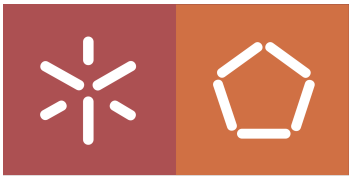

Departamento de Informática

Licenciatura em Engenharia Informática

Redes de Computadores

Universidade do Minho
Escola de Engenharia

Trabalho Prático n.º 4

Grupo n.º 18

Artur Carneiro Neto de Nóbrega Luís, n.º A95414
Hugo Ricardo Macedo Gomes, n.º A96842
Orlando José da Cunha Palmeira, n.º A97755

Braga, maio de 2022

Índice

1 - Acesso rádio

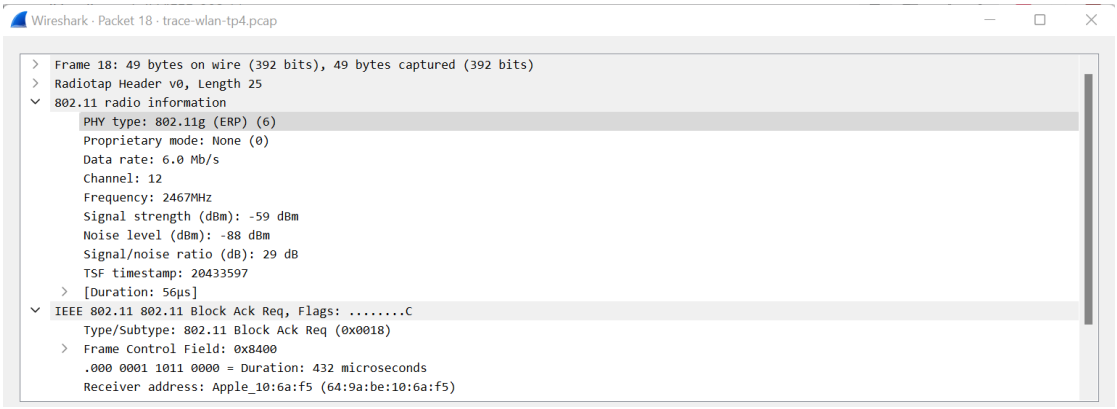

Figura 1 - Trama 802.11 n.º18

1.1 - Alínea 1)

A rede sem fios está a ser operada a 2467 MHz que corresponde ao canal 12.

1.2 - Alínea 2)

A versão da norma IEEE 802.11 que está a ser usada é a versão 802.11g.

1.3 - Alínea 3)

O débito da trama escolhida é de 6.0Mb/s não estando a operar no débito máximo pois a versão 802.11g permite uma capacidade de débito máximo de 54Mb/s. O motivo do débito da trama pode-se justificar por um elevado congestionamento da rede ou pela distância do *Access Point* (AP) ao *Host* ser muito significativa.

2 - Scanning Passivo e Scanning Ativo

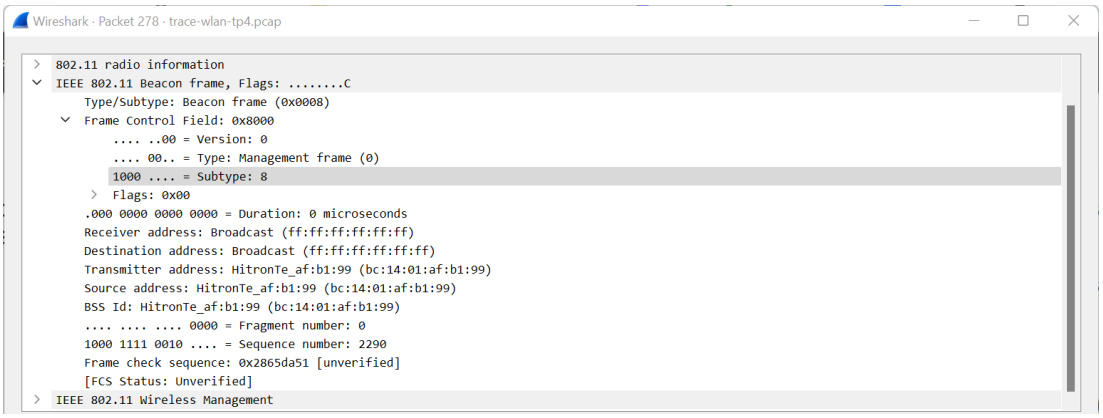

Figura 2 - Trama 802.11 n.º278

2.1 - Alínea 4)

Esta trama é do tipo *Management*. O valor do identificador do tipo é 00 e o valor do subtipo é 8 (1000). O cabeçalho da trama é no campo *Frame Control.*

