



JANEIRO 2021

**Universidade do Minho**  
Escola de Engenharia

## REDES DE COMPUTADORES

### **Grupo 54**

Adriano Maior, a89483

Joel Martins, a89575

Manuel Moreira, a89471

#### 4. Acesso Rádio

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

```
> Frame 354: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits)
  ▾ Radiotap Header v0, Length 25
    Header revision: 0
    Header pad: 0
    Header length: 25
    > Present flags
      MAC timestamp: 34343145
    > Flags: 0x10
      Data Rate: 1,0 Mb/s
      Channel frequency: 2467 [BG 12]
    > Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM
      Antenna signal: -66 dBm
      Antenna noise: -87 dBm
      Antenna: 0
```

A rede sem fios está a operar com frequência igual a 2467MHz, à qual corresponde o canal 12.

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

```
  ▾ 802.11 radio information
    PHY type: 802.11g (ERP) (6)
    Short preamble: False
    Proprietary mode: None (0)
    Data rate: 1,0 Mb/s
    Channel: 12
    Frequency: 2467MHz
    Signal strength (dBm): -66 dBm
    Noise level (dBm): -87 dBm
    Signal/noise ratio (dB): 21 dB
    TSF timestamp: 34343145
    > [Duration: 1632µs]
  > IEEE 802.11 Beacon frame, Flags: .....C
  > IEEE 802.11 Wireless Management
```

A versão da norma IEEE 802.11 que está a ser usada é a 802.11g.

**2. 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.**

```

▼ IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  ▼ Tagged parameters (140 bytes)
    > Tag: SSID parameter set: NOS_WIFI_Fon
    > 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 Number: DS Parameter set (3)
      Tag length: 1
      Current Channel: 12
    > Tag: Extended Supported Rates 6(B), 12(B), 24(B), 48, [Mbit/sec]
    > Tag: Traffic Indication Map (TIM): DTIM 1 of 3 bitmap
    > Tag: ERP Information
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: HT Information (802.11n D1.10)
    > Tag: Extended Capabilities (1 octet)
```

A trama foi enviada a um débito de 1Mb/s, sendo inferior ao débito máximo a que a interface WiFi pode operar até 54 Mb/s.

## 5. Scanning Passivo e Scanning Ativo

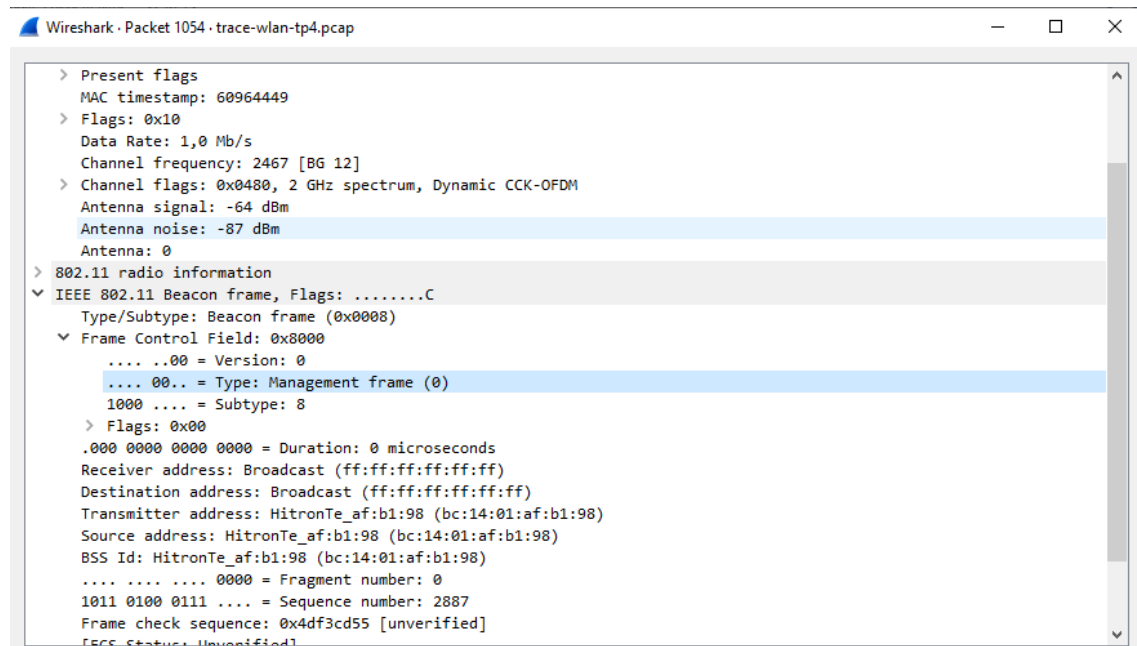
4. Selecione uma *trama beacon* (e.g., trama 10XX). Esta trama pertence a que tipo de tramas 802.11? Indique o valor dos seus identificadores de tipo e de subtipo. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?

