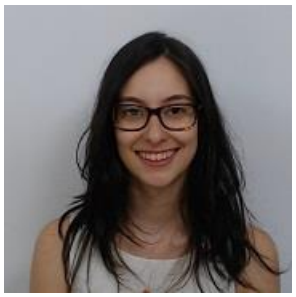
Relatório do Trabalho Prático 4

Redes de Computadores 2020/2021

a89506

Luís Miguel Lopes Pinto



a89599

Maria Beatriz Cardoso Gonçalves Barbosa e Moreira

a89574

Pedro Almeida Fernandes

Conteúdo

Acesso Rádio

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

R:. A frequência do espectro é 2GHz (mais especificamente 2467 Hz). O canal correspondente é BG 12.

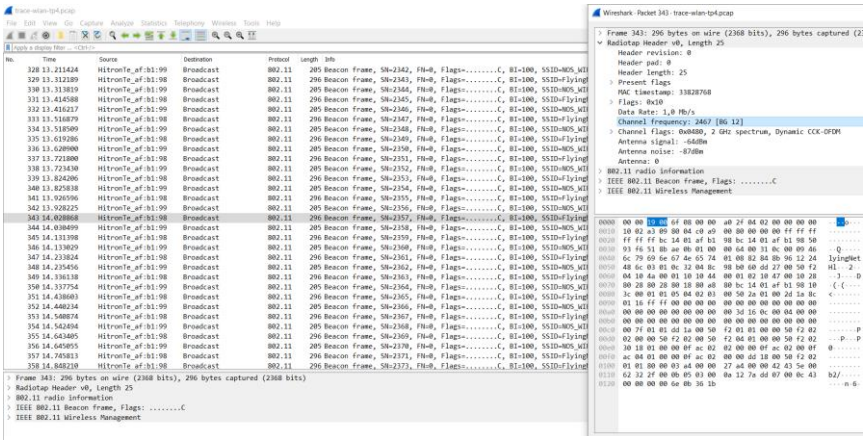


Figura 1 : *Exercício 1*

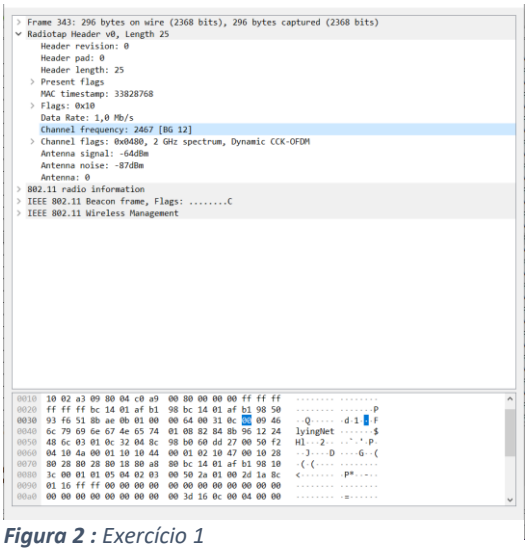


Figura 2 : *Exercício 1*

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

R:. A versão que está a ser usada é a 802.11g.

