山东大学 计算机 学院

计算机网络 课程实验报告

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 AUTHENICATION 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 AUTHENICATION frames sent from the host to and 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 == 11and 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 associated 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:…	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:…	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

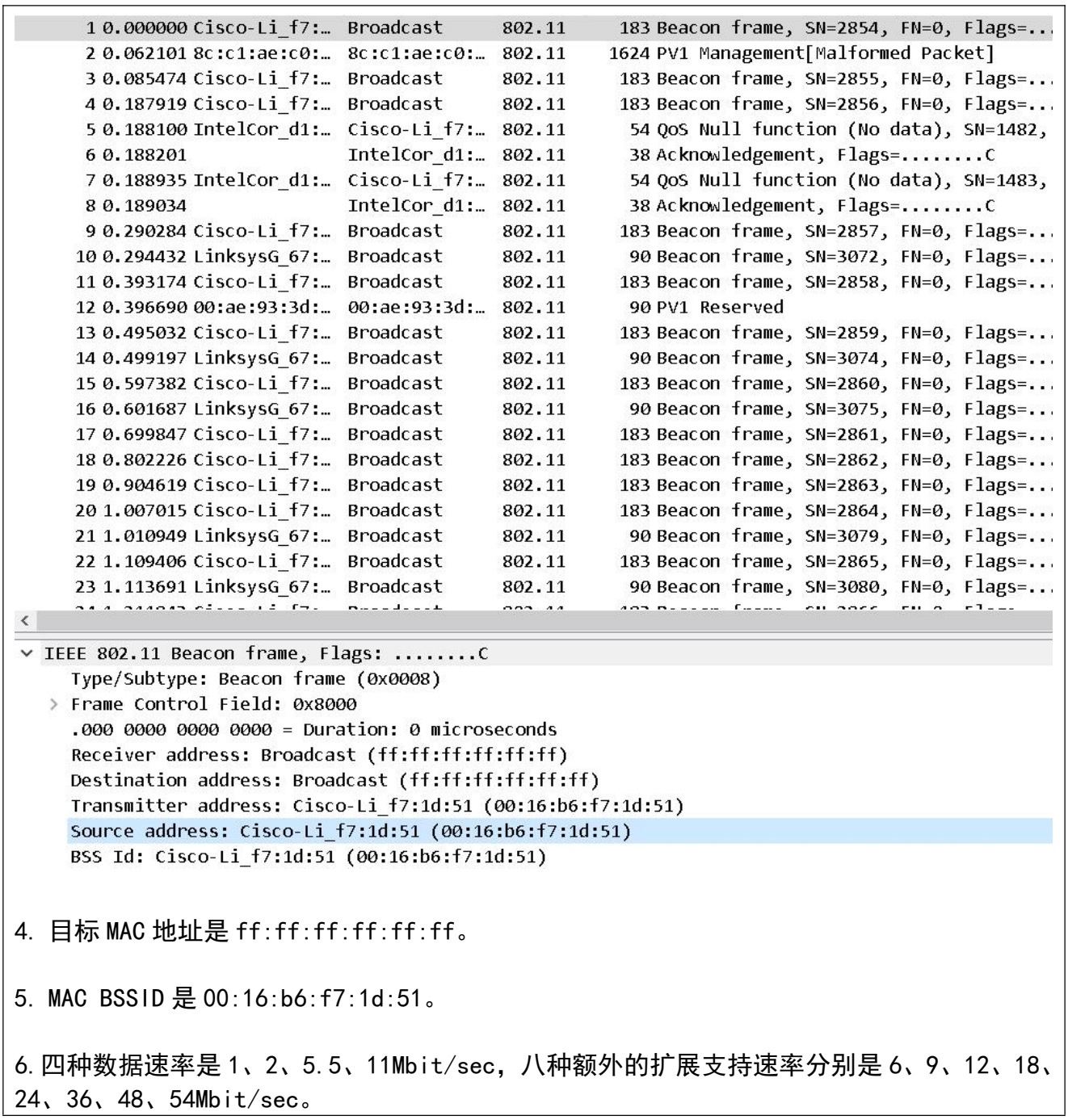
2. 时间间隔是 0.1024s，从 Beacon Interval 可知

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:…	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:…	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)
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  v Fixed parameters (12 bytes)
      Timestamp: 174319001986
      Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x0601
```

```
0000
0010
0020
0030
0040
