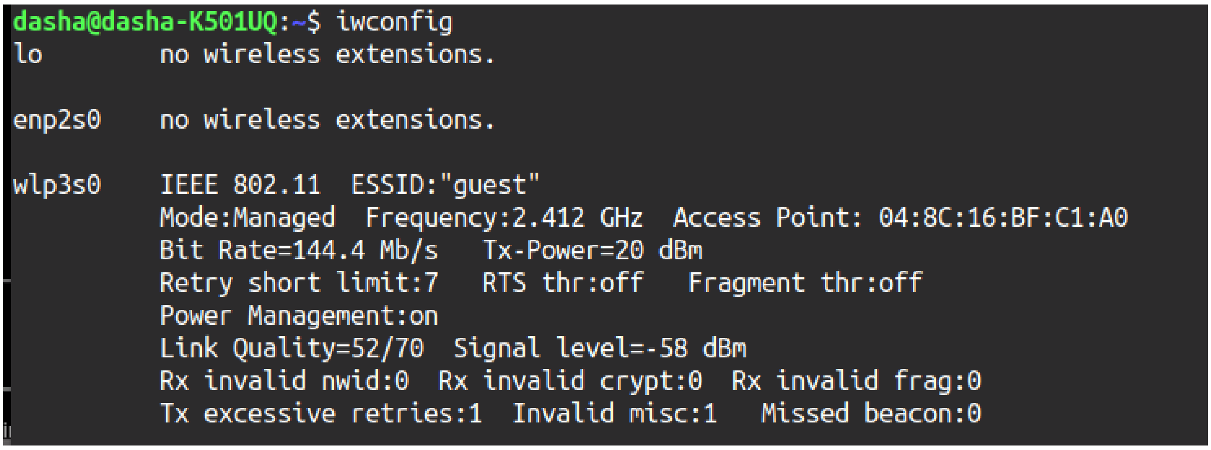
Wireshark

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

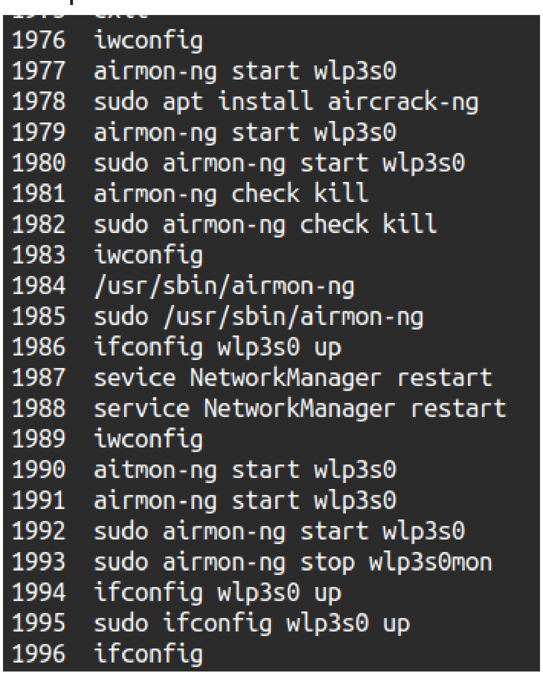
SSID (Service Set Identifier) — это символьное название беспроводной точки доступа Wi-Fi, служащее для идентификации её среди других точек пользователями или устройствами, подключающимися к сети.

