**电子科技大学**

**实**

**验**

**报**

**告**

学生姓名：李昊霖

学号：2019270102007

课程名称：计算机网络基础

指导教师：杨宁

日期： 2021 年 5 月 10 日

实验项目名称： 7-1 wireshark-802.11实验

报告评分： 教师签字：

**一、实验概要**

**实验目的:**

学习802.11协议，包括：信标帧，关联帧及其解除，响应帧，管理帧等内容，并通过分析报文进行实践。

**实验内容**：

查看 Pablo Brenner (Breezecom Communications)写的《802.11 协议技术指南》(A Technical Tutorial on the 802.11Protocol )(http://www.sss-mag.com/pdf/802\_11tut.pdf) 以及 Jim Geier 写的《了解 802.11 帧类型》 (http://www.wifiplanet.com/tutorials/article.php/1447501) 。查阅802.11 的圣经——它的标准书《ANSI / IEEE 标准 802.11,1999 版（R2003）》

使用作者捕获的 802.11 帧（抓包结果）进行分析并回答指导书上的相关问题。

**二、实验步骤、数据及分析结果**

**实验步骤:**

1. Getting Started

下载压缩包并且得到Wireshark\_802\_11.pcap。本结果由团队的一个作者在家庭网络使用 AirPcap 以及运行 Wireshark 的计算机得到，结果其中包括 Linksys 802.11g 的组合接入点（路由器），该接入点为两台有线 PC 和一台无线 PC 提供服务。

2. Beacon Frames

信标帧表示802.11 接入点存在。展开 IEEE 802.11 帧并在 Wireshark 中间窗口看到它的字段详细信息。回答问题1-6。

3. Data Transfer

作者抓包开始时，主机已经与 AP 关联，因此在做下面 AP 关联/解除关联之前，我们首先研究已经主机与关联 802.11 AP 的数据传输。回答问题7-8。

3. Association/Disassociation

802.11 中的关联使用 ASSOCIATE REQUEST 帧（从主机发送到 AP，帧类型 0 和子类型 0，参见本文中的第 7.3.3 节）和 ASSOCIATE RESPONSE 帧（由 AP 发送给具有主机，帧类型 0 和子类型 1，响应于接收到的 ASSOCIATE REQUEST）。回答问题9-15。