2.2 - Alínea 5)

Como esta trama é um *Beacon Frame* podemos concluir que a origem provém de um router e o destino será todos os dispositivos na rede.
Endereços MAC mencionados na trama:

- *Receiver*: `Broadcast`
- *Destination*: `Broadcast`
- *Transmitter*: `bc:14:01:af:b1:99`
- *Source*: `bc:14:01:af:b1:99`

2.3 - Alínea 6)

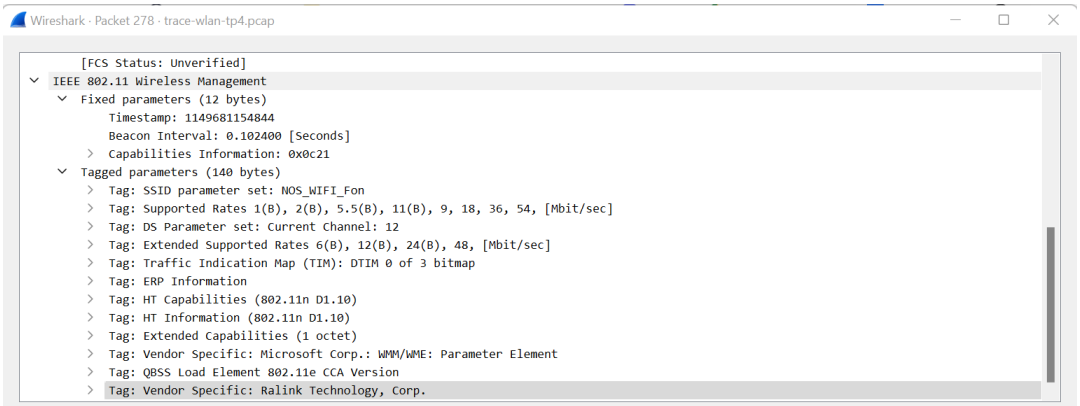

Figura 3 - Visualização dos campos *Supported Rates* e *Extended Supported Rates*

Os débitos base de uma trama *beacon* são de 1 Mb/s, 2 Mb/s, 5.5 Mb/s, 11 Mb/s, 9Mb/s, 18 Mb/s, 36 Mb/s e 54Mb/s. Os débitos adicionais de uma trama *beacon* são de 6 Mb/s, 12 Mb/s, 24 Mb/s e 48 Mb/s.

2.4 - Alínea 7)

No.	Time	Source	Destination	Protocol	Length	Info
276	10.446507	HitronTe_af:b1…	Broadcast	802.11	205	Beacon frame,
277	10.547214	HitronTe_af:b1…	Broadcast	802.11	296	Beacon frame,
278	10.548833	HitronTe_af:b1…	Broadcast	802.11	205	Beacon frame,

Figura 4 - Registo dos instantes de envio de duas tramas *beacon* consecutivas do mesmo AP

O intervalo de tempo previsto entre tramas *beacon* é de 0.102400 segundos (figura 3 - campo '*Beacon Interval*'). Na prática, a periodicidade de tramas *beacon* do mesmo AP não foi preciso uma vez que verificamos uma diferença entre a trama 278 e a trama 276 de 0.102326 segundos ($t_{trama\ 278} - t_{trama\ 276} = 10.548833 - 10.446507 = 0.102326\ s$).

O intervalo de tempo foi menor que o esperado pois ou a trama 276 ou a trama 278 poderá ter chegado atrasada o que fez com que a trama que foi enviada no tempo correto tenha chegado num instante de tempo muito próximo à trama atrasada ou até devido outra razão desconhecida.

2.5 - Alínea 8)

Os SSID's dos AP's que estão a operar na vizinhança da STA de captura são *FlyingNet* e *NOS_WIFI_Fon.* Para obter esta informação, filtrámos a captura do Wireshark com o seguinte filtro: `wlan.fc.type_subtype == 0x08` para se visualizar apenas as tramas *beacon*.

