

---

## TP4: – Redes sem Fios (Wi-Fi)

---

TRABALHO REALIZADO POR:

BEATRIZ RIBEIRO MONTEIRO  
PEDRO PEREIRA SOUSA  
TELMO JOSÉ PEREIRA MACIEL



A95437  
Beatriz Monteiro



A95826  
Pedro Sousa



A96569  
Telmo Maciel

# Índice

<b>1 Acesso Rápido</b>	<b>1</b>
1.1 Pergunta 1 . . . . .	1
1.2 Pergunta 2 . . . . .	1
1.3 Pergunta 3 . . . . .	1
<b>2 Scanning Passivo e Scanning Ativo</b>	<b>2</b>
2.1 Pergunta 4 . . . . .	2
2.2 Pergunta 5 . . . . .	2
2.3 Pergunta 6 . . . . .	2
2.4 Pergunta 7 . . . . .	3
2.5 Pergunta 8 . . . . .	3
2.6 Pergunta 9 . . . . .	4
2.7 Pergunta 10 . . . . .	4
2.8 Pergunta 11 . . . . .	5
<b>3 Processo de Associação</b>	<b>6</b>
3.1 Pergunta 12 . . . . .	6
3.2 Pergunta 13 . . . . .	6
<b>4 Transferência de Dados</b>	<b>7</b>
4.1 Pergunta 14 . . . . .	7
4.2 Pergunta 15 . . . . .	7
4.3 Pergunta 16 . . . . .	8
4.4 Pergunta 17 . . . . .	9
4.5 Pergunta 18 . . . . .	9
<b>5 Conclusão</b>	<b>11</b>

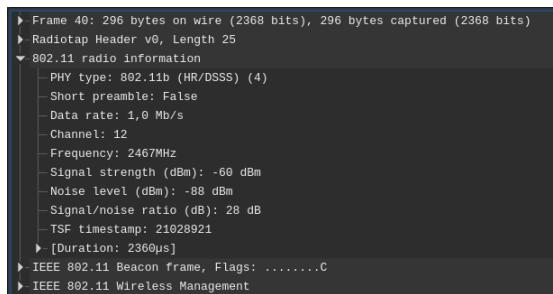
---

# 1 Acesso Rápido

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.

## 1.1 Pergunta 1

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



```
▶ Frame 40: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
▶ Radiotap Header v0, Length 25
▼ 802.11 radio information
    └─PHY type: 802.11b (HR/DSSS) (4)
        └─Short preamble: False
        └─Data rate: 1,0 Mb/s
        └─Channel: 12
        └─Frequency: 2467MHz
        └─Signal strength (dBm): -60 dBm
        └─Noise level (dBm): -88 dBm
        └─Signal/noise ratio (dB): 28 dB
        └─TSF timestamp: 21028921
        └─[Duration: 2360us]
    └─IEEE 802.11 Beacon frame, Flags: .....C
    └─IEEE 802.11 Wireless Management
```

Figure 1: Trama de ordem 40

A frequência do espetro que está a ser utilizada é 2467MHz, que corresponde ao canal 12, como é visivel na figura acima.

## 1.2 Pergunta 2

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

Como podemos ver na figura 1, a versão da norma a ser usada é 802.11b (HR/DSSS).

## 1.3 Pergunta 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.**

Como podemos ver na figura 1, a trama escolhida foi enviada a um débito de 1Mb/s. Este débito não corresponde ao máximo, dado que o máximo para a norma 802.11b é de 11Mb/s.

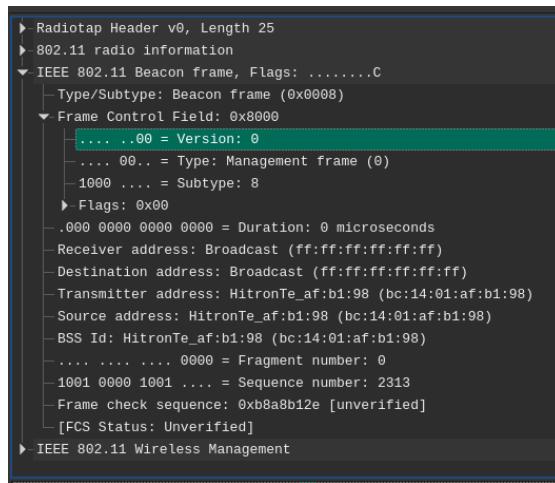
---

## 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(40).

### 2.1 Pergunta 4

Selecione a trama *beacon* de ordem 300 (260 + 40). 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)?



```
► 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
      .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 0000 1001 .... = Sequence number: 2313
      ► Frame check sequence: 0xb8a8b12e [unverified]
      [FCS Status: Unverified]
► IEEE 802.11 Wireless Management
```

Figure 2: Trama *beacon* de ordem 300

Como podemos verificar pela figura 2, esta trama pertence ao tipo 802.11b. O tipo é um *Management Frame* (00), e o subtipo é 8 (1000). Estes campos estão dentro do *frame control*.

