

# Redes sem Fios (Wi-Fi)

Filipa Rebelo and Joana Oliveira

Universidade do Minho, Departamento de Informática, 4710-057 Braga, Portugal  
email: {a90234,a87956}@alunos.uminho.pt

## 1 Acesso Rádio

Como pode ser observado, a sequência de bytes capturada inclui informação do nível físico (radiotap header, radio information), para além dos bytes correspondentes a tramas 802.11. Selecione a trama de ordem XX correspondente ao seu identificador de grupo (TurnoGrupo, e.g., 11).

### 1.1 Exercício 1

Identifique em que frequência do espectro está a operar a rede sem fios, e o canal que corresponde essa frequência.

Através da Figura 1 verifica-se que a frequência do espectro é 2467MHz e que o canal correspondente é 12.

```
» Frame 37: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits)
» Radiotap Header v0, Length 25
» 802.11 radio information
  PHY type: 802.11g (ERP) (6)
  Short preamble: False
  Proprietary mode: None (0)
  Data rate: 1,0 Mb/s
  Channel: 12
  Frequency: 2467MHz
  Signal strength (dBm): -62dBm
  Noise level (dBm): -88dBm
  Signal/noise ratio (dB): 26dB
  TSF timestamp: 20826497
» [Duration: 1632µs]
» IEEE 802.11 Beacon frame, Flags: .....C
» IEEE 802.11 Wireless Management
```

Fig. 1. Trama 802.11

### 1.2 Exercício 2

Identifique a versão da norma IEEE 802.11 que está a ser usada.

A versão que está a ser utilizada é a 802.11g, tal como observado no campo *PHY type* da Figura 1.

### 1.3 Exercício 3

Qual o débito a que foi enviada a trama escolhida? Será que esse débito corresponde ao débito máximo a que a interface Wi-Fi pode operar? Justifique.

O valor correspondente ao débito de envio da trama escolhida encontra-se no campo *Data Rate* e tem o valor de 1,0 Mb/s. Este valor é inferior a 54.0 Mb/s, que corresponde ao débito máximo permitido pela norma IEEE 802.11g.

## 2 Scanning Passivo e Scanning Ativo

Como referido, as tramas beacon permitem efetuar scanning passivo em redes IEEE 802.11 (Wi-Fi). Para a captura de tramas disponibilizada, e considerando XX o seu nº de grupo, responda às seguintes questões:

### 2.1 Exercício 4

Selecione a trama beacon de ordem (260 + XX). Esta trama pertence a que tipo de tramas 802.11? Indique o valor dos seus identificadores de tipo e de subtipo. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?

O tipo e subtipo da trama estão contidos nos campos *Type* e *Subtype* do *Frame Control Field* e têm, respetivamente, os valores 0 e 8.

```

> Frame 297: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
  > IEEE 802.11 Beacon frame, Flags: .....C
    Type/Subtype: Beacon frame (0x0000)
    > 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: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
      Source address: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
      BSS Id: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
      .... 0000 = Fragment number: 0
      1001 0000 0110 .... = Sequence number: 2310
      Frame check sequence: 0xc7953ee [unverified]
      [FCS Status: Unverified]
  > IEEE 802.11 Wireless Management
0000 00 00 19 00 6f 08 00 00 ee b8 de 01 00 00 00 00 .....0.....
0010 10 02 a3 09 00 04 be a9 00 00 00 00 00 ff ff ff .....
0020 ff ff ff bc 14 01 af b1 99 bc 14 01 af b1 99 60 .....^
0030 90 27 db 65 ae 0b 01 00 00 64 00 21 0c 00 0c 4e .....^e....d....N
0040 4f 53 5f 57 49 46 49 5f 46 6f 6e 01 08 82 84 8b OS_WIFI_Fon....
0050 96 12 24 48 0c 03 01 0c 32 04 8c 9b 6b 05 05 .....SHL...2....
0060 02 03 00 4a 01 2a 01 00 2d 1a 8c 01 16 ff ff 00 .....J*.....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0080 00 00 00 00 3d 16 0c 00 04 00 00 00 00 00 00 .....=.....
0090 00 00 00 00 00 00 00 00 00 00 00 00 7f 01 01 0d .....P.....
00a0 18 00 50 f2 02 01 01 80 00 03 a4 00 00 27 a4 00 .....
00b0 00 42 43 5e 00 62 32 2f 00 0b 05 03 00 0a 12 7a BC^b2/.....z
00c0 dd 07 00 0c 43 00 00 00 00 ee 53 79 6c .....C....Syl

```

Fig. 2. Trama 802.11

Observando a seguinte entrada da tabela fornecida no enunciado, é possível concluir que se trata de uma trama do tipo Management (00) e do subtipo Beacon (1000).