802.11g

Tipo -> 0 -> Management Frame

Subtipo -> 8 -> Beacon Frame

Esta informação encontra-se no campo de frame control (controlo de trama)



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

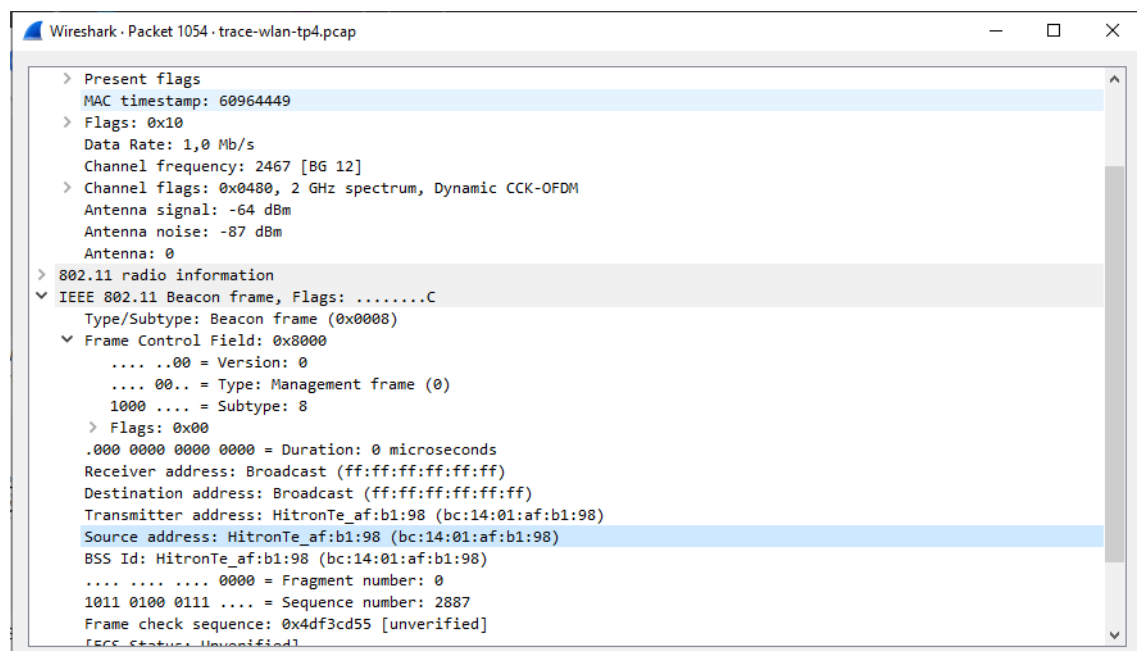
Endereço de origem: bc:14:01:af:b1:98

Endereço de destino: ff:ff:ff:ff:ff:ff

BSS Id: bc:14:01:af:b1:98

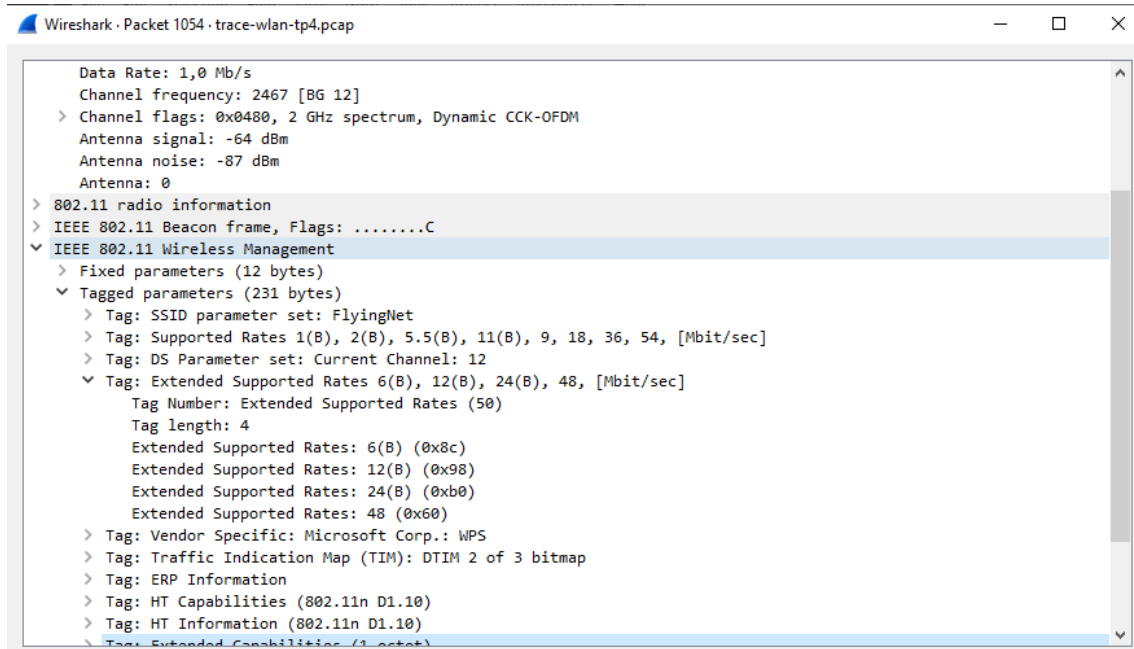
O destino é o endereço de broadcast, o que é normal considerando que esta trama é do subtipo beacon.

A origem é o AP que anuncia a sua presença às interfaces de rádio que estão dentro do seu alcance.



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?

