802.11 Trace Analysis

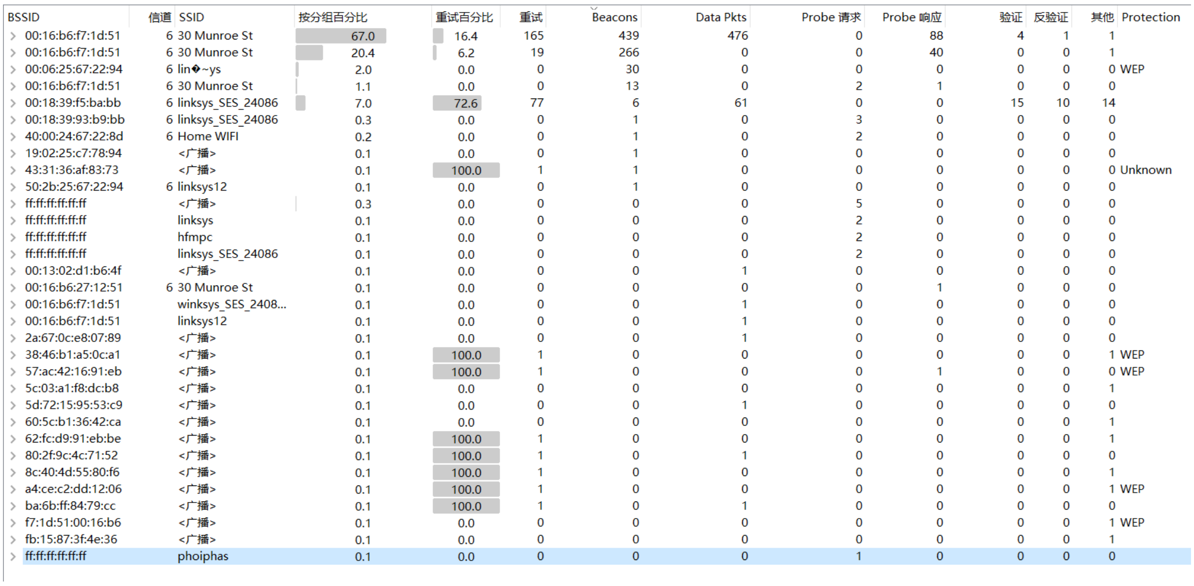
PB19111749 吴毅龙

1.

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

> 发出此跟踪中大多数信标帧的两个AP的SSID是什么?

在`Wireshark`的`无线LAN统计`中，按照`Beacons`从大到小进行排序。可知发送最多`Beacon`的两个`AP`的`SSID`分别是`30 Munroe St(00:16:b6:f7:1d:51)`和`lin�~ys(00:06:25:67:22:94)`



