**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).**

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

1. **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 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.

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

O índice da qualidade do sinal é de 11.

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

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*.

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

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”.

1. **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.**

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.

1. **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.**

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.

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.

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

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

1. **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.**

[Diferença entre probe request com SSID = “30 Munroe St” e SSID = Broadcast?]

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.

1. **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.**

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).

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).

1. **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).**

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.

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

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.

1. **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.

1. **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).

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.

1. **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*.

1. **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.

1. **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**

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.