



TP4 - Redes Sem Fios

Redes de Computadores - Grupo 12

Ana Teresa Gião Gomes A89536
André Carvalho da Cunha Martins A89586
Pedro Miguel de Soveral Pacheco Barbosa A89529



Fig. 1. A89536



Fig. 2. A89586



Fig. 3. A89529

6 de janeiro de 2021

Redes Sem Fios

André Martins, Ana Teresa Gomes, and Pedro Barbosa

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a89586,a89536,a89529}@alunos.uminho.pt

Acesso Rádio

1 Pergunta 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: 802.11g (ERP) (6)
  Short preamble: False
  Proprietary mode: None (0)
  Data rate: 1,0 Mb/s
  Channel: 12
  Frequency: 2467MHz
  Signal strength (dBm): -59 dBm
  Noise level (dBm): -88 dBm
  Signal/noise ratio (dB): 29 dB
  TSF timestamp: 19800120
  > [Duration: 2360µs]
```

Fig. 1. Frequência da rede sem fios

Como é possível observar na figura de cima, a rede sem fios está a operar numa frequência de 2467 MHz, correspondendo ao canal 12 do espetro.

2 Pergunta 2: Identifique a versão da norma IEEE 802.11 que está a ser usada.

```
▼ 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): -59 dBm
  Noise level (dBm): -88 dBm
  Signal/noise ratio (dB): 29 dB
  TSF timestamp: 19800120
  > [Duration: 2360µs]
```

Fig. 2. Versão da norma IEEE 802.11

A versão da norma IEEE 802.11 que está a ser utilizada é a versão 802.11g(6).

- 3 Pergunta 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.**

```
▼ 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): -59 dBm
  Noise level (dBm): -88 dBm
  Signal/noise ratio (dB): 29 dB
  TSF timestamp: 19800120
  > [Duration: 2360µs]
```

Fig. 3. Débito da trama

A trama foi enviada a 1 MBps

Este débito não corresponde ao máximo da interface WiFi, uma vez que a versão 802.11g é capaz de atingir um débito de 54 MBps.

Scanning passivo e scanning Ativo

- 4 Pergunta 4: Selecione uma trama beacon (e.g., trama 1012). 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)?**

A trama pertence ao tipo 802.11g. O tipo corresponde ao um Managment Frame enquanto que o subtipo corresponde a um Beacon, uma vez que o valor de identificação é igual a 8. Estes valores estão especificados na posição frame control entre os bits 3 e 8, nos campos type e subtype, respetivamente

```
▼ 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:b1:98 (bc:14:01:af:b1:98)
    Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
```

Fig. 4. Beacon Frame

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

Como é possível observar, identificamos 2 endereços MAC. O endereço da Source (bc:14:01:af:b1:99) e o endereço Destination (ff:ff:ff:ff:ff:ff). O endereço de source refere-se ao Hitron_af:b1:99 e o endereço Destination refere-se ao Broadcast e não um endereço físico de uma interface ativa.

```
> 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)
```

Fig. 5. Endereços MAC

6 Pergunta 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?

```
▼ IEEE 802.11 Wireless Management
  > 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: DS Parameter set: Current Channel: 12
    > Tag: Extended Supported Rates 6(B), 12(B), 24(B), 48, [Mbit/sec]
```

Fig. 6. Extended Supported Rates

Como é possível observar, os extended supported rates suportados pelo AP são de 6, 12, 24 e 48 Mbit/seg.

7 Pergunta 7: Qual 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 provenientes do mesmo AP é verificada? Tente explicar porquê.