### 2.2 Pergunta 5

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

Como podemos ver pela figura 2, tanto o *Source Address* como o *Transmittor Address* tem o seguinte *MAC Address*: bc:14:01:af:b1:98 enquanto o *MAC Address* do *Receiver Address* e do *Destination Address* é ff:ff:ff:ff:ff:ff.

O MAC Adress do *Receiver Address* e do *Destination Address* corresponde ao Broadcast, enquanto o do *Source Address* e o *Transmittor Address* correspondem ao HitronTe\_af:b1:98.

### 2.3 Pergunta 6

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

Como podemos ver pela figura 3, os débitos base são 1, 2, 5.5, 11, 9, 18, 36, 54 Mb/s, e os débitos adicionais são 6, 12, 24 e 48 Mb/s.

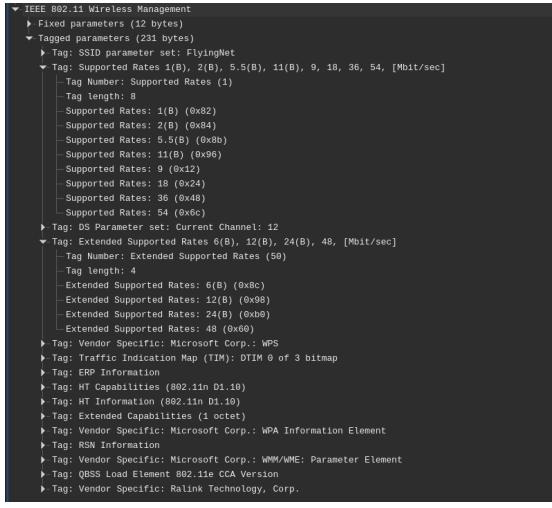


Figure 3: *Wireless Management - Extended Supported Rates e Supported Rates*

## 2.4 Pergunta 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.

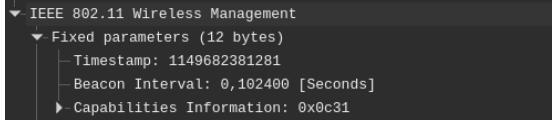


Figure 4: *Wireless Management - Fixed Parameters Trama 300*

O intervalo de tempo previsto entre tramas *beacon* consecutivas é 0.102400 segundos, como podemos ver pela figura 4.

No.	Time	Source	Destination	Protocol	Length	Info
298	11.673696	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2311, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
299	11.675316	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2312, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
300	11.776084	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2313, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Figure 5: Tramas 298 até 300

No entanto, na prática a periodicidade de tramas *beacon* provenientes do mesmo AP não é verificada com precisão, dado que se calcularmos o intervalo de tempo entre a trama 298 e 300, dá diferente (0.102388), mas bastante parecido.

## 2.5 Pergunta 8

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

Como podemos verificar pela figura 6, os SSIDs dos APs que estão a operar na vizinhança da STA de captura são *FlyingNet* e *NOS\_WIFI\_Fon*. Para obter os resultados, aplicamos o filtro visível na figura, e ordenamos por Source.

No.	Time	Source	Destination	Protocol	Length	Info
17440	131.379637	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=553, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17442	131.482028	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=555, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17454	131.584553	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=557, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17460	131.688857	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=559, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17462	131.789315	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=561, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17464	131.891685	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=563, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17466	131.994017	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=565, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17500	132.096556	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=567, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17502	132.198839	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=569, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17509	132.301343	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=571, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17511	132.403745	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=573, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17513	132.506037	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=575, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17515	132.608400	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=577, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17527	132.718857	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=579, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17529	132.813348	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=581, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17535	132.915741	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=583, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2	0.001662	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2084, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
4	0.104164	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2086, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
6	0.206582	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2088, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
8	0.308999	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2090, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
10	0.411376	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2092, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
12	0.513707	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2094, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
14	0.616191	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2096, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
29	0.718611	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2098, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
33	0.821009	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2100, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
35	0.923387	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2102, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
37	1.025663	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2104, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
39	1.128193	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2106, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
41	1.230650	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2108, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

Figure 6: Amostra

## 2.6 Pergunta 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.

Como é visível na figura que se segue, ao aplicarmos o filtro não foi apresentado qualquer tipo de erro.

