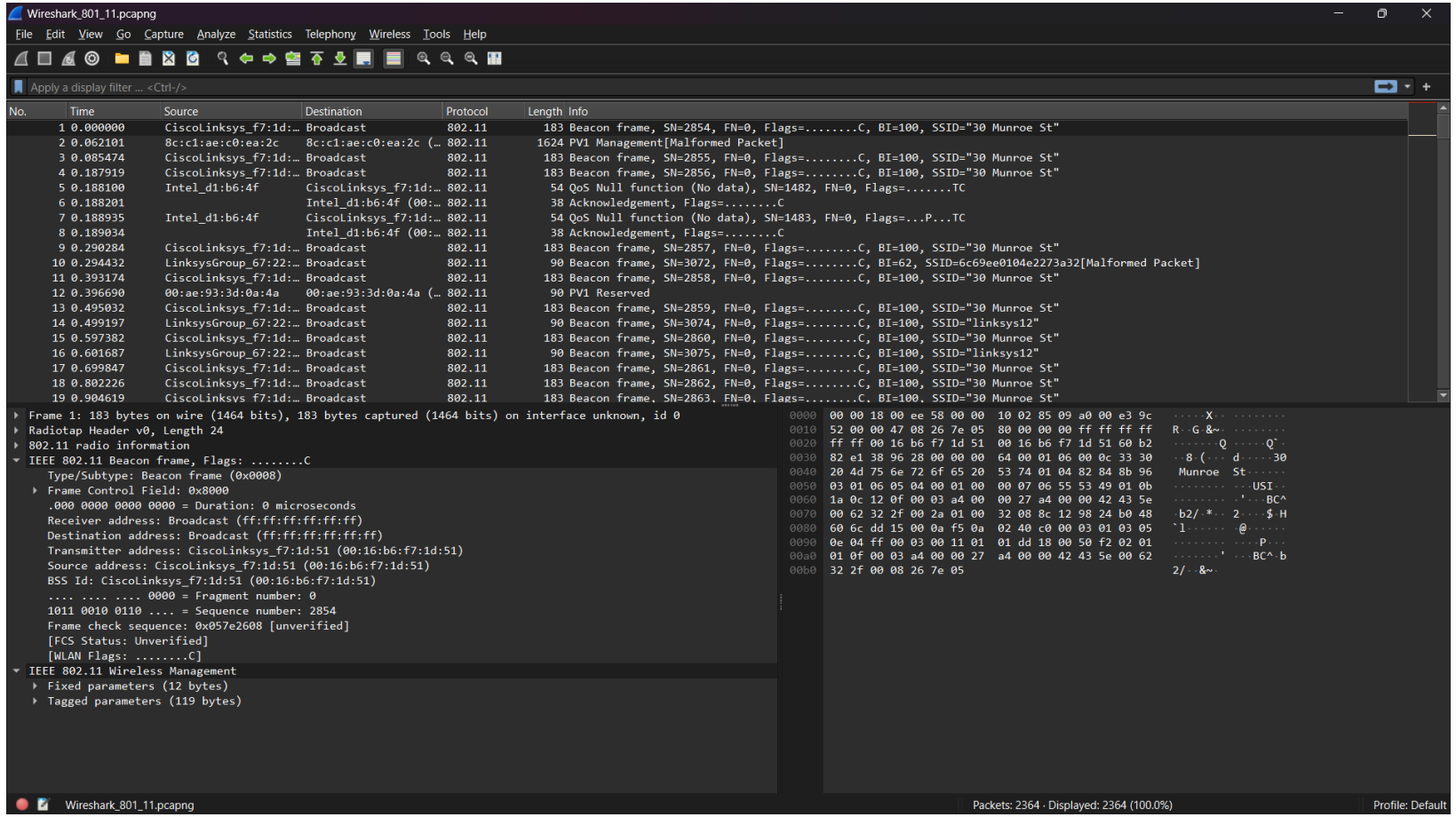
# 802.11 WiFi

Yogesh P
201EE138


Wireshark_801_11.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 CiscoLinksys_f7:1d:… Broadcast 802.11 183 Beacon frame, SN=2854, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
2 0.062101 8c:c1:ae:c0:ea:2c 8c:c1:ae:c0:ea:2c (… 802.11 1624 PV1 Management[Malformed Packet]
3 0.085474 CiscoLinksys_f7:1d:… Broadcast 802.11 183 Beacon frame, SN=2855, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
4 0.187919 CiscoLinksys_f7:1d:… Broadcast 802.11 183 Beacon frame, SN=2856, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
5 0.188100 Intel_d1:b6:4f CiscoLinksys_f7:1d:… 802.11 54 QoS Null function (No data), SN=1482, FN=0, Flags=.......TC
6 0.188201 Intel_d1:b6:4f (00:… 802.11 38 Acknowledgement, Flags=........C
7 0.188935 Intel_d1:b6:4f CiscoLinksys_f7:1d:… 802.11 54 QoS Null function (No data), SN=1483, FN=0, Flags=...P...TC
8 0.189034 Intel_d1:b6:4f (00:… 802.11 38 Acknowledgement, Flags=........C
9 0.290284 CiscoLinksys_f7:1d:… Broadcast 802.11 183 Beacon frame, SN=2857, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
10 0.294432 LinksysGroup_67:22:… Broadcast 802.11 90 Beacon frame, SN=3072, FN=0, Flags=........C, BI=62, SSID=6c69ee0104e2273a32[Malformed Packet]
11 0.393174 CiscoLinksys_f7:1d:… Broadcast 802.11 183 Beacon frame, SN=2858, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
12 0.396690 00:ae:93:3d:0a:4a 00:ae:93:3d:0a:4a (… 802.11 90 PV1 Reserved
13 0.495032 CiscoLinksys_f7:1d:… Broadcast 802.11 183 Beacon frame, SN=2859, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
14 0.499197 LinksysGroup_67:22:… Broadcast 802.11 90 Beacon frame, SN=3074, FN=0, Flags=........C, BI=100, SSID="linksys12"
15 0.597382 CiscoLinksys_f7:1d:… Broadcast 802.11 183 Beacon frame, SN=2860, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
16 0.601687 LinksysGroup_67:22:… Broadcast 802.11 90 Beacon frame, SN=3075, FN=0, Flags=........C, BI=100, SSID="linksys12"
17 0.699847 CiscoLinksys_f7:1d:… Broadcast 802.11 183 Beacon frame, SN=2861, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
18 0.802226 CiscoLinksys_f7:1d:… Broadcast 802.11 183 Beacon frame, SN=2862, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