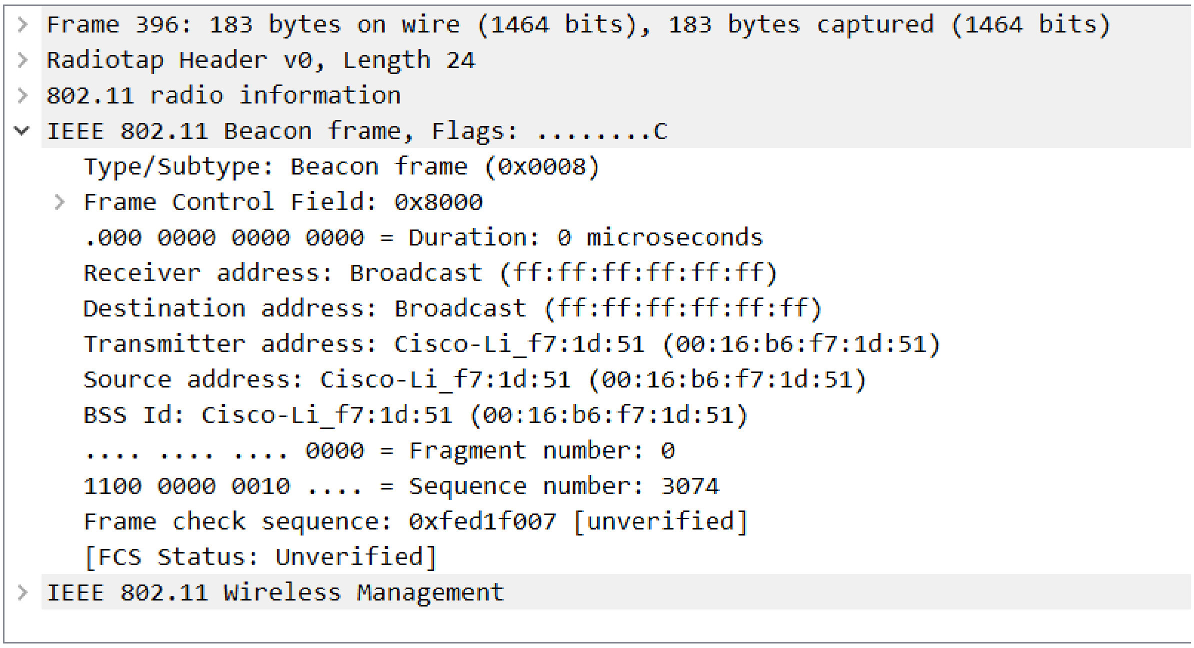
BSSID	信道	SSID	按分组百分比	重试百分比	重试	Beacons	Data Pkts	Probe 请求	Probe 响应	验证	反验证	其他	Protection
00:16:b6:f7:1d:51	6	30 Munroe St	67.0	16.4	165	439	476	0	88	4	1	1	
00:16:b6:f7:1d:51	6	30 Munroe St	20.4	6.2	19	266	0	0	40	0	0	1	
00:06:25:67:22:94	6	lin�~ys	2.0	0.0	0	30	0	0	0	0	0	0	WEP
00:16:b6:f7:1d:51	6	30 Munroe St	1.1	0.0	0	13	0	2	1	0	0	0	
00:18:39:f5:ba:bb	6	linksys_SES_24086	7.0	72.6	77	6	61	0	0	15	10	14	
00:18:39:93:b9:bb	6	linksys_SES_24086	0.3	0.0	0	1	0	3	0	0	0	0	
40:00:24:67:22:8d	6	Home WIFI	0.2	0.0	0	1	0	2	0	0	0	0	
19:02:25:c7:78:94		<广播>	0.1	0.0	0	1	0	0	0	0	0	0	
43:31:36:af:83:73		<广播>	0.1	100.0	1	1	0	0	0	0	0	0	Unknown
50:2b:25:67:22:94	6	linksys12	0.1	0.0	0	1	0	0	0	0	0	0	
ff:ff:ff:ff:ff:ff		<广播>	0.3	0.0	0	0	0	5	0	0	0	0	
ff:ff:ff:ff:ff:ff		linksys	0.1	0.0	0	0	0	2	0	0	0	0	
ff:ff:ff:ff:ff:ff		hfmpc	0.1	0.0	0	0	0	2	0	0	0	0	
ff:ff:ff:ff:ff:ff		linksys_SES_24086	0.1	0.0	0	0	0	2	0	0	0	0	