4. Other Frame types

作者的抓包结果中含许多 PROBE REQUEST 和 PROBE RESPONSE 帧。据此回答问题16。

**实验数据及分析:**

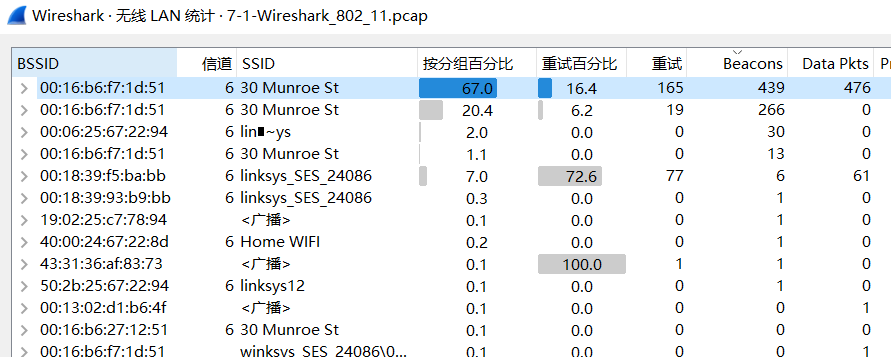
回答指导书问题**：**

问题1-6：

1. What are the SSIDs of the two access points that are issuing most of the beacon

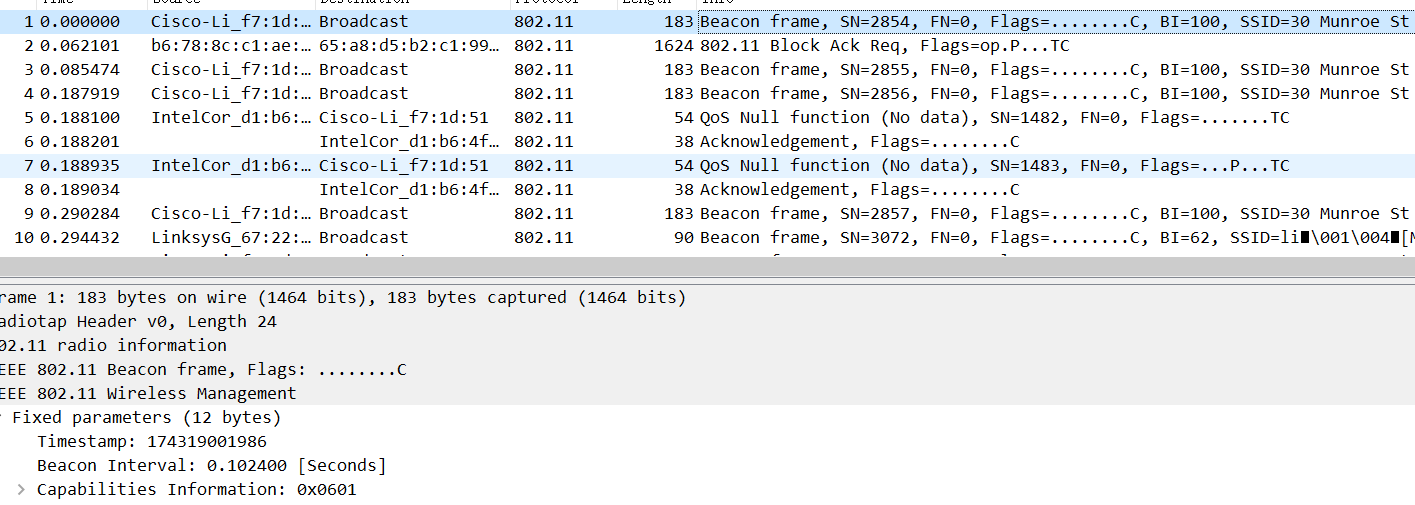
frames in this trace?

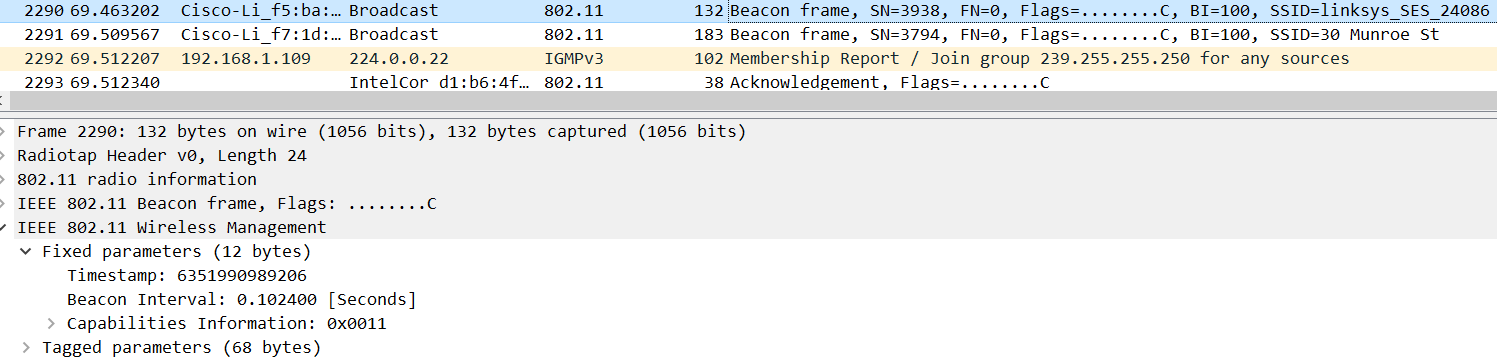
答:打开wireshark中的无线-wlan流量选项，并根据beacons排序可看到，最大的两个SSID为：30 Munroe St（前两个）和lin~ys（第三个）。



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).

