Trabalho Prático Nº4

Universidade do Minho

Ana Inês Leite

a96159@uminho.pt

Diana Filipa Ferreira Malheiro Teixeira

a97516@uminho.pt

Pedro Marcelo Bogas Oliveira

a95076@uminho.pt

Objetivo

Este trabalho tem como principal objetivo o estudo dos diferentes aspetos relativos ao protocolo IEEE 802.11.

Dentre estes aspetos, destacaram-se no decorrer deste trabalho o formato e tipo de tramas, o endereçamento dos componentes envolvidos na comunicação sem fios e operação do protocolo.

Questões

Acesso Rápido

Tal como pedido no enunciado, teremos capturado a trama 41, correspondente ao nosso número de grupo, onde, 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.

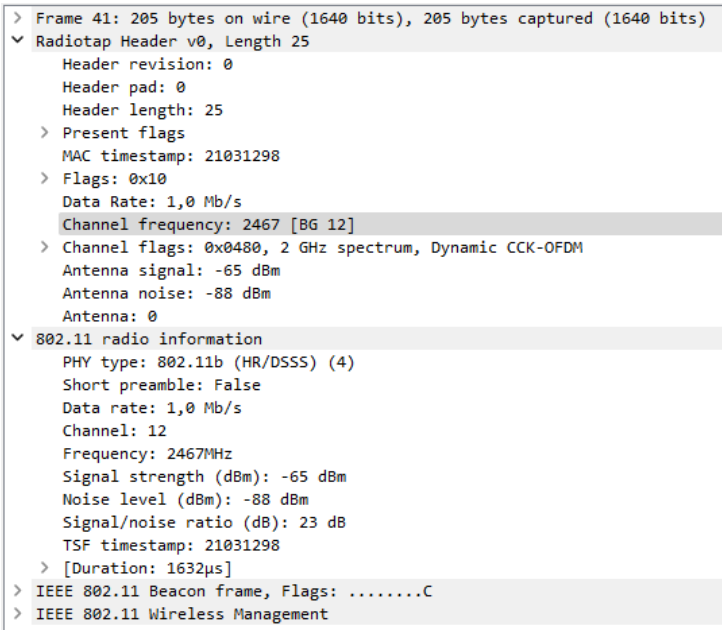


Figura 1 - Trama 802.11 correspondente ao nosso grupo

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

O espectro está a operar numa frequência de 2467 MHz, estando no canal 12, tal como indicado na figura anterior.

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

De acordo com figura anterior, está a ser usada a versão 802.11b, indicada no campo *PHY type*.

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.

A trama analisada foi enviada a um débito (*Data rate*) de 1,0 Mbps, o que se pode observar na figura 1. Não correspondendo este ao débito máximo, uma vez que o máximo desta versão é 11 Mbps, o que se pode observar na seguinte imagem.

IEEE 802.11 Wireless LAN

IEEE 802.11 standard	Year	Max data rate	Range	Frequency
802.11b	1999	11 Mbps	30m	2.4 GHz
802.11g	2003	54 Mbps	30m	2.4 GHz

Figura 2 - Max data rate das versões 802.11b e 802.11g

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 41 o nosso número de grupo, seguimos então para as seguintes questões:

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)?

Como podemos ver na figura a baixo, a trama beacon selecionada é do tipo Management Frame (0) e subtipo Beacon (8). Tal como especificado na secção *frame control field* do cabeçalho.

```
▼ 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
    .000 0000 0000 0000 = Duration: 0 microseconds
    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)
    Source address: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
    BSS Id: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
    .... .... .... 0000 = Fragment number: 0
    1001 0000 1010 .... = Sequence number: 2314
    Frame check sequence: 0xe015c680 [unverified]
    [FCS Status: Unverified]
▶ IEEE 802.11 Wireless Management
```

Figura 3 - Trama 301 (260+41)

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

- Receiver address: ff:ff:ff:ff:ff:ff
- Destination address: ff:ff:ff:ff:ff:ff
- Transmitter address: bc:14:01:af:b1:99
- Source address: bc:14:01:af:b1:99

Podendo concluir então que, uma vez que a origem da trama é o *Access Point* e o endereço MAC de destino é um endereço broadcast, que a trama é enviada para todos os dispositivos capazes de a receber no alcance de AP.

