

学号：	姓名：	班级：
实验题目： 实验十一 802.11 WiFi		
实验学时：2h	实验日期：2023.05.15	
实验目的： 学习 WIFI 的相关内容		
硬件环境： Windows10 家庭版		
软件环境： Wireshark		
实验步骤与内容： 实验内容： 1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace? 2. What are the intervals of time between the transmissions of the beacon frames the linksys_ses_24086 access point? From the 30 Munroe St. access point? (Hint: this interval of time is contained in the beacon frame itself). 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). 4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St?? 5. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from 30 Munroe St? 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? 7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). What are three MAC address fields in the 802.11frame? 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.

8. Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram? (Hint: review Figure 6.19 in the text if you are unsure of how to answer this question, or the corresponding part of the previous question. It's particularly important that you understand this).

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

10. 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? .

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

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

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 an AP and vice versa. 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? (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.)

14. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associate with an AP. At what time is there an ASSOCIATE REQUEST from host to the 30 Munroe St AP? 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.)

15. What transmission rates is the host willing to use? The AP? To answer this question, you will need to look into the parameters fields of the 802.11 wireless LAN management frame.

16. What are the sender, receiver and BSS ID MAC addresses in these frames? 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 earlier in this lab).

实验步骤:

本实验主要学习 WIFI 的相关内容, 采用作者给出的包进行分析。

1. 两个接入点的 SSID 分别是 30 Munroe St 和 linksys12。

1 0.000000	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
2 0.062101	8c:c1:ae:c0:...	8c:c1:ae:c0:...	802.11	1624 PV1 Management[Malformed Packet]
3 0.085474	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
4 0.187919	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
5 0.188100	IntelCor_d1:...	Cisco-Li_f7:...	802.11	54 QoS Null function (No data), SN=1482, FN=0, Flags=.....TC
6 0.188201	IntelCor_d1:...	IntelCor_d1:...	802.11	38 Acknowledgement, Flags=.....C
7 0.188935	IntelCor_d1:...	Cisco-Li_f7:...	802.11	54 QoS Null function (No data), SN=1483, FN=0, Flags=...P...TC
8 0.189034	IntelCor_d1:...	IntelCor_d1:...	802.11	38 Acknowledgement, Flags=.....C
9 0.290284	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2857, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
10 0.294432	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=6c69ee0104e2273a32[Malformed Packet]
11 0.393174	Cisco-Li_f7:...	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:...	00:ae:93:3d:...	802.11	90 PV1 Reserved
13 0.495032	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2859, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
14 0.499197	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3074, FN=0, Flags=.....C, BI=100, SSID="linksys12"
15 0.597382	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2860, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
16 0.601687	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3075, FN=0, Flags=.....C, BI=100, SSID="linksys12"
17 0.699847	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2861, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
18 0.802226	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2862, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
19 0.904619	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2863, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
20 1.007015	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2864, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
21 1.010949	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3079, FN=0, Flags=.....C, BI=100, SSID="linksys12"
22 1.109406	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2865, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
23 1.113691	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3080, FN=0, Flags=.....C, BI=100, SSID=2cdc6e6b7379733132