‘iwconfig’ - configure a wireless network interface



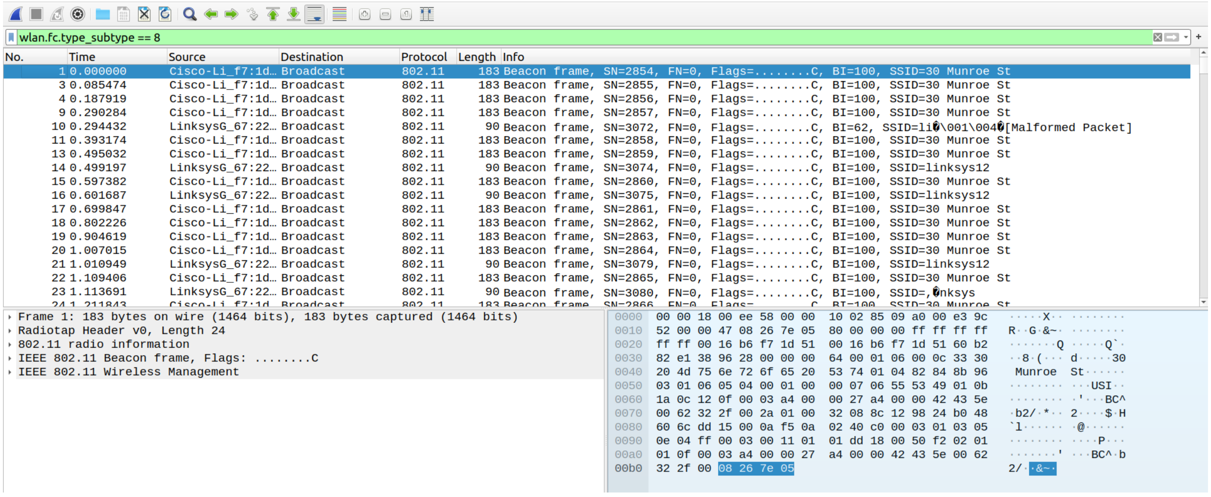
```
dasha@dasha-K501UQ:~$ iwconfig
lo        no wireless extensions.

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
```

Как выделить только beacon frames?
‘wlan.fc.type_subtype == 8’



wlan.fc.type_subtype == 8

```
No.   Time      Source             Destination  Protocol  Length Info
    1 0.000000  Cisco-Li_f7:1d…  Broadcast    802.11     183 Beacon frame, SN=2854, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
    3 0.085474  Cisco-Li_f7:1d…  Broadcast    802.11     183 Beacon frame, SN=2855, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
    4 0.187919  Cisco-Li_f7:1d…  Broadcast    802.11     183 Beacon frame, SN=2856, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
    9 0.290284  Cisco-Li_f7:1d…  Broadcast    802.11     183 Beacon frame, SN=2857, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   10 0.294432  LinksysG_67:22…  Broadcast    802.11      90 Beacon frame, SN=3072, FN=0, Flags=........C, BI=62, SSID=li�\001\004�[Malformed Packet]
   11 0.393174  Cisco-Li_f7:1d…  Broadcast    802.11     183 Beacon frame, SN=2858, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   13 0.495032  Cisco-Li_f7:1d…  Broadcast    802.11     183 Beacon frame, SN=2859, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   14 0.499197  LinksysG_67:22…  Broadcast    802.11      90 Beacon frame, SN=3074, FN=0, Flags=........C, BI=100, SSID=linksys12
   15 0.597382  Cisco-Li_f7:1d…  Broadcast    802.11     183 Beacon frame, SN=2860, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   16 0.601687  LinksysG_67:22…  Broadcast    802.11      90 Beacon frame, SN=3075, FN=0, Flags=........C, BI=100, SSID=linksys12
   17 0.699847  Cisco-Li_f7:1d…  Broadcast    802.11     183 Beacon frame, SN=2861, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   18 0.802226  Cisco-Li_f7:1d…  Broadcast    802.11     183 Beacon frame, SN=2862, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   19 0.904619  Cisco-Li_f7:1d…  Broadcast    802.11     183 Beacon frame, SN=2863, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   20 1.007015  Cisco-Li_f7:1d…  Broadcast    802.11     183 Beacon frame, SN=2864, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   21 1.010949  LinksysG_67:22…  Broadcast    802.11      90 Beacon frame, SN=3079, FN=0, Flags=........C, BI=100, SSID=linksys12
   22 1.109406  Cisco-Li_f7:1d…  Broadcast    802.11     183 Beacon frame, SN=2865, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   23 1.113691  LinksysG_67:22…  Broadcast    802.11      90 Beacon frame, SN=3080, FN=0, Flags=........C, BI=100, SSID=,�nksys
   24 1.211843  Cisco-Li_f7:1d…  Broadcast    802.11     183 Beacon frame, SN=2866, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
```

```
› Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
› Radiotap Header v0, Length 24
› 802.11 radio information
› IEEE 802.11 Beacon frame, Flags: ........C
› IEEE 802.11 Wireless Management
```