00	Management	1000	Beacon
----	------------	------	--------

**Fig. 3.** Entrada da tabela fornecida no enunciado

## 2.2 Exercício 5

**Para a trama acima, identifique todos os endereços MAC em uso. Que conclui quanto à sua origem e destino?**

Receiver address: ff:ff:ff:ff:ff:ff

Destination address: ff:ff:ff:ff:ff:ff

Transmitter address: bc:14:01:af:b1:99

Source address: bc:14:01:af:b1:99

É possível concluir que a origem da trama se trata de um *Access Point*, e que o endereço de destino (ff:ff:ff:ff:ff:ff) se trata de um endereço de *Broadcast*, o que significa que a trama é enviada para todos os hosts.

## 2.3 Exercício 6

**Uma trama beacon anuncia que o AP pode suportar vários débitos de base, assim como vários débitos adicionais (extended supported rates). Indique quais são esses débitos?**

Tal como é possível observar na figura abaixo, os débitos de base são: 1 Mb/s, 2 Mb/s, 5.5 Mb/s, 11 Mb/s, 9 Mb/s, 18 Mb/s, 36 Mb/s, 54 Mb/s. Os débitos adicionais são: 6 Mb/s, 12 Mb/s, 24 Mb/s, 48 Mb/s.

```

> IEEE 802.11 Beacon frame, Flags: .....C
- IEEE 802.11 Wireless Management
  - Fixed parameters (12 bytes)
    Timestamp: 1149682178855
    Beacon Interval: 0,102400 [Seconds]
    Capabilities Information: 0x0c21
  - Tagged parameters (140 bytes)
    - Tag: SSID parameter set: NOS_WIFI_Fon
    - Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
      Tag Number: Supported Rates (1)
      Tag length: 8
      Supported Rates: 1(B) (0x82)
      Supported Rates: 2(B) (0x84)
      Supported Rates: 5.5(B) (0x8b)
      Supported Rates: 11(B) (0x96)
      Supported Rates: 9 (0x12)
      Supported Rates: 18 (0x24)
      Supported Rates: 36 (0x48)
      Supported Rates: 54 (0x6c)
    - Tag: DS Parameter set: Current Channel: 12
    - Tag: Extended Supported Rates 6(B), 12(B), 24(B), 48, [Mbit/sec]
      Tag Number: Extended Supported Rates (50)
      Tag length: 4
      Extended Supported Rates: 6(B) (0x8c)
      Extended Supported Rates: 12(B) (0x98)
      Extended Supported Rates: 24(B) (0xb0)
      Extended Supported Rates: 48 (0x60)

```

Fig. 4. Débitos de base e débitos adicionais

## 2.4 Exercício 7

Qual o intervalo de tempo previsto entre tramas beacon consecutivas (este valor é anunciado na própria trama beacon)? Na prática, a periodicidade de tramas beacon provenientes do mesmo AP é verificada com precisão? Justifique.

O intervalo de tempo previsto entre tramas beacon consecutivas encontra-se no campo *Beacon Interval* da Figura 5 e tem o valor de 0.102400 segundos. Observando o campo *Timestamp* de duas tramas beacon provenientes do mesmo AP e fazendo a sua subtração,  $1149682383659 - 1149682281252 = 102407$ , é possível perceber que o seu valor é ligeiramente superior ao teórico, devido à existência de colisões.

```

> Frame 299: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....C
- IEEE 802.11 Wireless Management
  - Fixed parameters (12 bytes)
    Timestamp: 1149682281252
    Beacon Interval: 0,102400 [Seconds]
    Capabilities Information: 0x0c21
  - Tagged parameters (140 bytes)

```

Fig. 5. Primeira trama capturada

```

> Frame 301: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....C
> IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
    Timestamp: 1149682383659
    Beacon Interval: 0,102400 [Seconds]
  > Capabilities Information: 0x0c21
  > Tagged parameters (140 bytes)

```

Fig. 6. Segunda trama capturada

## 2.5 Exercício 8

Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura? Explícite o modo como obteve essa informação (por exemplo, se usou algum filtro para o efeito).