Para confirmar a nossa afirmação, procedemos do seguinte modo:

1. Visualizámos os pacotes filtrados pelo filtro anteriormente mencionado, obtendo o seguinte:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2083, FN=0, Flags=........C, BI=100, SSID=FlyingNet
2	0.001662	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2084, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
3	0.102552	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2085, FN=0, Flags=........C, BI=100, SSID=FlyingNet
4	0.104164	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2086, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
5	0.204951	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2087, FN=0, Flags=........C, BI=100, SSID=FlyingNet
6	0.206582	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2088, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
7	0.307368	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2089, FN=0, Flags=........C, BI=100, SSID=FlyingNet
8	0.308999	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2090, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
9	0.409749	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2091, FN=0, Flags=........C, BI=100, SSID=FlyingNet
10	0.411376	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2092, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
11	0.512117	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2093, FN=0, Flags=........C, BI=100, SSID=FlyingNet
12	0.513707	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2094, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
13	0.614562	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2095, FN=0, Flags=........C, BI=100, SSID=FlyingNet
14	0.616191	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2096, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
28	0.716961	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2097, FN=0, Flags=........C, BI=100, SSID=FlyingNet

Figura 5 - Porção da captura filtrada para visualização de tramas *beacon*

2. Verificámos que no intervalo de tempo de captura [0.000000, 0.716961] segundos, apenas se encontraram os SSID's *FlyingNet* e *NOS_WIFI_Fon.* Ora, como o intervalo de tempo entre tramas *beacon* é de 0.102400 segs (ver alínea 7) e o intervalo capturado na figura 5 é superior a esse *beacon interval*, podemos concluir que apenas as duas SSID's referidas é que se encontra perto da STA de captura.

2.6 - Alínea 9)

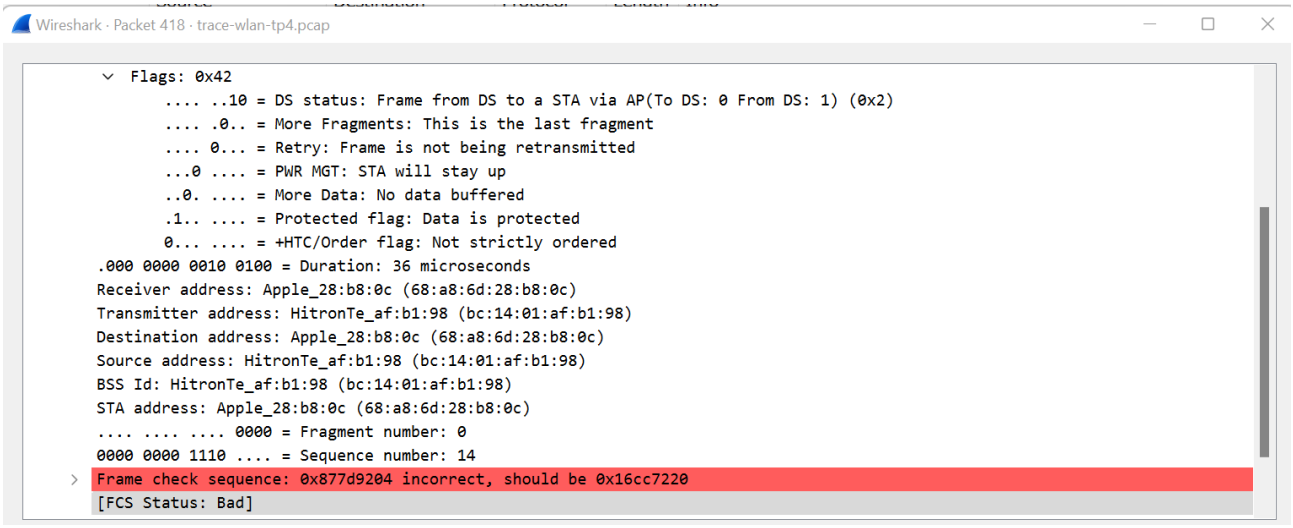

Figura 6 - Uma das tramas transmitida com erro

Como se pode verificar na figura acima, é apresentada a mensagem: "*Frame check sequence: 0x877d9204 incorrect, should be 0x16cc7220*", que nos confirma a existência do método de controlo de erros.
O uso de métodos de controlo de erros em redes sem fios é necessário, uma vez que estas não tanta estabilidade quanto as redes cabeladas e também estão mais sujeitas a fatores adversos tais como interferências de outros equipamentos que operem nas mesmas frequências ou pela perda de sinal gerada pela distância entre os equipamentos que estão a comunicar.

2.7 - Alínea 10)

Filtro que se pode utilizar para o efeito pretendido: wlan.fc.type == 0x00 && ((wlan.fc.type_subtype == 0x04) || (wlan.fc.type_subtype == 0x05)).

