中国科学技术大学计算机学院

《计算机网络实验报告》

实验题目：802.11 Trace Analysis

学生姓名：郑振东

学生学号：PB18111703

完成日期：2021 年 1 月 29 日

计算机实验教学中心制

2019 年 09 月

【QUESTIONS && ANSWERS】

- What are the SSIDs of the two APs that are issuing most of the beacon frames in this trace?

“30 Munroe St”和“linksys12”

打开 WireShark 的 WLAN Traffic 可以看出发送 beacon frame 最多的应该是“30 Munroe St”和一个疑是乱码的 SSID“lin■~ys”（图 1.1 所示）。

BSSID	信道	SSID	按分组百分比	重试百分比	重试	Beacons
00:16:b6:f7:1d:51	6	30 Munroe St	67.0	16.4	165	439
00:16:b6:f7:1d:51	6	30 Munroe St	20.4	6.2	19	266
00:06:25:67:22:94	6	lin■~ys	2.0	0.0	0	30
00:16:b6:f7:1d:51	6	30 Munroe St	1.1	0.0	0	13
00:18:39:f5:ba:bb	6	linksys_SES_24086	7.0	72.6	77	6
00:18:39:93:b9:bb	6	linksys_SES_24086	0.3	0.0	0	1
19:02:25:c7:78:94		<广播>	0.1	0.0	0	1
40:00:24:67:22:8d	6	Home WIFI	0.2	0.0	0	1
43:31:36:af:83:73		<广播>	0.1	100.0	1	1
50:2b:25:67:22:94	6	linksys12	0.1	0.0	0	1
00:13:02:d1:b6:4f		<广播>	0.1	0.0	0	0
00:16:b6:27:12:51	6	30 Munroe St	0.1	0.0	0	0
00:16:b6:f7:1d:51		winksys_SES_24086\001\004■■■■\003	0.1	0.0	0	0
00:16:b6:f7:1d:51		linksys12	0.1	0.0	0	0
2a:67:0c:e8:07:89		<广播>	0.1	0.0	0	0

图 1.1

将这个疑是乱码 SSID 的 BSSID 选作过滤器应用之后，可以发现过滤出的大多数包的 SSID 是“linksys12”（图 1.2 && 图 1.3 所示）。

（根据图 1.3 所示的内容，我发现还有几个新的 SSID 疑是“linksys12”的乱码，并且有很多包的 SSID 明明就是”linksys12”，但是为什么 WireShark 的 WLAN Traffic 界面显示出的结果却与此有较大偏差？我不是很懂，只好先把它们都当作“linksys12”发出来的帧。就算不用 WLAN Traffic 观察，直接翻看所有的包，也很容易看出“linksys12”发出的 beacon frame 包是第二多的）

