

## **TP4: Redes Sem Fios (802.11)**

Sérgio Jorge, João Freitas, and Alexandre Martins

University of Minho, Department of Informatics, 4710-057 Braga, Portugal  
e-mail: {a77730,a74814,a77523}@alunos.uminho.pt

### **1 Introdução**

O principal objetivo deste trabalho é o aprofundamento de conhecimentos das redes sem fios explorando vários aspetos do protocolo IEEE 802.11, incluindo os seus tipos e sub-tipos de tramas, através do estudo de uma captura fornecida pela equipa docente, recorrendo à ferramenta *Wireshark*.

## 2 Acesso Rádio

```
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): -62dBm
  Noise level (dBm): -87dBm
  TSF timestamp: 34957541
> [Duration: 1632µs]
```

Figura 1: Informação geral da trama escolhida: 365

### Questão 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 está a operar nos 2467 MHz, ou seja, no espectro dos 2 GHz. O canal que está a ser usado é o 12.

```
Channel frequency: 2467 [BG 12]
> Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM
```

Figura 2: Frequência e canal da operação

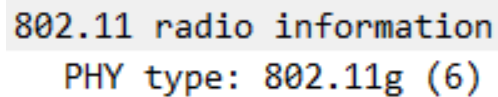
```
Channel: 12
Frequency: 2467MHz
```

Figura 3: Frequência e canal da operação

## Questão 2

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

A versão que está a ser utilizada é a IEEE 802.11g.



802.11 radio information  
PHY type: 802.11g (6)

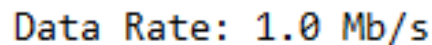
Figura 4: Versão da norma utilizada

## Questão 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."*

Uma vez que está a ser usada a versão IEEE 802.11g, esperam-se débitos até 54 Mbps. No entanto, a trama escolhida, de acordo com a figura 4, foi transmitida a 1.0 Mb/s.

São vários os fatores que impossibilitam uma trama de ser transmitida no débito máximo, como as interferências com máquinas a operar na mesma frequência, obstáculos, redes vizinhas... mas, o principal, acaba por ser, invariavelmente, a distância do host ao AP. Tal facto leva a que o sinal seja menor, implicando um BER mais alto e, por isso, a transmissão é feita de forma mais lenta porque dessa forma é possível reduzir o BER. Nas redes Wi-Fi, a força do sinal é, de facto, diretamente proporcional à taxa de transferência de dados.



Data Rate: 1.0 Mb/s

Figura 5: Débito da trama

### 3 Scanning Passivo e Scanning Ativo

#### Questão 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)?"*

Escolheu-se a trama 365. Esta trama é do tipo *Management Frame* (id 0) com subtipo *Beacon Frame* (id 8). Os seus identificadores estão especificados no cabeçalho IEEE 802.11 Beacon Frame.

```
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
```

Figura 6: Identificadores do tipo e subtipo da trama escolhida

## Questão 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 apropriado (tomando como base a resposta da alínea anterior) que lhe permita obter a listagem pretendida."

Para listar todos os SSIDs presentes na vizinhança, aplicou-se o filtro `wlan.fc.type_subtype == 0x0008`. Este filtro possibilita que apareçam só os *Beacon Frames*. Pela análise de todos, verificou-se pelos seus SSIDs que estão duas redes a operar na vizinhança: NOSFON e FlyingNet.

wlan.fc.type_subtype == 0x0008						
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
348	14.235456	HitronTe_af:b1:99	Broadcast	802.11	205	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	296	Beacon frame, SN=2364, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
351	14.438603	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	205	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
354	14.542494	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2368, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
355	14.643405	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2369, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
356	14.645055	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2370, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
357	14.745813	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2371, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
358	14.848210	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2373, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
359	14.849841	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2374, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
360	14.950611	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2375, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
361	14.952099	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2376, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
362	15.052889	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2377, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
363	15.054500	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2378, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
364	15.155412	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2379, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
365	15.156998	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2380, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
366	15.257723	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2381, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
367	15.259284	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2382, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
368	15.360157	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2383, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
369	15.361704	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2384, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

Figura 7: Beacon Frames das redes vizinhas

## Questão 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."

Através da figura 9, podemos verificar que o método de detecção de erros (CRC) está a ser utilizado. Podemos também confirmar, na Figura 8, que nem todas as tramas *Beacon* foram recebidas corretamente, pois todas as assinaladas a azul têm *FCS Status: Bad*.

