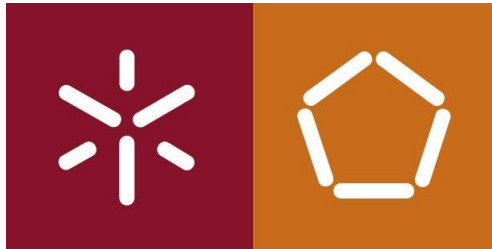


UNIVERSIDADE DO MINHO

MESTRADO INTEGRADO EM ENGENHARIA INFORMÁTICA



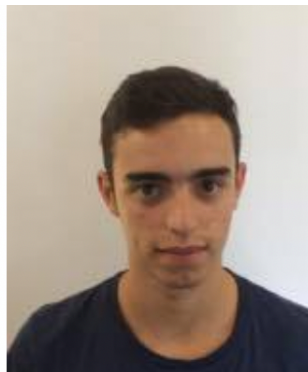
TP4 - Redes Sem Fios (802.11)

REDES DE COMPUTADORES

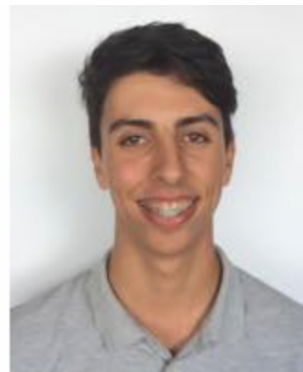
PL 4 GRUPO 8



Carla Cruz
A80564



Diogo Sobral
A82523



Pedro Freitas
A80975

December 15, 2018

Acesso Rádio

Como pode ser observado, a sequência de bytes capturada inclui informação do nível físico (*radio information*), para além dos *bytes* correspondentes a tramas 802.11. Para a trama correspondente 348,

1. **Identifique em que frequência do espectro está a operar a rede sem fios, e o canal que corresponde essa frequência.**

Como vemos na Figura 1, a rede sem fios está a operar a uma frequência de 2467 MHz, correspondendo ao canal 12 do espectro de frequências.

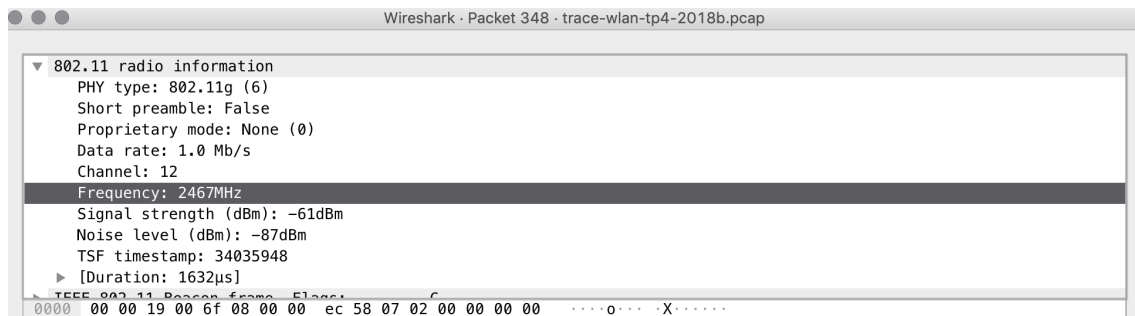


Figure 1: Frequência da rede sem fios

2. **Identifique a versão da norma IEEE 802.11 que está a ser usada.**

Pela Figura 2, podemos concluir está a ser usada a versão 802.11g(6).

