



UNIVERSIDADE DO MINHO

DEPARTAMENTO DE INFORMÁTICA

TP4: Redes Sem Fios
PL12 – Grupo 120

Francisco Peixoto (a84668) José Fernandes (a93163)
Henrique Parola (a93325)

Maio 2022

Conteúdo

1	Introdução	1
2	Questões e Respostas	2
3	Conclusão	12

1 Introdução

Este trabalho foi realizado no âmbito da disciplina de Redes de Computadores da Licenciatura em Engenharia Informática da universidade do Minho. O trabalho teve como objetivo explorar vários aspetos do protocolo IEEE 802.11, tais como informações físicas, o formato das tramas, o endereçamento dos componentes envolvidos na comunicação sem fios, os tipos de tramas mais comuns, métodos de contenção de canais, bem como a operação do protocolo.

2 Questões e Respostas

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

A frequência do espectro em que está a operar é 2467MHz, e a frequência corresponde ao canal 12.

```
Frame 120: 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): -65 dBm
  Noise level (dBm): -88 dBm
  Signal/noise ratio (dB): 23 dB
  TSF timestamp: 24305645
  [Duration: 2360µs]
IEEE 802.11 Beacon frame, Flags: .....C
IEEE 802.11 Wireless Management
```

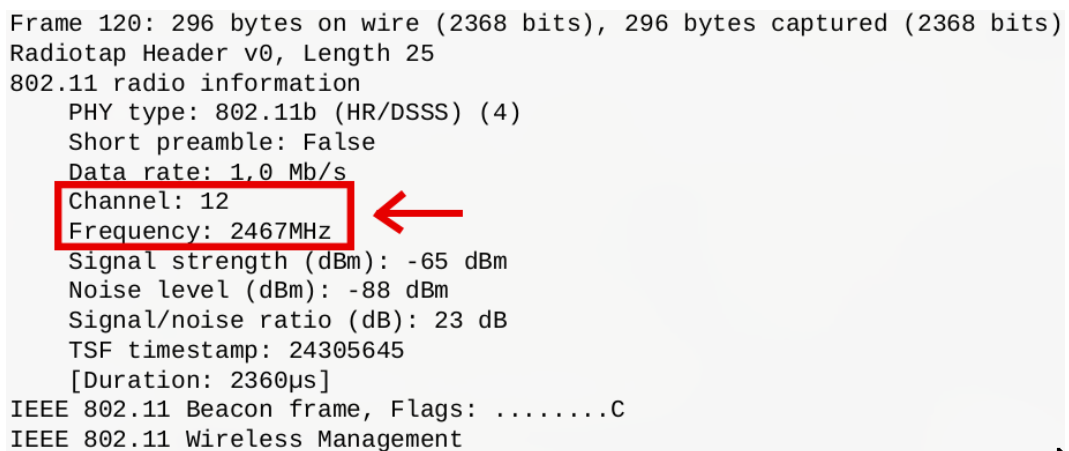


Figura 1: Frequência e canal capturados no Wireshark

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

A versão da norma utilizada é 802.11b.

```
Frame 120: 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)
```

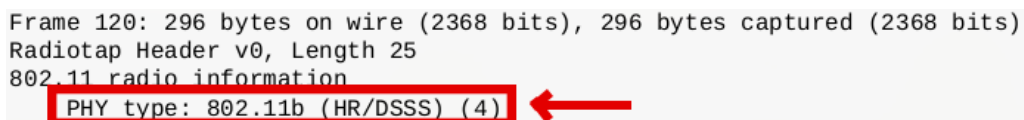


Figura 2: Versão da norma IEEE 802.11 capturada no Wireshark

3) 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 da trama enviada foi de 1Mb/s, este débito não corresponde ao débito máximo a que a interface WiFi pode operar, como demonstra a figura seguinte o débito máximo é de 11Mb/s, já que a norma utilizada é 802.11b [1].

```
Frame 120: 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
```

Figura 3: Débito enviado capturado no Wireshark

4) Selecione a trama beacon 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)?

