

# TP3: Redes Sem Fios (802.11)

Universidade do Minho

Departamento de Informática, 4710-057 Braga, Portugal

Redes de Computadores

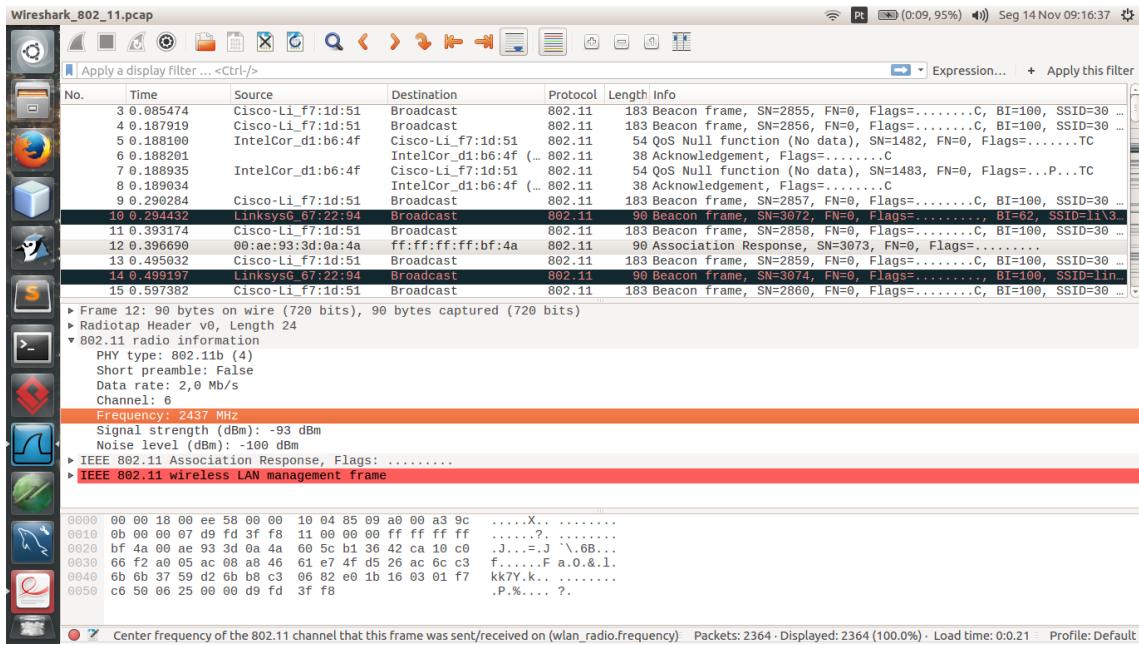
Autores:

Paulo Guedes, a74411@alunos.uminho.pt

Diogo Gomes, a73825@alunos.uminho.pt

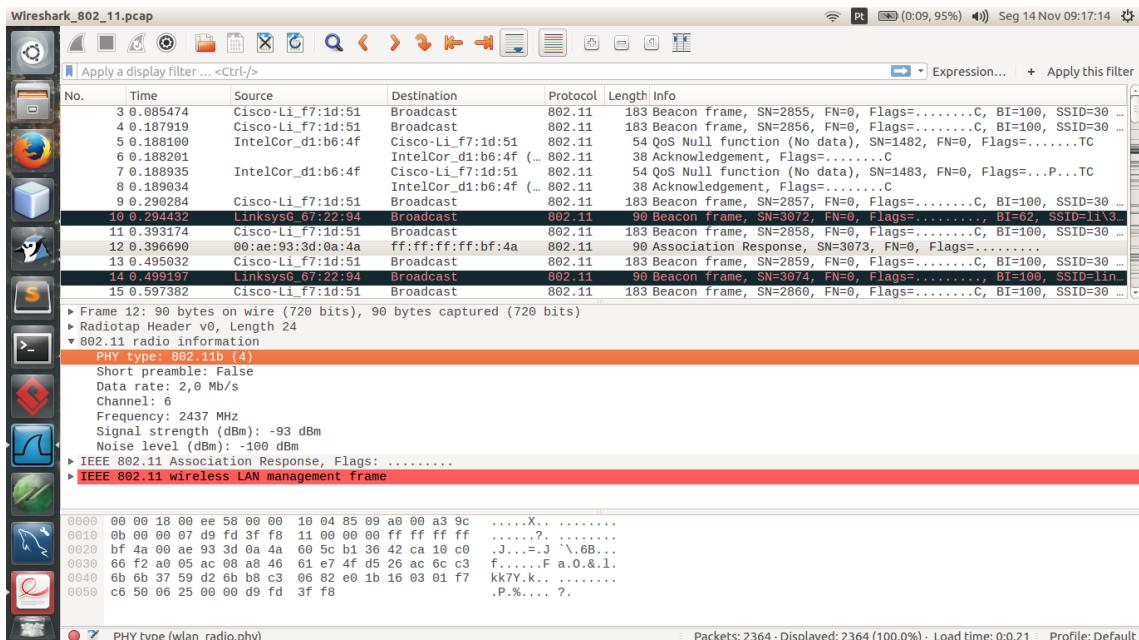
Carlos Campos, a74745@alunos.uminho.pt

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).



