

**Universidade do Minho**

”TP4: Redes sem Fios (Wi-Fi)

**Grupo 52**

Licenciatura em Engenharia Informática

**Redes de Computadores**

a85646	a98286	a87978
Hugo Teles Silva	Luís Ferreira	Tiago Cunha

#### 4. Acesso Rádio

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

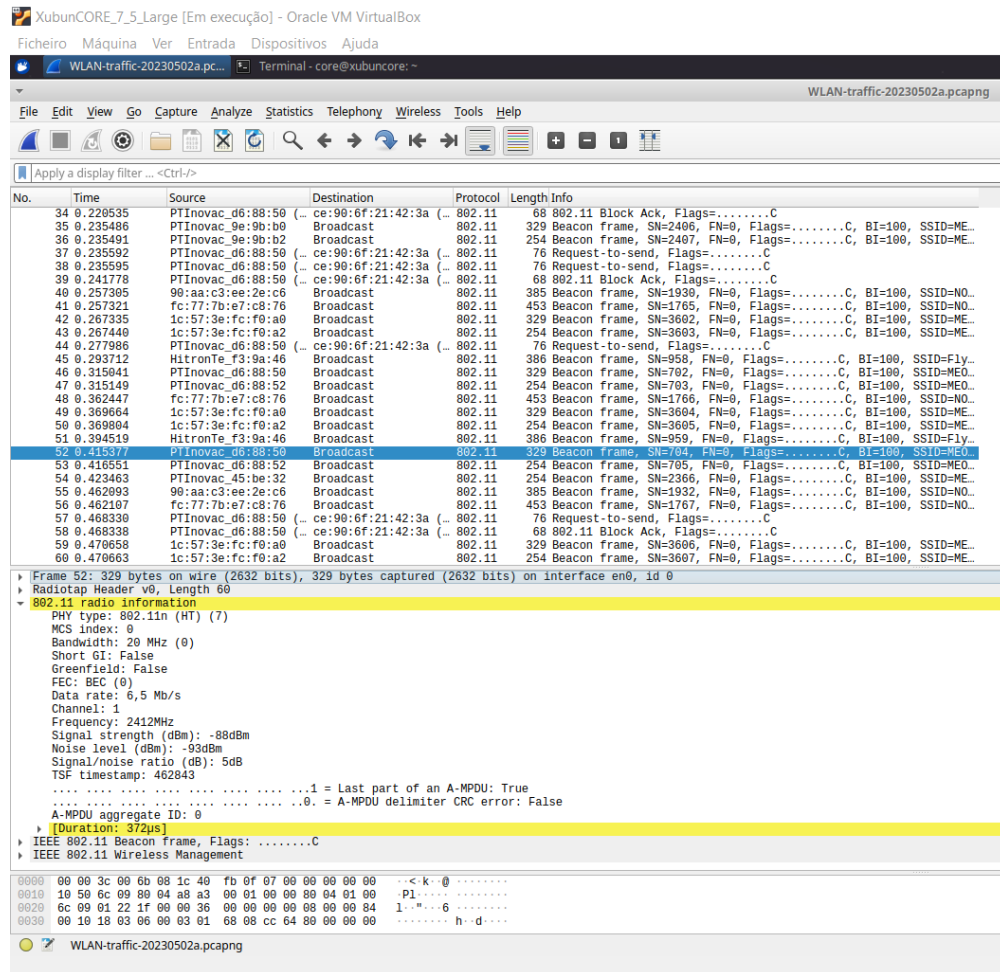


Figure 1: Trama 802.11 n<sup>o</sup>52

A rede sem fios está a ser operada a uma frequência de 2412MHz que corresponde ao canal 1.

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

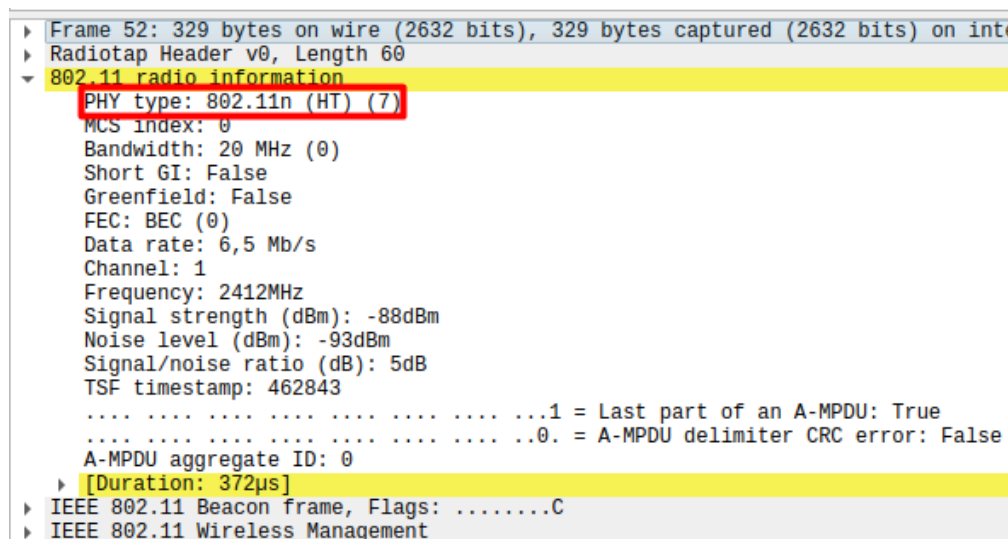


Figure 2: IEE 802.11 - Versão

A versão da norma IEEE 802.11 que está a ser utilizada é a versão 802.11n.