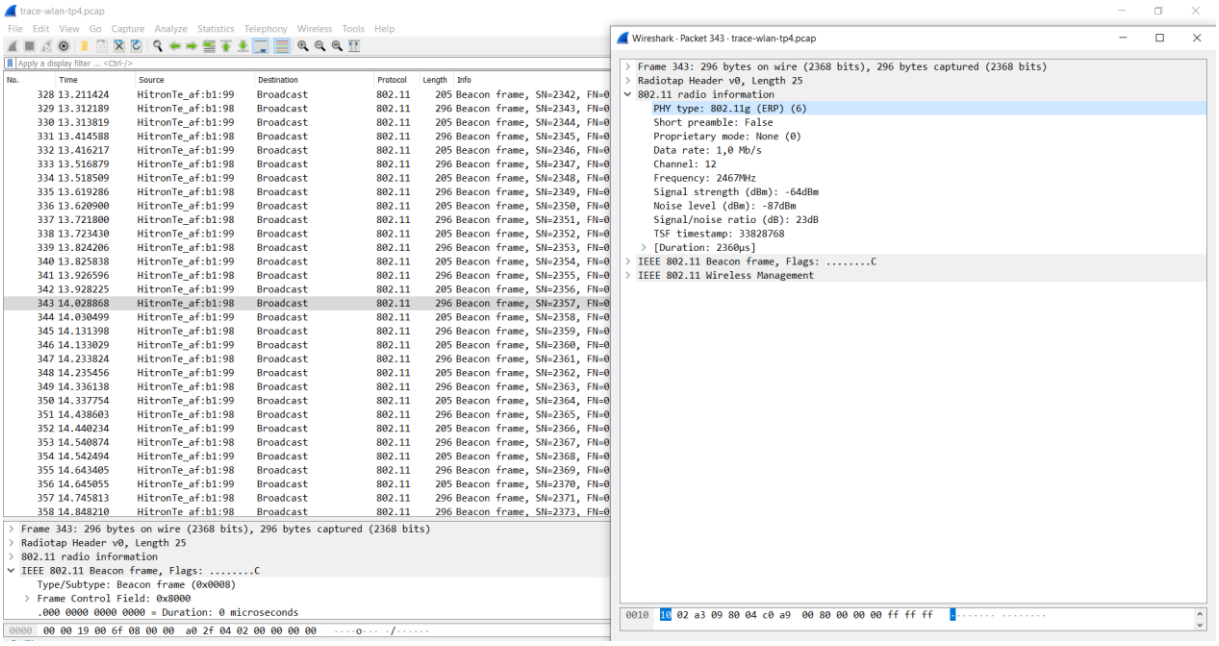


Figura 3 : *Exercício 2*

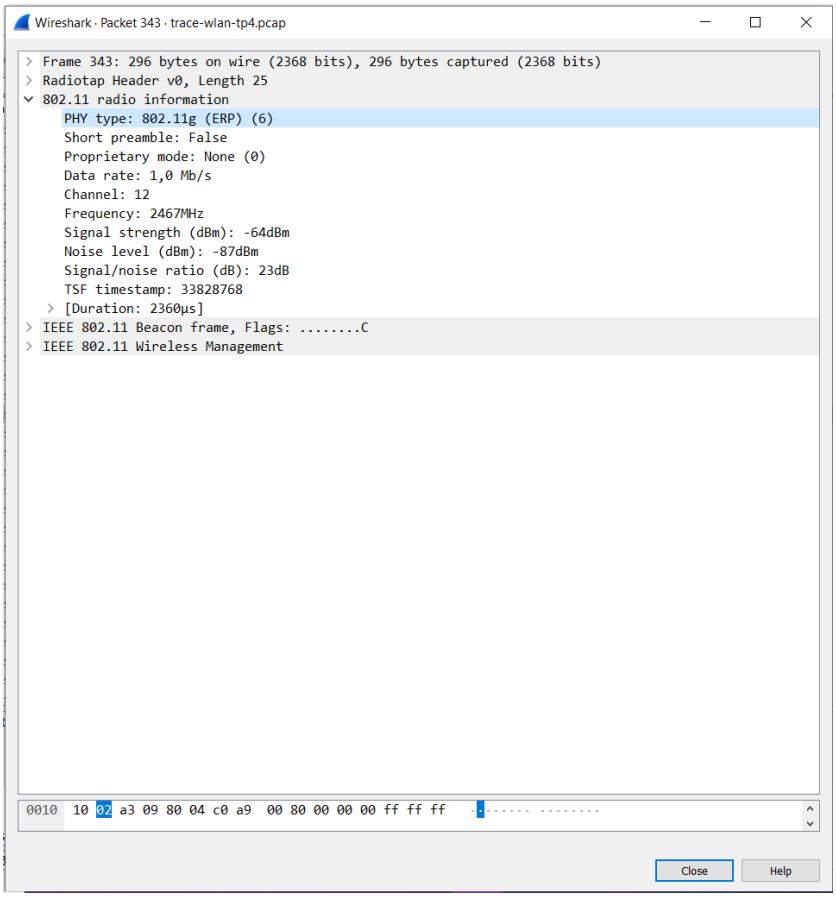


Figura 4 : *Exercício 2*

3 Qual o débito a que foi enviada a trama escolhida? Será que esse débito corresponde ao débito máximo a que a interface WiFi pode operar? Justifique.

R:. A trama escolhida foi enviada a um debito de 1 MBps. Não envia ao débito máximo da norma IEEE 802.11 (54 MBps) de modo a garantir que o beacon chega a todos os hosts.

