



**Universidade do Minho**  
Escola de Engenharia

2020

# REDES DE COMPUTADORES

TRABALHO PRÁTICO 4 – REDES SEM FIOS (802.11)

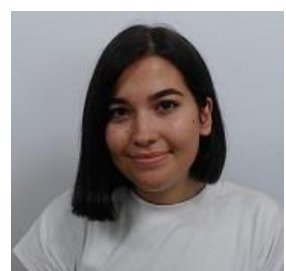
GRUPO 63



A89533 - Ana Carneiro



A89517 - Diogo Araújo



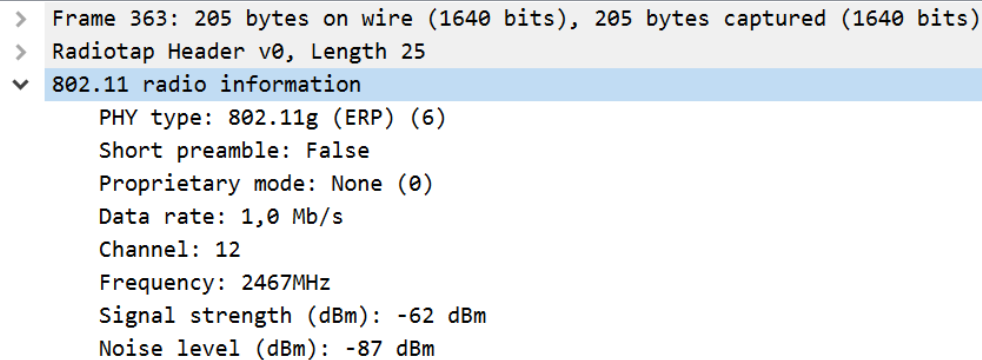
A89518 – Ema Dias

## ÍNDICE

ACESSO RÁDIO .....	3
1. Identifique em que frequência do espectro está a operar a rede sem fios, e o canal que corresponde essa frequência. ....	3
2. Identifique a versão da norma IEEE 802.11 que está a ser usada. ....	3
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. ....	3
SCANNING PASSIVO E SCANNING ATIVO .....	4
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)? .....	4
5. Para a trama acima, identifique todos os endereços MAC em uso. Que conclui quanto à sua origem e destino? .....	5
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? .....	5
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. ....	6
8. Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura? Explique o modo como obteve essa informação (por exemplo, se usou algum filtro para o efeito). 7	
9. Verifique se está a ser usado o método de deteção de erros (CRC). Justifique. ....	7
10. Estabeleça um filtro Wireshark apropriado que lhe permita visualizar todas as tramas probing request ou probing response, simultaneamente. ....	8
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? .....	9
PROCESSO DE ASSOCIAÇÃO .....	10
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. ....	10
13. Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo. .	10
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? .....	11
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? .....	11
16. Como interpreta a trama nº457 face à sua direccionalidade e endereçamento MAC? ....	12
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.) .....	12

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.....	13
CONCLUSÃO.....		15

## ACESSO RÁDIO



```
> Frame 363: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits)
> Radiotap Header v0, Length 25
v 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): -62 dBm
    Noise level (dBm): -87 dBm
```

Figura 1: Trama 363

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

O espectro está a operar a uma frequência de 2467MHz (frequency) e o canal correspondente é o 12 (channel).

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

Versão da norma IEEE 802.11 é 802.11g (ERP) (PHY type).

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 a que foi enviada a trama escolhida foi 1,0Mb/s, sendo que o valor de débito máximo a que a interface pode operar é de 54 Mb/s. Utiliza-se o valor mais pequeno para possibilitar que a trama chegue a todos os hosts.

## SCANNING PASSIVO E SCANNING ATIVO

Wireshark · Packet 1063 · trace-wlan-tp4.pcap

```
> Frame 1063: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits)
> Radiotap Header v0, Length 25
▼ 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): -61 dBm
    Noise level (dBm): -87 dBm
```

Figura 2: Trama 1063

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)?

```
✓ 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:b1:99 (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)
      .... 0000 = Fragment number: 0
      1011 0101 0000 .... = Sequence number: 2896
```

Figura 3: Informação da trama 1063

Através do valor do 0x8000, *type/subtype*, que em binário corresponde a 1000 e com recurso ao anexo que nos foi disponibilizado percebemos que o tipo é 00, subtipo é 1000 e *type description* é *management*.