2. 时间间隔是 0.1024s, 从 Beacon Interval 可知

1 0.000000	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2854, FN=0, Flags=.....C, BI
2 0.062101	8c:c1:ae:c0:...	8c:c1:ae:c0:...	802.11	1624 PV1 Management[Malformed Packet]
3 0.085474	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2855, FN=0, Flags=.....C, BI
4 0.187919	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2856, FN=0, Flags=.....C, BI
5 0.188100	IntelCor_d1:...	Cisco-Li_f7:...	802.11	54 QoS Null function (No data), SN=1482, FN=0, Flag
6 0.188201	IntelCor_d1:...	IntelCor_d1:...	802.11	38 Acknowledgement, Flags=.....C
7 0.188935	IntelCor_d1:...	Cisco-Li_f7:...	802.11	54 QoS Null function (No data), SN=1483, FN=0, Flag
8 0.189034	IntelCor_d1:...	IntelCor_d1:...	802.11	38 Acknowledgement, Flags=.....C
9 0.290284	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2857, FN=0, Flags=.....C, BI
10 0.294432	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3072, FN=0, Flags=.....C, BI
11 0.393174	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2858, FN=0, Flags=.....C, BI
12 0.396690	00:ae:93:3d:...	00:ae:93:3d:...	802.11	90 PV1 Reserved
13 0.495032	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2859, FN=0, Flags=.....C, BI
14 0.499197	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3074, FN=0, Flags=.....C, BI
15 0.597382	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2860, FN=0, Flags=.....C, BI
16 0.601687	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3075, FN=0, Flags=.....C, BI
17 0.699847	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2861, FN=0, Flags=.....C, BI
18 0.802226	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2862, FN=0, Flags=.....C, BI
19 0.904619	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2863, FN=0, Flags=.....C, BI
20 1.007015	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2864, FN=0, Flags=.....C, BI
21 1.010949	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3079, FN=0, Flags=.....C, BI
22 1.109406	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2865, FN=0, Flags=.....C, BI
23 1.113691	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3080, FN=0, Flags=.....C, BI

> Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)	0000
> Radiotap Header v0, Length 24	0010
> 802.11 radio information	0020
> IEEE 802.11 Beacon frame, Flags:C	0030
> IEEE 802.11 Wireless Management	0040
> Fixed parameters (12 bytes)	0050
Timestamp: 174319001986	0060
Beacon Interval: 0.102400 [Seconds]	0070
> Capabilities Information: 0x0601	0080
	0090

3. 源 MAC 地址是 00:16:b6:f7:1d:51。

1	0.000000	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2854, FN=0, Flags=...
2	0.062101	8c:c1:ae:c0:...	8c:c1:ae:c0:...	802.11	1624 PV1 Management[Malformed Packet]
3	0.085474	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2855, FN=0, Flags=...
4	0.187919	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2856, FN=0, Flags=...
5	0.188100	IntelCor_d1:...	Cisco-Li_f7:...	802.11	54 QoS Null function (No data), SN=1482,
6	0.188201	IntelCor_d1:...	IntelCor_d1:...	802.11	38 Acknowledgement, Flags=.....C
7	0.188935	IntelCor_d1:...	Cisco-Li_f7:...	802.11	54 QoS Null function (No data), SN=1483,
8	0.189034	IntelCor_d1:...	IntelCor_d1:...	802.11	38 Acknowledgement, Flags=.....C
9	0.290284	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2857, FN=0, Flags=...
10	0.294432	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3072, FN=0, Flags=...
11	0.393174	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2858, FN=0, Flags=...
12	0.396690	00:ae:93:3d:...	00:ae:93:3d:...	802.11	90 PV1 Reserved
13	0.495032	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2859, FN=0, Flags=...
14	0.499197	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3074, FN=0, Flags=...
15	0.597382	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2860, FN=0, Flags=...
16	0.601687	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3075, FN=0, Flags=...
17	0.699847	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2861, FN=0, Flags=...
18	0.802226	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2862, FN=0, Flags=...
19	0.904619	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2863, FN=0, Flags=...
20	1.007015	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2864, FN=0, Flags=...
21	1.010949	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3079, FN=0, Flags=...
22	1.109406	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2865, FN=0, Flags=...
23	1.113691	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3080, FN=0, Flags=...

```

<
▼ 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)

```

4. 目标 MAC 地址是 ff:ff:ff:ff:ff:ff。
5. MAC BSSID 是 00:16:b6:f7:1d:51。
6. 四种数据速率是 1、2、5.5、11Mbit/sec，八种额外的扩展支持速率分别是 6、9、12、18、24、36、48、54Mbit/sec。