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

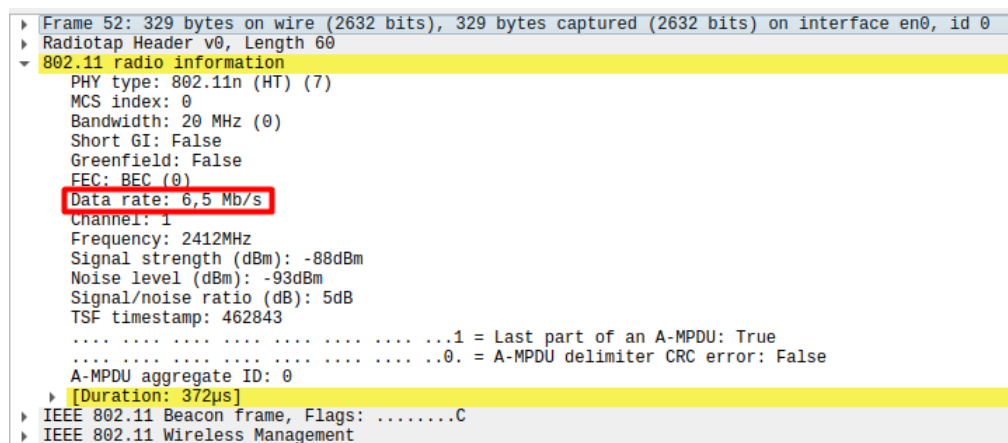


Figure 3: Débito da Trama nº52

O débito da trama escolhida é de 6.5 Mb/s, este débito não corresponde ao débito máximo, uma vez que a versão 802.11n suporta uma capacidade de débito máximo de 600 Mb/s. O débito desta trama escolhida pode ser justificado através da distância do Access Point ao Host ser significativa, pelo tipo de dispositivo que está conectado à rede Wi-fi ou pelo um elevado congestionamento da rede.

#### 4 Verifique qual a força do sinal (Signal strength) e a qualidade expectável de receção da trama

```

> Frame 52: 329 bytes on wire (2632 bits), 329 bytes captured (2632 bits) on interface en0, id 0
> Radiotap Header v0, Length 60
- 802.11 radio information
  PHY type: 802.11n (HT) (7)
  MCS index: 0
  Bandwidth: 20 MHz (0)
  Short GI: False
  Greenfield: False
  FEC: BEC (0)
  Data rate: 6,5 Mb/s
  Channel: 1
  Frequency: 2412MHz
  Signal strength (dBm): -88dBm
  Noise level (dBm): -93dBm
  Signal/noise ratio (dB): 5dB
  TSF timestamp: 462843
  ...1 = Last part of an A-MPDU: True
  ...0. = A-MPDU delimiter CRC error: False
  A-MPDU aggregate ID: 0
  [Duration: 372µs]
> IEEE 802.11 Beacon frame, Flags: .....C
> IEEE 802.11 Wireless Management
```

Figure 4: Força do sinal da Trama nº52

A força do sinal da trama escolhida é de -88 dBm sendo a qualidade expectável de receção da trama não confiável no que toca à força deste sinal. Contudo, uma vez que se encontra perto dos -90 dBm podemos dizer que há poucas chances de se conectar.

## 5. Scanning Passivo e Scanning Ativo

- 5 Selecione uma trama beacon cuja ordem (ou terminação) corresponda a XX. Esta trama pertence a que tipo de tramas 802.11? Identifique o valor dos identificadores de tipo e de subtipo da trama. 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
    ▸ Flags: 0x00
```

Figure 5: Frame control

Esta trama é do tipo Management. O seu valor de identificador é 00 e o valor do subtipo é 1000(8). Todas esta informação esta na parte de Frame Control do cabeçalho.

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

```
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: PTInovac_d6:88:50 (00:06:91:d6:88:50)
Source address: PTInovac_d6:88:50 (00:06:91:d6:88:50)
```

Figure 6: Mac addresses

Como a trama é um Beacon Frame concluímos que a origem é um router e o destino é todos os dispositivos da rede.

Endereços MAC observáveis:

1. Receiver: Broadcast
2. Destination: Broadcast
3. Transmitter: 00:06:91:d6:88:50
4. Source: 00:06:91:d6:88:50

- 7 Verifique se está a ser usado o método de detecção de erros (CRC). Justifique. Justifique o porquê de ser necessário usar detecção de erros em redes sem fios.

