计网实验3: 802.11

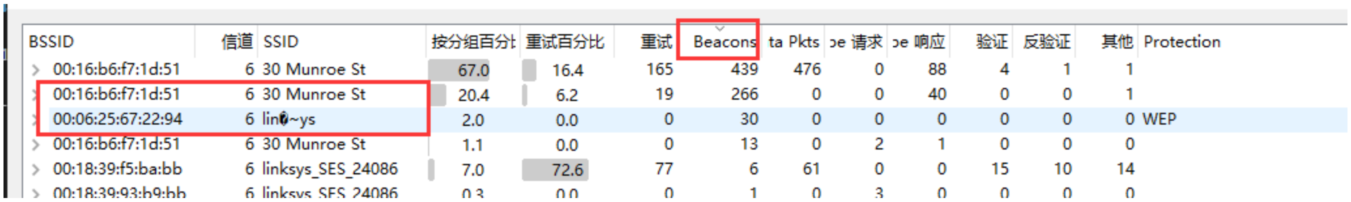
PB18111697 王章瀚

问题与回答

1.

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

主要是 `30 Munroe St(00:16:b6:f7:1d:51)` 和 `lin�~ys(00:06:25:67:22:94)`
这可以由 wireshark 的按 beacons 排序功能找出:



BSSID	信道	SSID	按分组百分比	重试百分比	重试	Beacons	ta Pkts	ɔe 请求	ɔe 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	

2.

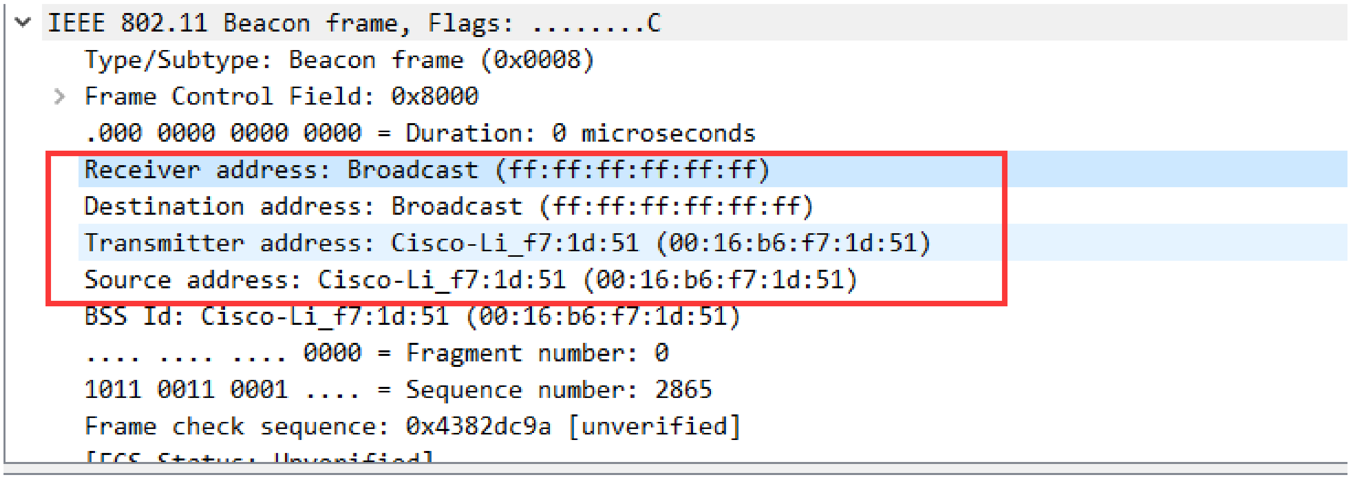
> What are the three addresses in the Beacon frame from the two APs respectively.

