

Universidade do Minho



# Redes de Computadores

## RC-TP2

MESTRADO INTEGRADO EM ENGENHARIA INFORMÁTICA

3º ANO

GRUPO 61

RENATO ANDRÉ ARAÚJO AZEVEDO  
GONÇALO COSTA DE ALMEIDA  
MARIA SOFIA MARTINHO GONÇALVES JORDÃO MARQUES

**A89547**  
**A88292**  
**A87963**

# Índice

<b>1</b>	<b>Introdução</b>	<b>3</b>
<b>2</b>	<b>Acesso Rádio</b>	<b>3</b>
2.1	Ex1 . . . . .	3
2.2	Ex2 . . . . .	3
2.3	Ex3 . . . . .	3
<b>3</b>	<b>Scanning Passivo e Scanning Ativo</b>	<b>3</b>
3.1	Ex4 . . . . .	3
3.2	Ex5 . . . . .	4
3.3	Ex6 . . . . .	4
3.4	Ex7 . . . . .	5
3.5	Ex8 . . . . .	5
3.6	Ex9 . . . . .	6
3.7	Ex10 . . . . .	6
3.8	Ex11 . . . . .	7
<b>4</b>	<b>Processo de Associação</b>	<b>7</b>
4.1	Ex12 . . . . .	7
4.2	Ex13 . . . . .	8
<b>5</b>	<b>Transferência de Dados</b>	<b>8</b>
5.1	Ex14 . . . . .	8
5.2	Ex15 . . . . .	8
5.3	Ex16 . . . . .	9
5.4	Ex17 . . . . .	9
5.5	Ex18 . . . . .	9
<b>6</b>	<b>Conclusão</b>	<b>10</b>

# 1 Introdução

No âmbito da cadeira de Redes Computadores foi-nos proposta a elaboração de um trabalho que terá como principal objetivo o estudo das redes sem fios e as suas principais vertentes, nomeadamente: o estudo do protocolo IEEE 802.11, onde exploramos o formato das tramas, o endereçamento dos componentes envolvidos na comunicação sem fios, os tipos de tramas, bem como o modo de operação do protocolo.

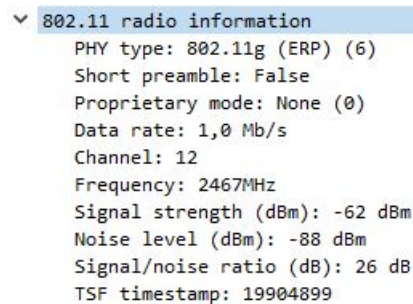
Esperamos, com este trabalho, atingir os objetivos definidos pelo docente.

## 2 Acesso Rádio

### 2.1 Ex1

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

O espectro está a operar na frequência 2467MHz (*Frequency: 12*), e o canal correspondente é o 12 (*Channel: 12*).



```
▼ 802.11 radio information
  PHY type: 802.11g (ERP) (6)
  Short preamble: False
  Proprietary mode: None (0)
  Data rate: 1,0 Mb/s
  Channel: 12
  Frequency: 2467MHz
  Signal strength (dBm): -62 dBm
  Noise level (dBm): -88 dBm
  Signal/noise ratio (dB): 26 dB
  TSF timestamp: 19904899
```

Figure 1: Informação do canal

### 2.2 Ex2

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

A versão da norma IEEE 802.11 utilizada é 802.11g, como podemos observar pelo campo *PHY type*.

### 2.3 Ex3

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.

O débito a que a trama foi enviada foi de 1 Mb/s, como podemos observar pela imagem no campo *Data rate*. No entanto esse débito não corresponde ao débito máximo a que a interface pode operar, uma vez que o protocolo 802.11g permite débitos até 54 Mb/s.

## 3 Scanning Passivo e Scanning Ativo

### 3.1 Ex4

Selecione uma trama beacon (e.g., trama 10XX). 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)?

Selecione a trama 1061 podemos verificar que esta corresponde a uma trama do tipo 802.11, sendo o seu tipo e subtipo identificados no campo frame control, como podemos retirar da imagem a baixo.