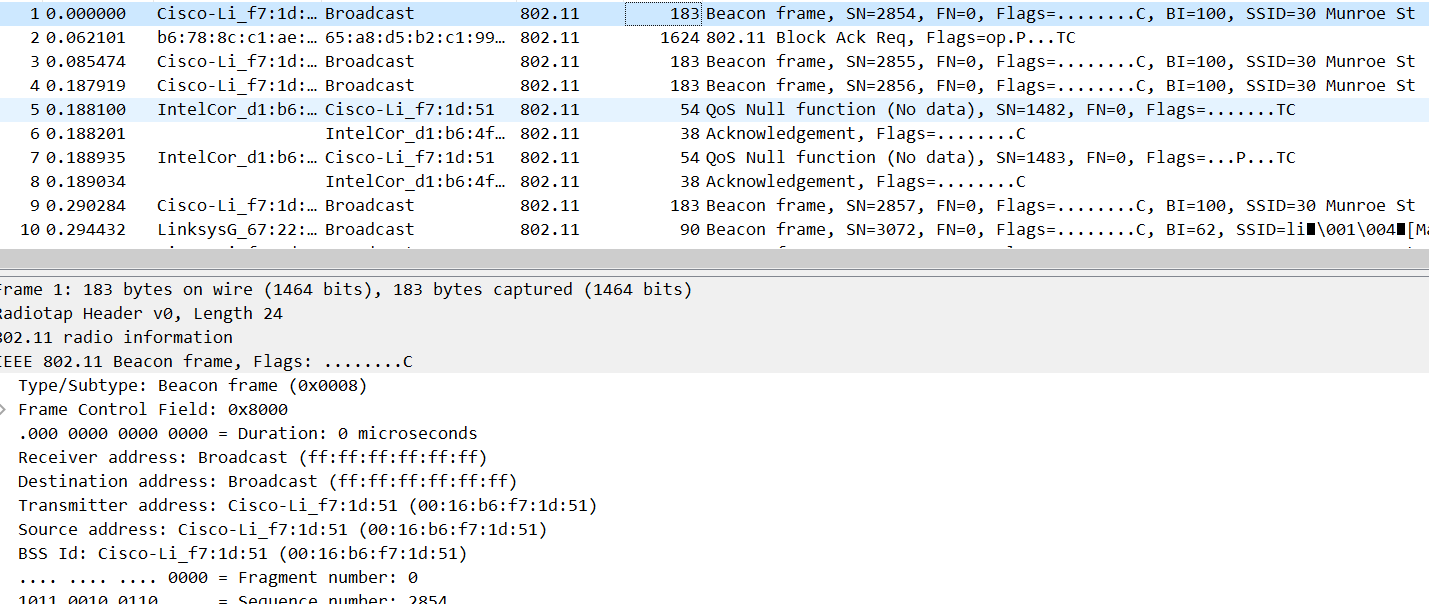
答：均为0.1024s。





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).

答：接收地址和目的地址均为广播地址 ff:ff:ff:ff:ff:ff；传输地址，源地址，BSS 地址均为路由地址 00:16:b6:f7:1d:51



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

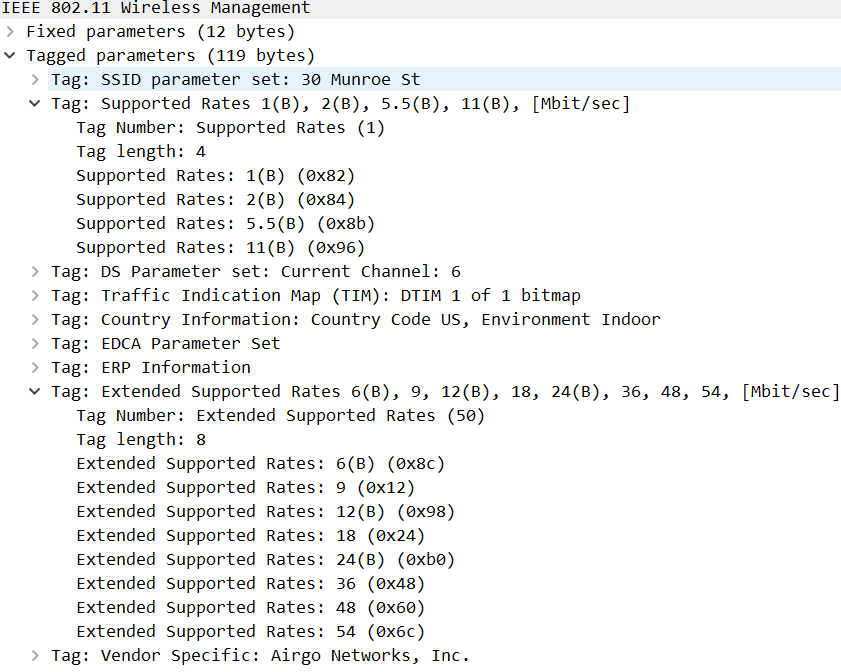
答：ff:ff:ff:ff:ff:ff

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

答：00:16:b6:f7:1d:51

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

答：如下图，四种数据速率：1B,2B,5.5B,11B; extended supported rates：6B,9,12B,18,24B,36,48,54.