00:13:02:d1:b6:4f		<广播>	0.1	0.0	0	0	1	0	0	0	0	0	
00:16:b6:27:12:51	6	30 Munroe St	0.1	0.0	0	0	0	0	1	0	0	0	
00:16:b6:f7:1d:51		winksys_SES_2408...	0.1	0.0	0	0	1	0	0	0	0	0	
00:16:b6:f7:1d:51		linksys12	0.1	0.0	0	0	1	0	0	0	0	0	
2a:67:0c:e8:07:89		<广播>	0.1	0.0	0	0	1	0	0	0	0	0	
38:46:b1:a5:0c:a1		<广播>	0.1	100.0	1	0	0	0	0	0	0	1	WEP
57:ac:42:16:91:eb		<广播>	0.1	100.0	1	0	0	0	1	0	0	0	WEP
5c:03:a1:f8:dc:b8		<广播>	0.1	0.0	0	0	0	0	0	0	0	1	
5d:72:15:95:53:c9		<广播>	0.1	0.0	0	0	1	0	0	0	0	0	
60:5c:b1:36:42:ca		<广播>	0.1	0.0	0	0	0	0	0	0	0	1	
62:fc:d9:91:eb:be		<广播>	0.1	100.0	1	0	0	0	0	0	0	1	
80:2f:9c:4c:71:52		<广播>	0.1	100.0	1	0	1	0	0	0	0	0	
8c:40:4d:55:80:f6		<广播>	0.1	100.0	1	0	0	0	0	0	0	1	
a4:ce:c2:dd:12:06		<广播>	0.1	100.0	1	0	0	0	0	0	0	1	WEP
ba:6b:ff:84:79:cc		<广播>	0.1	100.0	1	0	1	0	0	0	0	0	
f7:1d:51:00:16:b6		<广播>	0.1	0.0	0	0	0	0	0	0	0	1	WEP
fb:15:87:3f:4e:36		<广播>	0.1	0.0	0	0	0	0	0	0	0	1	
ff:ff:ff:ff:ff:ff		phoiphas	0.1	0.0	0	0	0	1	0	0	0	0	

