

Universidade do Minho

Relatório - Redes de Computadores

MIEI - 3º ano - 1º semestre Universidade do Minho

Redes sem fios (802.11)

Grupo 58



Dinis Peixoto A75353



Ricardo Pereira A74185



Marcelo Lima A75210

1. Questões e Respostas

1. Identifique em que frequência do espectro está a operar a rede sem fios, e o canal corresponde essa frequência (pode confirmar com a norma IEEE 802.11).

```
Frame 58: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
Radiotap Header v0, Length 24

# 802.11 radio information
PHY type: 802.11b (4)
Short preamble: False
Data rate: 1.0 Mb/s
Channel: 6
Frequency: 2437 MHz
Signal strength (dBm): −29 dBm
Noise level (dBm): −100 dBm

| [Duration: 1464 us]
| IEEE 802.11 Beacon frame, Flags: .......C
| IEEE 802.11 wireless LAN management frame
```

A rede sem fios tem de frequência 2437 MHz, o que corresponde ao canal 6, segundo a norma IEEE 802.11.

2. Qual o tipo do canal que está a ser usado para a comunicação rádio? Qual o débito a que foi enviada a trama escolhida?

```
Frame 58: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)

Radiotap Header v0, Length 24

802.11 radio information
PHY type: 802.11b (4)
Short preamble: False

Data rate: 1.0 Mb/s
Channel: 6
Frequency: 2437 MHz
Signal strength (dBm): −29 dBm
Noise level (dBm): −100 dBm

□ [Duration: 1464 us]
□ IEEE 802.11 Beacon frame, Flags: ......C
□ IEEE 802.11 wireless LAN management frame
```

```
▶ Frame 58: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
▶ Radiotap Header v0, Length 24
▼ 802.11 radio information
PHY type: 802.11b (4)
Short preamble: False
Data rate: 1.0 Mb/s
Channel: 6
Frequency: 2437 MHz
Signal strength (dBm): -29 dBm
Noise level (dBm): -100 dBm
▶ [Duration: 1464 us]
▶ IEEE 802.11 Beacon frame, Flags: .......C
▶ IEEE 802.11 wireless LAN management frame
```

O tipo de canal que está a ser usado é 802.11b, e a trama escolhida foi enviada a um débito de 1.0~Mb/s.

3. Indique qual o índice de qualidade do sinal.

```
Header length: 24

▶ Present flags

▶ Flags: 0x10

Data Rate: 1.0 Mb/s

Channel frequency: 2437 [BG 6]

▶ Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz spectrum SSI Signal: −29 dBm

SSI Noise: −100 dBm

Signal Quality: 100

Antenna: 0

SSI Signal: 71 dB

▶ RX flags: 0x6b74

▼ 802.11 radio information
```

Tal como podemos observar no *printscreen* o índice da qualidade do sinal é 100.

4. Qual o tipo de uma trama beacon? Indique quais os seus identificadores de tipo e subtipo. Em que parte da trama estão especificados?

```
Frame 58: 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
      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)
      Destination address: Broadcast (ff:ff:ff:ff:ff)
      00 00 18 00 ee 58 00 00 <u>10</u> 02 85 09 a0 00 e3 9c
                                                            d..Gtk.. .....Q
 0010 64 00 00 47 74 6b 11 99
                                 80 00 00 00 ff ff ff ff
       ff ff 00 16 b6 f7 1d 51
                                 64 00 01 06 00 0c 33 30
53 74 01 04 82 84 8b 96
 0030 82 61 5e 96 28 00 00 00
 0040
       20 4d 75 6e 72 6f 65 20
                                                             Munroe St.....
                                                             ....usi..
                                 00 27 a4 00 00 42 43 5e
32 08 8c 12 98 24 b0 48
 0060
       1a 0c 12 0f 00 03 a4 00
                                                             b2/.*.. 2....$.H
 0070
       00 62 32 2f 00 2a 01 00
       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
       01 0f 00 03 a4 00 00 27
                                                                      ...BC^.b
                                 a4 00 00 42 43 5e 00 62
 00b0 32 2f 00 74 6b 11 99
Byte 24: Subtype (wlan.fc.subtype)
```

A correspondente trama beacon é uma trama de gestão, como podemos verificar pelo seu campo Type: Management frame (0x00) e com o subtipo 8 (0x1000). Podemos verificar no printscreen que a informação sobre estes campos se encontra no byte 24 da trama.

5. Identifique os SSIDs dos APs (*Acess Points*) que estão a operar na rede e diga qual tende a proporcionar a melhor qualidade de sinal?

