



## **Trabalho Prático 4 - Redes sem Fios (Wi-Fi)**

### **Redes de Computadores**

---

#### **Grupo 7 - TP8**

Gabriela Santos Ferreira da Cunha - a97393

Nuno Guilherme Cruz Varela - a96455

Simão Jorge da Silva Costa - a95176

Descarregue da plataforma de ensino a captura *trace-wlan-tp4.pcap* e abra o ficheiro no Wireshark.

## 1 Acesso Rádio

Como pode ser observado, a sequência de bytes capturada inclui informação do nível físico (*radiotap header*, *radio information*), para além dos bytes correspondentes a tramas 802.11.

Selecione a trama de ordem XX correspondente ao seu identificador de grupo (TurnoGrupo, e.g., 11).

```
▶ Frame 87: 57 bytes on wire (456 bits), 57 bytes captured (456 bits)
▶ Radiotap Header v0, Length 25
▼ 802.11 radio information
  PHY type: 802.11g (ERP) (6)
  Short preamble: True
  Proprietary mode: None (0)
  Data rate: 6.0 Mb/s
  Channel: 12
  Frequency: 2467MHz
  Signal strength (dBm): -60dBm
  Noise level (dBm): -88dBm
  Signal/noise ratio (dB): 28dB
  TSF timestamp: 22936377
  [Duration: 68µs]
▶ IEEE 802.11 802.11 Block Ack, Flags: .....C
```

Figura 1: Trama de ordem 87.

**Exercício 1** Identifique em que frequência do espectro está a operar a rede sem fios, e o canal que corresponde essa frequência.

Através da figura 1, verificamos que o espetro está a operar a rede sem fios a uma frequência de 2467 Mhz e o canal é o 12.

**Exercício 2** Identifique a versão da norma IEEE 802.11 que está a ser usada.

A versão da norma IEEE 802.11 que está a ser usada é a 802.11g, contida no campo “PHY type”.

**Exercício 3** Qual o débito a que foi enviada a trama escolhida? Será que esse débito corresponde ao débito máximo a que a interface Wi-Fi pode operar? Justifique.

A trama escolhida foi enviada a 6 Mb/s, valor do campo “Data rate”. Uma vez que o débito máximo desta versão da norma IEEE 802.11 é 54 Mb/s, concluímos que o débito não corresponde ao débito máximo a que a interface Wi-Fi pode operar.

## 2 *Scanning* Passivo e *Scanning* Ativo

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

**Exercício 4** Selecione a trama *emphbeacon* de ordem (260 + XX). Esta trama pertence a que tipo de tramas 802.11? Indique o valor dos seus identificadores de tipo e de subtipo. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?

```
▶ Frame 347: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
▶ Radiotap Header v0, Length 25
▼ 802.11 radio information
  PHY type: 802.11g (ERP) (6)
  Short preamble: False
  Proprietary mode: None (0)
  Data rate: 1,0 Mb/s
  Channel: 12
  Frequency: 2467MHz
  Signal strength (dBm): -60dBm
  Noise level (dBm): -87dBm
  Signal/noise ratio (dB): 27dB
  TSF timestamp: 34033570
  ▶ [Duration: 2360µs]
▼ 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:b1:98 (bc:14:01:af:b1:98)
    Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    .... .... 0000 = Fragment number: 0
    1001 0011 1001 .... = Sequence number: 2361
    Frame check sequence: 0x55a094da [unverified]
    [FCS Status: Unverified]
▶ IEEE 802.11 Wireless Management
```

Figura 2: Trama de ordem 347.

Através da visualização da figura 2, podemos concluir que a trama é do tipo *Management Frame*(0) e o subtipo é 8 (*beacon*). Esta informação está presente no cabeçalho “Frame Control Field”.

**Exercício 5** Para a trama acima, identifique todos os endereços MAC em uso. Que conclui quanto à sua origem e destino?

Endereços MAC em uso:

- Receiver address : ff:ff:ff:ff:ff:ff
- Destination address : ff:ff:ff:ff:ff:ff
- Transmitter address : bc:14:01:af:b1:98
- Source address : bc:14:01:af:b1:98

Como o receiver address e o destination address são iguais, assim como o source address e o transmitter address, concluímos que o endereço origem é o Access Point que tem como endereço destino o broadcast, ou seja, a trama é enviada para todos os dispositivos dentro do *range* do Access Point.

