



Universidade do Minho  
Escola de Engenharia

## **Licenciatura em Engenharia Informática**

### **Trabalho Prático 4** **Redes de Computadores**

Ano Letivo de 2022/2023  
a100838, Jorge Teixeira  
a100066, Ricardo Jesus  
a100659, Rui Pinto  
Braga, maio de 2023

# Índice

<b>1</b>	<b>Introdução</b>	<b>2</b>
<b>2</b>	<b>Resolução das Questões</b>	<b>3</b>
2.1	Acesso Rádio . . . . .	3
2.2	Scanning Passivo e Scanning Ativo . . . . .	6
2.3	Processo de Associação . . . . .	12
2.4	Transferência de Dados . . . . .	13
<b>3</b>	<b>Conclusão</b>	<b>17</b>

## Lista de Figuras

2.1	Print Geral - Acesso Rádio. . . . .	3
2.2	Frequência do espectro. . . . .	3
2.3	Versão da norma IEEE 802.11 . . . . .	4
2.4	Débito de informação . . . . .	4
2.5	Signal Strenght . . . . .	5
2.6	Visão geral - Scanning passivo e ativo . . . . .	6
2.7	Características da trama beacon . . . . .	6
2.8	Endereços MAC . . . . .	7
2.9	Método de detecção de erro . . . . .	7
2.10	Os vários débitos de base de uma trama beacon . . . . .	8
2.11	Intervalos de tempo entre tramas beacon . . . . .	9
2.12	SSID's de AP's da vizinhança da STA . . . . .	10
2.13	STA request . . . . .	11
2.14	STA response . . . . .	11
2.15	Processo de associação entre STA e AP . . . . .	12
2.16	Diagrama das trocas de tramas . . . . .	12
2.17	Direcionalidade das tramas . . . . .	13
2.18	Endereços MAC da STA, AP e router de acesso ao DS . . . . .	13
2.19	Direcionalidade e endereçamento MAC . . . . .	14
2.20	Subtipos de tramas de controlo . . . . .	14
2.21	Trama com RTS/CTS . . . . .	15
2.22	Trama sem RTS/CTS . . . . .	16

# **1 Introdução**

Neste trabalho prático iremos abordar e explorar várias características do protocolo de comunicação de redes sem fios - o IEEE 802.11. Alguns dos aspetos abordados deste protocolo são, por exemplo, o formato e diferentes tipos das tramas, o endereçamento dos componentes envolvidos na comunicação sem fios bem como a operação do protocolo em si.

A trama escolhida pelo grupo foi a trama 10 (identificativa do nº do grupo).

## 2 Resolução das Questões

### 2.1 Acesso Rádio

1 0.000000	PTInovac_d6:88:50 (- ce:90:6f:21:42:3a (- 802.11	68 802.11 Block Ack, Flags=.....C
2 0.000011	PTInovac_d6:88:50 (- ce:90:6f:21:42:3a (- 802.11	68 802.11 Block Ack, Flags=.....C
3 0.005857	PTInovac_d6:88:50 Broadcast	802.11 329 Beacon frame, SN=696, FN=0, Flags=.....C, BI=100, SSID="MEO-D68850"
4 0.008710	PTInovac_d6:88:52 Broadcast	802.11 254 Beacon frame, SN=697, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
5 0.011922	PTInovac_45:be:32 Broadcast	802.11 254 Beacon frame, SN=2358, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
6 0.028491	PTInovac_9e:9b:b2 Broadcast	802.11 254 Beacon frame, SN=2403, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
7 0.037432	PTInovac_d6:88:50 (- ce:90:6f:21:42:3a (- 802.11	76 Request-to-send, Flags=.....C
8 0.050713	HitronTe_ee:2e:c6 Broadcast	802.11 385 Beacon frame, SN=1928, FN=0, Flags=.....C, BI=100, SSID="MOS-2EC6"
9 0.053270	HitronTe_e7:c8:76 Broadcast	802.11 453 Beacon frame, SN=1763, FN=0, Flags=.....C, BI=100, SSID="MOS-C876"
10 0.062174	Alticela_fc:f0:a0 Broadcast	802.11 329 Beacon frame, SN=3598, FN=0, Flags=.....C, BI=100, SSID="MEO-FCF0A0"
11 0.062181	Alticela_fc:f0:a2 Broadcast	802.11 254 Beacon frame, SN=3599, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
12 0.087642	HitronTe_f3:9a:46 Broadcast	802.11 386 Beacon frame, SN=956, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
13 0.104619	LGINnote_89:76:d2 HitronTe_ee:2e:c6	802.11 64 Null function (No data), SN=804, FN=0, Flags=.....TC
14 0.104627	LGINnote_89:76:d2 (- 802.11	48 Acknowledgement, Flags=.....C
15 0.110775	PTInovac_d6:88:50 Broadcast	802.11 329 Beacon frame, SN=698, FN=0, Flags=.....C, BI=100, SSID="MEO-D68850"
16 0.110784	PTInovac_d6:88:52 Broadcast	802.11 254 Beacon frame, SN=699, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"

> Frame 10: 329 bytes on wire (2632 bits), 329 bytes captured (2632 bits) on interface en0, id 0

> Radiotap Header v0, Length 60

▼ 802.11 radio information

PHY type: 802.11n (HT) (7)

MCS index: 0

Bandwidth: 20 MHz (0)

Short GI: False

Greenfield: False

FEC: BEC (0)

Data rate: 6.5 Mb/s

Channel: 1

Frequency: 2412MHz

Signal strength (dBm): -90 dBm

Noise level (dBm): -93 dBm

Signal/noise ratio (dB): 3 dB

TSF timestamp: 108071

.....1 = Last part of an A-MPDU: True

.....0 = A-MPDU delimiter CRC error: False

A-MPDU aggregate ID: 0

[Duration: 372µs]

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

> IEEE 802.11 Wireless Management

Figura 2.1: Print Geral - Acesso Rádio.

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

**R:** Assim como podemos ver assinalado na figura o canal e a frequência do espetro correspondente são, respetivamente, 1 e 2412MHz.

No.	Time	Source	Destination	Protocol	Length	Info
1 0.000000		PTInovac_d6:88:50 (- ce:90:6f:21:42:3a (- 802.11		68 802.11 Block Ack, Flags=.....C		
2 0.000011		PTInovac_d6:88:50 (- ce:90:6f:21:42:3a (- 802.11		68 802.11 Block Ack, Flags=.....C		
3 0.005857		PTInovac_d6:88:50 Broadcast		802.11 329 Beacon frame, SN=696, FN=0, Flags=.....C, BI=100, SSID="MEO-D68850"		
4 0.008710		PTInovac_d6:88:52 Broadcast		802.11 254 Beacon frame, SN=697, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"		
5 0.011922		PTInovac_45:be:32 Broadcast		802.11 254 Beacon frame, SN=2358, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"		
6 0.028491		PTInovac_9e:9b:b2 Broadcast		802.11 254 Beacon frame, SN=2403, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"		
7 0.037432		PTInovac_d6:88:50 (- ce:90:6f:21:42:3a (- 802.11		76 Request-to-send, Flags=.....C		
8 0.050713		HitronTe_ee:2e:c6 Broadcast		802.11 385 Beacon frame, SN=1928, FN=0, Flags=.....C, BI=100, SSID="MOS-2EC6"		
9 0.053270		HitronTe_e7:c8:76 Broadcast		802.11 453 Beacon frame, SN=1763, FN=0, Flags=.....C, BI=100, SSID="MOS-C876"		
10 0.062174		Alticela_fc:f0:a0 Broadcast		802.11 329 Beacon frame, SN=3598, FN=0, Flags=.....C, BI=100, SSID="MEO-FCF0A0"		
11 0.062181		Alticela_fc:f0:a2 Broadcast		802.11 254 Beacon frame, SN=3599, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"		
12 0.087642		HitronTe_f3:9a:46 Broadcast		802.11 386 Beacon frame, SN=956, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"		
13 0.104619		LGINnote_89:76:d2 HitronTe_ee:2e:c6		802.11 64 Null function (No data), SN=804, FN=0, Flags=.....TC		
14 0.104627		LGINnote_89:76:d2 (- 802.11		48 Acknowledgement, Flags=.....C		
15 0.110775		PTInovac_d6:88:50 Broadcast		802.11 329 Beacon frame, SN=698, FN=0, Flags=.....C, BI=100, SSID="MEO-D68850"		
16 0.110784		PTInovac_d6:88:52 Broadcast		802.11 254 Beacon frame, SN=699, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"		

