

TP3-Turno 1- Grupo 5

Francisco Torrinha – A91691

João Novais da Silva – A91671

Pedro Sequeira – A91660

1.

2467 Mhz, channel 12

```
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): -59 dBm
Noise level (dBm): -88 dBm
Signal/noise ratio (dB): 29 dB
TSF timestamp: 19800120
> [Duration: 2360µs]
```

2.

802.11g (6)

```
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): -59 dBm
Noise level (dBm): -88 dBm
Signal/noise ratio (dB): 29 dB
TSF timestamp: 19800120
> [Duration: 2360µs]
```

3.

Débito enviado: 1Mb/s débito máximo: 54Mb/s, não porque apenas é usado 1Mb/s e a rede Wi-fi suporta até 54Mb/s.

```
> Present flags
  MAC timestamp: 19800120
> Flags: 0x10
  Data Rate: 1.0 Mb/s
  Channel frequency: 2467 [BG 12]
> Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM
```

- > Tag: SSID parameter set: FlyingNet
- > 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]
- > Tag: Vendor Specific: Microsoft Corp.: WPS
- > Tag: Traffic Indication Map (TIM): DTIM 2 of 3 bitmap

4.

Beacon frame 0x0008.

- ▼ 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)

5.

FlyingNet.

- ▼ Tagged parameters (231 bytes)
  - ▼ Tag: SSID parameter set: FlyingNet
    - Tag Number: SSID parameter set (0)
    - Tag length: 9
    - SSID: FlyingNet

6.

Intervalo de tempo do Beacon: 0.102400 segundos. Não é verificada

- IEEE 802.11 Wireless Management
  - ▼ Fixed parameters (12 bytes)
    - Timestamp: 1149670605293
    - Beacon Interval: 0.102400 [Seconds]
    - > Capabilities Information: 0x0c31
  - > Tagged parameters (231 bytes)

7.

Os endereços estão registados em baixo.

```
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)
```

8.

O filtro é: wlan.fc.type\_subtype == 1 or wlan.fc.type\_subtype == 0.

wlan.fc.type_subtype == 1 or wlan.fc.type_subtype == 0			
No.	Time	Source	Destination
2490	70.383512	Apple_10:6a:f5	HitronTe_af:b1:98
2492	70.389339	HitronTe_af:b1:98	Apple_10:6a:f5
4696	83.665976	7c:ea:6d:ff:a2:cc	HitronTe_af:b1:98
4698	83.678873	HitronTe_af:b1:98	7c:ea:6d:ff:a2:cc
4699	83.680045	HitronTe_af:b1:98	7c:ea:6d:ff:a2:cc
7065	100.208375	d7:19:51:08:62:f9	6d:1b:44:1a:cc:11
7163	100.403689	0a:57:13:28:40:84	79:5c:58:10:7a:cc

9.

Num *Active Scanning*, as estações vão por cada canal de cada vez, mas em vez de ouvir passivamente os sinais nessa frequência, as estações enviam um *Probe Request Management Frame* perguntando qual rede esta livre neste canal.

In Active scanning, stations still go through each channel in turn, but instead of passively listening to the signals on that frequency, station send a Probe Request management frame asking what network is available on that channel.

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

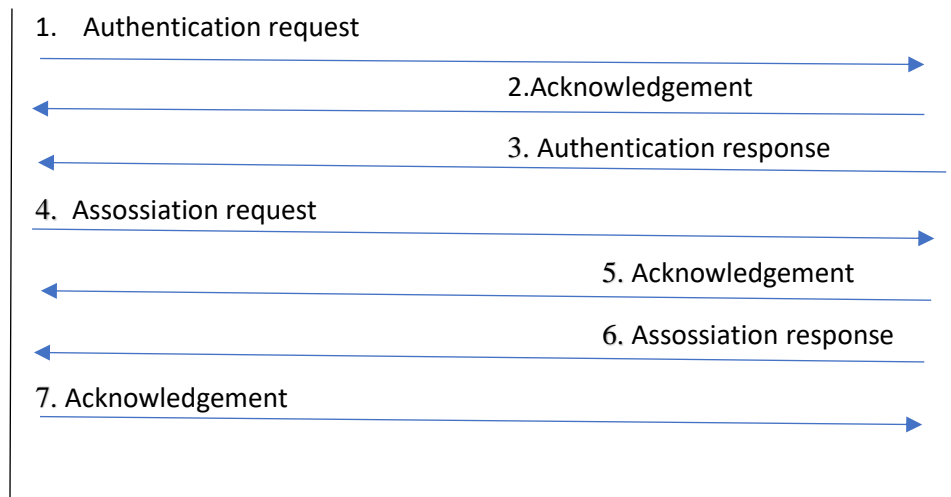
10.