Type: Management frame (0)  
Subtype: 8

```
> Frame 1061: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
▼ IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  ▼ Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
  > Flags: 0x00
```

Figure 2: Frame control trama 1061

### 3.2 Ex5

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

Os endereços MAC identificados na trama são ff:ff:ff:ff:ff:ff, que corresponde ao endereço MAC do destino, e o endereço bc:14:01:af:b1:99 que corresponde simultaneamente ao AP que transmitiu a trama e ao router à qual o AP está ligado, podendo concluir que o router e o AP estão juntos. Desta forma, podemos concluir que a origem da trama foi no AP e o destino é toda a rede, o que faz sentido, já que se trata de uma trama beacon.

```
▼ IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  ▼ Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
  > Flags: 0x00
  .000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  Transmitter address: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
  Source address: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
  BSS Id: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
  .... .... 0000 = Fragment number: 0
  1011 0100 1110 .... = Sequence number: 2894
  Frame check sequence: 0x848f7a6a [unverified]
  [FCS Status: Unverified]
```

Figure 3: Endereços da trama

### 3.3 Ex6

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

O AP consegue suportar vários débitos de base de 1 MB até 54 MB, além de débitos adicionais entre 6 MB até 48 MB, como podemos observar na seguinte imagem.

```

  Tagged parameters (140 bytes)
  > Tag: SSID parameter set: NOS_WIFI_Fon
  > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
    Tag Number: Supported Rates (1)
    Tag length: 8
    Supported Rates: 1(B) (0x82)
    Supported Rates: 2(B) (0x84)
    Supported Rates: 5.5(B) (0x8b)
    Supported Rates: 11(B) (0x96)
    Supported Rates: 9 (0x12)
    Supported Rates: 18 (0x24)
    Supported Rates: 36 (0x48)
    Supported Rates: 54 (0x6c)
  > Tag: DS Parameter set: Current Channel: 12
  > Tag: Extended Supported Rates 6(B), 12(B), 24(B), 48, [Mbit/sec]
    Tag Number: Extended Supported Rates (50)
    Tag length: 4
    Extended Supported Rates: 6(B) (0x8c)
    Extended Supported Rates: 12(B) (0x98)
    Extended Supported Rates: 24(B) (0xb0)
    Extended Supported Rates: 48 (0x60)
  > Tag: Traffic Indication Map (TIM): DTIM 2 of 3 bitmap
  > Tag: ERP Information

```

Figure 4: Debitos

### 3.4 Ex7

Qual 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 provenientes do mesmo AP é verificada? Tente explicar porquê.

O intervalo de tempo entre tramas consecutivas é visível no campo Beacon Interval ao qual corresponde o tempo 0,102400 [Seconds], enquanto que o intervalo verificado é de 0.102275. Tendo isso em conta é possível verificar que o tempo entre essas tramas consecutivas de facto não se verifica. Isto pode acontecer por alguma falta de precisão de um AP que pode estar a enviar a trama mais cedo do q o suposto.

```

1061 41.473937 HitronTe_af:b1:99 Broadcast 802.11 205 Beacon frame, SN=2894, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1062 41.574567 HitronTe_af:b1:98 Broadcast 802.11 296 Beacon frame, SN=2895, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1063 41.576212 HitronTe_af:b1:99 Broadcast 802.11 205 Beacon frame, SN=2896, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

```

Figure 5: Intervalo de tempo verificado

```

> Frame 1062: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....C
  IEEE 802.11 Wireless Management
    Fixed parameters (12 bytes)
      Timestamp: 1149712179717
      Beacon Interval: 0,102400 [Seconds]
    Capabilities Information: 0x0c31
    Tagged parameters (231 bytes)

```

Figure 6: Intervalo de tempo da trama beacon

### 3.5 Ex8

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).

Como vimos na pergunta 4, os Beacon tem o campo *Subtype* com o valor 0x08. Desta forma, podemos criar um filtro que escolha todas as tramas cujo campo tenha este valor, o que fica wlan.fc.type\_subtype == 0x08. Desta forma, podemos observar que os SSIDs dos APs que estão a operar na vizinhança da STA de captura são o NOS\_WIFI\_Fon e o FlyingNet.

wlan.fc.type_subtype == 0x8						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2083, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2	0.001662	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2084, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
3	0.102552	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2085, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
4	0.104164	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2086, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
5	0.204951	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2087, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
6	0.206582	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2088, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
7	0.307368	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2089, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
8	0.308999	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2090, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
9	0.409749	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2091, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
10	0.411376	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2092, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
11	0.512117	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2093, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
12	0.513707	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2094, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
13	0.614562	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2095, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
14	0.616191	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2096, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
28	0.716961	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2097, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
29	0.718611	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2098, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
32	0.819368	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2099, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
33	0.821009	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2100, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
34	0.921756	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2101, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
35	0.923387	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2102, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
36	1.024021	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2103, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
37	1.025663	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2104, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
38	1.126564	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2105, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
39	1.128193	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2106, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
40	1.228961	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2107, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
41	1.230650	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2108, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

Figure 7: Pontos de acesso na vizinhança

### 3.6 Ex9

Verifique se está a ser usado o método de deteção de erros (CRC). Justifique.

