



Universidade do Minho
Escola de Engenharia

Redes de Computadores

Trabalho Prático 4

Francisco Correia Franco A89458
António Jorge Nande Rodrigues A89585
Luís Enes Sousa A89597



A89458



A89585



A89597

Conteúdo

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

1 Acesso Rádio

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

Para a trama correspondente 352:

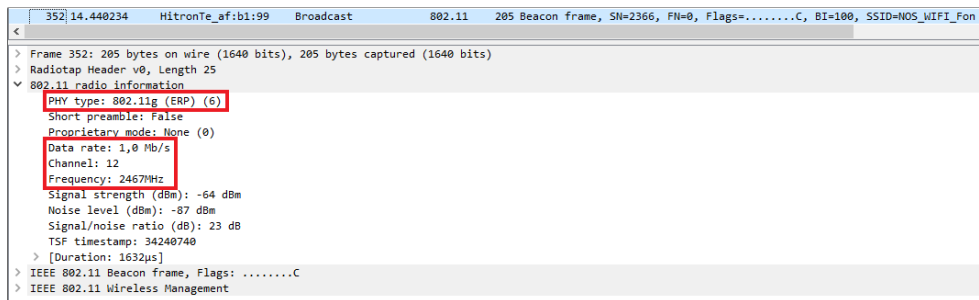


Figura 1: Trama 352

1.1 Pergunta 1

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

A rede sem fios está a operar na frequência 2467 MHz, correspondente ao canal 12.

1.2 Pergunta 2

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

A versão que está a ser usada é a 802.11g.

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 WiFi pode operar? Justifique.

A trama foi enviada a um débito de 1 Mb/s.

Ese débito não corresponde ao débito máximo a que a interface WiFi pode operar, pois esta suporta um débito de até 54 Mb/s.

2 Scanning Passivo e Scanning Ativo

Como referido, as tramas beacon permitem efetuar scanning passivo em redes IEEE 802.11 (WiFi). Para a captura de tramas disponibilizada, responda às seguintes questões:

2.1 Pergunta 4

Selecione uma trama beacon (e.g., trama 1052). 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)?

As tramas Beacon pertencem ao tipo de tramas de Gestão (Management frames). Os valores dos seus identificadores de tipo e de subtipo são, respetivamente, 0 e 8.

Estes identificadores estão especificados no byte 0x19 do cabeçalho. Mais especificamente, o identificador de subtipo encontra-se nos 4 bits mais significativos e o de tipo nos 2 bits seguintes.

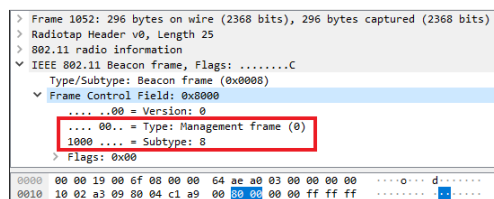


Figura 2: Tipo e subtipo da trama 1052

2.2 Pergunta 5

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

Estão em uso 3 endereços MAC: recetor ou destino (ff:ff:ff:ff:ff:ff - Broadcast), transmissor ou origem (bc:14:01:af:b1:98 - HitronTe_af:b1:98) e BSS Id (bc:14:01:af:b1:98 - HitronTe_af:b1:98).

Concluimos que a trama teve origem no dispositivo bc:14:01:af:b1:98 (HitronTe_af:b1:98) e destino nos vários dispositivos ligados à rede.

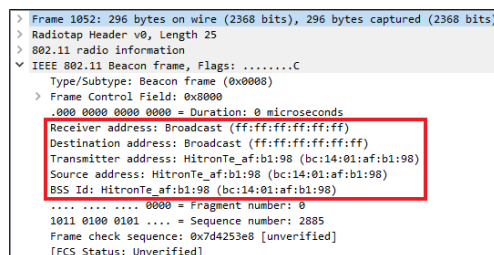


Figura 3: Endereços MAC na trama 1052

2.3 Pergunta 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 e 54 Mb/s.

Os débitos adicionais suportados são 6, 12, 24, 48 Mb/s.

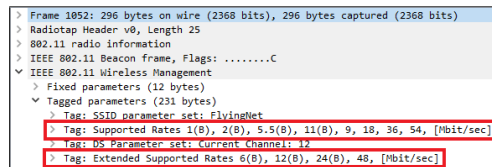


Figura 4: Débitos de base e adicionais da trama 1052

2.4 Pergunta 7

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 previsto entre tramas beacon consecutivas é 0.1024 segundos.

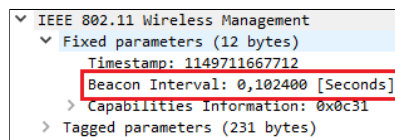


Figura 5: Intervalo de tempo previsto entre duas tramas Beacon

Na prática, a periodicidade não se verifica, embora seja por meras frações de segundo. Isto pode dever-se ao facto de existir tráfego associado ao Access Point. No exemplo da figura seguinte os intervalos observados são 0,102314 e 0,102538 segundos.

