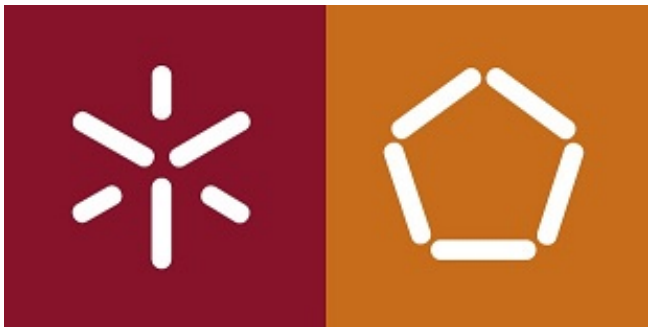


Universidade do Minho
Departamento de Informática

Trabalho Prático 4

Redes de Computadores

Grupo 126

Beatriz Rodrigues *(a93230)* Francisco Neves *(a93202)*
Guilherme Fernandes *(a93216)*

Maio 2022

Questões e Respostas

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

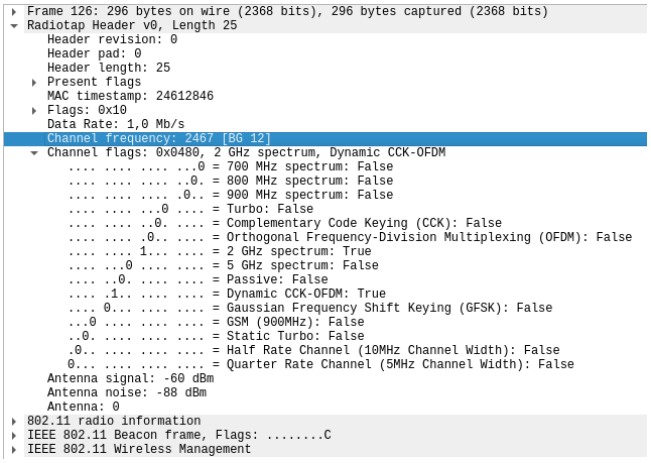


Figura 1.1: Frequência do Espectro

Tendo em conta o número e turno do grupo, foi escolhida a trama de ordem 126.

Assim sendo, a frequência do canal sobre a qual a rede está a operar é de 2467, o que corresponde ao canal de espectro 2 `GHz`.

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

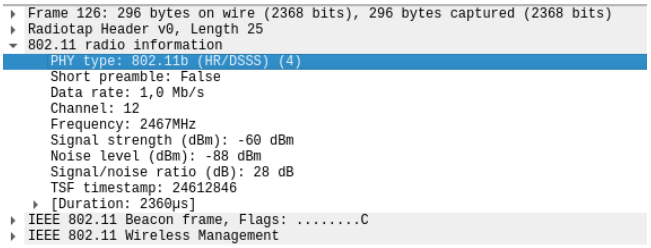


Figura 1.2: Versão da norma `IEEE 802.11`

Podemos verificar que a versão da norma `IEEE 802.11` a ser utilizada é a `802.11b`.

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.

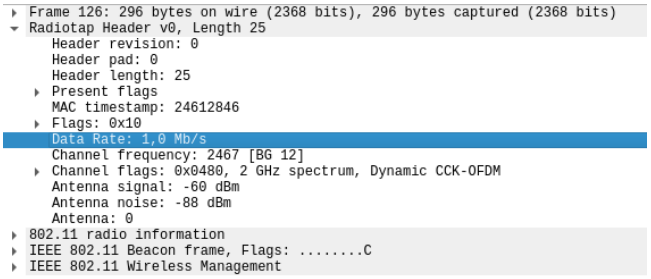


Figura 1.3: Débito de envio da trama

Podemos então verificar, pelo campo *Data Rate*, que a trama foi enviada a um débito de `1 Mb/s`. Assim, tendo em conta que o débito máximo que a versão `802.11b` da norma `IEEE 802.11` permite é de `11 Mb/s`, conclui-se que este débito não corresponde ao débito máximo a que a interface *Wi-Fi* pode operar.

