Universidade do Minho

Licenciatura em Engenharia Informática

Redes de Computadores

Grupo 135

TP4: Redes Sem Fios (*Wi-Fi*)

Joana Alves (A93290)

João Machado (A89510)

Rui Armada (A90468)

Maio 2022

Questões e Respostas

1 Questão 4 - Trama de ordem 135

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

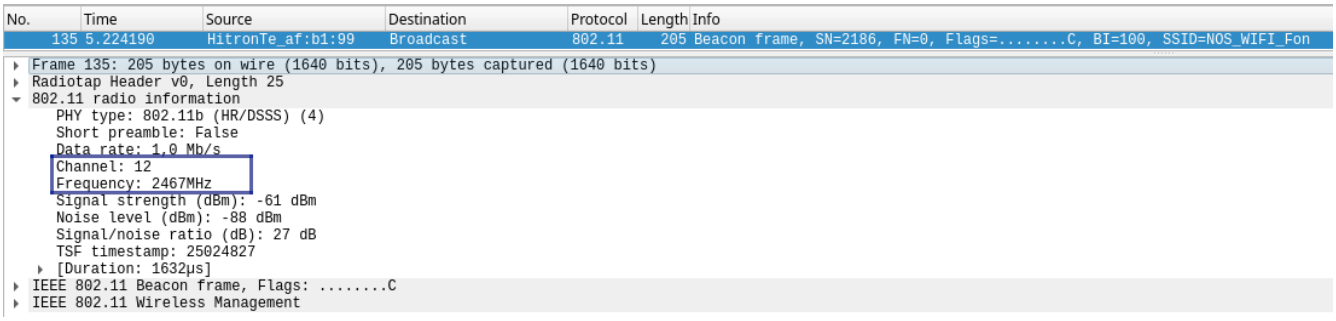


Figura 1: Captura da Trama Nº 135.

Pela Figura 1, através do campo *Frequency* conseguimos denotar que a rede sem fios está a operar a **2467MHz** e, através do campo *Channel* verificamos que corresponde ao canal **12**.

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

Pela Figura 1, no campo *PHY type*, conseguimos denotar a versão da norma IEEE 802.11 que está a ser utilizada, sendo esta a **802.11b**.

c. 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 escolhida foi enviada com o débito de **1.0 Mb/s** (podemos verificar este valor no campo *Data Rate*), no entanto, este débito não corresponde ao débito máximo a que a interface *Wi-Fi* pode operar, uma vez que na versão IEEE 802.11b, o débito máximo é de 11Mb/s.

2 Questão 5 - XX = 135

a. 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 subtipo. Em que parte concreta do cabeçalho da trama estão especificados? (ver anexo)

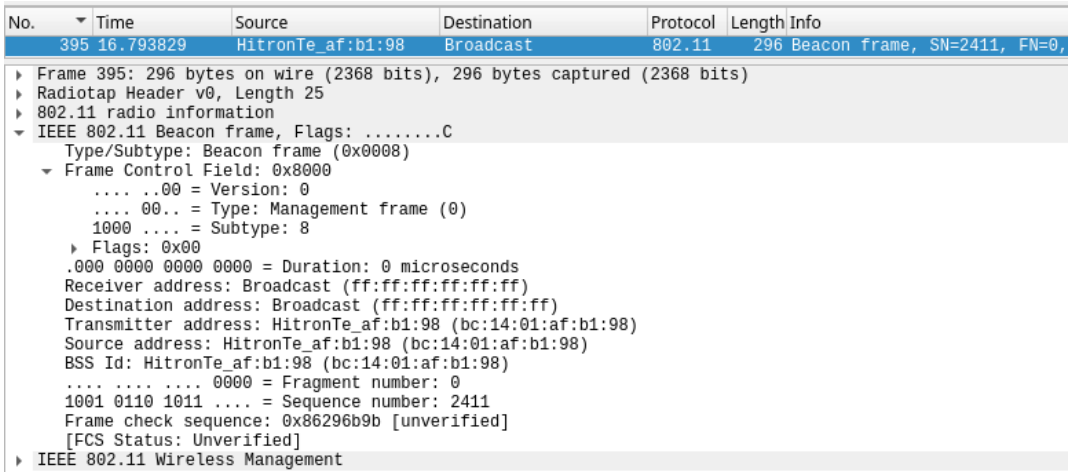
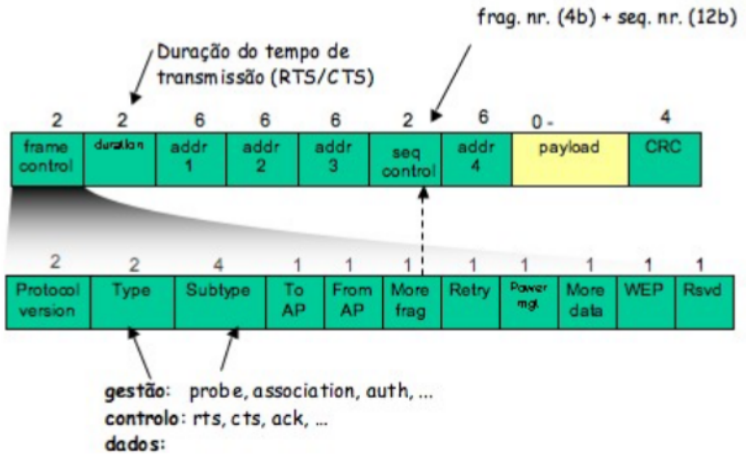