No.	Time	Source	Destination	Protocol	Length	Info
1052	41.062640	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2885, FN=0, Flags=.....C, BI=100, SSID=FlyingMet
1053	41.064241	HitronTe_af:b1:99	Broadcast	802.11	285	Beacon frame, SN=2886, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1054	41.164954	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2887, FN=0, Flags=.....C, BI=100, SSID=FlyingMet
1055	41.166591	HitronTe_af:b1:99	Broadcast	802.11	285	Beacon frame, SN=2888, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1056	41.267492	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2889, FN=0, Flags=.....C, BI=100, SSID=FlyingMet

Figura 6: Intervalo de tempo prático entre três tramas Beacon

2.5 Pergunta 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).

Pela observação de algumas tramas Beacon consecutivas, verificamos que existe um padrão de alternância entre dois APs. Isto significa que estão a operar dois APs na vizinhança da STA de captura, sendo os seus SSIDs 'FlyingNet' e 'NOS_WIFI_Fon'.

1052	41.062640	HitronTe_af:b1:98	Broadcast	802.11	296 Beacon frame, SN=2885, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1053	41.064241	HitronTe_af:b1:99	Broadcast	802.11	205 Beacon frame, SN=2886, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1054	41.164954	HitronTe_af:b1:98	Broadcast	802.11	296 Beacon frame, SN=2887, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1055	41.166591	HitronTe_af:b1:99	Broadcast	802.11	205 Beacon frame, SN=2888, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

Figura 7: SSIDs dos APs na vizinhança da STA de captura

2.6 Pergunta 9

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

Na figura seguinte verificamos que está presente um campo FCS na trama 1052. Isto significa que está a ser usado um método de deteção de erros.

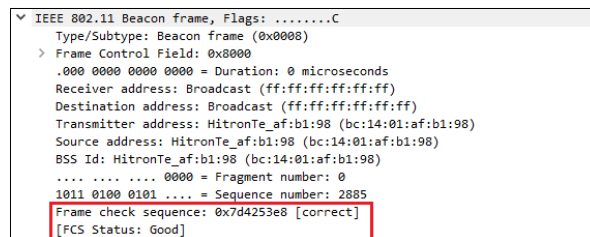


Figura 8: Campo FCS (Frame Check Sequence) na trama 1052

Através do uso do filtro '(wlan.fc.type_subtype == 0x08) && (wlan.fcs.status == bad)' conseguimos verificar que houve erros no envio de algumas tramas Beacon. Isto confirma a necessidade de usar deteção de erros em redes sem fios, pois estas são muito menos estáveis que, por exemplo, redes Ethernet.

No.	Time	Source	Destination	Protocol	Length	Info
6274	94.779008	36:00:a0:51:f4:19	43:46:86:ca:97:53	802.11	146	Beacon frame, SN=236, FN=9, Flags=..pPm..T.
6937	99.991379	be:05:24:9b:d6:a1	0e:8b: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:d7:53	802.11	146	Beacon frame, SN=3658, FN=10, Flags=..pPm..T.
7131	100.390016	62:4c:de:c5:a9:3a	34:c4:ca:22:ed:14	802.11	146	Beacon frame, SN=2211, FN=0, Flags=..pPm..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.

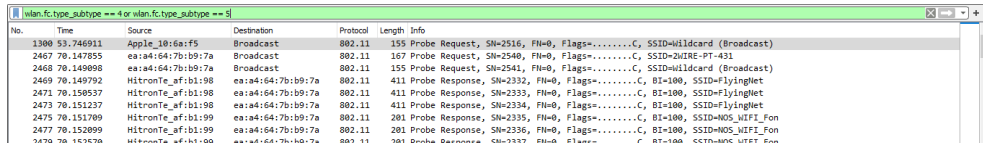
Figura 9: Filtro para detetar tramas Beacon com erros

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.

O filtro 'wlan.fc.type_subtype == 4 or wlan.fc.type_subtype == 5' limita as tramas apresentadas àquelas cujo subtipo é igual a 4 ou 5 (probing request ou probing response, respetivamente).



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=WiRE-PT-431
2468	70.149898	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	70.150837	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	70.151789	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2335, FN=0, Flags=.....C, BI=100, SSID=MOS_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=MOS_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=MOS_WIFI_Fon

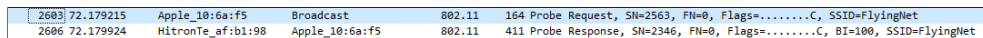
Figura 10: Filtro estabelecido no Wireshark

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?

A trama de probing request é enviada por uma STA (Apple_10:6a:f5) para todos os APs nas proximidades (Broadcast). Esta trama é enviada quando a STA quer localizar todos os APs perto de si.

A trama de probing response é enviada por um AP (HitronTe_af:b1:98) para a STA que enviou o probing request (Apple_10:6a:f5). Esta trama serve para informar a STA que este AP está disponível.



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

Figura 11: Probing request e respetivo probing response

3 Processo de Associação

Numa rede WiFi 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:

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.

Nas quatro primeiras tramas, encontramos as tramas de autenticação de ambas as partes. De seguida, temos a trama de pedido de associação ao AP. Por fim, temos a trama de resposta ao pedido de associação. De notar que todas as tramas neste processo são seguidas de uma trama de Acknowledgement, que informa o último remetente que a trama foi recebida.

