

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 espetro 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: 1632us]
    > IEEE 802.11 Beacon frame, Flags: .....
    > 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 subtípico. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?

O tipo e subtípico 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 vb, Length 25
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....
  Type/Subtype: Beacon frame (0x0000)
    + Frame Control Field: 0x0000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1000 .... = Subtype: 8
    + Flags: 0x00
      .0000 0000 0000 = Duration: 0 microseconds
      .0000 0000 0000 = Sequence number: 0
      Destination address: Broadcast (ffff:ffff:ffff:ffff:ffff:ffff)
      Transmitter address: MitronTe_af:b1:99 (bc:14:01:af:b1:99)
      Source address: MitronTe_af:b1:99 (bc:14:01:af:b1:99)
      BSS Id: MitronTe_af:b1:99 (bc:14:01:af:b1:99)
      .... ..0000 = Fragment number: 0
      1001 0000 0110 .... = Sequence number: 2310
      Frame check sequence: 0x6c7953ee [unverified]
      [FCS Status: Unverified]
> IEEE 802.11 Wireless Management
  0000 00 00 19 00 6f 08 00 00 ee b8 00 01 00 00 00 00 .....0.....
  0019 10 02 a3 09 80 04 b0 a9 00 88 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 a0 0b 01 00 00 64 00 21 00 00 00 4e 'e... -d- -N
  0040 4f 53 5f 57 49 46 40 5f 46 6f 60 01 00 b2 84 8b OS_WIFI_Fon...
  0050 80 00 00 00 00 03 00 00 00 00 00 00 00 00 b0 05 05 .SH1... 2...
  0060 02 03 00 40 01 00 00 2d 14 8c 81 16 ff ff 00 .....J...
  0070 00 00 00 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 00 00 .....=...
  0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7f 01 01 dd ..... .
  00a0 18 00 50 f2 02 01 01 00 00 03 a4 00 00 27 a4 00 ..P.... ...
  00b0 00 42 43 5e 00 62 32 2f 00 0b 05 03 00 0a 12 7a BCA: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: .....
> 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) (0x9e)
        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 (0xe0)

```

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: .....
> 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

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? Explicite o modo como obteve essa informação (por exemplo, se usou algum filtro para o efeito).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	HltronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2083, Fw=0, Flags=.....C, BI=100, SSID=FlyingNet
2	0.001662	HltronTe_af:b1:99	Broadcast	802.11	296	Beacon frame, SN=2084, Fw=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
3	0.003324	HltronTe_af:b1:98	Broadcast	802.11	129	Beacon frame, SN=2085, Fw=0, Flags=.....C, BI=100, SSID=FlyingNet
4	0.104164	HltronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2086, Fw=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
5	0.204951	HltronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2087, Fw=0, Flags=.....C, BI=100, SSID=FlyingNet
6	0.206582	HltronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2088, Fw=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
7	0.307363	HltronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2089, Fw=0, Flags=.....C, BI=100, SSID=FlyingNet
8	0.309029	HltronTe_af:b1:99	Broadcast	802.11	129	Beacon frame, SN=2090, Fw=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
9	0.409749	HltronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2091, Fw=0, Flags=.....C, BI=100, SSID=FlyingNet
10	0.411374	HltronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2092, Fw=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
11	0.512117	HltronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2093, Fw=0, Flags=.....C, BI=100, SSID=FlyingNet
12	0.513781	HltronTe_af:b1:99	Broadcast	802.11	129	Beacon frame, SN=2094, Fw=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
13	0.614562	HltronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2095, Fw=0, Flags=.....C, BI=100, SSID=FlyingNet
14	0.616191	HltronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2096, Fw=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
28	0.716961	HltronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2097, Fw=0, Flags=.....C, BI=100, SSID=FlyingNet
29	0.718611	HltronTe_af:b1:99	Broadcast	802.11	129	Beacon frame, SN=2098, Fw=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
32	0.815948	HltronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2099, Fw=0, Flags=.....C, BI=100, SSID=FlyingNet
33	0.821099	HltronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2100, Fw=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 == 0x08) & (wlan.fc.status == bad)]						
No.	Time	Source	Destination	Protocol	Length	Info
6274 94.779098	36:00:ae:51:f4:19	43:46:06:ca:97:53	802.11	146	Beacon Frame, SN=236, FN=9, Flags=.pmPRM.T.	