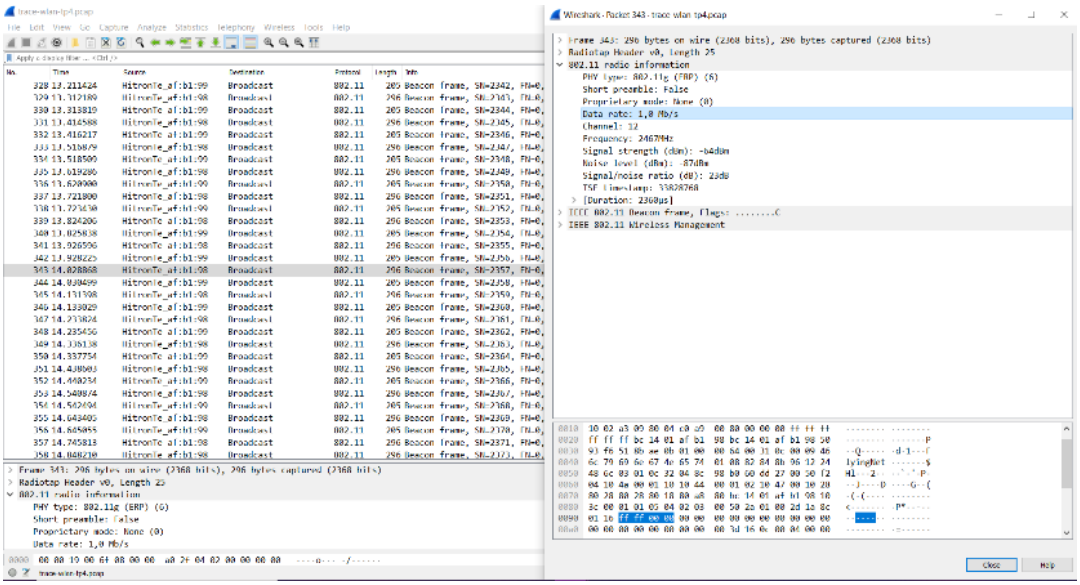


Figura 5 *: Exercício 3*

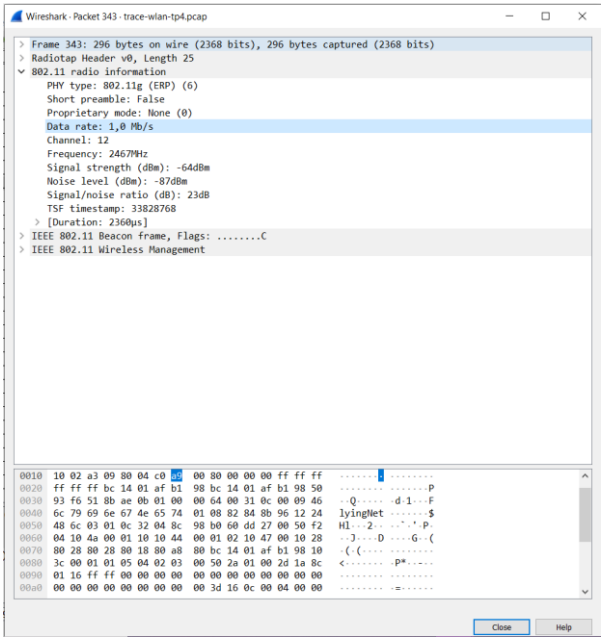


Figura 6 *: Exercício 3*

Scanning Passivo e Scanning Ativo

4 Selecione uma trama beacon (trama 1043). 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)?

R:. Esta trama pertence as tramas 802.11 de tipo Management. Tem identificadores de tipo 00 e de subtipo 1000. Estão especificadas no Frame Control Field.

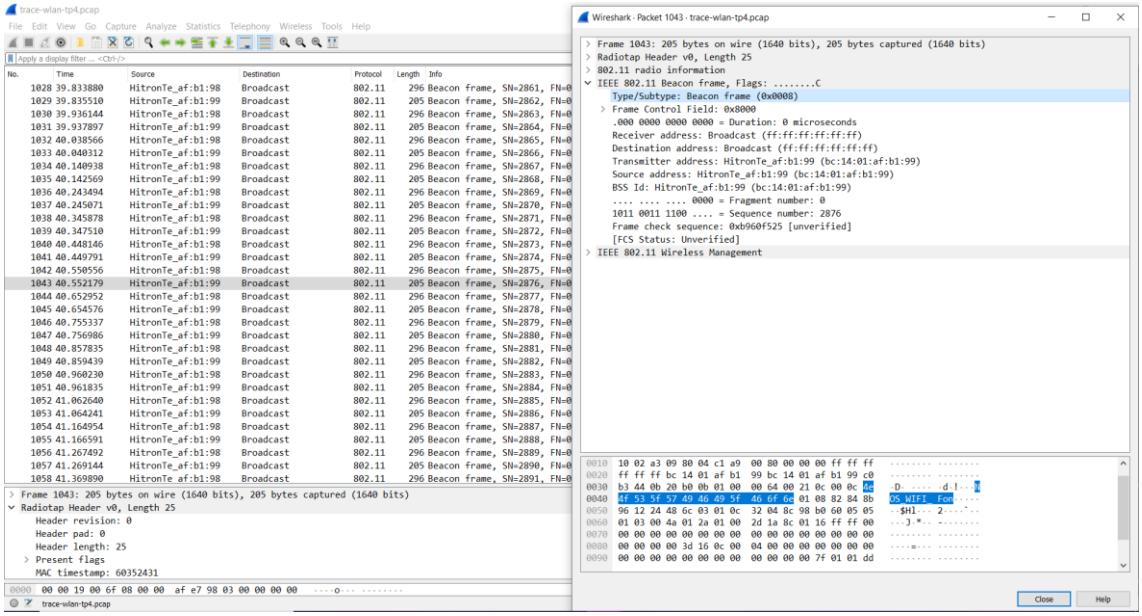


Figura 7 : *Exercício 4*

Table 1—Valid type and subtype combinations

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	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

Figura 8 : *Exercício 4*

```
Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
```

Figura 9 : *Exercício 4*

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

R:. Na trama conseguimos identificar 3 endereços MAC. Concluímos que a sua origem é um AP que emite a mensagem em Broadcast (para toda a gente).

Origem - (bc:14:01:af:b1:99)

Destino - (ff:ff:ff:ff:ff:ff)

Transmitter – (bc:14:01:af:b1:99)

```
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)
```

Figura 10 : *Exercício 5*

```
0000  00 00 19 00 6f 08 00 00  af e7 98 03 00 00 00 00
0010  10 02 a3 09 80 04 c1 a9  00 80 00 00 00 ff ff ff
0020  ff ff ff bc 14 01 af b1  99 bc 14 01 af b1 99 c0
0030  b3 44 0b 20 b0 0b 01 00  00 64 00 21 0c 00 0c 4e
0040  4f 53 5f 57 49 46 49 5f  46 6f 6e 01 08 82 84 8b
0050  96 12 24 48 6c 03 01 0c  32 04 8c 98 b0 60 05 05
0060  01 03 00 4a 01 2a 01 00  2d 1a 8c 01 16 ff ff 00
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0080  00 00 00 00 3d 16 0c 00  04 00 00 00 00 00 00 00
```

