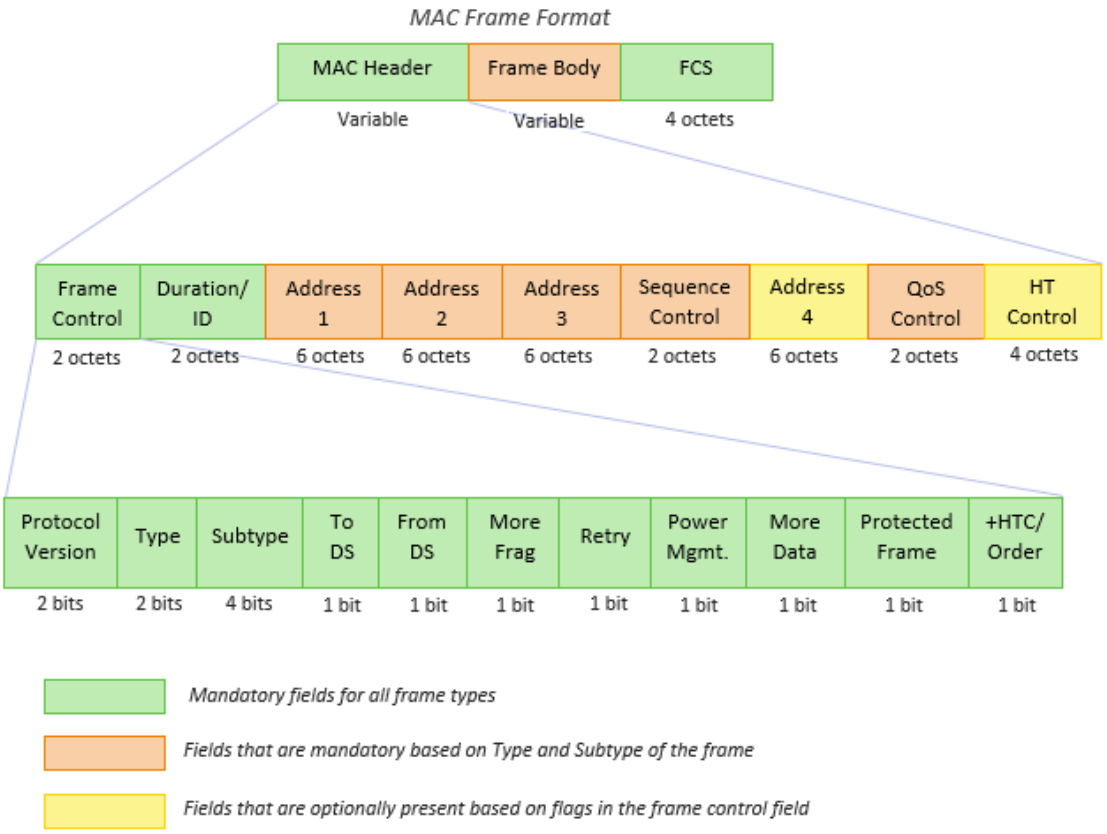
WIFI AND WIRESHARK

WIFI 802.11 FRAME



Оч хорошая статья про фрейм wifi.
Структура фрейма wifi/

Для удобства отображения заходим в Preferences -> layout и выбираем 2ю схему расположения окон.

SSID (Service Set Identifier) — это символьное название беспроводной точки доступа Wi-Fi, служащее для идентификации её среди других точек пользователями или устройствами, подключающимися к сети.

‘iwconfig’ - configure a wireless network interface

```
dasha@dasha-K501UQ:~$ iwconfig
lo        no wireless extensions.

enp2s0    no wireless extensions.

wlp3s0    IEEE 802.11  ESSID:"guest"
          Mode:Managed  Frequency:2.412 GHz  Access Point: 04:8C:16:BF:C1:A0
          Bit Rate=144.4 Mb/s   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=52/70  Signal level=-58 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:1  Invalid misc:1   Missed beacon:0
```