```
Frame check sequence: 0xed0e798d [unverified]
[FCS Status: Unverified]
```

Figure 7: FCS Status

Na imagem assim podemos ver uma mensagem de "FCS Status". Devido a esta mensagem sabemos que está a ser usado um método de controlo de erros.

A utilização de mecanismos de detecção de erros é importante para:

1. Garantir a integridade dos dados transmitidos ou armazenados ao detectar erros como inversões de bits ou falhas na transmissão.
2. Estabelecer confiança nos dados recebidos ao confirmar que os dados chegaram sem erros.
3. Corrigir erros de maneira eficaz ao fornecer informações valiosas para solução de problemas e diagnosticar problemas nos sistemas de transmissão ou armazenamento.

- 8 Uma trama beacon anuncia que o AP pode suportar vários débitos de base (B), assim como vários débitos adicionais (extended supported rates). Indique quais são esses débitos.

```
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
Tag: DS Parameter set: Current Channel: 1
Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
Tag: ERP Information
Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
```

Figure 8: Débitos

Os débitos base de uma trama beacon são 1 MB/S, 2 MB/S, 5.5 MB/s, 11 MB/S, 18 MB/S, 24 MB/S, 36 MB/S, 54 MB/S.

Os débitos adicionais são 6 MB/S, 9 MB/S, 12 MB/S, 48 MB/S.

- 9 Qual o intervalo de tempo previsto entre tramas beacon consecutivas (este valor é anunciado na própria trama beacon)? Na prática, a periodicidade de tramas beacon provenientes do mesmo AP é verificada com precisão? Justifique.

```
Beacon Interval: 0,102400 [Seconds]
```

Figure 9: Tempo esperado

O intervalo de tempo previsto é de 0,102400 segundos.

52	0.415377	PTInovac_d6:88:50	Broadcast	802.11	329
53	0.416551	PTInovac_d6:88:52	Broadcast	802.11	254
54	0.423463	PTInovac_45:be:32	Broadcast	802.11	254
55	0.462093	90:aa:c3:ee:2e:c6	Broadcast	802.11	385
56	0.462107	fc:77:7b:e7:c8:76	Broadcast	802.11	453
57	0.468330	PTInovac_d6:88:50 (... ce:90:6f:21:42:3a (...		802.11	76
58	0.468338	PTInovac_d6:88:50 (... ce:90:6f:21:42:3a (...		802.11	68
59	0.470658	1c:57:3e:fc:f0:a0	Broadcast	802.11	329

