

Rede de Computadores - Trabalho Prático nº 3

Redes Sem Fios (802.11)

William Sousa, Manuel Maciel e Rui Santos

Universidade do Minho, Departamento de Informática, 4710-057 Braga, Portugal
e-mail: {a61029,a68410,a67656}@alunos.uminho.pt

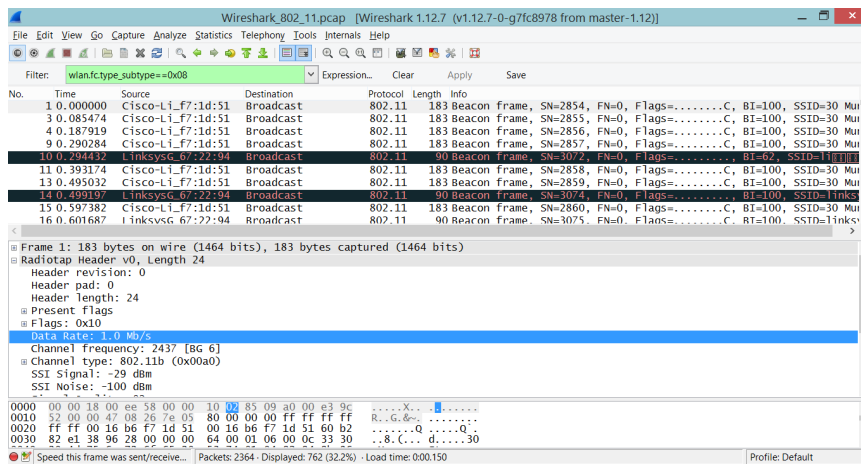
Resumo Neste relatório, iremos propor respostas para as perguntas da ficha de trabalho prática nº 3 que foi realizada no âmbito da unidade curricular de Redes de Computadores, lecionada no ano lectivo 2015/2016 do Mestrado Integrado de Engenharia Informática, portanto toda a estrutura de perguntas e respostas, presentes neste relatório, irão de encontro ao que foi pedido e/ou fornecido nessa ficha prática. Acreditamos, que as perguntas e respostas aqui apresentadas, de uma forma geral, ajudam a compreensão e análise de muitos conceitos relacionados com as redes de computadores, nomeadamente dos níveis mais baixos do modelo OSI (i.e., camada de ligação lógica e camada física) com especial atenção a tecnologia de rede local sem fios da norma IEEE 802.11.

1 Introdução

Numa primeira fase iremos tratar de analisar, com algum detalhe, uma serie de capturas de tramas, que foram previamente fornecidas com o enunciado, vamos analisar com especial atenção as tramas do tipo *management* e *control*. Depois iremos estudar um conjunto de propriedades, relacionadas, com as redes sem fios e das suas características, informação essa que pode ser facilmente verificada com auxílio de tramas beacon. Iremos ainda tentar identificar como o acesso ao meio é realizado, de que tipo/forma é feito a associação e desassociação aos APs e em que medida o Probing e a opção RTS/CTS ajudam a controlar e garantir uma melhor “qualidade de serviço em redes sem fios”.

2 Acesso Rádio

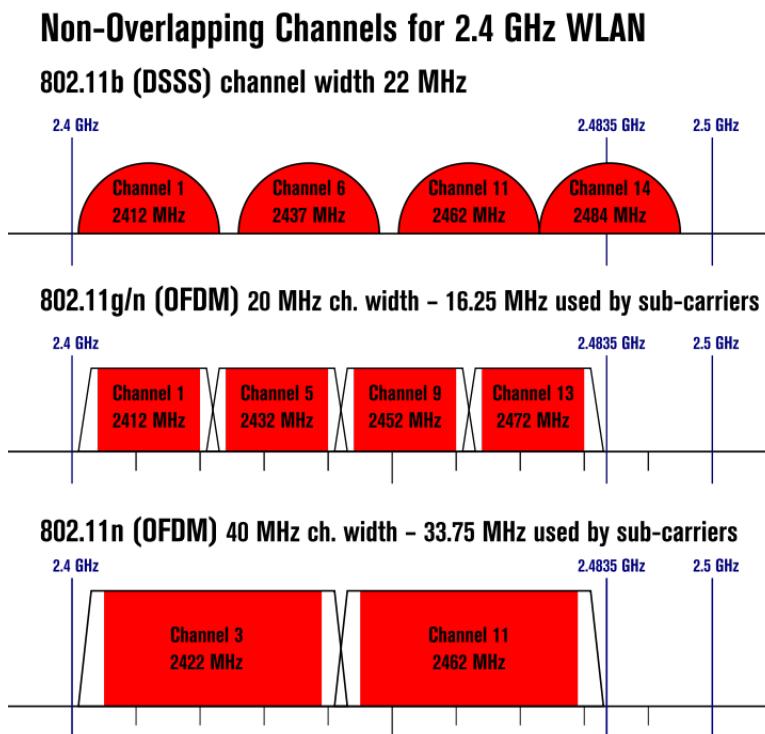
Wi-Fi, ou IEEE 802.11, é o standard para LANs sem fios, ou WLANs. A abreviatura Wi-Fi significa Wireless Fidelity, e tem semelhanças notórias com o Hi-Fi acrónimo. E representa todo um conjunto de protocolos da mesma família do Ethernet e Token Ring. [1]



2.1 Selecione uma das tramas e identifique em que frequência do espectro está a operar a rede sem fios. Tente identificar a que canal corresponde essa frequência (sugestão: ver norma IEEE 802.11).

Com base na imagem apresentada acima, podemos facilmente identificar que o Canal em que a rede está a operar é o canal 6, com uma frequência de 2437MHz. Esta frequência curiosamente está representada na trama em formato hexadecimal com representação em formato little endian, portanto o valor `0x8509`, que aparece na trama, é na realidade `0x0985 = 2437`.