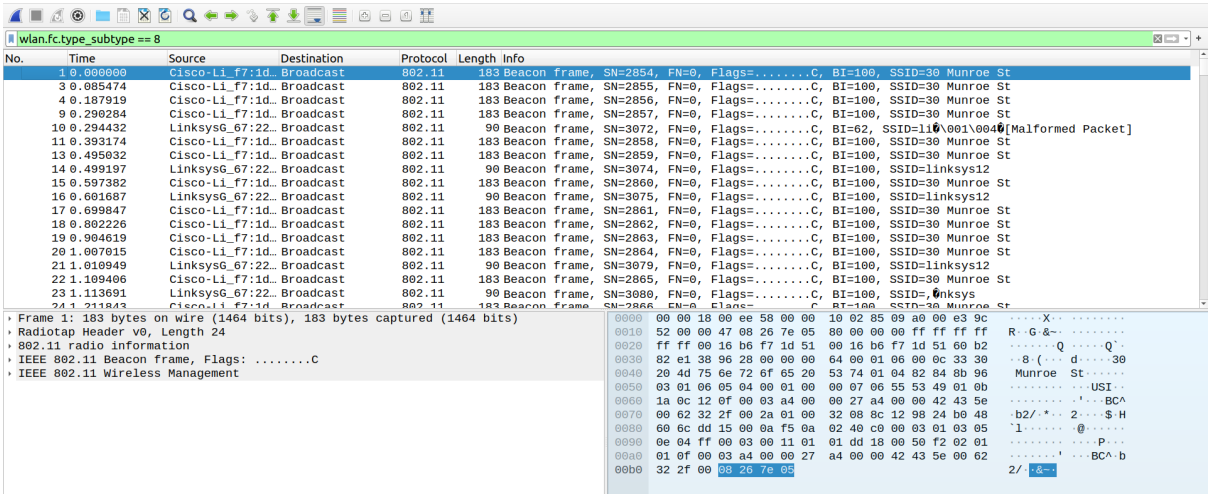
НИКОГДА НЕ ПИСАТЬ КОМАНДУ ‘sudo airmon-ng start wlp3s0’ !!! А то потом минус вифи… Как фиксить?

```
1976  iwconfig
1977  airmon-ng start wlp3s0
1978  sudo apt install aircrack-ng
1979  airmon-ng start wlp3s0
1980  sudo airmon-ng start wlp3s0
1981  airmon-ng check kill
1982  sudo airmon-ng check kill
1983  iwconfig
1984  /usr/sbin/airmon-ng
1985  sudo /usr/sbin/airmon-ng
1986  ifconfig wlp3s0 up
1987  sevice NetworkManager restart
1988  service NetworkManager restart
1989  iwconfig
1990  aitmon-ng start wlp3s0
1991  airmon-ng start wlp3s0
1992  sudo airmon-ng start wlp3s0
1993  sudo airmon-ng stop wlp3s0mon
1994  ifconfig wlp3s0 up
1995  sudo ifconfig wlp3s0 up
1996  ifconfig
```

BEACON FRAMES

Как выделить только beacon frames?

‘wlan.fc.type_subtype == 8’

