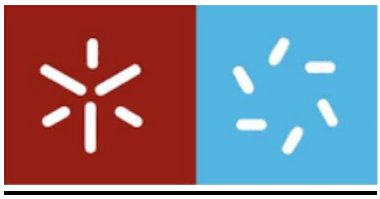


TP3: Redes Sem Fios

João Alves, A91646

Ivo Lima, A90214

Rúben Machado, A91656

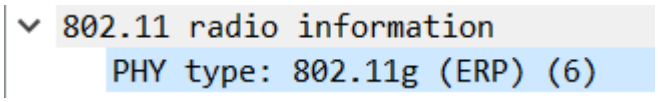
PL5 2º Turno

4. Acesso Rádio

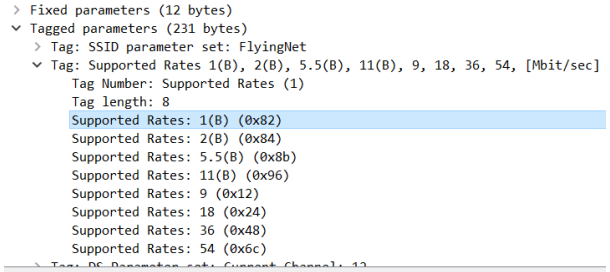
1. A rede sem fios está a operar na frequência 2467MHz que corresponde ao canal 12.

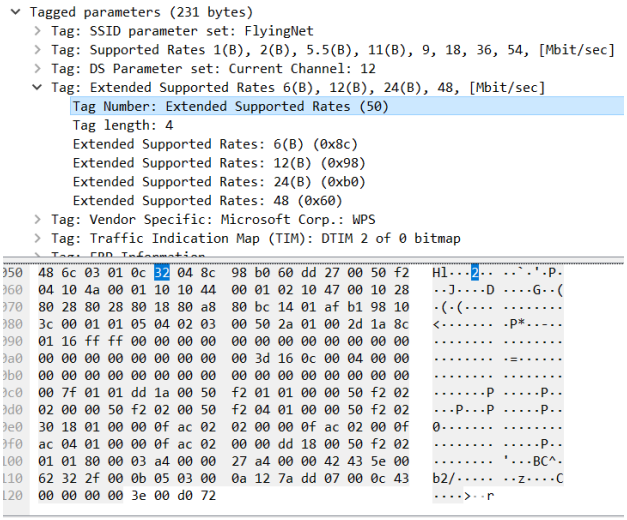
```
> Frame 325: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
> Radiotap Header v0, Length 25
v 802.11 radio information
    PHY type: 802.11g (ERP) (6)
    Short preamble: False
    Proprietary mode: None (0)
    Data rate: 1,0 Mb/s
    Channel: 12
    Frequency: 2467MHz
    Signal strength (dBm): -61dBm
    Noise level (dBm): -87dBm
    Signal/noise ratio (dB): 26dB
    TSF timestamp: 32907166
  > [Duration: 2360µs]
```

2. Trata-se da versão 802.11g.



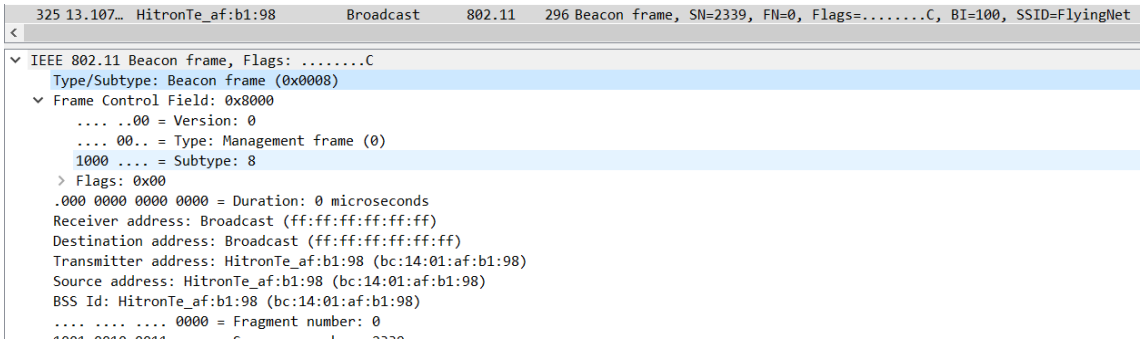
3. O debito a que foi enviada a trama escolhida é 1 Mbit/sec para 0x82. Não, pois o débito máximo a que a interface WiFi pode operar é 50 Mbit/sec.