O método de detenção de erro está a ser utilizado conforme podemos ver no exemplo. As redes sem fios estão sujeitas a taxas de erros muito mais intensas e variáveis do que as redes cabladas, devido a diversos factores, como ruído, interferência de outras fontes, obstrução do sinal, etc. Assim sendo é necessário a utilização da detenção de erros.

6274	94.779098	36:00:ae:51:f4:19	43:46:06:ca:97:53	802.11	146	Beacon frame, SN=238, FN=9, Flags=.pmPRM.T.
6937	99.991379	be:65:24:9b:d6:a1	0e:0b:77:ea:c1:bc	802.11	146	Beacon frame, SN=393, FN=10, Flags=....R.FT., BI=4913[Malformed Packet]
7013	100.184381	bd:09:48:c5:79:35	43:46:15:10:df:53	802.11	146	Beacon frame, SN=3658, FN=10, Flags=.pmPRM.T.
7131	100.398018	62:4c:de:c5:a9:3a	34:c4:ca:25:ed:14	802.11	146	Beacon frame, SN=2811, FN=0, Flags=.pmPRM.T.
7173	100.404266	84:84:4c:a8:fd:ea	d2:f4:d1:ff:e5:79	802.11	146	Beacon frame, SN=2338, FN=10, Flags=.pm....T.

> Frame 6274: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits)	
> Radiotap Header v0, Length 40	
> 802.11 radio information	
IEEE 802.11 Beacon frame, Flags: .pmPRM.T.	
Type/Subtype: Beacon frame (0x0008)	
> Frame Control Field: 0x827d	
.011 1010 0101 1010 = Duration: 14938 microseconds	
Receiver address: 43:46:06:ca:97:53 (43:46:06:ca:97:53)	
Destination address: 43:46:06:ca:97:53 (43:46:06:ca:97:53)	
Transmitter address: 36:00:ae:51:f4:19 (36:00:ae:51:f4:19)	
Source address: 36:00:ae:51:f4:19 (36:00:ae:51:f4:19)	
BSS Id: 4e:0e:f5:50:50:f3 (4e:0e:f5:50:50:f3)	
STA address: 36:00:ae:51:f4:19 (36:00:ae:51:f4:19)	
.... 1001 = Fragment number: 9	
0000 1110 .... = Sequence number: 236	
> Frame check sequence: 0xde578f50 incorrect, should be 0xd04b9c0c	
[FCS Status: Bad]	
> WEP parameters	
> Data (70 bytes)	

Figure 8: Trama com erros

### 3.7 Ex10

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

Uma vez que no campo Subtype, o *probing request* tem associado o valor 0x4 e o *probing response* tem associado o valor 0x5, então podemos aplicar o filtro "wlan.fc.type\_subtype in 0x4 0x5", que vai filtrar todas as tramas cujo valor no campo *Subtype* seja 0x4 ou 0x5.

### 3.8 Ex11

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?

Um exemplo de *probe request* para o qual houve um *probe response* foi o da imagem abaixo. Neste caso, para o *probe request* o sistema que envia a trama é o Apple\_10:6a:f5, e o destino são todos os AP que se encontram na rede, uma vez que é enviada em broadcast. Já no *probe response*, o sistema que envia a trama é o AP/router HitreonTe.af:b1:98 e o destinatário é o STA que fez o *probe request*, ou seja, o Apple\_10:6a:f5. Estas tramas servem para que um STA possa saber as informações de todos os AP disponíveis na rede, para posteriormente se associar a um deles.

```
2603 72.179215 Apple_10:6a:f5 Broadcast 802.11 164 Probe Request, SN=2563, FN=0, Flags=.....C, SSID=FlyingNet
2606 72.179924 HitronTe_af:b1:98 Apple_10:6a:f5 802.11 411 Probe Response, SN=2346, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
```