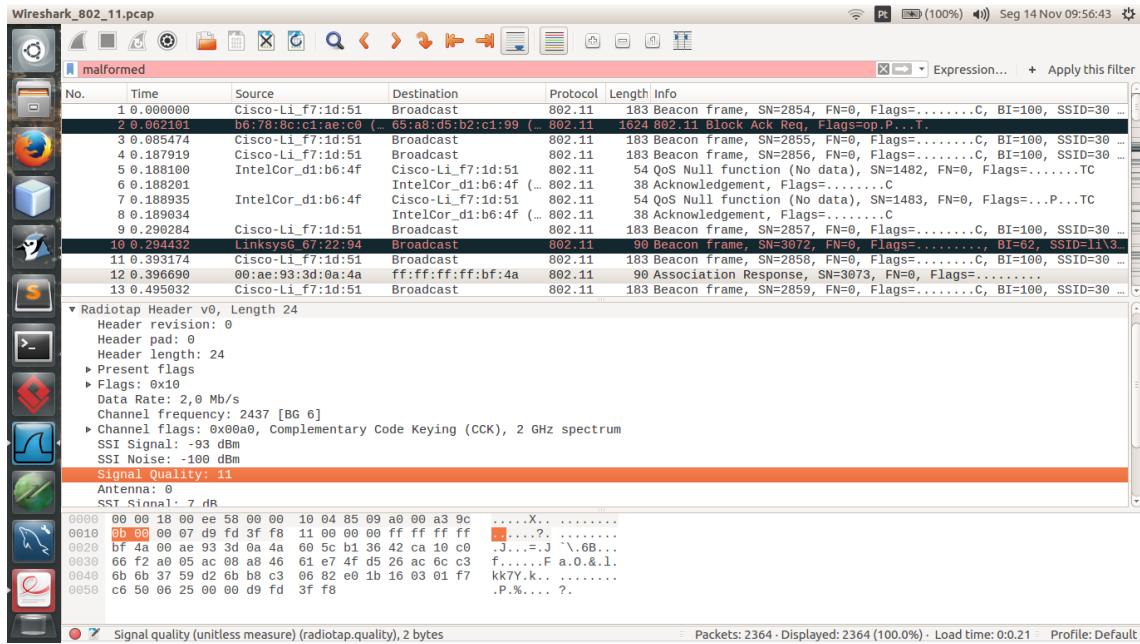
A rede está a operar a uma frequência de 2437 MHz e canal é o 6.

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?



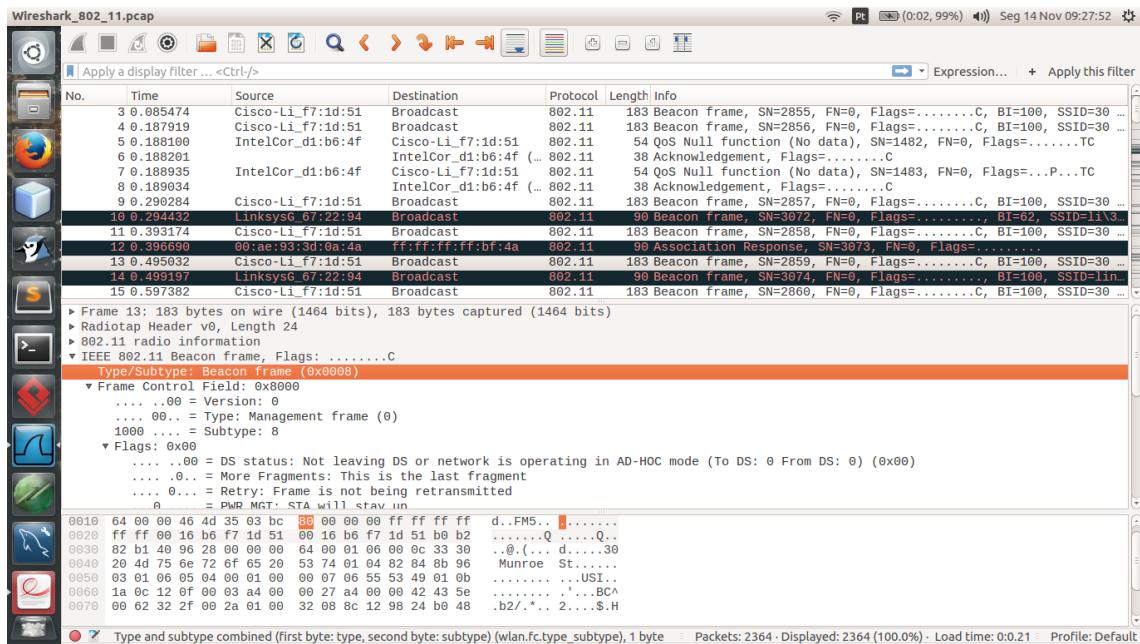
O canal a ser utilizado é o tipo 802.11b, e o débito a que foi enviada a trama é 2,0 Mb/s.

