

# Redes Sem Fios (802.11)

Etienne Costa(A76089)      Joana Cruz(A76270)  
Rafael Alves(A72629)

## Resumo

Este Trabalho tem como objectivo explorar vários aspectos do protocolo IEEE 802.11, tais como o formato das tramas, o enquadramento dos componentes envolvidos na comunicação sem fios, os tipos de tramas mais comuns, bem como a operação do protocolo.

## 1 Acesso Rádio

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

**Solution:** A rede sem fios está a operar a uma frequência de 2467 MHz, sendo que essa frequência corresponde ao canal 12.

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

**Solution:** A versão da norma IEEE 802.11 que está a ser utilizada é a 802.11g.

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.

**Solution:** A trama escolhida foi enviada com um débito de 1,0 Mb/s. Não, visto que o débito máximo que a interface Wifi pode operar são 54 Mbps.

```
▶ Frame 355: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
▶ Radiotap Header v0, Length 25
▼ 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): -61dBm
  Noise level (dBm): -87dBm
  TSF timestamp: 34443164
  ▶ [Duration: 2360µs]
▶ IEEE 802.11 Beacon frame, Flags: .....C
▶ IEEE 802.11 wireless LAN
```

Figura 1: Trama 355

## 2 Scanning Passivo e Scanning Ativo

1. 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 subtipo. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?

**Solution:** A figura 2 corresponde a trama selecionada, como podemos constatar na imagem podemos afirmar que é uma management frames ou seja tramas de gestão. Os valores dos seus identificadores de tipo e subtipo são os seguinte:

**Type :** 0 (1)

**Subtype :** 8 (2)

Estes valores podem ser encontrados no cabeçalho Frame Control Field.

2. 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.

**Solution:** Sendo que os SSIDs estão contidos nas tramas de gestão cujo valor do seu identificador de tipo é igual a 0 utilizamos o seguinte comando para filtrar as respectivas tramas de gestão.

*wlan.fc.type* == 0 (3)

De modo a filtrar os SSIDs dos APs que estão a operar na vizinhança da STA de captura necessitamos de filtrar as tramas de gestão cujo valor do identificador de subtipo é igual a 1 que por sua vez corresponde as tramas de anúncio (Beacon) utilizamos o seguinte comando para filtrar.

*wlan.fc.subtype* == 8 (4)

Fundindo os dois comando conseguimos listar os seguintes SSIDs:

- FlyingNet.
- NOS\_WIFI\_Fon.

355	14.643405	HitronTe_af:b1:98	Broadcast	802.11	296 Beacon frame, SN=2369, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
356	14.645055	HitronTe_af:b1:99	Broadcast	802.11	285 Beacon frame, SN=2370, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

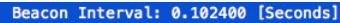
Figura 2: SSIDs Listados.

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

**Solution:** Podemos afirmar que está a ser usado o método de detecção de erros e que as tramas Beacon estão a ser recebidas corretamente visto que o status da frame check sequence é GOOD. A detecção de erros é usada neste tipo de redes locais pois a probabilidade de ocorrência de colisões é muito elevada levando assim a uma grande ocorrência de erros.

4. 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.

**Solution:** O intervalo de tempo previsto entre tramas beacon consecutivas é 0.1024 segundos. Na prática a periodicidade de tramas beacon não é verificada devido as colisões que ocorrem, algumas tramas são adiadas.




Beacon Interval: 0.102400 [Seconds]

Figura 3: Beacon Interval

5. 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.


**Solution:** O endereço MAC cujo SSID do AP é Flyingnet é o: **bc:14:01:af:b1:98**



Source address: HitronTe\_af:b1:98 (bc:14:01:af:b1:98)

Figura 4: SSID:FlyingNet

O endereço MAC cujo SSID do AP é NOS\_WIFI\_Fon é o: **bc:14:01:af:b1:99**

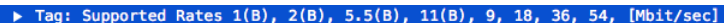


Source address: HitronTe\_af:b1:99 (bc:14:01:af:b1:99)

Figura 5: SSID:NOS WIFI Fon

6. As tramas beacon anunciam que o AP pode suportar vários débitos de base assim como vários "extended supported rates". Indique quais são esses débitos?