wlan.ssid					
No.	Time	Source	Destination	Protocol	Length Info
1	0.000000	HltronTe_af:b1:98	Broadcast	802.11	205 Beacon frame, SN=2083, Fn=0, Flags=.....C, BI=100, SSID=FlyingNet
2	0.001662	HltronTe_af:b1:98	Broadcast	802.11	205 Beacon frame, SN=2084, Fn=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
3	0.102552	HltronTe_af:b1:98	Broadcast	802.11	205 Beacon frame, SN=2085, Fn=0, Flags=.....C, BI=100, SSID=FlyingNet
4	0.104164	HltronTe_af:b1:98	Broadcast	802.11	205 Beacon frame, SN=2086, Fn=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
5	0.204951	HltronTe_af:b1:98	Broadcast	802.11	205 Beacon frame, SN=2087, Fn=0, Flags=.....C, BI=100, SSID=FlyingNet
6	0.206582	HltronTe_af:b1:98	Broadcast	802.11	205 Beacon frame, SN=2088, Fn=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
7	0.307368	HltronTe_af:b1:98	Broadcast	802.11	205 Beacon frame, SN=2089, Fn=0, Flags=.....C, BI=100, SSID=FlyingNet
8	0.308999	HltronTe_af:b1:98	Broadcast	802.11	205 Beacon frame, SN=2090, Fn=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
9	0.409749	HltronTe_af:b1:98	Broadcast	802.11	205 Beacon frame, SN=2091, Fn=0, Flags=.....C, BI=100, SSID=FlyingNet
10	0.411376	HltronTe_af:b1:98	Broadcast	802.11	205 Beacon frame, SN=2092, Fn=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
11	0.512117	HltronTe_af:b1:98	Broadcast	802.11	205 Beacon frame, SN=2093, Fn=0, Flags=.....C, BI=100, SSID=FlyingNet
12	0.513787	HltronTe_af:b1:98	Broadcast	802.11	205 Beacon frame, SN=2094, Fn=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
13	0.614562	HltronTe_af:b1:98	Broadcast	802.11	205 Beacon frame, SN=2095, Fn=0, Flags=.....C, BI=100, SSID=FlyingNet
14	0.616191	HltronTe_af:b1:98	Broadcast	802.11	205 Beacon frame, SN=2096, Fn=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
28	0.716961	HltronTe_af:b1:98	Broadcast	802.11	205 Beacon frame, SN=2097, Fn=0, Flags=.....C, BI=100, SSID=FlyingNet
29	0.718611	HltronTe_af:b1:98	Broadcast	802.11	205 Beacon frame, SN=2098, Fn=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
32	0.819368	HltronTe_af:b1:98	Broadcast	802.11	205 Beacon frame, SN=2099, Fn=0, Flags=.....C, BI=100, SSID=FlyingNet
33	0.821009	HltronTe_af:b1:98	Broadcast	802.11	205 Beacon frame, SN=2100, Fn=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

Fig. 7. Lista de SSIDs

Os SSIDs dos APs que estão a operar na vizinhança da STA de captura são o *FlyingNet* e o *NOS\_WIFI\_FON*. Para obter esta informação utilizamos então o filtro *wlan.ssid* e observamos o campo *Info*, sendo que apenas encontramos os SSIDs mencionados acima.

## 2.6 Exercício 9

Verifique se está a ser usado o método de deteção de erros (CRC). Sugestão: Use o filtro: `(wlan.fc.type_subtype == 0x08) && (wlan.fcs.status == bad)` Que conclui? Justifique o porquê de ser necessário usar deteção de erros em redes sem fios.

Usando o filtro sugerido no enunciado, obtivemos 5 tramas com erros, tal como se vê na Figura 8. Isto prova a existência do campo *FCS Status*, o que significa que está a ser usado o método de deteção de erros (CRC).

[wlan.fc.type_subtype == 0x00] && (wlan.fc.status == bad)					
No.	Time	Source	Destination	Protocol	Length Info
6274.94	779898	38:90:ae:51:f4:19	43:46:08:ca:97:53	802.11	146 Beacon frame, SN=238, FN=0, Flags=pmPRM.T.
6937.99	991379	be:65:24:9b:d6:a1	0e:0b:77:ea:c1:bc	802.11	146 Beacon frame, SN=393, FN=10, Flags=...R.FT., BI=4913[Malformed Packet]
7013.109	184381	bd:09:4b:c5:79:85	43:46:15:19:df:53	802.11	146 Beacon frame, SN=3058, FN=18, Flags=pmPRM.T.
7131.109	388916	62:4c:de:c5:a9:3a	34:c4:ca:25:ed:14	802.11	146 Beacon frame, SN=2811, FN=0, Flags=pmPRM.T.
7173.100	484266	84:84:4c:a8:fd:ea	d2:f4:d1:ff:e5:79	802.11	146 Beacon frame, SN=2338, FN=10, Flags=pm...T.

Fig. 8. Tramas Beacon com erros

O uso deste mecanismo é importante no sentido em que permite detetar qualquer tipo de interferência, corrompimento ou perda de informação no envio das tramas.

## 2.7 Exercício 10

Estabeleça um filtro Wireshark apropriado que lhe permita visualizar todas as tramas probing request ou probing response, simultaneamente.

Com o filtro `wlan.fc.type_subtype == 4 || wlan.fc.type_subtype == 5` conseguimos então visualizar as tramas pedidas.