**Exercício 6** Uma trama *beacon* anuncia que o AP pode suportar vários débitos de base, assim como vários débitos adicionais (*extended supported rates*). Indique quais são esses débitos?

```

▼ Fixed parameters (12 bytes)
  Timestamp: 1149684838906
  Beacon Interval: 0,102400 [Seconds]
  ► Capabilities Information: 0x0c31
▼ Tagged parameters (231 bytes)
  ► Tag: SSID parameter set: FlyingNet
  ▼ 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: Vendor Specific: Microsoft Corp.: WPS
  ► Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
  ► Tag: ERP Information
  ► Tag: HT Capabilities (802.11n D1.10)
  ► Tag: HT Information (802.11n D1.10)
  ► Tag: Extended Capabilities (1 octet)
  ► Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
  ► Tag: RSN Information

```

Figura 3: Trama de ordem 347.

Com base na figura 3, construímos a seguinte tabela com os débitos:

Débitos base	Débitos adicionais
1 Mb/s	6 Mb/s
2 Mb/s	12 Mb/s
5.5 Mb/s	24 Mb/s
11 Mb/s	48 Mb/s
9 Mb/s	
18 Mb/s	
36 Mb/s	
54 Mb/s	

Tabela 1: Débitos base e adicionais da trama.

**Exercício 7** Qual o intervalo de tempo previsto entre tramas *beacon* consecutivas (este valor é anunciado na própria trama *beacon*)? Na prática, a periodicidade de tramas *beacon* provenientes do mesmo AP é verificada com precisão? Justifique.

O intervalo de tempo previsto entre tramas *beacon* consecutivas é de 0.102400 segundos, como podemos verificar no campo “Beacon Interval“ da figura 3. Na prática, o valor não é exato, uma vez que o AP pode estar ocupado no momento em que tem de enviar a trama e deve-se também ao facto de neste tipo de ligação existir uma maior vulnerabilidade a interferências externas no sinal, o que pode alterar o momento em que o pacote é realmente recebido.

**Exercício 8** Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura? Explícite o modo como obteve essa informação (por exemplo, se usou algum filtro para o efeito).

No.	Time	Source	Destination	Protocol	Length	Info
1388	55.748911	Apple:18:6a:f5	Broadcast	802.11	155	Probe Request, SN=2516, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2488	70.149098	ea:84:64:7b:b9:7a	Broadcast	802.11	155	Probe Request, SN=2541, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
4455	82.621343	7c:ea:6d:ff:a2:cc	Broadcast	802.11	71	Probe Request, SN=62, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
4493	82.728818	7c:ea:6d:ff:a2:cc	Broadcast	802.11	71	Probe Request, SN=64, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
4494	82.728846	7c:ea:6d:ff:a2:cc	Broadcast	802.11	218	Probe Request, SN=65, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)

Figura 4: Filtro utilizado.

Os SSIDs dos APs que estão a operar na vizinhança da STA de captura são FlyingNet, NOS\_WIFI\_Fon e 2WIRE-PT-431. Para obter esta informação utilizamos o filtro “wlan.ssid” para mostrar todos os SSID’s e fomos acrescentando condições de modo a remover os AP’s repetidos.

**Exercício 9** Verifique se está a ser usado o método de deteção de erros (CRC).

Sugestão:

Use o filtro: `(wlan.fc.type_subtype == 0x08) && (wlan.fcs.status == bad)`.

Que conclui? Justifique o porquê de ser necessário usar deteção de erros em redes sem fios.

