

# TP4: Redes sem fios (802.11)

Diogo Afonso Costa, Daniel Maia, and Vitor Castro

University of Minho, Department of Informatics, 4710-057 Braga, Portugal  
e-mail: {a78034,a77531,a77870}@alunos.uminho.pt

**Abstract.** Este trabalho tem como objectivo explorar as particularidades do protocolo IEEE 802.11, especificamente, o formato das tramas, o endereçamento dos componentes envolvidos na comunicação sem fios e os tipos de tramas mais comuns, bem como a operação do protocolo.

## 1 Introdução

O protocolo IEEE 802.11 tem como objetivo oferecer conectividade sem fios entre diferentes estações (STAs).

Deste modo, este trabalho procura perceber alguns dos conceitos básicos associados a esta norma, assim como alguns dos principais processos que esta implementa e ainda as razões por detrás de algumas funcionalidades que a norma IEEE 802.11 oferece. Nomeadamente, realça-se a forma como é realizada a comunicação entre as diferentes STAs e o ponto de acesso (AP), acrescentando como é concretizada a associação de um novo STA ao AP, ou mesmo, como é, efetivamente, realizada a transferência de dados na rede.

Contudo, é de notar que por ser um protocolo que rege uma comunicação sem fios, existe um cuidado omnipresente no que toca à colisão de tramas, uma vez que o meio de propagação (ar) é partilhado pelos diferentes utilizadores.

## 2 Acesso Rádio (Para a trama correspondente 733)

### 2.1 Exercício 1

#### Questão

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

#### Resposta

A rede sem fios encontra-se a operar numa frequência de 2462MHz, que consequentemente pertence ao espectro dos 2GHz.

Além disso, o canal usado é o número 11.

#### Realização

```
Radiotap Header v0, Length 25
Header revision: 0
Header pad: 0
Header length: 25
Present flags
MAC timestamp: 186492754
Flags: 0x10
Data Rate: 1,0 Mb/s
Channel frequency: 2462 [BG 11]
Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM
...0... = Turbo: False
...0... = Complementary Code Keying (CCK): False
...0... = Orthogonal Frequency-Division Multiplexing (OFDM): False
...1... = 2 GHz spectrum: True
...0... = 5 GHz spectrum: False
...0... = Passive: False
...1... = Dynamic CCK-OFDM: True
...0... = Gaussian Frequency Shift Keying (GFSK): False
...0... = GSM (900MHz): False
...0... = Static Turbo: False
...0... = Half Rate Channel (10MHz Channel Width): False
...0... = Quarter Rate Channel (5MHz Channel Width): False
SSI Signal: -74dBm
SSI Noise: -85dBm
Antenna: 0
802.11 radio information
PHY type: 802.11g (6)
Short preamble: False
Proprietary mode: None (0)
Data rate: 1,0 Mb/s
Channel: 11
Frequency: 2462MHz
Signal strength (dbm): -74dBm
Noise level (dbm): -85dBm
TSF timestamp: 186492754
[Duration: 1992µs]
```

Fig. 1: Frequência do espectro em que a rede sem fios se encontra a operar assim como o respetivo canal.

## 2.2 Exercício 2

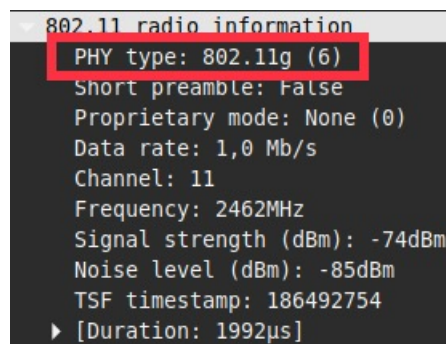
### Questão

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

### Resposta

A versão utilizada é a IEEE 802.11g.

### Realização

A screenshot of the Wireshark network protocol analyzer interface. The 'Packet Details' pane on the left shows a selected packet of type '802.11'. The '802.11 radio information' section is expanded, revealing several fields. The 'PHY type' field is highlighted with a red rectangular box and contains the text '802.11g (6)'. Other visible fields include 'Short preamble: False', 'Proprietary mode: None (0)', 'Data rate: 1,0 Mb/s', 'Channel: 11', 'Frequency: 2462MHz', 'Signal strength (dBm): -74dBm', 'Noise level (dBm): -85dBm', 'TSF timestamp: 186492754', and '[Duration: 1992µs]'.

```
802.11 radio information
  PHY type: 802.11g (6)
  Short preamble: False
  Proprietary mode: None (0)
  Data rate: 1,0 Mb/s
  Channel: 11
  Frequency: 2462MHz
  Signal strength (dBm): -74dBm
  Noise level (dBm): -85dBm
  TSF timestamp: 186492754
  ▶ [Duration: 1992µs]
```

Fig. 2: Versão da norma IEEE utilizada.

## 2.3 Exercício 3

### Questão

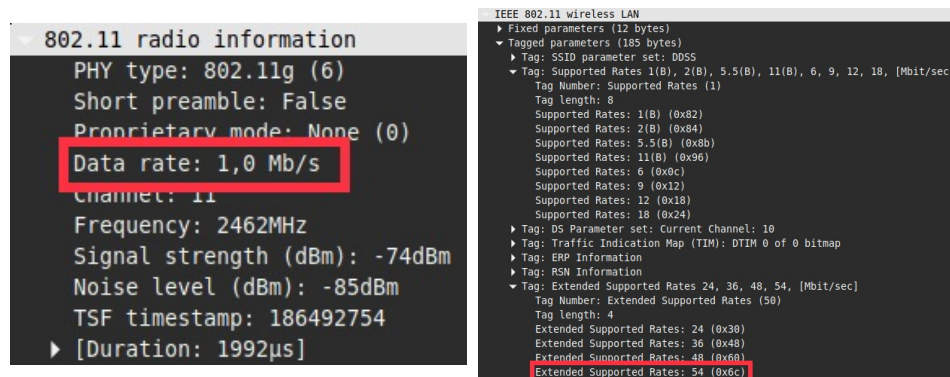
Qual o débito a que foi enviada a trama escolhida? Será que esse débito corresponde ao débito máximo a que a interface WiFi pode operar? Justifique.

### Resposta

A trama escolhida foi enviada a 1.0 Mb/s. Visto tratar-se de uma trama que usa a norma IEEE 802.11g tem-se por defeito acesso a débitos até 54 Mb/s [1].

Efetivamente, a razão pela qual o débito se encontra consideravelmente baixo em relação ao máximo permitido pode resultar de diferentes fatores. Nomeadamente, quando a distância entre o *host* e o ponto de acesso (AP) aumenta, o *signal-to-noise ratio* (SNR) diminui e o bit error ratio (BER) também. Por forma a combater o declínio na qualidade da ligação, caso a distância assim o justifique, o débito a que a trama é transmitida pode ser diminuído por forma a aumentar o SNR e a diminuir o BER. Deste modo, talvez por esta razão a frequência a que se encontra a operar a ligação seja relativamente baixa (2462 MHz) quando comparada com a frequência máxima que uma ligação 802.11g pode oferecer, ou seja, 5 GHz [1] [2] [3].