2.

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

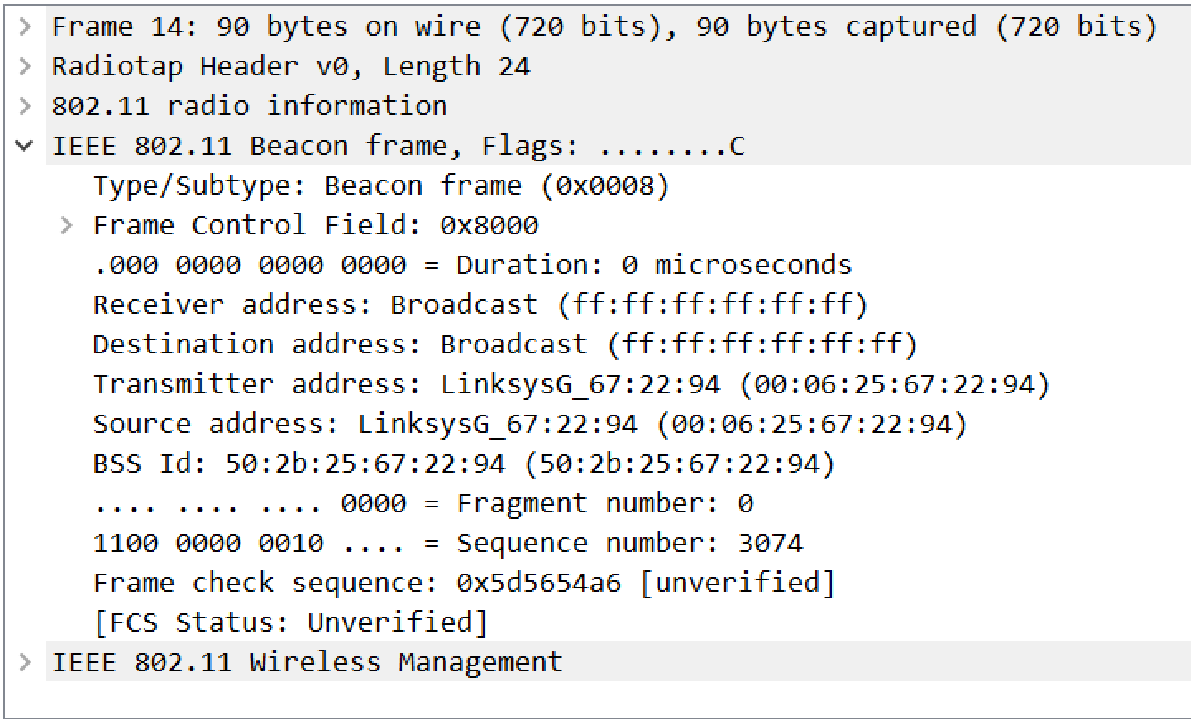
> 两个AP的信标帧中的三个地址分别是什么。

`30 Munroe St(00:16:b6:f7:1d:51)`如下图所示：



```
›  Frame 396: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
›  Radiotap Header v0, Length 24
›  802.11 radio information
⌄  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
      1100 0000 0010 .... = Sequence number: 3074
      Frame check sequence: 0xfed1f007 [unverified]
      [FCS Status: Unverified]
›  IEEE 802.11 Wireless Management
```

`linksys_ses_24086(00:06:25:67:22:94)`如下图所示：



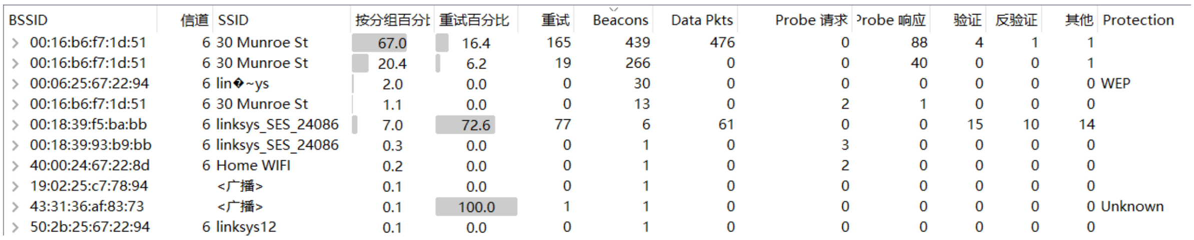
```
›  Frame 14: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
›  Radiotap Header v0, Length 24
›  802.11 radio information
⌄  IEEE 802.11 Beacon frame, Flags: ........C
      Type/Subtype: Beacon frame (0x0008)
   ›  Frame Control Field: 0x8000
      .000 0000 0000 0000 = Duration: 0 microseconds
      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: 50:2b:25:67:22:94 (50:2b:25:67:22:94)
      .... .... .... 0000 = Fragment number: 0
      1100 0000 0010 .... = Sequence number: 3074
      Frame check sequence: 0x5d5654a6 [unverified]
      [FCS Status: Unverified]
›  IEEE 802.11 Wireless Management
```

	Receiver Address	**Destination Address**	**Transmitter/source Address**
30 Munroe St (00:16:b6:f7:1d:51)	`ff:ff:ff:ff:ff:ff`	`ff:ff:ff:ff:ff:ff`	`00:16:b6:f7:1d:51`
lin�~ys (00:06:25:67:22:94)	`ff:ff:ff:ff:ff:ff`	`ff:ff:ff:ff:ff:ff`	`00:06:25:67:22:94`

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?

