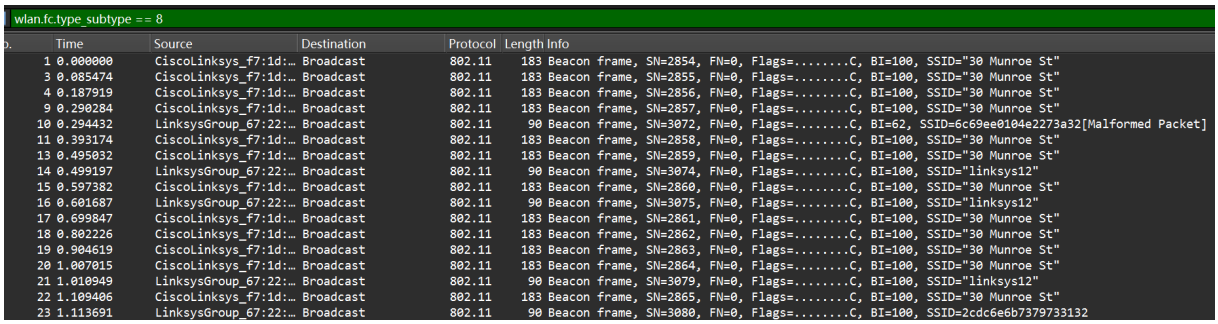
计算机学院 计算机网络 课程实验报告

实验题目： 802.11(WLAN)		学号：202200400053
日期：2024-05-31	班级： 2 班	姓名： 王宇涵
Email：1941497679@qq.com		

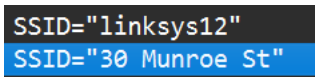
实验方法介绍：

使用 wireShark 进行抓包并分析，理解了 802.11 的工作原理，巩固了理论课知识.

实验过程描述：

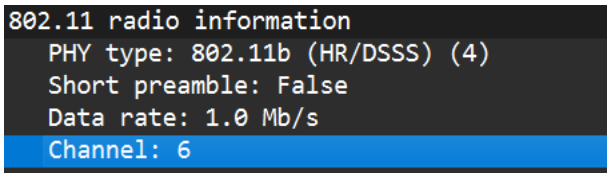


1. **在这个跟踪文件中，发出大多数信标帧的两个接入点的 SSID 是什么？【提示：查看 Info 字段。要仅显示信标帧，在 Wireshark 显示过滤器中输入`wlan.fc.type_subtype == 8`】。**



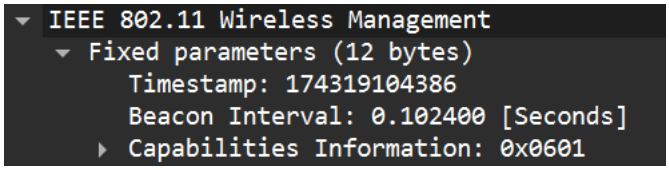
答：“30 Munroe St” 和 “linksys12”

2. **这两个接入点使用的 802.11 信道是什么？【提示：你需要深入查看 802.11 信标帧中的无线电信息】。**



答：6

3. **该接入点（AP）发送信标帧的时间间隔是多少？（提示：这个时间间隔包含在信标帧的一个字段中）。**



答：0.102400

4. **该接入点信标帧的源 MAC 地址是什么（十六进制表示）？请回想图 7.13 中的内容，源地址、目的地址和 BSS 是 802.11 帧中使用的三个地址。有关 802.11 帧结构的详细讨论，请参见 IEEE 802.11 标准文档第 9.2.3-9.2.4.1 节，这里有摘录。**

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

答：00:16:b6:f7:1d:51

5. 30 Munroe St 的信标帧的目的 MAC 地址是什么（十六进制表示）？

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

答：ff:ff:ff:ff:ff:ff

6. 30 Munroe St 的信标帧的 MAC BSS ID 是什么（十六进制表示）？

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

答：00:16:b6:f7:1d:51

7. 30 Munroe St 接入点的信标帧广告显示该接入点可以支持四个数据速率和八个附加的“扩展支持速率”。这些速率是什么？【注意：这些跟踪是在一个相当旧的 AP 上获取的】。

```
▸ 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]
```

答：1(B)，2(B)，5.5(B)，11(B);
6(B)，9(B)，12(B)，18(B)，24(B)，36(B)，48(B)，54(B)

```
474 24.811093   192.168.1.109   128.119.245.12   TCP   110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
```

8. 找到第一个 TCP 会话（下载 alice.txt）的 SYN TCP 段的 802.11 帧，时间为 t=24.8110。802.11 帧中的三个 MAC 地址字段是什么？这个帧中的哪个 MAC 地址对应无线主机(给出主机的 MAC 地址的十六进制表示）？哪个对应接入点？哪个对应第一跳路由器？发送这个 TCP 段的无线主机的 IP 地址是什么？TCP SYN 段的目标 IP 地址是什么？

```
Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
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)
STA address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
```

答：三个 MAC 地址字段：00:16:b6:f7:1d:51, 00:13:02:d1:b6:4f, 00:16:b6:f4:eb:a8;
对应无线主机：00:13:02:d1:b6:4f; 对应接入点：00:16:b6:f7:1d:51; 对应第一跳路由器：00:16:b6:f4:eb:a8
发送 TCP 段的无线主机 IP: 192.168.1.109 目标 IP: 128.119.245.12