19 0.904619 CiscoLinksys_f7:1d:… Broadcast 802.11 183 Beacon frame, SN=2863, FN=0, Flags=........C, BI=100, SSID="30 Munroe St"
Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface unknown, id 0
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Beacon frame, Flags: ........C
Type/Subtype: Beacon frame (0x0008)
Frame Control Field: 0x8000
.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: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
.... .... .... 0000 = Fragment number: 0
1011 0010 0110 .... = Sequence number: 2854
Frame check sequence: 0x057e2608 [unverified]
[FCS Status: Unverified]
[WLAN Flags: ........C]
IEEE 802.11 Wireless Management
Fixed parameters (12 bytes)
Tagged parameters (119 bytes)
0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e3 9c
0010 52 00 00 47 08 26 7e 05 80 00 00 00 ff ff ff ff
0020 ff ff 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 60 b2
0030 82 e1 38 96 28 00 00 00 64 00 01 06 00 0c 33 30
0040 20 4d 75 6e 72 6f 65 20 53 74 01 04 82 84 8b 96
0050 03 01 06 05 04 00 01 00 00 07 06 55 53 49 01 0b
0060 1a 0c 12 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e
0070 00 62 32 2f 00 2a 01 00 32 08 8c 12 98 24 b0 48
0080 60 6c dd 15 00 0a f5 0a 02 40 c0 00 03 01 03 05
0090 0e 04 ff 00 03 00 11 01 01 dd 18 00 50 f2 02 01
00a0 01 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e 00 62
00b0 32 2f 00 08 26 7e 05
Wireshark_801_11.pcapng
Packets: 2364 · Displayed: 2364 (100.0%)
Profile: Default

# 2. Beacon Frames

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

A: The 2 most common SSIDs are “30 Munroe St” and “linksys12”

2. What 802.11 channel is being used by both of these access points

A: Channel 6 is being used by both the access points.

3. What is the interval of time between the transmissions of beacon frames from this access point (AP)?

A: The interval of time between the transmissions of beacon frames is Beacon Interval: 0.102400 [Seconds]

4. What (in hexadecimal notation) is the source MAC address on the beacon frame from this access point? 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 9.2.3-9.2.4.1in the IEEE 802.11 standards document, excerpted here.

