Sheng Wang

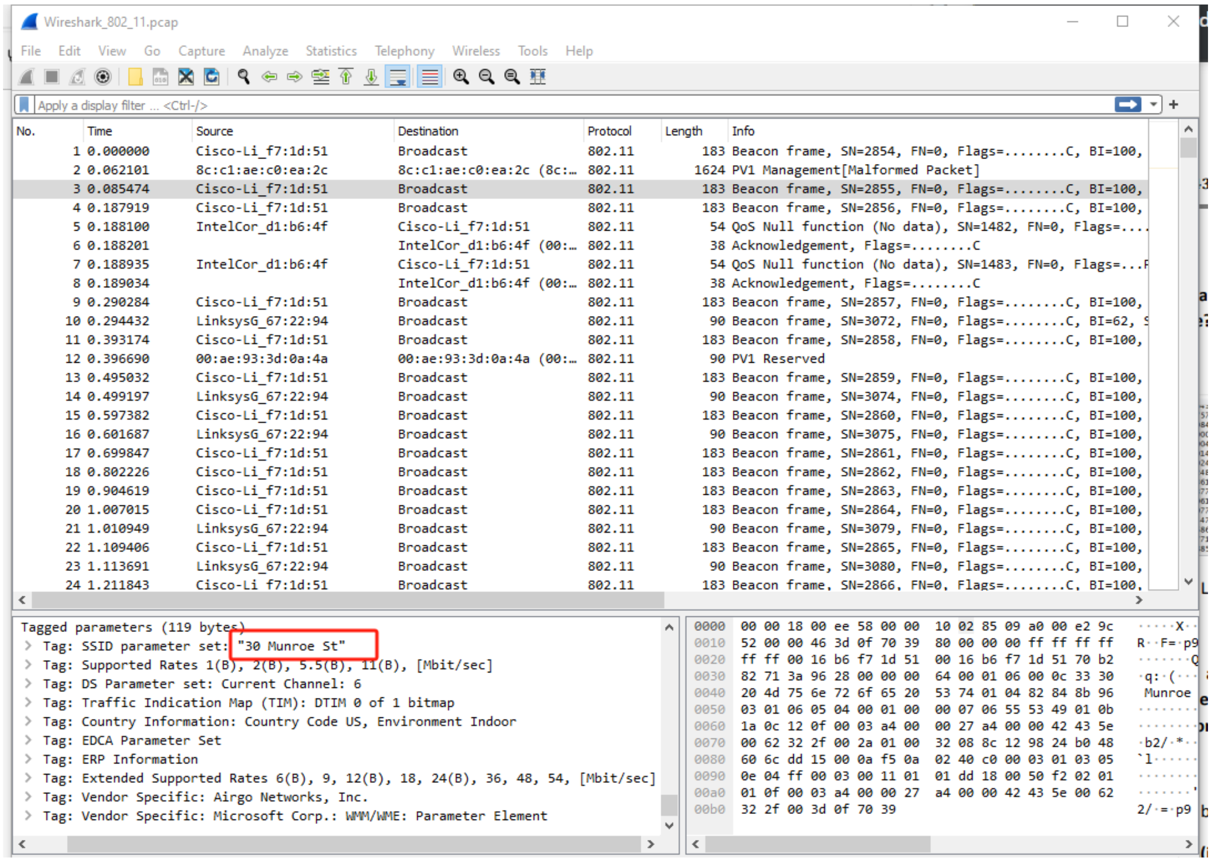
Wireshark-802.11 Lab 3

EE450

Abstract

In this lab, The WiFi protocol 802.11 will be researched within the wireshark. The host will connect the wifi and visit the website. The process of connecting and transmitting between access point and host will be shown below.

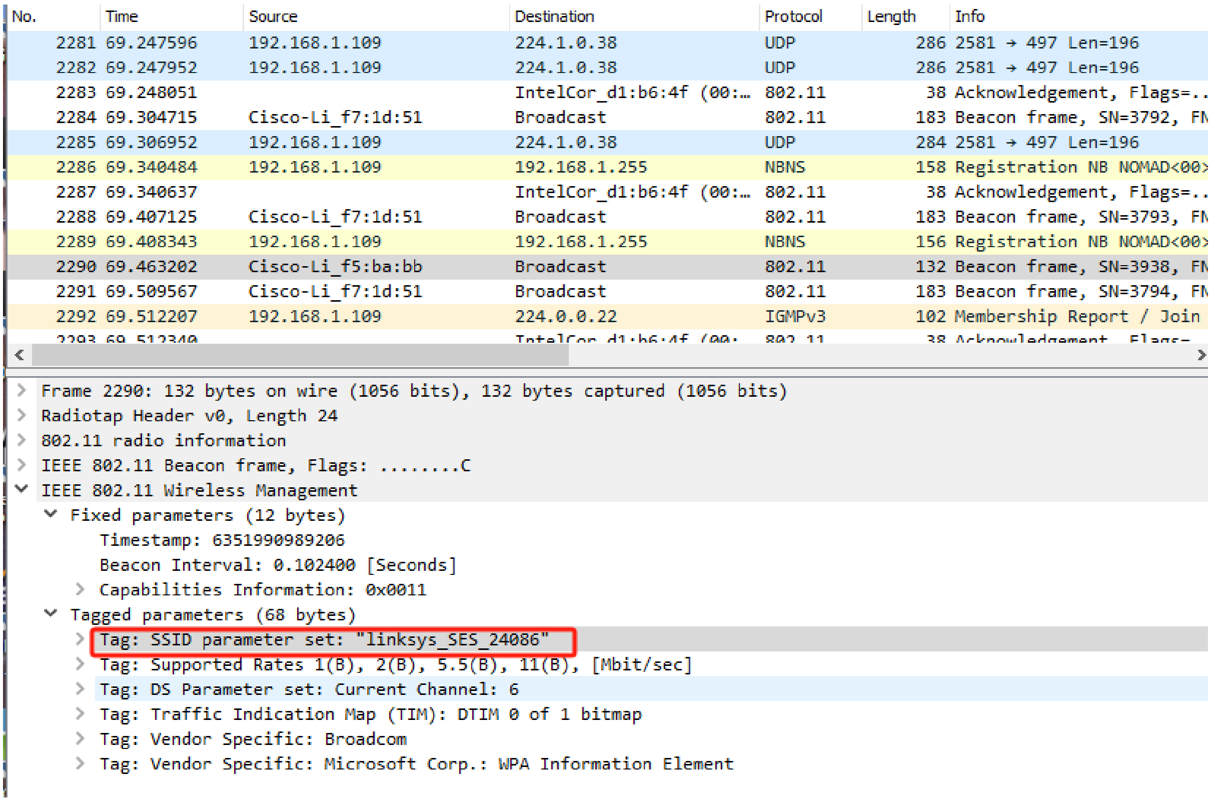
1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?



```
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,
    2 0.062101  8c:c1:ae:c0:ea:2c   8c:c1:ae:c0:ea:2c (8c:… 802.11    1624 PV1 Management[Malformed Packet]
    3 0.085474  Cisco-Li_f7:1d:51   Broadcast               802.11     183 Beacon frame, SN=2855, FN=0, Flags=........C, BI=100,
    4 0.187919  Cisco-Li_f7:1d:51   Broadcast               802.11     183 Beacon frame, SN=2856, FN=0, Flags=........C, BI=100,
    5 0.188100  IntelCor_d1:b6:4f   Cisco-Li_f7:1d:51       802.11      54 QoS Null function (No data), SN=1482, FN=0, Flags=....
    6 0.188201                      IntelCor_d1:b6:4f (00:… 802.11      38 Acknowledgement, Flags=........C
    7 0.188935  IntelCor_d1:b6:4f   Cisco-Li_f7:1d:51       802.11      54 QoS Null function (No data), SN=1483, FN=0, Flags=...F
    8 0.189034                      IntelCor_d1:b6:4f (00:… 802.11      38 Acknowledgement, Flags=........C
    9 0.290284  Cisco-Li_f7:1d:51   Broadcast               802.11     183 Beacon frame, SN=2857, FN=0, Flags=........C, BI=100,
   10 0.294432  LinksysG_67:22:94   Broadcast               802.11      90 Beacon frame, SN=3072, FN=0, Flags=........C, BI=62, S
   11 0.393174  Cisco-Li_f7:1d:51   Broadcast               802.11     183 Beacon frame, SN=2858, FN=0, Flags=........C, BI=100,
   12 0.396690  00:ae:93:3d:0a:4a   00:ae:93:3d:0a:4a (00:… 802.11      90 PV1 Reserved
   13 0.495032  Cisco-Li_f7:1d:51   Broadcast               802.11     183 Beacon frame, SN=2859, FN=0, Flags=........C, BI=100,
   14 0.499197  LinksysG_67:22:94   Broadcast               802.11      90 Beacon frame, SN=3074, FN=0, Flags=........C, BI=100,
   15 0.597382  Cisco-Li_f7:1d:51   Broadcast               802.11     183 Beacon frame, SN=2860, FN=0, Flags=........C, BI=100,
   16 0.601687  LinksysG_67:22:94   Broadcast               802.11      90 Beacon frame, SN=3075, FN=0, Flags=........C, BI=100,
   17 0.699847  Cisco-Li_f7:1d:51   Broadcast               802.11     183 Beacon frame, SN=2861, FN=0, Flags=........C, BI=100,
   18 0.802226  Cisco-Li_f7:1d:51   Broadcast               802.11     183 Beacon frame, SN=2862, FN=0, Flags=........C, BI=100,
   19 0.904619  Cisco-Li_f7:1d:51   Broadcast               802.11     183 Beacon frame, SN=2863, FN=0, Flags=........C, BI=100,
   20 1.007015  Cisco-Li_f7:1d:51   Broadcast               802.11     183 Beacon frame, SN=2864, FN=0, Flags=........C, BI=100,
   21 1.010949  LinksysG_67:22:94   Broadcast               802.11      90 Beacon frame, SN=3079, FN=0, Flags=........C, BI=100,
   22 1.109406  Cisco-Li_f7:1d:51   Broadcast               802.11     183 Beacon frame, SN=2865, FN=0, Flags=........C, BI=100,
   23 1.113691  LinksysG_67:22:94   Broadcast               802.11      90 Beacon frame, SN=3080, FN=0, Flags=........C, BI=100,
   24 1.211843  Cisco-Li_f7:1d:51   Broadcast               802.11     183 Beacon frame, SN=2866, FN=0, Flags=........C, BI=100,
```

```
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]
 > Tag: DS Parameter set: Current Channel: 6
 > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
 > Tag: Country Information: Country Code US, Environment Indoor
 > Tag: EDCA Parameter Set
 > Tag: ERP Information
 > Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
 > Tag: Vendor Specific: Airgo Networks, Inc.
 > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e2 9c   ·····X··
0010  52 00 00 46 3d 0f 70 39  80 00 00 00 ff ff ff ff   R··F=·p9
0020  ff ff 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 70 b2   ·······Q
0030  82 71 3a 96 28 00 00 00  64 00 01 06 00 0c 33 30   ·q:·(···
0040  20 4d 75 6e 72 6f 65 20  53 74 01 04 82 84 8b 96    Munroe
0050  03 01 06 05 04 00 01 00  00 07 06 55 53 49 01 0b   ········
0060  1a 0c 12 0f 00 03 a4 00  00 27 a4 00 00 42 43 5e   ········
0070  00 62 32 2f 00 2a 01 00  32 08 8c 12 98 24 b0 48   ·b2/·*··
0080  60 6c dd 15 00 0a f5 0a  02 40 c0 00 03 01 03 05   `l······
0090  0e 04 ff 00 03 00 11 01  01 dd 18 00 50 f2 02 01   ········
00a0  01 0f 00 03 a4 00 00 27  a4 00 00 42 43 5e 00 62   ·······'
00b0  32 2f 00 3d 0f 70 39                               2/·=·p9
```