[wlan.fc.type_subtype == 4    wlan.fc.type_subtype == 5]					
No.	Time	Source	Destination	Protocol	Length Info
1300.53	746911	Apple_10:6a:f5	Broadcast	802.11	155 Probe Request, SN=2516, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2467.70	147855	ea:a4:64:7b:b9:7a	Broadcast	802.11	167 Probe Request, SN=2546, FN=0, Flags=.....C, SSID=DWIRE-PT-431
2468.70	149098	ea:a4:64:7b:b9:7a	Broadcast	802.11	155 Probe Request, SN=2541, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2469.70	149792	NitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411 Probe Response, SN=2332, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2471.70	150537	NitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411 Probe Response, SN=2333, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2473.70	151237	NitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411 Probe Response, SN=2334, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2475.70	151709	NitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201 Probe Response, SN=2335, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2477.70	152099	NitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201 Probe Response, SN=2336, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2479.70	152570	NitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201 Probe Response, SN=2337, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2603.72	179215	Apple_10:6a:f5	Broadcast	802.11	164 Probe Request, SN=2563, FN=0, Flags=.....C, SSID=FlyingNet
2606.72	179924	NitronTe_af:b1:98	Apple_10:6a:f5	802.11	411 Probe Response, SN=2346, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2608.72	180590	NitronTe_af:b1:98	Apple_10:6a:f5	802.11	411 Probe Response, SN=2347, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2610.72	181275	NitronTe_af:b1:98	Apple_10:6a:f5	802.11	411 Probe Response, SN=2348, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2616.72	201570	Apple_10:6a:f5	Broadcast	802.11	164 Probe Request, SN=2565, FN=0, Flags=.....C, SSID=FlyingNet
2617.72	202150	NitronTe_af:b1:98	Apple_10:6a:f5	802.11	411 Probe Response, SN=2350, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2619.72	202807	NitronTe_af:b1:98	Apple_10:6a:f5	802.11	411 Probe Response, SN=2351, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2621.72	203485	NitronTe_af:b1:98	Apple_10:6a:f5	802.11	411 Probe Response, SN=2352, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2650.72	488998	Apple_10:6a:f5	Broadcast	802.11	164 Probe Request, SN=2585, FN=0, Flags=.....C, SSID=FlyingNet
2653.72	502553	Apple_10:6a:f5	Broadcast	802.11	164 Probe Request, SN=2586, FN=0, Flags=.....C, SSID=FlyingNet
2677.72	568343	Apple_10:6a:f5	Broadcast	802.11	164 Probe Request, SN=2589, FN=0, Flags=.....C, SSID=FlyingNet
2678.72	578258	Apple_10:6a:f5	Broadcast	802.11	164 Probe Request, SN=2599, FN=0, Flags=.....C, SSID=FlyingNet
4455.82	623143	7c:ea:6d:ff:a2:cc	Broadcast	802.11	71 Probe Request, SN=62, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
4493.82	726818	7c:ea:6d:ff:a2:cc	Broadcast	802.11	71 Probe Request, SN=64, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
4494.82	728646	7c:ea:6d:ff:a2:cc	Broadcast	802.11	218 Probe Request, SN=65, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
6193.94	198080	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=.....C, SSID=FlyingNet

Fig. 9. Tramas Probing Request e Probing Response

De modo a sabermos os valores relativos a cada subtipo de trama consultamos a tabela fornecida no enunciado e observamos os seguintes valores.

00	Management	0100	Probe request
00	Management	0101	Probe response

Fig. 10. Excerto da tabela dada no enunciado

## 2.8 Exercício 11

Identifique um probing request para o qual tenha havido um probing response. Face ao endereçamento usado, indique a que sistemas são endereçadas estas tramas e explique qual o propósito das mesmas?

No.	Time	Source	Destination	Protocol	Length	Info
1306	53.746911	Apple_10:6a:f5	Broadcast	802.11	155	Probe Request, SN=2516, FN=0, Flags=.....C, SSID=wildcard (Broadcast)
2467	70.147855	ea:a4:64:7b:b9:7a	Broadcast	802.11	167	Probe Request, SN=2540, FN=0, Flags=.....C, SSID=ZWIRE-PF-431
2468	70.149098	ea:a4:64:7b:b9:7a	Broadcast	802.11	155	Probe Request, SN=2541, FN=0, Flags=.....C, SSID=wildcard (Broadcast)
2469	70.149792	Hitronte_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2332, FN=0, Flags=.....C, B1=100, SSID=FlyingNet
2473	70.150537	Hitronte_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2333, FN=0, Flags=.....C, B1=100, SSID=FlyingNet
2473	70.151237	Hitronte_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2334, FN=0, Flags=.....C, B1=100, SSID=FlyingNet
2475	70.151709	Hitronte_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2335, FN=0, Flags=.....C, B1=100, SSID=WOS_WIFI_Fon
2477	70.152099	Hitronte_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2336, FN=0, Flags=.....C, B1=100, SSID=WOS_WIFI_Fon
2478	70.152570	Hitronte_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2337, FN=0, Flags=.....C, B1=100, SSID=WOS_WIFI_Fon
2603	72.179215	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2563, FN=0, Flags=.....C, SSID=FlyingNet
2608	72.179924	Hitronte_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2346, FN=0, Flags=.....C, B1=100, SSID=FlyingNet
2608	72.180590	Hitronte_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2347, FN=0, Flags=.....C, B1=100, SSID=FlyingNet
2610	72.181275	Hitronte_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2348, FN=0, Flags=.....C, B1=100, SSID=FlyingNet
2610	72.201570	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2565, FN=0, Flags=.....C, SSID=FlyingNet
2617	72.202150	Hitronte_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2350, FN=0, Flags=.....C, B1=100, SSID=FlyingNet