32 1.314223	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon	frame,	SN=2868,	FN=0,	Flags=C,	BI=100,	SSID=30	Munroe S	it
33 1.416593	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon	frame,	SN=2869,	FN=0,	Flags=C,	BI=100,	SSID=30	Munroe S	it
34 1.420565	LinksysG_67:22:94	Broadcast	802.11	90 Beacon	frame,	SN=3083,	FN=0,	Flags=,	BI=2058	0, SSID=1	linksys12	2
35 1.519009	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon	frame,	SN=2870,	FN=0,	Flags=C,	BI=100,	SSID=30	Munroe S	it
36 1.621422	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon	frame,	SN=2871,	FN=0,	Flags=C,	BI=100,	SSID=30	Munroe S	it
37 1.724031	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon	frame,	SN=2872,	FN=0,	Flags=C,	BI=100,	SSID=30	Munroe S	it
38 1.826193	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon	frame,	SN=2873,	FN=0,	Flags=C,	BI=100,	SSID=30	Munroe S	it
39 1.928599	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon	frame,	SN=2874,	FN=0,	Flags=C,	BI=100,	SSID=30	Munroe S	it
40 2.030907	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon	frame,	SN=2875,	FN=0,	Flags=C,	BI=100,	SSID=30	Munroe S	it
41 2.035064	LinksysG_67:22:94	Broadcast	802.11	90 Beacon	frame,	SN=3089,	FN=0,	Flags=,	BI=100,	SSID=lin	ıksys12	
42 2.133342	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon	frame,	SN=2876,	FN=0,	Flags=C,	BI=100,	SSID=30	Munroe S	it
43 2.137566	LinksysG_67:22:94	Broadcast	802.11	90 Beacon	frame,	SN=3090,	FN=0,	Flags=C,	BI=100,	SSID=lin	ksys12	
44 2.235695	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon	frame,	SN=2877,	FN=0,	Flags=C,	BI=100,	SSID=30	Munroe S	it
57 2.338148	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon	frame,	SN=2879,	FN=0,	Flags=C,	BI=100,	SSID=30	Munroe S	it
58 2.440572	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon	frame,	SN=2880,	FN=0,	Flags=C,	BI=100,	SSID=30	Munroe S	it
60 2.542945	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon	frame,	SN=2882,	FN=0,	Flags=C,	BI=100,	SSID=30	Munroe S	it
61 2.645319	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon	frame,	SN=2883,	FN=0,	Flags=C,	BI=100,	SSID=30	Munroe S	it

```
Header length: 24

▶ Present flags

▶ Flags: 0x10

Data Rate: 2.0 Mb/s

Channel frequency: 2437 [BG 6]

▶ Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz spectrum

SSI Signal: -93 dBm

SSI Noise: -100 dBm

Signal Quality: 11

Antenna: 0

SSI Signal: 7 dB

▶ RX flags: 0xa1e7, Bad PLCP

▼ 802.11 radio information

DEM tree: 902.11 (4)
```

32 1.314223	Cisco-Li_f7:1d:51	Broadcast	802.11 1	183 Beacon frame,	SN=2868, FN=0,	Flags=C, BI=100,	SSID=30 Munroe St
33 1.416593	Cisco-Li_f7:1d:51	Broadcast	802.11 1	183 Beacon frame,	SN=2869, FN=0,	Flags=C, BI=100,	SSID=30 Munroe St
34 1.420565	LinksysG_67:22:94	Broadcast	802.11	90 Beacon frame,	SN=3083, FN=0,	Flags=, BI=2058	0, SSID=linksys12
35 1.519009	Cisco-Li_f7:1d:51	Broadcast	802.11 1	183 Beacon frame,	SN=2870, FN=0,	Flags=C, BI=100,	SSID=30 Munroe St
36 1.621422	Cisco-Li_f7:1d:51	Broadcast	802.11 1	183 Beacon frame,	SN=2871, FN=0,	Flags=C, BI=100,	SSID=30 Munroe St
37 1.724031	Cisco-Li_f7:1d:51	Broadcast	802.11 1	183 Beacon frame,	SN=2872, FN=0,	Flags=C, BI=100,	SSID=30 Munroe St
38 1.826193	Cisco-Li_f7:1d:51	Broadcast	802.11 1	183 Beacon frame,	SN=2873, FN=0,	Flags=C, BI=100,	SSID=30 Munroe St
39 1.928599	Cisco-Li_f7:1d:51	Broadcast	802.11 1	183 Beacon frame,	SN=2874, FN=0,	Flags=C, BI=100,	SSID=30 Munroe St
40 2.030907	Cisco-Li_f7:1d:51	Broadcast	802.11 1	183 Beacon frame,	SN=2875, FN=0,	Flags=C, BI=100,	SSID=30 Munroe St
41 2.035064	LinksysG_67:22:94	Broadcast	802.11	90 Beacon frame,	SN=3089, FN=0,	Flags=, BI=100,	SSID=linksys12
42 2.133342	Cisco-Li_f7:1d:51	Broadcast	802.11 1	183 Beacon frame,	SN=2876, FN=0,	Flags=C, BI=100,	SSID=30 Munroe St
43 2.137566	LinksysG_67:22:94	Broadcast	802.11	90 Beacon frame,	SN=3090, FN=0,	Flags=C, BI=100,	SSID=linksys12
44 2.235695	Cisco-Li_f7:1d:51	Broadcast	802.11 1	183 Beacon frame,	SN=2877, FN=0,	Flags=C, BI=100,	SSID=30 Munroe St
57 2.338148	Cisco-Li_f7:1d:51	Broadcast	802.11 1	183 Beacon frame,	SN=2879, FN=0,	Flags=C, BI=100,	SSID=30 Munroe St
58 2.440572	Cisco-Li_f7:1d:51	Broadcast	802.11 1	183 Beacon frame,	SN=2880, FN=0,	Flags=C, BI=100,	SSID=30 Munroe St
60 2.542945	Cisco-Li_f7:1d:51	Broadcast	802.11 1	183 Beacon frame,	SN=2882, FN=0,	Flags=C, BI=100,	SSID=30 Munroe St
61 2.645319	Cisco-Li_f7:1d:51	Broadcast	802.11 1	183 Beacon frame,	SN=2883, FN=0,	Flags=C, BI=100,	SSID=30 Munroe St

```
▶ Present flags
▶ Flags: 0x10
Data Rate: 1.0 Mb/s
Channel frequency: 2437 [BG 6]
▶ Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz spect SSI Signal: -29 dBm
SSI Noise: -100 dBm

Signal Quality: 100
Antenna: 0
SSI Signal: 71 dB
▶ RX flags: 0x6b74
▼ 802.11 radio information
PHY type: 802.11b (4)
```

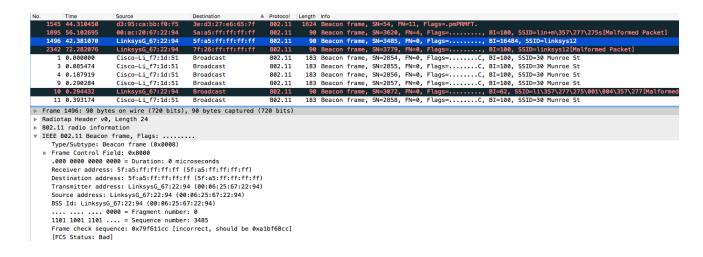
Através dos *printscreen* apresentados podemos verificar a existência de dois APs que estão a operar na rede, em que o primeiro tem de SSID linksys12 e o segundo 30 $Munroe\ St$. Ao analisarmos as tramas de cada um destes APs, verificámos que enquanto no primeiro caso (linksys12) a qualidade de sinal é 11 e no segundo caso $(30\ Munroe\ St)$ é 100. Assim, concluímos que o AP correspondente ao segundo SSID tem melhor qualidade de sinal.

