EE450

802.11 Lab Report

Yuhang Xiao

Abstract

This report investigates the behavior of the widely-used 802.11 wireless network protocol in detail. We will capture and analyze a trace of 802.11 frames, which consisting of a Linksys 802.11g combined access point/router, and frames are captured on channel 6. At first, the host is already associated with the 30 Munroe St AP, then it will make HTTP request to 128.119.245.12 and 128.119.240.19. After that, it will disconnect from the previous AP and try to connect to a new AP, linksys_ses_24086, and finally, it will re-connect with the original AP. During the process, multiple useful frames like beacon frame, AUTHENTICATION, DEAUTHENTICATION, ASSOCIATION REQUEST, ASSOCIATION RESPONSE, PROBE REQUEST and PROBE RESPONSE are captured. This report will dive into the details of these frames and help to understand the 802.11 protocol.

1.
The two access points' SSIDs are "30 Munroe St" and "linksys_SES_24086".

BSSID	Channel	SSID	Percent Packets	Percent Retry	Retry	Beacons	Data Pkts	Probe Reqs	Probe Resp	Auths	Deauths	Other	Protection
00:16:b6:f7:1d:51	6	30 Munroe St	94.7	0.0	0	718	0	0	0	0	0	0	
00:06:25:67:22:94	6	lin◆~ys	4.0	0.0	0	30	0	0	0	0	0	0	WEP
00:18:39:f5:ba:bb	6	linksys_SES_24086	0.8	0.0	0	6	0	0	0	0	0	0	
50:2b:25:67:22:94	6	linksys12	0.1	0.0	0	1	0	0	0	0	0	0	
43:31:36:af:83:73		<Broadcast>	0.1	100.0	1	1	0	0	0	0	0	0	Unknown
00:18:39:93:b9:bb	6	linksys_SES_24086	0.1	0.0	0	1	0	0	0	0	0	0	
19:02:25:c7:78:94		<Broadcast>	0.1	0.0	0	1	0	0	0	0	0	0	

Display filter: (wlan.fc.type == 0) && (wlan.fc.type_subtype == 8) Apply

2.
The beacon interval for both access points are 0.102400 seconds.

```
IEEE 802.11 Wireless Management
  Fixed parameters (12 bytes)
    Timestamp: 6351990989206
    Beacon Interval: 0.102400 [Seconds]
  > Capabilities Information: 0x0011
  Tagged parameters (68 bytes)
  > Tag: SSID parameter set: linksys_SES_24086
  > 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 0 of 1 bitmap
  > Tag: Vendor Specific: Broadcom
  > Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
```

```
IEEE 802.11 Wireless Management
  Fixed parameters (12 bytes)
    Timestamp: 174388019586
    Beacon Interval: 0.102400 [Seconds]
  > Capabilities Information: 0x0601
  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 0 of 1 bitmap
  > Tag: Country Information: Country Code US, Environment Indoor
  > Tag: EDCA Parameter Set
```

3.
The source MAC address is 00:16:b6:f7:1d:51.

```
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
  1110 1100 1101 .... = Sequence number: 3789
  Frame check sequence: 0x4043f9ca [unverified]
  [FCS Status: Unverified]
```

4.
The destination MAC address is ff:ff:ff:ff:ff:ff.

```
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
    1110 1100 1101 .... = Sequence number: 3789
    Frame check sequence: 0x4043f9ca [unverified]
    [FCS Status: Unverified]
```

5.
The MAC BSS ID address is 00:16:b6:f7:1d:51.

```
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
    1110 1100 1101 .... = Sequence number: 3789
    Frame check sequence: 0x4043f9ca [unverified]
    [FCS Status: Unverified]
```

6.
The support rates are 1, 2, 5.5, 11 Mbps. The extended supported rates are 6, 9, 12, 18, 24, 36, 48 and 54 Mbps.

```
IEEE 802.11 Wireless Management
  Fixed parameters (12 bytes)
      Timestamp: 174388019586
      Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x0601
  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 0 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.

The three MAC address field are 00:16:b6:f7:1d:51, 00:13:02:d1:b6:4f and 00:16:b6:f4:eb:a8. The MAC address for the wireless host is 00:13:02:d1:b6:4f. The MAC address for the access point is 00:16:b6:f7:1d:51. The MAC address for the first hop router is 00:16:b6:f4:eb:a8. The IP address of the host sending the TCP SYN is 192.168.1.109. The destination IP address is 128.119.245.12, which corresponds to the server gaia.cs.umass.edu.

```
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
> 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
```

8.

The three MAC address field are 91:2a:b0:49:b6:4f, 00:16:b6:f7:1d:51 and 00:16:b6:f4:eb:a8. The MAC address for the host is 91:2a:b0:49:b6:4f. The MAC address for the access point is 00:16:b6:f7:1d:51. The MAC address for the first-hop router is 00:16:b6:f4:eb:a8, which is also the sender MAC address. The sender IP address is 128.199.245.12, which corresponds to gaia.cs.umass.edu. Thus, it doesn't correspond to the sender MAC address.