418	17.718278	HitronTe_af:b1:98	Apple_28:b8:0c	802.11	226 QoS Data, SN=14, FN=0, Flags=p....F..
521	21.532819	2c:4a:44:cd:08:bb	6b:fb:df:6a:...	LLC	146 I P, N(R)=84, N(S)=14; DSAP 0x70 Individual, SSAP 0xc2 Command
531	21.547114	Apple_10:6a:f5		802.11	177 QoS Data, SN=3920, FN=0, Flags=p.....T.
536	21.549039	54:cd:94:fb:fd:00		LLC	177 S, func=RWR, N(R)=104; DSAP 0x2a Group, SSAP 0x16 Response
537	21.549138	d6:9b:be:10:6a:f5	HitronTe_af:...	802.11	146 QoS Data, SN=1907, FN=0, Flags=p.....F..
554	21.592635	a6:f2:81:a5:dc:12	Apple_10:6a:...	802.11	146 QoS Data, SN=832, FN=0, Flags=p....F..
558	21.593823	d5:8c:22:3a:bc:96	Apple_10:6a:...	802.11	146 QoS Data, SN=833, FN=0, Flags=p....F..
570	21.616222	HitronTe_af:b1:96	Apple_10:6a:...	802.11	146 QoS Data, SN=836, FN=0, Flags=p....F..
622	23.452285	HitronTe_af:b1:96	Apple_10:6a:...	802.11	142 QoS Data, SN=838, FN=0, Flags=p....F..
623	23.452286	HitronTe_af:b1:96	Apple_10:6a:...	802.11	142 QoS Data, SN=839, FN=0, Flags=p....F..
720	27.138613	HitronTe_af:b1:96	Apple_10:6a:...	802.11	146 QoS Data, SN=842, FN=0, Flags=p....F..
988	38.198935	HitronTe_af:b1:96	Apple_10:6a:...	802.11	146 QoS Data, SN=844, FN=0, Flags=p....F..
1314	53.768339	HitronTe_af:b1:96	Apple_10:6a:...	802.11	146 QoS Data, SN=845, FN=0, Flags=p....F..
1451	57.499463	HitronTe_af:b1:96	Apple_10:6a:...	802.11	146 QoS Data, SN=846, FN=0, Flags=p....F..
1455	57.583561		Apple_10:6a:...	802.11	1564 QoS Data, SN=1852, FN=0, Flags=p....F..

Figura 5: Erros detetados.

▶	Frame 418: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)
▶	Radiotap Header v0, Length 25
▶	802.11 radio information
▼	IEEE 802.11 QoS Data, Flags: .p....F..
	Type/Subtype: QoS Data (0x0028)
▶	Frame Control Field: 0x8842
	.000 0000 0010 0100 = Duration: 36 microseconds
	Receiver address: Apple_28:b8:0c (68:a8:6d:28:b8:0c)
	Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
	Destination address: Apple_28:b8:0c (68:a8:6d:28:b8:0c)
	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_28:b8:0c (68:a8:6d:28:b8:0c)
	.... .... 0000 = Fragment number: 0
	0000 0000 1110 .... = Sequence number: 14
▼	Frame check sequence: 0x877d9204 incorrect, should be 0x16cc7220
	▶ [Expert Info (Error/Malformed): Bad checksum [should be 0x16cc7220]]
	[FCS Status: Bad]
	▶ QoS Control: 0x0000
	▶ CCMP parameters
▶	Data (163 bytes)

Figura 6: Dados relativos à trama 418.

Como podemos ver pela figura 5, nem todas as tramas *beacon* são recebidas corretamente e, pela figura 6, verificamos que o método de deteção de erros (CRC) está a ser usado, visto que no campo “FCS” encontramos uma mensagem de erro.

As redes sem fios são mais propícias a erros devido à possível presença de diversos objetos a atrapalhar a propagação do sinal, desde paredes até superfícies metálicas a refletir o sinal ou aparelhos a operar na mesma gama de frequências. Assim, a deteção de erros é utilizada com vista a detetar possíveis interferências na rede, bastante frequentes neste tipo de comunicação.

No *trace* disponibilizado foi também registado *scanning* ativo (envolvendo tramas *probe request* e *probe response*), comum nas redes Wi-Fi como alternativa ao *scanning* passivo.

**Exercício 10** Estabeleça um filtro Wireshark apropriado que lhe permita visualizar todas as tramas *probing request* ou *probing response*, simultaneamente.

O filtro estabelecido para visualizar as tramas indicadas foi o seguinte:

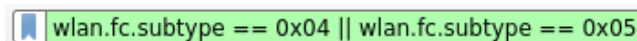


Figura 7: Filtro estabelecido.

**Exercício 11** Identifique um *probing request* para o qual tenha havido um *probing response*. Face ao endereçamento usado, indique a que sistemas são endereçadas estas tramas e explique qual o propósito das mesmas?

6193 94.190880	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6194 94.192895	HitronTe_af:b1:98	Apple_28:b8:...	802.11	411 Probe Response, SN=2474, FN=0, Flags=.....C, B1=100, SSID=FlyingNet
6195 94.192751	HitronTe_af:b1:98	Apple_28:b8:...	802.11	411 Probe Response, SN=2475, FN=0, Flags=.....C, B1=100, SSID=FlyingNet
6196 94.193504	HitronTe_af:b1:98	Apple_28:b8:...	802.11	411 Probe Response, SN=2476, FN=0, Flags=.....C, B1=100, SSID=FlyingNet

Figura 8: Tramas com o *probing request* e as respetivas *probing response*.