> 无线笔记本电脑从多少AP接收到信标帧？列出他们的MAC地址。为什么笔记本电脑可以从AP接收帧，即使它不与AP关联？



BSSID	信道	SSID	按分组百分l	重试百分比	重试	Beacons	Data Pkts	Probe 请求	›robe 响应	验证	反验证	其他	Protection
00:16:b6:f7:1d:51	6	30 Munroe St	67.0	16.4	165	439	476	0	88	4	1	1	
00:16:b6:f7:1d:51	6	30 Munroe St	20.4	6.2	19	266	0	0	40	0	0	1	
00:06:25:67:22:94	6	lin�~ys	2.0	0.0	0	30	0	0	0	0	0	0	WEP
00:16:b6:f7:1d:51	6	30 Munroe St	1.1	0.0	0	13	0	2	1	0	0	0	
00:18:39:f5:ba:bb	6	linksys_SES_24086	7.0	72.6	77	6	61	0	0	15	10	14	
00:18:39:93:b9:bb	6	linksys_SES_24086	0.3	0.0	0	1	0	3	0	0	0	0	
40:00:24:67:22:8d	6	Home WIFI	0.2	0.0	0	1	0	2	0	0	0	0	
19:02:25:c7:78:94		<广播>	0.1	0.0	0	1	0	0	0	0	0	0	
43:31:36:af:83:73		<广播>	0.1	100.0	1	1	0	0	0	0	0	0	Unknown
50:2b:25:67:22:94	6	linksys12	0.1	0.0	0	1	0	0	0	0	0	0	

如上图所示，电脑从如下几个`AP`收到`Beacon`，他们的`MAC`地址如下表所示：

SSID	MAC
`30 Munroe St`	00:16:b6:f7:1d:51
`lin�~ys`	00:06:25:67:22:94
`linksys_SES_24086`	00:18:39:f5:ba:bb
`linksys_SES_24086`	00:18:39:f5:b9:bb
`Home WIFI`	40:00:24:67:22:8d
`linksys12`	00:16:b6:f7:1d:51
`<广播>`	19:02:25:c7:78:94
`<广播>`	43:31:36:af:83:73

虽然没有与AP关联单仍可以收到帧的原因是

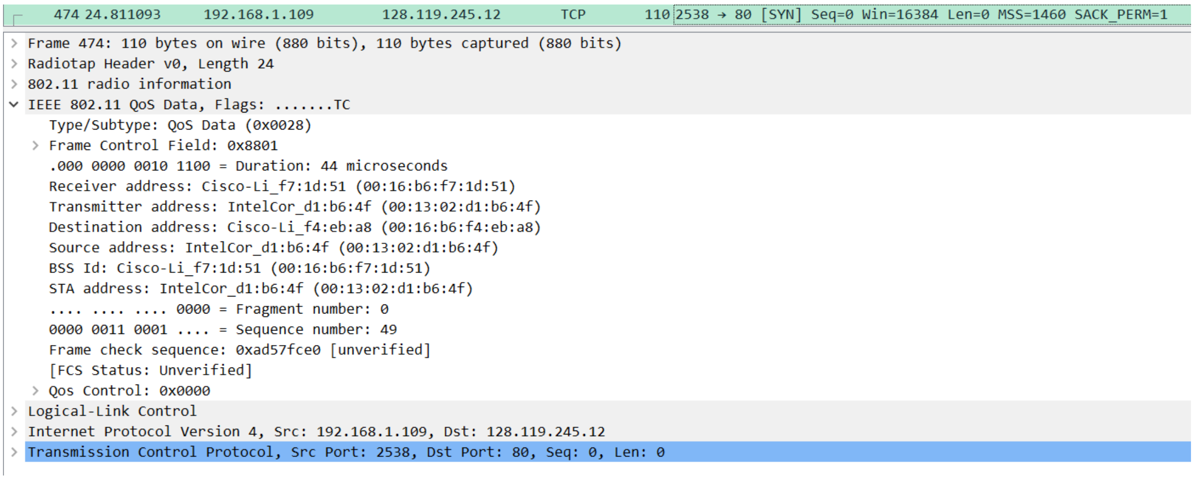
- 主机的被动扫描：AP周期性的发送信标帧（`Beacon frame`），主机接收之后选择一个AP，并向其发送关联请求帧
- 主机的主动扫描：主机广播探测请求帧，AP接收到之后发送探测响应帧。

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?