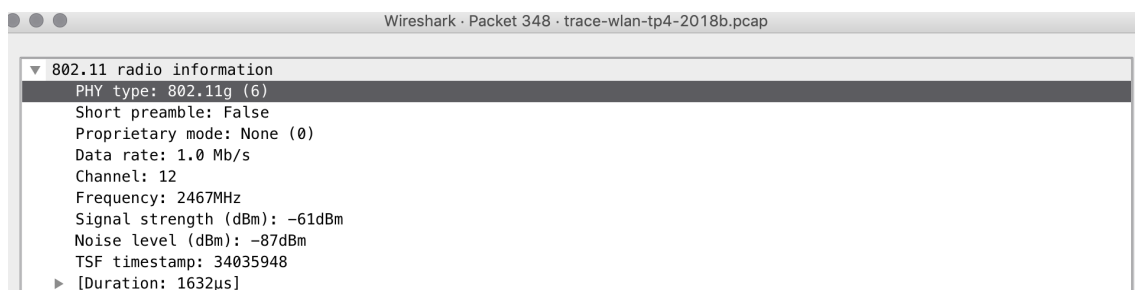


Figure 2: Versão da norma IEEE 802.11

3. Qual o débito a que foi enviada a trama escolhida? Será que esse débito corresponde ao débito máximo a que a interface WiFi pode operar? Justifique.

A trama escolhida foi enviada a 1.0Mbps.

Este débito não corresponde ao débito máximo da interface WiFi visto que, a versão 802.11g consegue atingir um débito de 58 Mbps.

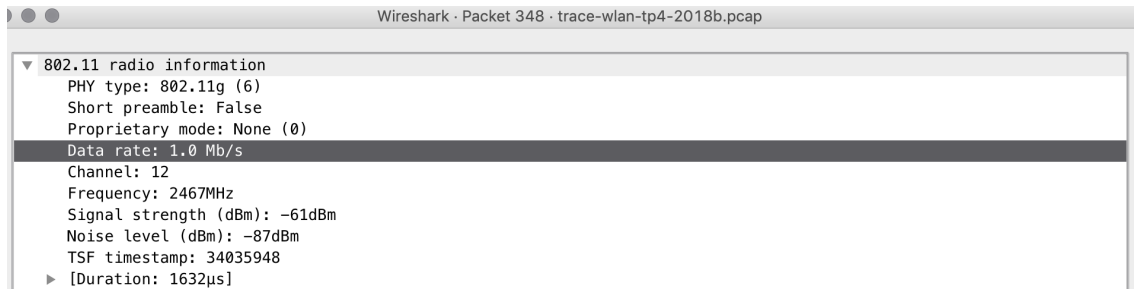


Figure 3: Débito da trama escolhida

Scanning Passivo e Scanning Ativo

As tramas *beacon* permitem efetuar *scanning* passivo em redes IEEE 802.11(WiFi). Para a captura de tramas disponibilizada, responda às seguintes questões:

4. Selecione uma *trama beacon* (e.g., a trama 348) Esta trama pertence a que tipo de tramas 802.11? Indique o valor dos seus identificadores de tipo e de subtipo. Em que parte concreta do cabeçalho da trama estão especificados(ver anexo)?

A trama Beacon pertence ao tipo 802.11g. O tipo corresponde a um *Management Frame (Frame de Gestão)*, enquanto que o subtipo tem o valor de identificação: 8 que corresponde a um *beacon*.

Estes valores estão especificados na posição da *frame control* entre os bits 3 e 8, nos campos *type* e *subtype* , respetivamente.