Para além disso, foi dito acima que o canal que opera a rede é o 6, sabemos isso com base numa tabela predefinida pela norma IEEE 802.11, que varia de país para país e depende também se está em a funcionar com canais em overlapping ou non-overlapping. Mas de uma maneira geral há ao todo 14 canais que variam entre as frequências 2.412Ghz e 2.484Ghz, como pode ser verificado na tabela fornecida pelo IEEE para a norma 802.11:

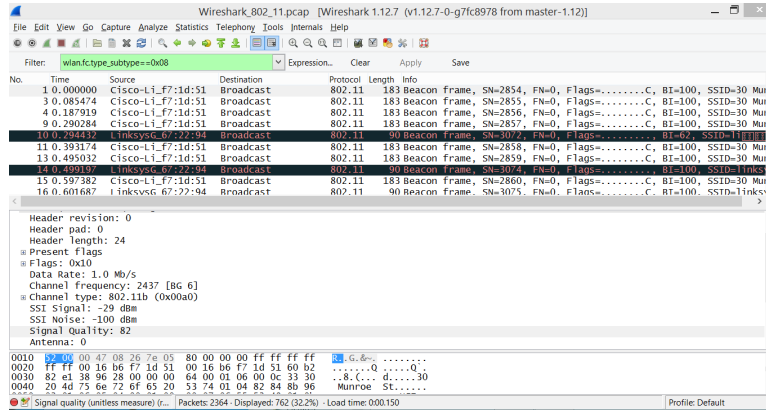


2.2 Qual o tipo do canal que está a ser usado para a comunicação rádio? Qual o débito a que foi enviada a trama escolhida?

Novamente, com auxílio da imagem acima apresentada, é fácil de identificar na trama, especificamente no campo RadioTap Header, qual o tipo e o debito que está a ser utilizado pela rede sem fios, que neste caso tem tipo 802.11b a funcionar a um débito de 1Mb/s.

2.3 Indique qual o índice de qualidade do sinal.

Como pode ser verificado na trama a seguir, a qualidade do sinal é de um factor numérico correspondente a 82, que infelizmente, após uma extensiva consulta tanto na pela especificações da norma fornecida pelo IEEE, como pela documentação fornecida pelo Wireshark Wiki, não fomos capaz de descortinar, como é calculado e como varia essa parametrização da qualidade do sinal.

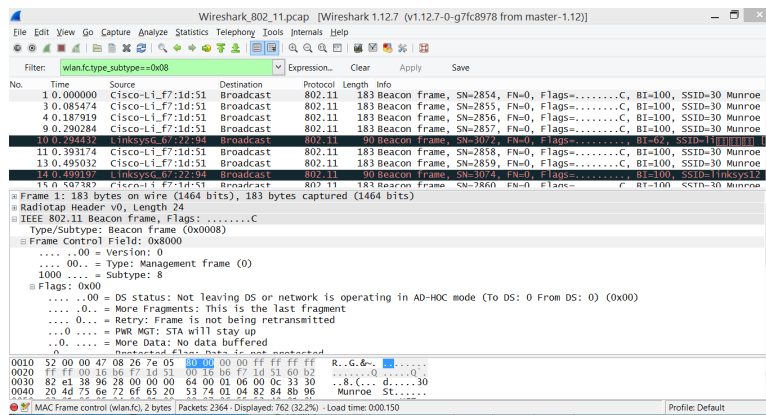


3 Tramas Beacon

As tramas beacon são tramas de manutenção, especificadas pela norma IEEE 802.11 baseadas em WLANs. Estas tramas contém toda a informação, necessária e essencial para difundir acerca da rede sem fios correspondente. As tramas beacon são transmitidas periodicamente para anunciar a presença de uma wireless LAN.

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

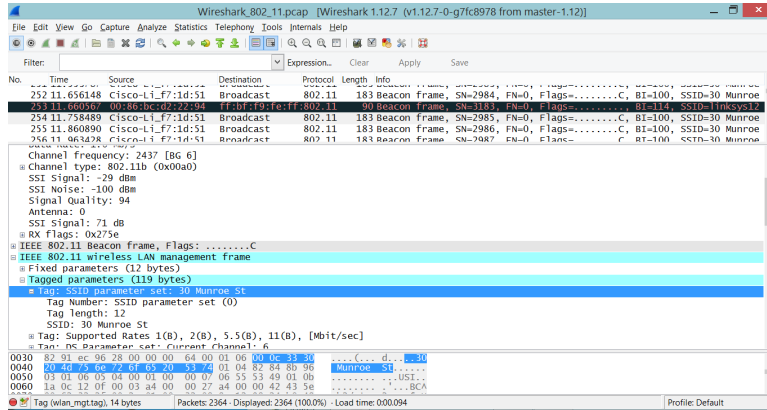
Tal como indicado na breve descrição acima fornecida, sobre as tramas beacons, estas são tramas de manutenção (*management frames*), e tal como indicado na tabela fornecida pelo enunciado, tem identificadores de tipo e subtipo iguais a 00 e 1000, em base binaria, respectivamente.