可以列表如下:

	30 Munroe St (00:16:b6:f7:1d:51)	**linksys_SES_24086 (00:06:25:67:22:94)**
Receiver Address	ff:ff:ff:ff:ff:ff	ff:ff:ff:ff:ff:ff
Destination Address	ff:ff:ff:ff:ff:ff	ff:ff:ff:ff:ff:ff
Transmitter/source Address	00:16:b6:f7:1d:51	00:06:25:67:22:94

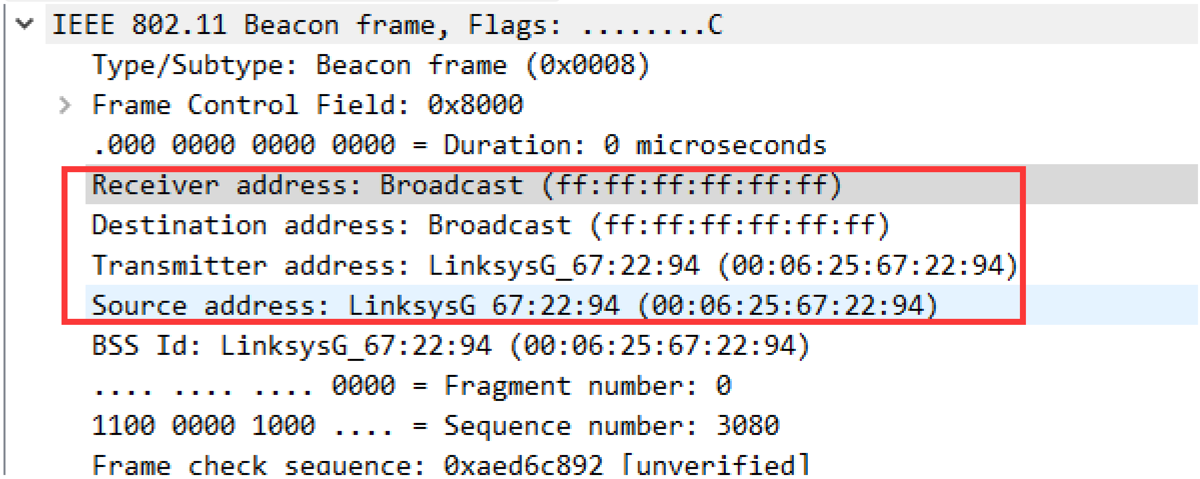
相应截图:

`30 Munroe St(00:16:b6:f7:1d:51)` 的对应下图:



```
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 0011 0001 .... = Sequence number: 2865
    Frame check sequence: 0x4382dc9a [unverified]
    [FCS Status: Unverified]
```

`linksys_SES_24086(00:06:25:67:22:94)` 的对应下图:

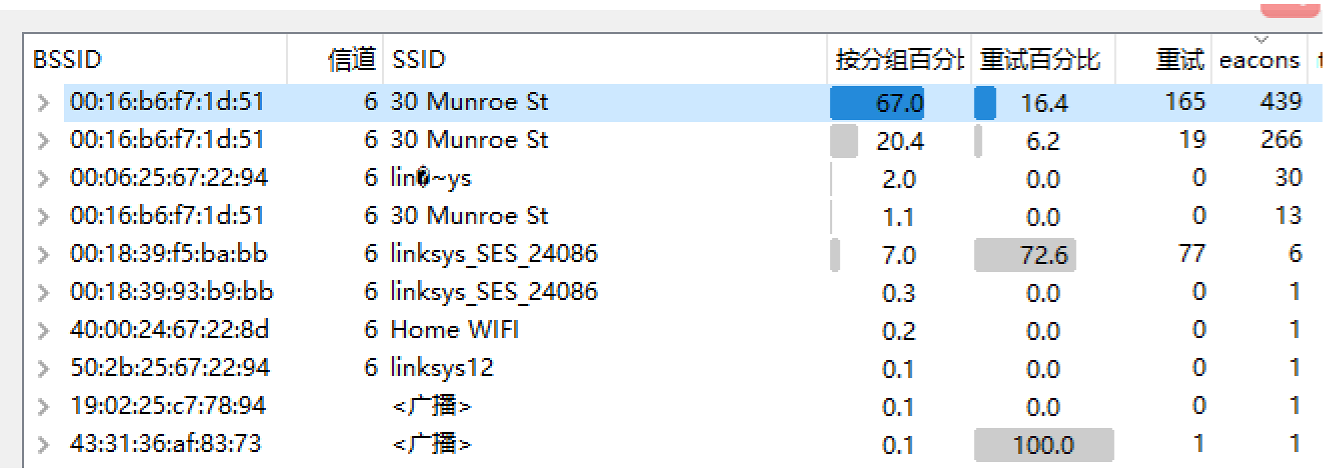


```
v IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  > Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: 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 1000 .... = Sequence number: 3080
    Frame check sequence: 0xaed6c892 [unverified]
```

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?