> Frame 10: 329 bytes on wire (2632 bits), 329 bytes captured (2632 bits) on interface en0, id 0

> Radiotap Header v0, Length 60

▼ 802.11 radio information

PHY type: 802.11n (HT) (7)

MCS index: 0

Bandwidth: 20 MHz (0)

Short GI: False

Greenfield: False

FEC: BEC (0)

Data rate: 6.5 Mb/s

Channel: 1

Frequency: 2412MHz

Signal strength (dBm): -90 dBm

Noise level (dBm): -93 dBm

Signal/noise ratio (dB): 3 dB

TSF timestamp: 108071

.....1 = Last part of an A-MPDU: True

.....0 = A-MPDU delimiter CRC error: False

A-MPDU aggregate ID: 0

[Duration: 372µs]

Figura 2.2: Frequência do espetro.

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

**R:** A versão da norma IEEE é a 802.11n.

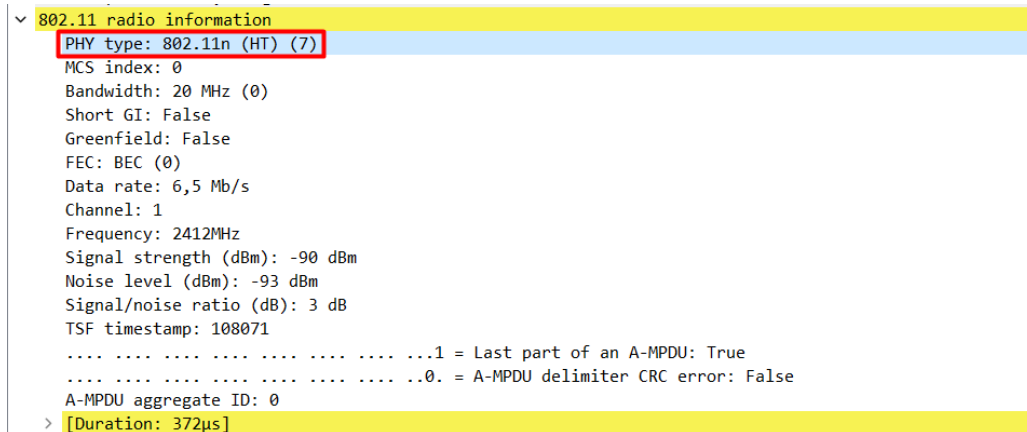


Figura 2.3: Versão da norma IEEE 802.11

### 2.1.3 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.

**R:** A trama foi enviada a 6,5 Mb/s, contudo este valor é inferior ao valor máximo de débito, teorico, imposto pelo protocolo IEEE 802.11n, correspondente a 450 Mbps.

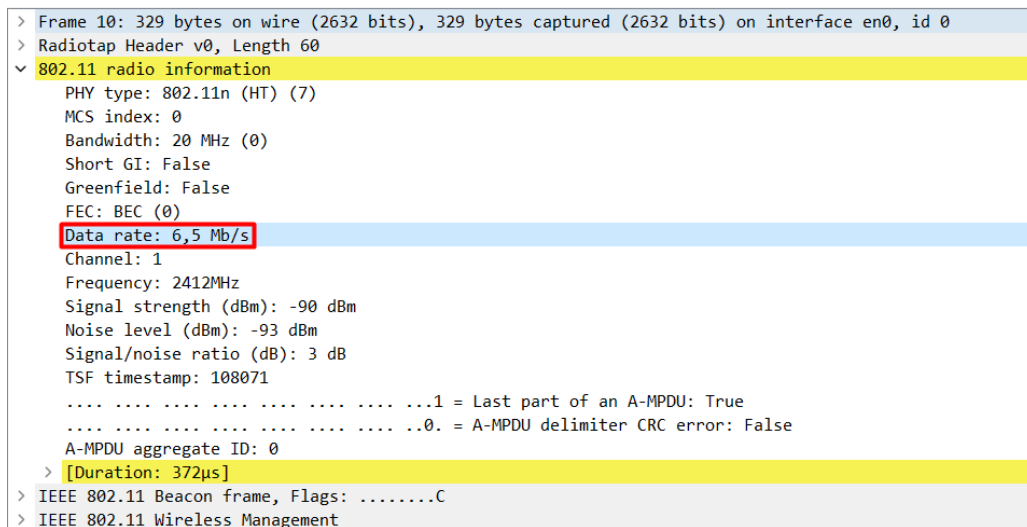


Figura 2.4: Débito de informação

#### 2.1.4 Verifique qual a força do sinal (Signal strength) e a qualidade expectável de receção da trama.

**R:** Sabendo as correspondências de qualidade esperada para cada força de sinal temos que as hipóteses de acontecer uma conexão são muito baixas para o nível demonstrado (-90 dBm)

```
> Frame 10: 329 bytes on wire (2632 bits), 329 bytes captured (2632 bits) on interface en0, id 0
> Radiotap Header v0, Length 60
  802.11 radio information
    PHY type: 802.11n (HT) (7)
    MCS index: 0
    Bandwidth: 20 MHz (0)
    Short GI: False
    Greenfield: False
    FEC: BEC (0)
    Data rate: 6,5 Mb/s
    Channel: 1
    Frequency: 2412MHz
    Signal strength (dBm): -90 dBm
    Noise level (dBm): -93 dBm
    Signal/noise ratio (dB): 3 dB
    TSF timestamp: 108071
    .... = Last part of an A-MPDU: True
    .... = A-MPDU delimiter CRC error: False
    A-MPDU aggregate ID: 0
  [Duration: 372µs]
> IEEE 802.11 Beacon frame, Flags: .....C
> IEEE 802.11 Wireless Management
```