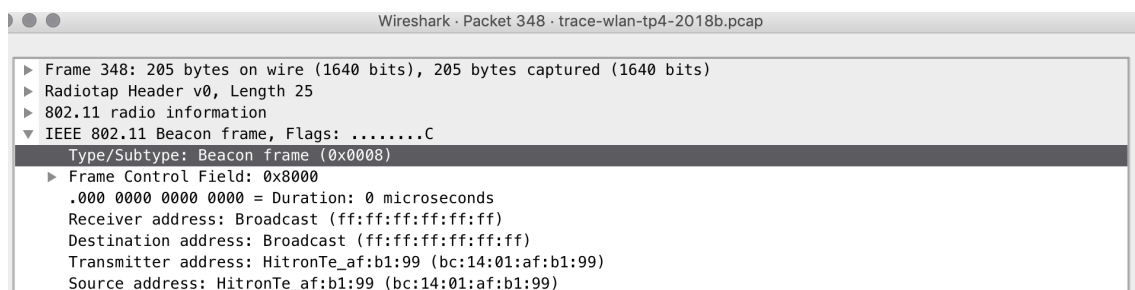


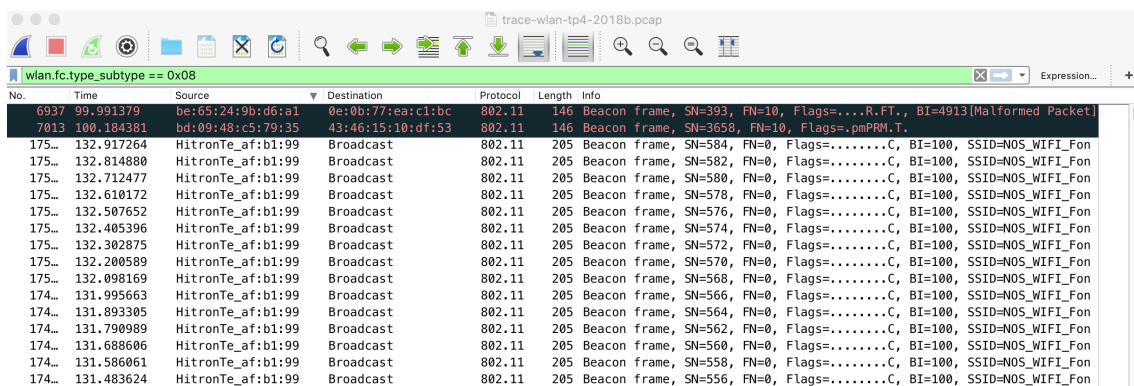
Figure 4: Tipo e Subtipo da Beacon Frame

5. Liste todos os SSIDs dos APs (*Access Points*) que estão a operar na vizinhança da STA de captura? Explícite o modo como obteve essa informação. Como sugestão pode construir um filtro de visualização apropriado (tomando como base a resposta da alínea anterior) que lhe permita obter a listagem pretendida.

Os SSIDs dos APs encontrados são:

- (i) FlyingNet
- (ii) NOS_WIFI_FON

Para encontrar os SSID diferentes começamos por aplicar no Wireshark o filtro `wlan.fc.type_subtype == 0x08` de modo a ficarmos apenas com tramas Beacon na nossa amostra. De seguida, ordenamos as tramas por ordem alfabética do Source ficando com o resultado da figura 5.

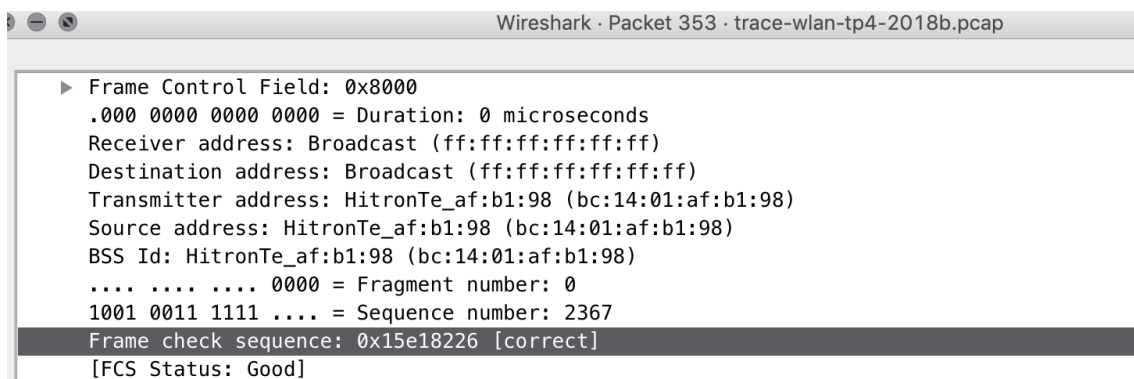


No.	Time	Source	Destination	Protocol	Length	Info
6937	99.991379	be:65:24:9b:d6:a1	0e:0b:77:ea:c1:bc	802.11	146	Beacon frame, SN=393, FN=10, Flags=...R.F.T., BI=4913 [Malformed Packet]
7013	100.184381	bd:09:48:c5:79:35	43:46:15:10:df:53	802.11	146	Beacon frame, SN=3658, FN=10, Flags=.pmPRM.T.
175...	132.917264	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=584, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
175...	132.814880	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=582, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
175...	132.712477	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=580, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
175...	132.610172	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=578, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
175...	132.507652	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=576, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
175...	132.405396	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=574, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
175...	132.302875	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=572, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
175...	132.200589	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=570, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
175...	132.098169	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=568, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
174...	131.995663	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=566, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
174...	131.893305	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=564, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
174...	131.790989	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=562, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
174...	131.688606	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=560, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
174...	131.586061	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=558, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
174...	131.483624	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=556, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

Figure 5: Amostra encontrada

Por fim, ao procurar na amostra obtida, chegamos à conclusão que apenas tínhamos dois SSIDs distintos.