2.8 - Alínea 11)

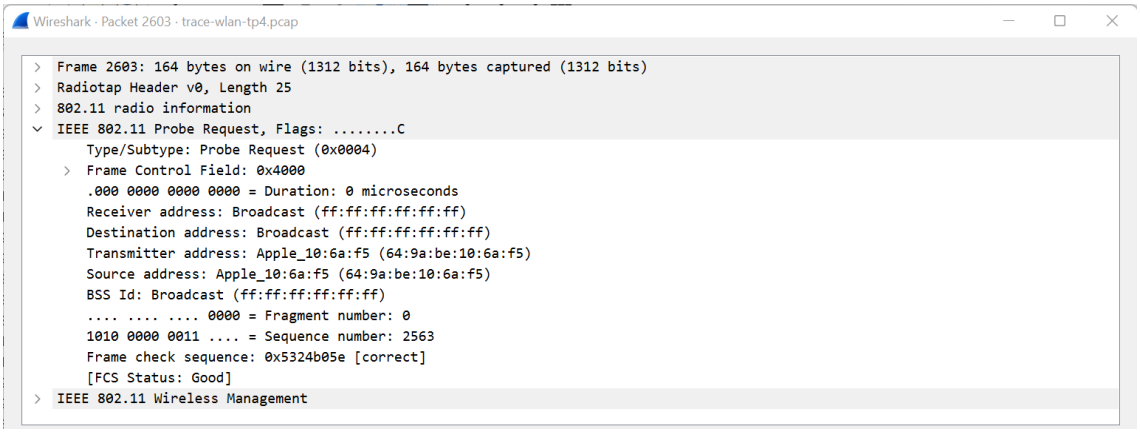

Figura 7 - Uma trama *Probe Request*

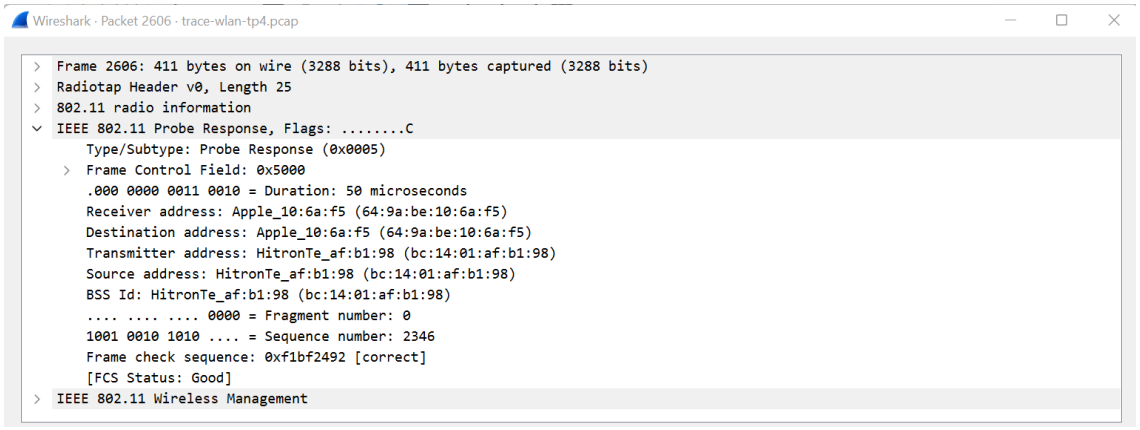

Figura 8 - Uma trama *Probe Response* relativa à trama da figura 6

Na trama de *Probe Request*, os endereços de origem e de destino são correspondentes à STA de captura e *broadcast,* respetivamente. Esta trama serve para a STA ter conhecimento de redes Wi-Fi que lhe estão próximas.
Na trama de *Probe Response*, os endereços de origem e de destino são correspondentes ao *Access Point* e à STA de captura, respetivamente. Esta trama serve para o *Access Point* indicar a presença da sua rede à STA que enviou o *Prob Request*.

3 - Processo de Associação

3.1 - Alínea 12)

No sentido de facilitar a procura de uma sequência de tramas correspondentes a um processo de associação temos de filtrar a captura do *Wireshark* de modo a obter *probe request*, *probe response*, *association request*, *association response* e *authentication* utilizando o seguinte filtro: wlan.fc.type == 0x00 && ((wlan.fc.type_subtype == 0x00) || (wlan.fc.type_subtype == 0x01) || (wlan.fc.type_subtype == 0x04) || (wlan.fc.type_subtype == 0x05) || (wlan.fc.type_subtype == 0x0b)).

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:b1:99	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
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 9 - Sequência de tramas correspondentes a um processo de associação

Na sequência da figura acima, as tramas correspondentes ao processo de associação são as seguintes: #1300, #2486, #2488, #2490 e #2492.

Seria expectável aparecer um pacote *probe response* após pacote o *probe request* (#1300). A não ocorrência do *probe response* pode ser derivada a atrasos ou congestionamento.

