
Redes - TP4

TRABALHO REALIZADO POR:

CARLOS MIGUEL LUZIA DE CARVALHO

RUBEN CÉSAR FERREIRA LUCAS

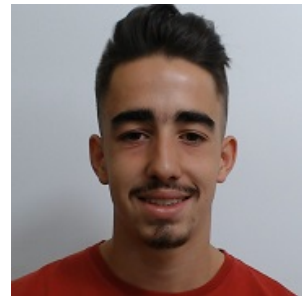
PAULO SILVA SOUSA



A89605
Carlos Carvalho



A89487
Ruben Lucas



A89465
Paulo Sousa

Índice

1	Acesso Rádio	1
2	Scanning Passivo e Scanning Ativo	3
3	Processo de Associação	9
4	Transferência de Dados	10
5	Conclusão	13

1 Acesso Rádio

Como pode ser observado, a sequência de bytes capturada inclui informação do nível físico (radio information), para além dos bytes correspondentes a tramas 802.11. Para a trama correspondente 3XX em que XX corresponde ao seu número de TurnoGrupo

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

A rede sem fios opera na frequência de 2467MHz correspondente ao canal 12.

```
▶ Frame 347: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
▶ Radiotap Header v0, Length 25
▼ 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]
```

Figure 1: Frequência da rede sem fios

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

A versão da norma IEEE 802.11 em uso é a 802.11g (6)

```
▶ Frame 347: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
▶ Radiotap Header v0, Length 25
▼ 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]
```

Figure 2: Versão da norma IEEE 802.11

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.

A rede sem fios têm uma data rate de 1.0Mb/s. Esta interface tem um data rate máximo de 54Mb/s. (Falta a explicação de ser 1.0 em vez de 54)

```
▶ Frame 347: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
▶ Radiotap Header v0, Length 25
▼ 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]
```

Figure 3: Débito da trama escolhida

4. Selecione uma trama beacon (e.g., trama 10XX). 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 1047 pertence ao tipo 802.11g (6). O tipo corresponde a um Management Frame (Frame de Gestão), enquanto que o subtipo tem o valor de identificação: 8 que corresponde a um beacon. (incompleto)

```
▶ Frame 1047: 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
  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:b1:99 (bc:14:01:af:b1:99)
    Source address: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
    BSS Id: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
    .... .... 0000 = Fragment number: 0
    1011 0100 0000 .... = Sequence number: 2880
    Frame check sequence: 0xc0004e76 [correct]
    [FCS Status: Good]
```

Figure 4: TODO: CAPTION MISSING

2 Scanning Passivo e Scanning Ativo

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

Os endereços MAC são ff:ff:ff:ff:ff:ff e bc:14:01:af:b1:99. Como podemos ver na imagem, sendo que ambas as flags from DS e to DS são ambas 0, podemos concluir que a trama ou pertence a uma rede ad-hoc ou não sai da rede wireless. Neste caso Corresponde a uma rede ad-hoc, tratando-se da NOS-WIFI-Fon.

```
> Frame 1047: 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
  Type/Subtype: Beacon frame (0x0008)
  √ Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
  √ 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 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:b1:99 (bc:14:01:af:b1:99)
  Source address: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
  BSS Id: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
  .... .... 0000 = Fragment number: 0
  1011 0100 0000 .... = Sequence number: 2880
  Frame check sequence: 0xc0004e76 [unverified]
  [FCS Status: Unverified]
> IEEE 802.11 Wireless Management
```

Figure 5: Trama 1047

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?

O AP com SSID *NOS_WIFI_Fon* pode suportar débitos de base de 1 até 54Mbps e “*extended supported Rates*” de 6 até 48Mbps:

347	14.233824	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2361, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
348	14.235456	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2362, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
349	14.336138	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2363, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
350	14.337754	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2364, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
351	14.438683	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2365, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
352	14.440234	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2366, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
353	14.540874	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2367, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
<div> <div>Fixed parameters (12 bytes)</div> <div>Timestamp: 114968433986</div> <div>Beacon Interval: 0.102400 [Seconds]</div> <div>Capabilities Information: 0x0c31</div> <div>Tagged parameters (231 bytes)</div> <div>Tag: SSID parameter set: FlyingNet</div> <div>Tag Number: SSID parameter set (0)</div> <div>Tag length: 9</div> <div>SSID: FlyingNet</div> <div>Tag: Supported Rates 1(0), 2(0), 5.5(0), 11(0), 9, 18, 36, 54, [Mbit/sec]</div> <div>Tag Number: Supported Rates (1)</div> <div>Tag length: 8</div> <div>Supported Rates: 1(0) (0x82)</div> <div>Supported Rates: 2(0) (0x84)</div> <div>Supported Rates: 5.5(0) (0x8b)</div> <div>Supported Rates: 11(0) (0x96)</div> <div>Supported Rates: 9 (0x12)</div> <div>Supported Rates: 18 (0x24)</div> <div>Supported Rates: 36 (0x48)</div> <div>Supported Rates: 54 (0x6c)</div> <div>Tag: DS Parameter set: Current Channel: 12</div> <div>Tag Number: DS Parameter set (3)</div> <div>Tag length: 1</div> <div>Current Channel: 12</div> <div>Tag: Extended Supported Rates 6(0), 12(0), 24(0), 48, [Mbit/sec]</div> <div>Tag Number: Extended Supported Rates (50)</div> <div>Tag length: 4</div> <div>Extended Supported Rates: 6(0) (0x8c)</div> <div>Extended Supported Rates: 12(0) (0x98)</div> <div>Extended Supported Rates: 24(0) (0xb0)</div> </div>						
0040	6c 79 69 6e 67 4e 65 74	01 08 82 84 8b 96 12 24	FlyingNet	\$	
0050	08 0e 03 01 0c 32 04 0c	09 1a 68 dd 21 00 50 f2	W	2P	
0060	04 10 4a 00 01 10 10 44	00 01 02 10 47 00 10 28	JDGC
0070	00 20 00 20 00 10 00 a8	80 bc 14 01 af b1 98 10	(.....
0080	5c 00 01 01 05 04 00 03	00 50 2a 01 00 2d 1a 8c	<	Pe
0090	01 16 ff ff 00 00 00 00	00 00 00 00 00 00 00 00
00a0	00 00 00 00 00 00 00 00	00 36 16 0c 00 04 00 00
00b0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00c0	00 7f 01 01 dd 1a 00 50	f2 01 01 00 00 50 f2 02PPPP
00d0	02 00 00 50 f2 02 02 50	f2 04 01 00 00 50 f2 02PPPP
00e0	30 18 01 00 00 0f ac 02	02 00 00 0f ac 02 00 0f	0
00f0	ac 04 01 00 00 0f c2 00	00 00 dd 18 00 50 f2 02P
0100	01 01 00 00 03 a4 00 00	27 a4 00 00 c2 43 5e 00	BC
0110	62 32 2f 00 0b 03 00 0a	0a 12 7a dd 07 00 0c 43	b2/	zC

