



TP4: Redes Sem Fios (802.11)

Redes de Computadores

Grupo 1 – PL4



Ana Pereira A81712



Ana Ribeiro A82474



Jéssica Lemos A82061

1 Questões e Respostas

4 Acesso Rádio

```
> Frame 341: 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 (6)
  Short preamble: False
  Proprietary mode: None (0)
  Data rate: 1.0 Mb/s
  Channel: 12
  Frequency: 2467MHz
  Signal strength (dBm): -64dBm
  Noise level (dBm): -87dBm
  TSF timestamp: 33726363
  > [Duration: 2360µs]
> IEEE 802.11 Beacon frame, Flags: .....C
> IEEE 802.11 wireless LAN
```

Figura 1 - Radio Information da trama 341

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

Como podemos observar na Figura 1, a frequência do espectro que está a operar na rede sem fios é 2467MHz, o que corresponde ao canal 12.

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

A versão da norma que está a ser utilizada é a 802.11g, como podemos visualizar no campo *PHY type* na Figura 1.

- 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.

```
v Tagged parameters (231 bytes)
  > 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
  v 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 2 - Extended Supported Rates da trama 341

Na Figura 1 podemos verificar que o débito de envio é 1.0Mb/s, o que não corresponde ao débito máximo teórico, dado que esse é 48Mb/s, como podemos constatar na Figura 2.

5 Scanning Passivo e Scanning Ativo

- 4) Selecione uma trama beacon (e.g., a trama 3XX). 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)?

```

> Frame 341: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
  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 0011 0011 .... = Sequence number: 2355
    Frame check sequence: 0xe676d70b [correct]
    [FCS Status: Good]
  IEEE 802.11 wireless LAN

```

Figura 3 – Tipo da trama 341

Esta trama corresponde a uma trama de gestão (Management type), como podemos visualizar na Figura 3 no campo *Type*. O seu identificador de tipo é 0 (0x00) e o de subtipo 8 (0x1000). É também possível observar que esta informação se encontra no byte 25 da trama.

- 5) Liste todos os SSIDs dos APs (Access Points) que estão a operar na vizinhança da STA de captura? Explícite o modo como obteve essa informação. Como sugestão pode construir um filtro de visualização apropriado (tomando como base a resposta da alínea anterior) que lhe permita obter a listagem pretendida.

Começamos por elaborar um filtro de visualização apropriado. Tendo em conta que as *beacon frames* apresentam *Type/Subtype* com valor 0x0008, chegamos ao filtro *wlan.fc.type_subtype==0x8*.

No.	Time	Source	Destination	Protocol	Length	Info
337	13.721800	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2351, FH=0, Flags=.....C, BI=100, SSID=Flyinglet
338	13.723430	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2352, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
339	13.824206	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2353, FH=0, Flags=.....C, BI=100, SSID=Flyinglet
340	13.825838	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2354, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
341	13.926596	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2355, FH=0, Flags=.....C, BI=100, SSID=Flyinglet
342	13.928225	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2356, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
343	14.028868	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2357, FH=0, Flags=.....C, BI=100, SSID=Flyinglet
344	14.030499	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2358, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
345	14.131398	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2359, FH=0, Flags=.....C, BI=100, SSID=Flyinglet
346	14.133029	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2360, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
347	14.233824	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2361, FH=0, Flags=.....C, BI=100, SSID=Flyinglet
348	14.235456	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2362, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
349	14.336138	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2363, FH=0, Flags=.....C, BI=100, SSID=Flyinglet
350	14.337754	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2364, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
351	14.438603	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2365, FH=0, Flags=.....C, BI=100, SSID=Flyinglet
352	14.440234	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2366, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
353	14.540874	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2367, FH=0, Flags=.....C, BI=100, SSID=Flyinglet
354	14.542494	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2368, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
355	14.643405	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2369, FH=0, Flags=.....C, BI=100, SSID=Flyinglet
356	14.645055	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2370, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

Figura 4 – Resultado da aplicação do filtro elaborado

