

# Redes Sem Fios (802.11)

André Gonçalves (A80368), Diogo Gonçalves (A81860), Maria Pires(A86268)

September 9, 2019

## Questões e Respostas

### 1 Acesso Rádio

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

A frequência do espectro é 246MHz que corresponde ao canal número 12.

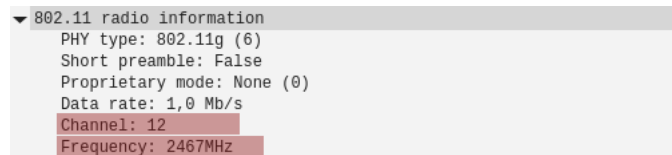


Figure 1: Canal e frequência em que a rede está a operar

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

A versão da norma usada é 802.11g.



Figure 2: norma IEEE 802.11

### 1.3 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.

O débito da trama escolhida é 1 Mb/s que corresponde a 8 Mbps, contudo o débito máximo desta interface é 54 Mbps uma vez que a norma usada é a 802.11g

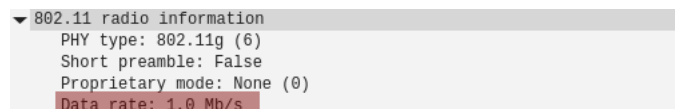


Figure 3: Legenda

## 2 Scanning Passivo e Scanning Ativo

### 2.1 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)?

A trama 325 é uma trama de gestão cujo identificador é 0 e o seu subtipo correspondente é *beacon* identificado por 1000 (8 em decimal). O tipo e subtipo da trama são sub-campos do campo de controlo do cabeçalho da trama.

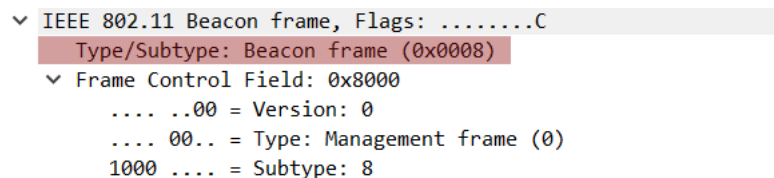


Figure 4: Tipo e subtipo da trama

**2.2** 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.

Através da resposta da linha anterior e do uso das tabelas de anexo concluímos que o filtro que nos permite visualizar os SSIDs dos APs da vizinhança é: wlan.fc.type\_subtype==8.

wlan.fc.type_subtype==8						
Time	Source	Destination	Protocol	Length	Info	
1 0.000000	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2083, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
2 0.001662	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2084, FN=0, Flags=.....C, BI=100, SSID=NOS_MIFI_Fon	
3 0.102552	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2085, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
4 0.104164	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2086, FN=0, Flags=.....C, BI=100, SSID=NOS_MIFI_Fon	
5 0.204951	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2087, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
6 0.206582	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2088, FN=0, Flags=.....C, BI=100, SSID=NOS_MIFI_Fon	
7 0.307368	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2089, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
8 0.308999	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2090, FN=0, Flags=.....C, BI=100, SSID=NOS_MIFI_Fon	
9 0.409749	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2091, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
10 0.411376	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2092, FN=0, Flags=.....C, BI=100, SSID=NOS_MIFI_Fon	
11 0.512117	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2093, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
12 0.513707	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2094, FN=0, Flags=.....C, BI=100, SSID=NOS_MIFI_Fon	
13 0.614562	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2095, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
14 0.616191	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2096, FN=0, Flags=.....C, BI=100, SSID=NOS_MIFI_Fon	
28 0.716961	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2097, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
29 0.718611	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2098, FN=0, Flags=.....C, BI=100, SSID=NOS_MIFI_Fon	
32 0.819368	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2099, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
33 0.821009	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2100, FN=0, Flags=.....C, BI=100, SSID=NOS_MIFI_Fon	
34 0.921756	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2101, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
35 0.923387	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2102, FN=0, Flags=.....C, BI=100, SSID=NOS_MIFI_Fon	
36 1.024021	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2103, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
37 1.025663	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2104, FN=0, Flags=.....C, BI=100, SSID=NOS_MIFI_Fon	
38 1.126564	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2105, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
39 1.128193	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2106, FN=0, Flags=.....C, BI=100, SSID=NOS_MIFI_Fon	
40 1.228961	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2107, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
41 1.230650	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2108, FN=0, Flags=.....C, BI=100, SSID=NOS_MIFI_Fon	