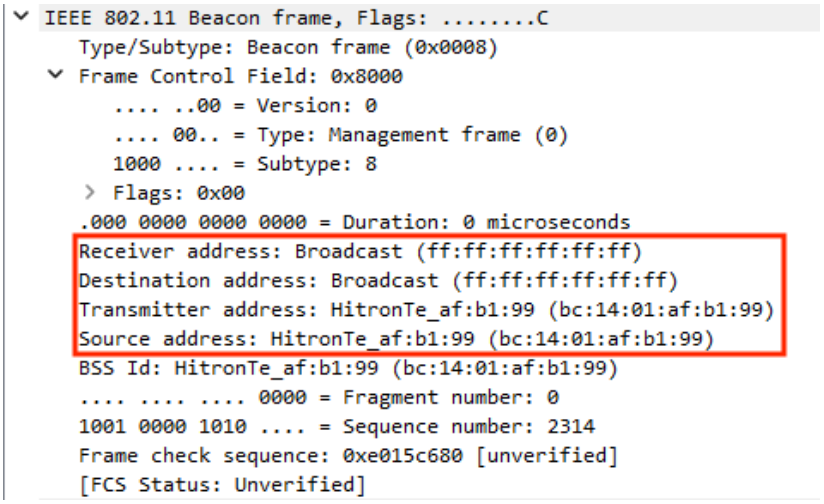


Figura 4 - Endereços MAC em uso

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?**

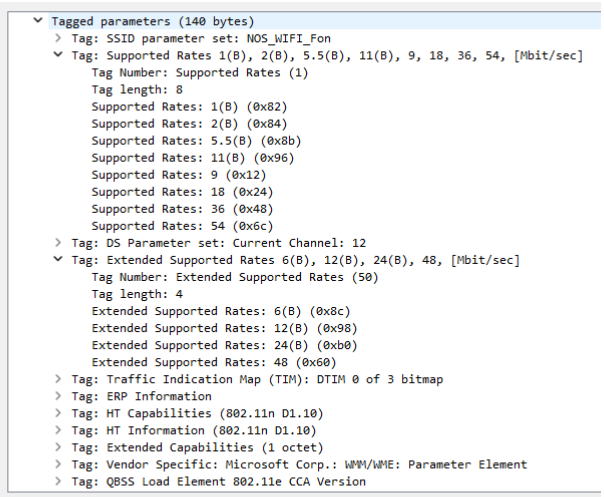


Figura 5 - Débitos suportados e débitos adicionais

Os débitos suportados pela trama, são:

- 1 Mb/s (básico)
- 2 Mb/s (básico)
- 5.5 Mb/s (básico)
- 11 Mb/s (básico)
- 9 Mb/s
- 18 Mb/s
- 36 Mb/s
- 54 Mb/s

Os débitos adicionais são:

- 6 Mb/s (básico)
- 12 Mb/s (básico)
- 24 Mb/s (básico)
- 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.

O intervalo de tempo previsto entre tramas beacon consecutivas, anunciado no em *IEEE 802.11 Wireless Management*, no campo *Beacon Interval* é de 0.102400 segundos. Sendo este valor, na prática, mais uma aproximação do que valor exato, uma vez que podem-se dar atrasos no envio da trama, por parte do AP, podendo então ocorrer alguns erros na precisão da periodicidade das mesmas.