```

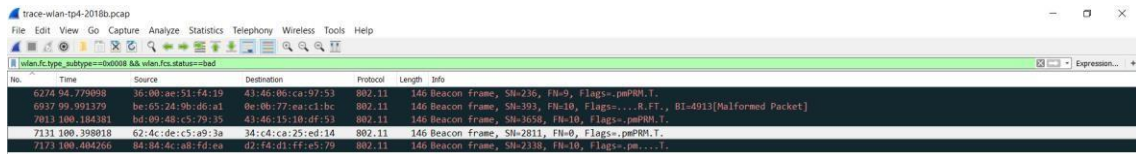
> Frame 341: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
  IEEE 802.11 Beacon frame, Flags: .....C
    IEEE 802.11 wireless LAN
      Fixed parameters (12 bytes)
      Tagged parameters (231 bytes)
        Tag: SSID parameter set: Flyinglet
          Tag Number: SSID parameter set (0)
          Tag length: 9
          SSID: Flyinglet
        Tag: Supported Rates 1(0), 2(0), 5.5(0), 11(0), 9, 18, 36, 54, [Mbit/sec]
        Tag: DS Parameter set: Current Channel: 12
        Tag: Extended Supported Rates 6(0), 12(0), 24(0), 48, [Mbit/sec]
        Tag: Vendor Specific: Microsoft Corp.: WPS
        Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
        Tag: ERP Information
        Tag: HT Capabilities (802.11n D1.10)
        Tag: HT Information (802.11n D1.10)

```

Figura 5 - SSID da trama 341

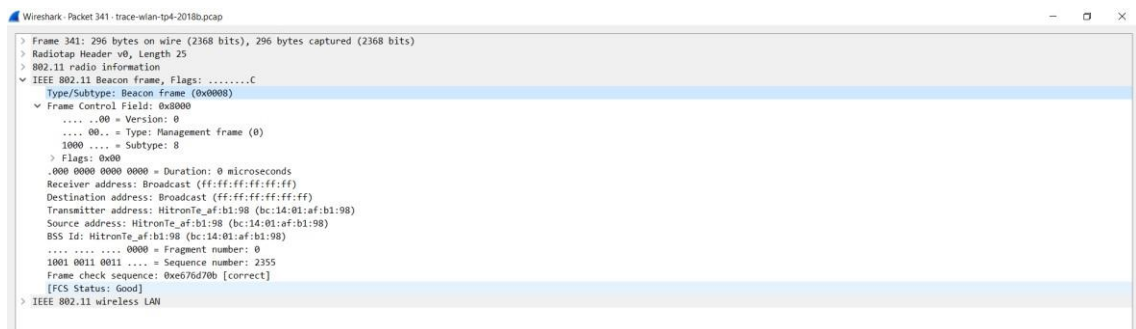
Assim, é possível verificar na Figura 4 os pontos de acesso de SSID que se encontram na vizinhança da trama apresentada na Figura 5. Assim, os SSIDs dos APs que estão a operar na vizinhança da STA de captura são: FlyingNet e NOS_WIFI_Fon.

- 6) Verifique se está a ser usado o método de deteção de erros (CRC), e se todas as tramas Beacon são recebidas corretamente. Justifique o porquê de usar deteção de erros neste tipo de redes locais.



No.	Time	Source	Destination	Protocol	Length	Info
6274	0.7778996	2:80:00:00:00:00	ca:92:53:53	802.11	146	Beacon frame, SN=236, FN=0, Flags=pmPRL.T.
6937	99.991379	bc:65:24:9b:d6:a1	0e:0b:77:ea:c1:bc	802.11	146	Beacon frame, SN=393, FN=10, Flags=...R.FT., B1=4911[Malformed Packet]
7011	100.184381	bd:09:48:c5:79:35	43:46:15:10:df:53	802.11	146	Beacon frame, SN=3658, FN=10, Flags=pmPRL.T.
7131	100.398018	62:4c:dc:c5:a9:3a	34:c4:ca:25:ed:14	802.11	146	Beacon frame, SN=2811, FN=0, Flags=pmPRL.T.
7173	100.404266	88:88:4c:a8:fd:ea	d2:f4:d1:ff:e5:79	802.11	146	Beacon frame, SN=2338, FN=10, Flags=pm...T.

Figura 6 - Resultado da aplicação do filtro elaborado