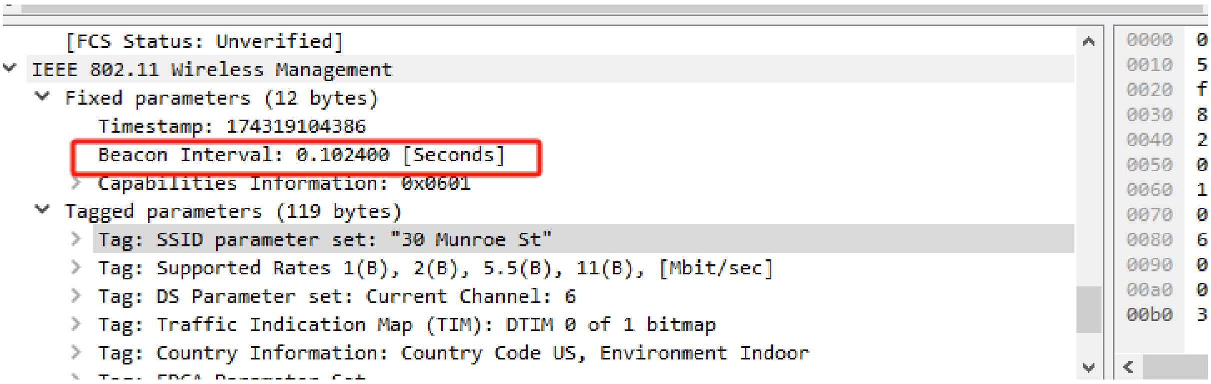


```
No.     Time        Source              Destination              Protocol  Length  Info
   2281 69.247596   192.168.1.109       224.1.0.38               UDP          286  2581 → 497 Len=196
   2282 69.247952   192.168.1.109       224.1.0.38               UDP          286  2581 → 497 Len=196
   2283 69.248051                       IntelCor_d1:b6:4f (00:…  802.11        38  Acknowledgement, Flags=..
   2284 69.304715   Cisco-Li_f7:1d:51   Broadcast                802.11       183  Beacon frame, SN=3792, FN
   2285 69.306952   192.168.1.109       224.1.0.38               UDP          284  2581 → 497 Len=196
   2286 69.340484   192.168.1.109       192.168.1.255            NBNS         158  Registration NB NOMAD<00>
   2287 69.340637                       IntelCor_d1:b6:4f (00:…  802.11        38  Acknowledgement, Flags=..
   2288 69.407125   Cisco-Li_f7:1d:51   Broadcast                802.11       183  Beacon frame, SN=3793, FN
   2289 69.408343   192.168.1.109       192.168.1.255            NBNS         156  Registration NB NOMAD<00>
   2290 69.463202   Cisco-Li_f5:ba:bb   Broadcast                802.11       132  Beacon frame, SN=3938, FN
   2291 69.509567   Cisco-Li_f7:1d:51   Broadcast                802.11       183  Beacon frame, SN=3794, FN
   2292 69.512207   192.168.1.109       224.0.0.22               IGMPv3       102  Membership Report / Join
   2293 69.512340                       IntelCor_d1:b6:4f (00:…  802.11        38  Acknowledgement, Flags=.
```

```
> Frame 2290: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  v Fixed parameters (12 bytes)
      Timestamp: 6351990989206
      Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x0011
  v Tagged parameters (68 bytes)
    > Tag: SSID parameter set: "linksys_SES_24086"
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 6
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: Vendor Specific: Broadcom
    > Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
```

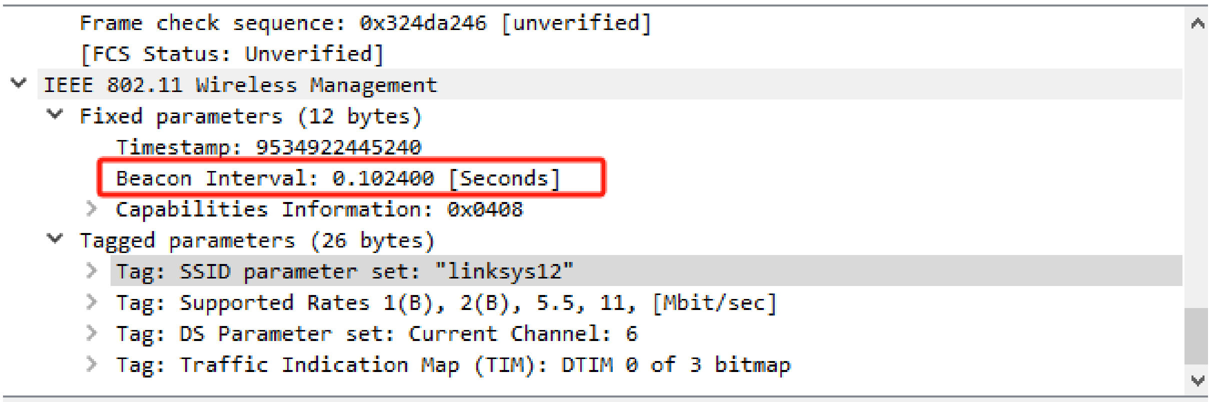
“30 Munroe St” and "linksys_SES_24086"

2. What are the intervals of time between the transmissions of the beacon frames the linksys_ses_24086 access point? From the 30 Munroe St. access point? (Hint: this interval of time is contained in the beacon frame itself)



```
      [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
  v Fixed parameters (12 bytes)
      Timestamp: 174319104386
      Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x0601
  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]
    > Tag: DS Parameter set: Current Channel: 6
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment Indoor
```

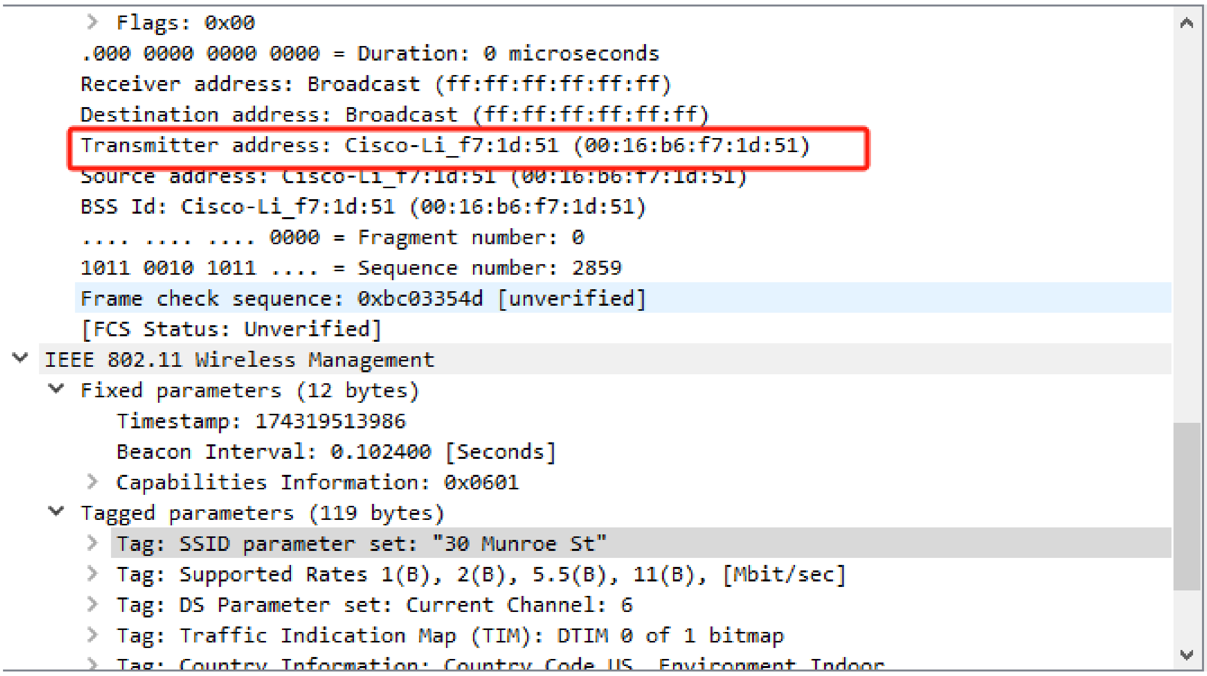
```
0000  0
0010  5
0020  f
0030  8
0040  2
0050  0
0060  1
0070  0
0080  6
0090  0
00a0  0
00b0  3
```



```
    Frame check sequence: 0x324da246 [unverified]
    [FCS Status: Unverified]
IEEE 802.11 Wireless Management
    Fixed parameters (12 bytes)
        Timestamp: 9534922445240
        Beacon Interval: 0.102400 [Seconds]
        Capabilities Information: 0x0408
    Tagged parameters (26 bytes)
        Tag: SSID parameter set: "linksys12"
        Tag: Supported Rates 1(B), 2(B), 5.5, 11, [Mbit/sec]
        Tag: DS Parameter set: Current Channel: 6
        Tag: Traffic Indication Map (TIM): DTIM 0 of 3 bitmap
```