Figure 5: SSIDs da vizinhança

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

Está a ser usado um método de correção de erros, como podemos observar através do campo Frame Check Sequence e que as tramas foram recebidas corretamente. Devido à partilha do meio é necessário coordenar as transmissões múltiplas e garantir que não há erros na transmissão e que os senders não interferem uns com os outros.

```

▼ 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 0010 0011 .... = Sequence number: 2339
    Frame check sequence: 0x72d0003e [correct]
    [FCS Status: Good]

```

Figure 6: FCS

2.4 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 entre as tramas de anúncio é de 0,102400 segundos. Estas tramas são transmitidas periodicamente na prática pelo AP de modo a anunciar a sua presença e permitir a sincronização com as interfaces ao seu alcance.

```

▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters (12 bytes)
    Timestamp: 0x0000010bae7d41e9
    Beacon Interval: 0,102400 [Seconds]
    ► Capabilities Information: 0x0c31

```

Figure 7: Intervalo de tempo entre o envio de tramas *beacon*

**2.5 Identifique e registre 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.**

Nas tramas *beacon* podem existir até 4 endereços MAC:

- *receiver address*: O endereço MAC do seguinte recetor da trama caso esse não seja imediatamente o destino final.
- *Destination address*: O endereço MAC do destino final da trama.
- *Transmitter address*: O endereço MAC do sistema que está a enviar diretamente a trama.
- *Source address*: O endereço MAC do transmissor original da trama.

Cujos endereços se encontram assinalados na figura 8:

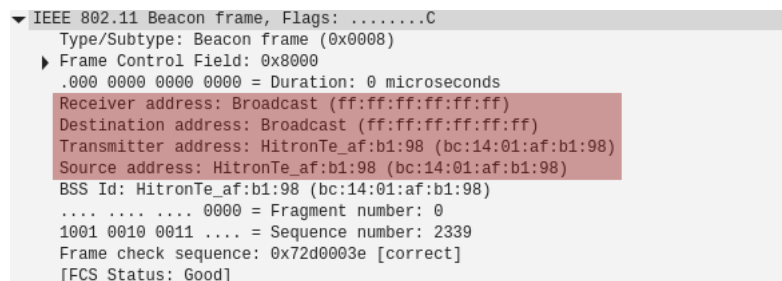


Figure 8: Endereços MAC contidos no cabeçalho de um trama *beacon*

**2.6 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 de base são os assinalados na figura 9.

- ▼ 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 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)
    - > Tag: DS Parameter set: Current Channel: 12
    - ▼ 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)

Figure 9: Débits suportados pelo AP

**2.7** Estabeleça um filtro Wireshark apropriado que lhe permita visualizar todas as tramas probing request ou probing response, simultaneamente. Face ao endereçamento usado, indique a que sistemas são endereçadas estas tramas e explique o proposito das mesmas

O filtro que nos permite visualizar as tramas probing request e probing response é: wlan.fc.type\_.subtype == 4 or wlan.fc.type\_.subtype == 5

wlan.fc.type_subtype==4 or 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:b1:99	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
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 10: Filtro de probing request e probing response

## 2.8 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 o proposito das mesmas

Estas tramas são utilizadas no processo de *scanning ativo*. Um host wireless faz broadcast de uma trama de probind request que é recebida por todos os APs que estão ao seu alcance. Os APs respondem a esse request com uma trama de probing response para que o host possa escolher a que AP se deve associar.

```

✓ 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]

Wireshark · Packet 2469 · trace-wlan-tp4-2018b.pcap

> Frame 2469: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
✓ 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]

```

Figure 11: Filtro de probing request e probing response

### 3 Processo de Associação

**3.1 Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.**

Sequência de tramas entre o STA 4321123441 e o AP 4312134:

```

> Frame 4690: 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
  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
    1110 1000 0101 .... = Sequence number: 3717
    Frame check sequence: 0xbc6947d3 [correct]
    [FCS Status: Good]
> IEEE 802.11 wireless LAN