```

> Frame 341: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
  > 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: HltronTe_af:b1:98 (bc:14:01:af:b1:98)
      Source address: HltronTe_af:b1:98 (bc:14:01:af:b1:98)
      BSS Id: HltronTe_af:b1:98 (bc:14:01:af:b1:98)
      .... ..0000 = Fragment number: 0
      1001 0011 0011 .... = Sequence number: 2355
      Frame check sequence: 0xe676d70b [correct]
      [FCS Status: Good]
    > IEEE 802.11 wireless LAN
  
```

Figura 7 - Trama Beacon sem erros



```

> Frame 7131: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits)
> Radiotap Header v0, Length 40
> 802.11 radio information
  > IEEE 802.11 Beacon frame, Flags: ..pmPRL.T.
    Type/Subtype: Beacon frame (0x0008)
    > Frame Control Field: 0x827d
      .... ..10 = Version: 2
      .... ..00.. = Type: Management frame (0)
      1000 .... = Subtype: 8
    > Flags: 0x7d
      Duration/ID: 7292 (reserved)
      Receiver address: 34:c4:ca:25:ed:14 (34:c4:ca:25:ed:14)
      Destination address: 34:c4:ca:25:ed:14 (34:c4:ca:25:ed:14)
      Transmitter address: 62:4c:dc:c5:a9:3a (62:4c:dc:c5:a9:3a)
      Source address: 62:4c:dc:c5:a9:3a (62:4c:dc:c5:a9:3a)
      BSS Id: 55:0e:b7:95:b0:54 (55:0e:b7:95:b0:54)
      STA address: 62:4c:dc:c5:a9:3a (62:4c:dc:c5:a9:3a)
      .... ..0000 = Fragment number: 0
      1010 1111 1011 .... = Sequence number: 2811
    > Frame check sequence: 0x20c0c0c0 [incorrect, should be 0x7d318e93]
    [FCS Status: Bad]
    > TKIP/CCMP parameters
    > Data (70 bytes)
      Data: f7f4855b6ce52aea9ff4547410fc766b75247ca4a1580639...
      [Length: 70]
  
```

Figura 8 - Trama Beacon com erros