### Realização



The figure consists of two side-by-side screenshots from a network analysis tool. The left screenshot, titled '802.11 radio information', shows various parameters: PHY type: 802.11g (6), Short preamble: False, Proprietary mode: None (0), Data rate: 1,0 Mb/s (highlighted with a red box), Channel: 11, Frequency: 2462MHz, Signal strength (dBm): -74dBm, Noise level (dBm): -85dBm, TSF timestamp: 186492754, and Duration: 1992µs. The right screenshot, titled 'IEEE 802.11 wireless LAN', shows a tree view of parameters. Under 'Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]', it lists supported rates: 1(B) (0x82), 2(B) (0x84), 5.5(B) (0x8b), 11(B) (0x96), 6 (0x0c), 9 (0x12), 12 (0x18), and 18 (0x24). Under 'Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]', it lists extended supported rates: 24 (0x30), 36 (0x48), 48 (0x60), and 54 (0x6c) (highlighted with a red box).

Fig. 3: Comparação do débito da trama com o máximo permitido na norma 802.11g.

### 3 Scanning Passivo e Scanning Ativo

#### 3.1 Exercício 4

##### Questão

Selecione uma trama beacon (cujo número de ordem inclua o seu número de grupo [33]). 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)?

##### Resposta

[Trama nº 233] Esta trama é uma *Management Frame* (identificador 00) de subtipo *Beacon* (identificador 1000 em binário, 8 em decimal). Os identificadores estão presentes em IEEE 802.11 Beacon Frame, no campo Frame Control, nos bits 4-5 e 0-3, respetivamente.

##### Realização

No.	Time	Source	Destination	Protocol	Length	Info
221	5.328037	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3035, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
222	5.329996	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3036, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
223	5.363373	Tp-LinkT_ee:f4:ca	Broadcast	802.11	250	Beacon frame, SN=2171, FN=0, Flags=.....C, BI=100, SSID=0055
224	5.430388	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3037, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
225	5.432251	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3038, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
226	5.532811	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3039, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
227	5.534673	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3040, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
228	5.635164	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3041, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
229	5.637059	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3042, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
230	5.670182	Tp-LinkT_ee:f4:ca	Broadcast	802.11	250	Beacon frame, SN=2175, FN=0, Flags=.....C, BI=100, SSID=0055
231	5.737657	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3043, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
232	5.739472	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3044, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
233	5.839995	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3045, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
234	5.841959	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3046, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
235	5.942522	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3047, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
236	5.944342	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3048, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
237	5.977022	Tp-LinkT_ee:f4:ca	Broadcast	802.11	250	Beacon frame, SN=2178, FN=0, Flags=.....C, BI=100, SSID=0055
238	6.044928	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3049, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
239	6.046755	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3050, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET

> Frame 233: 315 bytes on wire (2520 bits), 315 bytes captured (2520 bits) on interface 0

> Radiotap Header V0, Length 25

> 802.11 radio information

IEEE 802.11 Beacon frame, Flags: .....C

Type/Subtype: Beacon frame (0x0000)

Frame Control Field: 0x0000

.... 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\_1b:27:78 (bc:14:01:1b:27:78)

Source address: HitronTe\_1b:27:78 (bc:14:01:1b:27:78)

BSS Id: HitronTe\_1b:27:78 (bc:14:01:1b:27:78)

.... .... 0000 = Fragment number: 0

1011 1110 0101 .... = Sequence number: 3045

Fig. 4: Os identificadores do tipo e subtipo da trama *Beacon*.

## 3.2 Exercício 5

### Questão

Liste todos os SSIDs dos APs (Access Points) que estão a operar na vizinhança da STA de captura? Explique o modo como obteve essa informação. Como sugestão pode construir um filtro de visualização apropriado (tomando como base a resposta da alínea anterior) que lhe permita obter a listagem pretendida.

### Resposta

Ao aplicar o filtro `wlan.fc == 0x8000`, obtêm-se todas as tramas *beacon* enviadas pelos AP's circundantes. Observando o campo IEEE 802.11 wireless LAN -> Tagged parameters -> Tag: SSID parameter set -> SSID ao longo das tramas capturadas, determina-se que existem 3 AP's, com os SSID's ZON-2770, FON\_ZON\_FREE\_INTERNET e DDSS.

### Realização

No.	Time	Source	Destination	Protocol	Length	Info
227	5.534673	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3040, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
228	5.635164	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3041, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
229	5.637059	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3042, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
230	5.670182	Tp-LinkT_ee:f4:ca	Broadcast	802.11	250	Beacon frame, SN=2175, FN=0, Flags=.....C, BI=100, SSID=DDSS
231	5.737657	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3043, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
232	5.739472	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3044, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
233	5.839995	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3045, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
234	5.841959	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3046, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
235	5.942522	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3047, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
236	5.944342	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3048, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
237	5.977022	Tp-LinkT_ee:f4:ca	Broadcast	802.11	250	Beacon frame, SN=2178, FN=0, Flags=.....C, BI=100, SSID=DDSS
238	6.044920	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3049, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
239	6.046755	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3050, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
240	6.079395	Tp-LinkT_ee:f4:ca	Broadcast	802.11	250	Beacon frame, SN=2179, FN=0, Flags=.....C, BI=100, SSID=DDSS
241	6.147308	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3051, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
242	6.149175	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3052, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
243	6.250040	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3053, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
244	6.251932	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3054, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
245	6.352652	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3055, FN=0, Flags=.....C, BI=100, SSID=ZON-2770

> Frame 233: 315 bytes on wire (2520 bits), 315 bytes captured (2520 bits) on interface 0

> Radiotap Header v0, Length 25

> 802.11 radio information

> IEEE 802.11 Beacon frame, Flags: .....C

> IEEE 802.11 wireless LAN

> Fixed parameters (12 bytes)

> Tagged parameters (250 bytes)

> Tag: SSID parameter set: ZON-2770

> Tag Number: SSID parameter set (0)

> Tag Length: 8

> SSID: ZON-2770

> Tag: Supported Rates 1(8), 2(8), 5.5(8), 11(8), 9, 18, 36, 54, [Mbit/sec]

> Tag: DS Parameter set: Current Channel: 11

> Tag: Extended Supported Rates 6, 12, 24, 48, [Mbit/sec]

> Tag: AP Channel Report: Operating Class 32, Channel List : 1, 2, 3, 4, 5, 6, 7,

> Tag: AP Channel Report: Operating Class 33, Channel List : 5, 6, 7, 8, 9, 10, 11,

> Tag: Vendor Specific: Microsoft: WPS

> Tag: Traffic Indication Map (TIM): DTIM 2 of 0 bitmap

> Tag: ERP Information

> Tag: HT Capabilities (802.11n D1.10)

Fig. 5: O SSID da trama 233; O Wireshark destaca esta informação por defeito.

### 3.3 Exercício 6

#### Questão

Verifique se está a ser usado o método de detecção de erros (CRC), e se todas as tramas Beacon são recebidas corretamente. Justifique a conveniência em usar detecção de erros neste tipo de redes locais.

#### Resposta

Está de facto a ser utilizada CRC, nomeadamente através de frame check sequence (FCS). Nem todas as tramas beacon estão a ser recebidas corretamente, visto que é possível encontrar uma pequena percentagem de tramas com um FCS incorreto. É conveniente utilizar detecção de erros em redes sem fios visto que estes são por natureza dispostos a ter mais ruído do que os meios com fios, o que leva a uma maior probabilidade de corrupção de dados enviados. Deste modo, assegura-se que não ocorrem falhas de interpretação de informação ou desperdício de recursos.