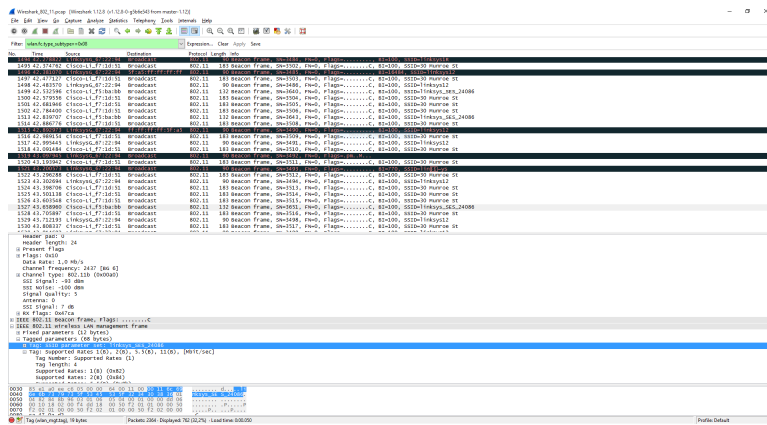
3.2 Identifique os SSIDs dos APs (Access Points) que estão a operar na rede e diga qual tende a proporcionar a melhor qualidade de sinal?

Os SSID (Service Set Identification) é o nome informal de uma BSS(Basic Service Set), ou seja, uma BSS é funcionalmente um domínio de contenção de um grupo local ou work-group network, por outras palavras, funciona como um broadcast domain. No caso do nosso trace, há um conjunto relativamente pequeno de APs a operar nessa rede, e na sua maior parte os dois APs que mais utilizam as beacon frames têm o SSID de 30 Munroe St e linksys_SES_24086 tal como se verificar nas duas imagens seguintes:

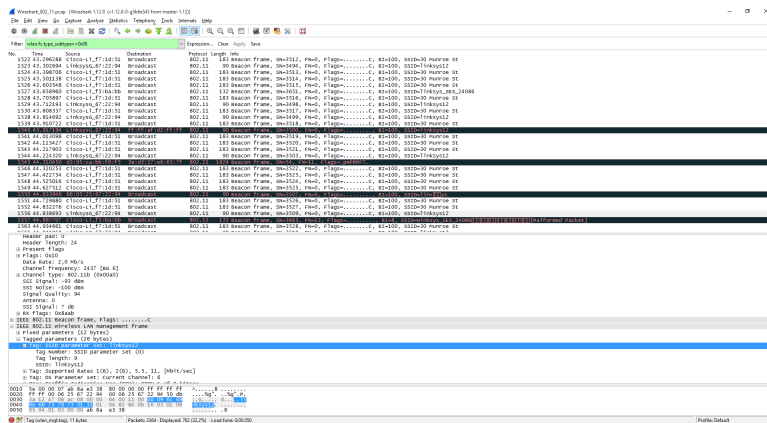
SSID: 30 Munroe St



SSID: linksys_SES_24086



Outro SSID, identificando assim todos os SSIDs disponíveis no trace fornecido, a operar nesta rede é o SSID linksys12, tal como pode ser verificado na imagem abaixo:

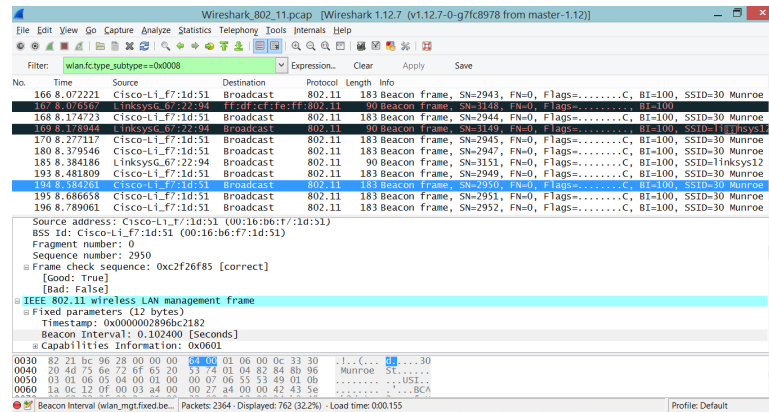


3.3 Para dois dos APs identificados, indique quais são os intervalos de tempo previstos entre as transmissões de tramas beacon? (nota: este valor é anunciado na própria trama beacon).

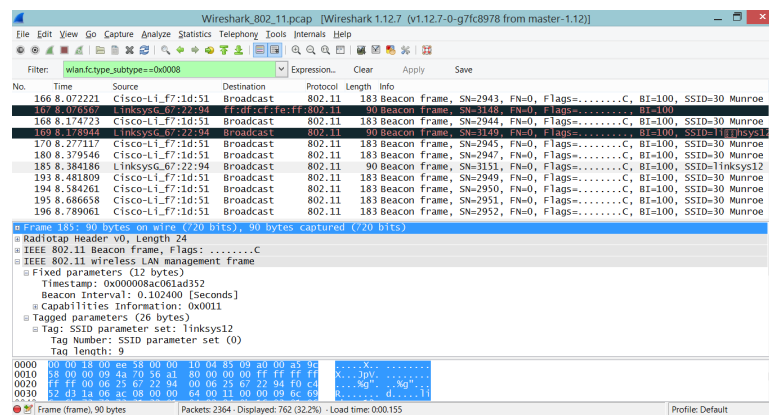
O intervalo temporal entre as tramas beacons, que é reportado pelos APs segundo a norma 802.11 para wireless LAN é de 0.1204segundos (i.e., pouco mais de 100 milissegundos), no entanto este é o valor anunciado e teórico do envio dos beacons mas por estarmos num meio contencioso, logo a disputa pelo acesso ao meio, não é o que se verifica, na verdade o

AP do 30 Munroe St produz muitos mais tramas beacon, neste trace, e de forma muito mais regular que as tramas beacons correspondentes ao AP do linksys_SES_24086, por exemplo. O valor dos intervalos temporais, das tramas beacons podem ser consultados nas imagens abaixo:

Trama Beacon do 30 Munroe St



Trama Beacon do linksys12



3.4 Na prática, a periodicidade de tramas beacon é verificada? Tente explicar porquê?

Tal como já explicado, e referenciado na alínea anterior, esta periodicidade nas tramas beacons não é verificada pois, naturalmente, uma wireless LAN corresponde a um meio contencioso, logo, pode não ser possível, ou justo, o acesso ao meio por todos os utilizadores, nesse caso APs a produzirem/difundirem tramas beacons e dependendo da localização física do host/receptor como das próprias características físicas do mundo/meio é possível, e bastante provável, que as tramas beacons, apesar de indicadas que são transmitidas em intervalos de cerca de 100 milisegundos não chegam, ou sejam difundidas, pelo meio a esse ritmo.