Figure 6: Trama 347 - SSID Fly

347	14.233824	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2361, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
348	14.235456	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2362, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
349	14.336138	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2363, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
350	14.337754	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2364, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
351	14.438683	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2365, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
352	14.440234	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2366, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
353	14.540874	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2367, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
<div> <div>Fixed parameters (12 bytes)</div> <div>Timestamp: 1149684841284</div> <div>Beacon Interval: 0.102400 [Seconds]</div> <div>Capabilities Information: 0x0c21</div> <div>Tagged parameters (140 bytes)</div> <div>Tag: SSID parameter set: NOS_WIFI_Fon</div> <div>Tag Number: SSID parameter set (0)</div> <div>Tag length: 12</div> <div>SSID: NOS_WIFI_Fon</div> <div>Tag: Supported Rates 1(0), 2(0), 5.5(0), 11(0), 9, 18, 36, 54, [Mbit/sec]</div> <div>Tag Number: Supported Rates (1)</div> <div>Tag length: 8</div> <div>Supported Rates: 1(0) (0x82)</div> <div>Supported Rates: 2(0) (0x84)</div> <div>Supported Rates: 5.5(0) (0x8b)</div> <div>Supported Rates: 11(0) (0x96)</div> <div>Supported Rates: 9 (0x12)</div> <div>Supported Rates: 18 (0x24)</div> <div>Supported Rates: 36 (0x48)</div> <div>Supported Rates: 54 (0x6c)</div> <div>Tag: DS Parameter set: Current Channel: 12</div> <div>Tag Number: DS Parameter set (3)</div> <div>Tag length: 1</div> <div>Current Channel: 12</div> <div>Tag: Extended Supported Rates 6(0), 12(0), 24(0), 48, [Mbit/sec]</div> <div>Tag Number: Extended Supported Rates (50)</div> <div>Tag length: 4</div> <div>Extended Supported Rates: 6(0) (0x8c)</div> <div>Extended Supported Rates: 12(0) (0x98)</div> <div>Extended Supported Rates: 24(0) (0xb0)</div> </div>						
0000	00 00 19 00 6f 00 00 00	ec 58 07 02 00 00 00 00	X
0010	10 02 a3 09 00 04 c3 a9	00 00 00 00 00 ff ff ff
0020	ff ff ff bc 14 01 01 01	99 bc 14 01 af b1 99 a0
0030	03 44 7b 0e a0 01 00 00	00 64 00 21 8c 00 0c 4e	p{	dN
0040	4f 53 5f 57 49 46 49 5f	46 6f 6e 01 08 82 84 8b	OS_WIFI_Fon
0050	00 02 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0060	00 03 00 4a 01 2a 01 00	2d 1a 9c 01 16 ff ff 00	J
0070	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0080	00 00 00 00 16 0c 00 04	00 00 00 00 00 00 00 00
0090	00 00 00 00 00 00 00 00	00 00 00 00 7f 01 01 dd
00a0	18 00 50 f2 02 01 00 00	00 03 a4 00 00 27 a4 00P
00b0	00 47 43 5e 00 02 32 2f	00 0b 05 03 00 0a 12 7a	BCb2/z
00c0	dd 07 00 0c 43 00 00 00	00 2e 59 59 f3CYYz

Figure 7: Trama 348 - SSID NOS_WIFI_Fon

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.

Como é demonstrado na figura a baixo, o intervalo estimado entre 2 tramas beacon consecutivas é de 0.102400

```

▶ Frame 1047: 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: 0x00000010bb0232b3f
    Beacon Interval: 0,102400 [Seconds]
  ▶ Capabilities Information: 0x0c21
  ▶ Tagged parameters (140 bytes)

```

Figure 8: Intervalo estimado entre tramas beacon

Na prática este valor não é exato, usando as tramas 1047, 1049 e 1051 obtem-se as diferenças de tempo de 0.102406s e 0.102398s, e usando as tramas 1048, 1050 e 1052 obtem-se as diferenças de tempo 0.102397s e 0.102407s. Estes valores são bastante próximos do número expectável, por norma quando existe uma maior quantidade de tráfego o valor da diferença será mais alto, pois o router necessita aumentar a performance.

Trama	Timestamps (s)	Diferença (s)
1047	0,1149711362879	0,102406
1049	0,1149711465285	
1051	0,1149711567683	0,102398

Table 1: Intervalos de tempo entre tramas beacon da rede Nos_wifi_fon

Trama	Timestamps (s)	Diferença (s)
1048	0,1149711462908	0,102397
1050	0,1149711565305	
1052	0,1149711667712	0,102407

Table 2: Intrevalos de tempo entre tramas beacon da rede Flyingnet

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

Os SSIDs dos APs que estão a operar na vizinhança são:

- NOS_WIFI_Fon
- FlyingNet
- 2WIRE-PT-431

A maneira que nós usamos para obter esta informação foi escolher uma trama beacon aleatória, aceder ao parametro SSID e usar o comando "Apply as Column". Após aplicar esse comando organizamos por SSID e vimos quais eram os SSIDs únicos.