6. Para dois dos APs identificados, indique quais são os intervalos de tempo previstos entre as transmissões de tramas beacon? (nota: este valor é anunciado na própria trama beacon. Na prática, a periodicidade de tramas beacon é verificada? Tente explicar porquê.

No.		Time	Source	Destination	Protocol	Length	Info							
	1	0.000000	Cisco-Li f7:1d:51	Broadcast	802.11			frame,	SN=2854,	FN=0,	Flags=C,	BI=100,	SSID=30 Munroe St	
	3	0.085474	Cisco-Li_f7:1d:51	Broadcast	802.11								SSID=30 Munroe St	
	4	0.187919	Cisco-Li_f7:1d:51	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:51	Broadcast	802.11	183	Beacon	frame,	SN=2857,	FN=0,	Flags=C,	BI=100,	SSID=30 Munroe St	
	10	0.294432	LinksysG_67:22:94	Broadcast	802.11	90	Beacon	frame,	SN=3072,	FN=0,	Flags=,	BI=62,	SSID=li\357\277\275\001\0	04\357\27
	11	0.393174	Cisco-Li_f7:1d:51	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:51	Broadcast	802.11	183	Beacon	frame,	SN=2859,	FN=0,	Flags=C,	BI=100,	SSID=30 Munroe St	
	14	0.499197	LinksysG_67:22:94	Broadcast	802.11	90	Beacon	frame,	SN=3074,	FN=0,	Flags=,	BI=100,	SSID=linksys12	
	15	0.597382	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon	frame,	SN=2860,	FN=0,	Flags=C,	BI=100,	SSID=30 Munroe St	
	16	0.601687	LinksysG_67:22:94	Broadcast	802.11	90	Beacon	frame,	SN=3075,	FN=0,	Flags=C,	BI=100,	SSID=linksys12	
	17	0.699847	Cisco-Li_f7:1d:51	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:51	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:51	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:51	Broadcast	802.11								SSID=30 Munroe St	
	21	1.010949	LinksysG_67:22:94	Broadcast	802.11	90	Beacon	frame,	SN=3079,	FN=0,	Flags=,	BI=100,	SSID=linksys12	
	22	1.109406	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon	frame,	SN=2865,	FN=0,	Flags=C,	BI=100,	SSID=30 Munroe St	
	23	1.113691	LinksysG_67:22:94	Broadcast	802.11	90	Beacon	frame,	SN=3080,	FN=0,	Flags=,	BI=100,	SSID=,\357\277\275nksys	

Tendo em conta a frequência de 2.4~GHz, o intervalo de tempo entre cada trama deverá ser, aproximadamente, 0.102400~segundos. No caso do AP $Cisco_Li_f7:1d:51$, e analisando as tramas 1 e 3, o intervalo de tempo é 0.085474. Considerámos este intervalo de tempo muito aproximado ao esperado, logo podemos verificar que a periodicidade das tramas é mantida. O mesmo não acontece no caso do AP $LinksysG_67:22:94$, em que ao analisar as tramas 10 e 14, reparamos que o intervalo de tempo é de 0.204765~segundos, um valor muito distante do intervalo de tempo esperado.

7. Identifique e registe todos os endereços MAC usados nas tramas *beacon* enviadas pelos APs. Recorde que fonte, destino e BSS ID são endereços contidos no cabeçalho das tramas 802.11. Para uma descrição detalhada da estrutura da trama 802.11, consulte o anexo ao enunciado.



```
99 Beacon frame, SN=3629, RN=4, Flags=..., BI=109, SSID=lin*m\357\277\2775\footnote{Malformed Packed Packed
                                                                                                             LinksysG_67:22:94
LinksysG_67:22:94
Cisco-Li_f7:1d:51
                                                                                                                                                                                                                             5f:a5:ff:ff:ff:ff
7f:26:ff:ff:ff
                        3 0.085474
                                                                                                              Cisco-Li f7:1d:51
                                                                                                                                                                                                                             Broadcast
                                                                                                                                                                                                                                                                                                                                             802.11
                        4 0.187919
9 0.290284
                                                                                                           Cisco-Li_f7:1d:51
Cisco-Li_f7:1d:51
LinksysG_67:22:94
Cisco-Li_f7:1d:51
                                                                                                                                                                                                                                                                                                                                             802.11
                                                                                                                                                                                                                                                                                                                                           802.11
802.11
                    11 0.393174
                                                                                                                                                                                                                             Broadcast
                                                                                                                                                                                                                                                                                                                                           802.11
  Frame 2342: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
```