6. Verifique se está a ser usado o método de deteção de erros (CRC), e se todas as tramas Beacon são recebidas corretamente. Justifique o porquê de usar deteção de erros neste tipo de redes locais.



Wireshark · Packet 353 · trace-wlan-tp4-2018b.pcap	
▶	Frame Control Field: 0x8000
	.000 0000 0000 0000 = Duration: 0 microseconds
	Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
	Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
	Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
	Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
	BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
 0000 = Fragment number: 0
	1001 0011 1111 = Sequence number: 2367
	Frame check sequence: 0x15e18226 [correct]
	[FCS Status: Good]

Figure 6: Trama beacon aleatória

Na figura 6 temos uma trama que foi escolhida de forma aleatória. Como podemos ver, neste caso, o frame check sequence foi utilizado sem que se tenha encontrado qualquer erro.

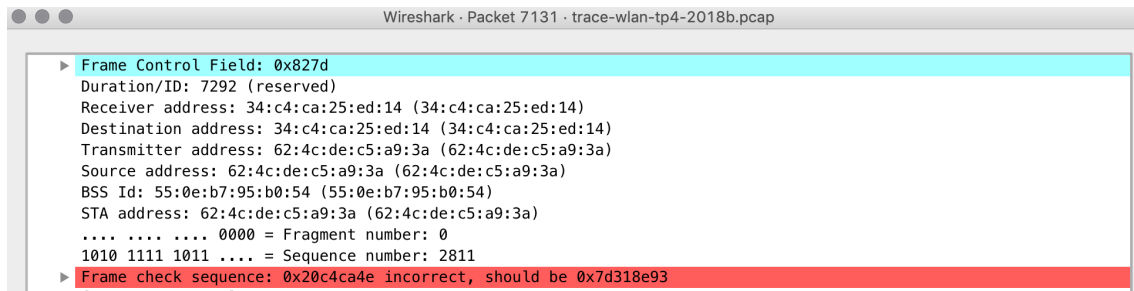


Figure 7: Trama beacon recebida incorreta

Ao contrário da figura 6 que foi recebida corretamente, a trama 7131 teve erros e o valor do FCS fica assim representado com um valor incorreto.

Como há grande probabilidade de haver colisões de tramas nas redes wifi originada pela liberdade que os dispositivos têm de transmitir informação para um AP é necessário recorrer ao uso do FCS para que se consiga saber de pontuais colisões que tenham acontecido.

7. Para dois dos APs identificados, indique qual é o intervalo de tempo previsto entre tramas *beacon* consecutivas? (Nota:este valor é anunciado na própria trama *beacon*). Na prática, a periodicidade de tramas *beacon* é verificada? Tente explicar porquê..

Como vemos pela figura 8 , o intervalo de tempo previsto entre tramas consecutivas: 0.102400 segundos.