1	0.000000	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2854, FN=0, Flags=...
2	0.062101	8c:c1:ae:c0:...	8c:c1:ae:c0:...	802.11	1624 PV1 Management[Malformed Packet]
3	0.085474	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2855, FN=0, Flags=...
4	0.187919	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2856, FN=0, Flags=...
5	0.188100	IntelCor_d1:...	Cisco-Li_f7:...	802.11	54 QoS Null function (No data), SN=1482,
6	0.188201	IntelCor_d1:...	IntelCor_d1:...	802.11	38 Acknowledgement, Flags=.....C
7	0.188935	IntelCor_d1:...	Cisco-Li_f7:...	802.11	54 QoS Null function (No data), SN=1483,
8	0.189034	IntelCor_d1:...	IntelCor_d1:...	802.11	38 Acknowledgement, Flags=.....C
9	0.290284	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2857, FN=0, Flags=...
10	0.294432	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3072, FN=0, Flags=...
11	0.393174	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2858, FN=0, Flags=...
12	0.396690	00:ae:93:3d:...	00:ae:93:3d:...	802.11	90 PV1 Reserved
13	0.495032	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2859, FN=0, Flags=...
14	0.499197	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3074, FN=0, Flags=...
15	0.597382	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2860, FN=0, Flags=...
16	0.601687	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3075, FN=0, Flags=...
17	0.699847	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2861, FN=0, Flags=...
18	0.802226	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2862, FN=0, Flags=...
19	0.904619	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2863, FN=0, Flags=...
20	1.007015	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2864, FN=0, Flags=...
21	1.010949	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3079, FN=0, Flags=...
22	1.109406	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2865, FN=0, Flags=...
23	1.113691	LinksysG_67:...	Broadcast	802.11	90 Beacon frame, SN=3080, FN=0, Flags=...
24	1.214012	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=2866, FN=0, Flags=...

▼ 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]

7. 三个 MAC 地址字段, 源 MAC 地址: 00:13:02:d1:b6:4f, 目标 MAC 地址: 00:16:b6:f4:eb:a8, BSS Id: 00:16:b6:f7:1d:51。其中源主机对应的是 00:13:02:d1:b6:4f, 接入点对应的是 00:16:b6:f7:1d:51, 路由器对应的是: 00:16:b6:f4:eb:a8。源 IP 地址是 192.168.1.109, 目标 IP 地址是 128.119.245.12。

480	24.828...	192.168.1.109	128.119.245.12	HTTP	537 GET /wireshark-labs/alice.txt HTTP/1.1
482	24.846...	128.119.245.12	192.168.1.109	TCP	108 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432
484	24.847...	128.119.245.12	192.168.1.109	TCP	108 [TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=
486	24.848...	128.119.245.12	192.168.1.109	TCP	415 80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6
488	24.850...	128.119.245.12	192.168.1.109	TCP	1562 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432
489	24.850...	128.119.245.12	192.168.1.109	TCP	1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=
490	24.851...	128.119.245.12	192.168.1.109	TCP	1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=
492	24.851...	128.119.245.12	192.168.1.109	TCP	1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=
494	24.851...	192.168.1.109	128.119.245.12	TCP	102 2538 → 80 [ACK] Seq=436 Ack=1774 Win=175
495	24.852...	192.168.1.109	128.119.245.12	TCP	102 [TCP Dup ACK 494#1] 2538 → 80 [ACK] Seq=
497	24.852...	128.119.245.12	192.168.1.109	TCP	1562 [TCP Spurious Retransmission] 80 → 2538
501	24.873...	128.119.245.12	192.168.1.109	TCP	1562 80 → 2538 [ACK] Seq=1774 Ack=436 Win=643
502	24.874...	128.119.245.12	192.168.1.109	TCP	1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=
504	24.874...	128.119.245.12	192.168.1.109	TCP	1562 80 → 2538 [ACK] Seq=3234 Ack=436 Win=643
507	24.875...	128.119.245.12	192.168.1.109	TCP	1562 80 → 2538 [ACK] Seq=4694 Ack=436 Win=643
509	24.875...	192.168.1.109	128.119.245.12	TCP	102 2538 → 80 [ACK] Seq=436 Ack=4694 Win=175
511	24.894...	199.93.245.12	192.168.1.109	TCP	1562 80 → 2538 [ACK] Seq=1 Ack=1 Win=6432 Len
513	24.895...	128.119.245.12	192.168.1.109	TCP	1562 80 → 2538 [ACK] Seq=6154 Ack=436 Win=643