Figure 9: Probing request e Probing response

## 4 Processo de Associação

### 4.1 Ex12

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

Estas tramas podem ser encontradas usando o filtro `wlan.fc.type_subtype == 0 || wlan.fc.type_subtype == 1 || wlan.fc.type_subtype == 11`, onde o primeiro campo corresponde a um pedido de associação, o segundo corresponde a uma resposta a um pedido de autenticação, e o último corresponde à autenticação.

```
2486 70.361782 Apple_10:6a:f5 HitronTe_af:b1:98 802.11 70 Authentication, SN=2542, FN=0, Flags=.....C
2487 70.362050 Apple_10:6a:f5 (64: 802.11 39 Acknowledgement, Flags=.....C
2488 70.381869 HitronTe_af:b1:98 Apple_10:6a:f5 802.11 59 Authentication, SN=2338, FN=0, Flags=.....C
2489 70.381878 HitronTe_af:b1:98 ( 802.11 39 Acknowledgement, Flags=.....C
2490 70.383512 Apple_10:6a:f5 HitronTe_af:b1:98 802.11 175 Association Request, SN=2543, FN=0, Flags=.....C, SSID=FlyingNet
2491 70.383873 Apple_10:6a:f5 (64: 802.11 39 Acknowledgement, Flags=.....C
2492 70.389339 HitronTe_af:b1:98 Apple_10:6a:f5 802.11 225 Association Response, SN=2339, FN=0, Flags=.....C
2493 70.389352 HitronTe_af:b1:98 ( 802.11 39 Acknowledgement, Flags=.....C
```

Figure 10: Tramas do processo de associação



## 4.2 Ex13

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

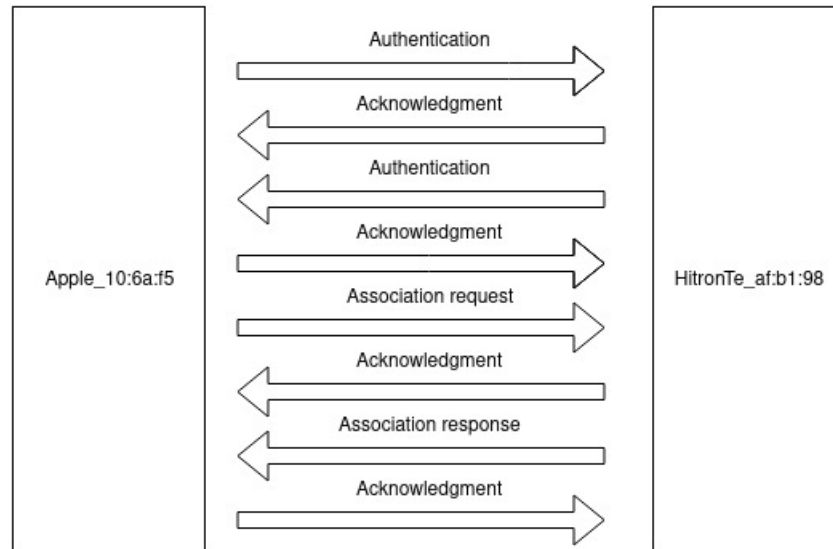


Figure 11: Tramas do processo de associação

## 5 Transferência de Dados

### 5.1 Ex14

Considere a trama de dados nº455. 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?

Uma vez que o campo To DS está a 0 e o *From DS* está a 1, podemos concluir que a direccionalidade da trama foi da estação para o Sistema de Distribuição. Desta forma, como o destino da trama é exterior ao BSS, podemos concluir que a direccionalidade da trama não é local à WLAN.

```
▼ Frame Control Field: 0x8842
.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
▼ Flags: 0x42
.... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
.... .0.. = More Fragments: This is the last fragment
.... 0... = Retry: Frame is not being retransmitted
...0 .... = PWR MGT: STA will stay up
..0. .... = More Data: No data buffered
.1.. .... = Protected flag: Data is protected
0... .... = Order flag: Not strictly ordered
```

Figure 12: Flags da trama 455

### 5.2 Ex15

Para a trama de dados nº455, 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?