> 查找包含此第一个TCP会话（下载alice.txt）的SYN TCP段的802.11帧。帧中的三个MAC地址是什么，这是无线笔记本电脑/AP/第一跳路由器的地址？

如下图为包含第一个TCP会话（下载alice.txt）的SYN TCP段的802.11帧。



```
   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
> 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
```

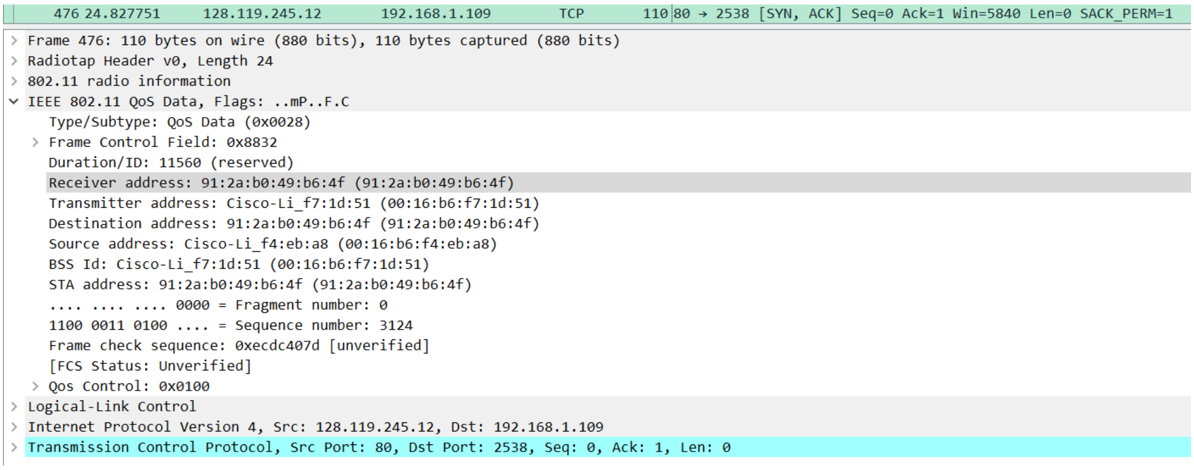
- Receiver address : `00:16:b6:f7:1d:51` -- AP
- Source /Transmitter address : `00:13:02:d1:b6:4f` -- wireless laptop
- Destination address : `00:16:b6:f4:eb:a8` -- first-hop rounter

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?

> 对于第一个TCP会话的SYN-ACK段，帧中的三个MAC地址是什么，无线笔记本电脑/AP/第一跳路由器的地址是什么?

如下图为第一个TCP会话的SYN-ACK段



```
   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
> 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
```

- Receiver/Destination address ： `91:2a:b0:49:b6:4f` -- wireless laptop
- Transmitter address ： `00:16:b6:f7:1d:51` -- AP
- Source address ： `00:16:b6:f4:eb:a8` -- first-hop router