#### Realização

No.	Time	Source	Destination	Protocol	Length	Info
945	26.843321	HitronTe_ib:27:78	Broadcast	802.11	315	Beacon frame, SN=3455, FH=0, Flags=.....C, BI=100, SSID=ZON-2778
946	26.845261	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3456, FH=0, Flags=.....C, BI=100, SSID=FOH_ZON_FREE_INTERNET
947	26.851857	Tp-Link_eef:fa:ca	Broadcast	802.11	250	Beacon frame, SN=2397, FH=0, Flags=.....C, BI=100, SSID=0055
948	26.945757	HitronTe_ib:27:78	Broadcast	802.11	315	Beacon frame, SN=3457, FH=0, Flags=.....C, BI=100, SSID=ZON-2778
949	26.947557	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3458, FH=0, Flags=.....C, BI=100, SSID=FOH_ZON_FREE_INTERNET
950	27.048137	HitronTe_ib:27:78	Broadcast	802.11	315	Beacon frame, SN=3459, FH=0, Flags=.....C, BI=100, SSID=ZON-2778
951	27.049919	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3460, FH=0, Flags=.....C, BI=100, SSID=FOH_ZON_FREE_INTERNET
952	27.108113	HitronTe_Sci5b:38	Broadcast	802.11	274	Beacon frame, SN=2728, FH=0, Flags=.....C, BI=100, SSID=MON-5B38-0001b\357\277\275\357\277\275\0225h\003\001\004\1f
953	27.150603	HitronTe_ib:27:78	Broadcast	802.11	315	Beacon frame, SN=3461, FH=0, Flags=.....C, BI=100, SSID=ZON-2778
954	27.152410	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3462, FH=0, Flags=.....C, BI=100, SSID=FOH_ZON_FREE_INTERNET
955	27.253286	HitronTe_ib:27:78	Broadcast	802.11	315	Beacon frame, SN=3463, FH=0, Flags=.....C, BI=100, SSID=ZON-2778
956	27.255173	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3464, FH=0, Flags=.....C, BI=100, SSID=FOH_ZON_FREE_INTERNET
957	27.355907	HitronTe_ib:27:78	Broadcast	802.11	315	Beacon frame, SN=3465, FH=0, Flags=.....C, BI=100, SSID=ZON-2778
958	27.357755	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3466, FH=0, Flags=.....C, BI=100, SSID=FOH_ZON_FREE_INTERNET
959	27.450258	HitronTe_ib:27:78	Broadcast	802.11	315	Beacon frame, SN=3467, FH=0, Flags=.....C, BI=100, SSID=ZON-2778
960	27.460131	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3468, FH=0, Flags=.....C, BI=100, SSID=FOH_ZON_FREE_INTERNET
961	27.560684	HitronTe_ib:27:78	Broadcast	802.11	315	Beacon frame, SN=3469, FH=0, Flags=.....C, BI=100, SSID=ZON-2778
962	27.562550	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3470, FH=0, Flags=.....C, BI=100, SSID=FOH_ZON_FREE_INTERNET
963	27.663048	HitronTe_ib:27:78	Broadcast	802.11	315	Beacon frame, SN=3471, FH=0, Flags=.....C, BI=100, SSID=ZON-2778
964	27.665931	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3472, FH=0, Flags=.....C, BI=100, SSID=FOH_ZON_FREE_INTERNET

Source address: HitronTe\_Sci5b:38 (68:b6:fc:5c:5b:38)

BSS Id: HitronTe\_Sci5b:38 (68:b6:fc:5c:5b:38)

.... .. 0000 = Fragment number: 0

1010 1010 1000 .... = Sequence Number: 2728

Frame check sequence: 0x3ac47ee incorrect, should be 0x37a9baf4

FCS Status: Bad!

IEEE 802.11 wireless LAN

Fixed parameters (12 bytes)

Tagged parameters (200 bytes)

Tag: SSID parameter set: MON-5B38-0001b\357\277\275\357\277\275\357\277\275\0225h\003\001\004\1f

Tag Number: SSID parameter set (0)

Tag length: 248

[Expert Info (Error/Malformed): SSID length (248) greater than maximum (32)]

SSID: MON-5B38-0001b\357\277\275\357\277\275\357\277\275\0225h\003\001\004\1f0300'3'b\001\002\003\357\277\275\003\006\03\01\005\006\0a\0t\0n\357\277\275\005

Tag: Schedule

Tag Number: Schedule (15)

Tag length: 172

[Expert Info (Error/Malformed): Tag Length is longer than remaining payload]

[Expert Info (Error/Malformed): Tag Length 172 wrong, must be = 14]

Fig. 6: O campo FCS de uma trama corrompida; nota-se que o *Wireshark* destaca os campos corrompidos.

### 3.4 Exercício 7

#### Questão

Para dois dos APs identificados, indique qual é o intervalo de tempo previsto entre tramas beacon consecutivas? (Nota: este valor é anunciado na própria trama beacon). Na prática, a periodicidade de tramas beacon é verificada? Tente explicar porquê.

#### Resposta

SSID ZON-2770: intervalo de acordo com a trama: 0.102400 s

SSID FON\_ZON\_FREE\_INTERNET: intervalo de acordo com a trama: 0.102400 s

Na prática, o valor do intervalo de tempo varia cerca de  $\pm 0.0001$  s relativamente ao intervalo previsto. Isto pode se dever ao facto de que é necessário fazer deteção de erros ao receber cada trama. Isto é tido em conta pelo beacon interval e, como o tempo necessário para fazer a verificação é imutável, ocorrem pequenas variâncias no intervalo entre tramas.

#### Realização

No.	Time	Source	Destination	Protocol	Length	Info
225	5.432251	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3038, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
226	5.532811	HitronTe_ib:27:79	Broadcast	802.11	315	Beacon frame, SN=3039, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
227	5.534673	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3040, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
228	5.635164	HitronTe_ib:27:79	Broadcast	802.11	315	Beacon frame, SN=3041, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
229	5.637059	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3042, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
230	5.670182	Tp-Link_eef4:ca	Broadcast	802.11	250	Beacon frame, SN=2175, FH=0, Flags=.....C, BI=100, SSID=0055
231	5.737657	HitronTe_ib:27:79	Broadcast	802.11	315	Beacon frame, SN=3043, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
232	5.739472	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3044, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
233	5.839995	HitronTe_ib:27:79	Broadcast	802.11	315	Beacon frame, SN=3045, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
234	5.841955	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3046, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
235	5.942522	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3047, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
236	5.944342	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3048, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
237	5.977022	Tp-Link_eef4:ca	Broadcast	802.11	250	Beacon frame, SN=2178, FH=0, Flags=.....C, BI=100, SSID=0055
238	6.044920	HitronTe_ib:27:79	Broadcast	802.11	315	Beacon frame, SN=3049, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
239	6.046755	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3050, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
240	6.079395	Tp-Link_eef4:ca	Broadcast	802.11	250	Beacon frame, SN=2179, FH=0, Flags=.....C, BI=100, SSID=0055
241	6.147300	HitronTe_ib:27:79	Broadcast	802.11	315	Beacon frame, SN=3051, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
242	6.149175	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3052, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
243	6.250408	HitronTe_ib:27:79	Broadcast	802.11	315	Beacon frame, SN=3053, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
244	6.251932	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3054, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET

Frame 233: 315 bytes on wire (2520 bits), 315 bytes captured (2520 bits) on interface 0

Radiotap Header v0, Length 25

802.11 radio information

IEEE 802.11 Beacon frame, Flags: .....C

IEEE 802.11 Wireless LAN

Fixed parameters (12 bytes)

Timestamp: 0x00000193da553143

Beacon Interval: 0.102400 (seconds)

Capabilities Information: 0x0431

Tagged parameters (250 bytes)

Tag: SSID parameter set: ZON-2770

Fig. 7: Um exemplo de um intervalo real entre duas tramas beacon do mesmo AP, igual a 0.102527 s.