O sistema correspondente ao *probing request* é o Apple\_28:b8:0c e ao *probing response* é o HitronTe\_af:b1:98. A trama *probing request* é enviada pela STA (Apple\_28:b8:0c) para todos os equipamentos de rede no seu alcance (*active scanning*). A trama *probing response* é enviada pelo AP, neste caso o HitronTe\_af:b1:98, para assinalar a sua presença e enviar informação acerca de si em resposta ao *probing request*.

### 3 Processo de Associação

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

**Para a sequência de tramas capturada:**

**Exercício 12** Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.

```

4692 83.663250 7c:ea:6d:ff:a2:cc HitronTe_af: 802.11 59 Authentication, SN=67, FN=0, Flags=.....C
4693 83.663574 7c:ea:6d:ff:a2:cc HitronTe_af: 802.11 39 Acknowledgement, Flags=.....C
4694 83.663681 HitronTe_af:b1:98 7c:ea:6d:ff:a2:cc 59 Authentication, SN=2439, FN=0, Flags=.....C
4695 83.663750 HitronTe_af: 802.11 39 Acknowledgement, Flags=.....C
4696 83.665976 7c:ea:6d:ff:a2:cc HitronTe_af: 802.11 153 Association Request, SN=68, FN=0, Flags=.....C, SSID=FlyingNet
4697 83.666176 HitronTe_af:b1:98 7c:ea:6d:ff:a2:cc 39 Acknowledgement, Flags=.....C
4698 83.678873 HitronTe_af:b1:98 7c:ea:6d:ff:a2:cc 225 Association Response, SN=2440, FN=0, Flags=.....C
4699 83.688045 HitronTe_af:b1:98 7c:ea:6d:ff:a2:cc 225 Association Response, SN=2440, FN=0, Flags=.....C
4700 83.688364 HitronTe_af: 802.11 39 Acknowledgement, Flags=.....C

```

Figura 9: Tramas correspondentes a um processo de associação completo entre a STA e o AP.

**Exercício 13** Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo.

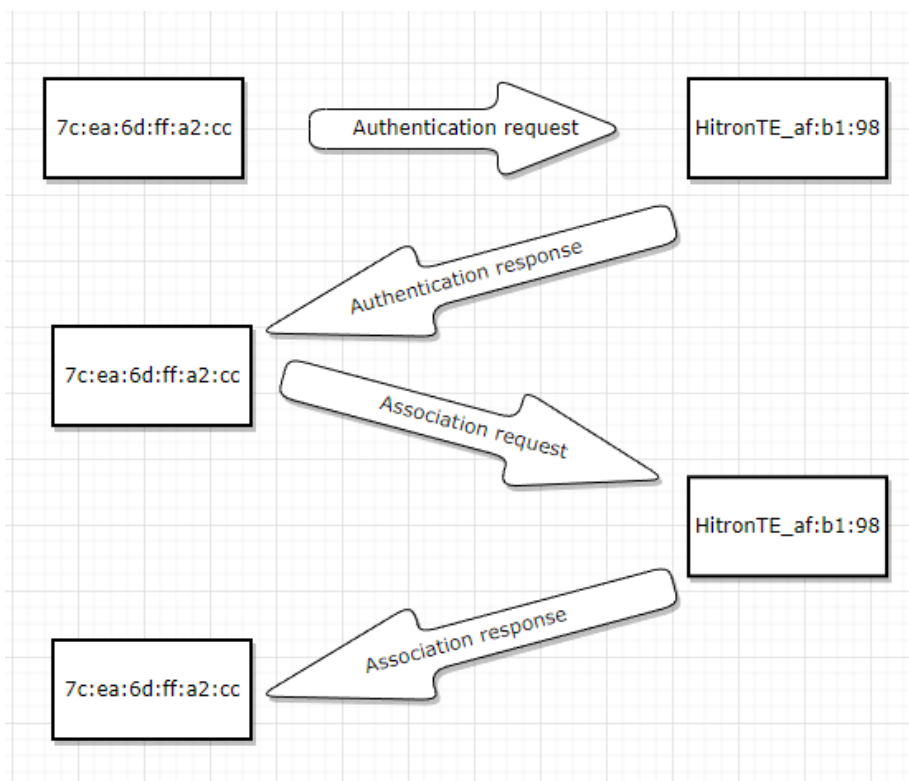


Figura 10: Diagrama de tramas trocadas.