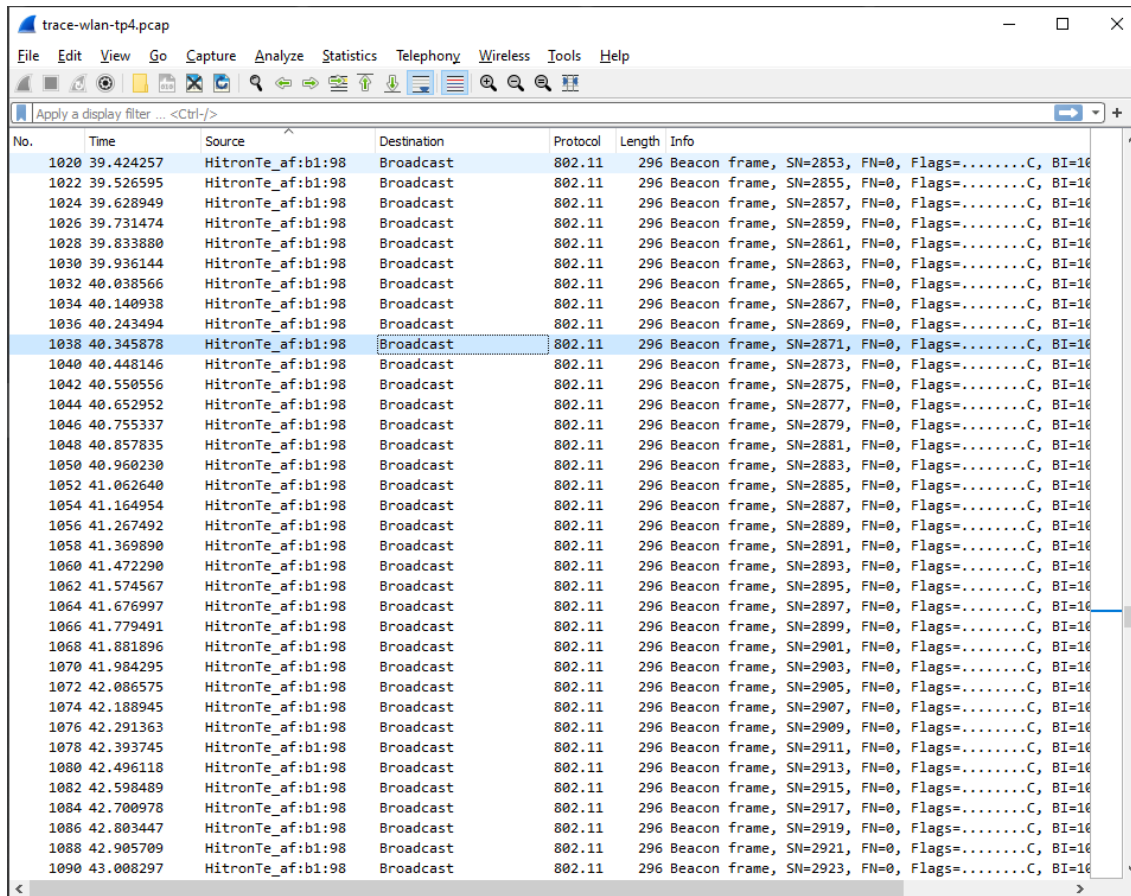
6,12,24,48 Mb/s



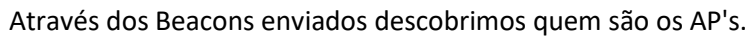
7. Qual o intervalo de tempo previsto entre tramas *beacon* consecutivas? (nota: este valor é anunciado na própria trama *beacon*). Na prática, a periodicidade de tramas *beacon* provenientes do mesmo AP é verificada? Tente explicar porquê.

Beacon Interval: 0,102400 Seconds

As tramas beacons sofrem intervalos ligeiramente superior, o que pode ser devido a dificuldades de transmissão que podem ocorrer por problemas de obstrução do meio.



No.	Time	Source	Destination	Protocol	Length	Info
1020	39.424257	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2853, FN=0, Flags=.....C, BI=102400
1022	39.526595	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2855, FN=0, Flags=.....C, BI=102400
1024	39.628949	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2857, FN=0, Flags=.....C, BI=102400
1026	39.731474	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2859, FN=0, Flags=.....C, BI=102400
1028	39.833880	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2861, FN=0, Flags=.....C, BI=102400
1030	39.936144	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2863, FN=0, Flags=.....C, BI=102400
1032	40.038566	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2865, FN=0, Flags=.....C, BI=102400
1034	40.140938	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2867, FN=0, Flags=.....C, BI=102400
1036	40.243494	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2869, FN=0, Flags=.....C, BI=102400
1038	40.345878	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2871, FN=0, Flags=.....C, BI=102400
1040	40.448146	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2873, FN=0, Flags=.....C, BI=102400
1042	40.550556	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2875, FN=0, Flags=.....C, BI=102400
1044	40.652952	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2877, FN=0, Flags=.....C, BI=102400
1046	40.755337	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2879, FN=0, Flags=.....C, BI=102400
1048	40.857835	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2881, FN=0, Flags=.....C, BI=102400
1050	40.960230	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2883, FN=0, Flags=.....C, BI=102400
1052	41.062640	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2885, FN=0, Flags=.....C, BI=102400
1054	41.164954	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2887, FN=0, Flags=.....C, BI=102400
1056	41.267492	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2889, FN=0, Flags=.....C, BI=102400
1058	41.369890	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2891, FN=0, Flags=.....C, BI=102400
1060	41.472290	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2893, FN=0, Flags=.....C, BI=102400
1062	41.574567	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2895, FN=0, Flags=.....C, BI=102400
1064	41.676997	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2897, FN=0, Flags=.....C, BI=102400
1066	41.779491	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2899, FN=0, Flags=.....C, BI=102400
1068	41.881896	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2901, FN=0, Flags=.....C, BI=102400
1070	41.984295	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2903, FN=0, Flags=.....C, BI=102400
1072	42.086575	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2905, FN=0, Flags=.....C, BI=102400
1074	42.188945	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2907, FN=0, Flags=.....C, BI=102400
1076	42.291363	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2909, FN=0, Flags=.....C, BI=102400
1078	42.393745	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2911, FN=0, Flags=.....C, BI=102400
1080	42.496118	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2913, FN=0, Flags=.....C, BI=102400
