



COMPUTER NETWORK

Lab 7

Student name: Nguyễn Minh Tâm
ID: 1952968

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

Ans:

The two access points that are issuing most of beacon frames in this trace have an SSID of “30 Munroe St” and “linksys_ses_24086”.

No.	Time	Source	Destination	Protocol	Length	Info
1492	09:05:49.248652	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3483, FN=0, Flags=.....C, BI=100, SSID=linksys12
1493	09:05:49.344811	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3501, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1494	09:05:49.351279	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3484, FN=0, Flags=.....C, BI=100, SSID=linksys1R
1495	09:05:49.447219	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3502, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1496	09:05:49.453527	LinksysG_67:22:94	5f:a5:ff:ff:ff:ff	802.11	90	Beacon frame, SN=3485, FN=0, Flags=.....C, BI=16484, SSID=linksys12
1497	09:05:49.549584	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3503, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1498	09:05:49.556027	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3486, FN=0, Flags=.....C, BI=100, SSID=linksys12
1499	09:05:49.605053	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3640, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
1500	09:05:49.652013	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3504, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1501	09:05:49.754403	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3505, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1502	09:05:49.856857	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3506, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1503	09:05:49.857019	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1566, FN=0, Flags=.....TC
1504	09:05:49.857119		IntelCor_d1:b6:4f (- 802.11		38	Acknowledgement, Flags=.....C

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?

Ans: They are both 0.1024s.

No.	Time	Source	Destination	Protocol	Length	Info
1492	09:05:49.248652	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3483, FN=0, Flags=.....C, BI=100, SSID=linksys12
1493	09:05:49.344811	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3501, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1494	09:05:49.351279	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3484, FN=0, Flags=.....C, BI=100, SSID=linksys1R
1495	09:05:49.447219	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3502, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1496	09:05:49.453527	LinksysG_67:22:94	5f:a5:ff:ff:ff:ff	802.11	90	Beacon frame, SN=3485, FN=0, Flags=.....C, BI=16484, SSID=linksys12
1497	09:05:49.549584	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3503, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1498	09:05:49.556027	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3486, FN=0, Flags=.....C, BI=100, SSID=linksys12
1499	09:05:49.605053	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3640, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
1500	09:05:49.652013	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3504, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1501	09:05:49.754403	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3505, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1502	09:05:49.856857	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3506, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1503	09:05:49.857019	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1566, FN=0, Flags=.....TC
1504	09:05:49.857119		IntelCor_d1:b6:4f (- 802.11		38	Acknowledgement, Flags=.....C

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
1101 1011 0000 = Sequence number: 3504
Frame check sequence: 0xa028b529 [unverified]
[FCS Status: Unverified]

IEEE 802.11 Wireless Management
Fixed parameters (12 bytes)
Timestamp: 174361600386
Beacon Interval: 0.102400 [Seconds]
Capabilities Information: 0x0601
Tagged parameters (119 bytes)



No.	Time	Source	Destination	Protocol	Length	Info
1492	09:05:49.248652	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3483, FN=0, Flags=.....C, BI=100, SSID=linksys12
1493	09:05:49.344811	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3501, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1494	09:05:49.351279	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3484, FN=0, Flags=.....C, BI=100, SSID=linksys1R
1495	09:05:49.447219	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3502, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1496	09:05:49.453527	LinksysG_67:22:94	5f:a5:ff:ff:ff:ff	802.11	90	Beacon frame, SN=3485, FN=0, Flags=.....C, BI=16484, SSID=linksys12
1497	09:05:49.549584	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3503, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1498	09:05:49.556027	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3486, FN=0, Flags=.....C, BI=100, SSID=linksys12
1499	09:05:49.605053	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3640, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
1500	09:05:49.652013	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3504, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1501	09:05:49.754403	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3505, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1502	09:05:49.856857	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3506, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1503	09:05:49.857019	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1566, FN=0, Flags=.....TC
1504	09:05:49.857119	IntelCor_d1:b6:4f	(.. 802.11	38	Acknowledgement, Flags=.....C	

Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
Source address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
BSS Id: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
..... 0000 = Fragment number: 0
1110 0011 1000 = Sequence number: 3640
Frame check sequence: 0x7c0930f2 [unverified]
[FCS Status: Unverified]