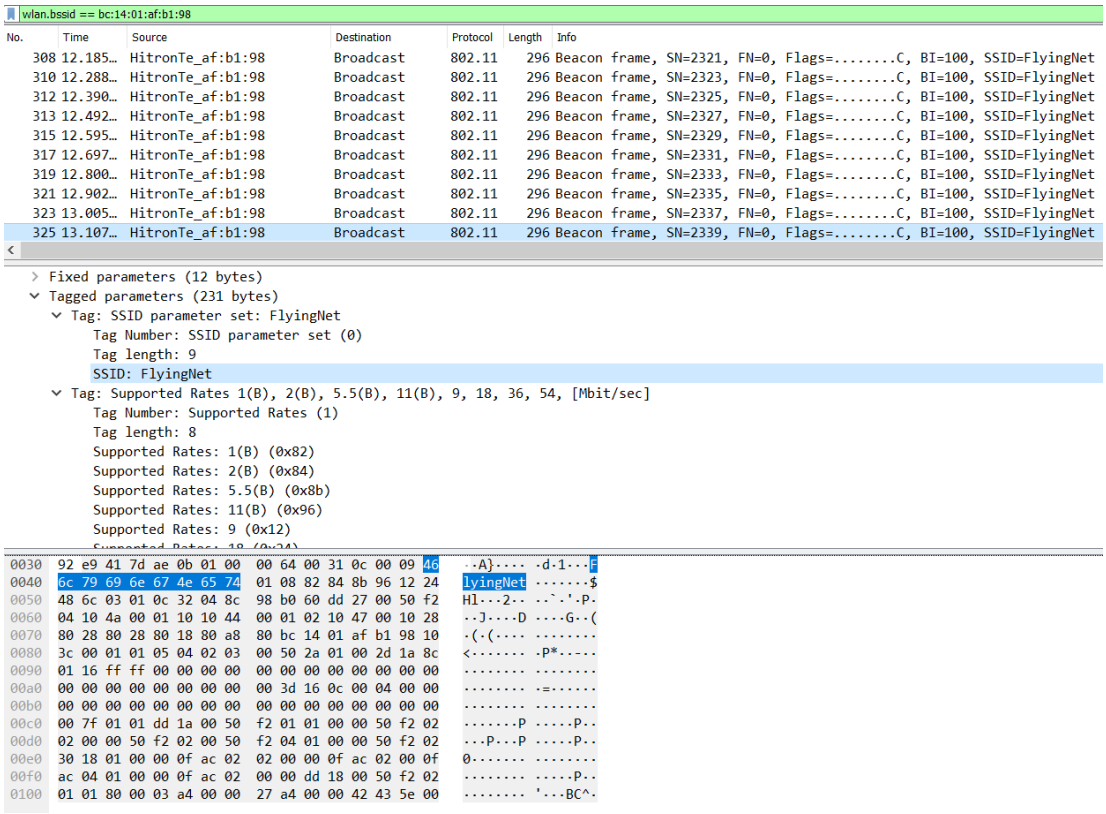


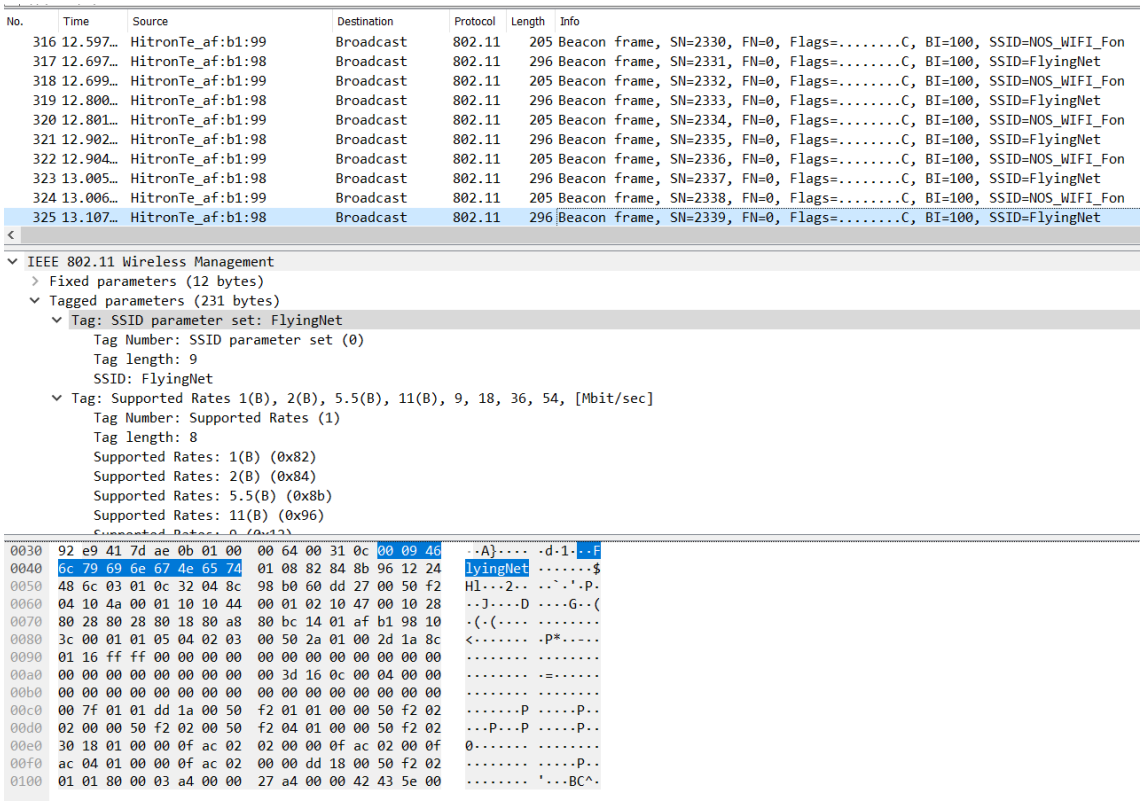
5. Scanning Passivo e Scanning Ativo

4. Sim pertence. O valor do identificador do tipo é 0 e do subtipo é 8. Estão especificados na Management frame.



5. Para construir a nossa resposta utilizamos primeiro um filtro wlan.bssid == bc:14:01:af:b1:98, e depois sem o filtro.





6. O intervalo é de 0.102400 segundos. É verificada, pois a cada 0.102400 segundos ele envia um *beacon*, porém nesta rede contenciosa é necessário competir para ter controlo do acesso, como tal caso ele demore mais tempo a tomar controlo é porque o acesso está ocupado por um anterior e por isso este novo *beacon* terá de esperar.

```
    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 0010 0011 .... = Sequence number: 2339
    Frame check sequence: 0x72d0003e [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 Wireless Management
  ▾ Fixed parameters (12 bytes)
      Timestamp: 1149683712489
      Beacon Interval: 0,102400 [Seconds]
    ▸ Capabilities Information: 0x0c31
  ▸ Tagged parameters (231 bytes)
```

```
0030  92 e9 41 7d ae 0b 01 00  00 64 00 31 0c 00 09 46   ··A}···· ·d·1···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 32 04 8c  98 b0 60 dd 27 00 50 f2   Hl···2·· ··`·'·P·
0060  04 10 4a 00 01 10 10 44  00 01 02 10 47 00 10 28   ··J····D ····G··(
0070  80 28 80 28 80 18 80 a8  80 bc 14 01 af b1 98 10   ·(·(···· ········
0080  3c 00 01 01 05 04 02 03  00 50 2a 01 00 2d 1a 8c   <······ ·P*··-··
0090  01 16 ff ff 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 3d 16 0c 00 04 00 00   ········ ·=······
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 7f 01 01 dd 1a 00 50  f2 01 01 00 00 50 f2 02   ·······P ·····P··