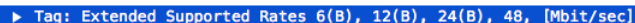
**Solution:** Os vários débitos de base que o AP pode suportar são:



► Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]

Figura 6: Supported Rates

Os vários extended supported rates são:



► Tag: Extended Supported Rates 6(B), 12(B), 24(B), 48, [Mbit/sec]

Figura 7: Supported Rates

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

**Solution:** Visto que os valores dos identificadores de subtipos de tramas probing request e reply são 4 e 5 temos o seguinte filtro:

*wlan.fc.type == 0 && (wlan.fc.subtype == 4 || wlan.fc.subtype == 5)*  
(5)

No.	Time	Source	Destination	Protocol	Info
1300	53.746911	Apple_10:6a:f5	Broadcast	802.11	Probe Request, SN=2516, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2467	70.147855	ea:a4:64:7b:b9:7a	Broadcast	802.11	Probe Request, SN=2540, FN=0, Flags=.....C, SSID=2WIRE-PT-431
2468	70.149098	ea:a4:64:7b:b9:7a	Broadcast	802.11	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	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	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	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	Probe Response, SN=2335, FN=0, Flags=.....C, BI=100, SSID=N05_WIFI_Fon
2477	70.152099	HitronTe_af:b1:99	ea:a4:64:7b:b9:7a	802.11	Probe Response, SN=2336, FN=0, Flags=.....C, BI=100, SSID=N05_WIFI_Fon
2479	70.152570	HitronTe_af:b1:99	ea:a4:64:7b:b9:7a	802.11	Probe Response, SN=2337, FN=0, Flags=.....C, BI=100, SSID=N05_WIFI_Fon
2603	72.179215	Apple_10:6a:f5	Broadcast	802.11	Probe Request, SN=2563, FN=0, Flags=.....C, SSID=FlyingNet
2606	72.179924	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	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	Probe Response, SN=2347, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Figura 8: Probe Request e Probe Response

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?

**Solution:** Quando uma STA está a procura de uma rede, ela envia uma trama chamada probe request, contendo o SSID da rede que ela procura. O AP que tiver o SSID em questão, envia o probe response. Com base nisso Temos a STA (Apple\_10:6a:f5) que envia uma trama probe request com o SSID igual a FlyingNet em broadcast ou seja para todos os APs. Uma vez que o AP(HitronTe\_af:b1:98) com o SSID específico foi encontrado, a estação inicia os passos de autenticação e associação para entrar na rede através deste AP.

2603	72.179215	Apple_10:6a:f5	Broadcast	802.11	Probe Request, SN=2563, FN=0, Flags=.....C, SSID=FlyingNet
2606	72.179924	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	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	Probe Response, SN=2347, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2610	72.181275	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	Probe Response, SN=2348, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Figura 9: Probe Request com Probe Response

```

▶ Frame 355: 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 0100 0001 .... = Sequence number: 2369
    Frame check sequence: 0x95a9c954 [correct]
    [FCS Status: Good]
▶ IEEE 802.11 wireless LAN

```

Figura 10: Trama Beacon 355

### 3 Processo de Associação

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.

2483	70.348997	HitronTe_af:b1:98	Broadcast	802.11	Beacon frame, SN=3457, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2484	70.350698	HitronTe_af:b1:99	Broadcast	802.11	Beacon frame, SN=3458, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2485	70.352671		Broadcom_04:6a:f5 (e0:3...	802.11	Clear-to-send, Flags=.....C
2486	70.361782	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	Authentication, SN=2542, FN=0, Flags=.....C
2487	70.362050		Apple_10:6a:f5 (64:9a:b...	802.11	Acknowledgement, Flags=.....C
2488	70.381869	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	Authentication, SN=2338, FN=0, Flags=.....C
2489	70.381878		HitronTe_af:b1:98 (bc:1...	802.11	Acknowledgement, Flags=.....C
2490	70.383512	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	Association Request, SN=2543, FN=0, Flags=.....C, SSID=FlyingNet
2491	70.383873		Apple_10:6a:f5 (64:9a:b...	802.11	Acknowledgement, Flags=.....C
2492	70.389339	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	Association Response, SN=2339, FN=0, Flags=.....C
2493	70.389352		HitronTe_af:b1:98 (bc:1...	802.11	Acknowledgement, Flags=.....C

Figura 11: Processo de associação completo.

