

Jayathilaka H.A.D.T.T.

E/16/156

CO513 - Lab 07

Wireless Wireshark Lab - 802.11

Wireshark_802_11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2	0.062101	b6:78:8c:c1:ae:c0 (..	65:a8:d5:b2:c1:99 (..	802.11	1624	802.11 Block Ack Req, Flags=op.P...TC
3	0.085474	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4	0.187919	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
5	0.188100	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1482, FN=0, Flags=.....TC
6	0.188201	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f (..	802.11	38	Acknowledgement, Flags=.....C
7	0.188935	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1483, FN=0, Flags=...P...TC
8	0.189034	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f (..	802.11	38	Acknowledgement, Flags=.....C
9	0.290284	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2857, 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=.....C, BI=62, SSID=li001004 [Malformed Packet]
11	0.294432	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2858, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

> Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)

> Radiotap Header v0, Length 24

> 802.11 radio information

> IEEE 802.11 Beacon frame, Flags:C

> IEEE 802.11 Wireless Management

0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e3 9cX.....
0010 52 00 00 47 08 26 7e 05 80 00 00 00 ff ff ff ff R...G&w.....
0020 ff ff 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 60 b2Q.....Q`
0030 82 e1 38 96 28 00 00 00 64 00 01 06 00 0c 33 30 ..8.(...d....30
0040 20 4d 75 6e 72 6f 65 20 53 74 01 04 82 84 8b 96 Munroe St.....
0050 03 01 06 05 04 00 01 00 00 07 06 55 53 49 01 0bUSI...
0060 1a 0c 12 0f 00 03 a4 00 00 27 a4 00 00 42 43 5eBC^
0070 00 62 32 2f 00 2a 01 00 32 08 8c 12 98 24 b0 48 ..b2/*...2...\$H
0080 60 6c dd 15 00 0a f5 0a 02 40 c0 00 03 01 03 05 `l.....@.....
0090 0e 04 ff 00 03 00 11 01 01 dd 18 00 50 f2 02 01P.....
00a0 01 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e 00 62BC^b
00b0 32 2f 00 08 26 7e 05 2/-&w.....

Wireshark_802_11.pcap | Packets: 2364 · Displayed: 2364 (100.0%) | Profile: Default

Exercise 1

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

SSID : 30 Munroe St

SSID : linksys_SES_24086

Wireshark_802_11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
7	0.188935	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1483, FN=0, Flags=...P...TC
8	0.189034	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
9	0.290284	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2857, 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=.....C, BI=62, SSID=li\001\004 [Malformed Packet]
11	0.393174	Cisco-Li_f7:1d:51	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	ff:ff:ff:ff:bf:4a	802.11	90	Association Response, SN=3073, FN=0, Flags=.....C
13	0.495032	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2859, 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=.....C, BI=100, SSID=linksys12
15	0.597382	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2860, 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
17	0.600847	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2861, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

> Frame 15: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)

> Radiotap Header v0, Length 24

> 802.11 radio information

> IEEE 802.11 Beacon frame, Flags:C

> IEEE 802.11 Wireless Management

```

0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e2 9c .....X.....
0010 64 00 00 46 c0 fb 2d 4c 80 00 00 00 ff ff ff ff .....F...L...
0020 ff ff 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 c0 b2 .....Q.....Q...
0030 87 41 42 96 28 00 00 00 64 00 01 06 00 0c 33 30 ..AB:(...d....30
0040 20 4d 75 6e 72 6f 65 20 53 74 01 04 82 84 8b 96 ..Munroe St....
0050 03 01 06 05 04 00 01 00 00 07 06 55 53 49 01 0b .....USI...
0060 1a 0c 12 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e .....BC^
0070 00 62 32 2f 00 2a 01 00 32 08 8c 12 98 24 b0 48 ..b2/*...2...$H
0080 00 6c dd 15 00 0a f5 0a 02 40 c0 00 03 01 03 05 ..L.....@....
0090 0e 04 ff 00 03 00 11 01 01 dd 18 00 50 f2 02 01 .....P....
00a0 01 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e 00 62 .....BC^b
00b0 32 2f 00 c0 fb 2d 4c .....2/....L