Figura 2.5: Signal Strenght

## 2.2 Scanning Passivo e Scanning Ativo

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	PTInovac_d6:88:50	(. ce:90:6f:21:42:3a (. 802.11	68	802.11 Block Ack, Flags=.....C	
2	0.000011	PTInovac_d6:88:50	(. ce:90:6f:21:42:3a (. 802.11	68	802.11 Block Ack, Flags=.....C	
3	0.000857	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=696, FN=0, Flags=.....C, BI=100, SSID="MEO-D68850"
4	0.008710	PTInovac_d6:88:50	Broadcast	802.11	254	Beacon frame, SN=697, FN=0, Flags=.....C, BI=100, SSID="MEO-WIFI"
5	0.011922	PTInovac_d5:be:32	Broadcast	802.11	254	Beacon frame, SN=2358, FN=0, Flags=.....C, BI=100, SSID="MEO-WIFI"
6	0.028491	PTInovac_3e:9b:b2	Broadcast	802.11	254	Beacon frame, SN=2403, FN=0, Flags=.....C, BI=100, SSID="MEO-WIFI"
7	0.037432	PTInovac_d6:88:50	(. ce:90:6f:21:42:3a (. 802.11	76	Request-to-send, Flags=.....C	
8	0.050713	HitronTe_ee:2e:c6	Broadcast	802.11	385	Beacon frame, SN=1928, FN=0, Flags=.....C, BI=100, SSID="MOS-2EC6"
9	0.053270	HitronTe_e7:c8:76	Broadcast	802.11	453	Beacon frame, SN=1763, FN=0, Flags=.....C, BI=100, SSID="MOS-C876"
10	0.062174	AlticeLa_fc:f0:a0	Broadcast	802.11	329	Beacon frame, SN=3598, FN=0, Flags=.....C, BI=100, SSID="MEO-FCF0A0"
11	0.062181	AlticeLa_fc:f0:a2	Broadcast	802.11	254	Beacon frame, SN=3599, FN=0, Flags=.....C, BI=100, SSID="MEO-WIFI"
12	0.007642	HitronTe_f3:9a:46	Broadcast	802.11	385	Beacon frame, SN=956, FN=0, Flags=.....C, BI=100, SSID="Flyinglet"
13	0.104619	LGInnote_89:76:d2	HitronTe_ee:2e:c6	802.11	64	Null function (No data), SN=804, FN=0, Flags=.....C
14	0.104627	LGInnote_89:76:d2	(. 802.11	48	Acknowledgement, Flags=.....C	
15	0.110775	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=698, FN=0, Flags=.....C, BI=100, SSID="MEO-D68850"
16	0.110784	PTInovac_d6:88:50	Broadcast	802.11	254	Beacon frame, SN=699, FN=0, Flags=.....C, BI=100, SSID="MEO-WIFI"

> Frame 10: 329 bytes on wire (2632 bits), 329 bytes captured (2632 bits) on interface en0, id 0	0000	00 00 3c 00 00 00 1c 40	27 a6 01 00 00 00 00 00	..c.k-@ .....
> Radiotap Header v0, Length 60	0010	10 a0 6c 09 80 04 a6 a3	00 01 00 00 80 04 01 00	..1.....C.....
> 802.11 radio information	0020	6c 09 01 22 1f 00 00 43	00 00 00 00 00 00 84 00	1.....C.....h..d.....
> IEEE 802.11 Beacon frame, Flags: .....C	0030	00 10 18 03 06 00 03 01	68 08 cc 64 80 00 00 00	.....W>.....
Type/Subtype: Beacon frame (0x0008)	0040	ff ff ff ff ff ff 1c 57	3e fc f0 a0 1c 57 3e fc f0	.....M>.....
Frame Control Field: 0x0000	0050	f0 a0 e0 e0 8c d1 10 c7	f6 01 00 00 64 00 11 14	.....d.....
.000 0000 0000 0000 = Duration: 0 microseconds	0060	00 0a 4d 45 4f 2d 46 43	46 30 41 30 01 08 82 84	.....MEO-FC F0A0.....
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)	0070	8b 96 24 30 48 6c 03 01	01 05 04 00 01 00 00 2a	.....\$H1.....*
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)	0080	01 00 32 04 0c 12 18 60	30 14 01 00 00 0f ac 04	.....2.....0.....
Transmitter address: AlticeLa_fc:f0:a0 (1c:57:3e:fc:f0:a0)	0090	01 00 00 0f ac 04 01 00	00 0f ac 02 0c 00 0b 05	.....2.....0.....
Source address: AlticeLa_fc:f0:a0 (1c:57:3e:fc:f0:a0)	00a0	00 00 3f 00 00 42 01 00	46 05 00 00 32 00 2d 00	.....2.....B.....F.....2.....
BSS Id: AlticeLa_fc:f0:a0 (1c:57:3e:fc:f0:a0)	00b0	1a ad 08 17 ff ff ff 00	00 00 00 00 00 00 00 00	.....2.....B.....F.....2.....
..... 0000 = Fragment number: 0	00c0	00 00 00 00 00 00 00 00	00 00 00 3d 16 01 08 00	.....=.....
1110 0000 1110 .... = Sequence number: 3598	00d0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....=.....
Frame check sequence: 0xe2cf9658 [unverified]	00e0	00 00 00 7f 08 04 00 08	00 00 00 00 40 dd 31 00	.....@.1.....
[FCS Status: Unverified]	00f0	50 f2 04 10 4a 00 01 10	10 44 00 01 02 10 47 00	P.....D.....G.....
> IEEE 802.11 Wireless Management	0100	10 5b ed 90 b5 3b 61 0f	fa 63 e9 2a ae 1f 83 b4	[.....a.....c.....*
	0110	44 10 3c 00 01 03 10 49	00 06 00 37 2a 00 01 20	D.....I.....7P.....
	0120	dd 00 10 18 02 00 00 00	1c 00 00 dd 18 00 50 f2	D.....I.....7P.....
	0130	02 01 01 84 00 03 a4 00	00 27 a4 00 00 42 43 5e	.....I.....7P.....
	0140	00 62 32 2f 00 58 96 cf	e2	b2/X.....BC^

Figura 2.6: Visão geral - Scanning passivo e ativo

**2.2.1 Selecione uma trama beacon cuja ordem (ou terminação) corresponda a XX. Esta trama pertence a que tipo de tramas 802.11? Identifique o valor dos identificadores de tipo e de subtipo da trama. Em que parte concreta do cabeçalho da trama estão especificados?**

**R:** Analisando detalhadamente a trama, nos campos do cabeçalho do protocolo vemos que se trata de uma trama de gestão ("Management frame") e o valor do subtipo desta é de 8.

> Frame 10: 329 bytes on wire (2632 bits), 329 bytes captured (2632 bits) on interface en0, id 0
> Radiotap Header v0, Length 60
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....C
Type/Subtype: Beacon frame (0x0008)
> 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: AlticeLa_fc:f0:a0 (1c:57:3e:fc:f0:a0)
Source address: AlticeLa_fc:f0:a0 (1c:57:3e:fc:f0:a0)
BSS Id: AlticeLa_fc:f0:a0 (1c:57:3e:fc:f0:a0)
..... 0000 = Fragment number: 0
1110 0000 1110 .... = Sequence number: 3598
Frame check sequence: 0xe2cf9658 [unverified]
[FCS Status: Unverified]
> IEEE 802.11 Wireless Management