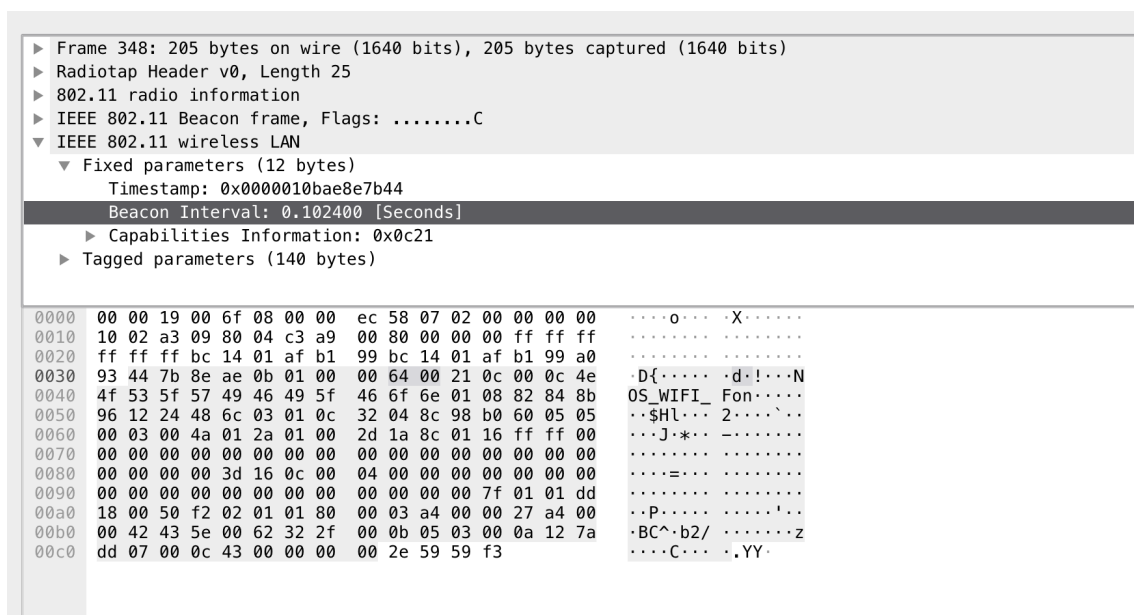


Figure 8: Intervalo de tempo entre Beacons

De facto na prática este intervalo não é respeitado, embora o valor seja muito próximo. O intervalo de tempo apresentado na trama *beacon* é uma aprox-

imação do tempo real dos intervalos, sendo que quando existe uma grande quantidade de tráfego o intervalo sai um pouco prejudicado, e é proporcional à quantidade de tráfego existente (quanto maior tráfego maior o intervalo de tempo entre *beacons*). Isto resulta de uma tentativa de melhoria de performance e velocidade da rede, pois quanto maior for o intervalo entre tramas *beacon* melhor será a velocidade e performance da mesma.

Assim pela figura 9 vemos que a diferença entre duas tramas *beacon* seguidas (348 e 350) é de 0.102298, ou seja, menos um pouco do que era esperado. Este valor mais precoce é devido a haver pouco tráfego na rede.

347	14.233824	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2361, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
348	14.235456	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2362, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
349	14.336138	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2363, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
350	14.337754	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2364, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

Figure 9: Frame da Beacon e seu número de pacote

8. Identifique e registre todos os endereços MAC usados nas tramas *beacon* enviadas pelos APs. Recorde que o endereçamento está definido no cabeçalho das tramas 802.11, podendo ser utilizados até quatro endereços com diferente semântica. Para uma descrição detalhada da estrutura da trama 802.11, consulte o anexo ao enunciado.

Como vemos pelas figuras 10 e 11, ambas as tramas 348 e 349, tanto o *Receiver Address* como o *Destination Address* têm o MAC address : ff:ff:ff:ff:ff:ff, o que corresponde ao broadcast.

Quanto ao *Transmitter Address* e *Source Address* as duas tramas já têm valores diferentes.

O AP correspondente à trama 348 tem *Transmitter Address* e *Source Address* com o valor : bc:14:01:af:b1:99, que corresponde ao STA HitronTe_af:b1:99.

O AP correspondente à trama 349 tem *Transmitter Address* e *Source Address* com o valor : bc:14:01:af:b1:98, que corresponde ao STA HitronTe_af:b1:98.