```

Figure 12: Frame nº1 da sequência - beacon frame



```

> Frame 4692: 59 bytes on wire (472 bits), 59 bytes captured (472 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
▼ IEEE 802.11 Authentication, Flags: .....C
  Type/Subtype: Authentication (0x000b)
  ▼ Frame Control Field: 0xb000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1011 .... = Subtype: 11
  > Flags: 0x00
    .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  Destination address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  Transmitter address: 7c:ea:6d:ff:a2:cc (7c:ea:6d:ff:a2:cc)
  Source address: 7c:ea:6d:ff:a2:cc (7c:ea:6d:ff:a2:cc)
  BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  .... .... 0000 = Fragment number: 0
  0000 0100 0011 .... = Sequence number: 67
  Frame check sequence: 0x5ad69812 [correct]

```

Figure 13: Frame nº2 da sequencia - pedido de autenticação

```

> Frame 4694: 59 bytes on wire (472 bits), 59 bytes captured (472 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
▼ IEEE 802.11 Authentication, Flags: .....C
  Type/Subtype: Authentication (0x000b)
  ▼ Frame Control Field: 0xb000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1011 .... = Subtype: 11
  > Flags: 0x00
    .000 0000 0011 0010 = Duration: 50 microseconds
  Receiver address: 7c:ea:6d:ff:a2:cc (7c:ea:6d:ff:a2:cc)
  Destination address: 7c:ea:6d:ff:a2:cc (7c:ea:6d:ff:a2:cc)
  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 1000 0111 .... = Sequence number: 2439
  Frame check sequence: 0x0d0ac5ec [correct]

```

Figure 14: Frame nº3 da sequencia - resposta de autenticação

```

> Frame 4696: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
▼ IEEE 802.11 Association Request, Flags: .....C
  Type/Subtype: Association Request (0x0000)
  ▼ Frame Control Field: 0x0000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    0000 .... = Subtype: 0
  > Flags: 0x00
    .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  Destination address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  Transmitter address: 7c:ea:6d:ff:a2:cc (7c:ea:6d:ff:a2:cc)
  Source address: 7c:ea:6d:ff:a2:cc (7c:ea:6d:ff:a2:cc)
  BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  .... .... 0000 = Fragment number: 0
  0000 0100 0100 .... = Sequence number: 68
  Frame check sequence: 0x63fc0673 [correct]

```

Figure 15: Frame nº4 da sequencia - pedido de associação

```

> Frame 4698: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
√ IEEE 802.11 Association Response, Flags: .....C
  Type/Subtype: Association Response (0x0001)
  ✓ Frame Control Field: 0x1000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    0001 .... = Subtype: 1
  > Flags: 0x00
    .000 0000 0011 0010 = Duration: 50 microseconds
  Receiver address: 7c:ea:6d:ff:a2:cc (7c:ea:6d:ff:a2:cc)
  Destination address: 7c:ea:6d:ff:a2:cc (7c:ea:6d:ff:a2:cc)
  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 1000 1000 .... = Sequence number: 2440
  Frame check sequence: 0x77f27360 [correct]

```

Figure 16: Frame nº5 da sequência - resposta de associação

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



Figure 17: Diagrama de scanning ativo

## 4 Transferência de Dados

4.1 Considere a trama de dados nº455. 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?

Com o campo Frame Control é possível verificar a direcionalidade da trama com a flag *DS status*, neste caso vem de um SD até um station passando por um AP. Esta trama é local à WLAN porque a trama é enviada através de um AP.

```
▼ 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
```

Figure 18: Flags

4.2 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?

- *STA*: d8:a2:5e:71:41:a1
- *AP*: bc:14:01:af:b1:91
- *Router de acesso ao sistema de distribuição*: bc:14:01:af:b1:91

```
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 19: MAC

### 4.3 Como interpreta a trama nº457 face à sua direcionalidade e endereçamento MAC?

Nesta trama podemos concluir que origina na Station, tem como destino o sistema distribuído e é enviada pelo AP.

- *Fonte:* d8:a2:5e:71:41:a1
- *Destino:* bc:14:01:af:b1:91

```
▼ 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
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 20: Legenda

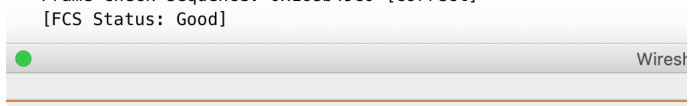
### 4.4 Que subtipo de tramas de controlo são transmitidas ao longo da transferência de dados acima mencionada? Tente explicar porque razão têm de existir (contrariamente ao que acontece numa rede Ethernet.)