Na figura seguinte podemos observar um processo de associação completo entre a STA e o AP.

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 (64:9a...	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 (bc...	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 (64:9a...	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 (bc...	802.11	39 Acknowledgement, Flags=.....C

Figura 12: Processo de associação completo

3.2 Pergunta 13

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

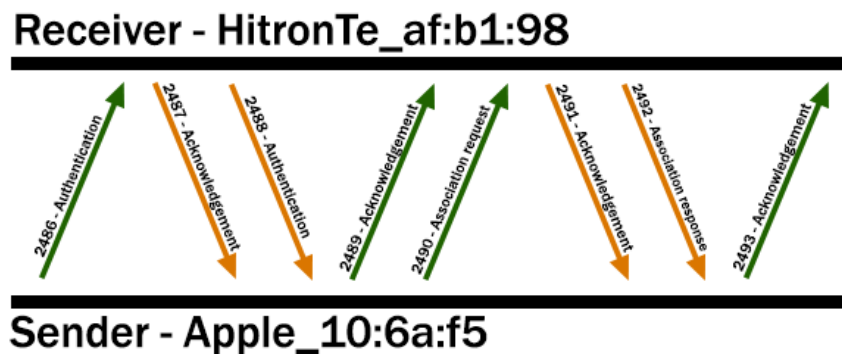


Figura 13: Diagrama representativo do processo de associação completo

4 Transferência de Dados

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

4.1 Pergunta 14

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?

Como podemos ver na figura seguinte, a trama vem do Sistema de Distribuição, logo não será local à WLAN.

```
> Frame 455: 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... .... = +HTC/Order flag: Not strictly ordered
```

Figura 14: Valor das flags DS no campo Frame Control da trama 455

4.2 Pergunta 15

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 à STA é Apple_71:41:a1, ao AP é HitronTe_af:b1:98 e ao router de acesso ao sistema de distribuição é HitronTe_af:b1:98.

```
> Frame 455: 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_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)
```

Figura 15: Endereços MAC da trama 455

4.3 Pergunta 16

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

A trama 457 tem origem na STA e vai em direção ao Sistema de Distribuição, através de um AP, ou seja, para fora da WLAN.

O endereço MAC da STA é Apple_71:41:a1, do AP é HitronTe_af:b1:98 e do router é HitronTe_af:b1:98.

```
> Frame 457: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on 0
> 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_71:41:a1 (d8:a2:5e:71:41:a1)
        Destination address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
```

Figura 16: Endereços MAC e Flags DS da trama 457

4.4 Pergunta 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.)

As tramas de controlo que são transmitidas ao longo do tempo são as tramas de Acknowledgement. Estas são enviadas sempre que o recetor de uma trama de dados não detetar erros na transmissão, de forma a informar o transmissor que a trama foi enviada com sucesso. Caso o transmissor original não receba esta trama de Acknowledgement num certo intervalo de tempo, este reenvia a trama.

As tramas Acknowledgement são necessárias, pois as redes sem fios são muito mais instáveis e sujeitas a ruído do que as redes Ethernet.

455	18.536644	HitronTe_af:b1:98	Apple_71:41:a1	802.11	226 QoS Data, SN=276, FN=0, Flags=.p....F.C
456	18.536653		HitronTe_af:b1:98 (bc:14:01:af:b1:98)	802.11	39 Acknowledgement, Flags=.....C
457	18.539762	Apple_71:41:a1	HitronTe_af:b1:98	802.11	178 QoS Data, SN=1209, FN=0, Flags=.p.....TC
458	18.540043		Apple_71:41:a1 (d8:a2:5e:71:41:a1)	802.11	39 Acknowledgement, Flags=.....C

Figura 17: Exemplo de tramas de dados intercaladas de tramas de controlo

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.

Como podemos ver na figura seguinte, está a ser usada a opção RTS/CTS.

Quanto à direccionalidade das tramas, estas estão a operar localmente à WLAN, pois as flags 'To DS' e 'From DS' estão ambas a 0. Sendo assim, os sistemas envolvidos são apenas a STA (Apple_71:41:a1) e o AP/Router (HitronTe_af:b1:98).

519	21.531991	Apple_10:6a:f5 (64:...	HitronTe_af:b1:98 (bc...	802.11	45 Request-to-send, Flags=.....C
520	21.532004	Apple_10:6a:f5 (64:9a...	HitronTe_af:b1:98 (bc...	802.11	39 Clear-to-send, Flags=.....C

>	Frame 519: 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)

Figura 18: Exemplo de tramas 'Request To Senf' e 'Clear To Send'

5 Conclusão

Neste trabalho prático, foi possível desenvolver competências acerca de redes sem fios.

Começamos por analisar as informações rádio associadas a redes sem fios.

Depois estudamos as diferenças entre Scanning Ativo e Scanning Passivo entre uma STA e um AP.

Proseguimos com o estudo do processo de associação entre um host e um AP.

Por fim, estudamos o processo de transferência de dados nestas redes sem fios.