Isto deve-se à necessidade que todos os clientes do *Access Point* recebe a trama *beacon*, pois, uma trama deste tipo tem como objetivo anunciar a presença e transmitir informações tais como a data e a hora. Assim, para a transmissão destas tramas opta-se, geralmente, pelos débitos mais baixos possíveis.

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)?

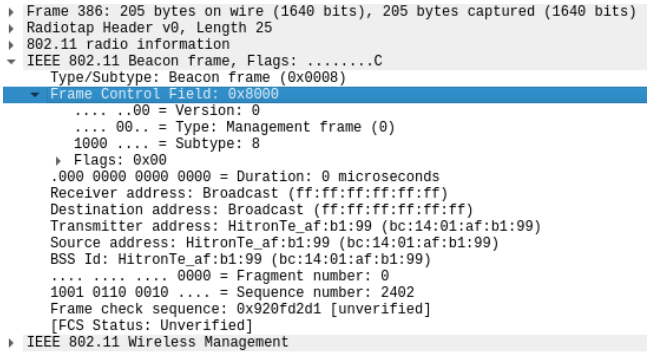


Figura 1.4: Tipo da trama

Tendo em conta o número do grupo, a trama escolhida é a de ordem `386`.

Assim, podemos verificar que esta trama é do tipo `0` (*Management frame*) e de subtipo `8`. Recorrendo à tabela em anexo do enunciado, podemos verificar que esta corresponde a uma trama do tipo de *Management* e subtipo *Beacon*.

00	Management	1000	Beacon

Figura 1.5: Entrada na tabela em anexo

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

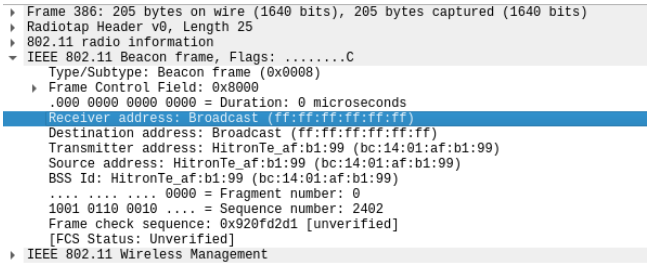


Figura 1.6: Endereços *MAC* em uso

Podemos verificar que os endereços de *MAC* em uso correspondem a `ff:ff:ff:ff:ff:ff` para os recetores e `bc:14:01:af:b1:99` para o emissor.

Tendo em conta a utilidade de uma trama deste tipo, seria de esperar que o endereço *MAC* de destino fosse este, visto corresponder ao endereço de *broadcast* (`ff:ff:ff:ff:ff:ff`), pois, este tipo de tramas deverá ser transmitido para todos os *hosts* da rede de forma a propagar a informação que contêm.

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?

Através da figura podemos observar que o *Access Point* suporta os seguintes débitos base:

- 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`.

