### 802.11 Trace Analysis 实验报告

#### 大数据学院 和泳毅 PB19010450

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

```
Time
                                            Destination
                                                                              Length Info
 1 0.000000
                    Cisco-Li_f7:1d:51
                                            Broadcast
                                                                                 183 Beacon frame, SN=2854, FN=0, Flags=......C, BI=100, SSID=30 Munroe St
                   Cisco-Li_f7:1d:51
Cisco-Li_f7:1d:51
Cisco-Li_f7:1d:51
 3 0.085474
                                            Broadcast
                                                                    802.11
                                                                                 183 Beacon frame, SN=2855, FN=0, Flags=......C, BI=100, SSID=30 Munroe St
 4 0.187919
                                                                                 183 Beacon frame, SN=2856, FN=0, Flags=.......C, BI=100, SSID=30 Munroe St
 9 0.290284
                                            Broadcast
                                                                    802.11
                                                                                 183 Beacon frame, SN=2857, FN=0, Flags=......C. BI=100, SSID=30 Munroe St
10 0.294432
                   LinksysG_67:22:94
Cisco-Li_f7:1d:51
                                                                     802.11
                                                                                  90 Beacon frame, SN=3072, FN=0, Flags=......C, BI=62, SSID=li■\001\004■[Malforme
                                            Broadcast
                                                                                 183 Beacon frame, SN=2858, FN=0, Flags=......C, BI=100, SSID=30 Munroe St
11 0.393174
                                            Broadcast
                                                                    802.11
13 0.495032
                   Cisco-Li_f7:1d:51
                                            Broadcast
                                                                     802.11
                                                                                 183 Beacon frame, SN=2859, FN=0, Flags=.......C, BI=100, SSID=30 Munroe St
14 0.499197
                                                                                  90 Beacon frame, SN=3074, FN=0, Flags=......C, BI=100, SSID=linksys12
                   LinksysG 67:22:94
                                            Broadcast
                                                                    802.11
15 0.597382
16 0.601687
                   Cisco-Li_f7:1d:51
LinksysG_67:22:94
                                                                                183 Beacon frame, SN=2860, FN=0, Flags=......, BI=100, SSID=30 Munroe St
90 Beacon frame, SN=3075, FN=0, Flags=.......C, BI=100, SSID=linksys12
                                            Broadcast
                                                                    802.11
                                            Broadcast
                                                                    802.11
                   Cisco-Li_f7:1d:51
Cisco-Li_f7:1d:51
                                                                                183 Beacon frame, SN=2861, FN=0, Flags=......C, BI=100, SSID=30 Munroe St
183 Beacon frame, SN=2862, FN=0, Flags=......C, BI=100, SSID=30 Munroe St
17 0.699847
                                            Broadcast
                                                                    802.11
18 0.802226
                                                                     802.11
19 0.904619
                   Cisco-Li_f7:1d:51
Cisco-Li_f7:1d:51
                                            Broadcast
                                                                    802.11
                                                                                183 Beacon frame, SN=2863, FN=9, Flags=......C, BI=100, SSID=30 Munroe St 183 Beacon frame, SN=2864, FN=0, Flags=......C, BI=100, SSID=30 Munroe St
20 1.007015
                                                                    802.11
21 1.010949
                   LinksysG 67:22:94
                                            Broadcast
                                                                    802.11
                                                                                  90 Beacon frame, SN=3079, FN=0, Flags=......C, BI=100, SSID=linksys12
22 1.109406
                    Cisco-Li_f7:1d:51
                                                                                 183 Beacon frame, SN=2865, FN=0, Flags=......C, BI=100, SSID=30 Munroe St
                   LinksysG_67:22:94
Cisco-Li_f7:1d:51
23 1.113691
                                            Broadcast
                                                                    802.11
                                                                                  90 Beacon frame, SN=3080, FN=0, Flags=......C, BI=100, SSID=. Inksys
24 1.211843
                                            Broadcast
                                                                     802.11
                                                                                 183 Beacon frame, SN=2866, FN=0, Flags=......C, BI=100, SSID=30 Munroe St
31 1.215947
                   LinksysG 67:22:94
                                            Broadcast
                                                                    802.11
                                                                                  90 Beacon frame, SN=3081, FN=0, Flags=......C, BI=100, SSID=linksys12
                   Cisco-Li_f7:1d:51
Cisco-Li_f7:1d:51
32 1.314223
                                            Broadcast
                                                                                 183 Beacon frame, SN=2868, FN=0, Flags=......C, BI=100, SSID=30 Munroe St
                                                                                183 Beacon frame, SN=2869, FN=0, Flags=......C, BI=100, SSID=30 Munroe St
33 1.416593
                                            Broadcast
                                                                    802.11
                   LinksysG_67:22:94
Cisco-Li_f7:1d:51
34 1,420565
                                            Broadcast
                                                                     802.11
                                                                                  90 Beacon frame, SN=3083, FN=0, Flags=......C, BI=20580, SSID=linksys12
35 1.519009
                                                                                 183 Beacon frame, SN=2870, FN=0, Flags=......C, BI=100, SSID=30 Munroe St
                                            Broadcast
                                                                    802.11
```