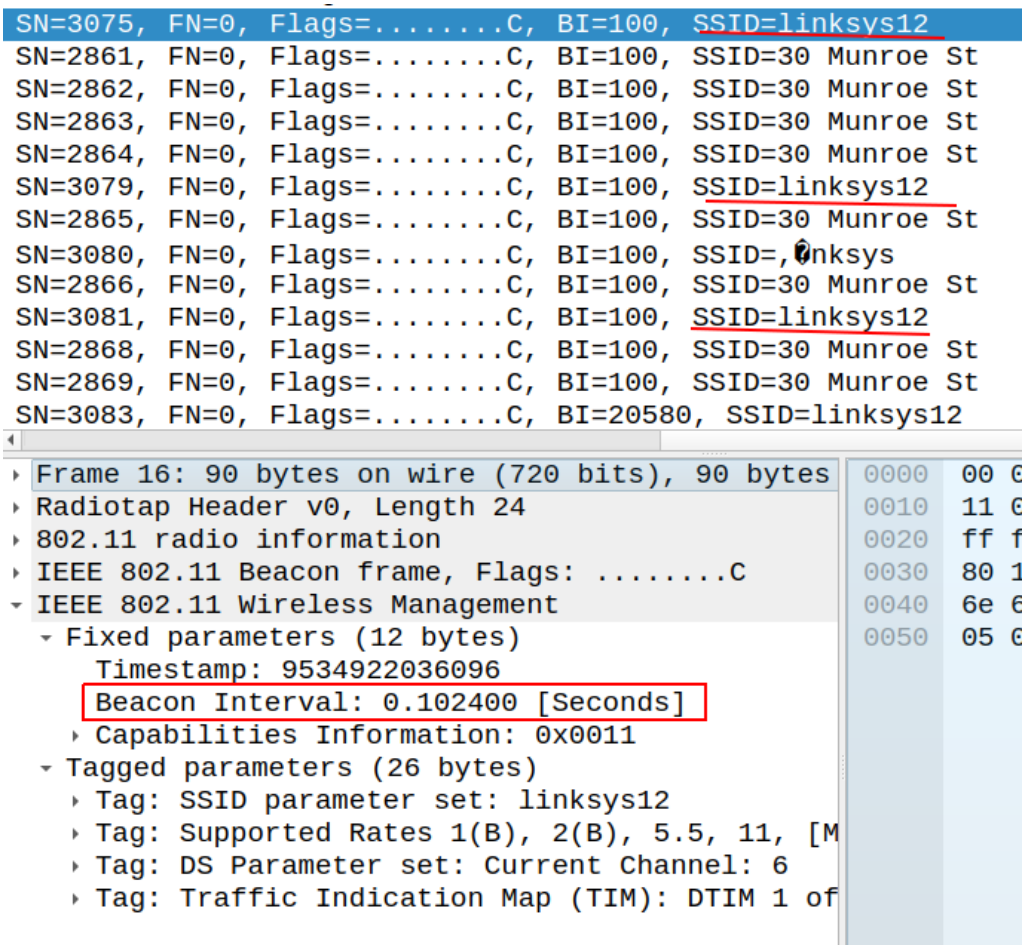


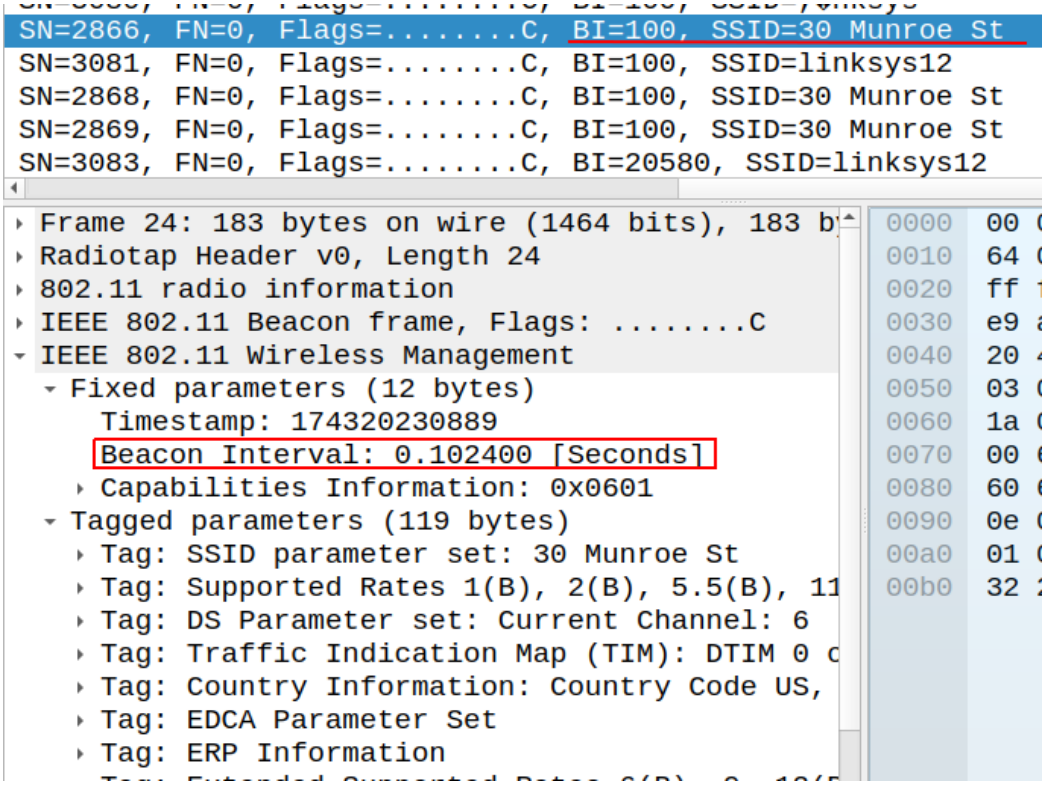
1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?

Как видим из последнего столбца видно, что самые распространенные точки доступа это Munroe St & linksys12.

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).