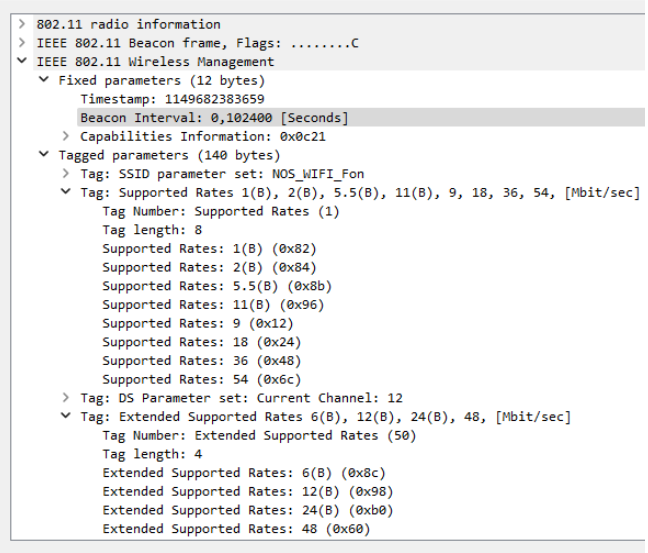


Figura 6 - Intervalo de tempo entre tramas beacon

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).**

Recorrendo ao uso do filtro “wlan.ssid”, obtivemos informação acerca dos SSIDs dos APs que operam na vizinhança da STA de captura.

E graças a este, Identificamos os seguintes SSIDs:

- FlyingNet
- NOS_WIFI_Fon

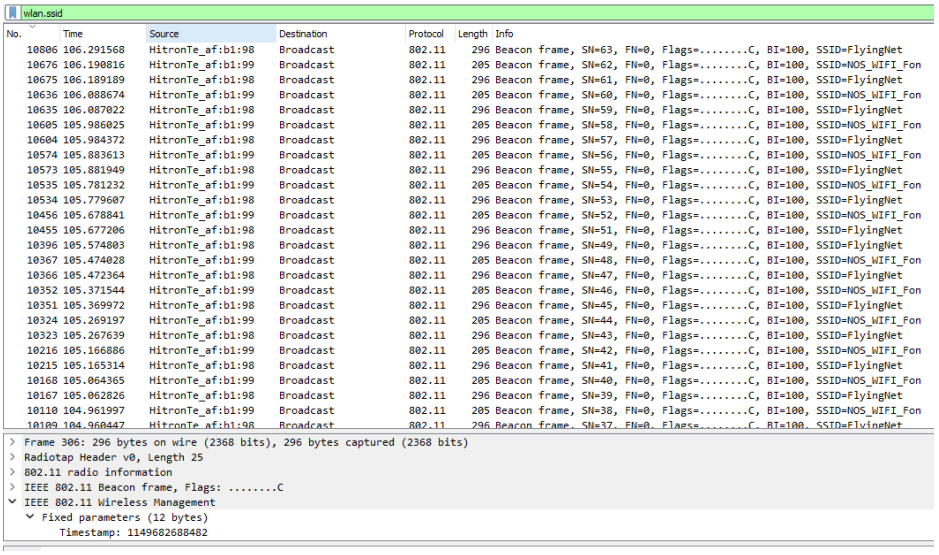
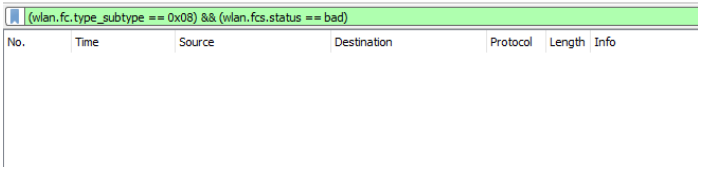


Figura 7 - Tramas beacon recebidas

9. **Verifique se está a ser usado o método de deteção de erros (CRC). Use o filtro *(wlan.fc.type_subtype == 0x08) && (wlan.fcs.status == bad). Que conclui? Justifique o porquê de ser necessário usar deteção de erros em redes sem fios.***

Usando o filtro “(wlan.fc.type_subtype == 0x08) && (wlan.fcs.status == bad)”, tal como sugerido no enunciado, o nosso grupo, mesmo após mudar as definições do wireshark, não conseguiu obter nenhuma trama de beacon com erros, não nos sendo então possível observar este método.

Sendo este muito importante e necessário, uma vez que é utilizado como forma de detetar qualquer tipo de obstrução, interferência ou colisão nas tramas.



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

Para visualizar todas as tramas *probing request* ou *probing response,* simultaneamente, utilizamos o filtro "(wlan.fc.type_subtype == 4) || (wlan.fc.type_subtype ==5)", uma vez que essas tramas, de acordo com a figura 9, dada nas aulas teóricas, têm esses subtipos.