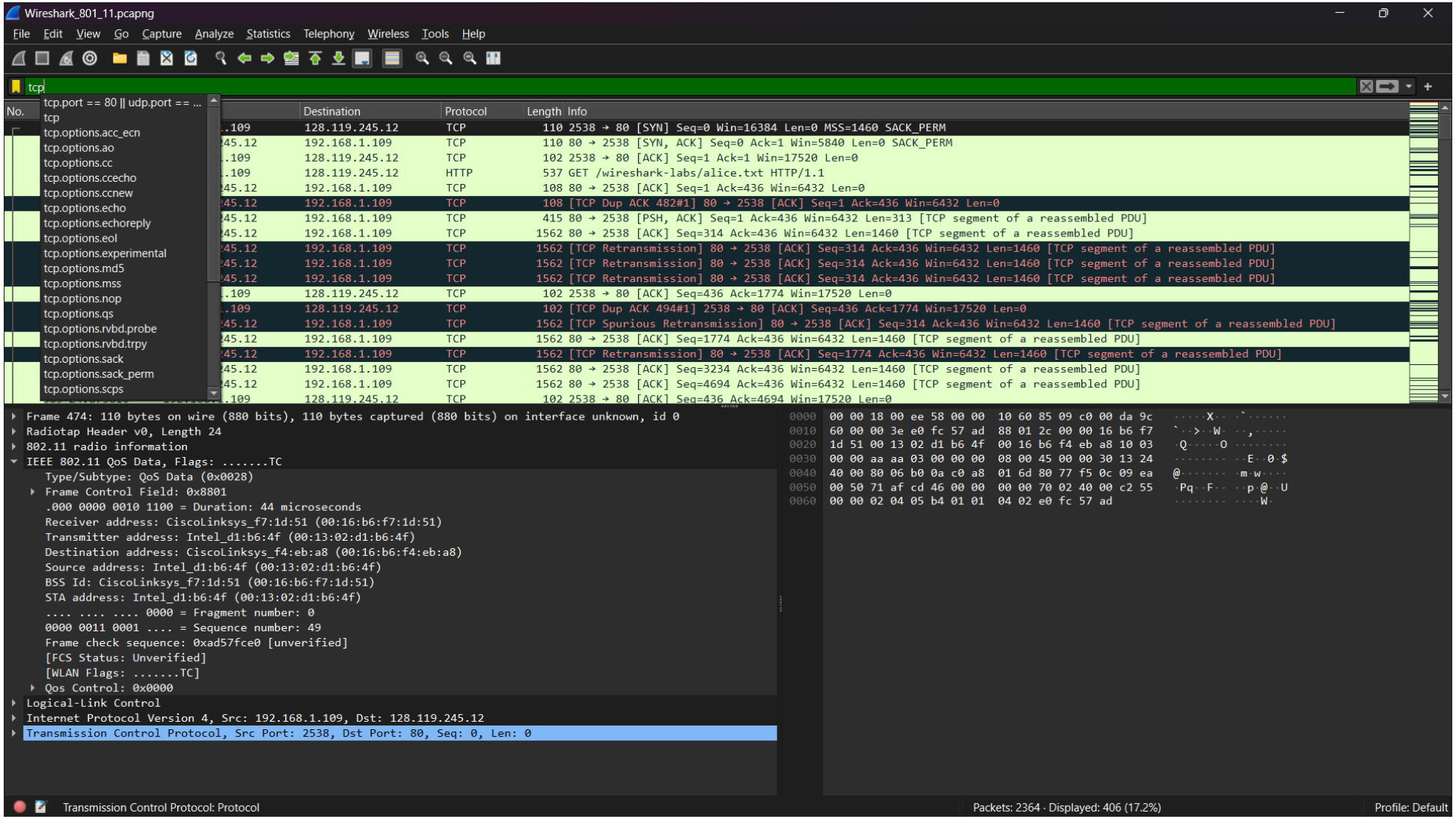
A:Source MAC address is: 00:16:b6:f7:1d:51

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

A: Destination MAC address is: ff:ff:ff:ff:ff:ff

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

A: MACBSSId:00:16:b6:f7:1d:51


Wireshark_801_11.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
tcp.port == 80 || udp.port == ...
tcp
tcp.options.acc_ecn
tcp.options.ao
tcp.options.cc
tcp.options.ccecho
tcp.options.ccnew
tcp.options.echo
tcp.options.echoreply
tcp.options.eol
tcp.options.experimental
tcp.options.md5
tcp.options.mss
tcp.options.nop
tcp.options.qs
tcp.options.rvbd.probe
tcp.options.rvbd.trpy
tcp.options.sack
tcp.options.sack_perm
tcp.options.scps
No. Destination Protocol Length Info
128.119.245.12 TCP 110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
192.168.1.109 TCP 110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM
128.119.245.12 TCP 102 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
128.119.245.12 HTTP 537 GET /wireshark-labs/alice.txt HTTP/1.1
192.168.1.109 TCP 108 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
192.168.1.109 TCP 108 [TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
192.168.1.109 TCP 415 80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP segment of a reassembled PDU]
192.168.1.109 TCP 1562 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
192.168.1.109 TCP 1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
192.168.1.109 TCP 1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
192.168.1.109 TCP 1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
128.119.245.12 TCP 102 2538 → 80 [ACK] Seq=436 Ack=1774 Win=17520 Len=0
128.119.245.12 TCP 102 [TCP Dup ACK 494#1] 2538 → 80 [ACK] Seq=436 Ack=1774 Win=17520 Len=0
192.168.1.109 TCP 1562 [TCP Spurious Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
192.168.1.109 TCP 1562 80 → 2538 [ACK] Seq=1774 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
192.168.1.109 TCP 1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=1774 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
192.168.1.109 TCP 1562 80 → 2538 [ACK] Seq=3234 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
192.168.1.109 TCP 1562 80 → 2538 [ACK] Seq=4694 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
128.119.245.12 TCP 102 2538 → 80 [ACK] Seq=436 Ack=4694 Win=17520 Len=0
Frame 474: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface unknown, id 0
Radiotap Header v0, Length 24
802.11 radio information
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: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
Destination address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
STA address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
.... .... .... 0000 = Fragment number: 0
0000 0011 0001 .... = Sequence number: 49
Frame check sequence: 0xad57fce0 [unverified]
[FCS Status: Unverified]
[WLAN Flags: .......TC]
Qos Control: 0x0000
Logical-Link Control
Internet Protocol Version 4, Src: 192.168.1.109, Dst: 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
0050 00 50 71 af cd 46 00 00 00 00 70 02 40 00 c2 55
0060 00 00 02 04 05 b4 01 01 04 02 e0 fc 57 ad
Transmission Control Protocol: Protocol
Packets: 2364 · Displayed: 406 (17.2%)
Profile: Default