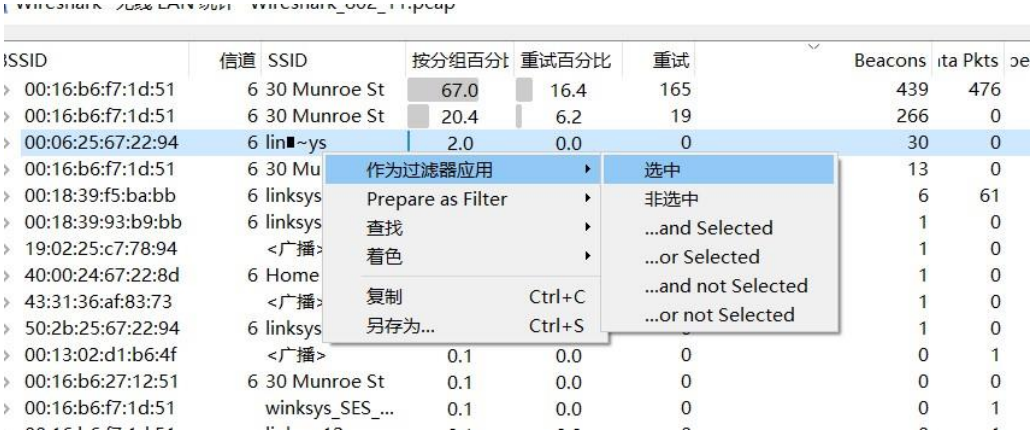
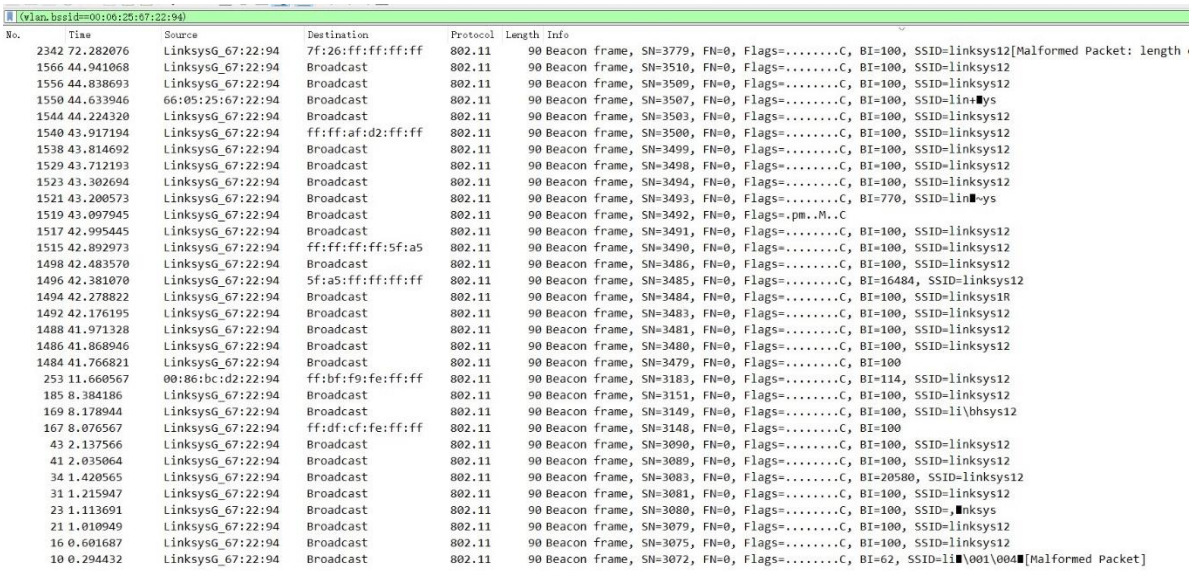


图 1.2



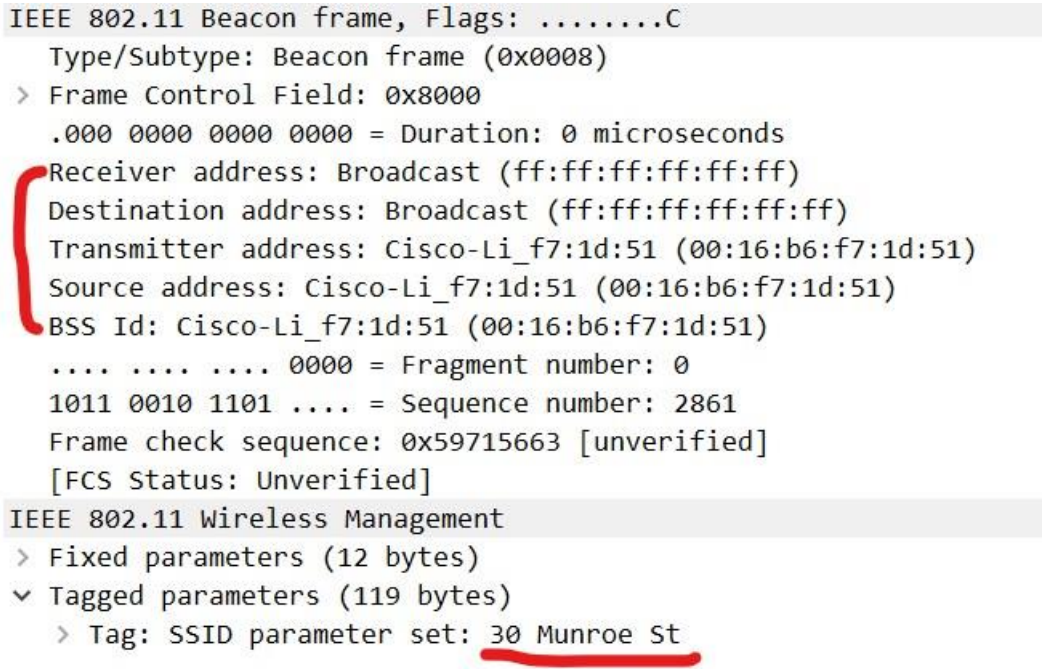
(wlan.bssid==00:06:25:67:22:94)