> IEEE 802.11 Wireless Management
 > Fixed parameters (12 bytes)
 Timestamp: 6351964057993
 Beacon Interval: 0.102400 [Seconds]
 > Capabilities Information: 0x0011
 > Tagged parameters (68 bytes)

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

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

No.	Time	Source	Destination	Protocol	Length	Info
1	09:05:07.072457	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2	09:05:07.134558	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	09:05:07.157931	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4	09:05:07.260376	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
5	09:05:07.260557	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1482, FN=0, Flags=.....TC
6	09:05:07.260658	IntelCor_d1:b6:4f	(.. 802.11	38	Acknowledgement, Flags=.....C	
7	09:05:07.261392	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	09:05:07.261491	IntelCor_d1:b6:4f	(.. 802.11	38	Acknowledgement, Flags=.....C	
9	09:05:07.362741	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2857, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
10	09:05:07.366889	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=li0010040[Malformed Packet]
11	09:05:07.465631	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2858, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
12	09:05:07.469147	00:ae:93:3d:0a:4a	ff:ff:ff:ff:bf:4a	802.11	90	Association Response, SN=3073, FN=0, Flags=.....C
13	09:05:07.567489	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2859, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

> 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: 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 0110 = Sequence number: 2854

Frame check sequence: 0x057e2608 [unverified]

[FCS Status: Unverified]

> IEEE 802.11 Wireless Management

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

Ans: The destination MAC address on the 30 Munroe St, beacon frame is ff:ff:ff:ff:ff:ff.



No.	Time	Source	Destination	Protocol	Length	Info
1	09:05:07.072457	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2	09:05:07.134558	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	09:05:07.157931	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4	09:05:07.260376	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
5	09:05:07.260557	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1482, FN=0, Flags=.....TC
6	09:05:07.260658		IntelCor_d1:b6:4f (-	802.11	38	Acknowledgement, Flags=.....C
7	09:05:07.261392	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	09:05:07.261491		IntelCor_d1:b6:4f (-	802.11	38	Acknowledgement, Flags=.....C
9	09:05:07.362741	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2857, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
10	09:05:07.366889	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=li001\0040[Malformed Packet]
11	09:05:07.465631	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2858, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
12	09:05:07.469147	00:ae:93:3d:0a:4a	ff:ff:ff:ff:bf:4a	802.11	90	Association Response, SN=3073, FN=0, Flags=.....C
13	09:05:07.567489	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2859, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

> 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: 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 0110 = Sequence number: 2854

Frame check sequence: 0x857e2608 [unverified]

[FCS Status: Unverified]

> IEEE 802.11 Wireless Management

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

Ans: The MAC BSS ID address on the 30 Munroe St, beacon frame is 00:16:b6:f7:1d:51. (Figure in question 3)

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

Ans:

The support rates are 1.0, 2.0, 5.5, 11.0 Mbps.

The extended rates are 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0 and 54.0 Mbps.

No.	Time	Source	Destination	Protocol	Length	Info
1	09:05:07.072457	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2	09:05:07.134558	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	09:05:07.157931	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4	09:05:07.260376	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
5	09:05:07.260557	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1482, FN=0, Flags=.....TC
6	09:05:07.260658	IntelCor_d1:b6:4f (-	802.11	38	Acknowledgement, Flags=.....C	
7	09:05:07.261392	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	09:05:07.261491	IntelCor_d1:b6:4f (-	802.11	38	Acknowledgement, Flags=.....C	
9	09:05:07.362741	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2857, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
10	09:05:07.366889	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=li0010040[Malformed Packet]
11	09:05:07.465631	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2858, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
12	09:05:07.469147	00:ae:93:3d:0a:4a	ff:ff:ff:ff:bf:4a	802.11	90	Association Response, SN=3073, FN=0, Flags=.....C
13	09:05:07.567489	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2859, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

> 802.11 radio information

> IEEE 802.11 Beacon frame, Flags:C

> IEEE 802.11 Wireless Management

> Fixed parameters (12 bytes)

> Tagged parameters (119 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: Traffic Indication Map (TIM): DTIM 1 of 1 bitmap

> 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

7. 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.



Ans:

The MAC address for the host sending the TCP SYN is 00:13:02:d1:b6:4f.
The MAC address for the destination, which 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. This corresponds to the server gaia.cs.umass.edu.