o. Time 40 2.0		ource					to do								
40 2.0		isco-Li f7:1d:51	Destination A Broadcast		rotocol 302.11	Length		fanna	CN-2075	EN-0	Flags=C,	DT-100	CCTD-30 M		C+
41 2.0		inksysG_67:22:94	Broadcast		302.11						Flags=,				3 C
42 2.1		isco-Li f7:1d:51	Broadcast		302.11						Flags=C.				
		- · · · · · · · · · · · · · · · · · · ·			302.11										Σť
43 2.1		inksysG_67:22:94	Broadcast								Flags=C,			,	٠.
44 2.2		isco-Li_f7:1d:51	Broadcast		302.11 302.11						Flags=C,				
57 2.3		isco-Li_f7:1d:51	Broadcast								Flags=C,				
58 2.4		isco-Li_f7:1d:51	Broadcast		302.11						Flags=C,				
60 2.5		isco-Li_f7:1d:51	Broadcast		302.11						Flags=C,				
61 2.6		isco-Li_f7:1d:51	Broadcast		302.11						Flags=C,				
62 2.7	47697 C	isco-Li_f7:1d:51	Broadcast	8	302.11	183	Beacon	τrame,	SN=2884,	FN=0,	Flags=C,	BI=100,	2210=30 M	unroe s	эt
Type/Su Frame C .000 00 Receive Destina Transmi Source BSS Id:	btype: Beaco Control Field 000 0000 0000 er address: B ation address tter address address: Cis cisco-Li_f7 0000	amme, Flags: In frame (00008) I: 0x8000 D = Duration: 0 micro Iroadcast (ff:ff:: Is Broadcast (ff:ff:: Ic Cisco-Li_f7:Id:51 Ico-Li_f7:Id:51 (00: I:di:51 (00:16:06:f7) D = Fragment number: = Sequence number: Ec: 0x99116574 [cor:	oseconds ff:ff:ff:ff) (00:16:06:f7:1d:51) 16:b6:f7:1d:51) 0 2880	•											

No.	Time	Source	Destination	▲ Protocol	Length									
	2.030907	Cisco-Li_f7:1d:51	Broadcast	802.11						Flags=C,				St
	2.035064	LinksysG_67:22:94	Broadcast	802.11						Flags=,				
	2.133342	Cisco-Li_f7:1d:51	Broadcast	802.11						Flags=C,				St
	2.137566	LinksysG_67:22:94	Broadcast	802.11						Flags=C,				
	2.235695	Cisco-Li_f7:1d:51	Broadcast	802.11						Flags=C,				
	2.338148	Cisco-Li_f7:1d:51	Broadcast	802.11						Flags=C,				
	2.440572	Cisco-Li_f7:1d:51	Broadcast	802.11						Flags=C,				
	2.542945	Cisco-Li_f7:1d:51	Broadcast	802.11						Flags=C,				
	2.645319	Cisco-Li_f7:1d:51	Broadcast	802.11						Flags=C,				
62	2.747697	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon	frame,	SN=2884,	FN=0,	Flags=C,	BI=100,	SSID=30	Munroe	St
▶ 802.1 ▼ IEEE : Typ ▶ Fra .00 Rec Des Tra Sou BSS	pe/Subtype: Beame Control F: 00 0000 0000 (ceiver addressistination addiaurce address: 5 Id: Linksys(ceiver) (ceiver) (c	mation frame, Flags: frame, Flags: eacon frame (0x0008) ield: 0x8000 geome = Duration: 0 mic s: Broadcast (ff:ff: fress: ElinksysG_67:22:94 (00 _567:22:94 (00 _567:22:94 (00:06:25:6 0000 = Fragment number = Sequence number uence: 0x7409lale7 [cor	roseconds :ff:ff:ff: :ff:ff:ff:ff: :f6:25:67:22:94) :06:25:67:22:94) :09:	14)										

Através dos printscreens em cima conseguimos identificar todos os endereços MAC usados nas correspondentes tramas, nos campos Receiver address, Destination address, Transmitter address, Source address.

8. As tramas *beacon* anunciam que o AP pode suportar vários débitos de base assim como vários *extended supported rates*. Indique quais são esses débitos?

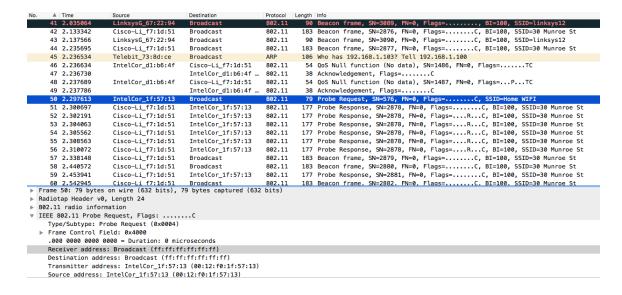
```
Tag Number: ERP Information (42)
Tag length: 1

► ERP Information: 0x00

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: AirgoNet
   Tag Number: Vendor Specific (221)
   Tag length: 21
       Tag: SSID parameter set: linksys12
           Tag Number: SSID parameter set (0)
           Tag length: 9
          SSID: linksys12
      Tag: Supported Rates 1(B), 2(B), 5.5, 11, [Mbit/sec]
           Tag Number: Supported Rates (1)
          Tag length: 4
          Supported Rates: 1(B) (0x82)
Supported Rates: 2(B) (0x84)
           Supported Rates: 5.5 (0x0b)
          Supported Rates: 11 (0x16)
      Tag: DS Parameter set: Current Channel: 6
           Tag Number: DS Parameter set (3)
           Tag length: 1
          Current Channel: 6
    ▼ Tag: Traffic Indication Map (TIM): DTIM 1 of 0 bitmap
           Tag Number: Traffic Indication Map (TIM) (5)
```

O AP com o SSID 30 Munroe St suporta débitos até 54 Mbits/seg que corresponde ao 802.11g. Enquanto o outro só suporta débitos até 11 Mbits/seg, ou seja, mantém-se pelo 802.11b.