Figura 2: Captura da Trama Nº 395.

A trama selecionada é a trama de ordem **395** e pertence ao tipo de tramas **802.11b (HR/DSSS)**. O campo de tipo tem como valor **0** que corresponde ao tipo *Management* e o campo de subtipo possui o valor **8** que corresponde ao subtipo *Beacon*. Estes valores estão especificados dentro dos primeiros dois *bytes* do cabeçalho alusivos à *frame control*, em particular, nos *bits* nº 3-4 (tipo - campo *Type*) e nº 5-8 (subtipo - campo *SubType*) como podemos ver pelo esquema abaixo (cedido pelos docentes):



b. 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:b1:98
- **Source Address:** bc:14:01:af:b1:98

Pela análise da trama, denotamos que tem como origem (*Source* e *Transmitter Address*) um endereço MAC válido (relativo ao AP). O AP envia periodicamente tramas *beacon* para anunciar a sua presença e transmitir informações a todas as interfaces rádio que estão dentro do seu alcance, daí o campo do endereço destino (*Receiver* e *Destination Address*) possuir o endereço com o valor ff:ff:ff:ff:ff:ff que corresponde a uma trama de *broadcast*.

c. 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?

A partir do campo *Tagged Parameters*, conseguimos denotar tanto os débitos base (*Supported Rates*) como os débitos adicionais (*Extended Rates*) suportados pelo AP.

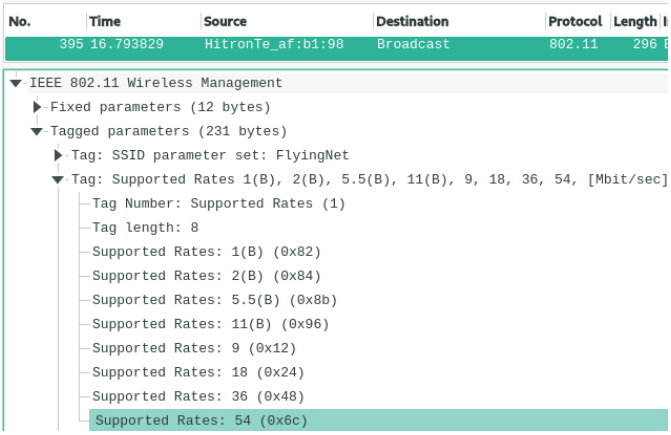


Figura 3: AP ***Supported*** *Rates*.