Figura 11 : *Exercício 5*

```
0000  00 00 19 00 6f 08 00 00  af e7 98 03 00 00 00 00
0010  10 02 a3 09 80 04 c1 a9  00 80 00 00 00 ff ff ff
0020  ff ff ff bc 14 01 af b1  99 bc 14 01 af b1 99 c0
0030  b3 44 0b 20 b0 0b 01 00  00 64 00 21 0c 00 0c 4e
0040  4f 53 5f 57 49 46 49 5f  46 6f 6e 01 08 82 84 8b
0050  96 12 24 48 6c 03 01 0c  32 04 8c 98 b0 60 05 05
0060  01 03 00 4a 01 2a 01 00  2d 1a 8c 01 16 ff ff 00
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0080  00 00 00 00 3d 16 0c 00  04 00 00 00 00 00 00 00
```

Figura 12 : *Exercício 5*

```
0000  00 00 19 00 6f 08 00 00  af e7 98 03 00 00 00 00
0010  10 02 a3 09 80 04 c1 a9  00 80 00 00 00 ff ff ff
0020  ff ff ff bc 14 01 af b1  99 bc 14 01 af b1 99 c0
0030  b3 44 0b 20 b0 0b 01 00  00 64 00 21 0c 00 0c 4e
0040  4f 53 5f 57 49 46 49 5f  46 6f 6e 01 08 82 84 8b
0050  96 12 24 48 6c 03 01 0c  32 04 8c 98 b0 60 05 05
0060  01 03 00 4a 01 2a 01 00  2d 1a 8c 01 16 ff ff 00
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0080  00 00 00 00 3d 16 0c 00  04 00 00 00 00 00 00 00
```

Figura 13 : *Exercício 5*

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?

R:.

Os débitos base são : .

```
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
   Tag Number: Supported Rates (1)
   Tag length: 8
   Supported Rates: 1(B) (0x82)
   Supported Rates: 2(B) (0x84)
   Supported Rates: 5.5(B) (0x8b)
   Supported Rates: 11(B) (0x96)
   Supported Rates: 9 (0x12)
   Supported Rates: 18 (0x24)
   Supported Rates: 36 (0x48)
   Supported Rates: 54 (0x6c)
```

Figura 14 : *Exercício 6*

Os débitos adicionais : .

```
Tag: Extended Supported Rates 6(B), 12(B), 24(B), 48, [Mbit/sec]
   Tag Number: Extended Supported Rates (50)
   Tag length: 4
   Extended Supported Rates: 6(B) (0x8c)
   Extended Supported Rates: 12(B) (0x98)
   Extended Supported Rates: 24(B) (0xb0)
   Extended Supported Rates: 48 (0x60)
```

Figura 15 : *Exercício 6*

7 Qual o intervalo de tempo previsto entre tramas beacon consecutivas? (nota: este valor é anunciado na própria trama beacon). Na prática, a periodicidade de tramas beacon provenientes do mesmo AP é verificada? Tente explicar porquê.

R:. O intervalo previsto entre tramas é 0.1024 segundos . Não, como podemos verificar nas seguintes imagens o valor prático é diferente (aproximadamente 0.0016 segundos). Isto pode acontecer devido a fatores como a falta de precisão de um AP ou à distância entre os endereços destino e envio.

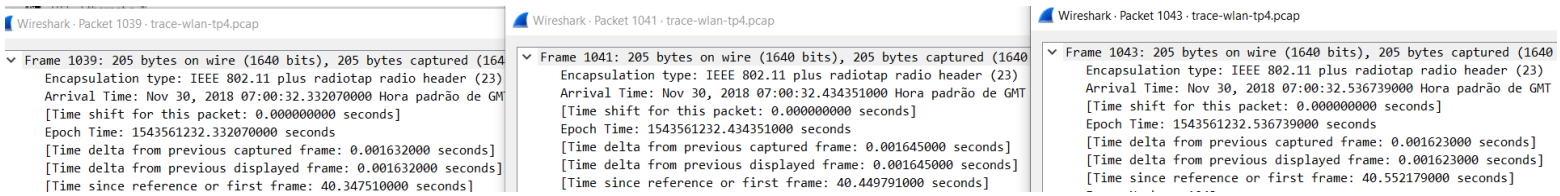


Figura 16 : *Exercício 7*

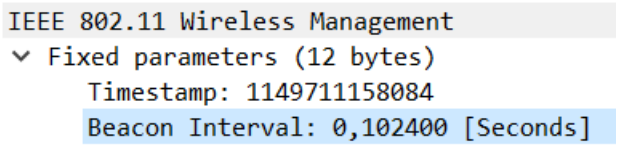


Figura 17 : *Exercício 7*

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).

R:.

1. usamos o filtro wlan.addr == ff : ff : ff : ff : ff : ff
2. ordenamos por source
3. vimos todos os SSIDs diferentes
4. concluimos que só existia dois, FlyingNet e NOS_WIFI_Fon

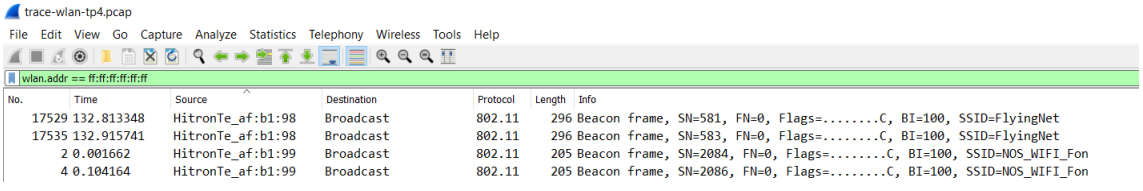


Figura 18 : *Exercício 8*

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

R:. O CRC é um processo do protocolo FCS. Após ativar este protocolo e o wlan.check_checksum percebemos que foram detetadas 5 tramas com esse filtro. Concluímos que faz sentido haver erros nas redes Wi-Fi uma vez que o meio é partilhado e é fácil ocorrerem erros de transmissão ou de reflexão.