Nas redes Wi-Fi é quase sempre utilizado o CRC de modo a detetar os erros, pois a maneira de corrigir estes é retransmitir a trama onde o erro ocorreu. Contrariamente a uma rede Ethernet, as redes Wi-Fi tem uma maior probabilidade de ocorrência de erros devido a vários fatores, sendo alguns deles, o meio onde é transmitida a informação, a distância entre o AP e o host, interferências de outras máquinas a operar na mesma frequência, etc.

wlan.fc.type_subtype == 0x0008 && wlan.fcs.status == "Bad"						
No.	Time	Source	Destination	Protocol	Length	Info
6274	94.779898	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.

Figura 8: Uso de um filtro para detetar Bad Packets

```
Frame check sequence: 0xd2d48a3d [correct]
[FCS Status: Good]
```

Figura 9: Campo de FCS de uma trama

### Questão 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."*

O intervalo de tempo previsto é de 0.102400 segundos, como se pode ver na figura 10. Esta periodicidade de tramas *Beacon* não se verifica ao longo do tempo porque assim como todas as outras, têm de obedecer ao algoritmo CSMA/CA. Se existirem tramas a ser transmitidas quando uma nova *Beacon* tem de ser transmitida, então esta espera. Isto leva a uma diferença entre o tempo previsto e o real.

```
Beacon Interval: 0.102400 [Seconds]
```

Figura 10: Intervalo de tempo entre beacons

### Questão 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"*

Observa-se o campo BSS Id para identificar os endereços MAC das tramas *Beacons* dos pontos de acesso, embora que, como são *Management Frames*, os campos *Transmitter address*, *Source address* e BSS coincidem.

- FlyingNet -> BSS Id = HitronTe\_af:b1:98 (bc:14:01:af:b1:98)
- NOS FON -> BSS Id = HitronTe\_af:b1:99 (bc:14:01:af:b1:99)

```
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)
```

Figura 11: Endereços de beacons enviados pela rede FlyingNet

```
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)
```

---

Figura 12: Endereços de beacons enviados pela rede NOSFON

### Questão 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?"*

Os débitos base suportados do AP são:

- 1 Mbit/sec
- 2 Mbit/sec
- 5.5 Mbit/sec
- 11 Mbit/sec

Os débitos não base suportados do AP são:

- 9 Mbit/sec
- 18 Mbit/sec
- 36 Mbit/sec
- 54 Mbit/sec

Os *extended supported rates* base são:

- 6 Mbit/sec
- 12 Mbit/sec
- 24 Mbit/sec

O *extended supported rate* não base é:

- 48 Mbit/sec

- > 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]

Figura 13: Débitos do AP

## Questão 10

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

Filtro utilizado: `wlan.fc.type_subtype == 5 || wlan.fc.type_subtype == 4`.

wlan.fc.type_subtype == 5    wlan.fc.type_subtype == 4						
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	281	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	281	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	281	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

Figura 14: Filtro para tramas probing request e probing response

## Questão 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?"*

Na trama 2468 identificou-se um probing request que foi direcionado a todos os APs ao alcance do host (ea:a4:64:7b:b9:7a), neste caso FlyingNet e NOSFON. Os probing request são tramas que são usadas quando os hosts querem saber os APs que estão no seu alcance ou quando necessitam de informações de outros hosts.

Imediatamente a seguir, verifica-se uma trama probing response, resposta à trama anterior, enviada pelo AP da FlyingNet.

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

Figura 15: Probing request e Probing response



```

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]