Frame 2468: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits) on 0  
 Radiotap Header v0, Length 25  
 802.11 radio information  
 IEEE 802.11 Probe Request, Flags: .....C  
 Type/Subtype: Probe Request (0x0004)  
 Frame Control Field: 0x0000  
 .... 00 = Version: 0  
 .... 00.. = Type: Management frame (0)  
 0100 .... = Subtype: 4  
 Flags: 0x00  
 0000 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: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)  
 Source address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)  
 BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)  
 .... 0000 = Fragment number: 0  
 1001 1110 1101 .... = Sequence number: 2541  
 Frame check sequence: 0xb4f53262 [correct]  
 FCS Status: Good  
 IEEE 802.11 Wireless Management

Fig. 11. Probing Request

No.	Time	Source	Destination	Protocol	Length	Info
1306	53.746911	Apple_10:6a:f5	Broadcast	802.11	155	Probe Request, SN=2516, FN=0, Flags=.....C, SSID=wildcard (Broadcast)
2467	70.147855	ea:a4:64:7b:b9:7a	Broadcast	802.11	167	Probe Request, SN=2540, FN=0, Flags=.....C, SSID=ZWIRE-PF-431
2468	70.149098	ea:a4:64:7b:b9:7a	Broadcast	802.11	155	Probe Request, SN=2541, FN=0, Flags=.....C, SSID=wildcard (Broadcast)
2469	70.149792	Hitronte_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2332, FN=0, Flags=.....C, B1=100, SSID=FlyingNet
2473	70.150537	Hitronte_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2333, FN=0, Flags=.....C, B1=100, SSID=FlyingNet
2473	70.151237	Hitronte_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2334, FN=0, Flags=.....C, B1=100, SSID=FlyingNet
2475	70.151709	Hitronte_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2335, FN=0, Flags=.....C, B1=100, SSID=WOS_WIFI_Fon
2477	70.152099	Hitronte_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2336, FN=0, Flags=.....C, B1=100, SSID=WOS_WIFI_Fon
2478	70.152570	Hitronte_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2337, FN=0, Flags=.....C, B1=100, SSID=WOS_WIFI_Fon
2603	72.179215	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2563, FN=0, Flags=.....C, SSID=FlyingNet
2608	72.179924	Hitronte_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2346, FN=0, Flags=.....C, B1=100, SSID=FlyingNet
2608	72.180590	Hitronte_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2347, FN=0, Flags=.....C, B1=100, SSID=FlyingNet
2610	72.181275	Hitronte_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2348, FN=0, Flags=.....C, B1=100, SSID=FlyingNet
2610	72.201570	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2565, FN=0, Flags=.....C, SSID=FlyingNet
2617	72.202150	Hitronte_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2350, FN=0, Flags=.....C, B1=100, SSID=FlyingNet

Frame 2469: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits) on 0  
 Radiotap Header v0, Length 25  
 802.11 radio information  
 IEEE 802.11 Probe Response, Flags: .....C  
 Type/Subtype: Probe Response (0x0005)  
 Frame Control Field: 0x0000  
 .... 00 = Version: 0  
 .... 00.. = Type: Management frame (0)  
 0101 .... = Subtype: 5  
 Flags: 0x00  
 0000 0000 0011 0010 = Duration: 50 microseconds  
 Receiver address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)  
 Destination address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)  
 Transmitter address: Hitronte\_af:b1:98 (bc:14:01:af:b1:98)  
 Source address: Hitronte\_af:b1:98 (bc:14:01:af:b1:98)  
 BSS Id: Hitronte\_af:b1:98 (bc:14:01:af:b1:98)  
 .... 0000 = Fragment number: 0  
 1001 0001 1100 .... = Sequence number: 2332  
 Frame check sequence: 0xbcb842e3 [correct]  
 FCS Status: Good  
 IEEE 802.11 Wireless Management

Fig. 12. Probing Response

O *Probing Request* é enviado para um endereço *Broadcast* e tem como objetivo receber informações relativamente a outros AP. O *Probing Response* responde ao pedido anterior com as informações do AP respetivo.