6937 99.991379	be:65:24:9b:06:a1	0e:0b:77:ea:c1:bc	802.11	146	Beacon Frame, SN=393, FN=10, Flags=...R.FT., BI=4913[Malformed Packet]	
7913 100.184381	bd:09:48:c5:79:35	43:46:15:10:df:53	802.11	146	Beacon Frame, SN=3699, FN=10, Flags=.pmPRM.T.	
7131 100.398018	62:4c:de:c5:a9:3a	34:c4:ca:25:ed:14	802.11	146	Beacon Frame, SN=2811, FN=0, Flags=.pmPRM.T.	
7378 100.494266	64:84:4c:a8:f0:ea	d2:f4:d1:ff:e9:79	802.11	146	Beacon Frame, SN=2358, FN=10, Flags=.pmPRM.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
1308 53.746911	Apple_19:08:a5:f5	Broadcast	802.11	155	Probe Request, SN=2516, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)	
2467 70.147855	ea:ad:64:70:b9:7a	Broadcast	802.11	167	Probe Request, SN=2546, FN=0, Flags=.....C, SSID=2WIRE-PT-43	
2468 70.149988	ea:ad:64:70:b9:7a	Broadcast	802.11	155	Probe Request, SN=2541, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)	
2469 70.150002	HitronTe_af:b1:98	ea:84:64:70:b9:7a	802.11	411	Probe Response, SN=2359, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
2471 70.158537	HitronTe_af:b1:98	ea:84:64:70:b9:7a	802.11	411	Probe Response, SN=2333, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
2473 70.151237	HitronTe_af:b1:98	ea:84:64:70:b9:7a	802.11	411	Probe Response, SN=2334, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon	
2475 70.151709	HitronTe_af:b1:99	ea:84:64:70:b9:7a	802.11	201	Probe Response, SN=2335, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon	
2477 70.152699	HitronTe_af:b1:99	ea:84:64:70:b9:7a	802.11	201	Probe Response, SN=2336, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon	
2478 70.152700	HitronTe_af:b1:99	ea:84:64:70:b9:7a	802.11	201	Probe Response, SN=2337, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon	
2683 72.179215	Apple_30:08:a5:f5	Broadcast	802.11	164	Probe Request, SN=2563, FN=0, Flags=.....C, SSID=FlyingNet	
2698 72.179924	HitronTe_af:b1:98	Apple_19:08:a5:f5	802.11	411	Probe Response, SN=2346, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
2698 72.180599	HitronTe_af:b1:98	Apple_19:08:a5:f5	802.11	411	Probe Response, SN=2347, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
2618 72.181275	HitronTe_af:b1:98	Apple_19:08:a5:f5	802.11	411	Probe Request, SN=2348, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
2619 72.181370	Apple_19:08:a5:f5	802.11	411	Probe Response, SN=2349, FN=0, Flags=.....C, BI=100, SSID=FlyingNet		
2617 72.282159	HitronTe_af:b1:98	Apple_19:08:a5:f5	802.11	411	Probe Response, SN=2350, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
2619 72.282887	HitronTe_af:b1:98	Apple_19:08:a5:f5	802.11	411	Probe Response, SN=2351, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
2621 72.283485	HitronTe_af:b1:98	Apple_19:08:a5:f5	802.11	411	Probe Response, SN=2352, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
2656 72.488906	Apple_19:08:a5:f5	Broadcast	802.11	164	Probe Request, SN=2585, FN=0, Flags=.....C, SSID=FlyingNet	
2655 72.588353	Apple_19:08:a5:f5	Broadcast	802.11	164	Probe Request, SN=2586, FN=0, Flags=.....C, SSID=FlyingNet	
2677 72.588343	Apple_19:08:a5:f5	Broadcast	802.11	164	Probe Request, SN=2589, FN=0, Flags=.....C, SSID=FlyingNet	
2678 72.578258	Apple_19:08:a5:f5	Broadcast	802.11	164	Probe Request, SN=2590, FN=0, Flags=.....C, SSID=FlyingNet	
4455 82.621343	7:ce:a6:ff:a2:cc	Broadcast	802.11	71	Probe Request, SN=62, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)	
4493 82.726818	7:ce:a6:ff:a2:cc	Broadcast	802.11	71	Probe Request, SN=64, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)	
4494 82.728646	7:ce:a6:ff:a2:cc	Broadcast	802.11	218	Probe Request, SN=65, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)	
6193 94.190808	Apple_29:b0:9c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet	

Fig. 9. Tramas Probing Request e Probing Response

De modo a sabermos os valores relativos a cada subtípico 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?