```

Wireshark_802_11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1985	59.110319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1986	59.113196	Cisco-Li_f5:ba:bb	Cisco-Li_f5:ba:bb	802.11	38	Acknowledgement, Flags=.....C
1987	59.116569	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1988	59.124450	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1989	59.132071	Cisco-Li_f5:ba:bb	Cisco-Li_f5:ba:bb	802.11	38	Acknowledgement, Flags=.....C
1990	59.138949	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1991	59.142195	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1992	59.167459	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3682, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1993	59.269983	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3683, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1994	59.325865	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3833, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
1995	59.373240	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3684, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

> Frame 1994: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits)

> Radiotap Header v0, Length 24

> 802.11 radio information

> IEEE 802.11 Beacon frame, Flags:C

> IEEE 802.11 Wireless Management

```

0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 a3 9c .....X.....
0010 0b 00 00 07 32 a9 ba cd 80 00 00 00 ff ff ff ff .....2.....
0020 ff ff 00 18 39 f5 ba bb 00 18 39 93 b9 bb 90 ef .....9.....9...
0030 96 f1 8f ef c6 05 00 00 64 00 11 00 00 11 6c 6f .....d.....li
0040 6e 6b 73 79 73 5f 53 45 53 5f 32 34 30 38 36 01 ..nksys_SE_S_24086
0050 04 82 84 8b 96 03 01 06 05 04 00 01 00 00 dd 06 .....P.....P...
0060 00 10 18 02 01 f4 dd 18 00 50 f2 01 01 00 00 50 .....P.....P...
0070 f2 02 01 00 00 50 f2 02 01 00 00 50 f2 02 00 00 .....P.....P...
0080 32 a9 ba cd .....2...

```

2. What are the intervals of time between the transmissions of the beacon frames and 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).
- From the 30 Munroe St. access point : 0.1024 s
- From linksys_ses_24086 access point : 0.1024 s

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.

The image shows a Wireshark capture of 802.11 frames. The packet list on the left shows several frames, with packet 3 (0.085474) selected. The packet details pane on the right shows the structure of the selected beacon frame. The frame control field is 0x0000, indicating a beacon frame. The receiver address is broadcast (ff:ff:ff:ff:ff:ff). The destination address is broadcast (ff:ff:ff:ff:ff:ff). The transmitter address is Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51). The source address is Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51). The BSS ID is Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51). The fragment number is 0. The sequence number is 2855. The frame check sequence is 0x39700f3d (unverified).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2	0.062101	b6:78:8c:c1:ae:c0	(... 65:a8:d5:b2:c1:99 (... 802.11	1624	802.11 Block Ack Req, Flags=op.P...TC	
3	0.085474	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4	0.187919	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
5	0.188100	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1482, FN=0, Flags=.....TC
6	0.188201		IntelCor_d1:b6:4f (... 802.11	38	Acknowledgement, Flags=.....C	
7	0.188935	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1483, FN=0, Flags=...P...TC
8	0.189034		IntelCor_d1:b6:4f (... 802.11	38	Acknowledgement, Flags=.....C	
9	0.290284	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2857, 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=.....C, BI=62, SSID=li_001\004 [Malformed Packet]
11	0.292174	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2858, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