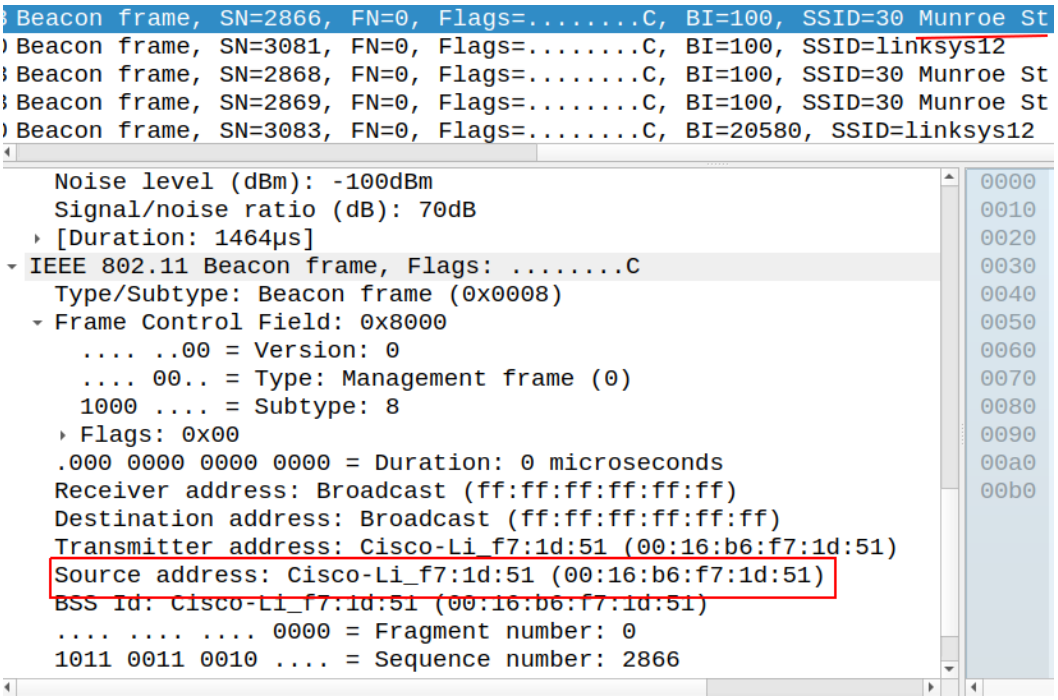
Для обоих точек доступа это время составляет
Beacon Interval: 0.102400 [Seconds]


SN=3075, FN=0, Flags=.....C, BI=100, SSID=linksys12
SN=2861, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
SN=2862, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
SN=2863, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
SN=2864, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
SN=3079, FN=0, Flags=.....C, BI=100, SSID=linksys12
SN=2865, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
SN=3080, FN=0, Flags=.....C, BI=100, SSID=,nksys
SN=2866, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
SN=3081, FN=0, Flags=.....C, BI=100, SSID=linksys12
SN=2868, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
SN=2869, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
SN=3083, FN=0, Flags=.....C, BI=20580, SSID=linksys12
Frame 16: 90 bytes on wire (720 bits), 90 bytes
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Beacon frame, Flags: C
IEEE 802.11 Wireless Management
Fixed parameters (12 bytes)
Timestamp: 9534922036096
Beacon Interval: 0.102400 [Seconds]
Capabilities Information: 0x0011
Tagged parameters (26 bytes)
Tag: SSID parameter set: linksys12
Tag: Supported Rates 1(B), 2(B), 5.5, 11, [M
Tag: DS Parameter set: Current Channel: 6
Tag: Traffic Indication Map (TIM): DTIM 1 of
0000 00 0
0010 11 0
0020 ff f
0030 80 1
0040 6e 6
0050 05 0


SN=2866, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
SN=3081, FN=0, Flags=.....C, BI=100, SSID=linksys12
SN=2868, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
SN=2869, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
SN=3083, FN=0, Flags=.....C, BI=20580, SSID=linksys12
Frame 24: 183 bytes on wire (1464 bits), 183 b
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Beacon frame, Flags: C
IEEE 802.11 Wireless Management
Fixed parameters (12 bytes)
Timestamp: 174320230889
Beacon Interval: 0.102400 [Seconds]
Capabilities Information: 0x0601
Tagged parameters (119 bytes)
Tag: SSID parameter set: 30 Munroe St
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11
Tag: DS Parameter set: Current Channel: 6
Tag: Traffic Indication Map (TIM): DTIM 0 c
Tag: Country Information: Country Code US,
Tag: EDCA Parameter Set
Tag: ERP Information
0000 00
0010 64
0020 ff
0030 e9
0040 20
0050 03
0060 1a
0070 00
0080 60
0090 0e
00a0 01
00b0 32

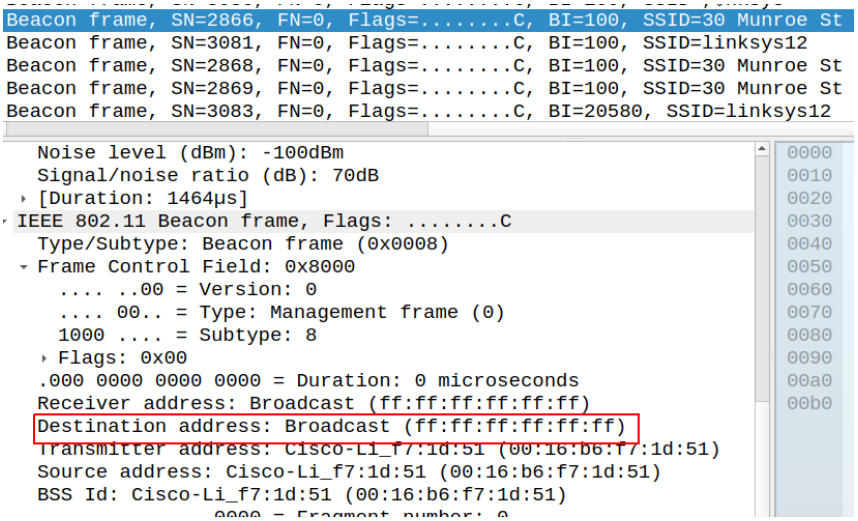
3. What (in hexadecimal notation) is the source MAC address on the beacon frame from 30 Munroe St? Recall from Figure 7.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE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