1082	42.598489	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2915, FN=0, Flags=.....C, BI=102400
1084	42.700978	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2917, FN=0, Flags=.....C, BI=102400
1086	42.803447	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2919, FN=0, Flags=.....C, BI=102400
1088	42.905709	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2921, FN=0, Flags=.....C, BI=102400
1090	43.008297	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2923, FN=0, Flags=.....C, BI=102400



trace-wlan-tp4.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(wlan.fc.subtype == 0x08) && (wlan.fc.type == 0x00)

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.TC
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.TC
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....TC
1	0.000000	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2083, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
3	0.102552	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2085, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
5	0.204951	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2087, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
7	0.307368	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2089, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
9	0.409749	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2091, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
11	0.512117	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2093, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
13	0.614562	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2095, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
28	0.716961	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2097, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
32	0.819368	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2099, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
34	0.921756	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2101, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
36	1.024021	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2103, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
38	1.126564	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2105, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
40	1.228961	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2107, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
42	1.331376	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2109, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
44	1.433766	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2111, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
46	1.536169	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2113, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
48	1.638484	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2115, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
50	1.741027	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2117, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
52	1.843381	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2119, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
54	1.945665	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2121, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
56	2.048037	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2123, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The main display area shows a list of captured packets, with the first 80 packets being 802.11 Beacon frames. The packet list has columns for Time, Source, Destination, Protocol, Length, and Info. The source and destination addresses are consistently HitronTf\_af:b1:99 and Broadcast. The protocol is 802.11, and the length is 205 bytes. The info column shows details about the beacon frame, including frame number, flags, and SSID.