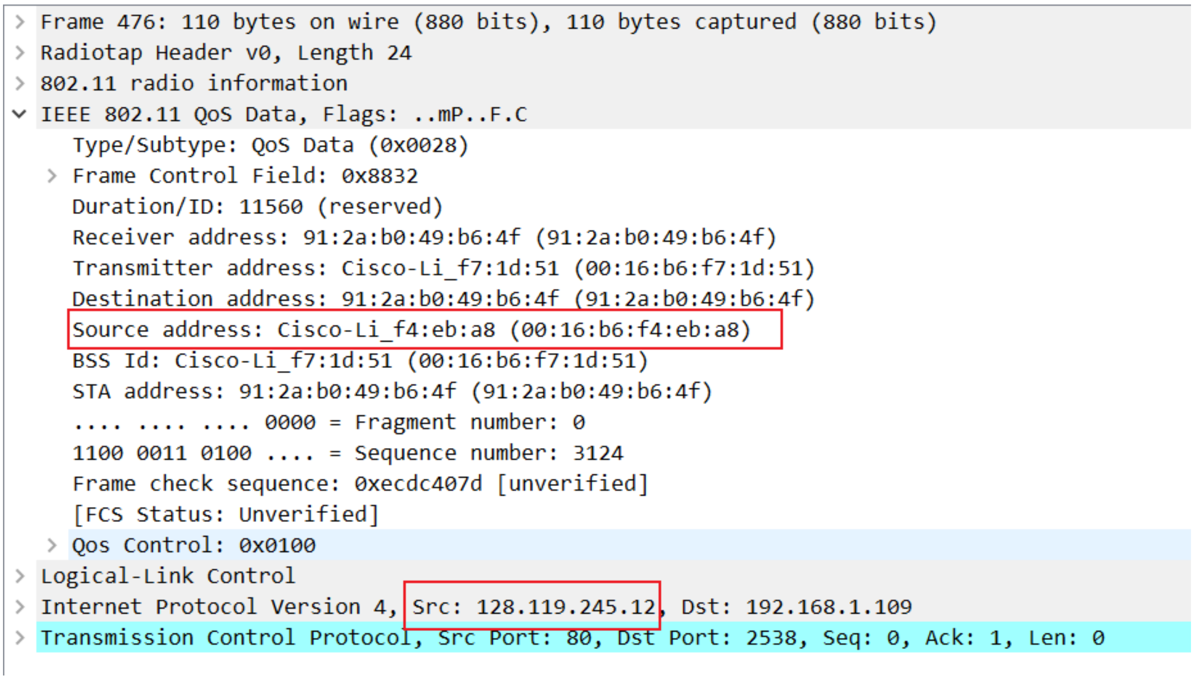
6.

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

> 对于上述SYN-ACK段，发送方MAC地址是否对应于web服务器的IP地址？为什么?

sender的MAC地址是`00:16:b6:f4:eb:a8`，Web服务器的IP地址是`128.119.245.12`，显然二者是没有对应关系的。

原因：服务器和 sender 不在同一个子网内部。



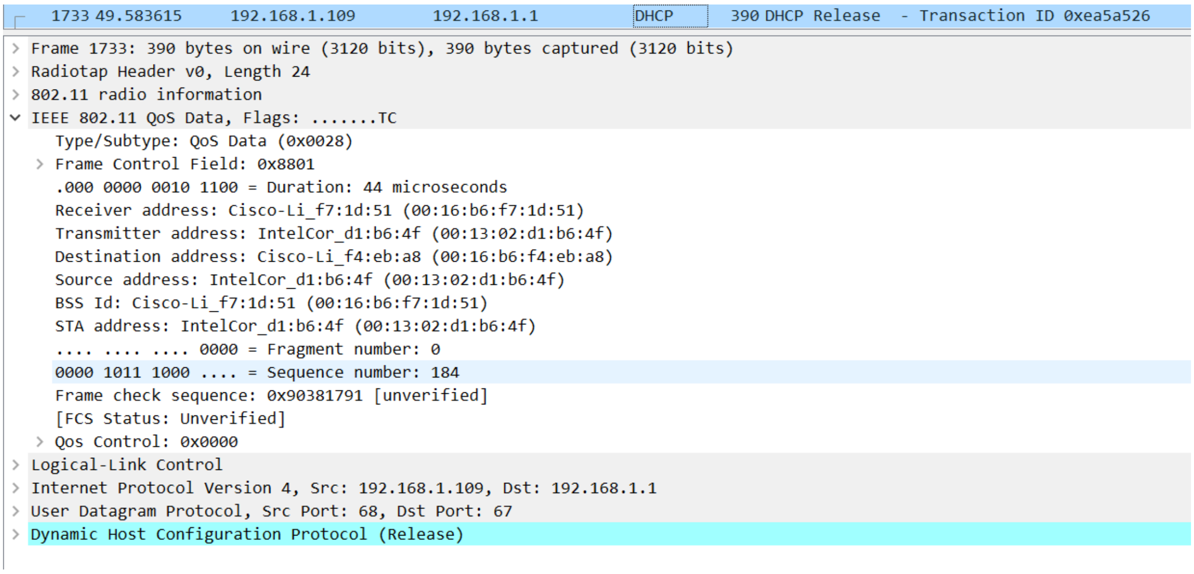
```
> Frame 476: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: ..mP..F.C
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8832
    Duration/ID: 11560 (reserved)
    Receiver address: 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
```

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?

