Universidade do Minho

Redes de Computadores

Trabalho Prático IV

Ano letivo 2021/2022

a97363, Gabriel Alexandre Monteiro da Silva

a96106, Miguel Silva Pinto

a97613, Pedro Miguel Castilho Martins

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 44 correspondente ao seu identificador de grupo.

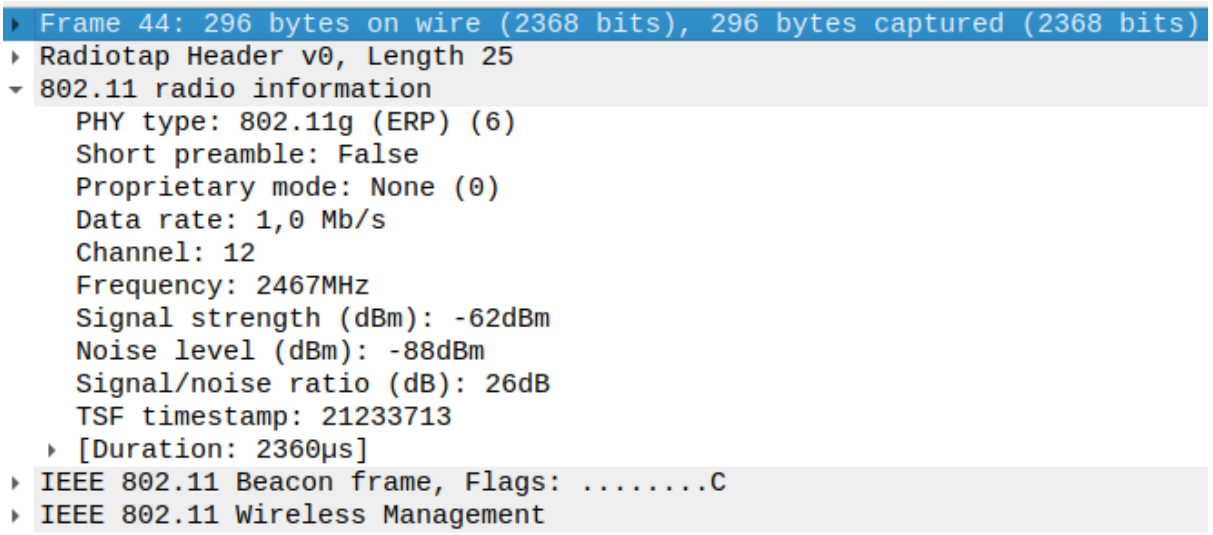


Fig. 1 - Trama 802.11 correspondente ao nosso grupo (44).

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

R: Está a operar a 2467 MHz (Frequency) e o canal correspondente é o 12 (Channel).

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

R: A versão que está a ser usada é 802.11g (ERP).

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.

R: A trama foi enviada com um débito de 1,0 Mb/s. Este débito não é o débito máximo da interface Wi-Fi, visto que o débito máximo da versão 802.11g é de 54 Mb/s.

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:

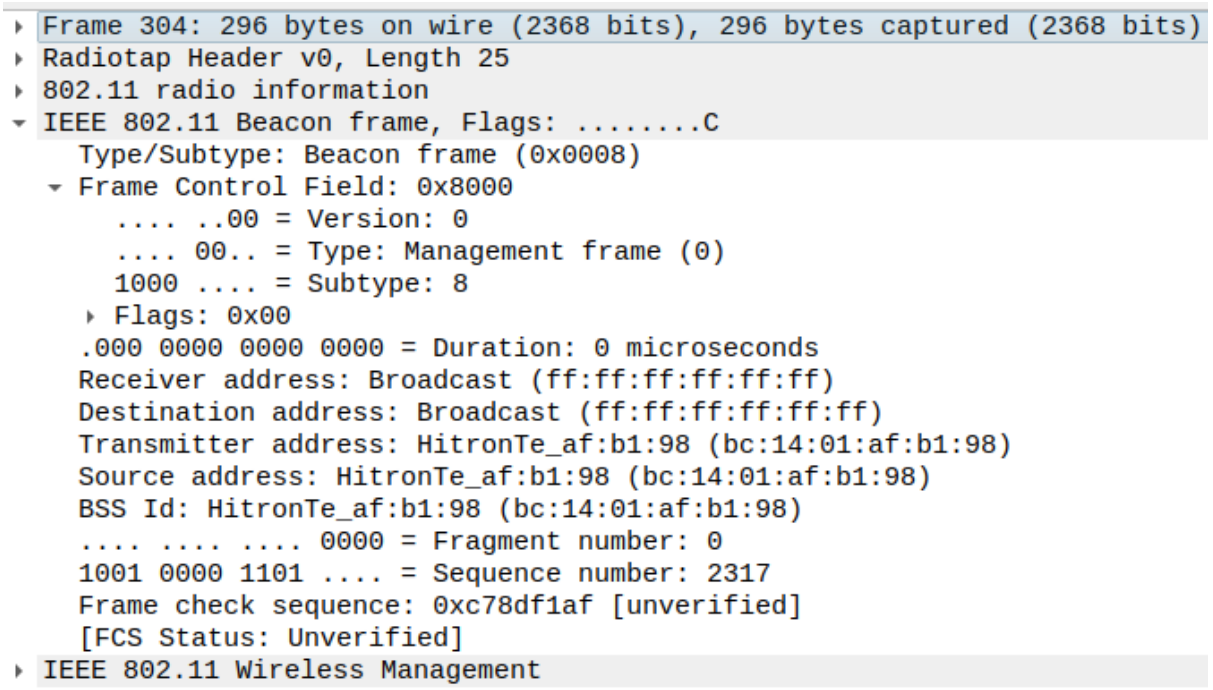


Fig. 2 - Trama 802.11 correspondente ao nosso grupo (260+44).

4. Selecione a trama beacon de ordem (260 + 44). 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)?

R: Com o valor 0x0008, o seu valor correspondente em binário é 1000, que através da tabela no anexo, verificamos que esta trama pertence às tramas de tipo Management e subtipo Beacon.

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

R:
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)
O endereço de destino é o endereço de broadcast que é enviado a todos os hosts da rede local, e o endereço de origem é do Access Point.

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?

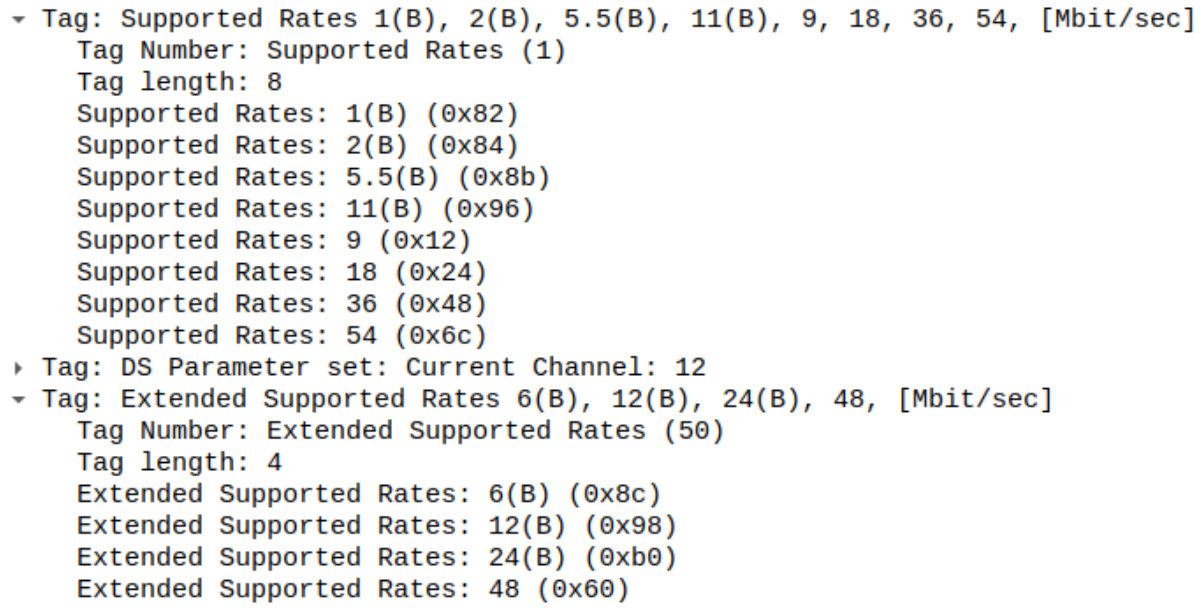


Fig. 3 - Débitos.