Ответ такой:
Source address: Cisco-Li_f7:1d:51 **(00:16:b6:f7:1d:51)**



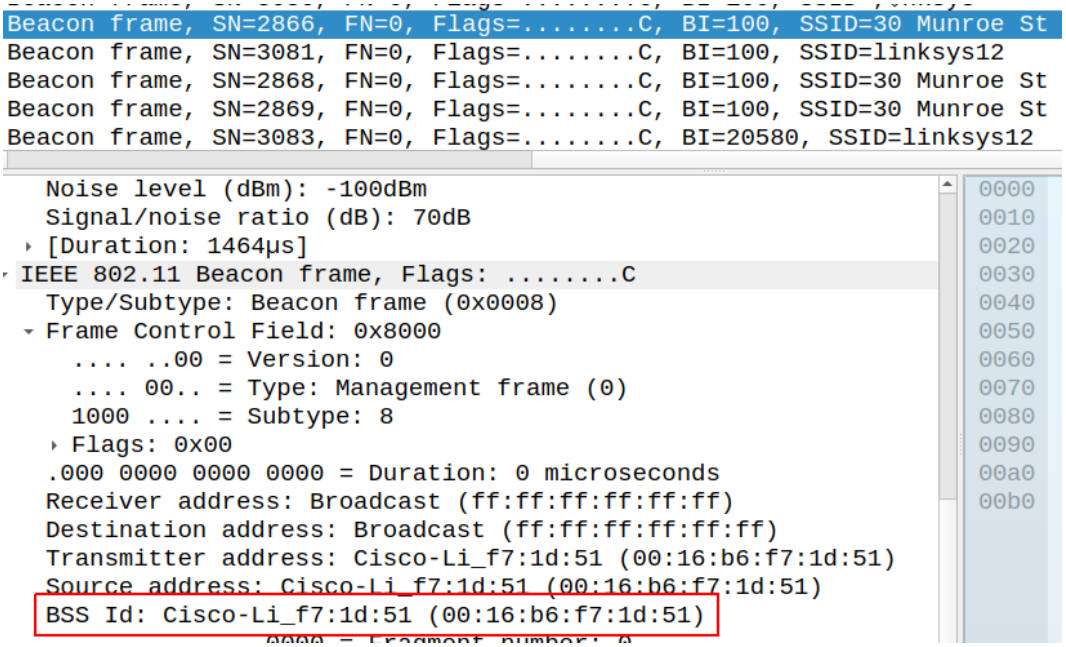
4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St??

