

TP4: Redes Sem Fios (802.11)

Diogo Braga, João Silva, and Ricardo Caçador

University of Minho, Department of Informatics, 4710-057 Braga, Portugal

e-mail: {a82547,a82005,a81064}@alunos.uminho.pt

PL4, Grupo 7

1 Acesso Rádio

1.1 Exercício 1

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

```
▼ 802.11 radio information
  PHY type: 802.11g (6)
  Short preamble: False
  Proprietary mode: None (0)
  Data rate: 1.0 Mb/s
  Channel: 12
  Frequency: 2467MHz
  Signal strength (dBm): -60dBm
  Noise level (dBm): -87dBm
  TSF timestamp: 34033570
  ► [Duration: 2360µs]
```

Fig. 1. 802.11 Radio Information

R: Como se pode observar na figura 1 delimitado a vermelho, a rede sem fios opera na frequência **2467 MHz**, no canal **12**.

1.2 Exercício 2

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

R: A versão usada é a **802.11g**. Tal pode ser verificado sublinhado a azul na 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 WiFi pode operar? Justifique.

R: A trama foi enviada a um débito de **1.0 Mb/s**, como se pode verificar na 1 sublinhado a verde. Este débito não corresponde ao máximo que a interface Wifi pode operar, pois segundo a norma 802.11g é oferecida uma velocidade máxima de 54 Mb/s.

2 Scanning Passivo e Scanning Ativo

2.1 Exercício 4

Selecione uma trama beacon (e.g., a trama 3XX). 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)?

```

▼ IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  ▼ Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8

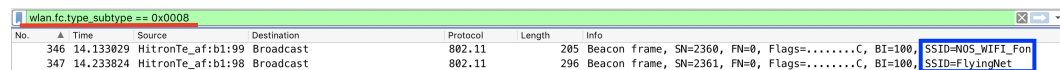
```

Fig. 2. Tipo e Subtipo da Trama

R: Esta trama é do tipo **Management**, e valor que o identifica é o **0**, como sublinhado na 2 a vermelho. O subtipo da trama é **Beacon**, e o valor que o identifica é o **8**, em binário **1000**. Estes valores estão especificados no byte 26 do cabeçalho da trama.

2.2 Exercício 5

Liste todos os SSIDs dos APs (Access Points) que estão a operar na vizinhança da STA de captura? Explícite o modo como obteve essa informação. Como sugestão pode construir um filtro de visualização o apropriado (tomando como base a resposta da alínea anterior) que lhe permita obter a listagem pretendida.



No.	Time	Source	Destination	Protocol	Length	Info
346	14.133029	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2360, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
347	14.233824	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2361, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Fig. 3. Diferentes SSID.

R: Como se pode observar na figura 3 delimitado a azul, os dois SSIDs dos Access Points que estão a operar na vizinhança da STA de captura são o **FlyingNet** e o **NOS_WIFI_Fon**. Todas as restantes tramas Beacon presentes na captura pertencem a estes dois SSIDs. Tal foi mais facilmente obtido usando o filtro de visualização **wlan.fc.type_subtype == 0x0008** sublinhado a vermelho na figura. Este comando filtra todos os subtipos que são Beacon.

2.3 Exercício 6

Verifique se está a ser usado o método de detecção de erros (CRC), e se todas as tramas Beacon são recebidas corretamente. Justifique o porquê de usar detecção de erros neste tipo de redes locais.

```

▼ IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  ▶ Frame Control Field: 0x8000
    .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: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    .... ..00 = Fragment number: 0
    1001 0011 1001 .... = Sequence number: 2361
    Frame check sequence: 0x55a094da [correct]
    [FCS Status: Good]

```

Fig. 4. Campo CRC.