(wlan.fc.type_subtype == 0x08) && (wlan.fcs.status == bad)						
No.	Time	Source	Destination	Protocol	Length	Info

Figure 7: Aplicação do filtro

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*.

## 2.7 Pergunta 10

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

Utilizamos o filtro " `(wlan.fc.type_subtype == 0x04) || (wlan.fc.type_subtype == 0x05)` " para visualizar as tramas probe request e probe response pois o subtype do probe request é 0x04 e do probe response é 0x05.

wlan.fc.type_subtype == 0x04    wlan.fc.type_subtype == 0x05						
No.	Time	Source	Destination	Protocol	Length	Info
1300	53.746911	Apple_10:6a:f5	Broadcast	802.11	155	Probe Request, SN=2516, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2467	70.147855	ea:a4:64:7b:b9:7a	Broadcast	802.11	167	Probe Request, SN=2540, FN=0, Flags=.....C, SSID=2WIRE-PT-431
2468	70.149098	ea:a4:64:7b:b9:7a	Broadcast	802.11	155	Probe Request, SN=2541, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2469	70.149792	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2332, FN=0, Flags=.....C, BI=100, SSID=flyingNet
2471	70.150537	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2333, FN=0, Flags=.....C, BI=100, SSID=flyingNet
2473	70.151237	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2334, FN=0, Flags=.....C, BI=100, SSID=flyingNet
2475	70.151709	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2335, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2477	70.152099	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2336, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2479	70.152570	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2337, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
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
2608	72.180590	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2347, FN=0, Flags=.....C, BI=100, SSID=flyingNet
2610	72.181275	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2348, FN=0, Flags=.....C, BI=100, SSID=flyingNet
2616	72.201570	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2565, FN=0, Flags=.....C, SSID=flyingNet
2617	72.202150	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2350, FN=0, Flags=.....C, BI=100, SSID=flyingNet
2619	72.202807	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2351, FN=0, Flags=.....C, BI=100, SSID=flyingNet
2621	72.203485	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2352, FN=0, Flags=.....C, BI=100, SSID=flyingNet
2650	72.488998	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2585, FN=0, Flags=.....C, SSID=flyingNet
2653	72.502553	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2586, FN=0, Flags=.....C, SSID=flyingNet
2677	72.568343	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2589, FN=0, Flags=.....C, SSID=flyingNet
2678	72.578258	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2590, FN=0, Flags=.....C, SSID=flyingNet
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	82.726818	7c:ea:6d:ff:a2:cc	Broadcast	802.11	71	Probe Request, SN=64, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
4494	82.730646	7c:ea:6d:ff:a2:cc	Broadcast	802.11	218	Probe Request, SN=66, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)

Figure 8: Filtro para visualizar as tramas probing request e probing response

## 2.8 Pergunta 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?

Na figura 9 podemos ver um probing request na trama 2603, que é emitida pela STA Apple 10:6a:f5 que emite um pedido de procura AP sendo emitido para todos os equipamentos da rede. A probing response chega-lhe pelo AP HitronTe af:b1:98 (trama 2606).

wlan.fc.type_subtype == 0x04    wlan.fc.type_subtype == 0x05						
No.	Time	Source	Destination	Protocol	Length	Info
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
2608	72.180590	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2347, FN=0, Flags=.....C, BI=100, SSID=flyingNet
2610	72.181275	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2348, FN=0, Flags=.....C, BI=100, SSID=flyingNet

Figure 9: Probe request e probe response

---

### 3 Processo de Associação

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

#### 3.1 Pergunta 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.**

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: Sequência de tramas com fase de autenticação

A figura 10 apresenta a sequência de tramas que corresponda a um processo de associação completo entre a STA Apple\_10:6a:f5 e o AP HitronTe\_af:b1:98, incluindo ainda a fase de autenticação.