Ответ такой: Destination address: **Broadcast (ff:ff:ff:ff:ff:ff)**



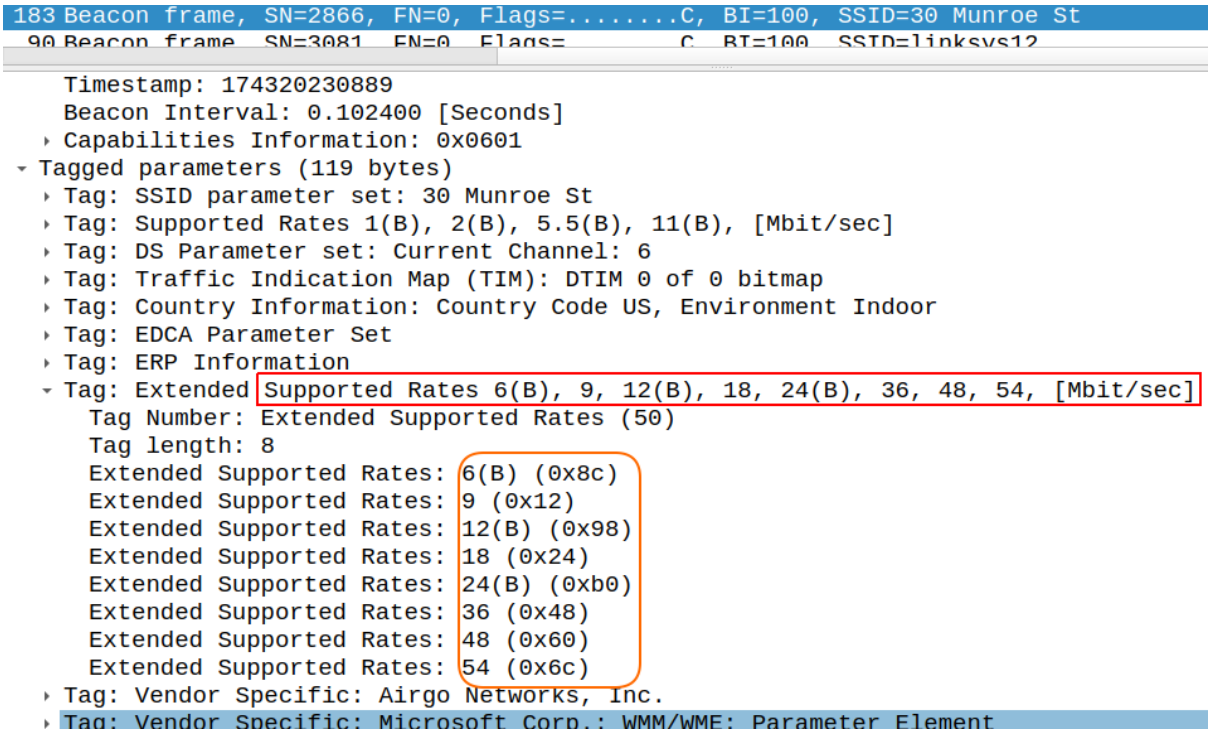
5. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from 30 Munroe St?

Ответ такой: BSS Id: Cisco-Li_f7:1d:51 (**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?

IEEE 802.11 Wireless Management -> Tagged parameters (119 bytes) ->
Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]



