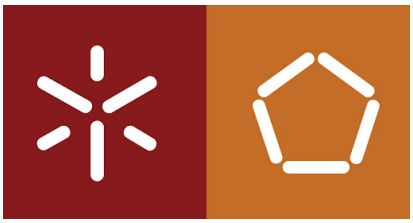

Universidade do Minho

Licenciatura/Mestrado Integrado em Engenharia Informática

Redes de Computadores - TP4

Grupo 94

Rui Guilherme Monteiro (A93179) Rui Moreira (A93232)
José Pereira (A89596)

Ano Lectivo 2021/2022

Conteúdo

Capítulo 1

Questões e Respostas

1.1 Acesso Rádio

Como indicado no enunciado, as seguintes respostas tiveram por base a trama 94.

1.1.1 Exercício 1

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

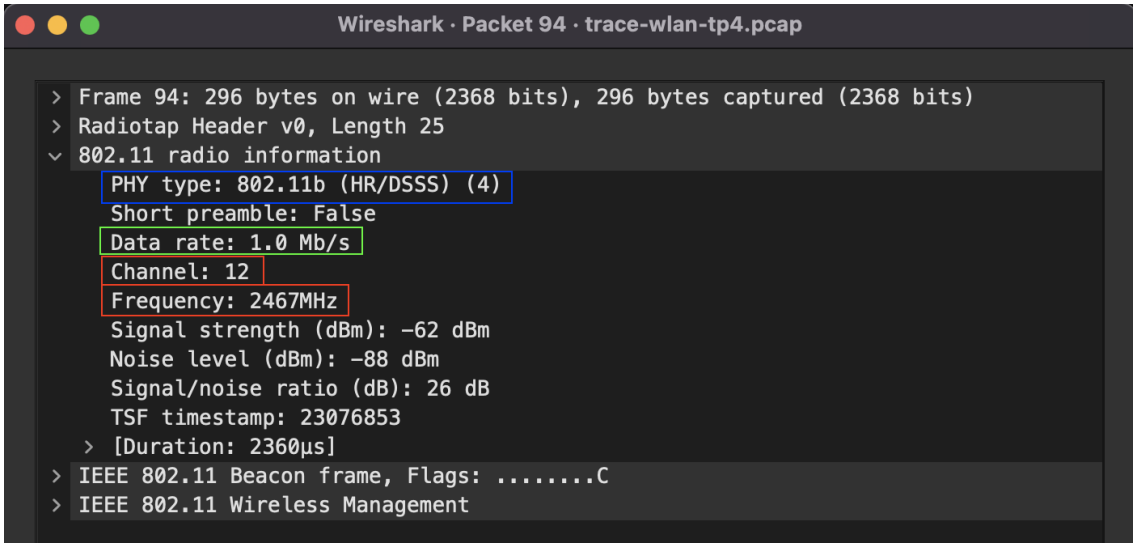

Figura 1.1: ALTERAR DPS

Como podemos observar pela figura 1.1 (na parte destacada a vermelho), a rede sem fios está a operar na frequência **2467 MHz**, que corresponde ao canal **12**.

1.1.2 Exercício 2

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

Observando novamente a figura 1.1, pelo campo *PHY type* (destacado a azul) , podemos afirmar que a versão da norma IEEE 802.11 que está a ser usada é **802.11b**

1.1.3 Exercício 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 escolhida foi enviada a um débito de **1.0Mb/s**, como podemos verificar pela parte destacada a verde da figura 1.1.

Este valor não corresponde ao debito máximo a que a interface Wi-fi pode operar, uma vez que o debito máximo desta versão IEEE 802.11b é 11Mb/s.

Como o objetivo de uma trama *beacon* é anunciar a sua presença e transmitir informações, é importante garantir que todos os *hosts* no *range* do AP detetem esta trama. Por este motivo, opta-se por valores de débito mais baixos possível.

