TP3 – Redes Sem Fios (802.11)

Questões e Respostas

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).**

```
802.11 radio information
    PHY type: 802.11b (4)
    Short preamble: False
    Data rate: 2.0 Mb/s
    Channel: 6
    Frequency: 2437 MHz
    Signal strength (dBm): -94 dBm
    Noise level (dBm): -100 dBm
  [Duration: 456 us]
```

A rede sem fios está a operar na frequência 2.437 GHz (2437 MHz). O canal correspondente a esta frequência é o canal 6.

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?**

```
802.11 radio information
    PHY type: 802.11b (4)
```

O tipo de canal que está a ser utilizador para a comunicação de rádio (*PHY type*) é o 802.11b. O débito a que foi enviada a trama é de 2.0 Mb/s.

3. **Indique qual o índice de qualidade do sinal.**

```
Radiotap Header v0, Length 24
    Header revision: 0
    Header pad: 0
    Header length: 24
  Present flags
  Flags: 0x10
    Data Rate: 2.0 Mb/s
    Channel frequency: 2437 [BG 6]
  Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz spectrum
    SSI Signal: -94 dBm
    SSI Noise: -100 dBm
    Signal Quality: 11
```

O índice da qualidade do sinal é de 11.

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

```
▾ Frame Control Field: 0x8000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1000 .... = Subtype: 8
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e3 9c
0010  5e 00 00 47 af f5 8c 7f  80 00 00 00 ff ff ff ff
0020  ff ff 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 00 b3
```

O tipo da trama *beacon* é "*Management frame (0)*". Os bits que identificam o tipo e o subtipo são, respetivamente, 00 e 1000. Estão presentes no campo de controlo da trama *beacon* (*Frame Control Field*).

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.**

Signal Quality: 94

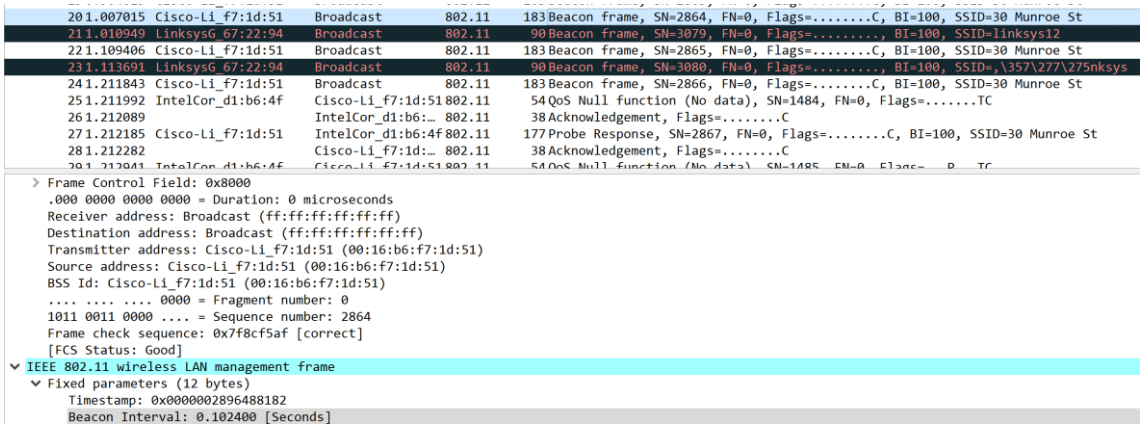
1 – Qualidade de uma trama na rede 30 Munroe St (trama nº 20)