3.5 Identifique e registre 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, veja a secção 7 da norma IEEE 802.11 (citada acima).

Vamos então proceder a descrição/indicação dos endereços MAC utilizados nas tramas beacons enviadas pelos APs, temos então:

Trama Beacon originada pelo AP com SSID linksys_SES_24086:

No.	Time	Source	Destination	Protocol	Length	Info
1499	42.552996	Cisco-Li-f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3640, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
1868	54.971071	Cisco-Li-f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3641, FN=0, Flags=.....C, BI=100, SSID=30 Munroe
1873	55.072697	Cisco-Li-f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3642, FN=0, Flags=.....C, BI=100, SSID=30 Munroe
1874	55.174099	Cisco-Li-f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3643, FN=0, Flags=.....C, BI=100, SSID=30 Munroe
1513	87.259409	Cisco-Li-f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3644, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
1875	55.276451	Cisco-Li-f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3644, FN=0, Flags=.....C, BI=100, SSID=30 Munroe
1876	55.378829	Cisco-Li-f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3645, FN=0, Flags=.....C, BI=100, SSID=30 Munroe
1877	55.481139	Cisco-Li-f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3646, FN=0, Flags=.....C, BI=100, SSID=30 Munroe

Frame 1513: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface 0	
IEEE 802.11 Beacon frame, Flags:	
Type/Subtype: Beacon frame (0x0008)	
Frame Control Field: 0x8000	
Duration: 0 microseconds	
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-f5:ba:bb (00:18:39:f5:ba:bb)	
Fragment number: 0	
Sequence number: 3643	
Frame check sequence: 0x6d3b3b87 [correct]	

0000	00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 a5 9cX.....
0010	64 00 00 09 87 30 30 6d 80 00 00 00 ff ff ff ff	d.....m.....
0020	ff ff 00 18 39 f5 ba bb 00 18 39 f5 ba bb 00 e3	...9...9.....
0030	8f 61 94 ee c6 09 00 00 64 00 11 00 00 11 6c 69	.a.....d...11
0040	6e 6b 73 79 f3 53 45 53 5f 32 34 30 38 36 01	...f...f...f...

Receptor/Destino: Broadcast (*ff : ff : ff : ff : ff : ff*)
Transmissor/Origem: Cisco-Li-f5:ba:bb (*00 : 18 : 39 : f5 : ba : bb*)

Trama Beacon originada pelo AP com SSID 30 Munroe St

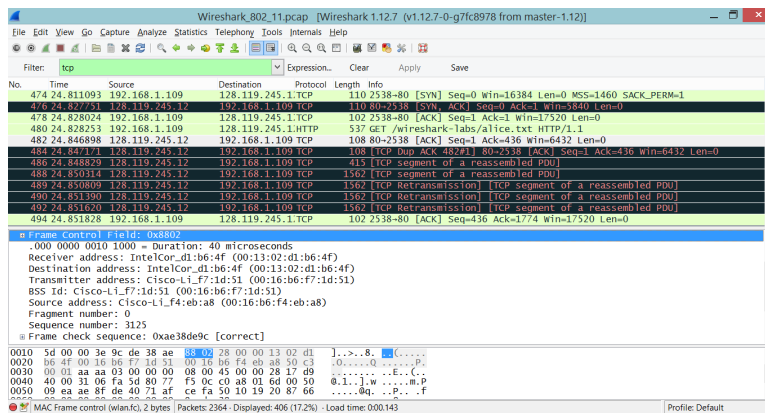
No.	Time	Source	Destination	Protocol	Length	Info
241	211843	Cisco-Li-f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2866, FN=0, Flags=.....C, BI=100, SSID=30 Munroe
311	215947	Linksys-G-67:22:94	Broadcast	802.11	90	Beacon frame, SN=3081, FN=0, Flags=.....C, BI=100, SSID=linksys12
321	314223	Cisco-Li-f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2868, FN=0, Flags=.....C, BI=100, SSID=30 Munroe
331	416593	Cisco-Li-f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2869, FN=0, Flags=.....C, BI=100, SSID=30 Munroe
341	420563	Linksys-G-67:22:94	Broadcast	802.11	90	Beacon frame, SN=3083, FN=0, Flags=.....C, BI=20380, SSID=linksys12
351	621422	Cisco-Li-f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2871, FN=0, Flags=.....C, BI=100, SSID=30 Munroe
371	724031	Cisco-Li-f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2872, FN=0, Flags=.....C, BI=100, SSID=30 Munroe
381	826193	Cisco-Li-f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2873, FN=0, Flags=.....C, BI=100, SSID=30 Munroe

Frame 35: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface 0	
IEEE 802.11 Beacon frame, Flags:	
Type/Subtype: Beacon frame (0x0008)	
Frame Control Field: 0x8000	
Duration: 0 microseconds	
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)	
Fragment number: 0	
Sequence number: 2870	

0000	00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e4 9cX.....
0010	58 00 00 48 51 2f 26 9e 80 00 00 00 ff ff ff ff	X..HROk.....
0020	ff ff 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 60 b3Q.....
0030	82 51 50 96 28 00 00 00 64 00 01 06 00 0c 33 30	.QP(....d....30
0040	20 4d 73 6e 72 6f 63 20 33 74 01 04 82 84 8b 96	Munroe St....