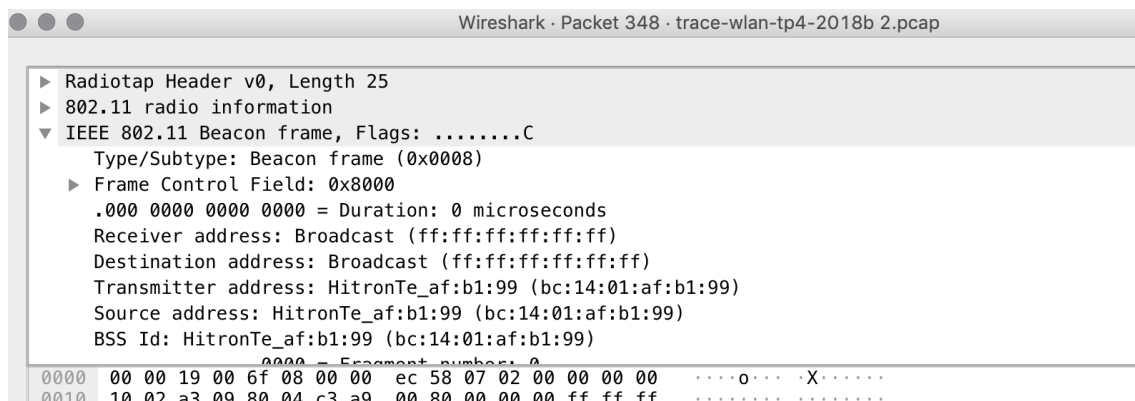


Figure 10: Endereços MAC da trama Beacon do pacote 348

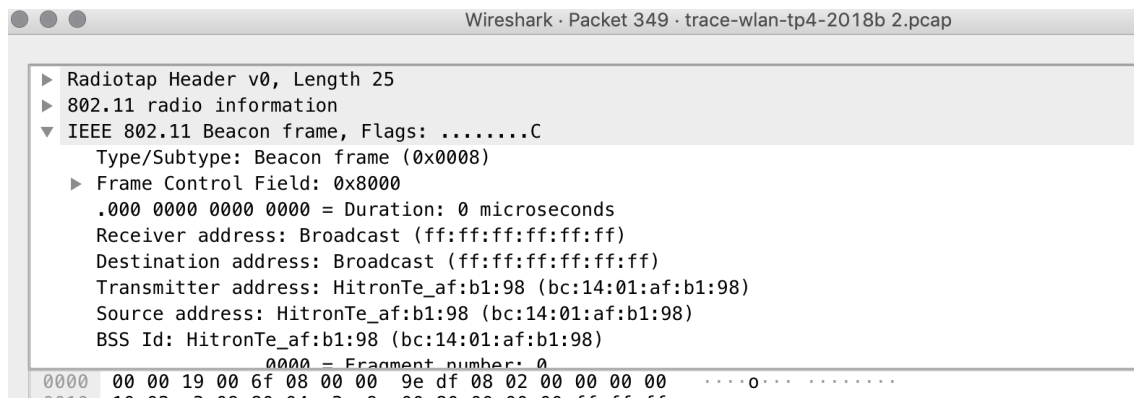


Figure 11: Endereços MAC da trama Beacon do pacote 349

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

Como vemos pela Figura 12, os *extended supported rates* suportados pelo AP são de: 6,12,24 e 48 Mbit/sec .

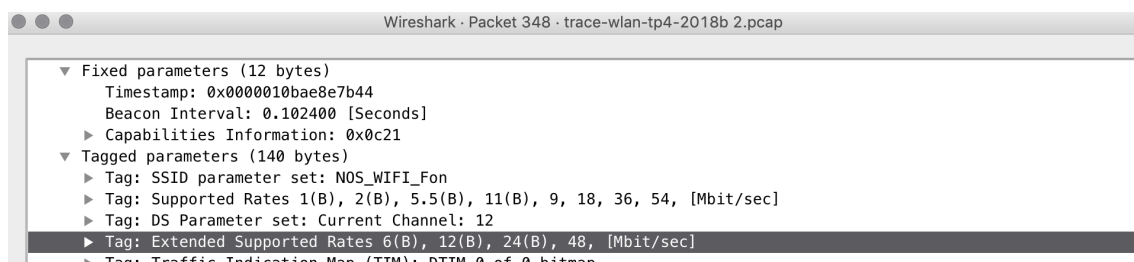


Figure 12: Extended Supported Rates da trama

No *trace* disponibilizado também foi registrado *scanning* ativo,i.e., envolvendo tramas *probe request* e *probe response*, comuns nas redes WiFi como alternativa ao *scanning* passivo.

10. Estabeleça um filtro Wireshark apropriado que lhe permita visualizar todas as tramas *probing request* ou *probing response*, simultaneamente.