7. 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? [Note: the traces were taken on a rather old AP].

A: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec] Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

8. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt) at t=24.8110. 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 for the TCP syn segment?

A: The MACaddress for the host sending the TCP SYN is 00:13:02:d1:b6:4f. The MAC address for the destination, which is the first hop router to which the host is connected, is 00:16:b6:f4:eb:a8. 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. The destination address is 128.199.245.12. It is important to understand that 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.

9. Does the destination IP address of this TCP SYN correspond to the host, access point, first-hop router, or the destination web server?

A: The destination IP address is 128.199.245.12. This corresponds to the destination web server gaia.cs.umass.edu.

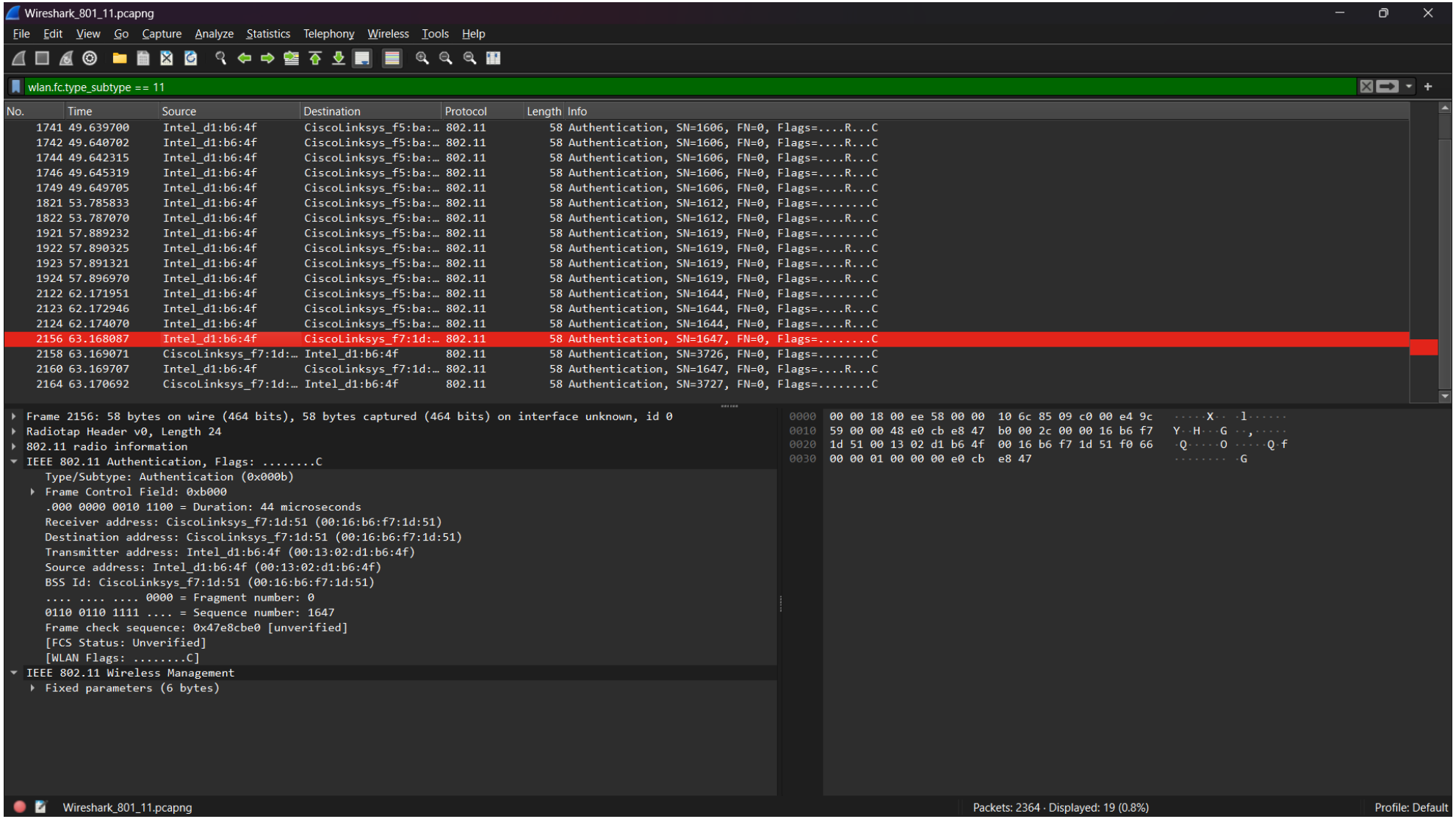
10. Find the 802.11 frame containing the SYNACK segment for this TCP session received at t=24.8277 What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram?