Receptor/Destino: Broadcast (*ff : ff : ff : ff : ff : ff*)
Transmissor/Origem: Cisco-Li-f7:1d:51 (*00 : 16 : b6 : f7 : 1d : 51*)

Trama Beacon originada pelo AP com SSID linksys12



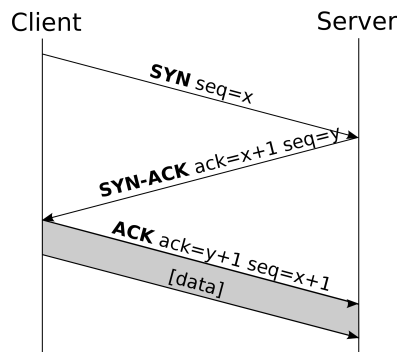
Que tem os seguintes campos de endereço MAC:

- Endereço receptor/destino (00 : 13 : 02 : d1 : b6 : 4f);
- Endereço transmissor (00 : 16 : b6 : f7 : 1d : 51);
- Endereço fonte (00 : 16 : b6 : f4 : eb : a8).

Neste caso, o endereço MAC do receptor e destino correspondem ao host, ou seja, IntelCor_d1:b6:4f. Sabemos ainda que o endereço MAC da fonte corresponde ao router, ou seja, Cisco-Li_f4:eb:a8.

4.3 Verifique como é especificada a direcionalidade das tramas no cabeçalho 802.11, tomando como exemplo as tramas identificadas em 10) e 11).

Tal como é esperado num processo TCP de sincronização, neste caso específico o TCP 3-way Handshake que refere-se aos (SYN, SYN-ACK e ACK), que são essencialmente três mensagens que são transmitidas com o intuito de estabelecer uma conexão pelo socket TCP, temos a seguinte direcionalidade:

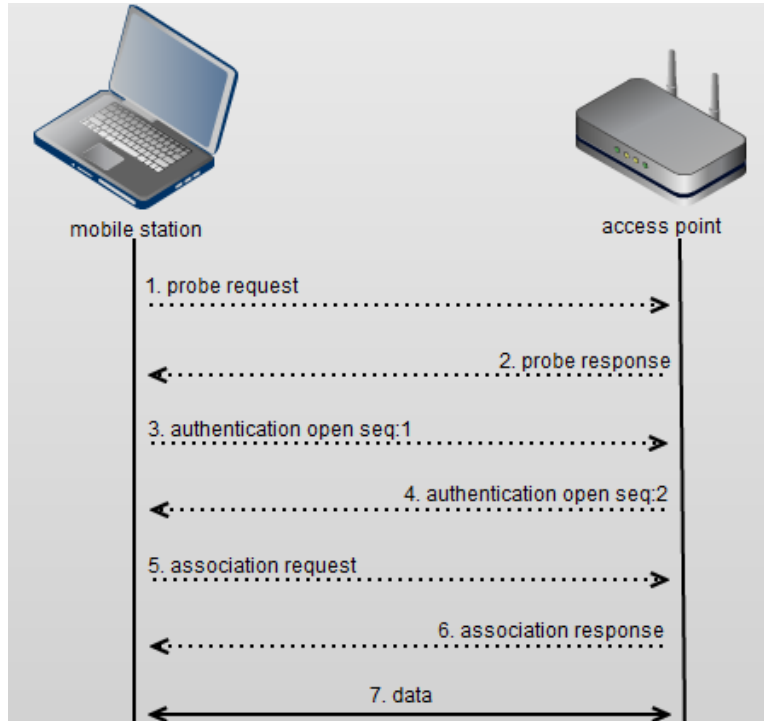


No caso, específico dessa imagem, o Client é o servidor que contém o ficheiro `alice.txt` e o Server é o host.

5 Associação e Desassociação

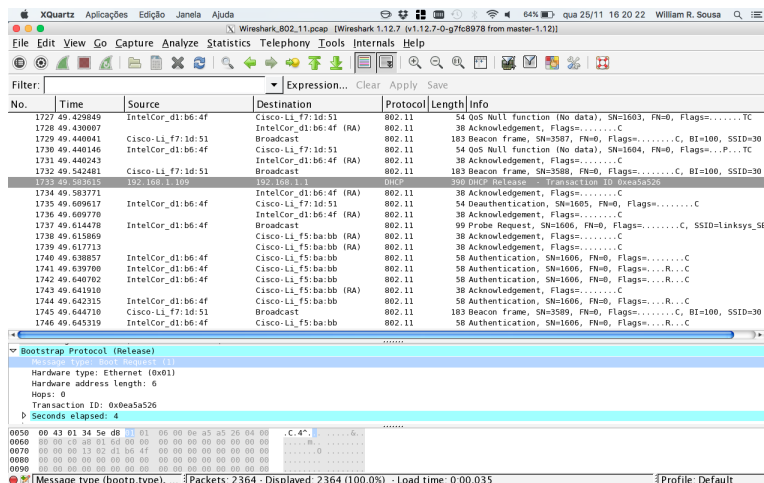
Um AP (Access Point) é basicamente uma “ponte” (bridge) que permite o tráfego entre estações móveis e outros dispositivos na rede. No entanto, antes que uma estação móvel possa enviar tráfego através do AP, ou receber, este tem de estabelecer um estado de conexão apropriado (Fonte: Cisco documents [3])

Uma associação genérica, segundo a norma 802.11, pode tomar a seguinte forma:



5.1 Que ação é tomada pelo host após $t=49.5s$ que determina a quebra de associação com o AP 30 Munroe St que existia desde que a captura de tramas começou? Como interpreta as tramas 802.11 subsequentes relacionadas com a anterior ação? Segundo a especificação IEEE 802.11, há alguma trama que seria esperada, mas não aparece?