0050
0060
0070
0080
0090
```

3. 源 MAC 地址是 00:16:b6:f7:1d:51。

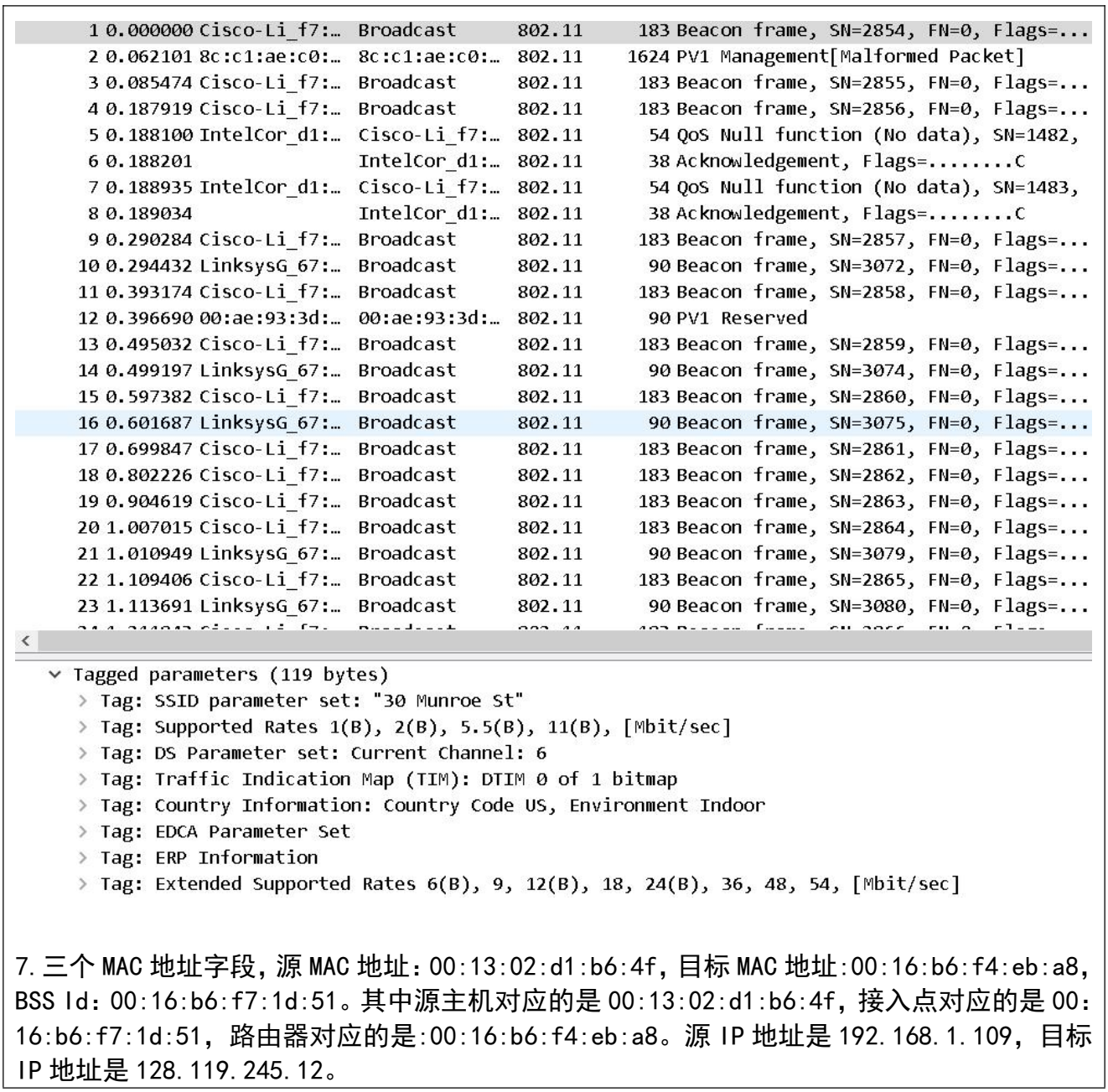


1	0.000000	Cisco-Li_f7:…	Broadcast	802.11	183	Beacon frame, SN=2854, FN=0, Flags=...
2	0.062101	8c:c1:ae:c0:…	8c:c1:ae:c0:…	802.11	1624	PV1 Management[Malformed Packet]
3	0.085474	Cisco-Li_f7:…	Broadcast	802.11	183	Beacon frame, SN=2855, FN=0, Flags=...
4	0.187919	Cisco-Li_f7:…	Broadcast	802.11	183	Beacon 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:…	