根据过滤出的所有信标帧来判断,发送最多信标帧的接入点的SSID为30 Munroe St。

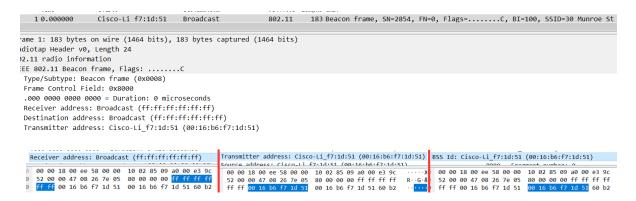
wlan.fc.type_subtype == 0x08 and wlan.ssid != "30 Munroe St"					
Tine	Source	Destination	Protocol	Length Info	
253 11.660567	00:86:bc:d2:22:94	ff:bf:f9:fe:ff:ff	802.11	90 Beacon frame, SN=3183, FN=0, Flags=C, BI=114, SSID=linksys12	
1486 41.868946	LinksysG_67:22:94	Broadcast	802.11	90 Beacon frame, SN=3480, 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	
1492 42.176195	LinksysG_67:22:94	Broadcast	802.11	90 Beacon frame, SN=3483, FN=0, Flags=C, BI=100, 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	
1496 42.381070	LinksysG_67:22:94	5f:a5:ff:ff:ff	802.11	90 Beacon frame, SN=3485, FN=0, Flags=C, BI=16484, 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	
1499 42.532596	Cisco-Li_f5:ba:bb	Broadcast	802.11	132 Beacon frame, SN=3640, FN=0, Flags=C, BI=100, SSID=linksys_SES_24086	
1513 42.839707	Cisco-Li_f5:ba:bb	Broadcast	802.11	132 Beacon frame, SN=3643, FN=0, Flags=C, BI=100, SSID=linksys_SES_24086	
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	
1517 42.995445	LinksysG_67:22:94	Broadcast	802.11	90 Beacon frame, SN=3491, 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	
1523 43.302694	LinksysG 67:22:94	Broadcast	802.11	90 Beacon frame, SN=3494, FN=0, Flags=C, BI=100, SSID=linksys12	
1527 43.658960	Cisco-Li f5:ba:bb	Broadcast	802.11	132 Beacon frame, SN=3651, FN=0, Flags=C, BI=100, SSID=linksys SES 24086	
1529 43.712193	LinksysG_67:22:94	Broadcast	802.11	90 Beacon frame, SN=3498, 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	
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	
1544 44.224320	LinksysG_67:22:94	Broadcast	802.11	90 Beacon frame, SN=3503, 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	
1556 44.838693	LinksysG 67:22:94	Broadcast	802.11	90 Beacon frame, SN=3509, FN=0, Flags=C, BI=100, SSID=linksys12	

将上述过滤信息去掉30 Munroe St后,发送最多信标帧的接入点的SSID为Linksys12。

综上,发送最多信标帧的两个接入点的SSID为30 Munroe St 和 Linksys12。

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

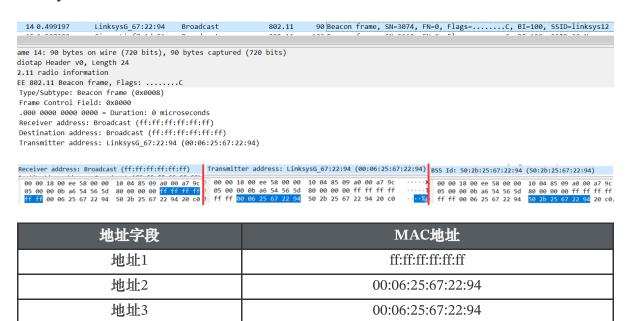
#### 30 Munroe St:



#### 观察具体地址字段:

地址字段	MAC地址
地址1	ff:ff:ff:ff:ff
地址2	00:16:b6:f7:1d:51
地址3	00:16:b6:f7:1d:51

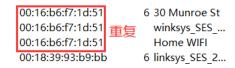
#### Linksys12:



3. 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?