> 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 0011 = Sequence number: 51

8. 三个 MAC 地址字段, 源 MAC 地址: 00:16:b6:f4:eb:a8, 目标 MAC 地址: 00:13:02:d1:b6:4f。BSS ID 是 00:16:b6:f7:1d:51。其中目标主机对应的是 00:13:02:d1:b6:4f, 接入点对应的是 00:16:b6:f7:1d:51, 路由器对应的是:00:16:b6:f4:eb:a8。源 IP 地址是 128.119.245.12, 目标 IP 地址是 192.168.1.109。

482	24.846...	128.119.245.12	192.168.1.109	TCP	108	80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=
484	24.847...	128.119.245.12	192.168.1.109	TCP	108	[TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 A
486	24.848...	128.119.245.12	192.168.1.109	TCP	415	80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432
488	24.850...	128.119.245.12	192.168.1.109	TCP	1562	80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Le
489	24.850...	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=31
490	24.851...	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=31
492	24.851...	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=31
494	24.851...	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=1774 Win=17520
495	24.852...	192.168.1.109	128.119.245.12	TCP	102	[TCP Dup ACK 494#1] 2538 → 80 [ACK] Seq=436
497	24.852...	128.119.245.12	192.168.1.109	TCP	1562	[TCP Spurious Retransmission] 80 → 2538 [AC
501	24.873...	128.119.245.12	192.168.1.109	TCP	1562	80 → 2538 [ACK] Seq=1774 Ack=436 Win=6432 L
502	24.874...	128.119.245.12	192.168.1.109	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=17
504	24.874...	128.119.245.12	192.168.1.109	TCP	1562	80 → 2538 [ACK] Seq=3234 Ack=436 Win=6432 L
507	24.875...	128.119.245.12	192.168.1.109	TCP	1562	80 → 2538 [ACK] Seq=4694 Ack=436 Win=6432 L
509	24.875...	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=436 Ack=4694 Win=17520
511	24.894...	199.93.245.12	192.168.1.109	TCP	1562	80 → 2538 [ACK] Seq=1 Ack=1 Win=6432 Len=14
513	24.895...	128.119.245.12	192.168.1.109	TCP	1562	80 → 2538 [ACK] Seq=6154 Ack=436 Win=6432 L

IEEE 802.11 QoS Data, Flags:F.C

Type/Subtype: QoS Data (0x0028)

> Frame Control Field: 0x8802

.000 0000 0010 1000 = Duration: 40 microseconds

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

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

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

.... 0000 = Fragment number: 0

1100 0011 0101 = Sequence number: 3125

Frame check sequence: 0xae38de9c [unverified]

[FCS Status: Unverified]

9. 在 $t=49.583615s$ 时主机向即将离开的网络中的 DHCP 服务器 (IP 地址为 192.168.1.1) 发送 DHCP release, 在 $t=49.609617s$ 时主机发送一个 DEAUTHENTICATION 帧, Deauthentication 帧是一种 Wi-Fi 管理帧, 用于在无线网络中注销客户端设备。