00d0  02 00 00 50 f2 02 00 50  f2 04 01 00 00 50 f2 02   ···P···P ·····P··
00e0  30 18 01 00 00 0f ac 02  02 00 00 0f ac 02 00 0f   0····· ········
00f0  ac 04 01 00 00 0f ac 02  00 00 dd 18 00 50 f2 02   ········ ·····P··
0100  01 01 80 00 03 a4 00 00  27 a4 00 00 42 43 5e 00   ········ '···BC^·
```

7. Temos o endereço ff:ff:ff:ff:ff:ff, o endereço bc:14:01:af:b1:98 e o endereço bc:14:01:af:b1:99.

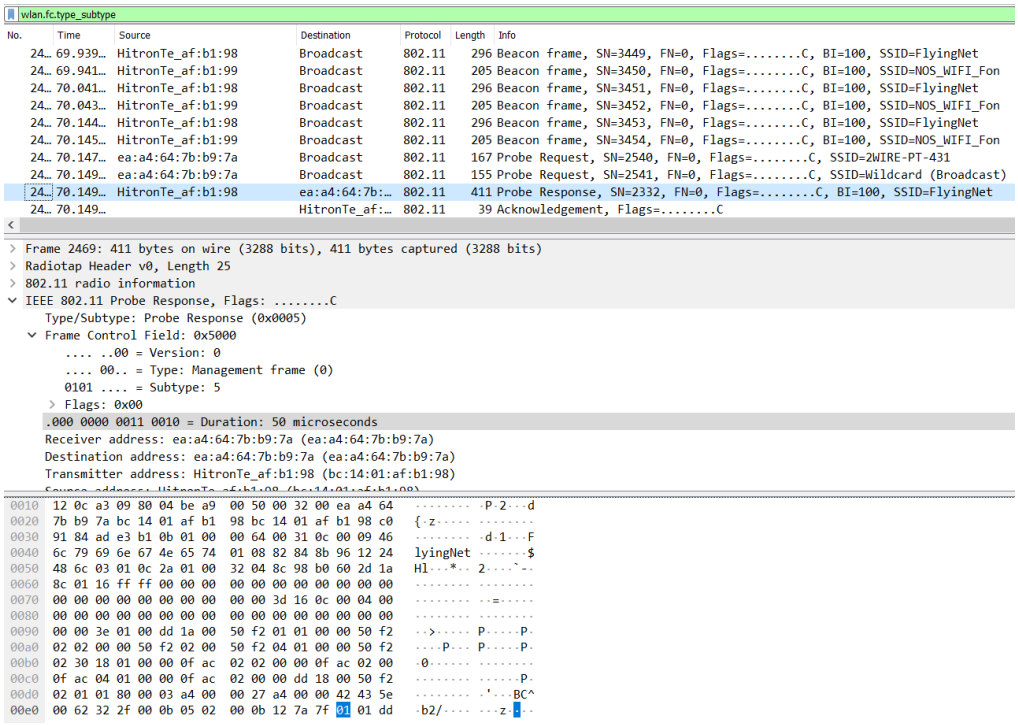
```
  Type/Subtype: Beacon frame (0x0008)
▾ Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
  ▸ Flags: 0x00
  .000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination address: 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 0010 0011 .... = Sequence number: 2339
  Frame check sequence: 0x72d0003e [unverified]
```

```
20  ff ff ff bc 14 01 af b1  98 bc 14 01 af b1 98 30   ·······  ·····0
30  92 e9 41 7d ae 0b 01 00  00 64 00 31 0c 00 09 46   ··A}···· ·d·1···F
40  6c 79 69 6e 67 4e 65 74  01 08 82 84 8b 96 12 24   lyingNet ·······$
50  48 6c 03 01 0c 32 04 8c  98 b0 60 dd 27 00 50 f2   Hl···2·· ··`·'·P·
60  04 10 4a 00 01 10 10 44  00 01 02 10 47 00 10 28   ··J····D ····G··(
70  80 28 80 28 80 18 80 a8  80 bc 14 01 af b1 98 10   ·(·(···· ········
80  3c 00 01 01 05 04 02 03  00 50 2a 01 00 2d 1a 8c   <······ ·P*··-··
90  01 16 ff ff 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
a0  00 00 00 00 00 00 00 00  00 3d 16 0c 00 04 00 00   ········ ·=······
b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
c0  00 7f 01 01 dd 1a 00 50  f2 01 01 00 00 50 f2 02   ·······P ·····P··
d0  02 00 00 50 f2 02 00 50  f2 04 01 00 00 50 f2 02   ···P···P ·····P··
e0  30 18 01 00 00 0f ac 02  02 00 00 0f ac 02 00 0f   0····· ········
f0  ac 04 01 00 00 0f ac 02  00 00 dd 18 00 50 f2 02   ········ ·····P··
```