A trama selecionada foi a trama 380, que como demonstra a figura seguinte é do tipo Management Frame. O tipo tem o identificador 00_2 e o subtipo tem o identificador 1000_2 que descreve que a trama capturada é uma trama *beacon*. Estão especificados no campo de Controlo de Frame.

```
Frame 380: 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
```

Figura 4: Informações da *trama beacon* capturada

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

- **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

Uma vez que está a ser transmitido uma trama Beacon, a origem desta trama será um AP e o destino será qualquer um dos *hosts* que estiverem no alcance do AP.

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?

Os débitos de base suportados são: 1, 2, 5.5, 11, 9, 18, 36, 54 (Mbit/sec). Os débitos adicionais suportados são: 6, 12, 24, 48 (Mbit/sec).

```
Frame 380: 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
IEEE 802.11 Wireless Management
  Fixed parameters (12 bytes)
  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: DS Parameter set: Current Channel: 12
    Tag: Extended Supported Rates 6(B), 12(B), 24(B), 48, [Mbit/sec]
```

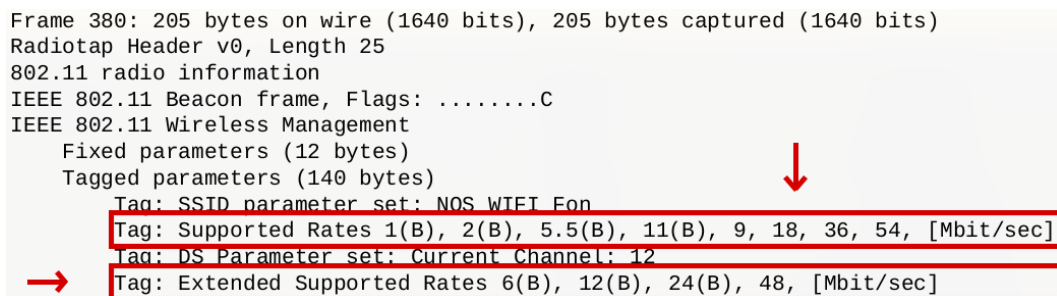


Figura 5: Débitos base e adicionais suportados pelo AP

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.

```
Frame 120: 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: 1149675110868
    Beacon Interval: 0,102400 [Seconds]
    Capabilities Information: 0x0c31
  Tagged parameters (231 bytes)
```

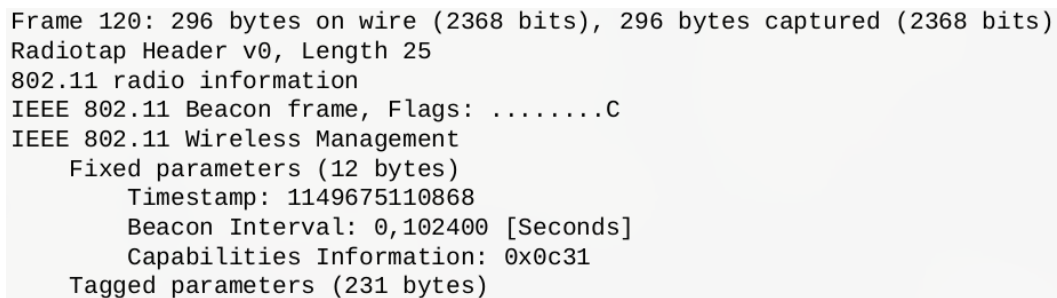


Figura 6: Informação intervalo de tramas beacon

O intervalo previsto entre tramas beacon consecutivas é de 0.1024 segundos. No entanto, na prática este valor varia uma vez que podem haver erros de transmissão. Desta forma na prática não se verifica esta periodicidade com esta precisão.

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).

Os SSIDs dos Aps que estão a operar na vizinha da STA de captura são:

- FlyingNet
- NOS_WIFI_Fon
- 2WIRE-PT-43

Para obter esta informação fez-se recurso à funcionalidade de WLAN Traffic que continha as estatísticas de tráfego wireless capturado. Nas estatísticas encontra-se 3 APs distintos.