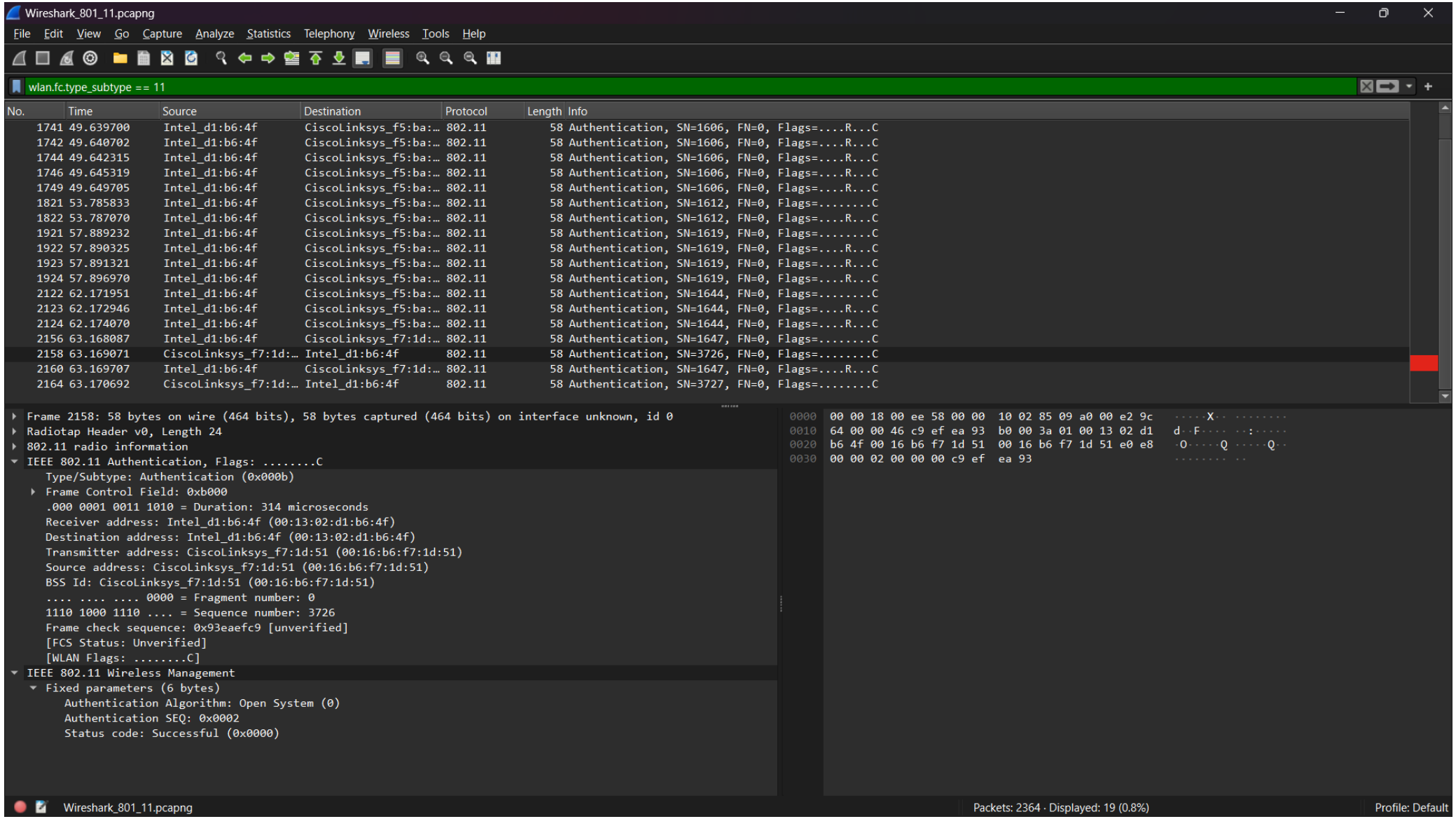
A: The MACaddress for the sender of the 802.11 frame containing the TCP SYNACK segment is 00:16:b6:f4:eb:a8, which is the 1st hop router to which the host is attached . The MACaddress for the destination, which is the host itself, is 91:2a:b0:49:b6:4f. The MACaddress for the BSS is 00:16:b6:f7:1d:51. 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.