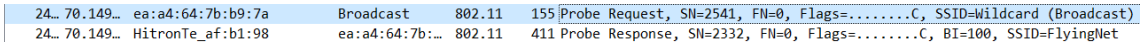
```
  Type/Subtype: Beacon frame (0x0008)
▾ Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
  ▸ Flags: 0x00
  .000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  Transmitter address: HitronTe_af:b1:99 (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
  1001 0010 0010 .... = Sequence number: 2338
  Frame check sequence: 0x5b047da1 [unverified]
```

```
00  00 00 19 00 6f 08 00 00  eb 98 f4 01 00 00 00 00   ····o··· ········
10  10 02 a3 09 80 04 c0 a9  00 80 00 00 00 ff ff ff   ········ ·····
20  ff ff ff bc 14 01 af b1  99 bc 14 01 af b1 99 20   ·······  ····· 
30  92 35 bb 7b ae 0b 01 00  00 64 00 21 0c 00 0c 4e   ·5·{···· ·d·!···N
40  4f 53 5f 57 49 46 49 5f  46 6f 6e 01 08 82 84 8b   OS_WIFI_ Fon·····
50  96 12 24 48 6c 03 01 0c  32 04 8c 98 b0 60 05 05   ··$Hl··· 2····`··
60  00 03 00 4a 01 2a 01 00  2d 1a 8c 01 16 ff ff 00   ···J·*·· -·······
70  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
80  00 00 00 00 3d 16 0c 00  04 00 00 00 00 00 00 00   ····=··· ········
90  00 00 00 00 00 00 00 00  00 00 00 00 7f 01 01 dd   ········ ········
a0  18 00 50 f2 02 01 01 80  00 03 a4 00 00 27 a4 00   ··P····· ·····'··
b0  00 42 43 5e 00 62 32 2f  00 0b 05 03 00 0a 12 7a   ·BC^·b2/ ·······z
c0  dd 07 00 0c 43 00 00 00  00 e1 7d 94 5b            ····C··· ··}·[
```

8. wlan.fc.type_subtype



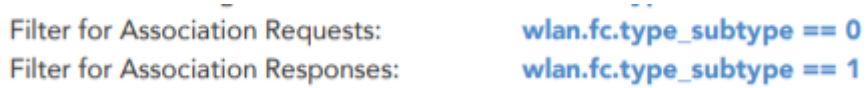
9. wlan.fc.type_subtype == 4 || wlan.fc.type_subtype == 5

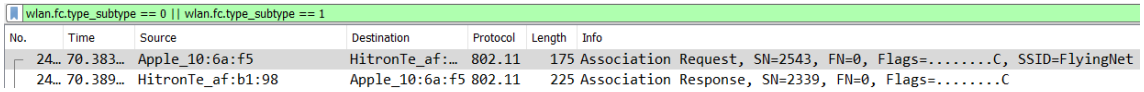


Um *probing request* é um *frame* especial enviado por uma estação cliente ao solicitar informações de qualquer ponto de acesso especificado pelo SSID, ou por todos os pontos de acesso na área especificados com o *Broadcast* SSID.

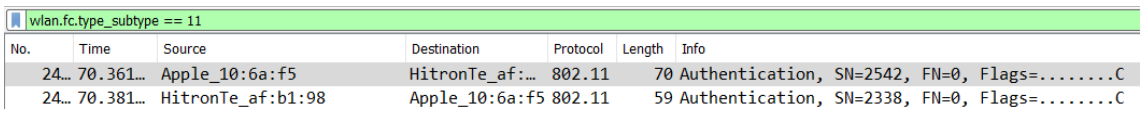
6. Processo de Associação

10.





Filtro para a autenticação (wlan.fc.type_subtype == 11)