No.	Time	Source	Destination	Protocol	Length	Info
2342	72.282076	LinksysG_67:22:94	7f:26:ff:ff:ff:ff	802.11	90	Beacon frame, SN=3779, FN=0, Flags=........C, BI=100, SSID=linksys12[Malformed Packet: length
1566	44.941068	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3510, FN=0, Flags=........C, BI=100, SSID=linksys12
1556	44.838693	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3509, FN=0, Flags=........C, BI=100, SSID=linksys12
1550	44.633946	66:05:25:67:22:94	Broadcast	802.11	90	Beacon frame, SN=3507, FN=0, Flags=........C, BI=100, SSID=lin+▮ys
1544	44.224320	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3503, FN=0, Flags=........C, BI=100, SSID=linksys12
1540	43.917194	LinksysG_67:22:94	ff:ff:af:d2:ff:ff	802.11	90	Beacon frame, SN=3500, FN=0, Flags=........C, BI=100, SSID=linksys12
1538	43.814692	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3499, FN=0, Flags=........C, BI=100, SSID=linksys12
1529	43.712193	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3498, FN=0, Flags=........C, BI=100, SSID=linksys12
1523	43.302694	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3494, FN=0, Flags=........C, BI=100, SSID=linksys12
1521	43.200573	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3493, FN=0, Flags=........C, BI=770, SSID=lin▮~ys
1519	43.097945	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3492, FN=0, Flags=.pm..M..C
1517	42.995445	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3491, FN=0, Flags=........C, BI=100, SSID=linksys12
1515	42.892973	LinksysG_67:22:94	ff:ff:ff:ff:5f:a5	802.11	90	Beacon frame, SN=3490, FN=0, Flags=........C, BI=100, SSID=linksys12
1498	42.483570	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3486, FN=0, Flags=........C, BI=100, SSID=linksys12
1496	42.381070	LinksysG_67:22:94	5f:a5:ff:ff:ff:ff	802.11	90	Beacon frame, SN=3485, FN=0, Flags=........C, BI=16484, SSID=linksys12
1494	42.278822	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3484, FN=0, Flags=........C, BI=100, SSID=linksys1R
1492	42.176195	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3483, FN=0, Flags=........C, BI=100, SSID=linksys12
1488	41.971328	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3481, FN=0, Flags=........C, BI=100, SSID=linksys12
1486	41.868946	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3480, FN=0, Flags=........C, BI=100, SSID=linksys12
1484	41.766821	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3479, FN=0, Flags=........C, BI=100
253	11.660567	00:86:bc:d2:22:94	ff:bf:f9:fe:ff:ff	802.11	90	Beacon frame, SN=3183, FN=0, Flags=........C, BI=114, SSID=linksys12
185	8.384186	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3151, FN=0, Flags=........C, BI=100, SSID=linksys12
169	8.178944	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3149, FN=0, Flags=........C, BI=100, SSID=li\bhsys12
167	8.076567	LinksysG_67:22:94	ff:df:cf:fe:ff:ff	802.11	90	Beacon frame, SN=3148, FN=0, Flags=........C, BI=100
43	2.137566	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3090, FN=0, Flags=........C, BI=100, SSID=linksys12
41	2.035064	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3089, FN=0, Flags=........C, BI=100, SSID=linksys12
34	1.420565	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3083, FN=0, Flags=........C, BI=20580, SSID=linksys12
31	1.215947	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3081, FN=0, Flags=........C, BI=100, SSID=linksys12
23	1.113691	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3080, FN=0, Flags=........C, BI=100, SSID=,▮nksys
21	1.010949	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3079, FN=0, Flags=........C, BI=100, SSID=linksys12
16	0.601687	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3075, FN=0, Flags=........C, BI=100, SSID=linksys12
10	0.294432	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3072, FN=0, Flags=........C, BI=62, SSID=li▮\001\004▮[Malformed Packet]

图 1.3

- What are the three addresses in the Beacon frame from the two APs respectively.