1733 49.583...	192.168.1.109	192.168.1.1	DHCP	390 DHCP Release - Transaction ID 0xea5a526
1734 49.583...		IntelCor_d1:...	802.11	38 Acknowledgement, Flags=.....C
1735 49.609...	IntelCor_d1:...	Cisco-Li_f7:...	802.11	54 Deauthentication, SN=1605, FN=0, Flags=..
1736 49.609...		IntelCor_d1:...	802.11	38 Acknowledgement, Flags=.....C
1737 49.614...	IntelCor_d1:...	Broadcast	802.11	99 Probe Request, SN=1606, FN=0, Flags=.....
1738 49.615...		Cisco-Li_f5:...	802.11	38 Acknowledgement, Flags=.....C
1739 49.617...		Cisco-Li_f5:...	802.11	38 Acknowledgement, Flags=.....C
1740 49.638...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58 Authentication, SN=1606, FN=0, Flags=....
1741 49.639...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58 Authentication, SN=1606, FN=0, Flags=....
1742 49.640...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58 Authentication, SN=1606, FN=0, Flags=....
1743 49.641...		Cisco-Li_f5:...	802.11	38 Acknowledgement, Flags=.....C
1744 49.642...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58 Authentication, SN=1606, FN=0, Flags=....
1745 49.644...	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=3589, FN=0, Flags=.....
1746 49.645...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58 Authentication, SN=1606, FN=0, Flags=....
1747 49.646...		Cisco-Li_f5:...	802.11	38 Acknowledgement, Flags=.....C
1748 49.647...		Cisco-Li_f5:...	802.11	38 Acknowledgement, Flags=.....C
1749 49.649...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58 Authentication, SN=1606, FN=0, Flags=....
1750 49.651...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	187 Association Request, SN=1607, FN=0, Flags=....

> Frame 1735: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

> Radiotap Header v0, Length 24

> 802.11 radio information

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)

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 0100 0101 - Sequence number: 1605

10. 从主机发送到 AP 的第一个身份验证帧是在 t=49.638857s 发出的。一共有 15 条身份验证消息。

wlan.fc.type_subtype==0x000b

No.	Time	Source	Destination	Protocol	Length	Info
1740	49.638...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	49.639...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1744	49.642...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1746	49.645...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1749	49.649...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1821	53.785...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58	Authentication, SN=1612, FN=0, Flags=.....C
1822	53.787...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
1921	57.889...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58	Authentication, SN=1619, FN=0, Flags=.....C
1922	57.890...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1923	57.891...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1924	57.896...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
2122	62.171...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58	Authentication, SN=1644, FN=0, Flags=.....C
2123	62.172...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2124	62.174...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2156	63.168...	IntelCor_d1:...	Cisco-Li_f7:...	802.11	58	Authentication, SN=1647, FN=0, Flags=.....C
2158	63.169...	Cisco-Li_f7:...	IntelCor_d1:...	802.11	58	Authentication, SN=3726, FN=0, Flags=.....C
2160	63.169...	IntelCor_d1:...	Cisco-Li_f7:...	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
2164	63.170...	Cisco-Li_f7:...	IntelCor_d1:...	802.11	58	Authentication, SN=3727, FN=0, Flags=.....C

Type/Subtype: Authentication (0x000b)
Frame Control Field: 0xb000
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)
.... = Fragment number: 0
1110 1000 1110 = Sequence number: 3726
Frame check sequence: 0x93eaefc9 [unverified]
[FCS Status: Unverified]
IEEE 802.11 Wireless Management
Fixed parameters (6 bytes)

0000
0010
0020
0030

11. 希望打开，Open System 为 0 时，表示无线网络采用了开放系统的身份验证方式。意味着连接到该网络的设备无需提供密码或其他身份验证信息，即可与网络进行关联。任何设备都可以尝试连接到该网络，无需事先共享特定的密钥或密码，如下图所示：