No.	Time	Source	Destination	Protocol	Length	Info
225	5.432251	HitronTe_ib:27:79	Broadcast	002.11	233	Beacon frame, SN=3038, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
226	5.532811	HitronTe_ib:27:79	Broadcast	002.11	315	Beacon frame, SN=3039, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
227	5.534673	HitronTe_ib:27:79	Broadcast	002.11	233	Beacon frame, SN=3040, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
228	5.635164	HitronTe_ib:27:79	Broadcast	002.11	315	Beacon frame, SN=3041, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
229	5.637959	HitronTe_ib:27:79	Broadcast	002.11	233	Beacon frame, SN=3042, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
230	5.670182	Tp-LinkT_ei:f4:c	Broadcast	002.11	250	Beacon frame, SN=2175, FH=0, Flags=.....C, BI=100, SSID=0055
231	5.737657	HitronTe_ib:27:79	Broadcast	002.11	315	Beacon frame, SN=3043, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
232	5.739472	HitronTe_ib:27:79	Broadcast	002.11	233	Beacon frame, SN=3044, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
233	5.832995	HitronTe_ib:27:79	Broadcast	002.11	315	Beacon frame, SN=3045, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
234	5.841959	HitronTe_ib:27:79	Broadcast	002.11	233	Beacon frame, SN=3046, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
235	5.842522	HitronTe_ib:27:79	Broadcast	002.11	315	Beacon frame, SN=3047, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
236	5.944542	HitronTe_ib:27:79	Broadcast	002.11	233	Beacon frame, SN=3048, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
237	5.977822	Tp-LinkT_ei:f4:c	Broadcast	002.11	250	Beacon frame, SN=2176, FH=0, Flags=.....C, BI=100, SSID=0055
238	6.044920	HitronTe_ib:27:79	Broadcast	002.11	315	Beacon frame, SN=3049, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
239	6.046755	HitronTe_ib:27:79	Broadcast	002.11	233	Beacon frame, SN=3050, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
240	6.079395	Tp-LinkT_ei:f4:c	Broadcast	002.11	250	Beacon frame, SN=2179, FH=0, Flags=.....C, BI=100, SSID=0055
241	6.147380	HitronTe_ib:27:79	Broadcast	002.11	315	Beacon frame, SN=3051, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
242	6.149175	HitronTe_ib:27:79	Broadcast	002.11	233	Beacon frame, SN=3052, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
243	6.250840	HitronTe_ib:27:79	Broadcast	002.11	315	Beacon frame, SN=3053, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
244	6.251932	HitronTe_ib:27:79	Broadcast	002.11	233	Beacon frame, SN=3054, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET

```

> Frame 234: 233 bytes on wire (1864 bits), 233 bytes captured (1864 bits) on interface 0
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....C
  IEEE 802.11 wireless LAN
    Fixed parameters (12 bytes)
      Timestamp: 0x00000193da653b25
      Beacon Interval: 0.102400 (Seconds)
      Capabilities Information: 0x0421
    Tagged parameters (168 bytes)
      Tag: SSID parameter set: FON_ZON_FREE_INTERNET

```

Fig. 8: Um exemplo de um intervalo real entre duas tramas beacon do mesmo AP, igual a 0.102383 s.

### 3.5 Exercício 8

#### Questão

Identifique e registre todos os endereços MAC usados nas tramas beacon enviadas pelos APs. Recorde que o endereçamento está definido no cabeçalho das tramas 802.11, podendo ser utilizados até quatro endereços com diferente semântica. Para uma descrição detalhada da estrutura da trama 802.11, consulte o anexo ao enunciado.

#### Resposta

Para identificar os endereços MAC das tramas beacon dos AP's, é necessário apenas observar o campo BSS Id de cada. Regista-se então:

- ZON-2770 Source address: HitronTe\_1b:27:78 (bc:14:01:1b:27:78)
- FON\_ZON\_FREE\_INTERNET Source address: HitronTe\_1b:27:79 (bc:14:01:1b:27:79)
- DDSS Source address: Tp-LinkT\_ee:f4:ca (f8:1a:67:ee:f4:ca)

É de notar que, como se tratam de Management Frames, os campos Transmitter Address, Source Address e BSS Id coincidem.

#### Realização

No.	Time	Source	Destination	Protocol	Length	Info
231	5.737657	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3043, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
232	5.739472	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3044, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
233	5.839995	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3045, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
234	5.841959	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3046, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
235	5.942522	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3047, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
236	5.944342	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3048, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
237	5.977022	Tp-LinkT_ee:f4:ca	Broadcast	802.11	250	Beacon frame, SN=2178, FN=0, Flags=.....C, BI=100, SSID=DDSS
238	6.044920	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3049, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
239	6.046755	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3050, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
240	6.079395	Tp-LinkT_ee:f4:ca	Broadcast	802.11	250	Beacon frame, SN=2179, FN=0, Flags=.....C, BI=100, SSID=DDSS
241	6.147308	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3051, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
242	6.149175	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3052, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
243	6.250040	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3053, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
244	6.251932	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3054, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
245	6.352652	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3055, FN=0, Flags=.....C, BI=100, SSID=ZON-2770

> Frame 233: 315 bytes on wire (2520 bits), 315 bytes captured (2520 bits) on interface 0

> Radiotap Header v0, Length 25

> 802.11 radio information

> IEEE 802.11 Beacon frame, Flags: .....C

Type/Subtype: Beacon frame (0x0008)

> Frame Control Field: 0x8000

.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\_1b:27:78 (bc:14:01:1b:27:78)

Source address: HitronTe\_1b:27:78 (bc:14:01:1b:27:78)

BSS Id: HitronTe\_1b:27:78 (bc:14:01:1b:27:78)

Fig. 9: Exemplo do endereço MAC de um AP.

### 3.6 Exercício 9

#### Questão

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

#### Resposta

Os débitos base dos AP's são de 1, 2, 5.5 e 11 Mbps; Os *extended supported rates* dos AP's são de 6, 12, 24 e 48 Mbps.