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

Sugestão: Use o filtro:

(wlan.fcs.status == bad)

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

Existem vários registos com um valor FCS Status de Bad. Isto significa que está a ser um método de deteção de erros. É necessário a utilização de erros em redes sem fios devido à maior probabilidade de erros devido a colisões no meio.

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

O filtro estabelecido foi:

(wlan.fc.type == 0x00 && (wlan.fc.subtype == 0x05 || wlan.fc.subtype == 0x04))

A partir da tabela em anexo do enunciado é possível reparar que o tipo das duas tramas tem o valor 00₂ e subtipo 0101₂ para Probe response e 0100₂ para Probe request.

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?

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 70.149998	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:b1:99	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:b1:99	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:b1:99	ea:a4:64:7b:b9:7a	802.11	201 Probe Response, SN=2337, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2603 72.170215	Apple_10:6a:f5	Broadcast	802.11	164 Probe Request, SN=2503, FN=0, Flags=.....C, SSID=FlyingNet
2686 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

Figura 7: *probing request* e *probing response*

O primeiro registo a azul representa o *probe request* enviado pela estação "Apple_10 : 6a : f5" para todos os APs da rede. O segundo representa um *probe response* do AP com o SSID "FlyingNet" para a estação "Apple_10:6a:f5". A resposta é ao primeiro registo azul uma vez que para enviar um novo *probe request* foi necessário esperar um tempo máximo para *probe responses* (MaxChannelTime). Assim exclui-se o facto de o segundo registo azul ser a resposta ao registo que se encontra no topo da lista de registos.

Estas tramas são endereçadas a todos os APs da rede que se encontram no alcance da estação que enviou o pedido. Estas tramas são usadas para obter informação sobre as capacidades dos APs dentro do alcance da estação.

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
2488 70.381869	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59 Authentication, SN=2338, FN=0, 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
2492 70.389339	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	225 Association Response, SN=2339, FN=0, Flags=.....C

Figura 8: Sequência de tramas

Para se obter estes resultados utilizou-se o filtro:

$$(wlan.fc.type == 0x0 \ (wlan.fc.subtype == 0x01 \ || \ wlan.fc.subtype == 0x0 \ || \ wlan.fc.subtype == 0xb))$$

Na figura acima pode-se verificar uma autenticação de sistema aberto. Em que a estação "Apple_10:6a:f5" envia uma trama de Authentication para o AP e o AP processa esta trama e devolve uma trama de autenticação como resposta. De seguida, com a autenticação concluída, segue uma trama de Association Request por parte da estação para o AP e uma Association response pelo AP para a estação.