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

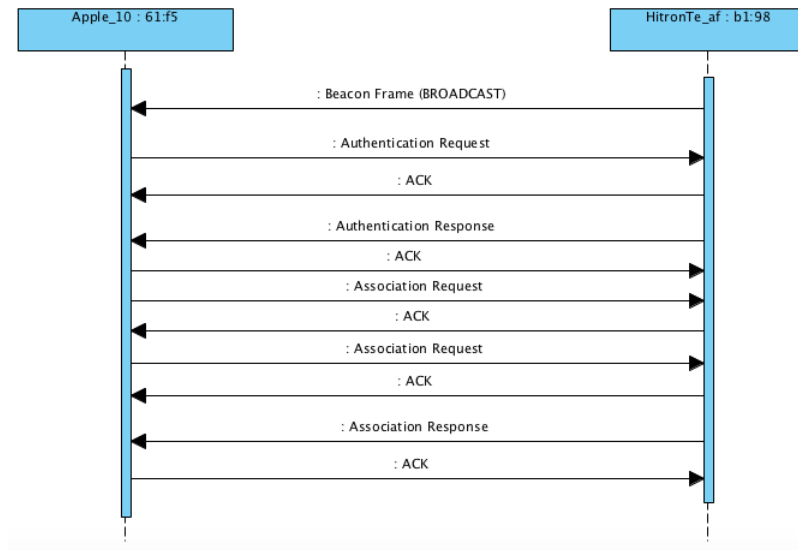


Figura 12: Sequência de tramas trocadas.

## 4 Transferência de Dados

1. 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?

**Solution:** Nesta trama a direccionalidade é : Frame from DS to a STA via AP (To Ds: 0 From Ds: 1).

2. 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?

**Solution:**

MAC STA (Receiver Address) : d8:a2:5e:71:41:a1.

MAC AP (Transmitter Address): bc:14:01:af:b1:98.

MAC Router (Source Address) : bc:14:01:af:b1:98.

```

455 18.536644 HitronTe_af:b1:98 Apple_71:41:a1 802.11 QoS Data, SN=276, FN=0, Flags=.p....F.C
.... ..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)

```

Figura 13: Frame 455 Adressing

3. Como interpreta a trama nº457 face à sua direccionalidade e endereçamento MAC?

**Solution:** Nesta trama a direccionalidade é : Frame from DS to a STA via AP (To Ds: 1 From Ds: 0).

MAC Router (Destination Address) : bc:14:01:af:b1:98.

MAC STA (Source Address): d8:a2:5e:71:41:a1.

MAC AP (Receiver Address) : bc:14:01:af:b1:98.

```

457 18.539762 Apple_71:41:a1 HitronTe_af:b1:98 802.11 QoS Data, SN=1209, FN=0, Flags=.p....TC
.... ..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)

```

Figura 14: Frame 457 Adressing

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.)

**Solution:** O subtipo de tramas de controlo transmitidas ao longo da transferência de dados acima mencionada é a Acknowledgment ou seja trama de confirmação da recepção. Elas têm que existir de modo a ser possível fazer a deteção de erros, sendo que quando não são encontrados erros é enviada uma Trama ACK para a STA emissora.

5. O uso de trama 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.

**Solution:** Relativamente a direccionalidade visto que estamos perante a tramas de dados os valores da direccionalidade serão sempre (To DS:0 From DS:0).

- STA:Apple\_10:6a:f5.
- AP:HitronTe\_af:b1:98.

wlan.fc.type==1&&(wlan.fc.subtype==11 wlan.fc.subtype==12)					
No.	Time	Source	Destination	Protocol	Info
8770	102.960131	Apple_10:6a:f5 (64:...	HitronTe_af:b1:98 (bc:1...	802.11	Request-to-send, Flags=.....C
8771	102.960136		Apple_10:6a:f5 (64:9a:b...	802.11	Clear-to-send, Flags=.....C
8775	102.960738	HitronTe_af:b1:98 (...)	Apple_10:6a:f5 (64:9a:b...	802.11	Request-to-send, Flags=.....C
8776	102.960743		HitronTe_af:b1:98 (bc:1...	802.11	Clear-to-send, Flags=.....C
▶ Frame 8770: 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)					

Figura 15: Tramas Request To Sent e Clear To Send

## 5 Conclusão

O protocolo de comunicação sem fios 802.11, dado as características do meio, exige uma implementação mais complexa do que o protocolo Ethernet anteriormente estudado. Este facto leva a existência de tramas com cabeçalhos mais complexos e de tamanho superior, que desempenham funções de controlo de erros e garantem a estabilidade das conexões. Uma das formas de garantir esta propriedade é através das tramas Beacon enviadas pelos APs que permitem que as stations optem pelo AP mais favorável. O processo de estabelecimento de uma conexão sem fios é conhecido por Associação, sendo precedido de uma fase de autenticação da station por parte do AP que rejeita ou aceita a identidade do primeiro. A transmissão de dados em redes sem fios é auxiliada pela troca de tramas de Acknowledgment(ACK) que confirmam a receção (correta) de uma determinada trama, sendo por vezes precedidas de tramas RTS e CTS que têm o intuito de prevenir a ocorrência de colisões durante a transmissão.