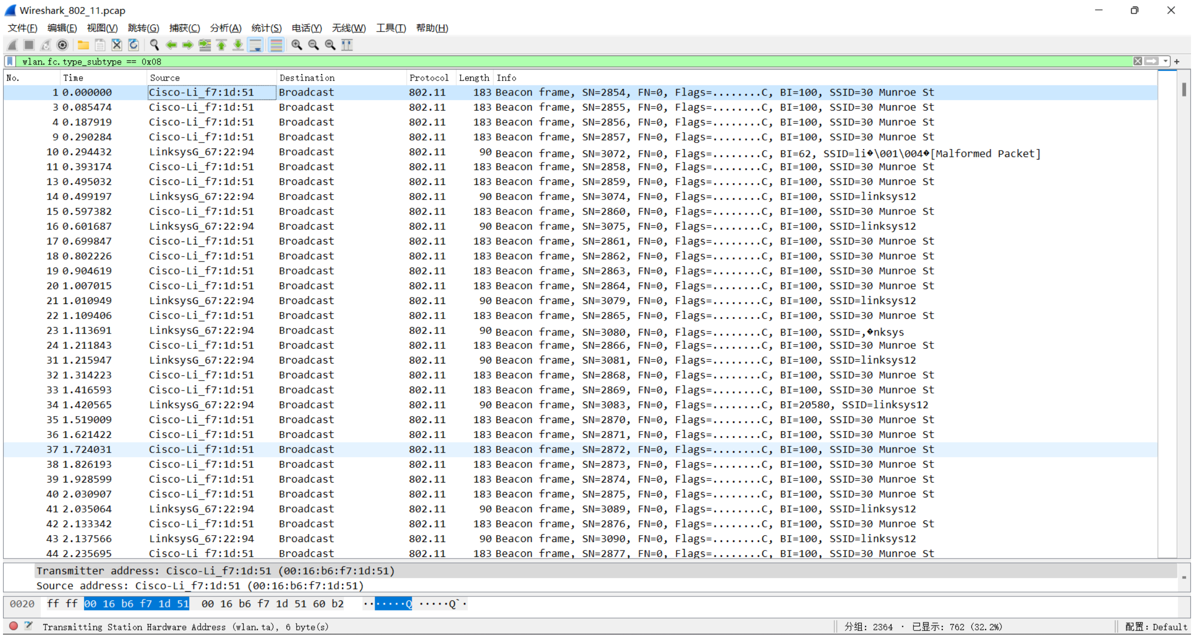
802.11 Trace Analysis

PB19030861 王湘峰

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

发送信标帧最多的AP是 **30 Munroe St** 和 **linksys12** .

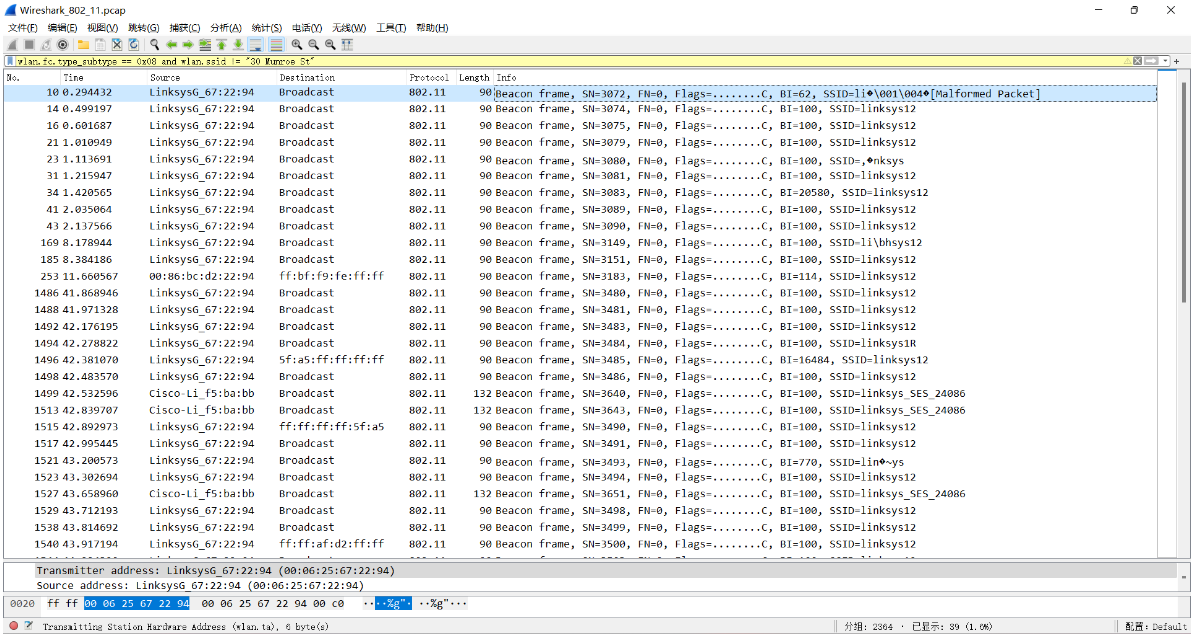
(下图为过滤出了所有beacon frame，可以看到最多的SSID为**30 Munroe St**)