### 3 Processo de Associação

Numa rede Wi-Fi estruturada, um host deve associar-se a um ponto de acesso antes de enviar dados. O processo de associação nas redes IEEE 802.11 é executada enviando a trama association request do host para o AP e a trama association response enviada pelo AP para o host, em resposta ao pedido de associação recebido. Este processo é antecedido por uma fase de autenticação.

#### 3.1 Exercício 12

Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.

Através do filtro presente na Figura 13 foi possível obter uma sequência de tramas que corresponde a um processo de associação completo entre STA e o AP, juntamente com a fase de autenticação.

wlan.fc.type == 0 && (wlan.fc.type_subtype == 0    wlan.fc.type_subtype == 1    wlan.fc.type_subtype == 11)						
No.	Time	Source	Destination	Protocol	Length	Info
2405	0.001192	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	73	Authentication, SN=2542, FN=0, Flags=.....C
2498	70.381869	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59	Authentication, SN=2338, FN=0, Flags=.....C
2498	70.383512	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	175	Association Request, SN=2543, FN=0, Flags=.....C, SSID=FlyingNet
2492	70.389339	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	225	Association Response, SN=2339, FN=0, Flags=.....C
4692	83.663250	7c:ea:6d:ff:a2:cc	HitronTe_af:b1:98	802.11	59	Authentication, SN=67, FN=0, Flags=.....C
4694	83.663681	HitronTe_af:b1:98	7c:ea:6d:ff:a2:cc	802.11	59	Authentication, SN=2439, FN=0, Flags=.....C
4696	83.665976	7c:ea:6d:ff:a2:cc	HitronTe_af:b1:98	802.11	153	Association Request, SN=68, FN=0, Flags=.....C, SSID=FlyingNet
4698	83.678973	HitronTe_af:b1:98	7c:ea:6d:ff:a2:cc	802.11	225	Association Response, SN=2440, FN=0, Flags=.....C
4699	83.688045	HitronTe_af:b1:98	7c:ea:6d:ff:a2:cc	802.11	225	Association Response, SN=2440, FN=0, Flags=.....C
6915	99.867142	a8:65:ea:f9:cf:a8	01:37:40:44:46:23	802.11	146	Authentication, SN=434, FN=3, Flags=p.P.M...
7043	100.196334	d9:88:93:0f:ec:e9	af:40:cd:40:5f:02	802.11	146	Authentication, SN=2467, FN=4, Flags=p.P.M...
7065	100.268315	d7:19:51:08:02:f9	6d:1b:44:1a:cc:11	802.11	146	Association Request, SN=2386, FN=7, Flags=p.P.M.T.
7163	100.403689	0a:57:13:28:40:04	79:5c:58:10:7a:cc	802.11	146	Association Response, SN=3497, FN=5, Flags=p.P.M.F..[Malformed Packet]
13210	107.753005	20:b4:c4:ad:d7:19	d5:a5:29:9d:fe:00	802.11	1183	Authentication, SN=78, FN=13, Flags=p.P.F..[Malformed Packet]
16451	115.725544	f9:31:55:63:20:86	6a:8f:cd:88:f4:35	802.11	146	Authentication, SN=1054, FN=19, Flags=p.P.F..[Malformed Packet]

Fig. 13. Sequência de tramas correspondente a um processo de associação



### 3.2 Exercício 13

Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo.

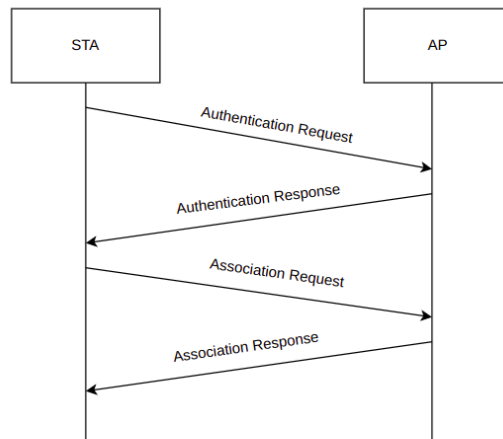


Fig. 14. Sequência de tramas trocadas no processo

## 4 Transferência de Dados

O trace disponibilizado, para além de tramas de gestão da ligação de dados, inclui tramas de dados e tramas de controlo da transferência desses mesmos dados.

### 4.1 Exercício 14

Considere a trama de dados nº431. Sabendo que o campo *Frame Control* contido no cabeçalho das tramas 802.11 permite especificar a direcionalidade das tramas, o que pode concluir face à direcionalidade dessa trama, será local à WLAN?

Através da observação da flag *DS status*, contida no campo *Frame Control*, é possível verificar que o valor de *to DS* é 0 e o valor de *from DS* é 1. Isto significa que a trama vem do DS para o STA, ou seja, não é local à WLAN.