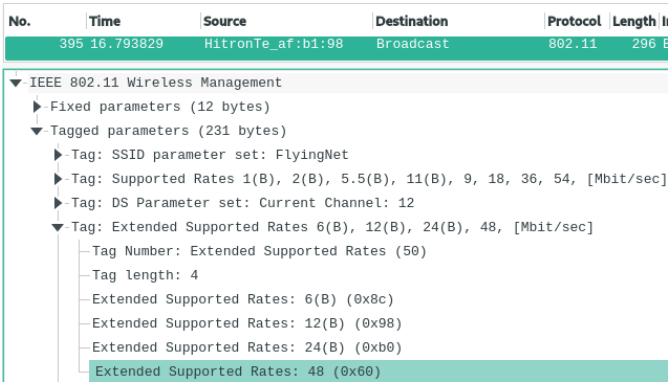


Figura 4: AP ***Extended*** *Rates*.

d. 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 valor do intervalo de tempo previsto entre tramas *beacon* consecutivas é anunciado na própria trama *Beacon*, estando presente no campo ***Beacon Interval***, neste caso, com o valor de **0.1024 segundos**. No entanto, este valor, apesar de estar definido na trama, pode não ser respeitado com precisão, podendo haver atrasos ou adiantamentos, uma vez que os tempos de transmissão do AP podem variar de acordo com a sua "carga" de transmissão no momento.

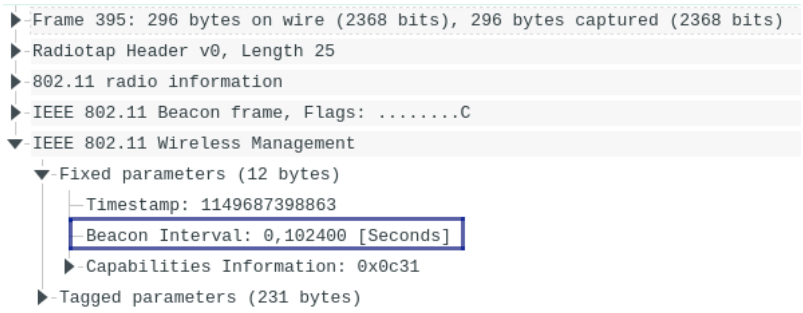


Figura 5: Intervalo de Tempo tramas *Beacon*.

e. Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura? Explicite o modo como obteve esta informação (por exemplo, se usou algum filtro para o efeito).

Para obtermos os SSIDs que estão a operar na vizinhança da STA de captura, tivemos de desenvolver um filtro a aplicar na ferramenta *Wireshark*. Assim, como sabemos que o tipo de tramas utilizadas pelos APs para anunciar a sua presença são as tramas *Beacon* e o seu valor é 8 (já consultado nas alíneas anteriores), aplicamos o seguinte filtro:

wlan.fc.type_subtype == 0x08

De seguida, obtivemos o seguinte resultado notando várias tramas que obedecem ao filtro, mas apenas dois SSID's distintos na vizinhança: **FlyingNet** e **NOS_WIFI_Fon**.

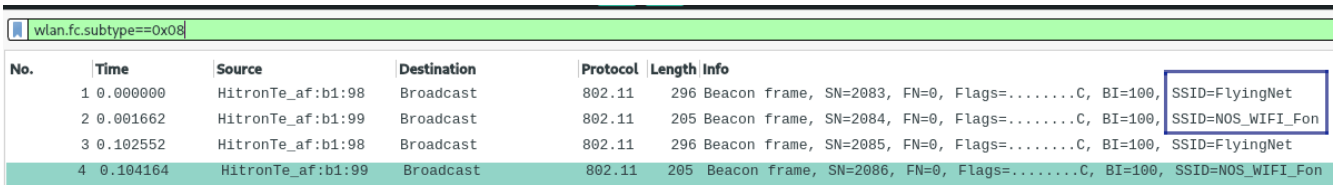


Figura 6: SSIDs na vizinhança da STA de captura.

Conseguimos confirmar que apenas existem estes dois SSIDs uma vez que quando adicionamos as seguintes condições ao filtro acima, o resultado foi vazio:

... && (wlan.ssid != NOS_WIFI_Fon) && (wlan.ssid != FlyingNet)

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

O campo ***Frame Check Sequence*** (FCS) é utilizado para verificar a integridade do pacote do lado que a recebe. O recetor analisa e calcula o valor CRC correto do pacote, comparando de seguida com o valor que realmente veio na trama. Assim, se os valores não coincidirem, o pacote é considerado corrumpido. Neste caso em particular, para obtermos as várias tramas *beacon* WLAN possivelmente corrumpidas, aplicamos o filtro fornecido pelos docentes:

$$\boxed{(\text{wlan.fc.type\_subtype} == 0\text{x}08) \;\&\&\; (\text{wlan.fcs.status} == \text{bad})}$$