“30 Munroe St”: （图 2.1 所示）
Destination address : ff:ff:ff:ff:ff:ff
Source address : 00:16:b6:f7:1d:51
BSS ID : 00:16:b6:f7:1d:51



```
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)
  .... .... .... 0000 = Fragment number: 0
  1011 0010 1101 .... = Sequence number: 2861
  Frame check sequence: 0x59715663 [unverified]
  [FCS Status: Unverified]
IEEE 802.11 Wireless Management
> Fixed parameters (12 bytes)
v Tagged parameters (119 bytes)
  > Tag: SSID parameter set: 30 Munroe St
```

图 2.1

“linksys12”：（图 2.2 所示）
Destination address : ff:ff:ff:ff:ff:ff
Source address : 00:06:25:67:22:94
BSS ID : 00:06:25:67:22:94

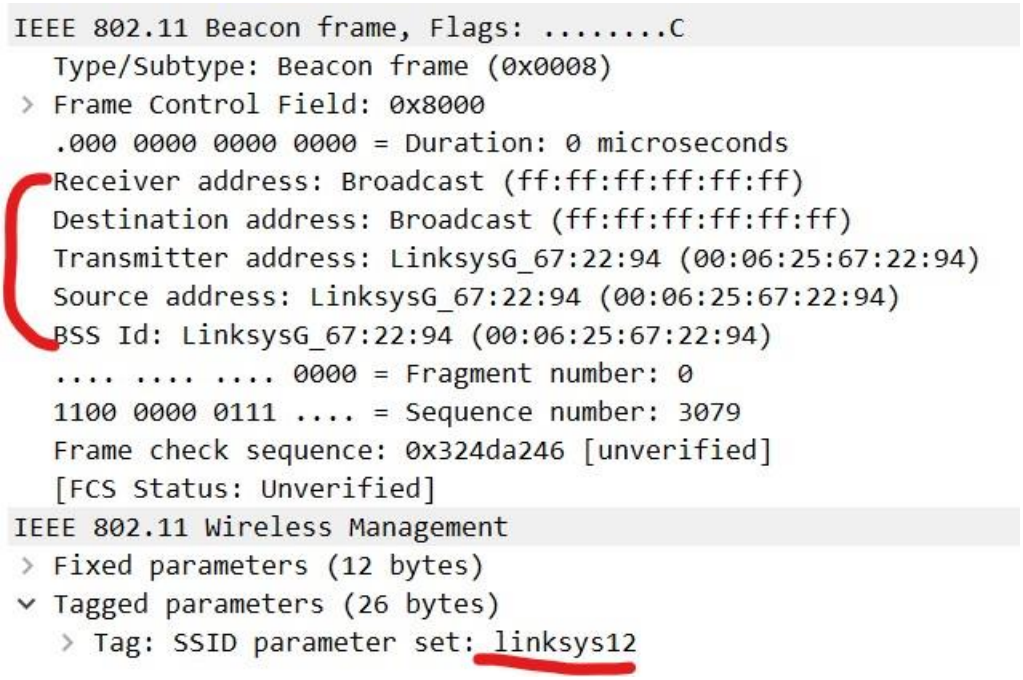


图 2.2

- How many APs the wireless laptop has received Beacon frames from? List their MAC addresses. Why the laptop can receive frames from an AP even though it does not associate with the AP?