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:41:64:7b:b9:7a	Broadcast	802.11	167	Probe Request, SN=2540, FN=0, Flags=....., C, SSID=2WIRE_PT-431		
2468 70.147855		ea:41:64:7b:b9:7a	Broadcast	802.11	167	Probe Request, SN=2541, FN=0, Flags=....., C, SSID=Wildcard (Broadcast)		
2469 70.149792		HironTe_af:b1:98	ea:41:64:7b:b9:7a	802.11	411	Probe Response, SN=2323, FN=0, Flags=....., C, BI=100, SSID=FlyingNet		
2471 70.150537		HironTe_af:b1:98	ea:41:64:7b:b9:7a	802.11	411	Probe Response, SN=2335, FN=0, Flags=....., C, BI=100, SSID=FlyingNet		
2473 70.151237		HironTe_af:b1:98	ea:41:64:7b:b9:7a	802.11	411	Probe Response, SN=2334, FN=0, Flags=....., C, BI=100, SSID=FlyingNet		
2475 70.151237		HironTe_af:b1:98	ea:41:64:7b:b9:7a	802.11	261	Probe Response, SN=2335, FN=0, Flags=....., C, BI=100, SSID=NOS_WIFI_Fon		
2477 70.152999		HironTe_af:b1:98	ea:41:64:7b:b9:7a	802.11	281	Probe Response, SN=2336, FN=0, Flags=....., C, BI=100, SSID=NOS_WIFI_Fon		
2479 70.152570		HironTe_af:b1:99	ea:41:64:7b:09:7a	802.11	281	Probe Response, SN=2337, FN=0, Flags=....., C, BI=100, SSID=NOS_WIFI_Fon		
2663 72.179215		Apple_10:6a:f5	Broadcast	802.11	167	Probe Request, SN=2563, FN=0, Flags=....., C, SSID=FlyingNet		
2666 72.179215		Apple_10:6a:f5	Broadcast	802.11	167	Probe Request, SN=2564, FN=0, Flags=....., C, BI=100, SSID=FlyingNet		
2668 72.180859		HironTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2347, FN=0, Flags=....., C, BI=100, SSID=FlyingNet		
2618 72.181275		HironTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2348, FN=0, Flags=....., C, BI=100, SSID=FlyingNet		
2619 72.181275		Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2565, FN=0, Flags=....., C, SSID=FlyingNet		
2617 72.202159		Apple_10:6a:f5	Apple_10:6a:f5	802.11	411	Probe Response, SN=2356, FN=0, Flags=....., C, BI=100, SSID=FlyingNet		

Fig. 11. Probing Request

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:41:64:7b:b9:7a	Broadcast	802.11	167	Probe Request, SN=2540, FN=0, Flags=....., C, SSID=2WIRE_PT-431		
2468 70.147855		ea:41:64:7b:b9:7a	Broadcast	802.11	167	Probe Request, SN=2541, FN=0, Flags=....., C, SSID=Wildcard (Broadcast)		
2469 70.149792		HironTe_af:b1:98	ea:41:64:7b:b9:7a	802.11	411	Probe Response, SN=2323, FN=0, Flags=....., C, BI=100, SSID=FlyingNet		
2471 70.150537		HironTe_af:b1:98	ea:41:64:7b:b9:7a	802.11	411	Probe Response, SN=2335, FN=0, Flags=....., C, BI=100, SSID=FlyingNet		
2473 70.151237		HironTe_af:b1:98	ea:41:64:7b:b9:7a	802.11	261	Probe Response, SN=2336, FN=0, Flags=....., C, BI=100, SSID=NOS_WIFI_Fon		