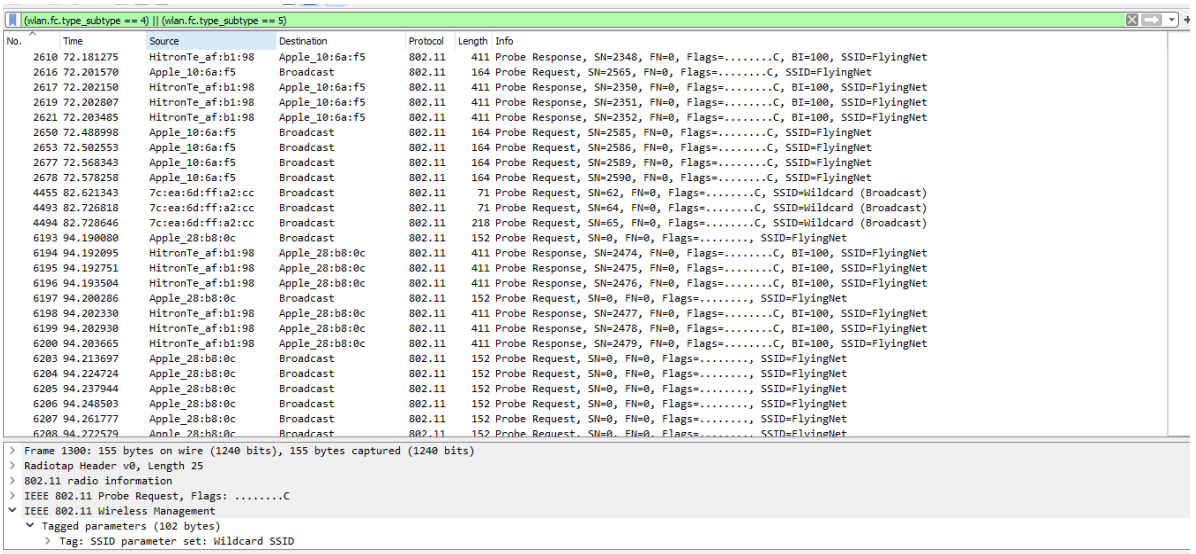


Figura 8 - Tramas probing request e probing response

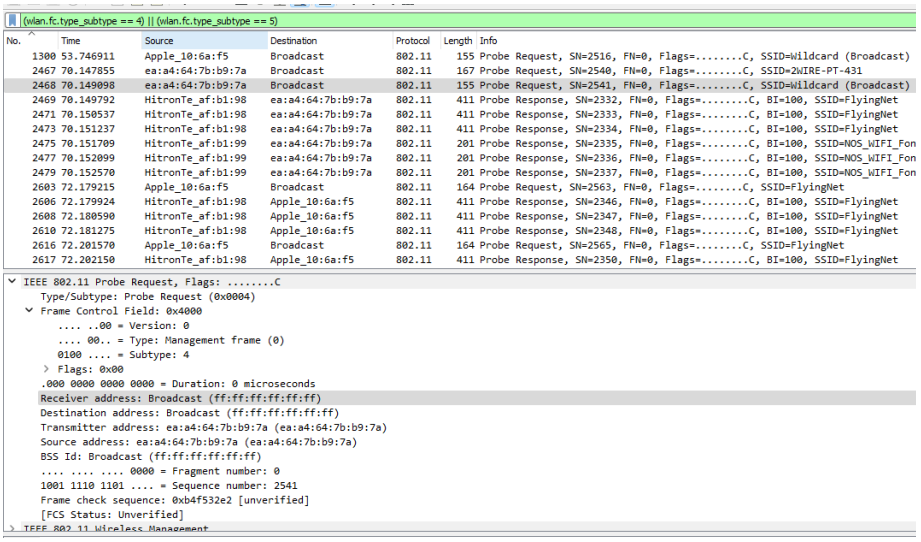
Type value	Type Description	Subtype Value	Subtype description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101	Action
00	Management	1110-1111	Reserved
01	Control	0000-0111	Reserved
01	Control	1000	Block Ack Request
01	Control	1001	Block Ack
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK

Figura 9 - 802.11 frame types and subtypes

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?