Figura 2.7: Características da trama beacon

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

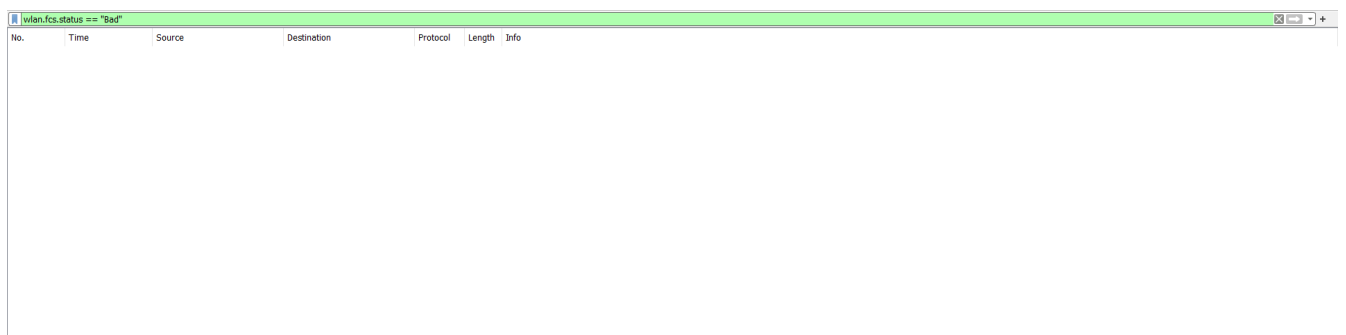
**R:** Relativamente à trama acima demonstrada, podemos concluir que a sua origem se trata de AlticeLa\_fc com o respetivo MAC apresentado na figura abaixo e o destino trata-se de Broadcast (com o MAC "default" de broadcast, também demonstrado na print).

```
> Frame 10: 329 bytes on wire (2632 bits), 329 bytes captured (2632 bits) on interface en0, id 0
> Radiotap Header v0, Length 60
> 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: AlticeLa_fc:f0:a0 (1c:57:3e:fc:f0:a0)
        Source address: AlticeLa_fc:f0:a0 (1c:57:3e:fc:f0:a0)
        BSS Id: AlticeLa_fc:f0:a0 (1c:57:3e:fc:f0:a0)
        .... 0000 = Fragment number: 0
        1110 0000 1110 .... = Sequence number: 3598
        Frame check sequence: 0xe2cf9658 [unverified]
        [FCS Status: Unverified]
    > IEEE 802.11 Wireless Management
```

Figura 2.8: Endereços MAC

### 2.2.3 Verifique se está a ser usado o método de deteção de erros (CRC). Justifique. Justifique o porquê de ser necessário usar deteção de erros em redes sem fios.

**R:** No campo FCS (Frame Check Sequence) status, é possível ver que este mesmo campo está "verified". Também é possível provar que não existiram erros, através do seguinte filtro: "*wlan.fcs.status == "Bad"*".



The image shows a Wireshark packet capture window. The filter bar at the top contains the text `wlan.fcs.status == "Bad"`. Below the filter bar is a table with the following columns: No., Time, Source, Destination, Protocol, Length, and Info. The table is currently empty, indicating that no packets matching the filter have been captured.

Figura 2.9: Método de deteção de erro



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

**R:** A figura abaixo demonstra os débitos apresentados na trama, em Mbps.

```
Source address: AlticeLa_fc:f0:a0 (1c:57:3e:fc:f0:a0)
BSS Id: AlticeLa_fc:f0:a0 (1c:57:3e:fc:f0:a0)
.... .... 0000 = Fragment number: 0
1110 0000 1110 .... = Sequence number: 3598
Frame check sequence: 0xe2cf9658 [unverified]
[FCS Status: Unverified]
✓ IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  ✓ Tagged parameters (229 bytes)
    > Tag: SSID parameter set: "ME0-FCF0A0"
    ✓ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 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: 18 (0x24)
      Supported Rates: 24 (0x30)
      Supported Rates: 36 (0x48)
      Supported Rates: 54 (0x6c)
    > Tag: DS Parameter set: Current Channel: 1
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: ERP Information
    ✓ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
      Tag Number: Extended Supported Rates (50)
      Tag length: 4
      Extended Supported Rates: 6 (0x0c)
      Extended Supported Rates: 9 (0x12)
      Extended Supported Rates: 12 (0x18)
      Extended Supported Rates: 48 (0x60)
    > Tag: RSN Information
```

Figura 2.10: Os vários débitos de base de uma trama beacon

**2.2.5 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.**

**R:** O intervalo de tempo previsto entre as tramas beacon é o apresentado abaixo. Este valor, na realidade, pode ser considerado quase como uma aproximação visto que o intervalo (teoricamente preciso) pode ser afetado por fatores como interferência derivada de outros dispositivos sem fios, obstáculos físicos e outros condicionamentos que causem atrasos e consequentemente um aumento do intervalo de tempo entre as tramas.

```
> Frame 10: 329 bytes on wire (2632 bits), 329 bytes captured (2632 bits) on interface en0, id 0
> Radiotap Header v0, Length 60
> 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: AlticeLa_fc:f0:a0 (1c:57:3e:fc:f0:a0)
    Source address: AlticeLa_fc:f0:a0 (1c:57:3e:fc:f0:a0)
    BSS Id: AlticeLa_fc:f0:a0 (1c:57:3e:fc:f0:a0)
    .... .... 0000 = Fragment number: 0
    1110 0000 1110 .... = Sequence number: 3598
    Frame check sequence: 0xe2cf9658 [unverified]
    [FCS Status: Unverified]
  ▼ IEEE 802.11 Wireless Management
    ▼ Fixed parameters (12 bytes)
      Timestamp: 2159413350796
      Beacon Interval: 0,102400 [Seconds]
    > Capabilities Information: 0x1411
  > Tagged parameters (229 bytes)
```

