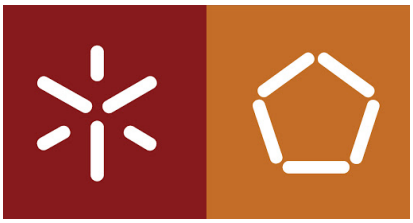


Universidade do Minho

Licenciatura em Engenharia Informática

Redes de Computadores
Trabalho Prático 4

Bernardo Saraiva (A93189)
José Gonçalves (A93204)
Gonçalo Santos (A93279)

03-05-2022

Conteúdo

1 4. Acesso Rádio **4**

1.1 1) Identifique em que frequência do espectro está a operar a rede sem fios, e o canal que corresponde essa frequência. 4

1.2 2) Identifique a versão da norma IEEE 802.11 que está a ser usada. 5

1.3 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. 5

2 5. Scanning Passivo e Scanning Ativo **7**

2.1 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)? 7

2.2 5) Para a trama acima, identifique todos os endereços MAC em uso. Que conclui quanto à sua origem e destino? 7

2.3 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? 8

2.4 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. 8

2.5 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). 8

2.6 9) Verifique se está a ser usado o método de deteção de erros (CRC). 8

2.7 10) Estabeleça um filtro Wireshark apropriado que lhe permita visualizar todas as tramas probing request ou probing response, simultaneamente. 9

2.8 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? 9

3 6. Processo de Associação **10**

3.1 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. 10

3.2 13) Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo. 10

4 7. Transferência de Dados **12**

4.1 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? . . . 12

4.2 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? 13

4.3 16)Como interpreta a trama nº433 face à sua direccionalidade e endereçamento MAC? 13

4.4 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.) 14

4.5 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 14

5 Conclusão **16**

Capítulo 1

4. Acesso Rádio

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

Uma vez que o identificador do grupo é o 131, após análise do campo *radio frequency*, foi possível verificar que se encontra no channel 12, com a frequência do espetro igual a 2467 MHz.