No.	Time	Source	Destination	Protocol	Length	Info
426	17.921853		Apple_10:6a:f5 (64:.. 802.11	802.11	39	Acknowledgement, Flags=.....C
427	17.922089	HitronTe_af:b1:98 (... Apple_10:6a:f5 (64:.. 802.11	Apple_10:6a:f5 (64:.. 802.11	802.11	49	802.11 Block Ack Req, Flags=.....C
428	17.922089	Apple_10:6a:f5 (64:.. HitronTe_af:b1:98 (... 802.11	HitronTe_af:b1:98 (... 802.11	802.11	57	802.11 Block Ack, Flags=.....C
429	17.922190	HitronTe_af:b1:98 (... Apple_10:6a:f5 (64:.. 802.11	Apple_10:6a:f5 (64:.. 802.11	802.11	49	802.11 Block Ack Req, Flags=.....C
430	17.922271	Apple_10:6a:f5 (64:.. HitronTe_af:b1:98 (... 802.11	HitronTe_af:b1:98 (... 802.11	802.11	57	802.11 Block Ack, Flags=.....C
431	17.922558	HitronTe_af:b1:98 (... Apple_10:6a:f5 (64:.. 802.11	Apple_10:6a:f5 (64:.. 802.11	802.11	49	802.11 Block Ack Req, Flags=.....C
432	17.922558		HitronTe_af:b1:98 (... 802.11	802.11	39	Acknowledgement, Flags=.....C
433	17.924985	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	178	QoS Data, SN=3680, FN=0, Flags=p.....TC
434	17.925290		Apple_10:6a:f5 (64:.. 802.11	802.11	39	Acknowledgement, Flags=.....C
435	17.927587	Apple_28:b8:0c	HitronTe_af:b1:98	802.11	49	Null Function (No data), SN=0, FN=0, Flags=.....T
+ Frame 431: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)						
+ Radiotap Header v0, Length 25						
+ 802.11 radio information						
+ IEEE 802.11 QoS Data, Flags: .p...F.C						
Type/Subtype: QoS Data (0x0028)						
+ Frame Control Field: 0x0042						
.... 00 = Version: 0						
.... 10.. = Type: Data frame (2)						
1000.... = Subtype: 8						
+ Flags: 0x42						
.... 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						
1.. .... = Protected flag: Data is protected						
0.. .... = Order flag: Not strictly ordered						
.000 0000 0010 0100 = Duration: 30 microseconds						
Receiver address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)						
Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)						
Destination address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)						
Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)						
BSS id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)						
STA address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)						
.... 0000 = Fragment number: 0						
0011 0011 1110 .... = Sequence number: 838						
Frame check sequence: 0x793feef8 [correct]						
[FCS Status: Good]						

Fig. 15. Trama de dados n.º431

## 4.2 Exercício 15

Para a trama de dados n.º431, transcreva os endereços MAC em uso, identificando qual o endereço MAC correspondente ao host sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição?

Observando mais uma vez a Figura 15 é possível concluir que os endereços MAC em uso são:

STA (Receiver Address): 64:9a:be:10:6a:f5

AP (Transmitter Address): bc:14:01:af:b1:98

Router de Acesso (Destination Address): 64:9a:be:10:6a:f5

## 4.3 Exercício 16

Como interpreta a trama n.º433 face à sua direccionalidade e endereçamento MAC?

Uma vez que os valores contidos na flag *DS status* são de 1 no *to DS* e de 0 no *from DS*, é possível concluir que a trama vai do STA para o DS.

Relativamente aos endereços MAC é possível ver que o *Receiver adress* e *Destination adress* são iguais, bem como o *Transmitter adress* e o *Source adress*.

Uma vez que o *Receiver Address* se refere ao recetor imediato do pacote, isto significa que este é enviado diretamente para o seu destino, sem necessidade de recorrer a pontos intermédios.