O host desconecta-se por causa do DHCP release, não interessa o motivo que deu origem a esse DHCP release, e para isso faz uma desautenticação da rede, no entanto, o host também deveria ter feito dissociação para, de facto, encerrar e fechar a conexão, tal como é previsto pelas especificações IEEE 802.11.

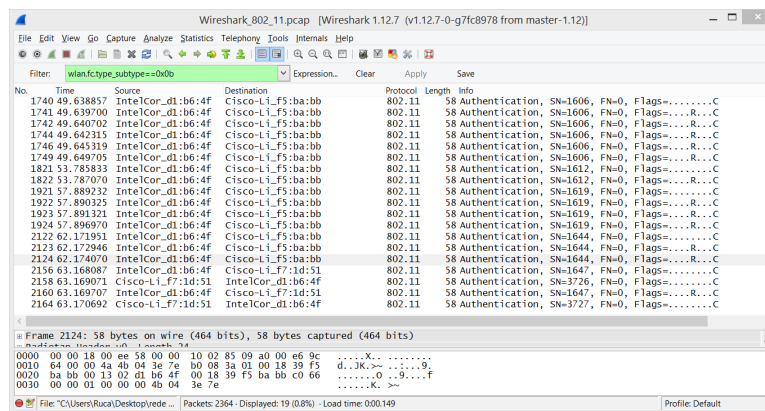


5.2 Examine o ficheiro de trace e procure tramas de autenticação enviadas pelo host para o AP e vice-versa (se filtrar os resultados por wlan.fc.type_subtype ajuda a localização). Quantas tramas de AUTHENTICATION são enviadas do host sem fios para o AP Linksys_SES_24086 AP? Durante que período de tempo?

Utilizando o filtro apropriado no Wireshark, ou seja, para filtrar os pacotes em tramas do tipo manutenção e subtipo Autenticação:

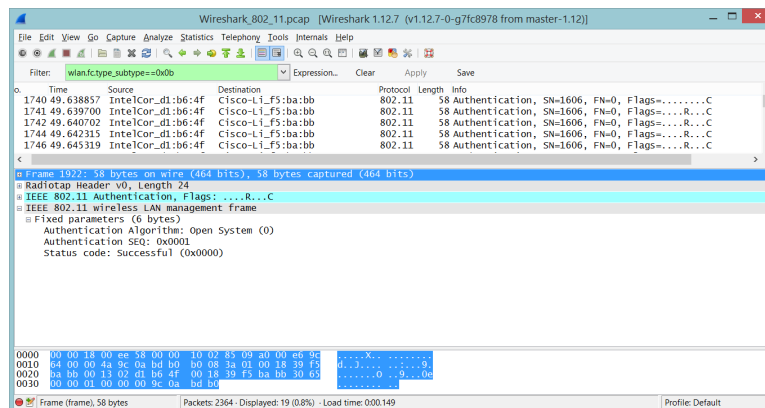
`Wlan.fc.type_subtype == 0x0b`

Temos o seguinte trace:



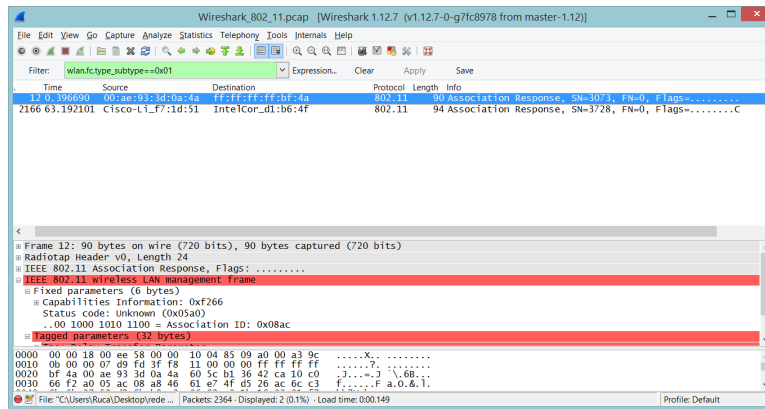
Como é fácil observar há um total de 19 pacotes, após efectuar o filtro, para além disso, é fácil verificar que apenas 4 desses pacotes não corresponde ao AP do `linksys_SES_24086` logo temos um total de $19 - 4 = 15$ tramas de autenticação enviadas pelo host para o AP e vice-versa. A janela de tempo que essas tramas ocorrem é relativamente pequena [49.63; 63.17], no entanto, dentro dessas janela há ainda um padrão de envios em “burst” correspondendo as seguintes janelas temporais: [49.63; 49.65], [53.78; 57.89] e [62.17; 63.17].

5.3 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?



Com base na imagem apresentada acima, podemos verificar que o campo do Authentication Algorithm encontra-se em Open System, pelo que podemos concluir que o host tenta aceder de forma aberta a rede, ou seja, sem utilizar nenhuma chave de autenticação. No entanto, por medidas de segurança, e não faria sentido que fosse de outra forma, o AP

não responde a nenhum dos pedidos de autenticação por parte do host, na verdade a janela temporal descrita na alínea anterior é exactamente todas as tentativas por parte do host de estabelecer ligação a rede, ou seja, durante [49.63; 63.17] o host tenta fazer conexão ao AP do linksys_SES_24086. E mais, com base no trace sabemos que a única resposta que há na captura é no instante de tempo 63.19s em que o host estabelece novamente conexão ao AP do 30 Munroe St, como se pode verificar na imagem abaixo:



6 Probing

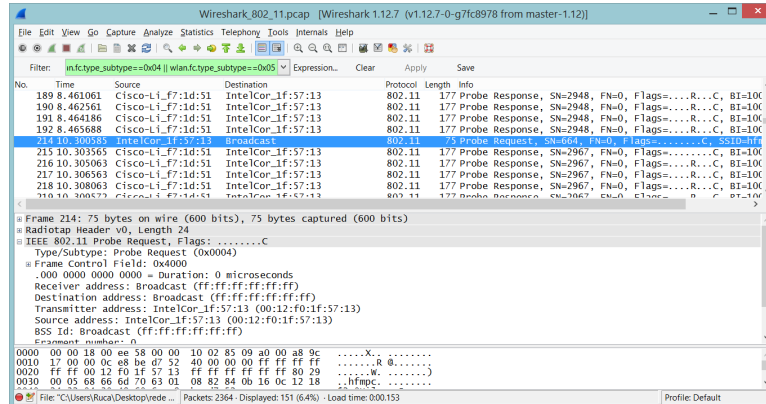
Um dos motivos pelo que um cliente faz um scanning (procura) é para determinar se existe um AP viável, o qual o cliente pode vir a tentar estabelecer conexão num futuro próximo. O cliente pode usar dois tipos diferentes de procura, nomeadamente procura activa ou passiva. Durante uma procura activa, o cliente transmite um probe request e “espera” por um probe response proveniente de um AP. Já com a procura passiva, o cliente escuta em cada canal de radio, frequências especificadas na norma 802.11 para o Wi-Fi, pelos beacons que são enviados periodicamente pelos APs. Uma procura passiva, geralmente, demora mais tempo, uma vez que o cliente deve “escutar” e esperar por um beacon, ao invés de ativamente proceder a utilização de probing para encontrar um AP. Outra limitação da procura passiva é que se o cliente, não esperar tempo suficiente em cada canal, o cliente pode “perder” alguns beacons provenientes dos APs. (fonte wifior <http://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning>)

6.1 Estabeleça um filtro adequado para localizar simultaneamente estes subtipos de trama de uma forma rápida e eficiente. Quais são os endereços MAC do originador, receptor e BSS ID nestas tramas? Qual é a função deste tipo de tramas?

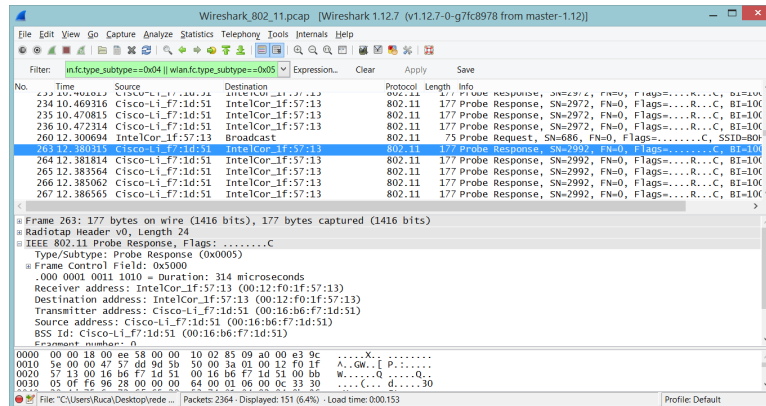
Um filtro adequado para localizar essas tramas é por exemplo:

```
wlan.fc.type_subtype==0x04 || wlan.fc.type_subtype==0x05
```

Com base na seguinte imagem:



No probe request temos um BSS id em broadcast, logo o endereço MAC correspondente é o (*ff : ff : ff : ff : ff*); temos ainda que a fonte tem o seguinte endereço MAC (*00 : 12 : f0 : 1f : 57 : 13*) que, como já visto anteriormente, corresponde ao endereço MAC do host. Num probe response, obviamente que há várias respostas, especificamente de todos os APs que “escutam” o Probe Request, vamos por exemplo, analisar o probe response imediatamente a seguir ao probe request, ou seja, temos a seguinte imagem:



Analisado a imagem, acima apresentada, temos que o BSS id é Cisco-Li_f7:1d:51 que corresponde, como já verificado anteriormente, ao 30 Munroe St, que por sua vez, tem o seguinte endereço MAC (*00 : 16 : b6 : f7 : 1d : 51*). E como origem e o destino dessa trama temos o seguinte endereço MAC (*00 : 12 : f0 : 1f : 57 : 13*), que como estamos fartos de saber, corresponde ao host.

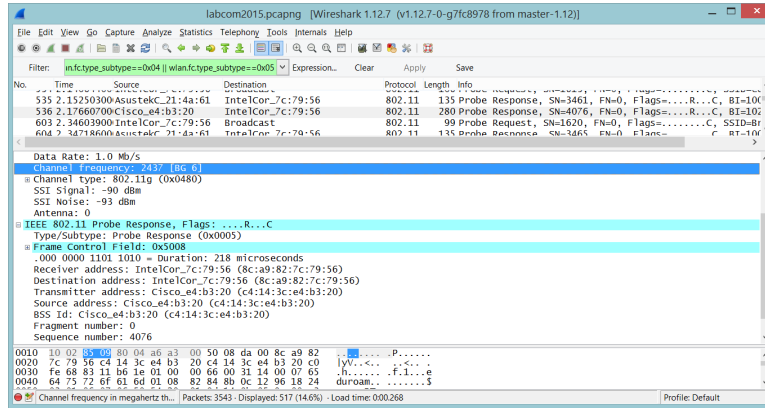
7 Opções RTS/CTS

RTS/CTS (Request to Send/Clear to Send) é um mecanismo opcional utilizado pelo norma IEEE 802.11 para wireless LAN, com o intuito de reduzir as frames collisions, introduzidas pelo problema do hidden node, que acontece quando um nodo na rede é visível para um dos APs dessa rede mas não para os outros nodos que comunicam com esse AP, o que leva a problemas ao da camada logica, nomeadamente ao subnível referente aos endereços MAC.