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



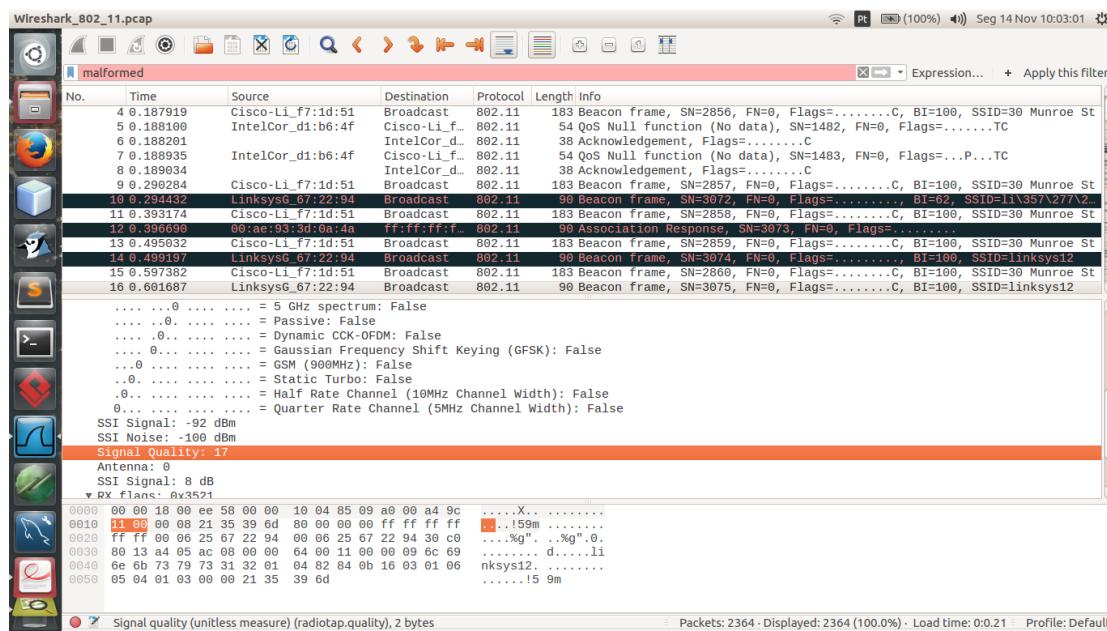
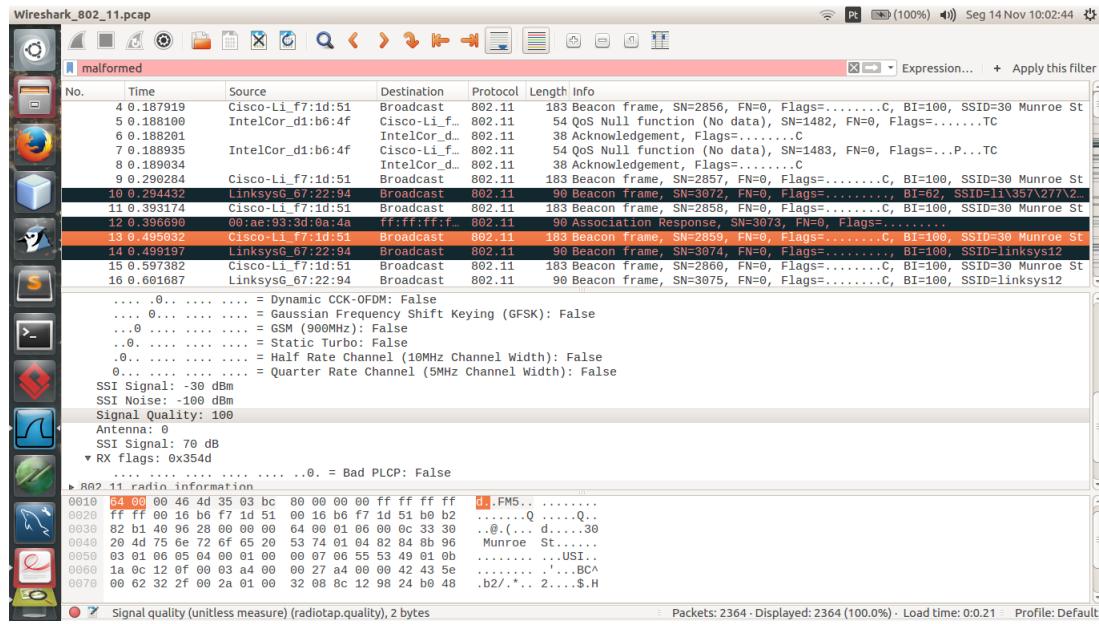
O índice de qualidade do sinal é 11.

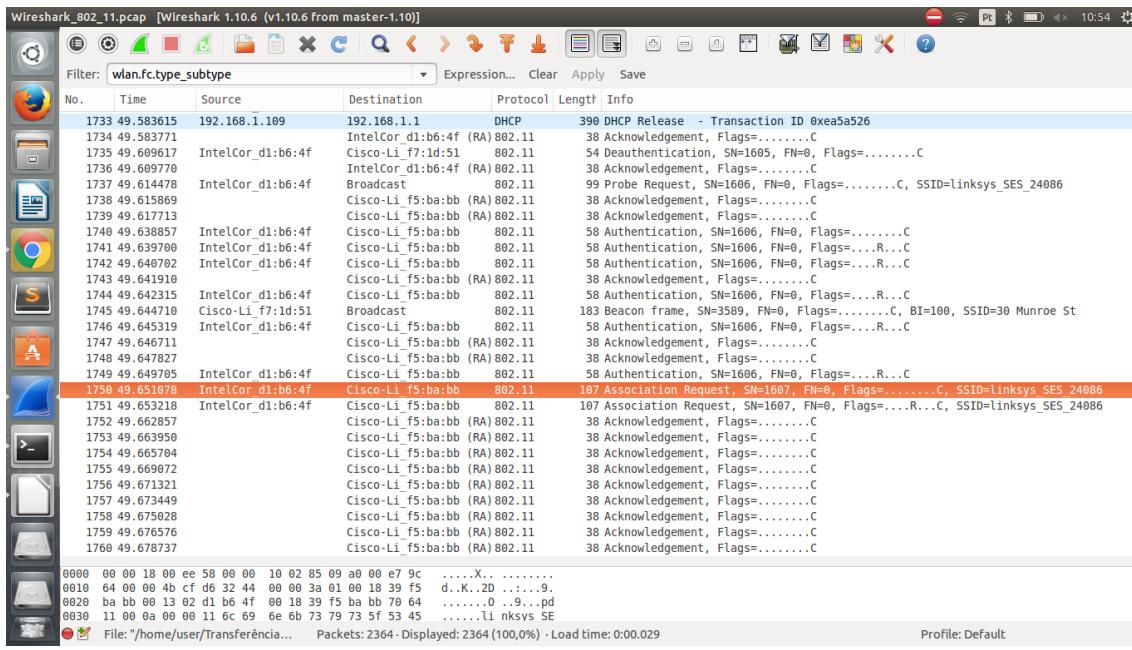
### 4. Qual o tipo de uma trama *beacon*? Indique quais os seus identificadores de tipo e subtipo. Em que parte da trama estão especificados?



A trama beacon é uma “Management frame”, sendo o identificador de tipo 00, e o identificador de subtipo é 1000, e os mesmos estão assinalados no screenshot.