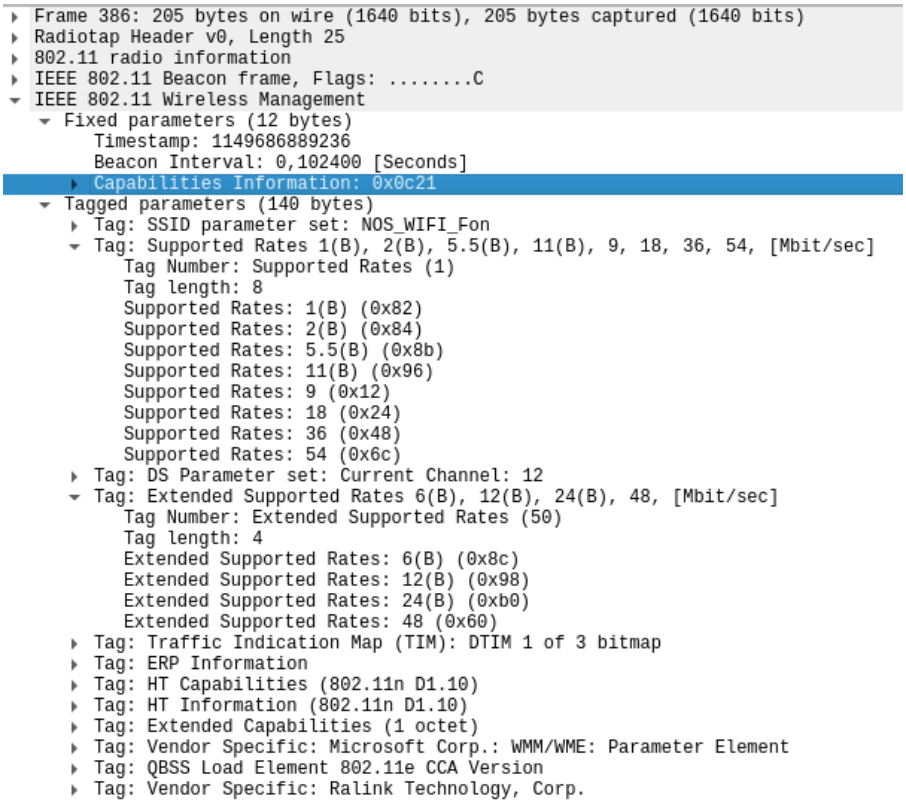


Figura 1.7: Débitos Suportados

Podemos ainda observar que suporta os seguintes débitos adicionais:

- 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.

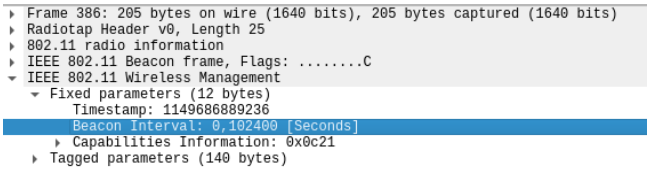
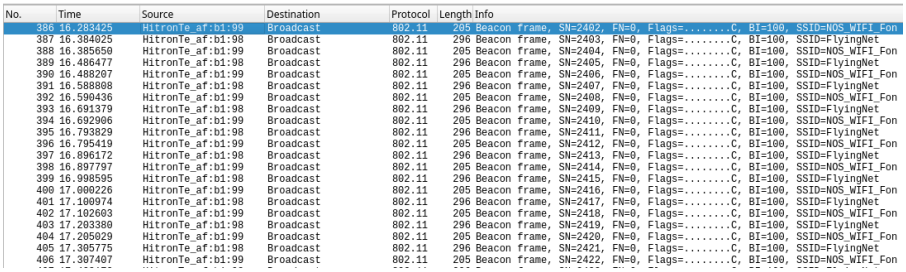


Figura 1.8: Intervalo de tempo previsto entre tramas *beacon* consecutivas

Como podemos verificar pela imagem acima, o intervalo de tempo previsto entre tramas *beacon* consecutivas é `0.102400 s`.



No.	Time	Source	Destination	Protocol	Length	Info
386	16.283425	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2402, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
387	16.384025	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2403, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
388	16.385650	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2404, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
389	16.486477	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2405, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
390	16.488207	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2406, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
391	16.588808	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2407, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
392	16.590436	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2408, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
393	16.691379	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2409, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
394	16.692906	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2410, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
395	16.793829	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2411, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
396	16.795419	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2412, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
397	16.896172	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2413, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
398	16.897797	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2414, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
399	16.998595	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2415, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
400	17.000226	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2416, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
401	17.100974	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2417, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
402	17.102603	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2418, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
403	17.203380	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2419, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
404	17.205029	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2420, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
405	17.305775	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2421, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
406	17.307407	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2422, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

Figura 1.9: Intervalo de tempo real entre tramas *beacon* consecutivas

No entanto, como podemos verificar pela imagem acima, o intervalo de tempo real entre tramas *beacon* do mesmo AP é ligeiramente superior ao previsto. Isto deve-se a possíveis atrasos e congestões na rede, assim como às propriedades do ambiente e condições físicas do ambiente de transmissão em que este se encontra.

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).

Os `SSIDs` dos *APs* que estão a operar na vizinhança da `STA` de captura são os seguintes:

- `NOS_WIFI_Fon`;
- `FlyingNet`;
- `2WIRE-PT-431`.