No.	Time	Source	Destination	Protocol	Length	Info
426	17.921853		Apple_10:6a:f5 (64:...	802.11	39	Acknowledgement, Flags=.....C
427	17.922089	HitronTe_af:b1:98 (...)	Apple_10:6a:f5 (64:...	802.11	49	802.11 Block Ack Req, Flags=.....C
428	17.922089	Apple_10:6a:f5 (64:...	HitronTe_af:b1:98 (...)	802.11	57	802.11 Block Ack, Flags=.....C
429	17.922190	HitronTe_af:b1:98 (...)	Apple_10:6a:f5 (64:...	802.11	49	802.11 Block Ack Req, Flags=.....C
430	17.922271	Apple_10:6a:f5 (64:...	HitronTe_af:b1:98 (...)	802.11	57	802.11 Block Ack, Flags=.....C
431	17.922542	HitronTe_af:b1:98 (...)	Apple_10:6a:f5 (64:...	802.11	226	QoS Data, SN=830, FN=0, Flags=p....F.C
432	17.922558		HitronTe_af:b1:98 (...)	802.11	39	Acknowledgement, Flags=.....C
433	17.924985	Apple_10:6a:f5 (64:...	HitronTe_af:b1:98 (...)	802.11	178	QoS Data, SN=3680, FN=0, Flags=p....TC
434	17.925290		Apple_10:6a:f5 (64:...	802.11	39	Acknowledgement, Flags=.....C
435	17.927587	Apple_28:b8:0c	HitronTe_af:b1:98 (...)	802.11	49	Null Function (No data), SN=0, FN=0, Flags=.....T
Frame 433: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on 0						
Radiotap Header v0, Length 25						
IEEE 802.11 radio information						
IEEE 802.11 QoS Data, Flags: .p....TC						
Type/Subtype: QoS Data (0x0020)						
Frame Control Field: 0x0841						
.... 00 = Version: 0						
.... 10.. = Type: Data frame (2)						
1000 .... = Subtype: 0						
Flags: 0x41						
.... 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						
.... 1.. = Protected flag: Data is protected						
.... 0.. = Order flag: Not strictly ordered						
0000 0001 0011 1010 = Duration: 314 microseconds						
Receiver address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)						
Transmitter address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)						
Destination address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)						
Source address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)						
BSS id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)						
STA address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)						
.... 0000 = Fragment number: 0						
1110 0110 0000 .... = Sequence number: 3680						
Frame check sequence: 0x841b593c [correct]						
[FCS Status: Good]						

Fig. 16. Trama de dados n.º433

#### 4.4 Exercício 17

Que subtipo de tramas de controlo são transmitidas ao longo da transferência de dados acima mencionada? Tente explicar porque razão têm de existir (contrariamente ao que acontece numa rede Ethernet.)

O subtipo de tramas de controlo que são transmitidas é Acknowledgement (ACK). Estas tramas permitem indicar que a transmissão foi efetuada com sucesso e que as tramas foram recebidas corretamente e são necessárias devido à suscetibilidade para erros que as redes Wi-Fi possuem.

431	17.922542	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	226	QoS Data, SN=830, FN=0, Flags=p....F.C
432	17.922558		HitronTe_af:b1:98 (...)	802.11	39	Acknowledgement, Flags=.....C
433	17.924985	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	178	QoS Data, SN=3680, FN=0, Flags=p....TC
434	17.925290		Apple_10:6a:f5 (64:...	802.11	39	Acknowledgement, Flags=.....C

Fig. 17. Tramas de Controlo

#### 4.5 Exercício 18

O uso de tramas Request To Send e Clear To Send, apesar de opcional, é comum para efetuar "pré-reserva" do acesso ao meio quando se pretende enviar tramas de dados, com o intuito de reduzir o número de colisões resultante maioritariamente de STAs escondidas. Para o exemplo acima, verifique se está a ser usada a opção RTS/CTS na troca de dados entre a STA e o AP/Router da WLAN, identificando a direccionalidade das tramas e os sistemas envolvidos. Dê um exemplo de uma transferência de dados em que é usada a opção RTC/CTS e um outro em que não é usada.

No exemplo acima não está a ser usada a opção RTS/CTS. No entanto, é possível verificar a sua utilização no exemplo apresentado na figura seguinte.

```

670 25.295262 HitronTe_af:b1:98 (< Apple_10:6a:f5 (64:.. 802.11 45 Request-to-send, Flags=.....C
671 25.295267 HitronTe_af:b1:98 (< Apple_10:6a:f5 (64:.. 802.11 39 Clear-to-send, Flags=.....C
672 25.295335 HitronTe_af:b1:96 Apple_10:6a:f5 802.11 146 QoS Data, SN=841, FN=0, Flags=p....F.C
673 25.295413 Apple_10:6a:f5 (64:.. HitronTe_af:b1:98 (< Apple_10:6a:f5 (64:.. 802.11 57 802.11 Block Ack, Flags=.....C
674 25.311730 Apple_10:6a:f5 HitronTe_af:b1:98 802.11 53 Null function (No data), SN=2505, FN=0, Flags=...P...TC
675 25.311751 Apple_10:6a:f5 (64:.. 802.11 39 Acknowledgement, Flags=.....C

```

**Fig. 18.** Exemplo de utilização da opção RTC/CTS

## 5 Conclusão

A realização deste trabalho prático permitiu-nos consolidar alguns dos conhecimentos abordados nas aulas teóricas relativamente às redes sem fios.

No que diz respeito à ferramenta *Wireshark*, esta foi utilizada com o recurso a filtros de pesquisa, elaborados por nós, e que nos permitiram obter respostas mais facilmente.

Foram ainda analisadas diversas tramas e identificados os seus tipos e subtipos, bem como a sua direccionalidade.

Em conclusão, acreditamos ter obtido o aproveitamento esperado na realização deste trabalho e também conhecimentos importantes relativos ao tema do mesmo.