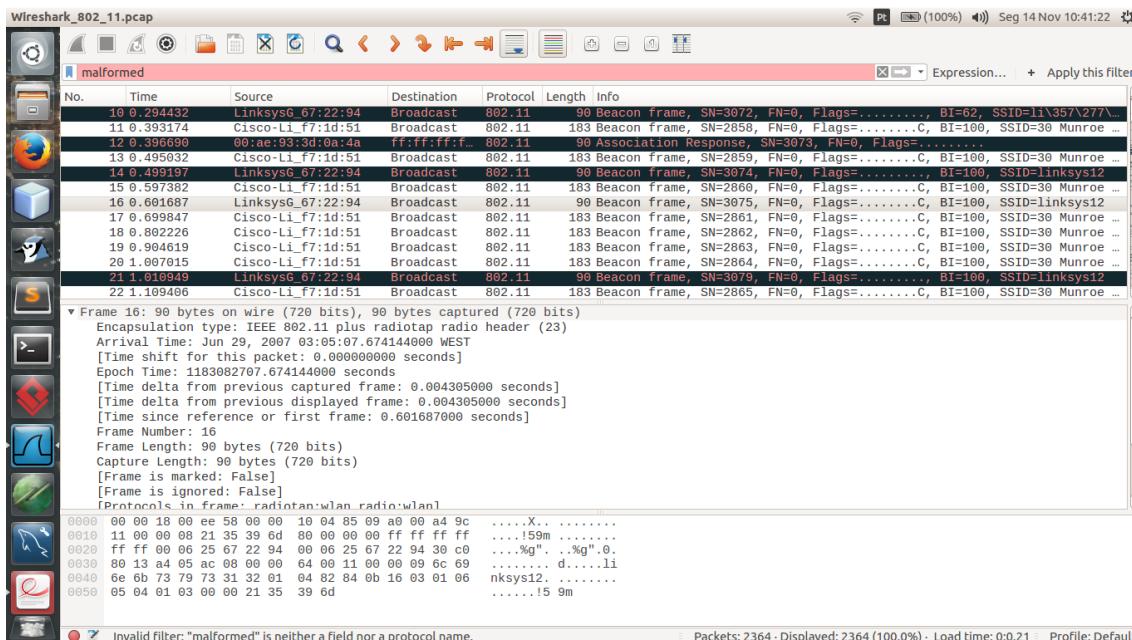
5. Identifique os SSIDs dos APs (Access Points) que estão a operar na rede e diga qual tende a proporcionar a melhor qualidade de sinal?

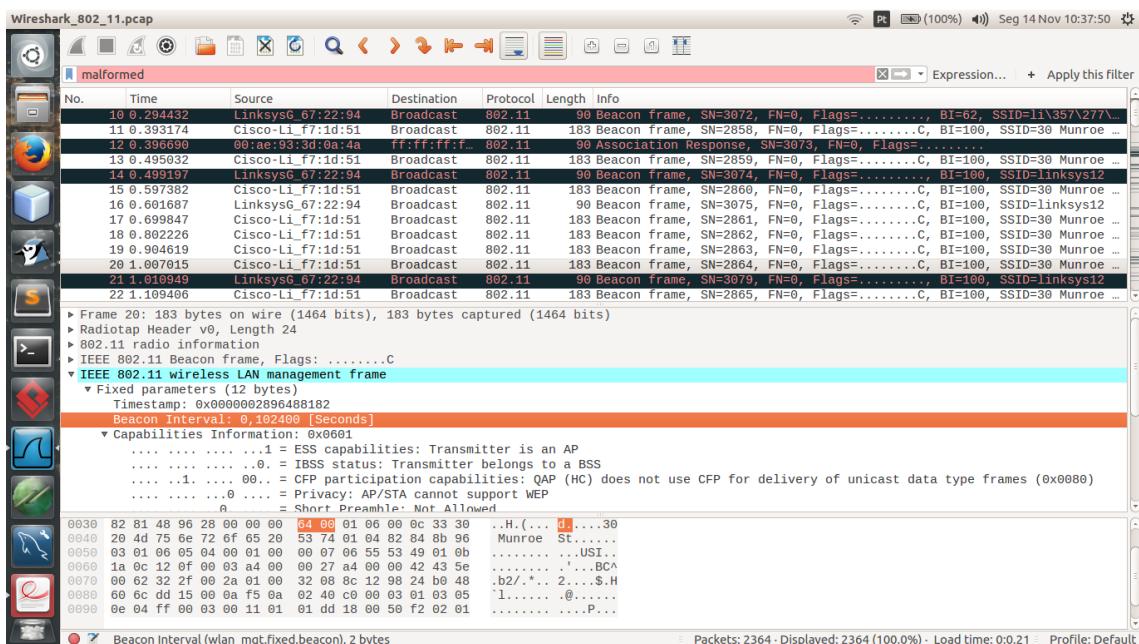
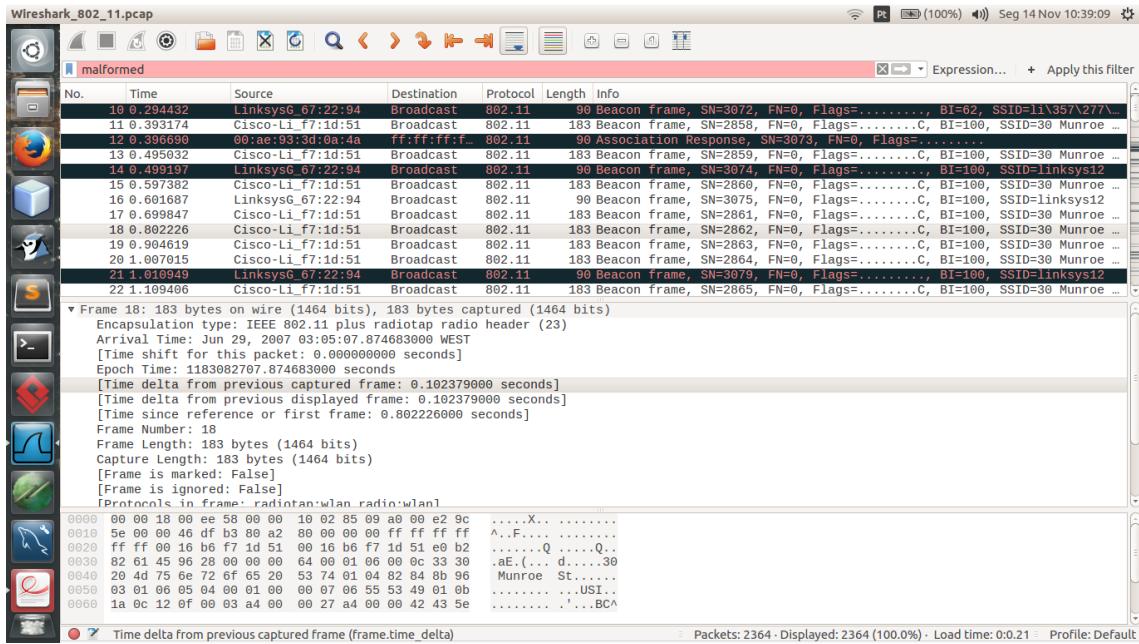