## 4 Transferência de Dados

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

**Exercício 14** Considere a trama de dados nº431. Sabendo que o campo *Frame Control* contido no cabeçalho das tramas 802.11 permite especificar a direccionalidade das tramas, o que pode concluir face à direccionalidade dessa trama, será local à WLAN?

```
▶ Frame 431: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▶ IEEE 802.11 QoS Data, Flags: .p....F.C
  Type/Subtype: QoS Data (0x0028)
  ▶ Frame Control Field: 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
```

Figura 11: Campo *Frame Control* da trama de ordem 431.

A partir da figura 11, verificamos que a flag “To DS” tem o valor 0 e “From DS” tem o valor 1. Com isto, podemos concluir que a trama tem origem no sistema de distribuição e destino numa STA e, portanto, não será local à WLAN.

**Exercício 15** Para a trama de dados nº431, transcreva os endereços MAC em uso, identificando qual o endereço MAC correspondente ao *host* sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição?

```
▶ Frame 431: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▶ IEEE 802.11 QoS Data, Flags: .p....F.C
  Type/Subtype: QoS Data (0x0028)
  ▶ Frame Control Field: 0x8842
    .000 0000 0010 0100 = Duration: 36 microseconds
    Receiver address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Destination address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    STA address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    .... ..0000 = Fragment number: 0
    0011 0011 1110 .... = Sequence number: 830
    Frame check sequence: 0x793feef8 [correct]
    [FCS Status: Good]
    ▶ Qos Control: 0x0000
    ▶ CCMP parameters
  ▶ Data (163 bytes)
```

Figura 12: Endereços MAC da trama de ordem 431.

O endereço MAC correspondente ao *host* sem fios (STA) é 64:9a:be:10:6a:f5, ao AP é bc:14:01:af:b1:98 e ao router de acesso ao sistema de distribuição é bc:14:01:af:b1:98.

**Exercício 16** Como interpreta a trama nº433 face à sua direccionalidade e endereçamento MAC?

```

▶ Frame 433: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits)
▶ Radiotap Header v0, Length 25
▶ 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 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Transmitter address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    Destination address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Source address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    STA address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)

```

Figura 13: Dados da trama de ordem 433.

A partir da figura 13, verificamos que a flag “To DS” tem o valor 1 e a flag “From DS” tem valor 0, portanto a trama foi enviada por um dispositivo dentro da rede local para um dispositivo fora desta. Isto pode ser comprovado pelo endereçamento MAC obtido na figura 13.

**Exercício 17** Que subtipo de tramas de controlo são transmitidas ao longo da transferência de dados acima mencionada? Tente explicar porque razão têm de existir (contrariamente ao que acontece numa rede Ethernet.)

Ao longo da transferência de dados mencionada, as tramas de controlo são do subtipo ACK (*Acknowledgement*). Estas tramas são uma estratégia para detetar a presença de erros e confirmar a receção da trama. Na ausência de erros, a STA recetora envia uma trama ACK para a STA emissora. Se a STA emissora não receber um ACK num certo período de tempo, a trama de dados necessita de ser retransmitida. Isto acontece na rede sem fios, ao contrário de uma rede ethernet, visto que é mais propícia a erros.

**Exercício 18** O uso de tramas *Request To Send* e *Clear To Send*, apesar de opcional, é comum para efetuar "pré-reserva" do acesso ao meio quando se pretende enviar tramas de dados, com o intuito de reduzir o número de colisões resultante maioritariamente de STAs escondidas. Para o exemplo acima, verifique se está a ser usada a opção RTS/CTS na troca de dados entre a STA e o AP/Router da WLAN, identificando a direccionalidade das tramas e os sistemas envolvidos.

Dê um exemplo de uma transferência de dados em que é usada a opção RTC/CTS e um outro em que não é usada.

