Redes de computadores

Trabalho Prático Nº4 – Redes sem Fios (Wi-Fi)

Pedro Calheno Pinto, Diogo do Rego Neto, and Samuel Macieira Ferreira

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a87983,a98197,a100654}@alunos.uminho.pt

1 Acesso Rápido

Como pode ser observado, a sequência de bytes capturada inclui meta-informação do nível físico (radiotap header, radio information) obtida do firmware da interface Wi-Fi, para além dos bytes correspondentes a tramas 802.11.

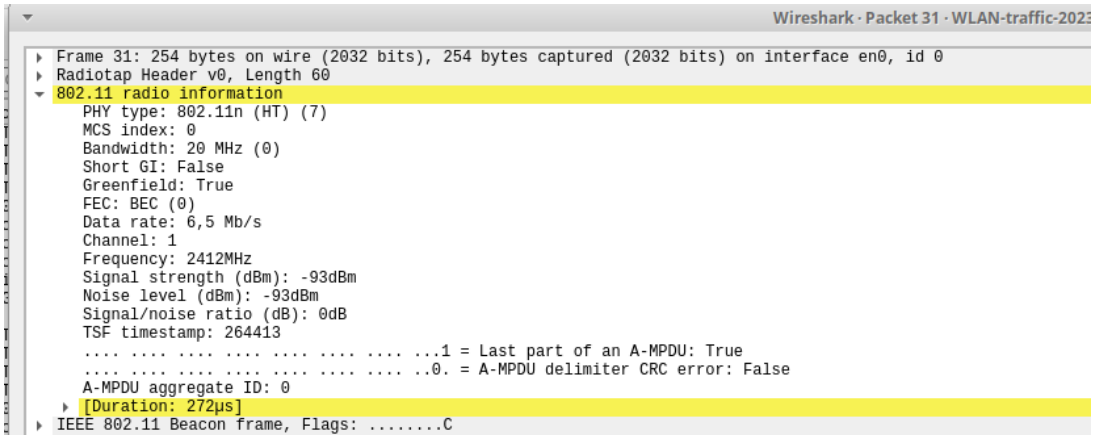


Fig. 1. Trama 802.11

1.1 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 a 2467Hz de frequência. O canal correspondente e 1. Isto pode ser verificado nas entrada Frequency e Channel da imagem acima.

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

Como nos indica o campo PHY type, está a ser usada a versão 802.11n.

1.3 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.

O débito a que foi enviada foi de 6,5 MB/s. Este valor não corresponde ao débito máximo desta interface Wi-Fi, visto que o débito máximo da versão 802.11n da norma IEEE 802.11 é 600 Mbit/s. Este débito pode ser justificado devido às várias melhorias e tecnologias introduzidas em relação às versões anteriores da norma IEEE 802.11.

1.4 Verifique qual a força do sinal (Signal strength) e a qualidade expectável de receção da trama, sabendo que:

No campo Signal strength, vemos que o valor da força do sinal é de -93dBm que, de acordo com a tabela, neste nível, verificamos que as chances de haver conexão são muito baixas.

Signal strength	Expected Quality
-90dBm	Chances of connecting are very low at this level
-80dBm	Unreliable signal strength
-67dBm	Reliable signal strength– the edge of what Cisco considers to be adequate to support Voice over WLAN
-55dBm	Anything down to this level can be considered excellent signal strength.
-30dBm	Maximum signal strength, you are probably standing right next to the access point.

Fig. 2. Tabela de força de sinal

1.5 Selecione uma trama beacon cuja ordem (ou terminação) corresponda a XX. Esta trama pertence a que tipo de tramas 802.11? Identifique o valor dos identificadores de tipo e de subtipo da trama. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?

Através da tabela presente no anexo podemos comprovar que o frame 31 com Type Value de 00 pertence a tramas de tipo Management e que o Subtype Value de 1000 indica um subtipo Beacon (8). Podemos ver nas figuras abaixo que estes valores se encontram na entrada Frame Control Field.

