

Trabalho Prático 3

Redes de Computadores

PL53

Gonalo Soares^[a93286], Mariana Rodrigues^[a93229], and Rita Teixeira^[a89494]

Universidade do Minho

1 Limitaes na captura de tráfego Wi-Fi

1.1 4. Acesso Rádio

```
▸ Frame 53: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits)
▸ Radiotap Header v0, Length 25
▾ 802.11 radio information
  PHY type: 802.11b (HR/DSSS) (4)
  Short preamble: False
  Data rate: 1.0 Mb/s
  Channel: 12
  Frequency: 2467MHz
  Signal strength (dBm): -60 dBm
  Noise level (dBm): -88 dBm
  Signal/noise ratio (dB): 28 dB
  TSF timestamp: 21645694
  ▸ [Duration: 1632μs]
▸ IEEE 802.11 Beacon frame, Flags: .....C
▸ IEEE 802.11 Wireless Management
```

Figura 1. Radio Information da trama nmero 53

1) Identifique em que frequncia do espectro est a operar a rede sem fios, e o canal que corresponde essa frequncia. Como pode ser observado na figura acima, a frequncia do espectro  a 2467 MHz, e o canal correspondente  o 12.

2) Identifique a verso da norma IEEE 802.11 que est a ser usada. A verso da norma IEEE que se encontra a ser usada  **802.11b (HR/DSSS)**, como pode se visualizar no campo **PHY type**.

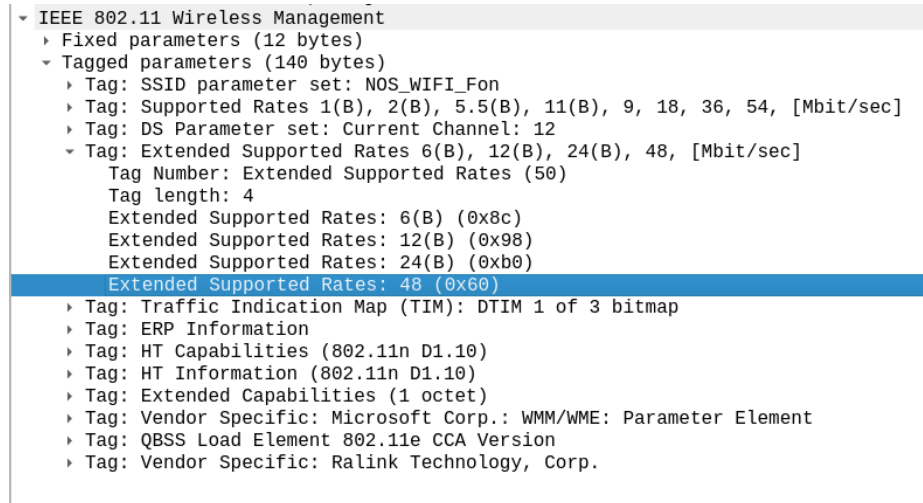


Figura 2. Tagged Parameters da trama nmero 53

3) Qual o dbito a que foi enviada a trama escolhida? Ser que esse dbito corresponde ao dbito mximo a que a interface Wi-Fi pode operar? Justifique. Como pode ser visto na figura 1.1, o dbito da trama  1.0 Mb/s o que no corresponde ao dbito mximo, dado este ser 48Mb/s.

Este dbito no  utilizado para garantir que o beacon chega a todos os hosts, utilizando assim o dbito mais baixo possvel.

1.2 Scanning Passivo e Scanning Ativo

```

▶ Frame 313: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
▶ Radiotap Header v0, Length 25
▼ 802.11 radio information
  PHY type: 802.11b (HR/DSSS) (4)
  Short preamble: False
  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: 32292770
  ▶ [Duration: 2360µs]
▼ 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
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    .... .... 0000 = Fragment number: 0
    1001 0001 0111 .... = Sequence number: 2327
    Frame check sequence: 0xf21b772e [unverified]
    [FCS Status: Unverified]
  ▶ IEEE 802.11 Wireless Management

```

Figura 3. Frame 303

4) Selecione a trama beacon de ordem (260 + XX). 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)? Esta trama pertence ao tipo de *Management Frame*, onde o seu identificador é o 0 (00) e o seu subtipo é o 8 (1000). Estão especificados nos campos Type e Subtype do frame control.