1.2 *Scanning* Passivo e *Scanning* Ativo

Como indicado no enunciado, as seguintes respostas tiveram por base a trama **354** (260+94):

1.2.1 Exercício 4

Selecione a trama *beacon* de ordem (260 + 94). 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)

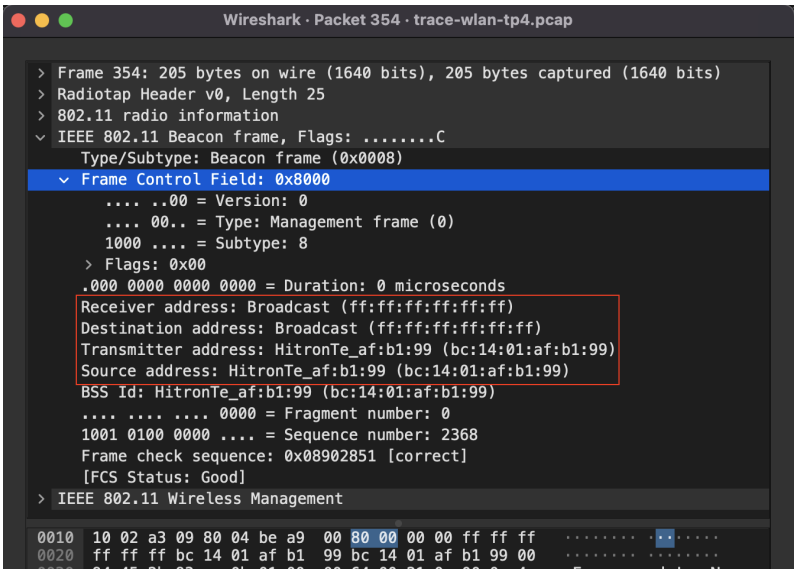

Figura 1.2: Trama *beacon* 354

Como podemos ver pela Figura 1.3, a trama é do tipo ***Management Frame*** **(00)** e do subtipo ***Beacon*** **(1000)**. Está especificado na secção de **frame control** do cabeçalho da trama.

00	Management	1000	Beacon

Figura 1.3: Entrada correspondente na tabela do enunciado

1.2.2 Exercício 5

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

Como podemos verificar pela Figura 1.3 (pela parte destacada a vermelho), os endereços em uso são:

- ***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

Os endereços MAC origem e destino são, respetivamente, bc:14:01:af:b1:99 e ff:ff:ff:ff:ff:ff. Logo podemos concluir que o endereço origem é o *Access Point*, e o endereço destino é o endereço *broadcast*, uma vez que o objetivo duma trama do tipo *Beacon* é transmitir informações a todos os *hosts* (STAs), ou seja, a trama deve ser recebida por todos os *hosts*.

1.2.3 Exercício 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?

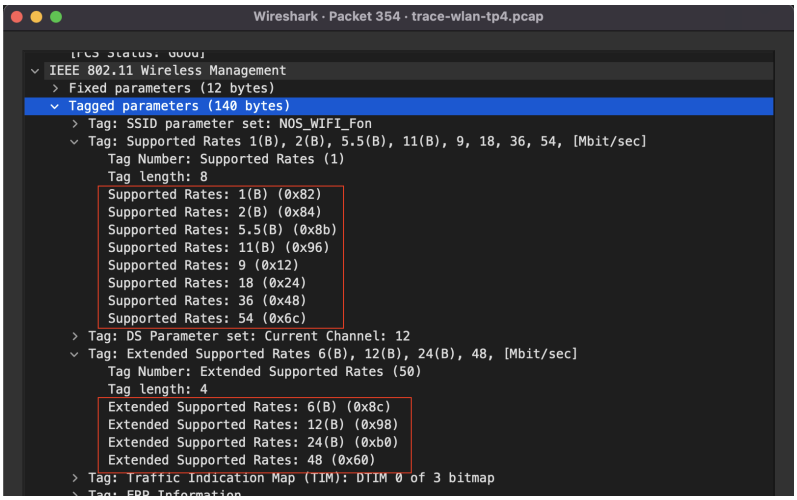

Figura 1.4: Trama *Beacon*

Os débitos de base suportados pelo AP são 1 (Básico), 2 (Básico), 5.5 (Básico), 11 (Básico), 9, 18, 36, 54 e os débitos adicionais são 6 (Básico), 12 (Básico), 24 (Básico) e 48.

1.2.4 Exercício 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.

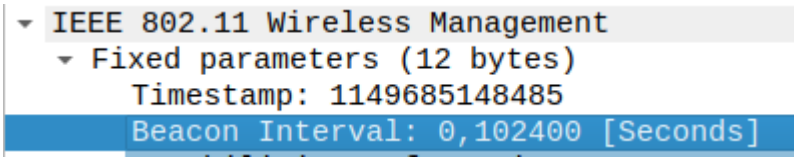

Figura 1.5: Intervalo de tempo previsto entre tramas *beacon* consecutivas

Analisando a Figura 1.5, o tempo previsto entre tramas é 0,102400 segundos.