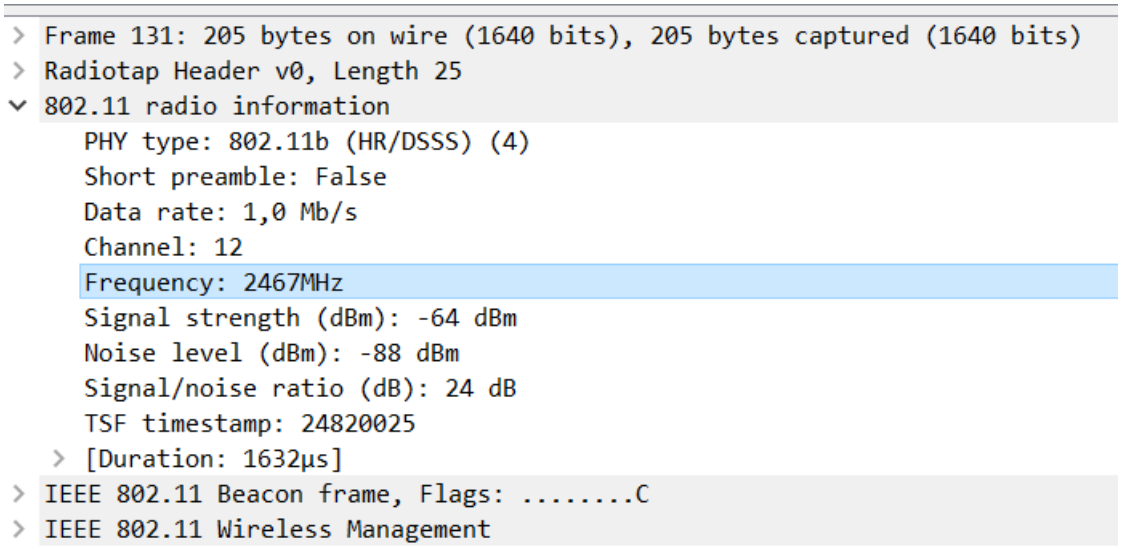


Figura 1.1: Análise da trama 131

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

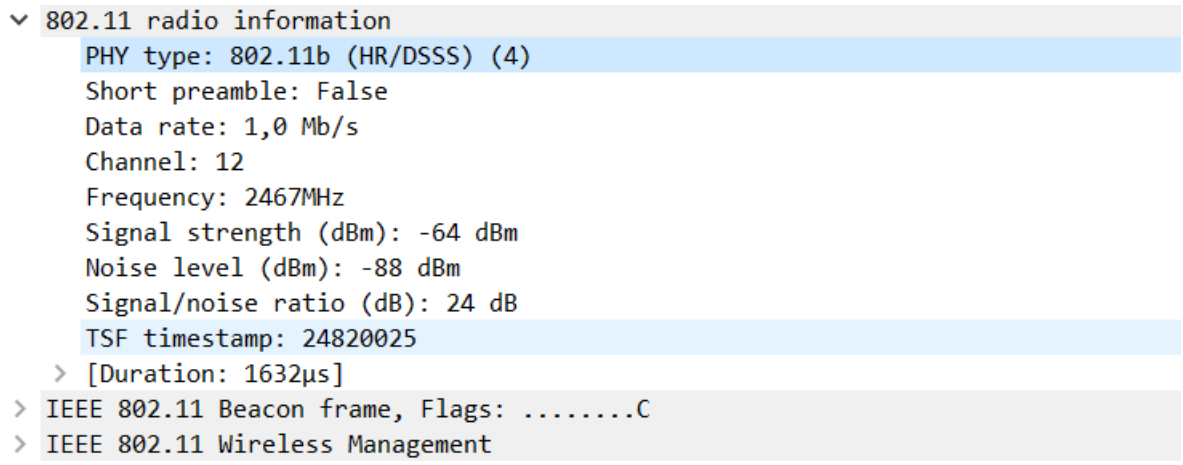


Figura 1.2: Análise da Versão da norma IEEE 802.11

Através da Figura 1.2, é possível verificar que está a ser usada a **versão b** da norma IEEE 802.11, ou seja, **802.11b**.

1.3 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.

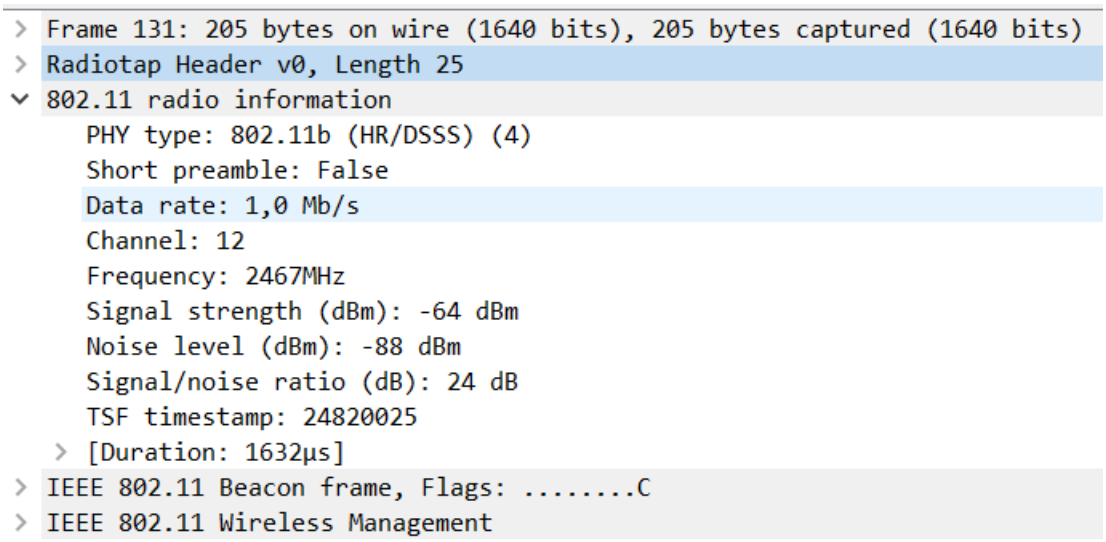


Figura 1.3: Análise do débito de envio da trama

Através do campo Data Rate, é possível verificar que o débito a que foi enviada a trama corresponde a 1Mb/s. Este débito não corresponde ao débito máximo a que a interface Wifi pode operar, sendo que este valor é 54Mb/s na norma IEEE 802.11.