No.	Time	Source	Destination	Protocol	Length	Info
466	09:05:31.865150	IntelCor_d1:b6:4f	Broadcast		90	Who has 192.168.1.1? Tell 192.168.1.109
467	09:05:31.865250		IntelCor_d1:b6:4f (.. 802.11	ARP	38	Acknowledgement, Flags=.....C
468	09:05:31.867888	Cisco-Li_f7:1d:51	Cisco-Li_f4:eb:e8	802.11	90	Fragmented IEEE 802.11 frame
469	09:05:31.868030		Cisco-Li_f7:1d:51 (.. 802.11		38	Acknowledgement, Flags=.....C
470	09:05:31.868130	192.168.1.109	68.87.71.226	DNS	125	Standard query 0x7892 A gaia.cs.umass.edu
471	09:05:31.868226		IntelCor_d1:b6:4f (.. 802.11		38	Acknowledgement, Flags=.....C
472	09:05:31.881782	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	09:05:31.881970		Cisco-Li_f7:1d:51 (.. 802.11		38	Acknowledgement, Flags=.....C
474	09:05:31.883550	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	09:05:31.883688		IntelCor_d1:b6:4f (.. 802.11		38	Acknowledgement, Flags=.....C
476	09:05:31.900208	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	09:05:31.900379		Cisco-Li_f7:1d:51 (.. 802.11		38	Acknowledgement, Flags=.....C
478	09:05:31.900481	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0

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

8. 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?

Ans:

The MAC address for the sender of the 802.11 frame containing the TCP SYNACK segment is 00:16:b6:f4:eb:a8, which is the first hop router to which the host is attached .

The MAC address for the destination, which the host itself, is 91:2a:b0:49:b6:4f.

The MAC address for the BSS is 00:16:b6:f7:1d:51.

The IP address of the server sending the TCP SYNACK is 128.199.245.12 (gaia.cs.umass.edu).

The destination address is 192.168.1.109 (our wireless PC).



No.	Time	Source	Destination	Protocol	Length	Info
466	09:05:31.865150	IntelCor_d1:b6:4f	Broadcast	ARP	90	Who has 192.168.1.1? Tell 192.168.1.109
467	09:05:31.865250		IntelCor_d1:b6:4f (... 802.11		38	Acknowledgement, Flags=.....C
468	09:05:31.867888	Cisco-Li_f7:1d:51	Cisco-Li_f4:eb:e8	802.11	90	Fragmented IEEE 802.11 frame
469	09:05:31.868030		Cisco-Li_f7:1d:51 (... 802.11		38	Acknowledgement, Flags=.....C
470	09:05:31.868130	192.168.1.109	68.87.71.226	DNS	125	Standard query 0x7892 A gaia.cs.umass.edu
471	09:05:31.868226		IntelCor_d1:b6:4f (... 802.11		38	Acknowledgement, Flags=.....C
472	09:05:31.881782	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	09:05:31.881970		Cisco-Li_f7:1d:51 (... 802.11		38	Acknowledgement, Flags=.....C
474	09:05:31.883550	192.168.1.109	128.119.245.12	TCP	110	2538 → 80 [SVN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
475	09:05:31.883688		IntelCor_d1:b6:4f (... 802.11		38	Acknowledgement, Flags=.....C
476	09:05:31.900208	128.119.245.12	192.168.1.109	TCP	110	80 → 2538 [SVN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1
477	09:05:31.900379		Cisco-Li_f7:1d:51 (... 802.11		38	Acknowledgement, Flags=.....C
478	09:05:31.900481	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0

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

> Logical-Link Control

9. What two actions are taken 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? Looking at the 802.11 specification, is there another frame that you might have expected to see, but don't see here?

Ans:

At t = 49.583615 a DHCP release is sent by the host to the DHCP server (whose IP address is 192.168.1.1) in the network that the host is leaving. At t = 49.609617, the host sends a DEAUTHENTICATION frame (Frametype = 00 [Management], subframe type = 12[Deauthentication]). One might have expected to see a DISASSOCIATION request to have been sent.