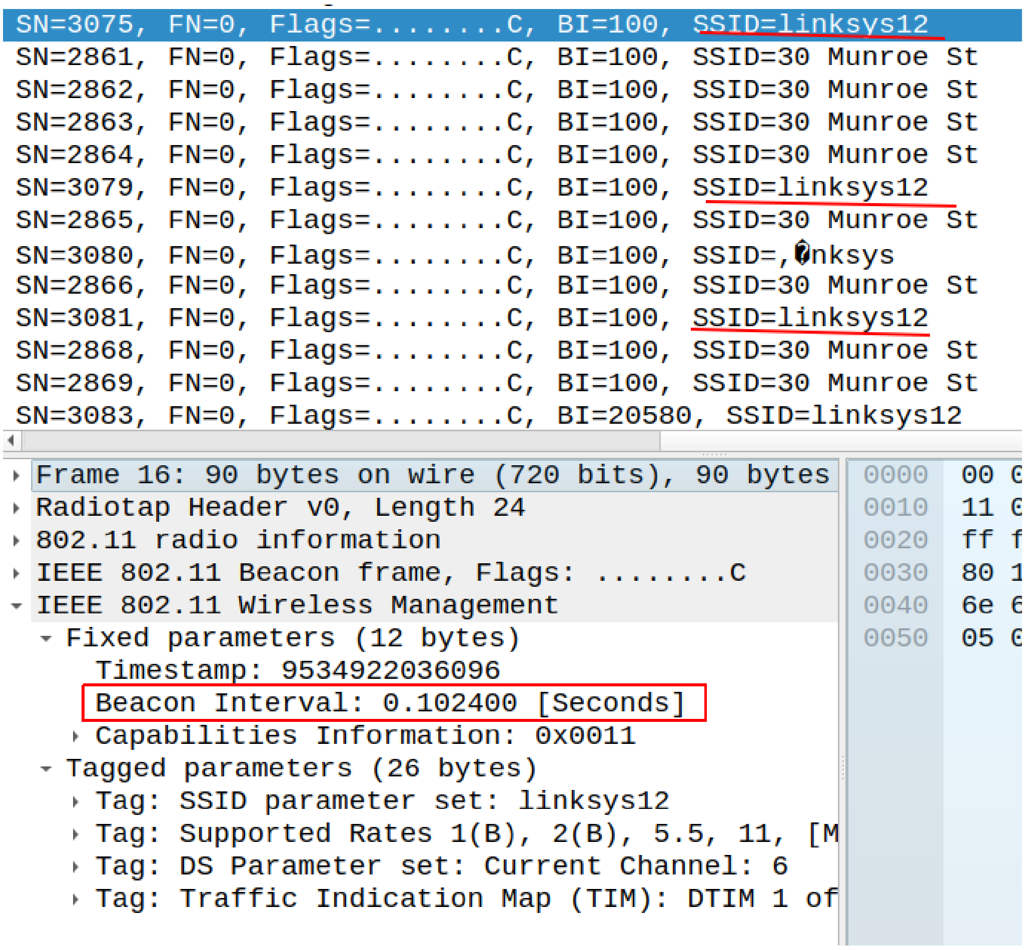
```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e3 9c   ·····X·· ········
0010  52 00 00 47 08 26 7e 05  80 00 00 00 ff ff ff ff   R··G·&~· ········
0020  ff ff 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 60 b2   ·······Q ·····Q`·
0030  82 e1 38 96 28 00 00 00  64 00 01 06 00 0c 33 30   ··8·(··· d·····30
0040  20 4d 75 6e 72 6f 65 20  53 74 01 04 82 84 8b 96    Munroe  St······
0050  03 01 06 05 04 00 01 00  00 07 06 55 53 49 01 0b   ········ ···USI··
0060  1a 0c 12 0f 00 03 a4 00  00 27 a4 00 00 42 43 5e   ········ ·'···BC^
0070  00 62 32 2f 00 2a 01 00  32 08 8c 12 98 24 b0 48   ·b2/·*·· 2····$·H
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   ········ ····P···
00a0  01 0f 00 03 a4 00 00 27  a4 00 00 42 43 5e 00 62   ·······' ···BC^·b
00b0  32 2f 00 08 26 7e 05                               2/··&~·
```

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).