BSSID	信道	SSID	按分组百分比	重试	试	Beacons	ita
00:16:b6:f7:1d:51	6	30 Munroe St	67.0	16.4	1...	439	
00:16:b6:f7:1d:51	6	30 Munroe St	20.4	6.2	19	266	
00:06:25:67:22:94	6	lin▮~ys	2.0	0.0	0	30	
00:16:b6:f7:1d:51	6	30 Munroe St	1.1	0.0	0	13	
00:18:39:f5:ba:bb	6	linksys_SES_24086	7.0	72.6	77	6	
00:18:39:93:b9:bb	6	linksys_SES_24086	0.3	0.0	0	1	
19:02:25:c7:78:94		<广播>	0.1	0.0	0	1	
40:00:24:67:22:8d	6	Home WIFI	0.2	0.0	0	1	
43:31:36:af:83:73		<广播>	0.1	00.(	1	1	
50:2b:25:67:22:94	6	linksys12	0.1	0.0	0	1	
[redacted]		[redacted]	0.1	0.0	0	0	
00:16:b6:27:12:51	6	30 Munroe St	0.1	0.0	0	0	
00:16:b6:f7:1d:51		winksys_SES_24086\001\004▮▮▮▮\003	0.1	0.0	0	0	
00:16:b6:f7:1d:51		linksys12	0.1	0.0	0	0	
2a:67:0c:e8:07:89		<广播>	0.1	0.0	0	0	
38:46:b1:a5:0c:a1		<广播>	0.1	00.(	1	0	
57:ac:42:16:91:eb		<广播>	0.1	00.(	1	0	
5c:03:a1:f8:dc:b8		<广播>	0.1	0.0	0	0	
5d:72:15:95:53:c9		<广播>	0.1	0.0	0	0	
60:5c:b1:36:42:ca		<广播>	0.1	0.0	0	0	
62:fc:d9:91:eb:be		<广播>	0.1	00.(	1	0	
80:2f:9c:4c:71:52		<广播>	0.1	00.(	1	0	
8c:40:4d:55:80:f6		<广播>	0.1	00.(	1	0	
a4:ce:c2:dd:12:06		<广播>	0.1	00.(	1	0	
ba:6b:ff:84:79:cc		<广播>	0.1	00.(	1	0	
f7:1d:51:00:16:b6		<广播>	0.1	0.0	0	0	
fb:15:87:3f:4e:36		<广播>	0.1	0.0	0	0	
ff:ff:ff:ff:ff:ff		phoiphas	0.1	0.0	0	0	
ff:ff:ff:ff:ff:ff		<广播>	0.3	0.0	0	0	
ff:ff:ff:ff:ff:ff		linksys	0.1	0.0	0	0	
ff:ff:ff:ff:ff:ff		hfmpc	0.1	0.0	0	0	
ff:ff:ff:ff:ff:ff		linksys_SES_24086	0.1	0.0	0	0	

图 3.1

参考图 3.1，我将 beacons 不为零的包按照地址 2 归类，地址 2 相同的包算作同一 AP 发出，这样可以得到实验者的笔记本一共收到了来自五个不同 AP 的 beacon frame。

它们的地址 2 就是其 MAC 地址，分别为：

“30 Munroe St”：00:16:b6:f7:1d:51（图 3.2）

```
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)
    .... .... .... 0000 = Fragment number: 0
    1011 0100 1010 .... = Sequence number: 2890
    Frame check sequence: 0x4fb51bfa [unverified]
    [FCS Status: Unverified]
IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v 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]
```

图 3.2

“linksys12” : 00:06:25:67:22:94（图 3.3）

```
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: LinksysG_67:22:94 (00:06:25:67:22:94)
   Source address: LinksysG_67:22:94 (00:06:25:67:22:94)
   BSS Id: LinksysG_67:22:94 (00:06:25:67:22:94)
   .... .... .... 0000 = Fragment number: 0
   1101 1010 1111 .... = Sequence number: 3503
   Frame check sequence: 0x6b6d2d2d [unverified]
   [FCS Status: Unverified]
IEEE 802.11 Wireless Management
 > Fixed parameters (12 bytes)
 v Tagged parameters (26 bytes)
     > Tag: SSID parameter set: linksys12
```

图 3.3

“linksys_SES_24086” : 00:18:39:f5:ba:bb（图 3.4）

```
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_f5:ba:bb (00:18:39:f5:ba:bb)
   Source address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
   BSS Id: Cisco-Li_93:b9:bb (00:18:39:93:b9:bb)
   .... .... .... 0000 = Fragment number: 0
   1110 1111 1001 .... = Sequence number: 3833
   Frame check sequence: 0xcdbaa932 [unverified]
   [FCS Status: Unverified]
IEEE 802.11 Wireless Management
 > Fixed parameters (12 bytes)
 v Tagged parameters (68 bytes)
     > Tag: SSID parameter set: linksys_SES_24086
```

图 3.4

“Home WIFI” : 00:ac:20:67:22:94（图 3.5）

```
IEEE 802.11 Beacon frame, Flags: ........C
   Type/Subtype: Beacon frame (0x0008)
 > Frame Control Field: 0x8000
   Duration/ID: 10752 (reserved)
   Receiver address: 5a:a5:ff:ff:ff:ff (5a:a5:ff:ff:ff:ff)
   Destination address: 5a:a5:ff:ff:ff:ff (5a:a5:ff:ff:ff:ff)
   Transmitter address: 00:ac:20:67:22:94 (00:ac:20:67:22:94)
   Source address: 00:ac:20:67:22:94 (00:ac:20:67:22:94)
   BSS Id: 40:00:24:67:22:8d (40:00:24:67:22:8d)
   .... .... .... 0100 = Fragment number: 4
   1110 0010 0100 .... = Sequence number: 3620
   Frame check sequence: 0x05b4c268 [unverified]
   [FCS Status: Unverified]
IEEE 802.11 Wireless Management
 > Fixed parameters (12 bytes)
 v Tagged parameters (26 bytes)
     > Tag: SSID parameter set: lin+m■s
```

