Redes de Computadores – TP3

Acesso Rádio

1 – Identifique em que frequência do espectro está a operar a rede sem fios, e o canal corresponde essa frequência (pode confirmar com a norma IEEE 802.11).

A rede sem fios está a operar a 2.4Ghz no canal 6.

```
802.11 radio information
    PHY type: 802.11g (6)
    Short preamble: False
    Proprietary mode: None (0)
    Data rate: 24.0 Mb/s
    Channel: 6
    Frequency: 2437 MHz
    Signal strength (dBm): -23 dBm
    Noise level (dBm): -100 dBm
```

2 – Qual o tipo de canal que está a ser usado para a comunicação rádio? Qual o débito a que foi enviada a trama escolhida?

Está a ser usado um canal do tipo 802.11g, com um débito de 24.0Mb/s.

```
802.11 radio information
    PHY type: 802.11g (6)
    Short preamble: False
    Proprietary mode: None (0)
    Data rate: 24.0 Mb/s
    Channel: 6
    Frequency: 2437 MHz
    Signal strength (dBm): -23 dBm
    Noise level (dBm): -100 dBm
```

3 – Indique qual o índice de qualidade de sinal.

O índice de qualidade de sinal é de 64.

```
SSI Signal: -23 dBm
SSI Noise: -100 dBm
Signal Quality: 64
```

Tramas Beacon

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

A trama Beacon é uma trama de gestão, com o identificador 0x0008.

```
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
```

```
0000  00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e3 9c   .....X..........
0010  52 00 00 47 08 26 7e 05 80 00 00 00 ff ff ff ff   R..G.&~.........
0020  ff ff 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 60 b2   .......Q.....Q`.
0030  82 e1 38 96 28 00 00 00 64 00 01 06 00 0c 33 30   ..8.(...d.....30
0040  20 4d 75 6e 72 6f 65 20 53 74 01 04 82 84 8b 96    Munroe St......
0050  03 01 06 05 04 00 01 00 00 07 06 55 53 49 01 0b   ...........USI..
0060  1a 0c 12 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e   .........'...BC^
0070  00 62 32 2f 00 2a 01 00 32 08 8c 12 98 24 b0 48   .b2/.*..2....$.H
0080  60 6c dd 15 00 0a f5 0a 02 40 c0 00 03 01 03 05   `l.......@......
0090  0e 04 ff 00 03 00 11 01 01 dd 18 00 50 f2 02 01   ............P...
00a0  01 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e 00 62   .......'...BC^.b
00b0  32 2f 00 08 26 7e 05                             2/..&~.
```

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

Os SSID dos APs são: “30 Munroe Street”, “linksys12”, “Broadcast”, “linksys_SES_24086”, “Home WIFI”, “phoiphas”, “concourse”, “linksys”, “BOHO2” e “BOWDOIN”. O serviço que proporciona a melhor qualidade de sinal é o “30 Munroe Street”, visto que o valor da qualidade de sinal varia sempre entre 70 e 100.

```
.C, SSID=30 Munroe St
.C, SSID=Broadcast
.C, SSID=Broadcast
.C, SSID=linksys_SES_24086
.C, SSID=linksys_SES_24086
.C, SSID=linksys_SES_24086
.C, SSID=Broadcast
.C, SSID=linksys_SES_24086
.C, SSID=linksys_SES_24086
.C, SSID=30 Munroe St
C, SSID=Home WIFI
C, SSID=phoiphas
C, SSID=concourse
C, SSID=Broadcast
C, SSID=linksys
C, SSID=hfmpc
C, SSID=BOHO2
C, SSID=BOWDOIN
C, SSID=Broadcast
```

6 – Para dois dos APs identificados, indique quais são os intervalos de tempo previstos entre as transmissões de tramas *beacon*? (nota: este valor é anunciado na própria trama *beacon*). Na prática, a periocidade de tramas *beacon* é verificada? Tente explicar porquê.

Para o AP "30 Monroe Street", o intervalo de tempo entre transmissões beacon é de 0.1024 segundos, e para o AP "linksys12", o intervalo de tempo é de 0.1024 segundos, o mesmo para o AP anterior.

```
IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
        Timestamp: 0x000000289638e182
        Beacon Interval: 0.102400 [Seconds]
        Capabilities Information: 0x0601
```

AP: 30 Munroe Street

```
IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
        Timestamp: 0x000008ac05a41380
        Beacon Interval: 0.102400 [Seconds]
        Capabilities Information: 0x0011
```

AP: linksys12

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.