3.2 - Alínea 13)

O seguinte diagrama traduz o processo de associação completo:

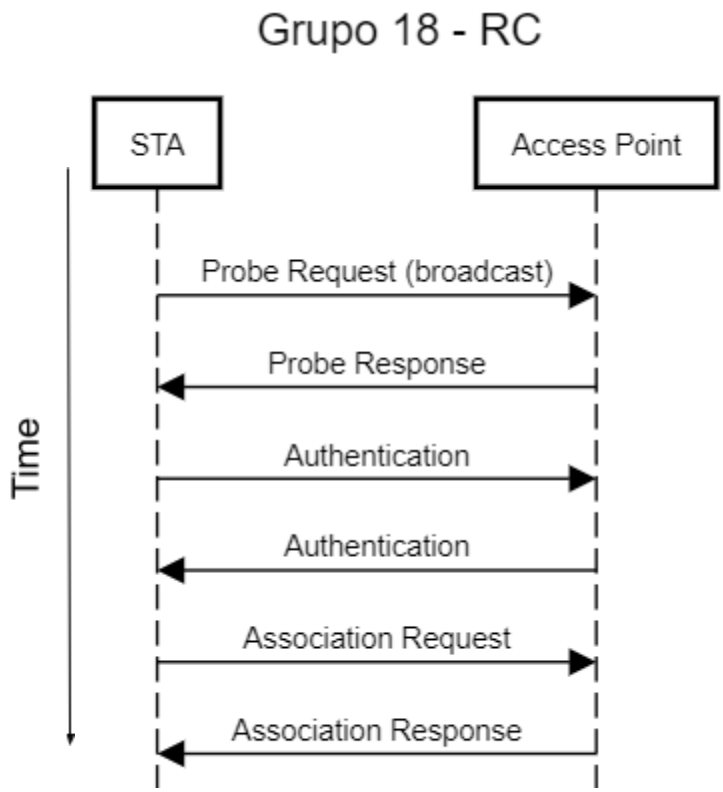

Figura 10 - Processo de associação completo

Observação: O diagrama da figura 10 foi construído no seguinte site: https://sequencediagram.org/

4 - Transferência de dados

4.1 - Alínea 14)