2475 70.151237		HironTe_af:b1:98	ea:41:64:7b:b9:7a	802.11	281	Probe Response, SN=2337, FN=0, Flags=....., C, BI=100, SSID=NOS_WIFI_Fon		
2479 70.152570		HironTe_af:b1:99	ea:41:64:7b:09:7a	802.11	281	Probe Response, SN=2338, FN=0, Flags=....., C, BI=100, SSID=NOS_WIFI_Fon		
2663 72.179215		Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2563, FN=0, Flags=....., C, SSID=FlyingNet		
2666 72.179215		Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2564, FN=0, Flags=....., C, BI=100, SSID=FlyingNet		
2668 72.179924		HironTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2349, FN=0, Flags=....., C, BI=100, SSID=FlyingNet		
2618 72.181275		HironTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2350, FN=0, Flags=....., C, BI=100, SSID=FlyingNet		
2619 72.181275		Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2565, FN=0, Flags=....., C, SSID=FlyingNet		
2617 72.201590		Apple_10:6a:f5	Apple_10:6a:f5	802.11	411	Probe Response, SN=2356, FN=0, Flags=....., C, BI=100, SSID=FlyingNet		

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
2486 70.361782	Apple_10:6a:f5	HironTe_af:b1:98	Apple_10:6a:f5	802.11	70	Authentication, SN=2542, FN=0, Flags=.....C
2488 70.381869	Apple_10:6a:f5	HironTe_af:b1:98	Apple_10:6a:f5	802.11	59	Authentication, SN=2338, FN=0, Flags=.....C
2489 70.381869	Apple_10:6a:f5	HironTe_af:b1:98	Apple_10:6a:f5	802.11	1	Authentication, SN=2338, FN=0, Flags=.....C, SSID=FlyingNet
2492 70.389339	HironTe_af:b1:98	Apple_10:6a:f5	Apple_10:6a:f5	802.11	225	Association Response, SN=2339, FN=0, Flags=.....C
4692 83.663250	7:c:ea:6d:ff:a2:cc	HironTe_af:b1:98	7:c:ea:6d:ff:a2:cc	802.11	59	Authentication, SN=67, FN=0, Flags=.....C
4694 83.663681	HironTe_af:b1:98	7:c:ea:6d:ff:a2:cc	7:c:ea:6d:ff:a2:cc	802.11	59	Authentication, SN=2439, FN=0, Flags=.....C
4696 83.665976	7:c:ea:6d:ff:a2:cc	HironTe_af:b1:98	7:c:ea:6d:ff:a2:cc	802.11	153	Association Request, SN=68, FN=0, Flags=.....C, SSID=FlyingNet
4698 83.678505	HironTe_af:b1:98	7:c:ea:6d:ff:a2:cc	7:c:ea:6d:ff:a2:cc	802.11	225	Association Response, SN=2440, FN=0, Flags=.....C
4699 83.678505	HironTe_af:b1:98	7:c:ea:6d:ff:a2:cc	7:c:ea:6d:ff:a2:cc	802.11	225	Association Response, SN=2440, FN=0, Flags=.....C
6019 90.957442	80:0c:9a:f5:c7:a0	7:c:37:40:44:40:73	802.11	146	Authentication, SN=414, FN=1, Flags=op.P.M...	
7943 100.196334	dd:88:93:0f:ec:e9	af:40:cd:40:5f:82	802.11	146	Authentication, SN=2467, FN=4, Flags=op.P.M...	