Both of them are 0.1024 seconds

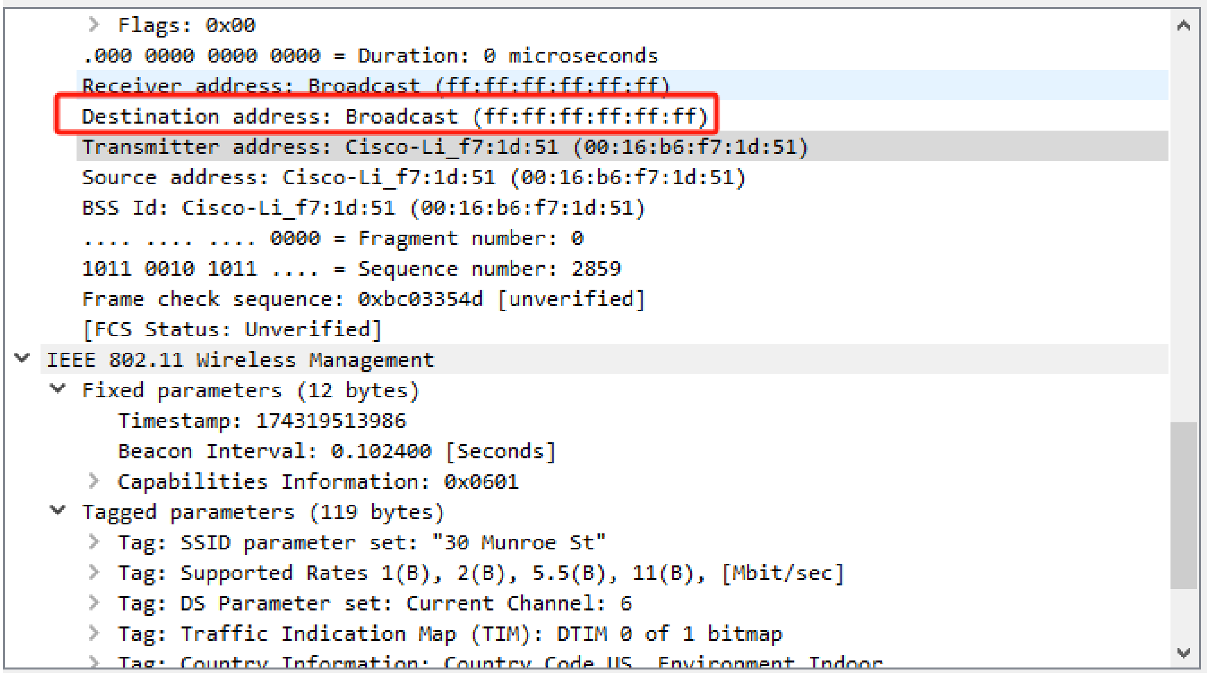
3. What (in hexadecimal notation) is the source MAC address on the beacon frame from 30 Munroe St? Recall from Figure 7.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE 802.11 standards document (cited above).



```
     > Flags: 0x00
       .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 1011 .... = Sequence number: 2859
       Frame check sequence: 0xbc03354d [unverified]
       [FCS Status: Unverified]
 v IEEE 802.11 Wireless Management
   v Fixed parameters (12 bytes)
         Timestamp: 174319513986
         Beacon Interval: 0.102400 [Seconds]
     > Capabilities Information: 0x0601
   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]
     > Tag: DS Parameter set: Current Channel: 6
     > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
     > Tag: Country Information: Country Code US, Environment Indoor
```

The source MAC address is 00:16:b6:f7:1d:51

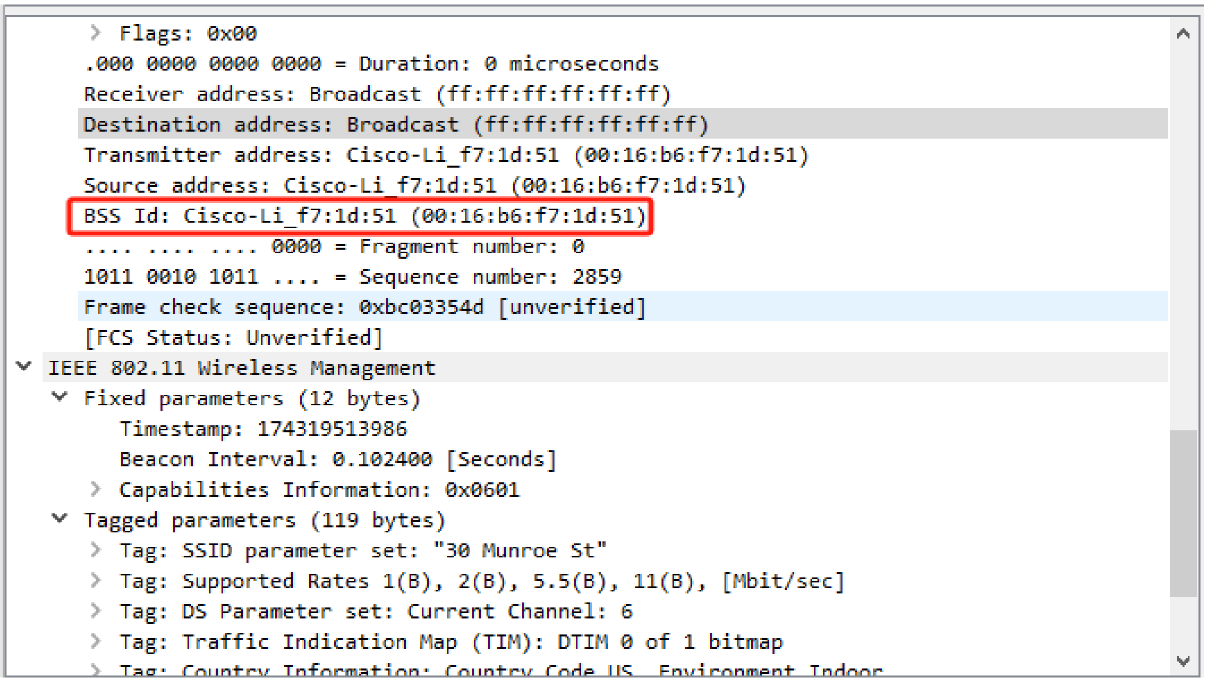
4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St??



```
    > Flags: 0x00
      .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 1011 .... = Sequence number: 2859
      Frame check sequence: 0xbc03354d [unverified]
      [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
  v Fixed parameters (12 bytes)
        Timestamp: 174319513986
        Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x0601
  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]
    > Tag: DS Parameter set: Current Channel: 6
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment Indoor
```

Destination MAC address is ff:ff:ff:ff:ff:ff

5. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from 30 Munroe St?

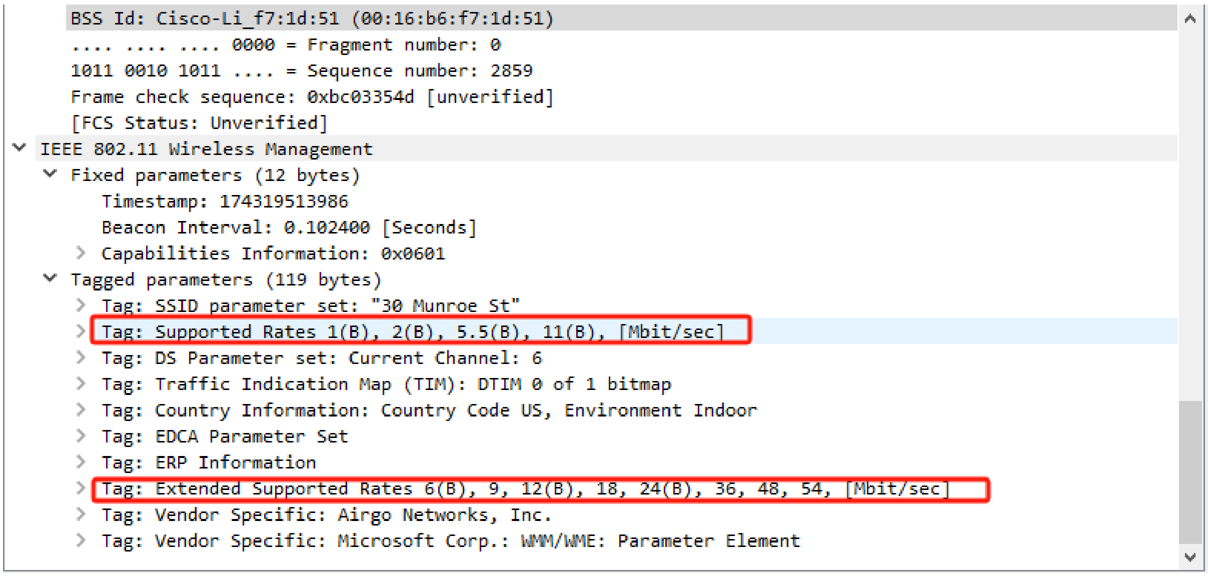


```
      > Flags: 0x00
      .000 0000 0000 0000 = Duration: 0 microseconds
      Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
      Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
      Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
      Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
      BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
      .... .... .... 0000 = Fragment number: 0
      1011 0010 1011 .... = Sequence number: 2859
      Frame check sequence: 0xbc03354d [unverified]
      [FCS Status: Unverified]
  v IEEE 802.11 Wireless Management
    v Fixed parameters (12 bytes)
        Timestamp: 174319513986
        Beacon Interval: 0.102400 [Seconds]
      > Capabilities Information: 0x0601
    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]
      > Tag: DS Parameter set: Current Channel: 6
      > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
      > Tag: Country Information: Country Code US, Environment Indoor
```

