

## Trabalho Prático Nº4 – Redes sem Fios (WIFI)

**Grupo 17** - Ana Rita Poças (a97284) , Bernard Georges (a96326) e João Pedro Braga (a97368)

### 4. Acesso Rádio

**Selecione a trama de ordem XX correspondente ao seu identificador de grupo:**

Trama de ordem 17

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

A frequência = 2467 MHz e o canal correspondente é 12.

Frequency: 2467MHz

Channel: 12

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

802.11 Block Ack (0x0019)

✓ IEEE 802.11 802.11 Block Ack, Flags: .....C

Type/Subtype: 802.11 Block Ack (0x0019)

> Frame Control Field: 0x9400

**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.**

O débito que foi enviado à trama = 24,0 Mb/s

Data rate: 24,0 Mb/s

Sendo o máximo data rate da interface **IEEE 802.11g Wi-Fi** igual a 54 Mbps, temos que o débito enviado não corresponde ao débito máximo.

### 5. Scanning Passivo e Scanning Ativo

Como referido, as tramas beacon permitem efetuar scanning passivo em redes IEEE 802.11 (Wi-Fi). Para a captura de tramas disponibilizada, e considerando XX o seu nº de grupo, responda às seguintes questões:

**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)?**

Trama beacon de ordem  $260 + 17 = 277$

Esta trama pertence ao tipo/subtipo Beacon frame (0x0008).

Identificador de tipo (binário): 00 (Management)

Identificador de subtipo: 1000 (Beacon)

Está especificado na parte de controlo da trama (frame control).

Type/Subtype: Beacon frame (0x0008)

```

▼ Frame Control Field: 0x8000
.... ..00 = Version: 0
.... 00.. = Type: Management frame (0)
1000 .... = Subtype: 8

```

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

```

Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)

```

Uma vez que um endereço MAC Broadcast é do tipo “one to all”, temos que este transmite para todos os dispositivos. Isto é feito de forma a informar a presença e o mantimento da rede da sua origem. No destino, já sabemos de onde vem a informação.

6) Uma trama beacon anuncia que o AP pode suportar vários débitos de base, assim como vários débitos adicionais (extended supported rates). Indique quais são esses débitos?

```

Extended Supported Rates: 6(B) (0x8c)
Extended Supported Rates: 12(B) (0x98)
Extended Supported Rates: 24(B) (0xb0)
Extended Supported Rates: 48 (0x60)

```

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.

```
Beacon Interval: 0.102400 [Seconds]
```

No.	Time	Source	Destination	Protocol	Length	Info
277	10.547214	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2289, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
278	10.548833	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2290, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
279	10.649623	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2291, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Para comprovar o intervalo fixo definido (0.102400 segundos), decidimos comparar o tempo de chegada de tramas provenientes da mesma rede (mesmo SSID). Ao ser feita a subtração, verificamos um valor de 0.102409 que é proximo de seu valor de intervalo, este erro pode ser devido alguns fatores de interferência durante a transmissão entre o AP e o host.

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).

```

SSID=NOS_WIFI_Fon
SSID=FlyingNet

```

De forma a obter esta informação,

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

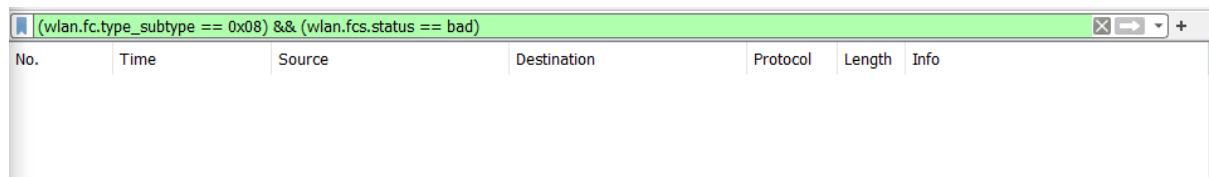
Sugestão: Use o filtro:

```
(wlan.fc.type_subtype == 0x08) && (wlan.fcs.status == bad)
```

Que conclui?

Ao correr o filtro (wlan.fc.type\_subtype == 0x08) && (wlan.fcs.status == bad)

não obtivemos qualquer informação, concluímos que o método de detecção não está a ser utilizado.