图 3.5

“<广播>”：d3:95:ca:bb:f0:f5（图 3.6）

```
v IEEE 802.11 Beacon frame, Flags: .pmPRMFTC
     Type/Subtype: Beacon frame (0x0008)
   > Frame Control Field: 0x807f
     .110 0001 1000 1100 = Duration: 24972 microseconds
     Receiver address: 3e:d3:27:e6:65:7f (3e:d3:27:e6:65:7f)
     Destination address: 3e:d3:27:e6:65:7f (3e:d3:27:e6:65:7f)
     Transmitter address: d3:95:ca:bb:f0:f5 (d3:95:ca:bb:f0:f5)
     Source address: d3:95:ca:bb:f0:f5 (d3:95:ca:bb:f0:f5)
     BSS Id: 43:31:36:af:83:73 (43:31:36:af:83:73)
     .... .... .... 1011 = Fragment number: 11
     0000 0011 0110 .... = Sequence number: 54
     Frame check sequence: 0x53cd28be [unverified]
     [FCS Status: Unverified]
   > TKIP/CCMP parameters
> Data (1564 bytes)
```

图 3.6

笔记本电脑没有与 AP 建立链接，却能收到 AP 发送的帧的原因：
802.11 标准要求每个 AP 周期性地发送信标帧，而且如果笔记本电脑执行主动扫描，向其周围广播探测请求帧的话，位于笔记本电脑范围内的所有 AP 也会发一个探测响应帧。因此笔记本电脑在进入课本所描述的 WiFi 丛林之后，当它在选择某个 AP 来建立连接时，可以收到一个或者多个还未与其建立连接的接入点发送的帧。

- Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). What are the three MAC addresses in the frame, which is the address for wireless laptop / AP / first-hop router?

所要求的帧如图 4.1 所示：

图 4.1

这个帧里面的 MAC 地址如图 4.2 所示：
Receiver address/BSS ID : 00:16:b6:f7:1d:51
Source/Transmitter address : 00:13:02:d1:b6:4f
Destination address : 00:16:b6:f4:eb:a8

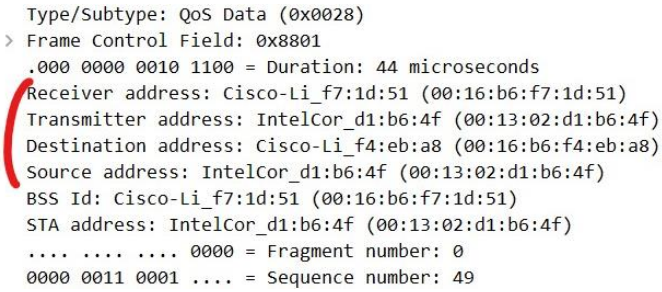


图 4.2

以下参考图 4.3
wireless laptop 的 MAC 地址：00:13:02:d1:b6:4f
wireless laptop 的 IP 地址：192.168.1.109
AP 的 MAC 地址：00:16:b6:f7:1d:51
第一跳路由器的 MAC 地址：00:16:b6:f4:eb:a8