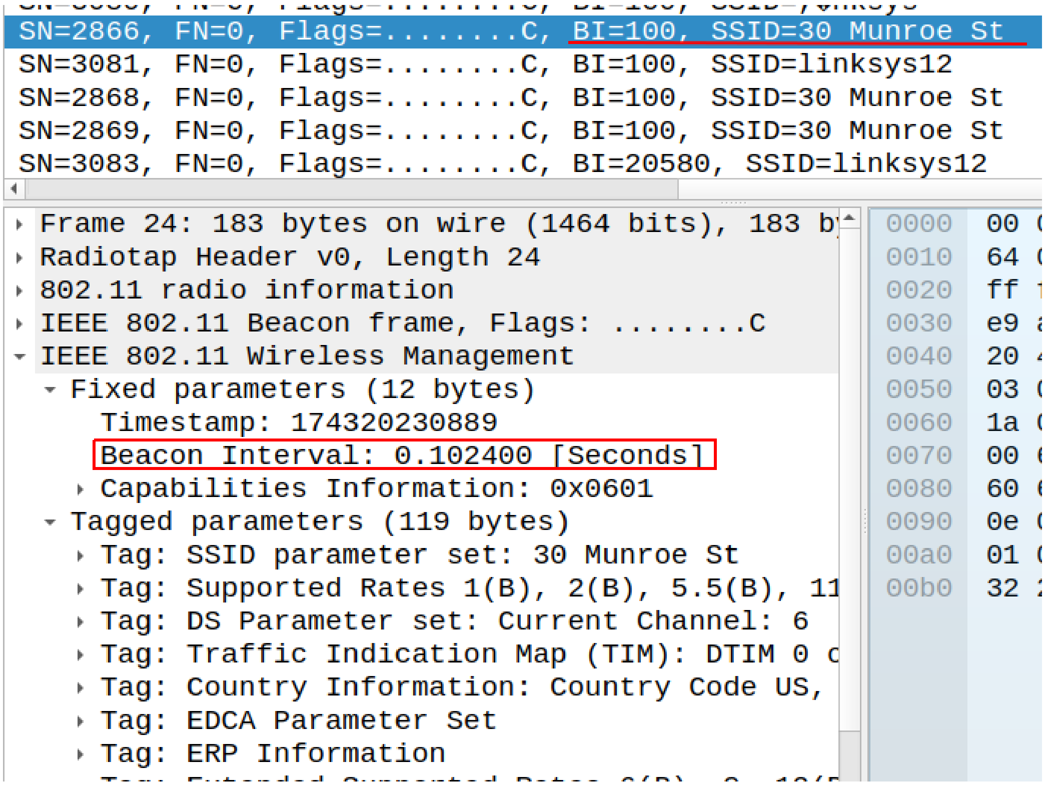
Для обоих точек доступа это время составляет
Beacon Interval: 0.102400 [Seconds]



```
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
```