9. Indique a que sistemas são endereçadas estas tramas e qual o seu propósito?



No.		Time	Source	Destination		Length	
		2.035064	LinksysG_67:22:94	Broadcast	802.11		Beacon frame, SN=3089, FN=0, Flags=, BI=100, SSID=linksys12
		2.133342	Cisco-Li_f7:1d:51	Broadcast	802.11		Beacon frame, SN=2876, FN=0, Flags=C, BI=100, SSID=30 Munroe St
	43	2.137566	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3090, FN=0, Flags=C, BI=100, SSID=linksys12
	44	2.235695	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2877, FN=0, Flags=C, BI=100, SSID=30 Munroe St
	45	2.236534	Telebit_73:8d:ce	Broadcast	ARP	106	Who has 192.168.1.103? Tell 192.168.1.100
	46	2.236634	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1486, FN=0, Flags=TC
	47	2.236730		IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=C
	48	2.237689	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1487, FN=0, Flags=PTC
	49	2.237786		IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=C
	50	2.297613	IntelCor_1f:57:13	Broadcast	802.11	79	Probe Request, SN=576, FN=0, Flags=C, SSID=Home WIFI
	51	2.300697	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=C, BI=100, SSID=30 Munroe St
	52	2.302191	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=RC, BI=100, SSID=30 Munroe St
	53	2.304063	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=RC, BI=100, SSID=30 Munroe St
	54	2.305562	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=RC, BI=100, SSID=30 Munroe St
	55	2.308563	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=RC, BI=100, SSID=30 Munroe St
	56	2.310072	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=RC, BI=100, SSID=30 Munroe St
	57	2.338148	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2879, FN=0, Flags=C, BI=100, SSID=30 Munroe St
	58	2.440572	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2880, FN=0, Flags=C, BI=100, SSID=30 Munroe St
	59	2.453941	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2881, FN=0, Flags=C, BI=100, SSID=30 Munroe St
		2.542945	Cisco-Li f7:1d:51	Broadcast	802.11		Beacon frame. SN=2882. FN=0. Flags=C. BI=100. SSID=30 Munroe St
				177 bytes captured (1	L416 bits	;)	
		ap Header v0,					
		l radio informa					
▼ I			esponse, Flags:	c			
			be Response (0x0005)				
▶		me Control Fie					
			10 = Duration: 314 mi				
			IntelCor_1f:57:13 (0				
			ss: IntelCor_1f:57:13				
			ss: Cisco-Li_f7:1d:51				
	Sou	rce address: C	isco-Li_f7:1d:51 (00:	16:b6:f7:1d:51)			

A trama referente ao probe request, tem origem origem num STA (00:12:f0:1f:57:13). A STA envia uma trama Probe Request quando precisa obter informações de uma outra estação. Desta forma, esta trama torna-se útil para uma STA determinar quais os APs que estão dentro do seu alcance rádio (active scanning), isto é, ao enviar a trama Probe Request em broadcast, as APs dentro do seu alcance vão responder com uma trama Probe Response, que contém informações sobre as taxas de dados suportadas, etc. Neste caso a AP com endereço 00:16:b6:f7:1d:51, foi a que respondeu.

10. O campo Frame Control contido no cabeçalho das tramas 802.11 permite especificar a direccionalidade das tramas. Identifique a direccionalidade das tramas indicadas acima ($n^{o}1016$ e $n^{o}1066$). Este aspecto é fundamental para entender o endereçamento MAC em redes sem fios.

```
Source
192.168.1.109
1007 32.793652
                                             68.87.71.226
                                                                               124 Standard query 0xa592 A www.cs.umass.edu
                                                                    DNS
1008 32.793753
                                             IntelCor_d1:b6:4f ...
                                                                    802.11
                                                                                38 Acknowledgement, Flags=.....
                     68.87.71.226
1009 32.807210
                                            192,168,1,109
                                                                    DNS
                                                                               140 Standard query response 0xa592 A www.cs.umass.edu A 128.119.240.19
                                            Cisco-Li_f7:1d:51
     32.807383
                                                                                38 Acknowledgement, Flags=.....C
                     192.168.1.109
1011 32.808574
                                            128.119.240.19
                                                                    TCP
                                                                               110 2541-80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
1012 32.808691
                                                                    802.11
                                             IntelCor d1:b6:4f ...
                                                                                38 Acknowledgement, Flags=.....
                     128.119.240.19
1013 32.825631
                                             192.168.1.109
                                                                    TCP
                                                                               110 80→2541 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
                                            Cisco-Li f7:1d:51
1014 32.825780
                                                                    802.11
                                                                                38 Acknowledgement, Flags=.....
1015 32.825892
                                             IntelCor_d1:b6:4f ..
                                                                                38 Acknowledgement, Flags=.....
1016 32.825992
                     192.168.1.109
                                             128.119.240.19
                                                                    HTTP
                                                                               512 GET / HTTP/1.1
     32.826103
                                             IntelCor_d1:b6:4f
                                                                    802.11
                                                                                   Acknowledgement, Flags=.....
                                                                               108 80-2541 [ACK] Seq=1 Ack=411 Win=6432 Len=0
38 Acknowledgement, Flags=.....C
1018 32.843967
                     128,119,240,19
                                            192.168.1.109
                                                                    TCP
1019 32.844070
                                            Cisco-Li_f7:1d:51 ...
                                                                    802.11
1020 32.844590
1021 32.844694
                     128.119.240.19
                                            192.168.1.109
Cisco-Li_f7:1d:51 ...
                                                                               375 [TCP segment of a reassembled PDU]
                                                                    802.11
                                                                                   Acknowledgement, Flags=.....
    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
```

Nesta trama a direcionalidade é *To DS: 1 From DS: 0*, logo o sender/transmiter é um MAC STA ($IntelCor_d1:b6:4f$), o receiver é um MAC AP ($Cisco-Li_f7:1d:51$) e o destination é um MAC Router ($Cisco-Li_f4:eb:a8$).