BSS Id is 00:16:b6:f7:1d:51

6. The beacon frames from the 30 Munroe St access point advertise that the access point

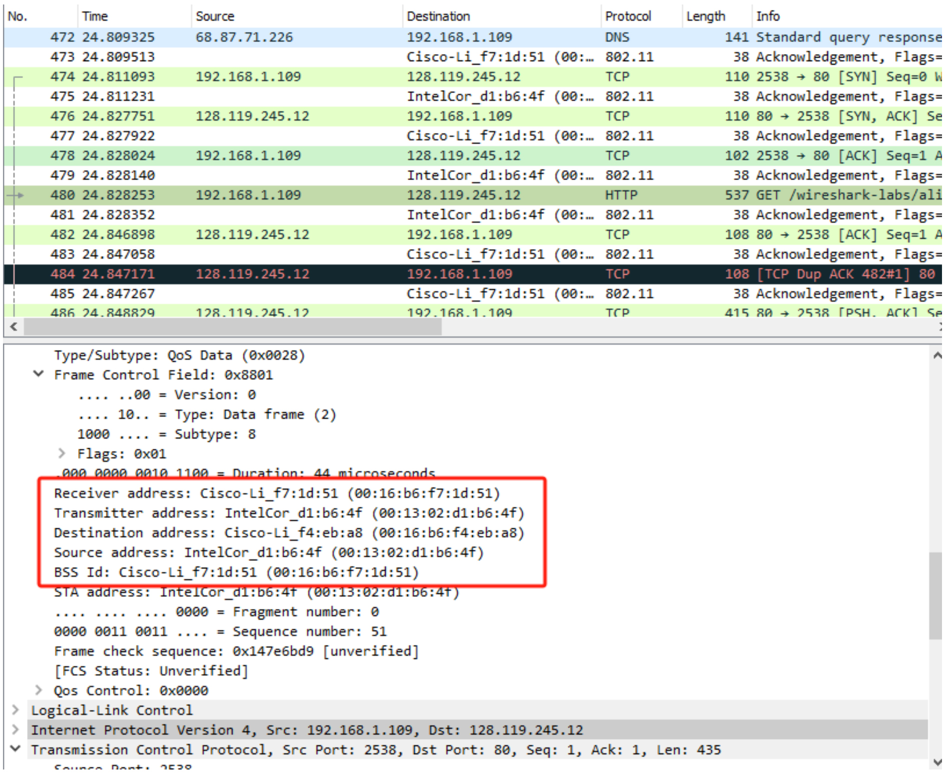
can support four data rates and eight additional “extended supported rates.” What are these rates?



```
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    .... .... .... 0000 = Fragment number: 0
    1011 0010 1011 .... = Sequence number: 2859
    Frame check sequence: 0xbc03354d [unverified]
    [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
  v Fixed parameters (12 bytes)
      Timestamp: 174319513986
      Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x0601
  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]
    > Tag: DS Parameter set: Current Channel: 6
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment Indoor
    > Tag: EDCA Parameter Set
    > Tag: ERP Information
    > Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: Vendor Specific: Airgo Networks, Inc.
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

Support four data rates: 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
Eight additional rates: 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

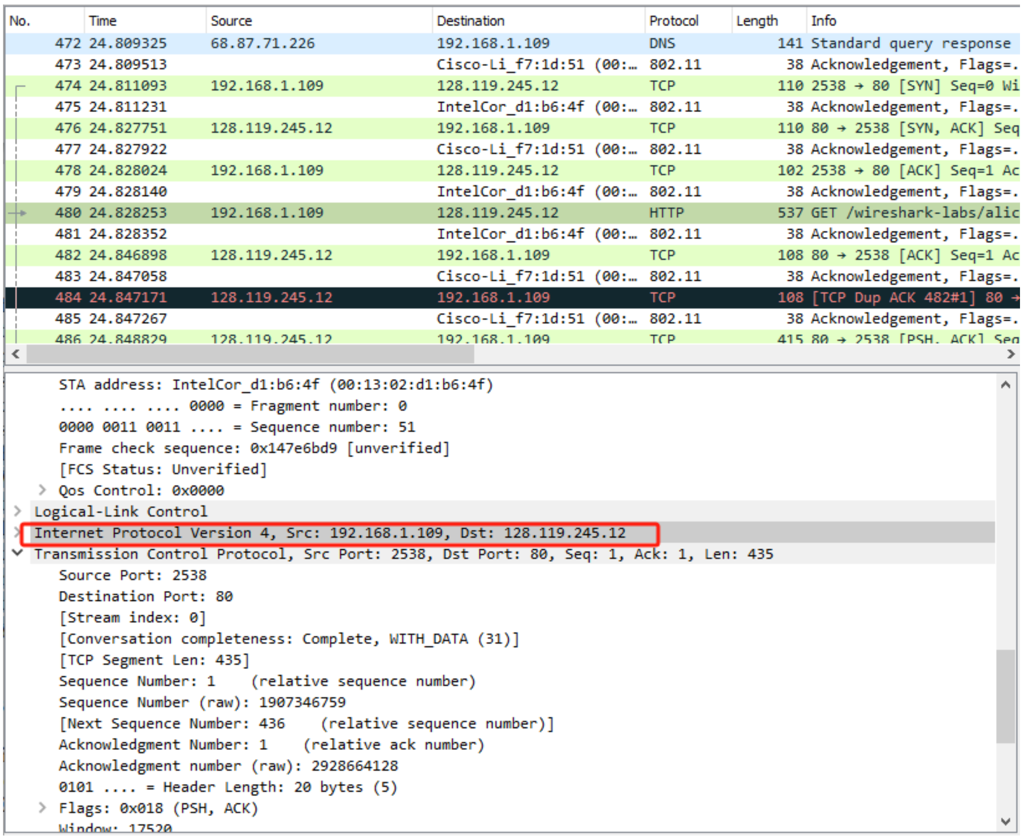
7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). What are three MAC address fields in the 802.11 frame?
   Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)?
   To the access point?
   To the first-hop router?
   What is the IP address of the wireless host sending this TCP segment?
   What is the destination IP address?
   Does this destination IP address correspond to the host, access point, first-hop router, or some other network-attached device? Explain.



```
No.       Time          Source            Destination                 Protocol   Length  Info
     472 24.809325     68.87.71.226      192.168.1.109               DNS           141 Standard query response
     473 24.809513                       Cisco-Li_f7:1d:51 (00:…     802.11         38 Acknowledgement, Flags=
     474 24.811093     192.168.1.109     128.119.245.12              TCP           110 2538 → 80 [SYN] Seq=0 W
     475 24.811231                       IntelCor_d1:b6:4f (00:…     802.11         38 Acknowledgement, Flags=
     476 24.827751     128.119.245.12    192.168.1.109               TCP           110 80 → 2538 [SYN, ACK] Se
     477 24.827922                       Cisco-Li_f7:1d:51 (00:…     802.11         38 Acknowledgement, Flags=
     478 24.828024     192.168.1.109     128.119.245.12              TCP           102 2538 → 80 [ACK] Seq=1 A
     479 24.828140                       IntelCor_d1:b6:4f (00:…     802.11         38 Acknowledgement, Flags=
     480 24.828253     192.168.1.109     128.119.245.12              HTTP          537 GET /wireshark-labs/ali
     481 24.828352                       IntelCor_d1:b6:4f (00:…     802.11         38 Acknowledgement, Flags=
     482 24.846898     128.119.245.12    192.168.1.109               TCP           108 80 → 2538 [ACK] Seq=1 A
     483 24.847058                       Cisco-Li_f7:1d:51 (00:…     802.11         38 Acknowledgement, Flags=
     484 24.847171     128.119.245.12    192.168.1.109               TCP           108 [TCP Dup ACK 482#1] 80
     485 24.847267                       Cisco-Li_f7:1d:51 (00:…     802.11         38 Acknowledgement, Flags=
     486 24.848829     128.119.245.12    192.168.1.109               TCP           415 80 → 2538 [PSH, ACK] Se
```

```
    Type/Subtype: QoS Data (0x0028)
  ⌄ Frame Control Field: 0x8801
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
    > Flags: 0x01
   .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 0011 .... = Sequence number: 51
    Frame check sequence: 0x147e6bd9 [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: 1, Ack: 1, Len: 435
    Source Port: 2538
```

Those MAC address fields are destination, source address and BBS Id.
MAC address of host: 00:13:02:d1:b6:4f
MAC address of access point: 00:16:b6:f7:1d:51
MAC address of first-hop router: 00:16:b6:f4:eb:a8



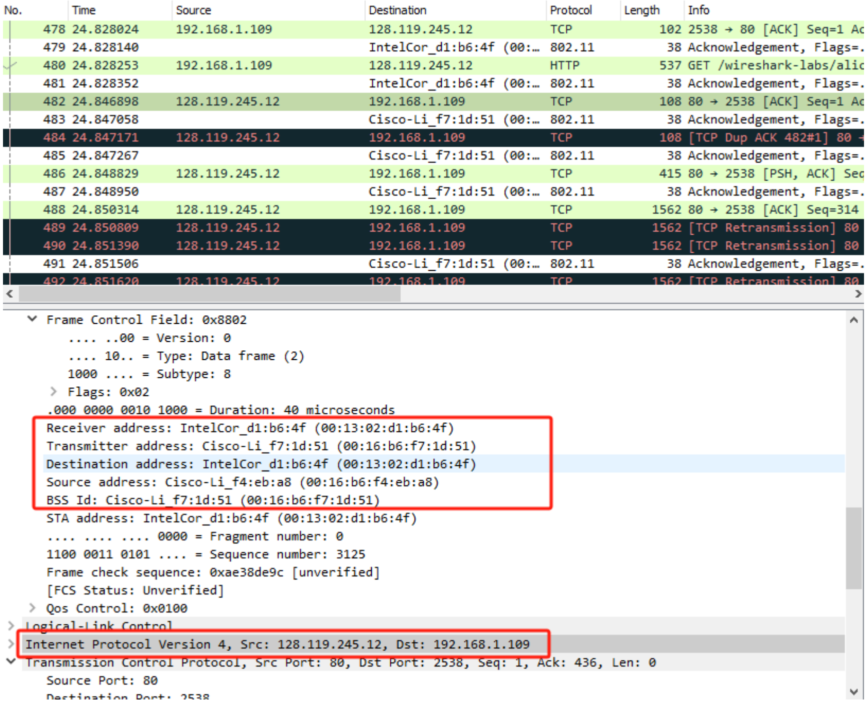
```
No.   Time       Source          Destination              Protocol  Length Info
  472 24.809325  68.87.71.226    192.168.1.109            DNS          141 Standard query response
  473 24.809513                  Cisco-Li_f7:1d:51 (00:…  802.11        38 Acknowledgement, Flags=.
  474 24.811093  192.168.1.109   128.119.245.12           TCP          110 2538 → 80 [SYN] Seq=0 Wi
  475 24.811231                  IntelCor_d1:b6:4f (00:…  802.11        38 Acknowledgement, Flags=.
  476 24.827751  128.119.245.12  192.168.1.109            TCP          110 80 → 2538 [SYN, ACK] Seq
  477 24.827922                  Cisco-Li_f7:1d:51 (00:…  802.11        38 Acknowledgement, Flags=.
  478 24.828024  192.168.1.109   128.119.245.12           TCP          102 2538 → 80 [ACK] Seq=1 Ac
  479 24.828140                  IntelCor_d1:b6:4f (00:…  802.11        38 Acknowledgement, Flags=.
  480 24.828253  192.168.1.109   128.119.245.12           HTTP         537 GET /wireshark-labs/alic
  481 24.828352                  IntelCor_d1:b6:4f (00:…  802.11        38 Acknowledgement, Flags=.
  482 24.846898  128.119.245.12  192.168.1.109            TCP          108 80 → 2538 [ACK] Seq=1 Ac
  483 24.847058                  Cisco-Li_f7:1d:51 (00:…  802.11        38 Acknowledgement, Flags=.
  484 24.847171  128.119.245.12  192.168.1.109            TCP          108 [TCP Dup ACK 482#1] 80 →
  485 24.847267                  Cisco-Li_f7:1d:51 (00:…  802.11        38 Acknowledgement, Flags=.
  486 24.848829  128.119.245.12  192.168.1.109            TCP          415 80 → 2538 [PSH, ACK] Seq
```