No entanto, apesar do filtro estar bem construído não obtivemos qualquer resultado de tramas capturadas que obedecessem ao mesmo (Figura 8). Para além disto, notamos que caso apenas aplicássemos a primeira parte do filtro (*wlan.fc.type_subtype == 0x08*), obtínhamos tramas que, ao analisarmos o conteúdo da mesma, continham o valor *unverified* no campo FCS (Figura 7), não podendo tirar conclusões sobre a utilização do método de deteção de erros CRC.

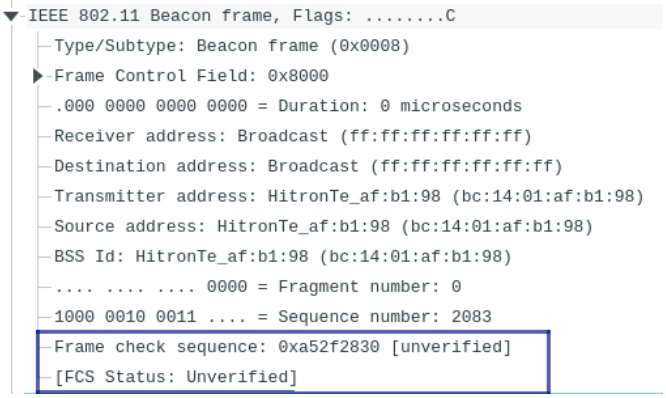


Figura 7: Primeira captura.

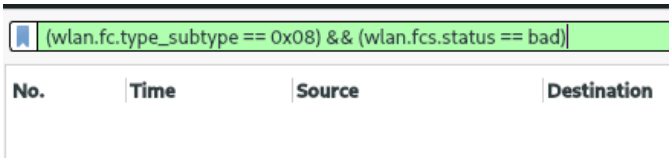


Figura 8: Resultado do filtro completo.

Após uma pesquisa *online* sobre a ferramenta *Wireshark*, descobrimos que esta opção estaria desativada. Como tal, ativamos a opção seguindo os passos encontrados neste site: Enabling FCS. Voltamos a analisar o tráfego capturado, inserindo o filtro completo mas voltamos a obter um resultado vazio. Assim, atribuímos o não obtermos tramas *beacon* corrumpidas a mau funcionamento da ferramenta ou da captura, uma vez que quando apenas aplicamos a segunda parte do filtro, ou seja, filtrar quaisquer tramas corrumpidas, o *Wireshark* consegue apresentar resultados.

Uma vez que redes *Wi-Fi* se propagam pelo meio (sem fios), estas são propícias a erros, pois estão vulneráveis a interferências como obstáculos que não consigam ultrapassar ou que provoquem distorção no conteúdo transmitido. Como tal, a utilização de métodos de deteção de erros é fulcral para evitar falhas na transmissão de tramas, uma vez que uma mudança em apenas um *bit* pode ter como consequência a corrupção do pacote.

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

De forma a restringir a procura de tramas *probing request* e *response*, apenas nos bastou aplicar o filtro ao campo do subtipo da trama, isto é, igualar o tipo e subtipo aos seus valores devidos em hexadecimal: **0x04** (*management probe request*) e **0x05** (*management probe response*).

(wlan.fc.type_subtype == 0x04) **or** (wlan.fc.type_subtype == 0x05)

De forma a verificarmos o bom funcionamento do filtro apresentamos um *print* do seu resultado na ferramenta *Wireshark*, onde captamos ambos os tipos de tramas:

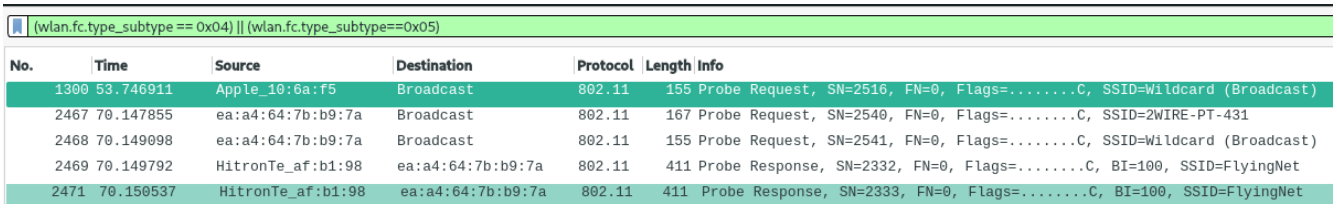


Figura 9: Resultado da aplicação do filtro.

h. 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?