11. 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). A:

a) At t =49.583615 a DHCP release is sent by the host to the DHCP server in the network that the host is leaving.

b) b) At t =49.609617, the host sends a DEAUTHENTICATION frame (Frametype = 00 [Management], subframe type = 12[Deauthentication]).


Wireshark_801_11.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
wlan.fc.type_subtype == 11
No. Time Source Destination Protocol Length Info
1741 49.639700 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1606, FN=0, Flags=....R...C
1742 49.640702 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1606, FN=0, Flags=....R...C
1744 49.642315 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1606, FN=0, Flags=....R...C
1746 49.645319 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1606, FN=0, Flags=....R...C
1749 49.649705 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1606, FN=0, Flags=....R...C
1821 53.785833 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1612, FN=0, Flags=........C
1822 53.787070 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1612, FN=0, Flags=....R...C
1921 57.889232 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1619, FN=0, Flags=........C
1922 57.890325 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1619, FN=0, Flags=....R...C
1923 57.891321 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1619, FN=0, Flags=....R...C
1924 57.896970 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1619, FN=0, Flags=....R...C
2122 62.171951 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1644, FN=0, Flags=........C
2123 62.172946 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1644, FN=0, Flags=....R...C
2124 62.174070 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1644, FN=0, Flags=....R...C
2156 63.168087 Intel_d1:b6:4f CiscoLinksys_f7:1d:… 802.11 58 Authentication, SN=1647, FN=0, Flags=........C
2158 63.169071 CiscoLinksys_f7:1d:… Intel_d1:b6:4f 802.11 58 Authentication, SN=3726, FN=0, Flags=........C
2160 63.169707 Intel_d1:b6:4f CiscoLinksys_f7:1d:… 802.11 58 Authentication, SN=1647, FN=0, Flags=....R...C
2164 63.170692 CiscoLinksys_f7:1d:… Intel_d1:b6:4f 802.11 58 Authentication, SN=3727, FN=0, Flags=........C
Frame 2156: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface unknown, id 0
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Authentication, Flags: ........C
Type/Subtype: Authentication (0x000b)
Frame Control Field: 0xb000
.000 0000 0010 1100 = Duration: 44 microseconds
Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
Destination address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
.... .... .... 0000 = Fragment number: 0
0110 0110 1111 .... = Sequence number: 1647
Frame check sequence: 0x47e8cbe0 [unverified]
[FCS Status: Unverified]
[WLAN Flags: ........C]
IEEE 802.11 Wireless Management
Fixed parameters (6 bytes)
0000 00 00 18 00 ee 58 00 00 10 6c 85 09 c0 00 e4 9c
0010 59 00 00 48 e0 cb e8 47 b0 00 2c 00 00 16 b6 f7
0020 1d 51 00 13 02 d1 b6 4f 00 16 b6 f7 1d 51 f0 66
0030 00 00 01 00 00 00 e0 cb e8 47
Wireshark_801_11.pcapng
Packets: 2364 · Displayed: 19 (0.8%)
Profile: Default


Wireshark_801_11.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
wlan.fc.type_subtype == 11
No. Time Source Destination Protocol Length Info
1741 49.639700 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1606, FN=0, Flags=....R...C
1742 49.640702 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1606, FN=0, Flags=....R...C
1744 49.642315 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1606, FN=0, Flags=....R...C
1746 49.645319 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1606, FN=0, Flags=....R...C
1749 49.649705 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1606, FN=0, Flags=....R...C
1821 53.785833 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1612, FN=0, Flags=........C
1822 53.787070 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1612, FN=0, Flags=....R...C
1921 57.889232 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1619, FN=0, Flags=........C
1922 57.890325 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1619, FN=0, Flags=....R...C
1923 57.891321 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1619, FN=0, Flags=....R...C
1924 57.896970 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1619, FN=0, Flags=....R...C
2122 62.171951 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1644, FN=0, Flags=........C
2123 62.172946 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1644, FN=0, Flags=....R...C
2124 62.174070 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 58 Authentication, SN=1644, FN=0, Flags=....R...C
2156 63.168087 Intel_d1:b6:4f CiscoLinksys_f7:1d:… 802.11 58 Authentication, SN=1647, FN=0, Flags=........C
2158 63.169071 CiscoLinksys_f7:1d:… Intel_d1:b6:4f 802.11 58 Authentication, SN=3726, FN=0, Flags=........C
2160 63.169707 Intel_d1:b6:4f CiscoLinksys_f7:1d:… 802.11 58 Authentication, SN=1647, FN=0, Flags=....R...C
2164 63.170692 CiscoLinksys_f7:1d:… Intel_d1:b6:4f 802.11 58 Authentication, SN=3727, FN=0, Flags=........C
Frame 2158: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface unknown, id 0
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Authentication, Flags: ........C
Type/Subtype: Authentication (0x000b)
Frame Control Field: 0xb000
.000 0001 0011 1010 = Duration: 314 microseconds
Receiver address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
Destination address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
.... .... .... 0000 = Fragment number: 0
1110 1000 1110 .... = Sequence number: 3726
Frame check sequence: 0x93eaefc9 [unverified]
[FCS Status: Unverified]
[WLAN Flags: ........C]
IEEE 802.11 Wireless Management
Fixed parameters (6 bytes)
Authentication Algorithm: Open System (0)
Authentication SEQ: 0x0002
Status code: Successful (0x0000)
0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e2 9c
0010 64 00 00 46 c9 ef ea 93 b0 00 3a 01 00 13 02 d1
0020 b6 4f 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 e0 e8
0030 00 00 02 00 00 00 c9 ef ea 93
Wireshark_801_11.pcapng
Packets: 2364 · Displayed: 19 (0.8%)
Profile: Default