Os endereços MAC da trama beacon associada ao AP "30 Munroe Street" são os seguintes:

- ff:ff:ff:ff:ff:ff

- 00:16:b6:f7:1d:51

- 00:16:b6:f7:1d:51 (BSS ID)

```
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)
```

```
0000  00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e3 9c
0010  52 00 00 47 08 26 7e 05 80 00 00 00 ff ff ff ff
0020  ff ff 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 60 b2
0030  82 e1 38 96 28 00 00 00 64 00 01 06 00 0c 33 30
0040  20 4d 75 6e 72 6f 65 20 53 74 01 04 82 84 8b 96
0050  03 01 06 05 04 00 01 00 00 07 06 55 53 49 01 0b
0060  1a 0c 12 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e
0070  00 62 32 2f 00 2a 01 00 32 08 8c 12 98 24 b0 48
0080  60 6c dd 15 00 0a f5 0a 02 40 c0 00 03 01 03 05
0090  0e 04 ff 00 03 00 11 01 01 dd 18 00 50 f2 02 01
00a0  01 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e 00 62
00b0  32 2f 00 08 26 7e 05
```

Os endereços MAC da trama beacon associada ao AP “linksys_SES_24086” são os seguintes:

- ff:ff:ff:ff:ff:ff
- 00:18:39:f5:ba:bb
- 00:18:39:93:b9:bb

```
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
Source address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
BSS Id: Cisco-Li_93:b9:bb (00:18:39:93:b9:bb)
00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 a3 9c   .....X.. ........
0b 00 00 07 32 a9 ba cd  80 00 00 00 ff ff ff ff   ....2... ........
ff ff 00 18 39 f5 ba bb  00 18 39 93 b9 bb 90 ef   ....9... ..9.....
96 f1 8f ef c6 05 00 00  64 00 11 00 00 11 6c 69   ........ d.....li
6e 6b 73 79 73 5f 53 45  53 5f 32 34 30 38 36 01   nksys_SE S_24086.
04 82 84 8b 96 03 01 06  05 04 00 01 00 00 dd 06   ........ ........
00 10 18 02 01 f4 dd 18  00 50 f2 01 01 00 00 50   ........ .P.....P
f2 02 01 00 00 50 f2 02  01 00 00 50 f2 02 00 00   .....P.. ...P....
32 a9 ba cd                                        2...
```

Os endereços MAC da trama beacon associada ao AP “linksys12” são os seguintes:

- ff:ff:af:d2:ff:ff
- 00:06:25:67:22:94
- 00:06:25:67:22:94

```
Receiver address: ff:ff:af:d2:ff:ff (ff:ff:af:d2:ff:ff)
Destination address: ff:ff:af:d2:ff:ff (ff:ff:af:d2: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)
00 00 18 00 ee 58 00 00  10 04 85 09 a0 00 a3 9c   .....X.. ........
0b 00 00 07 3b 29 f5 24  80 00 00 00 ff ff af d2   ....;).$ ........
ff ff 00 06 25 67 22 94  00 06 25 67 22 94 c0 da   ....%g". ..%g"...
97 02 39 08 ac 08 00 00  64 00 11 00 00 09 6c 69   ..9..... d.....li
6e 6b 73 79 73 31 32 01  04 82 84 0b 16 03 01 06   nksys12. ........
05 04 01 03 00 00 3b 29  f5 24                     ......;) .$
```

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?

Para a trama beacon associada ao AP "30 Munroe Street", os débitos base são de 1, 2, 5.5 e 11 Mbit/s, e as "extended supported rates" são de 6, 9, 12, 18, 24, 36, 48 e 54 Mbit/s.

```
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    Tag Number: Supported Rates (1)
    Tag length: 4
    Supported Rates: 1(B) (0x82)
    Supported Rates: 2(B) (0x84)
    Supported Rates: 5.5(B) (0x8b)
    Supported Rates: 11(B) (0x96)
Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag Number: Extended Supported Rates (50)
    Tag length: 8
    Extended Supported Rates: 6(B) (0x8c)
    Extended Supported Rates: 9 (0x12)
    Extended Supported Rates: 12(B) (0x98)
    Extended Supported Rates: 18 (0x24)
    Extended Supported Rates: 24(B) (0xb0)
    Extended Supported Rates: 36 (0x48)
    Extended Supported Rates: 48 (0x60)
    Extended Supported Rates: 54 (0x6c)
```

(O trace disponibilizado contém tramas probe request e probe response comuns na operação das redes WiFi, como alternativa ao scanning passivo efectuado pelo AP.)