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:…	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=...

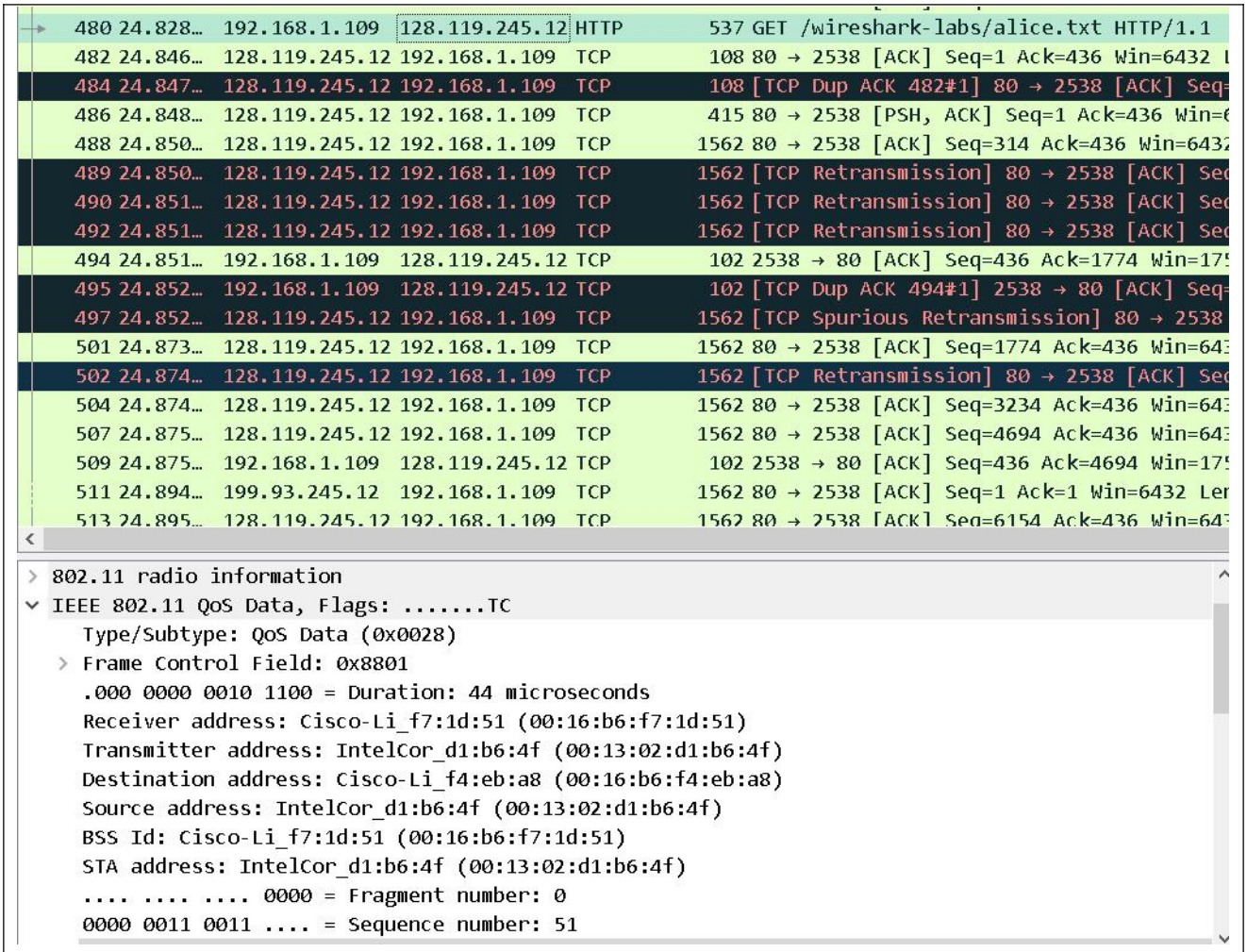
4. 目标 MAC 地址是 ff:ff:ff:ff:ff:ff。

5. MAC BSSID 是 00:16:b6:f7:1d:51。

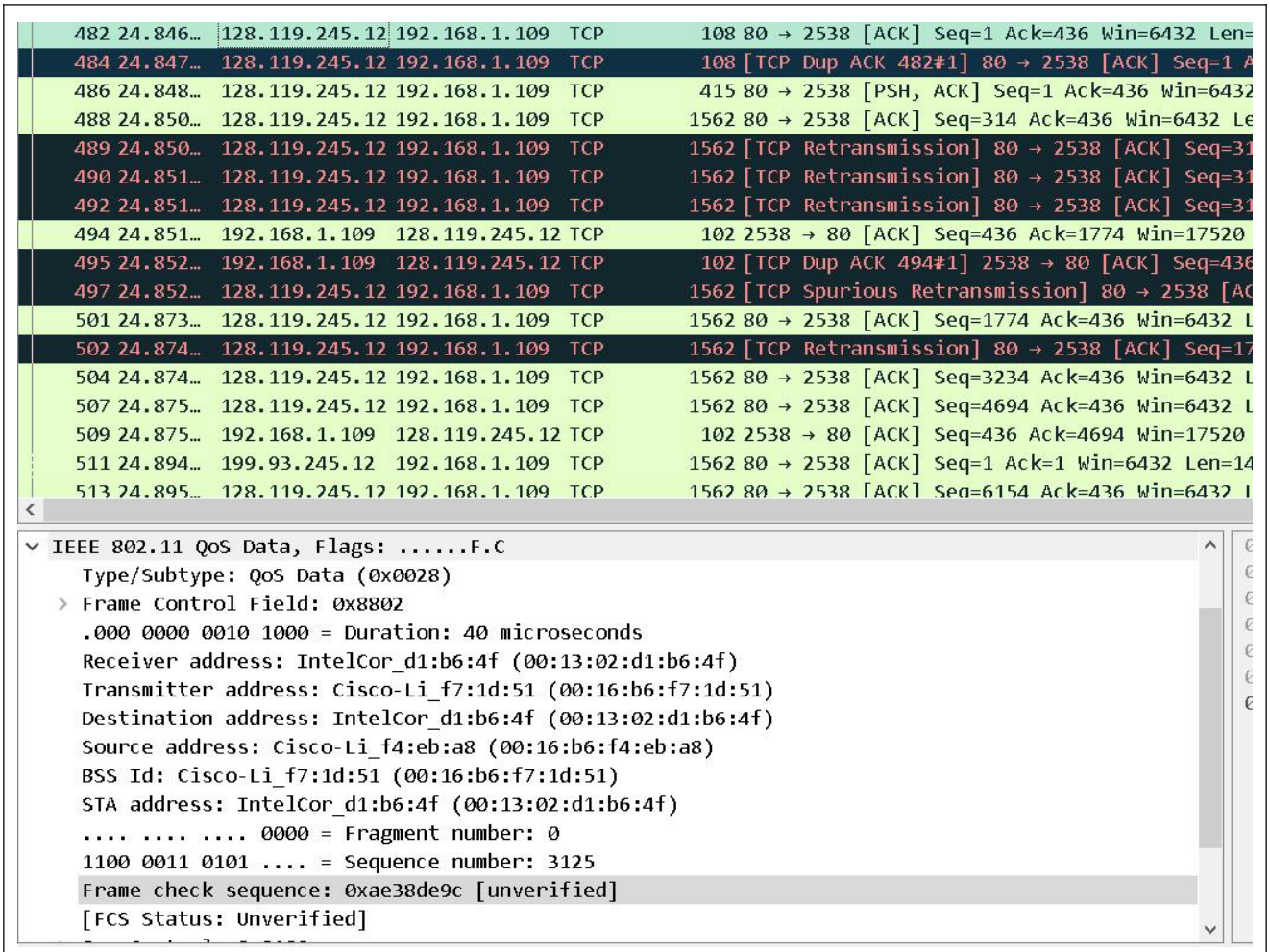
6. 四种数据速率是 1、2、5.5、11Mbit/sec，八种额外的扩展支持速率分别是 6、9、12、18、24、36、48、54Mbit/sec。



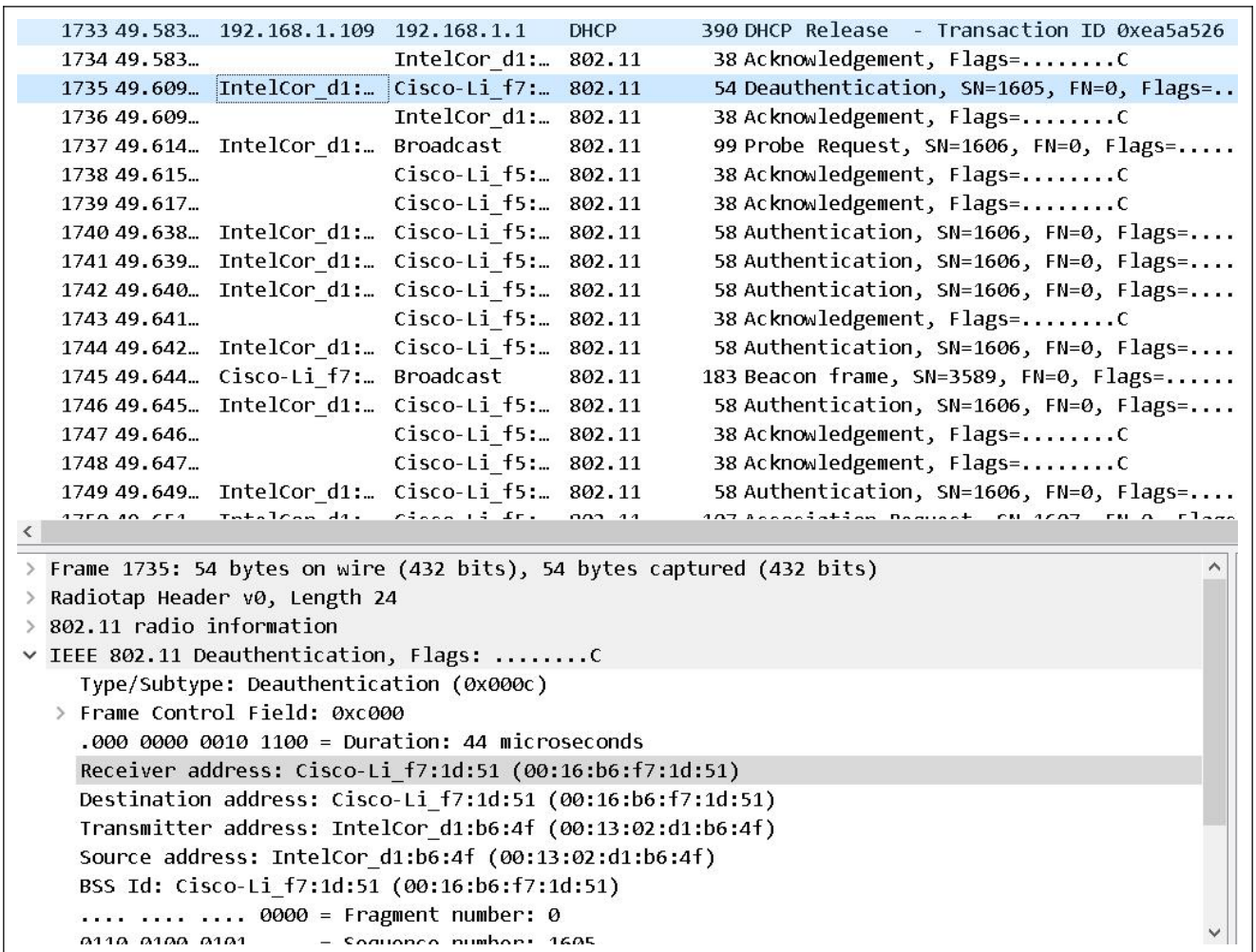
7. 三个 MAC 地址字段，源 MAC 地址：00:13:02:d1:b6:4f，目标 MAC 地址:00:16:b6:f4:eb:a8，BSS Id：00:16:b6:f7:1d:51。