R: Os débitos suportados pela trama são 1 Mb/s, 2 Mb/s, 5.5 Mb/s, 11 Mb/s, 9 Mb/s, 18 Mb/s, 36 Mb/s, 54 Mb/s. E os débitos adicionais são 6 Mb/s, 12 Mb/s, 24 Mb/s, 48 Mb/s.

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.

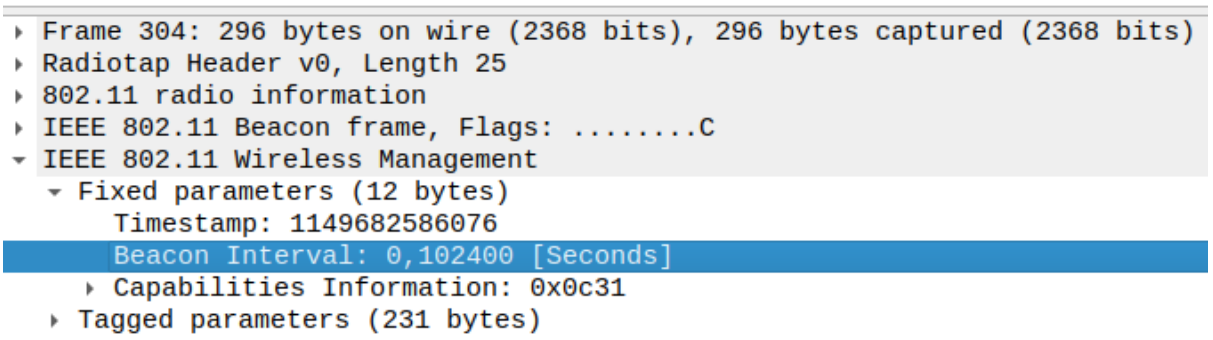
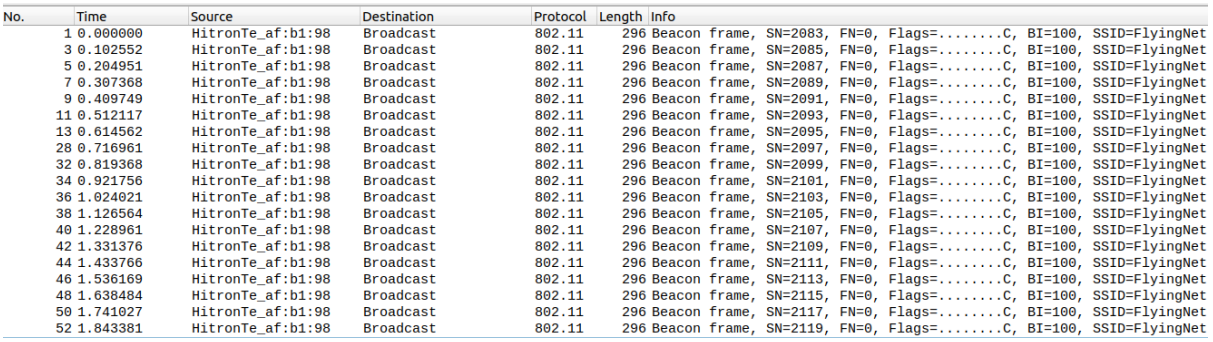


Fig. 4 - Intervalo entre tramas beacon.

R: O intervalo de tempo previsto entre tramas beacon consecutivas é de 0,102400 segundos.



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
3	0.102552	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2085, FN=0, Flags=........C, BI=100, SSID=FlyingNet
5	0.204951	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2087, FN=0, Flags=........C, BI=100, SSID=FlyingNet
7	0.307368	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2089, FN=0, Flags=........C, BI=100, SSID=FlyingNet
9	0.409749	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2091, FN=0, Flags=........C, BI=100, SSID=FlyingNet
11	0.512117	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2093, FN=0, Flags=........C, BI=100, SSID=FlyingNet
13	0.614562	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2095, FN=0, Flags=........C, BI=100, SSID=FlyingNet
28	0.716961	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2097, FN=0, Flags=........C, BI=100, SSID=FlyingNet
32	0.819368	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2099, FN=0, Flags=........C, BI=100, SSID=FlyingNet
34	0.921756	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2101, FN=0, Flags=........C, BI=100, SSID=FlyingNet
36	1.024021	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2103, FN=0, Flags=........C, BI=100, SSID=FlyingNet
38	1.126564	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2105, FN=0, Flags=........C, BI=100, SSID=FlyingNet
40	1.228961	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2107, FN=0, Flags=........C, BI=100, SSID=FlyingNet
42	1.331376	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2109, FN=0, Flags=........C, BI=100, SSID=FlyingNet
44	1.433766	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2111, FN=0, Flags=........C, BI=100, SSID=FlyingNet
46	1.536169	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2113, FN=0, Flags=........C, BI=100, SSID=FlyingNet
48	1.638484	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2115, FN=0, Flags=........C, BI=100, SSID=FlyingNet
50	1.741027	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2117, FN=0, Flags=........C, BI=100, SSID=FlyingNet
52	1.843381	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2119, FN=0, Flags=........C, BI=100, SSID=FlyingNet