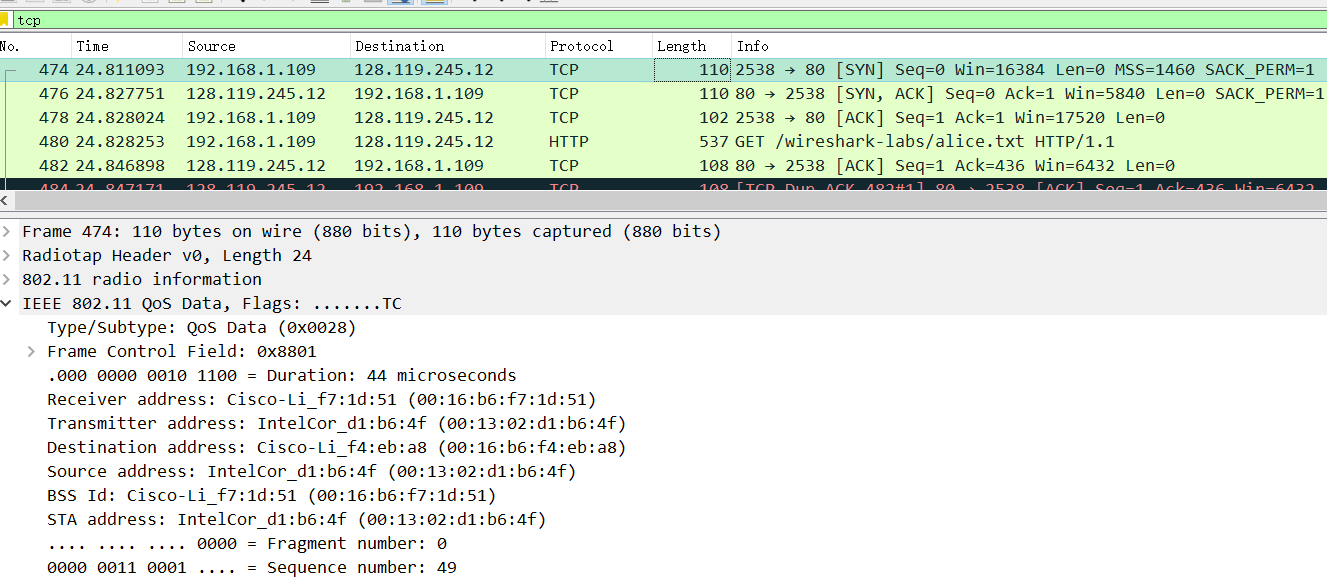


问题7-8：

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 802.11 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.

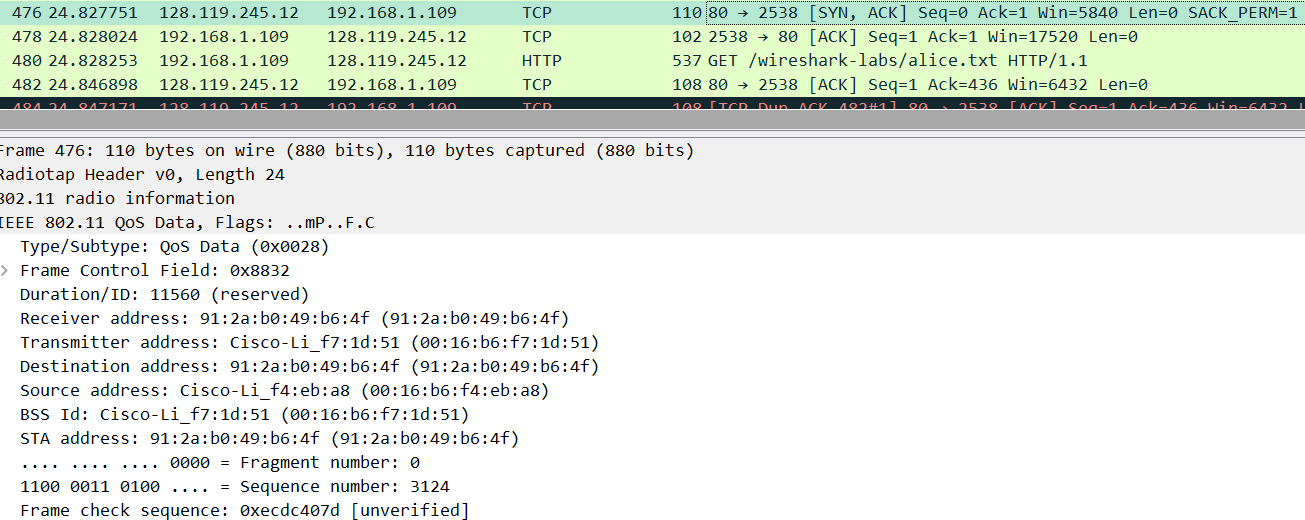
答：接收地址，目的地址，BSS 地址是无线路由器的地00:16:b6:f7:1d:51；源地址，传输地址，STA 地址是作者主机地址 00:13:02:d1:b6:4f。