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110–0111	Reserved
00	Management	1000	Beacon
00	Management	1001	Announcement traffic indication message (ATIM)
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101–1111	Reserved
01	Control	0000–1001	Reserved

Figura 4: informações do anexo

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

Na figura 3 conseguimos ver os seguintes endereços MAC:

Receiver Address: ff:ff:ff:ff:ff:ff

Destination Address: ff:ff:ff:ff:ff:ff

Transmitter Address: bc:14:01:af:b1:99

Source Address: bc:14:01:af:b1:99

O endereço de destino é um endereço de Broadcast e por isso transmite para todos os hosts na rede. O endereço de origem é o endereço MAC correspondente ao AP.

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?

```

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

```

**Figura 5: Débitos da trama**

Os débitos suportados são 1 Mb/s, 2 Mb/s, 5.5 Mb/s, 11Mb/s, 9Mb/s, 18 Mb/s, 36 Mb/s, 54 Mb/s, tal como é possível visualizar na figura 5.

Já os débitos adicionais são 6Mb/s, 12Mb/s, 24Mb/s e 48 Mb/s, tal como referido na figura 6.

```

> 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)

```

**Figura 6: Débitos adicionais da trama**

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.

```

802.11 Radio Information
> IEEE 802.11 Beacon frame, Flags: .....C
▼ IEEE 802.11 Wireless Management
  ▼ Fixed parameters (12 bytes)
    Timestamp: 1149712182095
    Beacon Interval: 0,102400 [Seconds]
    > Capabilities Information: 0x0c21
  ▼ Tagged parameters (140 bytes)

```

Figura 7: Informação sobre intervalo de tempo entre tramas

Através da figura 5, percebemos que o intervalo de tempo entre tramas beacon é de 0,102400 segundos.

No.	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
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
58	2.150630	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2125, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
60	2.252991	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2127, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
62	2.355327	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2129, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
64	2.457796	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2131, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
66	2.560185	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2133, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Figura 8: Filtro de tramas de SSID = FlyingNet

Time	Source	Destination	Protocol	Length	Info
2	0.001662	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2084, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
4	0.104164	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2086, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
6	0.206582	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2088, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
8	0.308999	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2090, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
10	0.411376	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2092, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
12	0.513707	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2094, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
14	0.616191	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2096, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
19	0.718611	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2098, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
33	0.821009	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2100, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
35	0.923387	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2102, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
37	1.025663	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2104, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
39	1.128193	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2106, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
41	1.230650	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2108, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
43	1.332996	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2110, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
45	1.435394	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2112, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
47	1.537783	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2114, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
49	1.640067	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2116, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
51	1.742627	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2118, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
53	1.845003	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2120, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
55	1.947283	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2122, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
57	2.049766	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2124, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
59	2.152134	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2126, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
61	2.254671	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2128, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
63	2.357010	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2130, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
65	2.459307	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2132, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
67	2.561756	HitronTe_af:b1:99	Broadcast	205	Beacon frame, SN=2134, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

Figura 9: Filtro de tramas de SSID = Nos\_WIFI\_Fon

Para perceber se as tramas provenientes do mesmo AP são periódicas, realizamos um filtro e avaliamos o intervalo de tempo entre as mesmas, verificamos que não há periodicidade.

8. 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).

