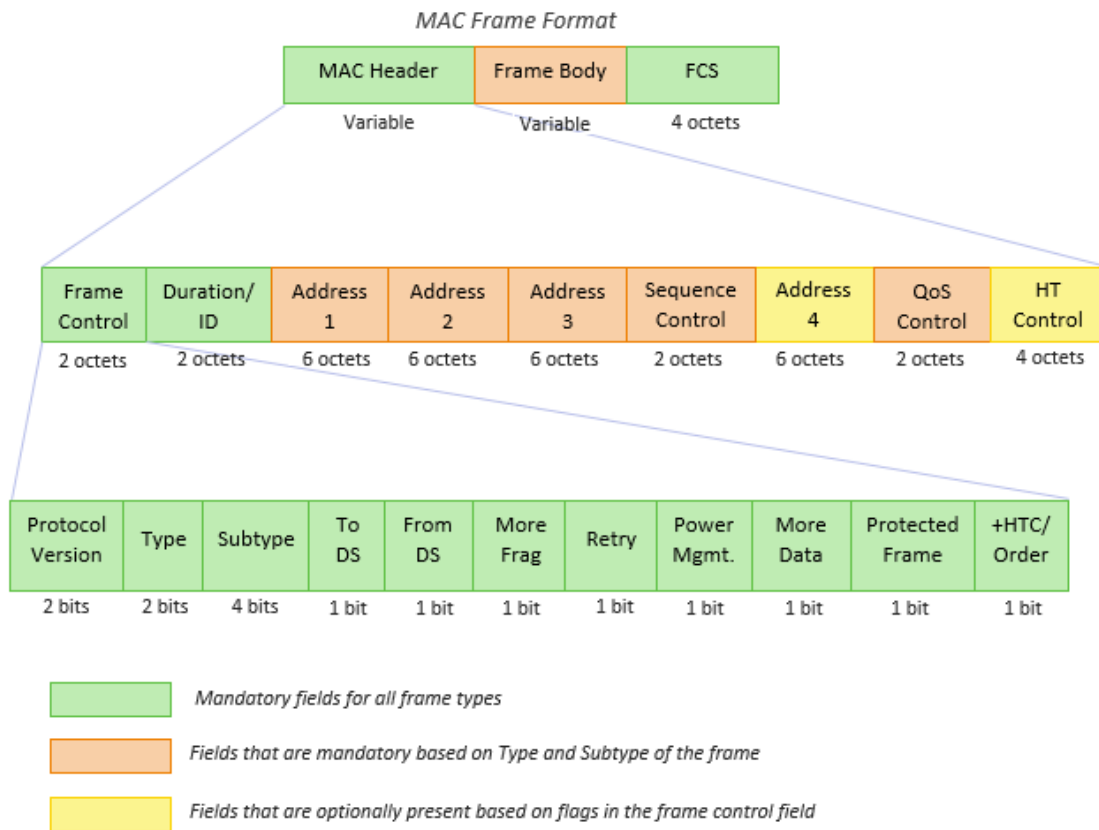


# WIFI AND WIRESHARK

## 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 service NetworkManager restart
1988 service NetworkManager restart
1989 iwconfig
1990 airmon-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

Beacon Frame - кадр маяка

Как выделить только beacon frames?

'wlan.fc.type\_subtype == 8'