其中源主机对应的是 00:13:02:d1:b6:4f，接入点对应的是 00：16:b6:f7:1d:51，路由器对应的是:00:16:b6:f4:eb:a8。源 IP 地址是 192.168.1.109，目标 IP 地址是 128.119.245.12。



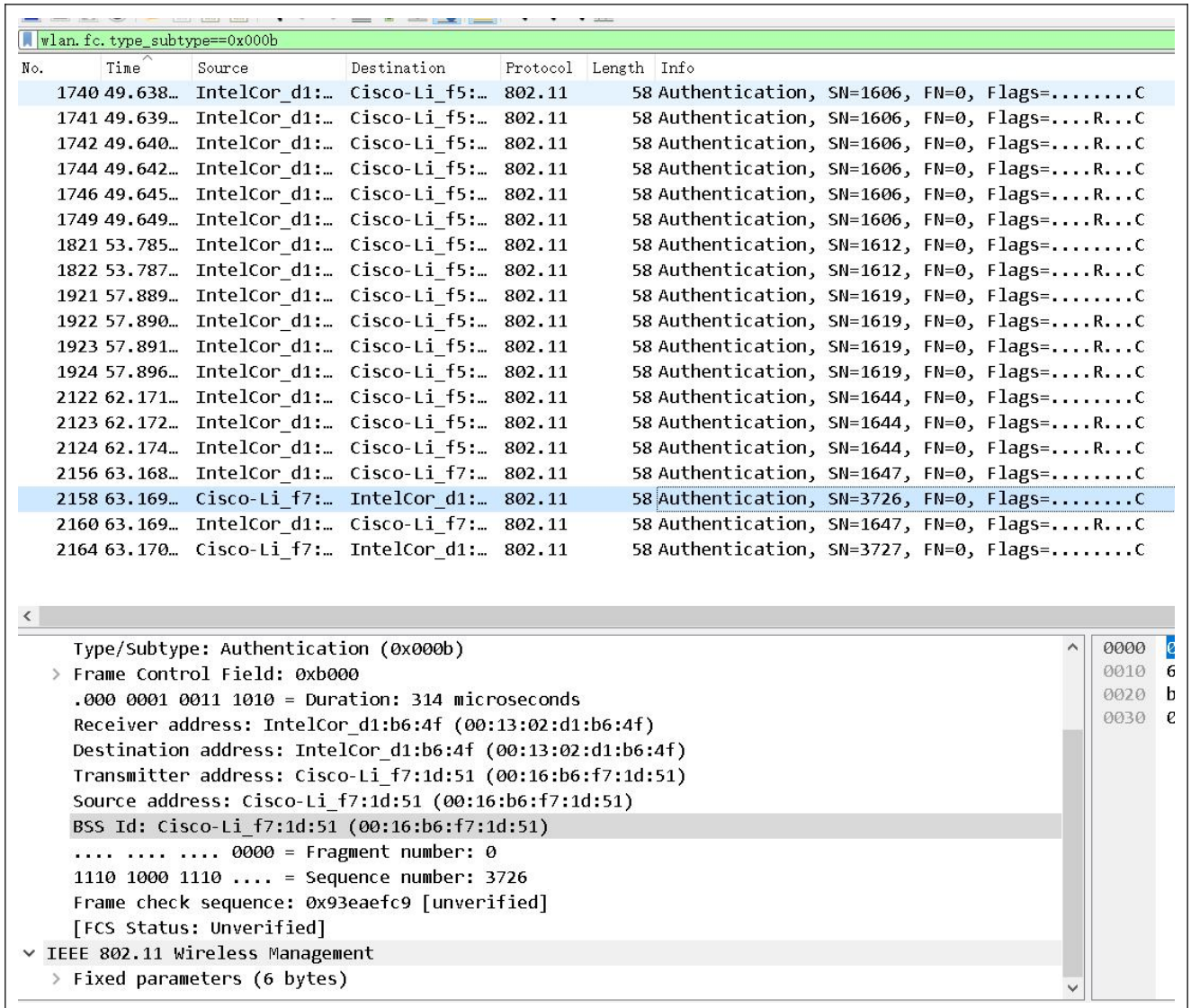
8. 三个 MAC 地址字段，源 MAC 地址：00:16:b6:f4:eb:a8，目标 MAC 地址：00:13:02:d1:b6:4f。BSS ID 是 00:16:b6:f7:1d:51。其中目标主机对应的是 00:13:02:d1:b6:4f，接入点对应的是 00:16:b6:f7:1d:51，路由器对应的是:00:16:b6:f4:eb:a8。源 IP 地址是 128.119.245.12，目标 IP 地址是 192.168.1.109。



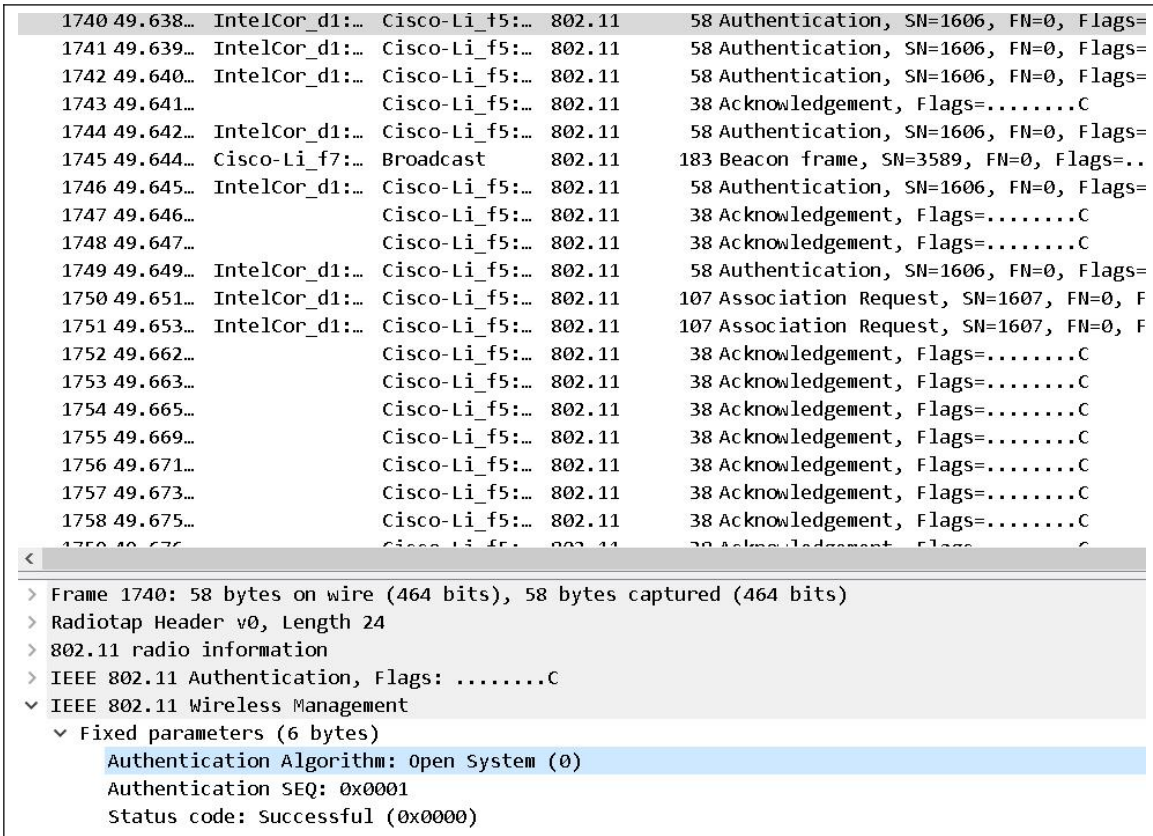