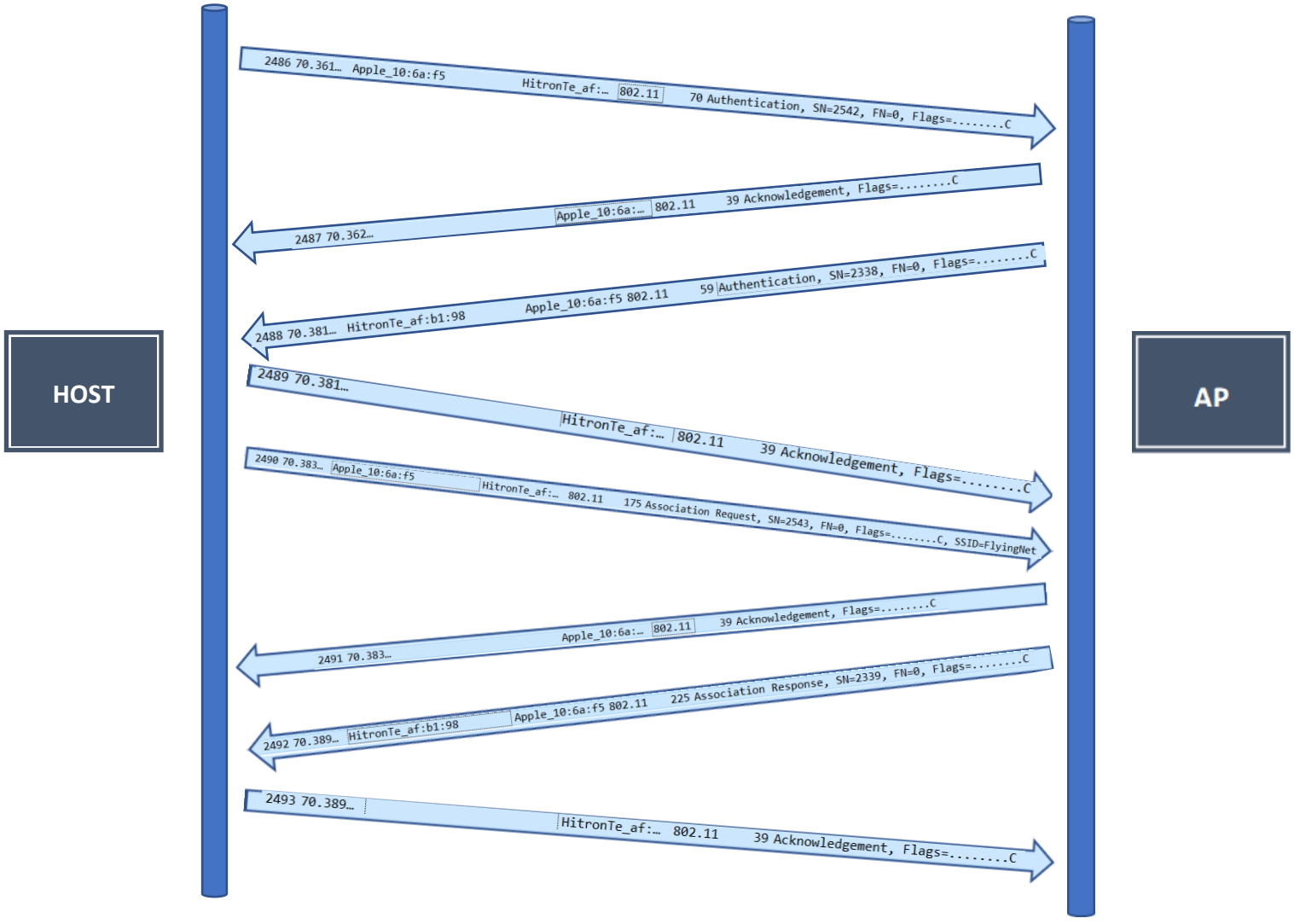


11.

2485	70.352…		Broadcom_04:…	802.11	39 Clear-to-send, Flags=........C
2486	70.361…	Apple_10:6a:f5	HitronTe_af:…	802.11	70 Authentication, SN=2542, FN=0, Flags=........C
2487	70.362…		Apple_10:6a:…	802.11	39 Acknowledgement, Flags=........C
2488	70.381…	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59 Authentication, SN=2338, FN=0, Flags=........C
2489	70.381…		HitronTe_af:…	802.11	39 Acknowledgement, Flags=........C
2490	70.383…	Apple_10:6a:f5	HitronTe_af:…	802.11	175 Association Request, SN=2543, FN=0, Flags=........C, SSID=FlyingNet
2491	70.383…		Apple_10:6a:…	802.11	39 Acknowledgement, Flags=........C
2492	70.389…	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	225 Association Response, SN=2339, FN=0, Flags=........C
2493	70.389…		HitronTe_af:…	802.11	39 Acknowledgement, Flags=........C
2494	70.451…	HitronTe_af:b1:98	Broadcast	802.11	296 Beacon frame, SN=3459, FN=0, Flags=........C, BI=100, SSID=FlyingNet

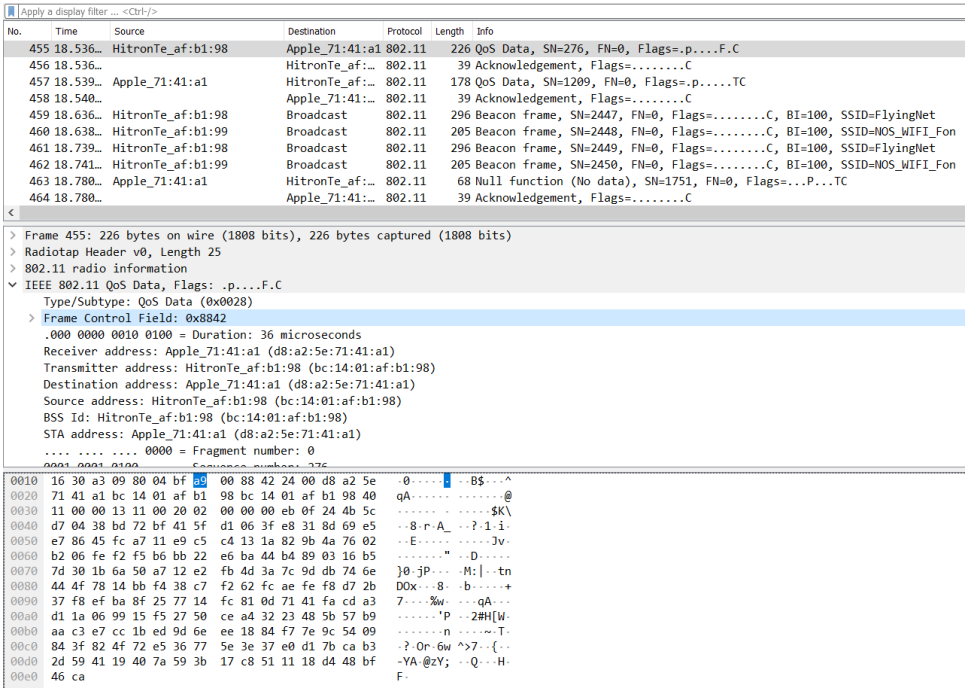
```
Frame 2485: 39 bytes on wire (312 bits), 39 bytes captured (312 bits)
Radiotap Header v0, Length 25
802.11 radio information
IEEE 802.11 Clear-to-send, Flags: ........C
   Type/Subtype: Clear-to-send (0x001c)
▾ Frame Control Field: 0xc400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
      1100 .... = Subtype: 12
   ▸ Flags: 0x00
   .111 0001 0100 1000 = Duration: 29000 microseconds
   Receiver address: Broadcom_04:6a:f5 (e0:3e:44:04:6a:f5)
   Frame check sequence: 0x6b563b07 [unverified]
   [FCS Status: Unverified]
```

