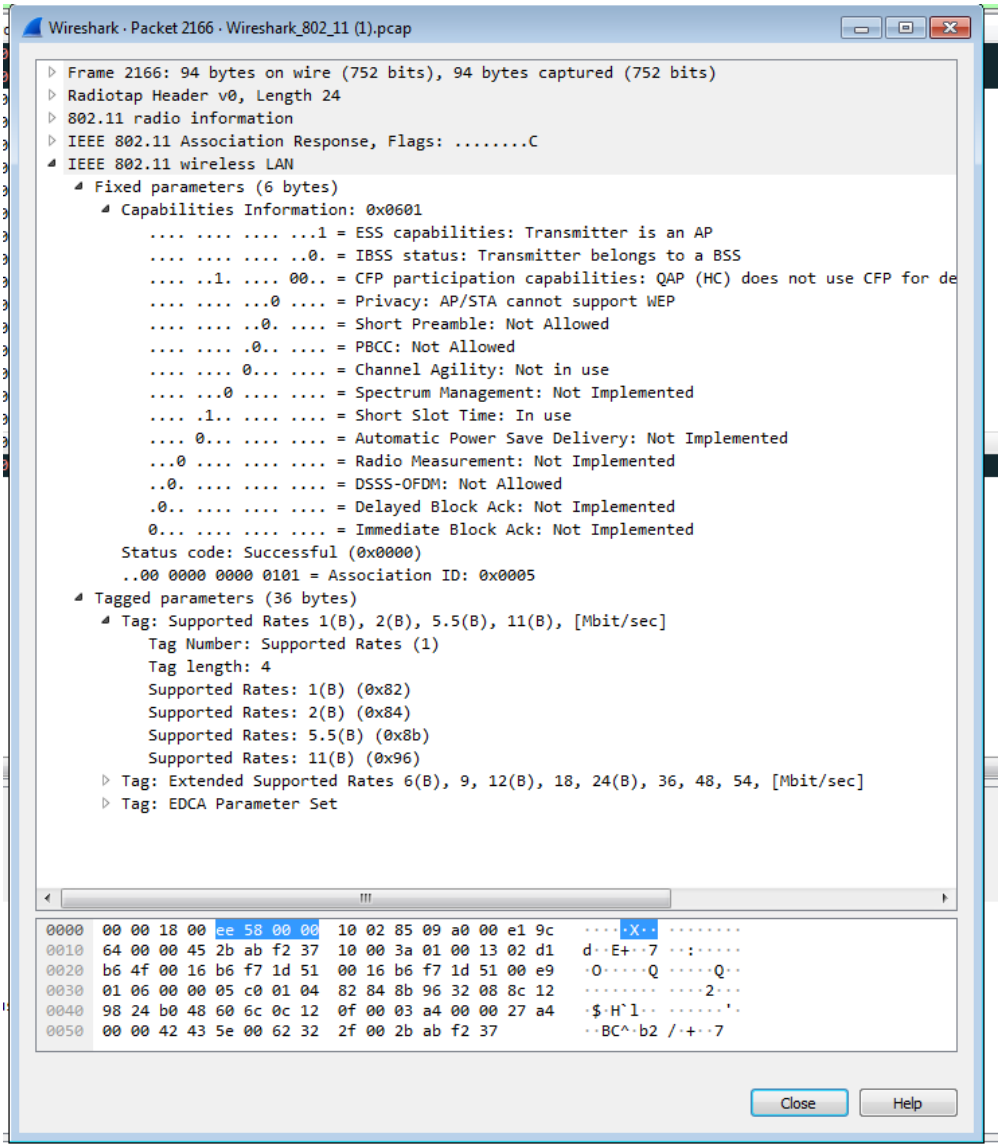


At the time 63.169910 an association request frame is sent from the host to the 30 munroe st access point. At t= 63.192101 a response is then sent back to the host from the access point.

15.