9. 这个 TCP SYN 的目标 IP 地址对应主机、接入点、第一跳路由器还是目标 Web 服务器？

答：第一跳路由器

10. 找到在 t=24.8277 收到的这个 TCP 会话的 SYNACK 段的 802.11 帧。802.11 帧中的三个 MAC 地址字段是什么？这个帧中的哪个 MAC 地址对应主机？哪个对应接入点？哪个对应第一跳路由器？帧中的发送者 MAC 地址是否对应发送这个 TCP 段的设备的 IP 地址？（提示：如果你不确定如何回答这个问题，请查看课本中的图 6.19 或前一个问题的相应部分。理解这一点特别重要）。

```
Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
Transmitter address: CiscoLinksys_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: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
```

答：三个 MAC 地址字段 :91:2a:b0:49:b6:4f ; 00:16:b6:f7:1d:51; 00:16:b6:f4:eb:a8

对应无线主机：91:2a:b0:49:b6:4f; 对应接入点 ：00:16:b6:f7:1d:51; 对应第一跳路由器：00:16:b6:f4:eb:a8

帧中的发送者 MAC 地址对应发送这个 TCP 段的设备的 IP 地址.

11. 主机在大约 t=49 之后采取了哪两个动作（即发送了哪些帧）来结束与最初在捕获开始时已建立的 30 Munroe St AP 的关联？（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                   Intel_d1:b6:4f (00:… 802.11     38 Acknowledgement, Flags=........C
1735 49.609617   Intel_d1:b6:4f  CiscoLinksys_f7:1d:… 802.11     54 Deauthentication, SN=1605, FN=0, Flags=........C
```

答：IP 层 : DHCP Release; 802.11 层 : Deauthentication

12. 首先让我们看一下 AUTHENTICATION 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`显示从主机到 AP 及其反向发送的 AUTHENTICATION 帧。主机请求的认证形式是什么？

```
Authentication Algorithm: Open System (0)
```

答：Open System, 开放系统

13. 从主机到 AP 的这个认证帧的 Authentication SEQ 值（认证序列号）是什么？

```
Authentication SEQ: 0x0001
```

答：0x0001

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

```
Status code: Successful (0x0000)
```

答：接受

15. 从 AP 到主机的这个认证帧的 Authentication SEQ 值是什么？

```
Authentication SEQ: 0x0002
```

答：0x0002

16. 帧中所指示的 SUPPORTED RATES 中包含哪些速率？请在下面的答案中不包括任何被指示为 EXTENDED SUPPORTED RATES 的速率。

```
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
   Tag Number: Supported Rates (1)
   Tag length: 8
   Supported Rates: 1(B) (0x82)
   Supported Rates: 2(B) (0x84)
   Supported Rates: 5.5(B) (0x8b)
   Supported Rates: 11(B) (0x96)
   Supported Rates: 6(B) (0x8c)
   Supported Rates: 9 (0x12)
   Supported Rates: 12(B) (0x98)
   Supported Rates: 18 (0x24)
```

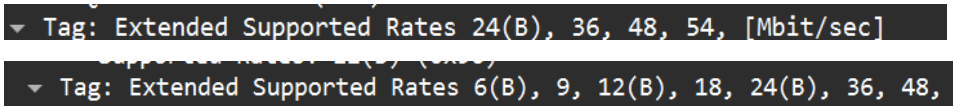
答：1(B)，2(B)，5.5(B)，11(B)，6(B)，9(B)，12(B)，18(B).

17. ASSOCIATION RESPONSE 指示了成功的关联响应还是失败的关联响应？

```
Status code: Successful (0x0000)
```

答：成功的关联响应

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）扩展支持速率相匹配？



答：匹配

分析：

802.11 是一种无线局域网（WLAN）技术，其工作原理涉及无线信号的传输和接收。

通过 802.11 协议，设备可以在无线网络中进行通信，其中包括接入点（AP）和终端设备（如笔记本电脑、智能手机等）。

在这个跟踪文件中，我们分析了一些 802.11 帧，以了解网络中的活动。我们发现了两个主要的接入点，它们分别使用“30 Munroe St”和“linksys12”作为 SSID，并且它们都在信道 6 上运行。

从跟踪文件中的信标帧间隔字段，我们了解到接入点发送信标帧的间隔为 0.102400 秒。

此外，我们还分析了一些 TCP 会话的 802.11 帧，了解了与主机、接入点和第一跳路由器相关的 MAC 地址，以及发送和目标 IP 地址。

通过分析认证帧，我们确定了主机请求的认证形式和 AP 的响应，以及支持的速率。

总的来说，通过分析 802.11 帧，我们可以更深入地了解无线网络中的活动和通信过程。

结论：

通过分析 802.11 跟踪文件，我学到了如何使用 Wireshark 来查看和分析无线网络。

我学会了使用 Wireshark 的过滤器来筛选出特定类型的帧，例如信标帧和认证帧，以便更轻松地分析网络活动。

通过观察不同帧的详细信息，我了解了 802.11 协议中各种字段的含义，例如 SSID、MAC 地址和认证状态码等。

我还学会了识别关键事件，如关联和认证过程，以及如何解释这些事件中涉及的帧的含义。

通过这次实验，我对无线网络的工作原理有了更深入的了解，并且提高了使用网络分析工具的技能。