Figura 2.11: Intervalos de tempo entre tramas beacon

## 2.2.6 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).

**R:** Através do filtro presente na seguinte imagem (*wlan.ssid*), conseguimos apresentar os SSID's dos AP's que estão a operar. Alguns exemplos deles são "MEO-WIFI", "FlyingNet" e "MEO-D68850", representadas, respetivamente, pelas tramas números 11, 12 e 15.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.005857	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=696, FN=0, Flags=.....C, BI=100, SSID="MEO-D68850"
4	0.008710	PTInovac_d6:88:52	Broadcast	802.11	254	Beacon frame, SN=697, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
5	0.011922	PTInovac_45:be:32	Broadcast	802.11	254	Beacon frame, SN=2358, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
6	0.028491	PTInovac_9e:9b:b2	Broadcast	802.11	254	Beacon frame, SN=2403, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
8	0.050713	HitronTe_e7:c8:76	Broadcast	802.11	385	Beacon frame, SN=1928, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
9	0.053270	HitronTe_e7:c8:76	Broadcast	802.11	453	Beacon frame, SN=1763, FN=0, Flags=.....C, BI=100, SSID="NOS-C876"
10	0.062174	AlticeLa_fc:f0:a0	Broadcast	802.11	329	Beacon frame, SN=3598, FN=0, Flags=.....C, BI=100, SSID="MEO-FCF0A0"
11	0.062181	AlticeLa_fc:f0:a2	Broadcast	802.11	254	Beacon frame, SN=3599, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
12	0.087642	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=956, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
15	0.110775	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=698, FN=0, Flags=.....C, BI=100, SSID="MEO-D68850"
16	0.110784	PTInovac_d6:88:52	Broadcast	802.11	254	Beacon frame, SN=699, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
17	0.131556	PTInovac_9e:9b:b0	Broadcast	802.11	329	Beacon frame, SN=2404, FN=0, Flags=.....C, BI=100, SSID="MEO-9E9B80"
18	0.131662	PTInovac_9e:9b:b2	Broadcast	802.11	254	Beacon frame, SN=2405, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
19	0.154872	HitronTe_e7:c8:76	Broadcast	802.11	385	Beacon frame, SN=1929, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
20	0.154922	HitronTe_e7:c8:76	Broadcast	802.11	453	Beacon frame, SN=1764, FN=0, Flags=.....C, BI=100, SSID="NOS-C876"
21	0.164886	AlticeLa_fc:f0:a0	Broadcast	802.11	329	Beacon frame, SN=3600, FN=0, Flags=.....C, BI=100, SSID="MEO-FCF0A0"
22	0.165158	AlticeLa_fc:f0:a2	Broadcast	802.11	254	Beacon frame, SN=3601, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
23	0.191194	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=957, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
29	0.212403	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=700, FN=0, Flags=.....C, BI=100, SSID="MEO-D68850"
30	0.212528	PTInovac_d6:88:52	Broadcast	802.11	254	Beacon frame, SN=701, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
31	0.218972	PTInovac_45:be:32	Broadcast	802.11	254	Beacon frame, SN=2362, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
33	0.219227	PTInovac_29:a9:c2	Broadcast	802.11	270	Beacon frame, SN=3067, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
35	0.235486	PTInovac_9e:9b:b0	Broadcast	802.11	329	Beacon frame, SN=2406, FN=0, Flags=.....C, BI=100, SSID="MEO-9E9B80"
36	0.235491	PTInovac_9e:9b:b2	Broadcast	802.11	254	Beacon frame, SN=2407, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
40	0.257305	HitronTe_e7:c8:76	Broadcast	802.11	385	Beacon frame, SN=1930, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
41	0.257321	HitronTe_e7:c8:76	Broadcast	802.11	453	Beacon frame, SN=1765, FN=0, Flags=.....C, BI=100, SSID="NOS-C876"
42	0.267335	AlticeLa_fc:f0:a0	Broadcast	802.11	329	Beacon frame, SN=3602, FN=0, Flags=.....C, BI=100, SSID="MEO-FCF0A0"
43	0.267440	AlticeLa_fc:f0:a2	Broadcast	802.11	254	Beacon frame, SN=3603, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
45	0.293712	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=958, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
46	0.315041	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=702, FN=0, Flags=.....C, BI=100, SSID="MEO-D68850"
47	0.315149	PTInovac_d6:88:52	Broadcast	802.11	254	Beacon frame, SN=703, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
48	0.362447	HitronTe_e7:c8:76	Broadcast	802.11	453	Beacon frame, SN=1766, FN=0, Flags=.....C, BI=100, SSID="NOS-C876"
49	0.369664	AlticeLa_fc:f0:a0	Broadcast	802.11	329	Beacon frame, SN=3604, FN=0, Flags=.....C, BI=100, SSID="MEO-FCF0A0"
50	0.369804	AlticeLa_fc:f0:a2	Broadcast	802.11	254	Beacon frame, SN=3605, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
51	0.394519	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=959, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
52	0.415377	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=704, FN=0, Flags=.....C, BI=100, SSID="MEO-D68850"
53	0.416551	PTInovac_d6:88:52	Broadcast	802.11	254	Beacon frame, SN=705, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
54	0.423463	PTInovac_45:be:32	Broadcast	802.11	254	Beacon frame, SN=2366, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"

Figura 2.12: SSID's de AP's da vizinhança da STA

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

**R:** De modo a visualizar as tramas probing request e probing response, estabelecemos o seguinte filtro no Wireshark:

*wlan.fc.type\_subtype == 4 || wlan.fc.type\_subtype == 5*

## 2.2.8 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?

**R:** Derivado pelo "scan ativo", é enviado, em broadcast, um "probing request" pela estação (STA) com MAC address 58:b1:0f:1a:10:f6. O AP responde ao anterior através de um "probing response" contendo informações sobre as suas características com o intuito de se estabelecer uma ligação.

150	1.381604	HitronTe_f3:9a:46	SamsungE_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
151	1.382387	HitronTe_f3:9a:46	SamsungE_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=.....R...C, BI=100, SSID="FlyingNet"
152	1.391750	HitronTe_f3:9a:46	SamsungE_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=.....R...C, BI=100, SSID="FlyingNet"
153	1.391879	HitronTe_ee:2e:c6	SamsungE_1a:10:f6	802.11	485	Probe Response, SN=2192, FN=0, Flags=.....R...C, BI=100, SSID="NOS-2EC6"
155	1.399123	SamsungE_1a:10:f6	Broadcast	802.11	122	Probe Request, SN=1124, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
277	2.710713	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2193, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
279	2.720237	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2193, FN=0, Flags=.....R...C, BI=100, SSID="NOS-2EC6"
334	3.297107	PTInovac_45:be:32	ea:52:54:89:2b:72	802.11	224	Probe Response, SN=2424, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
335	3.297177	PTInovac_45:be:32	ea:52:54:89:2b:72	802.11	224	Probe Response, SN=2424, FN=0, Flags=.....R...C, BI=100, SSID="MEO-WiFi"
336	3.300315	PTInovac_45:be:32	ea:52:54:89:2b:72	802.11	224	Probe Response, SN=2424, FN=0, Flags=.....R...C, BI=100, SSID="MEO-WiFi"
788	7.826332	AltoBeam_08:32:99	Broadcast	802.11	110	Probe Request, SN=1111, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
789	7.832355	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2195, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
791	7.835604	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2195, FN=0, Flags=.....R...C, BI=100, SSID="NOS-2EC6"
793	7.838631	AltoBeam_08:32:99	Broadcast	802.11	110	Probe Request, SN=1112, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
796	7.859430	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
797	7.862565	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....R...C, BI=100, SSID="NOS-2EC6"
798	7.868818	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....R...C, BI=100, SSID="NOS-2EC6"
962	9.389248	PTInovac_29:a9:c0	ARRISGro_a9:9e:98	802.11	434	Probe Response, SN=3266, FN=0, Flags=.....C, BI=100, SSID="Masmorra do Sexo"
963	9.396704	PTInovac_29:a9:c0	ARRISGro_a9:9e:98	802.11	434	Probe Response, SN=3266, FN=0, Flags=.....R...C, BI=100, SSID="Masmorra do Sexo"
> Frame 155: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface en0, id 0						0000 00 00 24 00 0f 08 00 40 56 1e 16 00 00 00 00 00
> Radiotap Header v0, Length 36						0010 10 02 6c 09 80 04 a2 a2 00 04 00 10 18 03 04 00
> 802.11 radio information						0020 b0 02 6d 5a 40 00 00 00 ff ff ff ff ff ff 58 b1
IEEE 802.11 Probe Request, Flags: .....C						0030 0f 1a 10 f6 ff ff ff ff ff ff ff 46 00 01 04
Type/Subtype: Probe Request (0x0004)						0040 02 04 0b 16 32 08 0c 12 18 24 30 48 60 6c 03 01
> Frame Control Field: 0x0000						0050 01 2d 1a 6e 01 03 ff 00 00 00 00 00 00 00 00
.0000 0000 0000 0000 = Duration: 0 microseconds						0060 00 00 00 00 00 00 00 00 00 00 00 dd 07 00
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)						0070 50 f2 08 00 00 00 92 43 c3 ea
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)						
Transmitter address: SamsungE_1a:10:f6 (58:b1:0f:1a:10:f6)						
Source address: SamsungE_1a:10:f6 (58:b1:0f:1a:10:f6)						
BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)						
..... = Fragment number: 0						
0100 0110 0100 ..... = Sequence number: 1124						
Frame check sequence: 0xac34392 [unverified]						
[FCS Status: Unverified]						