IEEE 802.11 Beacon frame, Flags:C
Type/Subtype: Beacon frame (0x0008)
> Frame Control Field: 0x0000
.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: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
.... 0000 = Fragment number: 0
1011 0010 0111 = Sequence number: 2855
Frame check sequence: 0x39700f3d [unverified]

```
0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e2 9c .....X.....
0010 52 00 00 46 3d 0f 70 39 00 00 00 00 ff ff ff ff R=F=p9.....
0020 ff ff 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 70 b2 .....C.....Qp:
0030 82 71 3a 96 28 00 00 00 64 00 01 06 00 0c 33 30 q:(...d...30...
0040 20 4d 75 6e 72 6f 65 20 53 74 01 04 82 84 8b 96 Munroe St.....
0050 03 01 06 05 04 00 01 00 00 07 06 55 53 49 01 0b .....USI...
0060 1a 0c 12 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e .....BC^...
0070 00 62 32 2f 00 2a 01 00 32 08 8c 12 98 24 b0 48 b2/*...2...$H
0080 60 6c dd 15 00 0a f5 0a 02 40 c0 00 03 01 03 05 `l.....@.....
0090 0e 04 ff 00 03 00 11 01 01 dd 18 00 50 f2 02 01 .....P...
00a0 01 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e 00 62 .....BC^b
00b0 32 2f 00 3d 0f 70 39 2f:=p9
```

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 is ff:ff:ff:ff:ff:ff.

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

The MAC BSS id is on the beacon frame from 30 Munroe St 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?

Four data rates : 1.0Mb/s, 2.0Mb/s, 5.5Mb/s, 11.0Mb/s

Extended supported rates : 6.0Mb/s, 9.0Mb/s, 12.0Mb/s, 18.0Mb/s, 24.0Mb/s, 36.0Mb/s, 48.0Mb/s, 54.0Mb/s

Wireshark · Packet 461 · Wireshark_802_11.pcap

```

> Frame 461: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Probe Response, Flags: .....C
> IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  > Tagged parameters (113 bytes)
    > Tag: SSID parameter set: 30 Munroe St
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 6
    > Tag: Country Information: Country Code US, Environment Indoor
    > Tag: EDCA Parameter Set
    > Tag: ERP Information
    > Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: Vendor Specific: Airgo Networks, Inc.
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

```

0000 00 00 18 00 ee 58 00 00 10 6c 85 09 c0 00 da 9c ...X...l...
0010 59 00 00 3e 1a 48 23 50 50 00 28 00 00 13 02 d1 Y...HMP P:(...
0020 b6 4f 00 16 b6 f7 1d 51 00 16 b6 27 12 51 10 c3 O...Q...Q...
0030 f4 08 b3 97 28 00 00 00 64 00 01 06 00 0c 33 30 (... d...30
0040 20 4d 75 6e 72 6f 65 20 53 74 01 04 82 84 8b 96 Munroe St...
0050 03 01 06 07 06 55 53 49 01 0b 1a 0c 12 0f 00 03 ...USI...
0060 a4 00 00 27 a4 00 00 42 43 5e 00 62 32 2f 00 2a ...B C^b2/*
0070 01 00 32 08 8c 12 98 24 b0 48 60 6c dd 15 00 0a ...2...\$ H^l...
0080 f5 0a 02 40 c0 00 03 01 03 05 0e 04 ff 00 03 00 ...@...m w...
0090 11 01 01 dd 18 00 05 f2 02 01 01 0f 00 03 a4 00 ...P...
00a0 00 27 a4 00 00 42 43 5e 00 62 32 2f 00 1a 48 23 ...BC^b2/H#

Close Help

Exercise 2

7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt).

Wireshark_802_11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

Packet list Narrow & Wide Case sensitive String SYN Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
472	24.809325	68.87.71.226	192.168.1.109	DNS	141	Standard query response 0x7892 A gaia.cs.umass.edu A 128.119.245.12
473	24.809513		Cisco-Li_f7:1d:51 (... 802.11	38	Acknowledgement, Flags=.....C	
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	

> Frame 474: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
> 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: 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 [unverified]
[FCS Status: Unverified]
> QoS Control: 0x0000
> Logical-Link Control

0010 60 00 00 3e e0 fc 57 ad 88 01 2c 00 00 16 b6 f7 ...>...W...
0020 1d 51 00 13 02 d1 b6 4f 00 16 b6 f4 eb a8 10 03 Q...O...
0030 00 00 aa aa 03 00 00 00 08 00 45 00 00 30 13 24 ...E...0\$
0040 40 00 80 06 b0 0a c0 a8 01 6d 80 77 f5 0c 09 ea @...m w...