O filtro usado foi de forma a obter *probing response* e *probing request*, ou seja , tramas cujo valor do tipo é 0 e o valor do subtipo é 4 para *request* e 5 para *response*.

Como podemos ver Figura 13 o filtro usado foi: wlan.fc.type_subtype == 4 or wlan.fc.type_subtype == 5 .

No.	Time	Source	Destination	Protocol	Length	Info
1300	53.746911	Apple_10:6a:f5	Broadcast	802.11	155	Probe Request, SN=2516, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2467	70.147855	ea:a4:64:7b:b9:7a	Broadcast	802.11	167	Probe Request, SN=2540, FN=0, Flags=.....C, SSID=2WIRE-PT-431
2468	70.149098	ea:a4:64:7b:b9:7a	Broadcast	802.11	155	Probe Request, SN=2541, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2469	70.149792	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2332, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2471	70.150537	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2333, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2473	70.151237	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2334, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2475	70.151709	HitronTe_af:b1:99	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2335, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_F
2477	70.152099	HitronTe_af:b1:99	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2336, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_F
2479	70.152570	HitronTe_af:b1:99	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2337, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_F
2603	72.179215	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2563, FN=0, Flags=.....C, SSID=FlyingNet
2606	72.179924	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2346, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2608	72.180590	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2347, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2610	72.181275	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2348, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2616	72.201570	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2565, FN=0, Flags=.....C, SSID=FlyingNet
2617	72.202150	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2350, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2619	72.202807	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2351, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2621	72.203485	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2352, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2650	72.488998	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2585, FN=0, Flags=.....C, SSID=FlyingNet
2653	72.502553	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2586, FN=0, Flags=.....C, SSID=FlyingNet
2677	72.568343	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2589, FN=0, Flags=.....C, SSID=FlyingNet
2678	72.578258	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2590, FN=0, Flags=.....C, SSID=FlyingNet
4455	82.621343	7c:ea:6d:ff:a2:cc	Broadcast	802.11	71	Probe Request, SN=62, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
4493	82.726818	7c:ea:6d:ff:a2:cc	Broadcast	802.11	71	Probe Request, SN=64, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)

Frame 1300: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits) on 0

Radiotap Header v0, Length 25

802.11 radio information

IEEE 802.11 Probe Request, Flags:C

Figure 13: Filtro estabelecido e respetivo resultado visual

11. Identifique um *probing request* para o qual tenha havido um *probing response*. Face ao endereçamento usado, indique a que sistemas são endereçadas estas tramas e explique qual o propósito das mesmas?

Tal como podemos ver na Figura 14 existe um *probing request* na trama de dados nº 2603 e a respetiva *probing response* na trama de dados nº 2610 .

A trama correspondente ao *probing request* é emitida pela STA Apple_10:6a:f5 que a emite para procurar um AP, sendo emitida assim para todos os equipamentos da rede. A resposta a este pedido, vem a *probing response* do AP HitronTe_af:b1:98 para a STA.

Um *probing request* trata-se de um pedido vindo do STA Apple_10:6a:f5 para saber informações de algum AP na área. Depois de ser enviado o pedido, o AP devolve uma *probing response* para informar o STA que ele está disponível e devolve informação para as duas estações poderem comunicar.

2603	72.179215	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2563, FN=0, Flags=.....C, SSID=FlyingNet
2606	72.179924	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2346, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2608	72.180590	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2347, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2610	72.181275	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2348, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2616	72.201570	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2565, FN=0, Flags=.....C, SSID=FlyingNet

Figure 14: Probing Request e respetivo Probing Response

Processo de Associação

Numa rede WiFi estruturada um *host* deve associar-se a um ponto de acesso antes de enviar dados. O processo de associação de redes IEEE 802.11 é executada enviando trama *association request* do host para o AP e a trama *association response* enviado pelo AP para o *host*, em resposta ao pedido de associação recebido. Este processo é antecedido por uma fase de autenticação.

Para a sequência de tramas capturada:

12. Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.

A figura abaixo mostra uma sequência de tramas responsáveis pelo processo de associação entre o STA: Apple_10:6a:f5 e o AP: HitronTe_af:b1:98.

