# TP3: Redes sem fios (802.11)

**Universidade do Minho**
**Daniel Regado, Maria Barbosa**
**[a85137,a85290]@alunos.uminho.pt**

## 4. Acesso Rádio

1. Está a operar a uma frequência de 2437MHz no canal 6.

   Para a trama 14, de acordo com o nosso grupo:

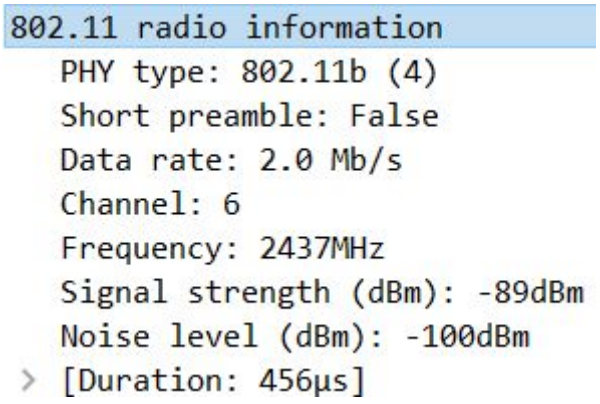
   ```
   802.11 radio information
       PHY type: 802.11b (4)
       Short preamble: False
       Data rate: 2.0 Mb/s
       Channel: 6
       Frequency: 2437MHz
   ```

   **Table 36—Operating frequency range**

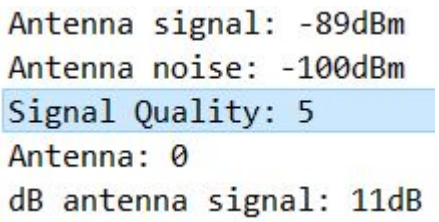
| Lower Limit | Upper limit | Regulatory range | Geography |
|---|---|---|---|
| 2.402 GHz | 2.480 GHz | 2.400–2.4835 GHz | North America |
| 2.402 GHz | 2.480 GHz | 2.400–2.4835 GHz | Europe[a] |
| 2.473 GHz | 2.495 GHz | 2.471–2.497 GHz | Japan |
| 2.447 GHz | 2.473 GHz | 2.445–2.475 GHz | Spain |
| 2.448 GHz | 2.482 GHz | 2.4465–2.4835 GHz | France |
| NOTE—The frequency ranges in this table are subject to the geographic-specific regulatory authorities. | | | |

   [a]Excluding Spain and France.

2. Quanto ao tipo do canal, este é do tipo 802.11b, e está com um débito de 2.0Mb/s.

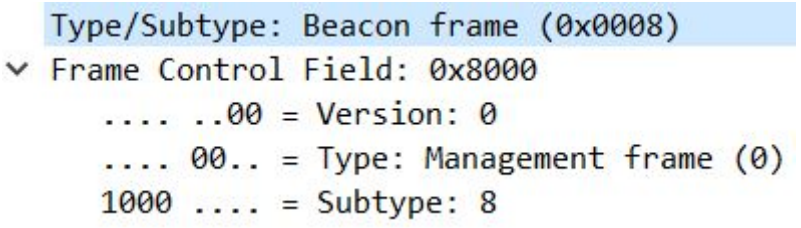



3. A qualidade do sinal é 5 (qualidade muito reduzida).




# 5. TRAMAS BEACON

4. Um beacon é do tipo Management frame, sendo os identificadores de tipo 0x0 e de subtipo 0x8. Esta informação encontra-se no Frame Control Field.




5. Encontramos 2 redes, uma com SSID linksys12 e outra 30 Munroe St Depois de analisar vários pacotes, concluímos que o que tem melhor sinal é o linksys12, com força de sinal a rondar os -90 dBm, comparando com valores que rondam -30 dBm do outro AP.

   Para o AP linksys12 (trama 16):

```
Frequency: 2437MHz
Signal strength (dBm): -92dBm
Noise level (dBm): -100dBm
```

Para o AP 30 Munroe St (trama 17):

```
Frequency: 2437MHz
Signal strength (dBm): -29dBm
Noise level (dBm): -100dBm
```

6. Nos beacons, quando analisamos os endereços de receiver, destination, transmitter e source, verificamos que em todos os casos, os endereços de receiver e destination corresponder a broadcast (ff:ff:ff:ff:ff:ff), e os restantes endereços (source e transmitter) correspondem ao endereço do AP que está a transmitir a trama beacon.

   Exemplos:
   Trama 13 (breacon de 30 Munroe St)

```
IEEE 802.11 Beacon frame, Flags: ........C
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
```

   Trama 16 (beacon de linksys12)

```
IEEE 802.11 Beacon frame, Flags: ........C
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: LinksysG_67:22:94 (00:06:25:67:22:94)
Source address: LinksysG_67:22:94 (00:06:25:67:22:94)
```

7. No caso dos probe request, estes são endereçados como broadcast. Posteriormente, os probe response são endereçados a quem fez o probe request.
   Tem o propósito de fazer procura ativa de APs. Em vez de esperar por beacons (procura passiva), uma STA envia um probe request em broadcast,

e espera que APs respondam.

```
1629 46.780197    IntelCor_d1:b6:4f  Broadcast          802.11    82 Probe Request, SN=1577, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
1630 46.781816    Cisco-Li_f7:1d:51  IntelCor_d1:b6:4f  802.11   177 Probe Response, SN=3559, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
```

Neste exemplo, temos a station com SSID Wildcard a fazer um probe request (em broadcast como é suposto), com o posterior probe response do AP com SSID 30 Munroe St.