De modo a obter esta informação, escreveu-se o seguinte *script* em `BASH`:

```
cat capture.txt | grep -o 'SSID=.*' | sort | uniq
```

Sendo que `capture.txt` representa o ficheiro de captura exportado num ficheiro de *plain text*.

Executando isto, obteve-se como resposta o seguinte *output*:

```
SSID=2WIRE-PT-431
SSID=FlyingNet
SSID=NOS_WIFI_Fon
SSID=Wildcard (Broadcast)
```

No entanto, a *SSID Wildcard* é representativa do *broadcast* no *Wireshark*.

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.

Na versão do *Wireshark* utilizada (Wireshark 3.6.3 (Git commit 6d348e4611e2)) não é capturada qualquer trama com erros de verificação.

No entanto, a deteção de erros em redes sem fios revela-se muito importante, pois permite detetar tramas corrompidas, algo que poderá acontecer com uma relativa facilidade, devido à fragilidade que este tipo de redes fornece. Efetuando esta verificação permite-se que exista uma tentativa de recuperar informação perdida.

Figura 1.10: Utilização do filtro sugerido

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

O filtro apropriado deverá ser $wlan.fc.type\_subtype == 4 \parallel wlan.fc.type\_subtype == 5$, de forma a visualizar todas as tramas *probing request* ou *probing response* em simultâneo, como ilustrado na imagem.

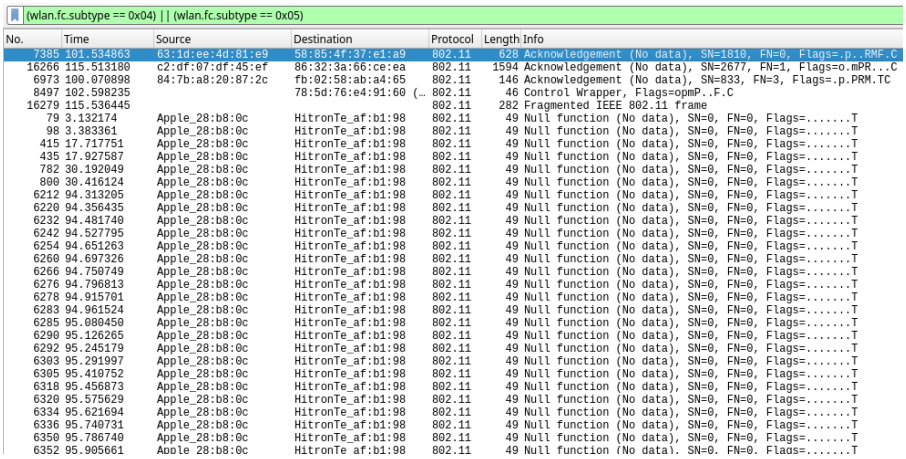


Figura 1.11: Tramas *probing request* ou *probing response*

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?

Um *probing request* tem a função de procurar obter informações acercas de *AP*. A *probing response* irá ser proveniente de um *AP*, concedendo-lhe informações relativas a si próprio.

Neste caso, uma vez que o *receiver address* e o *destination address* do *probing request* são endereçados ao *broadcast address*, compreende-se que esta trama foi enviada com o propósito de alcançar todos os *AP* ao alcance da *STA* a enviar o *probing request*.