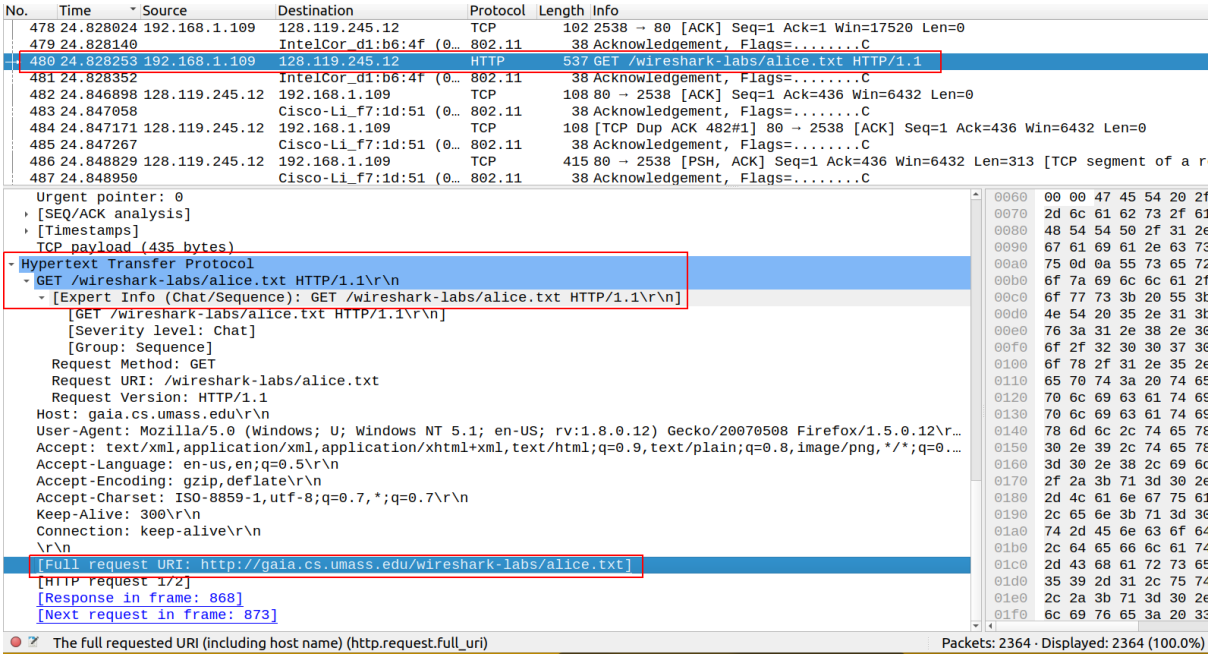
DATA TRANSFER

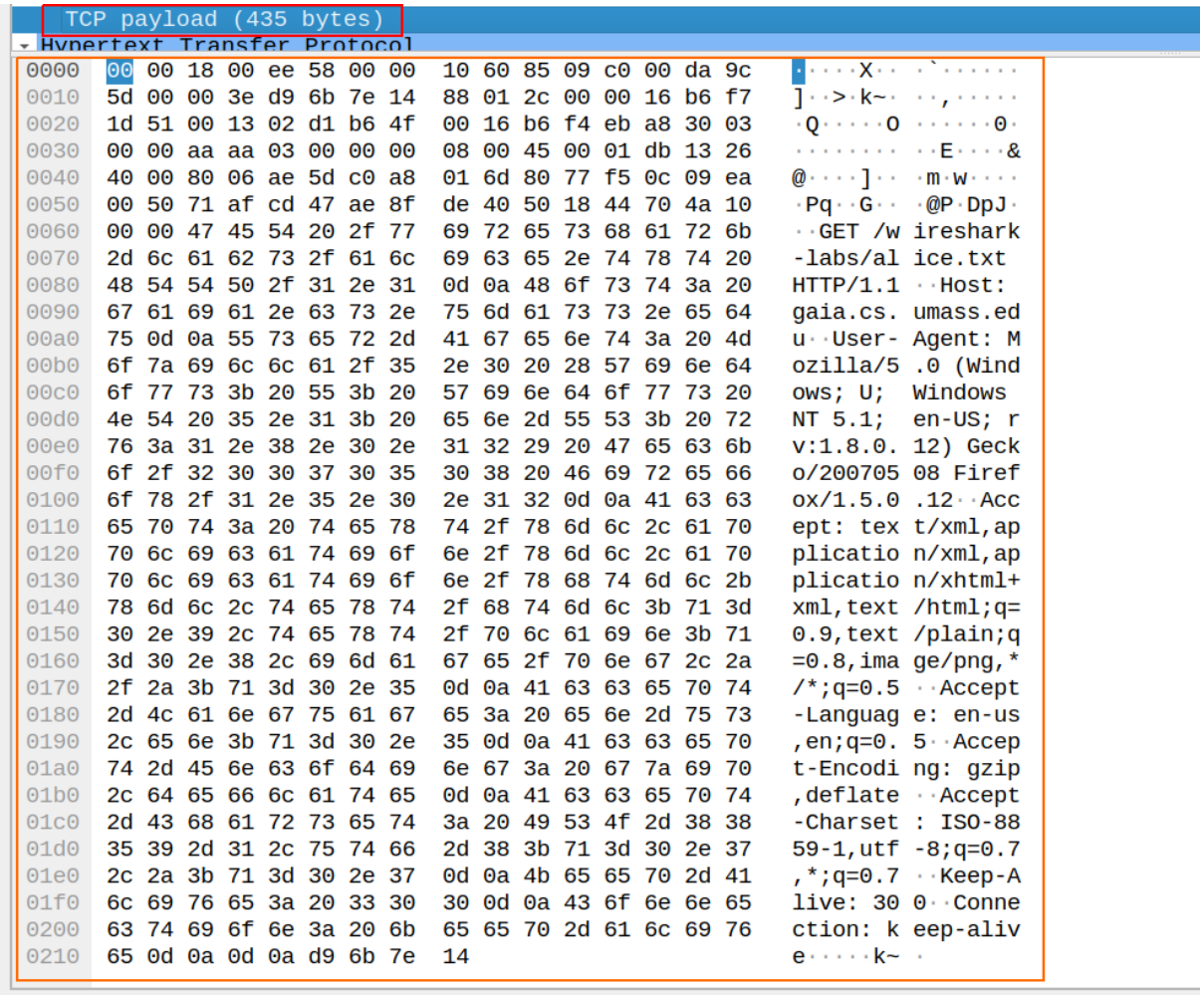
AP - Access Point

Since the trace starts with the host already associated with the AP, let first look at data transfer over an 802.11 association before looking at AP association/disassociation. Recall that in this trace, at t = 24.82, the host makes an HTTP request to http://gaia.cs.umass.edu/wireshark-labs/alice.txt. The IP address of gaia.cs.umass.edu is 128.119.245.12. Then, at t=32.82, the host makes an HTTP request to http://www.cs.umass.edu.

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.

Почитать про мак-адреса в wifi тут.