7965 100.208371	d7:19:51:08:62:f9	6d:1b:44:1a:cc:11	802.11	146	Association Request, SN=2586, FN=7, Flags=pmRNM.T	
7163 100.463689	0a:57:13:28:40:84	79:5c:58:10:7e:cc	802.11	146	Association Response, SN=3497, FN=5, Flags=so.MP..F..[Malformed Packet]	
13218 100.7530985	20:b4:c4:ad:d1:19	d5:a5:29:9b:fe:00	802.11	1183	Authentication, SN=79, FN=13, Flags=so..PR.F..[Malformed Packet]	
10451 115.725544	f0:31:95:63:20:86	6a:6f:c0:68:f4:55	802.11	146	Authentication, SN=1084, FN=10, Flags=so.P...[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.

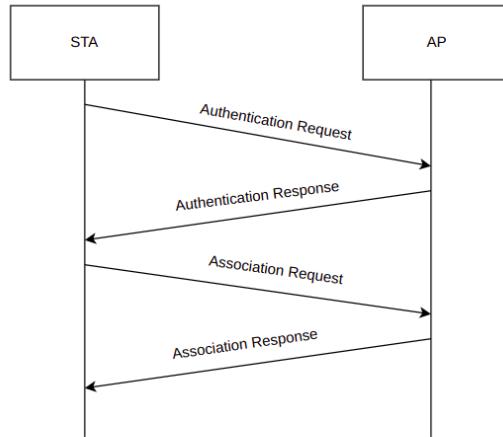


Fig. 14. Sequência de tramas trocadas no processo

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 direccionalidade das tramas, o que pode concluir face à direccionalidade 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			39 Acknowledgement, Flags=.....C
427 17. 922089		HironTe_af:b1:98 (.. Apple_10:6a:f5 (64:.. 802.11			49 802.11 Block Ack Req, Flags=....C
428 17. 922099		Apple_10:6a:f5 (64:.. HironTe_af:b1:98 (..			57 802.11 Block Ack, Flags=.....C
429 17. 922199		HironTe_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:.. HironTe_af:b1:98 (..			57 802.11 Block Ack, Flags=.....C
431 17. 922558		HironTe_af:b1:98 (..			49 Acknowledgement, Flags=.....F.C
432 17. 922558		Apple_10:6a:f5 (64:.. HironTe_af:b1:98 (..			39 Acknowledgement, Flags=.....C
433 17. 924985		Apple_10:6a:f5 (64:.. HironTe_af:b1:98 (..			178 QoS Data, SN=3680, FN=0, Flags=p....TC
434 17. 925298		Apple_10:6a:f5 (64:.. HironTe_af:b1:98 (..			39 Acknowledgement, Flags=.....C
435 17. 927587		Apple_28:b8:0c (..			49 Null Function (No data), SN=0, FN=0, Flags=.....T
Frame 431: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)					
RadioLink Header, Length: 26 bytes (208 bits)					
802.11 radio information					
- IEEE 802.11 QoS Data, Flags: .p....F.C					
- Type/Subtype: QoS Data (0x0028)					
- Frame Control: 0x00000000000000000000000000000000					
-00 = Version: 1					
- ..0.. = 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) (0x02)					
-0..1 = More Fragments: This is the last fragment					
-0.. = Retry: Frame is not being retransmitted					
- ..0 = PWR MGT: STA will stay up					
- ..0. = More Data: Data buffered					
- 1.... = Intercepted flag: Data was intercepted					
- 0.... = Order flag: Not strictly ordered					
.000 0000 0010 0100 = Duration: 36 microseconds					
Receive address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)					
Transmitter address: HironTe_af:b1:98 (bc:14:01:af:b1:98)					
Destination address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)					
Source address: HironTe_af:b1:98 (bc:14:01:af:b1:98)					
BSS Id: HironTe_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					
0000 0000 1000 0000 = Sequence number: 830					
Frame check sequence: 0x793feef8 [correct]					
[FCS Status: Good]					

Fig. 15. Trama de dados n.º431

4.2 Exercício 15

Para a trama de dados nº431, 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 Adress): 64:9a:be:10:6a:f5

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

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

4.3 Exercício 16