No.	Time	Source	Destination	Protocol	Length	Info
6274	94.779098	36:00:ae:51:f4:19	43:46:06:ca:97:53	802.11	146	Beacon frame, SN=236, FN=9, Flags=pmPRM.T.
6937	99.991379	be:65:24:9b:d6:a1	0e:0b:77:ea:c1:bc	802.11	146	Beacon frame, SN=393, FN=10, Flags=...R.FT., BI=4913 [Malformed Packet]
7013	100.1043...	ba:09:40:e5:79:35	43:46:06:ca:97:53	802.11	146	Beacon frame, SN=3058, FN=10, Flags=pmPRM.T.
7131	100.3980...	62:4c:de:c5:a9:3a	34:c4:ca:25:ed:14	802.11	146	Beacon frame, SN=2811, FN=0, Flags=pmPRM.T.
7173	100.4042...	84:84:4c:a8:fd:ea	d2:f4:d1:ff:e5:79	802.11	146	Beacon frame, SN=2338, FN=10, Flags=pm...T.
2	0.001662	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2084, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
4	0.104164	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2086, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
6	0.206582	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2088, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
8	0.308999	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2090, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
10	0.411376	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2092, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
12	0.513787	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2094, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

Fig. 5. Tramas Beacon com erros.

R: Como se pode verificar na figura 4 sublinhado a vermelho, está a ser usado o **Frame Check Sequence** no campo CRC. Este campo é usado para que quem recebe a trama consiga detetar erros nos bits. Num ambiente Wireless, neste caso 802.11, a existência destes erros é muito mais comum.

Como se pode constatar na figura 5, existem 5 tramas Beacon cujo campo CRC indica a existência de erros.

2.4 Exercício 7

Para dois dos APs identificados, indique qual é 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 é verificada? Tente explicar porquê.

```

> Frame 347: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....C
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters (12 bytes)
    Timestamp: 0x0000010bae8e71fa
    Beacon Interval: 0.102400 [Seconds]
  > Capabilities Information: 0x0c31
  > Tagged parameters (231 bytes)

```

Fig. 6. Beacon Interval da trama 347.

```

> Frame 348: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....C
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters (12 bytes)
    Timestamp: 0x0000010bae8e7b44
    Beacon Interval: 0.102400 [Seconds]
  > Capabilities Information: 0x0c21
  > Tagged parameters (140 bytes)

```

Fig. 7. Beacon Interval da trama 348.

```

[Time delta from previous captured frame: 0.100795000 seconds]
[Time delta from previous displayed frame: 0.100795000 seconds]
[Time since reference or first frame: 14.233824000 seconds]

```

Fig. 8. Tempo entre tramas.

R: Como se pode verificar na figura 6 sublinhado a vermelho, o intervalo de tempo previsto para a trama 347 é **0.102400 s**. Para a trama 348 o intervalo de tempo previsto é também **0.102400 s**, tal como pode ser verificado sublinhado a azul na 7.

Analisando várias tramas nota-se que a periodicidade é verificada, pois o tempo entre tramas Beacon é muito próximo ao **Beacon Interval**, como se pode constatar na figura 8.

2.5 Exercício 8

Identifique e registe todos os endereços MAC usados nas tramas beacon enviadas pelos APs. Recorde que o endereçamento está definido no cabeçalho das tramas 802.11, podendo ser utilizados até quatro endereços com diferente semântica. Para uma descrição detalhada da estrutura da trama 802.11, consulte o anexo ao enunciado.

```
▼ IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  ▶ Frame Control Field: 0x8000
    .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: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  .... 0000 = Fragment number: 0
  1001 0011 1001 .... = Sequence number: 2361
  Frame check sequence: 0x55a094da [correct]
  [FCS Status: Good]
```

Fig. 9. Addressing de uma trama Beacon.

R: Como se pode observar na figura 9, estamos perante 3 endereços MAC. O endereço 1 é **ff:ff:ff:ff:ff:ff**, o endereço 2 é **bc:14:01:af:b1:98**, e o endereço 3 é **bc:14:01:af:b1:98**. Neste caso, o endereço 4 não está a ser usado.