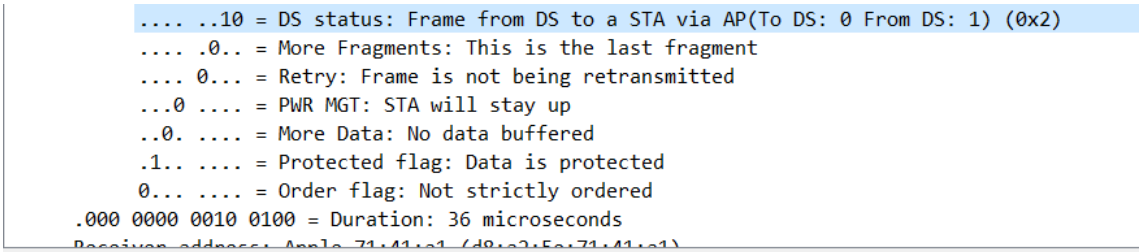
```
00  00 00 19 00 6f 08 00 00  4c a3 5f 05 00 00 00 00    ····o··· L_·····
10  12 0c a3 09 80 04 c9 a8  00 c4 00 48 71 e0 3e 44    ········ ···Hq·>D
20  04 6a f5 07 3b 56 6b                                ·j··;Vk
```

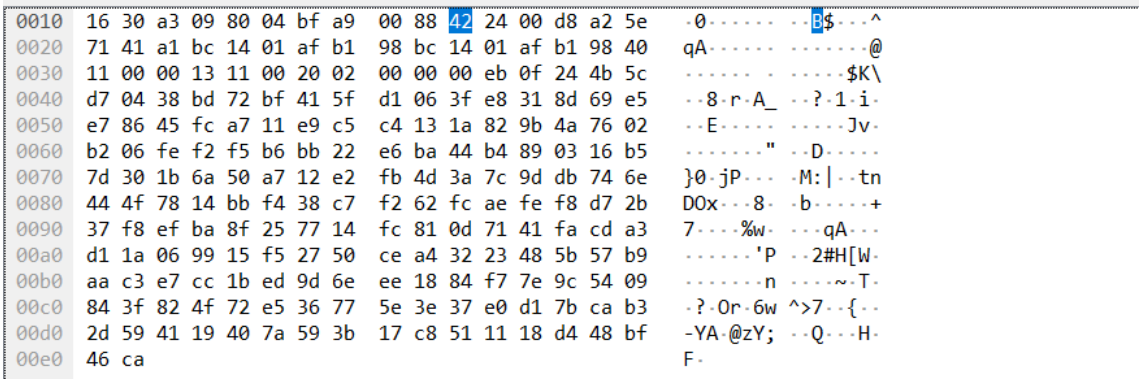


7. Transferência de Dados

12. A partir da direccionalidade desta trama podemos concluir que o *frame* desloca-se do DS para um STA via AP e que é local à WLAN, mas vem de fora.







13.

```
> Frame Control Field: 0x8842
  .000 0000 0010 0100 = Duration: 36 microseconds
  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)
  .... .... .... 0000 = Fragment number: 0
  0001 0001 0100 .... = Sequence number: 276
  Frame check sequence: 0xca46bf48 [unverified]
  [FCS Status: Unverified]
> Qos Control: 0x0000
> CCMP parameters
Data (162 bytes)
```

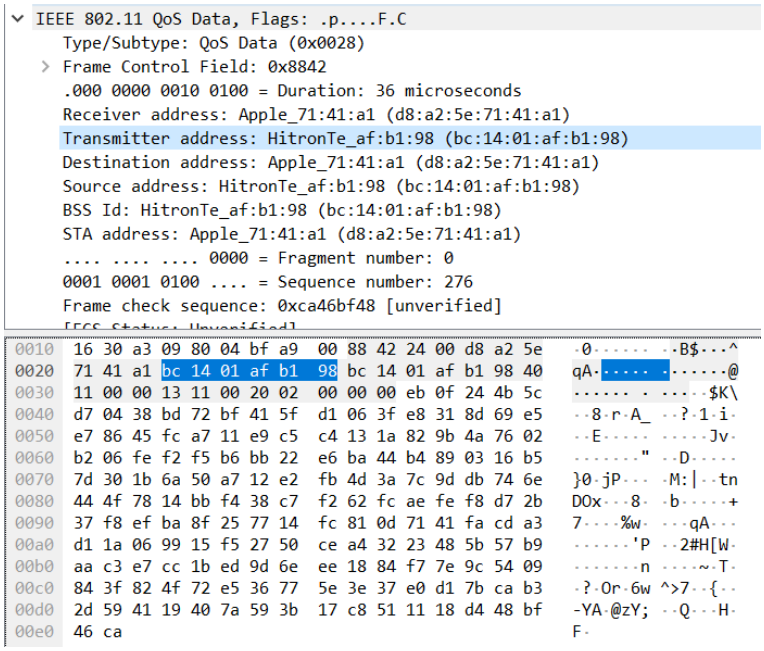
```
0010  16 30 a3 09 80 04 bf a9  00 88 42 24 00 d8 a2 5e   ·0······ ··B$···^
0020  71 41 a1 bc 14 01 af b1  98 bc 14 01 af b1 98 40   qA·····  ·······@
0030  11 00 00 13 11 00 20 02  00 00 00 eb 0f 24 4b 5c   ······ ·  ·····$K\
0040  d7 04 38 bd 72 bf 41 5f  d1 06 3f e8 31 8d 69 e5   ··8·r·A_ ··?·1·i·
0050  e7 86 45 fc a7 11 e9 c5  c4 13 1a 82 9b 4a 76 02   ··E····· ·····Jv·
0060  b2 06 fe f2 f5 b6 bb 22  e6 ba 44 b4 89 03 16 b5   ·······" ··D·····
0070  7d 30 1b 6a 50 a7 12 e2  fb 4d 3a 7c 9d db 74 6e   }0·jP··· ·M:|··tn
0080  44 4f 78 14 bb f4 38 c7  f2 62 fc ae fe f8 d7 2b   DOx···8· ·b·····+
0090  37 f8 ef ba 8f 25 77 14  fc 81 0d 71 41 fa cd a3   7····%w· ···qA···
00a0  d1 1a 06 99 15 f5 27 50  ce a4 32 23 48 5b 57 b9   ·····'P ··2#H[W·
00b0  aa c3 e7 cc 1b ed 9d 6e  ee 18 84 f7 7e 9c 54 09   ·······n ····~·T·
00c0  84 3f 82 4f 72 e5 36 77  5e 3e 37 e0 d1 7b ca b3   ·?·Or·6w ^>7··{··
00d0  2d 59 41 19 40 7a 59 3b  17 c8 51 11 18 d4 48 bf   -YA·@zY; ··Q···H·
00e0  46 ca                                             F·
```