Signal Quality: 11

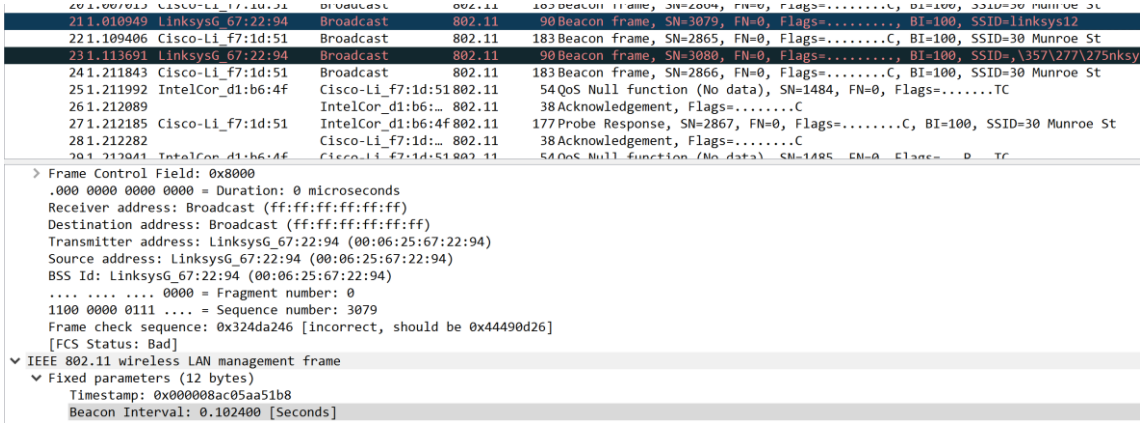
2 - ***Qualidade de uma trama na rede linksys12 (trama nº 21)***

Os SSIDs dos *access points* que estão a operar na rede são "30 Munroe St" e "linksys12". O AP que tende a proporcionar a melhor qualidade do sinal é o "30 Munroe St", visto que o *Signal Quality* é superior quando comparado com o outro AP.

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 periodicidade de tramas *beacon* é verificada? Tente explicar porquê.**



3 – Beacon Interval na rede 30 Munroe St (trama nº 20)



4 – Beacon Interval na rede linksys12 (trama nº 21)

Tanto o AP cujo SSID é “30 Munroe St” como o que é “linksys12” têm um intervalo entre envios de tramas (*beacon interval*) de 0.1024 segundos.

No entanto, na prática, o que se verifica é que a receção das tramas de *beacon* do “30 Munroe St” ocorre num tempo bastante próximo ao *beacon interval*, enquanto que no caso do “linksys12”, existe uma grande variação na receção das tramas.

Tal pode explicar-se como sendo uma implicação direta da menor qualidade de sinal registada para o “linksys12” que, apesar de até poder enviar as tramas *beacon* no tempo especificado pelo seu *beacon interval*, não são recebidas pelo computador no qual se fez a captura.

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.**

```
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)
```

5 - 30 Munroe St

Para o AP cujo SSID é "30 Munroe St", os endereços MAC da fonte, destino e BSS ID são, respetivamente, 00:16:b6:f7:1d:51, ff:ff:ff:ff:ff:ff (que denota o *broadcast*) e 00:16:b6:f7:1d:51.

```
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)
```

6 – linksys12

Para o AP cujo SSID é "linksys12", os endereços MAC da fonte, destino e BSS ID são, respetivamente, 00:06:25:67:22:94, ff:ff:ff:ff:ff:ff (que denota o *broadcast*) e 00:06:25:67:22:94.

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.**

```
Supported Rates: 2(B) (0x84)
Supported Rates: 5.5 (0x0b)
Supported Rates: 11 (0x16)
```

Os débitos suportados são 1, 2, 5.5 e 11 Mb/s.

9. **O trace disponibilizado contém tramas *probe request* e *probe response* comuns na operação das redes Wi-Fi, como alternativa ao *scanning* passivo efetuado pelo AP. Indique a que sistemas são endereçadas estas tramas e qual o seu propósito.**

   Na linha 1594, existe um *probe request* endereçado ao AP "30 Munroe St" por parte do *host*, com o intuito de obter informações acerca do AP em questão.

   Na linha 1737, existe um *probe request* igual ao da linha 1594 mas que é endereçado a outro AP ("linksys_SES_24086").

   Na linha 1595, existe um outro *probe request* que não é endereçado a um AP em específico mas que está sob a forma de *broadcast*. Este tipo de *probe request* serve para o *host* obter informações acerca de todos os APs existentes no seu alcance rádio.

   Em todos os casos acima mencionados, estamos perante *active snanning* que se diferencia do *passive scanning* pelo facto de não ser o AP a enviar informações aos hosts da sua rede local (através de tramas *beacon*), mas um *host* a procurar obter informações acerca de um ou mais APs no seu alcance.