#### Realização

No.	Time	Source	Destination	Protocol	Length	Info
231	5.737657	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3043, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
232	5.739472	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3044, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
233	5.839995	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3045, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
234	5.841959	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3046, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
235	5.942522	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3047, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
236	5.944342	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3048, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
237	5.977022	Tp-LinkT_ee:f4:ca	Broadcast	802.11	250	Beacon frame, SN=2178, FN=0, Flags=.....C, BI=100, SSID=DDSS
238	6.044920	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3049, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
239	6.046755	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3050, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
240	6.079395	Tp-LinkT_ee:f4:ca	Broadcast	802.11	250	Beacon frame, SN=2179, FN=0, Flags=.....C, BI=100, SSID=DDSS
241	6.147308	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3051, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
242	6.149175	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3052, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
243	6.250040	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3053, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
244	6.251932	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3054, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
245	6.352652	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3055, FN=0, Flags=.....C, BI=100, SSID=ZON-2770

0... .. = Immediate Block Ack: Not Implemented

Tagged parameters (250 bytes)

- Tag: SSID parameter set: ZON-2770
- Tag: Supported Rates 1(0), 2(0), 5.5(0), 11(0), 9, 18, 36, 54, [Mbit/sec]
- Tag: DS Parameter set: Current Channel: 11
- Tag: Extended Supported Rates 6, 12, 24, 48, [Mbit/sec]
- Tag: AP Channel Report: Operating Class 32, Channel List : 1, 2, 3, 4, 5, 6, 7,
- Tag: AP Channel Report: Operating Class 33, Channel List : 5, 6, 7, 8, 9, 10, 11,
- Tag: Vendor Specific: Microsoft: WPS
- Tag: Traffic Indication Map (TIM): DTIM 2 of 0 bitmap

Fig. 10: Exemplo dos débitos suportados por um AP.

### 3.7 Exercício 10

#### Questão

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

#### Resposta

Observando o campo Frame Control Field das tramas, conclui-se que as tramas probing request e probing response têm estes valores iguais a 4 e a 5, respectivamente. Assim, é possível aplicar o filtro `wlan.fc.type_subtype == 4 || wlan.fc.type_subtype == 5` para obter o resultado desejado.

#### Realização

No.	Time	Source	Destination	Protocol	Length	Info
25	0.887560	fb:dd:ca:50:5c:e1	4e:50:76:a2:9e:e2	802.11	437	Probe Response, SN=1982, FN=6, Flags=...PR.F..., BI=19364[Malformed Packet]
331	22.915081	92:60:ec:04:ef:e3	92:60:ec:04:ef:e3	802.11	445	Probe Response, SN=3650, FN=0, Flags=...pm.R...T
1191	35.434264	HonHaiPr_95:96:a0	Broadcast	802.11	78	Probe Request, SN=701, FN=0, Flags=.....C, SSID=DDSS
1195	35.458438	HonHaiPr_95:96:a0	Broadcast	802.11	78	Probe Request, SN=702, FN=0, Flags=.....C, SSID=DDSS
1200	35.565576	Tp-LinkT_ee:f4:ca	HonHaiPr_95:96:a0	802.11	411	Probe Response, SN=387, FN=0, Flags=.....C, BI=100, SSID=DDSS[Malformed Packet]
1207	35.590593	Tp-LinkT_ee:f4:ca	HonHaiPr_95:96:a0	802.11	411	Probe Response, SN=388, FN=0, Flags=...R...C, BI=100, SSID=DDSS[Malformed Packet]
1220	35.911182	Tp-LinkT_ee:f4:ca	HonHaiPr_95:96:a0	802.11	411	Probe Response, SN=389, FN=0, Flags=...R...C, BI=100, SSID=DDSS[Malformed Packet]
1251	36.721161	Tp-LinkT_ee:f4:ca	HonHaiPr_95:96:a0	802.11	411	Probe Response, SN=390, FN=0, Flags=...R...C, BI=100, SSID=DDSS[Malformed Packet]
1252	36.727882	Tp-LinkT_ee:f4:ca	HonHaiPr_95:96:a0	802.11	411	Probe Response, SN=390, FN=0, Flags=...R...C, BI=100, SSID=DDSS[Malformed Packet]
1253	36.745467	Tp-LinkT_ee:f4:ca	HonHaiPr_95:96:a0	802.11	411	Probe Response, SN=391, FN=0, Flags=...R...C, BI=100, SSID=DDSS[Malformed Packet]
1254	36.748743	Tp-LinkT_ee:f4:ca	HonHaiPr_95:96:a0	802.11	411	Probe Response, SN=391, FN=0, Flags=...R...C, BI=100, SSID=DDSS[Malformed Packet]
1267	37.175017	HonHaiPr_95:96:a0	Broadcast	802.11	78	Probe Request, SN=738, FN=0, Flags=.....C, SSID=DDSS
1273	37.377451	HonHaiPr_95:96:a0	Broadcast	802.11	78	Probe Request, SN=741, FN=0, Flags=.....C, SSID=DDSS
1275	37.393755	HonHaiPr_95:96:a0	Broadcast	802.11	78	Probe Request, SN=742, FN=0, Flags=.....C, SSID=DDSS
1732	51.360336	Tp-LinkT_ee:f4:ca	Azurewav_2b:78:7e	802.11	411	Probe Response, SN=2687, FN=0, Flags=...R...C, BI=100, SSID=DDSS[Malformed Packet]

Fig. 11: Timeline do Wireshark após a aplicação do filtro.

### 3.8 Exercício 11

#### Questão

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?

#### Resposta

Identificou-se uma trama Probe Request na trama nº 1903. Escolheu-se esta visto que é a primeira trama Probe Request enviada pelo STA Apple d1:fe:a8. As tramas Probe Response recebidas estão endereçadas aos AP's DDSS, ZON-2770 e FON\_ZON\_FREE\_INTERNET.

As tramas Probe Request são utilizadas quando a STA necessita de informações de uma outra estação ou quer determinar quais AP's estão em alcance.

As tramas Probe Response, como o nome indica, respondem às tramas Probe Request, enviando informação sobre as taxas de dados suportadas pelos AP's que as enviam, entre outras.

#### Realização

No.	Time	Source	Destination	Protocol	Length	Info
1254	36.748743	Tp-LinkT_ee:f4:ca	HonHaiPr_95:96:a0	802.11	411	Probe Response, SN=391, FN=0, Flags=...R...C, BI=100, SSID=DDSS[Malformed Packet]
1267	37.175017	HonHaiPr_95:96:a0	Broadcast	802.11	78	Probe Request, SN=738, FN=0, Flags=.....C, SSID=DDSS
1273	37.377451	HonHaiPr_95:96:a0	Broadcast	802.11	78	Probe Request, SN=741, FN=0, Flags=.....C, SSID=DDSS
1275	37.393755	HonHaiPr_95:96:a0	Broadcast	802.11	78	Probe Request, SN=742, FN=0, Flags=.....C, SSID=DDSS
1732	51.360336	Tp-LinkT_ee:f4:ca	Azurewav_2b:78:7e	802.11	411	Probe Response, SN=2687, FN=0, Flags=...R...C, BI=100, SSID=DDSS[Malformed Packet]
1903	56.174180	Apple_d1:fe:a8	Broadcast	802.11	142	Probe Request, SN=1124, FN=0, Flags=.....C, SSID=Broadcast
1904	56.177666	HitronTe_1b:27:78	Apple_d1:fe:a8	802.11	410	Probe Response, SN=3293, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
1906	56.181301	HitronTe_1b:27:78	Apple_d1:fe:a8	802.11	410	Probe Response, SN=3294, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
1908	56.184851	Tp-LinkT_ee:f4:ca	Apple_d1:fe:a8	802.11	411	Probe Response, SN=2738, FN=0, Flags=...R...C, BI=100, SSID=DDSS[Malformed Packet]
1910	56.188580	HitronTe_1b:27:78	Apple_d1:fe:a8	802.11	410	Probe Response, SN=3295, FN=0, Flags=.....C, BI=100, SSID=ZON-2770
1912	56.190740	HitronTe_1b:27:79	Apple_d1:fe:a8	802.11	210	Probe Response, SN=3296, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
1914	56.192770	HitronTe_1b:27:79	Apple_d1:fe:a8	802.11	210	Probe Response, SN=3297, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
1916	56.194750	HitronTe_1b:27:79	Apple_d1:fe:a8	802.11	210	Probe Response, SN=3298, FN=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
1918	56.196264	Apple_d1:fe:a8	Broadcast	802.11	142	Probe Request, SN=1125, FN=0, Flags=.....C, SSID=Broadcast
1919	56.199785	HitronTe_1b:27:78	Apple_d1:fe:a8	802.11	410	Probe Response, SN=3299, FN=0, Flags=.....C, BI=100, SSID=ZON-2770

Type/Subtype: Probe Request (0x0004)

Frame Control Field: 0x4000

- .....00 = Version: 0
  - .....00. = Type: Management frame (0)
  - 0100 .... = Subtype: 4
- > 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: Apple\_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
- Source address: Apple\_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
- BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
- .... .... 0000 = Fragment number: 0

Fig. 12: Uma trama Probe Request (a vermelho) e as respetivas tramas Probe Response (a verde).