AP

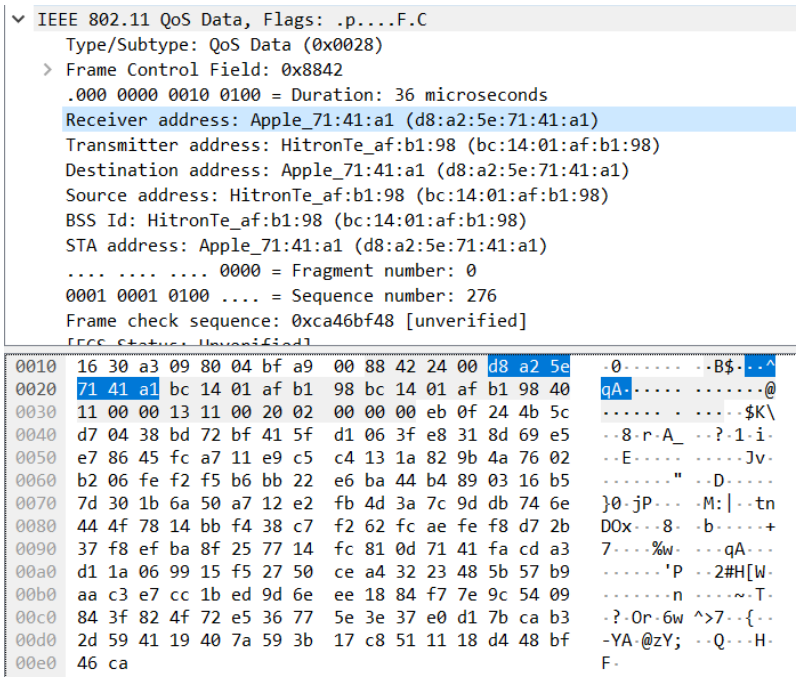
```
v IEEE 802.11 QoS Data, Flags: .p....F.C
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8842
    .000 0000 0010 0100 = Duration: 36 microseconds
    Receiver address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
    Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Destination 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)
    .... .... .... 0000 = Fragment number: 0
    0001 0001 0100 .... = Sequence number: 276
    Frame check sequence: 0xca46bf48 [unverified]
    [FCS Status: Unverified]
```

```
0010  16 30 a3 09 80 04 bf a9  00 88 42 24 00 d8 a2 5e   ·0······ ··B$···^
0020  71 41 a1 bc 14 01 af b1  98 bc 14 01 af b1 98 40   qA·····  ·······@
0030  11 00 00 13 11 00 20 02  00 00 00 eb 0f 24 4b 5c   ······ ·  ·····$K\
0040  d7 04 38 bd 72 bf 41 5f  d1 06 3f e8 31 8d 69 e5   ··8·r·A_ ··?·1·i·
0050  e7 86 45 fc a7 11 e9 c5  c4 13 1a 82 9b 4a 76 02   ··E····· ·····Jv·
0060  b2 06 fe f2 f5 b6 bb 22  e6 ba 44 b4 89 03 16 b5   ·······" ··D·····
0070  7d 30 1b 6a 50 a7 12 e2  fb 4d 3a 7c 9d db 74 6e   }0·jP··· ·M:|··tn
0080  44 4f 78 14 bb f4 38 c7  f2 62 fc ae fe f8 d7 2b   DOx···8· ·b·····+
0090  37 f8 ef ba 8f 25 77 14  fc 81 0d 71 41 fa cd a3   7····%w· ···qA···
00a0  d1 1a 06 99 15 f5 27 50  ce a4 32 23 48 5b 57 b9   ·····'P ··2#H[W·
00b0  aa c3 e7 cc 1b ed 9d 6e  ee 18 84 f7 7e 9c 54 09   ·······n ····~·T·
00c0  84 3f 82 4f 72 e5 36 77  5e 3e 37 e0 d1 7b ca b3   ·?·Or·6w ^>7··{··
00d0  2d 59 41 19 40 7a 59 3b  17 c8 51 11 18 d4 48 bf   -YA·@zY; ··Q···H·
00e0  46 ca                                             F·
```

MAC do router de acesso ao sistema de distribuição (DS)