No.	Time	Source	Destination	Protocol	Length	Info
10	0.000000	Cisco-L1-f7:1d...	Broadcast	802.11	183	Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
3	0.085474	Cisco-L1-f7:1d...	Broadcast	802.11	183	Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4	0.187919	Cisco-L1-f7:1d...	Broadcast	802.11	183	Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
9	0.290284	Cisco-L1-f7:1d...	Broadcast	802.11	183	Beacon frame, SN=2857, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
10	0.294432	Linksys6_67:22...	Broadcast	802.11	90	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=110\001\0040(Malformed Packet)
11	0.393174	Cisco-L1-f7:1d...	Broadcast	802.11	183	Beacon frame, SN=2858, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
13	0.495032	Cisco-L1-f7:1d...	Broadcast	802.11	183	Beacon frame, SN=2859, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
14	0.499197	Linksys6_67:22...	Broadcast	802.11	90	Beacon frame, SN=3074, FN=0, Flags=.....C, BI=100, SSID=linksys12
15	0.597382	Cisco-L1-f7:1d...	Broadcast	802.11	183	Beacon frame, SN=2860, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
16	0.601687	Linksys6_67:22...	Broadcast	802.11	90	Beacon frame, SN=3075, FN=0, Flags=.....C, BI=100, SSID=linksys12
17	0.699847	Cisco-L1-f7:1d...	Broadcast	802.11	183	Beacon frame, SN=2861, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
18	0.802226	Cisco-L1-f7:1d...	Broadcast	802.11	183	Beacon frame, SN=2862, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
19	0.904619	Cisco-L1-f7:1d...	Broadcast	802.11	183	Beacon frame, SN=2863, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
20	1.007015	Cisco-L1-f7:1d...	Broadcast	802.11	183	Beacon frame, SN=2864, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
21	1.010949	Linksys6_67:22...	Broadcast	802.11	90	Beacon frame, SN=3076, FN=0, Flags=.....C, BI=100, SSID=linksys12
22	1.109408	Cisco-L1-f7:1d...	Broadcast	802.11	183	Beacon frame, SN=2865, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
23	1.113691	Linksys6_67:22...	Broadcast	802.11	90	Beacon frame, SN=3080, FN=0, Flags=.....C, BI=100, SSID=linksys12
24	1.211843	Cisco-L1-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) on interface 0  
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 00 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 39 ..8(.....d....39  
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 .....BCA.....  
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 .....!.....P.....  
00b0 32 2f 00 00 25 7e 05 2f 00 00 42 43 5e 00 62 .....&.....BCA b

Что такое SSID?

**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. SSID представляет собой строку, размером до 32 байт, которая передается широкоэвещательно в эфир. Расположенные рядом с сетью устройства принимают название и если им разрешено присоединиться к точке доступа, то соединяются с ней.

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 обеих 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=linksys

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 6

0010 11 6

0020 ff f

0030 80 1

0040 6e 6

0050 05 6

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 6

0010 64 0

0020 ff 7

0030 e9 a

0040 20 4

0050 03 0

0060 1a 0

0070 00 0

0080 60 0

0090 0e 0

00a0 01 0

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
```

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
```



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)
```

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
```

## DATA TRANSFER

### AP - Access Point

Согласно процессу «[трёхкратного рукопожатия](#)» TCP, клиент посылает пакет с установленным флагом SYN (*synchronize*). В ответ на него сервер должен ответить комбинацией флагов SYN+ACK (*acknowledges*). После этого клиент должен ответить пакетом с флагом ACK, после чего соединение считается установленным.

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](#).

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 Ack=1 Win=17520 Len=0
479	24.828140		IntelCor_d1:b6:4f (0...	802.11	38	Acknowledgement, Flags=.....C
480	24.828253	192.168.1.109	128.119.245.12	HTTP	537	GET /wireshark-labs/alice.txt HTTP/1.1
481	24.828352		IntelCor_d1:b6:4f (0...	802.11	38	Acknowledgement, Flags=.....C
482	24.846898	128.119.245.12	192.168.1.109	TCP	108	80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
483	24.847058		Cisco-Li_f7:1d:51 (0...	802.11	38	Acknowledgement, Flags=.....C
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
485	24.847267		Cisco-Li_f7:1d:51 (0...	802.11	38	Acknowledgement, Flags=.....C
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 r
487	24.848950		Cisco-Li_f7:1d:51 (0...	802.11	38	Acknowledgement, Flags=.....C