## 4 Processo de Associação

### 4.1 Exercício 12

#### Questão

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

#### Resposta

Uma possível sequência de tramas que correspondem a um processo de associação completo são as identificadas pelos números 2027 (autenticação STA -> AP), 2029 (autenticação AP -> STA), 2031 (pedido de associação) e 2035 (resposta ao pedido de associação). Além destas é possível identificar tramas de confirmação de recepção (*Acknowledgment*) entre todas as tramas trocadas entre o STA e o AP.

#### Realização

2027	57.879941	Apple_d1:fe:a8	HitronTe_1b:27:78	802.11	70 Authentication, SN=1147, FN=0, Flags=.....C	16:20:55,012164
2028	57.879219		Apple_d1:fe:a8 (a4:d1:802.11	39 Acknowledgement, Flags=.....C	16:20:55,012342	
2029	57.879965	HitronTe_1b:27:78	Apple_d1:fe:a8	802.11	59 Authentication, SN=3308, FN=0, Flags=.....C	16:20:55,013088
2030	57.880197		HitronTe_1b:27:78 (bc:802.11	39 Acknowledgement, Flags=.....C	16:20:55,013320	
2031	57.881708	Apple_d1:fe:a8	HitronTe_1b:27:78	802.11	185 Association Request, SN=1148, FN=0, Flags=.....	16:20:55,014831
2032	57.882683		Apple_d1:fe:a8 (a4:d1:802.11	39 Acknowledgement, Flags=.....C	16:20:55,015206	
2033	57.887191	HitronTe_1b:27:78	Broadcast	802.11	315 Beacon frame, SN=4061, FN=0, Flags=.....C, BI	16:20:55,020314
2034	57.888974	HitronTe_1b:27:79	Broadcast	802.11	233 Beacon frame, SN=4062, FN=0, Flags=.....C, BI	16:20:55,022097
2035	57.890902	HitronTe_1b:27:78	Apple_d1:fe:a8	802.11	225 Association Response, SN=3309, FN=0, Flags=.....	16:20:55,024025
2036	57.891033		HitronTe_1b:27:78 (bc:802.11	39 Acknowledgement, Flags=.....C	16:20:55,024156	

Fig. 13: Sequência de tramas trocadas no processo de associação.

## 4.2 Exercício 13

### Questão

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

### Resposta

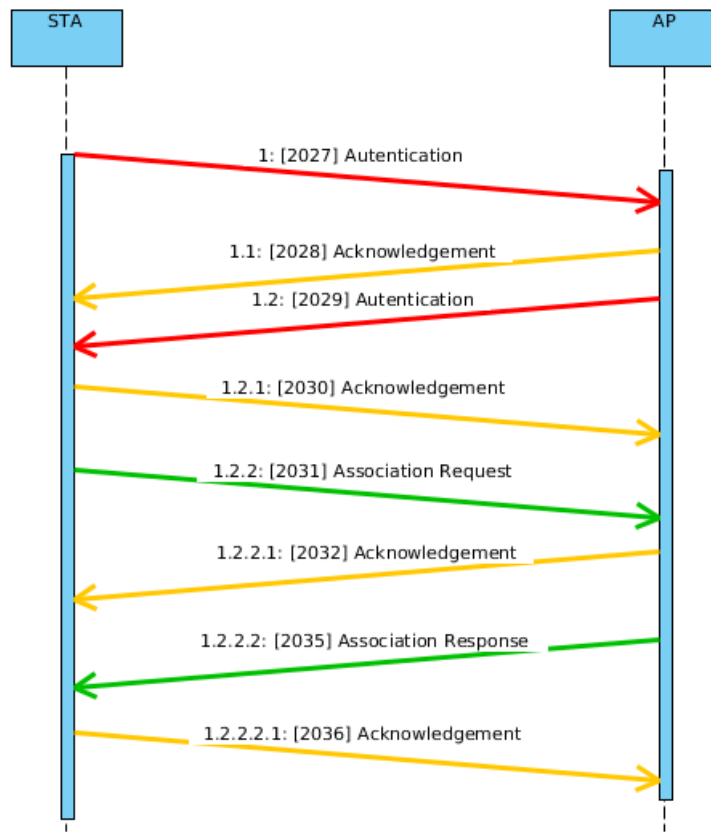


Fig. 14: Diagrama da sequência de tramas trocadas no processo de associação, realizado no *Visual Paradigm*.

## 5 Transferência de Dados

### 5.1 Exercício 14

#### Questão

Considere a trama de dados nº1054. 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?

#### Resposta

O campo Frame Control transporta diversos dados associados ao controlo, especificando a Protocol Version, Type e Subtype. Para além destas informações, tem ainda diversas flags, entre as quais é possível encontrar a *To AP* e a *From AP*. Pela análise destas últimas, é possível perceber a direccionalidade da trama. Depois de observado o Frame Control da trama de dados nº. 1054, verificou-se que:

- To DS: 1
- From DS: 0

Com isto, conclui-se que a direccionalidade é para o *Distributed System*, ou seja, a infraestrutura que liga os múltiplos *APs*, logo a trama não é local à WLAN.

#### Realização

```
> Frame 1054 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0
> Radiotap Header v0, Length 40
> 802.11 radio information
  IEEE 802.11 QoS Data, Flags: .p....TC
    Type/Subtype: QoS Data (0x0028)
    Frame Control Field: 0x8841
      ....00 = Version: 0
      ....10.. = Type: Data frame (2)
      1000.... = Subtype: 8
    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
      .000 0000 0010 1100 = Duration: 44 microseconds
```

Fig. 15: Informações de controlo da trama 1054.



## 5.2 Exercício 15

### Questão

Para a trama de dados nº1054, 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?

### Resposta

Como os campos *To AP* e *From AP* são 1 e 0, respetivamente, então:

- **BSS Id:** corresponde ao AP
- **STA address:** corresponde ao *host*

Assim sendo, pode-se afirmar que os endereços *MAC* são:

- **STA:** a4:d1:d2:d1:fe:a8
- **AP:** bc:14:01:1b:27:78
- **Router:** bc:14:01:1b:27:76

### Realização

```
Receiver address: HitronTe_1b:27:78 (bc:14:01:1b:27:78)
Destination address: HitronTe_1b:27:76 (bc:14:01:1b:27:76)
Transmitter address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
Source address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
BSS Id: HitronTe_1b:27:78 (bc:14:01:1b:27:78)
STA address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
```

Fig. 16: Endereços envolvidos na trama 1054.