802.11 radio information (wlan_radio) Packets: 2364 · Displayed: 2364 (100.0%) Profile: Default

7.1. What are three MAC address fields in the 802.11 frame?

- BSS Id
- Source address
- Destination

7.2. Which MAC address in this frame corresponds to the wireless host (in Hexadecimal Representation)?

00:13:02:d1:b6:4f

7.3. Which MAC address in this frame corresponds to the access point ?

00:16:b6:f4:eb:a8

7.4. Which MAC address in this frame corresponds to the first-hop router?

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

7.5. What is the IP address of the wireless host sending this TCP segment?

192.168.1.109

7.6. What is the destination IP address?

128.199.245.12

7.7. Does this destination IP address correspond to the host, access point, first-hop router, or some other network-attached device? Explain.

Yes, Destination IP address is corresponding to the host. The frame's destination MAC address is not the same as the destination IP address of the IP packet contained within it.

8. Find the 802.11 frame containing the SYNACK segment for this TCP session.

The image shows a Wireshark capture of a network session. The packet list on the left shows several packets, with packet 476 highlighted. The packet details pane on the right shows the structure of the 802.11 frame for packet 476, including the IEEE 802.11 QoS Data, Frame Control Field, and various addresses (Receiver, Transmitter, Destination, Source, BSS Id, STA address). The packet list shows the following details:

No.	Time	Source	Destination	Protocol	Length	Info
472	24.809325	68.87.71.226	192.168.1.109	DNS	141	Standard query response 0x7892 A gaia.cs.umass.edu A 128.119.245.12
473	24.809513		Cisco-Li_f7:1d:51 (.. 802.11	802.11	38	Acknowledgement, Flags=.....C
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	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	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	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	802.11	38	Acknowledgement, Flags=.....C

The packet details pane for packet 476 shows the following information:

- Frame 476: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
- Radiotap Header v0, Length 24
- 802.11 radio information
- IEEE 802.11 QoS Data, Flags: ..mP..F.C
- Type/Subtype: QoS Data (0x0028)
- Frame Control Field: 0x8832
- 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: 0xecd407d [unverified]
- [FCS Status: Unverified]
- QoS Control: 0x0100

8.1. What are three MAC address fields in the 802.11 frame?

- BSS Id : 00:16:b6:f7:1d:51
- Destination : 00:13:02:d1:b6:4f
- source address : 00:16:b6:f4:eb:a8

8.2. Which MAC address in this frame corresponds to the host?

00:13:02:d1:b6:4f

8.3. Which MAC address in this frame corresponds to the access point?

00:16:b6:f4:eb:a8

8.4. Which MAC address in this frame corresponds to the first-hop router?

00:16:b6:f4:eb:a8

8.5. 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: refer text book in reference list if you are unsure of how to answer this question, or the corresponding part of the previous question).

Because the TCP SYNACK's IP address is 128:199:245:12 and the destination IP address is 192.168.1.109, the sender MAC address in the frame does not correspond to the IP address of the device that transmitted the TCP segment enclosed within this datagram.

Exercise 3

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?