```

Figura 16: Probing 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]

```

Figura 17: Probing response

## 4 Processo de Associação

### Questão 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."*

O processo tem início na trama 2486 e termina na trama 2493.

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 (-	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:b1:9-	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 (-	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:b1:9-	802.11	39 Acknowledgement, Flags=.....C
2494 70.451472	HitronTe_af:b1:98	Broadcast	802.11	296 Beacon frame, SN=3459, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2495 70.453086	HitronTe_af:b1:99	Broadcast	802.11	205 Beacon frame, SN=3460, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2496 70.453444	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	53 Null function (No data), SN=2544, FN=0, Flags=.....TC
2497 70.453460		Apple_10:6a:f5 (-	802.11	39 Acknowledgement, Flags=.....C

Figura 18: Processo de associação entre STA e AP

### Questão 13

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

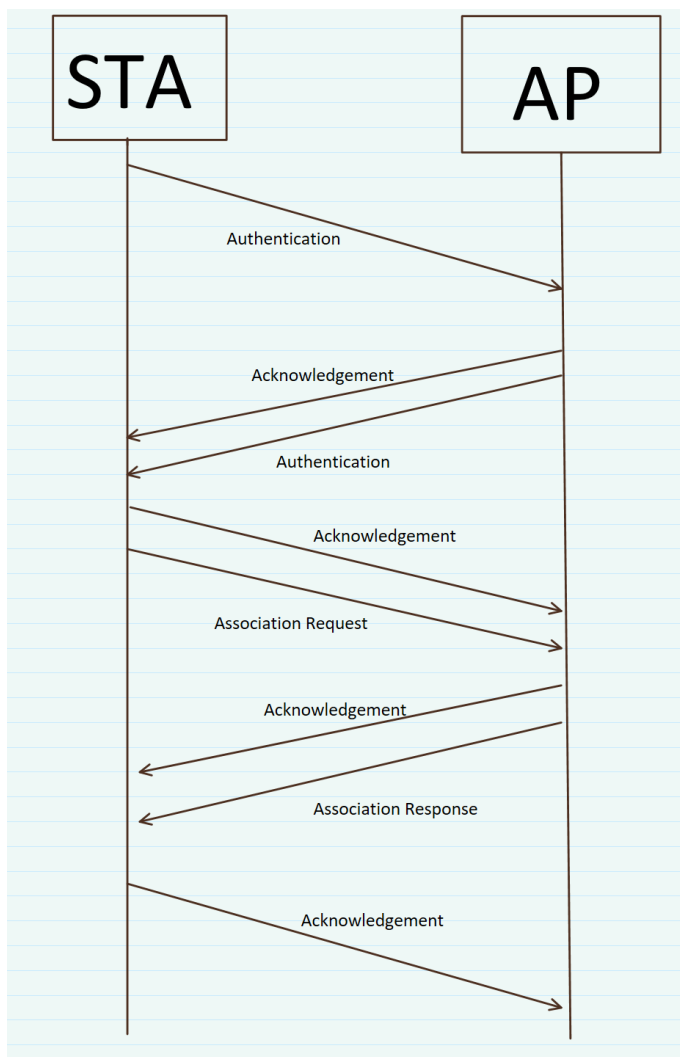


Figura 19: Diagrama de sequência das tramas.

## 5 Transferência de Dados

### Questão 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?"

O professor, na aula prática, sugeriu que a trama nº455 fosse substituída pela trama nº818.

A trama tem direção do *Distribution System* para a STA, pois tem o campo *From DS* a 1, o que significa que vem do *Distribution System*. O AP envia, então, a trama para o dispositivo com o MAC Apple\_10:6a:f5. É, por isso, uma comunicação do sistema distribuído para a WLAN local.

```
▼ 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
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:b1:96 (bc:14:01:af:b1:96)
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 20: Direção da trama nº818

### Questão 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 trama nº455, não se verificou a presença de três endereços diferentes. Deste modo, o professor sugeriu a análise da trama 818.

Na atual situação e tendo em conta as *flags*, verifica-se que o STA address é o endereço do host e o BSS Id é o endereço do AP. Por isso:

- Endereço STA: Apple\_71:41:a1 (d8:a2:5e:71:41:a1)
- Endereço AP: HitronTe\_af:b1:98 (bc:14:01:af:b1:98)
- Endereço Router: HitronTe\_af:b1:96 (bc:14:01:af:b1:96)

```

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:b1:96 (bc:14:01:af:b1:96)
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 21: Endereços da trama nº818

### Questão 16

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

O professor, na aula prática, sugeriu que a trama nº457 fosse substituída pela trama nº1434.

A partir das *flags* To DS e From DS, é possível verificar a direccionalidade da trama. Neste caso, conclui-se que a direccionalidade é para o sistema distribuído. Aliás, essa é também uma informação que se pode obter a partir dos endereços especificados na figura 22, onde se constata que o endereço origem é a STA e o endereço destino corresponde ao router.