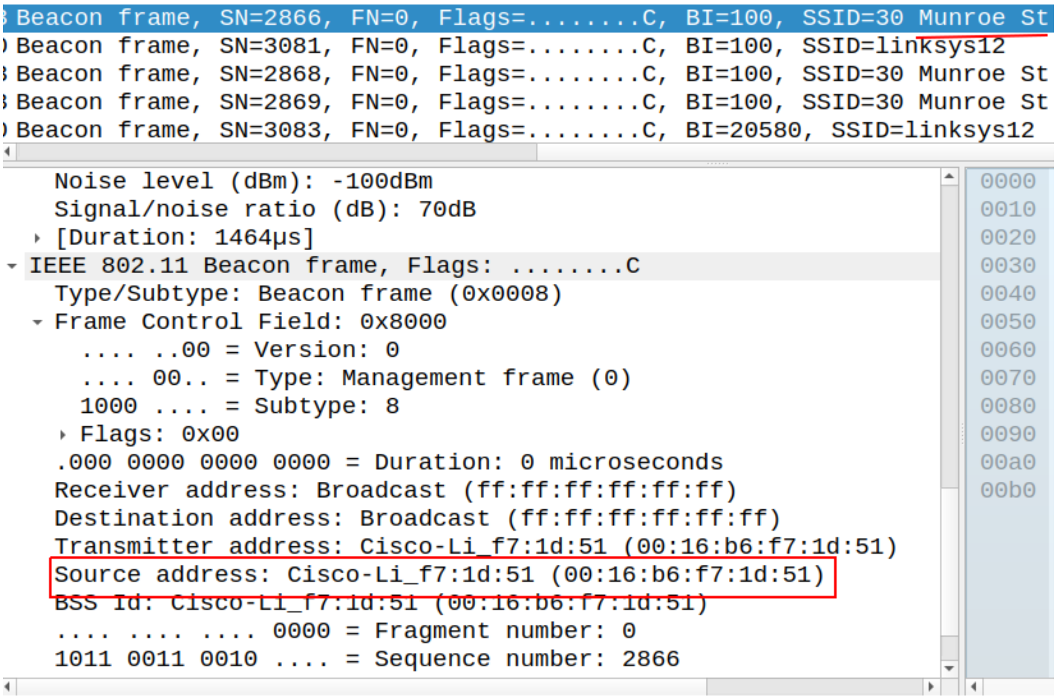
```
SN=3080, FN=0, Flags=........C, BI=100, SSID=,�nksys
SN=2866, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
SN=3081, FN=0, Flags=........C, BI=100, SSID=linksys12
SN=2868, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
SN=2869, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
SN=3083, FN=0, Flags=........C, BI=20580, SSID=linksys12
```

```
Frame 24: 183 bytes on wire (1464 bits), 183 by
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 o
    Tag: Country Information: Country Code US,
    Tag: EDCA Parameter Set
    Tag: ERP Information
    Tag: Extended Supported Rates 6(B), 9, 12(B
```

```
0000  00 (
0010  64 (
0020  ff f
0030  e9 a
0040  20 4
0050  03 (
0060  1a (
0070  00 (
0080  60 (
0090  0e (
00a0  01 (
00b0  32 2
```

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)**



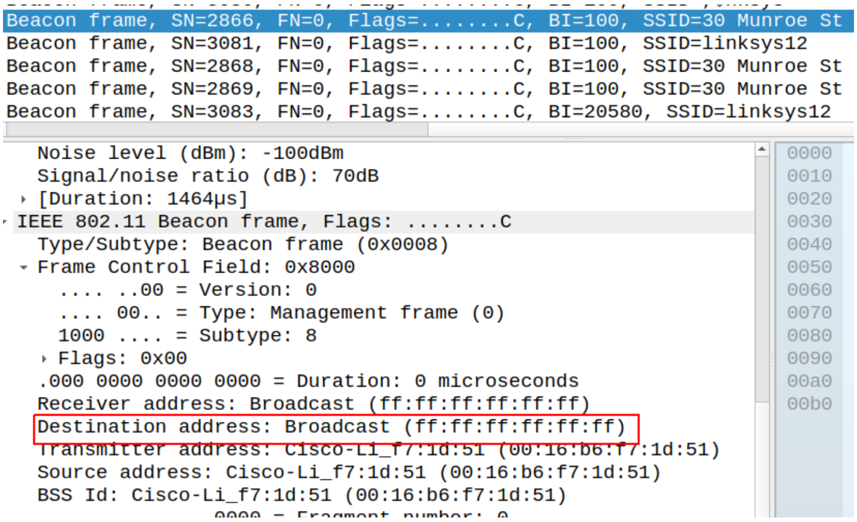
```
Beacon frame, SN=2866, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
Beacon frame, SN=3081, FN=0, Flags=........C, BI=100, SSID=linksys12
Beacon frame, SN=2868, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
Beacon frame, SN=2869, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
Beacon frame, SN=3083, FN=0, Flags=........C, BI=20580, SSID=linksys12
```

```
    Noise level (dBm): -100dBm
    Signal/noise ratio (dB): 70dB
  ▸ [Duration: 1464µs]
▾ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  ▾ Frame Control Field: 0x8000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1000 .... = Subtype: 8
    ▸ 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 0011 0010 .... = Sequence number: 2866
```

```
0000
0010
0020
0030
0040
0050
0060
0070
0080
0090
00a0
00b0
```