   Podemos ainda verificar que existem tramas do tipo *probe response*, por exemplo, na linha 27, em que o AP "30 Munroe St" responde ao *probe request* do *host*, enviando informações como sendo as taxas de dados suportadas.

10. **O campo *Frame Control* contido no cabeçalho das tramas 802.11 permite especificar a direcionalidade das tramas. Identifique a direcionalidade das tramas indicadas acima (nº 1016 e nº 1066). Este aspeto é fundamental para entender o endereçamento MAC em redes sem fios.**

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

7 - Trama 1016

A trama 1016 tem "01" como bits da flag que indica a direcionalidade. O que nos diz que a trama em causa vai da máquina (STA) para o sistema de distruibuição (DS) através do *access point* (AP).

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

8 – Trama 1066

A trama 1066 tem "10" como bits da *flag* que indica a direcionalidade. O que nos diz que a trama em causa vai desde o sistema de distribuição (DS) para a máquina (STA) através do *access point* (AP).

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).**

```
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)
```

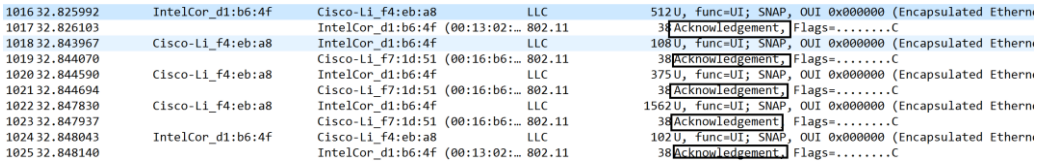
De acordo com a direcionalidade explicitada acima, o endereço MAC do *router* de acesso ao sistema de distribuição (*destination*) é 00:16:b6:f4:eb:a8, o do AP (*transmitter*) é 00:16:b6:f7:1d:51 e o do *host* sem fios (*source*) é 00:13:02:d1:d6:4f.

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

```
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)
```

De acordo com a direcionalidade explicitada acima, o endereço MAC do *host* sem fios (*destination*) é 00:13:02:d1:d6:4f, o do AP (*transmitter*) é 00:16:b6:f7:1d:51 e o do *router* de acesso ao sistema de distribuição (*source*) é 00:16:b6:f4:eb:a8.

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).**



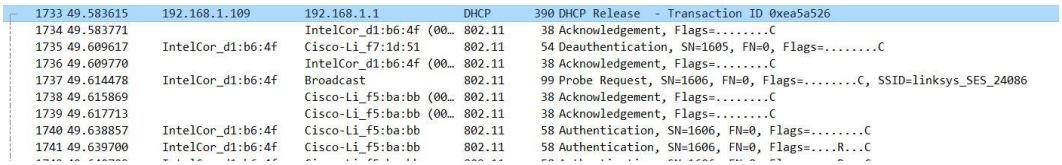
As tramas de controlo que são transmitidas são tramas de confirmação da receção (ACK - *Acknowlegment*). São endereçadas aos diversos sistemas (STAs ou APs) que recebem as tramas.

Contrariamente ao que acontece numa rede *Ethernet* em que existe *collision detection* – em oposição à *collision avoidance* das redes sem fios –, as redes *wireless* são redes bastante mais suscetíveis à ocorrência de erros e colisões, por exemplo, entre *hosts* pertencentes à mesma rede local, que, no entanto, não sabem da presença um do outro e, por isso, enviam tramas ao mesmo tempo.

A existência de tramas de confirmação da receção (ACK - *Acknowlegment*) serve, exatamente, para contrariar esta desvantagem, sinalizando à estação emissora a receção correta de uma trama por parte da estação recetora. Apesar de, no fundo, estas tramas gerarem mais tráfego na rede, conseguem minimizar as colisões existentes.

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?

Sim, na sequência do *probe request* que foi enviado pela estação (STA) ao *access point* linksys_SES_24086, era esperado um *probe response* enviado pelo AP (que conteria informações sobre, por exemplo, as taxas de dados suportadas).