9. 在 t=49.583615s 时主机向即将离开的网络中的 DHCP 服务器(IP 地址为 192.168.1.1)发送 DHCP release，在 t=49.609617s 时主机发送一个 DEAUTHENTICATION 帧，Deauthentication 帧是一种 Wi-Fi 管理帧，用于在无线网络中注销客户端设备。



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。

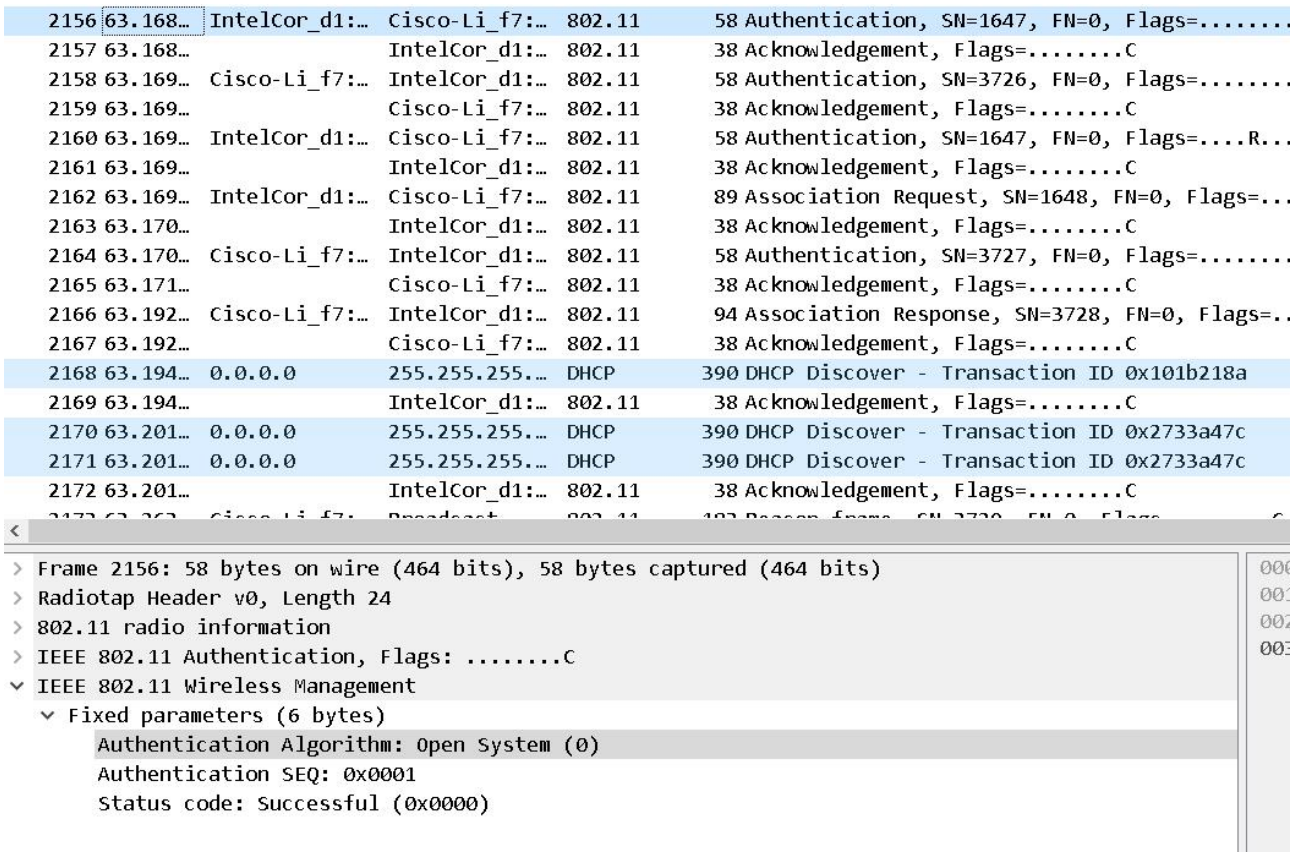


11. 希望打开，Open System 为 0 时，表示无线网络采用了开放系统的身份验证方式。意味着连接到该网络的设备无需提供密码或其他身份验证信息，即可与网络进行关联。任何设备都可以尝试连接到该网络，无需事先共享特定的密钥或密码，如下图所示：

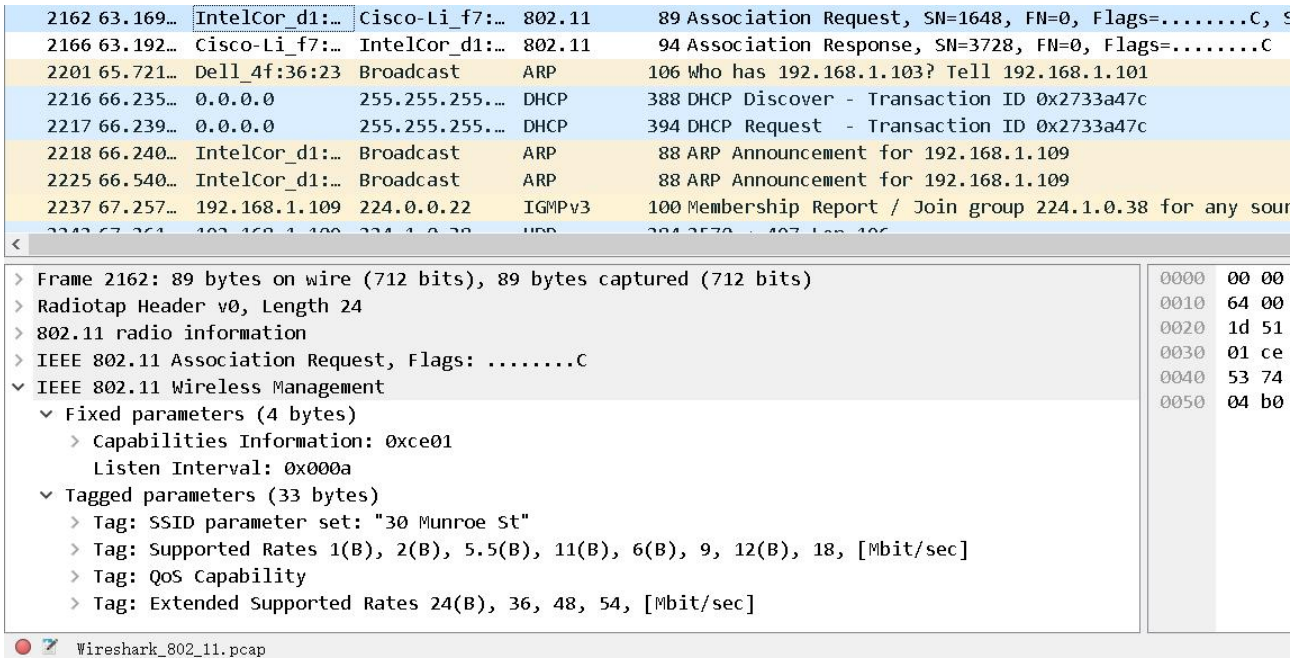


12. 没有看见，这可能是因为 AP 被配置为在与该 AP 关联时需要一个密钥，因此 AP 可能会忽略(即不响应)开放访问请求，这种情况表明该 AP 设置了需要进行身份验证或加密才能与其进行关联。当设备尝试以开放系统的方式进行关联时，AP 会忽略请求，并不会回复。