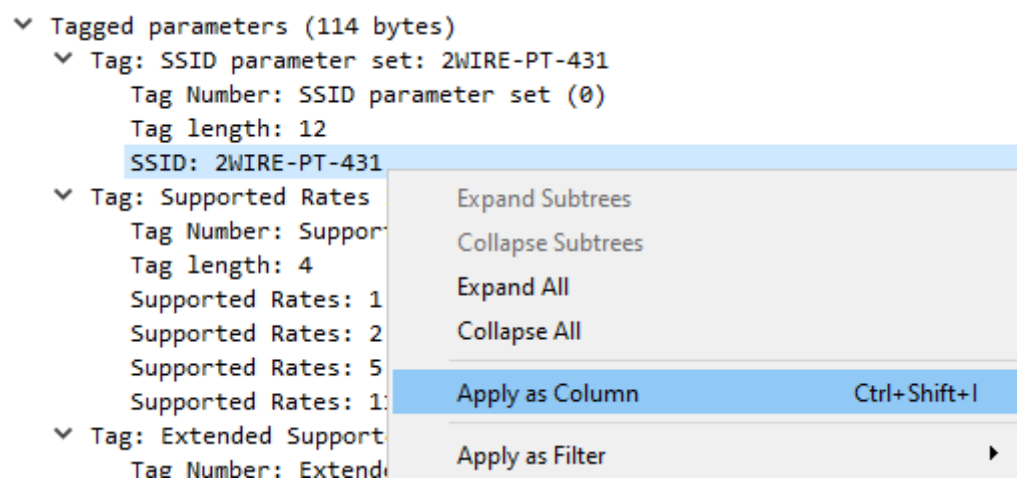


Figure 9: Como usar o comando "Apply as Column"

9. Verifique se está a ser usado o método de deteção de erros (CRC). Justifique. Use o filtro: (wlan.fc.type_subtype == 0x08) && (wlan.fcs.status == bad) Que conclui? Justifique o porquê de usar deteção de erros em redes sem fios. No trace disponibilizado foi também registado scanning ativo (envolvendo tramas probe request e probe response), comum nas redes Wi-Fi como alternativa ao scanning passivo.

Através da figura 11, concluímos que o CRC está ativo porque no campo FCS podemos encontrar uma mensagem de erro.

wlan.fc.type_subtype == 0x08 && wlan.fcs.status == bad						
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	100.184381	bd:09:48:c5:79:35	43:46:15:10:df:53	802.11	146	Beacon frame, SN=3658, FN=10, Flags=.pmPRM.T.
7131	100.398018	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	100.404266	84:84:4c:a8:fd:ea	d2:f4:d1:ff:e5:79	802.11	146	Beacon frame, SN=2338, FN=10, Flags=.pm....T.

Figure 10: Filtro aplicado

>	Frame 7131: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits)
>	Radiotap Header v0, Length 40
>	802.11 radio information
▼	IEEE 802.11 Beacon frame, Flags: .pmPRM.T.
	Type/Subtype: Beacon frame (0x0008)
>	Frame Control Field: 0x827d
	Duration/ID: 7292 (reserved)
	Receiver address: 34:c4:ca:25:ed:14 (34:c4:ca:25:ed:14)
	Destination address: 34:c4:ca:25:ed:14 (34:c4:ca:25:ed:14)
	Transmitter address: 62:4c:de:c5:a9:3a (62:4c:de:c5:a9:3a)
	Source address: 62:4c:de:c5:a9:3a (62:4c:de:c5:a9:3a)
	BSS Id: 55:0e:b7:95:b0:54 (55:0e:b7:95:b0:54)
	STA address: 62:4c:de:c5:a9:3a (62:4c:de:c5:a9:3a)
 0000 = Fragment number: 0
	1010 1111 1011 = Sequence number: 2811
▼	Frame check sequence: 0x20c4ca4e incorrect, should be 0x7d318e93
	> [Expert Info (Error/Malformed): Bad checksum [should be 0x7d318e93]]
	[FCS Status: Bad]
>	TKIP/CCMP parameters
>	Data (70 bytes)

Figure 11: Trama 7131

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

O filtro que utilizamos para visualizar as tramas probing request ou probing response foi o que está presente na figura 12. Utilizamos este filtro porque o subtype do Probe Request é 0x0004 e o subtype do Probe Response é 0x0005.

wlan.fc.type_subtype == 4 wlan.fc.type_subtype == 5					
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:b1:98	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:b1:98	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:b1:98	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
2608	72.180590	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411 Probe Response, SN=2347, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2610	72.181275	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411 Probe Response, SN=2348, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2616	72.201570	Apple_10:6a:f5	Broadcast	802.11	164 Probe Request, SN=2565, FN=0, Flags=.....C, SSID=FlyingNet
2617	72.202150	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411 Probe Response, SN=2350, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2619	72.202807	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411 Probe Response, SN=2351, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2621	72.203485	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411 Probe Response, SN=2352, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Figure 12: Filtro utilizado para visualizar as tramas probing request ou probing response

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?