主机IP地址192.168.1.109，目的IP地址128.119.245.12，第一跳路由器应为192.168.1.1。



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)

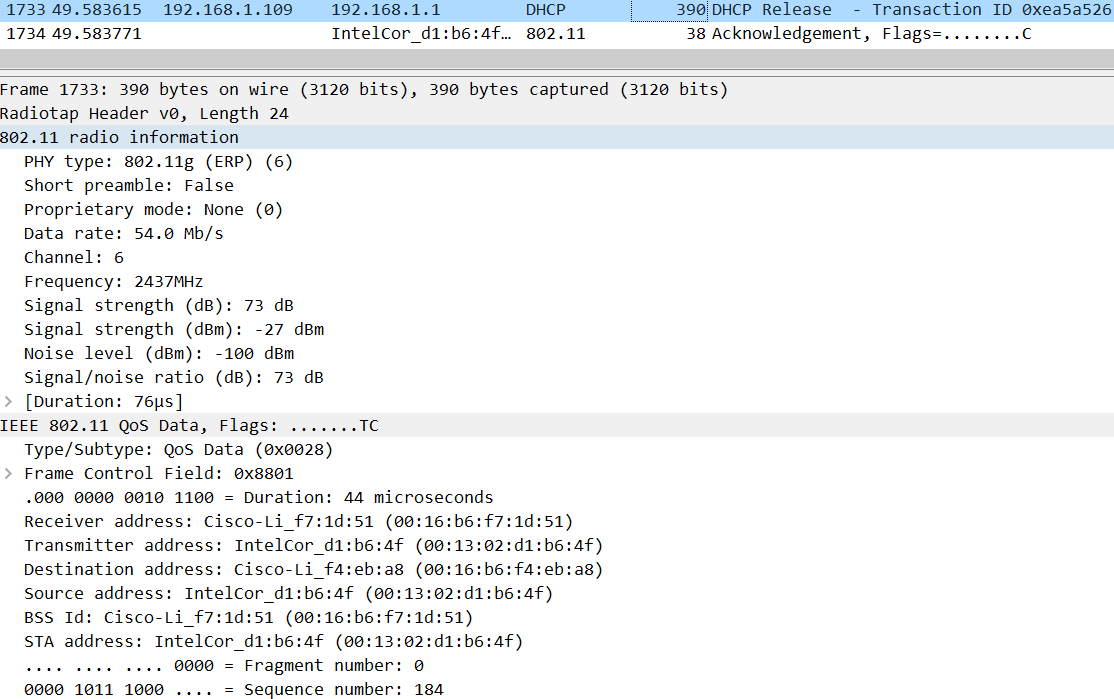
答：接收地址，传输地址，目的地址；传输地址；接收地址；

不对应，发送方 MAC 地址是00:16:b6:f7:1d:51，发送此 TCP 报文的设备的 IP 地址对应00:16:b6:f4:eb:a8(源地址)