2485	70.352671		Broadcom_04:6a:f5 (...)	802.11	39 Clear-to-send, Flags=.....C
2486	70.361782	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	70 Authentication, SN=2542, FN=0, Flags=.....C
2487	70.362050		Apple_10:6a:f5 (64:...	802.11	39 Acknowledgement, Flags=.....C
2488	70.381869	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59 Authentication, SN=2338, FN=0, Flags=.....C
2489	70.381878		HitronTe_af:b1:98 (...)	802.11	39 Acknowledgement, Flags=.....C
2490	70.383512	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	175 Association Request, SN=2543, FN=0, Flags=.....C, SSID=FlyingNet
2491	70.383873		Apple_10:6a:f5 (64:...	802.11	39 Acknowledgement, Flags=.....C
2492	70.389339	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	225 Association Response, SN=2339, FN=0, Flags=.....C
2493	70.389352		HitronTe_af:b1:98 (...)	802.11	39 Acknowledgement, Flags=.....C

11.

Mobile station

access point



12.

Sim, é local WLAN.

Flags: 0x42

```
.... ..10 = DS status: Frame from DS to a STA via AP (To DS: 0 From DS: 1) (0x2)
.... .0.. = More Fragments: This is the last fragment
.... 0... = Retry: Frame is not being retransmitted
...0 .... = PWR MGT: STA will stay up
..0. .... = More Data: No data buffered
.1.. .... = Protected flag: Data is protected
0... .... = Order flag: Not strictly ordered
```

13.

A comunicação está a ser feita entre dois dispositivos da rede, o router e a máquina local.

```
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)
```

14.

A comunicação está a ser feita da máquina para o router.

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
```

15.

O subtipo das tramas de controlo que são transmitidas ao longo da transferência é 8. As tramas de controlo são auxiliares na transmissão das tramas de dados, gerem o acesso ao meio wireless e motivam a execução de funções ao nível MAC.

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)
```

Estão a ser ambas as opções Request to Send (RTS) e Clear to Send (CTS) na troca entre a STA e o AP/Router.

▶ Frame 554: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits)

▼ Radiotap Header v0, Length 40

Header revision: 0

Header pad: 0

Header length: 40

Present flags

MAC timestamp

Flags: 0x54

Channel free

Channel flags: 0x0480, 2 GHz sp

Antenna signal: -68dBm

Antenna noise: -87dBm

Antenna: 0

Channel number: 12

Channel frequency:  
Channel flags: 0x00

Channel flags: 0x00010480, 2 GHz spectrum, Dynamic CCK-OFDM, HT Channel (20MHz Channel Width)  
MCS information

MCS Information  
[Data Rate: 65.4]

2.11 radio information

IEEE 802.11 QoS Data El

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
```

```
..0. .... = More Data: No data buffered
1        = Protected flag: Data is protected
```

```

.1... .... = Protected flag: Data is protected
0          = Order flag: Not strictly ordered

```

000 0000 0010 0100 = Duration: 36 microseconds

```

.0000 0000 0010 0100 = Duration: 30 microseconds
Receiver address: Apple 10:6a:7b (64:9a:be:10:6a:7b)

```

Transmitter address: HitronTe af:aa:41 (bc:14:01:af:aa:41)

Transmitter address: 11c0101e\_01:aa:41 (bc:14:01:aa:41)

Qos Control (wlan.qos), 2 bytes

## CONCLUSÃO:

Este trabalho foi crucial no auxílio á aprendizagem do funcionamento do protocolo 802.11 a cada um dos elementos do grupo.