Filter: wlan.addr == ff:ff:ff:ff:ff:ff

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2083, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
2	0.001662	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2084, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
3	0.102552	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2085, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
4	0.104164	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2086, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
5	0.204951	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2087, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
6	0.206582	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2088, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
7	0.307368	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2089, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
8	0.308999	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2090, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
9	0.409749	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2091, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
10	0.411376	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2092, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
11	0.512117	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2093, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
12	0.513787	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2094, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
13	0.614562	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2095, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
14	0.616191	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2096, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
28	0.716961	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2097, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
29	0.718611	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2098, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
32	0.819368	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2099, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
33	0.821009	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2100, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
34	0.921756	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2101, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
35	0.923387	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2102, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
36	1.024021	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2103, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
37	1.025663	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2104, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
38	1.126564	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2105, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
39	1.128193	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2106, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
40	1.228961	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2107, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
41	1.230650	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2108, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
42	1.331376	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2109, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
43	1.332996	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2110, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
44	1.433766	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2111, FH=0, Flags=.....C, BI=100, SSID=FlyingNet

Figura 10: Filtro Usado

De forma listar os SSIDs dos APs que estão a operar na vizinhança da STA de captura – FlyingNet e NOS-WIFI-FON – usamos o seguinte filtro:

```
wlan.addr = ff:ff:ff:ff:ff:ff
```

9. Verifique se está a ser usado o método de deteção de erros (CRC). Justifique.

Filter: (wlan.fc.type\_subtype == 0x08) && (wlan.fcs.status == bad)

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.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 11: Tramas com erros

Tal como esta explicito na figura 11 conseguimos concluir que existem tramas com erros. Usa-se o campo Frame Checksum (figura 12) de forma a verificar se a trama foi transmitida de forma correta ou não, pois as redes wifi serem mais suscetíveis a erros, pois são transmitidas em meios sem fios. As tramas com erros têm de ser retransmitidas tal como esta explicito no campo *reentry* da figura 12.



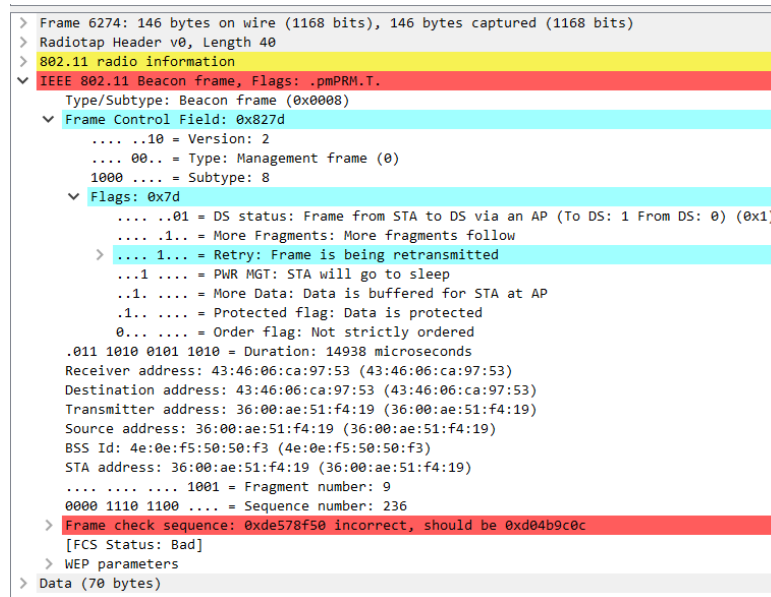


Figura 12: Informação sobre uma trama incorreta

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

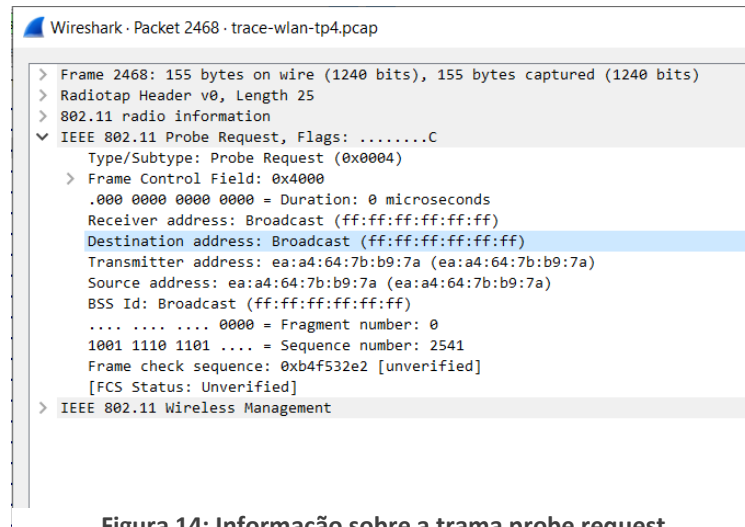
No.	Time	Source	Destination	Protocol	Length	Info
1300	53.746911	Apple_10:6a:f5	Broadcast	802.11	155	Probe Request, SN=2516, FN=0, Flags=.....C, SSID=wildcard (Broadcast)
2467	70.147855	ea:a4:64:7b:b9:7a	Broadcast	802.11	167	Probe Request, SN=2540, FN=0, Flags=.....C, SSID=2WIRE-PT-431
2468	70.149098	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

