

Redes sem Fios (Wi-Fi) - Trabalho Prático 4

Tiago Alves a80872, Francisco Costa a95227, Cláudio Bessa a97063

19 de maio de 2022

1 Secção Questão-Resposta

1.1 Acesso Rápido

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

```
▼ 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): -61 dBm
  Noise level (dBm): -88 dBm
  Signal/noise ratio (dB): 27 dB
  TSF timestamp: 22260090
  > [Duration: 1632µs]
```

Figura 1: Frequência de espectro

R: Estamos a usar canal 12, frequência de 2.4GHz a 1Mbits/s.

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

```
▼ 802.11 radio information
  PHY type: 802.11b (HR/DSSS) (4)
```

Figura 2: Versão da norma IEEE 802.11

R: 802.11b, devido ao reconhecido do *Wireshark* mas sendo uma trama do tipo 802.11g.

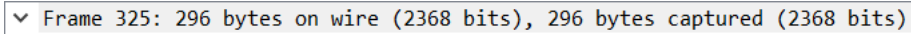
- 1.1.3 Qual o débito a que foi enviada a trama escolhida? Será que esse débito corresponde ao débito máximo a que a interface Wi-Fi pode operar? Justifique

```
▼ 802.11 radio information
  PHY type: 802.11b (HR/DSSS) (4)
  Short preamble: False
  Data rate: 1,0 Mb/s
```

Figura 3: Débito máximo interface Wi-Fi

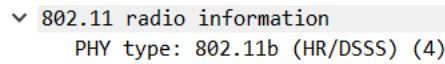
1.2 *Scanning* Passivo e *Scanning* Ativo

- 1.2.1 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)?



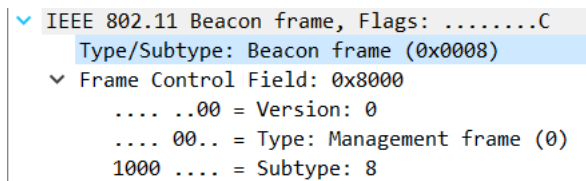
▼ Frame 325: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)

Figura 4: Frame atribuída ao grupo



▼ 802.11 radio information
PHY type: 802.11b (HR/DSSS) (4)

Figura 5: Tipo de trama



▼ 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

Figura 6: Tipo e Subtipo do Beacon Frame

R: Após efetuar $260 + 65 = 325$ verificamos que o *frame* atribuído seria o 325. Verificamos após isso que o *frame* seria do tipo 802.11b. O seu *Beacon Frame* é do tipo (*type*) 0x00 e o subtipo (*subtype*) 0x08.

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

```
> Frame Control Field: 0x8000
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
```

Figura 7: MAC *addresses* em uso

R:

1.2.3 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?

```

v 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
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 8: Débitos

R: rates suportados (debitos base) e extended rates (debitos adicionais)

1.2.4 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.