Figure 10: Tempo real

Na imagem acima observamos que demorou 0.055281 entre as tramas beacon ( 0.470658 (segunda trama 329) - 0.415377 (Primeira trama 329)). Como tal a periodicidade de tramas beacons nao foi prevista com precisão.

Isto pode ser devido a uma das tramas ter chegado atrasada e fazendo com que a outra chegasse num intervalo de tempo menor do que o esperado.

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

3	0.005857	PTIn...	Broadcast	802.11	329 Beacon frame, SN=696, FN=0, Flags=.....C, BI=100, SSID=MEO...
4	0.008710	PTIn...	Broadcast	802.11	254 Beacon frame, SN=697, FN=0, Flags=.....C, BI=100, SSID=MEO...
5	0.011922	PTIn...	Broadcast	802.11	254 Beacon frame, SN=2358, FN=0, Flags=.....C, BI=100, SSID=ME...
6	0.028491	PTIn...	Broadcast	802.11	254 Beacon frame, SN=2403, FN=0, Flags=.....C, BI=100, SSID=ME...
8	0.050713	90:a...	Broadcast	802.11	385 Beacon frame, SN=1928, FN=0, Flags=.....C, BI=100, SSID=NO...
9	0.053270	fc:7...	Broadcast	802.11	453 Beacon frame, SN=1763, FN=0, Flags=.....C, BI=100, SSID=NO...
10	0.062174	1c:5...	Broadcast	802.11	329 Beacon frame, SN=3598, FN=0, Flags=.....C, BI=100, SSID=ME...
11	0.062181	1c:5...	Broadcast	802.11	254 Beacon frame, SN=3599, FN=0, Flags=.....C, BI=100, SSID=ME...
12	0.087642	Hitr...	Broadcast	802.11	386 Beacon frame, SN=956, FN=0, Flags=.....C, BI=100, SSID=Fly...
15	0.110775	PTIn...	Broadcast	802.11	329 Beacon frame, SN=698, FN=0, Flags=.....C, BI=100, SSID=MEO...

Figure 11: Beacons na vizinhança

Atraves do filtro "wlan.fc.type\_subtype == 0x08" conseguimos filtrar apenas as tramas beacon.

O intervalo de tempo representado na imagem acima é superior ao beacon interval falado na alinea anterior. Como tal podemos determinar que os SSIDs que operão na vizinhança são MEO-D68850, MEO-WiFi, NOS-2EC6, NOS-C876, MEO-FCF0A0 e FlyingNet.

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

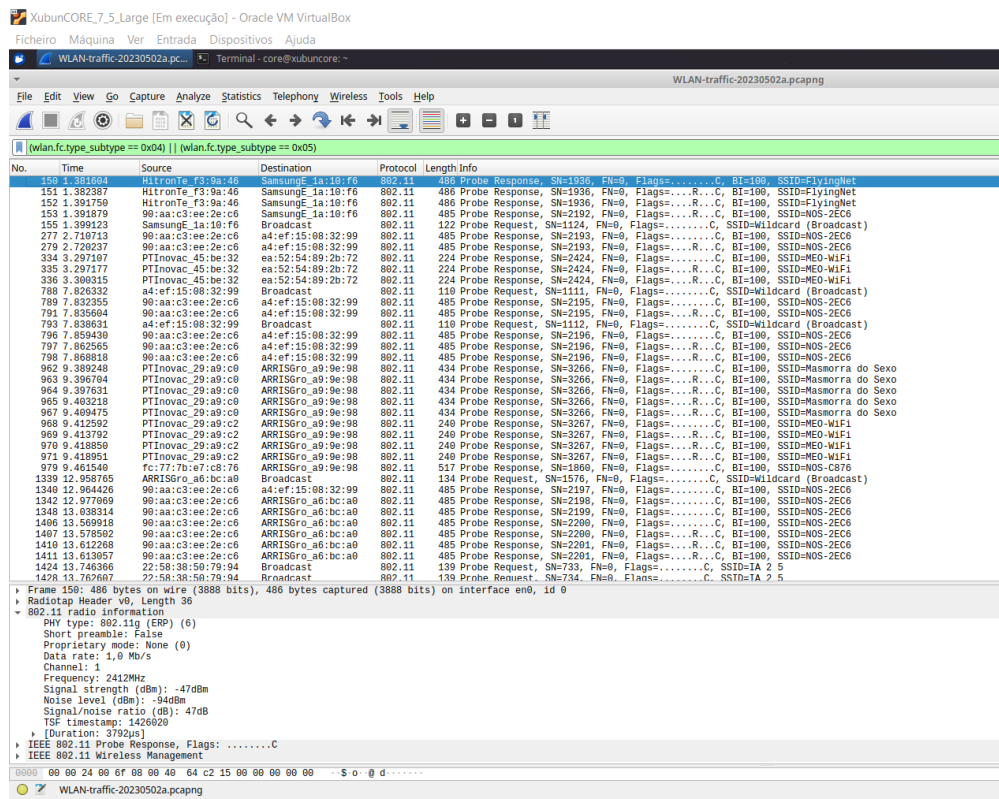


Figure 12: Filtro - Probe Response/Request

Filtro: `(wlan.fc.type_subtype == 0x04) || (wlan.fc.type_subtype == 0x05)`



- 12 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?