São enviadas tramas de Acknowledgment(ACK), que depois de receber uma trama de dados, a estação irá enviar esta trama para indicar se foi encontrado algum erro. No caso de a estação que enviou a mensagem não receber esta trama num determinado período de tempo reenviará a trama de dados. Este tipo de trama tem que existir porque num meio partilhado existe um risco muito grande da perda de pacotes, isto não acontece numa rede Ethernet porque como esta é física existe um risco muito menor de perda de pacotes.

#### 4.5 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 direcionalidade das tramas e os sistemas envolvidos.

Para o exemplo acima, nas tramas 455 e 457, não é utilizado a opção RTS/CTS. Mas, utilizando outro caso de estudo, podemos concluir que o uso da opção RTS e CTS permite diminuir as colisões de tramas introduzidas pelo *hidden node problem*. O objetivo destes tipos de tramas é permitir com que o recetor e o emissor saibam o estado de cada um, isto permite que quando o emissor estiver pronto para enviar envia a trama RTS e espera por um CTS que indica que o recetor esta pronto para receber a informação. Diminuindo assim o número de colisões no recetor.

```
Type/Subtype: Request-to-send (0x001b)
► Frame Control Field: 0xb400
.000 0000 1101 0010 = Duration: 210 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: 0x168b49c0 [correct]
[FCS Status: Good]
```



Wireless

```
Frame 16: 39 bytes on wire (312 bits), 39 bytes captured (312 bits) on interface 0
Radiotap Header v0, Length 25
802.11 radio information
IEEE 802.11 Clear-to-send, Flags: .....C
Type/Subtype: Clear-to-send (0x001c)
► Frame Control Field: 0xc400
.000 0000 1010 0110 = Duration: 166 microseconds
Receiver address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
Frame check sequence: 0x4561453c [correct]
[FCS Status: Good]
```

Figure 21: RTS/CTS

## 5 Conclusões

Na realização deste trabalho sobre redes 802.11 deparamo-nos com o padrão 802.11g e foi-nos possível analisar a frequência e débitos das mesmas. As tramas no nível de redes sem fios são bastante mais complexas que as tramas Ethernet isto porque a comunicação é feita num meio partilhado em vez de um meio cablado. Existem 3 grandes tipos de tramas, com vários subtipos, que foram exploradas neste trabalho. Mais concretamente as tramas *Management*, de *Control* e de *Data*. As tramas do tipo *Management* são usadas pelas estações para se juntarem ou saírem de um BSS(Basic Service Sets). As tramas do tipo *Control* tem como finalidade assistir a transmissão correta das restantes tramas. O objetivo das tramas *Data* é a transmissão e comunicação de informação. Neste trabalho foram analisadas os vários subtipos de tramas com o intuito de perceber como é realizada toda a troca de informação entre os vários intervenientes.

A primeira fase do trabalho consistia em perceber o tipo de frequência e o débito usado nesta rede e a norma em que iríamos trabalhar ao longo do guião.

A segunda parte tem como objetivo perceber como era realizado o Scanning Passivo e o Scanning Ativo, e como os diferentes tipos de tramas são utilizados para esse fim.

A terceira parte consiste em perceber como é realizado o processo de associação de uma determinada station a um determinado AP e utilizar a ferramenta Wireshark de modo a perceber como é feita a troca de tramas de forma a conseguir essa associação.

Na última parte foi analisada a transferência de dados entre vários atores numa rede e os mecanismos utilizados por estes de modo a diminuir a ocorrência de erros.

Concluído o guião podemos fazer uma apreciação positiva do trabalho realizado uma vez que foi consolidada a matéria dada nas teorias com o guião prático tornando assim fácil a aprendizagem dos conteúdos.