Figura 13: Filtro probe request e response

De forma a conseguir filtrar todas as tramas de probe request e probe response, utilizamos o filtro da figura 13 (representado a verde):

```
wlan.fc.type_subtype == 4 || wlan.fc.type_subtype == 5
```

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?



**Figura 14: Informação sobre a trama probe request**

São endereçadas para todos os dispositivos na rede local, porque é um endereço de Broadcast, tal como esta representado na figura 14. O envio desta trama é feito quando a STA precisa de obter informações sobre uma outra estação. Esta trama é útil para determinar quais os APs que estão dentro do alcance da STA.

## 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.

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
2487	70.362050	Apple_10:6a:f5	Apple_10:6a:f5 (64:9a...	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 (bc...	HitronTe_af:b1:98 (bc...	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 (64:9a...	Apple_10:6a:f5 (64:9a...	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 (bc...	HitronTe_af:b1:98 (bc...	802.11	39	Acknowledgement, Flags=.....C

Figura 15: Sequencia de tramas de um processo de associação

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

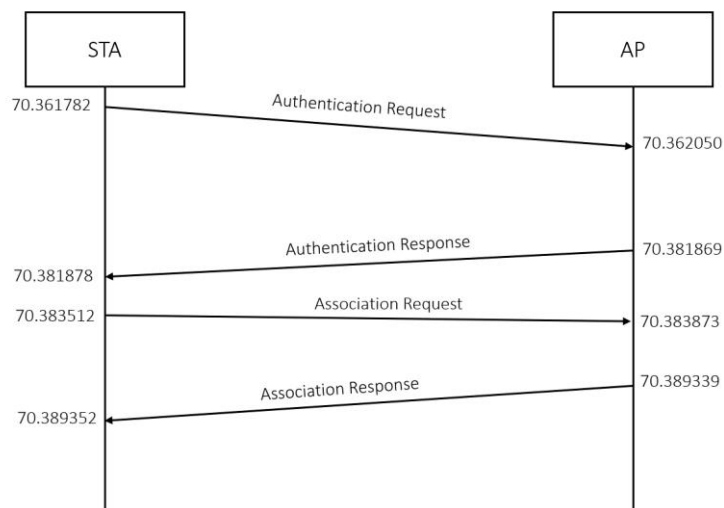


Figura 16: Diagrama do processo de associação

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?