Urgent pointer: 0  
[SEQ/ACK analysis]  
[Timestamps]  
TCP payload (435 bytes)  
Hypertext Transfer Protocol  
GET /wireshark-labs/alice.txt HTTP/1.1  
[Expert Info (Chat/Sequence): GET /wireshark-labs/alice.txt HTTP/1.1  
[Severity level: Chat]  
[Group: Sequence]  
Request Method: GET  
Request URI: /wireshark-labs/alice.txt  
Request Version: HTTP/1.1  
Host: gaia.cs.umass.edu  
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  
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,\*/\*;q=0...  
Accept-Language: en-us,en;q=0.5  
Accept-Encoding: gzip,deflate  
Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7  
Keep-Alive: 300  
Connection: keep-alive  
Full request URI: http://gaia.cs.umass.edu/wireshark-labs/alice.txt  
[HTTP request 172]  
[Response in frame: 868]  
[Next request in frame: 873]

0000 00 00 47 45 54 20 2f  
0070 2d 6c 61 62 73 2f 61  
0080 48 54 54 50 2f 31 2e  
0090 67 61 69 61 2e 63 73  
00a0 75 0d 0a 55 73 65 72  
00b0 6f 7a 69 6c 6c 61 2f  
00c0 6f 77 73 3b 20 55 3f  
00d0 4e 54 20 35 2e 31 3f  
00e0 76 3a 31 2e 38 2e 3e  
00f0 6f 2f 32 30 30 37 3e  
0100 6f 78 2f 31 2e 35 2e  
0110 65 70 74 3a 20 74 65  
0120 70 6c 69 63 61 74 65  
0130 70 6c 69 63 61 74 65  
0140 78 6d 6c 2c 74 65 7e  
0150 30 2e 39 2c 74 65 7e  
0160 3d 30 2e 38 2c 69 6c  
0170 2f 2a 3b 71 3d 30 2e  
0180 2d 4c 61 6e 67 75 61  
0190 2c 65 6e 3b 71 3d 3e  
01a0 74 2d 45 6e 63 6f 64  
01b0 2c 64 65 6e 6c 61 74  
01c0 2d 43 68 61 72 73 65  
01d0 35 39 2d 31 2c 75 74  
01e0 2c 2a 3b 71 3d 30 2e  
01f0 6c 69 76 65 3a 20 35

The full requested URI (including host name) (http.request.full\_uri) Packets: 2364 · Displayed: 2364 (100.0%)