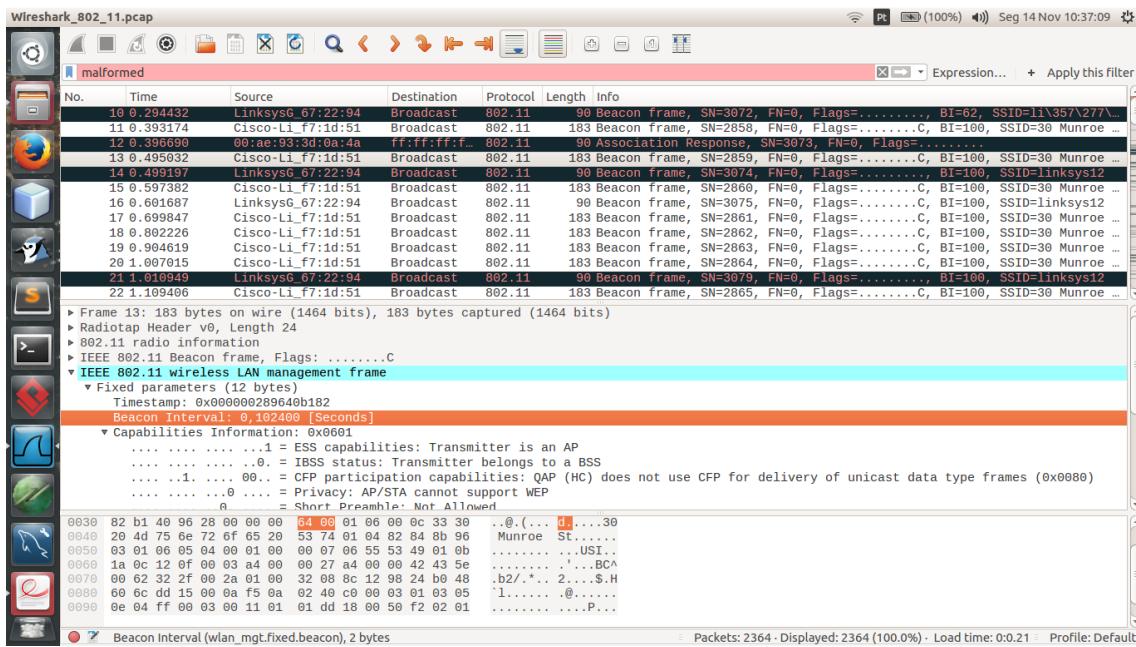


Identificamos 3 SSIDs dos APs, o linksys12, o 30 Munroe St e o lynksys\_SES\_24086. Verificamos que o que tem melhor qualidade de sinal é o 30 Munroe St com qualidade de 100.

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.