问题9-16：

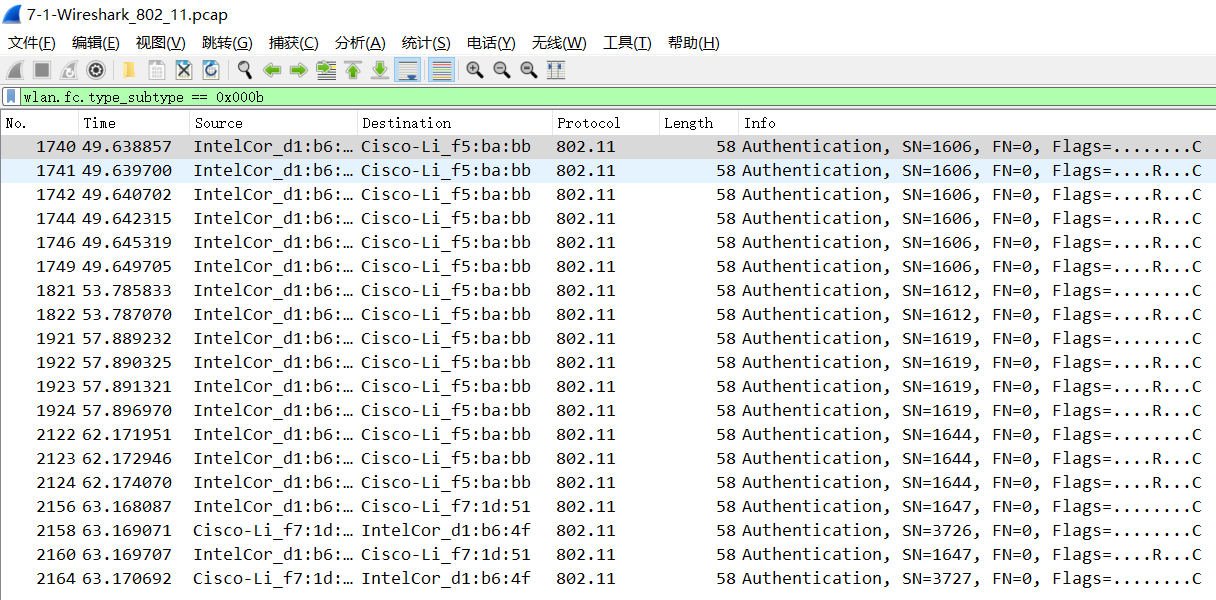
9. What two actions are taken (i.e., frames are sent) by the host in the trace just after t=49, to end the association with the 30 Munroe St AP that was initially in place when trace collection began? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification,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

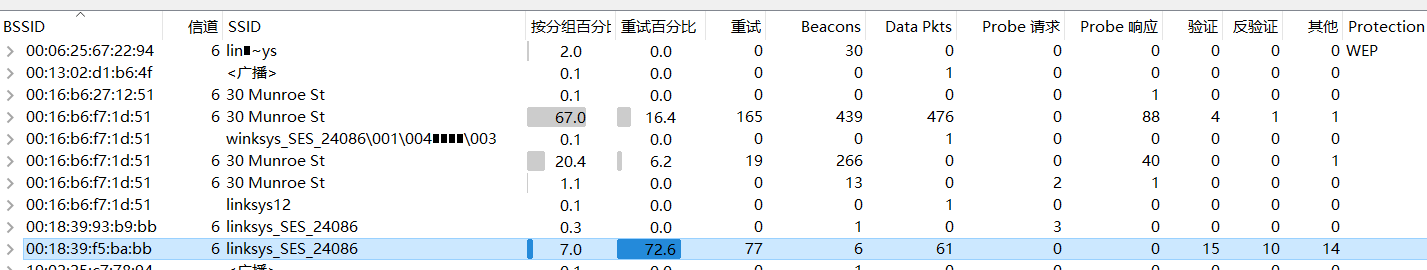
答：发送DHCP报文解除关联帧。



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

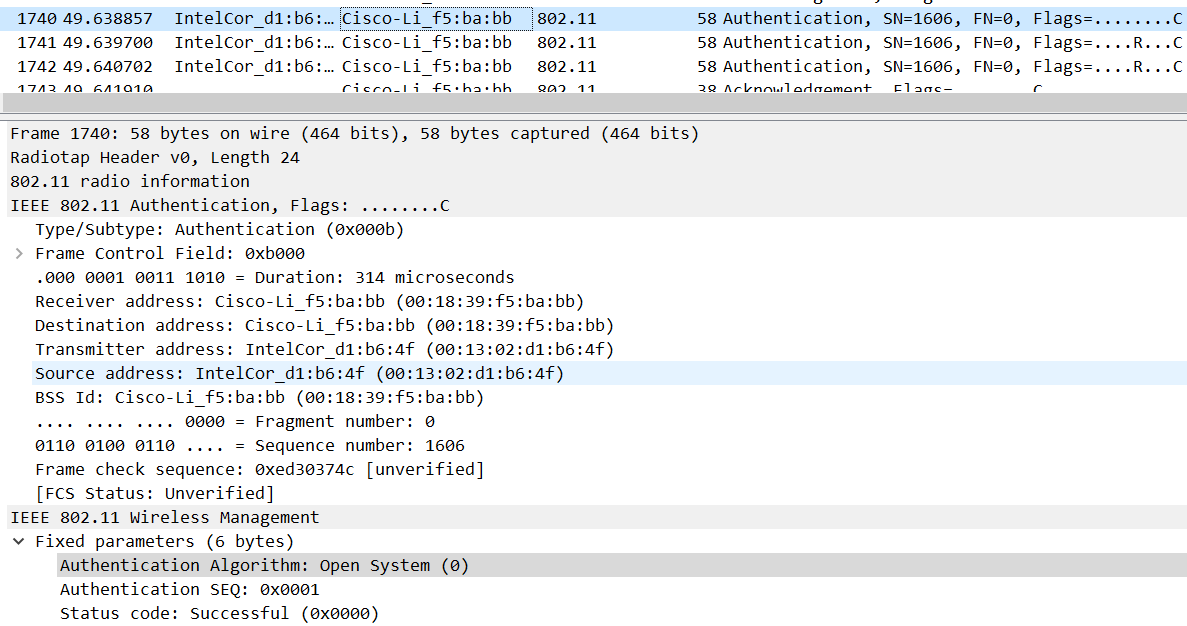
答：AUTHENICATION及回复帧如下图，AUTHENTICATION 消息共15条。