TCP payload (435 bytes)										
Hypertext Transfer Protocol										
0000	00	00	18	00	ee	58	00	00	10 60 85 09 c0 00 da 9c	. . . . .X . . . . .
0010	5d	00	00	3e	d9	6b	7e	14	88 01 2c 00 00 16 b6 f7	] . . > . k ~ . . . . .
0020	1d	51	00	13	02	d1	b6	4f	00 16 b6 f4 eb a8 30 03	. Q . . . . .0 . . . . .
0030	00	00	aa	aa	03	00	00	00	08 00 45 00 01 db 13 26	. . . . . . . E . . . . .
0040	40	00	80	06	ae	5d	c0	a8	01 6d 80 77 f5 0c 09 ea	@ . . . .] . . . m . w . . .
0050	00	50	71	af	cd	47	ae	8f	de 40 50 18 44 70 4a 10	. P q . . G . . . @ P . D p J .
0060	00	00	47	45	54	20	2f	77	69 72 65 73 68 61 72 6b	. . GET /w ireshark
0070	2d	6c	61	62	73	2f	61	6c	69 63 65 2e 74 78 74 20	-labs/al ice.txt
0080	48	54	54	50	2f	31	2e	31	0d 0a 48 6f 73 74 3a 20	HTTP/1.1 . . Host:
0090	67	61	69	61	2e	63	73	2e	75 6d 61 73 73 2e 65 64	gaia.cs. umass.ed
00a0	75	0d	0a	55	73	65	72	2d	41 67 65 6e 74 3a 20 4d	u . . User- Agent: M
00b0	6f	7a	69	6c	6c	61	2f	35	2e 30 20 28 57 69 6e 64	ozilla/5 .0 (Wind
00c0	6f	77	73	3b	20	55	3b	20	57 69 6e 64 6f 77 73 20	ows; U; Windows
00d0	4e	54	20	35	2e	31	3b	20	65 6e 2d 55 53 3b 20 72	NT 5.1; en-US; r
00e0	76	3a	31	2e	38	2e	30	2e	31 32 29 20 47 65 63 6b	v:1.8.0. 12) Geck
00f0	6f	2f	32	30	30	3f	30	35	30 38 20 46 69 72 65 66	o/200705 08 Firef
0100	6f	78	2f	31	2e	35	2e	30	2e 31 32 0d 0a 41 63 63	ox/1.5.0 .12 . Acc
0110	65	70	74	3a	20	74	65	78	74 2f 78 6d 6c 2c 61 70	ept: tex t/xml, ap
0120	70	6c	69	63	61	74	69	6f	6e 2f 78 6d 6c 2c 61 70	plicatio n/xml, ap
0130	70	6c	69	63	61	74	69	6f	6e 2f 78 68 74 6d 6c 2b	plicatio n/xhtml+
0140	78	6d	6c	2c	74	65	78	74	2f 68 74 6d 6c 3b 71 3d	xml, text /html; q=
0150	30	2e	39	2c	74	65	78	74	2f 70 6c 61 69 6e 3b 71	0.9, text /plain; q
0160	3d	30	2e	38	2c	69	6d	61	67 65 2f 70 6e 67 2c 2a	=0.8, ima ge/png, *
0170	2f	2a	3b	71	3d	30	2e	35	0d 0a 41 63 63 65 70 74	/*; q=0.5 . . Accept
0180	2d	4c	61	6e	67	75	61	67	65 3a 20 65 6e 2d 75 73	-Languag e: en-us
0190	2c	65	6e	3b	71	3d	30	2e	35 0d 0a 41 63 63 65 70	, en; q=0. 5 . . Accep
01a0	74	2d	45	6e	63	6f	64	69	6e 67 3a 20 67 7a 69 70	t-Encodi ng: gzip
01b0	2c	64	65	66	6c	61	74	65	0d 0a 41 63 63 65 70 74	, deflate . . Accept
01c0	2d	43	68	61	72	73	65	74	3a 20 49 53 4f 2d 38 38	-Charset : ISO-88
01d0	35	39	2d	31	2c	75	74	66	2d 38 3b 71 3d 30 2e 37	59-1, utf -8; q=0.7
01e0	2c	2a	3b	71	3d	30	2e	37	0d 0a 4b 65 65 70 2d 41	, *; q=0.7 . . Keep-A
01f0	6c	69	76	65	3a	20	33	30	30 0d 0a 43 6f 6e 6e 65	live: 30 0 . . Conne
0200	63	74	69	6f	6e	3a	20	6b	65 65 70 2d 61 6c 69 76	ction: k eep-aliv
0210	65	0d	0a	0d	0a	d9	6b	7e	14	e . . . . . k ~ . .

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'

http							
No.	Time	Source	Destination	Protocol	Length	Info	
480	24.828253	192.168.1.109	128.119.245.12	HTTP	537	GET /wireshark-labs/alice.txt HTTP/1.1	
868	25.126724	128.119.245.12	192.168.1.109	HTTP	400	HTTP/1.1 200 OK (text/plain)	
873	25.185381	192.168.1.109	128.119.245.12	HTTP	444	GET /favicon.ico HTTP/1.1	
875	25.209241	128.119.245.12	192.168.1.109	HTTP/X...	1527	HTTP/1.1 404 Not Found	
10...	32.825992	192.168.1.109	128.119.240.19	HTTP	512	GET / HTTP/1.1	