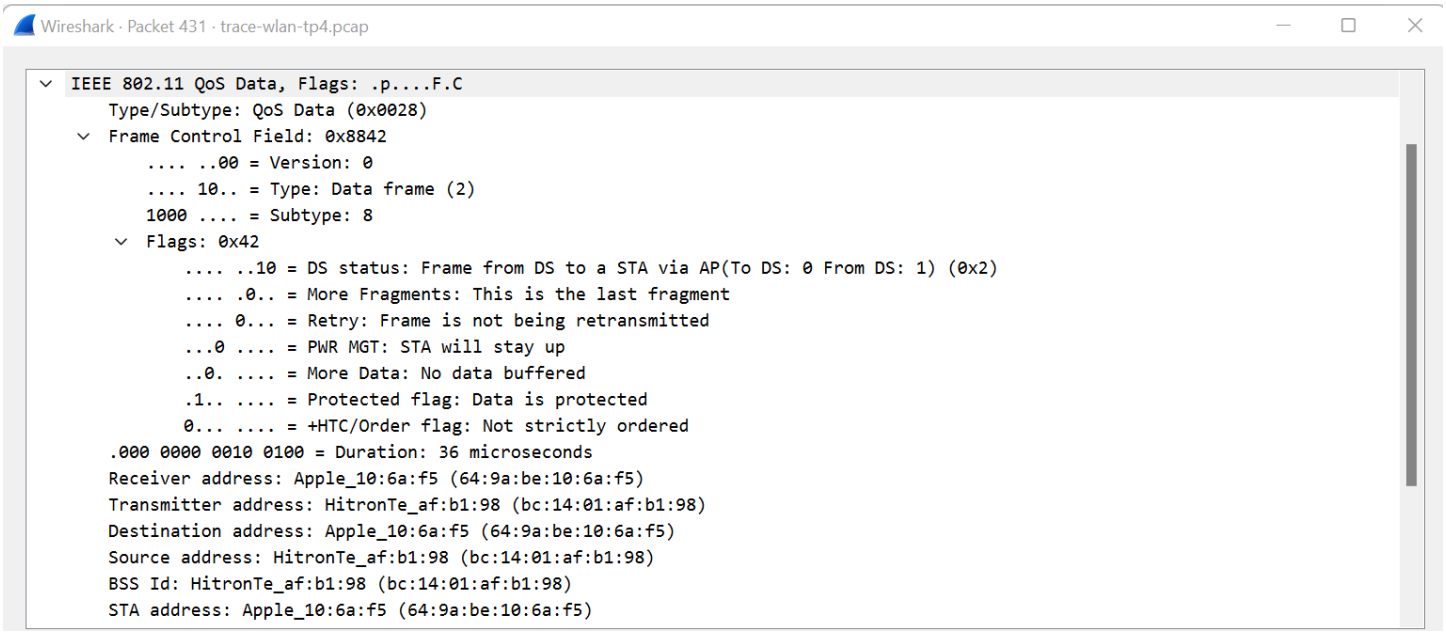

Figura 11 - Alguns dados da trama n.º 431

Os valores de *To DS* e *From DS* são, respetivamente, 0 e 1. Isto indica que a direcionalidade da trama é do exterior da WLAN para a STA, pelo que a direcionalidade não é local à WLAN.

4.2 - Alínea 15)

Endereços MAC solicitados.

- STA: 64:9A:BE:10:6A:F5
- AP: BC:14:01:AF:B1:98
- Router de acesso ao DS: BC:14:01:AF:B1:98

4.3 - Alínea 16)

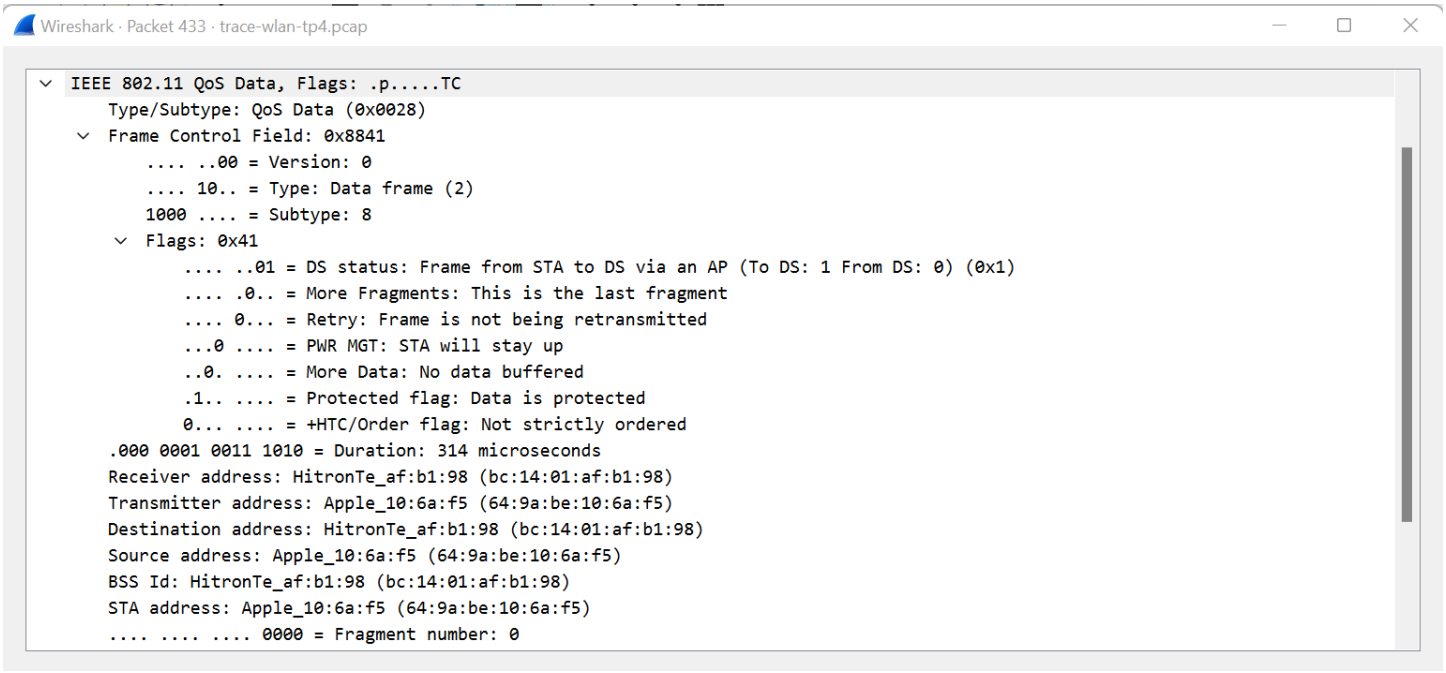

Figura 12 - Alguns dados da trama n.º 433

A direcionalidade desta trama é da STA para o exterior da WLAN (tendo em conta que os valores de *To DS* e *From DS* são 1 e 0, respetivamente).
Quanto ao endereçamento MAC, conseguimos verificar que o endereço da STA é 64:9A:BE:10:6A:F5, o endereço do AP é BC:14:01:AF:B1:98 e o endereço do router de acesso ao DS é BC:14:01:AF:B1:98.