Começamos por elaborar um filtro, `wlan.fc.type_subtype==0x0008 && wlan.fc.status==bad`, de modo a poder concluir se todas as tramas Beacon são recebidas corretamente. Como podemos observar na Figura 6, nem todas são recebidas corretamente. Sendo de destacar a diferença entre uma trama Beacon com erros, Figura 8, e uma trama sem erros, Figura 7. Como podemos verificar nas figuras anteriormente apresentadas, no campo *Frame check sequence*, é usado o método de deteção de erros (CRC).

A deteção de erros é fundamental neste tipo de redes locais uma vez que a probabilidade de existirem colisões é considerável. É de notar que este método de deteção de erros é de fácil implementação.

- 7) Para dois dos APs identificados, indique qual é 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 é verificada? Tente explicar porquê.

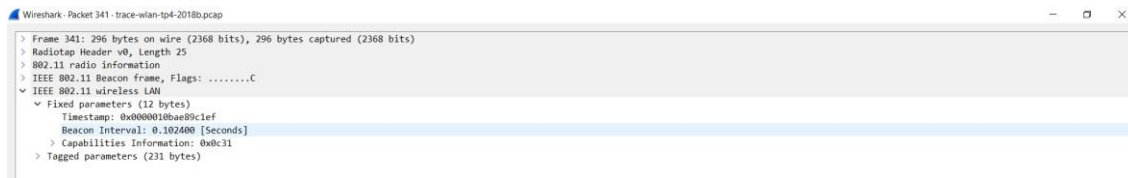


Figura 9 - Beacon interval da trama 341

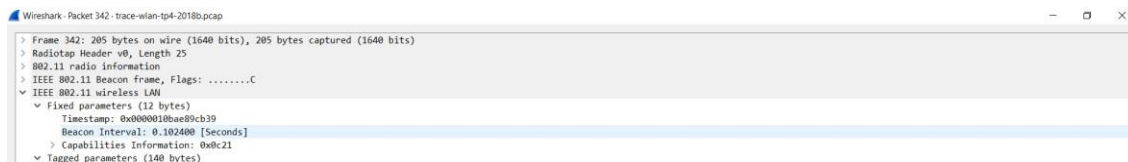


Figura 10 - Beacon interval da trama 342

Consideremos as tramas 341 e 342, que correspondem aos APs de SSID FlyingNet e NOS_WIFI_Fon, respetivamente. Como podemos constatar nas Figuras 9 e 10, é de esperar uma periodicidade de 0.102400 segundos. Contudo, esta não se verifica sempre. Por exemplo, escolhendo as tramas 341 e 343, ambas com AP de SSID FlyingNet, temos $14.02886813.926596 = 0.102272$. Este valor não varia muito uma vez que o tráfego não é elevado contudo, neste tipo de ligações existe maior suscetibilidade a interferências externas, existindo também atenuação do sinal pelo que é difícil ser atingida a periodicidade.

- 8) Identifique e registe todos os endereços MAC usados nas tramas *beacon* enviadas pelos APs. Recorde que o endereçamento está definido no cabeçalho das tramas 802.11, podendo ser utilizados até quatro endereços com diferente semântica. Para uma descrição detalhada da estrutura da trama 802.11, consulte o anexo ao enunciado.**

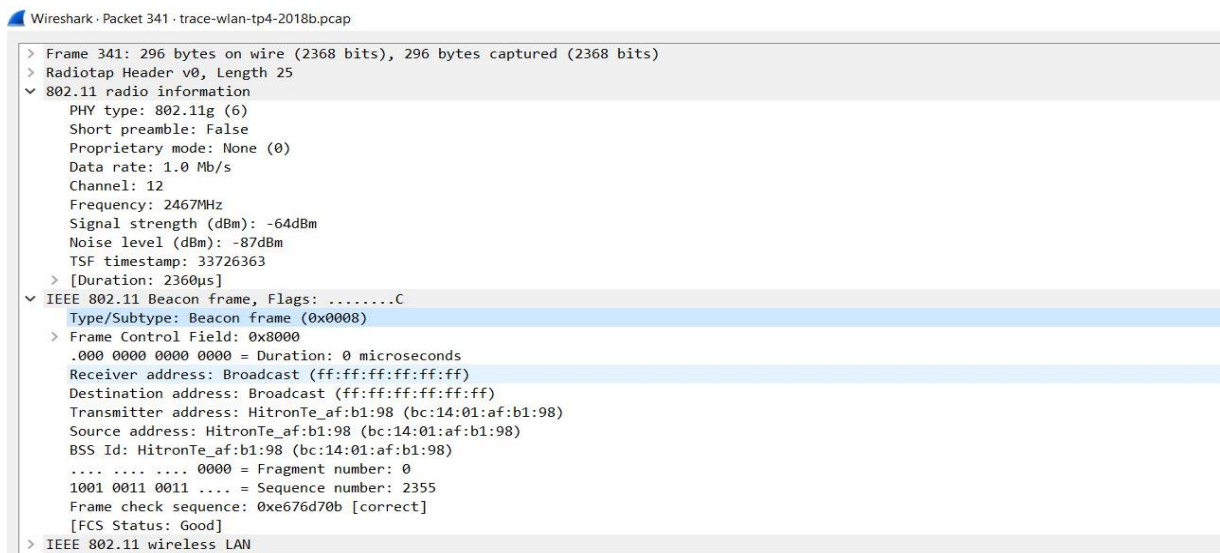


Figura 11 - Trama 341