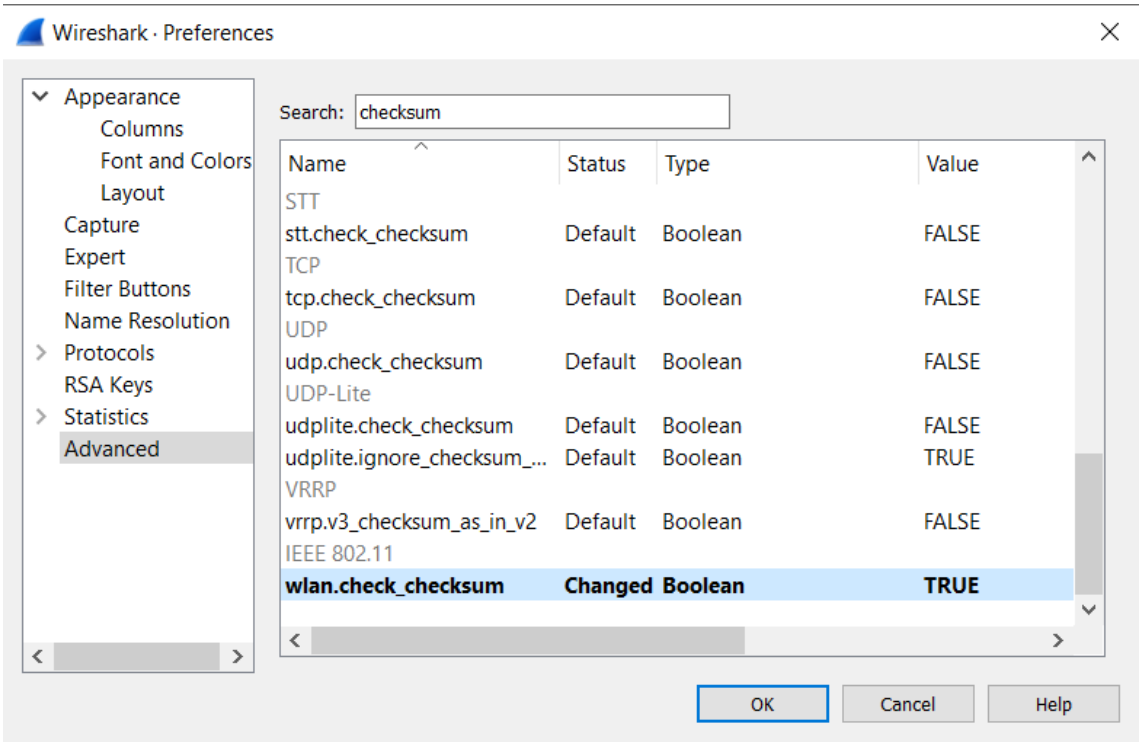


Figura 19 *: Exercício 9*

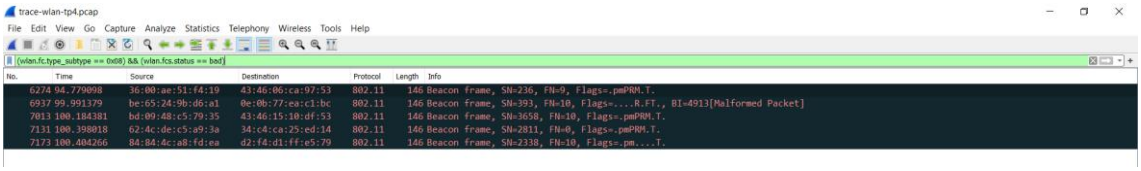


Figura 20 *: Exercício 9*

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

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

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?

R:. O probe request é um broadcast cuja o endereço mac source é o mesmo que o endereço mac destination do probe response.