Wireshark_802_11.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
wlan.fc.type_subtype == 0x08
```

```
No.   Time      Source             Destination  Protocol Length Info
    1 0.000000  Cisco-Li_f7:1d:51  Broadcast    802.11    183 Beacon frame, SN=2854, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
    3 0.085474  Cisco-Li_f7:1d:51  Broadcast    802.11    183 Beacon frame, SN=2855, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
    4 0.187919  Cisco-Li_f7:1d:51  Broadcast    802.11    183 Beacon frame, SN=2856, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
    9 0.290284  Cisco-Li_f7:1d:51  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  Broadcast    802.11     90 Beacon frame, SN=3072, FN=0, Flags=........C, BI=62, SSID=li�\001\004�[Malformed Packet]
   11 0.393174  Cisco-Li_f7:1d:51  Broadcast    802.11    183 Beacon frame, SN=2858, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   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  LinksysG_67:22:94  Broadcast    802.11     90 Beacon frame, SN=3074, FN=0, Flags=........C, BI=100, SSID=linksys12
   15 0.597382  Cisco-Li_f7:1d:51  Broadcast    802.11    183 Beacon frame, SN=2860, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   16 0.601687  LinksysG_67:22:94  Broadcast    802.11     90 Beacon frame, SN=3075, FN=0, Flags=........C, BI=100, SSID=linksys12
   17 0.699847  Cisco-Li_f7:1d:51  Broadcast    802.11    183 Beacon frame, SN=2861, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   18 0.802226  Cisco-Li_f7:1d:51  Broadcast    802.11    183 Beacon frame, SN=2862, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   19 0.904619  Cisco-Li_f7:1d:51  Broadcast    802.11    183 Beacon frame, SN=2863, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   20 1.007015  Cisco-Li_f7:1d:51  Broadcast    802.11    183 Beacon frame, SN=2864, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   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  Broadcast    802.11    183 Beacon frame, SN=2865, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   23 1.113691  LinksysG_67:22:94  Broadcast    802.11     90 Beacon frame, SN=3080, FN=0, Flags=........C, BI=100, SSID=,�nksys
   24 1.211843  Cisco-Li_f7:1d:51  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
   32 1.314223  Cisco-Li_f7:1d:51  Broadcast    802.11    183 Beacon frame, SN=2868, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   33 1.416593  Cisco-Li_f7:1d:51  Broadcast    802.11    183 Beacon frame, SN=2869, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   34 1.420565  LinksysG_67:22:94  Broadcast    802.11     90 Beacon frame, SN=3083, FN=0, Flags=........C, BI=20580, SSID=linksys12
   35 1.519009  Cisco-Li_f7:1d:51  Broadcast    802.11    183 Beacon frame, SN=2870, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   36 1.621422  Cisco-Li_f7:1d:51  Broadcast    802.11    183 Beacon frame, SN=2871, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   37 1.724031  Cisco-Li_f7:1d:51  Broadcast    802.11    183 Beacon frame, SN=2872, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   38 1.826193  Cisco-Li_f7:1d:51  Broadcast    802.11    183 Beacon frame, SN=2873, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   39 1.928599  Cisco-Li_f7:1d:51  Broadcast    802.11    183 Beacon frame, SN=2874, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   40 2.030907  Cisco-Li_f7:1d:51  Broadcast    802.11    183 Beacon frame, SN=2875, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   41 2.035064  LinksysG_67:22:94  Broadcast    802.11     90 Beacon frame, SN=3089, FN=0, Flags=........C, BI=100, SSID=linksys12
   42 2.133342  Cisco-Li_f7:1d:51  Broadcast    802.11    183 Beacon frame, SN=2876, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   43 2.137566  LinksysG_67:22:94  Broadcast    802.11     90 Beacon frame, SN=3090, FN=0, Flags=........C, BI=100, SSID=linksys12
   44 2.235695  Cisco-Li_f7:1d:51  Broadcast    802.11    183 Beacon frame, SN=2877, FN=0, Flags=........C, BI=100, SSID=30 Munroe St

    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)

0020  ff ff 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 60 b2   ·······Q ·····Q`·