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

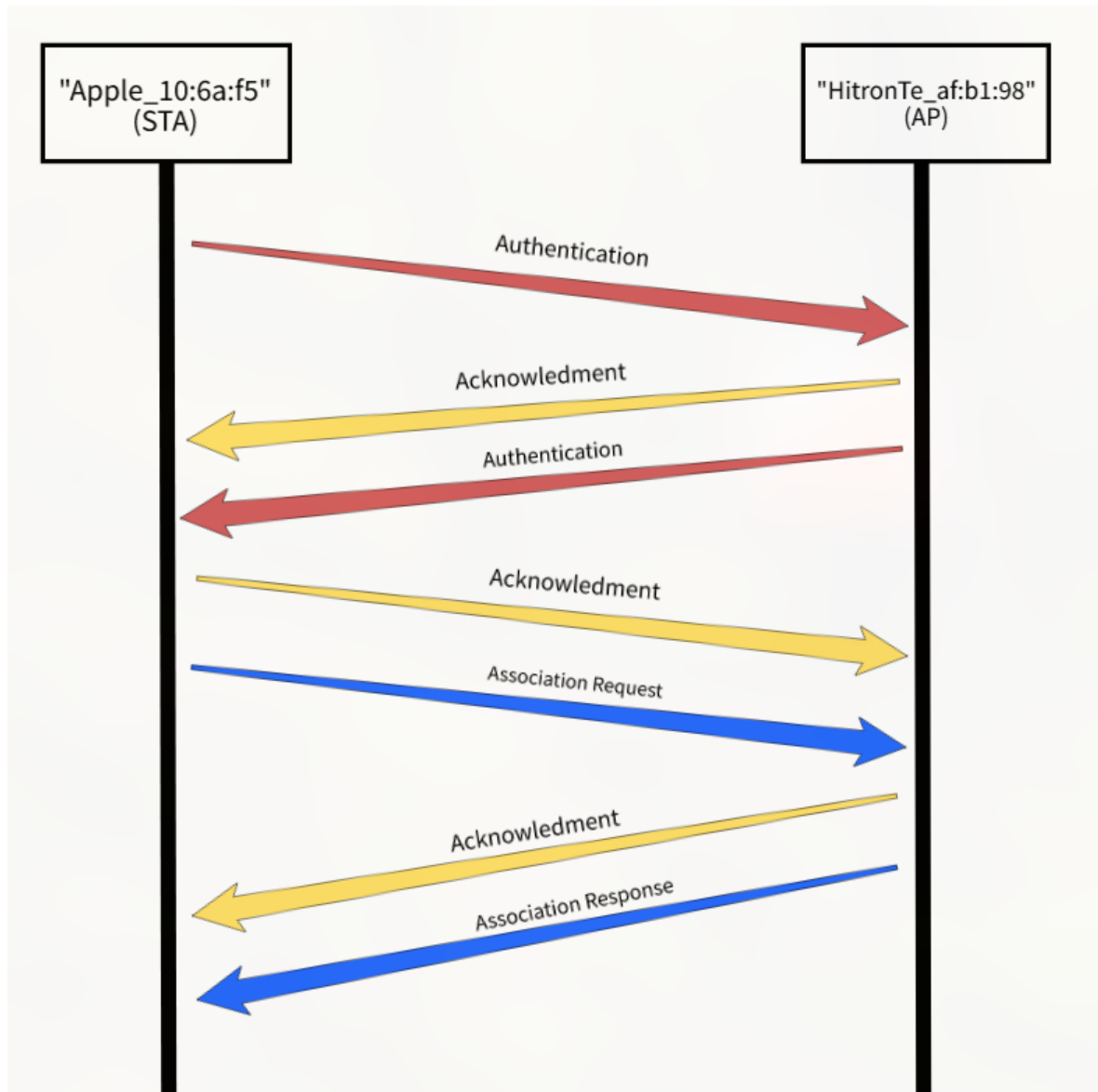


Figura 9: Diagrama com a sequência de tramas (2486 até 2493)

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?

```
No.      Time      Source      Destination      Protocol Length Info
  431  17.922542  HitronTe_af:b1:98  Apple_10:6a:f5    802.11    226    QoS Data, SN=830, FN=0, Flags=.p....F.C
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)
```

Figura 10: Informação trama de dados número 431

A partir do campo Frame Control podemos saber que a trama vem de um DS para uma estação por via de um AP. Uma vez que a flag From DS tem valor 1 e To DS 0. Uma vez que a trama veio de um DS pode-se concluir que a trama não é local à WLAN.

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?

```
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)
```

Figura 11: Informação trama de dados número 433

- Endereço STA: 64:9a:be:10:6a:f5
- Endereço Transmitter (AP): bc:14:01:af:b1:98
- Router de acesso ao sistema de distribuição: bc:14:01:af:b1:98

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

A trama nº433 tem uma direcção contrária à trama nº 431. Esta tem uma direcção da estação para o DS, passando pelo um AP, uma vez que a flag To DS tem valor 1 e From DS 0, algo que se pode verificar a partir da tabela dos anexos

No.	Time	Source	Destination	Protocol	Length	Info
433	17.924985	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	178	QoS Data, SN=3680, FN=0, Flags=.p....TC