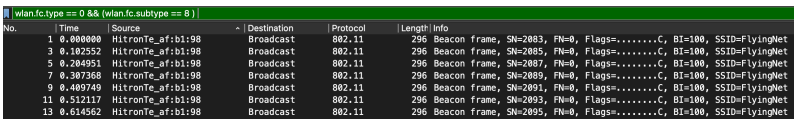

Figura 1.6: Intervalo de tempo observado entre tramas *beacon* consecutivas

Na prática, este intervalo de tempo acaba por ser um valor aproximado do tempo previsto. Como se pode ver pela Figura 1.6, este valor é ligeiramente superior (por exemplo nas primeiras duas tramas a diferença do tempo previsto é de + 0.000152s). Isto deve-se ao facto que o AP pode estar ocupado no momento em que devia enviar a trama *beacon* e/ou às condições físicas do meio de transmissão, que podem levar a que haja um atraso no envio da mesma.

1.2.5 Exercício 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).

Utilizando o filtro *wlan.ssid*, observando a coluna *info*, verifica-se que os *SSIDs* que estão a operar na vizinha da *STA* de captura são *FlyingNet* e *NOS_WIFI_Fon*.

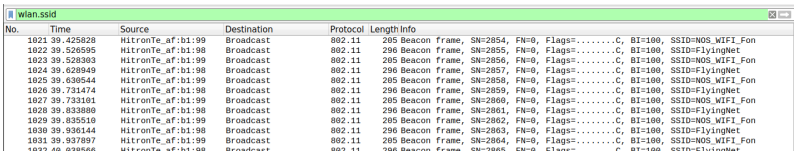

Figura 1.7: Listagem de SSIDs

1.2.6 Exercício 9

Verifique se está a ser usado o método de deteção de erros (CRC). Que conclui?

Sugestão: Use o filtro: (wlan.fc.type_subtype == 0x08) (wlan.fcs.status == bad)

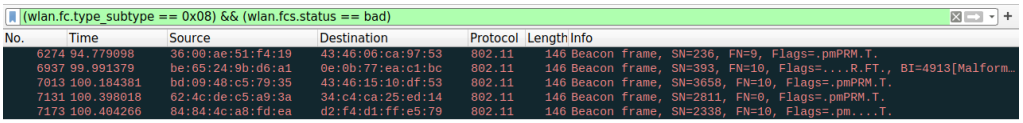

Figura 1.8: Lista de tramas *Beacon* com erros, aplicando o filtro fornecido

Ao aplicar o filtro, é possível verificar a existência de 5 tramas de *Beacon*, confirmando pela existência do campo *FCS Status* que está a ser usada deteção de erros.

Este mecanismo de detecção de erros é importante para conseguir identificar possíveis interferências na transmissão devido à possibilidade de existirem obstáculos presentes no meio físico.

1.2.7 Exercício 10

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

Como podemos ver pela Figura 1.9, as tramas *probing request* ou *probing response* são do tipo 00, e subtipo 0100 (4) e 0101 (5), respectivamente.

00	Management	0100	Probe request
00	Management	0101	Probe response

Figura 1.9: Tipo e subtipo das tramas *probing request* e *probing response*

Assim, com o seguinte filtro, é possivel visualizar todas as tramas *probing request* ou *probing response*, simultaneamente.