```

▼ Frame Control Field: 0x8841
    .... 00 = Version: 0
    .... 10.. = Type: Data frame (2)
    1000 .... = Subtype: 8
    ▼ Flags: 0x41
        .... 001 = 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 0000 0011 0000 = Duration: 48 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:b1:96 (bc:14:01:af:b1:96)
    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 22: Frame control da trama nº1434

### Questão 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.)"*

Estão a ser utilizadas tramas de controlo com o subtipo 1101 que corresponde a tramas *ACK*. Estas tramas são enviadas pelo recetor, logo após a receber a trama, para confirmar a transmissão. Caso esta trama não seja recebida por parte de quem enviou a informação, então a informação volta a ser transmitida. As tramas *ACK* permitem ajudar no *CSMA/CA* Carrier-sense multiple access with collision avoidance, pois é necessário um *ACK* para poder voltar a retransmitir informação na rede.

```
Frame Control Field: 0x8841
.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
```

Figura 23: Frame Control Field de uma Data Frame

```
Type/Subtype: Acknowledgement (0x001d)
Frame Control Field: 0xd400
.... ..00 = Version: 0
.... 01.. = Type: Control frame (1)
1101 .... = Subtype: 13
```

Figura 24: Frame Control Field de uma Control Frame

## Questão 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."

O uso deste tipo de tramas é opcional e verifica-se, principalmente, em situações em que é necessário enviar dados com um tamanho razoável. Por isso, verifica-se na figura 25 que, o STA Apple\_10:6a:f5 envia um *Request to Send* e obtém resposta *Clear to Send*. De seguida, há de facto transferência de um volume de dados considerável.

525	21.532275	HitronTe_af:b1:9...	Apple_10:6a:f5 (...)	802.11	49	802.11 Block Ack Req, Flags=.....C
526	21.532345	Apple_10:6a:f5 (...)	HitronTe_af:b1:9...	802.11	57	802.11 Block Ack, Flags=.....C
527	21.532554	HitronTe_af:b1:9...	Apple_10:6a:f5 (...)	802.11	49	802.11 Block Ack Req, Flags=.....C
528	21.532564	Apple_10:6a:f5 (...)	HitronTe_af:b1:9...	802.11	57	802.11 Block Ack, Flags=.....C
529	21.547047	Apple_10:6a:f5 (...)	HitronTe_af:b1:9...	802.11	45	Request-to-send, Flags=.....C
530	21.547057		Apple_10:6a:f5 (...)	802.11	39	Clear-to-send, Flags=.....C
531	21.547114	Apple_10:6a:f5	HitronTe_af:b1:96	802.11	177	QoS Data, SN=3020, FN=0, Flags=.p.....T.
532	21.547116	HitronTe_af:b1:9...	Apple_10:6a:f5 (...)	802.11	57	802.11 Block Ack, Flags=.....C
533	21.548964	Apple_10:6a:f5 (...)	HitronTe_af:b1:9...	802.11	45	Request-to-send, Flags=.....C
534	21.548970		Apple_10:6a:f5 (...)	802.11	39	Clear-to-send, Flags=.....C
535	21.549039	54:dd:94:fb:fb:00	07:90:8b:06:29:49	LLC	177	I, N(R)=42, N(S)=0; DSAP NULL LSAP Group, SS
536	21.549043	HitronTe_af:b1:9...	Apple_10:6a:f5 (...)	802.11	57	802.11 Block Ack, Flags=.....C
537	21.549136	d6:9b:be:10:6a:f5	HitronTe_af:b1:96	802.11	146	QoS Data, SN=1997, FN=0, Flags=.p.....T.

Figura 25: RTS e CTS entre STA e AP

## 6 Conclusão

Neste trabalho aprofundou-se o conhecimento do funcionamento interno das redes sem fios 802.11. Em particular, estudou-se as comunicações entre estações, endereçamento, tipos e sub-tipos de tramas e seu conteúdo.

Consolidou-se o funcionamento e o conceito de deteção de erros e controlo de envio de volumes de dados (RTS e CTS), assim como o de *beacons* e a sua funcionalidade em redes deste tipo. A exploração de *probing* também se tornou relevante para entender comunicação por meio de ar.

Concluiu-se, na realidade, que as redes sem fios são altamente dinâmicas e concorrentes e têm uma complexidade muito mais elevada do que as redes Ethernet.