### 5.3 Exercício 16

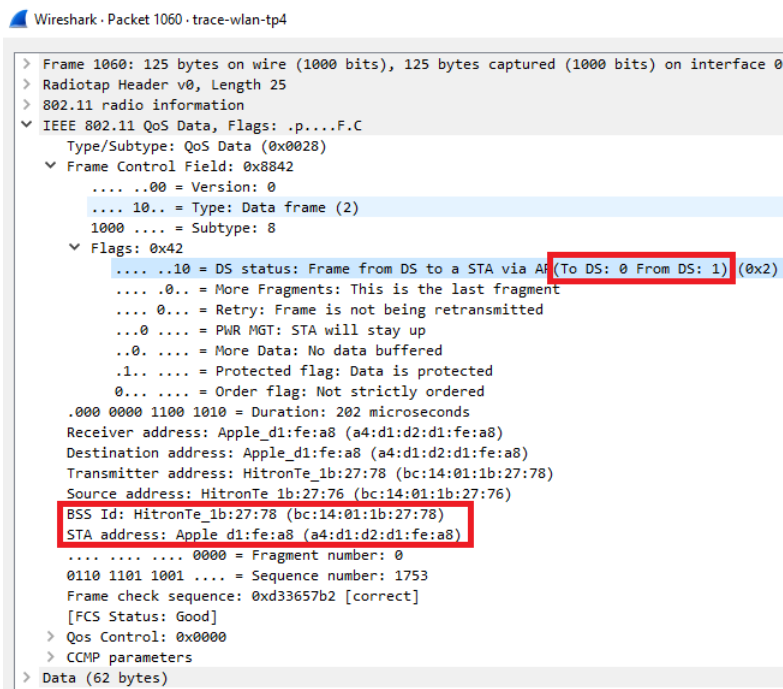
#### Questão

Como interpreta a trama nº1060 face à sua direccionalidade e endereçamento MAC?

#### Resposta

O campo *To AP* e *From AP* é 0 e 1, respetivamente, estando por isso a trama a ser transmitida pela *edge* do sistema distribuído, no caso o AP com *MAC Address bc:14:01:1b:27:76*, como se pode verificar pelo campo *BSS Id*. Este AP envia a trama para a o dispositivo cujo *MAC Address* é *a4:d1:d2:d1:fe:a8*, visível no campo *STA Address*. É, por isso, uma comunicação do sistema distribuído para a WLAN local.

#### Realização



```
Wireshark · Packet 1060 · trace-wlan-tp4

> Frame 1060: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface 0
> 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: 0x8842
      ....0000 = 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 1100 1010 = Duration: 202 microseconds
      Receiver address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
      Destination address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
      Transmitter address: HitronTe_1b:27:78 (bc:14:01:1b:27:78)
      Source address: HitronTe_1b:27:76 (bc:14:01:1b:27:76)
      BSS Id: HitronTe_1b:27:78 (bc:14:01:1b:27:78)
      STA address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
      ....0000 = Fragment number: 0
      0110 1101 1001 .... = Sequence number: 1753
      Frame check sequence: 0xd33657b2 [correct]
      [FCS Status: Good]
    > Qos Control: 0x0000
    > CCHP parameters
  > Data (62 bytes)
```

Fig. 17: Direcionamento da trama 1054.

## 5.4 Exercício 17

### Questão

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.)

### Resposta

Vai-se proceder à análise da troca de dados, desde a *frame* 1050 até à 1060. Em 1050, é transmitido um *Beacon Frame*, anunciando a existência daquele *AP* aos *STA* ao seu alcance. Então, o *STA* com MAC **a4:d1:d2:d1:fe:a8** envia um *request-to-send* ao *AP*, ficando a trama ao nível da *WLAN* local. Recebido o sinal *clear-to-send*, é iniciada a troca de dados. Uma das tramas de maior importância é a 1059, em que é enviado um bloco **ACK**, que permite a verificação de erros e transmissão de dados. De facto, devido às características das redes *Wireless*, como o meio de transmissão partilhado, é necessário um maior controlo de dados do que o na *Ethernet*, bem como estratégias de prevenção de colisões (implementadas, por exemplo, através de RTS-CTS).

### Realização

1050	31.043920	HitronTe_1b:27:78	Broadcast	802.11	315 Beacon frame, SN=3537, FN=0, Flags=.....
1051	31.045753	HitronTe_1b:27:79	Broadcast	802.11	233 Beacon frame, SN=3538, FN=0, Flags=.....
1052	31.139152	Apple_d1:fe:a8 (a4:...	HitronTe_1b:27:78 (...)	802.11	45 Request-to-send, Flags=.....C
1053	31.139166	Apple_d1:fe:a8 (a4:...	Apple_d1:fe:a8 (a4:...	802.11	39 Clear-to-send, Flags=.....C
1054	31.139171	Apple_d1:fe:a8	HitronTe_1b:27:76	802.11	122 QoS Data, SN=4006, FN=0, Flags=.p....TC
1055	31.139280	HitronTe_1b:27:78 (...)	Apple_d1:fe:a8 (a4:...	802.11	57 802.11 Block Ack, Flags=.....C
1056	31.139774	HitronTe_1b:27:78 (...)	Apple_d1:fe:a8 (a4:...	802.11	49 802.11 Block Ack Req, Flags=.....C
1057	31.140244	Apple_d1:fe:a8 (a4:...	HitronTe_1b:27:78 (...)	802.11	57 802.11 Block Ack, Flags=.....C
1058	31.140255	Apple_d1:fe:a8	HitronTe_1b:27:78	802.11	68 Null function (No data), SN=1106, FN=0, Fl:
1059	31.140315	Apple_d1:fe:a8 (a4:...	Apple_d1:fe:a8 (a4:...	802.11	39 Acknowledgement, Flags=.....C
1060	31.141446	HitronTe_1b:27:76	Apple_d1:fe:a8	802.11	125 QoS Data, SN=1753, FN=0, Flags=.p....F.C

Fig. 18: Informação sobre tramas 1050 a 1060.

1050	31.043920	HitronTe_1b:27:78	Broadcast	802.11	315 Beacon frame, SN=3537, FN=0, Flags=..
1051	31.045753	HitronTe_1b:27:79	Broadcast	802.11	233 Beacon frame, SN=3538, FN=0, Flags=..
1052	31.139152	Apple_d1:fe:a8 (a4:...	HitronTe_1b:27:78 (...	802.11	45 Request-to-send, Flags=.....C
1053	31.139166	Apple_d1:fe:a8 (a4:...	HitronTe_1b:27:76	802.11	39 Clear-to-send, Flags=.....C
1054	31.139171	Apple_d1:fe:a8	HitronTe_1b:27:78	802.11	122 QoS Data, SN=4006, FN=0, Flags=p....
1055	31.139280	HitronTe_1b:27:78 (...	Apple_d1:fe:a8 (a4:...	802.11	57 802.11 Block Ack, Flags=.....C
1056	31.139774	HitronTe_1b:27:78 (...	Apple_d1:fe:a8 (a4:...	802.11	49 802.11 Block Ack Req, Flags=.....C
1057	31.140244	Apple_d1:fe:a8 (a4:...	HitronTe_1b:27:78 (...	802.11	57 802.11 Block Ack, Flags=.....C
1058	31.140255	Apple_d1:fe:a8	HitronTe_1b:27:78	802.11	68 Null function (No data), SN=1106, FN=
1059	31.140315	Apple_d1:fe:a8 (a4:...	HitronTe_1b:27:78	802.11	39 Acknowledgement, Flags=.....C
1060	31.141446	HitronTe_1b:27:76	Apple_d1:fe:a8	802.11	125 QoS Data, SN=1753, FN=0, Flags=p....
1061	31.146301	HitronTe_1b:27:78	Broadcast	802.11	315 Beacon frame, SN=3539, FN=0, Flags=..

```

> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Request-to-send, Flags: .....C
  Type/Subtype: Request-to-send (0x001b)
  > Frame Control Field: 0xb400
    .... 00 = Version: 0
    .... 01.. = Type: Control frame (1)
    1011 .... = Subtype: 11
    > 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 0101 0110 = Duration: 86 microseconds
      Receiver address: HitronTe_1b:27:78 (bc:14:01:1b:27:78)
      Transmitter address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)