```
▶ Frame 788: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface en0, id 0
▶ Radiotap Header v0, Length 36
▶ 802.11 radio information
▼ 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: a4:ef:15:08:32:99 (a4:ef:15:08:32:99)
    Source address: a4:ef:15:08:32:99 (a4:ef:15:08:32:99)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    .... 0000 = Fragment number: 0
    0100 0101 0111 .... = Sequence number: 1111
    Frame check sequence: 0x098f83be [unverified]
    [FCS Status: Unverified]
  ▶ IEEE 802.11 Wireless Management
```

Figure 13: Probe Request

```
▶ Frame 789: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface en0, id 0
▶ Radiotap Header v0, Length 36
▶ 802.11 radio information
▼ IEEE 802.11 Probe Response, Flags: .....C
  Type/Subtype: Probe Response (0x0005)
  ▶ Frame Control Field: 0x5000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: a4:ef:15:08:32:99 (a4:ef:15:08:32:99)
    Destination address: a4:ef:15:08:32:99 (a4:ef:15:08:32:99)
    Transmitter address: 90:aa:c3:ee:2e:c6 (90:aa:c3:ee:2e:c6)
    Source address: 90:aa:c3:ee:2e:c6 (90:aa:c3:ee:2e:c6)
    BSS Id: 90:aa:c3:ee:2e:c6 (90:aa:c3:ee:2e:c6)
    .... 0000 = Fragment number: 0
    1000 1001 0011 .... = Sequence number: 2195
    Frame check sequence: 0xd9b31174 [unverified]
    [FCS Status: Unverified]
  ▶ IEEE 802.11 Wireless Management
```

Figure 14: Probe Response

Para o probe request, os endereços de origem e de destino correspondem à STA de captura e ao broadcast, respetivamente. O propósito de uma trama de probe request é que uma STA solicite informações quanto a APs disponíveis numa rede Wi-fi. Para o probe response, os endereços de origem e de destino correspondem ao Access Point (AP) e à STA de captura, respetivamente. O propósito de uma trama de probe response é que um Access Point (AP) responda a um probe request.

## 6. Processo de Associação

# 13 Identifique uma sequência de tramas que corresponda a um processo de associação realizado com sucesso entre a STA e o AP, incluindo a fase de autenticação.

7896 68.719369	AzureWav_0f:0e:9b	Broadcast	802.11	255 Probe Request, SN=579, FN=0, Flags=.....C, SSID=FlyingNet
7897 68.719374	AzureWav_0f:0e:9b	Broadcast	802.11	246 Probe Request, SN=580, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
7898 68.723917	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	486 Probe Response, SN=1963, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
7818 68.728115	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	486 Probe Response, SN=1964, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
7812 68.743829	8e:86:6e:06:f1:d7	Broadcast	802.11	164 Probe Request, SN=354, FN=0, Flags=.....C, SSID=GRUPO GV
7836 69.004902	fc:77:7b:e7:c8:76	86:03:6f:34:55:9f	802.11	517 Probe Response, SN=2463, FN=0, Flags=.....C, BI=100, SSID=NOS-C876
7837 69.012427	PTInovac_45:be:30	86:03:6f:34:55:9f	802.11	380 Probe Response, SN=3736, FN=0, Flags=.....C, BI=100, SSID=ME0-45BE30
7839 69.013982	PTInovac_45:be:30	86:03:6f:34:55:9f	802.11	380 Probe Response, SN=3736, FN=0, Flags=.....R...C, BI=100, SSID=ME0-45BE30
7841 69.017017	PTInovac_45:be:30	86:03:6f:34:55:9f	802.11	380 Probe Response, SN=3736, FN=0, Flags=.....R...C, BI=100, SSID=ME0-45BE30
7842 69.020396	PTInovac_45:be:30	86:03:6f:34:55:9f	802.11	380 Probe Response, SN=3736, FN=0, Flags=.....R...C, BI=100, SSID=ME0-45BE30