2.6 Exercício 9

As tramas beacon anunciam que o AP pode suportar vários débitos de base assim como vários "extended supported rates". Indique quais são esses débitos?

```
▼ IEEE 802.11 wireless LAN
  ▶ Fixed parameters (12 bytes)
  ▼ Tagged parameters (231 bytes)
    ▶ Tag: SSID parameter set: FlyingNet
    ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 12
    ▶ Tag: Extended Supported Rates 6(B), 12(B), 24(B), 48, [Mbit/sec]
    ▶ Tag: Vendor Specific: Microsoft Corp.: WPS
    ▶ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▶ Tag: ERP Information
    ▶ Tag: HT Capabilities (802.11n D1.10)
    ▶ Tag: HT Information (802.11n D1.10)
    ▶ Tag: Extended Capabilities (1 octet)
    ▶ Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
    ▶ Tag: RSN Information
    ▶ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    ▶ Tag: QBSS Load Element 802.11e CCA Version
    ▶ Tag: Vendor Specific: Ralink Technology, Corp.
```

Fig. 10. Débitos Suportados.

R: Os débitos de base suportados encontram-se na figura 10 sublinhados a vermelho, enquanto os *extended supported rates* se encontram sublinhados a azul.

2.7 Exercício 10

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

No.	Time	Source	Destination	Protocol	Length	Info
1300	53.746911	Apple_10:6a:f5	Broadcast	802.11	155	Probe Request, SN=2516, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2467	70.147855	ea:a4:64:7b:b9:7a	Broadcast	802.11	167	Probe Request, SN=2540, FN=0, Flags=.....C, SSID=2WIRE-PT-431
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
2603	72.179215	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2563, FN=0, Flags=.....C, SSID=FlyingNet
2606	72.179924	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2346, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Fig. 11. Probing Requests e Probing Responses.

R: O filtro de visualização utilizado foi `wlan.fc.type_subtype == 0x0004 || wlan.fc.type_subtype == 0x0005`.

2.8 Exercício 11

Identifique um *probing request* para o qual tenha havido um *probing response*. Faça ao endereçamento usado, indique a que sistemas são endereçadas estas tramas e explique qual o propósito das mesmas?

```

▼ IEEE 802.11 Probe Request, Flags: .....C
  Type/Subtype: Probe Request (0x0004)
  ▶ Frame Control Field: 0x4000
    .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: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)
    Source address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    .... 0000 = Fragment number: 0
    1001 1110 1101 .... = Sequence number: 2541
    Frame check sequence: 0xb4f532e2 [correct]
    [FCS Status: Good]

```

Fig. 12. Probe Request.

```

▼ IEEE 802.11 Probe Response, Flags: .....C
  Type/Subtype: Probe Response (0x0005)
  ▶ Frame Control Field: 0x5000
    .000 0000 0011 0010 = Duration: 50 microseconds
    Receiver address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)
    Destination address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)
    Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    .... 0000 = Fragment number: 0
    1001 0001 1100 .... = Sequence number: 2332
    Frame check sequence: 0xbce842e3 [correct]
    [FCS Status: Good]

```

Fig. 13. Probe Response.

R: Como se pode verificar nas figuras 12 e 13, inicialmente ocorreu um Probe Request proveniente de um aparelho com o endereço MAC **ea:a4:64:7b:b9:7a**, de seguida um AP com o endereço MAC **bc:14:01:af:b1:98** enviou um Probe Response de modo a poder dizer aparelho que se encontra disponível para que haja associação entre os dois.

3 Processo de Associação

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.

wlan.fc.type_subtype == 4 wlan.fc.type_subtype == 5 wlan.fc.type_subtype == 0 wlan.fc.type_subtype == 1 wlan.fc.type_subtype == 11						
No.	A	Time	Source	Destination	Protocol	Length
1300	53.746911		Apple_10:6a:f5	Broadcast	802.11	155
2467	70.147855		ea:a4:64:7b:b9:7a	Broadcast	802.11	167
2468	70.149098		ea:a4:64:7b:b9:7a	Broadcast	802.11	155
2469	70.149792		HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411
2471	70.150537		HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411
2473	70.151237		HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411
2475	70.151709		HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201
2477	70.152099		HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201
2479	70.152570		HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201
2486	70.361782		Apple_10:6a:f5	HitronTe_af:b1:98	802.11	70
2488	70.381869		HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59
2490	70.383512		Apple_10:6a:f5	HitronTe_af:b1:98	802.11	175
2492	70.389339		HitronTe_af:b1:98	Apple_10:6a:f5	802.11	225

Fig. 14. Processo de associação.