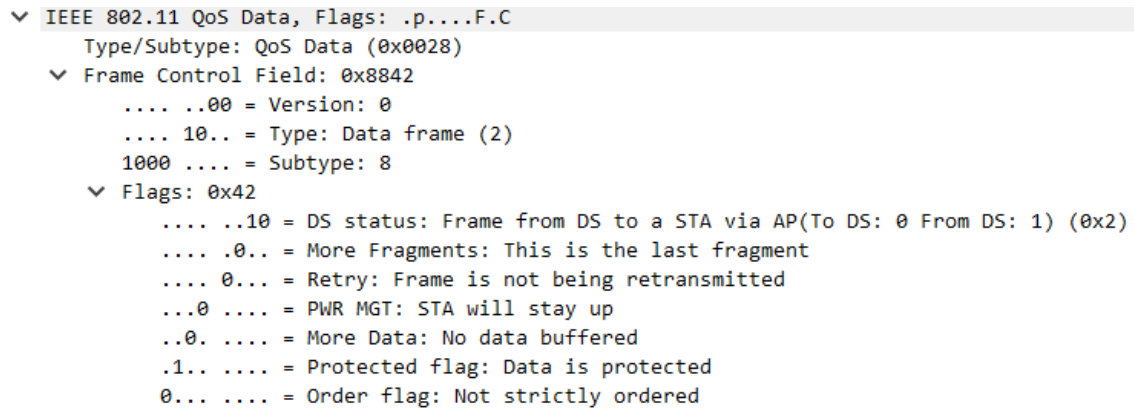


Figura 17: Trama 455 informação relativa à direccionalidade

A direccionalidade é dada pelo campo DS STATUS. Através dos identificadores (To DS e From DS) conseguimos concluir que a trama vem do centro de distribuição (From DS = 1) para o ambiente wireless (To DS = 0) via AP.

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?

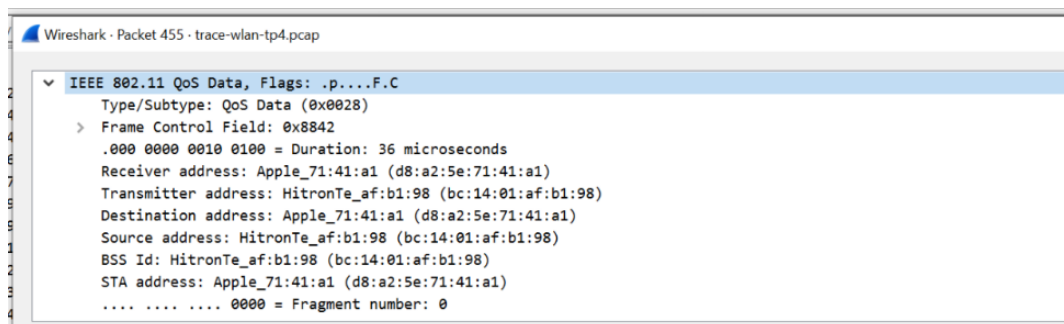


Figura 18: Trama 455

Os endereços MAC em uso são:

- d8:a2:5e:71:41:a1 – correspondente ao *receiver address* e ao *destination address*.
- bc:14:01:af:b1:98 – correspondente ao *transmitter address* e ao *source address* -

O endereço correspondente ao STA (*Apple\_71:41:a1*) é d8:a2:5e:71:41:a1. Já o endereço correspondente ao AP (*HitronTe\_af:b1:98*) é bc:14:01:af:b1:98.

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

O campo da direccionalidade diz que a trama vem do STA para DS via AP. Os endereçamentos são:

Address 1: BSSID

Address 2: origem

Address 3: destino rever

```

▼ IEEE 802.11 QoS Data, Flags: .p.....TC
  Type/Subtype: QoS Data (0x0028)
  ▼ Frame Control Field: 0x8841
    .... ..00 = Version: 0
    .... 10.. = Type: Data frame (2)
    1000 .... = Subtype: 8
  ▼ 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
  
```

**Figura 19: Informação sobre a trama 457**

### 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.)

Os subtipos das tramas de controlo é 8 que identifica o subtipo acknowledgement. Tem de existir subtipos, já que a rede wifi é mais suscetível a falhas e, posto isto, são enviadas tramas de controlo de forma a ver se a informação está a ser enviada corretamente.

No.	Time	Source	Destination	Protocol	Length	Info
455	18.536644	HitronTe_af:b1:98	Apple_71:41:a1	802.11	226	QoS Data, SN=276, FN=0, Flags=.p....F.C
456	18.536653	HitronTe_af:b1:98 (bc...	HitronTe_af:b1:98 (bc...	802.11	39	Acknowledgement, Flags=.....C
457	18.539762	Apple_71:41:a1	HitronTe_af:b1:98	802.11	178	QoS Data, SN=1209, FN=0, Flags=.p....TC
458	18.540043	Apple_71:41:a1 (d8:a2...	Apple_71:41:a1 (d8:a2...	802.11	39	Acknowledgement, Flags=.....C

**Figura 20: Tramas de controlo**

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.