No.		Time	Source	Destination	Protocol	Length	
	1053	32.892184	192.168.1.109	128.119.240.19	TCP	102	2542→80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
	1054	32.892285		IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=C
	1055	32.892394	192.168.1.109	128.119.240.19	HTTP	484	GET /includes/csweb.css HTTP/1.1
	1056	32.892888	192.168.1.109	128.119.240.19	TCP	484	[TCP Retransmission] 2542→80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=382
	1057	32.892986		IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=C
	1058	32.903185	128.119.101.5	192.168.1.109	TCP	110	80-2543 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
	1059	32.903327		Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=C
	1060	32.903427	192.168.1.109	128.119.101.5	TCP	102	2543-80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
	1061	32.903534		IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=C
	1062	32.903631	192.168.1.109	128.119.101.5	HTTP	440	GET /favicon.ico HTTP/1.1
	1063	32.903728		IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=C
+	1064	32.909728	128.119.240.19	192.168.1.109	TCP	1562	[TCP segment of a reassembled PDU]
	1065	32.909832		Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=C
4-	1066	32.909945	128.119.240.19	192.168.1.109	HTTP	464	HTTP/1.1 200 OK (text/html)
	1067	32.910053		Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=C
		1000 = Su	btype: 8				
	₩ 1	lags: 0x02					
		10 =	DS status: Frame from	DS to a STA via AP(T	o DS: 0	From DS	S: 1) (0x2)
		0 =	More Fragments: This	is the last fragment			
		0 =	Retry: Frame is not b	eing retransmitted			
		0 =	PWR MGT: STA will sta	y up			
		0 =	More Data: No data bu	ffered			
		.0 =	Protected flag: Data	is not protected			
		0 =	Order flag: Not stric	tly ordered			

Nesta trama a direcionalidade é *To DS: 0 From DS: 1*, logo o sender é um MAC Router (*Cisco-Li_f4:eb:a8*), o transmiter é um MAC AP (*Cisco-Li_f7:1d:51*) e o destination/receiver é um MAC STA (*IntelCor_d1:b6:4f*).

11. Para a trama 802.11 que contém o pedido GET, indique os três endereços MAC em uso, identificando qual o endereço MAC correspondente ao *host* sem fios, ao AP e ao router de acesso ao sistema de distribuição (DS)?

```
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)
   Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
   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)
   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 [correct]
   [FCS Status: Good]
  Qos Control: 0x0000
Os endereços MAC em uso são os seguintes:
Host sem fios - 00:13:02:d1:b6:4f (transmitter)
AP - 00:16:b6:f7:1d:51 (receiver)
Router - 00:16:b6:f4:eb:a8 (destination)
```

12. Para a trama 802.11 que contém a resposta ao pedido GET, indique e identifique quais os três endereços MAC em uso?

```
▼ Frame Control Field: 0x8802
    .... ..00 = Version: 0
     .... 10.. = Type: Data frame (2)
    1000 .... = Subtype: 8
  ▼ Flags: 0x02
       .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
       .... .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 1000 = Duration: 40 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_f4:eb:a8 (00:16:b6:f4:eb:a8)
  BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
```

Os endereços MAC em uso são os seguintes: Host sem fios - 00:13:02:d1:b6:4f (receiver/destination) AP - 00:16:b6:f7:1d:51 (transmitter) Router - 00:16:b6:f4:eb:a8 (source)

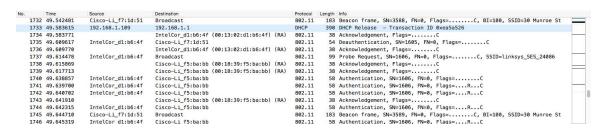
13. Que subtipo de tramas de controlo são transmitidas ao longo da interação acima mencionada? Verifique a que sistemas são endereçadas. Tente explicar proque razão têm de existir (contrariamente ao que acontece numa rede Ethernet.).

```
Time
1015 32.825892
                                                                       Protocol Length Info
                                               IntelCor d1:b6:4f ...
                                                                       802.11
                                                                                   38 Acknowledgement, Flags=.....C
                       192.168.1.109
 1016 32.825992
                                                                                  512 GET / HTTP/1.1
                                               128.119.240.19
                                                                      HTTP
 1017 32.826103
1018 32.843967
                                                                                  38 Acknowledgement, Flags=......C
108 80→2541 [ACK] Seq=1 Ack=411 Win=6432 Len=0
                       128.119.240.19
                                               192.168.1.109
 1019 32.844070
                                               Cisco-Li_f7:1d:51 ...
                                                                                   38 Acknowledgement, Flags=.....C
 1020 32.844590
                       128,119,240,19
                                               192,168,1,109
                                                                       TCP
                                                                                 375 [TCP segment of a reassembled PDU]
 1021 32.844694
                                               Cisco-Li_f7:1d:51 ...
                                                                      802.11
                                                                                   38 Acknowledgement, Flags=.....C
                                               192.168.1.109
Cisco-Li_f7:1d:51 ...
 1022 32,847830
                       128.119.240.19
                                                                       TCP
                                                                                 1562 [TCP segment of a reassembled PDU]
                                                                      802.11
 1023 32.847937
                                                                                   38 Acknowledgement, Flags=.....C
 1024 32.848043
                       192.168.1.109
                                               128.119.240.19
                                                                       TCP
                                                                                  102 2541→80 [ACK] Seq=411 Ack=1734 Win=17520 Len=0
 1025 32,848140
                                                                      802.11
                                               IntelCor d1:b6:4f ...
                                                                                   38 Acknowledgement, Flags=.....C
                       Cisco-Li_f7:1d:51
                                                                                  183 Beacon frame, SN=3318, FN=0, Flags=......C,
 1026 32.851998
                                                                                1562 [TCP segment of a reassembled PDU]
1562 [TCP segment of a reassembled PDU]
                       128.119.240.19
 1028 32.868617
 1029 32.868757
                                               Cisco-Li_f7:1d:51 ... 802.11
                                                                                  38 Acknowledgement, Flags=.....C
Type/Subtype: Acknowledgement (0x001d)
▼ Frame Control Field: 0xd400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
1101 .... = Subtype: 13
   ▼ Flags: 0x00
        .... ..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
               .... = Order flag: Not strictly ordered
   .000 0000 0000 0100 = Duration: 4 microseconds
   Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
   Frame check sequence: 0x64c4665e [correct]
   [FCS Status: Good]
```

```
Protocol
1015 32.825892
                                            IntelCor d1:b6:4f
                                                                              38 Acknowledgement,
                    192.168.1.109
1016 32.825992
                                           128.119.240.19
                                                                  HTTP
                                                                             512 GET / HTTP/1.1
1017 32.826103
                                            IntelCor_d1:b6:4
                                                                              38 Acknowledgement, Flags=.....C
                                                                             108 80→2541 [ACK] Seq=1 Ack=411 Win=6432 Len=0
1018 32,843967
                    128.119.240.19
                                           192,168,1,109
                                                                  TCP
                     128.119.240.19
                                                                             375 [TCP segment of a reassembled PDU]
38 Acknowledgement, Flags=.....C
1020 32.844590
                                            192.168.1.109
                                                                   ТСР
1021 32.844694
                                           Cisco-Li_f7:1d:51
                                                                  802.11
1022 32.847830
                     128.119.240.19
                                            192.168.1.109
                                                                  TCP
                                                                            1562 [TCP segment of a reassembled PDU]
                                                                  802.11
1023 32.847937
                                           Cisco-Li_f7:1d:51
                                                                              38 Acknowledgement, Flags=.....C
1024 32.848043
                     192.168.1.109
                                            128.119.240.19
                                                                             102 2541→80 [ACK] Seq=411 Ack=1734 Win=17520 Len=0
                                                                  TCP
                                                                             38 Acknowledgement, Flags=.....C
183 Beacon frame, SN=3318, FN=0, Flags=......C, BI=1
1025 32.848140
                                           IntelCor d1:b6:4f
                                                                  802.11
                     Cisco-Li_f7:1d:51
                                           Broadcast
1027 32.867322
                                            192,168,1,109
                                                                  TCP
1028 32.868617
                                            192.168.1.109
                                                                                  [TCP segment of a reassembled PDU]
1029 32.868757
                                            Cisco-Li_f7:1d:51 ...
                                                                  802.11
Type/Subtype: Acknowledge
Frame Control Field: 0xd400
    .... ..00 = Version: 0
     ... 01.. = Type: Control frame (1)
    1101 .... = Subtype: 13
  ▼ Flags: 0x00
       .... ..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... = Order flag: Not strictly ordered .000 0000 0000 0000 = Duration: 0 microseconds
 Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
 Frame check sequence: 0x31425c0a [correct]
 [FCS Status: Good]
```