Estas tramas endereçam o probing request (sobre quais as redes 802.11 que se encontram na sua proximidade) ao AP. Por sua vez, o AP responde com a informação correspondente.

Figura 10 - Probing Request



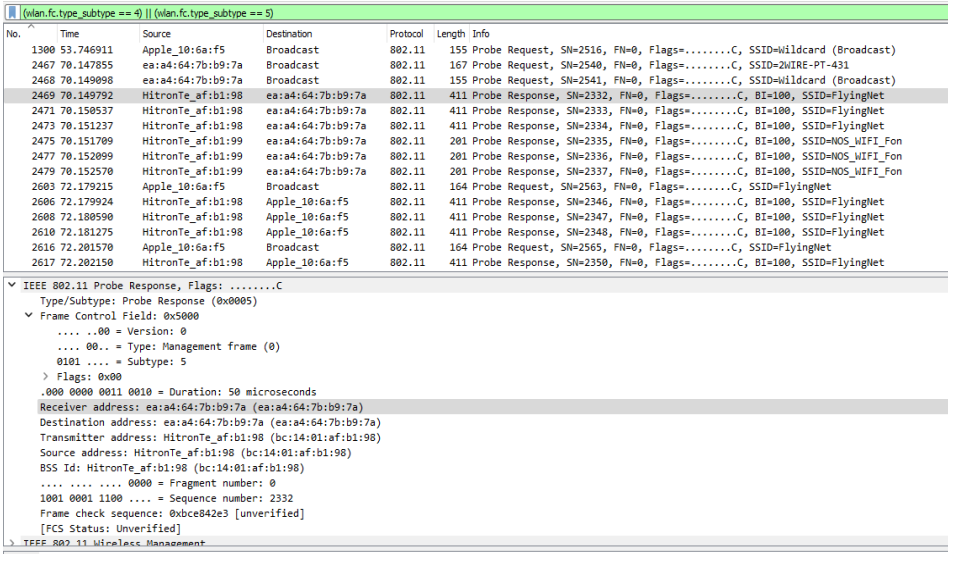


Figura 11 - Probing Reply

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.

Para a sequência de tramas capturada:

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.

Uma vez que um processo de associação completo entre a STA e o AP é feito com base no STA:

- analisar os canais, procurando tramas *beacon* com o nome e endereço MAC do AP
- selecionar o AP a que se quer associar
- fazer autenticação
- usar o DHCP para pôr o seu IP na subnet do AP

De acordo com a figura 9, mostrada anteriormente, iremos então usar o filtro que procura, dentro do tipo 0 (managment), o subtipo beacon (8), association request (0), association response (1) ou autentificação (11), ou seja, usamos o filtro: “wlan.fc.type==0 && (wlan.fc.subtype==0 || wlan.fc.subtype==1 || wlan.fc.subtype==8 || wlan.fc.subtype==11)”.