1740 49.638...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58 Authentication, SN=1606, FN=0, Flags=
1741 49.639...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58 Authentication, SN=1606, FN=0, Flags=
1742 49.640...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58 Authentication, SN=1606, FN=0, Flags=
1743 49.641...		Cisco-Li_f5:...	802.11	38 Acknowledgement, Flags=.....C
1744 49.642...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58 Authentication, SN=1606, FN=0, Flags=
1745 49.644...	Cisco-Li_f7:...	Broadcast	802.11	183 Beacon frame, SN=3589, FN=0, Flags=..
1746 49.645...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58 Authentication, SN=1606, FN=0, Flags=
1747 49.646...		Cisco-Li_f5:...	802.11	38 Acknowledgement, Flags=.....C
1748 49.647...		Cisco-Li_f5:...	802.11	38 Acknowledgement, Flags=.....C
1749 49.649...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	58 Authentication, SN=1606, FN=0, Flags=
1750 49.651...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	107 Association Request, SN=1607, FN=0, F
1751 49.653...	IntelCor_d1:...	Cisco-Li_f5:...	802.11	107 Association Request, SN=1607, FN=0, F
1752 49.662...		Cisco-Li_f5:...	802.11	38 Acknowledgement, Flags=.....C
1753 49.663...		Cisco-Li_f5:...	802.11	38 Acknowledgement, Flags=.....C
1754 49.665...		Cisco-Li_f5:...	802.11	38 Acknowledgement, Flags=.....C
1755 49.669...		Cisco-Li_f5:...	802.11	38 Acknowledgement, Flags=.....C
1756 49.671...		Cisco-Li_f5:...	802.11	38 Acknowledgement, Flags=.....C
1757 49.673...		Cisco-Li_f5:...	802.11	38 Acknowledgement, Flags=.....C
1758 49.675...		Cisco-Li_f5:...	802.11	38 Acknowledgement, Flags=.....C
1759 49.676...		Cisco-Li_f5:...	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				
v IEEE 802.11 Wireless Management				
v Fixed parameters (6 bytes)				
Authentication Algorithm: Open System (0)				
Authentication SEQ: 0x0001				
Status code: Successful (0x0000)				

12. 没有看见，这可能是因为 AP 被配置为在与该 AP 关联时需要一个密钥，因此 AP 可能会忽略(即不响应)开放访问请求，这种情况表明该 AP 设置了需要进行身份验证或加密才能与其进行关联。当设备尝试以开放系统的方式进行关联时，AP 会忽略请求，并不会回复。

13. 在 t=63.168087s 时发送了身份认证帧，在 t=63.168087s 有一个认证帧从无线主机发出。在 t = 63.169071s，有一个从反向发送的 AUTHENTICATION 帧。

2156	63.168...	IntelCor_d1:...	Cisco-Li_f7:...	802.11	58 Authentication, SN=1647, FN=0, Flags=.....
2157	63.168...		IntelCor_d1:...	802.11	38 Acknowledgement, Flags=.....C
2158	63.169...	Cisco-Li_f7:...	IntelCor_d1:...	802.11	58 Authentication, SN=3726, FN=0, Flags=.....
2159	63.169...		Cisco-Li_f7:...	802.11	38 Acknowledgement, Flags=.....C
2160	63.169...	IntelCor_d1:...	Cisco-Li_f7:...	802.11	58 Authentication, SN=1647, FN=0, Flags=....R...
2161	63.169...		IntelCor_d1:...	802.11	38 Acknowledgement, Flags=.....C
2162	63.169...	IntelCor_d1:...	Cisco-Li_f7:...	802.11	89 Association Request, SN=1648, FN=0, Flags=...
2163	63.170...		IntelCor_d1:...	802.11	38 Acknowledgement, Flags=.....C
2164	63.170...	Cisco-Li_f7:...	IntelCor_d1:...	802.11	58 Authentication, SN=3727, FN=0, Flags=.....
2165	63.171...		Cisco-Li_f7:...	802.11	38 Acknowledgement, Flags=.....C
2166	63.192...	Cisco-Li_f7:...	IntelCor_d1:...	802.11	94 Association Response, SN=3728, FN=0, Flags=..
2167	63.192...		Cisco-Li_f7:...	802.11	38 Acknowledgement, Flags=.....C
2168	63.194...	0.0.0.0	255.255.255...	DHCP	390 DHCP Discover - Transaction ID 0x101b218a
2169	63.194...		IntelCor_d1:...	802.11	38 Acknowledgement, Flags=.....C
2170	63.201...	0.0.0.0	255.255.255...	DHCP	390 DHCP Discover - Transaction ID 0x2733a47c
2171	63.201...	0.0.0.0	255.255.255...	DHCP	390 DHCP Discover - Transaction ID 0x2733a47c
2172	63.201...		IntelCor_d1:...	802.11	38 Acknowledgement, Flags=.....C

<

> Frame 2156: 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)