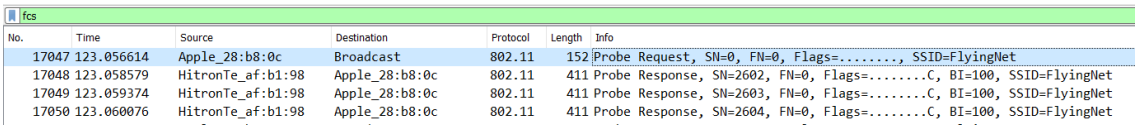


Figura 21 : *Exercício 11*

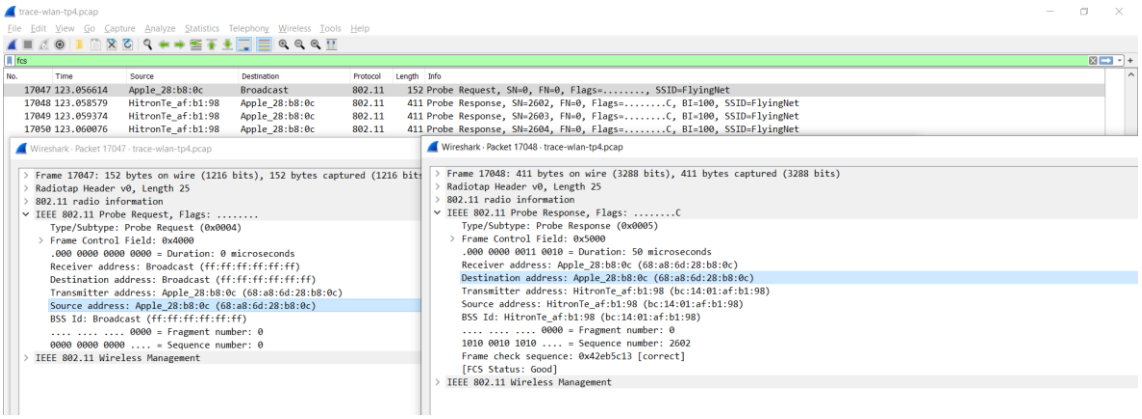


Figura 22 : *Exercício 11*

Processo de Associação

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.

R:. wlan.fc.type == 0 && (wlan.fc.type_subtype == 0 | | wlan.fc.type_subtype == 1 || wlan.fc.type_subtype == 11)

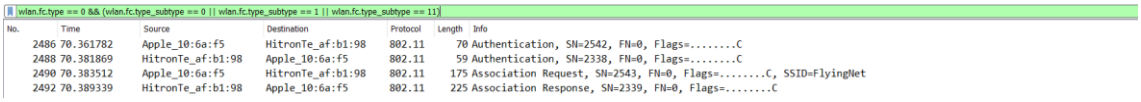


Figura 19 : *Exercício 12*

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

R:.

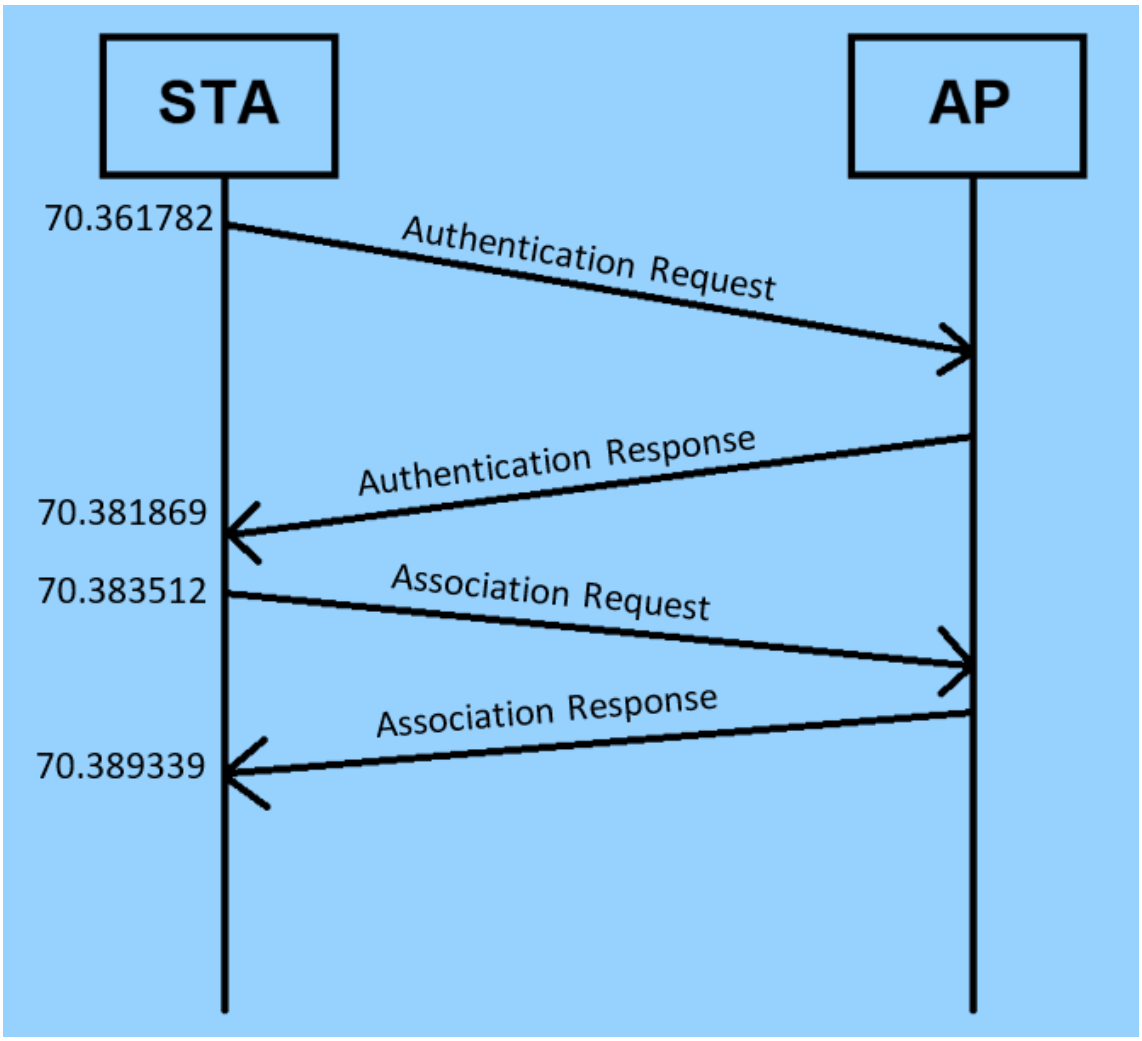


Figura 20 : *Exercício 13*

Transferência de Dados

14 Considere a trama de dados nº455. 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?

R:. Em relação ao direcionamento da trama podemos verificar que entra num ambiente wireless vindo de DS para STA. Sendo uma trama data de um DS para um DS concluímos que será local.