O endereço MAC correspondente ao host sem fios (STA) é d8:a2:5e:71:41:a1, já o do AP é d8:a2:5e:71:41:a1, e por fim, o endereço MAC do router de acesso ao sistema de distribuição é bc:14:01:af:b1:98.

```
Receiver address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
Destination address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
STA address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
```

Figure 13: Endereços MAC

### 5.3 Ex16

**Como interpreta a trama nº457 face à sua direccionalidade e endereçamento MAC?**

Uma vez que o campo To DS está a 1 e o *From DS* está a 0, podemos concluir que a direccionalidade da trama foi do Sistema de Distribuição para a estação. Além disso, podemos concluir que

```
▼ 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
```

Figure 14: Flags da trama 457

### 5.4 Ex17

**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.)**

Ao longo da transferência de dados, são transmitidas tramas de controlo de erros denominadas acknowledgments. Estas tramas são fundamentais nas redes sem fios, uma vez que nestas a probabilidade de ocorrência de erros é muito superior à de uma rede ethernet, por exemplo, não estando implementado nenhum método de controlo de erros. Para contornar este problema, as estações enviam sempre um acknowledgment para comunicar ao emissor que a mensagem foi bem recebida, o que permite determinar se ocorreram erros na transferencia de dados.

### 5.5 Ex18

**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.**

Como podemos observar na imagem, as tramas RTS (*Request To Send*) e CTS (*Clear To Send*) estão a ser utilizadas na troca de dados entre o AP e o STA, sendo a trama 533 um RTS e a trama 534 um CTS. Neste caso, o STA corresponde ao Apple\_10:6a:f5 e o AP ao Hitreonte\_af:b1:98. Além disso, como as flags *To DS* e *From DS* estão ambas a zero, podemos concluir que a direccionalidade da trama é local à WLAN.

```

533 21.548964 Apple_10:6a:f5 (64:... HitronTe_af:b1:98 (... 802.11 45 Request-to-send, Flags=.....C
534 21.548970 Apple_10:6a:f5 (64:... 802.11 39 Clear-to-send, Flags=.....C

```

Figure 15: Tramas RTS e CTL

```

534 21.548970 Apple_10:6a:f5 (64:... 802.11 39 Clear-to-send, Flags=.....C
535 21.549039 54:dd:94:fb:fb:00 LLC 177 S, func=RNRR, N(R)=104; DSAP 0x2a Group, SSAP 0x16 Response
<
> Frame 534: 39 bytes on wire (312 bits), 39 bytes captured (312 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
v IEEE 802.11 Clear-to-send, Flags: .....C
  Type/Subtype: Clear-to-send (0x001c)
  v Frame Control Field: 0xc400
    .... ..00 = Version: 0
    .... 01.. = Type: Control frame (1)
    1100 .... = Subtype: 12
  v 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 0111 0010 = Duration: 114 microseconds
  Receiver address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
  Frame check sequence: 0xc7363dda [unverified]
  [FCS Status: Unverified]

```

Figure 16: Trama 534

```

533 21.548964 Apple_10:6a:f5 (64:... HitronTe_af:b1:98 (... 802.11 45 Request-to-send, Flags=.....C
534 21.548970 Apple_10:6a:f5 (64:... 802.11 39 Clear-to-send, Flags=.....C
<
> Frame 533: 45 bytes on wire (360 bits), 45 bytes captured (360 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
v IEEE 802.11 Request-to-send, Flags: .....C
  Type/Subtype: Request-to-send (0x001b)
  v Frame Control Field: 0xb400
    .... ..00 = Version: 0
    .... 01.. = Type: Control frame (1)
    1011 .... = Subtype: 11
  v 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 1001 1110 = Duration: 158 microseconds
  Receiver address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  Transmitter address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
  Frame check sequence: 0x7dc72f1c [unverified]
  [FCS Status: Unverified]

```

Figure 17: Trama 533

## 6 Conclusão

Este trabalho prático serviu de complemento às aulas teóricas e ajudou a consolidar a matéria lecionada nas mesmas.

Depois de finalizado o trabalho prático, relativo às Redes Wireless, obtivemos mais conhecimentos sobre o funcionamento ao nível da rede das redes wi-fi. Conceitos como, tipos e subtipos de tramas, STA, AP e direcionalidade de tramas foram recordados e aplicados. Além disso investimos mais tempo a compreender quais o funcionamento dos filtros no WireShark para encontrar diversas tramas, o que se revelou uma mais valia tendo em conta as perguntas onde foram úteis.

Desta forma, consideramos que os objetivos pretendidos pelo trabalho foram cumpridos.