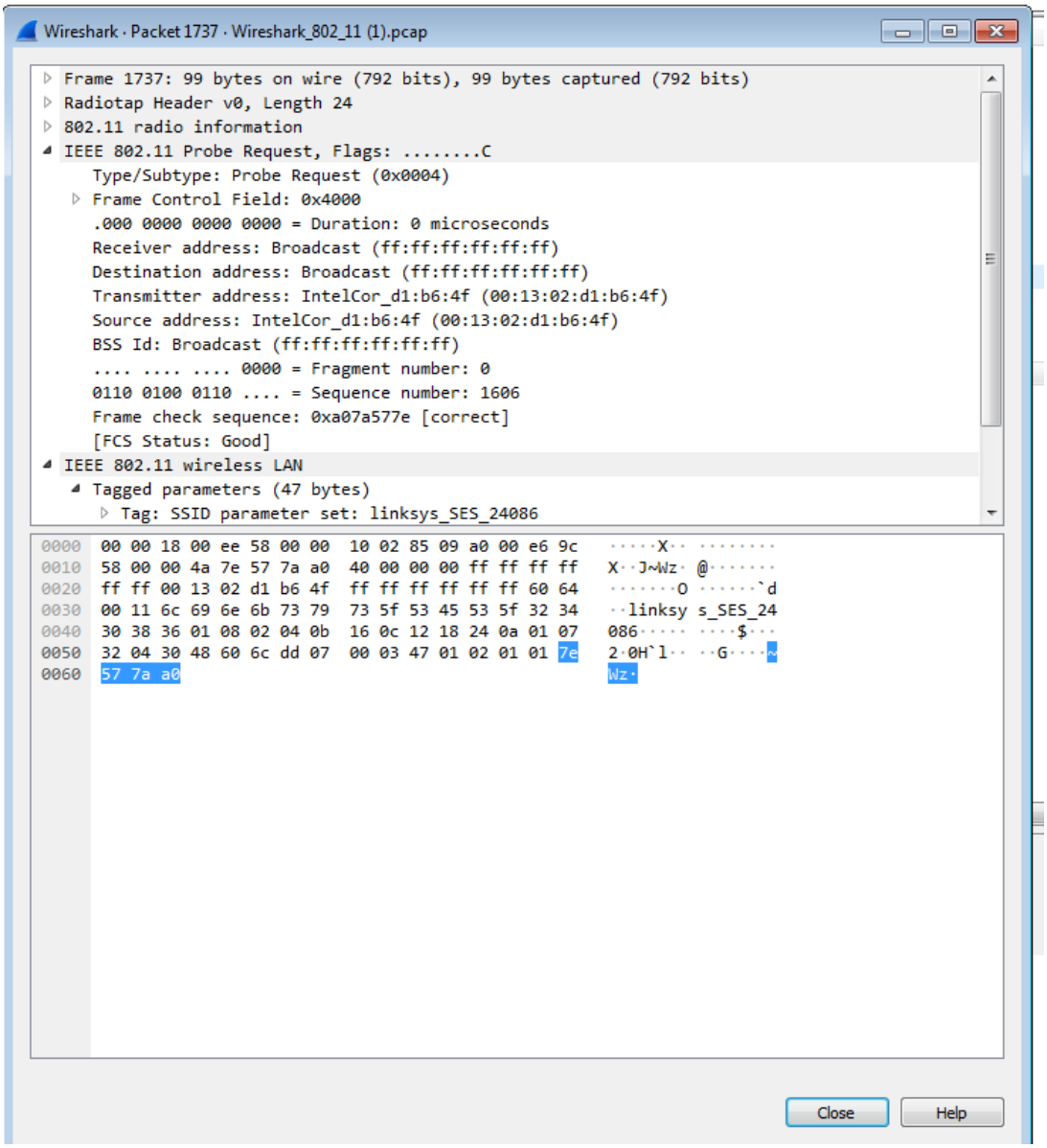


The transmission rates the host is willing to use are in Mbits/sec which are 1,2,5.5,11,6,9,12 and 18 Mbits/sec.