Transmitting Station Hardware Address (wlan.ta), 6 byte(s)    分组: 2364 · 已显示: 762 (32.2%)    配置: Default
```

（下图为去除掉**30 Munroe St**后的beacon frame信息，易知第二多的AP是**linksys12**）

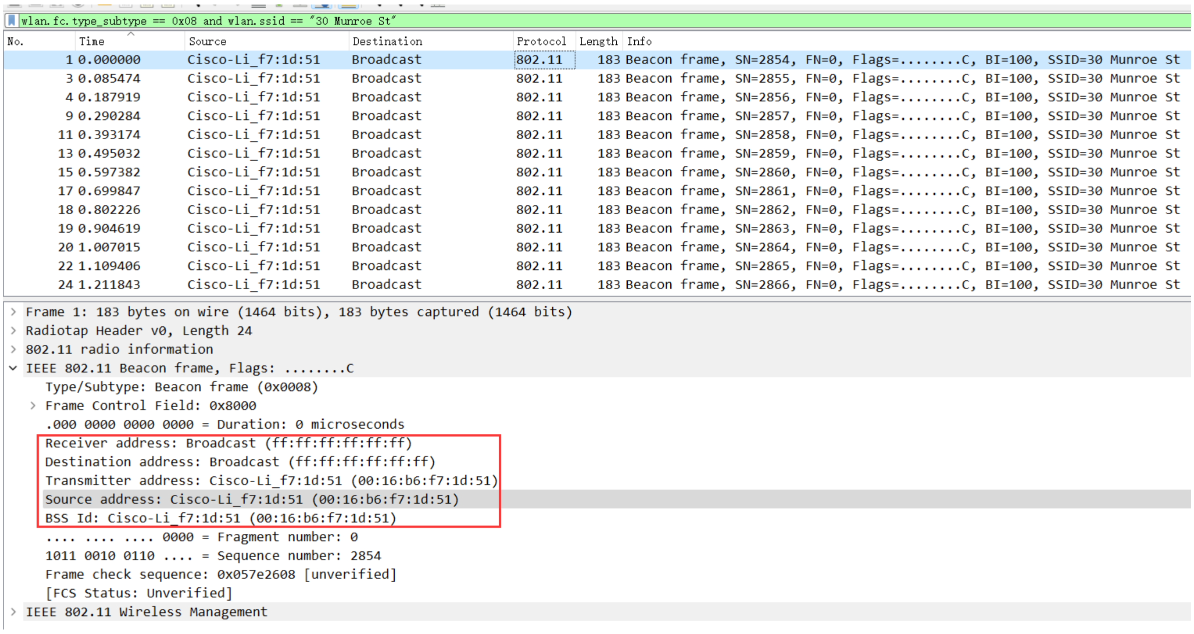

Wireshark_802_11.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
wlan.fc.type_subtype == 0x08 and wlan.ssid != "30 Munroe St"
```