No.	Time	Source	Destination	Protocol	Length	Info
1729	09:05:56.512498	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3587, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1730	09:05:56.512603	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	09:05:56.512700		IntelCor_d1:b6:4f (... 802.11		38	Acknowledgement, Flags=.....C
1732	09:05:56.614938	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3588, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1733	09:05:56.656072	192.168.1.109	192.168.1.1	DHCP	390	DHCP Release - Transaction ID 0xea5a526
1734	09:05:56.656228		IntelCor_d1:b6:4f (... 802.11		38	Acknowledgement, Flags=.....C
1735	09:05:56.682074	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	Deauthentication, SN=1605, FN=0, Flags=.....C
1736	09:05:56.682227		IntelCor_d1:b6:4f (... 802.11		38	Acknowledgement, Flags=.....C
1737	09:05:56.686935	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1606, FN=0, Flags=.....C, SSID=linksys_SES_24086
1738	09:05:56.688326		Cisco-Li_f5:ba:bb (... 802.11		38	Acknowledgement, Flags=.....C
1739	09:05:56.690170		Cisco-Li_f5:ba:bb (... 802.11		38	Acknowledgement, Flags=.....C
1740	09:05:56.711314	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	09:05:56.712157	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....R...C

Frame 1733: 390 bytes on wire (3120 bits), 390 bytes captured (3120 bits)

Encapsulation type: IEEE 802.11 plus radiotap radio header (23)

Arrival Time: Jun 29, 2007 09:05:56.656072000 SE Asia Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1183082756.656072000 seconds

[Time delta from previous captured frame: 0.041134000 seconds]

[Time delta from previous displayed frame: 0.041134000 seconds]

[Time since reference or first frame: 49.583615000 seconds]

Frame Number: 1733

Frame Length: 390 bytes (3120 bits)

Capture Length: 390 bytes (3120 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: radiotap:wlan_radio:wlan:llc:ip:udp:dhcp]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]



No.	Time	Source	Destination	Protocol	Length	Info
1729	09:05:56.512498	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3587, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1730	09:05:56.512603	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	09:05:56.512700		IntelCor_d1:b6:4f (..	802.11	38	Acknowledgement, Flags=.....C
1732	09:05:56.614938	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3588, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1733	09:05:56.656072	192.168.1.109	192.168.1.1	DHCP	390	DHCP Release - Transaction ID 0xea5a526
1734	09:05:56.656228		IntelCor_d1:b6:4f (..	802.11	38	Acknowledgement, Flags=.....C
1735	09:05:56.682074	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	Deauthentication, SN=1605, FN=0, Flags=.....C
1736	09:05:56.682227		IntelCor_d1:b6:4f (..	802.11	38	Acknowledgement, Flags=.....C
1737	09:05:56.686935	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1606, FN=0, Flags=.....C, SSID=linksys_SES_24086
1738	09:05:56.688326		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1739	09:05:56.690170		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1740	09:05:56.711314	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	09:05:56.712157	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C

[Time delta from previous captured frame: 0.025846000 seconds]
[Time delta from previous displayed frame: 0.025846000 seconds]
[Time since reference or first frame: 49.609617000 seconds]
Frame Number: 1735
Frame Length: 54 bytes (432 bits)
Capture Length: 54 bytes (432 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: radiotap:wlan_radio:wlan]
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Deauthentication, Flags:C
Type/Subtype: Deauthentication (0x000c)
> Frame Control Field: 0xc000
.000 0000 0010 1100 = Duration: 44 microseconds
Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

10. How many AUTHENTICATION messages are sent from the wireless host to the linksys_ses_24086 AP (which has a MAC address of Cisco_Li_f5:ba:bb) starting at around t=49?
Ans: The first AUTHENTICATION from the host to the AP is at t = 49.638857.