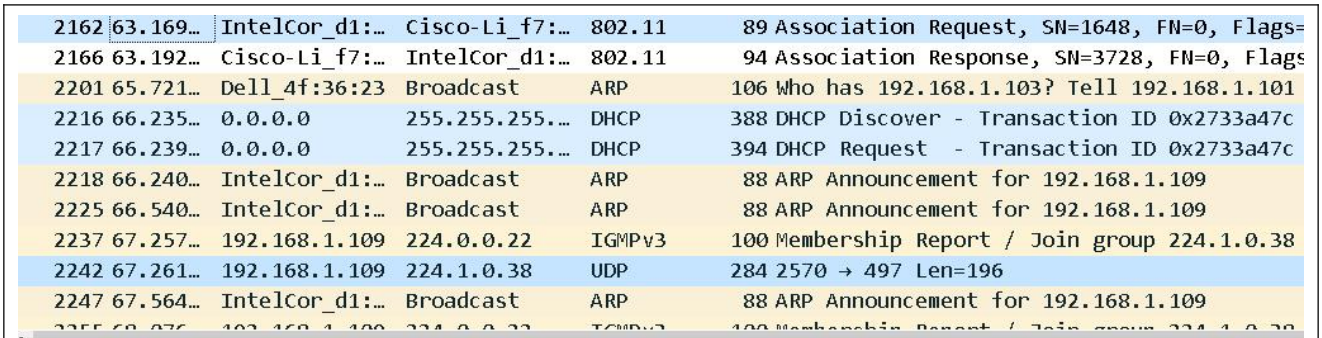
13. 在 t=63.168087s 时发送了身份认证帧，在 t=63.168087s 有一个认证帧从无线主机发出。在 t = 63.169071s，有一个从反向发送的 AUTHENTICATION 帧。

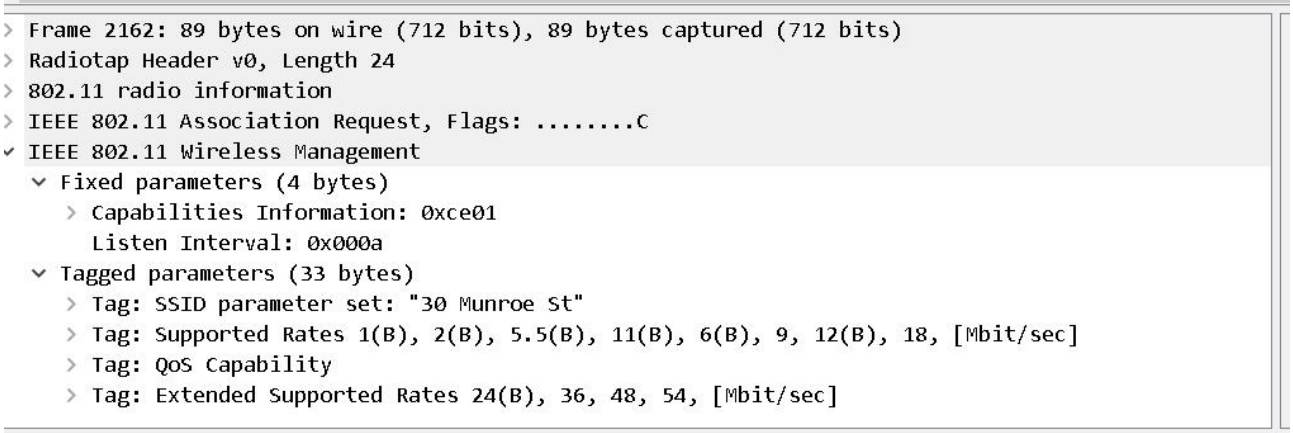


14. t=63.169910s 有一个关联请求帧无线主机从发送出，在 t=63.192101s 时有关联响应发出。

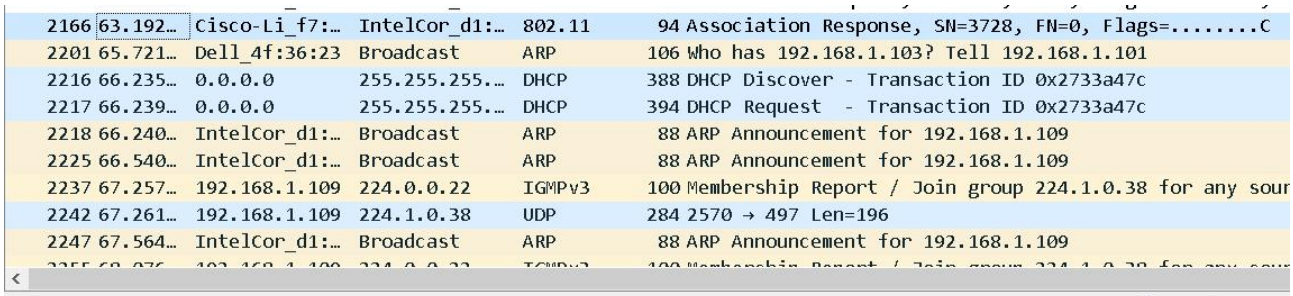


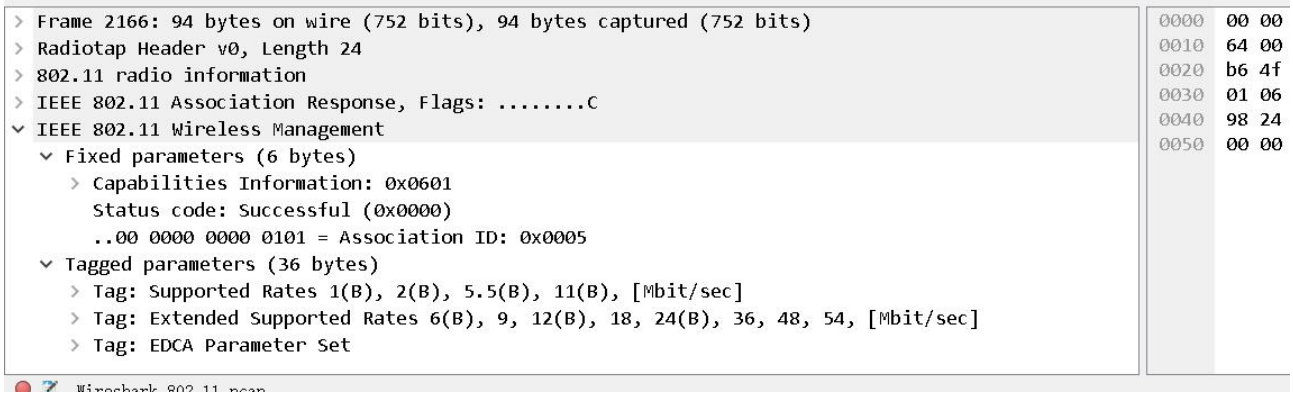
15. 主机传输速率：1、2、5.5、11、6、9、12、18、24、32、48and 54 Mbps