Capítulo 2

5. Scanning Passivo e Scanning Ativo

2.1 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)?

A trama que irá ser analisada será a trama 391(260+131). Esta trama é do tipo *management*, isto devido ao segundo e terceiro bit da trama estarem a 0, e do subtipo *Beacon Frame*. Esta informação está contida no quarto, quinto, sexto e sétimo bit da trama, sendo que neste cenário só tem o quarto bit ativo.

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

Nesta trama são usados 4 endereços MAC, existindo apenas dois endereços distintos, este sendo o endereço da origem e do emissor que é bc:14:01:af:b1:98, e o do destinatário e de quem vai receber a trama que é ff:ff:ff:ff:ff:ff

2.3 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?

débitos base: 1, 2, 5.5, 11, 9, 18, 36, 54 [Mbit/sec]

débitos adicionais: 6, 12, 24, 48 [Mbit/sec]

2.4 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 entre tramas beacon é de 0,102400 s. Este tempo na pratica não é aplicado com precisão, uma vez que o tempo entre a trama anterior e a atual é de 0,100601 s e entre a trama atual e a seguinte é 0.001628s.

2.5 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).

De forma a conseguir obter a lista dos SSIDs dos APs na vizinhança, foi usado um filtro no wireshark iterativamente de forma a ir filtrando os SSID conhecidos, verificando que existem quatro APs na vizinhança: FlyingNet, NOS_WIFI_Fon, Wildcard SSID e 2WIRE-PT-431

2.6 9) Verifique se está a ser usado o método de deteção de erros (CRC).

Nas tramas apresentadas esta a ser usado um método de deteção de erros, uma vez que o campo FCS não se encontra vazio.

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

```
wlan.fc.type_subtype == 4 || wlan.fc.type_subtype == 5
```

2.8 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 são dirigidas a qualquer access point que esteja na rede, isto de forma a fazer procura ativa em vez de procura passiva, isto é, uma estação vai de canal a canal procurando access points que estejam disponíveis nesse canal.

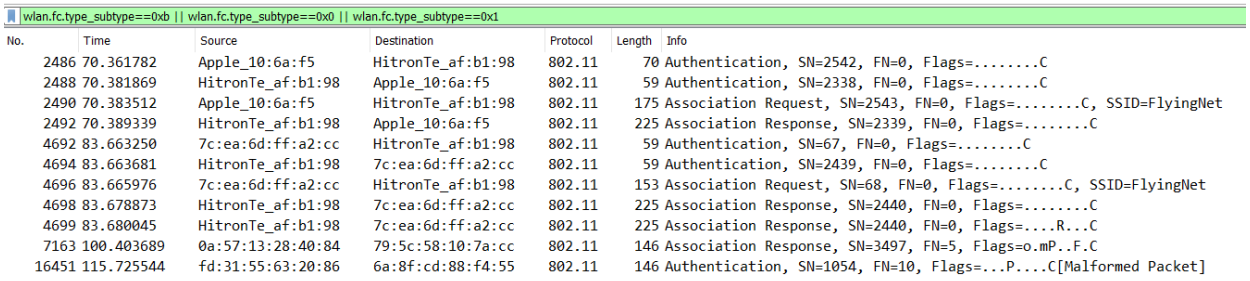
Capítulo 3

6. Processo de Associação

3.1 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.