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

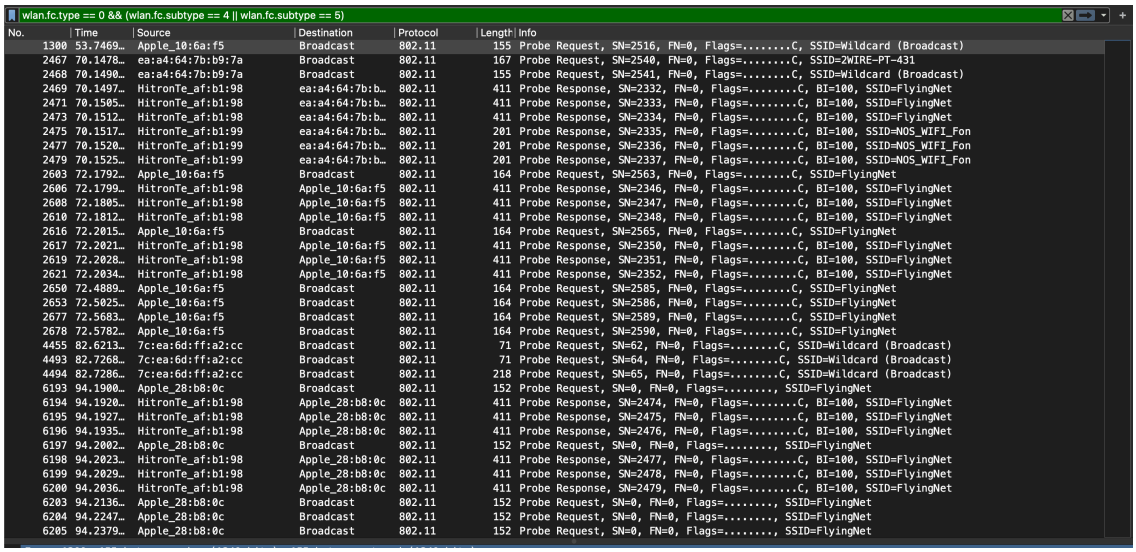

Figura 1.10: Filtro para visualizar tramas *probing request* e *probing response*

1.2.8 Exercício 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

```
2468 70.149098   ea:a4:64:7b:b9:7a   Broadcast          802.11   155 Probe Request, SN=2541, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
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_Fon
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_Fon
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_Fon
```