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)

Figura 12: Informação trama de dados número 433

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 transmissão foram utilizados 3 tipos de tramas de controlo. Nomeadamente:

- Request to Send (RTS)
- Clear to Send (CTS)
- Acknowledgement (ACK)

No.	Time	Source	Destination	Protocol	Length	Info
162	6.653376	Apple_10:6a:f5 (64:9a:be:10:6a:f5)	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (RA)	802.11	45	Request-to-send, Flags=.....C

Frame 162: 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

Figura 13: Informação trama de Controlo RTS número 162

No.	Time	Source	Destination	Protocol	Length	Info
163	6.653389	Apple_10:6a:f5 (64:9a:be:10:6a:f5)	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (RA)	802.11	39	Clear-to-send, Flags=.....C

Frame 163: 39 bytes on wire (312 bits), 39 bytes captured (312 bits)
 Radiotap Header v0, Length 25
 802.11 radio information
 IEEE 802.11 Clear-to-send, Flags:C
 Type/Subtype: Clear-to-send (0x001c)
 Frame Control Field: 0xc400
 00 = Version: 0
 01.. = Type: Control frame (1)
 1100 = Subtype: 12

Figura 14: Informação trama de Controlo CTS número 163

No.	Time	Source	Destination	Protocol	Length	Info
434	17.925298	Apple_10:6a:f5 (64:9a:be:10:6a:f5)	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (RA)	802.11	39	Acknowledgement, Flags=.....C

Frame 434: 39 bytes on wire (312 bits), 39 bytes captured (312 bits)
 Radiotap Header v0, Length 25
 802.11 radio information
 IEEE 802.11 Acknowledgement, Flags:C
 Type/Subtype: Acknowledgement (0x001d)
 Frame Control Field: 0xd400
 00 = Version: 0
 01.. = Type: Control frame (1)
 1101 = Subtype: 13

Figura 15: Informação trama de Controlo Acknowledgement número 434

A utilização destas tramas deve-se à partilha do meio por parte de vários dispositivos e também a uma maior suscetibilidade para erros por parte da tecnologia a ser usada no

meio físico. Algo que não se verifica numa rede Ethernet, que costuma ser organizada com dispositivos ligados com apenas uma ligação de Ethernet por dispositivo (à exceção de hubs e switches) e cuja ocorrência de erros é muito reduzida. Para mitigar colisões, faz-se recurso a tramas de controlo para tentar garantir que para quantidades grandes de dados não há vários dispositivos a enviar dados ao mesmo tempo, uma vez que o sensing pode não ser suficiente dado a nodos escondidos.

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 RTS/CTS e um outro em que não é usada

```
No.      Time      Source      Destination      Protocol Length Info
 1441  57.451328  Apple_10:6a:f5 (64:9a:be:10:6a:f5) (TA) HitronTe_af:b1:98 (bc:14:01:af:b1:98) (RA) 802.11  45  Request-to-
send, Flags=.....C
Frame 1441: 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
.... 0000 = Version: 0
.... 01.. = Type: Control frame (1)
1011 .... = Subtype: 11
Flags: 0x00
.... 0000 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
```

Figura 16: Informação trama Controlo RTS número 1441

```
No.      Time      Source      Destination      Protocol Length Info
 1442  57.451335  Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA) 802.11  39  Clear-to-send, Flags=.....C
Frame 1442: 39 bytes on wire (312 bits), 39 bytes captured (312 bits)
Radiotap Header v0, Length 25
802.11 radio information
IEEE 802.11 Clear-to-send, Flags: .....C
Type/Subtype: Clear-to-send (0x001c)
Frame Control Field: 0xc400
.... 0000 = Version: 0
.... 01.. = Type: Control frame (1)
1100 .... = Subtype: 12
Flags: 0x00
.... 0000 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
```

Figura 17: Informação trama Controlo CTS número 1442

No.	Time	Source	Destination	Protocol	Length	Info
1443	57.451401	Apple_10:6a:f5	HitronTe_af:b1:96	802.11	146	QoS Data, SN=3692, FN=0, Flags=.p....TC