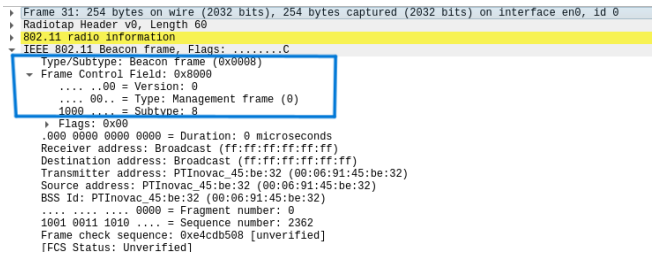


Fig. 3. Tabela de força de sinal

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

```
.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: PTInovac_45:be:32 (00:06:91:45:be:32)
Source address: PTInovac_45:be:32 (00:06:91:45:be:32)
BSS Id: PTInovac_45:be:32 (00:06:91:45:be:32)
```

O Receiver Address e o Destination Address têm o MAC address ff:ff:ff:ff:ff:ff, que corresponde ao broadcast O Source Address é o MAC address do MAC AP. No caso do destino a trama é enviada para todos os dispositivos capazes de a receber num determinado alcance.

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

Podemos identificar a presença de cinco tramas de beacon com erros, com base na informação do campo FCS Status. A existência desse campo indica que um método de detecção de erros está a ser utilizado. A detecção de erros em redes sem fio é utlizada para identificar interferências ou bloqueios nas tramas.

1.8 Uma trama beacon anuncia que o AP pode suportar vários débitos de base (B), assim como vários débitos adicionais (extended supported rates). Indique quais são esses débitos.

Como podemos ver na imagem o AP consegue suportar débitos de 6, 12, 24 e 48 Mbit/sec.