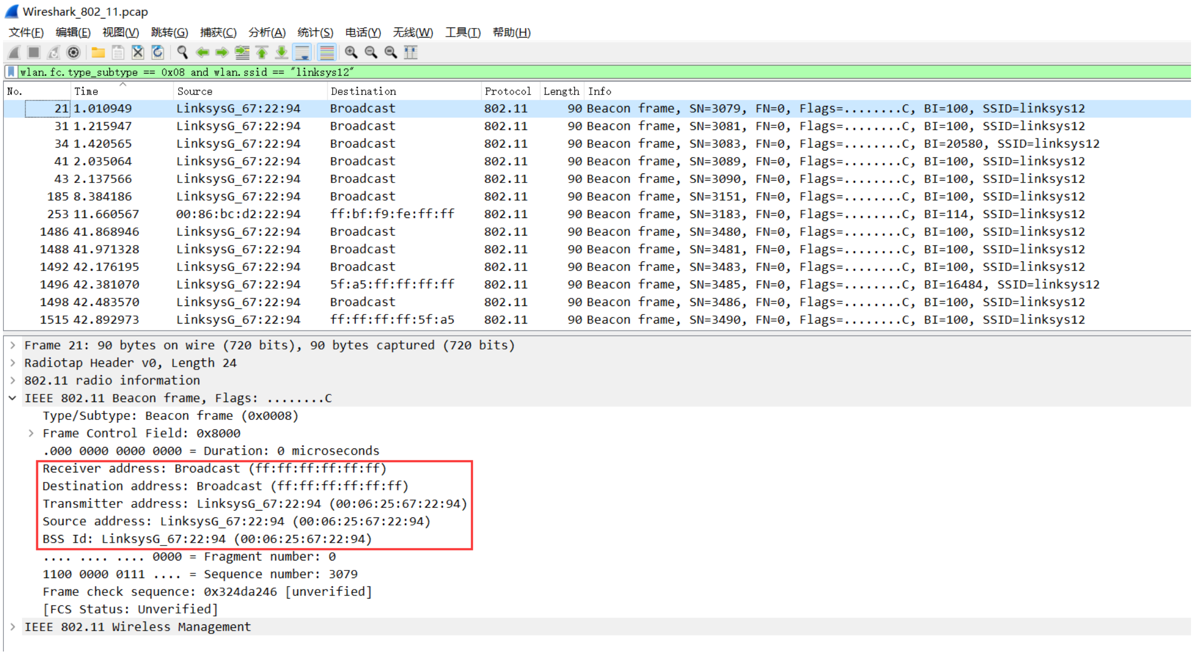
```
No.   Time       Source             Destination        Protocol Length Info
   10 0.294432   LinksysG_67:22:94  Broadcast          802.11     90 Beacon frame, SN=3072, FN=0, Flags=........C, BI=62, SSID=li�\001\004�[Malformed Packet]
   14 0.499197   LinksysG_67:22:94  Broadcast          802.11     90 Beacon frame, SN=3074, 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
   21 1.010949   LinksysG_67:22:94  Broadcast          802.11     90 Beacon frame, SN=3079, 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
   31 1.215947   LinksysG_67:22:94  Broadcast          802.11     90 Beacon frame, SN=3081, 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
   41 2.035064   LinksysG_67:22:94  Broadcast          802.11     90 Beacon frame, SN=3089, FN=0, Flags=........C, BI=100, SSID=linksys12
   43 2.137566   LinksysG_67:22:94  Broadcast          802.11     90 Beacon frame, SN=3090, 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
  185 8.384186   LinksysG_67:22:94  Broadcast          802.11     90 Beacon frame, SN=3151, FN=0, Flags=........C, BI=100, SSID=linksys12
  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: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

    Transmitter address: LinksysG_67:22:94 (00:06:25:67:22:94)
    Source address: LinksysG_67:22:94 (00:06:25:67:22:94)

0020  ff ff 00 06 25 67 22 94  00 06 25 67 22 94 00 c0   ····%g"· ··%g"···

Transmitting Station Hardware Address (wlan.ta), 6 byte(s)    分组: 2364 · 已显示: 39 (1.6%)    配置: Default
```

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

Address/AP	30 Munroe St	linksys12
address1	ff:ff:ff:ff:ff:ff	ff:ff:ff:ff:ff:ff
address2	00:16:b6:f7:1d:51	00:06:25:67:22:94
address3	00:16:b6:f7:1d:51	00:06:25:67:22:94



```
wlan.fc.type_subtype == 0x08 and wlan.ssid == "30 Munroe St"
No.     Time        Source              Destination         Protocol  Length Info
      1 0.000000    Cisco-Li_f7:1d:51   Broadcast           802.11    183 Beacon frame, SN=2854, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
      3 0.085474    Cisco-Li_f7:1d:51   Broadcast           802.11    183 Beacon frame, SN=2855, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
      4 0.187919    Cisco-Li_f7:1d:51   Broadcast           802.11    183 Beacon frame, SN=2856, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
      9 0.290284    Cisco-Li_f7:1d:51   Broadcast           802.11    183 Beacon frame, SN=2857, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
     11 0.393174    Cisco-Li_f7:1d:51   Broadcast           802.11    183 Beacon frame, SN=2858, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
     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
     15 0.597382    Cisco-Li_f7:1d:51   Broadcast           802.11    183 Beacon frame, SN=2860, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
     17 0.699847    Cisco-Li_f7:1d:51   Broadcast           802.11    183 Beacon frame, SN=2861, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
     18 0.802226    Cisco-Li_f7:1d:51   Broadcast           802.11    183 Beacon frame, SN=2862, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
     19 0.904619    Cisco-Li_f7:1d:51   Broadcast           802.11    183 Beacon frame, SN=2863, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
     20 1.007015    Cisco-Li_f7:1d:51   Broadcast           802.11    183 Beacon frame, SN=2864, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
     22 1.109406    Cisco-Li_f7:1d:51   Broadcast           802.11    183 Beacon frame, SN=2865, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
     24 1.211843    Cisco-Li_f7:1d:51   Broadcast           802.11    183 Beacon frame, SN=2866, FN=0, Flags=........C, BI=100, SSID=30 Munroe St

> Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v 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 0110 .... = Sequence number: 2854
    Frame check sequence: 0x057e2608 [unverified]
    [FCS Status: Unverified]
> IEEE 802.11 Wireless Management
```