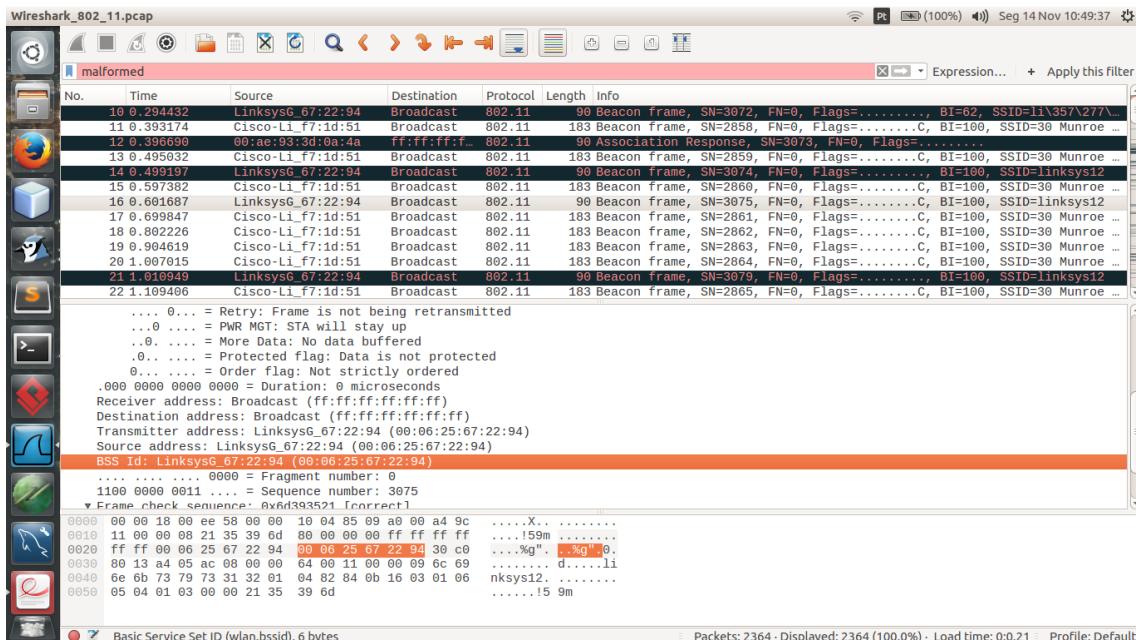




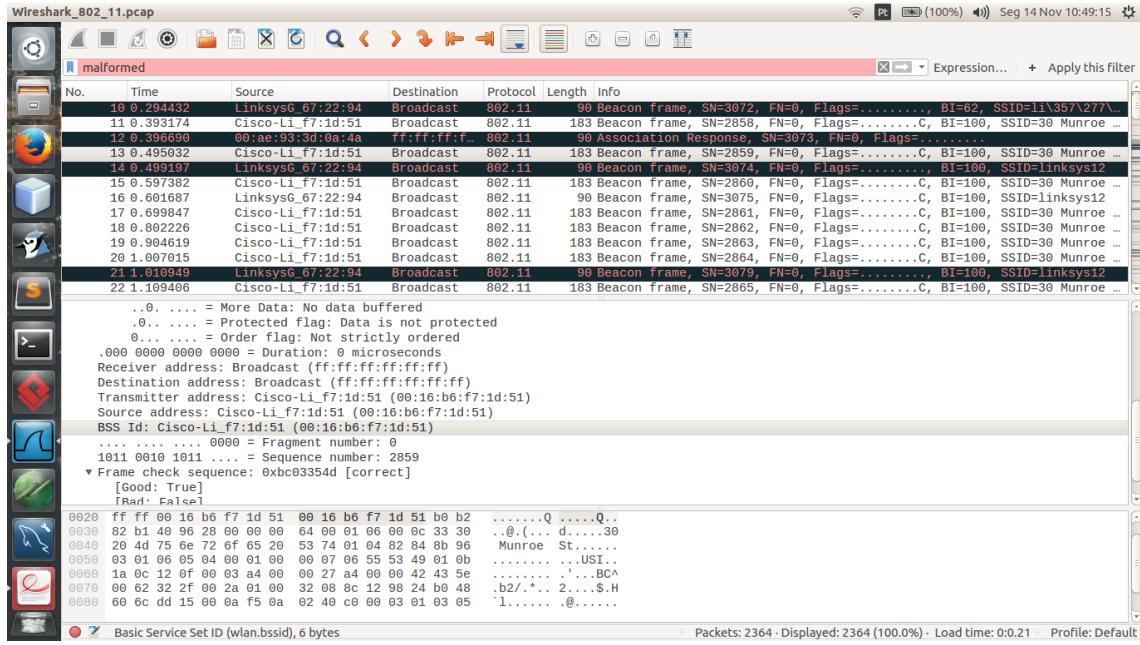


Como podemos verificar os intervalos são iguais, de 0,102400 segundos, para os APs 30 Munroe St e para linksys12. Podemos também verificar que a periodicidade da trama beacon acontece apenas para os APs 30 Munroe St, sendo uma das razões para isto acontecer a possibilidade de existirem barreiras durante a transmissão.

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.

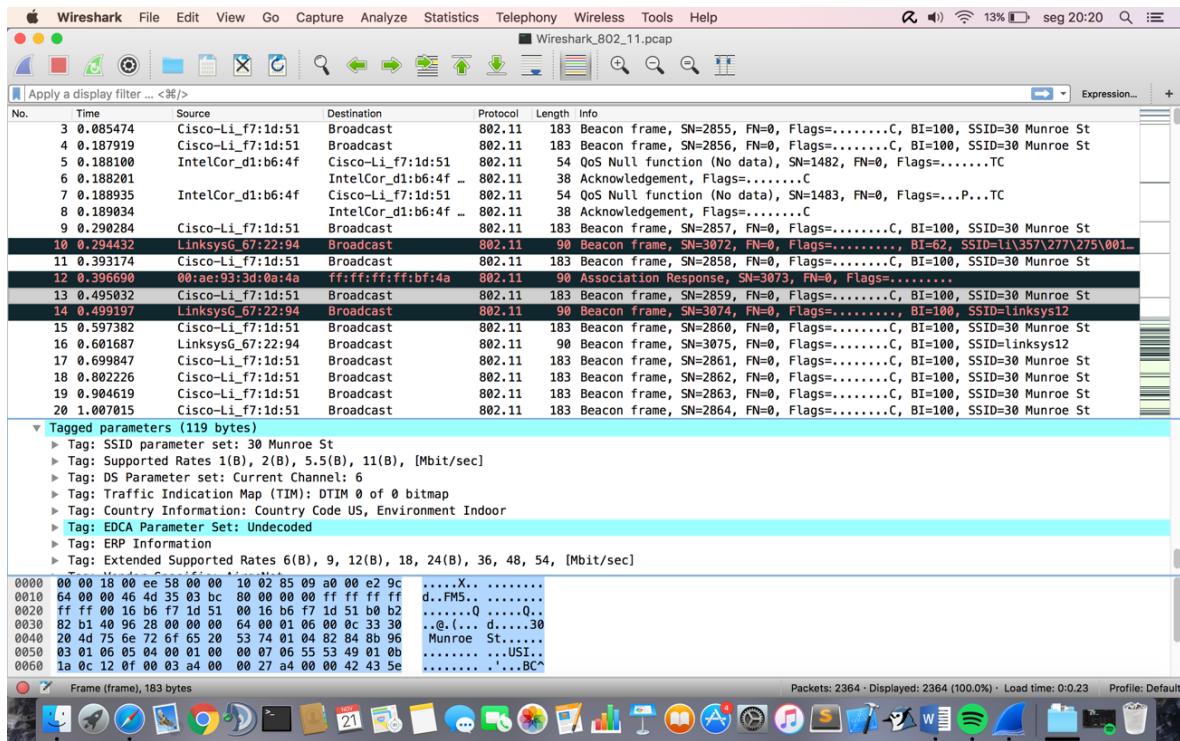


Para o AP LinksysG\_67:22:94, temos o endereço de destino ff:ff:ff:ff:ff:ff, que significa que chega a todos os utilizadores. E o endereço de origem 00:06:25: 67:22:94. Sendo esta uma trama beacon o endereço do transmissor vai se igual ao BSSID, isto é 00:06:25:67:22:94.



Para o AP Cisco-Li\_f7:1d:51, temos o endereço de destino ff:ff:ff:ff:ff:ff, que significa que chega a todos os utilizadores. E o endereço de origem 00:16: b6: f7:1d:51. Sendo esta uma trama beacon o endereço do transmissor vai se igual ao BSSID, isto é 00:16: b6: f7:1d:51.

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?