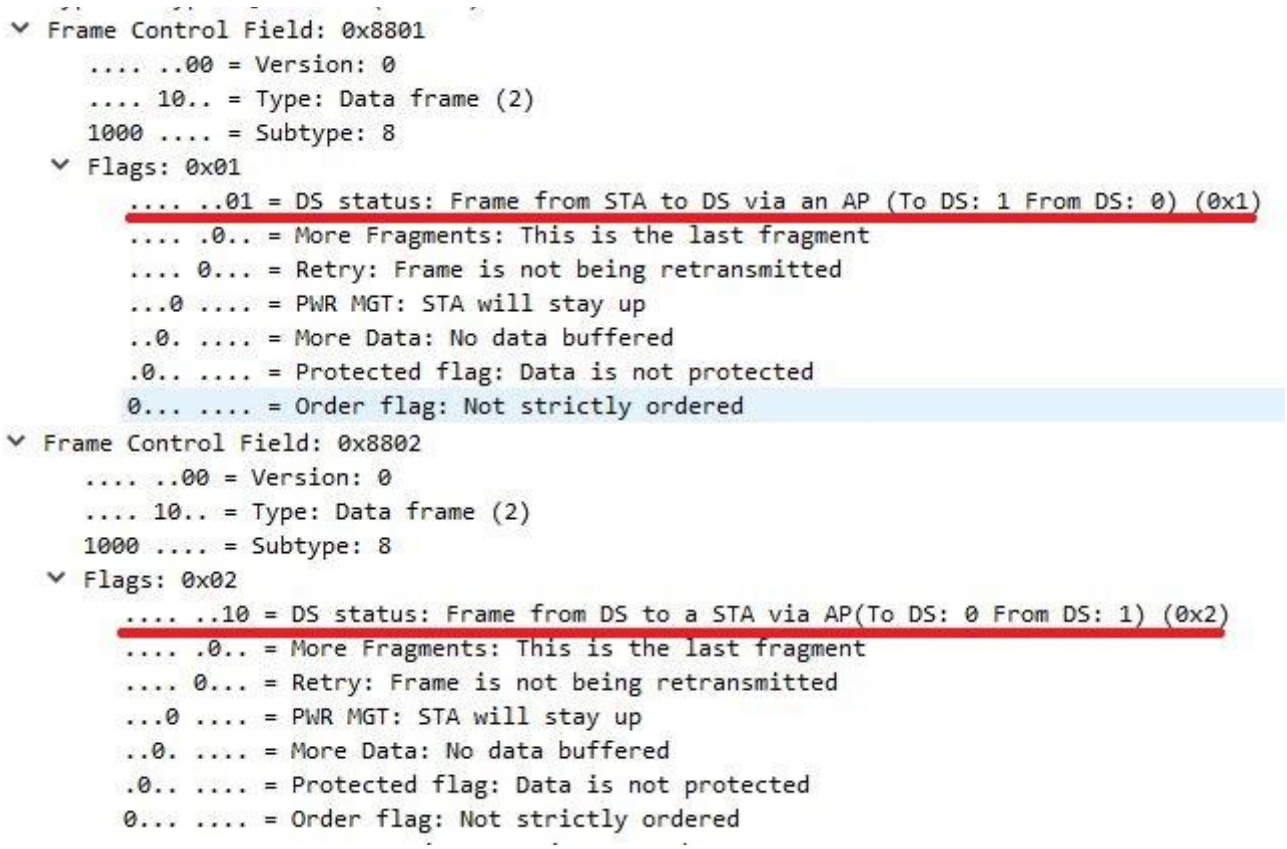
9 – Indique a que sistemas são endereçadas estas tramas e qual o seu propósito?

A probe request é enviada pelo sistema que pretende aceder a um AP, e tem como propósito expor as capacidades de conexão do sistema a possíveis APs (taxa de transferência, por exemplo). Quando o AP recebe esta request, analisa-a para ver se ambos são compatíveis, e então envia um probe response, com informação relevante, como o SSID, tipos de encriptação, entre outros.

Transferências 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 aspeto é fundamental para entender o endereçamento MAC em redes sem fios.

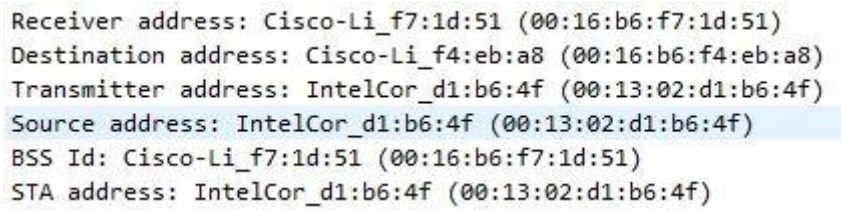
A direccionalidade da trama 1016 é para o Distributed System, e a direccionalidade da trama 1066 é do Distributed System.