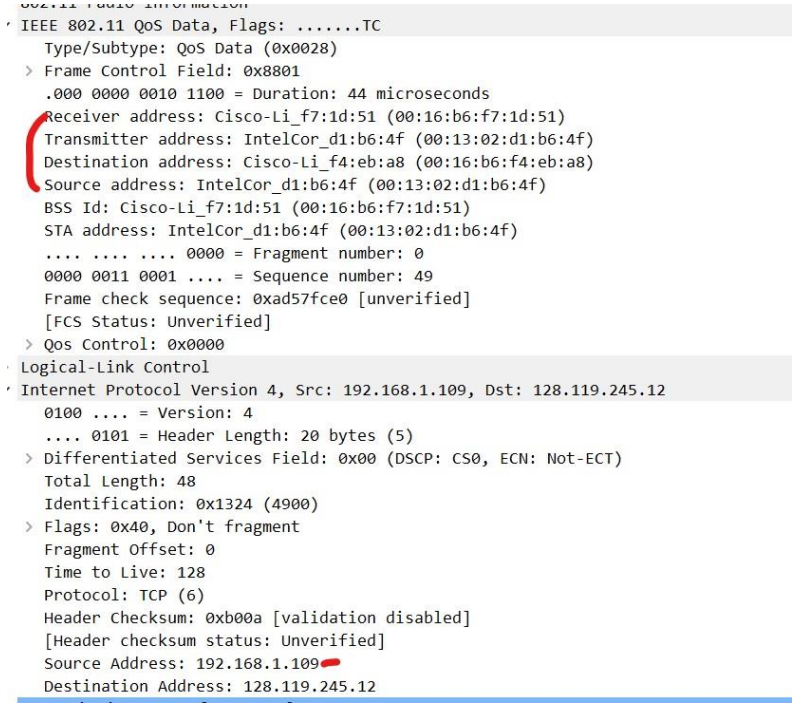


图 4.3

- For the SYN-ACK segment of the first TCP session, what are the three MAC addresses in the frame, and which is the address for wireless laptop / AP / first-hop router?

所要求的帧如图 5.1 所示：

图 5.1

这个帧里面的 MAC 地址如图 5.2 所示：

Receiver/Destination address : 91:2a:b0:49:b6:4f

Transmitter address/BSS ID : 00:16:b6:f7:1d:51

Source address : 00:16:b6:f4:eb:a8

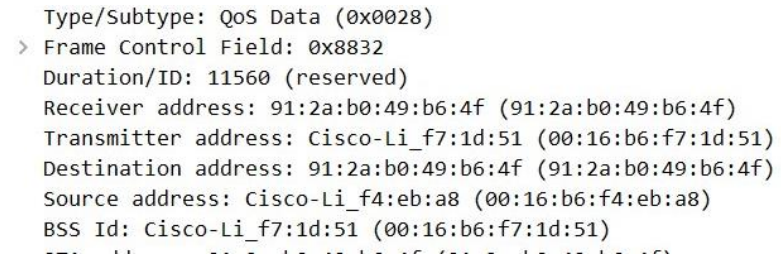


图 5.2

以下参考图 5.3

wireless laptop 的 MAC 地址：91:2a:b0:49:b6:4f

wireless laptop 的 IP 地址：192.168.1.109

AP 的 MAC 地址：00:16:b6:f7:1d:51

第一跳路由器的 MAC 地址：00:16:b6:f4:eb:a8

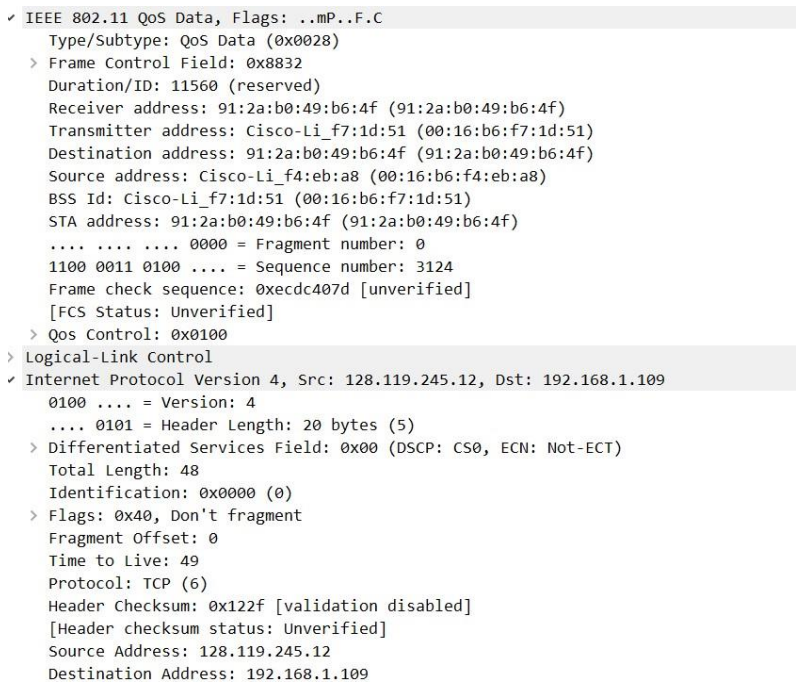


图 5.3

- For the above mentioned SYN-ACK segment, is the sender MAC address corresponds to the web server's IP address? Why?