No.	Time	Source	Destination	Protocol	Length	Info
1731	09:05:56.512700		IntelCor_d1:b6:4f (..	802.11	38	Acknowledgement, Flags=.....C
1732	09:05:56.614938	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3588, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1733	09:05:56.656072	192.168.1.109	192.168.1.1	DHCP	390	DHCP Release - Transaction ID 0xea5a526
1734	09:05:56.656228		IntelCor_d1:b6:4f (..	802.11	38	Acknowledgement, Flags=.....C
1735	09:05:56.682074	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	Deauthentication, SN=1605, FN=0, Flags=.....C
1736	09:05:56.682227		IntelCor_d1:b6:4f (..	802.11	38	Acknowledgement, Flags=.....C
1737	09:05:56.686935	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1606, FN=0, Flags=.....C, SSID=linksys_SES_24086
1738	09:05:56.688326		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1739	09:05:56.690170		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1740	09:05:56.711314	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	09:05:56.712157	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	09:05:56.713159	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1743	09:05:56.714367		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C

v Frame 1740: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
Arrival Time: Jun 29, 2007 09:05:56.711314000 SE Asia Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1183082756.711314000 seconds
[Time delta from previous captured frame: 0.021144000 seconds]
[Time delta from previous displayed frame: 0.021144000 seconds]
[Time since reference or first frame: 49.638857000 seconds]
Frame Number: 1740
Frame Length: 58 bytes (464 bits)
Capture Length: 58 bytes (464 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: radiotap:wlan_radio:wlan]
> Radiotap Header v0, Length 24
> 802.11 radio information

11. Does the host want the authentication to require a key or be open?
Ans: The host is requesting that the association be open.



No.	Time	Source	Destination	Protocol	Length	Info
1731	09:05:56.512700		IntelCor_d1:b6:4f (..	802.11	38	Acknowledgement, Flags=.....C
1732	09:05:56.614938	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3588, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1733	09:05:56.656072	192.168.1.109	192.168.1.1	DHCP	390	DHCP Release - Transaction ID 0xea5a526
1734	09:05:56.656228		IntelCor_d1:b6:4f (..	802.11	38	Acknowledgement, Flags=.....C
1735	09:05:56.682074	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	Deauthentication, SN=1605, FN=0, Flags=.....C
1736	09:05:56.682227		IntelCor_d1:b6:4f (..	802.11	38	Acknowledgement, Flags=.....C
1737	09:05:56.686935	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1606, FN=0, Flags=.....C, SSID=linksys_SES_24086
1738	09:05:56.688326		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1739	09:05:56.690170		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1740	09:05:56.711314	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	09:05:56.712157	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	09:05:56.713159	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1743	09:05:56.714367		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C

> Frame 1740: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)

> Radiotap Header v0, Length 24

> 802.11 radio information

> IEEE 802.11 Authentication, Flags:C

> IEEE 802.11 Wireless Management

> Fixed parameters (6 bytes)

Authentication Algorithm: Open System (0)

Authentication SEQ: 0x0001

Status code: Successful (0x0000)

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

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

13. At what times are there an AUTHENTICATION frame from the host to the 30 Munroe St. AP, and when is there a reply AUTHENTICATION sent from that AP to the host in reply?

Ans:

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

At t = 63.169071 there is an AUTHENTICATION from sent in the reverse direction from the BSS to the wireless host.

No.	Time	Source	Destination	Protocol	Length	Info
1821	09:06:00.858290	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=.....C
1822	09:06:00.859527	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
1921	09:06:04.961689	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=.....C
1922	09:06:04.962782	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1923	09:06:04.963778	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1924	09:06:04.969427	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
2122	09:06:09.244408	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=.....C
2123	09:06:09.245403	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2124	09:06:09.246527	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2156	09:06:10.240544	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=.....C
2158	09:06:10.241528	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=.....C
2160	09:06:10.242164	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
2164	09:06:10.243149	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=3727, FN=0, Flags=.....C

[Time since reference or first frame: 63.168087000 seconds]

Frame Number: 2156

Frame Length: 58 bytes (464 bits)

Capture Length: 58 bytes (464 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: radiotap:wlan_radio:wlan]

> Radiotap Header v0, Length 24

> 802.11 radio information

> IEEE 802.11 Authentication, Flags:C

Type/Subtype: Authentication (0x000b)

> Frame Control Field: 0xb000

.0000 0000 0010 1100 = Duration: 44 microseconds

Receiver address: Cisco-Li_f7:1d:51 (00:16:b7:f7:1d:51)

Destination address: Cisco-Li_f7:1d:51 (00:16:b7:f7:1d:51)

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: Cisco-Li_f7:1d:51 (00:16:b7:f7:1d:51)

.... 0000 = Fragment number: 0

0110 0110 1111 = Sequence number: 1647

Frame check sequence: 0x47e8cbe0 [unverified]