```

v IEEE 802.11 Wireless Management
  v Fixed parameters (12 bytes)
    Timestamp: 1149683712489
    Beacon Interval: 0,102400 [Seconds]

```

Figura 9: Velocidade de envio da trama

R: Na pratica este intervalo não será exatamente o previsto, sendo que as condições físicas do meio tendem a interferir com o sinal na velocidade de envio da trama.

1.2.5 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).

323 13.005001	HitronTe_af:b1:98	Broadcast	802.11	296 Beacon frame, SN=2337, FN=0, Flags=.....C, BI=100, SSID=FlyingNe
324 13.006518	HitronTe_af:b1:99	Broadcast	802.11	205 Beacon frame, SN=2338, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI
325 13.107409	HitronTe_af:b1:98	Broadcast	802.11	296 Beacon frame, SN=2339, FN=0, Flags=.....C, BI=100, SSID=FlyingNe
326 13.109035	HitronTe_af:b1:99	Broadcast	802.11	205 Beacon frame, SN=2340, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI
327 13.209790	HitronTe_af:b1:98	Broadcast	802.11	296 Beacon frame, SN=2341, FN=0, Flags=.....C, BI=100, SSID=FlyingNe
328 13.211424	HitronTe_af:b1:99	Broadcast	802.11	205 Beacon frame, SN=2342, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI
329 13.312189	HitronTe_af:b1:98	Broadcast	802.11	296 Beacon frame, SN=2343, FN=0, Flags=.....C, BI=100, SSID=FlyingNe
330 13.313819	HitronTe_af:b1:99	Broadcast	802.11	205 Beacon frame, SN=2344, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI

Figura 10: SSID da vizinhança

R: Os SSID da vizinhança são essencialmente os designados por *FlyingNet* e *NOS-WIFI-FON* como podemos observar nas tramas capturadas.

1.2.6 Verifique se está a ser usado o método de deteção de erros (CRC)

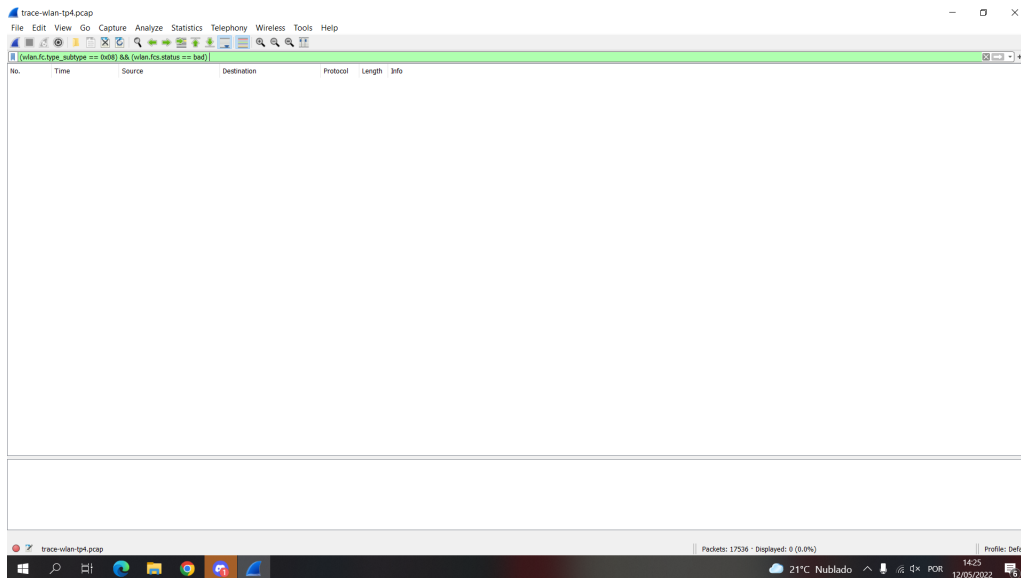


Figura 11: Método de deteção de erros

R: Podemos concluir que neste trace disponibilizado, não ocorreram erros. A importância de deteção de erros em redes sem fios é muito alta, pois um bit errado na transmissão pode torná-la completamente inutilizável.

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

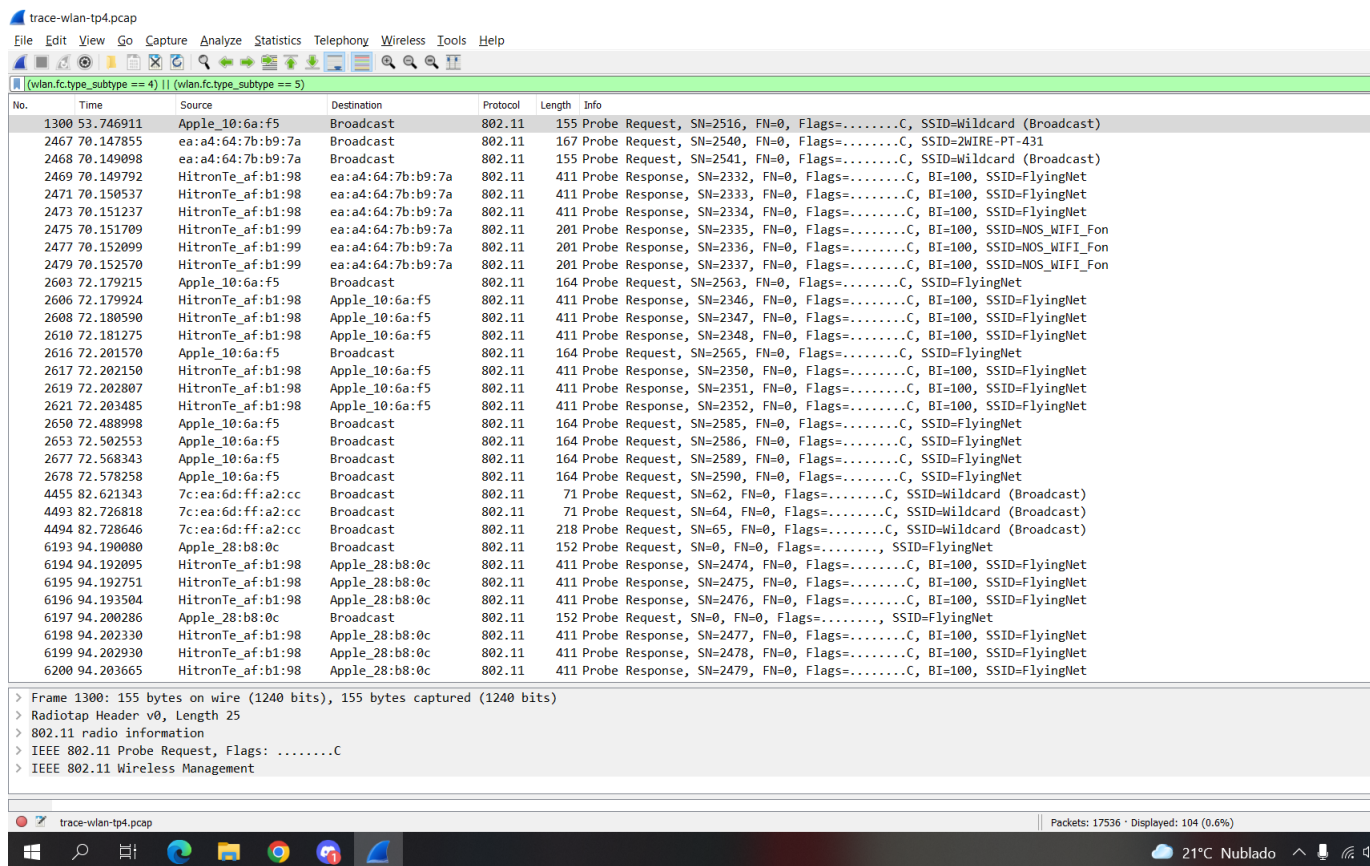


Figura 12: Tipo e Subtipo do Beacon Frame

R: Com os filtros,

`(wlan.fc.type_subtype == 4)` ou `(wlan.fc.type_subtype == 5)`,

podemos observar as probe request e response simultaneamente.

Subtype 4 = Probe request

Subtype 5 = Probe response

1.2.8 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?