Time	Source	Destination	Protocol	Length	Info
278.10.548833	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2290, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
280.10.651246	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2292, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
282.10.753667	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2294, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
284.10.856059	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2296, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
286.10.958458	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2298, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
288.11.060824	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2300, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
290.11.163258	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2302, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
293.11.368126	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2306, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
295.11.470471	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2308, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
297.11.572919	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2310, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
299.11.675316	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2312, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
301.11.777656	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2314, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
303.11.880219	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2316, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
305.11.982619	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2318, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
307.12.085007	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2320, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
309.12.187402	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2322, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
311.12.289807	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2324, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
314.12.494618	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2328, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
316.12.597010	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2330, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
318.12.699435	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2332, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
320.12.801833	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2334, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
322.12.904212	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2336, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
324.13.006518	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2338, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
326.13.109035	HitronTf_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2340, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon



**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.**

Existem pacotes com erros de formação.

Redes sem fios sofrem muitos erros devido ao meio pelo qual são enviadas as tramas, uma vez que existem muitos obstáculos.

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

O filtro inserido foi o seguinte:

**(wlan.fc.subtype == 0x4 || wlan.fc.subtype == 0x5) && wlan.fc.type == 0x0**

**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?**

**Probe Request:**

Receiver: ff:ff:ff:ff:ff:ff

Destination: ff:ff:ff:ff:ff:ff

Transmitter: ea:a4:64:7b:b9:7a

Source: ea:a4:64:7b:b9:7a

Broadcast para todos os APs disponíveis na área

**Probe Response:**

Receiver: ea:a4:64:7b:b9:7a

Destination: ea:a4:64:7b:b9:7a

Transmitter: HitronTe\_af:b1:98 (bc:14:01:af:b1:98)

Source: HitronTe\_af:b1:98 (bc:14:01:af:b1:98)

Para o host que fez probe request, neste caso (ea:a4:64:7b:b9:7a).

Wireshark · Packet 2468 · trace-wlan-tp4.pcap

> 802.11 radio information  
IEEE 802.11 Probe Request, Flags: .....C  
Type/Subtype: Probe Request (0x0004)  
Frame Control Field: 0x4000  
.... 0000 = Version: 0  
.... 00.. = Type: Management frame (0)  
0100 .... = Subtype: 4  
> Flags: 0x00  
.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]  
> IEEE 802.11 Wireless Management

0000	00 00 19 00 6f 08 00 00	34 84 5c 05 00 00 00 00	..... 4.....
0010	10 02 a3 09 08 04 cc a9	00 40 00 00 00 ff ff ff	..... @.....
0020	ff ff ff ea a4 64 7b b9	7a ff ff ff ff ff ff d0	..... d{ z.....
0030	9e 00 00 01 04 02 04 0b	16 32 08 0c 12 18 24 30	..... 2..... \$0
0040	48 60 6c 03 01 0c 2d 1a	21 40 17 ff 00 00 00 00	H'l..... !@.....
0050	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	..... ..
0060	00 00 7f 08 04 00 08 84	00 00 00 40 6b 07 0f ff	..... @k.....
0070	ff ff ff ff dd 0b 00	17 f2 0a 00 01 04 00 00	..... ..
0080	00 00 dd 08 00 50 f2 08	00 0e 00 00 dd 09 00 10	..... P.....
0090	18 02 00 00 10 00 00 e2	32 f5 b4	..... 2.....