No.	Time	Source	Destination	Protocol	Length	Info
1821	09:06:00.858290	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=.....C
1822	09:06:00.859527	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
1921	09:06:04.961689	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=.....C
1922	09:06:04.962782	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1923	09:06:04.963778	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1924	09:06:04.969427	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
2122	09:06:09.244408	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=.....C
2123	09:06:09.245403	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2124	09:06:09.246527	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2156	09:06:10.240544	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=.....C
2158	09:06:10.241528	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=.....C
2160	09:06:10.242164	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
2164	09:06:10.243149	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=.....C

[Time since reference or first frame: 63.169071000 seconds]
Frame Number: 2158
Frame Length: 58 bytes (464 bits)
Capture Length: 58 bytes (464 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: radiotap:wlan_radio:wlan]
> 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: 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 1000 1110 = Sequence number: 3726
Frame check sequence: 0x93eae9c9 [unverified]

14. At what time is there an ASSOCIATE REQUEST from host to the 30 Munroe St AP? When is the corresponding ASSOCIATE REPLY sent?

Ans:

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

At t = 63.192101 there is an ASSOCIATE RESPONSE from sent in the reverse direction from the BSS to the wireless host.

No.	Time	Source	Destination	Protocol	Length	Info
1827	09:06:00.866025	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	09:06:04.976156	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	09:06:04.977402	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	09:06:04.983652	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	09:06:04.988402	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	09:06:04.996656	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	09:06:05.008673	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	09:06:05.011653	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	09:06:09.249402	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	09:06:09.250651	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	09:06:10.242367	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	09:06:10.264558	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C
2307	09:06:17.252406	Cisco-Li_f5:ba:7b	f9:ff:ff:ff:ff:ff	802.11	132	Fragmented IEEE 802.11 frame

[Time since reference or first frame: 63.169910000 seconds]
Frame Number: 2162
Frame Length: 89 bytes (712 bits)
Capture Length: 89 bytes (712 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: radiotap:wlan_radio:wlan]
> 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: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Destination address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
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: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
.... 0000 = Fragment number: 0
0110 0111 0000 = Sequence number: 1648
Frame check sequence: 0xfe3badc6 [unverified]



No.	Time	Source	Destination	Protocol	Length	Info
1827	09:06:00.866025	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	09:06:04.976156	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	09:06:04.977402	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	09:06:04.983652	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	09:06:04.988402	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	09:06:04.996656	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	09:06:05.008673	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	09:06:05.011653	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	09:06:09.249402	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	09:06:09.250651	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	09:06:10.242367	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	09:06:10.264558	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C
2307	09:06:17.252406	Cisco-Li_f5:ba:7b	f9:ff:ff:ff:ff:ff	802.11	132	Fragmented IEEE 802.11 frame

[Time since reference or first frame: 63.192101000 seconds]

Frame Number: 2166
Frame Length: 94 bytes (752 bits)
Capture Length: 94 bytes (752 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: radiotap:wlan_radio:wlan]

> 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)
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 1001 0000 = Sequence number: 3728
Frame check sequence: 0x37f2ab2b [unverified]

15. What transmission rates is the host willing to use? The AP?

Ans:

In the ASSOCIATION REQUEST frame the supported rates are advertised as 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, and 54 Mbps.

The same rates are advertised in the ASSOCIATION RESPONSE.

No.	Time	Source	Destination	Protocol	Length	Info
1827	09:06:00.866025	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	09:06:04.976156	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	09:06:04.977402	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	09:06:04.983652	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	09:06:04.988402	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	09:06:04.996656	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	09:06:05.008673	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	09:06:05.011653	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	09:06:09.249402	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	09:06:09.250651	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	09:06:10.242367	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	09:06:10.264558	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C
2307	09:06:17.252406	Cisco-Li_f5:ba:7b	f9:ff:ff:ff:ff:ff	802.11	132	Fragmented IEEE 802.11 frame

> Frame 2162: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
IEEE 802.11 Association Request, Flags:C
IEEE 802.11 Wireless Management
Fixed parameters (4 bytes)
Capabilities Information: 0x0001
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]