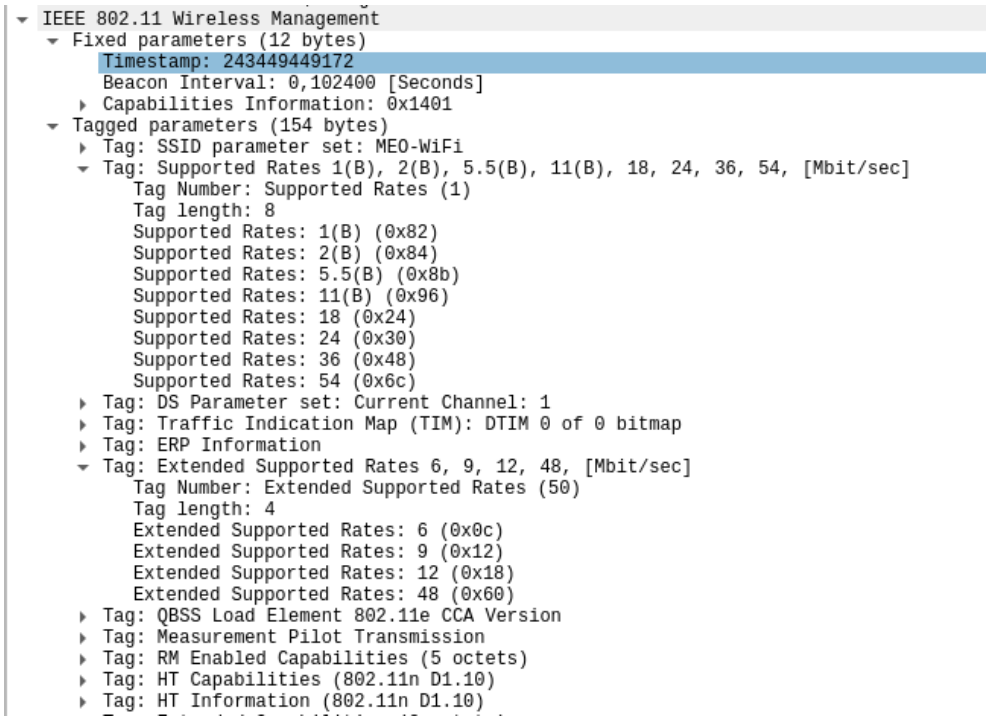


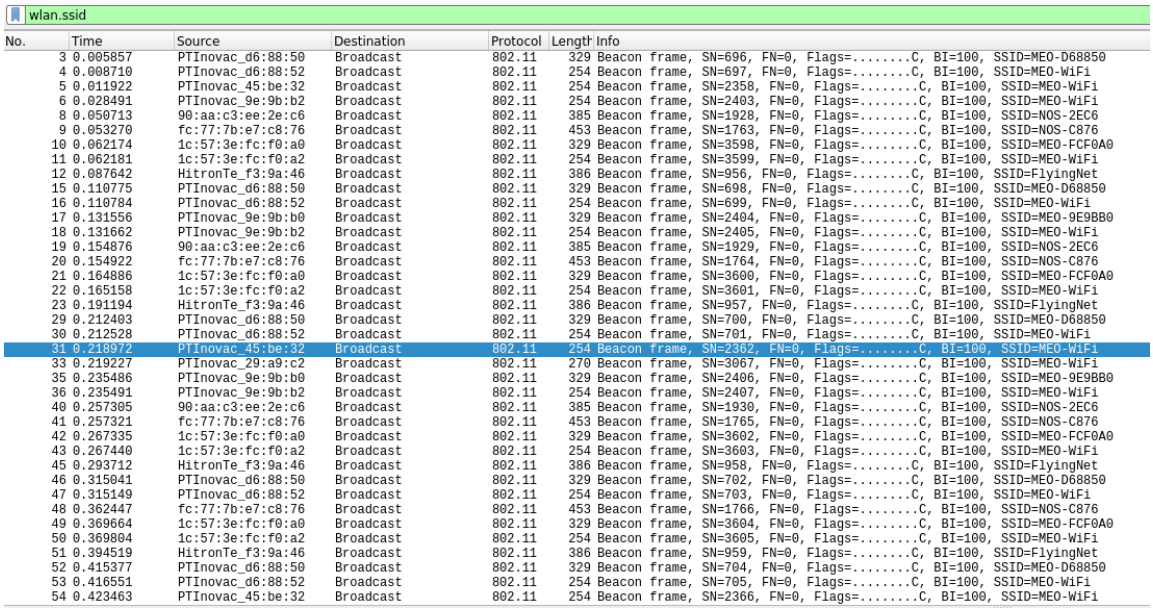
Fig. 4. Débitos da trama

1.9 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.

Como podemos ver na figura 4, o intrevalo de tempo previsto é 0.102400 segundos, na prática a periodicidade não é exata mas é bastante precisa, sendo que ela aumenta quanto maior for o tráfego.

1.10 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 que estão a operar na vizinhança da STA de captura são os que se pode visualizar na imagem. Para obtermos os SSIDS aplicamos o filtro "wlan.ssid". Através deste filtro, podemos ver que, para um certo intervalo de tempo, são recebidas tramas beacon provenientes dos vários APs diferentes.