Frame 1443: 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....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_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:b1:96 (bc:14:01:af:b1:96)
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 18: Informação trama de dados número 1443

Na sequência das imagens acima pode-se reparar numa sequência de pacotes de RTS/CTS seguidos de uma trama de dados. A trama RTS (nº 1441) tem direção da STA até ao AP. A trama CTS (nº 1442) tem direção do AP para a STA. Estas duas interações foram feitas localmente na WLAN. Por outro lado, a trama de dados (nº 1443) tem direção da STA para o DS com passagem no AP. Pode-se salientar, no entanto, que geralmente é utilizado a "pré-reserva" do meio para quantidades grandes de dados. Algo que não se verificou neste exemplo, uma vez que, pela flag de tipo 10₂ e subtipo da trama com flag 1000₂ se conclui que se trata de uma trama reservada, neste caso associada a Quality of Service (QoS). Como se pode verificar pelo tamanho da trama, esta é pequena comparada com uma trama de beacon, que é enviada sem reservar o meio.

No.	Time	Source	Destination	Protocol	Length	Info
120	4.505605	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2171, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Frame 120: 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
Type/Subtype: Beacon frame (0x0008)
Frame Control Field: 0x8000
....00 = Version: 0
....00.. = Type: Management frame (0)
1000.... = Subtype: 8

Figura 19: Informação trama de Beacon número 120

115	4.200168	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2166, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
116	4.300945	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2167, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
117	4.302574	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2168, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
118	4.403343	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2169, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
119	4.404989	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2170, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
120	4.505605	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2171, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
121	4.507225	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2172, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
122	4.608149	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2173, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
123	4.609774	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2174, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
124	4.710550	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2175, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
125	4.712101	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2176, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

Figura 20: Sequência de tramas de Beacon (120-125)

Pelas imagens acima podemos identificar um exemplo onde não é usada a opção RTS/CTS. Na segunda imagem podemos confirmar que de facto não foram enviadas tramas de controlo antes da trama Beacon (nº 120).

3 Conclusão

Este trabalho foi importante para um conhecimento mais profundo do protocolo 802.11 de redes Wireless. Foi nos possível descobrir de forma prática o nível físico da norma IEEE 802.11. Como as informações relativas ao canal a ser utilizado e frequência da onda a ser usada, como também o débito de informação que está a ser usado.

Numa segunda parte, foi nos possível familiarizar e discutir sobre a informação enviada em Beacon frames, assim como a informação que estes transportam.

Numa terceira parte, deu-se especial atenção ao controlo de erros e compreendeu-se que são uma componente muito importante deste protocolo.

Numa quarta parte, fomos capazes de percorrer o caminho que uma estação faz de modo a conseguir entrar numa rede WLAN. Foi possível perceber como as estações conseguem fazer um scanning dos APs à sua volta (scanning ativo), ou como os APs periodicamente enviam informação sobre as suas características para as estações (scanning passivo). De seguida com essa informação as estações poderiam se autenticar, apenas se verificou uma autenticação de sistema aberto. De seguida a estação podia pedir para se associar ao AP e finalmente pertencer à rede WLAN.

Numa quinta parte, deu-se importância a compreender como é possível detetar o tráfego que tem destino em DS e tráfego que provém de DSs. Foi ainda possível identificar o caso especial em que um AP faz parte de um DS sendo também um router.

Por fim, focou-se na aprendizagem de como são implementados na prática métodos de contenção, nomeadamente o uso de RTS e CTS. Algo que se reparou que nem sempre são utilizados e podem ser utilizados até para dados que contém pouca informação que foi algo que não se estava à espera.

Referências

- [1] Tutorialspoint, *What are the IEEE 802.11 Wireless LAN Standards?*, <https://www.tutorialspoint.com/what-are-the-ieee-802-11-wireless-lan-standards#:~:text=IEEE>