R:

O filtro de visualização utilizado foi `wlan.fc.type_subtype == 4 || wlan.fc.type_subtype == 5 || wlan.fc.type_subtype == 0 || wlan.fc.type_subtype == 1 || wlan.fc.type_subtype == 11`.

O processo de Scanning ativo já foi identificado em questões anteriores. É então de grande importância referir as tramas de autenticação quem são respectivamente a trama 2486 e a trama 2488, e as tramas de associação que são respectivamente a trama 2490 e a trama 2492.

3.2 Exercício 13

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

R:

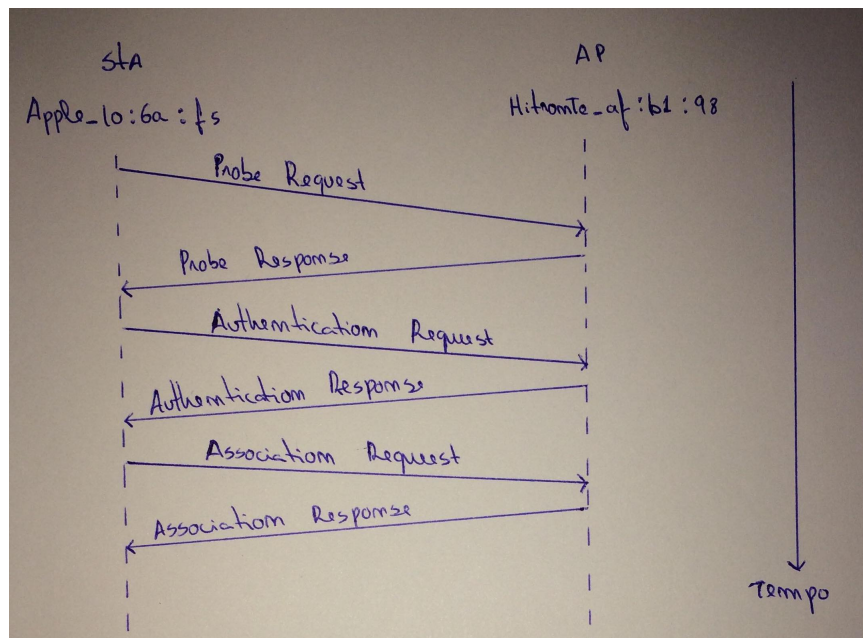


Fig. 15. Diagrama de tramas.

4 Transferência de Dados

4.1 Exercício 14

Considere a trama de dados no 455. 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?

```
▼ IEEE 802.11 QoS Data, Flags: .p....F.C
  Type/Subtype: QoS Data (0x0028)
  ▼ Frame Control Field: 0x8842
    .... 00 = Version: 0
    .... 10.. = Type: Data frame (2)
    1000 .... = Subtype: 8
  ▼ 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... .... = Order flag: Not strictly ordered
  .000 0000 0010 0100 = Duration: 36 microseconds
```

Fig. 16. Direcionalidade da trama 455.

R: Como se pode verificar na figura 16 sublinhado a vermelho, a direcionalidade da trama é **To DS: 0 From DS: 1**, o que significa que a trama é recebida pela station proveniente do sistema de distribuição via AP. A trama é local à WLAN.

4.2 Exercício 15

Para a trama de dados no 455, 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?

```
▼ IEEE 802.11 QoS Data, Flags: .p....F.C
  Type/Subtype: QoS Data (0x0028)
  ▶ Frame Control Field: 0x8842
  .000 0000 0010 0100 = Duration: 36 microseconds
  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)
  BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  STA address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
```

Fig. 17. Endereços da trama 455.

R: Como se pode verificar na figura 17, o endereço MAC correspondente ao STA é **d8:a2:5e:71:41:a1**. Este corresponde também ao Receiver Address e ao Destination Address, visto estes identificarem o mesmo equipamento. O endereço MAC correspondente ao AP é o mesmo que o do router de acesso, apesar de estarem em campos da trama diferentes. Referimo-nos ao **bc:14:01:af:b1:98**. Este endereço MAC corresponde ao Source Address, ao Transmitter Address e ao BSSID.