14. t=63.169910s 有一个关联请求帧无线主机从发送出,在 t=63.192101s 时有关联响应发出。

2162	63.169...	IntelCor_d1:...	Cisco-Li_f7:...	802.11	89 Association Request, SN=1648, FN=0, Flags=.....C, s
2166	63.192...	Cisco-Li_f7:...	IntelCor_d1:...	802.11	94 Association Response, SN=3728, FN=0, Flags=.....C
2201	65.721...	Dell_4f:36:23	Broadcast	ARP	106 Who has 192.168.1.103? Tell 192.168.1.101
2216	66.235...	0.0.0.0	255.255.255...	DHCP	388 DHCP Discover - Transaction ID 0x2733a47c
2217	66.239...	0.0.0.0	255.255.255...	DHCP	394 DHCP Request - Transaction ID 0x2733a47c
2218	66.240...	IntelCor_d1:...	Broadcast	ARP	88 ARP Announcement for 192.168.1.109
2225	66.540...	IntelCor_d1:...	Broadcast	ARP	88 ARP Announcement for 192.168.1.109
2237	67.257...	192.168.1.109	224.0.0.22	IGMPv3	100 Membership Report / Join group 224.1.0.38 for any sour

<

> 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: 0xce01

Listen Interval: 0x000a

▼ Tagged parameters (33 bytes)

Tag: SSID parameter set: "30 Munroe St"

Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]

Tag: QoS Capability

Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]

0000 00 00

0010 64 00

0020 1d 51

0030 01 ce

0040 53 74

0050 04 b0

Wireshark_802_11.pcap

15. 主机传输速率: 1、2、5.5、11、6、9、12、18、24、32、48and 54 Mbps

2162	63.169...	IntelCor_d1:...	Cisco-Li_f7:...	802.11	89 Association Request, SN=1648, FN=0, Flags=
2166	63.192...	Cisco-Li_f7:...	IntelCor_d1:...	802.11	94 Association Response, SN=3728, FN=0, Flags=
2201	65.721...	Dell_4f:36:23	Broadcast	ARP	106 Who has 192.168.1.103? Tell 192.168.1.101
2216	66.235...	0.0.0.0	255.255.255...	DHCP	388 DHCP Discover - Transaction ID 0x2733a47c
2217	66.239...	0.0.0.0	255.255.255...	DHCP	394 DHCP Request - Transaction ID 0x2733a47c
2218	66.240...	IntelCor_d1:...	Broadcast	ARP	88 ARP Announcement for 192.168.1.109
2225	66.540...	IntelCor_d1:...	Broadcast	ARP	88 ARP Announcement for 192.168.1.109
2237	67.257...	192.168.1.109	224.0.0.22	IGMPv3	100 Membership Report / Join group 224.1.0.38
2242	67.261...	192.168.1.109	224.1.0.38	UDP	284 2570 → 497 Len=196
2247	67.564...	IntelCor_d1:...	Broadcast	ARP	88 ARP Announcement for 192.168.1.109
2255	68.076...	192.168.1.109	224.0.0.22	IGMPv3	100 Membership Report / Join group 224.1.0.38

> 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: 0xce01

Listen Interval: 0x000a

> Tagged parameters (33 bytes)

> Tag: SSID parameter set: "30 Munroe St"

> Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]

> Tag: QoS Capability

> Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]

AP 传输速率：1、2、5.5、11、6、9、12、18、24、32、48and 54 Mbps。

2166	63.192...	Cisco-Li_f7:...	IntelCor_d1:...	802.11	94 Association Response, SN=3728, FN=0, Flags=.....C
2201	65.721...	Dell_4f:36:23	Broadcast	ARP	106 Who has 192.168.1.103? Tell 192.168.1.101
2216	66.235...	0.0.0.0	255.255.255...	DHCP	388 DHCP Discover - Transaction ID 0x2733a47c
2217	66.239...	0.0.0.0	255.255.255...	DHCP	394 DHCP Request - Transaction ID 0x2733a47c
2218	66.240...	IntelCor_d1:...	Broadcast	ARP	88 ARP Announcement for 192.168.1.109
2225	66.540...	IntelCor_d1:...	Broadcast	ARP	88 ARP Announcement for 192.168.1.109
2237	67.257...	192.168.1.109	224.0.0.22	IGMPv3	100 Membership Report / Join group 224.1.0.38 for any sour
2242	67.261...	192.168.1.109	224.1.0.38	UDP	284 2570 → 497 Len=196
2247	67.564...	IntelCor_d1:...	Broadcast	ARP	88 ARP Announcement for 192.168.1.109
2255	68.076...	192.168.1.109	224.0.0.22	IGMPv3	100 Membership Report / Join group 224.1.0.38 for any sour