Para conseguirmos obter um par *probing response* e *probing request*, tivemos de analisar os endereços das tramas e procurar uma correspondência, ou seja, para o endereço destino de *Response*, encontrar um *Request* que possua esse endereço no campo origem. Obtivemos o seguinte par:

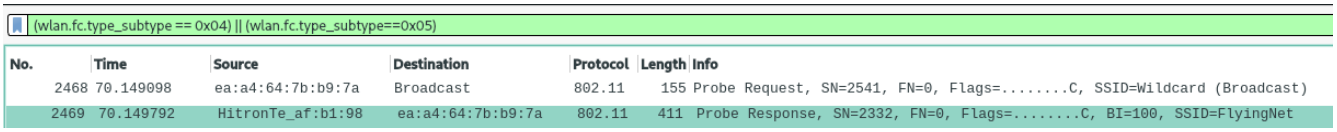


Figura 10: Par *Resquest-Response*.

Analisando o conteúdo das tramas, conseguimos denotar que a trama correspondente ao *Probing Request* possui como endereço MAC de origem **ea:a4:64:7b:b9:7a** e como destino **ff:ff:ff:ff:ff:ff**, concluindo que se trata de uma trama de *broadcast*, tendo como origem um dispositivo com interesse em ligar-se a uma rede. Relativamente à trama de *Probing Response*, esta possui o endereço MAC de origem com o valor **bc:14:01:af:b1:98** e como endereço destino o endereço **ea:a4:64:7b:b9:7a**, conferindo assim a propriedade referida acima sobre a correspondência de endereços.

Assim, estas tramas servem para que dispositivos se consigam ligar a redes, através de pedidos (*requests*) e respostas dos APs (*response*). Neste caso em particular, o dispositivo interessado em conectar-se, recebeu do AP não só o endereço MAC do mesmo como também o SSID da rede que o AP é responsável.

3 Questão 6

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

Um processo de associação completo envolve vários tipos de tramas como: *Association Request*, *Association Response*, *Authentication* e, por fim, *Acknowledgement*. Assim, desenvolvemos um filtro que pesquisasse todas estas tramas para facilitar a pesquisa de todo o processo. Os valores dos subtipos no filtro foram utilizados de acordo com o anexo fornecido dos docentes. Apresentamos, então, o filtro desenvolvido seguido do processo de associação identificado:

(wlan.fc.type_subtype	==	0x00)	**or**
(wlan.fc.type_subtype	==	0x01)	**or**
(wlan.fc.type_subtype	==	0x0b)	**or**
(wlan.fc.type_subtype	==	0x1d)	

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 11: Processo de associação completo entre a STA e o AP

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

A partir das tramas obtidas na alínea anterior, desenvolvemos o seguinte diagrama ilustrando as mensagens trocadas entre STA e o AP durante o processo de associação:

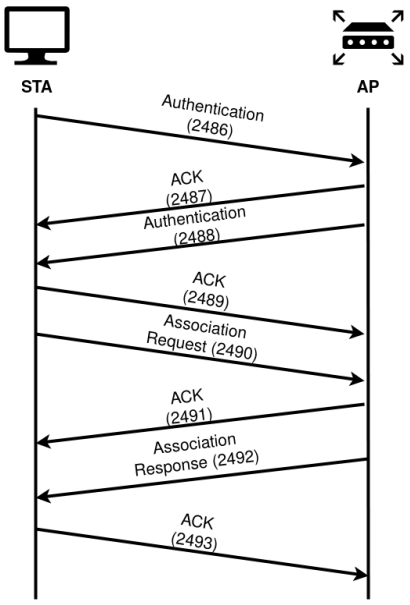


Figura 12: Sequência de tramas trocadas durante o processo

4 Questão 7

a. 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?