4.3 Exercício 16

Como interpreta a trama no 457 face à sua direccionalidade e endereçamento MAC?

```

▼ 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... .... = Order flag: Not strictly ordered
.000 0001 0011 1010 = Duration: 314 microseconds

```

Fig. 18. Direccionalidade da trama 457.

```

▼ IEEE 802.11 QoS Data, Flags: .p....TC
Type/Subtype: QoS Data (0x0028)
► Frame Control Field: 0x8841
.000 0001 0011 1010 = Duration: 314 microseconds
Receiver address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
Transmitter address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
Destination address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
Source address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
STA address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
.... .... 0000 = Fragment number: 0

```

Fig. 19. Endereços da trama 457.

R: Como se pode verificar na figura 16 sublinhado a vermelho, a direccionalidade da trama é **To DS: 1 From DS: 0**, o que significa que a trama é enviada pela station para o sistema de distribuição via AP.

Quanto aos endereços MAC, estes são exactamente os opostos da trama 455 uma vez que a trama vai da estação para o AP e não do AP para a estação como se verificava na trama 455.

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).

R: Os subtipos de tramas de controlo transmitidas são **Request-to-send**, **Clear-to-send** e **Acknowledgement**. Este tipo de tramas de controlo nas redes 802.11 têm de existir pois são a forma de lidar com as colisões que ocorrem através de estações escondidas, de uma forma geral este "protocolo" faz uma reserva de meio para poder transmitir.

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 direccionalidade das tramas e os sistemas envolvidos.


```

▼ IEEE 802.11 Request-to-send, Flags: .....C
Type/Subtype: Request-to-send (0x001b)
▼ Frame Control Field: 0xb400
.... ..00 = Version: 0
.... ..01.. = Type: Control frame (1)
1011 .... = Subtype: 11
▼ Flags: 0x00
.... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
.... ..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
.0.. .... = Protected flag: Data is not protected
0... .... = Order flag: Not strictly ordered
.000 0000 1010 0010 = Duration: 162 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)
Frame check sequence: 0xfce4fa85 [correct]
[FCS Status: Good]

```

Fig. 20. Trama Request-to-Send.

```

▼ IEEE 802.11 Clear-to-send, Flags: .....C
Type/Subtype: Clear-to-send (0x001c)
▼ Frame Control Field: 0xc400
.... ..00 = Version: 0
.... ..01.. = Type: Control frame (1)
1100 .... = Subtype: 12
▼ Flags: 0x00
.... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
.... ..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
.0.. .... = Protected flag: Data is not protected
0... .... = Order flag: Not strictly ordered
.000 0000 0111 0110 = Duration: 118 microseconds
Receiver address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
Frame check sequence: 0x437c3320 [correct]
[FCS Status: Good]

```

Fig. 21. Trama Clear-to-Send.

R: Sim, estão a ser usadas tramas RTS/CTS.

Primeiro a trama Request-to-Send é enviada da estação para o AP para tentar reservar o meio para transmitir, esta é feita em modo ad-hoc, uma vez que os campos ToDS e FromDS estão a 0, como é possível verificar na figura 20 sublinhado a vermelho.

O AP responde fazendo broadcast de uma trama Clear-to-Send, para avisar todas as estações quem pode transmitir. Esta trama é transmitida em modo ad-hoc uma vez que os campos ToDS e FromDS estão a 0, como é possível verificar na figura 21 sublinhado a vermelho.

5 Conclusão

Neste trabalho prático abordamos principalmente temas relacionados com Wireless e Redes Móveis.

Na primeira secção abordamos as frequências no qual as redes sem fios operam.

Na segunda e terceira secção trabalhamos com scanning ativo e passivo, nomeadamente as tramas beacon no primeiro caso, e os probing response e probing request no segundo caso.

Na quarta e última secção abordamos o endereçamento das tramas, com especial foco nas tramas de controlo.

Concluindo, com este guião exploramos a fundo as questões do nível de ligação de dados em 802.11, e conseguimos de forma muito prática consolidar os conceitos mais teóricos do funcionamento deste tipo de redes.