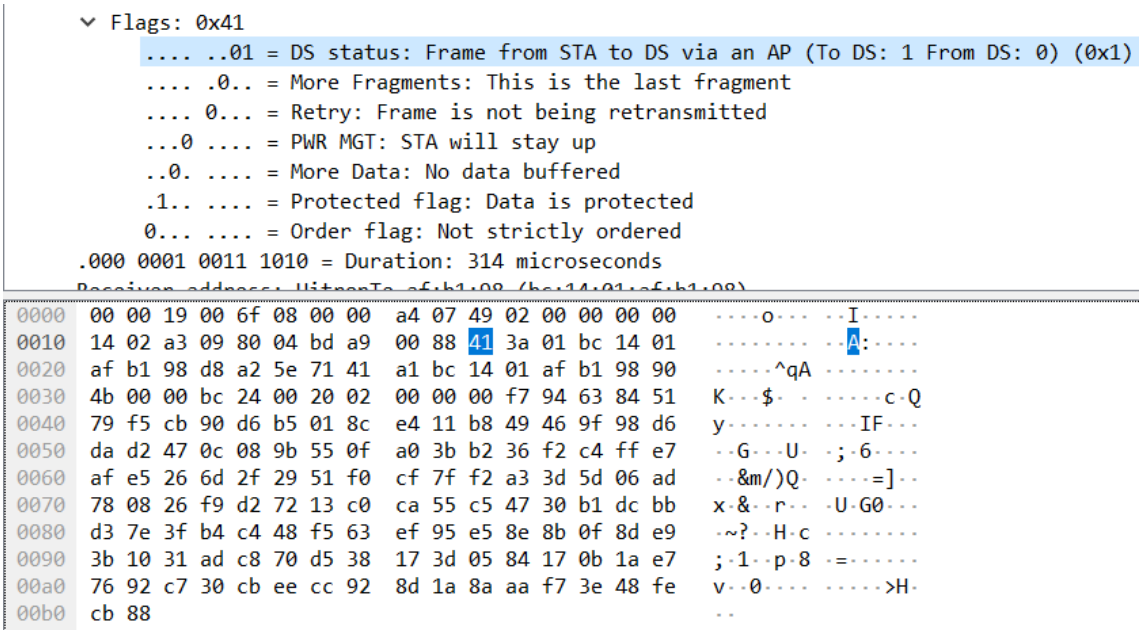


MAC do *host* sem fios



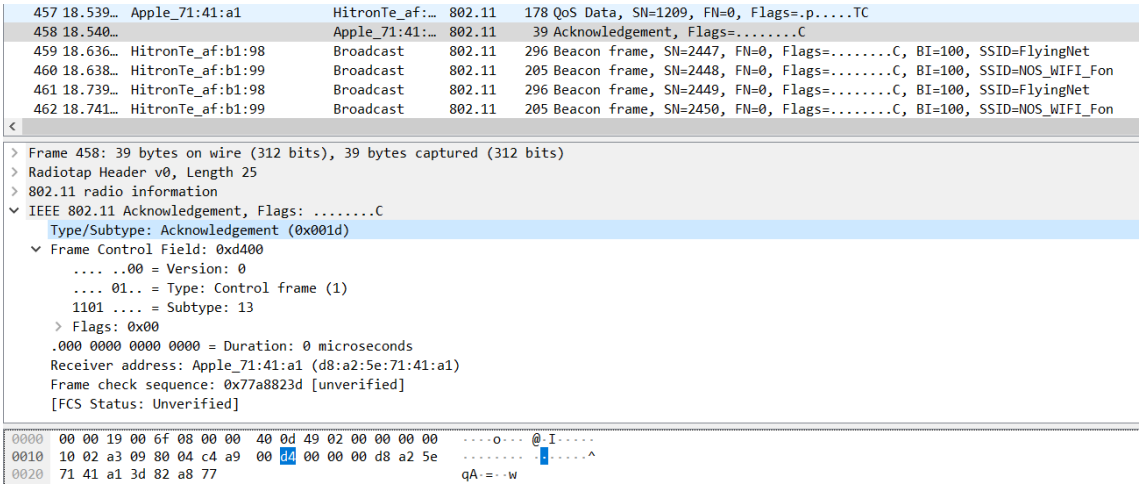
A partir do facto de que só estão dois endereços MAC diferentes em uso podemos concluir que apenas o router de acesso e o *host* sem fios participam na trama, fazendo o router papel de DS e AP.

14. A direccionalidade da trama é do STA para o DS através de um AP.

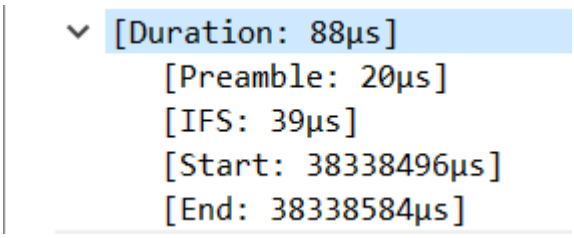


Sendo o MAC do router do DS: 00:11:22:33:44:55:66:77, temos que o AP fica com o DS anterior: bc:14:01:af:b1:98; e o MAC do *host* permanecem d8:a2:5e:71:41:a1.

15. O subtipo de tramas é *Acknowledgement*. A razão pela qual têm de existir é porque é um meio Wifi (e não Ethernet) suscetível a erros.



16. Sim está a ser usada a opção RTS/CTS, pois existe um compasso de espera característico desta opção.



Conclusão

Após a realização deste trabalho, o nosso grupo aprofundou os conhecimentos à cerca dos tópicos propostos, nomeadamente: o formato das tramas, o endereçamento dos componentes envolvidos na comunicação sem fios, os tipos de tramas mais comuns, bem como a operação do protocolo. Como tal adquirimos uma maior aptidão tanto a nível teórico como a nível prático. Com o auxílio do *Wireshark*, exploramos as diferentes matérias, referidas anteriormente, adquirindo os diversos conhecimentos de forma interativa. Desta forma, este trabalho prático promoveu uma experiência útil e enriquecedora que nos proporcionou uma melhor compreensão das matérias lecionadas.