4.4 - Alínea 17)

Os subtipos de tramas de controlo presentes são *Acknowledgement* (ACK), *Request-To-Send* (RTS) e *Clear-To-Send* (CTS).
As tramas ACK servem para informar o remetente que o pacote foi recebido com sucesso pelo destinatário. As tramas RTS servem para o remetente fazer uma reserva do meio ao AP que responde com tramas CTS para informar o remetente que pode iniciar a transmissão.
As tramas RTS e CTS servem essencialmente para evitar a ocorrência de colisões na transmissão. Contudo, estas duas são opcionais.

4.5 - Alínea 18)

Através da aplicação do filtro *(wlan.fc.type == 0x01 && ((wlan.fc.subtype == 0x0b) || (wlan.fc.subtype == 0x0c))) || wlan.fc.type == 0x02,* obtivemos os seguintes resultados:

(wlan.fc.type == 0x01 && ((wlan.fc.subtype == 0x0b) || (wlan.fc.subtype == 0x0c))) || wlan.fc.type == 0x02

No.	Time	Source	Destination	Protocol	Length	Info
15	0.631114	Apple_10:6a:f5 (64:…	HitronTe_af:b1:9…	802.11	45	Request-to-send, Flags=........C
16	0.631128		Apple_10:6a:f5 (…	802.11	39	Clear-to-send, Flags=........C
20	0.631550	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	53	Null function (No data), SN=2488, FN=0, Flags=.......TC
23	0.631798	Apple_10:6a:f5 (64:…	HitronTe_af:b1:9…	802.11	45	Request-to-send, Flags=........C
24	0.631860		Apple_10:6a:f5 (…	802.11	39	Clear-to-send, Flags=........C
26	0.692802	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	53	Null function (No data), SN=2489, FN=0, Flags=...P...TC
30	0.718794	Apple_10:6a:f5	IPv4mcast_fb	802.11	583	Data, SN=2226, FN=0, Flags=.pm...F.C
31	0.719096	Apple_10:6a:f5	IPv6mcast_fb	802.11	603	Data, SN=2227, FN=0, Flags=.p....F.C
78	3.130636		Apple_28:b8:0c (…	802.11	39	Clear-to-send, Flags=........C
79	3.132174	Apple_28:b8:0c	HitronTe_af:b1:98	802.11	49	Null function (No data), SN=0, FN=0, Flags=.......T
81	3.132873		Apple_28:b8:0c (…	802.11	39	Clear-to-send, Flags=........C
82	3.133515	Apple_28:b8:0c	IPv6mcast_fb	802.11	399	QoS Data, SN=42, FN=0, Flags=.p.....T
85	3.133889		Apple_28:b8:0c (…	802.11	39	Clear-to-send, Flags=........C
86	3.134265	Apple_28:b8:0c	IPv4mcast_fb	802.11	379	QoS Data, SN=25, FN=0, Flags=.p..R..T
90	3.176237	Apple_1a:eb:dc	IPv4mcast_fb	802.11	376	Data, SN=2229, FN=0, Flags=.pm...F.C
91	3.176449	Apple_1a:eb:dc	IPv6mcast_fb	802.11	396	Data, SN=2230, FN=0, Flags=.pm...F.C
92	3.176565	Apple_28:b8:0c	IPv6mcast_fb	802.11	402	Data, SN=2231, FN=0, Flags=.pm...F.C
93	3.176779	Apple_28:b8:0c	IPv4mcast_fb	802.11	382	Data, SN=2232, FN=0, Flags=.p....F.C
98	3.383361	Apple_28:b8:0c	HitronTe_af:b1:98	802.11	49	Null function (No data), SN=0, FN=0, Flags=.......T
162	6.653376	Apple_10:6a:f5 (64:…	HitronTe_af:b1:9…	802.11	45	Request-to-send, Flags=........C
163	6.653389		Apple_10:6a:f5 (…	802.11	39	Clear-to-send, Flags=........C
165	6.653491	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	53	Null function (No data), SN=2490, FN=0, Flags=.......TC
173	6.658172	Apple_10:6a:f5 (64:…	HitronTe_af:b1:9…	802.11	45	Request-to-send, Flags=........C

Figura 13 - Captura filtrada para mostrar pacotes de dados e controlo

Como podemos verificar na figura 13, estão a ser trocadas tramas com a opção RTS e CTS entre o AP e a STA.