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)?

Os três endereços MAC são:

- Host sem fios – 00:13:02:d1:b6:4f
- AP – 00:16:b6:f7:1d:51
- Router de acesso ao SD – 00:16:b6:f4:eb:a8



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

Os três endereços MAC são:

- Host sem fios – 00:13:02:d1:b6:4f
- AP – 00:16:b6:f7:1d:51
- Router de acesso ao SD – 00:16:b6:f4:eb:a8

```
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)
```

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.)

Em ambas as tramas são transmitidas tramas de controlo do tipo QoS (Quality of Service). No pedido GET (trama nº1016), o endereço MAC de destino é: 00:16:b6:f4:eb:a8 e na resposta ao pedido GET (trama nº1066), o endereço MAC de destino é: 00:13:02:d1:b6:4f.

```
   Type/Subtype: QoS Data (0x0028)
▾  Frame Control Field: 0x8801
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
   ›  Flags: 0x01
   .000 0000 0010 1100 = Duration: 44 microseconds
   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)
```

Trama 1016

```
   Type/Subtype: QoS Data (0x0028)
▾  Frame Control Field: 0x8802
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
   ›  Flags: 0x02
   .000 0000 0010 1000 = Duration: 40 microseconds
   Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
   Destination address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
```

Trama 1066

Estas tramas têm de existir para garantir que os dados transmitidos e recebidos vêm livres de erros.

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?

A tramas são a 1734, 1735 e 1736. As tramas que não aparecem são as probes, pois o router desassocia o endereço IP do computador, e o computador não está a tentar associar-se ao mesmo.

1733	49.583615	IntelCor_d1:b6:4f	Cisco-Li_f4:eb:a8	LLC	390 U, func=UI; SNAP, OUI 0x000000 (Encapsulated Ethernet), PID 0x0800
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

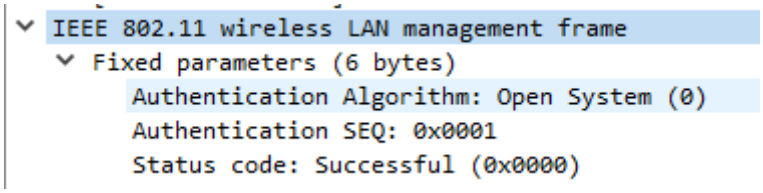
15 – Examine o ficheiro de trace e procure tramas de autenticação enviadas pelo host para o AP (se filtrar os resultados por wlan.fc.type_subtype ajuda a localização). Quantas tramas de authentication são enviadas do host sem fios para o AP linksys_SES_24086?

São enviadas 15 tramas de authentication.

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

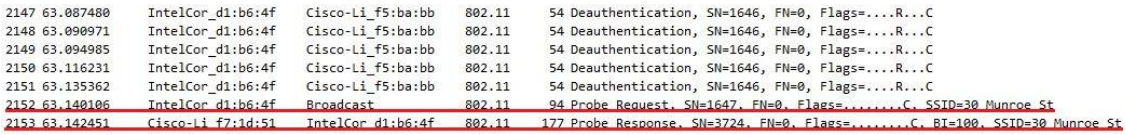
16 – O host tenta usar algum algoritmo de autenticação/chave ou tenta aceder de forma aberta (consulte o authentication algorithm na trama)? Existe alguma resposta do AP linksys_SES_24086 ao pedido de autenticação? Porquê?

O host tenta aceder ao AP linksys_SES_24086 de forma aberta, e fá-lo sem sucesso, pois o AP não tem acesso aberto.



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.

Depois de se deligar do AP linksys_SES_24086, com sucessivas tramas de deauthentication, o host volta a conectar-se ao AP 30 Munroe St., como evidenciado nas tramas 2152 e 2153, em que o host envia um probe request e tem resposta do AP (probe response).



Conclusão

Com este trabalho prático terminado, adquirimos uma melhor noção sobre o funcionamento das redes Wi-Fi 802.11.

Comparativamente à captura do tráfego proveniente de um cabo Ethernet, a captura de tráfego proveniente de redes Wi-Fi é muito mais complexa, com tramas de controlo e tramas de gestão que não existiam, necessárias agora para garantir a ligação a um AP e a validade dos dados que circulam, já para não falar das tramas de dados, que contém informação adicional sobre o endereço MAC do AP, entre outros.

Toda este conhecimento adicional que adquirimos sobre esta ligação de rede, deu-nos um novo apreço sobre esta tecnologia, que tanto usamos no nosso dia a dia.

PL2.8

João Araújo A75364

João Almeida A75209

João Amorim A74806