TODO falta os bytes

5) Para a trama acima, identifique todos os endereços MAC em uso. Que conclui quanto à sua origem e destino? Como pode ser confirmado na imagem tanto o *Receiver address*, como para o *Destination address* apresentam o valor Broadcast (ff:ff:ff:ff:ff:ff), ou seja o destino é todos os dispositivos que se encontram na rede wireless. Já ambos os endereços MACs do *Transmitter address* e do *Source address* apresentam o mesmo valor: HitronTe_af:b1:98 (bc:14:01:af:b1:98).

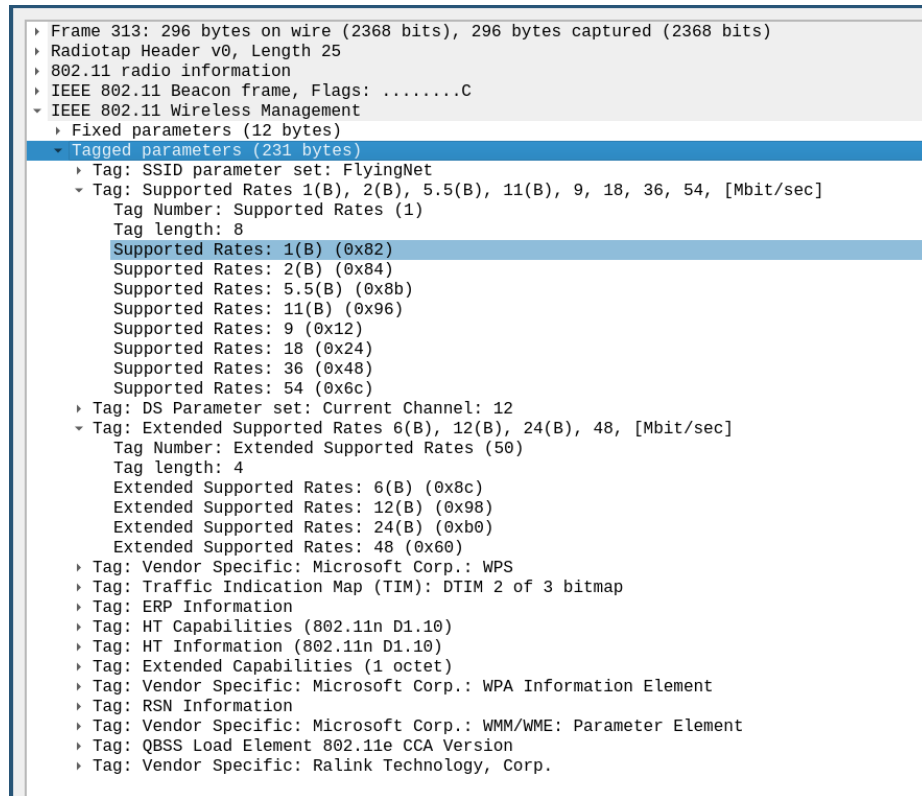


Figura 4. D bitos da trama 313

6) Uma trama beacon anuncia que o AP pode suportar v rios d bitos de base, assim como v rios d bitos adicionais (extended supported rates). Indique quais s o esses d bitos? O AP com o nome *FlyingNet* pode suportar d bitos de base de 1, 2, 5.5, 11, 9, 18, 36 e 54 Mbit/sec.