Wireshark_802_11.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
wlan.fc.type_subtype == 0x08 and wlan.ssid == "linksys12"
No.     Time        Source              Destination         Protocol  Length Info
     21 1.010949    LinksysG_67:22:94   Broadcast           802.11    90 Beacon frame, SN=3079, FN=0, Flags=........C, BI=100, 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
     34 1.420565    LinksysG_67:22:94   Broadcast           802.11    90 Beacon frame, SN=3083, FN=0, Flags=........C, BI=20580, 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
     43 2.137566    LinksysG_67:22:94   Broadcast           802.11    90 Beacon frame, SN=3090, FN=0, Flags=........C, BI=100, 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
    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
   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
   1498 42.483570   LinksysG_67:22:94   Broadcast           802.11    90 Beacon frame, SN=3486, 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

> Frame 21: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v 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
    1100 0000 0111 .... = Sequence number: 3079
    Frame check sequence: 0x324da246 [unverified]
    [FCS Status: Unverified]
> IEEE 802.11 Wireless Management
```

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?

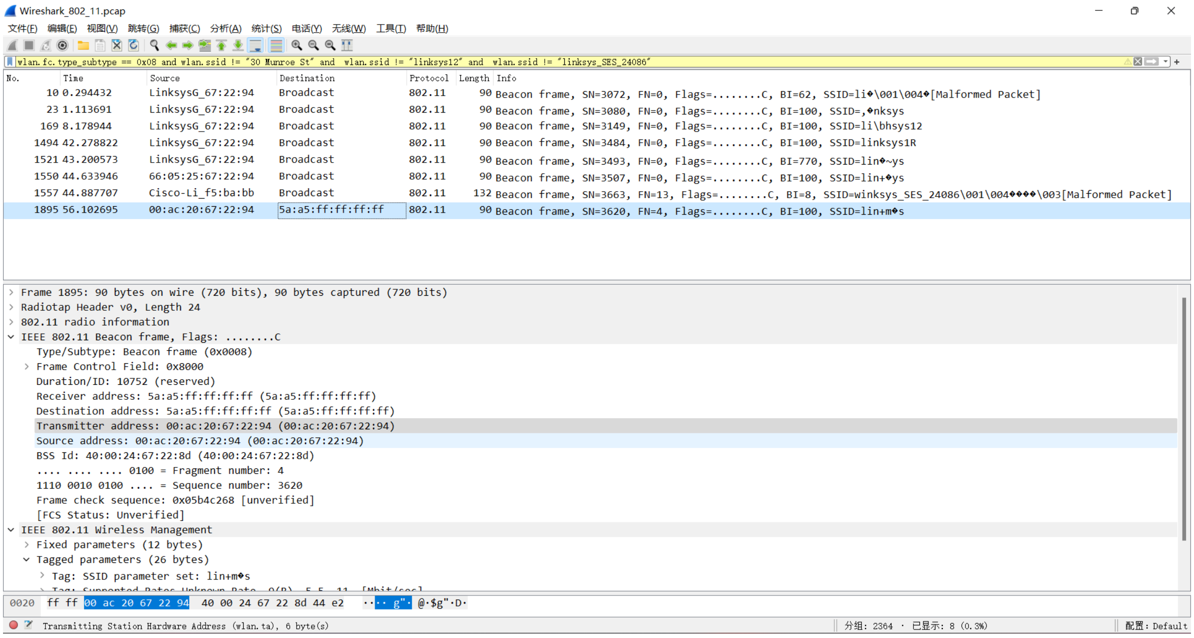
一共有3个收到信标帧的AP：30 Munroe St, linksys12, linksys_SES_24806.

SSID	Address
30 Munroe St	00:16:b6:f7:1d:51
linksys12	00:06:25:67:22:94
linksys_SES_24806	00:18:39:93:b9:bb

解释：

根据IEEE 802.11a/b/g/n 协议，每个AP每隔一定时间（几十毫秒到几秒不等）向周围的STA和AP广播beacon帧，以此让别的STA和AP与之相连接。所以收到的beacon帧是AP的广播帧。

（下图为去除主要的三个AP后得到的beacon frame，对每个帧观察发现其BSSID总是和上面三种之一重合，以此推断这些SSID其实是信号失真导致的，一共只收到了3个AP的帧）


Wireshark_802_11.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
wlan.fc.type_subtype == 0x08 and wlan.ssid != "30 Munroe St" and  wlan.ssid != "linksys12" and  wlan.ssid != "linksys_SES_24086"
```

```
No.    Time       Source              Destination         Protocol Length Info
  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]
  23   1.113691   LinksysG_67:22:94   Broadcast           802.11    90 Beacon frame, SN=3080, FN=0, Flags=........C, BI=100, SSID=,�nksys
 169   8.178944   LinksysG_67:22:94   Broadcast           802.11    90 Beacon frame, SN=3149, FN=0, Flags=........C, BI=100, SSID=li\bhsys12
1494  42.278822   LinksysG_67:22:94   Broadcast           802.11    90 Beacon frame, SN=3484, FN=0, Flags=........C, BI=100, SSID=linksys1R
1521  43.200573   LinksysG_67:22:94   Broadcast           802.11    90 Beacon frame, SN=3493, FN=0, Flags=........C, BI=770, SSID=lin�~ys
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
1557  44.887707   Cisco-Li_f5:ba:bb   Broadcast           802.11   132 Beacon frame, SN=3663, FN=13, Flags=........C, BI=8, SSID=winksys_SES_24086\001\004����\003[Malformed Packet]
1895  56.102695   00:ac:20:67:22:94   5a:a5:ff:ff:ff:ff   802.11    90 Beacon frame, SN=3620, FN=4, Flags=........C, BI=100, SSID=lin+m�s
```

```
> Frame 1895: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v 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]
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (26 bytes)
    > Tag: SSID parameter set: lin+m�s
    > Tag: Supported Rates Unknown Rate, 9(B), 5.5, 11, [Mbit/sec]
```