```
Wireshark · Packet 342 · trace-wlan-tp4-2018b.pcap
> Frame 342: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
  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
      1001 0011 0100 .... = Sequence number: 2356
      Frame check sequence: 0xc7f89cea [correct]
      [FCS Status: Good]
    > IEEE 802.11 wireless LAN
```

Figura 12 - Trama 342

Nas tramas beacon enviadas pelos APs estão presentes quatro endereços: o *Receiver Address*, o *Destination Address*, o *Transmitter Address* e o *Source Address*. Para todos os SSID o *Receiver Address* e o *Destination Address* têm o valor de ff:ff:ff:ff:ff:ff (Broadcast) como podemos verificar nas Figuras 11 e 12. Podemos também observar que o endereço MAC do *Transmitter Address* e do *Source Address* são idênticos, tomando os valores bc:14:01:af:b1:98 e bc:14:01:af:b1:99 para as tramas 341 e 342, respectivamente.

9) As tramas *beacon* anunciam que o AP pode suportar vários débitos de base assim como vários “*extended supported rates*”. Indique quais são esses débitos?

```
Wireshark · Packet 341 · trace-wlan-tp4-2018b.pcap
> Frame 341: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
  IEEE 802.11 Beacon frame, Flags: .....C
    IEEE 802.11 wireless LAN
      > Fixed parameters (12 bytes)
      > Tagged parameters (231 bytes)
        > Tag: SSID parameter set: FlyingNet
        > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
          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
        > 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)
        > Tag: Vendor Specific: Microsoft Corp.: WPS
        > Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
        > Tag: ERP Information
```

Figura 13 - Débitos da trama 341

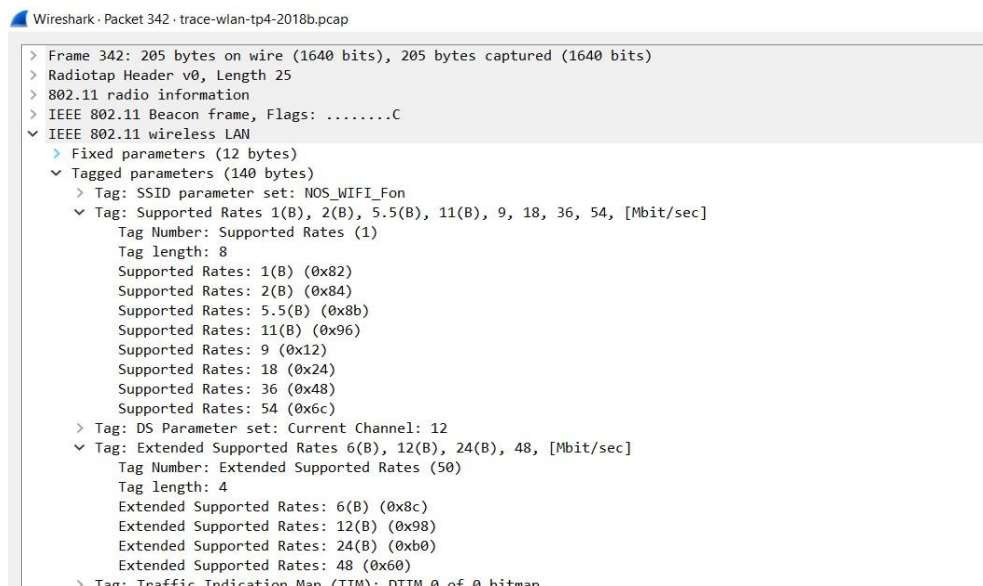


Figura 14 - Débitos da trama 342

O AP com SSID FlyingNet (trama 341) pode suportar débitos de base de 1 até 54 Mbs e extended supported rates de 6 até 48 Mbs, como podemos observar na Figura 13. Conseguimos constatar através da Figura 14 que o AP com SSID NOS_WIFI_ZON (trama 342) apresenta exatamente os mesmos débitos.

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

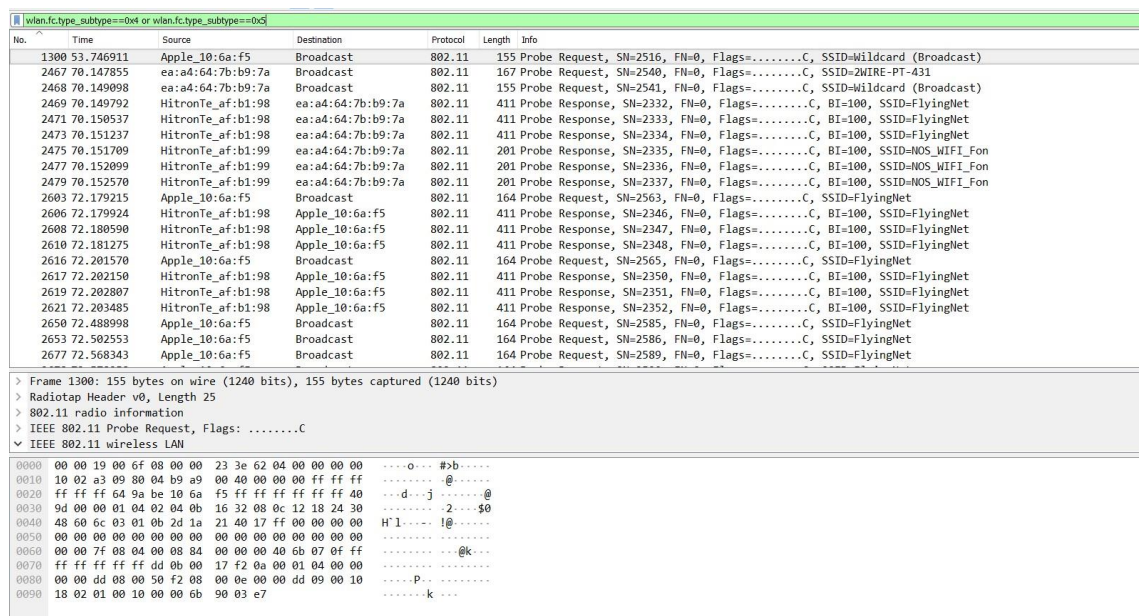


Figura 15 - Filtro aplicado

As tramas *probing request* e *probing response* apresentam subtipo 4 e 5, respectivamente. Então para visualizarmos essas tramas aplicámos o filtro presente na figura 15, *wlan.fc.type_subtype==0x4 or wlan.fc.type_subtype==0x5*.

- 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?

wlan.fc.type_subtype == 0x4 or wlan.fc.type_subtype == 0x5						
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
2475	70.151709	HitronTe_af:b1:99	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2335, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2477	70.152099	HitronTe_af:b1:99	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2336, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2479	70.152570	HitronTe_af:b1:99	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2337, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2603	72.179215	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2563, FN=0, Flags=.....C, SSID=FlyingNet