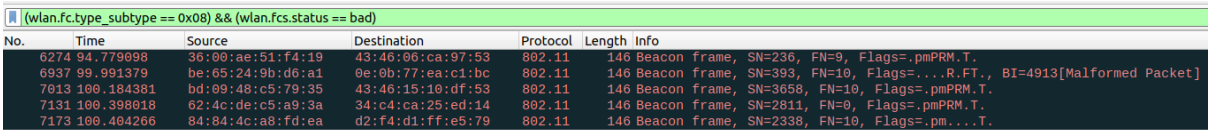
Fig. 5 - Tramas SSID=FlyingNet.

A periodicidade das tramas provenientes do mesmo AP não é verificada com precisão como podemos ver na coluna Time da **figura 5**, devido à possibilidade de o AP estar a realizar outra tarefa no exato momento em que deveria mandar a trama beacon, causando uma imprecisão na periodicidade do envio das tramas.

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).

R: Existem 2 SSIDs a operar na vizinhança da STA que são *FlyingNet* e *NOS_WIFI_Fon*. Obtemos essa informação ao utilizar o filtro “wlan.ssid”.

9. Verifique se está a ser usado o método de deteção de erros (CRC).
Que conclui?
Justifique o porquê de ser necessário usar deteção de erros em redes sem fios.



(wlan.fc.type_subtype == 0x08) && (wlan.fcs.status == bad)

No.	Time	Source	Destination	Protocol	Length	Info
6274	94.779098	36:00:ae:51:f4:19	43:46:06:ca:97:53	802.11	146	Beacon frame, SN=236, FN=9, Flags=.pmPRM.T.
6937	99.991379	be:65:24:9b:d6:a1	0e:0b: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:df:53	802.11	146	Beacon frame, SN=3658, FN=10, Flags=.pmPRM.T.
7131	100.398018	62:4c:de:c5:a9:3a	34:c4:ca:25:ed:14	802.11	146	Beacon frame, SN=2811, FN=0, Flags=.pmPRM.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.

Fig. 6 - Filtro (wlan.fc.type_subtype == 0x08) && (wlan.fcs.status == bad).

R: Uma vez que as redes WiFi estão mais suscetíveis a erros, devido a serem transmitidas sem a utilização de fios, é necessário usar um método de deteção de erros. Como podemos ver na imagem em cima são detectadas tramas Beacon com o campo (FCS Status: Bad) indicando que foi detectado um erro na trama.

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.

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

(wlan.fc.type_subtype==5)||(wlan.fc.type_subtype==4)

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 (Broadcas…
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 (Broadcas…
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_…
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_…
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_…
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

Fig. 7 - Filtro (wlan.fc.type_subtype==5) || (wlan.fc.type_subtype==4).

.

R: (wlan.fc.type_subtype==5) || (wlan.fc.type_subtype==4).

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?

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

Fig. 8 - Probing request e response.

R: O probing request é enviado por um host, com um endereço de broadcast, destinado a alcançar um AP. De seguida, um AP irá responder com um probe response, endereçado ao host que enviou o probe request.

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.

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.

2485	70.352671		Broadcom_04:6a:f5 (…	802.11	39	Clear-to-send, Flags=.......C
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

Fig. 9 - Processo de associação.