Os “*extended supported rates*” são 6, 9, 12, 18, 24, 36, 48, 54 Mbps e os débitos suportados são 1, 2, 5.5 e 11 Mbps

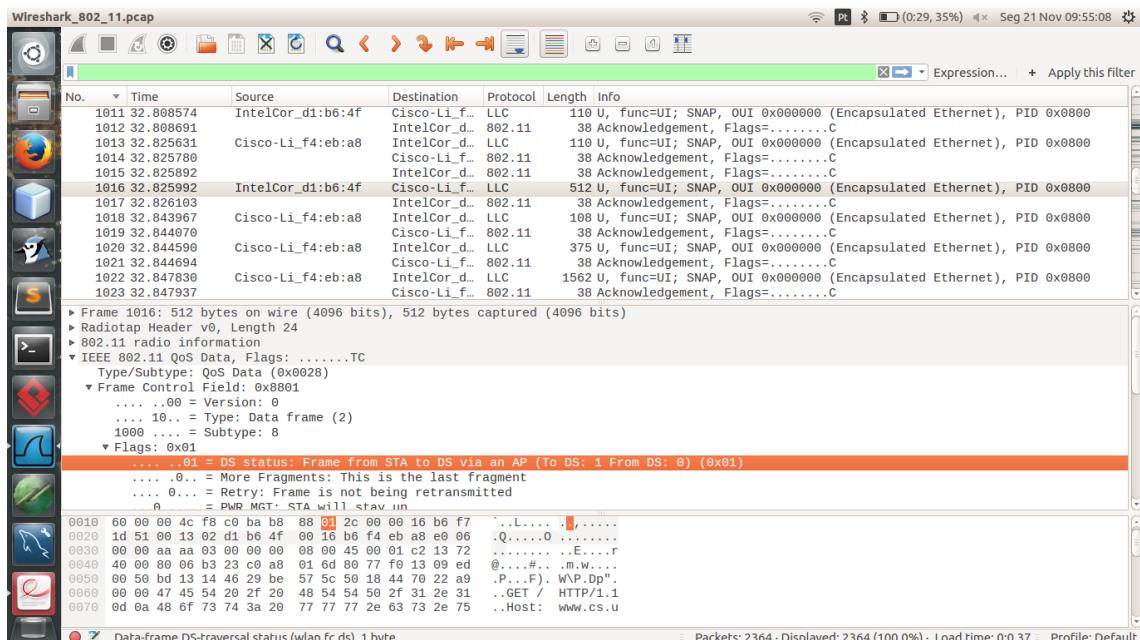
9. Indique a que sistemas são endereçadas estas tramas e qual o seu propósito?

AS tramas beacon têm como objetivos indicar que o AP está presente e transmitir as suas informações. Estas tramas são enviadas em para todos os sistemas na LAN.

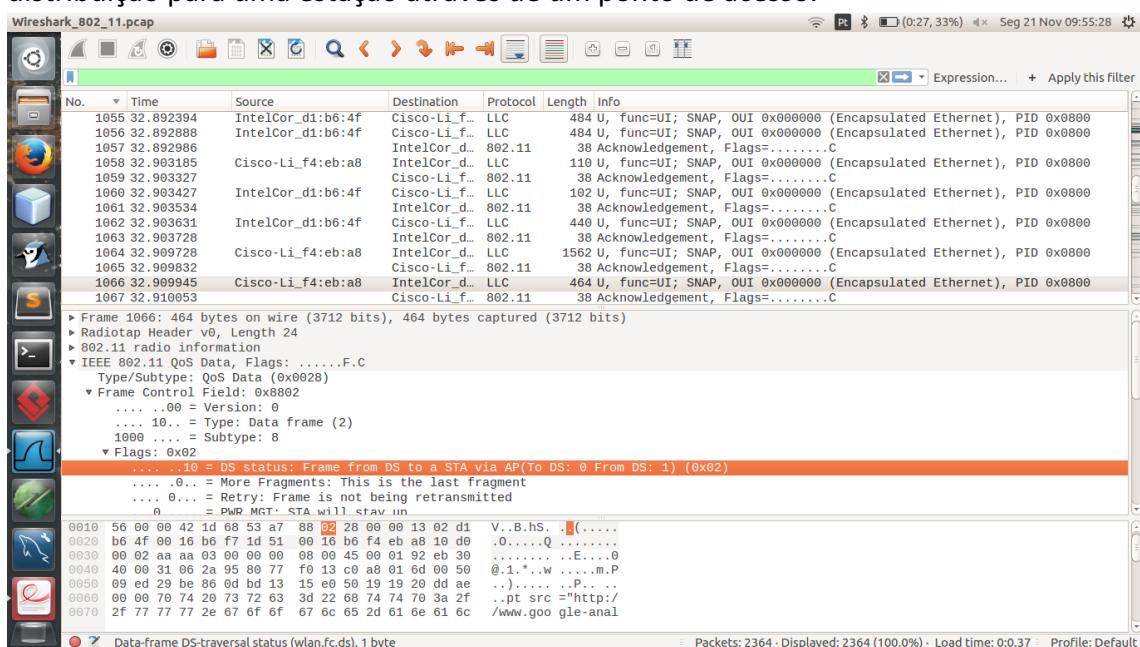
10. O campo *Frame Control* contido no cabeçalho das tramas 802.11 permite especificar a direccionalidade das tramas. Identifique a direccionalidade das tramas indicadas acima (no1016 e no1066).

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

Na trama 1016 a direccionalidade é 0x8801, correspondente a 1000 1000 0000 0001, na parte assinalada podemos verificar que a trama é enviada de uma estação para um sistema de distribuição através de um ponto de acesso.



Na trama 1066 a direccionalidade é 0x8802, correspondente a 1000 1000 0000 0010, na parte assinalada podemos verificar que a trama é enviada por um sistema de distribuição para uma estação através de um ponto de acesso.



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)?

The Wireshark capture shows a sequence of 802.11 frames. Frame 1016 is highlighted, containing a GET request to 'www.cs.u'. The details pane shows the frame structure and fields. The source MAC is 00:13:02:d1:b6:4f, the destination MAC is 00:16:b6:f4:eb:a8, and the BSSID/AP MAC is 00:16:b6:f7:1d:51.

Endereço MAC do host sem fios: 00:13:02: d1: b6:4f

Endereço MAC do router de acesso ao DS: 00:16: b6: f4: eb:a8

Endereço MAC do AP: 00:16: b6: f7:1d:51

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

The Wireshark capture shows a sequence of 802.11 frames. Frame 1066 is highlighted, containing a response to the previous GET request. The details pane shows the frame structure and fields. The source MAC is 00:16:b6:f4:eb:a8, the destination MAC is 00:13:02:d1:b6:4f, and the BSSID/AP MAC is 00:16:b6:f7:1d:51.