2605	72.179924	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2346, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2608	72.180590	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2347, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Figura 16 - Probing request e Probing response

Na Figura 16 é possível verificar que a trama 2468 representa um *probing request* e a 2469 é um *probing response* correspondente. A frame 2468 é uma STA (ea:a4:64:7b:b9:7a), que é emitida para todos os equipamentos da rede, de modo a encontrar um AP. A trama 2469, por sua vez, é a resposta do AP (HitronTe_af:b1:98) para a STA.

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.

Inicialmente aplicamos um filtro, de modo a identificar as tramas *association request* e *association response*. De seguida, selecionamos as tramas 2490 e 2492 representadas na Figura 17.

wlan.fc.type_subtype == 0 or wlan.fc.type_subtype == 1						
No.	Time	Source	Destination	Protocol	Length	Info
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
4696	83.665976	7c:ea:6d:ff:a2:cc	HitronTe_af:b1:98	802.11	153	Association Request, SN=68, FN=0, Flags=.....C, SSID=FlyingNet
4698	83.678873	HitronTe_af:b1:98	7c:ea:6d:ff:a2:cc	802.11	225	Association Response, SN=2440, FN=0, Flags=.....C
4699	83.680045	HitronTe_af:b1:98	7c:ea:6d:ff:a2:cc	802.11	225	Association Response, SN=2440, FN=0, Flags=.....C
7065	100.208375	d7:19:51:08:62:f9	6d:1b:44:1a:cc:11	802.11	146	Association Request, SN=2586, FN=7, Flags=..pmPRM.T.
7163	100.403689	0a:57:13:28:40:84	79:5c:58:10:7a:cc	802.11	146	Association Response, SN=3497, FN=5, Flags=0.mP..F..[Malformed Packet]

Figura 17 – Captura com o filtro elaborado

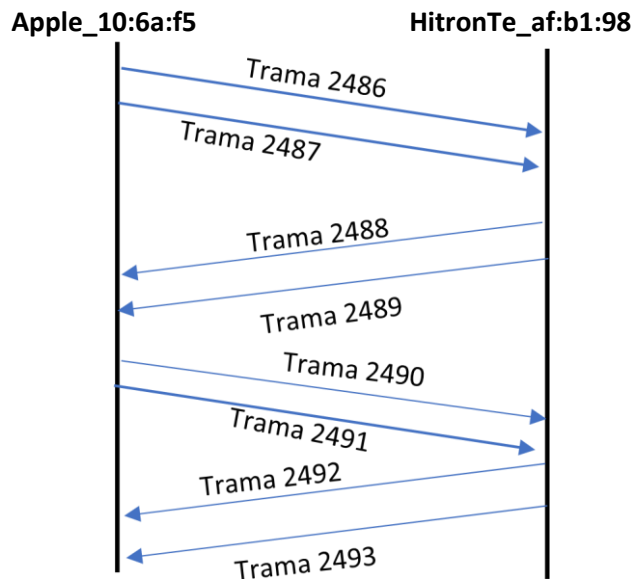
Posteriormente, analisamos a captura sem filtro ordenada pelo tempo. Ao observar a Figura 18, identificamos duas tramas de autenticação (2486 e 2488) e duas de confirmação (2487 e 2489). De referir que a fase de autenticação começa com a trama de autenticação 2486 e termina com a trama de confirmação 2489. Depois inicia-se a fase de associação com uma trama de pedido de associação (2490), que termina com a trama de confirmação 2493, que permite concluir que a trama enviada não continha erros.

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:..	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	Apple_10:6a:f5 (64:..	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	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	Apple_10:6a:f5 (64:..	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
2496	70.453444	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	53	Null function (No data), SN=2544, FN=0, Flags=.....TC
2497	70.453460	Apple_10:6a:f5	Apple_10:6a:f5 (64:..	802.11	39	Acknowledgement, Flags=.....C

Figura 18 – Captura sem filtros

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

Neste diagrama está presente a sequência de todas as tramas trocadas no processo de associação, incluindo a fase de autenticação.



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?

