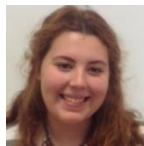




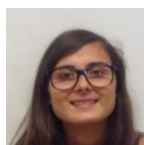
Universidade do Minho
Escola de Engenharia

Redes de Computadores:
Redes Sem Fios 802.11

Grupo de Trabalho 2



Ana Esmeralda Fernandes A74321



Bárbara Nadine Freitas Oliveira A75614



Miguel Dias Miranda A74726

Novembro de 2016



Conteúdo

Parte 4: Acesso Rádio	3
Parte 5: Beacon	4
Parte 6: Transferência de Dados	7
Parte 7: Associação e Desassociação	9
Conclusão	11

Parte 4: Acesso Rádio

- 1) Identifique em que frequência do espectro está a operar a rede sem fios, e o canal a que corresponde essa frequência (pode confirmar com a normal IEEE 802,11).

Tendo como objeto de estudo a trama 22 da captura fornecida, a mesma foi transmitida numa rede que estava a operar no canal 6 a uma frequência de 2437MHz.

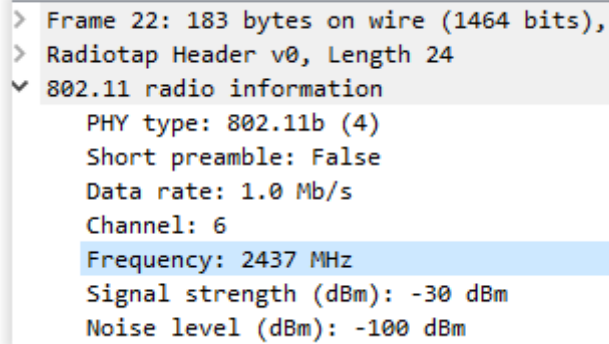


Figura 1- Canal e frequência da trama 22

- 2) Qual o tipo do canal que está a ser usado para a comunicação rádio? Qual o débito a que foi enviada a trama escolhida?

O canal usado é do tipo 802.11b e o débito da trama é de 1Mb/s.

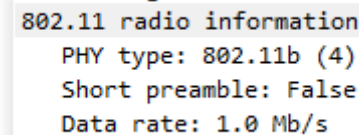


Figura 2- Tipo do canal trama 22

- 3) Indique qual o índice de qualidade do sinal.

A qualidade do sinal apresenta um índice de qualidade de 94%.

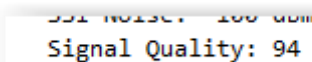


Figura 3 - Qualidade do sinal da trama 22

Parte 5: Beacon

- 4) **Qual o tipo de trama Beacon? Indique quais os seus identificadores de tipo e subtipo. Em que parte da trama estão especificados?**

A trama Beacon é do tipo Management Frame e subtipo 0x0008, que são especificados no primeiro header da trama, designado de frame control field.

```
▼ 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 4 - Tipo da trama 22

- 5) **Identifique os SSIDs dos APs (Access Points) que estão a operar na rede e diga qual tende a proporcionar a melhor qualidade de sinal?**

Alguns dos SSIDs encontrados na captura: 30 Munroe St, Linksys_SES_24086, Linksys, BOWDOIN, BOHO2, concouse, phoiphaz.

Dos SSIDs encontrados o 30 Munroe St é o AP de quem mais se receberam tramas beacon e aquele que apresenta sempre os maiores valores de Signal Quality. É, portanto, o AP mais usado.