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)**



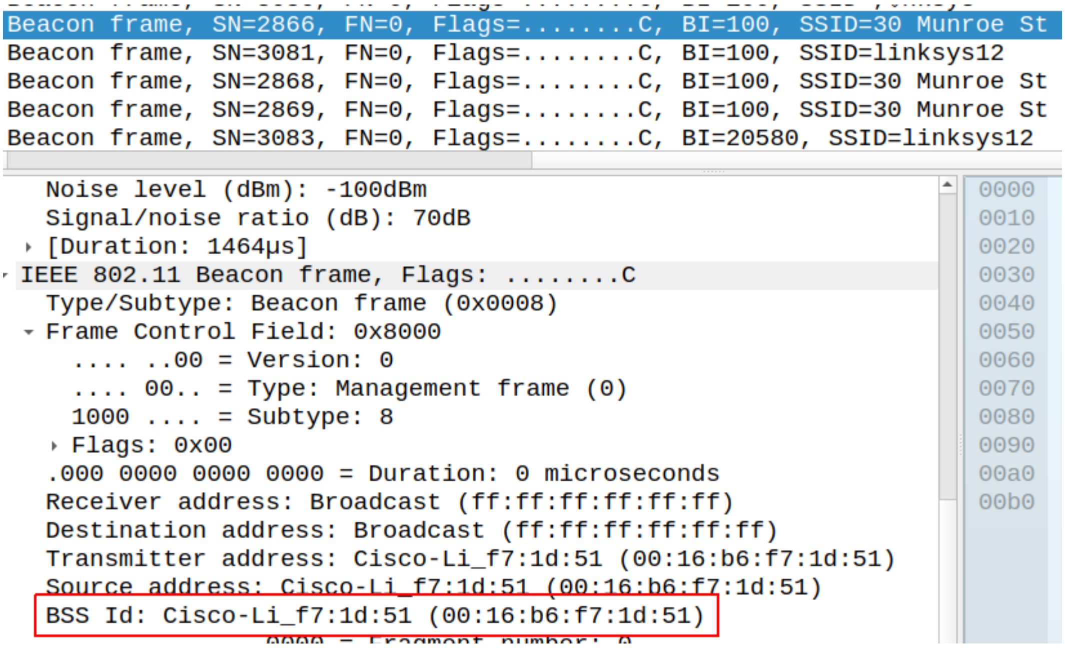
```
Beacon frame, SN=2866, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
Beacon frame, SN=3081, FN=0, Flags=........C, BI=100, SSID=linksys12
Beacon frame, SN=2868, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
Beacon frame, SN=2869, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
Beacon frame, SN=3083, FN=0, Flags=........C, BI=20580, SSID=linksys12
```

```
    Noise level (dBm): -100dBm
    Signal/noise ratio (dB): 70dB
  ▸ [Duration: 1464µs]
▾ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  ▾ Frame Control Field: 0x8000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1000 .... = Subtype: 8
    ▸ 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
```

```
0000
0010
0020
0030
0040
0050
0060
0070
0080
0090
00a0
00b0
```

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**)