#### 3.2 Pergunta 13

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

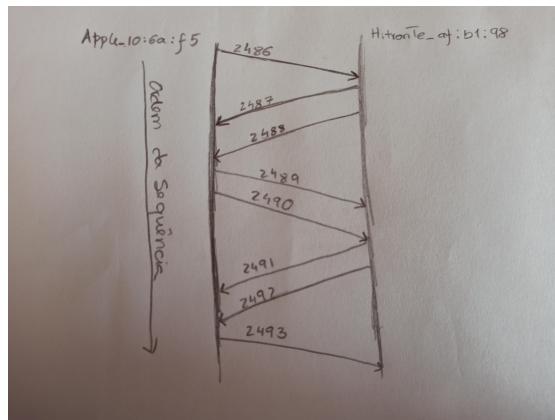


Figure 11: Diagrama que ilustra a sequência de todas as tramas trocadas

---

## 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.

### 4.1 Pergunta 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?

```
└─ 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.... .... = +HTC/Order flag: Not strictly ordered
```

Figure 12: *Frame Control* : Trama 431

Como é possível ver na figura 12 a flag *To DS* = 0 e a *From DS* = 1, permite-nos concluir que não se trata de um WLAN.

### 4.2 Pergunta 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?

Pela figura 13 podemos verificar que o endereço MAC do *host* sem fios (STA) é Apple\_10:6a:f5, o do AP é HitronTe\_af:b1:98 e o do *router* de acesso ao sistema de distribuição é HitronTe\_af:b1:98.

```

▶ 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 [unverified]
        └ [FCS Status: Unverified]
    ▶ Qos Control: 0x0000
    ▶ CCMP parameters
    ▶ Data (163 bytes)

```

Figure 13: Trama 431

### 4.3 Pergunta 16

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

Podemos ver que a trama 433 tem origem na STA e está a ser transmitida para fora da rede local uma vez que os valores das flags To DS é 1 e o From DS é 0.

O endereço MAC da STA é Apple\_10:6a:f5, do AP e do router é HitronTe\_af:b1:98.

```

> 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... .... = +HTC/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)
      .... .... 0000 = Fragment number: 0
      1110 0110 0000 .... = Sequence number: 3680
    Frame check sequence: 0x841b593c [unverified]
    [FCS Status: Unverified]
  > Qos Control: 0x0000
  > CCMP parameters
> Data (115 bytes)

```

Figure 14: Trama 433

#### 4.4 Pergunta 17

Que subtípido 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*.)

Como podemos ver na figura abaixo, no intervalo entre duas tramas QoS existe uma trama Acknowledgment. É necessário existir estas tramas de controlo pois nas redes wireless, ao contrário das redes Ethernet, a ocorrência de erros é bastante mais comum, sendo necessário estas para detetar a existência ou não de erros na transferência de dados na trama anterior.

431 17.922542	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	226 QoS Data, SN=830, FN=0, Flags=.p.....F.C
432 17.922558		HitronTe_af:b1:98	(... 802.11	39 Acknowledgement, Flags=.....C
433 17.924985	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	178 QoS Data, SN=3680, FN=0, Flags=.p.....TC

#### 4.5 Pergunta 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.

Através da figura abaixo podemos ver duas tramas, uma Request-to-send e outra Clear-to-send. Como as flags To DS e From DS estão ambas a 0, concluímos que as redes estão a operar localmente. Como podemos ver na figura, o STA envia um RTS para o AP da wlan e, em seguida, o AP envia um CTS para o STA. Posto isto, os únicos sistemas envolvidos são o STA (Apple\_10:6a:f5) e o AP (HitronTe\_af:b1:98).

```
15 0.631114      Apple_10:6a:f5 (64:... HitronTe_af:b1:98 (... 802.11      45 Request-to-send, Flags=....C
16 0.631128                      Apple_10:6a:f5 (64:... 802.11      39 Clear-to-send, Flags=....C
```

```
> Frame 15: 45 bytes on wire (360 bits), 45 bytes captured (360 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
-> IEEE 802.11 Request-to-send, Flags: ....C
    Type/Subtype: Request-to-send (0x001b)
    << Frame Control Field: 0xb400
        .... ..00 = Version: 0
        .... 01.. = Type: Control frame (1)
        1011 .... = Subtype: 11
    << Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0... .... = Protected flag: Data is not protected
        0.... .... = +HTC/Order flag: Not strictly ordered
        .000 0000 1101 0010 = Duration: 210 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: 0x168b49c0 [unverified]
    [FCS Status: Unverified]
```

Figure 15: Tramas Request-to-send e Clear-to-send e valores das flags da trama RTS

---

## 5 Conclusão

Neste trabalho melhoramos o nosso conhecimento sobre as redes sem fios, e aprendemos mais em específico sobre o protocolo 802.11.

Usando o wireshark, estudamos as conexões entre APs e STAs, analisando o envio de Beacon Frames, Probing requests e responses, e Request-to-Send e Clear-to-Send.

Para concluir, este trabalho permitiu-nos perceber melhor o comportamento dos dados transmitidos nas redes sem fios, aprofundando os nossos conhecimentos.