```
SSID=30 Munroe St  SSID=BOWDOIN  SSID=phoiphaz  SSID=linksys_SES_24086
SSID=concouse
```

Figura 5 - Alguns dos SSID encontrados. Por análise do campo Radiotap Header v0/Signal Quality concluímos que o AP 30 Munroe St é o que tem sempre melhor qualidade de sinal

6) Para dois APs identificados, indique quais são os intervalos de tempo previstos entre as transmissões de tramas Beacon? Na prática, a periodicidade de tramas Beacon é verificada? Tente explicar porquê?

Considerando a nossa frame 22 relativa ao AP 30 Munroe St, o intervalo de tempo indicado no campo Beacon interval é de 0.102400 segundos. Analisando o tempo entre os vários Beacon deste AP concluímos que o período de tempo é aproximadamente constante entre cada beacon. No entanto não podemos generalizar estes registos para todos os AP porque para nos restantes a periodicidade não é verificada. Tal facto poderá acontecer pela distância a que os outros AP se encontram da nossa estação de acesso o que causa que nem todas as comunicações cheguem até ao nosso AP ou cheguem com erros. Por outro lado, podem também não manter a sua periodicidade porque quando a AP tenta enviar o seu beacon, pode não ter permissão para enviar naquele instante (por haver outras comunicações ativas na rede) e, portanto, tem que ficar em idle e esperar um momento oportuno para enviar o beacon, perdendo assim a periodicidade teórica.

1 0.000000	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
3 0.085474	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4 0.187919	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
9 0.290284	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2857, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
11 0.393174	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2858, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
13 0.495032	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2859, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
15 0.597382	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2860, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
17 0.699847	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2861, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
18 0.802226	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2862, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
19 0.904619	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2863, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
20 1.007015	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2864, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
22 1.109406	Cisco-Li_f7:1d:51	Broadcast	802.11	Beacon Interval: 0.102400 [Seconds]
24 1.211843	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2865, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
32 1.314223	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2868, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
33 1.416593	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2869, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
35 1.519009	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2870, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

Figura 6- Pelos valores de tempo da segunda coluna concluímos que o intervalo de tempo de envio de tramas beacon é de facto periódico e com o tempo de aproximadamente 0.104segundos entre cada novo envio.

7) Identifique e registe todos os endereços MAC usados nas tramas beacon enviadas pelos APs. Recorde que fonte, destino e BSS ID são endereços contidos no cabeçalho das tramas 802.11. Para uma descrição detalhada da estrutura da trama 802.11, consulte o anexo ao enunciado.

Nos campos BSS id, Source e Transmitter é indicado o endereço do AP. Nos campos Receiver e Destination está indicado o endereço de broadcast.

```
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)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