# 6. TRANSFERÊNCIA DE DADOS

8. Para o HTTP GET (trama 1016): Frame from STA to DS via an AP

```
▾ Flags: 0x01
      .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
```

Para o HTTP RESPONSE (trama 1066) Frame from DS to a STA via AP

```
▾ Flags: 0x02
      .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
```

9. Estão presentes 3 endereços MAC em uso, (00:16:b6:f7:1d:51), (00:16:b6:f4:eb:a8) e (00:13:02:d1:b6:4f).
Estes têm a seguintes correspondência:

Host sem fios: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) (Source e Transmitter)
AP: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51) (Receiver)
Router de acesso ao DS: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8) (Destination)

```
Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
```

10. Estão presentes na mesma 3 endereços MAC em uso, (00:16:b6:f7:1d:51), (00:16:b6:f4:eb:a8) e (00:13:02:d1:b6:4f).
    Estes têm as seguintes correspondências:

    Host sem fios: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) (Destination e Receiver)
    AP: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51) (Transmitter)
    Router de acesso ao DS: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8) (Source)

```
Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Destination address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
```

# 7. ASSOCIAÇÃO E DESASSOCIAÇÃO

11. O campo Authentication Algorithm indica-nos que o host não está a tentar usar nenhum algoritmo de autenticação nem chave, e que está a tentar aceder de forma aberta (Authentication Algorithm: Open System (0)).
    Não existe nenhuma resposta porque a autenticação no AP linksys_SES_24086 não é válida, e por essa razão, não existe nenhuma trama “Association Response”.

    (Trama 1921)

```
IEEE 802.11 wireless LAN
▾ Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0001
      Status code: Successful (0x0000)
```

    (Tramas seguintes, sem Association Response)

```
1921 57.889232   IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11    58 Authentication, SN=1619, FN=0, Flags=........C
1922 57.890325   IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11    58 Authentication, SN=1619, FN=0, Flags=....R...C
1923 57.891321   IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11    58 Authentication, SN=1619, FN=0, Flags=....R...C
1924 57.896970   IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11    58 Authentication, SN=1619, FN=0, Flags=....R...C
1925 57.902320                      Cisco-Li_f5:ba:b…  802.11    38 Acknowledgement, Flags=........C
1926 57.903699   IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11   107 Association Request, SN=1620, FN=0, Flags=........C, SSID=linksys_SES_24086
1927 57.904945   IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb  802.11   107 Association Request, SN=1620, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1928 57.906194                      Cisco-Li_f5:ba:b…  802.11    38 Acknowledgement, Flags=........C
```

12. As tramas usadas para a tentativa de associação ao AP 30 Munroe St. estão apresentadas em baixo, de forma cronológica (colocada a última trama em caso de retransmissão).

| | | | | | | |
|---|---|---|---|---|---|---|
| 2152 | 63.140106 | IntelCor_d1:b6:4f | Broadcast | 802.11 | 94 | Probe Request, SN=1647, FN=0, Flags=........C, SSID=30 Munroe St |
| 2153 | 63.142451 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 177 | Probe Response, SN=3724, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 2156 | 63.168087 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 58 | Authentication, SN=1647, FN=0, Flags=........C |
| 2160 | 63.169707 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 58 | Authentication, SN=1647, FN=0, Flags=....R...C |
| 2162 | 63.169910 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 89 | Association Request, SN=1648, FN=0, Flags=........C, SSID=30 Munroe St |
| 2166 | 63.192101 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 94 | Association Response, SN=3728, FN=0, Flags=........C |

# Conclusões

Este trabalho foi realizado, com o objetivo de aprofundar conhecimentos sobre os conteúdos lecionados nas aulas teóricas de sistemas e comunicação de redes no âmbito do capítulo Redes Wireless, focando-se na operação do protocolo IEEE 802.11, formato das tramas e no endereçamento dos componentes envolvidos na comunicação sem fios.

Através da sua realização, foi possível verificar na rede que efetivamente, tal como se tinha estudado nas aulas teóricas, o AP, com o objetivo de anunciar a sua presença, faz o envio periódico de tramas beacon em broadcast (envia para todas as interfaces rádio que estão dentro do seu alcance). Conseguimos também verificar a existência de tramas probe request e probe response como método alternativo de scanning passivo.

Uma vez que há a necessidade de um host se associar a um ponto de acesso antes de efetuar o envio dos dados, tivemos a oportunidade de entender melhor o

funcionamento do processo de associação, através da análise das tramas association request enviada pelo host e da trama association response enviado pelo AP. Foi também objeto de estudo a transferência de dados sobre um host já associado com o AP, estudando a direcionalidade das tramas, que se torna fundamental para entender os endereços MAC em redes sem fios.

Consideramos que os objetivos deste trabalho foram alcançados, uma vez que permitiu a consolidação de conteúdos previamente lecionados bem como adquirir novos conhecimentos.