O subtipo das tramas de controlo que são transmitidas ao longo da iteração acima mencionada é *Acknowlegement*. Depois de receber uma trama de dados, a STA receptora irá utilizar um código de verificação para detectar a presença de erros, e envia uma trama ACK para a STA emissora, se não forem encontrados erros. Se a STA emissora não receber um ACK dentro de um determinado período de tempo, retransmite a trama. Os sistemas endereçados são o AP e o STA.

14. Identifique e interprete as tramas 802.11 enviadas pelo *host* decorrentes do pedido *DHCP Release* que determina a quebra de associação que existia com o AP 30 Munroe St. Segundo a norma IEEE 802.11, há alguma trama que seria esperada, mas não aparece?



As tramas enviadas pelo host, decorrentes do pedido *DHCP Release* que determinam a quebra de associação que existia com o AP 30 Munroe St são as tramas que se seguem à trama 1733 (trama do pedido DHCP), isto é, as tramas *Acknowledgement*, *Deauthentication* (responsáveis pela desautenticação), seguidas das tramas *Acknowledgment*, *Probe Request* e *Authentication* (responsáveis pela tentativa de autenticação). A trama que seria esperada mas não aparece é a trama de *Dissociation*.

15. Examine o ficheiro de trace e procure tramas de autenticação enviadas pelo

host para o AP (se filtrar os resultados por wlan.fc.type_subtype ajuda a localização). Quantas tramas de authentication são enviadas do host sem fios para o AP linksys_SES_24086?

wlan.fc	.type_subtype =	= 0xB						
o. 🛦	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, Flags=C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication,	SN=1606,	FN=0, Flags=RC
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication,	SN=1606,	FN=0, Flags=RC
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication,	SN=1606,	FN=0, Flags=RC
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication,	SN=1606,	FN=0, Flags=RC
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication,	SN=1606,	FN=0, Flags=RC
1821	53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication,	SN=1612,	FN=0, Flags=C
1822	53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication,	SN=1612,	FN=0, Flags=RC
1921	57.889232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication,	SN=1619,	FN=0, Flags=C
1922	57.890325	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication,	SN=1619,	FN=0, Flags=RC
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication,	SN=1619,	FN=0, Flags=RC
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication,	SN=1619,	FN=0, Flags=RC
2122	62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication,	SN=1644,	FN=0, Flags=C
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication,	SN=1644,	FN=0, Flags=RC
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication,	SN=1644,	FN=0, Flags=RC
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication,	SN=1647,	FN=0, Flags=C
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication,	SN=3726,	FN=0, Flags=C
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication,	SN=1647,	FN=0, Flags=RC
2164	63.170692	Cisco-Li f7:1d:51	IntelCor d1:b6:4f	802.11	58	Authentication,	SN=3727,	FN=0, Flags=C

```
1734 49.583771
                                         IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) (RA)
                                                                                      802.11
                                                                                                 38 Acknowledgement,
                    IntelCor_d1:b6:4f
 1735 49.609617
                                         Cisco-Li_f7:1d:51
                                                                                       802.11
                                                                                                 54 Deauthentication
 1736 49.609770
                                         IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) (RA)
                                                                                      802.11
                                                                                                 38 Acknowledgement.
                    IntelCor d1:b6:4f
 1737 49.614478
                                         Broadcast
                                                                                      802.11
                                                                                                 99 Probe Request, S
 1738 49.615869
                                         Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb) (RA)
                                                                                      802.11
                                                                                                 38 Acknowledgement,
 1739 49.617713
                                         Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb) (RA)
                                                                                      802.11
                                                                                                 38 Acknowledgement,
                                         Cisco-Li_f5:ba:bb
 1740 49.638857
                    IntelCor_d1:b6:4f
                                                                                       802.11
                                                                                                 58 Authentication,
 1741 49.639700
                    IntelCor d1:b6:4f
                                         Cisco-Li f5:ba:bb
                                                                                                 58 Authentication.
                                                                                      802.11
                                         Cisco-Li_f5:ba:bb
                    IntelCor_d1:b6:4f
                                                                                                 58 Authentication.
 1742 49.640702
                                                                                      802.11
Frame 1740: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
Radiotap Header v0. Length 24
802.11 radio information
IEEE 802.11 Authentication, Flags: ......C
IEEE 802.11 wireless LAN management frame
 ▼ Fixed parameters (6 bytes)
     Authentication Algorithm: Open System (0)
     Authentication SEQ: 0x0001
     Status code: Successful (0x0000)
```

Pela observação dos *printscreens* podemos verificar que são enviadas 15 tramas de *authentication* para o AP *linksys_SES_24086* que tem o endereço MAC *Cisco-Li_f7:1d:51*.