如下图所示, 根据下表可以看出来,



BSSID	信道	SSID	按分组百分比	重试百分比	重试	eacons
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
40:00:24:67:22:8d	6	Home WIFI	0.2	0.0	0	1
50:2b:25:67:22:94	6	linksys12	0.1	0.0	0	1
19:02:25:c7:78:94		<广播>	0.1	0.0	0	1
43:31:36:af:83:73		<广播>	0.1	100.0	1	1

主要的 AP 共有 8 个, 如下所示:

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

之所以可以收到来自没连接上的 AP 的 frames, 主要有主动和被动两种原因.

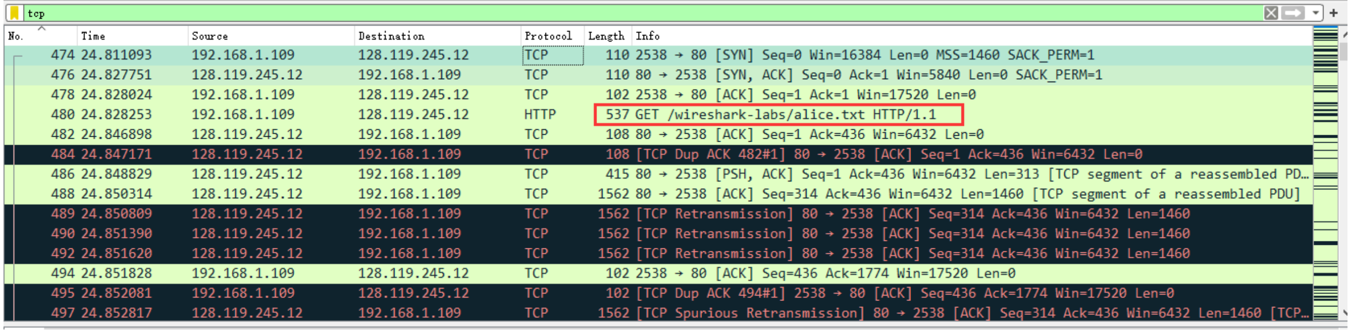
- 被动方面: 是因为 "802.11 标准要求每个 AP 周期性地发送信标帧(beacon frame)".
- 主动方面: 无线主机也可以执行主动扫描, 通过向位于无线主机范围内的所有 AP 广播探测帧完成.

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

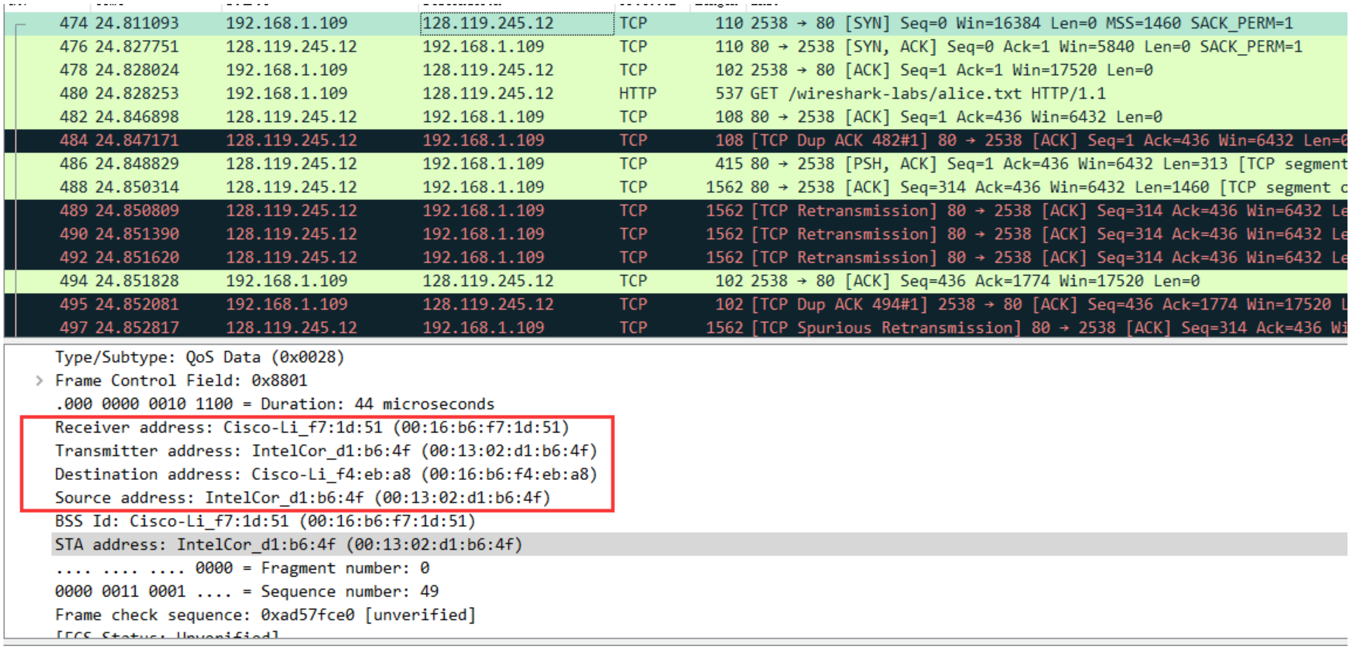
> address for wireless laptop / AP / first-hop router?