> 在*t=49*之后，主机在跟踪中采取了哪两个操作（即发送帧），以结束与*30 Munroe St*AP的关联?

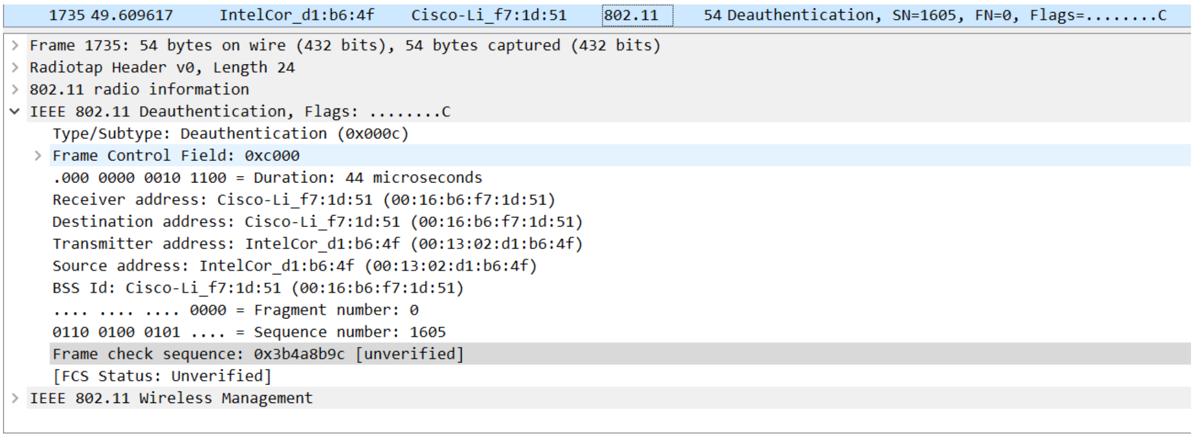
- 向 DHCP 服务器发送 release 以释放占用



```
  1733 49.583615    192.168.1.109    192.168.1.1    DHCP    390 DHCP Release  - Transaction ID 0xea5a526

> Frame 1733: 390 bytes on wire (3120 bits), 390 bytes captured (3120 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 1011 1000 .... = Sequence number: 184
    Frame check sequence: 0x90381791 [unverified]
    [FCS Status: Unverified]
  > Qos Control: 0x0000
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.1.109, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Release)
```

- 向AP发送了 Deauthentication解除认证



```
1735 49.609617     IntelCor_d1:b6:4f     Cisco-Li_f7:1d:51     802.11     54 Deauthentication, SN=1605, FN=0, Flags=........C
> Frame 1735: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Deauthentication, Flags: ........C
    Type/Subtype: Deauthentication (0x000c)
  > Frame Control Field: 0xc000
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    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)
    .... .... .... 0000 = Fragment number: 0
    0110 0100 0101 .... = Sequence number: 1605
    Frame check sequence: 0x3b4a8b9c [unverified]
    [FCS Status: Unverified]
> IEEE 802.11 Wireless Management
```

8.

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

> 你能捕捉到类似的痕迹吗？为什么？

Windows下无法直接用wireshark捕获802.11帧，原因是因为捕获802.11帧需要设置网卡为监控模式（即monitor mode，非混杂模式），但是可以使用microsoft network monitor，微软提供的一个免费检测工具来抓包。

具体的操作方法详见 Windows下捕获802.11数据包