  不一致。
  显然 web server 所处的子网和实验者笔记本电脑所处的子网不是同一个子网（从 IP 可以看出）。上述 SYN-ACK 帧中的发送者 MAC 地址其实是和实验者笔记本电脑处在同一子网中的路由器某一端口的 MAC 地址。根据 ARP，数据报在跨子网传输时，发送者和接收者的 MAC 地址都会不停更新。

- 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?

  首先向即将离开的子网中的 DHCP 服务器发送一个 DHCP Release 报文（图 7.1 所示），请求断开连接。

图 7.1

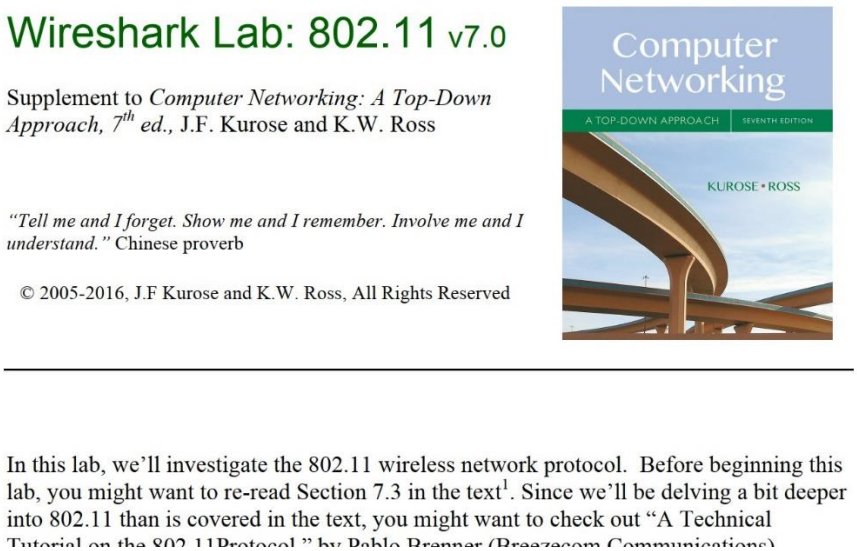
然后主机发送了一个 Deauthentication 帧，来请求取消身份认证。

图 7.2

- Can you capture a similar trace? Why or why not?

  可以。
  虽然带有 802.11 协议的无线网卡（NIC）设备驱动无法将捕获/接收的 802.11 帧用于 Wireshark 实验分析。但是可以买一个小的 USB 网卡 AirPcap 用以捕获 802.11 帧来提供给 Wireshark 实验分析。当我们拥有了设备之后就可以仿照实验者的操作，来抓取类似的包。

（这题的答案参考官方实验文档的部分内容-------图 8.1 && 图 8.2）



Wireshark Lab: 802.11 v7.0

Supplement to *Computer Networking: A Top-Down Approach, 7th ed.*, J.F. Kurose and K.W. Ross

"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb

In this lab, we'll investigate the 802.11 wireless network protocol. Before beginning this lab, you might want to re-read Section 7.3 in the text[1]. Since we'll be delving a bit deeper into 802.11 than is covered in the text, you might want to check out "A Technical Tutorial on the 802.11Protocol" by Pablo Brenner (Breezecom Communications)

图 8.1

In all of the Wireshark labs thus far, we've captured frames on a wired Ethernet connection. Here, since 802.11 is a wireless link-layer protocol, we'll be capturing frames "in the air." Unfortunately, many device drivers for wireless 802.11 NICs don't provide the hooks to capture/copy received 802.11 frames for use in Wireshark (see Figure 1 in Lab 1 for an overview of packet capture). Thus, in this lab, we'll provide a trace of captured 802.11 frames for you to analyze and assume in the questions below that you are using this trace. If you're able to capture 802.11 frames using your version of Wireshark, you're welcome to do so. Additionally, if you're really into frame capture, you can buy a small USB device, AirPcap, http://www.cacetech.com, that captures 802.11 frames and provides integrated support for Wireshark.

图 8.2