Endereço MAC do host sem fios(Destination): 00:13:02: d1: b6:4f

Endereço MAC do router de acesso ao DS(Source): 00:16: b6: f4: eb: a8

Endereço MAC do AP: 00:16: b6: f7:1d:51

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.)

Podemos verificar que é de tipo principal Control e subtipo Acknowledgement(ACK).

**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 trama 1733:

The Wireshark interface displays a network capture named "Wireshark\_802\_11.pcap". The timeline shows several frames. Frame 1733 is highlighted as a "DHCP Release - Transaction ID 0xea5a526". The details pane shows the frame structure, including the IEEE 802.11 header and payload. The bytes pane shows the raw hex and ASCII data. The bottom status bar indicates "File: /home/user/Transferência... Packets: 2364 · Displayed: 2364 (100,0%) · Load time: 0:00:078 · Profile: Default".

### A trama 1735 de desassociação:

The Wireshark interface displays a network capture named "Wireshark\_802\_11.pcap". Frame 1735 is highlighted as a "54 bytes on wire (432 bits), 54 bytes captured (432 bits)" IEEE 802.11 Deauthentication frame. The details pane shows the frame structure, including the IEEE 802.11 header and payload. The bytes pane shows the raw hex and ASCII data. The bottom status bar indicates "File: /home/user/Transferência... Packets: 2364 · Displayed: 2364 (100,0%) · Load time: 0:00:078 · Profile: Default".

Era esperado ver esta trama de desassociação.

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.

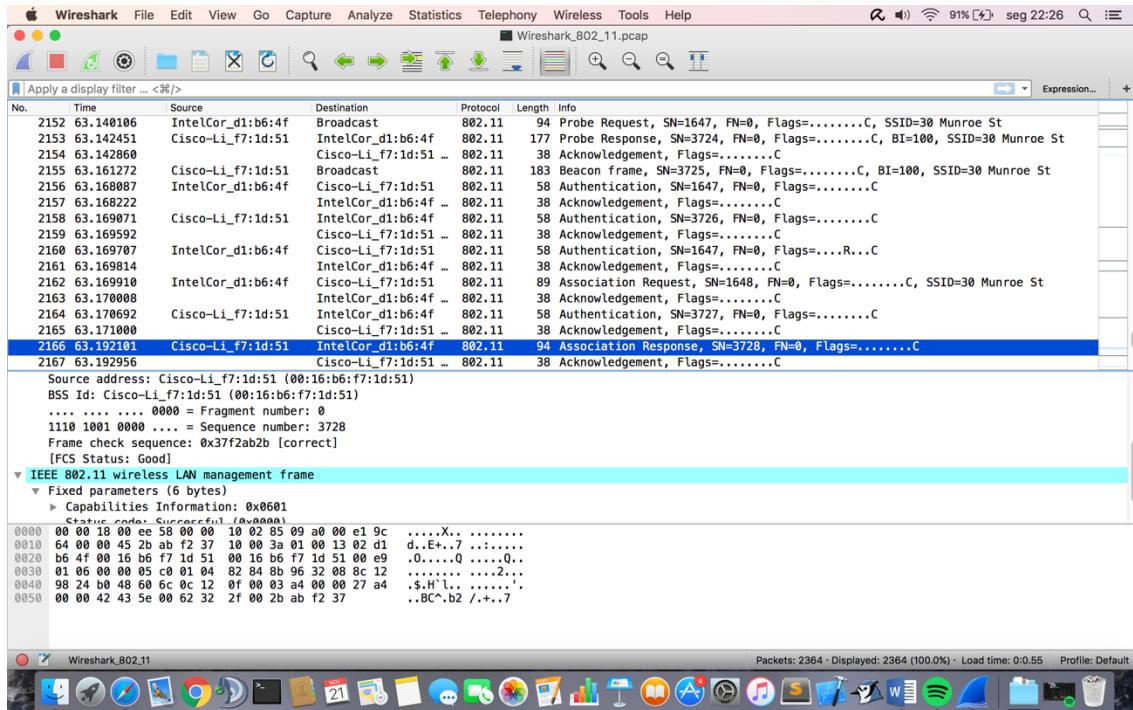
16. O *host* tenta usar algum algoritmo de autenticação/chave ou tenta aceder de forma aberta (consulte o *authentication algorithm* na trama)? Existe alguma resposta do AP *linksys\_SES\_24086* ao pedido de autenticação? Porquê?

Authentication Algorithm: Open System (0)  
Authentication SEQ: 0x0001  
Status code: Successful (0x0000)

0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e5 9c ....X.. ....:  
0010 64 00 00 49 3e cf 61 1e b0 00 3a 01 00 18 39 f5 d..I->.a. ....9..  
0020 ba bb 00 13 02 d1 b6 4f 00 18 39 f5 ba bb 30 65 .....0..9...0e  
0030 00 00 01 00 00 00 3e cf 61 1e .....>. a.

O host tenta aceder de forma aberta como podemos ver a parte assinalada no screenshot, e podemos também verificar que não existe nenhuma resposta por parte do AP, possivelmente por ser Open System.

**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.



## Conclusões

Neste trabalho expandimos o nosso conhecimento o protocolo utilizado, isto é o protocolo IEEE 802.11.

Após termos realizados estes dois últimos trabalhos, observamos que algumas diferenças entre estes. Alguns dos aspectos positivos do protocolo IEEE 802.11 é a uma maior acessibilidade, comparando há Ethernet, sendo que este protocolo também abrange um maior número de dispositivos. Para além de que o número de entradas Ethernet restringirem o número de aparelhos ligados, enquanto o protocolo IEEE 802.11 não tem essas limitações.

Pelo contrário, podemos verificar que caso não haja APs disponíveis é impossível comunicar com o exterior da rede. Outro ponto onde o protocolo IEEE 802.11 é pior que a Ethernet será o facto de este ser muito sensível aos obstáculos no meio de comunicação, sejam eles, por exemplo, materiais refletores, entre outros.

Para concluir, foi possível entender este protocolo melhor, tal como este protocolo escolhe o melhor AP disponível, ou sobre as tramas beacon, e aprimorar os nossos conhecimentos sobre o Wireshark.