The image shows a Wireshark packet capture window. The filter bar at the top contains the expression `(wlan.fc.type_subtype == 0x08) && (wlan.fcs.status == bad)`. The packet list below shows a single packet with the following details:

No.	Time	Source	Destination	Protocol	Length	Info
						Frame check sequence: 0x3d782a65 [unverified] [FCS Status: Unverified]

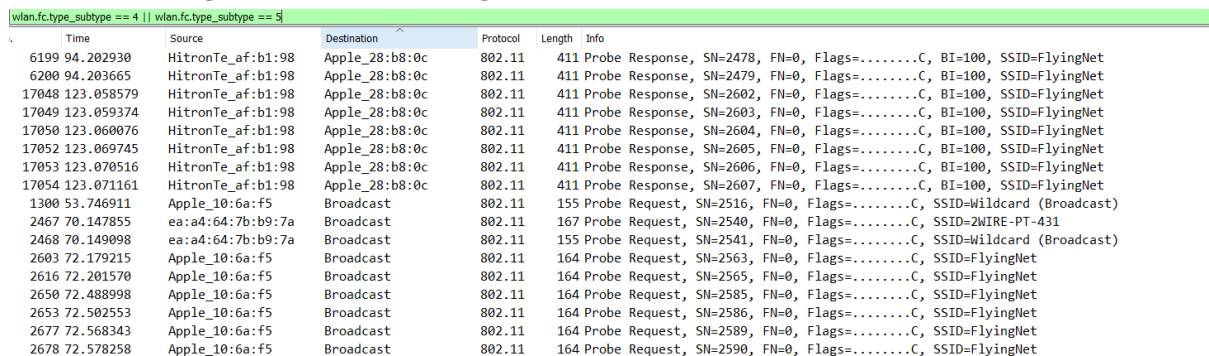
Frame check sequence: 0x3d782a65 [unverified]  
[FCS Status: Unverified]

**Justifique o porquê de ser necessário usar detecção de erros em redes sem fios.**

A transmissão no meio sem fios é muito mais vulnerável à influência de interferências externas visto que muitos canais de comunicação estão a coexistir no mesmo meio, o que pode originar erros durante a transmissão da mensagem entre a fonte e o destinatário. Assim sendo, técnicas de detecção de erros permitem a detecção prévia desses erros para a posterior reconstrução da mensagem original na maioria dos casos.

**No trace disponibilizado foi também registado scanning ativo (envolvendo tramas probe request e probe response), comum nas redes Wi-Fi como alternativa ao scanning passivo.**

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



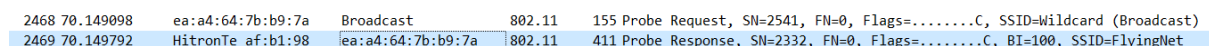
The image shows a Wireshark packet capture window with the filter `wlan.fc.type_subtype == 4 || wlan.fc.type_subtype == 5`. The packet list shows several probe requests and responses:

No.	Time	Source	Destination	Protocol	Length	Info
6199	94.202930	HitronTe_af:b1:98	Apple_28:b8:0c	802.11	411	Probe Response, SN=2478, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
6200	94.203665	HitronTe_af:b1:98	Apple_28:b8:0c	802.11	411	Probe Response, SN=2479, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17048	123.058579	HitronTe_af:b1:98	Apple_28:b8:0c	802.11	411	Probe Response, SN=2602, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17049	123.059374	HitronTe_af:b1:98	Apple_28:b8:0c	802.11	411	Probe Response, SN=2603, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17050	123.060076	HitronTe_af:b1:98	Apple_28:b8:0c	802.11	411	Probe Response, SN=2604, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17052	123.069745	HitronTe_af:b1:98	Apple_28:b8:0c	802.11	411	Probe Response, SN=2605, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17053	123.070516	HitronTe_af:b1:98	Apple_28:b8:0c	802.11	411	Probe Response, SN=2606, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
17054	123.071161	HitronTe_af:b1:98	Apple_28:b8:0c	802.11	411	Probe Response, SN=2607, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
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)
2603	72.179215	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2563, FN=0, Flags=.....C, SSID=FlyingNet
2616	72.201570	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2565, FN=0, Flags=.....C, SSID=FlyingNet
2650	72.488998	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2585, FN=0, Flags=.....C, SSID=FlyingNet
2653	72.502553	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2586, FN=0, Flags=.....C, SSID=FlyingNet
2677	72.568343	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2589, FN=0, Flags=.....C, SSID=FlyingNet
2678	72.578258	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2590, FN=0, Flags=.....C, SSID=FlyingNet