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

```

## Различия между DA, SA, RA, TA

Basically yes. In 802.11 you can see a different number of these depending on where the frame is coming from and where it's going:

- "Destination Address" or "DA" is the MAC of the final destination of the frame.
- "Source Address" or "SA" is the MAC of the original sender of the frame.
- "Receiver Address" or "RA" is the MAC of the next immediate recipient of the frame.
- "Transmitter Address" or "TA" is the MAC of the system that is directly transmitting the frame.

So, original source (SA), final destination (DA), and the immediate sending/receiving systems (TA/RA) are four different MACs. Formal definitions would be found in the 802.11 standard itself:

## Ин Рашн лангуаге

DA — Destination address — адрес получателя;

SA — Source address — адрес отправителя, назначении такое же как и в Ethernet.

RA — Receiver address — используется, чтобы указать устройства, которые принимают данные из беспроводной среды;

TA — Transmitter address — используется, чтобы указать устройства, которые передают данные в эту среду.

### [Differences between AP and Router](#)

Точка доступа - это просто точка доступа. WiFi-роутер - это роутер+точка доступа, два в одном.

Читать [тут](#):

- роутер подключается непосредственно к оборудованию провайдера и раздает IP-адреса. Точка доступа просто ретранслирует подключение, не подключаясь к провайдеру напрямую;
- точка доступа «раздает» Интернет по беспроводной технологии. К роутеру или модему, связанному с провайдером, она может подключаться по Wi-Fi или посредством кабеля. Маршрутизатор поддерживает оба типа связи;
- точка доступа, в отличие от роутера, не имеет встроенного брандмауэра.

Как вообще происходит передача данных в 802.11? Читать [тут](#).

Тоже хорошая статья на [Хабре](#).

Хорошая [статья](#) в пдфке.

Теперь ответы на вопросы.

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

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)
.... = Fragment number: 0
0000 0110 1110 .... = Sequence number: 110
Frame check sequence: 0xb8bac0f8 [unverified]
[FCS Status: Unverified]
```

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

Wireless host (source addr): 00:13:02:d1:b6:4f

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.”](#)

- To the access point? AP: 00:16:b6:f7:1d:51
- To the first-hop router? First hop router: 00:16:b6:f4:eb:a8
- Destination? 00:16:b6:f4:eb:a8

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).

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

What are three MAC address fields in the 802.11 frame?

```
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
```

- Which MAC address in this frame corresponds to the host? 91:2a:b0:49:b6:4f
- To the access point? 00:16:b6:f4:eb:a8
- To the first-hop router? 00:16:b6:f7:1d:51

## ASSOCIATION/DISASSOCIATION

[Bax-bax-bax must read.](#)

Recall from Section 7.3.1 in the text that a host must first associate with an access point before sending data. Association in 802.11 is performed using the ASSOCIATE REQUEST frame (sent from host to AP, with a frame type 0 and subtype 0, see Section 7.3.3 in the text) and the ASSOCIATE RESPONSE frame (sent by the AP to a host with a frame type 0 and subtype of 1, in response to a received ASSOCIATE REQUEST). For a detailed explanation of each field in the 802.11 frame, see page 34 (Section 7) of the 802.11 spec at <http://gaia.cs.umass.edu/wireshark-labs/802.11-1999.pdf> .

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?

In some digital communication protocols, ACK -- short for acknowledgement -- refers to a signal that a device sends to indicate that data has been received successfully.



## Как работает TCP-протокол?

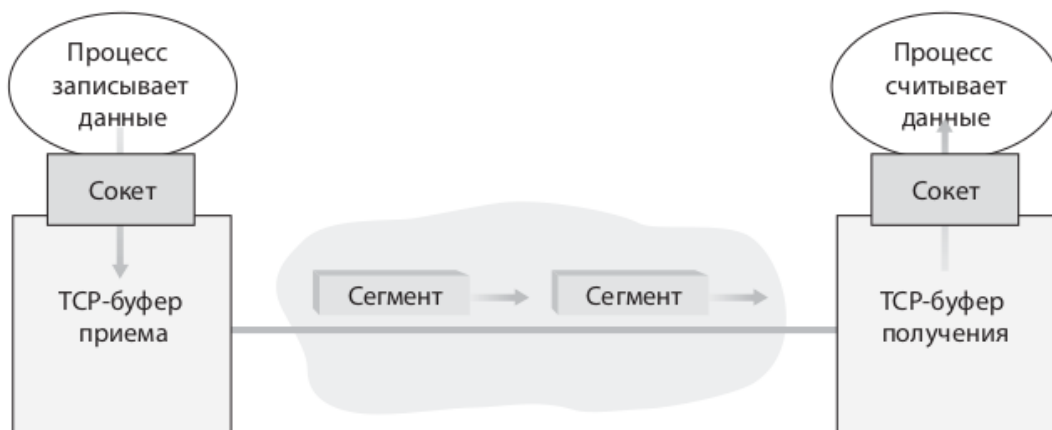
Соединение TCP обеспечивает **дуплексную** передачу файлов. Если оно установлено между процессом А на одном хосте и процессом Б на другом хосте, то данные прикладного уровня могут одновременно передаваться как от процесса А к процессу Б, так и в обратном направлении. Кроме того, TCP-соединение всегда является **двухточечным**, то есть устанавливается между единственной парой отправитель-получатель. Другими словами, при использовании протокола TCP невозможно осуществлять широковещательную передачу данных (см. раздел 4.7), когда они передаются от одного отправителя нескольким получателям за одну операцию. Для протокола TCP два хоста — компания, а три уже толпа!