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

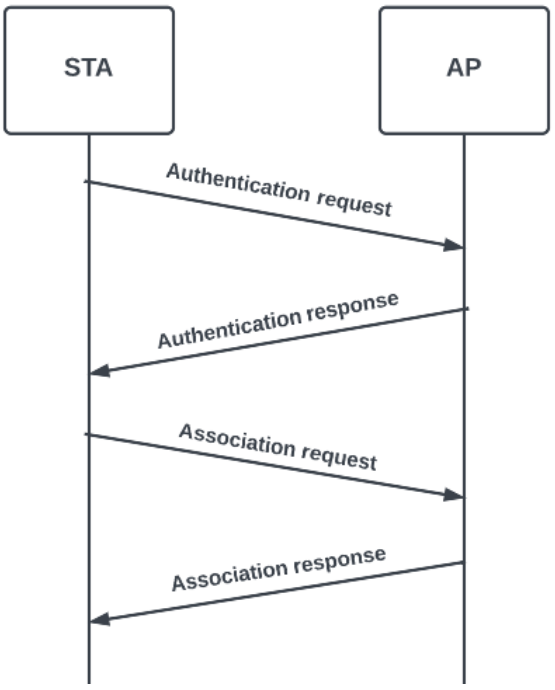


Fig. 10 - Diagrama do processo de associação.

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.

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?

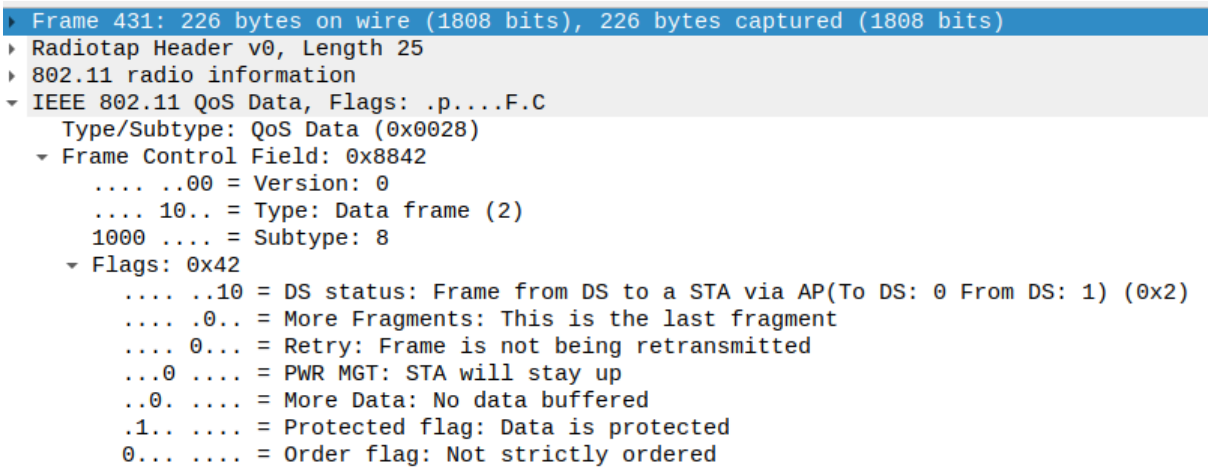


Fig. 11 - Trama de dados (nº 431).

R: Pelo campo “DS status” conseguimos observar que o valor do “To DS” é 0 e o valor de “From DS” é 1. Isso indica que a trama está a ser enviada do DS para a STA via AP, ou seja a trama vem de fora da WLAN, logo não é local.

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?