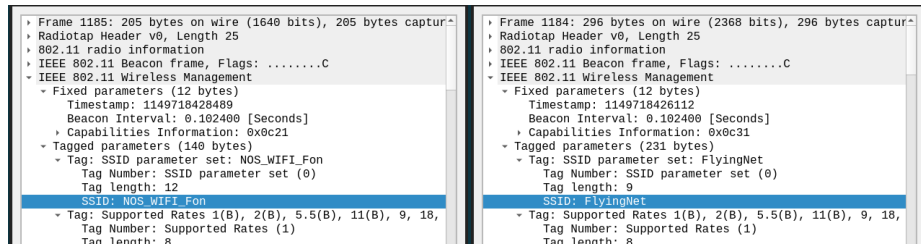


Figura 5. Trama 1185 e 1184

7) 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. Para este exercício resolvemos considerar as tramas 1185 e 1184, que correspondem aos APs de SSID NOS_WIFI_FON e FlyingNet, respectivamente. Como pode ser visto na imagem acima, é de esperar uma periodicidade de 0.102400 segundos. Contudo, esta não se verifica sempre, devido ao congestionamento da rede local nomeadamente na espera para a transmissão quando o meio se encontra ocupado.

wlan.fc.type_subtype==0x8					
No.	Time	Source	Destination	Protocol	Length Info
1	0.000000	HitronTe_af:bl...	Broadcast	802...	296 Beacon frame, SN=2083, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2	0.001662	HitronTe_af:bl...	Broadcast	802...	205 Beacon frame, SN=2084, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
3	0.102552	HitronTe_af:bl...	Broadcast	802...	296 Beacon frame, SN=2085, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
4	0.104164	HitronTe_af:bl...	Broadcast	802...	205 Beacon frame, SN=2086, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
5	0.204951	HitronTe_af:bl...	Broadcast	802...	296 Beacon frame, SN=2087, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
6	0.206582	HitronTe_af:bl...	Broadcast	802...	205 Beacon frame, SN=2088, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
7	0.307368	HitronTe_af:bl...	Broadcast	802...	296 Beacon frame, SN=2089, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
8	0.308999	HitronTe_af:bl...	Broadcast	802...	205 Beacon frame, SN=2090, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
9	0.409749	HitronTe_af:bl...	Broadcast	802...	296 Beacon frame, SN=2091, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
10	0.411376	HitronTe_af:bl...	Broadcast	802...	205 Beacon frame, SN=2092, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
11	0.512117	HitronTe_af:bl...	Broadcast	802...	296 Beacon frame, SN=2093, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Figura 6. Resultado obtido do filtro: wlan.fc.type_subtype==0x8

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). Os SSIDs dos APs que operam na vizinhança são apenas o NOS_WIFI_Fon e o FlyingNet, foi possível obter esta informação usando o filtro: (wlan.fc.type_subtype==0x8).

Para comprovamos que só existem apenas estes dois, fizemos um teste:

No.	Time	Source	Destination	Protocol	Length	Info
13	53.746911	Apple_10:6a:f5	Broadcast	802.11	155	Probe Request, SN=2516, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
24	70.147855	ea:a4:64:7b:b9	Broadcast	802.11	167	Probe Request, SN=2540, FN=0, Flags=.....C, SSID=ZWIRE-PT-431
24	70.149098	ea:a4:64:7b:b9	Broadcast	802.11	155	Probe Request, SN=2541, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
24	70.149792	HitronTe_af:b1	ea:a4:64:7b:b9	802.11	411	Probe Response, SN=2332, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
24	70.150537	HitronTe_af:b1	ea:a4:64:7b:b9	802.11	411	Probe Response, SN=2333, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
24	70.151237	HitronTe_af:b1	ea:a4:64:7b:b9	802.11	411	Probe Response, SN=2334, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
24	70.151709	HitronTe_af:b1	ea:a4:64:7b:b9	802.11	201	Probe Response, SN=2335, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
24	70.152099	HitronTe_af:b1	ea:a4:64:7b:b9	802.11	201	Probe Response, SN=2336, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
24	70.152570	HitronTe_af:b1	ea:a4:64:7b:b9	802.11	201	Probe Response, SN=2337, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
26	72.179215	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2563, FN=0, Flags=.....C, SSID=FlyingNet
26	72.179924	HitronTe_af:b1	Apple_10:6a:f5	802.11	411	Probe Response, SN=2346, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
26	72.180590	HitronTe_af:b1	Apple_10:6a:f5	802.11	411	Probe Response, SN=2347, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
26	72.181275	HitronTe_af:b1	Apple_10:6a:f5	802.11	411	Probe Response, SN=2348, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
26	72.201570	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2565, FN=0, Flags=.....C, SSID=FlyingNet
26	72.202150	HitronTe_af:b1	Apple_10:6a:f5	802.11	411	Probe Response, SN=2350, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
26	72.202807	HitronTe_af:b1	Apple_10:6a:f5	802.11	411	Probe Response, SN=2351, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
26	72.203485	HitronTe_af:b1	Apple_10:6a:f5	802.11	411	Probe Response, SN=2352, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
26	72.480908	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2585, FN=0, Flags=.....C, SSID=FlyingNet
26	72.502553	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2586, FN=0, Flags=.....C, SSID=FlyingNet
26	72.508343	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2589, FN=0, Flags=.....C, SSID=FlyingNet
26	72.782558	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2598, FN=0, Flags=.....C, SSID=FlyingNet
44	82.621343	7c:ea:6d:ff:a2	Broadcast	802.11	71	Probe Request, SN=62, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
44	82.726818	7c:ea:6d:ff:a2	Broadcast	802.11	71	Probe Request, SN=64, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
44	82.728646	7c:ea:6d:ff:a2	Broadcast	802.11	218	Probe Request, SN=65, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
61	94.190800	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
61	94.192095	HitronTe_af:b1	Apple_28:b8:0c	802.11	411	Probe Response, SN=2474, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
61	94.192751	HitronTe_af:b1	Apple_28:b8:0c	802.11	411	Probe Response, SN=2475, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
61	94.193504	HitronTe_af:b1	Apple_28:b8:0c	802.11	411	Probe Response, SN=2476, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
61	94.200286	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
61	94.202330	HitronTe_af:b1	Apple_28:b8:0c	802.11	411	Probe Response, SN=2477, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
61	94.202930	HitronTe_af:b1	Apple_28:b8:0c	802.11	411	Probe Response, SN=2478, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
62	94.203605	HitronTe_af:b1	Apple_28:b8:0c	802.11	411	Probe Response, SN=2479, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
62	94.213697	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
62	94.224724	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
62	94.227944	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
62	94.248503	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
62	94.261777	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
62	94.272579	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
62	94.285744	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
62	94.296433	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
62	94.358606	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
62	94.369617	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
62	94.382980	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
62	94.394120	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
62	94.407423	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
62	94.418665	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet

Figura 9. Filtro aplicado e resultados obtidos

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? Observando a imagem, podemos verificar que a trama 2468 é um *probing request*. Uma STA (ea:a4:64:7b:b9:7), que foi imitada para todos os dispositivos da rede, de modo a encontrar quais os APs que estão dentro do seu alcance rádio. Já a trama 2469, é um *probing response*, ou seja, uma resposta do HitronTe.af:b1:98 (bc:14:01:af:b1:98) para a STA.

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=ZWIRE-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	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	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	802.11	411	Probe Response, SN=2334, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2475	70.151709	HitronTe_af:b1:98	ea:a4:64:7b:b9	802.11	201	Probe Response, SN=2335, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

Figura 10. Probing request e Probing Response

2 Processo de Associao

12) Identifique uma seqncia de tramas que corresponda a um processo de associao completo entre a STA e o AP, incluindo a fase de autenticao. Comeamos por procurar as tramas de autenticao com um filtro visvel na figura a seguir:

wlan.fc.type_subtype == 11					
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
4692	83.663250	7c:ea:6d:ffa2:cc	HitronTe_af:b1:98	802.11	59 Authentication, SN=67, FN=0, Flags=.....C
4694	83.663681	HitronTe_af:b1:98	7c:ea:6d:ffa2:cc	802.11	59 Authentication, SN=2439, FN=0, Flags=.....C
16451	115.725544	fd:31:55:63:20:86	6a:8f:cd:88:f4:55	802.11	146 Authentication, SN=1054, FN=10, Flags=...P....C[Malformed Packet]

Figura 11. Procura de tramas de autenticao

De seguida, optamos por seguir a primeira trama de autenticao:

2484	70.350698	HitronTe_af:b1:99	Broadcast	802.11	205 Beacon frame, SN=3458, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2485	70.352671		Broadcast, 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
2494	70.451472	HitronTe_af:b1:98	Broadcast	802.11	296 Beacon frame, SN=3459, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2495	70.453086	HitronTe_af:b1:99	Broadcast	802.11	205 Beacon frame, SN=3460, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

Figura 12. Processo de associao no wireshark

Na figura a cima, podemos ver o processo de associao a ocorrer antecedido por uma fase de autenticao.