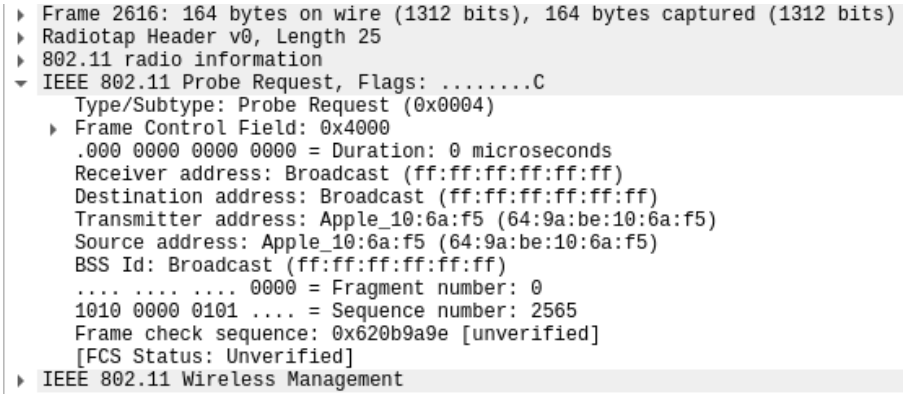


Figura 1.12: *Probing Request*

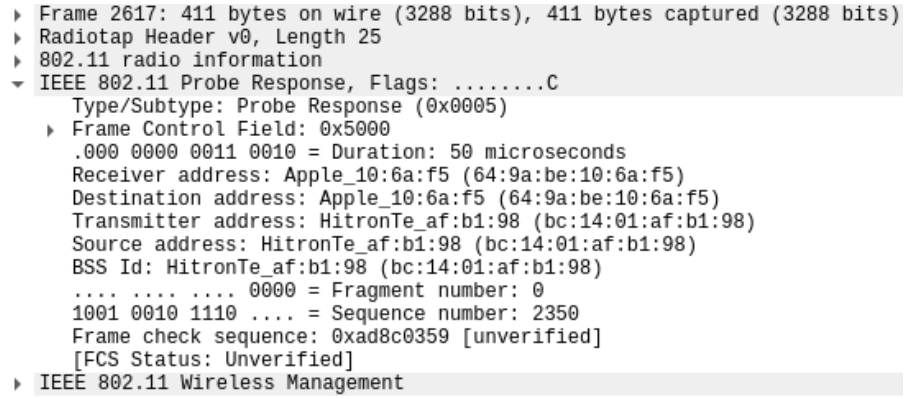
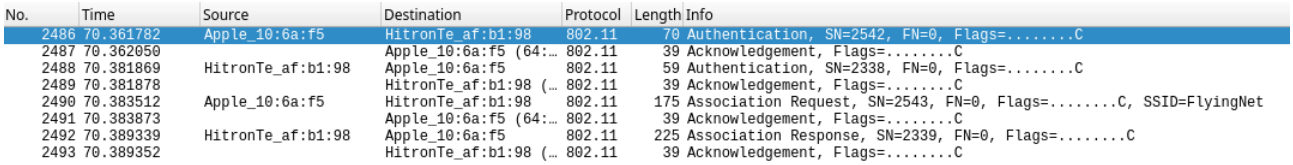


Figura 1.13: *Probing Response*

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.



No.	Time	Source	Destination	Protocol	Length	Info
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

Figura 1.14: Processo de associação completo entre a *STA* e o *AP*

Um exemplo deste caso, tal como ilustrado na figura é entre as tramas de ordem 2486 e 2493.