wlan.ssid

No.	Time	Source	Destination	Protocol	Length	Info
3	0.005857	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=696, FN=0, Flags=........C, BI=100, SSID=MEO-D68850
4	0.008710	PTInovac_d6:88:52	Broadcast	802.11	254	Beacon frame, SN=697, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
5	0.011922	PTInovac_45:be:32	Broadcast	802.11	254	Beacon frame, SN=2358, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
6	0.028491	PTInovac_9e:9b:b2	Broadcast	802.11	254	Beacon frame, SN=2403, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
8	0.050713	90:aa:c3:ee:2e:c6	Broadcast	802.11	385	Beacon frame, SN=1928, FN=0, Flags=........C, BI=100, SSID=NOS-2EC6
9	0.053270	fc:77:7b:e7:c8:76	Broadcast	802.11	453	Beacon frame, SN=1763, FN=0, Flags=........C, BI=100, SSID=NOS-C876
10	0.062174	1c:57:3e:fc:f0:a0	Broadcast	802.11	329	Beacon frame, SN=3598, FN=0, Flags=........C, BI=100, SSID=MEO-FCF0A0
11	0.062181	1c:57:3e:fc:f0:a2	Broadcast	802.11	254	Beacon frame, SN=3599, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
12	0.087642	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=956, FN=0, Flags=........C, BI=100, SSID=FlyingNet
15	0.110775	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=698, FN=0, Flags=........C, BI=100, SSID=MEO-D68850
16	0.110784	PTInovac_d6:88:52	Broadcast	802.11	254	Beacon frame, SN=699, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
17	0.131556	PTInovac_9e:9b:b0	Broadcast	802.11	329	Beacon frame, SN=2404, FN=0, Flags=........C, BI=100, SSID=MEO-9E9BB0
18	0.131662	PTInovac_9e:9b:b2	Broadcast	802.11	254	Beacon frame, SN=2405, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
19	0.154876	90:aa:c3:ee:2e:c6	Broadcast	802.11	385	Beacon frame, SN=1929, FN=0, Flags=........C, BI=100, SSID=NOS-2EC6
20	0.154922	fc:77:7b:e7:c8:76	Broadcast	802.11	453	Beacon frame, SN=1764, FN=0, Flags=........C, BI=100, SSID=NOS-C876
21	0.164886	1c:57:3e:fc:f0:a0	Broadcast	802.11	329	Beacon frame, SN=3600, FN=0, Flags=........C, BI=100, SSID=MEO-FCF0A0
22	0.165158	1c:57:3e:fc:f0:a2	Broadcast	802.11	254	Beacon frame, SN=3601, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
23	0.191194	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=957, FN=0, Flags=........C, BI=100, SSID=FlyingNet
29	0.212403	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=700, FN=0, Flags=........C, BI=100, SSID=MEO-D68850
30	0.212528	PTInovac_d6:88:52	Broadcast	802.11	254	Beacon frame, SN=701, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
31	0.218972	PTInovac_45:be:32	Broadcast	802.11	254	Beacon frame, SN=2362, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
33	0.219227	PTInovac_29:a9:c2	Broadcast	802.11	270	Beacon frame, SN=3067, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
35	0.235486	PTInovac_9e:9b:b0	Broadcast	802.11	329	Beacon frame, SN=2406, FN=0, Flags=........C, BI=100, SSID=MEO-9E9BB0
36	0.235491	PTInovac_9e:9b:b2	Broadcast	802.11	254	Beacon frame, SN=2407, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
40	0.257305	90:aa:c3:ee:2e:c6	Broadcast	802.11	385	Beacon frame, SN=1930, FN=0, Flags=........C, BI=100, SSID=NOS-2EC6
41	0.257321	fc:77:7b:e7:c8:76	Broadcast	802.11	453	Beacon frame, SN=1765, FN=0, Flags=........C, BI=100, SSID=NOS-C876
42	0.267335	1c:57:3e:fc:f0:a0	Broadcast	802.11	329	Beacon frame, SN=3602, FN=0, Flags=........C, BI=100, SSID=MEO-FCF0A0
43	0.267440	1c:57:3e:fc:f0:a2	Broadcast	802.11	254	Beacon frame, SN=3603, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
45	0.293712	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=958, FN=0, Flags=........C, BI=100, SSID=FlyingNet
46	0.315041	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=702, FN=0, Flags=........C, BI=100, SSID=MEO-D68850
47	0.315149	PTInovac_d6:88:52	Broadcast	802.11	254	Beacon frame, SN=703, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
48	0.362447	fc:77:7b:e7:c8:76	Broadcast	802.11	453	Beacon frame, SN=1766, FN=0, Flags=........C, BI=100, SSID=NOS-C876
49	0.369664	1c:57:3e:fc:f0:a0	Broadcast	802.11	329	Beacon frame, SN=3604, FN=0, Flags=........C, BI=100, SSID=MEO-FCF0A0
50	0.369804	1c:57:3e:fc:f0:a2	Broadcast	802.11	254	Beacon frame, SN=3605, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
51	0.394519	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=959, FN=0, Flags=........C, BI=100, SSID=FlyingNet
52	0.415377	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=704, FN=0, Flags=........C, BI=100, SSID=MEO-D68850
53	0.416551	PTInovac_d6:88:52	Broadcast	802.11	254	Beacon frame, SN=705, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
54	0.423463	PTInovac_45:be:32	Broadcast	802.11	254	Beacon frame, SN=2366, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi

Fig. 5. Tráfego após aplicar filtro wlan.ssid

1.11 Estabeleça um filtro Wireshark apropriado que lhe permita visualizar todas as tramas probing request e probing response, simultaneamente

O filtro que permite visualizar as tramas probing é:

wlan.fc.type == 0 (wlan.fc.subtype == 4 || wlan.fc.subtype ==5)

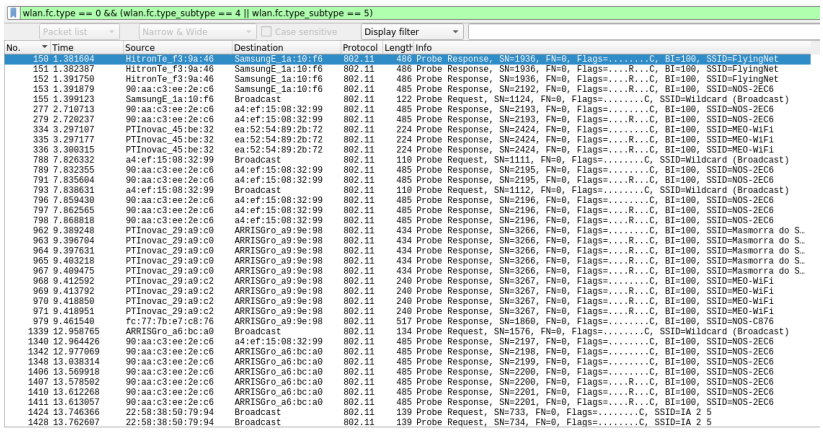


Fig. 6. Tráfego após aplicar filtro probbing

1.12 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?

Uma estação envia um probing request em broadcast para descobrir quais redes 802.11 estão ao seu redor. O probing request é um tipo de frame de management no padrão 802.11 que é usado pelas estações (dispositivos cliente) para solicitar informações sobre as redes sem fio disponíveis.

Quando um Access Point (AP) recebe o probing request, este responde enviando um probing response à estação que fez a solicitação. O probing response contém informações relativas ao AP, como o SSID (Service Set Identifier), a taxa de transferência suportada, os canais disponíveis, as opções de segurança e outras informações relevantes.

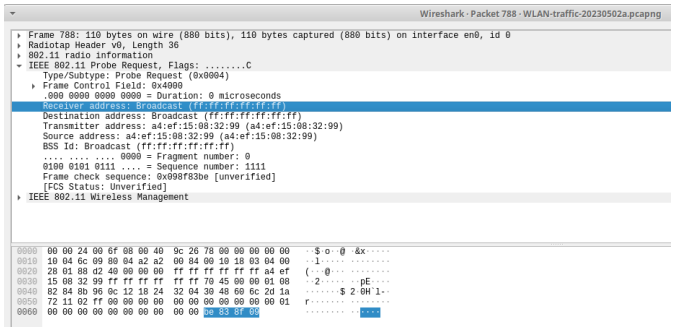


Fig. 7. Probing Request

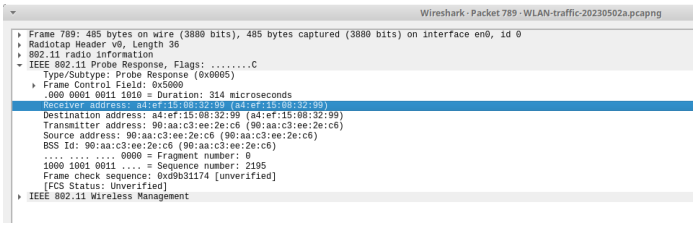


Fig. 8. Probing Response

1.13 Identifique uma sequência de tramas que corresponda a um processo de associação realizado com sucesso entre a STA e o AP, incluindo a fase de autenticação.