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

答：是。

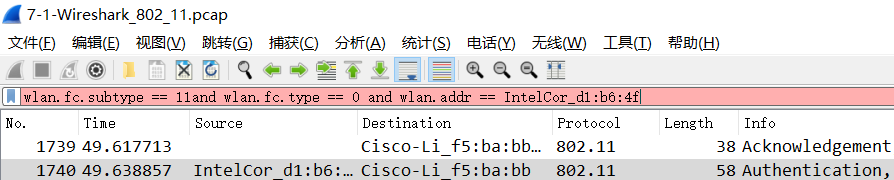


12. Do you see a reply AUTHENTICATION from the linksys\_ses\_24086 AP in the trace?

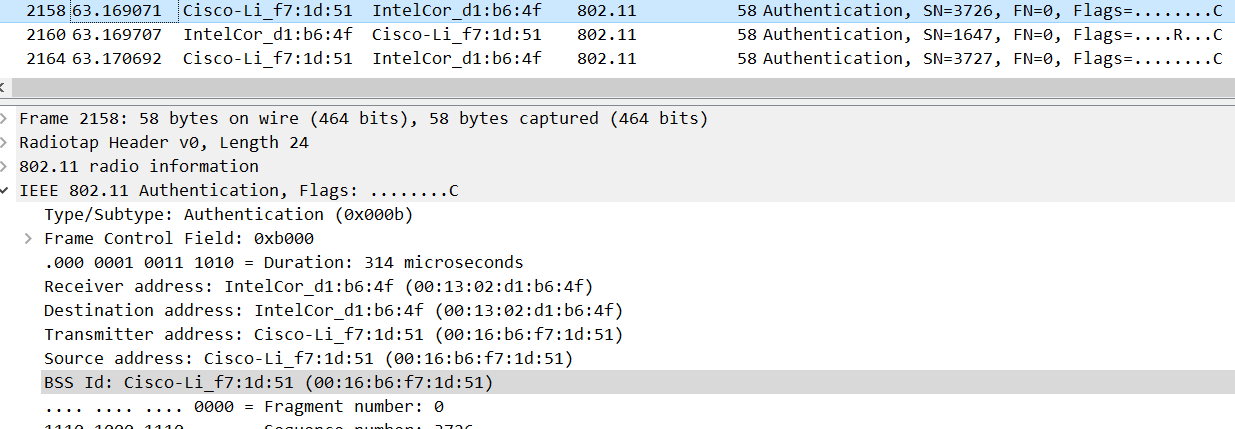
答：无。linksys\_ses\_24086 AP未回复AUTHENTICATION。

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.)