Um probing request é um pedido do STA por informações de algum AP na área. Depois de enviado o pedido o AP devolve o probing response para informar o STA que está disponível e a informação para as duas estações conseguirem comunicar.

Neste caso da figura existe um probing request na trama 2616 e a respetiva probing response na trama 2621. A trama correspondente ao probing request é emitida pela STA Apple 10:6a:f5 que emite um pedido de procura AP sendo emitido para todos os equipamentos da rede, a resposta ao pedido chega-lhe como probing response do AP HitronTe af:b1:98. De seguida tendo escolhido o AP a associar-se, este envia-lhe uma association request frame (ao AP) , que lhe responde com uma association response frame.

2616	72.201570	Apple_10:6a:f5	Broadcast	802.11	164 Probe Request, SN=2565, FN=0, Flags=.....C, SSID=FlyingNet
2617	72.202150	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411 Probe Response, SN=2350, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2619	72.202807	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411 Probe Response, SN=2351, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2621	72.203485	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411 Probe Response, SN=2352, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Figure 13: Probe Request e respetiva Probe Response

3 Processo de Associação

Numa rede WiFi estruturada, um host deve associar-se a um ponto de acesso antes de enviar dados. O processo de associação nas redes IEEE 802.11 é executada enviando a trama association request do host para o AP e a trama association response enviada pelo AP para o host, em resposta ao pedido de associação recebido. Este processo é antecedido por uma fase de autenticação. Para a sequência de tramas capturada:

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.

Na figura 14 podemos ver uma sequência de tramas que corresponde a um processo de associação completo entre a STA e o AP.

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

Figure 14: Sequencia de tramas no processo de associação

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

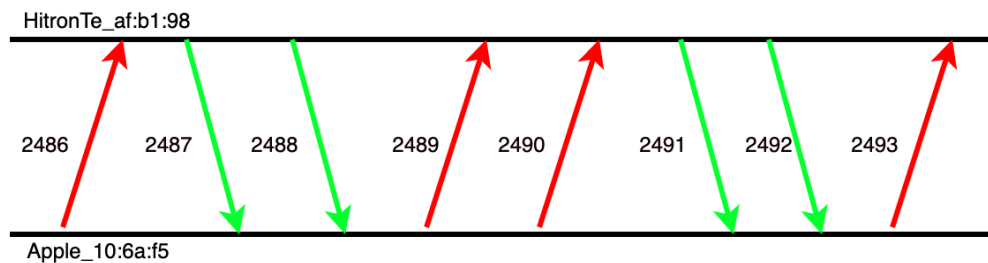


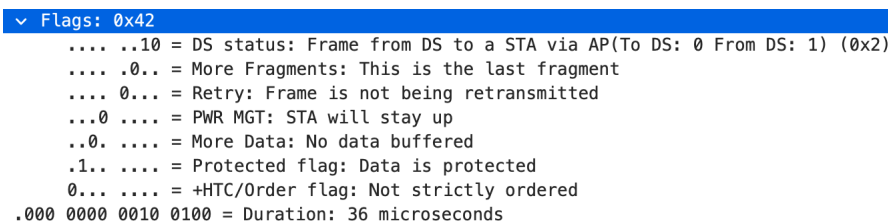
Figure 15: Diagrama da sequência de tramas trocadas

4 Transferência de Dados

O trace disponibilizado, para além de tramas de gestão da ligação de dados, inclui tramas de dados e de controlo da transferência desses mesmos 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?

Como podemos ver na figura a baixo a flag To DS tem o valor 0 e a From DS tem o valor 1, o que nos leva a concluir que a trama recebida veio do sistema de distribuição e assim sendo não é local à WLAN.