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)
BSS Id: LinksysG_67:22:94 (00:06:25:67:22:94)
```

Figure 7- Endereços MAC usados na trama beacon

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

Como é visível na imagem o AP 30 Munroe St da captura em análise aceita como valores de débito 1 Mbit/s, 2 Mbit/s, 5.5 Mbit/s e por fim 11 Mbit/s

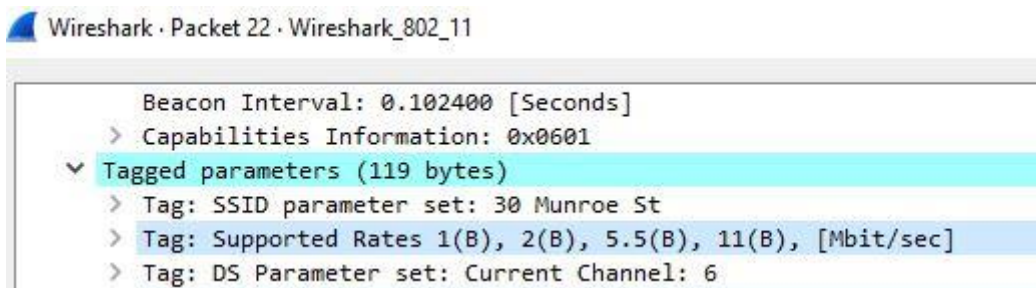


Figure 8- Débitos possíveis do AP 30 Munroe St

9) Indique a que sistemas são endereçadas estas tramas e qual o seu propósito?

Considerando alguns dos probe request em análise, verificamos que o seu destino tem como endereço MAC o valor ff:ff:ff:ff:ff:ff, ou seja, são enviados para todos os dispositivos e APs da rede. Por outro lado, o probe response já não tem como destino um broadcast geral, mas sim um endereço específico, que é quem efetuou o probe request. Este destino, ao receber os diferentes probe response fica a saber as informações e débitos possíveis das outras estações que se encontram na sua rede.

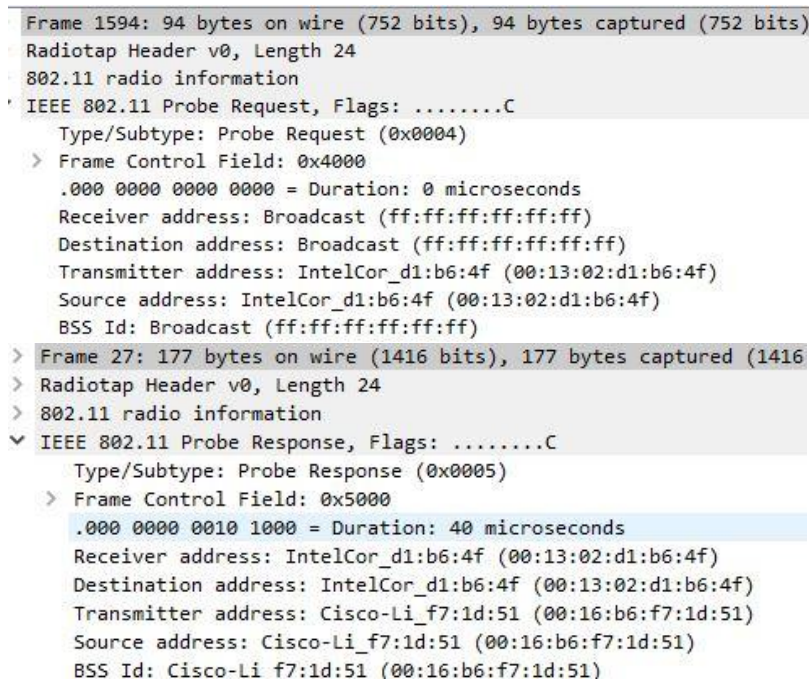
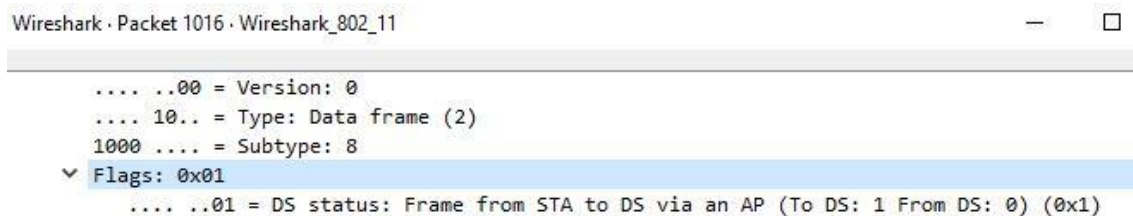


Figure 9- Exemplo de uma frame probe request com broadcast e uma probe response, com um endereço de destino específico, que indica quem realizou o probe request que gerou a resposta.

Parte 6: Transferência de Dados

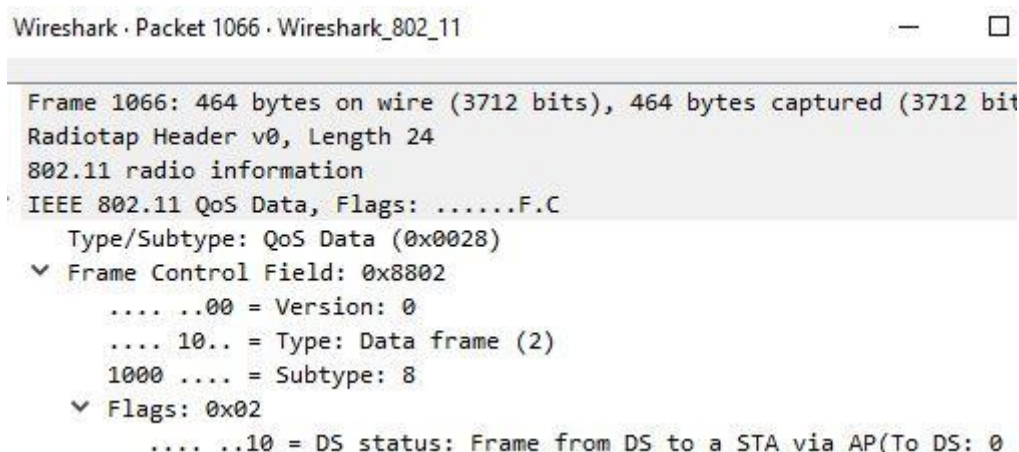
- 10) O campo Frame Control contido no cabeçalho das tramas 802.11 permite especificar a direccionalidade das tramas. Identifique a direccionalidade das tramas indicadas acima (nº1016 e nº1066). Este aspecto é fundamental para entender o endereçamento MAC em redes sem fios.