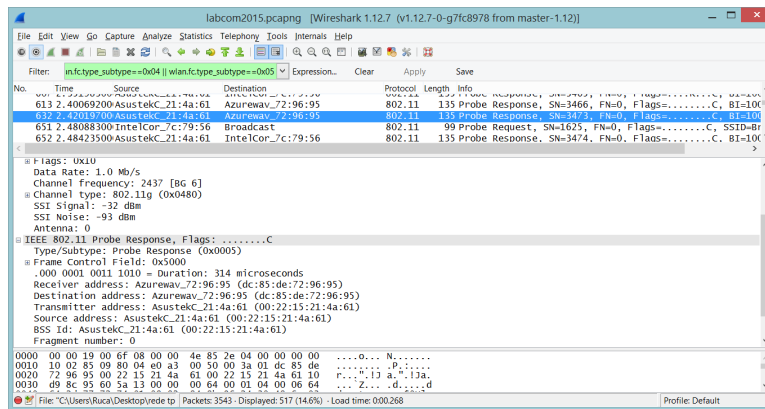
7.1 Certifique-se do tipo de canal que está a ser usado e identifique os APs que, maioritariamente, estão a ser anunciados.

Canais 802.11g A maior parte dos probes enviados pelos AP's, corresponde a duas redes. Uma delas é a rede com o SSID=eduroam, que tem o como AP o Cisco_e4:b3:20 com

o endereço MAC correspondente ($c4 : 14 : 3c : e4 : b3 : 20$), para além disso conseguimos ainda inferir, com base no probe, que funciona essa rede opera no canal 6 com frequência 2437MHz que é do tipo 802.11g.



A outra rede tem o SSID=dd-wrt, que tem o como AP o AsustekC.21:4a:61 com o endereço MAC correspondente ($00 : 22 : 15 : 21 : 4a : 61$), para além disso conseguimos ainda inferir, com base no probe, que funciona essa rede opera no canal 6 com frequência 2437MHz que é do tipo 802.11g.

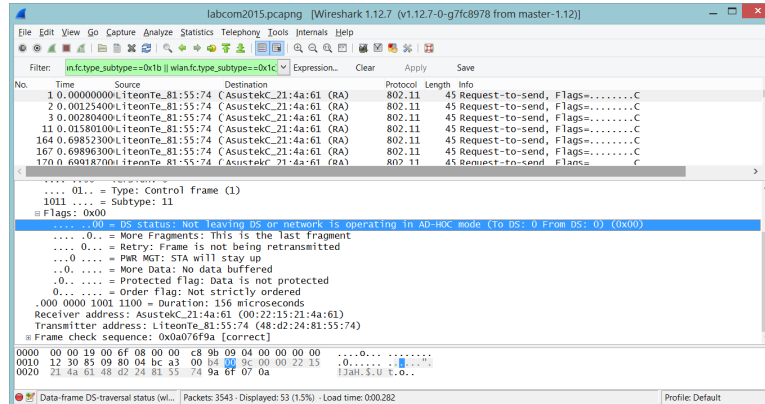


7.2 Tomando como exemplo a estação cujo o endereço MAC é AsustekC.21:4a:61 ($00 : 22 : 15 : 21 : 4a : 61$), identifique a ocorrência de troca de dados envolvendo tramas de controlo RTS/CTS. Verifique a seu sentido de envio (toDS, fromDS). Registe o endereçamento MAC dos sistemas envolvidos, explicando o seu papel no processo de troca de dados.

Utilizando um filtro apropriado, nomeadamente:

```
wlan.addr == 00:22:15:21:4a:61 &&
( wlan.fc.type_subtype==0x1b || wlan.fc.type_subtype==0x1c)
```

Temos a seguinte captura:



Com base na figura, acima apresentada, podemos verificar que tanto a flag toDS como a fromDS tem o *valor* = 0. E como a transmissão Wi-Fi é feita num meio contencioso, e como já referido anteriormente há o problema do hidden node, há a necessidade de impor algum controlo sobre a rede, neste caso é usado a opção RTS/CTS prevista na norma da IEEE 802.11, de modo a regular a transmissão de dados, e minimizar os problemas ao nível das colisões e coerência de endereços MAC. A fonte de envio do RTS é o LiteonTe_81:55:74, e o destino AsustekC_21:4a:61, portanto o LiteonTe_81:55:74 informa o AsustekC_21:4a:61 que deseja/está pronto para utilizar o meio.

8 Conclusão

Neste relatório que foi realizado com o intuito de propor respostas as perguntas apresentadas na ficha prática nº3, no âmbito da unidade curricular de Redes de Computadores, acreditamos termos respondido de forma clara e bem fundamentada as questões aqui apresentadas, e apesar de durante a realização da ficha prática termos tido, de uma forma geral, dificuldades relacionadas com a compreensão e relação entre muitas questões aqui apresentadas, depois de despendir algumas horas de estudo e concluir a ficha, com o apoio das aulas práticas, conseguimos fundamentar e sedimentar muito dos conceitos que pensávamos já conhecer. Avaliamos por isso, a realização dessa ficha prática de forma muito positiva, pois de outra forma, dificilmente teríamos capacidades e/ou motivação para aprofundar e estudar certos detalhes dos protocolos aqui apresentados, e toda a vasta matéria aqui abordada.

Referências

1. Wireshark Wikipedia : <https://wiki.wireshark.org/Ethernet> (25/11/2015)
2. IEEE 802.11 Wireless LANs : <https://standards.ieee.org/about/get/802/802.11.html> (25/11/2015)
3. Cisco Association Explained : <https://documentation.meraki.com/> (25/11/2015)