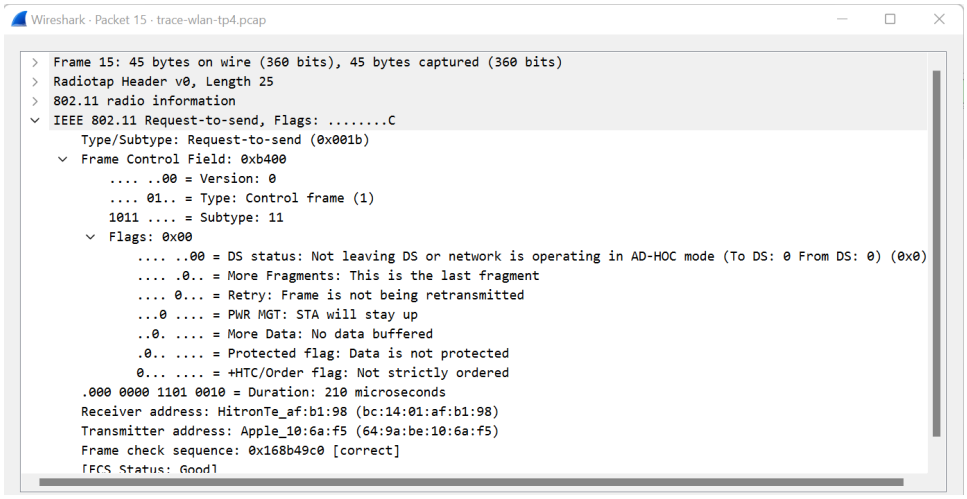

Figura 14 - Trama RTS enviada pela STA

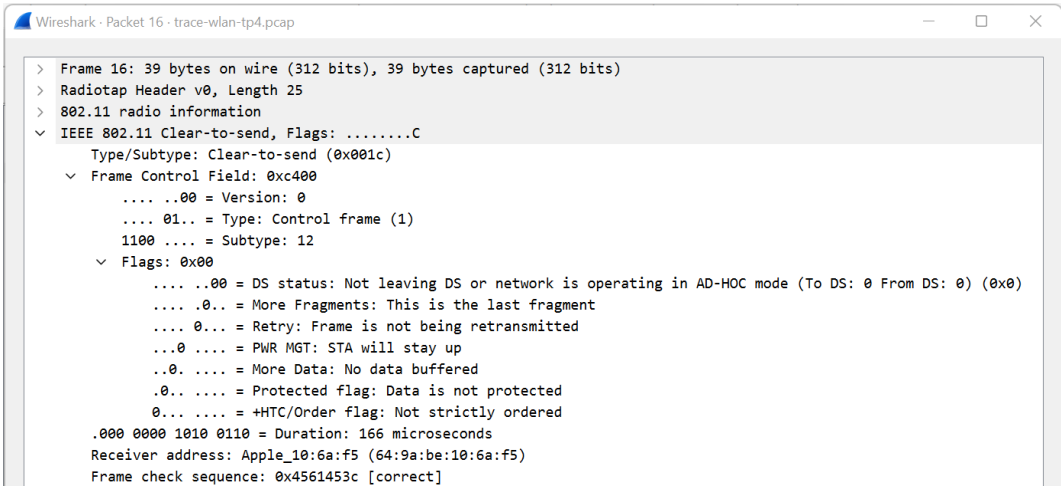

Figura 15 - Trama CTS enviada pelo AP

Através das figuras 14 e 15, verificámos que em ambas as tramas RTS e CTS os campos *To DS* e *From DS* têm valor 0, o que indica que a direcionalidade das tramas é local à WLAN.
Os sistemas envolvidos são a STA (64:9A:BE:10:6A:F5) e o AP (BC:14:01:AF:B1:98).

5 - Conclusão

Este trabalho prático permitiu aprofundar os conhecimentos acerca do protocolo IEEE 802.11. Através da resolução dos exercícios juntamente com a análise da captura fornecida, fomos capazes de verificar que nem sempre o envio de tramas é feito num débito considerado ideal. Na parte de *Scanning Ativo* e *Passivo* conseguimos ver na prática como é que as STA's e os AP's comunicam entre si para estabelecer conexões e como é as STA's conseguem saber quais as redes presentes ao seu redor.
Na secção *Processo de Associação* conseguimos ver como é que as STA's conseguem estabelecer a conexão com a rede escolhida.
Finalmente, na parte de *Transferência de Dados*, pudemos ver como analisar a direcionalidade das tramas através das informações nelas presentes bem como interpretar o seu endereçamento MAC.