Na figura podemos ver o processo de associação entre os dois dispositivos.

8510	73.542828	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	73 Action, SN=1, FN=0, Flags=........C
8511	73.542835		HitronTe_f3:9a:46 (…	802.11	48 Acknowledgement, Flags=........C
8512	73.542839	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	73 Action, SN=612, FN=0, Flags=........C
8513	73.542845		AzureWav_0f:0e:9b (…	802.11	48 Acknowledgement, Flags=........C

Fig. 9. Tramas trocadas no processo

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

O diagrama abaixo ilustra as tramas trocadas no processo

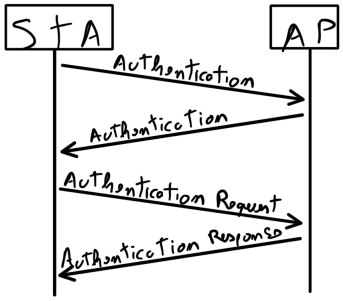


Fig. 10. Tramas trocadas no processo

1.15 Considere a trama de dados nº8503. 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?

Através do campo DS status podemos verificar que o valor to DS é 1 e o de from DS é 0. O valor destas flags permite inferir a direcionalidade dessa trama. Assim, podemos concluir que a trama vem do STA para o DS, ou seja, é local à WLAN.

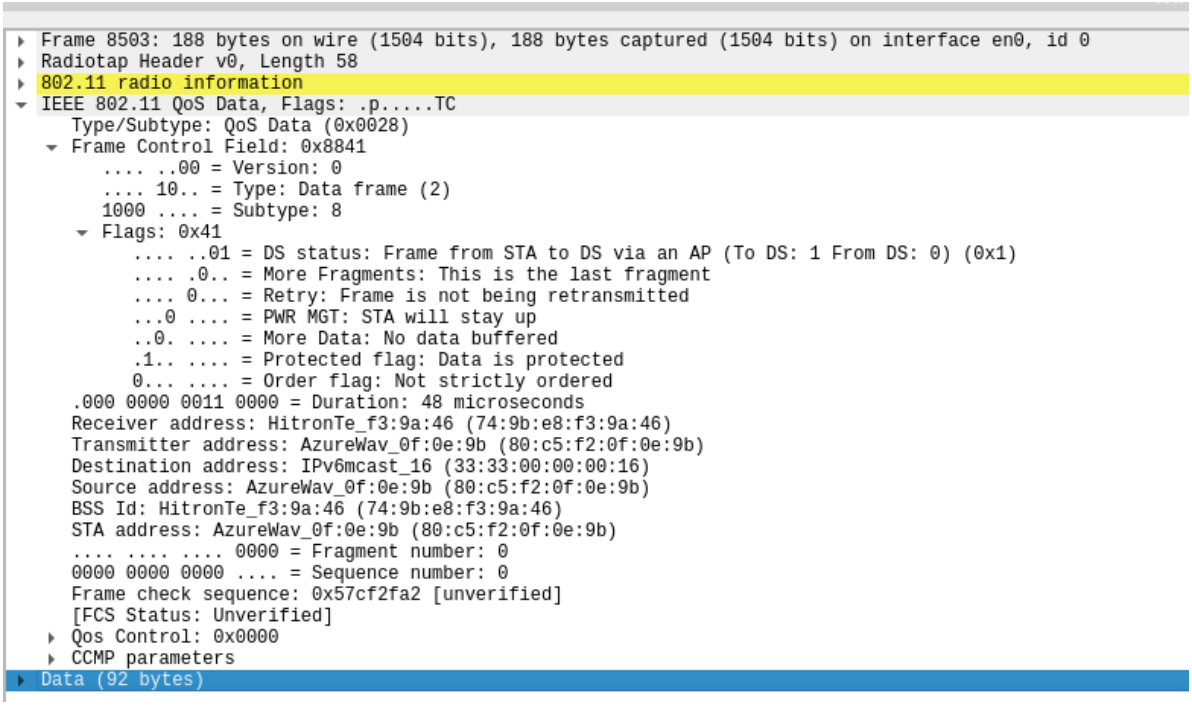


Fig. 11. Frame Control da trama de dados nº 8503

1.16 Para a trama de dados nº8503, transcreva os endereços MAC em uso, identificando quais os endereços correspondentes à estação sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição (DS)?