No.	Time	Source	Destination	Protocol	Length	Info
15	0.631114	Apple_10:6a:f5 (64:9a...	HitronTe_af:b1:98 (bc...	802.11	45	Request-to-send, Flags=.....C
16	0.631128		Apple_10:6a:f5 (64:9a...	802.11	39	Clear-to-send, Flags=.....C
17	0.631191	HitronTe_af:b1:98 (bc...	Apple_10:6a:f5 (64:9a...	802.11	57	802.11 Block Ack, Flags=.....C
18	0.631333	HitronTe_af:b1:98 (bc...	Apple_10:6a:f5 (64:9a...	802.11	49	802.11 Block Ack Req, Flags=.....C
19	0.631414	Apple_10:6a:f5 (64:9a...	HitronTe_af:b1:98 (bc...	802.11	57	802.11 Block Ack, Flags=.....C
20	0.631550	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	53	Null function (No data), SN=2488, FN=0, Flags=.....TC
21	0.631595		Apple_10:6a:f5 (64:9a...	802.11	39	Acknowledgement, Flags=.....C
22	0.631709	HitronTe_af:b1:98 (bc...	Apple_10:6a:f5 (64:9a...	802.11	49	802.11 Block Ack Req, Flags=.....C

**Figura 21: Tramas RTS e CTS**

Na trama do exemplo acima (figura 20), a opção RTS/CTS não está a ser usada na troca de dados entre a STA e o AP/Router da Wlan. Contudo, podemos verificar que existem outras tramas que a usam figura 21.

```
> Frame 15: 45 bytes on wire (360 bits), 45 bytes captured (360 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
✓ IEEE 802.11 Request-to-send, Flags: .....C
  Type/Subtype: Request-to-send (0x001b)
  ✓ Frame Control Field: 0xb400
    .... ..00 = Version: 0
    .... 01.. = Type: Control frame (1)
    1011 .... = Subtype: 11
  ✓ Flags: 0x00
    .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
    .... .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.. .... = Protected flag: Data is not protected
    0... .... = Order flag: Not strictly ordered
    .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]
```

**Figura 22: Informação sobre a direccionalidade e o endereçamento RTS**

A direccionalidade da trama RTS, pode ser verificada através do DS status que identifica que esta trama opera em ambiente wireless. Estas tramas são usadas como forma de enviar um pedido para transmissão de mensagens entre o sistema o host e AP.

```

> Frame 16: 39 bytes on wire (312 bits), 39 bytes captured (312 bits)
> 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
    .... 0000 = Version: 0
    .... 01.. = Type: Control frame (1)
    1100 .... = Subtype: 12
    ▼ Flags: 0x000
      .... 0000 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
      .... 00.. = 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.. .... = Protected flag: Data is not protected
      0... .... = Order flag: Not strictly ordered
      .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]

```

**Figura 23: Informação sobre a direcionalidade e endereçamento do CTS**

A direcionalidade da trama CTS, pode ser verificada através do DS status que identifica que esta trama opera em ambiente wireless. Estas tramas são usadas como forma de confirmação da transmissão de mensagens entre o sistema AP e o host.

## CONCLUSÃO

---

Este trabalho prático serviu para aprofundar conceitos e termos já abordados nas aulas teóricas sobre concepções wireless e redes moveis, permitindo assim consolidar a matéria deste capítulo.

Essencialmente foi possível estudar em concreto as redes 802.11 (ou redes wi-fi). Além disso, foram abordados conceitos como os tipos, subtipos e direcionalidade das tramas, STA e AP. Deste modo, foi nos pedido para identificar campos das tramas, assim como os endereços MAC usados para as mesmas. Abordamos o conceito de débitos de AP e periodicidade entre tramas. Verificamos a utilização do método de deteção de erros e trabalhamos com tramas *probing request* e *probing response*. Além disso, conseguimos analisar as fases de autenticação e associação entre um STA e um AP.

Foi também possível aprender e ter uma noção de como usar filtros no WireShark, de forma a podermos obter a informação necessária para responder às questões.

Em suma, com as pesquisas feitas para conseguir obter os filtros aprofundamos os nossos conhecimentos, pois deparamo-nos com inúmeras informações relativas à temática das tramas. Deste modo, temos confiança que conseguimos dar resposta a todas as questões e fazê-lo enquanto expandimos o nosso domínio na área.