Para conseguir obter a sequência de tramas correspondentes ao processo de associação, efetuou-se uma pesquisa filtrada no ficheiro de captura wireshark fornecido e consultou-se a tabela presente no enunciado, convertendo-se os valores binários correspondentes ao subtype pretendido para hexadecimal, pesquisando-se em seguida pela flag wlan.fc.type_subtype referente a esse valor.

```
wlan.fc.type_subtype==0xb || wlan.fc.type_subtype==0x0 || wlan.fc.type_subtype==0x1
```



wlan.fc.type_subtype==0xb || wlan.fc.type_subtype==0x0 || wlan.fc.type_subtype==0x1

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
2488	70.381869	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59	Authentication, SN=2338, FN=0, 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
2492	70.389339	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	225	Association Response, SN=2339, FN=0, Flags=........C
4692	83.663250	7c:ea:6d:ff:a2:cc	HitronTe_af:b1:98	802.11	59	Authentication, SN=67, FN=0, Flags=........C
4694	83.663681	HitronTe_af:b1:98	7c:ea:6d:ff:a2:cc	802.11	59	Authentication, SN=2439, FN=0, Flags=........C
4696	83.665976	7c:ea:6d:ff:a2:cc	HitronTe_af:b1:98	802.11	153	Association Request, SN=68, FN=0, Flags=........C, SSID=FlyingNet
4698	83.678873	HitronTe_af:b1:98	7c:ea:6d:ff:a2:cc	802.11	225	Association Response, SN=2440, FN=0, Flags=........C
4699	83.680045	HitronTe_af:b1:98	7c:ea:6d:ff:a2:cc	802.11	225	Association Response, SN=2440, FN=0, Flags=....R...C
7163	100.403689	0a:57:13:28:40:84	79:5c:58:10:7a:cc	802.11	146	Association Response, SN=3497, FN=5, Flags=o.mP..F.C
16451	115.725544	fd:31:55:63:20:86	6a:8f:cd:88:f4:55	802.11	146	Authentication, SN=1054, FN=10, Flags=...P....C[Malformed Packet]