如下图所示即为一个 GET 的 http 请求来请求 `alice.txt` 文件.



```
tcp
No.   Time       Source          Destination     Protocol Length Info
  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
  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
  478 24.828024  192.168.1.109   128.119.245.12  TCP       102 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
  480 24.828253  192.168.1.109   128.119.245.12  HTTP      537 GET /wireshark-labs/alice.txt HTTP/1.1
  482 24.846898  128.119.245.12  192.168.1.109   TCP       108 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
  484 24.847171  128.119.245.12  192.168.1.109   TCP       108 [TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
  486 24.848829  128.119.245.12  192.168.1.109   TCP       415 80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP segment of a reassembled PD…
  488 24.850314  128.119.245.12  192.168.1.109   TCP      1562 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
  489 24.850809  128.119.245.12  192.168.1.109   TCP      1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460
  490 24.851390  128.119.245.12  192.168.1.109   TCP      1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460
  492 24.851620  128.119.245.12  192.168.1.109   TCP      1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460
  494 24.851828  192.168.1.109   128.119.245.12  TCP       102 2538 → 80 [ACK] Seq=436 Ack=1774 Win=17520 Len=0
  495 24.852081  192.168.1.109   128.119.245.12  TCP       102 [TCP Dup ACK 494#1] 2538 → 80 [ACK] Seq=436 Ack=1774 Win=17520 Len=0
  497 24.852817  128.119.245.12  192.168.1.109   TCP      1562 [TCP Spurious Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP…
```

对应的第一个 TCP session 的 SYN TCP segment 应该是 No.474 这一个报文. 如下图所示:



```
  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
  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
  478 24.828024  192.168.1.109   128.119.245.12  TCP       102 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
  480 24.828253  192.168.1.109   128.119.245.12  HTTP      537 GET /wireshark-labs/alice.txt HTTP/1.1
  482 24.846898  128.119.245.12  192.168.1.109   TCP       108 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
  484 24.847171  128.119.245.12  192.168.1.109   TCP       108 [TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
  486 24.848829  128.119.245.12  192.168.1.109   TCP       415 80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP segment
  488 24.850314  128.119.245.12  192.168.1.109   TCP      1562 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment c
  489 24.850809  128.119.245.12  192.168.1.109   TCP      1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Le
  490 24.851390  128.119.245.12  192.168.1.109   TCP      1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Le
  492 24.851620  128.119.245.12  192.168.1.109   TCP      1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Le
  494 24.851828  192.168.1.109   128.119.245.12  TCP       102 2538 → 80 [ACK] Seq=436 Ack=1774 Win=17520 Len=0
  495 24.852081  192.168.1.109   128.119.245.12  TCP       102 [TCP Dup ACK 494#1] 2538 → 80 [ACK] Seq=436 Ack=1774 Win=17520 L
  497 24.852817  128.119.245.12  192.168.1.109   TCP      1562 [TCP Spurious Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Wi

    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]
```