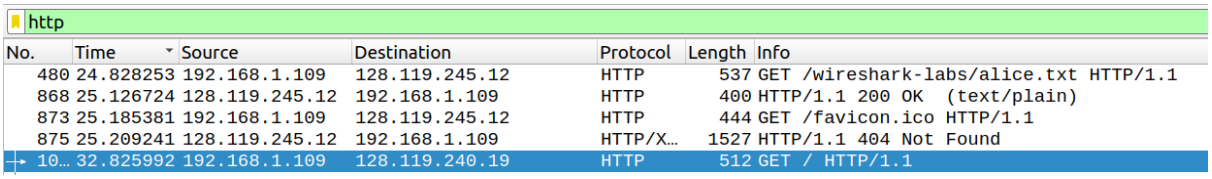




Тыкаем на ‘IEEE 802.11 QoS Data, Flags: .....TC’ и получаем:

```
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]
```

Теперь для запроса на http://www.cs.umass.edu
В поиске пишем ‘http’



Находим нужный запрос.

```
    [Bytes sent since last PSH flag: 410]
  [Timestamps]
    [Time since first frame in this TCP stream: 0.017418000 seconds]
    [Time since previous frame in this TCP stream: 0.000361000 seconds]
  TCP payload (410 bytes)
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      [GET / HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /
    Request Version: HTTP/1.1
  Host: www.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://www.cs.umass.edu/]
  [HTTP request 1/1]
  [Response in frame: 1066]
```

Проверили, что это правда он))

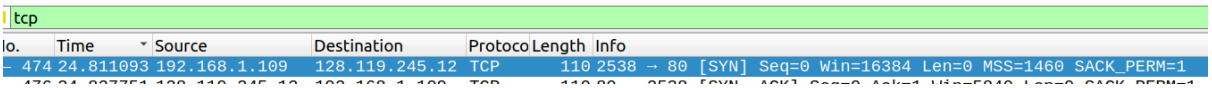
Мак-адреса

```
IEEE 802.11 QoS Data, Flags: .......TC
  Type/Subtype: QoS Data (0x0028)
  Frame Control Field: 0x8801
    .... ..00 = Version: 0
    .... 10.. = Type: Data frame (2)
    1000 .... = Subtype: 8
    Flags: 0x01
      .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
      .... .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... .... = 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 0110 1110 .... = Sequence number: 110
  Frame check sequence: 0xb8bac0f8 [unverified]
  [FCS Status: Unverified]
  Qos Control: 0x0000
```

Поближе глянем да.

```
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 0110 1110 .... = Sequence number: 110
Frame check sequence: 0xb8bac0f8 [unverified]
[FCS Status: Unverified]
```

Теперь ответики на вопросики.



Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)?

Transmitter addr: 00:13:02:d1:b6:4f

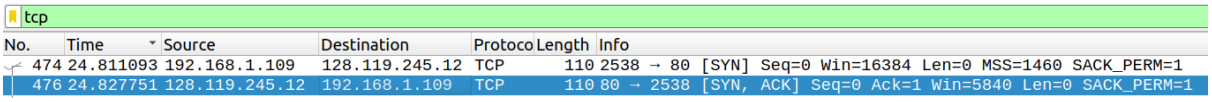
"For a beacon frame in 802.11, the transmitter address and the Source address are the same."

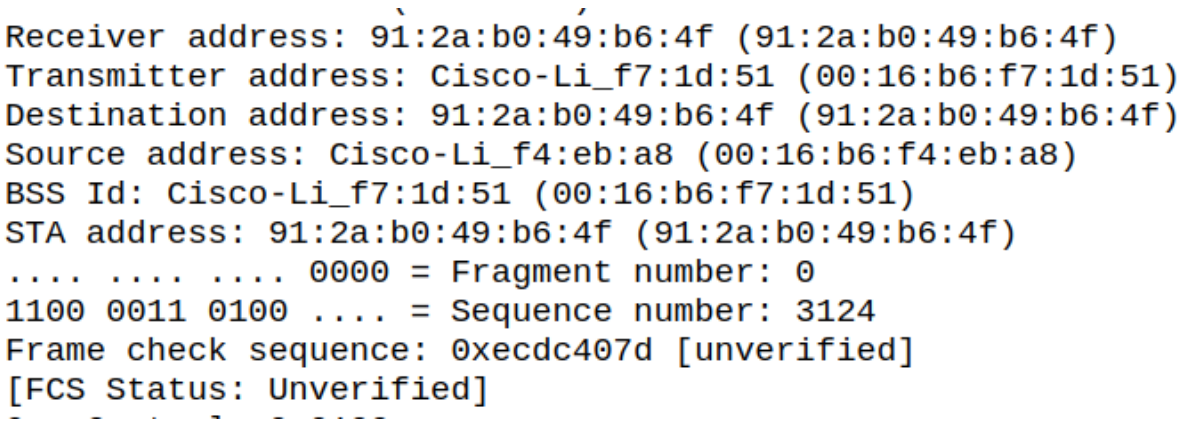
AP: 00:16:b6:f7:1d:51

First hop router:00:16:b6:f4:eb:a8

НАПИСАТЬ ЧЕГО-НИТЬ ПРО ОБЪЯНЕНИЕ

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).





host: 91:2a:b0:49:b6:4f
AP: 00:16:b6:f4:eb:a8
First-hop router: 00:16:b6:f7:1d:51