```
    STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    .... .... .... 0000 = Fragment number: 0
    0000 0011 0011 .... = Sequence number: 51
    Frame check sequence: 0x147e6bd9 [unverified]
    [FCS Status: Unverified]
  > Qos Control: 0x0000
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 2538, Dst Port: 80, Seq: 1, Ack: 1, Len: 435
    Source Port: 2538
    Destination Port: 80
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 435]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1907346759
    [Next Sequence Number: 436    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2928664128
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 17520
```

IP of host: 192.168.1.109
Dst IP: 128.119.245.12

The destination IP address corresponds to the host, due to it being the IP of the web server.

8. Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame?
   Which MAC address in this frame corresponds to the host?
   To the access point?
   To the first-hop router?
   Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram? (Hint: review Figure 6.19 in the text if you are unsure of how to answer this question, or the corresponding part of the previous question. It's particularly important that you understand this).



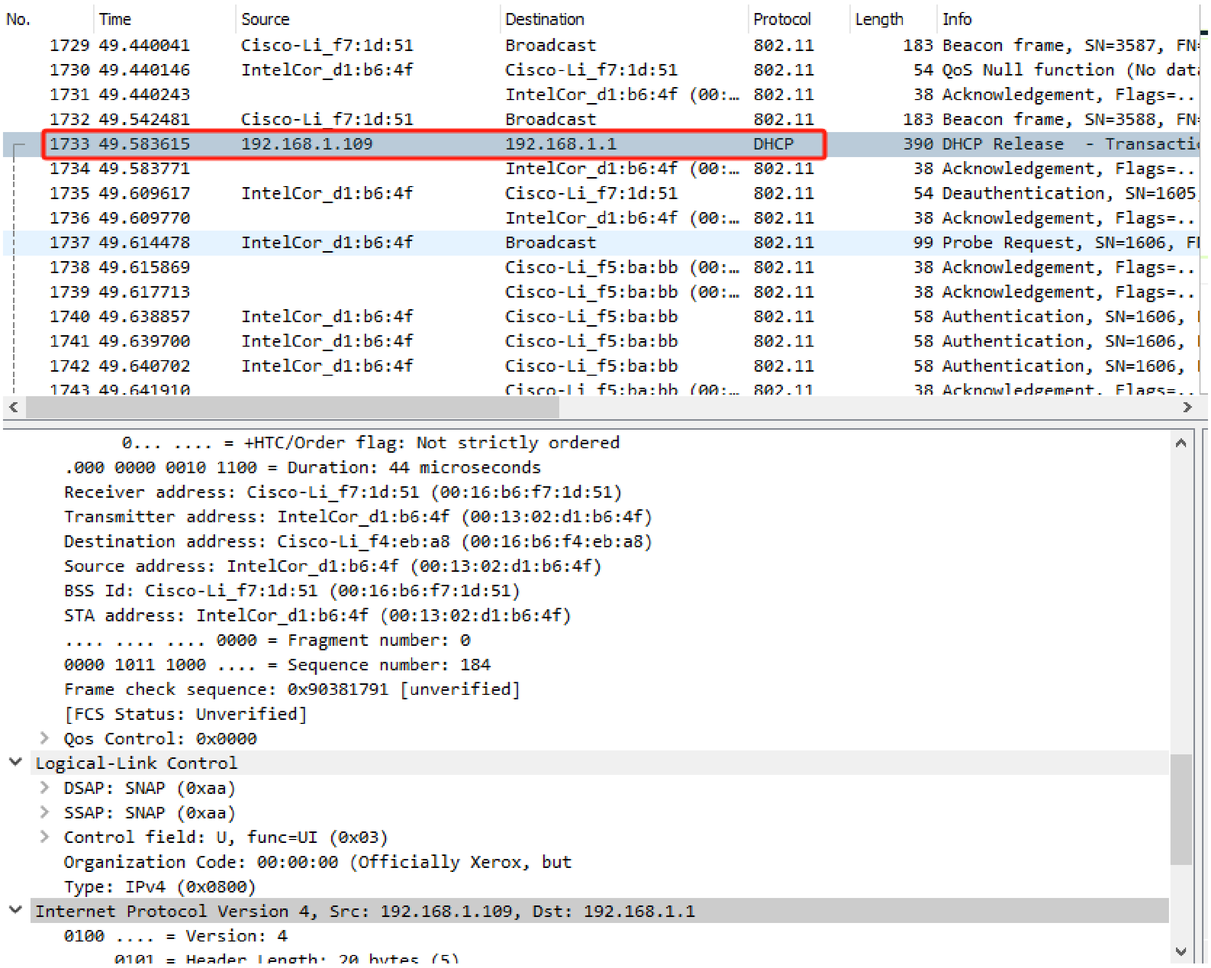
```
No.     Time       Source          Destination              Protocol  Length Info
    478 24.828024  192.168.1.109   128.119.245.12           TCP          102 2538 → 80 [ACK] Seq=1 Ac
    479 24.828140                  IntelCor_d1:b6:4f (00:…  802.11        38 Acknowledgement, Flags=.
    480 24.828253  192.168.1.109   128.119.245.12           HTTP         537 GET /wireshark-labs/alic
    481 24.828352                  IntelCor_d1:b6:4f (00:…  802.11        38 Acknowledgement, Flags=.
    482 24.846898  128.119.245.12  192.168.1.109            TCP          108 80 → 2538 [ACK] Seq=1 Ac
    483 24.847058                  Cisco-Li_f7:1d:51 (00:…  802.11        38 Acknowledgement, Flags=.
    484 24.847171  128.119.245.12  192.168.1.109            TCP          108 [TCP Dup ACK 482#1] 80 →
    485 24.847267                  Cisco-Li_f7:1d:51 (00:…  802.11        38 Acknowledgement, Flags=.
    486 24.848829  128.119.245.12  192.168.1.109            TCP          415 80 → 2538 [PSH, ACK] Sec
    487 24.848950                  Cisco-Li_f7:1d:51 (00:…  802.11        38 Acknowledgement, Flags=.
    488 24.850314  128.119.245.12  192.168.1.109            TCP         1562 80 → 2538 [ACK] Seq=314
    489 24.850809  128.119.245.12  192.168.1.109            TCP         1562 [TCP Retransmission] 80
    490 24.851390  128.119.245.12  192.168.1.109            TCP         1562 [TCP Retransmission] 80
    491 24.851506                  Cisco-Li_f7:1d:51 (00:…  802.11        38 Acknowledgement, Flags=.
    492 24.851620  128.119.245.12  192.168.1.109            TCP         1562 [TCP Retransmission] 80

   Frame Control Field: 0x8802
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
    > Flags: 0x02
   .000 0000 0010 1000 = Duration: 40 microseconds
   Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
   Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
   Destination address: IntelCor_d1:b6:4f (00:13:02:d1: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: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
   .... .... .... 0000 = Fragment number: 0
   1100 0011 0101 .... = Sequence number: 3125
   Frame check sequence: 0xae38de9c [unverified]
   [FCS Status: Unverified]
 > Qos Control: 0x0100
> Logical-Link Control
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.109
v Transmission Control Protocol, Src Port: 80, Dst Port: 2538, Seq: 1, Ack: 436, Len: 0
   Source Port: 80
   Destination Port: 2538
```

address 1 is receiver address: 00:13:02:d1:b6:4f, which is the host's MAC address
address 2 is transmitter address: 00:16:b6:f7:1d:51, which is the AP's MAC address
address 3 is BSS Id: 00:16:b6:f7:1d:51. which is MAC of router

The sender's MAC address does not correspond to the ip address of the device that sent the TCP serment. The source IP is 128.119.245.12, which is the IP of the web server. The sender's MAC address is 00:16:b6:f7:1d:51, which is the AP's MAC address.

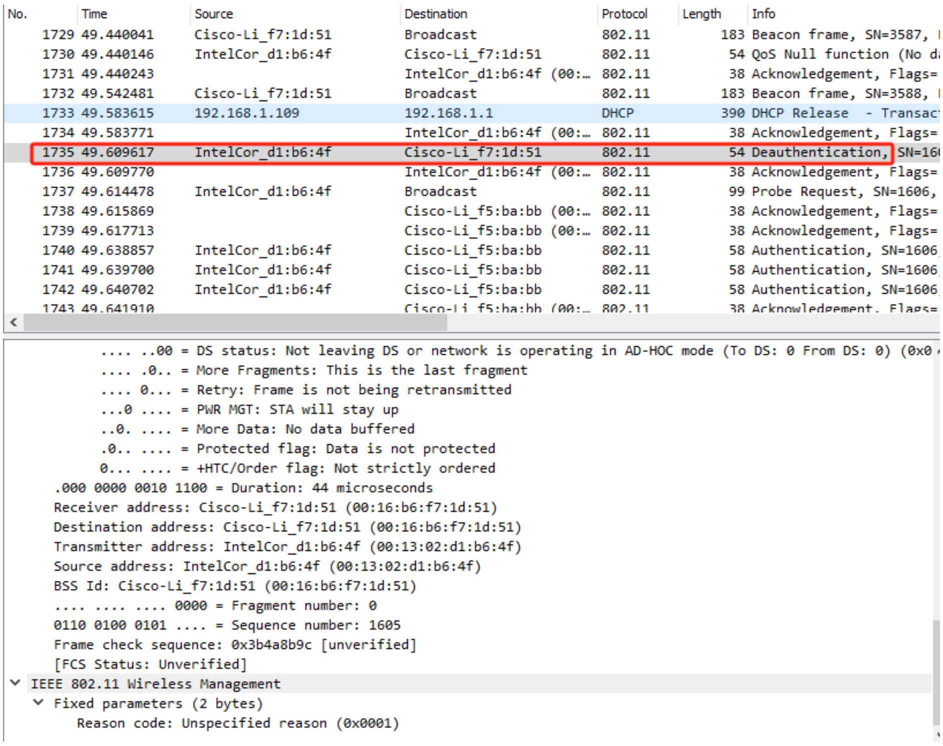
9. What two actions are taken (i.e., frames are sent) by the host in the trace just after t=49, to end the association with the 30 Munroe St AP that was initially in place when trace collection began? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification, is there another frame that you might have expected to see, but don't see here?



```
No.   Time       Source              Destination             Protocol  Length Info
 1729 49.440041  Cisco-Li_f7:1d:51   Broadcast               802.11       183 Beacon frame, SN=3587, FN
 1730 49.440146  IntelCor_d1:b6:4f   Cisco-Li_f7:1d:51       802.11        54 QoS Null function (No dat
 1731 49.440243                      IntelCor_d1:b6:4f (00:… 802.11        38 Acknowledgement, Flags=..
 1732 49.542481  Cisco-Li_f7:1d:51   Broadcast               802.11       183 Beacon frame, SN=3588, FN
 1733 49.583615  192.168.1.109       192.168.1.1             DHCP         390 DHCP Release  - Transacti
 1734 49.583771                      IntelCor_d1:b6:4f (00:… 802.11        38 Acknowledgement, Flags=..
 1735 49.609617  IntelCor_d1:b6:4f   Cisco-Li_f7:1d:51       802.11        54 Deauthentication, SN=1605
 1736 49.609770                      IntelCor_d1:b6:4f (00:… 802.11        38 Acknowledgement, Flags=..
 1737 49.614478  IntelCor_d1:b6:4f   Broadcast               802.11        99 Probe Request, SN=1606, F
 1738 49.615869                      Cisco-Li_f5:ba:bb (00:… 802.11        38 Acknowledgement, Flags=..
 1739 49.617713                      Cisco-Li_f5:ba:bb (00:… 802.11        38 Acknowledgement, Flags=..
 1740 49.638857  IntelCor_d1:b6:4f   Cisco-Li_f5:ba:bb       802.11        58 Authentication, SN=1606,
 1741 49.639700  IntelCor_d1:b6:4f   Cisco-Li_f5:ba:bb       802.11        58 Authentication, SN=1606,
 1742 49.640702  IntelCor_d1:b6:4f   Cisco-Li_f5:ba:bb       802.11        58 Authentication, SN=1606,
 1743 49.641910                      Cisco-Li_f5:ba:bb (00:… 802.11        38 Acknowledgement, Flags=..
```