Endereço STA: 74:9b:e8:f3:9a:46 (Receiver address)

Endereço AP: 80:c5:f2:0f:0e:9b (Transmitter address)

Endereço do router de acesso: 33:33:00:00:00:16 (Destination address)

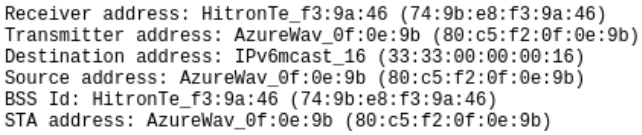


Fig. 12. Trama de dados nº 8503

1.17 Como interpreta a trama nº8521 face à sua direccionalidade e endereçamento MAC?

Podemos inferir a direcionalidade da trama a partir da análise das flags to DS e from DS, que assumem os valores 0 e 1, respetivamente. Assim concluimos que o trama vem do DS para o STA.

```
Receiver address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
Transmitter address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
Destination address: IPv6mcast_16 (33:33:00:00:00:16)
Source address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
BSS Id: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
STA address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
```

Fig. 13. Trama de dados nº 8503

1.18 Que subtipo de tramas de controlo são transmitidas ao longo da transferência de dados acima mencionada? Tente explicar a razão de terem de existir (contrariamente ao que acontece numa rede Ethernet.)

São transmitidas as tramas de controlo ACK. Estas tramas são necessárias como indicador de que a transmissão foi efetuada com sucesso. Quando a estação recebe uma trama ACK, esta é um aviso positivo por parte do AP a indicar que tudo correu com sucesso.

```
8510 73.542828    HitronTe_f3:9a:46   AzureWav_0f:0e:9b    802.11     73 Action, SN=1, FN=0, Flags=........C
8511 73.542835                        HitronTe_f3:9a:46 (… 802.11     48 Acknowledgement, Flags=........C
8512 73.542839    AzureWav_0f:0e:9b   HitronTe_f3:9a:46    802.11     73 Action, SN=612, FN=0, Flags=........C
8513 73.542845                        AzureWav_0f:0e:9b (… 802.11     48 Acknowledgement, Flags=........C
```

Fig. 14. Trama de dados ACK

1.19 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.

Na figura que as tramas selecionadas correspondem a um RTS e a um CTS, também vemos a opção RTS/CTS na troca de dados entre STA e o AP/Router da WLAN.

```
533 21.548964   Apple_10:6a:… HitronTe_af:… 802.11     45 Request-to-send, Flags=........C
534 21.548970                 Apple_10:6a:… 802.11     39 Clear-to-send, Flags=........C
```

Fig. 15.

2 Conclusão

Durante nosso trabalho, adquirimos um conhecimento aprofundado sobre o protocolo IEEE 802.11, o que nos permitiu compreender diversos conceitos importantes. Exploramos as características e elementos das redes sem fio, bem como o endereçamento das tramas Wi-Fi e os mecanismos de controle de acesso. Ao analisarmos mais detalhadamente as tramas de dados contidas nos vários pacotes capturados, obtivemos informações valiosas sobre o funcionamento de toda a rede.

Uma ferramenta fundamental que utilizamos ao longo do trabalho foi o Wireshark. Através do seu uso e da pesquisa de filtros apropriados, conseguimos extrair informações relevantes de forma mais eficiente. Os filtros permitiram-nos segmentar e visualizar as tramas específicas que desejávamos investigar, facilitando a obtenção de respostas precisas..

No geral, a combinação do conhecimento adquirido sobre o protocolo 802.11, juntamente com a utilização do Wireshark foi fundamental para o sucesso deste trabalho. Esta abordagem permitiu-nos explorar as nuances da rede sem fio e obter boas ideias para a compreensão e melhoria do seu funcionamento.