```

Fig. 19: Envio de *RTS* na trama 1052.

1050	31.043920	HitronTe_1b:27:78	Broadcast	802.11	315 Beacon frame, SN=3537, FN=0, Flags=.....
1051	31.045753	HitronTe_1b:27:79	Broadcast	802.11	233 Beacon frame, SN=3538, FN=0, Flags=.....
1052	31.139152	Apple_d1:fe:a8 (a4:...	HitronTe_1b:27:78 (...	802.11	45 Request-to-send, Flags=.....C
1053	31.139166	Apple_d1:fe:a8 (a4:...	HitronTe_1b:27:76	802.11	39 Clear-to-send, Flags=.....C
1054	31.139171	Apple_d1:fe:a8	HitronTe_1b:27:78	802.11	122 QoS Data, SN=4006, FN=0, Flags=p....TC
1055	31.139280	HitronTe_1b:27:78 (...	Apple_d1:fe:a8 (a4:...	802.11	57 802.11 Block Ack, Flags=.....C
1056	31.139774	HitronTe_1b:27:78 (...	Apple_d1:fe:a8 (a4:...	802.11	49 802.11 Block Ack Req, Flags=.....C
1057	31.140244	Apple_d1:fe:a8 (a4:...	HitronTe_1b:27:78 (...	802.11	57 802.11 Block Ack, Flags=.....C
1058	31.140255	Apple_d1:fe:a8	HitronTe_1b:27:78	802.11	68 Null function (No data), SN=1106, FN=0, I
1059	31.140315	Apple_d1:fe:a8 (a4:...	HitronTe_1b:27:78	802.11	39 Acknowledgement, Flags=.....C
1060	31.141446	HitronTe_1b:27:76	Apple_d1:fe:a8	802.11	125 QoS Data, SN=1753, FN=0, Flags=p....F.C
1061	31.146301	HitronTe_1b:27:78	Broadcast	802.11	315 Beacon frame, SN=3539, FN=0, Flags=.....

```

> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Clear-to-send, Flags: .....C
  Type/Subtype: Clear-to-send (0x001c)
  > Frame Control Field: 0xc400
    .... 00 = Version: 0
    .... 01.. = Type: Control frame (1)
    1100 .... = Subtype: 12
    > 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 0010 1010 = Duration: 42 microseconds
      Receiver address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
      Frame check sequence: 0x9e5474de [correct]

```

Fig. 20: Envio de *CTS* no trama 1053.

## 5.5 Exercício 18

### Questão

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.

### Resposta

O STA com MAC **a4:d1:d2:d1:fe:a8** envia um *request-to-send* ao AP com MAC **bc:14:01:1b:27:78**. Este tipo de pedidos é opcional, sendo mais utilizado quando os dados que serão enviados de seguida são de tamanho considerável. De facto, na situação em análise, devido ao estabelecer de comunicação, são transmitidos muitos dados.

### Realização

1050	31.043920	HitronTe_1b:27:78	Broadcast	802.11	315 Beacon frame, SN=3537, FN=0, Flags=.....
1051	31.045753	HitronTe_1b:27:79	Broadcast	802.11	233 Beacon frame, SN=3538, FN=0, Flags=.....
1052	31.139152	Apple_d1:fe:a8 (a4:...	HitronTe_1b:27:78 (...)	802.11	45 Request-to-send, Flags=.....C
1053	31.139166	Apple_d1:fe:a8 (a4:...	Apple_d1:fe:a8 (a4:...	802.11	39 Clear-to-send, Flags=.....C
1054	31.139171	Apple_d1:fe:a8	HitronTe_1b:27:76	802.11	122 QoS Data, SN=4006, FN=0, Flags=p....TC
1055	31.139280	HitronTe_1b:27:78 (...)	Apple_d1:fe:a8 (a4:...	802.11	57 802.11 Block Ack, Flags=.....C
1056	31.139774	HitronTe_1b:27:78 (...)	Apple_d1:fe:a8 (a4:...	802.11	49 802.11 Block Ack Req, Flags=.....C
1057	31.140244	Apple_d1:fe:a8 (a4:...	HitronTe_1b:27:78 (...)	802.11	57 802.11 Block Ack, Flags=.....C
1058	31.140255	Apple_d1:fe:a8	HitronTe_1b:27:78	802.11	68 Null function (No data), SN=1106, FN=0, Fl:
1059	31.140315		Apple_d1:fe:a8 (a4:...	802.11	39 Acknowledgement, Flags=.....C
1060	31.141446	HitronTe_1b:27:76	Apple_d1:fe:a8	802.11	125 QoS Data, SN=1753, FN=0, Flags=p....F.C

Fig. 21: RTS-CTS e posterior troca de dados.

## 6 Conclusões

Neste trabalho exploraram-se diversas particularidades do protocolo 802.11. Estando num contexto de redes sem fios, o formato de tramas e protocolos de controlo implementados são visivelmente mais complexos quando comparados com os das tramas *Ethernet*.

Adquiriu-se compreensão acerca de *Beacons* e a sua utilização nos sistemas, bem como a relação estabelecida entre os *STA* e os *AP*.

Aumentou o conhecimento sobre os métodos de deteção de erros e controlo de envio de dados, pelo estudo de *RTS-CTS*.

O estudo do *probing* tornou mais evidente a necessidade deste tipo de comunicação, permitindo uma consolidação de conhecimentos.

De facto, nas redes *Wireless* em particular, existe um enorme e necessário *overhead*, pelo facto do meio de comunicação usado (ar) ser concorrente e dinâmico, o que tornou relevante o estudo destas características.

## References

1. James F. Kurose, K.W.R.: Computer Networking: A Top Down Approach. (Addison-Wesley)
2. Wikipedia: Bit error rate. [https://en.wikipedia.org/wiki/Bit\\_error\\_rate](https://en.wikipedia.org/wiki/Bit_error_rate) (2017) [Online; acedido a 10-Dezembro-2017].
3. Wikipedia: Relação sinal-ruído. [https://pt.wikipedia.org/wiki/Rela%C3%A7%C3%A3o\\_sinal-ru%C3%ADdo](https://pt.wikipedia.org/wiki/Rela%C3%A7%C3%A3o_sinal-ru%C3%ADdo) (2017) [Online; acedido a 10-Dezembro-2017].