```

> [Duration: 1232µs]
▼ IEEE 802.11 Probe Request, Flags: .....C
  Type/Subtype: Probe Request (0x0004)
  > Frame Control Field: 0x4000
    .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: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)
    Source address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)

```

Figura 13: Source ea:a4:64:7b:b9:7a

```

> [Duration: 200µs]
▼ IEEE 802.11 Probe Response, Flags: .....C
  Type/Subtype: Probe Response (0x0005)
  > Frame Control Field: 0x5000
    .000 0000 0011 0010 = Duration: 50 microseconds
    Receiver address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)
    Destination address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)
    Transmitter address: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
    Source address: HitronTe_af:b1:99 (bc:14:01:af:b1:99)

```

Figura 14: Pedido de HitronTe-af:b1:99

2468	70.149098	ea:a4:64:7b:b9:7a	Broadcast	802.11	155 Probe Request, S
2469	70.149792	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411 Probe Response,
2471	70.150537	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411 Probe Response,
2473	70.151237	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411 Probe Response,
2475	70.151709	HitronTe_af:b1:99	ea:a4:64:7b:b9:7a	802.11	201 Probe Response,
2477	70.152099	HitronTe_af:b1:99	ea:a4:64:7b:b9:7a	802.11	201 Probe Response,
2479	70.152570	HitronTe_af:b1:99	ea:a4:64:7b:b9:7a	802.11	201 Probe Response,

Figura 15: Resposta emitida

R: A *probe request* (nº2468) manda um pedido para a rede, com *source* ea:a4:64:7b:b9:7a, a *probe response* (nº2479) responde ao pedido.

HitronTe-af:b1:99 trata-se da fonte da resposta e o transmissor, a partir dele rumo à fonte do pedido inicial.

1.3 Processos de Associação

1.3.1 Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.

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

Figura 16: Autenticação entre STA e AP

R: Da linha 2486 a 2488 temos a autenticação entre a STA e o AP, na linha 2490 e 2492 temos a associação entre a STA e o AP. Isto trata-se da associação completa, pois existem apenas 3 estados de ligação 802.11.

- Não autenticado e não associado
- Autenticado e não associado
- Autenticado e associado

Anterior quer a autenticação e à associação existem as probes que permitem às máquinas na rede saberem que outras máquinas se encontram ligadas.

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

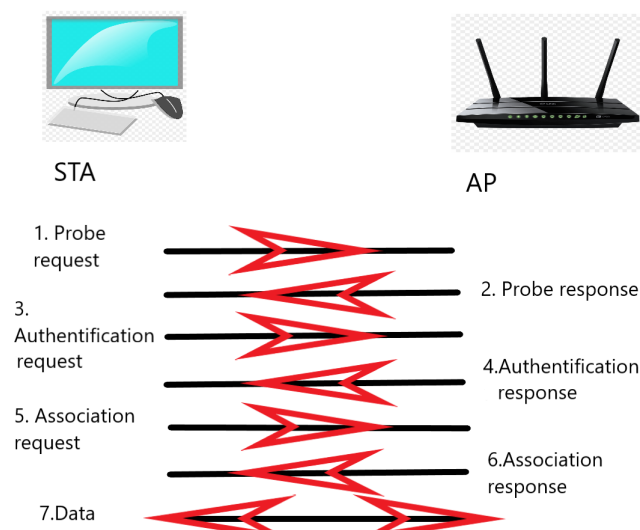


Figura 17: Diagrama ilustrativo das tramas trocadas

1.4 Transferência de Dados

- 1.4.1 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?