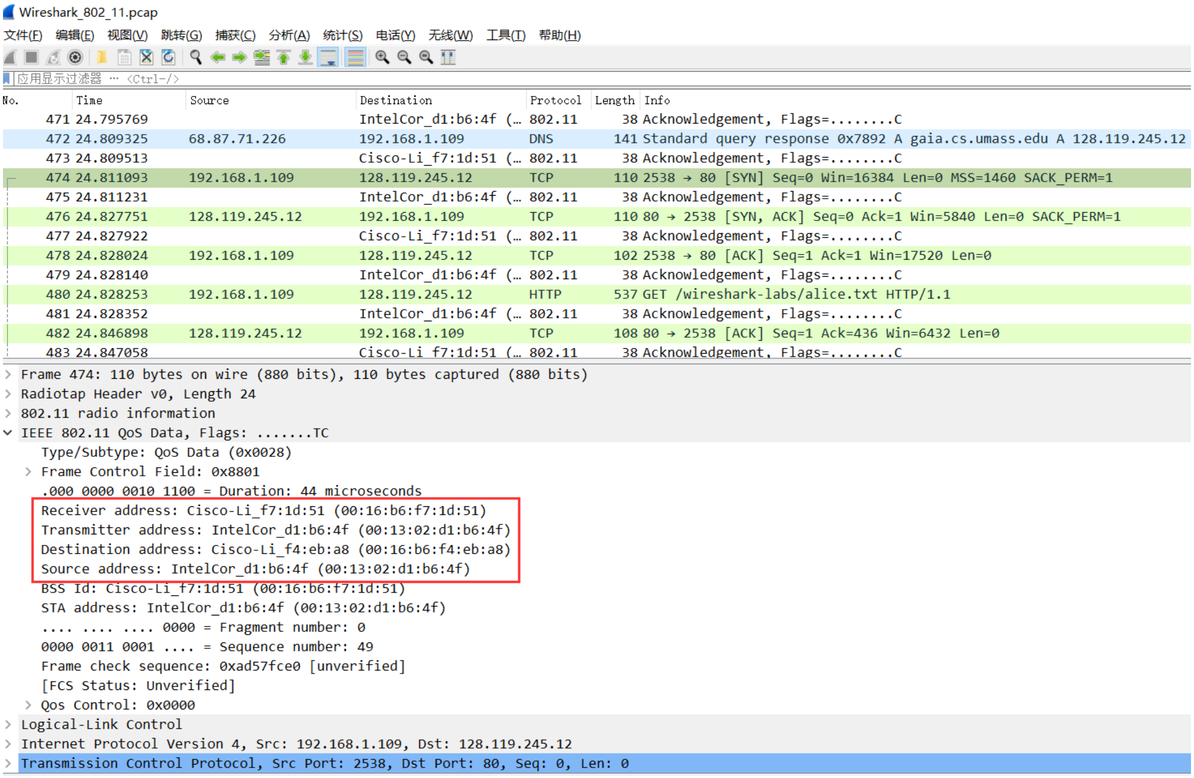
```
0020  ff ff 00 ac 20 67 22 94  40 00 24 67 22 8d 44 e2   ···· g"· @·$g"·D·
```

```
Transmitting Station Hardware Address (wlan.ta), 6 byte(s)    分组: 2364 · 已显示: 8 (0.3%)    配置: Default
```

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?