12. Let’s look first at AUTHENTICATION frames. At t = 63.1680, our host tries to associate with the 30 Munroe St AP. What form of authentication is the host requesting?

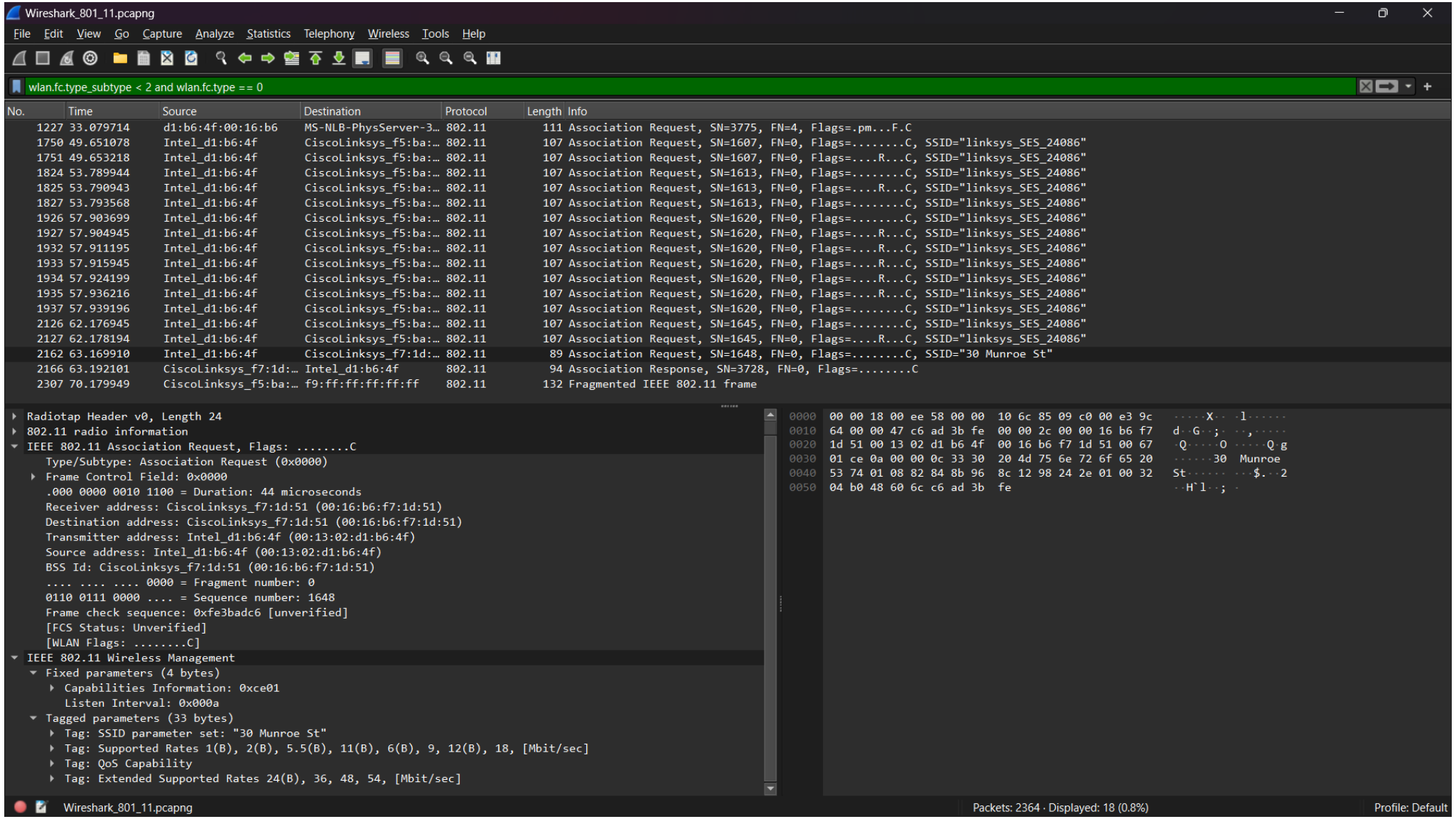
The host is requesting an Open System (0) form of authentication.