答：题目中给的过滤条件无法使用，如图

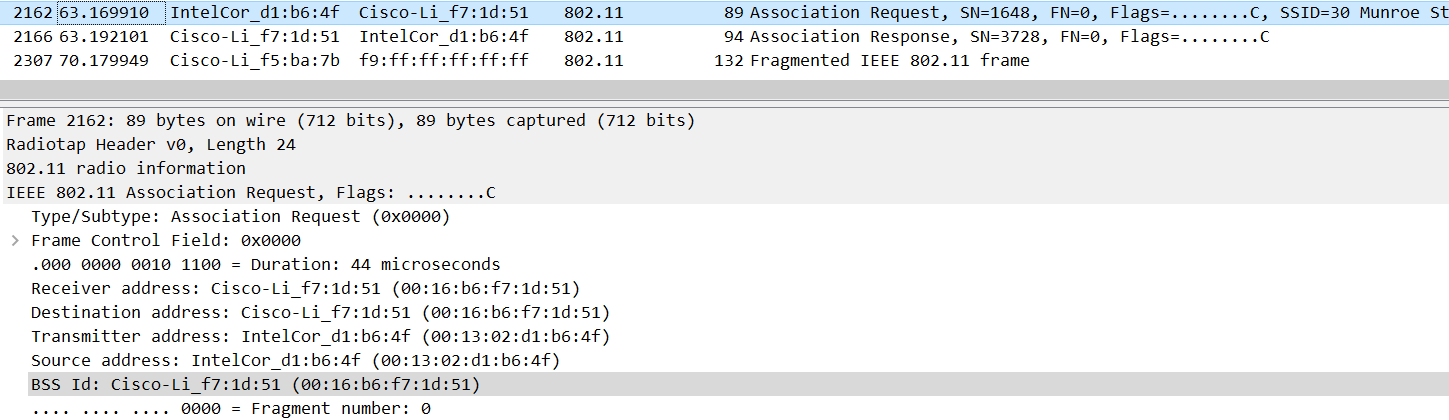


修改过滤条件后，发送时间63.169071s，响应时间 63.170692s。



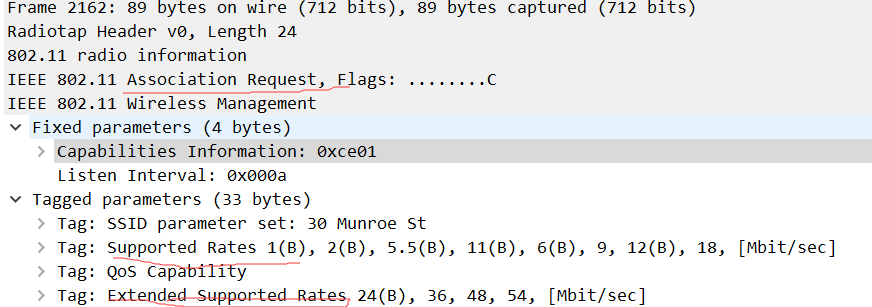
14. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associated with an AP. At what time is there an ASSOCIATE REQUEST from host to the 30 Munroe St AP? When is the corresponding ASSOCIATE REPLY sent? (Note that you can use the 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.)

答：ASSOCIATE REQUEST 时间63.169910s，响应63.192101s。

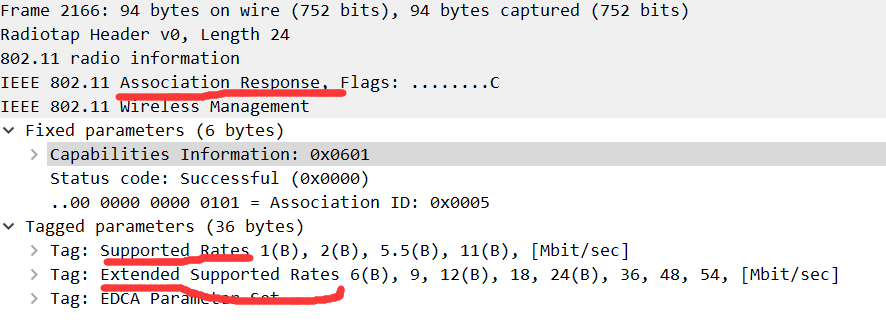


15. What transmission rates is the host willing to use? The AP? To answer this question, you will need to look into the parameters fields of the 802.11 wireless LAN management frame.

答：关联请求帧有 8 种支持速率，4 种扩展速率。



关联请求响应帧有 4 种支持速率，8 种扩展速率。



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).

答：请求帧的接收地址，目的地址，BSS 地址均为广播地址ff:ff:ff:ff:ff:ff，源地址和传输地址为主机网卡的mac，在实验文件中为00:12:f0:1f:57:13。

响应帧的源地址，传输地址，BSS 地址为00:16:b6:f7:1d:51，目的地址和接收地址为发送请求的mac地址，本文件中为00:12:f0:1f:57:13 。

**三、总结及心得体会**

本次实验学习了802.11协议内容，并深入了解各种数据帧的报文内容。

**四、对本实验过程及方法、手段的改进建议**

可以提供学生自己抓包802.11帧的方法，分析自己抓获的报文。