(表格1从上至下依次为Address1, Address2, Address3)

Receiver Address	**00:16:b6:f7:1d:51**	**AP**
Transmitter Address	**00:13:02:d1:b6:4f**	**wireless laptop**
Destination Address	**00:16:b6:f4:eb:a8**	**first-hop router**


Wireshark_802_11.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>

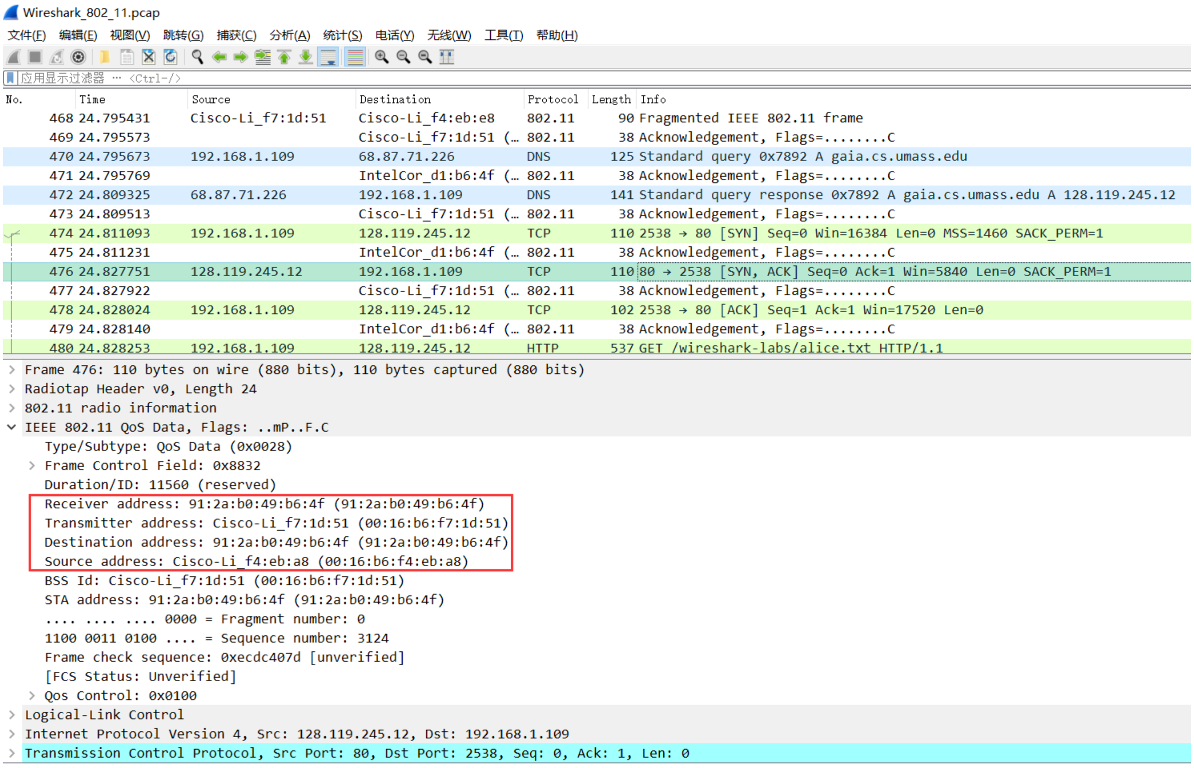
```
No.    Time        Source          Destination           Protocol Length Info
   471 24.795769                   IntelCor_d1:b6:4f (… 802.11      38 Acknowledgement, Flags=........C
   472 24.809325   68.87.71.226    192.168.1.109        DNS        141 Standard query response 0x7892 A gaia.cs.umass.edu A 128.119.245.12
   473 24.809513                   Cisco-Li_f7:1d:51 (… 802.11      38 Acknowledgement, Flags=........C
   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=1
   475 24.811231                   IntelCor_d1:b6:4f (… 802.11      38 Acknowledgement, Flags=........C
   476 24.827751   128.119.245.12  192.168.1.109        TCP        110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1
   477 24.827922                   Cisco-Li_f7:1d:51 (… 802.11      38 Acknowledgement, Flags=........C
   478 24.828024   192.168.1.109   128.119.245.12       TCP        102 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
   479 24.828140                   IntelCor_d1:b6:4f (… 802.11      38 Acknowledgement, Flags=........C
   480 24.828253   192.168.1.109   128.119.245.12       HTTP       537 GET /wireshark-labs/alice.txt HTTP/1.1
   481 24.828352                   IntelCor_d1:b6:4f (… 802.11      38 Acknowledgement, Flags=........C
   482 24.846898   128.119.245.12  192.168.1.109        TCP        108 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
   483 24.847058                   Cisco-Li_f7:1d:51 (… 802.11      38 Acknowledgement, Flags=........C
```

```
> Frame 474: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8801
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
    Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    .... .... .... 0000 = Fragment number: 0
    0000 0011 0001 .... = Sequence number: 49
    Frame check sequence: 0xad57fce0 [unverified]
    [FCS Status: Unverified]
  > Qos Control: 0x0000
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 2538, Dst Port: 80, Seq: 0, Len: 0
```

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?