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

> 802.11 radio information  
IEEE 802.11 Probe Response, Flags: .....C  
Type/Subtype: Probe Response (0x0005)  
Frame Control Field: 0x5000  
.... 0000 = Version: 0  
.... 00.. = Type: Management frame (0)  
0101 .... = Subtype: 5  
> Flags: 0x00  
.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]  
> IEEE 802.11 Wireless Management

0000	00 00 19 00 6f 08 00 00	ee 88 5c 05 00 00 00 00	..... 4.....
0010	12 0c a3 09 08 04 be a9	00 50 00 32 00 ea a4 64	..... P2...d
0020	7b b9 7a bc 14 01 af b1	98 bc 14 01 af b1 98 c0	{ z.....
0030	91 84 ad e3 b1 0b 01 00	00 64 00 31 0c 00 09 46	..... d1...F
0040	6c 79 69 6e 67 4e 65 74	01 08 82 84 8b 96 12 24	lyingNet..... \$
0050	48 6c 03 01 0c 2a 01 00	32 04 8c 98 b0 60 2d 1a	H'l...*... 2.....
0060	8c 01 16 ff ff 00 00 00	00 00 00 00 00 00 00 00	..... ..
0070	00 00 00 00 00 00 00 00	00 00 3d 16 0c 00 04 00	..... =.....
0080	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	..... ..
0090	00 00 3e 01 00 dd 1a 00	50 f2 01 01 00 00 50 f2	...>..... P.....P
00a0	02 02 00 00 50 f2 02 00	50 f2 04 01 00 00 50 f2	...P... P.....P
00b0	02 30 18 01 00 00 0f ac	02 02 00 00 0f ac 02 00	0..... P.....P
00c0	0f ac 04 01 00 00 0f ac	02 00 00 dd 18 00 50 f2	..... ..
00d0	02 01 01 80 00 03 a4 00	00 27 a4 00 00 42 43 5e	..... BC^
00e0	00 62 32 2f 00 0b 05 02	00 0b 12 7a 7f 01 01 dd	b2/..... z.....
00f0	07 00 0c 43 00 00 00 00	dd 9d 00 50 f2 04 10 4a	...C..... P...J
0100	00 01 10 10 44 00 01 02	10 3b 00 01 03 10 47 00	...D..... ;...G
0110	10 28 80 28 80 28 80 18	80 a8 80 bc 14 01 af b1	( ( ( ( .....
0120	98 10 21 00 18 52 61 6c	69 6e 6b 20 54 65 63 68	! Ralink Tech
0130	6e 6f 6c 6f 67 79 2c 20	43 6f 72 70 2e 10 23 00	nology, Corp.#
0140	1c 52 61 6c 69 6e 6b 20	57 69 72 65 6c 65 73 73	Ralink Wireless
0150	20 41 63 63 65 73 73 20	50 6f 69 6e 74 10 24 00	Access Point.\$
0160	06 52 54 32 38 36 30 10	42 00 08 31 32 33 34 35	RT2860 B-12345
0170	36 37 38 10 54 00 08 00	06 00 50 f2 04 00 01 10	678-T... P.....
0180	11 00 09 52 61 6c 69 6e	6b 41 50 53 10 08 00 02	Ralink kAPS.....

No.: 2469 · Time: 70.149792 · Source: HitronTe\_af:b1:98 · Destination: ea:a4:64:7b:b9:7a · Protocol: 802.11 · Length: 411 · Info: Probe Response, SN=2332, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Close Help

## 6. Processo de Associação

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.

Uma sequência de tramas que corresponde a um processo de associação completo entre a STA e o AP pode ser visto na figura abaixo, juntamente com o filtro usado.

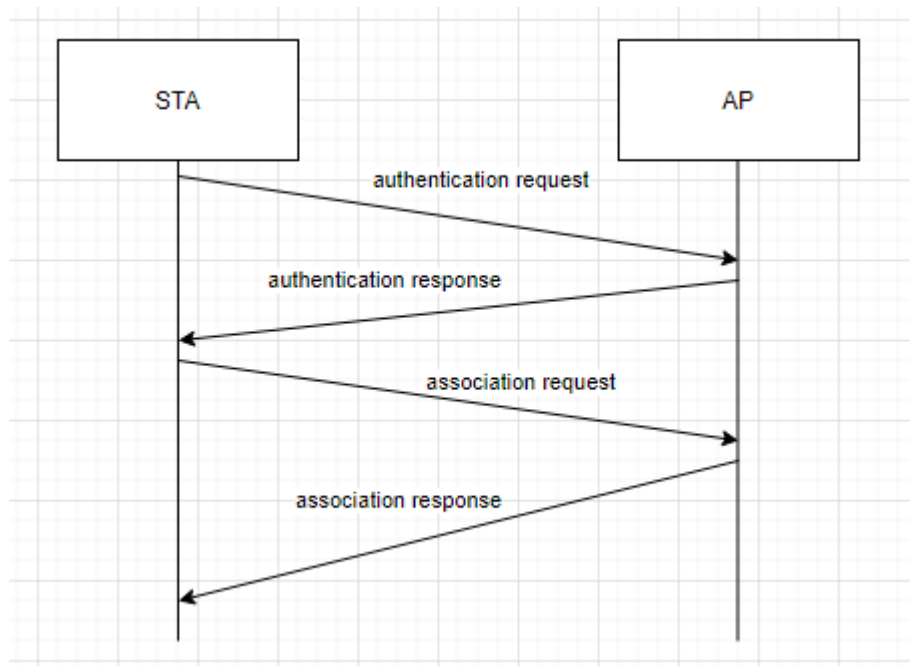
trace-wlan-tp4.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.fc.type\_subtype == 0x0000 || wlan.fc.type\_subtype == 0x0001 || wlan.fc.type\_subtype == 0x000b