```
▼ IEEE 802.11 Wireless Management
  ▼ Fixed parameters (12 bytes)
    Timestamp: 1149709619690
    Beacon Interval: 0,102400 [Seconds]
  > Capabilities Information: 0x0c31
```

Fig. 7. Intervalo entre tramas beacon consecutivas

O intervalo entre 2 tramas beacon consecutivas é de 0,102400 segundos. Na prática, este intervalo não é respeitado, sendo apenas uma aproximação. Quando se verifica um elevado tráfego, o intervalo aumenta proporcionalmente à quantidade de tráfego. Como se pode verificar na figura seguinte, o intervalo entre duas tramas consecutivas é menor do que o esperado (0,0015 segundos entre tramas 1012 e 1013) uma vez que o tráfego é muito menor.

| | | | | |
|----------------|-------------------|-----------|--------|--|
| 1012 39.014662 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 Beacon frame, SN=2845, FN=0, Flags=.....C, BI=100, SSID=FlyingNet |
| 1013 39.016210 | HitronTe_af:b1:99 | Broadcast | 802.11 | 205 Beacon frame, SN=2846, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon |

Fig. 8. Intervalo entre tramas beacon consecutivas

8 Pergunta 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 encontrandos são :

- 1) Flying Net
- 2) NOS_WIFI_FON

Para encontrar os SSIDs utilizamos o filtro `wlan.fc.type_subtype == 0x08`, para apenas ficarmos com as tramas beacon da nossa amostra. Após esta análise, reparamos que apenas existem dois SSIDs diferentes, o Flying Net e o NOS_WIFI_FON

| wlan.fc.type_subtype == 0x08 | | | | | | | |
|------------------------------|------------------|-------------------|-------------|----------|--------|--|--|
| | Time | Source | Destination | Protocol | Length | Info | |
| | 16943.120.525403 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 | Beacon frame, SN=341, FN=0, Flags=.....C, BI=100, SSID=FlyingNet | |
| | 16945.120.627622 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 | Beacon frame, SN=343, FN=0, Flags=.....C, BI=100, SSID=FlyingNet | |
| | 16947.120.730075 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 | Beacon frame, SN=345, FN=0, Flags=.....C, BI=100, SSID=FlyingNet | |
| | 16949.120.832426 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 | Beacon frame, SN=347, FN=0, Flags=.....C, BI=100, SSID=FlyingNet | |
| | 16951.120.934812 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 | Beacon frame, SN=349, FN=0, Flags=.....C, BI=100, SSID=FlyingNet | |
| | 16953.121.037221 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 | Beacon frame, SN=351, FN=0, Flags=.....C, BI=100, SSID=FlyingNet | |
| | 16955.121.139672 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 | Beacon frame, SN=353, FN=0, Flags=.....C, BI=100, SSID=FlyingNet | |
| | 16957.121.242070 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 | Beacon frame, SN=355, FN=0, Flags=.....C, BI=100, SSID=FlyingNet | |
| | 16959.121.344467 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 | Beacon frame, SN=357, FN=0, Flags=.....C, BI=100, SSID=FlyingNet | |
| | 16961.121.446739 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 | Beacon frame, SN=359, FN=0, Flags=.....C, BI=100, SSID=FlyingNet | |
| | 16963.121.549200 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 | Beacon frame, SN=361, FN=0, Flags=.....C, BI=100, SSID=FlyingNet | |

Fig. 9. SSIDs

9 Pergunta 9: Verifique se está a ser usado o método de deteção de erros (CRC). Justifique. Use o filtro:(`wlan.fc.type_subtype == 0x08`) (`wlan.fcs.status == bad`) Que conclui? Justifique o porquê de usar deteção de erros em redes sem fios.

Como vemos na figura, o campo Frame Check Sequence encontra-se sempre Unverified, mostrando, assim, que o método de deteção de erros (CRC) não está a ser utilizado.

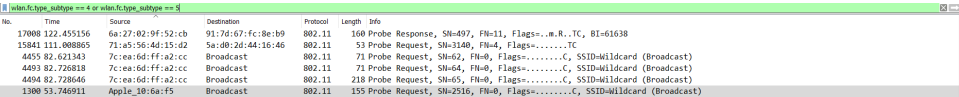
| |
|---|
| 0000 = Fragment number: 0 |
| 1111 1110 1111 = Sequence number: 4079 |
| Frame check sequence: 0x2aedcef8 [unverified] |
| [FCS Status: Unverified] |

Fig. 10. CRC

A deteção de erros é utilizada em redes sem fios uma vez que a probabilidade de existirem colisões é maior, pois existe uma maior liberdade dos dispositivos a transmitir informação para um AP.