Figura 3.1: Filtro de pesquisa por subtipo de authentication e association

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

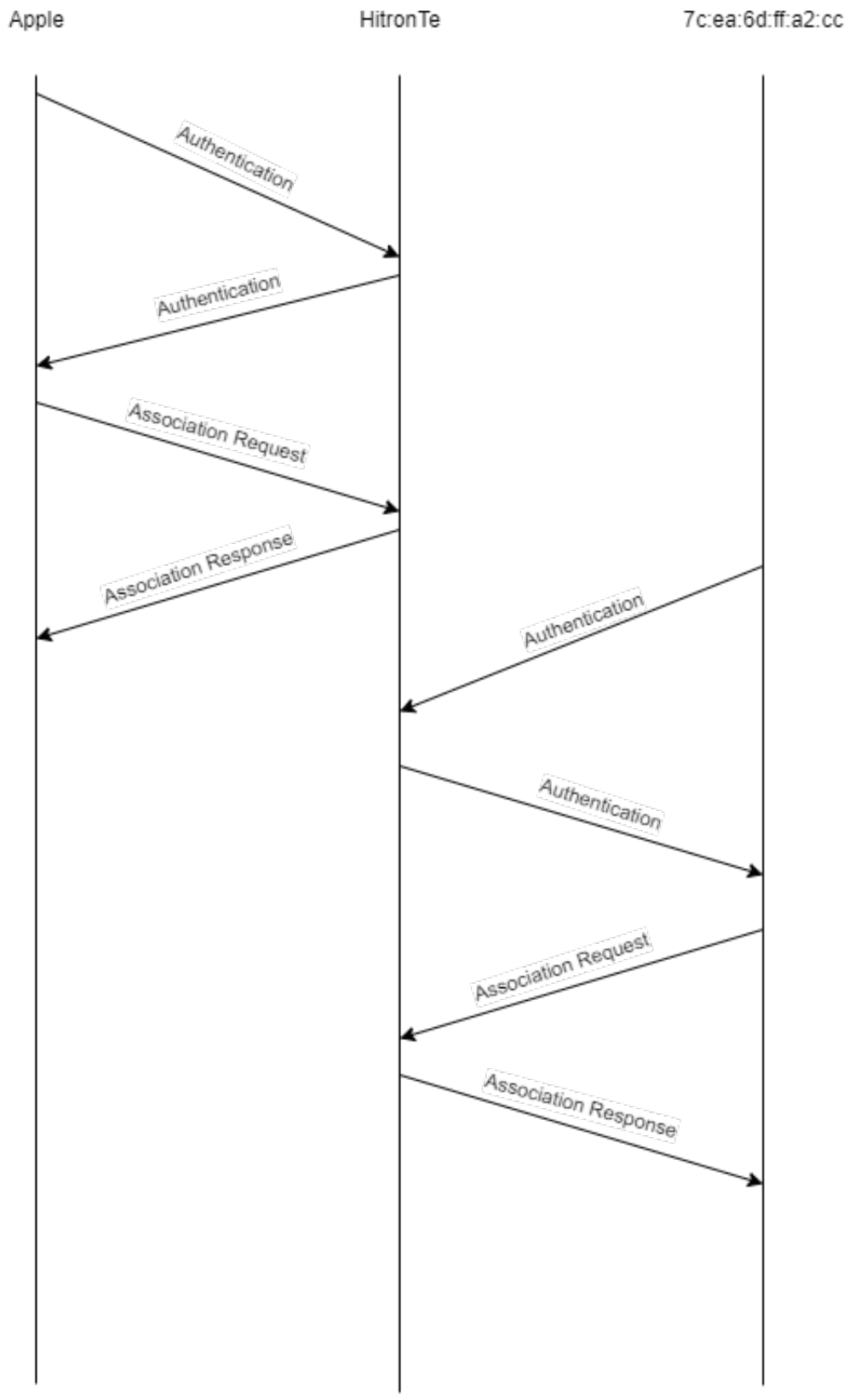


Figura 3.2: Diagrama correspondente à sequencia de troca das tramas envolvidas no processo

Capítulo 4

7. Transferência de Dados

4.1 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?

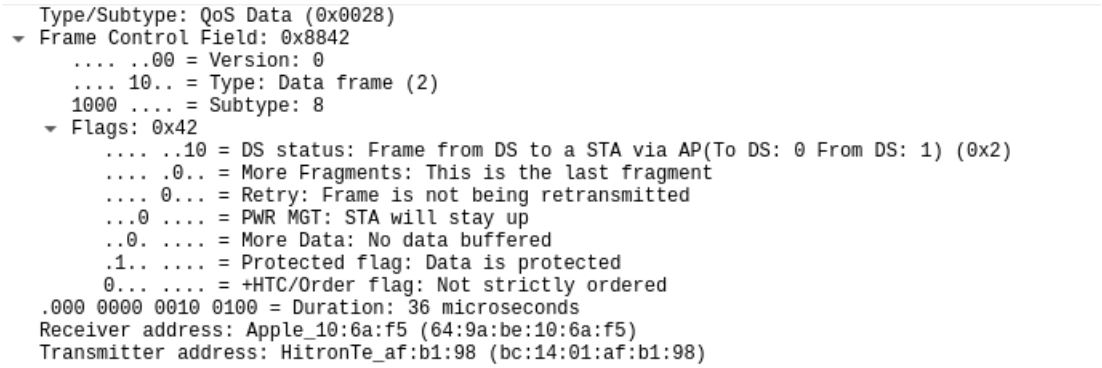


Figura 4.1: Frame Control Trama nº431

Através da flag DS status do frame control, é possível verificar que a trama não é local à WLAN, uma vez que o campo **from DS** se encontra ativado. Deste modo, é possível perceber que a trama tem como origem o DS e como destino o STA.

4.2 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?

```
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)
```

Figura 4.2: Endereços Mac em uso

- Host sem fios(STA) - 64:9a:be:10:6a:f5
- AP (Transmitter adress) - bc:14:01:af:b1:98
- Router acesso (Destination Address)- 64:9a:be:10:6a:f5

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

```
▾ 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
```

Figura 4.3: Frame Control Trama nº433

É possível concluir a direcionalidade da trama através do cabeçalho frame control, ao analisar mais uma vez a flag DS status. Como o campo **To DS** se encontra a 1 e o **From DS** a 0, então a trama dirige-se do STA para o DS.