> 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

0000 00 00
0010 64 00
0020 b6 4f
0030 01 06
0040 98 24
0050 00 00

16. 根据描述，在时间 $t=2.297613s$ ，主机发送了一个 PROBE REQUEST（探测请求）。该请求的源地址为 00:12:f0:1f:57:13，目的地址为 ff:ff:ff:ff:ff:ff，BSSID 也为 ff:ff:ff:ff:ff:ff。在时间 $t = 2.300697s$ ，有一个 PROBE RESPONSE（探测响应）被发送出去。该响应的源地址为 00:16:b6:f7:1d:51，目的地址为主机发送请求的地址，BSSID 是 00:16:b6:f7:1d:51。

PROBE REQUEST 是由主机进行主动扫描以寻找接入点的一种请求。通过发送 PROBE REQUEST，主机可以广播其请求，以寻找周围可用的接入点。PROBE REQUEST 中的目的地址通常设置为广播地址 ff:ff:ff:ff:ff:ff，这样可以确保所有接入点都能收到请求。

PROBE RESPONSE 是由接入点发送给发送请求的主机的响应。当接入点接收到 PROBE REQUEST 后,它会根据请求的内容生成一个 PROBE RESPONSE,并将其发送回请求的主机。PROBE RESPONSE 中的源地址通常设置为接入点的 MAC 地址,以标识响应的来源。
通过这种方式,主机可以通过发送 PROBE REQUEST 并接收 PROBE RESPONSE 来发现附近的接入点,从而选择要连接的合适的接入点。

50	2.297613	IntelCor_1f:...	Broadcast	802.11	79	Probe Request, SN=576, FN=0, Flags=.....C,
51	2.300697	Cisco-Li_f7:...	IntelCor_1f:...	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C
52	2.302191	Cisco-Li_f7:...	IntelCor_1f:...	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C
53	2.304063	Cisco-Li_f7:...	IntelCor_1f:...	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C
54	2.305562	Cisco-Li_f7:...	IntelCor_1f:...	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C
55	2.308563	Cisco-Li_f7:...	IntelCor_1f:...	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C
56	2.310072	Cisco-Li_f7:...	IntelCor_1f:...	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C
57	2.338148	Cisco-Li_f7:...	Broadcast	802.11	183	Beacon frame, SN=2879, FN=0, Flags=.....C,
58	2.440572	Cisco-Li_f7:...	Broadcast	802.11	183	Beacon frame, SN=2880, FN=0, Flags=.....C,
59	2.453941	Cisco-Li_f7:...	IntelCor_1f:...	802.11	177	Probe Response, SN=2881, FN=0, Flags=.....C
60	2.542945	Cisco-Li_f7:...	Broadcast	802.11	183	Beacon frame, SN=2882, FN=0, Flags=.....C,
61	2.645319	Cisco-Li_f7:...	Broadcast	802.11	183	Beacon frame, SN=2883, FN=0, Flags=.....C,
62	2.747697	Cisco-Li_f7:...	Broadcast	802.11	183	Beacon frame, SN=2884, FN=0, Flags=.....C,
63	2.850114	Cisco-Li_f7:...	Broadcast	802.11	183	Beacon frame, SN=2885, FN=0, Flags=.....C,

> Frame 51: 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_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

0000
0010
0020
0030
0040
0050
0060
0070
0080
0090
00a0
00b0

结论分析与体会:

通过本次实验,对路由器和基站二者之间的区别有了进一步地认知,通过具体查看相关包,更好地理解 WIFI 工作过程,对 WIFI 相关知识的记忆更加清晰。