```
Wireshark · Packet 455 · trace-wlan-tp4-2018b.pcap
> Frame 455: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
  IEEE 802.11 QoS Data, Flags: .p....F.C
    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.... = PMR MGT: STA will stay up
        ..0.... = More Data: No data buffered
        ..1.... = Protected flag: Data is protected
        0.... = Order flag: Not strictly ordered
        .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 [correct]
        [FCS Status: Good]
      > Qos Control: 0x0000
      > CCMP parameters
    > Data (163 bytes)
```

Figura 19 - Trama 455

Podemos constatar na Figura 19, através da flag *DS status*, que a trama 455 sai do sistema de distribuição (HitronTe_af:b1:98) para o STA (Apple_71:41:a1) através do AP (HitronTe_af:b1:98). Ou seja, a direccionalidade da trama é local à WLAN.

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?

```
> Frame 455: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
  IEEE 802.11 QoS Data, Flags: .p....F.C
    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
        .1.... = Protected flag: Data is protected
        0... = Order flag: Not strictly ordered
      .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: 0xc46bf48 [correct]
      [FCS Status: Good]
    > Qos Control: 0x0000
    > CCMP parameters
    > Data (163 bytes)
```

Figura 20 - Trama de dados 455

O endereço MAC do host sem fios é o bc:14:01:af:b1:98, como é possível observar no campo Transmitter address na Figura 20. O endereço MAC do AP é d8:a2:5e:71:41:a1, como podemos verificar no Receiver address, enquanto que o endereço MAC do router de acesso pode ser visualizado no Destination address, sendo neste caso d8:a2:5e:71:41:a1.

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