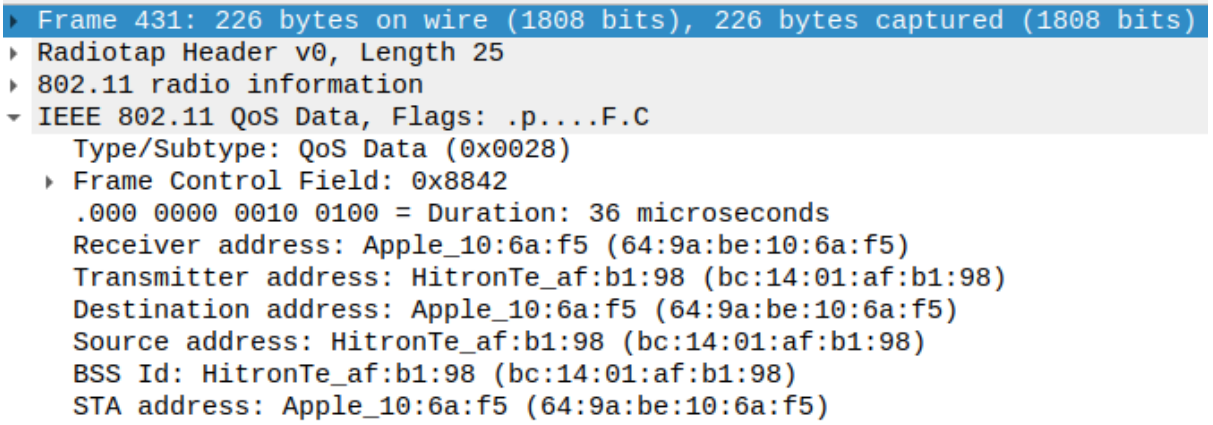


Fig. 12 - Trama de dados (nº 431).

R:

Endereço STA : 64:9a:be:10:6a:f5 (Apple_10) (Destination address)
Endereço AP : bc:14:01:af:b1:96 (HitronTe_af) (Transmitter address)
Endereço router de acesso : bc:14:01:af:b1:96 (HitronTe_af) (Source address).

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

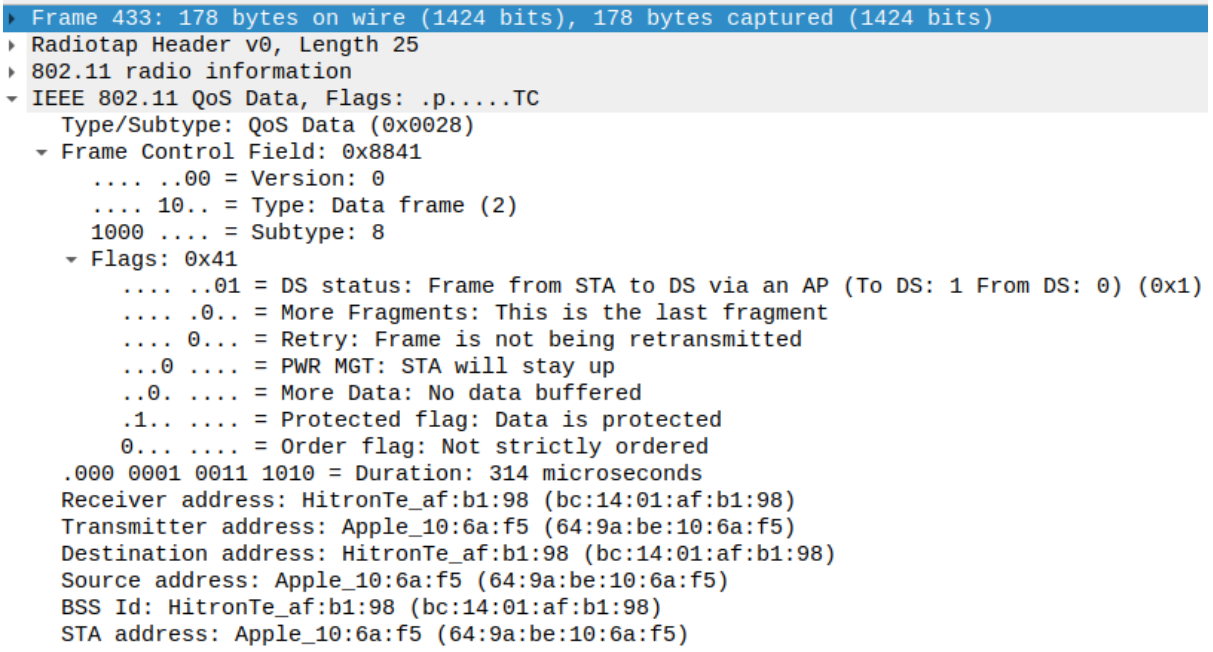


Fig. 12 - Trama de dados (nº 433).

R: O campo DS status diz agora que a trama vem do STA para o DS via AP, sendo os seu endereços MAC:
Address1: BSSID = (Receiver Address) = bc:14:01:af:b1:96
Address2: TA = (Transmitter Address) = 64:9a:be:10:6a:f5
Address3: DA = (Destination Address) = bc:14:01:af:b1:96.

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.)