```
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: 0xecdc407d [unverified]
    [FCS Status: Unverified]
  > Qos Control: 0x0100
> Logical-Link Control
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.109
> Transmission Control Protocol, Src Port: 80, Dst Port: 2538, Seq: 0, Ack: 1, Len: 0
```

9.
A DHCP Release frame is sent by the host to the DHCP server. Then, the host sends a DEAUTHENTICATION frame. A DISASSOCIATION request frame is expected to send but don't see here.

No.	Time	Source	Destination	Protocol	Length	Info
1728	49.430007		IntelCor_d1:b6:4f…	802.11	38	Acknowledgement, Flags=.....C
1729	49.440041	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3587, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1730	49.440146	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1604, FN=0, Flags=...P...TC
1731	49.440243		IntelCor_d1:b6:4f…	802.11	38	Acknowledgement, Flags=.....C
1732	49.542481	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3588, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1733	49.583615	192.168.1.109	192.168.1.1	DHCP	390	DHCP Release - Transaction ID 0xea5a526
1734	49.583771		IntelCor_d1:b6:4f…	802.11	38	Acknowledgement, Flags=.....C
1735	49.609617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	Deauthentication, SN=1605, FN=0, Flags=.....C
1736	49.609770		IntelCor_d1:b6:4f…	802.11	38	Acknowledgement, Flags=.....C
1737	49.614478	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1606, FN=0, Flags=.....C, SSID=linksys_SES_24086
1738	49.615869		Cisco-Li_f5:ba:bb…	802.11	38	Acknowledgement, Flags=.....C
1739	49.617713		Cisco-Li_f5:ba:bb…	802.11	38	Acknowledgement, Flags=.....C
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1743	49.641910		Cisco-Li_f5:ba:bb…	802.11	38	Acknowledgement, Flags=.....C

10.
There are 15 AUTHENTICATION messages sent from the wireless host to the linksys_ses_24086 AP starting at around t=49.

(wlan.da == 00:18:39:f5:ba:bb) && (wlan.fc.type_subtype == 11)

No.	Time	Source	Destination	Protocol	Length	Info
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1821	53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=.....C
1822	53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
1921	57.889232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=.....C
1922	57.890325	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
2122	62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=.....C
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C

11.
The host wants the authentication to be open because the frame specifies the Authentication Algorithm is Open System.

```
> 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
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0001
      Status code: Successful (0x0000)
```

12.
Applying the filter that the source address is the address of linksys_ses_24086 AP, there is no reply sent.

(wlan.sa == 00:18:39:f5:ba:bb)

No.	Time	Source	Destination	Protocol	Length	Info
1499	42.532596	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3640, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
1513	42.839707	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3643, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
1527	43.658960	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3651, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
1557	44.887707	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3663, FN=13, Flags=.....C, BI=8, SSID=winksys_SES_24086\001\004[illegible]\003…
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
2290	69.463202	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3938, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
2296	69.667955	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3940, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
2321	71.101576	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3954, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086

13.
At t = 63.168087, there is an AUTHENTICATION frame sent from the wireless host to the 30 Munroe St AP. At t = 63.169071 there is a reply AUTHENTICATION frame sent from the AP to the host. There is another sending at t = 63.169707 and replying at t = 63.170692.

(wlan.fc.type_subtype == 11) && (wlan.addr == 00:13:02:d1:b6:4f)

No.	Time	Source	Destination	Protocol	Length	Info
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.
At t = 63.169910 there is an ASSOCIATION REQUEST frame sent from host to the 30 Munroe St AP. At t = 63.192101 there is an ASSOCIATION RESPONSE frame sent from the AP to the wireless host.

(wlan.fc.type_subtype <= 2) && (wlan.addr == 00:13:02:d1:b6:4f)

No.	Time	Source	Destination	Protocol	Length	Info
1934	57.924199	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1935	57.936216	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1937	57.939196	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086
2126	62.176945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1645, FN=0, Flags=.....C, SSID=linksys_SES_24086
2127	62.178194	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1645, FN=0, Flags=....R...C, SSID=linksys_SES_24086
2162	63.169910	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	89	Association Request, SN=1648, FN=0, Flags=.....C, SSID=30 Munroe St
2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C

15.
Looking into the ASSOCIATION REQUEST and ASSOCIATION RESPONSE frame, after combining the supported rate and extended supported rate, both host and the AP are willing to use the transmission rates of 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

```
> IEEE 802.11 Association Request, Flags: .....C
v IEEE 802.11 Wireless Management
  v Fixed parameters (4 bytes)
    > Capabilities Information: 0xce01
      Listen Interval: 0x000a
  v 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]
```

```
> IEEE 802.11 Association Response, Flags: ........C
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
    > Capabilities Information: 0x0601
      Status code: Successful (0x0000)
      ..00 0000 0000 0101 = Association ID: 0x0005
  v 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.

In PROBE REQUEST frames, the sender MAC address is 00:13:02:d1:b6:4f, the receiver and BSS ID MAC address is ff:ff:ff:ff:ff:ff. In PROBE RESPONSE frames, the sender MAC address is 00:16:b6:f7:1d:51, which is also the BSS ID MAC address. The receiver MAC address is 00:13:02:d1:b6:4f. A PROBE REQUEST frame is a broadcast for a host to find an AP. A PROBE RESPONSE is a response message from the AP to the host. They are used for active scanning.

```
v IEEE 802.11 Probe Request, Flags: ........C
    Type/Subtype: Probe Request (0x0004)
  > Frame Control Field: 0x4000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    .... .... .... 0000 = Fragment number: 0
    0110 0010 0111 .... = Sequence number: 1575
    Frame check sequence: 0xe5498848 [unverified]
```

```
v 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
    1101 1101 1100 .... = Sequence number: 3548
    Frame check sequence: 0x5e3fc99d [unverified]
```

Conclusion

This report dived into the details of the ubiquitous 802.11 (WiFi) protocol. A trace of captured 802.11 frames was analyzed and discussed. First, the multiple MAC addresses inside the 802.11 frames were discussed and their purposes were clarified. Then, the AUTHENTICATION behavior in 802.11 protocol was explored. After that, the ASSOCIATION REQUEST and the ASSOCIATION RESPONSE frame were discussed in details when the host tried to reconnect with the original AP. Finally, the active association was briefly explored by the captured PROBE REQUEST and PROBE RESPONSE frame. Through this report, the main behaviors of 802.11 protocol are explored and clarified.