```

Wireshark · Packet 1016 · Wireshark_802_11
.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
▼ Flags: 0x01
.... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
  
```

Figure 10- frame 1016: pela flag 0x01 concluímos que é uma ligação da estação para o sistema de distribuição.



```

Wireshark · Packet 1066 · Wireshark_802_11
Frame 1066: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bit
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 QoS Data, Flags: .....F.C
Type/Subtype: QoS Data (0x0028)
▼ Frame Control Field: 0x8802
.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
▼ Flags: 0x02
.... ..10 = DS status: Frame from DS to a STA via AP (To DS: 0
  
```

Figure 11 - frame 1066: pela flag 0x02 verificamos que a ligação é realizada do sistema de distribuição para a estação.

- 11) Para a trama 802.11 que contém o pedido GET, indique os três endereços MAC em uso, identificando qual o endereço MAC correspondente ao host sem fios, ao AP e ao router de acesso ao sistema de distribuição (DS)?

Considerando o pedido na frame 1016, o endereço MAC dos host sem fios tem como endereço o valor 00:13:02:d1:b6:4f visto no campo Transmitter address. O endereço do AP é visto no Receiver address e tem como valor 00:16:b6:f7:1d:51. Por fim, o router de acesso ao DS tem o endereço 00:16:b6:f4:eb:a8 visto no campo Destination address.

```

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

Figure 12- Endereços Mac da frame 1016

12) Para a trama 802.11 que contém a resposta ao pedido GET, indique e identifique quais os três endereços MAC em uso?

Considerando a resposta ao pedido GET na frame 1066, o endereço MAC dos host sem fios tem como endereço o valor 00:16:b6:f7:1d:51 visto no campo Transmitter address. O endereço do AP é visto no Receiver address e tem como valor 00:13:02:d1:b6:4f. Por fim, o router de acesso ao DS tem o endereço 00:13:02:d1:b6:4f visto no campo Destination address.

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

Figure 13 - Endereços Mac da frame 1066

13) Que subtipo de tramas de controlo são transmitidas ao longo da interação acima mencionada? Verifique a que sistemas são endereçadas. Tente explicar porque razão têm de existir (contrariamente ao que acontece numa rede Ethernet.)

```
> [Duration: 96 us]
IEEE 802.11 QoS Data, Flags: .....TC
Type/Subtype: QoS Data (0x0028)
> Frame Control Field: 0x8801
NOISE LEVEL (uBm): -100 uBm
> [Duration: 96 us]
IEEE 802.11 QoS Data, Flags: .....F.C
Type/Subtype: QoS Data (0x0028)
> Frame Control Field: 0x8802
```

Figure 14- Subtipo da trama 1016 e 1066 respetivamente

Parte 7: Associação e Desassociação

14) Identifique e interprete as tramas 802.11 enviadas pelo host decorrentes do pedido DHCP Release que determina a quebra de associação que existia com o AP 30 Munroe ST. Segundo a norma IEEE 802.11, há alguma trama que seria esperada, mas não aparece?

Na trama 1733 o host envia o pedido “DHCP Release” com o intuito de fazer a libertação da ligação com o AP; depois na trama 1734 é feito o envio do “Acknowledgement” onde é confirmado que o pedido chegou bem; na trama 1735 é enviado um pedido de “Deauthentication” onde o host se desconecta do AP e depois dessa desconexão o host procura autenticar-se novamente a outro AP enviando varias tramas “Authentication”.