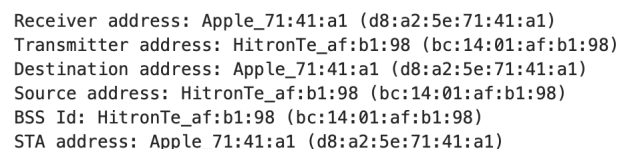


```
▼ Flags: 0x42
.... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
.... .0.. = More Fragments: This is the last fragment
.... 0... = Retry: Frame is not being retransmitted
...0 .... = PWR MGT: STA will stay up
..0. .... = More Data: No data buffered
.1.. .... = Protected flag: Data is protected
0... .... = +HTC/Order flag: Not strictly ordered
.000 0000 0010 0100 = Duration: 36 microseconds
```

Figure 16: Valores das Flags da trama 455

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?

Na figura podemos ver que o endereço Mac correspondente ao wireless host é Apple 71:41:a1, ao AP HitronTe af:b1:98 e ao router de acesso ao sistema de distribuição é HitronTe af:b1:98.



```
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)
```

Figure 17: Endereços MAC da trama 455

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

Observando as figuras podemos concluir que a trama está a ser transmitida para fora da rede local uma vez que os valores das flags To DS está a 1 e o From DS a 0. Podemos também concluir quanto ao endereço MAC o AP corresponde ao receiver address, a STA corresponde ao transmitter address e o router corresponde ao destination address.

```

  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

```

Figure 18: Valores das Flags da trama 457

```

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)

```

Figure 19: Endereços MAC da trama 457

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.)

Como podemos ver na figura a baixo, no intervalo entre as duas tramas QoS transmitidas temos a existência de uma terceira trama Acknowledgment, isto, deve-se ao facto de nas redes wireless ao contrário das redes Eterneth a ocorrência de erros ser algo muito mais comum, sendo assim necessário o uso de tramas Acknowledgment para detetar a existência ou não de erros na transferência de dados na trama anterior, permitindo assim ao dispositivo através da resposta desta trama determinar se deve ou não reenviar o pacote.

455	18.536644	HitronTe_af:b1:98	Apple_71:41:a1	802.11	226	QoS Data, SN=276, FN=0, Flags=.p....F.C
456	18.536653		HitronTe_af:b1:98 ...	802.11	39	Acknowledgement, Flags=.....C
457	18.539762	Apple_71:41:a1	HitronTe_af:b1:98	802.11	178	QoS Data, SN=1209, FN=0, Flags=.p....TC

Figure 20: Pacotes de QoS

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.

Através da figura 22, como as flags To DS e From DS estão ambas a 0, concluímos que as redes estão a operar localmente. Assim, como podemos ver na figura 21, o STA envia um Request-to-send para o AP da WLAN e, em seguida, o AP da WLAN envia um Clear-to-send para o STA.

```
162 6.653376      Apple_10:6a:f5 (64... HitronTe_af:b1:98 ... 802.11      45 Request-to-send, Flags=.....C
163 6.653389      Apple_10:6a:f5 (64... Apple_10:6a:f5 (64... 802.11      39 Clear-to-send, Flags=.....C
```

Figure 21: Tramas Request-to-send e Clear-to-send

```

▼ 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... .... = +HTC/Order flag: Not strictly ordered
.000 0000 1001 1110 = Duration: 158 microseconds
```

Figure 22: Valores das Flags da trama 162

5 Conclusão

No desenvolvimento deste terceiro trabalho prático foi possível aprofundar o conhecimento sobre as redes sem fio (wireless) e, além disso, ver com mais detalhe o protocolo IEEE 802.11.

Para a realização deste trabalho utilizamos o Wireshark com uma captura fornecida pelos docentes na plataforma E-learning.

Para além disso, percebemos que podem existir tipos de tramas, como por exemplo as tramas de controlo, que são fundamentais para a deteção de erros nas redes wireless (muito propícias à ocorrência de colisões em alternativa as redes com fio).

Por último, foi-nos possível analisar alguns dos processos de conexões entre STA e AP, assim como o comportamento destes no envio de probing requests e probing solves, Beacons, e ainda, Request-To-Send e Clear-To-Send.

Concluindo, conseguimos consolidar conceitos e protocolos, e ainda perceber determinados comportamentos dos dados transmitidos por redes wireless.