No.	Time	Source	Destination	Protocol	Length	Info
2486	70.361782	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	70	Authentication, SN=2542, FN=0, Flags=.....C
2488	70.381869	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59	Authentication, SN=2338, FN=0, 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
2492	70.389339	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	225	Association Response, SN=2339, FN=0, Flags=.....C

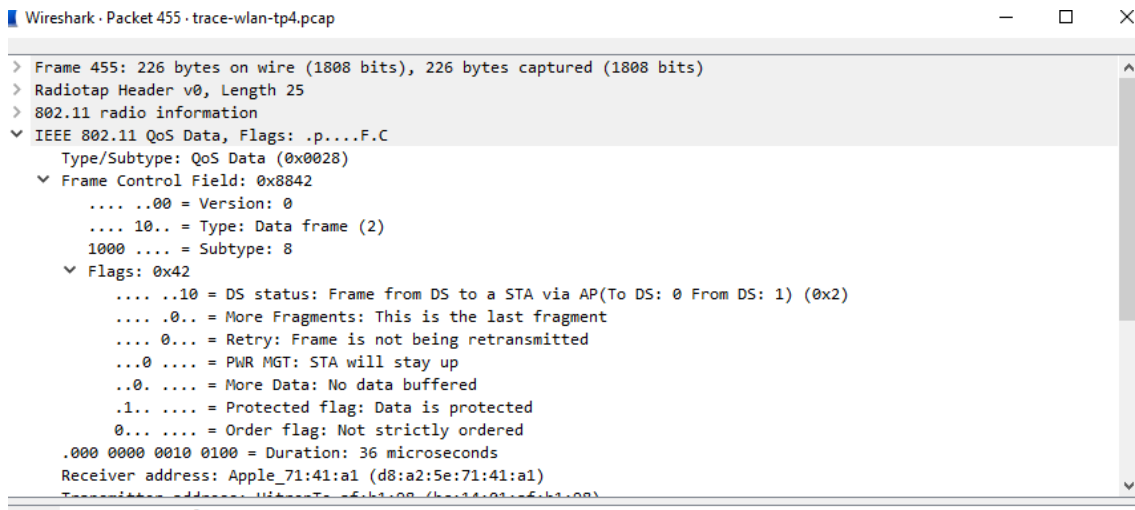
13. Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo.



## 7. Transferência de 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?**

Não, o pacote é oriundo do Sistema de Distribuição e tem como destino um STA, como se pode ver na figura abaixo.



**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?**

Destination address: Apple\_71:41:a1 (d8:a2:5e:71:41:a1)