Figura 1.11: Lista de tramas *Probing Request* e *Probing Response*

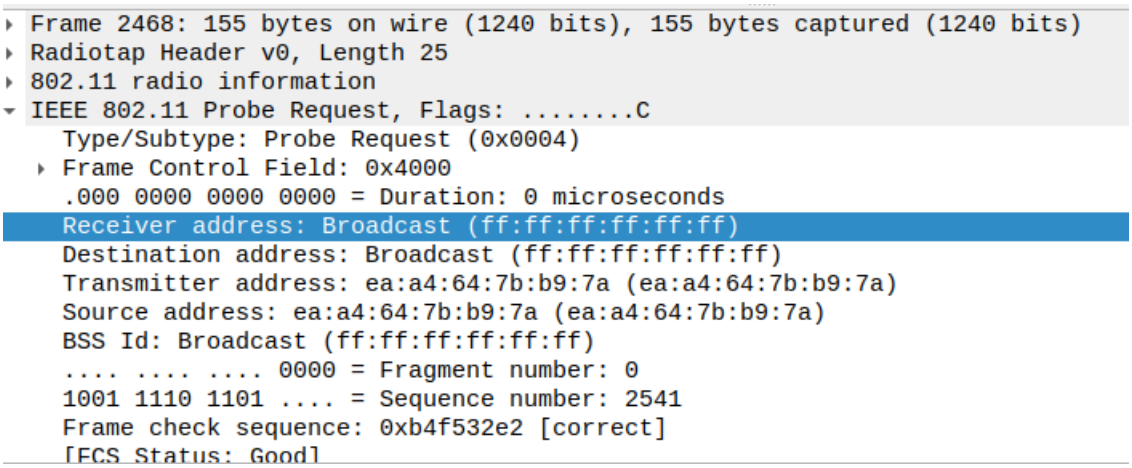

Figura 1.12: Probe request

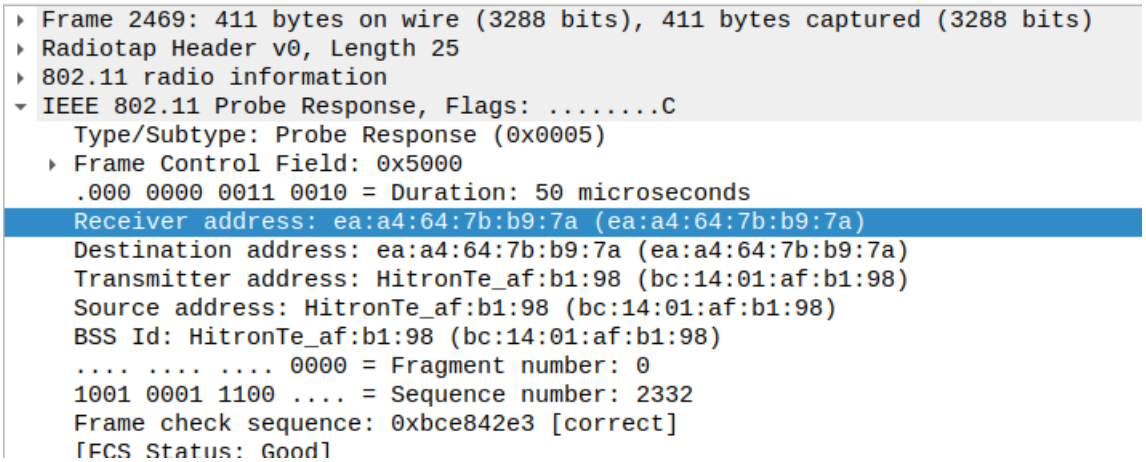

Figura 1.13: Probing response

As tramas de *Probing Request* são endereçadas a todos os APs que alcance, ou seja, a *Broadcast*. Sendo que estas tramas são usadas no *Active Scanning*, tendo como propósito obter informações acerca de outras APs, de forma a se associarem.

Estas informações são enviadas através de tramas *probing response*, pelos própios APs para o endereço que fez o *request*.

1.3 Processo de Associação

1.3.1 Exercício 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.

2486	70.3617…	Apple_10:6a:f5	HitronTe_af:b…	802.11	70	Authentication, SN=2542, FN=0, Flags=.......C
2487	70.3620…		Apple_10:6a:f…	802.11	39	Acknowledgement, Flags=.......C
2488	70.3818…	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59	Authentication, SN=2338, FN=0, Flags=.......C
2489	70.3818…		HitronTe_af:b…	802.11	39	Acknowledgement, Flags=.......C
2490	70.3835…	Apple_10:6a:f5	HitronTe_af:b…	802.11	175	Association Request, SN=2543, FN=0, Flags=.......C, SSID=FlyingNet
2491	70.3838…		Apple_10:6a:f…	802.11	39	Acknowledgement, Flags=.......C
2492	70.3893…	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	225	Association Response, SN=2339, FN=0, Flags=.......C
2493	70.3893…		HitronTe_af:b…	802.11	39	Acknowledgement, Flags=.......C

Figura 1.14: Sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação

1.3.2 Exercício 13

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

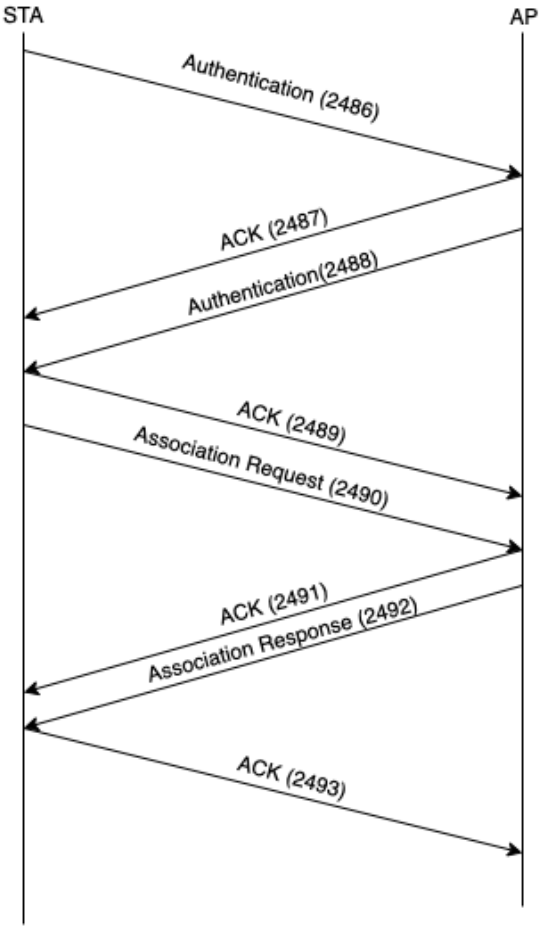

Figura 1.15: Diagrama da sequência de todas as tramas trocadas no processo

1.4 Transferência de Dados

1.4.1 Exercício 14

Considere a trama de dados nº 431. 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?

```
> Frame 431: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: .p....F.C
    Type/Subtype: QoS Data (0x0028)
  v Frame Control Field: 0x8842
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
    v 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
    .000 0000 0010 0100 = Duration: 36 microseconds
    Receiver address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Destination address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    STA address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    .... .... .... 0000 = Fragment number: 0
    0011 0011 1110 .... = Sequence number: 830
    Frame check sequence: 0x793feef8 [correct]
    [FCS Status: Good]
  > Qos Control: 0x0000
  > CCMP parameters
```

Figura 1.16: Trama 431

Como se pode observar na figura 1.16, no campo *Frame Control*, analisando a *flag DS status*, podemos afirmar que esta trama tem direcionabilidade *To DS: 0 From DS: 1* e que o valor dessa *flag* é 10, o que significa que o pacote de dados vem do DS para o STA, ou seja vem de fora da rede local, logo, conclui-se que a trama não será local à WLAN.