Como o host procura obter ligação com um novo AP, como é analisado pelo pedido da trama 1750 (“Association request” para linksys_SES_24086), espera que este lhe envie uma trama de associação (“Association Response”) para confirmar a possível ligação entre eles. Contudo, esta trama nunca chega a surgir.

1733	49.583615	192.168.1.109	192.168.1.1	DHCP	390 DHCP Release - Transaction ID 0xea5a526
1734	49.583771		IntelCor_d1:b6:4f	(-) 802.11	38 Acknowledgement, Flags=.....C
1735	49.609617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54 Deauthentication, SN=1605, FN=0, Flags=.....C
1736	49.609770		IntelCor_d1:b6:4f	(-) 802.11	38 Acknowledgement, Flags=.....C
1737	49.614478	IntelCor_d1:b6:4f	Broadcast	802.11	99 Probe Request, SN=1606, FN=0, Flags=.....C, SSID=linksys_SES_24086
1738	49.615869		Cisco-Li_f5:ba:bb	(-) 802.11	38 Acknowledgement, Flags=.....C
1739	49.617713		Cisco-Li_f5:ba:bb	(-) 802.11	38 Acknowledgement, Flags=.....C
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=.....C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=.....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=.....R...C
1743	49.641910		Cisco-Li_f5:ba:bb	(-) 802.11	38 Acknowledgement, Flags=.....C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=.....R...C
1745	49.644710	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=3589, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=.....R...C
1747	49.646711		Cisco-Li_f5:ba:bb	(-) 802.11	38 Acknowledgement, Flags=.....C
1748	49.647827		Cisco-Li_f5:ba:bb	(-) 802.11	38 Acknowledgement, Flags=.....C
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=.....R...C
1750	49.651078	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107 Association Request, SN=1607, FN=0, Flags=.....C, SSID=linksys_SES_24086
1751	49.653218	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107 Association Request, SN=1607, FN=0, Flags=.....C, SSID=linksys_SES_24086

Figura 15- frames para processo de desassociação e tentativa de associação com um novo AP

15) Examine o ficheiro de trace e procure tramas de autenticação enviadas pelo host para o AP. Quantas tramas de authentication são enviadas do host sem fios para o AP linksys_SES_24086?

São enviadas 19 tramas de authentication pelo host.

1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=.....C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=.....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=.....R...C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=.....R...C
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=.....R...C
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=.....R...C
1821	53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1612, FN=0, Flags=.....C
1822	53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1612, FN=0, Flags=.....R...C
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
2122	62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1644, FN=0, Flags=.....C
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1644, FN=0, Flags=.....R...C
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1644, FN=0, Flags=.....R...C
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
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58 Authentication, SN=3726, FN=0, Flags=.....C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58 Authentication, SN=3727, FN=0, Flags=.....C

Figura 16 - Tramas "Authentication" enviadas para o AP Linksys_SES_24086

16) O host tenta usar algum algoritmo de autenticação/chave ou tenta aceder de forma aberta? Existe alguma resposta do AP linksys_SES_24086 ao pedido de autenticação? Porquê?

O host utiliza o algoritmo “Open System” para se autenticar, logo tenta aceder de forma aberta. Este processo é usado quando um host tenta ganhar acesso a uma rede wifi aberta, onde ambos utilizam os mesmos protocolos de privacidade.

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

Figura 17 - Campo Authentication Algorithm da frame Authentication 1740

Da nossa análise ao problema não encontramos na captura nenhuma trama de resposta (do tipo “Association response”) por parte do AP linksys_SES_24086. Pensamos que o AP tenha rejeitado o pedido de ligação do host por serem distintos a nível de protocolos de ligação.

17) Verifique que, após a tentativa de associação falhada, o host volta a associar-se ao AP 30 Munroe ST. Identifique as tramas usadas para o efeito.

Na trama 2152 o host envia um Probe Request para o AP em 30 Munroe ST, na trama 2153 o AP referido responde ao host com uma trama Probe Response, seguido depois de um Acknowledgement por parte de Host e do envio de tramas de Authentication e Acknowledgement entre os dois sistemas.