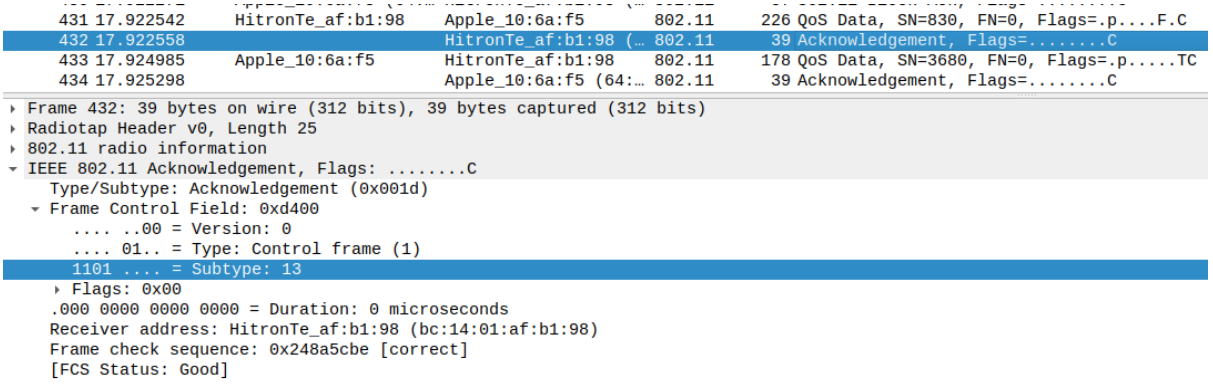


Fig. 13 - Trama “Acknowledgement”.

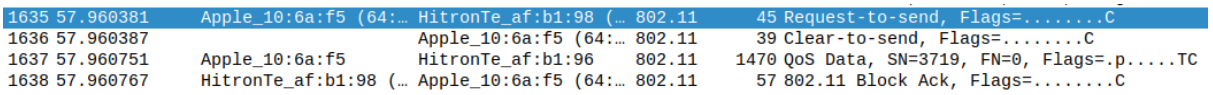
R: O subtipo das tramas de controlo é 13 que identificam o subtipo “Acknowledgement”. Estas tramas de controlo são necessárias para garantir que os dados foram transmitidos com sucesso, pois a rede Wi-Fi é mais suscetível a falhas do que a rede Ethernet.

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.

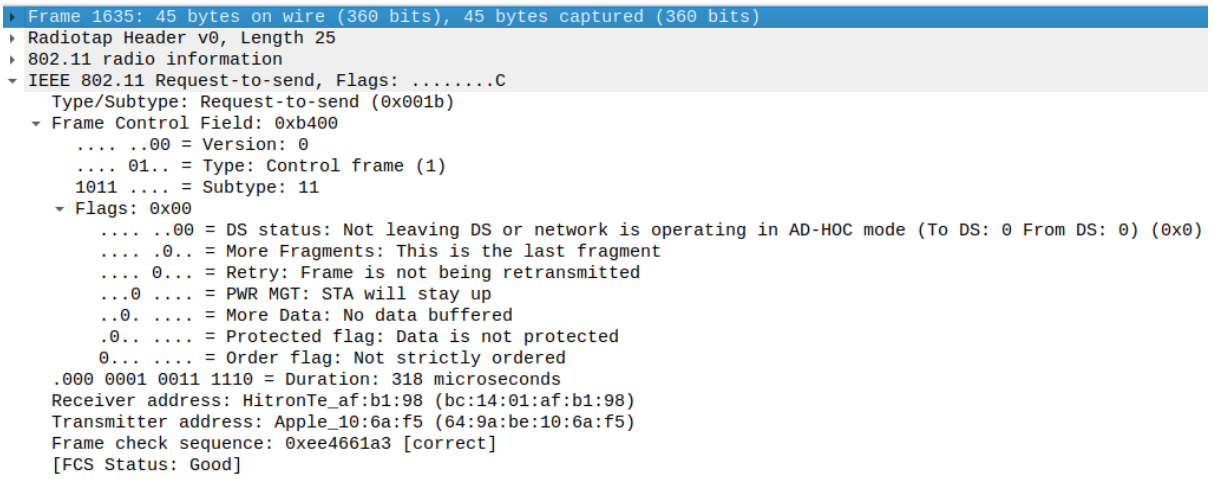
R: Para o exemplo acima não está a ser usada a opção RTS/CTS na troca de dados entre a STA e o AP/Router.