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 (00…	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 (00…	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 (00…	802.11	38	Acknowledgement, Flags=........C
1739	49.617713		Cisco-Li_f5:ba:bb (00…	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

A partir da linha 1733 até à 1736, a estação envia um pedido de dissociação ao AP "30 Munroe St", obtendo as respetivas confirmações (ACK – *Acknowledgment)*. De seguida, na linha 1737, a estação (STA) envia um *probe request* para o AP ao qual se pretende associar, esperando uma resposta (*probe response*) que não surge. Nas linhas seguintes tenta associar-se ao AP mas não consegue fazê-lo.

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?

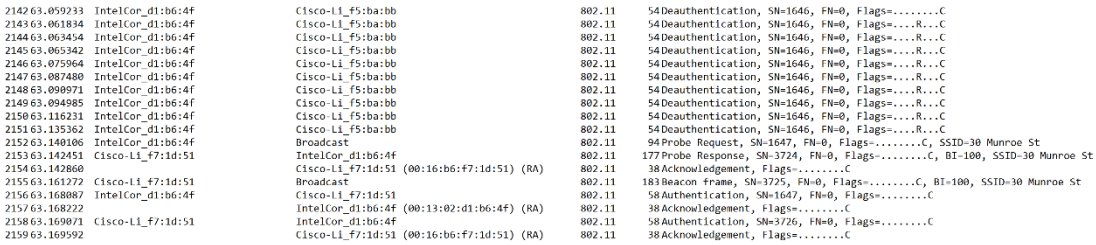
Entre as linhas 1740 e 1749, são enviadas seis tramas de autenticação (*open system*) pelo *host* para o AP. Nas linhas 1821 e 1822 são enviadas outras duas. Da linha 1921 à 1924 são enviadas mais quatro. Finalmente, nas linhas 2121, 2122 e 2123 são enviadas outras três tramas. Ao todo são enviadas 15 tramas de autenticação.

Estas tramas têm como finalidade pedir ao AP que aceite (ou rejeite) a identidade do *host*.

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 autenticar-se ao AP de forma aberta visto que o seu *authentication algortithm* é "*Open System (0)*" (no pedido de autenticação presente na linha 1740). Não existe nenhuma resposta do AP linksys_SES_24086 visto que se trata de um AP sem 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.



Primeiramente, o *host* efetua a dissociação do AP linksys_SES_24086 através do envio de tramas *deauthentication* (da linha 2142 à 2151).

De seguida, na linha 2152, é enviado um *probe request* ao AP "30 Munroe St" (já conhecido), sendo recebida a resposta (*probe response*) na linha seguinte.

Depois, o *host* envia um conjunto de pedidos de autenticação ao AP "30 Munroe St" (linhas 2156 e 2160), sendo recebidas respostas (do tipo *authentication*) enviadas pelo AP.

Finalmente, existe um pedido de associação (trama do tipo *association request)* ao AP, enviado pelo *host* (linha 2162), e a respetiva resposta por parte do AP (do tipo *association reply*) na linha 2166.

É também importante notar que, para comunicação entre o *host* e o AP, existe ainda uma trama do tipo ACK (*Acknowledgement*).

Conclusões

Este TP3 permitiu-nos pôr em prática os conhecimentos teóricos adquiridos nas aulas de Redes de Computadores e, assim, compreender melhor os mesmos de um ponto de vista mais real. Desta vez estivemos a fazer a análise de uma captura feita a partir de uma rede sem fios (802.11).

Neste trabalho, para além de analisarmos as diferenças na qualidade da ligação de um *host* a dois APs distintos, vimos também a diferença entre uma ligação com uma rede sem fios e uma ligação *Ethernet* (TP2). Nas redes sem fios estamos sujeitos a mais interferências e ruídos que poderão afetar a qualidade da ligação, havendo a necessidade de evitar colisões (*collision avoidance)*. Numa ligação via cabo *Ethernet*, como se consegue observar o tráfego (i.e. existe um maior controlo sobre o tráfego da rede), existe, em oposição às redes *wireless*, uma deteção das colisões (*collision detection*).

Quanto às redes sem fios, este trabalho permitiu-nos também observar os diferentes tipos de tramas de gestão, controlo e dados utilizadas. Aprendemos ainda como uma estação comunica com o sistema de distribuição (DS) e com os pontos de acesso (*access point*), por exemplo na troca de tramas de confirmação de receção (*ACK*) ou de autenticação (*Authentication*).