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

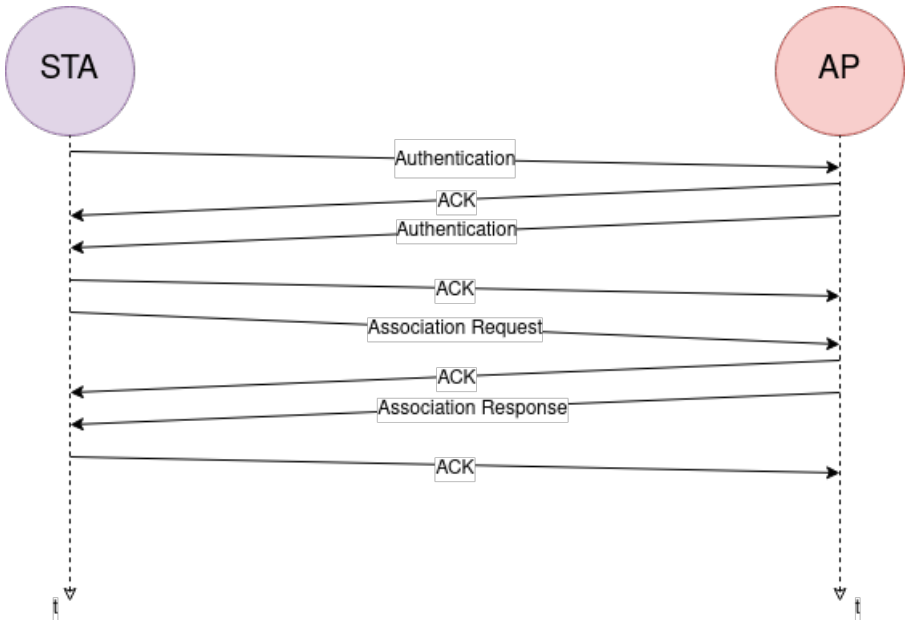


Figura 1.15: Diagrama temporal ilustrativo das tramas trocadas

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?

```
▾ 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 1.16: Frame Control da trama nº431

Consultando a flag DS status, verificamos que o seu valor corresponde a `0x2` (o valor do campo `To DS` é false e do campo `From DS` é true). Isto indica que a trama não é local à *WLAN*, uma vez que vem do *DS* para o *STA*.

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?

Os endereços *MAC* correspondentes ao *host* sem fios (STA), ao AP e ao *router* de acesso ao sistema de distribuição são, respetivamente, `64:9a:be:10:6a:f5`, `64:9a:be:10:6a:f5` e `bc:14:01:af:b1:98`.

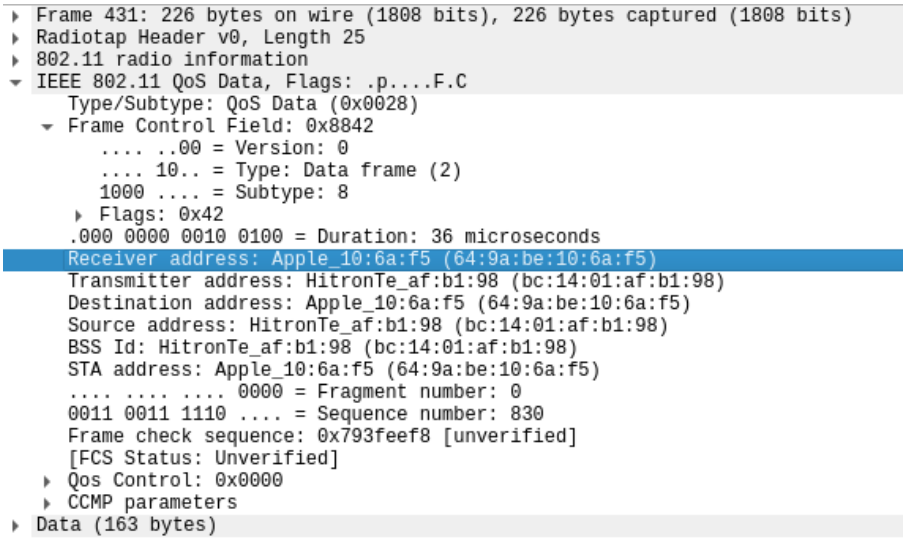


Figura 1.17: Endereços *MAC*

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

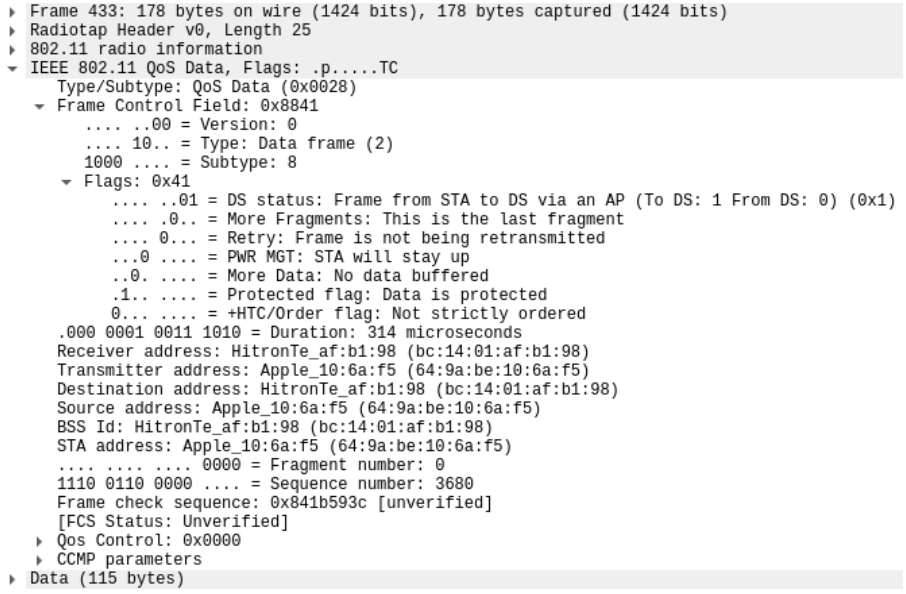


Figura 1.18: Frame 433

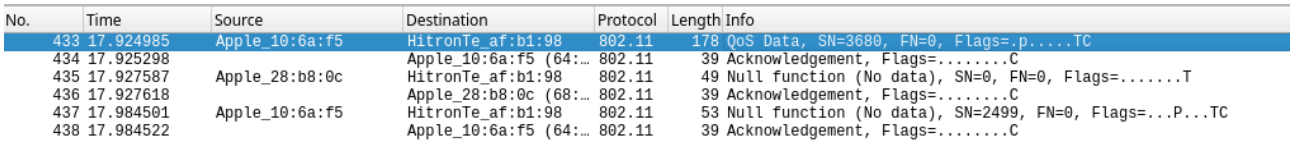
Em termos de direccionionalidade, esta trama vem do *STA* para o *DS*.

Os endereços *MAC* de origem e do transmissor são o mesmo, assim como os de destino e do recetor.

Isto significa que a trama vai deixar a rede local, sem qualquer tipo de intermediação.

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.)

Tal como podemos verificar pela imagem acima, as tramas de controlo transmitidas são `ACKs` (*Acknowledgements*) que indicam que a transmissão foi efetuada com sucesso.



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
434	17.925298		Apple_10:6a:f5 (64:…	802.11	39	Acknowledgement, Flags=........C
435	17.927587	Apple_28:b8:0c	HitronTe_af:b1:98	802.11	49	Null function (No data), SN=0, FN=0, Flags=.......T