因此我们可以知道, 三个对应的 MAC address 为

Receiver address -- 00:16:b6:f7:1d:51 -- AP

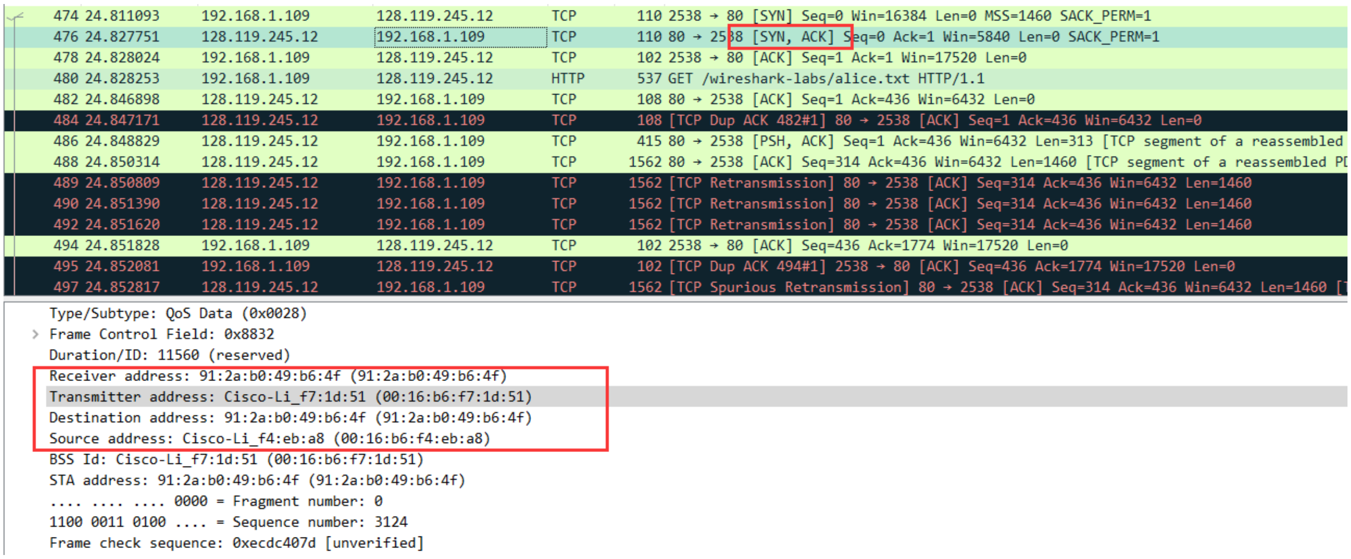
Source address -- 00:13:02:d1:b6:4f -- wireless laptop

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?

如下图所示, 第 476 号 segment 即所要查找的.



```
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
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
478 24.828024   192.168.1.109    128.119.245.12   TCP    102 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
480 24.828253   192.168.1.109    128.119.245.12   HTTP   537 GET /wireshark-labs/alice.txt HTTP/1.1
482 24.846898   128.119.245.12   192.168.1.109    TCP    108 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
484 24.847171   128.119.245.12   192.168.1.109    TCP    108 [TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
486 24.848829   128.119.245.12   192.168.1.109    TCP    415 80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP segment of a reassembled
488 24.850314   128.119.245.12   192.168.1.109    TCP   1562 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PD
489 24.850809   128.119.245.12   192.168.1.109    TCP   1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460
490 24.851390   128.119.245.12   192.168.1.109    TCP   1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460
492 24.851620   128.119.245.12   192.168.1.109    TCP   1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460
494 24.851828   192.168.1.109    128.119.245.12   TCP    102 2538 → 80 [ACK] Seq=436 Ack=1774 Win=17520 Len=0
495 24.852081   192.168.1.109    128.119.245.12   TCP    102 [TCP Dup ACK 494#1] 2538 → 80 [ACK] Seq=436 Ack=1774 Win=17520 Len=0
497 24.852817   128.119.245.12   192.168.1.109    TCP   1562 [TCP Spurious Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [
```

```
  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]
```

其中有:

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

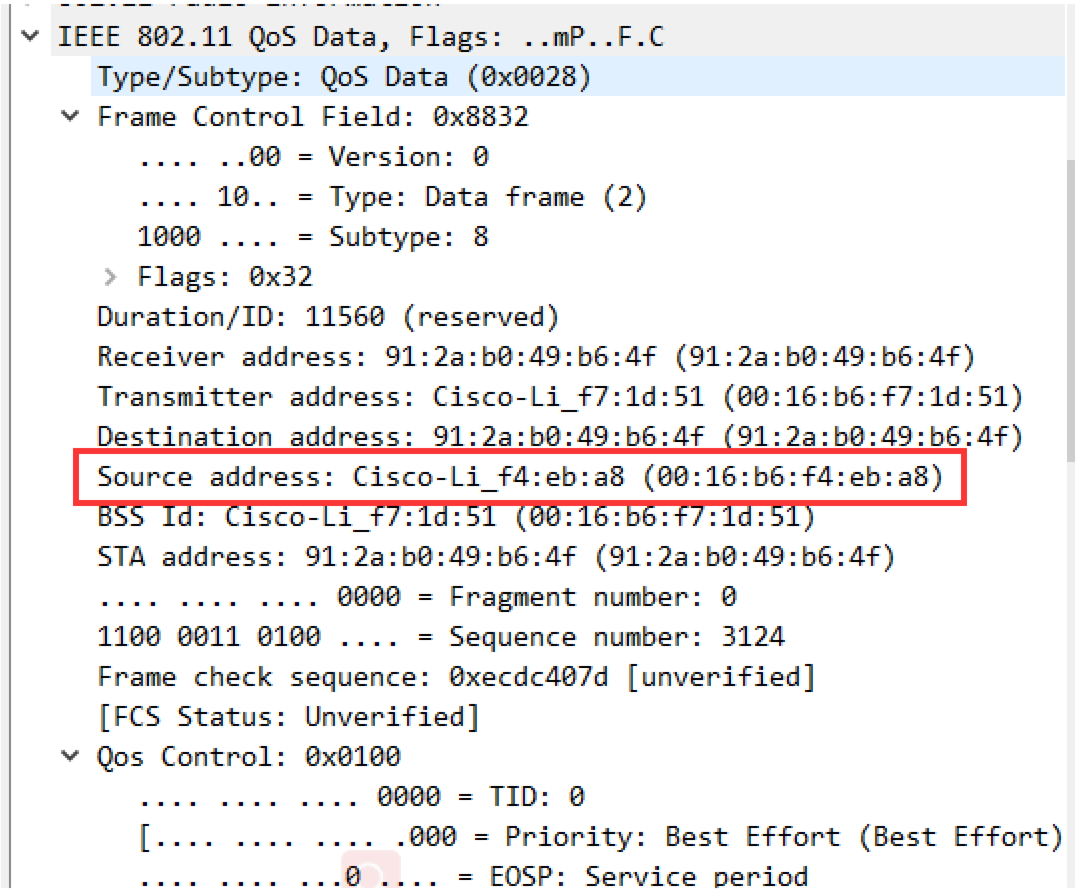
Transmitter address -- 00:16:b6:f7:1d:51 -- AP

Source address -- 00:16:b6:f4:eb:a8 -- first-hop router

6.