```
        0... .... = +HTC/Order flag: Not strictly ordered
    .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
v Logical-Link Control
  > DSAP: SNAP (0xaa)
  > SSAP: SNAP (0xaa)
  > Control field: U, func=UI (0x03)
    Organization Code: 00:00:00 (Officially Xerox, but
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.1.109, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
```

The host sent a DHCP message to 192.168.1.1 to tell the DHCP server that the host will leave and release the ip address of the host.

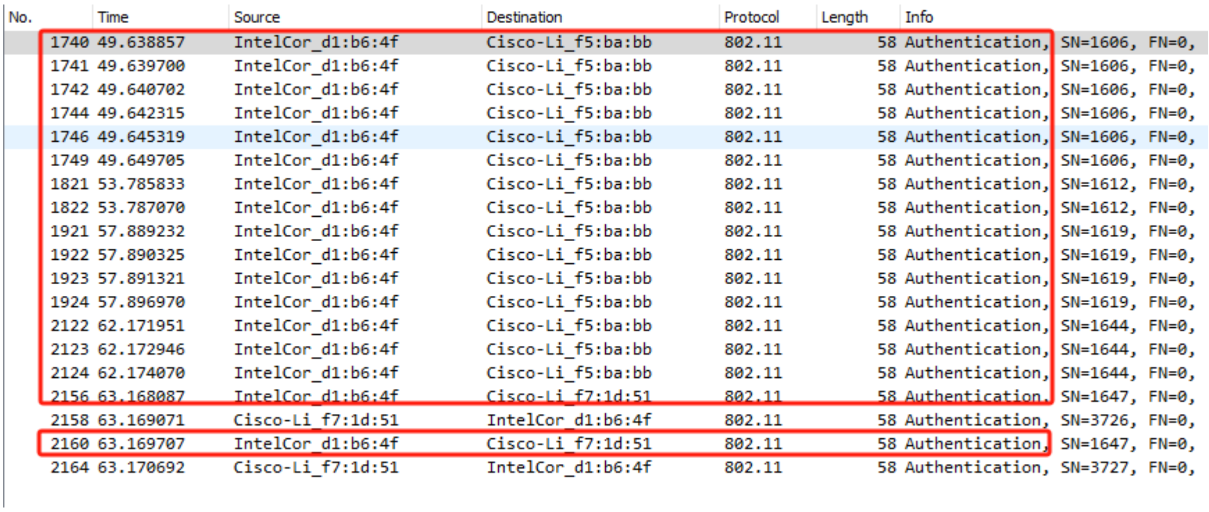


```
No.     Time       Source             Destination            Protocol  Length Info
   1729 49.440041  Cisco-Li_f7:1d:51  Broadcast              802.11       183 Beacon frame, SN=3587, 
   1730 49.440146  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51      802.11        54 QoS Null function (No d
   1731 49.440243                     IntelCor_d1:b6:4f (00:… 802.11        38 Acknowledgement, Flags=
   1732 49.542481  Cisco-Li_f7:1d:51  Broadcast              802.11       183 Beacon frame, SN=3588, 
   1733 49.583615  192.168.1.109      192.168.1.1            DHCP         390 DHCP Release  - Transac
   1734 49.583771                     IntelCor_d1:b6:4f (00:… 802.11        38 Acknowledgement, Flags=
   1735 49.609617  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51      802.11        54 Deauthentication, SN=16
   1736 49.609770                     IntelCor_d1:b6:4f (00:… 802.11        38 Acknowledgement, Flags=
   1737 49.614478  IntelCor_d1:b6:4f  Broadcast              802.11        99 Probe Request, SN=1606,
   1738 49.615869                     Cisco-Li_f5:ba:bb (00:… 802.11        38 Acknowledgement, Flags=
   1739 49.617713                     Cisco-Li_f5:ba:bb (00:… 802.11        38 Acknowledgement, Flags=
   1740 49.638857  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1606
   1741 49.639700  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1606
   1742 49.640702  IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb      802.11        58 Authentication, SN=1606
   1743 49.641910                     Cisco-Li_f5:ba:bb (00:… 802.11        38 Acknowledgement, Flags=
```

```
            .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = Protected flag: Data is not protected
            0... .... = +HTC/Order flag: Not strictly ordered
      .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]
v IEEE 802.11 Wireless Management
   v Fixed parameters (2 bytes)
         Reason code: Unspecified reason (0x0001)
```

The host sent a DEAUTHENTICATION frame in the second step.
The DEAUTHENTICATION request frame is expected to be seen, but not in here.

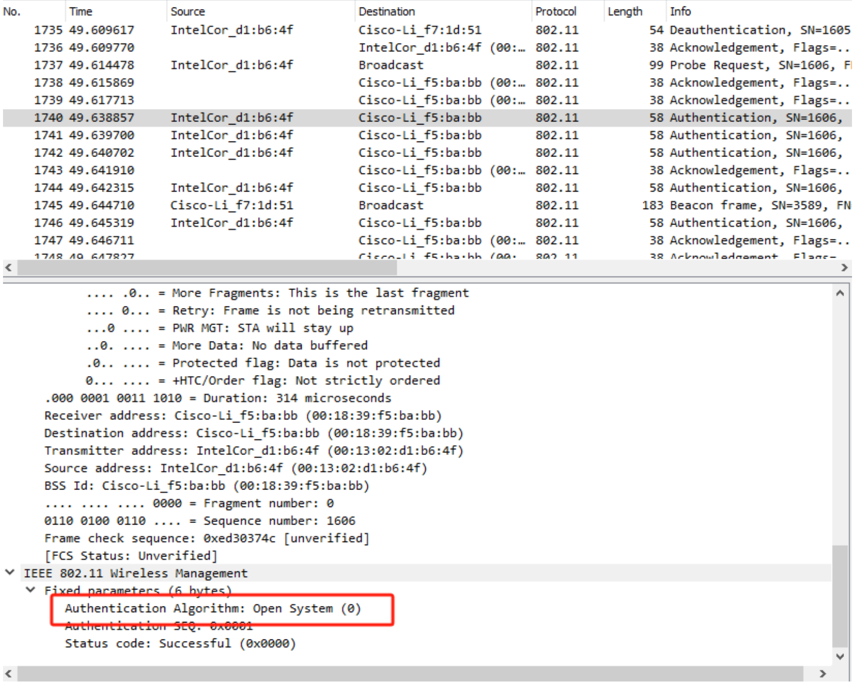
10. Examine the trace file and look for AUTHENICATION frames sent from the host to an AP and vice versa. How many AUTHENTICATION messages are sent from the wireless host to the linksys_ses_24086 AP (which has a MAC address of Cisco_Li_f5:ba:bb) starting at around t=49?



No.	Time	Source	Destination	Protocol	Length	Info
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0,
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0,
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0,
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0,
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0,
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0,
1821	53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0,
1822	53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0,
1921	57.889232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0,
1922	57.890325	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0,
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0,
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0,
2122	62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0,
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0,
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0,
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0,
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0,
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0,
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0,

There are 17 AUTHENTICATION messages.

11. Does the host want the authentication to require a key or be open?



No.	Time	Source	Destination	Protocol	Length	Info
1735	49.609617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	Deauthentication, SN=1605
1736	49.609770		IntelCor_d1:b6:4f (00:…	802.11	38	Acknowledgement, Flags=..
1737	49.614478	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1606, F
1738	49.615869		Cisco-Li_f5:ba:bb (00:…	802.11	38	Acknowledgement, Flags=..
1739	49.617713		Cisco-Li_f5:ba:bb (00:…	802.11	38	Acknowledgement, Flags=..
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606,
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606,
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606,
1743	49.641910		Cisco-Li_f5:ba:bb (00:…	802.11	38	Acknowledgement, Flags=..
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606,
1745	49.644710	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3589, FN
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606,
1747	49.646711		Cisco-Li_f5:ba:bb (00:…	802.11	38	Acknowledgement, Flags=..
1748	49.647827		Cisco-Li_f5:ba:bb (00:	802.11	38	Acknowledgement, Flags=

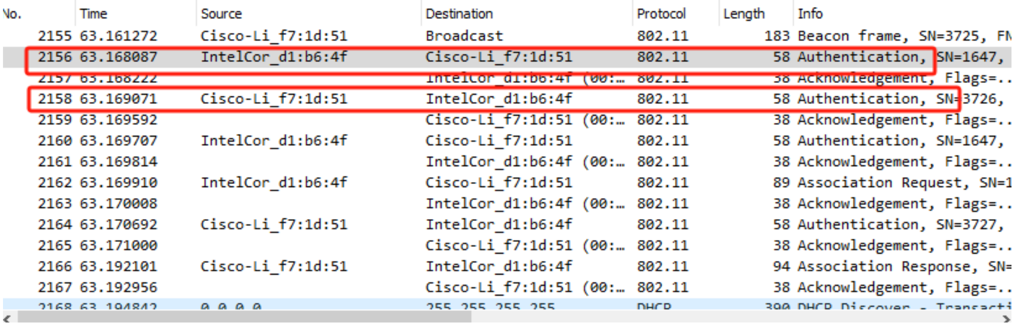
```
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = +HTC/Order flag: Not strictly ordered
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
    Destination address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
    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_f5:ba:bb (00:18:39:f5:ba:bb)
    .... .... .... 0000 = Fragment number: 0
    0110 0100 0110 .... = Sequence number: 1606
    Frame check sequence: 0xed30374c [unverified]
    [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0001
      Status code: Successful (0x0000)
```

The host wants the authentication to be open.

12. Do you see a reply AUTHENTICATION from the linksys_ses_24086 AP in the trace?

No, there is no reply, the AP may need authentication for a key, it ignores the request from the host.

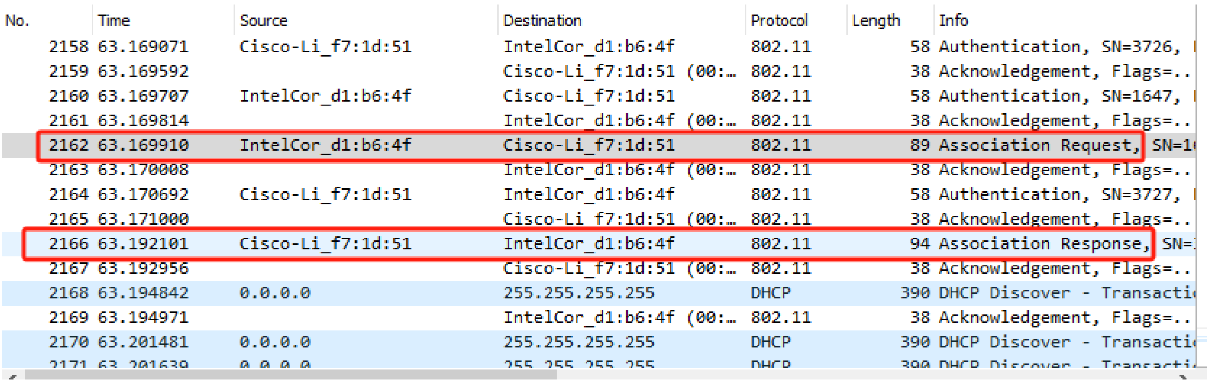
13.