Ao analisarmos a trama, mais especificamente o campo *Frame Control*, conseguimos denotar o valor das *flags* do mesmo. Para a pergunta em questão, a *flag* que procuramos é a **DS *status***, tendo esta dois valores a preencher: *To* DS/AP (destino no AP) e *From* DS/AP (origem no AP). De acordo com a trama, os valores de *To* DS e *From* DS são, respetivamente, **0** e **1**, ou seja, estamos perante uma trama que foi enviada através de um AP para um STA, podendo concluir que a trama é local à WLAN.

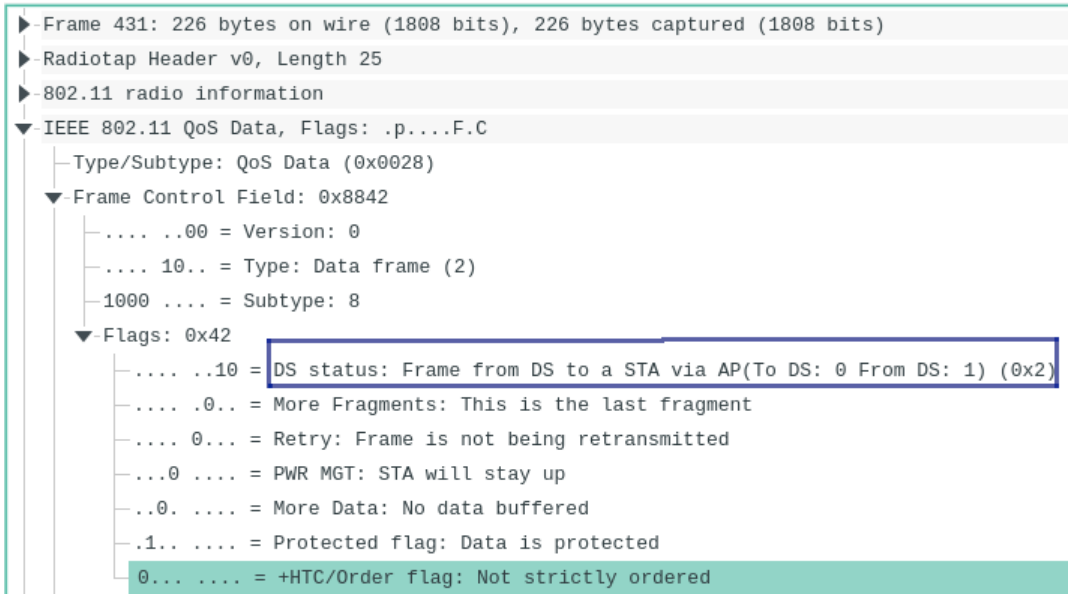


Figura 13: Captura da Trama Nº 431.

b. 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?

Para além da análise da trama, utilizamos a funcionalidade *hexdump* do *Wireshark*, tendo assim acesso aos *bytes* ordenados da trama. Como tal, conseguimos distinguir três endereços: *receiver* (**64:9a:be:10:6a:f5**), *transmitter* (**bc:14:01:af:b1:98**) e *router interface* (**bc:14:01:af:b1:98**).

Como podemos verificar, o endereço do *host* sem fios (STA) corresponde ao endereço do *receiver*, logo esta trama tem como destino o mesmo. Relativamente aos endereços do AP e do *router*, estes são idênticos, o que nos leva a concluir que o AP realiza tanto as funcionalidades de *routing* como de transmissão de tramas.