7846 69.038291	PTInovac_45:be:30	86:03:6f:34:55:9f	802.11	380 Probe Response, SN=3736, FN=0, Flags=.....R...C, BI=100, SSID=ME0-45BE30
7847 69.044465	PTInovac_45:be:32	86:03:6f:34:55:9f	802.11	224 Probe Response, SN=3739, FN=0, Flags=.....C, BI=100, SSID=ME0-WiFi1
7848 69.044470	PTInovac_45:be:32	86:03:6f:34:55:9f	802.11	224 Probe Response, SN=3739, FN=0, Flags=.....R...C, BI=100, SSID=ME0-WiFi1
7849 69.051546	PTInovac_45:be:32	86:03:6f:34:55:9f	802.11	224 Probe Response, SN=3739, FN=0, Flags=.....R...C, BI=100, SSID=ME0-WiFi1
7850 69.051647	PTInovac_45:be:32	86:03:6f:34:55:9f	802.11	224 Probe Response, SN=3739, FN=0, Flags=.....R...C, BI=100, SSID=ME0-WiFi1
7851 69.054725	PTInovac_45:be:32	86:03:6f:34:55:9f	802.11	224 Probe Response, SN=3739, FN=0, Flags=.....R...C, BI=100, SSID=ME0-WiFi1
7852 69.060984	PTInovac_45:be:30	86:03:6f:34:55:9f	802.11	380 Probe Response, SN=3740, FN=0, Flags=.....C, BI=100, SSID=ME0-45BE30
7853 69.061967	PTInovac_45:be:30	86:03:6f:34:55:9f	802.11	380 Probe Response, SN=3740, FN=0, Flags=.....R...C, BI=100, SSID=ME0-45BE30
7854 69.064266	PTInovac_45:be:30	86:03:6f:34:55:9f	802.11	380 Probe Response, SN=3740, FN=0, Flags=.....R...C, BI=100, SSID=ME0-45BE30
7855 69.067466	PTInovac_45:be:30	86:03:6f:34:55:9f	802.11	380 Probe Response, SN=3740, FN=0, Flags=.....R...C, BI=100, SSID=ME0-45BE30
7856 69.073804	PTInovac_45:be:30	86:03:6f:34:55:9f	802.11	380 Probe Response, SN=3740, FN=0, Flags=.....R...C, BI=100, SSID=ME0-45BE30
7858 69.083893	PTInovac_45:be:32	86:03:6f:34:55:9f	802.11	224 Probe Response, SN=3741, FN=0, Flags=.....R...C, BI=100, SSID=ME0-WiFi1
7859 69.085125	PTInovac_45:be:32	86:03:6f:34:55:9f	802.11	224 Probe Response, SN=3741, FN=0, Flags=.....R...C, BI=100, SSID=ME0-WiFi1
7860 69.087615	PTInovac_45:be:32	86:03:6f:34:55:9f	802.11	224 Probe Response, SN=3741, FN=0, Flags=.....R...C, BI=100, SSID=ME0-WiFi1
7861 69.089623	PTInovac_45:be:32	86:03:6f:34:55:9f	802.11	224 Probe Response, SN=3741, FN=0, Flags=.....R...C, BI=100, SSID=ME0-WiFi1
7862 69.091637	PTInovac_45:be:32	86:03:6f:34:55:9f	802.11	224 Probe Response, SN=3741, FN=0, Flags=.....R...C, BI=100, SSID=ME0-WiFi1
7897 69.373452	90:aa:c3:ee:2e:c6	a4:ef:15:08:32:99	802.11	485 Probe Response, SN=2255, FN=0, Flags=.....C, BI=100, SSID=NOS-2EC6
7898 69.381146	90:aa:c3:ee:2e:c6	a4:ef:15:08:32:99	802.11	485 Probe Response, SN=2255, FN=0, Flags=.....R...C, BI=100, SSID=NOS-2EC6
7901 69.396712	90:aa:c3:ee:2e:c6	a4:ef:15:08:32:99	802.11	485 Probe Response, SN=2256, FN=0, Flags=.....C, BI=100, SSID=NOS-2EC6
7902 69.396848	90:aa:c3:ee:2e:c6	a4:ef:15:08:32:99	802.11	485 Probe Response, SN=2256, FN=0, Flags=.....R...C, BI=100, SSID=NOS-2EC6
7903 69.399866	90:aa:c3:ee:2e:c6	a4:ef:15:08:32:99	802.11	485 Probe Response, SN=2256, FN=0, Flags=.....R...C, BI=100, SSID=NOS-2EC6
7938 69.784472	86:d7:6d:19:9e:53	Broadcast	802.11	160 Probe Request, SN=896, FN=0, Flags=.....C, SSID= Vodafone-48683C
8139 71.812790	90:aa:c3:ee:2e:c6	46:c1:d5:0e:6e:98	802.11	485 Probe Response, SN=2257, FN=0, Flags=.....R...C, BI=100, SSID=NOS-2EC6
8140 71.813488	90:aa:c3:ee:2e:c6	46:c1:d5:0e:6e:98	802.11	485 Probe Response, SN=2257, FN=0, Flags=.....R...C, BI=100, SSID=NOS-2EC6
8142 71.839235	90:aa:c3:ee:2e:c6	46:c1:d5:0e:6e:98	802.11	485 Probe Response, SN=2258, FN=0, Flags=.....R...C, BI=100, SSID=NOS-2EC6