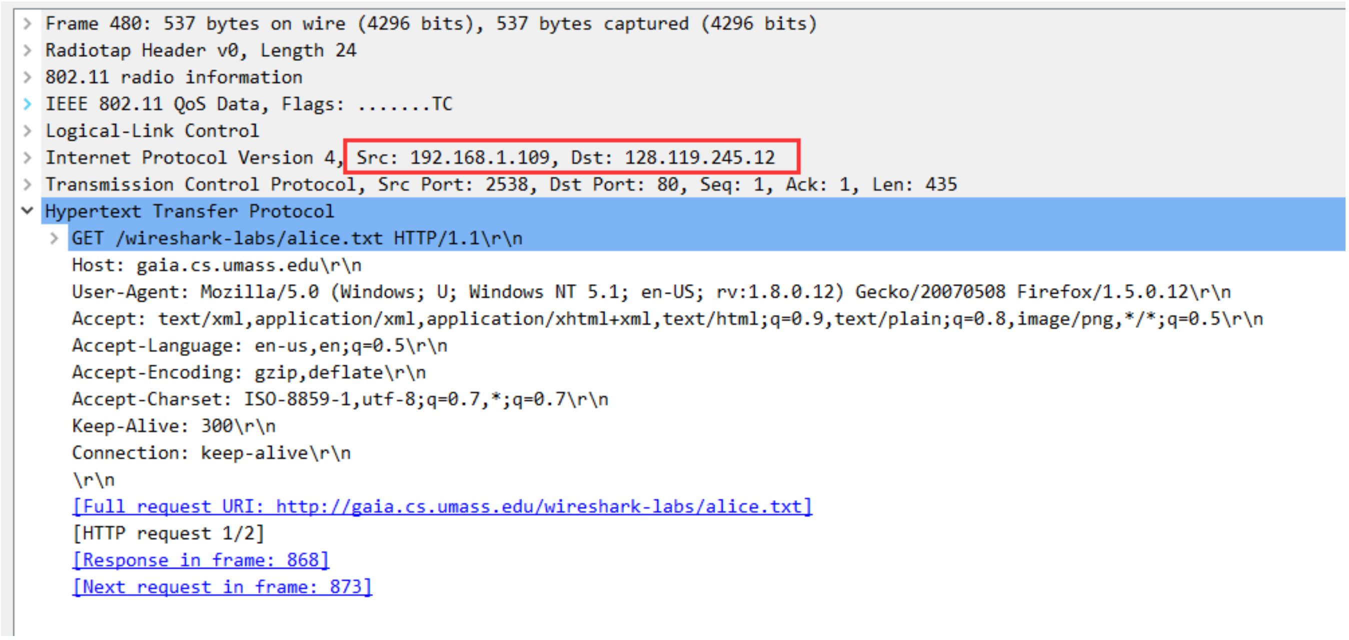
> For the above mentioned SYN-ACK segment, is the sender MAC address corresponds to the web server's IP address? Why?

sender 的 MAC 可从下图得知为 `00:16:b6:f4:eb:a8`



```
IEEE 802.11 QoS Data, Flags: ..mP..F.C
  Type/Subtype: QoS Data (0x0028)
  Frame Control Field: 0x8832
    .... ..00 = Version: 0
    .... 10.. = Type: Data frame (2)
    1000 .... = Subtype: 8
    Flags: 0x32
  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
    .... .... .... 0000 = TID: 0
    [.... .... .... .000 = Priority: Best Effort (Best Effort)
    .... .... ...0 .... = EOSP: Service period
```

web server 的 IP 从下图得知为 `128.119.245.12`



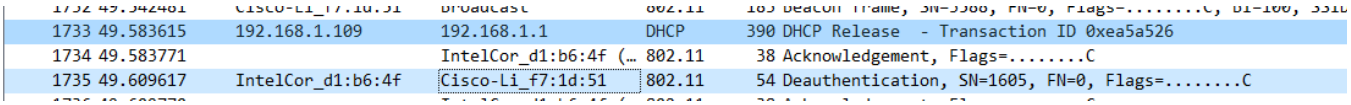
```
Frame 480: 537 bytes on wire (4296 bits), 537 bytes captured (4296 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 QoS Data, Flags: .......TC
Logical-Link Control
Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 2538, Dst Port: 80, Seq: 1, Ack: 1, Len: 435
Hypertext Transfer Protocol
  GET /wireshark-labs/alice.txt HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.12) Gecko/20070508 Firefox/1.5.0.12\r\n
  Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5\r\n
  Accept-Language: en-us,en;q=0.5\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
  Keep-Alive: 300\r\n
  Connection: keep-alive\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/alice.txt]
  [HTTP request 1/2]
  [Response in frame: 868]
  [Next request in frame: 873]
```

这显然不是相对应的. 因为服务器和 sender 不在同一个子网内部, 所以 sender 的 MAC 地址取决于它子网的情况, 如下一跳路由器的 MAC 地址. 当跨越子网的时候, 对应 MAC 地址会发生改变.

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?

观察到下图两个蓝色的 frames. 第一个是向 DHCP 服务器发送 release 以释放占用. 第二个是向主机发送了 Deauthentication.



```
1732 49.542481   Cisco-Li_f7:1d:51   Broadcast            802.11   183 Beacon frame, SN=3588, FN=0, Flags=........C, BI=100, SSID
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
```

8.

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

可以. 我们只需要在在相应的时刻, 按上面的操作步骤向相同的 AP 和 WebServer 发送相同的请求就可以完成.

但我们也需要相应的设备:

> 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