- A DHCP release is sent to 192.168.1.1 at t=49.583615
- The host sends a DEAUTHENTICATION frame at t=49.609617

Wireshark_802.11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

Packet list Narrow & Wide Case sensitive String SYN Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
1710	48.826299		IntelCor_d1:b6:4f (- 802.11	802.11	38	Acknowledgement, Flags=.....C
1711	48.928080	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3581, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1712	49.020125	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1599, FN=0, Flags=.....TC
1713	49.020257		IntelCor_d1:b6:4f (- 802.11	802.11	38	Acknowledgement, Flags=.....C
1714	49.020356	128.119.101.5	192.168.1.109	TCP	108	80 → 2543 [SYN, PSH, ECN, NS] Seq=2758133200 Win=7504 [Malformed Packet]
1715	49.020948	192.168.1.109	128.119.101.5	TCP	102	2543 → 80 [ACK] Seq=1 Ack=1 Win=16132 Len=0
1716	49.021047		IntelCor_d1:b6:4f (- 802.11	802.11	38	Acknowledgement, Flags=.....C
1717	49.030423	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3583, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1718	49.132768	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3584, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1719	49.132884	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1600, FN=0, Flags=...P...TC
1720	49.132981		IntelCor_d1:b6:4f (- 802.11	802.11	38	Acknowledgement, Flags=.....C
1721	49.224975	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1601, FN=0, Flags=.....TC
1722	49.225104		IntelCor_d1:b6:4f (- 802.11	802.11	38	Acknowledgement, Flags=.....C
1723	49.235239	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3585, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1724	49.235340	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1602, FN=0, Flags=...P...TC
1725	49.235439		IntelCor_d1:b6:4f (- 802.11	802.11	38	Acknowledgement, Flags=.....C
1726	49.337573	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3586, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
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	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	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	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	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_SE5_24086
1738	49.615869		Cisco-Li_f5:ba:bb (- 802.11	802.11	38	Acknowledgement, Flags=.....C
1739	49.617713		Cisco-Li_f5:ba:bb (- 802.11	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

Frame 546: 38 bytes on wire (304 bits) 38 bytes captured (304 bits)

MAC Frame control (wlan.fc), 2 bytes

Packets: 2364 · Displayed: 2364 (100.0%)

Profile: Default

Type here to search

8:56 PM 10/6/2021

10. Examine the trace file and look for AUTHENTICATION 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? .

17 AUTHENTICATION messages are sent from the wireless host to the linksys_ses_24086 AP

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

Yes

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

No

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 AUTHENTICATION frames sent from the host to and AP and vice versa. At what times is there an AUTHENTICATION frame from the host to 30 Munroe St. AP, and when is there a reply AUTHENTICATION sent from that AP to the host in reply? (Note that you can use the filter expression "wlan.fc.subtype == 11 and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the AUTHENTICATION frames in this trace for this wireless host.)

When t = 63.168087, there is an AUTHENTICATION frame starting at 00:13:02:d1:b6:4f and ending at 00:16:b7:f7:1d:51. At t = 63.169071, the AUTHENTICATION is returned.

Wireshark_802_11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.fc.subtype == 11 and wlan.fc.type == 0

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=.....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=.....C
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=.....C
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=.....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=.....C
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=.....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. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to be associated with an AP.

14.1. At what time is there an ASSOCIATE REQUEST from host to the 30 Munroe St AP?

At t=63.169910 s

14.2. When is the corresponding ASSOCIATE REPLY sent? (Note that you can use the filter expression “wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f” to display only the ASSOCIATE REQUEST and ASSOCIATE RESPONSE frames for this trace.)

At t=63.192101 s

Wireshark_802_11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f

No.	Time	Source	Destination	Protocol	Length	Info
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=.....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=.....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=.....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=.....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=.....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=.....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=.....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=.....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

> Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)

> Radiotap Header v0, Length 24

> 802.11 radio information

> IEEE 802.11 Association Response, Flags:C

Type/Subtype: Association Response (0x0001)

> Frame Control Field: 0x1000

..000 0001 0011 1010 = Duration: 314 microseconds

Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)