Figura 2.13: STA request

No.	Time	Source	Destination	Protocol	Length	Info
150	1.381604	HitronTe_f3:9a:46	SamsungE_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
151	1.382387	HitronTe_f3:9a:46	SamsungE_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=.....R...C, BI=100, SSID="FlyingNet"
152	1.391750	HitronTe_f3:9a:46	SamsungE_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=.....R...C, BI=100, SSID="FlyingNet"
153	1.391879	HitronTe_ee:2e:c6	SamsungE_1a:10:f6	802.11	485	Probe Response, SN=2192, FN=0, Flags=.....R...C, BI=100, SSID="NOS-2EC6"
155	1.399123	SamsungE_1a:10:f6	Broadcast	802.11	122	Probe Request, SN=1124, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
277	2.710713	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2193, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
279	2.720237	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2193, FN=0, Flags=.....R...C, BI=100, SSID="NOS-2EC6"
334	3.297107	PTInovac_45:be:32	ea:52:54:89:2b:72	802.11	224	Probe Response, SN=2424, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
335	3.297177	PTInovac_45:be:32	ea:52:54:89:2b:72	802.11	224	Probe Response, SN=2424, FN=0, Flags=.....R...C, BI=100, SSID="MEO-WiFi"
336	3.300315	PTInovac_45:be:32	ea:52:54:89:2b:72	802.11	224	Probe Response, SN=2424, FN=0, Flags=.....R...C, BI=100, SSID="MEO-WiFi"
788	7.826332	AltoBeam_08:32:99	Broadcast	802.11	110	Probe Request, SN=1111, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
789	7.832355	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2195, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
791	7.835604	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2195, FN=0, Flags=.....R...C, BI=100, SSID="NOS-2EC6"
793	7.838631	AltoBeam_08:32:99	Broadcast	802.11	110	Probe Request, SN=1112, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
796	7.859430	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
797	7.862565	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....R...C, BI=100, SSID="NOS-2EC6"
798	7.868818	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....R...C, BI=100, SSID="NOS-2EC6"
962	9.389248	PTInovac_29:a9:c0	ARRISGro_a9:9e:98	802.11	434	Probe Response, SN=3266, FN=0, Flags=.....C, BI=100, SSID="Masmorra do Sexo"
963	9.396704	PTInovac_29:a9:c0	ARRISGro_a9:9e:98	802.11	434	Probe Response, SN=3266, FN=0, Flags=.....R...C, BI=100, SSID="Masmorra do Sexo"
> Frame 277: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface en0, id 0						0030 c3 ee 2e c6 00 aa c3 ee 2e c6 10 89 f
> Radiotap Header v0, Length 36						0040 06 00 00 00 64 00 31 04 00 08 4e 4f f
> 802.11 radio information						0050 43 36 01 08 82 84 8b 96 8c 12 98 24 f
IEEE 802.11 Probe Response, Flags: .....C						0060 06 50 54 20 01 0d 14 2a 01 00 32 04 f
Type/Subtype: Probe Response (0x0005)						0070 2d 1a ad 09 03 ff ff ff ff 00 00 00 00
> Frame Control Field: 0x5000						0080 00 01 00 00 00 00 00 00 00 00 00 00
.0000 0001 0011 1010 = Duration: 314 microseconds						0090 04 00 00 00 00 00 00 00 00 00 00 00
Receiver address: AltoBeam_08:32:99 (a4:ef:15:08:32:99)						00a0 00 00 00 00 7f 08 04 00 0f 02 00 00
Destination address: AltoBeam_08:32:99 (a4:ef:15:08:32:99)						00b0 b2 79 8a 33 ea ff 00 00 ea ff 00 20
Transmitter address: HitronTe_ee:2e:c6 (90:aa:c3:ee:2e:c6)						00c0 00 fc ff dd 18 00 50 f2 02 01 01 80
Source address: HitronTe_ee:2e:c6 (90:aa:c3:ee:2e:c6)						00d0 00 27 a4 00 00 42 5e 00 62 32 2f
BSS Id: HitronTe_ee:2e:c6 (90:aa:c3:ee:2e:c6)						00e0 03 7f 01 01 00 00 07 7f dd 16 8c fd
..... = Fragment number: 0						00f0 49 4c 51 03 02 09 72 01 8c 16 00 00
1000 1001 0001 ..... = Sequence number: 2193						0100 dd 1a 00 50 f2 01 01 00 50 f2 02
Frame check sequence: 0xa9a74476 [unverified]						0110 f2 04 00 52 f2 02 01 00 50 f2 02
[FCS Status: Unverified]						0120 00 0f ac 02 00 00 0f ac 04 00 0f
						0130 00 0f ac 02 00 00 dd 9f 00 50 f2 03
						0140 10 10 44 00 01 02 10 3b 00 01 03 10

Figura 2.14: STA response

## 2.3 Processo de Associação

### 2.3.1 Identifique uma sequência de tramas que corresponda a um processo de associação realizado com sucesso entre a STA e o AP, incluindo a fase de autenticação.

**R:** Aplicando o filtro "`wlan.fc.type==0 && (wlan.fc.subtype==0 || wlan.fc.subtype==1 || wlan.fc.subtype==11 || wlan.fc.subtype==8)`" conseguimos filtrar uma sequência de tramas correspondente a um processo de associação, incluindo a fase de autenticação.

No.	Time	Source	Destination	Protocol	Length	Info
8464	73.347725	PTInovac_9e:9b:b0	Broadcast	802.11	329	Beacon frame, SN=3913, FN=0, Flags=.....C, BI=100, SSID="MEO-9E9B80"
8465	73.371127	HitronTe_ee:2e:c6	Broadcast	802.11	385	Beacon frame, SN=2711, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
8466	73.371206	HitronTe_e7:c8:76	Broadcast	802.11	453	Beacon frame, SN=2513, FN=0, Flags=.....C, BI=100, SSID="NOS-C876"
8467	73.381342	AlticeLa_fc:f0:a0	Broadcast	802.11	329	Beacon frame, SN=955, FN=0, Flags=.....C, BI=100, SSID="MEO-FCF0A0"
8468	73.381714	AlticeLa_fc:f0:a2	Broadcast	802.11	254	Beacon frame, SN=956, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
8469	73.408082	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=1701, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
8470	73.428400	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=2249, FN=0, Flags=.....C, BI=100, SSID="MEO-D68850"
8471	73.428531	PTInovac_d6:88:52	Broadcast	802.11	254	Beacon frame, SN=2250, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
8472	73.450730	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	70	Authentication, SN=262, FN=0, Flags=.....C
8474	73.450775	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	70	Authentication, SN=1965, FN=0, Flags=.....C
8476	73.459546	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	164	Association Request, SN=263, FN=0, Flags=.....C, SSID="FlyingNet"
8478	73.459638	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	210	Association Response, SN=1966, FN=0, Flags=.....C
8485	73.472986	HitronTe_e7:c8:76	Broadcast	802.11	453	Beacon frame, SN=2514, FN=0, Flags=.....C, BI=100, SSID="NOS-C876"
8497	73.510424	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=1702, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
8505	73.530748	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=2251, FN=0, Flags=.....C, BI=100, SSID="MEO-D68850"
8508	73.531678	PTInovac_d6:88:52	Broadcast	802.11	254	Beacon frame, SN=2252, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
8509	73.534969	PTInovac_d5:be:32	Broadcast	802.11	254	Beacon frame, SN=3831, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
8538	73.576711	HitronTe_ee:2e:c6	Broadcast	802.11	385	Beacon frame, SN=2713, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
8539	73.587818	AlticeLa_fc:f0:a2	Broadcast	802.11	254	Beacon frame, SN=959, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"