Como interpreta a trama nº433 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 que o *Receiver adress* e *Destination adress* são iguais, bem como o *Transmitter adress* e o *Source adress*. Uma vez que o *Receiver Adress* 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     Hirontrc_af:bf:98  {Apple:10:6a:f5  64:...:802.11      49 802.11 Block Ack Red, Flags=.....C
428 17.922099     Apple:10:6a:f5  {64:...:802.11      39 Acknowledgement, Flags=.....C
429 17.922109     Hirontrc_af:bf:98  {Apple:10:6a:f5  64:...:802.11      49 802.11 Block Ack, Flags=.....C
430 17.922273     Apple:10:6a:f5  {64:...:802.11      39 Acknowledgement, Flags=.....C
431 17.922542     Apple:10:6a:f5  {Hirontrc_af:bf:98 64:...:802.11      57 802.11 Block Ack, Flags=.....C
432 17.922558     Hirontrc_af:bf:98  {Apple:10:6a:f5  64:...:802.11      39 Null Function (No data), SN=830, FN=0, Flags=.....F..C
433 17.924985     Apple:10:6a:f5  {Hirontrc_af:bf:98 64:...:802.11      178 QoS Data, SN=380, FN=0, Flags=....TC
434 17.925001     Apple:10:6a:f5  {Hirontrc_af:bf:98 64:...:802.11      39 Acknowledgement, Flags=.....C
435 17.925787     Apple:10:6a:f5  {Hirontrc_af:bf:98 64:...:802.11      49 Null Function (No data), SN=0, FN=8, Flags=.....T

Frame 433: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits)
   Radiotap Header: Vlue, Length 25
   802.11 radio frame information
   IEEE 802.11 DS/RTS/CTS/ACK Flags: D....TC
   Type/Subtype: QoS Data (0x0020)
     - Frame Control Field: 0x8841
       .... ..00 = Version: 0
       .... ..00 = Type: Data (frame (2))
       1000 ... .00 = Subtype: 8
     - Flags (0x14)
       .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
       .... ..00 = More Fragments: This is the last fragment
       .... ..00 = Retry: Frame is not being retransmitted
       .... ..00 = DS Will Not Acknowledge
       .... ..00 = More Data: No data buffered
       .1. .... ..00 = Protected flag: Data is protected
       0.... ..00 = Order flag: Not strictly ordered
     - 0000 0001 0011 1010 = Duration: 314 microseconds
   Reference Address: Hirontrc_af:bf:98 (bc:14:01:af:bf:98) (0x18:01:00:00:00:00)
   Reference Transmitter address: Apple:30:be:6f (4d:9a:be:10:a6:f5) (0x18:01:00:00:00:00)
   Destination address: Hirontrc_af:bf:98 (bc:14:01:af:bf:98) (0x18:01:00:00:00:00)
   Source address: Apple:10:6a:f5 (4d:9a:be:10:a6:f5) (0x18:01:00:00:00:00)
   BSS ID: Hirontrc_af:bf:98 (bc:14:01:af:bf:98) (0x18:01:00:00:00:00)
   STA address: Hirontrc_af:bf:98 (bc:14:01:af:bf:98) (0x18:01:00:00:00:00)
   Sequence number: 0
   1110 0110 0000 .... = Sequence number: 3680
   Frame check sequence: 0x8a1b593c [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:bi:98 Apple_10:6a:f5 . 802.11 226 QoS Data, SN=830, FN=0, Flags=....F.C
432 17_922558 HitronTe_af:bi:98 Apple_10:6a:f5 . 802.11 39 Acknowledgement, Flags=....C
433 17_924985 Apple_10:6a:f5 HitronTe_af:bi:98 . 802.11 178 QoS Data, SN=3689, FN=0, Flags=....TC
434 17_925928 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 (... 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 (... 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.