13) Efetue um diagrama que ilustre a seqncia de todas as tramas trocadas no processo. Segue-se o diagrama com a seqncia de tramas trocadas no processo da associao:

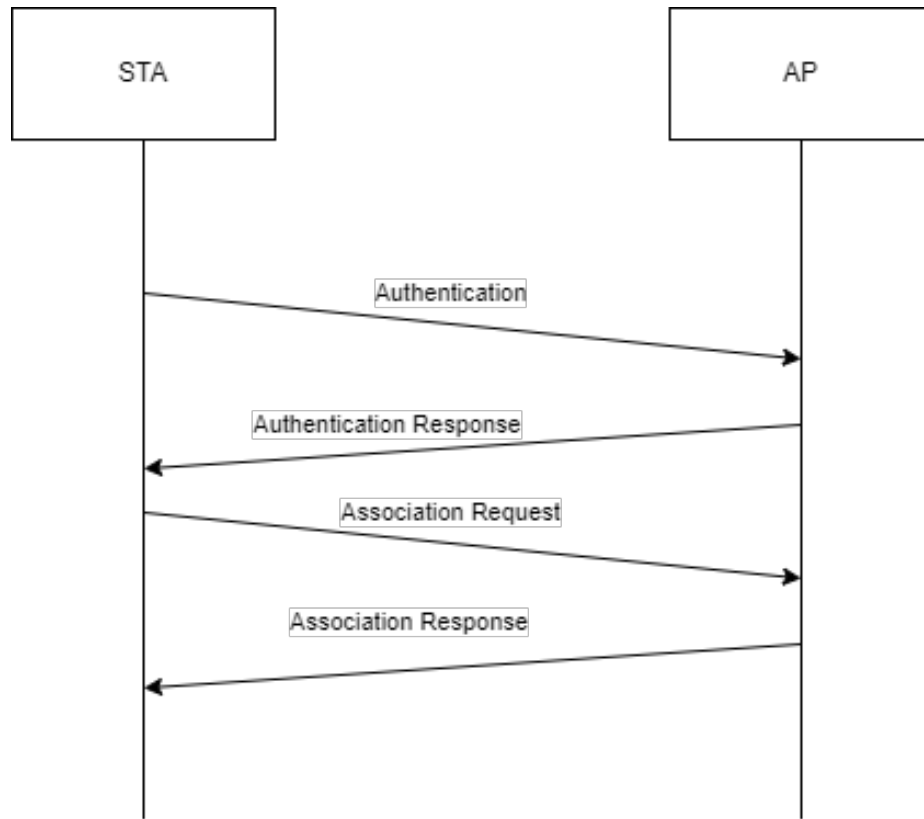


Figura 13. Diagrama do processo de associação

3 Transferência de Dados

14) Considere a trama de dados nº431. 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? Segue-se a direccionalidade obtida da trama de dados nº 431:

Podemos verificar que o campo **To DS** se encontra a 0 e o campo **From DS** a 1. Sendo assim, podemos dizer que a trama não será local à **WLAN**, visto que esta é originada de um DS (*Distribution System*).

```

.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
v 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... .... = +HTC/Order flag: Not strictly ordered

```

Figura 14. Direccionalidade da trama de dados n^o 431

15) Para a trama de dados n^o431, transcreva os endereos MAC em uso, identificando qual o endereo MAC correspondente ao host sem fios (STA), ao AP e ao router de acesso ao sistema de distribuico? Na imagem seguinte podemos ver os endereos obtidos no *Wireshark*.

```

> Frame Control Field: 0x8842
.000 0000 0010 0100 = Duration: 36 microseconds
Receiver address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
Destination address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
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_10:6a:f5 (64:9a:be:10:6a:f5)

```

Figura 15. Endereos MAC da trama n^o 431

Sendo assim, o endereo *MAC* do *STA* seria **64:9a:be:10:6a:f5**. Do *AP* seria **bc:14:01:af:b1:98**. E o *router* de acesso teria o *MAC* **bc:14:01:af:b1:98**. De notar que o *AP* e o router correspondem ao mesmo dispositivo.

