

学号：202400130240	姓名：贾宗翰	班级：24.6
实验题目：Wireshark Lab:802.11 WiFi v8.1		
实验学时：2h	实验日期：2025.11.18	
实验目的：研究 802.11 无线网络协议		
硬件环境： 联想拯救者		
软件环境： Wireshark; edge 浏览器		
实验步骤与内容： 在本实验中，我们将研究 802.11 无线网络协议。在开始本实验之前，您可能需要重新阅读正文 1 中的第 7.3 节。由于我们将深入研究 802.11，而不是正文中的内容，因此您可能需要查看巴勃罗布伦纳（Breezecom Communications）撰写的“关于 802.11 协议的技术说明”， http://www.sss-mag.com/pdf/802_11tut.pdf 。当然，这里有 802.11 的“圣经”——4,379 页的标准本身，“ANSI/IEEE Std 802.11-2020”。但是我们从规范中提取了 www.example.com 部分 9.2.4.1，并在这里添加了一个方便的 802.11 Wireshark 显示过滤器的备忘单，这两个对本实验非常有用。在本实验中，我们将从计算机/笔记本电脑上的无线 802.11 WiFi 接口捕获跟踪。假设您已经连接到 WiFi 网络（我们将其称为您的家庭网络），以下是跟踪收集开始时采取的操作：1. 向 www.example.com 发出 HTTP 请求 http://gaia.cs.umass.edu/wireshark-labs/alice.txt 2. 向 www.example.com 发出请求 http://www.cs.umass.edu 3. 断开与家庭网络的连接 4.（可选步骤）尝试连接到另一个 802.11 无线网络，该网络正在接收信标通告，而您无权访问该网络，因此您的连接尝试将失败。5. 再次（成功）连接到家庭网络 要回答下面的一些问题，您需要查看 Wireshark 显示屏最右侧列中的“信息”字段中的详细信息；要回答其他问题，您需要深入了解 Wireshark 中间窗口中的“802.11 协议”帧和子字段。		
		
1. 在此跟踪中发出大多数信标帧的两个接入点的 SSID 是什么？[提示：查看信息字段。要仅显示信标帧，请在 Wireshark 显示过滤器中输入 <code>wlan.fc.type_subtype == 8</code>]。		

```
SSID="30 Munroe St"  
SSID="30 Munroe St"  
SSID="30 Munroe St"  
SSID="30 Munroe St"
```

2. 这两个接入点正在使用哪个 802.11 信道[提示: 您需要深入了解 802.11 信标帧中的无线电信息]

```
Tag: DS Parameter set: Current Channel: 6
```

现在让我们看看在 t=0.085474 发送的信标帧。

```
3 0.085474 CiscoLinksys_f7:
```

3. 从这个接入点 (AP) 发送信标帧之间的时间间隔是多少? (提示: 此时间间隔包含在信标帧本身的字段中)。

```
Beacon Interval: 0.102400 [Seconds]  
Capabilities Information: 0x0601
```

4. 来自此接入点的信标帧上的源 MAC 地址是什么 (十六进制表示法)? 在图 7.13 中, 源地址、目的地址和 BSS 是 802.11 帧中使用的三个地址。为了详细讨论 802.11 帧结构, 参见 IEEE 802.11 标准文档中的第 9.2.3– 9.2.4.1 节, 此处摘录。

```
Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
```

5. 什么是来自 30 Munroe St 的信标帧上的目的 MAC 地址?

```
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
```

6. 什么 (十六进制表示法) 是来自 30 Munroe St 的信标帧上的 MAC BSS ID?

```
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
```

7. 来自 30 Munroe St 接入点的信标帧通告该接入点可以支持四种数据速率和八种附加的“扩展支持速率”。这些速率是什么? [注意: 这是在一个相当古老的 AP 上拍摄的痕迹]。

```
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]
```

3. 数据传输由于跟踪是从已经与 AP 关联的主机开始的, 因此在查看 AP 关联/解除关联之前, 让我们先看看通过 802.11 关联的数据传输。回想一下, 在此跟踪中, 在 t = 24.82 时, 主机向 <http://gaia.cs.umass.edu/wireshark-labs/alice.txt> 发出 HTTP 请求。gaia.cs.umass.edu 的 IP 地址为 128.119.245.12。然后, 在 t=32.82 时, 主机向 <http://www.cs.umass.edu> 发出 HTTP 请求。

8. 查找包含第一个 TCP 会话的 SYN TCP 段的 802.11 帧(下载 [alice.txt](#) 的)在 t=24.8110。802.11 帧中有哪三个 MAC 地址字段? 此帧中的哪一个 MAC 地址对应于无线主机(给出主机 MAC 地址的十六进制表示)? 到 AP? 到第一跳路由器? 发送此 TCP 数据段的无线主机的 IP 地址是什么? TCP SYN 段的目的 IP 地址是什么?

```
Destination address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)  
Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)  
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
```