BSS Id: HitronTe\_af:b1:98 (bc:14:01:af:b1:98) AP

Source address: HitronTe\_af:b1:98 (bc:14:01:af:b1:98) Router

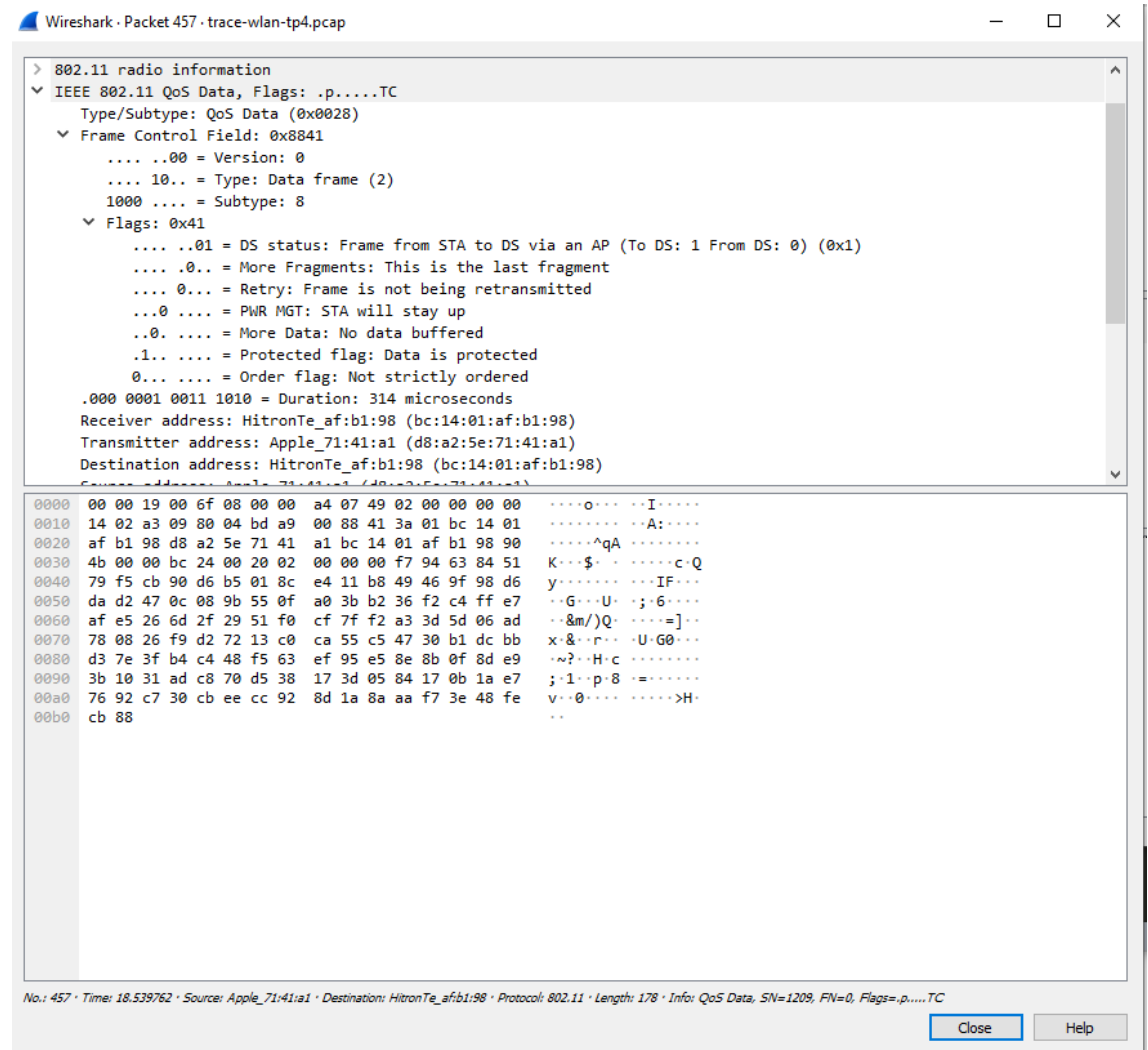
## 16. Como interpreta a trama nº457 face à sua direccionalidade e endereçamento MAC?

A trama vai de um STA para o Sistema de Distribuição.

BSS Id: HitronTe\_af:b1:98 (bc:14:01:af:b1:98) AP

STA address: Apple\_71:41:a1 (d8:a2:5e:71:41:a1) STA

Destination address: HitronTe\_af:b1:98 (bc:14:01:af:b1:98) Router



## 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.)

O subtipo de tramas são de *acknowledgment*. Nas redes Wi-Fi existem dificuldades que não se encontram em redes Ethernet. Por exemplo, esta é mais suscetível a falhas, sendo assim enviadas tramas de controlo. Estas são responsáveis por fazerem chegar a confirmação que diz que as tramas foram enviadas corretamente recebidas.

**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.**

Relativamente ao exemplo anterior não é utilizada esta opção, no entanto esta opção foi utilizada na troca de outras mensagens que se encontram na captura do *wireshark* disponibilizada.

## **Conclusão**

Com a realização deste trabalho prático, foram exploramos diversos aspetos acerca do protocolo IEEE 802.11, das quais se destacaram, o formato das tramas, o endereçamento dos componentes envolvidos na comunicação sem fios, bem como a operação do protocolo.

Também vimos de perto o funcionamento do scanning ativo e do scanning passivo, e aprendemos que existem três tipos de tramas: as tramas de gestão, responsáveis por estabelecer e manter a comunicação entre as STAs; as tramas de controlo, que ajudam na troca de tramas de dados entre as STAs; e as tramas de dados, responsáveis pela transmissão e comunicação de dados.