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

**11) Identifique um probing request para o qual tenha havido um probing response.**

**Face ao endereçamento usado, indique a que sistemas são endereçadas estas tramas e explique qual o propósito das mesmas?**



The image shows a Wireshark packet capture window with the filter `wlan.fc.type_subtype == 4 || wlan.fc.type_subtype == 5`. The packet list shows a probe request and its response:

No.	Time	Source	Destination	Protocol	Length	Info
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

No request, temos um dispositivo com um endereçamento que faz um broadcast para saber os access points que se encontram próximos. E no response, um access point (neste caso um AP da rede FlyingNet) devolve a informação pedida pelo dispositivo inicial e como já sabemos de onde provém a informação não necessitamos de um endereço MAC do tipo Broadcast, sendo apenas um endereço do dispositivo que pediu a informação.

## 6. Processo de Associação

Numa rede Wi-Fi estruturada, um host deve associar-se a um ponto de acesso antes de enviar dados. O processo de associação nas redes IEEE 802.11 é executada enviando a trama association request do host para o AP e a trama association response enviada pelo AP para o host, em resposta ao pedido de associação recebido. Este processo é antecedido por uma fase de autenticação. Para a sequência de tramas capturada:

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.

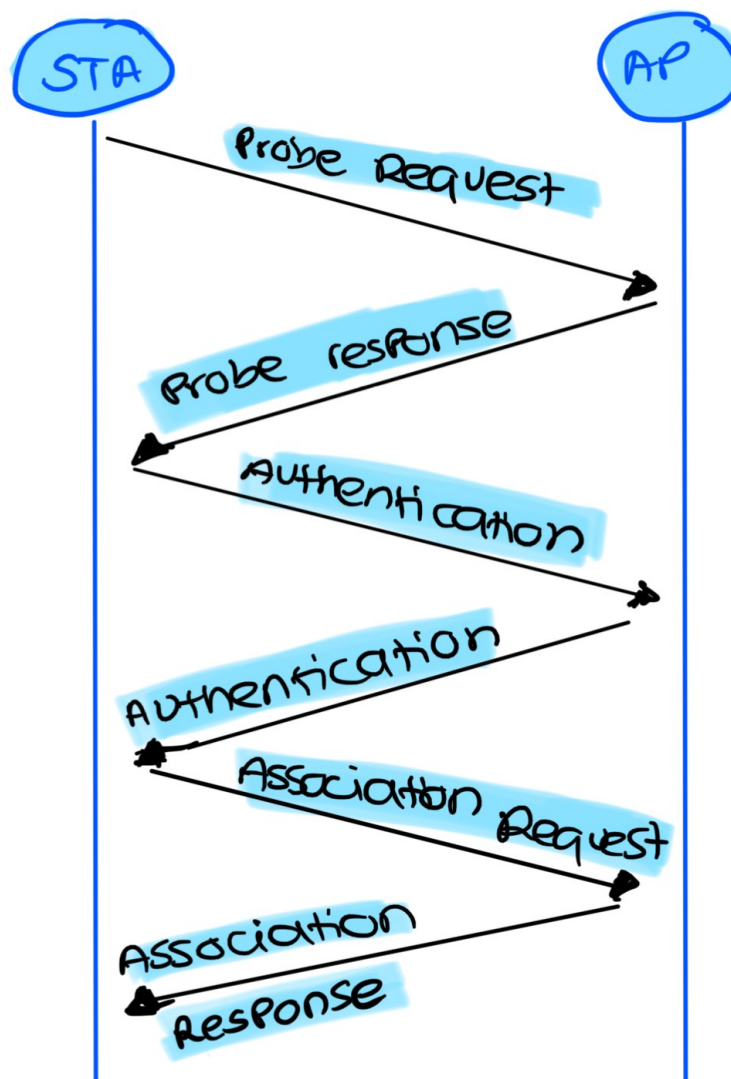
### Authentication

4692 83.663250	7c:ea:6d:ff:a2: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:ff:a2:cc	802.11	59 Authentication, SN=2439, FN=0, Flags=.....C

### Association

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

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



## 7. Transferência de Dados

O trace disponibilizado, para além de tramas de gestão da ligação de dados, inclui tramas de dados e tramas de controlo da transferência desses mesmos dados.