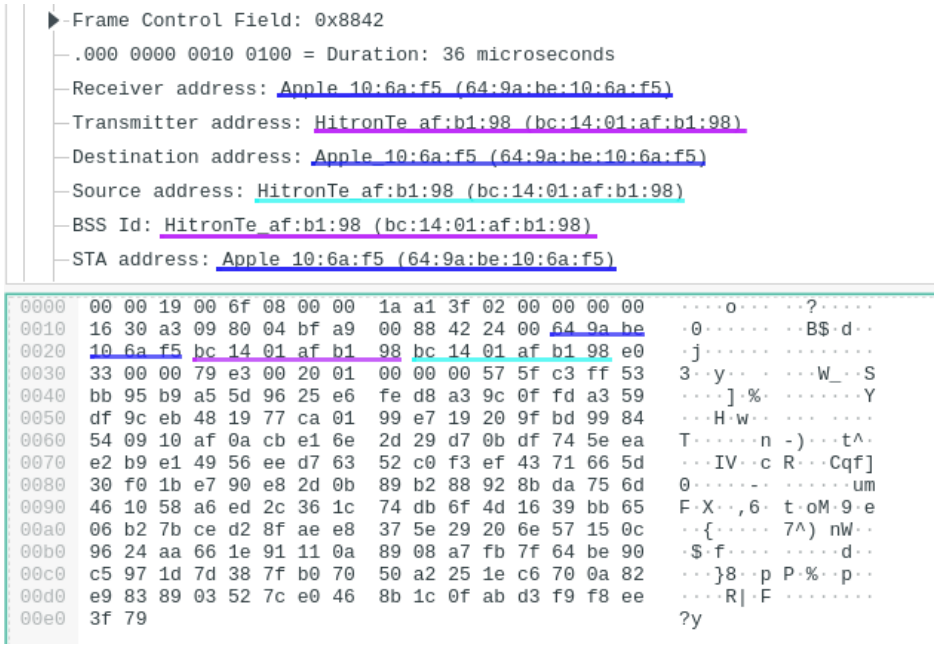


Figura 14: Endereços MAC contidos na trama.

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

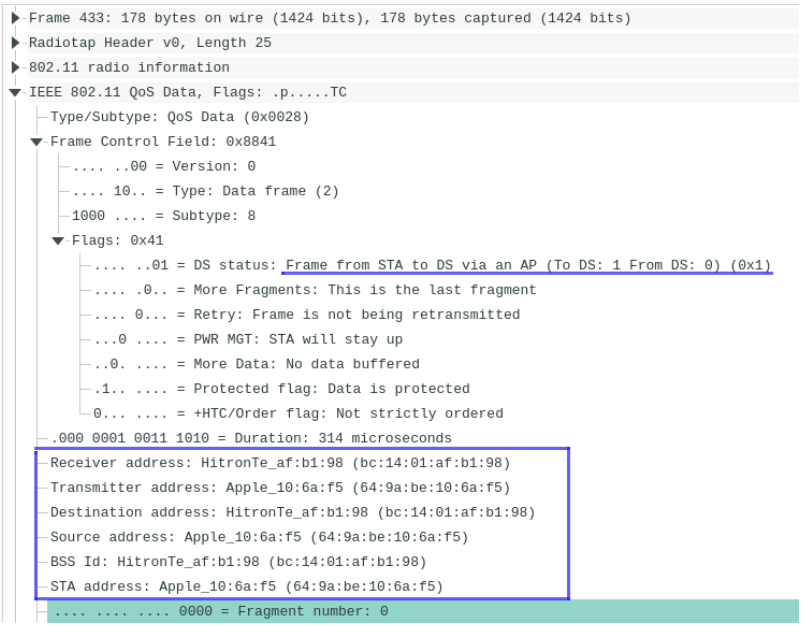


Figura 15: Captura da Trama Nº 433.

Ao analisarmos as *flags* presentes no campo *Frame Control*, denotamos que os valores de *To* DS e *From DS* são, respetivamente, 1 e 0, ou seja, contrariamente à trama analisada anteriormente, esta é direcionada ao AP tendo como origem o STA. Para além disto, poderíamos chegar à mesma conclusão a partir da análise dos endereços MAC presentes na trama: *receiver* (**bc:14:01:af:b1:98**), *transmitter* (**64:9a:be:10:6a:f5**) e *destination* (**bc:14:01:af:b1:98**).

d. 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.)

Ao longo de uma transferência de dados são transmitidas tramas de controlo do subtipo *Request To Send* e *Clear To Send*. Estas tramas têm como objetivo evitar colisões e controlar a transmissão de dados pelo meio, uma vez que vários dispositivos podem estar ligados a um AP e, caso transmitam simultaneamente, vão existir colisões e como consequência a corrupção de pacotes.

Assim, podemos resumir o comportamento destas tramas de controlo da seguinte forma: o STA envia tramas com pedidos de conexão (RTS) para o AP, respondendo o AP, em *broadcast*, uma trama CTS. A trama CTS é "ouvida" por todos os nós, permitindo ao STA enviar os dados ao AP sem interrupções.