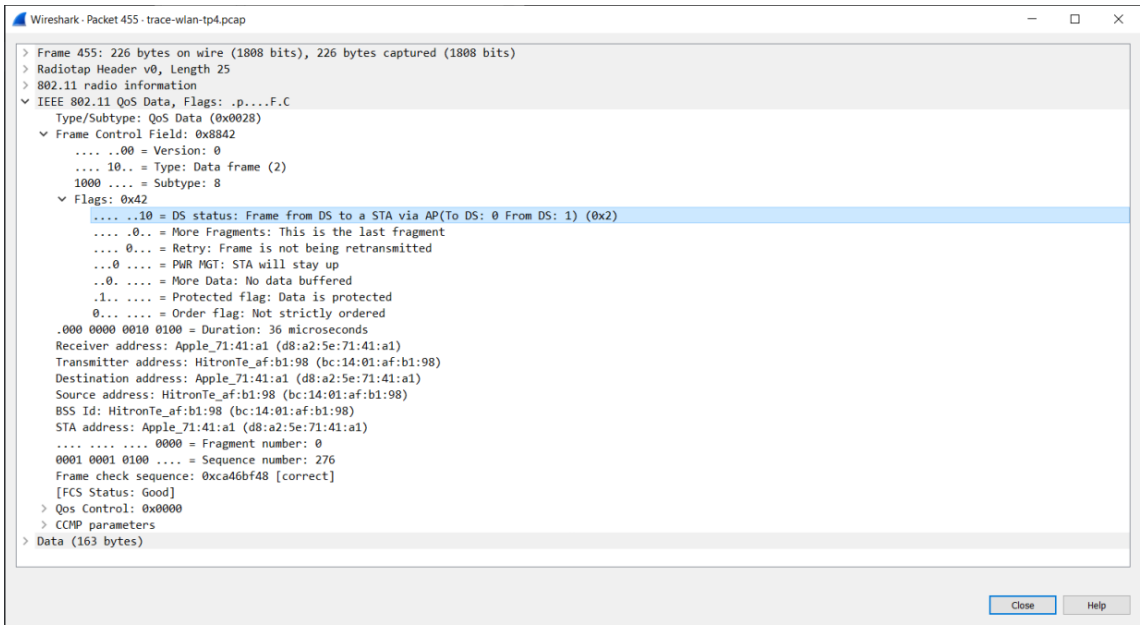


Figura 21 : *Exercício 14*

15 Para a trama de dados nº455, 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?

R:.

Host sem fios (STA): (d8:a2:5e:71:41:a1) <- Address 1

AP : (bc:14:01:af:b1:98) <- Address 2

Router de acesso ao SD: (bc:14:01:af:b1:98) <- Address 3

```
Receiver address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
Destination address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
```

Figura 22 : *Exercício 15*

16 Como interpreta a trama nº457 face à sua direccionalidade e endereçamento MAC?

R:. Quanto a direccionalidade da trama podemos verificar na figura 27 que vai do STA para o DS via um AP, ou seja, do DS: 0 para o DS: 1.

Conseguimos identificar que o pacote está a mover-se para fora do ambiente wireless passando para um dispositivo na rede do centro de distribuição.

BSSID <- Address 1

Source <- Address 2

Destination <- Address 3

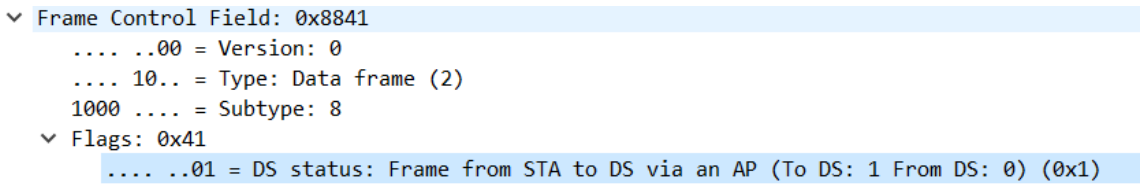


Figura 23 : *Exercício 16*

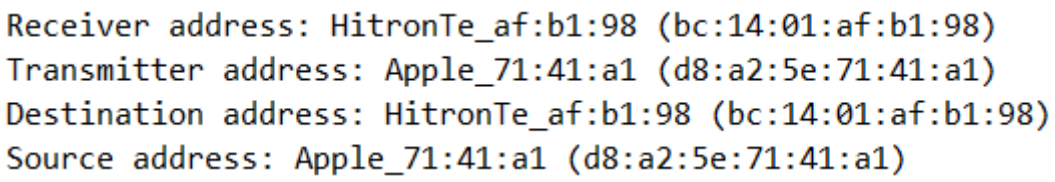


Figura 24 : *Exercício 16*

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.)