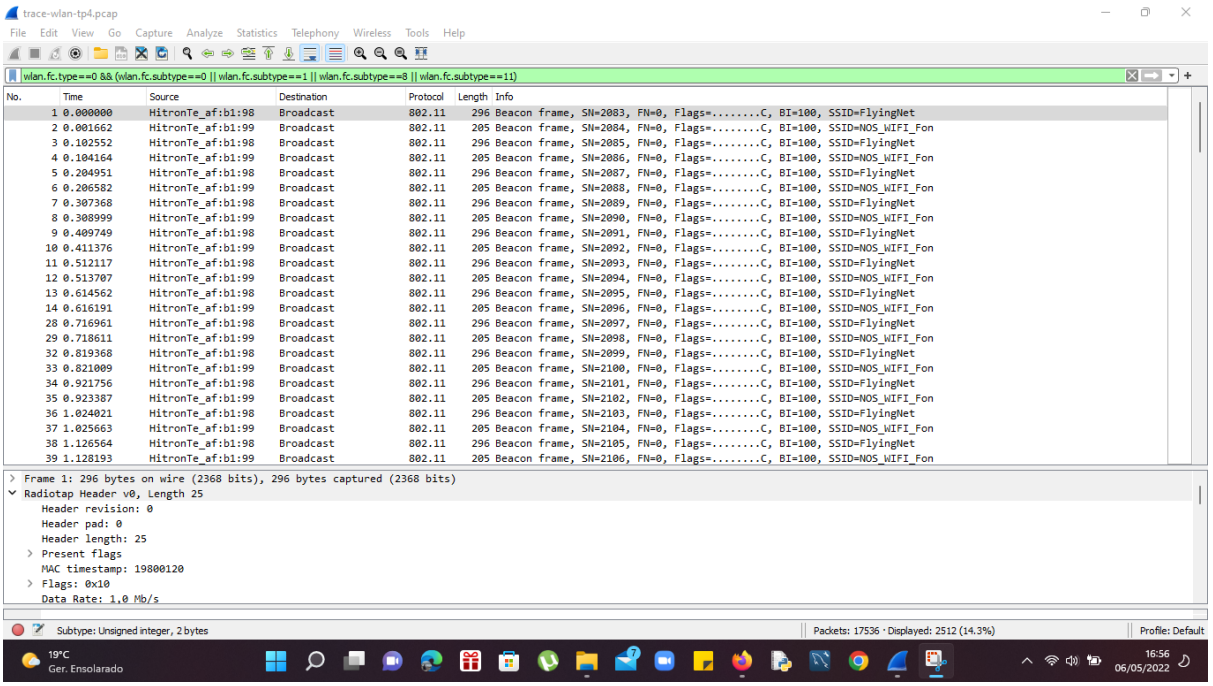


Figura 12 - Sequências de tramas relativas ao processo de associação

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

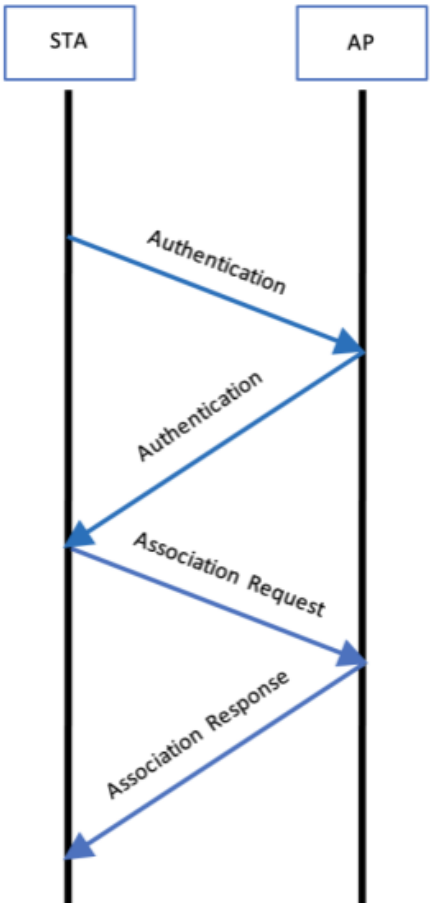


Figura 13 - Diagrama ilustrativo da sequência de todas as tramas trocadas no processo

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.

toDS	fromDS	addr1	addr2	addr3	addr4	obs.
0	0	DA	SA	BSSID	-	ad hoc
0	1	DA	BSSID	SA	-	do AP
1	0	BSSID	SA	DA	-	para AP
1	1	RA	TA	DA	SA	dentro DS

Ficha 14 - 802.11 frame: addressing

14. Considere a trama de dados nº431. Sabendo que o campo Frame Control contido no cabeçalho das tramas 802.11 permite especificar a direcionalidade das tramas, o que pode concluir face à direcionalidade dessa trama, será local à WLAN?

Analisando o campo DS Status, percebemos que se trata da seguinte direcionalidade: **To DS = 0 e From DS = 1.**

Posto isto, e com base nos conceitos abordados nas aulas teóricas, percebemos que a direcionalidade da trama não é local à WLAN.