Figura 2.15: Processo de associação entre STA e AP

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

**R:** Construímos um diagrama que ilustra a sequência de trocas das tramas no processo anterior.

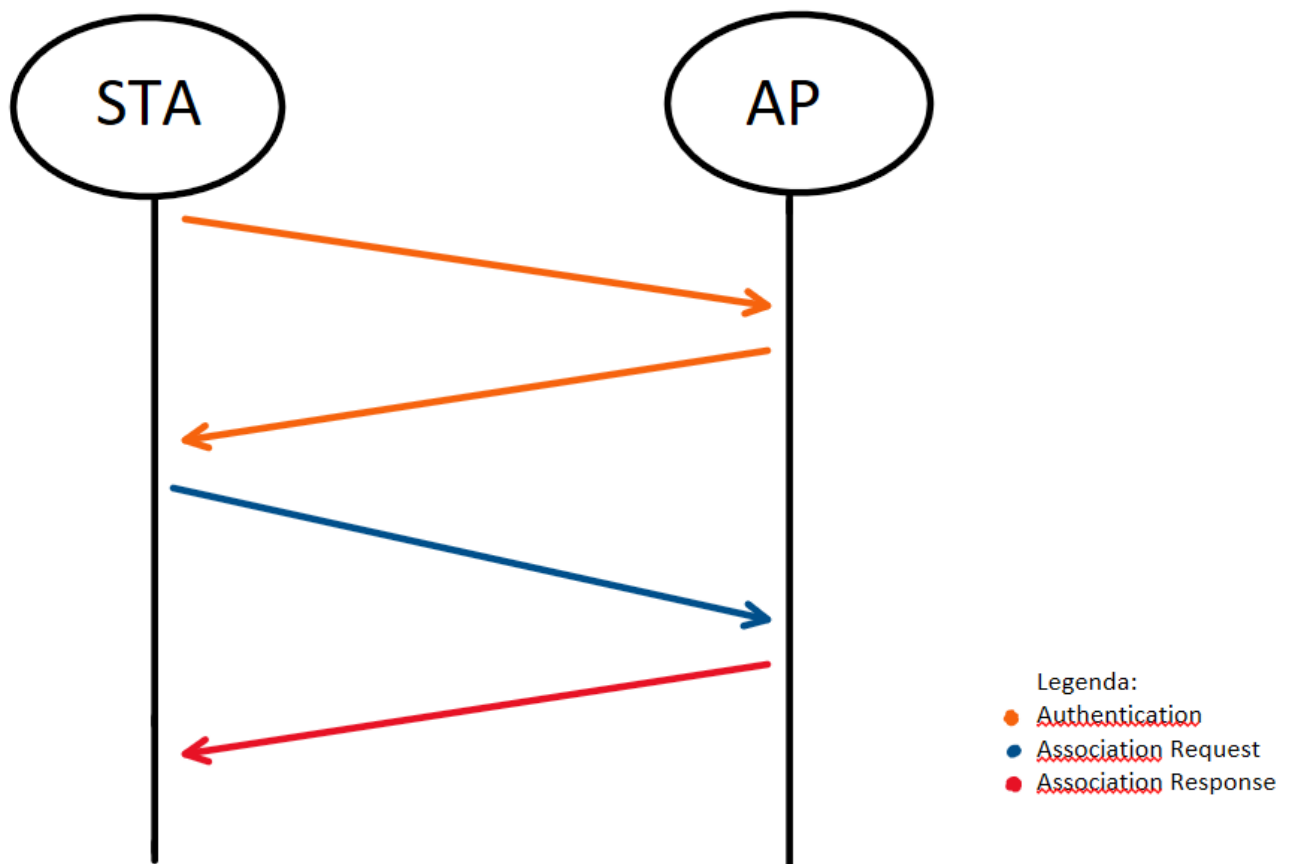


Figura 2.16: Diagrama das trocas de tramas

## 2.4 Transferência de Dados

### 2.4.1 Considere a trama de dados nº8503. 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?

**R:** Tal como ilustra a figura, vemos que as flags "To DS"(para o servidor de distribuição) e "From DS" estão respetivamente a 1 e 0, podemos afirmar que as tramas são destinadas ao DS, provenientes do STA do cliente através do AP.

```
> Frame 8503: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits) on interface en0, id 0
> Radiotap Header v0, Length 58
> 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... .... = +HTC/Order flag: Not strictly ordered
        .000 0000 0011 0000 = Duration: 48 microseconds
        Receiver address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
```

Figura 2.17: Direccionalidade das tramas

### 2.4.2 Para a trama de dados nº8503, transcreva os endereços MAC em uso, identificando quais os endereços correspondentes à estação sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição (DS)?

**R:** Observando a trama em questão temos que:

- **STA** (receiver address) - 80:c5:f2:0f:0e:9b
- **AP** (transmitter address) - 74:9b:e8:f3:9a:46
- **router de acesso** (destination address) - 33:33:00:00:00:16

```
  Frame Control Field: 0x8841
    .... ..00 = Version: 0
    .... 10.. = Type: Data frame (2)
    1000 .... = Subtype: 8
    > Flags: 0x41
    .000 0000 0011 0000 = Duration: 48 microseconds
    Receiver address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
    Transmitter address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
    Destination address: IPv6mcast_16 (33:33:00:00:00:16)
    Source address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
    BSS Id: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
    STA address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
    .... .... 0000 = Fragment number: 0
    0000 0000 0000 .... = Sequence number: 0
    Frame check sequence: 0x57cf2fa2 [correct]
    [FCS Status: Good]
  > Qos Control: 0x0000
  > CCMP parameters
> Data (92 bytes)
```

Figura 2.18: Endereços MAC da STA, AP e router de acesso ao DS



### 2.4.3 Como interpreta a trama nº8521 face à sua direccionalidade e endereçamento MAC?

**R:** Através das flags do DS (sistema de distribuição), contrariamente à trama que vimos anteriormente, sabemos que a trama vem de DS (sistema de distribuição) para o STA, via AP. Na figura seguinte encontram-se também os endereços MAC correspondentes à origem e destino.

```

.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
v 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... .... = +HTC/Order flag: Not strictly ordered
.000 0000 0011 1100 = Duration: 60 microseconds
Receiver address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
Transmitter address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
Destination address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
Source address: 76:9b:e8:f3:9a:43 (76:9b:e8:f3:9a:43)
BSS Id: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
STA address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
.... ..0000 = Fragment number: 0

```

Figura 2.19: Direccionalidade e endereçamento MAC

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

**R:** Ao longo da transferência de dados, são transmitidas tramas **RTS** (Request-to-send) que solicita permissão para enviar a trama, **CTS** (Clear-to-send) que é basicamente o recetor a ceder permissão para se dar o envio) e **ACK** (Acknowledgment) que confirma que recebeu a trama de dados. Dá-se numa rede **WLAN** para tentar aumentar a eficácia das comunicações sem fio.