Теперь рассмотрим, как устанавливается TCP-соединение. Предположим, процесс, запущенный на одном хосте, желает установить

соединение с процессом, выполняющимся на другом хосте. Напомним, что процесс, который инициирует соединение, называется *клиентским*, другой же — *серверным*. Процесс клиентского приложения в первую очередь информирует транспортный уровень клиента о том, что хочет установить соединение с серверным процессом. Клиентская программа. Сейчас достаточно знать, что сначала клиент отправляет специальный TCP-сегмент; затем сервер отвечает вторым специальным TCP-сегментом; и, наконец, клиент снова отвечает третьим специальным сегментом. Первые два сегмента не несут никакой полезной нагрузки, то есть не содержат никаких данных прикладного уровня; третий сегмент уже может содержать такие данные. Процедура установления включает отправку трех сегментов, поэтому зачастую ее называют **тройным руко-**

Когда TCP-соединение установлено, оба прикладных процесса могут отправлять данные друг другу. Давайте рассмотрим процесс передачи данных от клиентского процесса серверному. Процесс клиента передает поток данных через сокет («дверь» процесса), как описано в разделе 2.7. Как только данные прошли через эту дверь, они попадают в распоряжение протокола TCP, запущенного на стороне клиента. Как показано на рис. 3.28, протокол TCP направляет эти данные в **буфер передачи** — один из буферов, создаваемых при установлении соединения. Время от времени TCP будет получать часть данных из буфера и передавать их сетевому уровню. Интересной особенностью спецификации TCP<sup>421</sup> является свобода в выборе моментов для отправки данных, находящихся в буфере. Согласно спецификации, протокол TCP должен «передать эти данные в виде сегментов в любой подходящий для этого момент времени». Максимальный объем данных, который может быть извлечен из буфера и помещен в сегмент, ограничивается **максимальным размером сегмента** (Maximum Segment Size, **MSS**). Обычно MSS устанавливается на основе предварительного измерения длины наибольшего фрагмента канального уровня, который может быть передан текущим хостом (так называемый **максимальный передаваемый блок** (Maximum Transmission Unit, **MTU**)), чтобы быть уверен-

ными, что TCP-сегмент, инкапсулированный в IP-дейтаграмму, вместе с длиной TCP/IP заголовка (обычно 40 байт) полностью будет помещен в фрагмент канального уровня. MTU для протоколов канального уровня Ethernet и PPP равен 1500 байт. Следовательно, значение MSS как правило составляет 1460 байт. Также были предложены подходы для определения MTU для всего маршрута — наибольшего фрагмента канального уровня, который может быть отправлен по всем каналам от начального узла до конечного<sup>440</sup> — и определения MSS на основе значения MTU для всего маршрута. Заметим, что MSS — это максимальное количество данных прикладного уровня в сегменте, а не максимальный размер TCP-сегмента вместе с заголовком. Такая терминология является несколько запутанной, однако распространенной, поэтому мы вынуждены ее придерживаться.



**Рис. 3.28.** Буферы приема и передачи в протоколе TCP