```
No.    Time       Source             Destination              Protocol  Length Info
  2155 63.161272  Cisco-Li_f7:1d:51  Broadcast                802.11       183 Beacon frame, SN=3725, FN
  2156 63.168087  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51        802.11        58 Authentication, SN=1647,
  2157 63.168222                     IntelCor_d1:b6:4f (00:…  802.11        38 Acknowledgement, Flags=..
  2158 63.169071  Cisco-Li_f7:1d:51  IntelCor_d1:b6:4f        802.11        58 Authentication, SN=3726,
  2159 63.169592                     Cisco-Li_f7:1d:51 (00:…  802.11        38 Acknowledgement, Flags=..
  2160 63.169707  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51        802.11        58 Authentication, SN=1647,
  2161 63.169814                     IntelCor_d1:b6:4f (00:…  802.11        38 Acknowledgement, Flags=..
  2162 63.169910  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51        802.11        89 Association Request, SN=1
  2163 63.170008                     IntelCor_d1:b6:4f (00:…  802.11        38 Acknowledgement, Flags=..
  2164 63.170692  Cisco-Li_f7:1d:51  IntelCor_d1:b6:4f        802.11        58 Authentication, SN=3727,
  2165 63.171000                     Cisco-Li_f7:1d:51 (00:…  802.11        38 Acknowledgement, Flags=..
  2166 63.192101  Cisco-Li_f7:1d:51  IntelCor_d1:b6:4f        802.11        94 Association Response, SN=
  2167 63.192956                     Cisco-Li_f7:1d:51 (00:…  802.11        38 Acknowledgement, Flags=..
  2168 63.194842  0.0.0.0            255.255.255.255          DHCP         390 DHCP Discover - Transacti
```

At t = 63.168087, the host sent an AUTHENTICATION frame to AP.
Yes, there is a reply from the host.
At t = 63.169071, The AP sent an AUTHENTICATION frame to host.

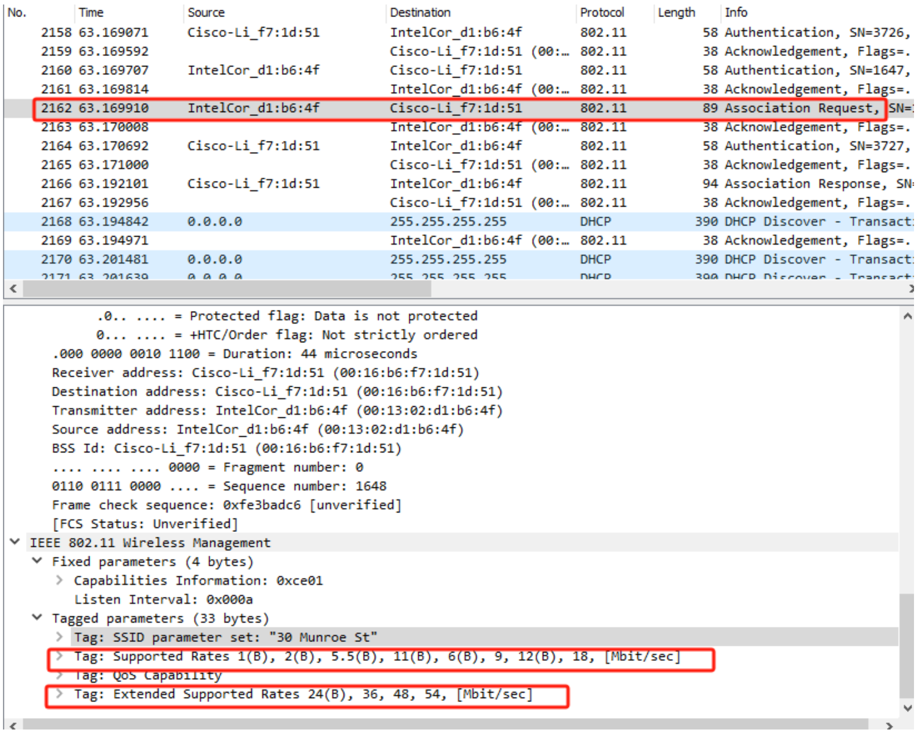
14.



```
No.    Time       Source             Destination              Protocol  Length Info
  2158 63.169071  Cisco-Li_f7:1d:51  IntelCor_d1:b6:4f        802.11        58 Authentication, SN=3726,
  2159 63.169592                     Cisco-Li_f7:1d:51 (00:…  802.11        38 Acknowledgement, Flags=..
  2160 63.169707  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51        802.11        58 Authentication, SN=1647,
  2161 63.169814                     IntelCor_d1:b6:4f (00:…  802.11        38 Acknowledgement, Flags=..
  2162 63.169910  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51        802.11        89 Association Request, SN=1
  2163 63.170008                     IntelCor_d1:b6:4f (00:…  802.11        38 Acknowledgement, Flags=..
  2164 63.170692  Cisco-Li_f7:1d:51  IntelCor_d1:b6:4f        802.11        58 Authentication, SN=3727,
  2165 63.171000                     Cisco-Li_f7:1d:51 (00:…  802.11        38 Acknowledgement, Flags=..
  2166 63.192101  Cisco-Li_f7:1d:51  IntelCor_d1:b6:4f        802.11        94 Association Response, SN=
  2167 63.192956                     Cisco-Li_f7:1d:51 (00:…  802.11        38 Acknowledgement, Flags=..
  2168 63.194842  0.0.0.0            255.255.255.255          DHCP         390 DHCP Discover - Transacti
  2169 63.194971                     IntelCor_d1:b6:4f (00:…  802.11        38 Acknowledgement, Flags=..
  2170 63.201481  0.0.0.0            255.255.255.255          DHCP         390 DHCP Discover - Transacti
  2171 63.201639  0.0.0.0            255.255.255.255          DHCP         390 DHCP Discover - Transacti…
```

At t = 63.169910, the Host sent an ASSOCIATE REQUEST frame to AP.
At t = 63.192101, the AP sent the ASSOCIATE RESPONSE frame to host.

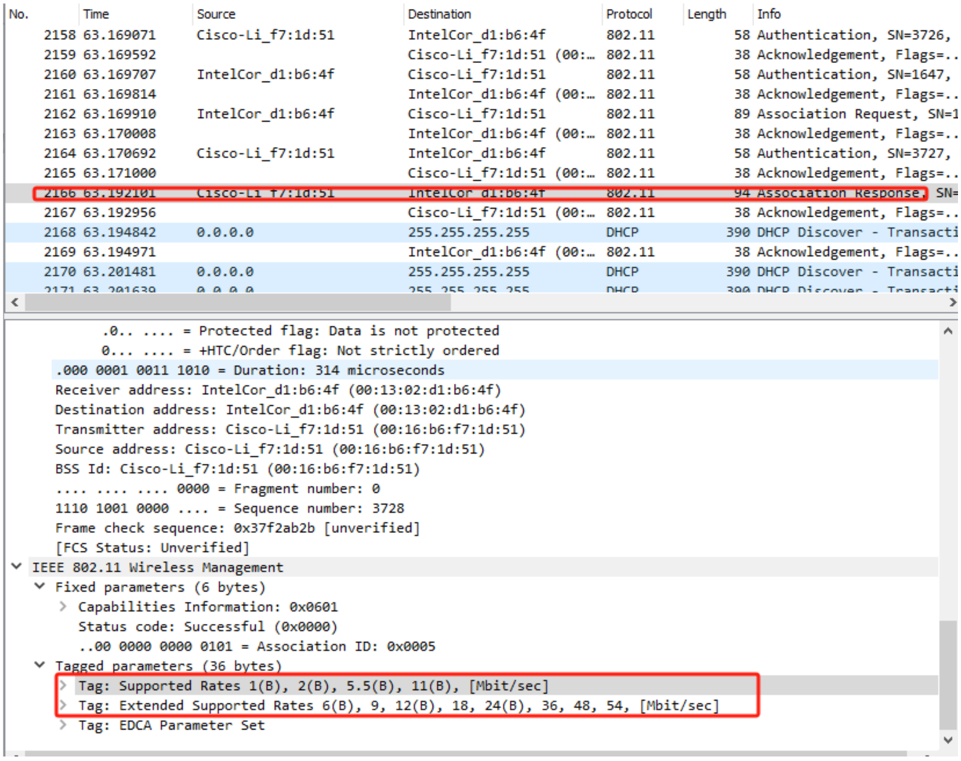
15.



```
No.     Time       Source             Destination                Protocol  Length Info
   2158 63.169071  Cisco-Li_f7:1d:51  IntelCor_d1:b6:4f          802.11       58 Authentication, SN=3726,
   2159 63.169592                     Cisco-Li_f7:1d:51 (00:…    802.11       38 Acknowledgement, Flags=.
   2160 63.169707  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51          802.11       58 Authentication, SN=1647,
   2161 63.169814                     IntelCor_d1:b6:4f (00:…    802.11       38 Acknowledgement, Flags=.
   2162 63.169910  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51          802.11       89 Association Request, SN=
   2163 63.170008                     IntelCor_d1:b6:4f (00:…    802.11       38 Acknowledgement, Flags=.
   2164 63.170692  Cisco-Li_f7:1d:51  IntelCor_d1:b6:4f          802.11       58 Authentication, SN=3727,
   2165 63.171000                     Cisco-Li_f7:1d:51 (00:…    802.11       38 Acknowledgement, Flags=.
   2166 63.192101  Cisco-Li_f7:1d:51  IntelCor_d1:b6:4f          802.11       94 Association Response, SN
   2167 63.192956                     Cisco-Li_f7:1d:51 (00:…    802.11       38 Acknowledgement, Flags=.
   2168 63.194842  0.0.0.0            255.255.255.255            DHCP        390 DHCP Discover - Transact
   2169 63.194971                     IntelCor_d1:b6:4f (00:…    802.11       38 Acknowledgement, Flags=.
   2170 63.201481  0.0.0.0            255.255.255.255            DHCP        390 DHCP Discover - Transact
   2171 63.201639  0.0.0.0            255.255.255.255            DHCP        390 DHCP Discover - Transact
```