Porém nesta troca de dados a opção RTS/CTS é utilizada:



```
1635 57.960381    Apple_10:6a:f5 (64:… HitronTe_af:b1:98 (… 802.11      45 Request-to-send, Flags=........C
1636 57.960387                        Apple_10:6a:f5 (64:… 802.11      39 Clear-to-send, Flags=........C
1637 57.960751    Apple_10:6a:f5      HitronTe_af:b1:96    802.11    1470 QoS Data, SN=3719, FN=0, Flags=.p.....TC
1638 57.960767    HitronTe_af:b1:98 (… Apple_10:6a:f5 (64:… 802.11      57 802.11 Block Ack, Flags=........C
```

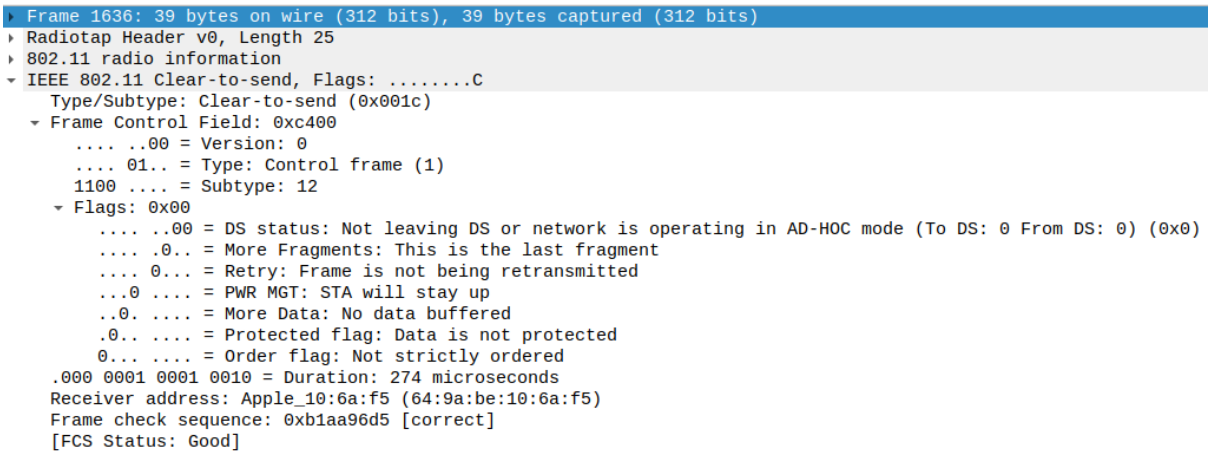
Fig. 14 - Troca de dados com opção RTS/CTS.



```
▸ Frame 1635: 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... .... = Order flag: Not strictly ordered
    .000 0001 0011 1110 = Duration: 318 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: 0xee4661a3 [correct]
    [FCS Status: Good]
```

Fig. 15 - Trama RTS.

Como podemos ver no campo DS status a trama RTS está a operar na network em AD-HOC mode. Esta trama é usada para mandar um pedido para transmissão de dados entre a STA e o AP.



```
▸ Frame 1636: 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
    ▾ 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... .... = Order flag: Not strictly ordered
    .000 0001 0001 0010 = Duration: 274 microseconds
    Receiver address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    Frame check sequence: 0xb1aa96d5 [correct]
    [FCS Status: Good]
```

Fig. 16 - Trama CTS.

O campo da trama CTS também opera na network em AD-HOC mode e é usada para mandar a confirmação que os dados podem ser transmitidos.

Conclusão

Com este trabalho prático conseguimos reforçar o que aprendemos nas aulas teóricas sobre as redes Wi-Fi e redes móveis. Através do Wireshark conseguimos perceber a comunicação entre os diversos dispositivos das redes wireless, visualizando todos os protocolos e tramas envolvidas no processo de comunicação entre diversos dispositivos relacionados com as redes sem fios.

Foi possível aprofundar o nosso conhecimento nas redes 802.11, bem como o tipo, subtipo, e direcionalidade das tramas. Aprendemos o conceito de autenticação e de reserva do meio de comunicação através das tramas RTS/CTS, o conceito de scanning passivo/ativo e a diferença entre as tramas beacon e probe request/response.

Em suma, achamos que este trabalho ajudou-nos a melhorar o nosso conhecimento sobre as redes wireless e redes móveis obtido nas aulas teóricas.