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



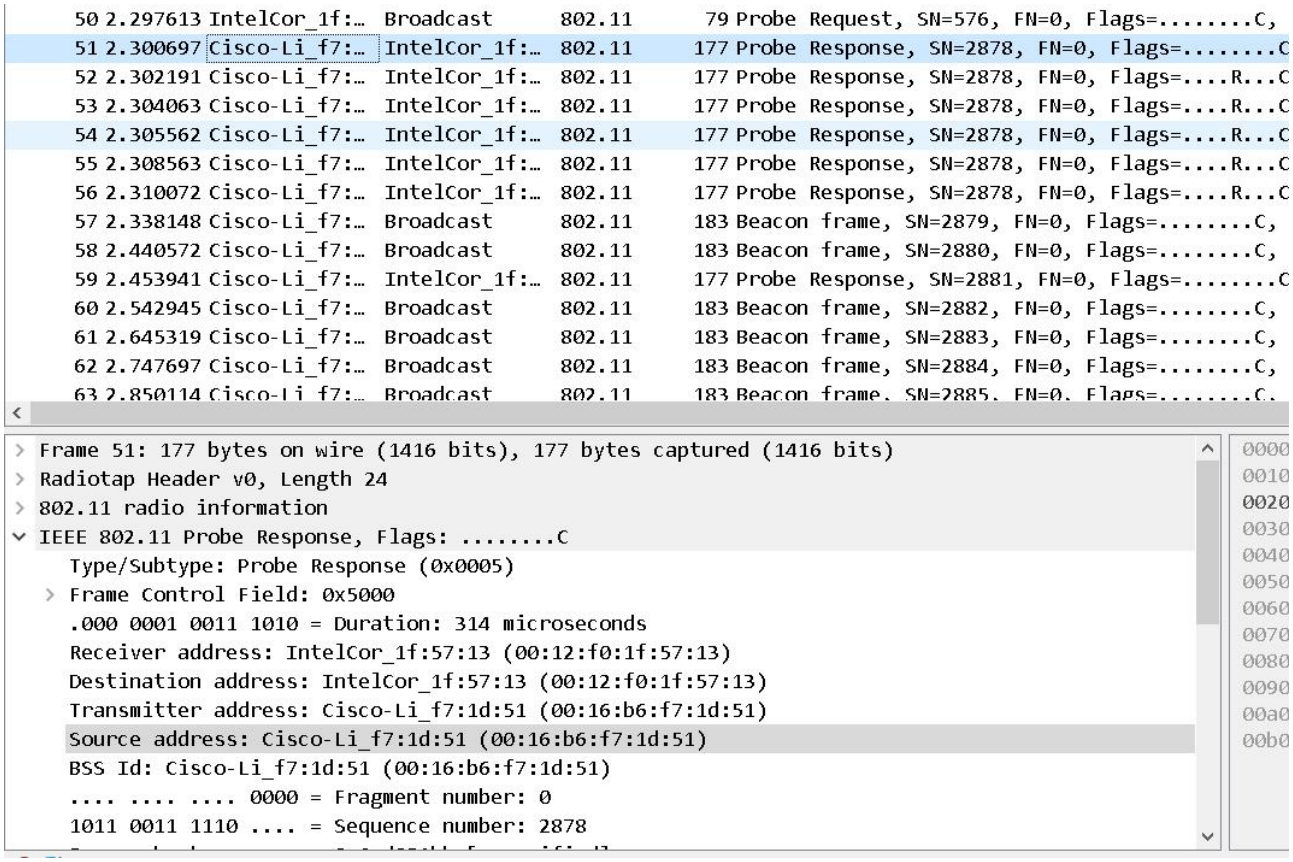


16. 根据描述，在时间 t=2.297613s，主机发送了一个 PROBE REQUEST（探测请求）。该请求的源地址为 00:12:f0:1f:57:13，目的地址为 ff:ff:ff:ff:ff:ff，BSSID 也为 ff:ff:ff:ff:ff:ff。在时间 t = 2.300697s，有一个 PROBE RESPONSE（探测响应）被发送出去。该响应的源地址为 00:16:b6:f7:1d:51，目的地址为主机发送请求的地址，BSSID 是 00:16:b6:f7:1d:51。

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。



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，更好地理解了 WIFI 工作过程，对 WIFI 相关知识的记忆更加清晰。