426 17.921853	HitronTe_af:b1:98 (bc:14:01:af:b1:98)	Apple_10:6a:f5 (64:9a:be:10:6a:f5)	802.11	39 Acknowledgement, Flags=.....C
427 17.922089	Apple_10:6a:f5 (64:9a:be:10:6a:f5)	HitronTe_af:b1:98 (bc:14:01:af:b1:98)	802.11	49 802.11 Block Ack Req, Flags=.....C
428 17.922099	Apple_10:6a:f5 (64:9a:be:10:6a:f5)	HitronTe_af:b1:98 (bc:14:01:af:b1:98)	802.11	57 802.11 Block Ack, Flags=.....C
429 17.922190	HitronTe_af:b1:98 (bc:14:01:af:b1:98)	Apple_10:6a:f5 (64:9a:be:10:6a:f5)	802.11	49 802.11 Block Ack Req, Flags=.....C
430 17.922271	Apple_10:6a:f5 (64:9a:be:10:6a:f5)	HitronTe_af:b1:98 (bc:14:01:af:b1:98)	802.11	57 802.11 Block Ack, Flags=.....C
431 17.922542	HitronTe_af:b1:98 (bc:14:01:af:b1:98)	Apple_10:6a:f5 (64:9a:be:10:6a:f5)	802.11	226 QoS Data, SN=830, FH=0, Flags=p....F.C
432 17.922558	Apple_10:6a:f5 (64:9a:be:10:6a:f5)	HitronTe_af:b1:98 (bc:14:01:af:b1:98)	802.11	39 Acknowledgement, Flags=.....C
433 17.923005	Apple_10:6a:f5 (64:9a:be:10:6a:f5)	HitronTe_af:b1:98 (bc:14:01:af:b1:98)	802.11	146 QoS Data, SN=830, FH=0, Flags=p....F.C
434 17.925296	Apple_28:b8:0c (08:00:27:00:00:00:28:b8:0c)	Apple_10:6a:f5 (64:9a:be:10:6a:f5)	802.11	39 Acknowledgement, Flags=.....C
435 17.927587	HitronTe_af:b1:98 (bc:14:01:af:b1:98)	Apple_28:b8:0c (08:00:27:00:00:00:28:b8:0c)	802.11	49 Null function (No data), SN=0, FH=0, Flags=.....T
436 17.927618	Apple_28:b8:0c (08:00:27:00:00:00:28:b8:0c)	HitronTe_af:b1:98 (bc:14:01:af:b1:98)	802.11	39 Acknowledgement, Flags=.....C

Figura 14: Exemplo da não utilização da opção RTS/CTS.

572 21.687311	HitronTe_af:b1:98 (bc:14:01:af:b1:98)	Apple_10:6a:f5 (64:9a:be:10:6a:f5)	802.11	45 Request-to-send, Flags=.....C
573 21.687325	HitronTe_af:b1:98 (bc:14:01:af:b1:98)	HitronTe_af:b1:98 (bc:14:01:af:b1:98)	802.11	39 Clear-to-send, Flags=.....C
574 21.687338	HitronTe_af:b1:98 (bc:14:01:af:b1:98)	Apple_10:6a:f5 (64:9a:be:10:6a:f5)	802.11	146 QoS Data, SN=837, FH=0, Flags=p....F.C

Figura 15: Exemplo da utilização da opção RTS/CTS.

▶	Frame 574: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits)
▶	Radiotap Header v0, Length 40
▶	802.11 radio information
▼	IEEE 802.11 QoS Data, Flags: .p....F.C
	Type/Subtype: QoS Data (0x0028)
▼	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
	.000 0000 0010 0100 = Duration: 36 microseconds
	Receiver address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
	Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
	Destination address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
	Source address: HitronTe_af:b1:96 (bc:14:01:af:b1:96)
	BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
	STA address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)

Figura 16: Informação da trama de exemplo da utilização da opção RTS/CTS.

Através da figura 15, verificamos que está a ser usada a opção RTS/CTS, visto que os *frames* 572 e 573 correspondem a tramas do tipo *Request To Send* e *Clear To Send*, respetivamente. Quanto à direcionalidade das tramas e sistemas envolvidos, concluímos a partir da figura 16 que a trama vem de um sistema distribuído para a STA.

## 5 Conclusão

A realização deste trabalho prático apresentou, pela primeira vez, o conceito da comunicação sem fios de um modo prático, onde pudemos explorar o protocolo IEEE 802.11.

Inicialmente, começamos por analisar as características das ondas rádio associadas às redes sem fios. Numa segunda parte, estudamos as diferenças entre *scanning passivo* e *scanning ativo*, estudando o endereçamento dos componentes envolvidos neste tipo de comunicação. Em seguida, foi estudado um processo de associação de um *host* e um AP, onde, previamente à transferência de dados, é necessário o envio de uma trama Association Request do *host* para o AP e uma Association Response como resposta do AP. Por último, estudamos o processo de transferência de dados e os protocolos inerentes.

De um modo geral, consideramos que tivemos um bom desempenho ao longo dos trabalhos práticos, uma vez que aprendemos a analisar capturas de diversos protocolos correspondentes a diferentes camadas protocolares e complementamos os nossos conhecimentos teóricos, assim como pretendido.