```
▼ 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)
```

Figura 18: Origem do *frame*

R: Na *flag* podemos ver que a *frame* vem do DS (distribution system) para uma STA (station). Ou seja a *frame* vem de um *router* para uma *station*.

- 1.4.2 Para a trama de dados nº431, 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?

```
.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 19: Endereços MAC

R: O endereço MAC correspondente ao host sem fios (STA) é 64:9a:be:10:6a:f5 sendo este o destino.

O AP é bc:14:01:af:b1:98 e o *router* de acesso ao sistema de distribuição também é bc:14:01:af:b1:98 sendo este o *source*.

1.4.3 Como interpreta a trama nº433 face à sua direccionalidade e endereçamento MAC?

```
▼ 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)
```

Figura 20: Trama nº 433

R: Aqui podemos observar o contrário ao observado no exercício 15, o STA está a ser transmitido através do AP para o DS, sendo que os MAC addresses seguem este mesmo padrão.

- STA 64:9a:be:10:6a:f5
- AP 64:9a:be:10:6a:f5
- DS bc:14:01:af:b1:98

1.4.4 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.)

R: Ao longo das tramas acima utilizados o subtipo é 8 (1000) que se refere ao QoS, que de sua vez se refere, ao quality of service data. Estes dados ajudam a prevenir colisões. Ao contrário das tramas *ethernet*, o protocolo aqui usado estabelece comunicação entre o transmissor e o recetor, pelo que no caso de perda de informação tem de haver a possibilidade da recuperação desses dados através da retransmissão desses.

1.4.5 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. Dê um exemplo de uma transferência de dados em que é usada a opção RTC/CTS e um outro em que não é usada.

R: Estas duas tramas existem de maneira a evitar as colisões entre os diferentes equipamentos presentes na rede Wi-Fi,

Estas começam por efetuar um pedido de comunicação (RTS), aguardando depois o sinal de resposta da trama (CTS)..Esta por consequente sinaliza a possibilidade de estabelecimento da comunicação entre dispositivos. Após isso é reservada memória para as interações necessárias evitando qualquer tipo de problemas, interferências, na comunicação entre *transmitter* e *receiver*.

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
435 17.927587	Apple_28:b8:0c	HitronTe_af:b1:98	802.11	49 Null function (No data), SN=0, FN=0, Flags=.....T
436 17.927618		Apple_28:b8:0c (68:...	802.11	39 Acknowledgement, Flags=.....C
437 17.984501	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	53 Null function (No data), SN=2499, FN=0, Flags=...P...TC
438 17.984522		Apple_10:6a:f5 (64:...	802.11	39 Acknowledgement, Flags=.....C

Figura 21: Sem RTS/CTS

561 21.595512	Apple_10:6a:f5 (64:...	HitronTe_af:b1:98 (...)	802.11	45 Request-to-send, Flags=.....C
562 21.595518		Apple_10:6a:f5 (64:...	802.11	39 Clear-to-send, Flags=.....C
563 21.595634	HitronTe_af:b1:98 (...)	Apple_10:6a:f5 (64:...	802.11	57 802.11 Block Ack, Flags=.....C
564 21.606584	HitronTe_af:b1:98	Broadcast	802.11	296 Beacon frame, SN=2505, FN=0, Flags=.....C, BI=100, SSID=FlyingNe
565 21.608194	HitronTe_af:b1:99	Broadcast	802.11	205 Beacon frame, SN=2506, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI
566 21.608284	Apple_10:6a:f5	IPv4mcast_fb	802.11	261 Data, SN=2249, FN=0, Flags=.pm...F.C
567 21.608366	Apple_10:6a:f5	IPv6mcast_fb	802.11	281 Data, SN=2250, FN=0, Flags=.p....F.C
568 21.616206	HitronTe_af:b1:98 (...)	Apple_10:6a:f5 (64:...	802.11	45 Request-to-send, Flags=.....C
569 21.616217		HitronTe_af:b1:98 (...)	802.11	39 Clear-to-send, Flags=.....C
570 21.616222	HitronTe_af:b1:96	Apple_10:6a:f5	802.11	146 QoS Data, SN=836, FN=0, Flags=.p....F.C

Figura 22: Com RTS/CTS

2 Conclusão

R: Neste trabalho prático reconhecemos algumas das principais diferenças entre as ligações em redes sem fios e redes com fios. Obtivemos algumas dificuldades na parte de reconhecimento de tramas "*request to send*" e "*clear to send*" até conseguirmos de igual forma relacionar com comportamentos similares que existem em tramas *ethernet*.