Na trama 2162 é enviado um Association request, por parte do Host para o AP 30 Munroe St e de seguida, na trama 2166 o AP confirma este pedido de ligação do host. Concluimos que se trata de uma confirmação do pedido porque a trama de resposta enviada pelo AP tem nela informações sobre o id de ligação e as suas taxas de débito suportadas.

Com este processo o Host fica assim ligado novamente ao AP em 30 Munroe St.

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
2154 63.142860	Cisco-Li_f7:1d:51	Cisco-Li_f7:1d:51	802.11	38 Acknowledgement, Flags=.....C
2155 63.161272	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=3725, 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
2157 63.168222	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38 Acknowledgement, Flags=.....C
2158 63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58 Authentication, SN=3726, FN=0, Flags=.....C
2159 63.169592	Cisco-Li_f7:1d:51	Cisco-Li_f7:1d:51	802.11	38 Acknowledgement, 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
2161 63.169814	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38 Acknowledgement, Flags=.....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
2163 63.170008	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	38 Acknowledgement, Flags=.....C
2164 63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58 Authentication, SN=3727, FN=0, Flags=.....C
2165 63.171000	Cisco-Li_f7:1d:51	Cisco-Li_f7:1d:51	802.11	38 Acknowledgement, Flags=.....C
2166 63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94 Association Response, SN=3728, FN=0, Flags=.....C

Figura 18- Tramas 2152 até 2160 usadas para o host volta a associar-se ao AP 30 Munroe St

```
> Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Association Response, Flags: .....C
  IEEE 802.11 wireless LAN management frame
    Fixed parameters (6 bytes)
    Tagged parameters (36 bytes)
      Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
      Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
```

Figura 19 - Informação enviada na frame de Association response do AP para o Host



Conclusão

Com a realização do relatório e análise da captura pudemos ficar a compreender melhor o funcionamento das redes sem fios.

Na abordagem ao primeiro conjunto de perguntas, concluímos que o funcionamento da rede Wifi opera numa frequência próxima dos 2.4 GHz, essencialmente por uma questão de compatibilidade com serviços e equipamentos anteriores. Verificamos também que a trama analisada segue o protocolo específico 802.11b.

Na compreensão do scanning passivo, com envio de tramas Beacon, compreendemos que estas são enviadas pelos APs em broadcast, para qualquer estação que esteja no seu alcance. Com este processo, informam a sua presença e alguns dados sobre si, como o seu SSID, a qualidade do seu sinal e a que taxas de transferência/débito podem operar.

Apesar do envio destas tramas ser teoricamente periódico, a sua receção nas estações não é tão regular quanto esperado: isto acontece porque o AP pode não ter acesso à rede no momento em que pretende enviar o seu Beacon ou até mesmo porque a estação, devido à distância ou interferências, nem sempre recebe os pacotes enviados pelo AP.

Nos processos de scanning ativo, analisamos as tramas de Probe Request e Probe Response. Neste procedimento apreendemos que quando uma estação precisa de saber informações sobre alguma outra estação da sua rede, envia uma Probe Request em broadcast, para qualquer recetor que esteja na rede. A este pedido, todas as estações ou APs que se encontrem na mesma rede irão responder de forma específica à estação que realizou o Probe Request, dando-lhe algumas informações sobre si, tal como as informações disponibilizadas em tramas beacon.

Por fim, na análise dos processos de associação e desassociação esclarecemos o funcionamento das tramas de Autenticação e Confirmação, quando uma estação ou AP confirma a chegada de um pedido. Concluímos também que um AP pode rejeitar a associação com um determinado Host se os seus protocolos de ligação forem distintos. Nesta situação de rejeição o host procura um novo AP ou volta a associar-se com o AP com que estava anteriormente ligado.

Ana Esmeralda Fernandes A74321
Bárbara Nadine Freitas Oliveira A75614
Miguel Dias Miranda A74726

Redes de Computadores
TP3: Redes sem Fios 802.11
Novembro de 2016