8510 73.542828	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	73 Action, SN=1, FN=0, Flags=.....C, Dialog Token=1
8511 73.542835		HitronTe_f3:9a:46 (...)	802.11	48 Acknowledgement, Flags=.....C
8512 73.542839	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	73 Action, SN=612, FN=0, Flags=.....C, Dialog Token=1
8513 73.542845		AzureWav_0f:0e:9b (...)	802.11	48 Acknowledgement, Flags=.....C
8514 73.544132	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	73 Action, SN=2, FN=0, Flags=.....C, Dialog Token=1
8515 73.544136		HitronTe_f3:9a:46 (...)	802.11	48 Acknowledgement, Flags=.....C
8516 73.544143	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	73 Action, SN=613, FN=0, Flags=.....C, Dialog Token=1
8517 73.544147	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	73 Action, SN=613, FN=0, Flags=...R...C, Dialog Token=1
8518 73.544151		AzureWav_0f:0e:9b (...)	802.11	48 Acknowledgement, Flags=.....C
8519 73.544155	HitronTe_f3:9a:46 (...)	AzureWav_0f:0e:9b (...)	802.11	76 Request-to-send, Flags=.....C
8520 73.544159		HitronTe_f3:9a:46 (...)	802.11	72 Clear-to-send, Flags=.....C
8521 73.544163	76:9b:e8:f3:9a:43	AzureWav_0f:0e:9b	802.11	444 QoS Data, SN=2, FN=0, Flags=.p....F.C
8522 73.544167	AzureWav_0f:0e:9b (...)	HitronTe_f3:9a:46 (...)	802.11	68 802.11 Block Ack, Flags=.....C
8523 73.544170	HitronTe_f3:9a:46 (...)	AzureWav_0f:0e:9b (...)	802.11	76 Request-to-send, Flags=.....C
8524 73.544174		HitronTe_f3:9a:46 (...)	802.11	72 Clear-to-send, Flags=.....C
8525 73.544215	76:9b:e8:f3:9a:43	AzureWav_0f:0e:9b	802.11	282 QoS Data, SN=0, FN=0, Flags=.p..R.F.C
8526 73.544219	AzureWav_0f:0e:9b (...)	HitronTe_f3:9a:46 (...)	802.11	68 802.11 Block Ack, Flags=.....C
8527 73.544224	PTInovac_d6:88:50 (...)	ce:90:6f:21:42:3a (...)	802.11	76 Request-to-send, Flags=.....C
8528 73.552942	PTInovac_d6:88:50 (...)	ce:90:6f:21:42:3a (...)	802.11	76 Request-to-send, Flags=.....C

Figura 2.20: Subtipos de tramas de controlo

**2.4.5 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.**

**R:** Tal como evidenciado pela figura anterior, está a ser usada a opção RTS/CTS e possui uma direccionalidade de "0 para 0" (cujo valor, demonstrado na figura imediatamente a seguir, indica que esta trama está a ser transmitida localmente dentro do WLAN). Ambas têm o mesmo endereço de destino e o mesmo endereço que o STA, contudo, o endereço de origem não corresponde a nenhum dispositivo conhecido pelo que é possível concluir que a direccionalidade da trama é AP → STA.

```
Type/Subtype: Beacon frame (0x0008)
  Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
  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... .... = +HTC/Order flag: Not strictly ordered
  .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_e7:c8:76 (fc:77:7b:e7:c8:76)
  Source address: HitronTe_e7:c8:76 (fc:77:7b:e7:c8:76)
  BSS Id: HitronTe_e7:c8:76 (fc:77:7b:e7:c8:76)
  .... .... 0000 = Fragment number: 0
  0111 0011 0111 .... = Sequence number: 1847
  Frame check sequence: 0xd93c3bb1 [correct]
  [FCS Status: Good]
```

Figura 2.21: Trama com RTS/CTS



No.	Time	Source	Destination	Protocol	Length	Info
8516	73.544143	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	73	Action, SN=613, FN=0, Flags=.....C, Dialog Token=1
8517	73.544147	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	73	Action, SN=613, FN=0, Flags=....R...C, Dialog Token=1
8518	73.544151		AzureWav_0f:0e:9b (...)	802.11	48	Acknowledgement, Flags=.....C
8519	73.544155	HitronTe_f3:9a:46 (...)	AzureWav_0f:0e:9b (...)	802.11	76	Request-to-send, Flags=.....C
8520	73.544159		HitronTe_f3:9a:46 (...)	802.11	72	Clear-to-send, Flags=.....C
8521	73.544163	76:9b:e8:f3:9a:43	AzureWav_0f:0e:9b	802.11	444	QoS Data, SN=2, FN=0, Flags=.p....F.C
8522	73.544167	AzureWav_0f:0e:9b (...)	HitronTe_f3:9a:46 (...)	802.11	68	802.11 Block Ack, Flags=.....C
8523	73.544170	HitronTe_f3:9a:46 (...)	AzureWav_0f:0e:9b (...)	802.11	76	Request-to-send, Flags=.....C
8524	73.544174		HitronTe_f3:9a:46 (...)	802.11	72	Clear-to-send, Flags=.....C
8525	73.544215	76:9b:e8:f3:9a:43	AzureWav_0f:0e:9b	802.11	282	QoS Data, SN=0, FN=0, Flags=.p...R.F.C
8526	73.544219	AzureWav_0f:0e:9b (...)	HitronTe_f3:9a:46 (...)	802.11	68	802.11 Block Ack, Flags=.....C
8527	73.544224	PTInovac_d6:88:50 (...)	ce:90:6f:21:42:3a (...)	802.11	76	Request-to-send, Flags=.....C
8528	73.552942	PTInovac_d6:88:50 (...)	ce:90:6f:21:42:3a (...)	802.11	76	Request-to-send, Flags=.....C
8529	73.559878	PTInovac_d6:88:50 (...)	ce:90:6f:21:42:3a (...)	802.11	76	Request-to-send, Flags=.....C
8530	73.560175	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	73	Action, SN=614, FN=0, Flags=.....C, Dialog Token=1
8531	73.560179		AzureWav_0f:0e:9b (...)	802.11	48	Acknowledgement, Flags=.....C
8532	73.561406	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	73	Action, SN=3, FN=0, Flags=.....C, Dialog Token=1
8533	73.561412		HitronTe_f3:9a:46 (...)	802.11	48	Acknowledgement, Flags=.....C
8534	73.561415	AzureWav_0f:0e:9b	IPv4mcast_16	802.11	152	QoS Data, SN=2, FN=0, Flags=.p....TC

.... 00.. = Type: Management frame (0)	0000 00 00 24 00 6f 08 00
1101 .... = Subtype: 13	0010 10 02 6c 09 80 04 d2
Flags: 0x00	0020 28 01 6b bf d0 00 3a
.... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0)	0030 e8 f3 9a 46 74 9b e8
.... .0.. = More Fragments: This is the last fragment	0040 00 1b 10 00 00 c3 22
.... 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... .... = +HTC/Order flag: Not strictly ordered	
.000 0001 0011 1010 = Duration: 314 microseconds	
Receiver address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)	
Destination address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)	
Transmitter address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)	
Source address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)	
BSS Id: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)	
.... .... 0000 = Fragment number: 0	
0000 0000 0011 .... = Sequence number: 3	

Figura 2.22: Trama sem RTS/CTS

Nesta última figura, é possível ver que não está a ser usado RTS/CTS. Como a direcionalidade destas tramas também é "0 para 0" e o endereço de origem e destino também são os mesmos, podemos concluir exatamente o mesmo que concluímos para a trama anterior.

### **3 Conclusão**

Através do trabalho prático conseguimos consolidar as informações sobre o funcionamento da rede sem fios. Desde os vários tipos e subtipos de tramas até à direcionalidade das mesmas, fomos capazes de compreender melhor os conceitos anteriormente lecionados nas aulas teóricas.

Para além disso, conseguimos ainda aprimorar os nossos métodos de trabalho enquanto um grupo.