R:. Tramas de acknowledgement. Como a rede sem fios é muito mais suscetível a erros, existem tramas de controlo que são enviadas como confirmação de que as tramas foram recebidas de uma forma correta.

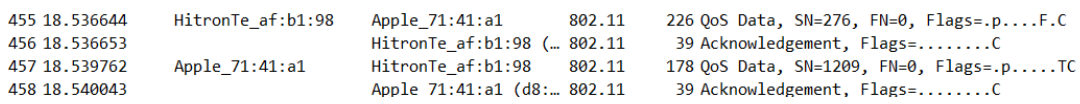


Figura 25 : *Exercício 17*

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.

R:. Só há um sistema envolvido, ou seja, o próprio DS. Sendo o endereçamento de RTS (64:9a:be:10:6a:f5) e de CTS (bc:14:01:af:b1:98).

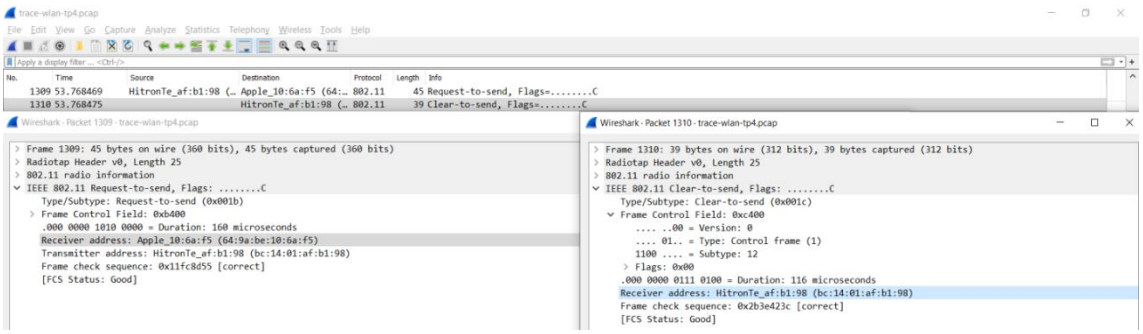


Figura 30 : *Exercício 18*

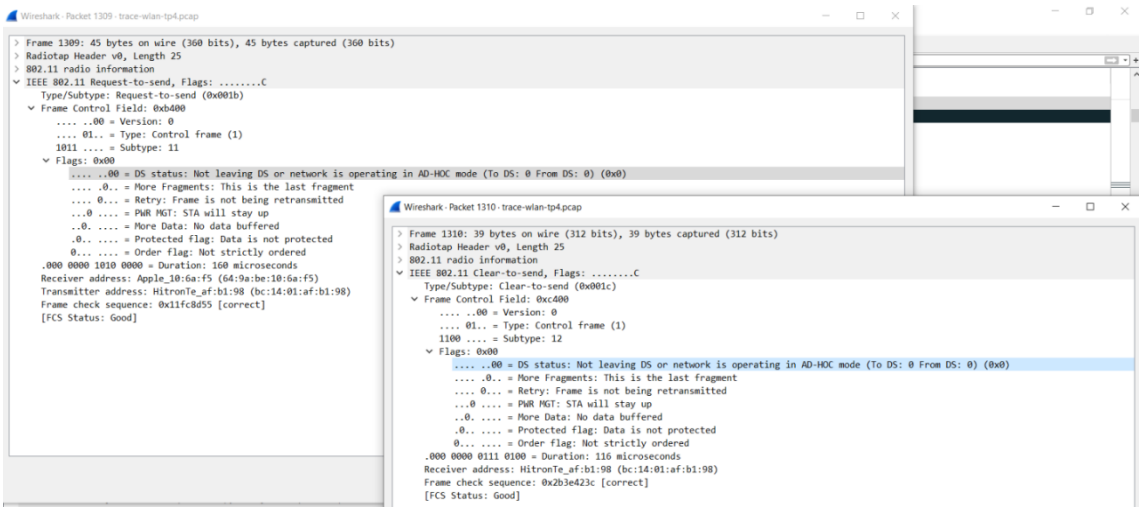


Figura 31 : *Exercício 18*

Conclusão

Com este trabalho prático complementamos os conhecimentos obtidos nas aulas teóricas sobre o capitulo de Wireless And Mobile Networks (redes sem fios). Dentro desta focamo-nos no protocolo IEEE 802.11.

Primeiramente obtivemos um melhor entendimento sobre o formato das tramas. Neste contexto, utilizamos a "Table 1 – Valid type and subtype combinations" para averiguar o tipo e subtipo de diversas tramas, tendo também verificado a direccionalidade de cada uma delas através dos seus adresses , mais concretamente receiver, transmitter, destination e source.

Respetivamente a deteção e correção de erros, usamos como ferramenta de auxilio o campo CRC (Cyclic Redundancy Check), conseguindo assim detetar as tramas danificadas. Visto que foram detetadas 5 tramas, comprovamos que a rede Wi-Fi é suscetível a erros, uma vez que é vulnerável às condições do meio.

De seguida, analisamos o processo de comunicação entre STA (station) e AP (acess point), com especial atenção nos processos de associação completo e autenticação.

Durante a realização deste trabalho foram também utilizados diversos filtros de modo a facilitar a analise das tramas capturadas pelo whireshark.