```
        .0.. .... = Protected flag: Data is not protected
        0... .... = +HTC/Order flag: Not strictly ordered
    .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 0111 0000 .... = Sequence number: 1648
    Frame check sequence: 0xfe3badc6 [unverified]
    [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
  v Fixed parameters (4 bytes)
    > Capabilities Information: 0xce01
      Listen Interval: 0x000a
  v Tagged parameters (33 bytes)
    > Tag: SSID parameter set: "30 Munroe St"
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
    > Tag: QoS Capability
    > Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
```

For host: 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, 24(B), 36, 48, 54[Mbit/sec] are supported

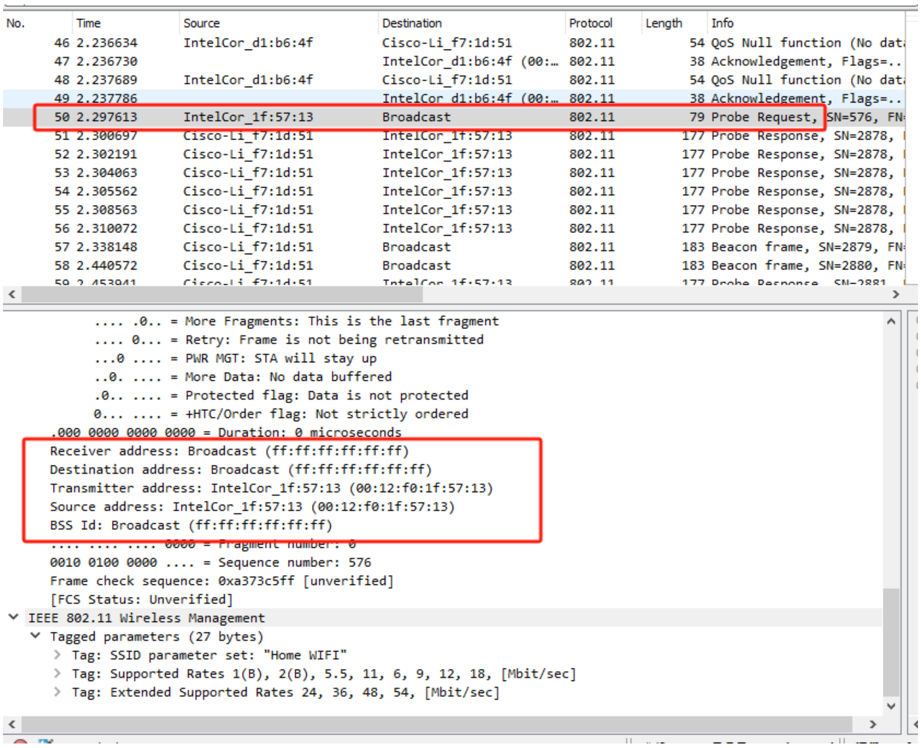


```
No.     Time       Source             Destination                Protocol  Length Info
   2158 63.169071  Cisco-Li_f7:1d:51  IntelCor_d1:b6:4f          802.11       58 Authentication, SN=3726,
   2159 63.169592                     Cisco-Li_f7:1d:51 (00:…    802.11       38 Acknowledgement, Flags=..
   2160 63.169707  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51          802.11       58 Authentication, SN=1647,
   2161 63.169814                     IntelCor_d1:b6:4f (00:…    802.11       38 Acknowledgement, Flags=..
   2162 63.169910  IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51          802.11       89 Association Request, SN=1
   2163 63.170008                     IntelCor_d1:b6:4f (00:…    802.11       38 Acknowledgement, Flags=..
   2164 63.170692  Cisco-Li_f7:1d:51  IntelCor_d1:b6:4f          802.11       58 Authentication, SN=3727,
   2165 63.171000                     Cisco-Li_f7:1d:51 (00:…    802.11       38 Acknowledgement, Flags=..
   2166 63.192101  Cisco-Li_f7:1d:51  IntelCor_d1:b6:4f          802.11       94 Association Response, SN=
   2167 63.192956                     Cisco-Li_f7:1d:51 (00:…    802.11       38 Acknowledgement, Flags=..
   2168 63.194842  0.0.0.0            255.255.255.255            DHCP        390 DHCP Discover - Transacti
   2169 63.194971                     IntelCor_d1:b6:4f (00:…    802.11       38 Acknowledgement, Flags=..
   2170 63.201481  0.0.0.0            255.255.255.255            DHCP        390 DHCP Discover - Transacti
   2171 63.201639  0.0.0.0            255.255.255.255            DHCP        390 DHCP Discover - Transacti
```

```
        .0.. .... = Protected flag: Data is not protected
        0... .... = +HTC/Order flag: Not strictly ordered
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    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
    1110 1001 0000 .... = Sequence number: 3728
    Frame check sequence: 0x37f2ab2b [unverified]
    [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
    > Capabilities Information: 0x0601
      Status code: Successful (0x0000)
      ..00 0000 0000 0101 = Association ID: 0x0005
  v Tagged parameters (36 bytes)
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    > Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: EDCA Parameter Set
```

For AP: 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, 24(B), 36, 48, 54[Mbit/sec] are supported

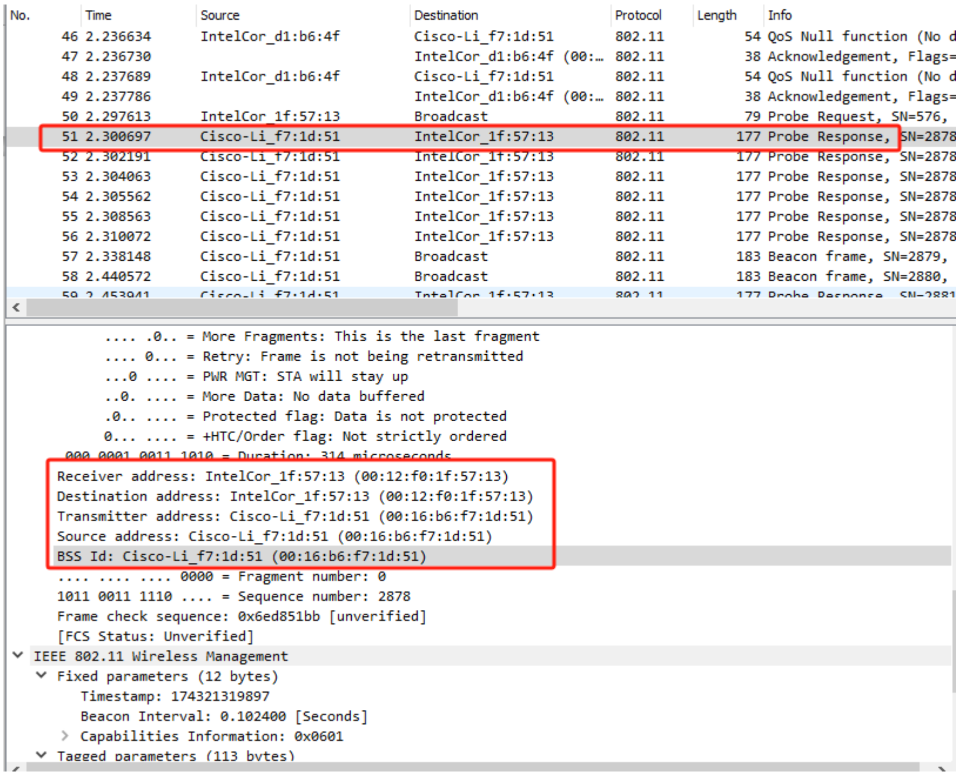
16.



```
No.   Time        Source               Destination          Protocol  Length  Info
   46 2.236634    IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51    802.11       54 QoS Null function (No data
   47 2.236730                         IntelCor_d1:b6:4f (00:… 802.11    38 Acknowledgement, Flags=..
   48 2.237689    IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51    802.11       54 QoS Null function (No data
   49 2.237786                         IntelCor_d1:b6:4f (00:… 802.11    38 Acknowledgement, Flags=..
   50 2.297613    IntelCor_1f:57:13    Broadcast            802.11       79 Probe Request, SN=576, FN
   51 2.300697    Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11      177 Probe Response, SN=2878,
   52 2.302191    Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11      177 Probe Response, SN=2878,
   53 2.304063    Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11      177 Probe Response, SN=2878,
   54 2.305562    Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11      177 Probe Response, SN=2878,
   55 2.308563    Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11      177 Probe Response, SN=2878,
   56 2.310072    Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11      177 Probe Response, SN=2878,
   57 2.338148    Cisco-Li_f7:1d:51    Broadcast            802.11      183 Beacon frame, SN=2879, FN
   58 2.440572    Cisco-Li_f7:1d:51    Broadcast            802.11      183 Beacon frame, SN=2880, FN
   59 2.453041    Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11      177 Probe Response, SN=2881
```

```
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = +HTC/Order flag: Not strictly ordered
    .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: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    Source address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    .... .... .... 0000 = Fragment number: 0
    0010 0100 0000 .... = Sequence number: 576
    Frame check sequence: 0xa373c5ff [unverified]
    [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
  v Tagged parameters (27 bytes)
    > Tag: SSID parameter set: "Home WIFI"
    > Tag: Supported Rates 1(B), 2(B), 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
    > Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
```

There is a PROBE REQUEST at t = 2.297613.
The sender is 00:12:f0:1f:57:13
The receiver is ff:ff:ff:ff:ff:ff
The BSS ID MAC address is ff:ff:ff:ff:ff:ff



```
No.   Time        Source               Destination          Protocol  Length  Info
   46 2.236634    IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51    802.11       54 QoS Null function (No d
   47 2.236730                         IntelCor_d1:b6:4f (00:… 802.11    38 Acknowledgement, Flags=
   48 2.237689    IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51    802.11       54 QoS Null function (No d
   49 2.237786                         IntelCor_d1:b6:4f (00:… 802.11    38 Acknowledgement, Flags=
   50 2.297613    IntelCor_1f:57:13    Broadcast            802.11       79 Probe Request, SN=576,
   51 2.300697    Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11      177 Probe Response, SN=2878
   52 2.302191    Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11      177 Probe Response, SN=2878
   53 2.304063    Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11      177 Probe Response, SN=2878
   54 2.305562    Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11      177 Probe Response, SN=2878
   55 2.308563    Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11      177 Probe Response, SN=2878
   56 2.310072    Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11      177 Probe Response, SN=2878
   57 2.338148    Cisco-Li_f7:1d:51    Broadcast            802.11      183 Beacon frame, SN=2879,
   58 2.440572    Cisco-Li_f7:1d:51    Broadcast            802.11      183 Beacon frame, SN=2880,
   59 2.453041    Cisco-Li_f7:1d:51    IntelCor_1f:57:13    802.11      177 Probe Response, SN=2881
```

```
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = +HTC/Order flag: Not strictly ordered
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    Destination address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    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 1110 .... = Sequence number: 2878
    Frame check sequence: 0x6ed851bb [unverified]
    [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
  v Fixed parameters (12 bytes)
      Timestamp: 174321319897
      Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x0601
  v Tagged parameters (113 bytes)
```

There is a PROBE RESPONSE at t = 2.300697
The sender is 00:16:b6:f7:1d:51
The receiver is 00:12:f0:1f:57:13

The BSS ID MAC address is 00:16:b6:f7:1d:51

This is used to find available APs around the wifi node(active scanning). When Ap received REQUEST, they will answer it by PROBE RESPONSE.

there is a PROBE REQUEST sent with source 00:12:f0:1f:57:13, destination: ff:ff:ff:ff:ff:ff, and a BSSID of ff:ff:ff:ff:ff:ff. At t = 2.300697 there is a PROBE RESPONSE sent with source: 00:16:b6:f7:1d:51, destination and a BSSID of 00:16:b6:f7:1d:51. A PROBE REQUEST is used by a host in active scanning to find an Access Point (see Figure 6.9 on page 531 in the text). A PROBE RESPONSE is sent by the access point to the host sending the request.

Conclusion:

When a wifi node wants to connect the AP, it has two modes: passive scanning and active scanning. When the host wants to visit a website on the internet. It will send a frame to AP first, then AP sends this frame to the router second. When the server sends back a frame, AP will also receive that frame from the router then send it to the host. In addition, when a host disconnects wifi, it will also send a DHCP message to the DHCP server.