```
> Frame 457: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
  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
      .000 0001 0011 1010 = Duration: 314 microseconds
      Receiver address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
      Transmitter address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
      Destination address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
      Source address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
      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
      0100 1011 1001.... = Sequence number: 1209
      Frame check sequence: 0x88cbfe48 [correct]
      [FCS Status: Good]
    > Qos Control: 0x0000
    > CCMP parameters
    > Data (115 bytes)
```

Figura 21 - Trama de dados 457

Como podemos observar no campo DS status da Figura 21 o pacote chega do sistema de distribuição à STA via AP, o que permite concluir que a direccionalidade não é local à WLAN. Os endereços MAC podem ser observados nos campos identificados na alínea anterior, sendo que neste caso, o STA corresponde ao recetor, o sistema distribuído à origem e o AP ao transmissor.

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 é transmitida uma trama de controlo do subtipo confirmação de receção – Acknowledgement. Estas são responsáveis pela detecção de erros nas tramas de dados. Dada a grande vulnerabilidade desta rede face a erros e como não existem mecanismos de detecção de erros, torna-se imperativo controlar a integridade dos dados que são transmitidos. Desta forma, através do uso destas tramas é possível colmatar este problema. Assim, após a receção de uma trama, a STA receptora introduz um código de verificação para detetar a presença de erros. De seguida é enviada uma trama acknowledgement para a STA emissora, caso não tenham sido detetados erros. Caso a STA não receba a trama dentro de um determinado tempo, esta será retransmitida.



Figura 22 - Trama Acknowledgement

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.

Podemos constatar que a opção RTS/CTS na troca de dados entre a STA e o AP/Router da WLAN está a ser usada. Na Figura 23, podemos observar um exemplo de trama *request-to-send* e na Figura 24 um *clear-to-send*, que correspondem às *frames* 162 e 163, respectivamente. Nestas figuras também é possível verificar que a direccionalidade das duas tramas é definida, dado que **To DS: 0 From DS: 0**, que indica que a comunicação é feita entre STAs e APs. Como podemos observar, a STA emissora (Apple_10:6a:f5) envia um *request-to-send* ao AP (HitronTe_af:b1:98) e este irá, posteriormente, enviar um *clear-to-send* a indicar que pode iniciar a transmissão.

```
Wireshark - Packet 162 - trace-wlan-tp4-2018b.pcap
> Frame 162: 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) (0x0)
      .... 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 1001 1110 = Duration: 158 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: 0x7dc72f1c [correct]
    [FCS Status: Good]
```

Figura 23 - Trama Request-to-send

```
Wireshark - Packet 163 - trace-wlan-tp4-2018b.pcap
> Frame 163: 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
      .... 00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
      .... 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 0111 0010 = Duration: 114 microseconds
    Receiver address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    Frame check sequence: 0xc7363dda [correct]
    [FCS Status: Good]
```

Figura 24 - Trama Clear-to-send

2 Conclusão

Neste trabalho prático tivemos a oportunidade de explorar os vários aspetos do protocolo IEEE 802.11. Analisando a captura fornecida, começamos por interpretar as informações referentes ao nível físico, *radio information*. Nesta, observamos também os diferentes tipos de tramas, desde as Tramas de Gestão, Tramas de Controlo e Tramas de Dados, bem como os seus subtipos.

De seguida, passamos ao estudo do *scanning passivo* e *scanning ativo*. O *scanning* passivo é responsável pelo envio de um sinal periodicamente de tramas Beacon a todas as estações da rede, de modo ao AP indicar a sua presença e transmitir informação. Enquanto o *scanning* ativo envolve tramas de *probe request* e *probe response*. As primeiras são utilizadas com o intuito de se ter conhecimento das estações que estão no seu alcance. Enquanto as segundas, são a resposta das estações que receberam as tramas anteriormente indicadas.

Posteriormente verificamos como ocorre o processo de associação identificando sequências de tramas trocadas neste processo. Por fim, estudamos as transferências de dados e os protocolos associados.