No.	Time	Source	Destination	Protocol	Length	Info
1827	09:06:00.866025	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	09:06:04.976156	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	09:06:04.977402	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	09:06:04.983652	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	09:06:04.988402	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	09:06:04.986656	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	09:06:05.008673	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	09:06:05.011653	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
2126	09:06:09.249402	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
2127	09:06:09.250651	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	09:06:10.242367	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	89	Association Request, SN=1648, FN=0, Flags=.....R...C, SSID=30 Munroe St
2166	09:06:10.264558	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C
2307	09:06:17.252406	Cisco-Li_f5:ba:7b	f9:ff:ff:ff:ff:ff	802.11	132	Fragmented IEEE 802.11 frame

> 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

> IEEE 802.11 Wireless Management

- > Fixed parameters (6 bytes)
 - > Capabilities Information: 0x0601
 - > Status code: Successful (0x0000)
 - > ..00 0000 0000 0101 = Association ID: 0x0005
- > Tagged parameters (36 bytes)
 - > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
 - > Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
 - > Tag: EDCA Parameter Set

16. What are the sender, receiver and BSS ID MAC addresses in these frames? What is the purpose of these two types of frames?

Ans:

At t = 2.297613 there is a PROBE REQUEST sent with source 00:12:f0:1f:57:13, destination and a BSS ID of ff:ff:ff:ff:ff:ff.

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

A PROBE REQUEST is used by a host in active scanning to find an Access Point.

No.	Time	Source	Destination	Protocol	Length	Info
46	09:05:09.309091	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1486, FN=0, Flags=.....TC
47	09:05:09.309187	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=.....C
48	09:05:09.310146	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1487, FN=0, Flags=...P...TC
49	09:05:09.310243	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=.....C
50	09:05:09.370070	IntelCor_1f:57:13	Broadcast	802.11	79	Probe Request, SN=576, FN=0, Flags=.....C, SSID=Home WIFI
51	09:05:09.373154	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
52	09:05:09.374648	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....R...C, BI=100, SSID=30 Munroe St
53	09:05:09.376520	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....R...C, BI=100, SSID=30 Munroe St
54	09:05:09.378019	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....R...C, BI=100, SSID=30 Munroe St
55	09:05:09.381020	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....R...C, BI=100, SSID=30 Munroe St
56	09:05:09.382529	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....R...C, BI=100, SSID=30 Munroe St
57	09:05:09.410605	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2879, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
58	09:05:09.513029	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2880, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

[Time since reference or first frame: 2.297613000 seconds]

Frame Number: 50

Frame Length: 79 bytes (632 bits)

Capture Length: 79 bytes (632 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: radiotap:wlan_radio:wlan]

> 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_1f:57:13 (00:12:f0:1f:57:13)
 - > Source address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
 - > BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
 - > 0000 = Fragment number: 0
 - > 0010 0100 0000 = Sequence number: 576
 - > Frame check sequence: 0xa373c5ff [unverified]
 - > [FCS Status: Unverified]



No.	Time	Source	Destination	Protocol	Length	Info
46	09:05:09.309091	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1486, FN=0, Flags=.....TC
47	09:05:09.309187		IntelCor_d1:b6:4f (...)	802.11	38	Acknowledgement, Flags=.....C
48	09:05:09.310146	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1487, FN=0, Flags=...P...TC
49	09:05:09.310243		IntelCor_d1:b6:4f (...)	802.11	38	Acknowledgement, Flags=.....C
50	09:05:09.370070	IntelCor_1f:57:13	Broadcast	802.11	79	Probe Request, SN=576, FN=0, Flags=.....C, SSID=Home WIFI
51	09:05:09.373154	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
52	09:05:09.374648	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
53	09:05:09.376520	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
54	09:05:09.378019	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
55	09:05:09.381020	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
56	09:05:09.382529	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
57	09:05:09.410605	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2879, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
58	09:05:09.513029	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2880, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

[Time since reference or first frame: 2.300697000 seconds]

Frame Number: 51

Frame Length: 177 bytes (1416 bits)

Capture Length: 177 bytes (1416 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: radiotap:wlan_radio:wlan]

> 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_1f:57:13 (00:12:f0:1f:57:13)

Destination address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)

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 0011 1110 = Sequence number: 2878

Frame check sequence: 0x6ed851bb [unverified]

[FCS Status: Unverified]