Address	信道 SSID
> 00:16:b6:f7:1d:51	6 30 Munroe St
> 00:16:b6:f7:1d:51	winksys_SES
> 00:16:b6:f7:1d:51	Home WIFI
> 00:18:39:93:b9:bb	6 linksys_SES_2
> 00:18:39:f5:ba:bb	6 linksys_SES_2
> ff:ff:ff:ff:ff	linksys_SES_2
> 00:16:b6:27:12:51	6 30 Munroe St
> 00:16:b6:f7:1d:51	6 30 Munroe St
> ff:ff:ff:ff:ff	30 Munroe St
> 00:06:25:67:22:94	6 lin∎~ys
> 50:2b:25:67:22:94	6 linksys12
> ff:ff:ff:ff:ff	phoiphas
> ff:ff:ff:ff:ff	linksys
> ff:ff:ff:ff:ff	hfmpc

首先根据无线LAN统计获得大概的信息,首先根据BSSID去重:



其次,由于我们关注于AP周期性发送的信标帧,我们逐一排查去除其他帧,如probe request帧:

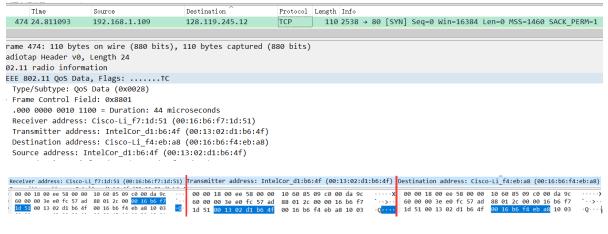
49 2.237786		IntelCor_d1:b6:4f (	802.11	38 Acknowledgement, Flags=C	
50 2.297613	IntelCor_1f:57:13	Broadcast	802.11	79 Probe Request SN=576, FN=0, Flags=C, SSID=Home WIFI	
51 2.300697	Cisco-Li f7:1d:51	IntelCor 1f:57:13	802.11	177 Probe Response, SN=2878, FN=0, Flags=C, BI=100, SSID=30 N	

最后,一共有3个AP: 330 Munroe St, linksys12, linksys\_SES\_24806.

AP	MAC
30 Munroe St	00:16:b6:f7:1d:51
linksys_SES_24806	00:18:39:f5:ba:bb
linksys12	00:06:25:67:22:94

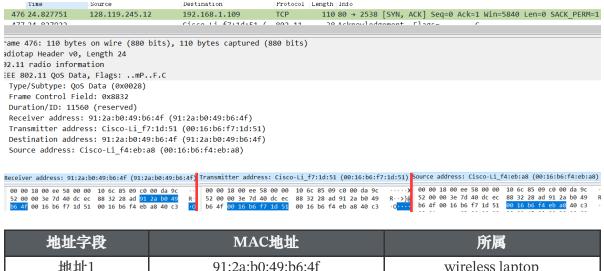
首先根据802.11标准,AP会周期性的发送信标帧,笔记本为了得知正在发送信标帧的AP,会扫描11个信道,找出来可能位于该区域的AP所发出的信标帧。这样会使笔记本没有与AP关联也收到帧。其次笔记本也可以通过主动扫描,向范围内所有AP广播探测帧,此后AP会用一个探测响应帧应答探测请求帧,这也使得笔记本在未与AP关联前收到帧。

4. 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?



地址字段	MAC地址	所属
地址1	00:16:b6:f7:1d:51	AP
地址2	00:13:02:d1:b6:4f	wireless laptop
地址3	00:16:b6:f4:eb:a8	first-hop router

# 5. 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?



地址字段	MAC地址	所属
地址1	91:2a:b0:49:b6:4f	wireless laptop
地址2	00:16:b6:f7:1d:51	AP
地址3	00:16:b6:f4:eb:a8	first-hop router

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

不对应。在发送SYN-ACK时,当以太网帧到达AP,该AP在将其传输到无线信道前,先将802.3以太网帧转换为一个802.11帧,将发送方MAC地址填入AP自身的MAC地址。所以上述发送方MAC地址指向AP,而不是web服务器的IP地址。

## 7. 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?

1731 49.440243		IntelCor_d1:b6:4f ( 802.11	38 Acknowledgement, Flags=C
1732 49.542481	Cisco-Li_f7:1d:51	Broadcast 802.11	183 Beacon frame, SN=3588, FN=0, Flags=C, BI=100, SSID=30 Munroe St
1733 49.583615	192.168.1.109	192.168.1.1 DHCP	390 DHCP Release - Transaction ID 0xea5a526
1734 49.583771		IntelCor_d1:b6:4f ( 802.11	38 Acknowledgement, Flags=C
1735 49.609617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51 802.11	54 Deauthentication, SN=1605, FN=0, Flags=C
1736 49.609770		IntelCor_d1:b6:4f ( 802.11	38 Acknowledgement, Flags=C
1737 49.614478	IntelCor_d1:b6:4f	Broadcast 802.11	99 Probe Request, SN=1606, FN=0, Flags=C, SSID=linksys_SES_24086
1738 49.615869		Cisco-Li f5:ha:hh ( 802.11	38 Acknowledgement. Flags=C

做了两个操作,一个是IP层操作,一个是802.11层操作。其中IP层操作为发送DHCP释放帧 (DHCP Release) ,802.11层操作为发送解除认证帧 (Deauthentication) 。

#### 8. Can you capture a similar trace? Why or why not?

本机目前不能,因为无线网卡不是监听模式时,网卡驱动会自动把802.11帧转换为以太网帧,在Windows系统中无法捕获到802.11帧。需在Linux系统中将无线网卡设置为监听模式,且在Linux系统中抓包。