(表格1从上至下依次为Address1, Address2, Address3)

Receiver Address	**00:13:02:d1:b6:4f**	**wireless laptop**
Transmitter Address	**00:16:b6:f7:1d:51**	**AP**
Source Address	**00:16:b6:f4:eb:a8**	**first-hop router**


Wireshark_802_11.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>

```
No.    Time        Source            Destination           Protocol Length Info
   468 24.795431   Cisco-Li_f7:1d:51 Cisco-Li_f4:eb:e8    802.11      90 Fragmented IEEE 802.11 frame
   469 24.795573                     Cisco-Li_f7:1d:51 (… 802.11      38 Acknowledgement, Flags=........C
   470 24.795673   192.168.1.109     68.87.71.226         DNS        125 Standard query 0x7892 A gaia.cs.umass.edu
   471 24.795769                     IntelCor_d1:b6:4f (… 802.11      38 Acknowledgement, Flags=........C
   472 24.809325   68.87.71.226      192.168.1.109        DNS        141 Standard query response 0x7892 A gaia.cs.umass.edu A 128.119.245.12
   473 24.809513                     Cisco-Li_f7:1d:51 (… 802.11      38 Acknowledgement, Flags=........C
   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=1
   475 24.811231                     IntelCor_d1:b6:4f (… 802.11      38 Acknowledgement, Flags=........C
   476 24.827751   128.119.245.12    192.168.1.109        TCP        110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1
   477 24.827922                     Cisco-Li_f7:1d:51 (… 802.11      38 Acknowledgement, Flags=........C
   478 24.828024   192.168.1.109     128.119.245.12       TCP        102 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
   479 24.828140                     IntelCor_d1:b6:4f (… 802.11      38 Acknowledgement, Flags=........C
   480 24.828253   192.168.1.109     128.119.245.12       HTTP       537 GET /wireshark-labs/alice.txt HTTP/1.1
```

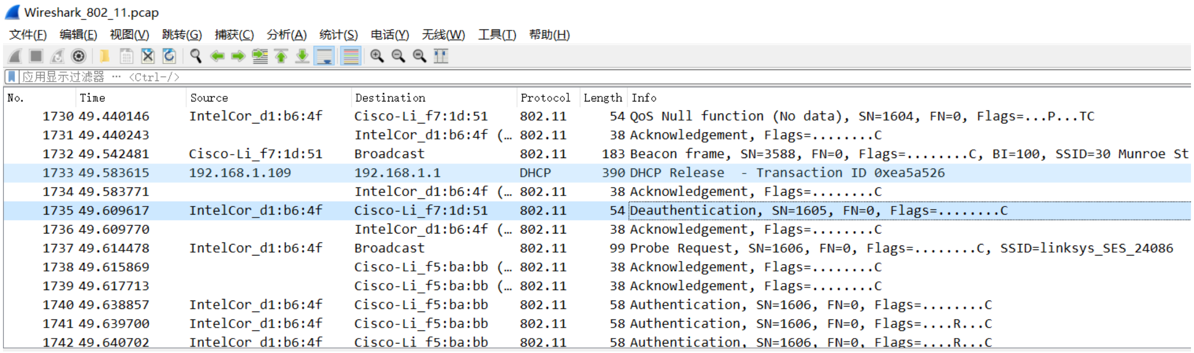
```
> Frame 476: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: ..mP..F.C
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8832
    Duration/ID: 11560 (reserved)
    Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Transmitter address: Cisco-Li_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: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    .... .... .... 0000 = Fragment number: 0
    1100 0011 0100 .... = Sequence number: 3124
    Frame check sequence: 0xecdc407d [unverified]
    [FCS Status: Unverified]
  > Qos Control: 0x0100
> Logical-Link Control
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.109
> Transmission Control Protocol, Src Port: 80, Dst Port: 2538, Seq: 0, Ack: 1, Len: 0
```

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

答：不是的，发送端的MAC地址是AP的而非web服务器的。在数据链路层，帧的发送地址与接收地址为相邻节点的MAC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?

1. Release DHCP
2. Deauthentication


Wireshark_802_11.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1730	49.440146	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1604, FN=0, Flags=...P...TC
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:ba:bb (…	802.11	38	Acknowledgement, Flags=........C
1739	49.617713		Cisco-Li_f5:ba:bb (…	802.11	38	Acknowledgement, Flags=........C
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=........C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C

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

由于本人的电脑网卡不支持monitor功能，无法捕捉802.11帧，故不能复现该实验。