8185 72.219458	PTInovac_d6:88:50	32:86:aa:fc:00:92	802.11	380 Probe Response, SN=2224, FN=0, Flags=.....C, BI=100, SSID=ME0-D68850
8186 72.229308	PTInovac_d6:88:50	32:86:aa:fc:00:92	802.11	380 Probe Response, SN=2224, FN=0, Flags=.....R...C, BI=100, SSID=ME0-D68850
8187 72.229450	PTInovac_d6:88:50	32:86:aa:fc:00:92	802.11	380 Probe Response, SN=2224, FN=0, Flags=.....R...C, BI=100, SSID=ME0-D68850
8188 72.233246	PTInovac_d6:88:50	32:86:aa:fc:00:92	802.11	380 Probe Response, SN=2224, FN=0, Flags=.....R...C, BI=100, SSID=ME0-D68850
8189 72.235763	PTInovac_d6:88:52	32:86:aa:fc:00:92	802.11	224 Probe Response, SN=2225, FN=0, Flags=.....C, BI=100, SSID=ME0-WiFi1
8190 72.238933	PTInovac_d6:88:52	32:86:aa:fc:00:92	802.11	224 Probe Response, SN=2225, FN=0, Flags=.....R...C, BI=100, SSID=ME0-WiFi1
8192 72.243155	PTInovac_d6:88:52	32:86:aa:fc:00:92	802.11	224 Probe Response, SN=2225, FN=0, Flags=.....R...C, BI=100, SSID=ME0-WiFi1
8193 72.250454	PTInovac_d6:88:52	32:86:aa:fc:00:92	802.11	224 Probe Response, SN=2225, FN=0, Flags=.....R...C, BI=100, SSID=ME0-WiFi1
8194 72.250561	PTInovac_d6:88:52	32:86:aa:fc:00:92	802.11	224 Probe Response, SN=2225, FN=0, Flags=.....R...C, BI=100, SSID=ME0-WiFi1
8499 72.927955	PTInovac_45:be:30	86:0c:40:4f:c3:80	802.11	380 Probe Response, SN=3818, FN=0, Flags=.....C, BI=100, SSID=ME0-45BE30
8410 72.935677	PTInovac_45:be:30	86:0c:40:4f:c3:80	802.11	380 Probe Response, SN=3818, FN=0, Flags=.....R...C, BI=100, SSID=ME0-45BE30
8411 72.935759	PTInovac_45:be:32	86:0c:40:4f:c3:80	802.11	224 Probe Response, SN=3819, FN=0, Flags=.....C, BI=100, SSID=ME0-WiFi1
8472 73.450730	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	70 Authentication, SN=262, FN=0, Flags=.....C
8474 73.450775	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	70 Authentication, SN=1965, FN=0, Flags=.....C
8476 73.455946	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	164 Association Request, SN=263, FN=0, Flags=.....C, SSID=FlyingNet
8478 73.459638	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	210 Association Response, SN=1966, FN=0, Flags=.....C

Figure 15: Sequência de tramas

De modo a obter uma sequência de tramas que corresponda a um processo de associação realizado com sucesso entre a STA e o AP (Access Point), houve a necessidade de aplicar um filtro no Wireshark.

Filtro: "wlan.fc.type\_subtype == 0x04 || wlan.fc.type\_subtype == 0x05 || wlan.fc.type\_subtype == 0x00 || wlan.fc.type\_subtype == 0x01 || wlan.fc.type\_subtype == 0x03 || wlan.fc.type\_subtype == 0x0b"

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

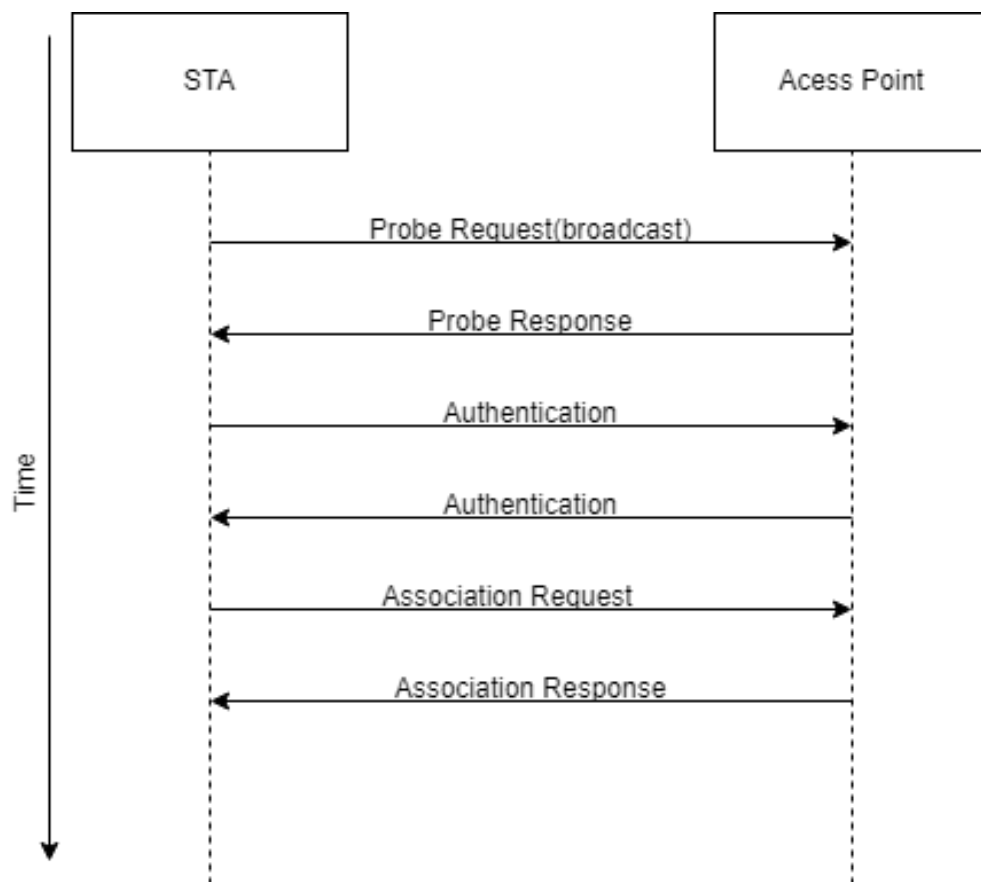


Figure 16: Diagrama

## 7. Transferência de Dados

- 15 Considere a trama de dados nº8503. 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?

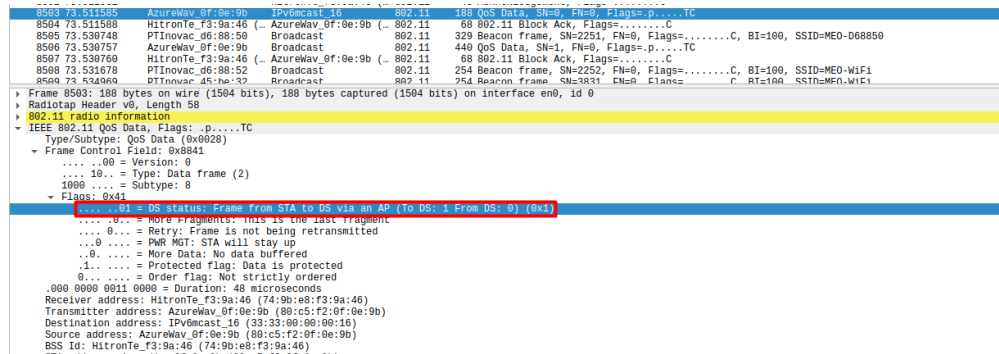


Figure 17: Trama de dados nº8503 - Frame Control

Através dos valores de To DS e From DS, que são respetivamente 1 e 0, podemos concluir que a direccionalidade desta trama é do AP (Access Point) para a STA, sendo local à WLAN, uma vez que a source trata-se de um STA e a destination trata-se de um AP (Access Point).

- 16 Para a trama de dados nº8503, transcreva os endereços MAC em uso, identificando quais os endereços correspondentes à estação sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição (DS)?