Contrariamente, nas redes *Ethernet*, este sistema não é implementado, pois estas utilizam dispositivos como *switches* e *hubs* que conseguem redirecionar e distribuir o tráfego na rede, em particular, na utilização de *switches*, cada dispositivo tem um canal de transmissão único e direto, permitindo assim evitar colisões.

e. 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 verificarmos se existiu algum controlo de colisões através das tramas RTS e CTS, começamos por analisar as tramas capturadas nos instantes imediatamente antes e depois da trama nº 433. Desta forma, obtivemos as seguintes tramas, não obtendo quaisquer tramas de controlo de colisões:

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

Figura 16: Tramas capturadas na envolvência da trama nº433.

Assim, para encontrarmos uma transferência de dados que utilize este controlo e de modo a facilitar a sua pesquisa no ficheiro de captura, desenvolvemos o seguinte filtro que irá filtrar todas as tramas RTS e CTS assim como todas as tramas de dados, tendo retirado, novamente, os valores dos subtipos do anexo dos docentes.

```
(wlan.fc.type_subtype == 0x1b) or (wlan.fc.type_subtype == 0x1c) or
(wlan.fc.type_subtype >= 0x20 and wlan.fc.type_subtype <= 0x2f)
```

Após a aplicação do filtro, o *Wireshark* apresentou várias tramas que obedeciam ao mesmo, tendo o grupo captado duas transmissões de dados que diferem na sua direcionalidade, ou seja, uma com a comunicação no sentido AP -> STA e outra no sentido STA -> AP.

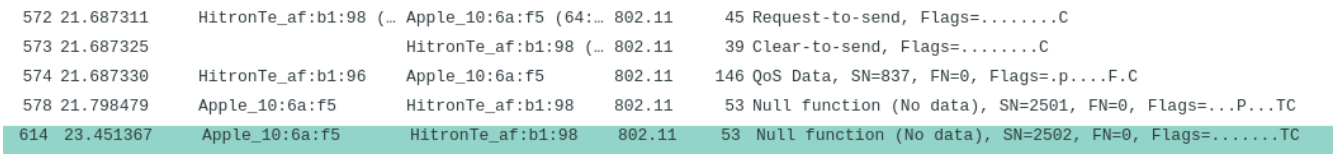


Figura 17: Conjunto de tramas no sentido AP -> STA.

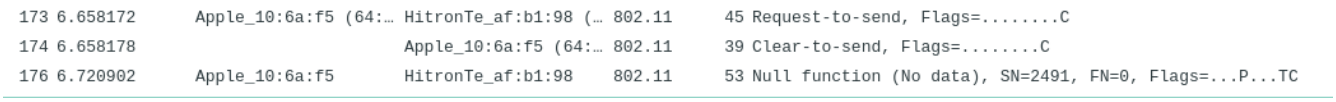


Figura 18: Conjunto de tramas no sentido STA -> AP.

Como podemos verificar pelas Figuras 17 e 18, o dispositivo de origem envia uma trama RTS ao dispostivo destino e, depois de aceite, através do envio de uma segunda trama (CTS), trocam dados entre si assim como tramas de confirmação (*Acknowledgement*).

5 Conclusão

Com a conclusão deste guião prático, encontramo-nos, em geral, satisfeitos com o trabalho desenvolvido, tendo alcançado todos os objetivos propostos pelos docentes no enunciado.

Em particular, este trabalho prático incidiu sobre a resolução de vários exercícios e problemas da área de redes, nomeadamente as redes sem fios (*Wi-Fi*). Assim, o grupo teve a oportunidade de aprofundar os seus conhecimentos no estudo de endereços MAC, interpretação do protocolo 802.11 e, por fim, utilização de controlo de colisões. Para além disso, mais uma vez, foi necessário o manuseamento da ferramenta *wireshark*, provando, novamente, a sua utilidade prática no contexto de análise de tráfego.

Em suma, a construção e desenvolvimento deste trabalho prático permitiu a todo o grupo aprofundar os seus conhecimentos no que toca às redes sem fios, atingindo uma ampla percepção de vários assuntos englobados pelas mesmas.