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

Para obter as tramas probing request e probing response foi necessário definir um filtro que nos permitisse isolar tramas do type 0 e subtype 4, para requeste, e subtype 5, para response. Assim sendo, o fitro definido foi `wlan.fc.type_subtype == 4 or wlan.fc.type_subtype == 5`



| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|------------|-------------------|-------------------|----------|--------|---|
| 17000 | 122.455156 | 6a:27:02:9f:52:cb | 91:7d:67:fc:8e:b9 | 802.11 | 100 | Probe Response, Sfi=497, Ffi=11, Flags=.....R..TC, BI=61638 |
| 15841 | 111.008805 | 71:a5:56:4d:15:d2 | 5a:00:2d:44:16:46 | 802.11 | 53 | Probe Request, Sfi=3140, Ffi=4, Flags=.....TC |
| 4455 | 92.621343 | 7c:ea:6d:ff:a2:cc | Broadcast | 802.11 | 71 | Probe Request, Sfi=62, Ffi=0, Flags=.....C, SSID=Wildcard (Broadcast) |
| 4403 | 82.728818 | 7c:ea:6d:ff:a2:cc | Broadcast | 802.11 | 71 | Probe Request, Sfi=64, Ffi=0, Flags=.....C, SSID=Wildcard (Broadcast) |
| 4404 | 82.728646 | 7c:ea:6d:ff:a2:cc | Broadcast | 802.11 | 218 | Probe Request, Sfi=65, Ffi=0, Flags=.....C, SSID=Wildcard (Broadcast) |
| 1300 | 53.746911 | Apple_10:6a:f5 | Broadcast | 802.11 | 155 | Probe Request, Sfi=2516, Ffi=0, Flags=.....C, SSID=Wildcard (Broadcast) |

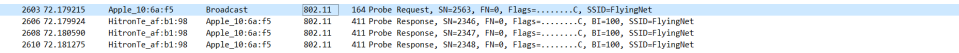
Fig. 11. Probing request e probing response

11 Pergunta 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?

Como podemos verificar na figura, existe um probing request na trama 2603 e o respetivo probing response na trama 2610.

A trama de probing request é emitida STA (Station) Apple_10:6a:f5 para procurar um AP, sendo enviada para todos os equipamentos. A resposta, o probing response, vem do AP HitronTe_af:b1:98 para a STA

Um probing request serve para saber informações sobre um AP na área. Depois do probing request ser emitido, o AP emite uma probing response para informar que está disponível, permitindo, assim, a comunicação entre a STA e o AP.



| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|-------------------|----------------|----------|--------|--|
| 2603 | 72.179215 | Apple_10:6a:f5 | Broadcast | 802.11 | 164 | Probe Request, Sfi=2563, Ffi=0, Flags=.....C, SSID=FlyingIlet |
| 2606 | 72.179924 | HitronTe_af:b1:98 | Apple_10:6a:f5 | 802.11 | 411 | Probe Response, Sfi=2346, Ffi=0, Flags=.....C, BI=100, SSID=FlyingIlet |
| 2608 | 72.180590 | HitronTe_af:b1:98 | Apple_10:6a:f5 | 802.11 | 411 | Probe Response, Sfi=2347, Ffi=0, Flags=.....C, BI=100, SSID=FlyingIlet |
| 2610 | 72.181275 | HitronTe_af:b1:98 | Apple_10:6a:f5 | 802.11 | 411 | Probe Response, Sfi=2348, Ffi=0, Flags=.....C, BI=100, SSID=FlyingIlet |

Fig. 12. Probing request e probing response

Processo de Associação

Numa rede WiFi 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 oAP 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.

12 Pergunta 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.

A imagem mostra uma sequência de tramas correspondentes a um processo de associação entre a STA Apple_10:6a:f5 e o AP HitronTe_af:b1:98.

| | | | | |
|----------------|-------------------|-----------------------------|----------------------------------|--|
| 2486 70.361782 | Apple_10:6a:f5 | HitronTe_af:b1:98 | 802.11 | 70 Authentication, Sh=2542, Fh=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, Sh=2338, Fh=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, Sh=2543, Fh=0, Flags=.....C, SSID=Flyinglet |
| 2491 70.383073 | | 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, Sh=2339, Fh=0, Flags=.....C |
| 2493 70.389352 | | HitronTe_af:b1:98 (. 802.11 | 39 Acknowledgement, Flags=.....C | |

Fig. 13. Processo de associação

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

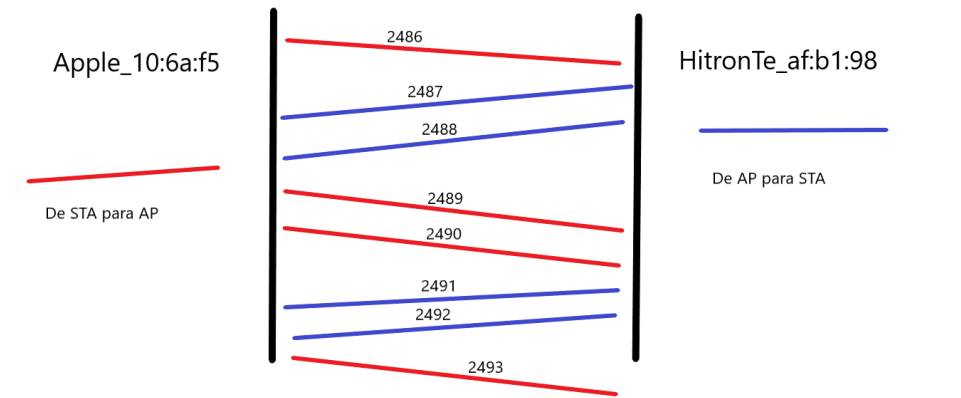


Fig. 14. Diagrama

Transferência de Dados

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

14 Pergunta 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?