4.4 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.)

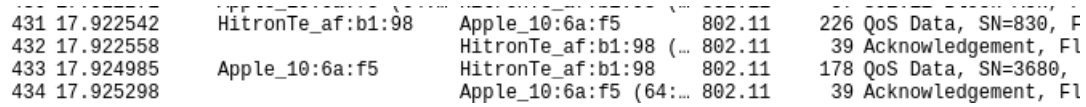


Figura 4.4: Tansferência acima mencionada

Como é possível verificar na Figura 4.4 são transmitidas ao longo da tranferência tramas do tipo **Acknowledgement**. Dado que em tranferências através do protocolo 802.11 colisões e perdas são mais frequentes do que com o protocolo Ethernet, por as tranferências ocorrerem em redes sem fio, estes pacotes surgem como um aviso por parte do AP a indicar que a partilha de dados ocorreu com sucesso.

4.5 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

No exemplo acima, não é possível verificar tramas RTS/CTS, no entanto, ao longo da captura é possível, como acontece na Figura 4.5, apresentada de seguida.

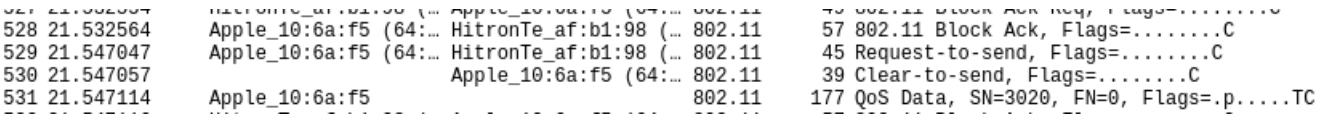


Figura 4.5: Tansferência com RTS/CTS

Como é possível observar na Figura 4.6, as tramas deste tipo não vão deixar o sistema de distribuição. Quanto aos dispositivos envolvidos, estes correspondem ao AP, STA e restantes hosts, sendo que o STA envia um RTS ao AP para pedir autorização para enviar dados e é respondido por

uma trama CTS vinda do AP, que autoriza a tranferência. Para que não aconteçam colisões todos os hosts são informados que o STA se encontra a enviar dados e por isso também são envolvidos na transferências destas tramas.

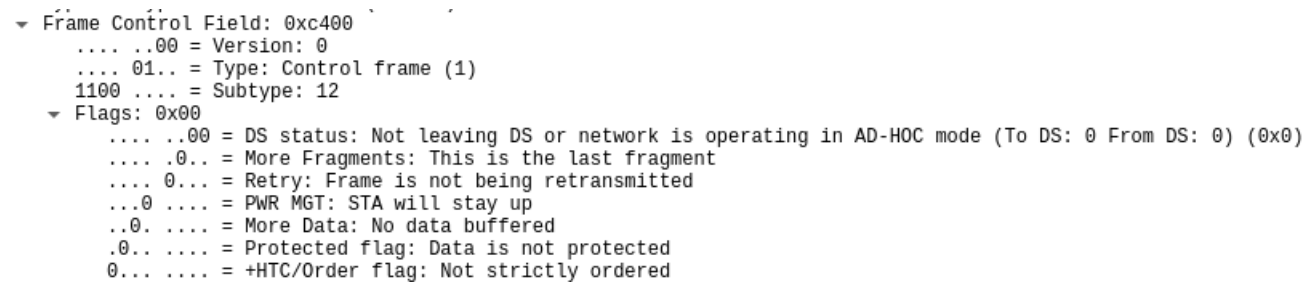


Figura 4.6: Frame control pacote 530

Capítulo 5

Conclusão

Com o desenvolvimento do presente trabalho prático, foi possível aplicar e consolidar a matéria lecionada nas aulas, através da sua aplicação num contexto prático.

Deste modo, conclui-se que o trabalho desenvolvido cumpre com os requisitos, tendo ajudado na aprendizagem da temática Redes sem Fios (Wi-Fi), nomeadamente sobre o protocolo 802.11 da norma IEEE e a análise de conexões entre STA e AP's.