16) Como interpreta a trama n^o433 face  sua direccionalidade e en-
dereamento MAC? Segue-se as informaoes relativas  trama n^o 433:

Podemos observar que a trama tem origem no *STA* e  direccional para fora da rede local. Ainda podemos ver que o *Source address* e o *Transmitter address* contem o endereo *MAC* do *STA* e o *Receiver address* e o *Destination address* correspondem ao endereo do AP e do router que neste caso so a mesma mquina.

```

  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... .... = +HTC/Order flag: Not strictly ordered
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Transmitter address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    Destination address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Source address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    STA address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    .... .... 0000 = Fragment number: 0

```

Figura 16. Informações sobre a trama nº 433

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**.) Ao longo da transferência de dados, as tramas de controlo principalmente utilizadas são **Acknowledgment (ACK)**. Estas permitem confirmar a chegada de uma dada trama.

A principal diferença entre um rede 802.11 e uma rede Ethernet é que a gestão de rede **wifi** é bastante mais difícil e complexa. Isto porque, por exemplo, o sinal de radio atenua ao longo da sua propagação e há interferência de frequências usadas por outros dispositivos. Estes problemas não ocorrem em redes **Ethernet**.

18) O uso de tramas Request To Send e Clear To Send, apesar de opcional,   comum para efetuar "pr -reserva" do acesso ao meio quando se pretende enviar tramas de dados, com o intuito de reduzir o n mero de colis es resultante maioritariamente de STAs escondidas. Para o exemplo acima, verifique se est  a ser usada a op  o RTS/CTS na troca de dados entre a STA e o AP/Router da WLAN, identificando a direccionalidade das tramas e os sistemas envolvidos. D  um exemplo de uma transfer ncia de dados em que   usada a op  o RTC/CTS e um outro em que n o   usada. Segue-se um exemplo que utiliza a op  o RTC/CTS:

572	21.687311	HitronTe_af:b1:98 (... Apple_10:6a:f5 (64:... 802.11	45	Request-to-send, Flags=.....C
573	21.687325	HitronTe_af:b1:98 (... 802.11	39	Clear-to-send, Flags=.....C
574	21.687330	HitronTe_af:b1:96 Apple_10:6a:f5 802.11	146	QoS Data, SN=837, FN=0, Flags=.p....F.C

Figura 17. Exemplo de uma transfer ncia com RTC/CTS

De seguida, temos um exemplo que n o utiliza a op  o RTC/CTS:

430	17.922271	Apple_10:6a:f5 (64:... HitronTe_af:b1:98 (... 802.11	57	802.11 Block Ack, Flags=.....C
431	17.922542	HitronTe_af:b1:98 Apple_10:6a:f5 802.11	226	QoS Data, SN=830, FN=0, Flags=.p....F.C
432	17.922558	HitronTe_af:b1:98 (... 802.11	39	Acknowledgement, Flags=.....C
433	17.924985	Apple_10:6a:f5 HitronTe_af:b1:98 802.11	178	QoS Data, SN=3680, FN=0, Flags=.p....TC
434	17.925298	Apple_10:6a:f5 (64:... 802.11	39	Acknowledgement, Flags=.....C

Figura 18. Exemplo de uma transfer ncia sem RTC/CTS

4 Conclus o

Com a realiza  o deste trabalho pr tico tivemos n o s o a oportunidade de explorar os diversos aspetos do protocolo IEEE 802.11, como consolidar a mat ria lecionada nas aulas te ricas.