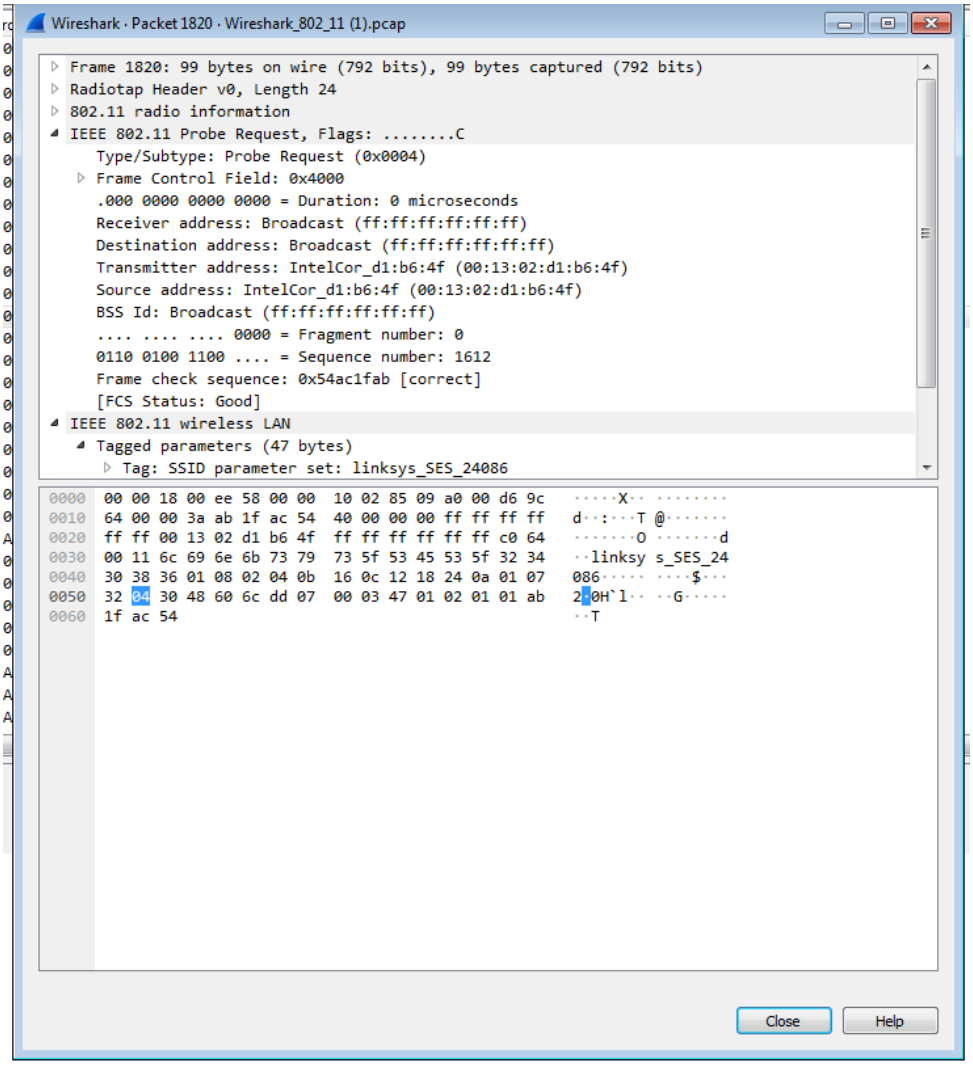


The transmission rates the acess point is willing to use are 1,2,5.5,11 which are the supported rates in Mbits/sec and the additional supported rates 6,9,18,24,36,48 and 54 Mbits/sec. These rates that the access point is willing to use are the same as the rates the host is trying to use.

16.



The sender MAC address in these frames is 00:13:02:d1:b6:4f, receiver MAC address is ff:ff:ff:ff:ff:ff and the BSS id MAC address is ff:ff:ff:ff:ff:ff


Wireshark · Packet 1820 · Wireshark_802_11 (1).pcap
Frame 1820: 99 bytes on wire (792 bits), 99 bytes captured (792 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: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
.... 0000 = Fragment number: 0
0110 0100 1100 .... = Sequence number: 1612
Frame check sequence: 0x54ac1fab [correct]
[FCS Status: Good]
IEEE 802.11 wireless LAN
Tagged parameters (47 bytes)
Tag: SSID parameter set: linksys_SES_24086
0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 d6 9c
0010 64 00 00 3a ab 1f ac 54 40 00 00 00 ff ff ff ff
0020 ff ff 00 13 02 d1 b6 4f ff ff ff ff ff ff c0 64
0030 00 11 6c 69 6e 6b 73 79 73 5f 53 45 53 5f 32 34
0040 30 38 36 01 08 02 04 0b 16 0c 12 18 24 0a 01 07
0050 32 04 30 48 60 6c dd 07 00 03 47 01 02 01 01 ab
0060 1f ac 54
Close
Help