有这三个 mac 地址字段，其中 source 对应主机，destination 对应第一跳路由器，BSS Id 对应 AP。

```
Source Address: 192.168.1.109
Destination Address: 128.119.245.12
```

发送此 TCP 数据段的无线主机的 IP 地址对应 source，destination 对应目标 ip。

9. 此 TCP SYN 的目的 IP 地址是对应于主机、接入点、第一跳路由器还是目的 Web 服务器？目的 web 服务器。

10. 查找包含在 t=24.8277 接收的此 TCP 会话的 SYNACK 段的 802.11 帧，802.11 帧中有哪三个 MAC 地址字段？此帧中的哪个 MAC 地址对应于主机？接入点？第一跳路由器？帧中的发送方 MAC 地址是否对应于发送此数据报中封装的 TCP 数据段的设备的 IP 地址？（提示：如果你不确定如何回答这个问题，或者上一个问题的相应部分，请回顾课文中的图 6.19。理解这一点特别重要）。

先定位：

```
476 24.827751 128.119.245.12 192.168.1.109
```

Mac 字段：

```
► Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
► Source address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
► BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
```

主机：destination，第一跳路由器：source，接入点：BSS id。

回想一下正文中的第 7.3.1 节，主机在发送数据之前必须首先与接入点关联。（从主机发送到 AP，帧类型为 0，子类型为 0，参见本文中的第 7.3.3 节）和 ASSOCIATE RESPONSE 帧（由 AP 发送到具有帧类型 0 和子类型 1 的主机，以响应接收到的关联请求）。并且在执行关联之前，主机和 AP 必须就当主机与 AP 关联时将使用的认证的形式达成一致；该协议是使用认证帧完成的。回想一下，我们的跟踪从已经与接入点关联的主机开始。大约 t=49，主机与接入点断开关联，等待一段时间，然后再次重新认证并与接入点重新关联。

11. 主机在 t=49 之后采取了哪两个动作（即发送帧），以结束与 30 Munroe St AP 的关联（该关联在跟踪收集开始时最初处于适当位置）？（提示：一个是 IP 层动作，一个是 802.11 层动作）。

```
1733 49.583615 192.168.1.109 192.168.1.1 DHCP 390 DHCP Release - Transaction ID 0xea5a526
1734 49.583771 192.168.1.109 Intel_d1:b6:4f 802.11 38 Acknowledgement, Flags=.....C
1735 49.609617 Intel_d1:b6:4f CiscoLinksys_f7:1d:51 802.11 54 Deauthentication, SN=1605, FN=0, Flags=.....C
```

在 IP 层，发送 DHCP 释放消息；

在 802.11，层取消身份验证帧传输。

现在让我们看看认证和与接入点关联的过程。我们将查看在图 4 所示的时间捕获的四个特定帧。

12. 让我们先看看验证帧。在 t = 63.1680 时，我们的主机尝试与 30 Munroe St AP 关联。使用 Wireshark 显示过滤器 wlan.fc.subtype == 11 显示从主机发送到 AP 的验证帧，反之亦然。主机请求的验证形式是什么？

IEEE 802.11 Wireless Management

▼ Fixed parameters (6 bytes)

Authentication Algorithm: Open System (0)

Authentication SEQ: 0x0001

Status code: Successful (0x0000)

13. 什么是身份验证 SEQ 值（认证序列号）从主机到 AP？

见上，是 0x0001

14. 在 $t = 63.1690$ 接收 AP 对认证请求的响应。AP 是否接受了主机请求的认证形式？

IEEE 802.11 Wireless Management

▼ Fixed parameters (6 bytes)

Authentication Algorithm: Open System (0)

Authentication SEQ: 0x0002

Status code: Successful (0x0000)

从 status code 可见成功接收。

15. 从 AP 到主机的此认证帧的认证 SEQ 值是什么？

见上，0x0002.

现在让我们看看在 $t = 63.1699$ 发送的 ASSOCIATION REQUEST 和在 $t = 66.1921$ 接收的 ASSOCIATION RESPONSE。0 显示关联请求和响应帧。

16. 帧中指示的费率为“已排序费率”。请不要在下面的答案中包括任何指示为扩展支持速率。

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

17. 关联响应是否指示成功或不成功的关联响应？

怀疑题目打错了，应该是 63.1921:

2166 63.192101

然后回答问题:

Status code: Successful (0x0000)

所以确实指示了。

18. 主机提供的最快（最大）扩展支持速率是否与 AP 能够提供的最快（最大）扩展支持速率匹配？

主机:

Tag: QoS Capability

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

AP:

Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

最大都是 54，可以匹配。

结论分析与体会：

通过此次实验，我对于 802.11 协议的认知进一步加深，对于 AP, BSSid 的关系的理解也更进一步。