13. What is the Authentication SEQ value (authentication sequence number) of this authentication frame from host to AP?

A: Authentication SEQ value of this authentication frame is 0x0001.

14. The AP response to the authentication request is received at t = 63.1690. Has the AP accepted the form of authentication requested by the host?

A:Yes the AP accepted the form of authentication requested by the host.


Wireshark_801_11.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
wlan.fc.type_subtype < 2 and wlan.fc.type == 0
No. Time Source Destination Protocol Length Info
1227 33.079714 d1:b6:4f:00:16:b6 MS-NLB-PhysServer-3… 802.11 111 Association Request, SN=3775, FN=4, Flags=.pm...F.C
1750 49.651078 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 107 Association Request, SN=1607, FN=0, Flags=........C, SSID="linksys_SES_24086"
1751 49.653218 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 107 Association Request, SN=1607, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
1824 53.789944 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 107 Association Request, SN=1613, FN=0, Flags=........C, SSID="linksys_SES_24086"
1825 53.790943 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 107 Association Request, SN=1613, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
1827 53.793568 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 107 Association Request, SN=1613, FN=0, Flags=........C, SSID="linksys_SES_24086"
1926 57.903699 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 107 Association Request, SN=1620, FN=0, Flags=........C, SSID="linksys_SES_24086"
1927 57.904945 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
1932 57.911195 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
1933 57.915945 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
1934 57.924199 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
1935 57.936216 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
1937 57.939196 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 107 Association Request, SN=1620, FN=0, Flags=........C, SSID="linksys_SES_24086"
2126 62.176945 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 107 Association Request, SN=1645, FN=0, Flags=........C, SSID="linksys_SES_24086"
2127 62.178194 Intel_d1:b6:4f CiscoLinksys_f5:ba:… 802.11 107 Association Request, SN=1645, FN=0, Flags=....R...C, SSID="linksys_SES_24086"
2162 63.169910 Intel_d1:b6:4f CiscoLinksys_f7:1d:… 802.11 89 Association Request, SN=1648, FN=0, Flags=........C, SSID="30 Munroe St"
2166 63.192101 CiscoLinksys_f7:1d:… Intel_d1:b6:4f 802.11 94 Association Response, SN=3728, FN=0, Flags=........C
2307 70.179949 CiscoLinksys_f5:ba:… f9:ff:ff:ff:ff:ff 802.11 132 Fragmented IEEE 802.11 frame
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Association Request, Flags: ........C
Type/Subtype: Association Request (0x0000)
Frame Control Field: 0x0000
.000 0000 0010 1100 = Duration: 44 microseconds
Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
Destination address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
.... .... .... 0000 = Fragment number: 0
0110 0111 0000 .... = Sequence number: 1648
Frame check sequence: 0xfe3badc6 [unverified]
[FCS Status: Unverified]
[WLAN Flags: ........C]
IEEE 802.11 Wireless Management
Fixed parameters (4 bytes)
Capabilities Information: 0xce01
Listen Interval: 0x000a
Tagged parameters (33 bytes)
Tag: SSID parameter set: "30 Munroe St"
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
Tag: QoS Capability
Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
0000 00 00 18 00 ee 58 00 00 10 6c 85 09 c0 00 e3 9c
0010 64 00 00 47 c6 ad 3b fe 00 00 2c 00 00 16 b6 f7
0020 1d 51 00 13 02 d1 b6 4f 00 16 b6 f7 1d 51 00 67
0030 01 ce 0a 00 00 0c 33 30 20 4d 75 6e 72 6f 65 20
0040 53 74 01 08 82 84 8b 96 8c 12 98 24 2e 01 00 32
0050 04 b0 48 60 6c c6 ad 3b fe
Wireshark_801_11.pcapng
Packets: 2364 · Displayed: 18 (0.8%)
Profile: Default

15. What is the Authentication SEQ value of this authentication frame from AP to Host?

A: Authentication SEQ: 0x0002

16. What rates are indicated in the frame as SUPPORTED RATES. Do not include in your answers below any rates that are indicated as EXTENDED SUPPORTED RATES.

A: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec] (can be observed in the above figure)

17. Does the ASSOCIATION RESPONSE indicate a Successful or Unsuccessful association response?

A: The ASSOCIATION RESPONSE indicates a Successful association response by displaying the Status code as Successful (0x0000).

18. Does the fastest (largest) Extended Supported Rate the host has offered match the fastest (largest) Extended Supported Rate the AP is able to provide?

A: Yes, the fastest (largest) Extended Supported Rate the host has offered matches the fastest (largest) Extended Supported Rate the AP is able to provide which is 54 MBit/s.