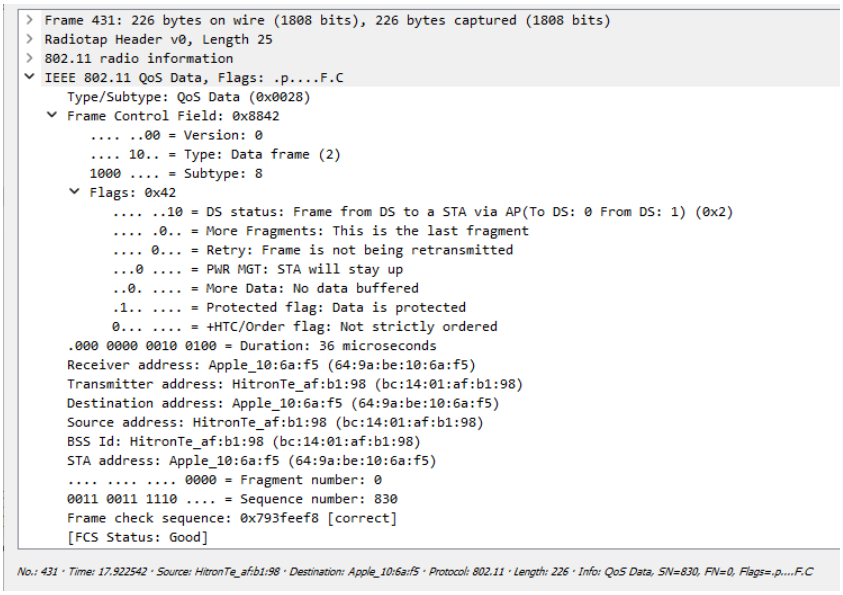


Figura 15 - Frame Control da trama nº431

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?

Endereços MAC:

- STA = 64:9a:be:10:6a:f5
- AP = bc:14:01:af:b1:98
- Router = 64:9a:be:10:6a:f5

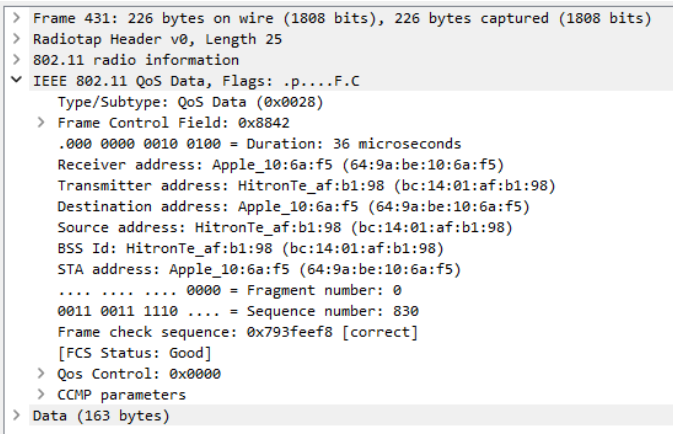


Figura 16 - Endereços MAC em uso na trama de dados nº431

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

Analisando o campo DS Status, percebemos que se trata da seguinte direcionalidade: **To DS = 1 e From DS = 0.**

Posto isto, e com base nos conceitos abordados nas aulas teóricas, percebemos que a direcionalidade da trama vai de STA para DS.

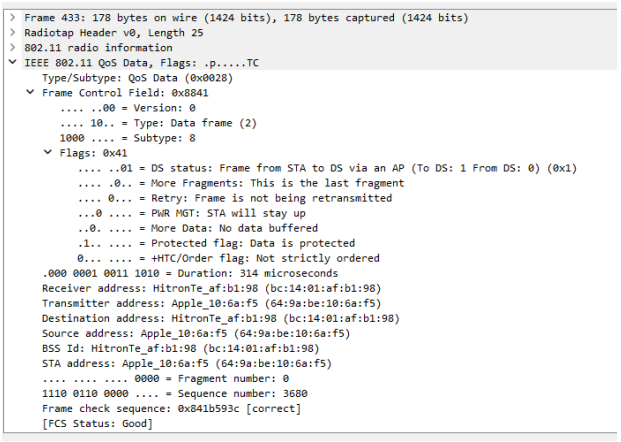


Figura 17 - Trama nº433

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 transmitidas ao longo da transferência de dados são do subtipo controlo ACK (de tipo 1, subtipo 13 - ver figura 9), que são tramas necessárias, uma vez que são utilizadas para enviar informação relativa ao sucesso da transmissão. Ou seja, quando a estação a recebe, esta é um aviso do AP a dizer que correu tudo bem.