```
Receiver address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
Transmitter address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
Destination address: IPv6mcast_16 (33:33:00:00:00:16)
Source address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
BSS Id: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
STA address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
```

Figure 18: Trama de dados nº8503 - MAC Address

STA MAC Address: 80:c5:f2:0f:0e:9b  
AP MAC Address: 74:9b:e8:f3:9a:46  
DS MAC Address: 80:c5:f2:0f:0e:9b

## 17 Como interpreta a trama nº8521 face à sua direccionalidade e endereçamento MAC?

```

▼ 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 0011 1100 = Duration: 60 microseconds
    Receiver address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
    Transmitter address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
    Destination address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
    Source address: 76:9b:e8:f3:9a:43 (76:9b:e8:f3:9a:43)
    BSS Id: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
    STA address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
    .... .... 0000 = Fragment number: 0

```

Figure 19: Trama 8521

A direccionalidade desta trama é do exterior da rede WLAN para o STA. Sabemos isto devido ao valor das flags "To DS: 0" e "From DS: 1".

No endereçamento Mac temos:

1. Endereço do STA: 80:c5:f2:0f:0e:9b
2. Endereço AP: 74:9b:e8:f3:9a:46
3. Endereço do router de acesso: 76:9b:e8:f3:9a:43

No que toca ao endereçamento MAC, verificou-se que o MAC Address da STA corresponde ao MAC Address da source.

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

Os subtipos de tramas de controlo transmitidas durante a transferência de dados numa rede WLAN incluem Acknowledgement (ACK), Request-to-send (RTS), Clear-to-send (CTS) e 802.11 Block Ack (neste caso). Estas tramas são necessárias para coordenar o acesso ao meio e evitar colisões. Ao contrário das redes Ethernet, onde todas as estações partilham um meio físico comum e podem detectar colisões, as tramas de controlo em WLAN permitem uma coordenação mais precisa do acesso ao meio, garantindo uma transmissão eficiente de dados. O ACK é usado para confirmar o recebimento correto das tramas de dados. As tramas RTS e CTS são usadas para reservar o acesso ao meio antes de enviar dados, evitando colisões causadas por estações "escondidas". Nas redes sem fios, onde as estações podem estar em diferentes alcances e não detectar a atividade umas das outras, o uso de tramas RTS/CTS melhora a eficiência da transmissão.

8519	73.544155	HitronTe_f3:9a:46 ...	AzureWav_0f:0e:9b ...	802.11	76	Request-to-send, Flags=.....C
8520	73.544159	HitronTe_f3:9a:46 ...	HitronTe_f3:9a:46 ...	802.11	72	Clear-to-send, Flags=.....C
8521	73.544163	76:9b:e8:f3:9a:43	AzureWav_0f:0e:9b	802.11	444	QoS Data, SN=2, FN=0, Flags=.p....F.C
8522	73.544167	AzureWav_0f:0e:9b ...	HitronTe_f3:9a:46 ...	802.11	68	802.11 Block Ack, Flags=.....C

Figure 20: Tramas 8521, subsequentes e consequentes

- 19 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. Dê um exemplo de uma transferência de dados em que é usada a opção RTC/CTS e um outro em que não é usada.

Para o exemplo acima está a ser usada a opção RTS/CTS para reservar o acesso ao meio antes de enviar tramas de dados. Como é visível, existe um RTS seguido de um CTS. Já na trama 8503, do exercício 15) tal não acontece.

8501	73.511579	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	73	Action, SN=0, FN=0, Flags=.....C, Dialog Token=1
8502	73.511582	HitronTe_f3:9a:46	HitronTe_f3:9a:46	802.11	48	Acknowledgement, Flags=.....C
8503	73.511585	AzureWav_0f:0e:9b	IPv6mcast_16	802.11	188	QoS Data, SN=0, FN=0, Flags=.p....TC
8504	73.511588	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	68	802.11 Block Ack, Flags=.....C
8505	73.530748	PTinovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=2251, FN=0, Flags=.....C, BI=100,
8506	73.530757	AzureWav_0f:0e:9b	Broadcast	802.11	440	QoS Data, SN=1, FN=0, Flags=.p....TC
8507	73.530760	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	68	802.11 Block Ack, Flags=.....C

Figure 21: Tramas 8503, subsequentes e consequentes

## 20 Conclusões

A realização deste trabalho prático permitiu obter e aplicar conhecimentos sobre o protocolo IEEE 802.11, sobre como STAs e APs comunicam entre si, como STAs sabem quais são as redes ao seu redor, como STAs também conseguem conectar-se a uma rede disponível e sobre a interpretação da direccionalidade e do endereçamento MAC de uma trama. A aplicação de filtros no Wireshark facilitou a obtenção de respostas para as perguntas 10, 11 e 13.