```
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
```

Fig. 15. Flag DS

O valor de From DS tem o valor igual a 1 e a flag To DS tem valor igual a 0, logo a trama recebida está a vir do sistema de distribuição e não será local à WLAN.

15 Pergunta 15: Para a trama de dados nº455, transcreva os endereços MAC em uso, identificando qual o endereço MAC correspondente a ohost sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição?

O endereço MAC da STA é Apple_71:41:a1, o AP HitronTe_af:b1:98 e o router de acesso ao sistema tem o endereço MAC HitronTe_af:b1:98.

```
> 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)
```

Fig. 16. Endereços MAC

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

A trama 457 tem a flag To Ds com valor igual a 1 e a flag From DS com valor igual a 0, mostrando, assim, que a trama está a ser transmitida para fora da rede local.

```
▼ 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
```

Fig. 17. Trama 457

```
Type/Subtype: QoS Data (0x0028)
> Frame Control Field: 0x8841
.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)
```

Fig. 18. Trama 457

17 Pergunta 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.)

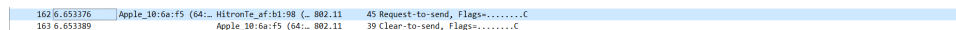
| | | | | |
|---------------|-------------------|-------------------|--------|---|
| 455 18.536644 | HitronTe_af:b1:98 | Apple_71:41:a1 | 802.11 | 226 QoS Data, Sfi=276, Ffi=0, Flags=p....F.C |
| 456 18.536653 | HitronTe_af:b1:98 | HitronTe_af:b1:98 | 802.11 | 39 Acknowledgement, Flags=.....C |
| 457 18.539762 | Apple_71:41:a1 | HitronTe_af:b1:98 | 802.11 | 178 QoS Data, Sfi=3269, Ffi=0, Flags=p.....TC |

Fig. 19. Pacotes QoS

Como vemos na imagem, vemos o envio de duas tramas QoS (Quality of Service), com o envio de uma terceira trama entre as duas, sendo uma trama de Acknowledgement. Uma vez que as redes WiFi são muito mais propícias a sofrerem colisões do que uma rede Ethernet (devido à liberdade dos dispositivos transmitirem informação sempre que quiserem), o envio da trama de controlo após a transferência de dados permite saber se houve, ou não, erro ao transmitir a primeira trama.

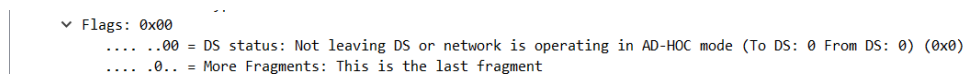
Devido a este mecanismo, o dispositivo consegue saber se deve, ou não, reenviar o pacote, consoante tenha ocorrido algum erro.

18 Pergunta 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.



162 6.653376 Apple_10:6a:f5 (64:.. HitronTe_af:bl:98 (.. 802.11 45 Request-to-send, Flags=.....C
163 6.653389 Apple_10:6a:f5 (64:.. 802.11 39 Clear-to-send, Flags=.....C

Fig. 20. Tramas RTS e CTS



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

Fig. 21. Flags to DS e From DS

O valor das flags To DS e From DS é igual a 0, mostrando que as redes estão a operar a um nível local. O STA Apple_71:41a1) envia um RTS para o AP HitronTe_af:bl:98. Posteriormente, o AP envia um CTS para o STA.

19 Conclusão

Este último trabalho prático incidiu, principalmente, na abordagem de redes sem fios. Durante a realização do mesmo, analisamos a conexão entre STA e APs eo envio de tramas como Beacon, probing requests, probing responses, RTS e CLS. Através da análise de cada uma dessas tramas, percebemos a sua importância em gerir uma rede sem fios e em como interpretar os seus dados.