14) Considere a trama de dados nº 431. 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)
    .... .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
```

A direccionalidade da trama apresentada é do DS para a STA, via AP. ( toDS = 0, fromDS = 1), logo podemos concluir que estamos a partir de uma estação wireless em direção a um host/estação.

Como fromDS = 1, sabemos que a trama vem de fora, logo não é local à WLAN.

Para ser local à WLAN, é necessário que ambos os toDS e fromDS sejam 0.

15) Para a trama de dados nº 431, 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?

```
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)
```

Os endereços MAC em uso são os seguintes:

STA: 64:9a:be:10:6a:f5 (**receiver address & destination address**)

AP: bc:14:01:af:b1:98 (**transmitter address**)

Router Address: bc:14:01:af:b1:98 (**source address**)

## 16) Como interpreta a trama nº433 face à sua direccionalidade e endereçamento MAC?

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

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)

Podemos concluir que partimos de um STA (**source address**), via AP (**transmitter address**) em direção ao DS (**destination address**).

STA Address = 64:9a:be:10:6a:f5 (Source Address & Transmitter Address)

AP Address = bc:14:01:af:b1:98 (Destination Address & Receiver Address)

## 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.)

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 17.984591	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

### Type/Subtype: Acknowledgement (0x001d)

Ao longo da transferência de dados, são transmitidas tramas de controlo do tipo Acknowledgement, que indicam a transmissão correta de tramas de dados sem erros. Esta trama é enviada pela STA recetora para a STA emissora no caso de não ter sido detetado nenhum erro nas tramas recebidas. Caso contrário, após algum tempo sem receber um ACK, a STA emissora retransmite a trama. Isto permite um melhor controlo de erros, bastante importante num ambiente wireless (ambiente vulnerável a interferências), ao contrário de uma rede Ethernet que é um ambiente bastante mais controlado e menos vulnerável a interferências. Além disso, esta trama serve para controlar as comunicações entre dispositivos, de forma a impedir colisões, ao informar todos os dispositivos acessíveis que o dispositivo está a comunicar com outro.



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

```
173 6.658172      Apple_10:6a:f5 (64:... HitronTe_af:b1:98 (... 802.11      45 Request-to-send, Flags=.....C
174 6.658178      Apple_10:6a:f5 (64:... 802.11      39 Clear-to-send, Flags=.....C
```

Conforme podemos observar acima, na comunicação entre 64:9a:be:10:6a:f5 e bc:14:01:af:b1:98 está a ser usada a opção RTS/CTS.

Request To Send: enviada por 64:9a:be:10:6a:f5 (STA), recebida por bc:14:01:af:b1:98 (AP/Router).

Clear To Send: recebida por 64:9a:be:10:6a:f5 (STA).

```
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
```

O exemplo acima é um exemplo de comunicação **com** RTS/CTS.

O exemplo seguinte é um exemplo de comunicação **sem** RTS/CTS.

```
962 37.890030      HitronTe_af:b1:96      IPv4mcast_7f:ff:fa      802.11      379 Data, SN=2264, FN=0, Flags=.pm...F.C
963 37.890203      HitronTe_af:b1:96      IPv4mcast_7f:ff:fa      802.11      388 Data, SN=2265, FN=0, Flags=.pm...F.C
964 37.890410      HitronTe_af:b1:96      IPv4mcast_7f:ff:fa      802.11      431 Data, SN=2266, FN=0, Flags=.pm...F.C
965 37.890558      HitronTe_af:b1:96      IPv4mcast_7f:ff:fa      802.11      443 Data, SN=2267, FN=0, Flags=.pm...F.C
966 37.890773      HitronTe_af:b1:96      IPv4mcast_7f:ff:fa      802.11      445 Data, SN=2268, FN=0, Flags=.pm...F.C
967 37.890937      HitronTe_af:b1:96      IPv4mcast_7f:ff:fa      802.11      459 Data, SN=2269, FN=0, Flags=.p....F.C
```

## Conclusão

A realização deste trabalho prático, possibilitou a consolidação dos conceitos que tínhamos adquirido, em especial o conceito de Redes sem Fios (WIFI), que serão necessários para o bom aproveitamento da Unidade Curricular, bem como no decorrer das nossas aprendizagens como futuros Engenheiros Informáticos.