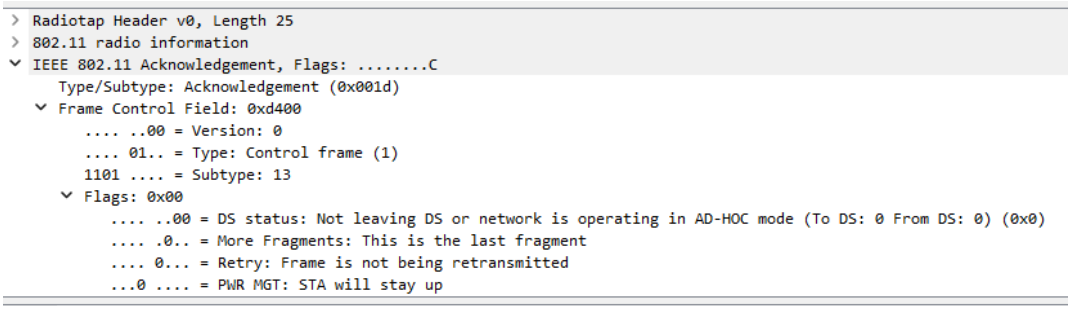


Figura 18 - Tramas de controlo transmitidas

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 direcionalidade 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 não está a ser usada a opção RTS/CTS na troca de dados, tal como se pode ver na seguinte figura:

o.	Time	Source	Destination	Protocol	Length	Info
428	17.922099	Apple_10:6a:f5 (64:…	HitronTe_af:b1:98 (…	802.11	57	802.11 Block Ack, Flags=........C
429	17.922190	HitronTe_af:b1:98 (…	Apple_10:6a:f5 (64:…	802.11	49	802.11 Block Ack Req, Flags=........C
430	17.922271	Apple_10:6a:f5 (64:…	HitronTe_af:b1:98 (…	802.11	57	802.11 Block Ack, Flags=........C
431	17.922542	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	226	QoS Data, SN=830, FN=0, Flags=.p....F.C
432	17.922558		HitronTe_af:b1:98 (…	802.11	39	Acknowledgement, Flags=........C
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
439	18.022592	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2435, FN=0, Flags=........C, BI=100, SSID=FlyingNet
440	18.024220	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2436, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
441	18.124979	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2437, FN=0, Flags=........C, BI=100, SSID=FlyingNet
442	18.126609	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2438, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
443	18.227383	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2439, FN=0, Flags=........C, BI=100, SSID=FlyingNet
444	18.229008	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2440, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
445	18.329740	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2441, FN=0, Flags=........C, BI=100, SSID=FlyingNet
446	18.331430	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2442, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
447	18.432190	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2443, FN=0, Flags=........C, BI=100, SSID=FlyingNet
448	18.433841	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2444, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
449	18.534506	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2445, FN=0, Flags=........C, BI=100, SSID=FlyingNet
450	18.536100	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2446, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
451	18.536165	Apple_71:41:a1	HitronTe_af:b1:98	802.11	68	Null function (No data), SN=1750, FN=0, Flags=.......TC

Figura 19 - Tramas correspondentes ao exemplo anterior

No entanto, esta está presente noutros lugares, como é o caso de, por exemplo:

```
543 21.551568     Apple_10:6a:f5 (64:… HitronTe_af:b1:98 (… 802.11     45 Request-to-send, Flags=........C
544 21.551576                          Apple_10:6a:f5 (64:… 802.11     39 Clear-to-send, Flags=........C
545 21.551751     HitronTe_af:b1:98 (… Apple_10:6a:f5 (64:… 802.11     57 802.11 Block Ack, Flags=........C
```

Figura 20 - Utilização da opção RTS/CTS

Conclusão

Com a realização deste trabalho prático, foi-nos possível expandir o nosso conhecimento no que diz respeito às redes Wireless e a certos aspetos do protocolo IEEE 802.11, aprendendo diversos conceitos, tais como: mecanismos de controlo de acesso, processo de associação nas redes IEEE 802.11, o formato das tramas, endereçamento dos componentes envolvidos na comunicação sem fios e a operação do protocolo, por exemplo.