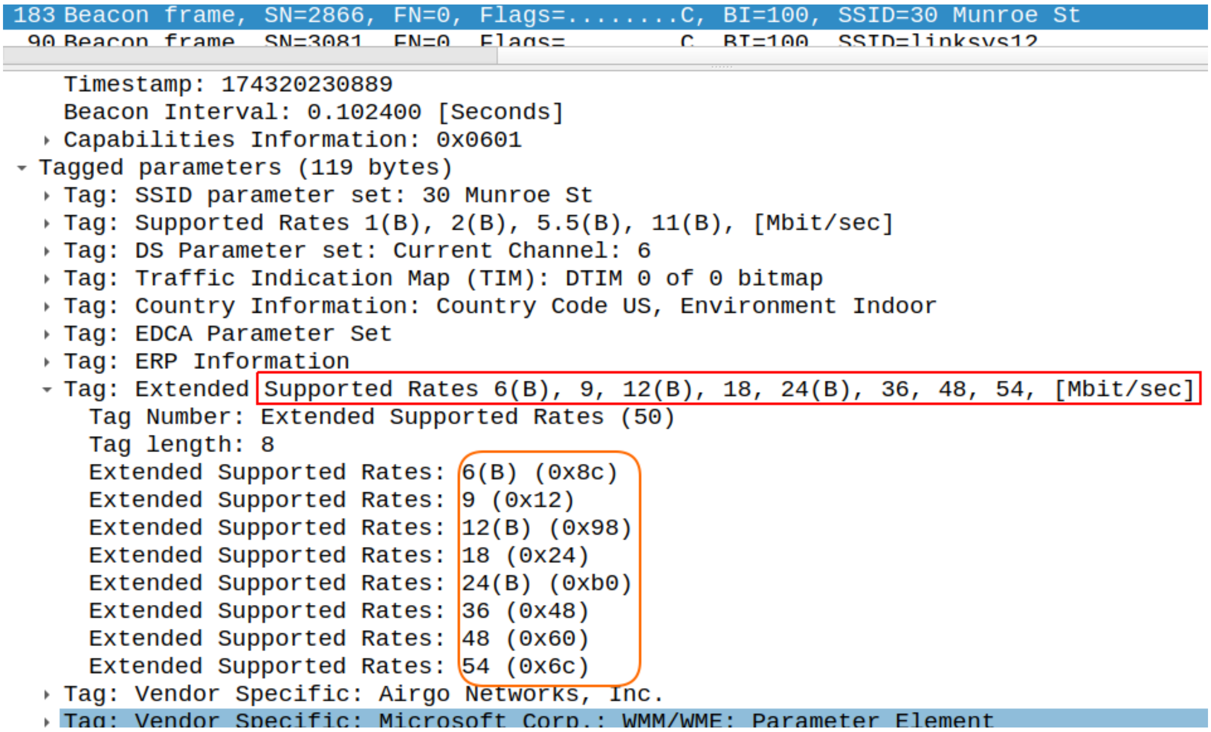
```
Beacon frame, SN=2866, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
Beacon frame, SN=3081, FN=0, Flags=........C, BI=100, SSID=linksys12
Beacon frame, SN=2868, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
Beacon frame, SN=2869, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
Beacon frame, SN=3083, FN=0, Flags=........C, BI=20580, SSID=linksys12
```

```
   Noise level (dBm): -100dBm
   Signal/noise ratio (dB): 70dB
 ▸ [Duration: 1464µs]
▾ IEEE 802.11 Beacon frame, Flags: ........C
   Type/Subtype: Beacon frame (0x0008)
 ▾ Frame Control Field: 0x8000
     .... ..00 = Version: 0
     .... 00.. = Type: Management frame (0)
     1000 .... = Subtype: 8
   ▸ 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
```

```
0000
0010
0020
0030
0040
0050
0060
0070
0080
0090
00a0
00b0
```

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]



```
183 Beacon frame, SN=2866, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
 90 Beacon frame, SN=3081, FN=0, Flags=........C, BI=100, SSID=linksys12
```

```
     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(B), [Mbit/sec]
   ▸ Tag: DS Parameter set: Current Channel: 6
   ▸ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 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 Number: Extended Supported Rates (50)
       Tag length: 8
       Extended Supported Rates: 6(B) (0x8c)
       Extended Supported Rates: 9 (0x12)
       Extended Supported Rates: 12(B) (0x98)
       Extended Supported Rates: 18 (0x24)
       Extended Supported Rates: 24(B) (0xb0)
       Extended Supported Rates: 36 (0x48)
       Extended Supported Rates: 48 (0x60)
       Extended Supported Rates: 54 (0x6c)
   ▸ Tag: Vendor Specific: Airgo Networks, Inc.
   ▸ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```