16. O host tenta usar algum algoritmo de autenticação/chave ou tenta aceder de forma aberta (consulte o authentication algorithm na trama)? Existe alguma resposta do AP linksys_SES_24086 ao pedido de autenticação? Porquê?

```
Frame 1740: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
Radiotap Header v0, Length 24

802.11 radio information

IEEE 802.11 Authentication, Flags: ......C

IEEE 802.11 wireless LAN management frame

▼ Fixed parameters (6 bytes)
    Authentication Algorithm: Open System (0)
Authentication SEQ: 0x0001
    Status code: Successful (0x0000)
```

O algoritmo usado pelo host na autenticação é o open system. Não existe

resposta por parte do AP, pois trata-se de uma tentativa de autenticação de forma aberta, isto é, sem chave. No entanto, a chave deveria ser necessária.

17. Verifique que, após a tentativa de associação falhada, o *host* volta a associar-se ao AP 30 Munroe St. Identifique as tramas usadas para o efeito.

No.	A	Time	Source	Destination	Protocol	Length Info
	2141	62.956104	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=3722, FN=0, Flags=C, BI=100, SSID=30 Munroe St
	2142	63.059233	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54 Deauthentication, SN=1646, FN=0, Flags=C
	2143	63.061834	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54 Deauthentication, SN=1646, FN=0, Flags=RC
	2144	63.063454	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54 Deauthentication, SN=1646, FN=0, Flags=RC
	2145	63.065342	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54 Deauthentication, SN=1646, FN=0, Flags=RC
	2146	63.075964	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54 Deauthentication, SN=1646, FN=0, Flags=RC
	2147	63.087480	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54 Deauthentication, SN=1646, FN=0, Flags=RC
	2148	63.090971	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54 Deauthentication, SN=1646, FN=0, Flags=RC
	2149	63.094985	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54 Deauthentication, SN=1646, FN=0, Flags=RC
	2150	63.116231	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54 Deauthentication, SN=1646, FN=0, Flags=RC
	2151	63.135362	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54 Deauthentication, SN=1646, FN=0, Flags=RC
	2152	63.140106	IntelCor_d1:b6:4f	Broadcast	802.11	94 Probe Request, SN=1647, FN=0, Flags=C, SSID=30 Munroe St
		63.142451	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177 Probe Response, SN=3724, FN=0, Flags=C, BI=100, SSID=30 Munroe St
		63.142860		Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51) (RA)	802.11	38 Acknowledgement, Flags=C
	2155	63.161272	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=3725, FN=0, Flags=C, BI=100, SSID=30 Munroe St
	2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58 Authentication, SN=1647, FN=0, Flags=C
	2157	63.168222		IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) (RA)	802.11	38 Acknowledgement, Flags=C
	2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58 Authentication, SN=3726, FN=0, Flags=C
		63.169592		Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51) (RA)	802.11	38 Acknowledgement, Flags=C
	2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58 Authentication, SN=1647, FN=0, Flags=RC
		63.169814		IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) (RA)	802.11	38 Acknowledgement, Flags=C
		63.169910	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	89 Association Request, SN=1648, FN=0, Flags=C, SSID=30 Munroe St
	2163	63.170008		IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) (RA)	802.11	38 Acknowledgement, Flags=C
	2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58 Authentication, SN=3727, FN=0, Flags=C
	2165	63.171000		Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51) (RA)	802.11	38 Acknowledgement, Flags=C
		63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94 Association Response, SN=3728, FN=0, Flags=C
		63.192956		Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51) (RA)	802.11	38 Acknowledgement, Flags=C
		63.194842	0.0.0.0	255.255.255.255	DHCP	390 DHCP Discover - Transaction ID 0x101b218a
		63.194971		IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) (RA)	802.11	38 Acknowledgement, Flags=C
		63.201481	0.0.0.0	255.255.255.255	DHCP	390 DHCP Discover - Transaction ID 0x2733a47c
		63.201639	0.0.0.0	255.255.255.255	DHCP	390 DHCP Discover - Transaction ID 0x2733a47c
		63.201736		IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) (RA)	802.11	38 Acknowledgement, Flags=C
	2172	62 262517	Cicco-Li f7.1d.51	Broadcast	992 11	192 Boscon framo CN-2720 FN-A Flage- C RT-100 CCTD-20 Munroo C+

As tramas utilizadas para o efeito, são as tramas compreendidas entre os números 2152 e 2168. Após a tentativa de autenticação consegue um *Association Response*, ficando assim conetado ao AP.

2. Conclusão

Após a realização deste trabalho prático podemos afirmar que ficamos bastante mais esclarecidos relativamente ao protocolo IEEE 802.11, tanto ao nível do formato das tramas que o constituiem, como ao nível do endereçamento dos componentes que fazem parte da comunicação sem fios. Relativamente às tramas, ficamos a saber que estas se dividem em três tipos, as Tramas de Gestão, responsáveis por estabelecer e manter a comunicação entre as STAs, as Tramas de Controlo, responsáveis por ajudar na troca de tramas de dados entre as STAs, e as Tramas de Dados que são responsáveis pela transmissão e comunicação de dados.