Destination address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)

```

0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e1 9c .....X.....
0010 64 00 00 45 2b ab f2 37 10 00 3a 01 00 13 02 d1 d...E+...7...
0020 b6 4f 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 00 e9 ..O.....Q...Q..
0030 01 06 00 00 05 c0 01 04 82 84 8b 96 32 08 8c 12 .....2.....
0040 98 24 b0 48 60 6c 0c 12 0f 00 03 a4 00 00 27 a4 ..$H^1.....
0050 00 00 42 43 5e 00 62 32 2f 00 2b ab f2 37 ..BC^b2 /+...7

```

MAC Frame control (wlan.fc), 2 bytes

Packets: 2364 • Displayed: 16 (0.7%)

Profile: Default

15. To answer this question, you will need to look into the parameters fields of the 802.11 wireless LAN management frame.

15.1. What transmission rates is the host willing to use?

The possible rates that both host and AP willing to use are 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, 54 Mbps.

15.2. What transmission rates is the AP? willing to use?

The possible rates that both host and AP willing to use are 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, 54 Mbps.

Exercise 4

16. Our trace contains a number of PROBE REQUEST and PROBE RESPONSE frames.

16.1. What are the sender, receiver and BSS ID MAC addresses in these frames?

Probe request

- Source: 00:12:f0:1f:57:13,
- destination: ff:ff:ff:ff:ff:ff,
- BSSID: ff:ff:ff:ff:ff:ff

Probe response

- Source: 00:16:b6:f7:1d:51,
- destination: 00:16:b6:f7:1d:51,
- BSSID: 00:16:b6:f7:1d:51

The image shows a Wireshark packet capture of an 802.11 wireless LAN network. The top pane displays a list of captured packets. The bottom pane shows a detailed view of a selected packet (No. 2018), which is an IEEE 802.11 Probe Response frame. The packet details include the Frame Control field, Duration, Receiver address, Destination address, Transmitter address, Source address, BSS ID, Fragment number, Sequence number, and Frame check sequence. The packet bytes pane shows the raw data of the frame.

No.	Time	Source	Destination	Protocol	Length	Info
2012	60.143694		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
2013	60.149192		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
2014	60.191465	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3693, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2015	60.248091	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	52	Null function (No data), SN=1626, FN=0, Flags=...P...TC
2016	60.249322	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	52	Null function (No data), SN=1626, FN=0, Flags=...PR..TC
2017	60.250820	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	52	Null function (No data), SN=1626, FN=0, Flags=...PR..TC
2018	60.256570	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=3694, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2019	60.258075	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=3694, FN=0, Flags=...R...C, BI=100, SSID=30 Munroe St
2020	60.259945	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=3694, FN=0, Flags=...R...C, BI=100, SSID=30 Munroe St
2021	60.280076	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=3695, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2022	60.284196	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	52	Null function (No data), SN=1627, FN=0, Flags=.....TC

Frame 2018: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)

Radiotap Header v0, Length 24

802.11 radio information

IEEE 802.11 Probe Response, Flags:C

Type/Subtype: Probe Response (0x0005)

Frame Control Field: 0x5000

.000 0001 0011 1010 = Duration: 314 microseconds

Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)

Destination address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)

Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

..... 0000 = Fragment number: 0

1110 0110 1110 = Sequence number: 3694

Frame check sequence: 0x89d81da4 [unverified]

[FCS Status: Unverified]

IEEE 802.11 Wireless Management

Fixed parameters (12 bytes)

Tagged parameters (113 bytes)

Tag: SSID parameter set: 30 Munroe St

0010 64 00 00 45 a4 1d d8 89 50 00 3a 01 00 13 02 d1 d...E....P:.....

MAC Frame control (wlan.fc), 2 bytes

Packets: 2364 · Displayed: 2364 (100.0%)

Profile: Default

16.2. What is the purpose of these two types of frames? (To answer this last question, you'll need to dig into the online references cited at the end of this lab sheet).

The probe request is a broadcast from the host to look for an access point. The probe response is used by the access point to respond to the host.