436	17.927618		Apple_28:b8:0c (68:…	802.11	39	Acknowledgement, Flags=........C
437	17.984501	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	53	Null function (No data), SN=2499, FN=0, Flags=...P...TC
438	17.984522		Apple_10:6a:f5 (64:…	802.11	39	Acknowledgement, Flags=........C

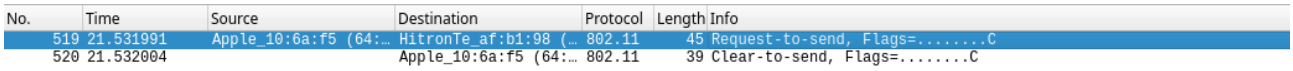
Figura 1.19: Tramas de *Acknowledgement*

Ao contrário daquilo que acontecia com as redes *Ethernet*, é necessária a existência de tramas de controlo deste género devido à grande suscetibilidade de perdas no contexto das redes sem fio. Assim, recorrendo a tramas deste tipo, os pontos podem comunicar entre si indicando que a transmissão está a correr de forma correta.

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.

Para o exemplo acima, este tipo de tramas não é utilizado, sendo este, portanto, um exemplo de um caso em que uma transferência de dados não utiliza a opção `RTC/CTS`.

Podemos ainda verificar uma situação em que estas tramas são utilizadas, por exemplo a partir da trama de ordem `519`:



No.	Time	Source	Destination	Protocol	Length	Info
519	21.531991	Apple_10:6a:f5 (64:…	HitronTe_af:b1:98 (…	802.11	45	Request-to-send, Flags=.......C
520	21.532004		Apple_10:6a:f5 (64:…	802.11	39	Clear-to-send, Flags=.......C

Figura 1.20: Utilização de tramas `RTC/CTS`

Conclusões

Este trabalho prático visava a aplicação do conhecimentos acerca das temáticas relacionadas com Redes *Wireless* (como, por exemplo, o endereçamento, tipos e subtipos de tramas *Wi-Fi* ou mecanismos de controlo de acesso).

Para tal, foi utilizada ferramenta *Wireshark* para a captação e análise de tramas, especificamente tramas `802.11`, sendo aplicados filtros para isolar as tramas relevantes para o objetivo pretendido.