1.4.2 Exercício 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 em uso são: **64:9a:be:10:6a:f5** correspondente à STA (*receiver* e *destination*) e **bc:14:01:af:b1:98** correspondente ao AP e Router (*transmitter* e *source*).

1.4.3 Exercício 16

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

```
Frame 433: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits)
Radiotap Header v0, Length 25
802.11 radio information
IEEE 802.11 QoS Data, Flags: .p.....TC
  Type/Subtype: QoS Data (0x0028)
▾ Frame Control Field: 0x8841
    .... ..00 = Version: 0
    .... 10.. = Type: Data frame (2)
    1000 .... = Subtype: 8
  ▾ Flags: 0x41
      .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
      .... .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
  .000 0001 0011 1010 = Duration: 314 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)
  Destination address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  Source address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
  BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  STA address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
```

Figura 1.17: Trama 433

Observando a figura 1.17, verificamos que a direcionalidade da trama nº433 é *To DS: 1 From DS: 0*, o que significa que a trama vem do STA para o DS. No que toca ao endereçamento MAC, tanto o de *destination* como o do *receiver* são bc:14:01:af:b1:98, já o endereço MAC de *source* e do *transimitter* é 64:9a:be:10:6a:f5.

1.4.4 Exercício 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*.)

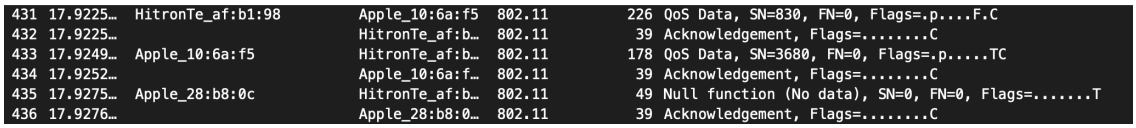

Figura 1.18: Sequência de tramas acima mencionada

Ao longo da transferência de dados, o subtipo das tramas de controlo transmitidas é **1101** (**Acknowledgment**).

Contrariamente ao que acontece numa rede *Ethernet*, estas tramas são necessárias devido à possibilidade de falhas de transmissão e/ou colisões. Deste modo, estas são a confirmação da receção da trama por parte do destinatário.

1.4.5 Exercício 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.

Como se pode ver pela Figura 1.18, não estão a ser usadas as tramas *Request To Send* e *Clear To Send*.

Um exemplo de uma transferência de dados onde é usada a opção *RTC/CTS* é a Figura 1.19. Neste caso, a *STA* envia a trama *RTS* para o *AP/router* correspondente, sendo respondida por uma trama *CTS* pelo *AP/router*. Os *hosts* da rede irão receber a informação que o AP vai estar ocupado durante um certo de tempo, para que não haja risco de colisões no AP.

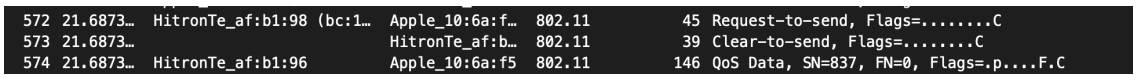

Figura 1.19: Exemplo de uma transferência de dados em que é usado RTC/CTS

Capítulo 2

Conclusão

Através da realização deste trabalho prático, tivemos a oportunidade de consolidar os nossos conhecimentos em relação aos temas de Acesso Rádio, *Scanning* Ativo e Passivo, Processo de Associação e Transferência de Dados.

Através de uma captura *Wireshark* fornecida pela equipa docente, foi possível analisar o protocolo IEEE 802.11, cujas tramas foram objeto de análise.

Em suma, pensamos ter cumprido os objetivos a que nos propusemos, aprofundando o conhecimento nas componentes exploradas durante o trabalho prático.