2486	70.361782	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	70	Authentication, SN=2542, FN=0, Flags=.....C
2487	70.362050		Apple_10:6a:f5 (64...	802.11	39	Acknowledgement, Flags=.....C
2488	70.381869	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59	Authentication, SN=2338, FN=0, Flags=.....C
2489	70.381878		HitronTe_af:b1:98 ...	802.11	39	Acknowledgement, Flags=.....C
2490	70.383512	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	175	Association Request, SN=2543, FN=0, Flags=.....C, SSID=FlyingNet
2491	70.383873		Apple_10:6a:f5 (64...	802.11	39	Acknowledgement, Flags=.....C
2492	70.389339	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	225	Association Response, SN=2339, FN=0, Flags=.....C
2493	70.389352		HitronTe_af:b1:98 ...	802.11	39	Acknowledgement, Flags=.....C

Figure 15: Sequência de Tramas no processo de associação

13. Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo.

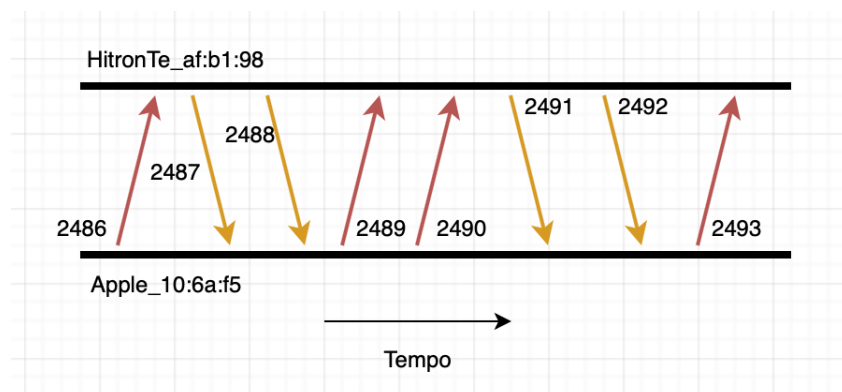


Figure 16: Diagrama da sequência de tramas trocadas.

Transferência de Dados

O *trace* disponibilizado, para além de tramas de gestão da ligação de dados, inclui tramas de dados e controlo da transferência desses mesmos dados.

14. Considere a trama de dados nº455. Sabendo que o campo *Frame Control* contido no cabeçalho das tramas 802.11 permite especificar a direcionalidade das tramas, o que pode concluir face à direcionalidade dessa trama, será local à WLAN?

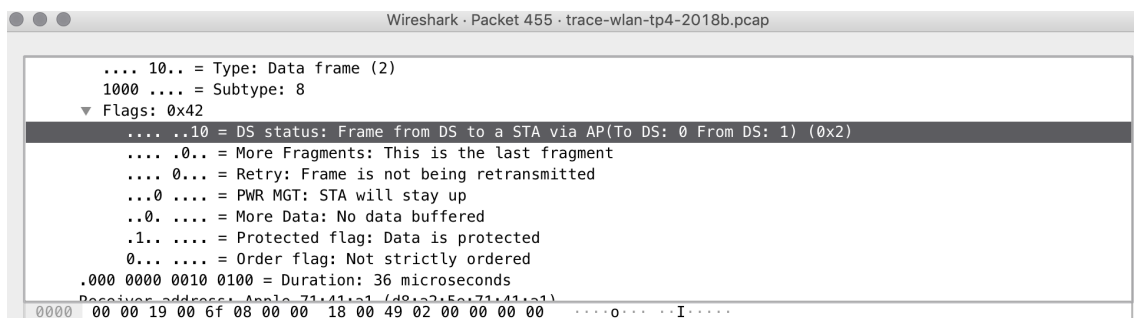


Figure 17: Valores flags DS

A flag do From DS tem o valor 1 e a flag To DS o valor 0 o que significa que a trama recebida está a vir do sistema de distribuição logo não será local à WLAN.

15. Para a trama de dados nº455, transcreva os endereços MAC em uso, identificando qual o endereço MAC correspondente ao *host* sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição?

O STA tem o endereço mac Apple_71:41:a1, o AP HitronTe_af:b1:98 e o router de acesso ao sistema tem o endereço mac HitronTe_af:b1:98.

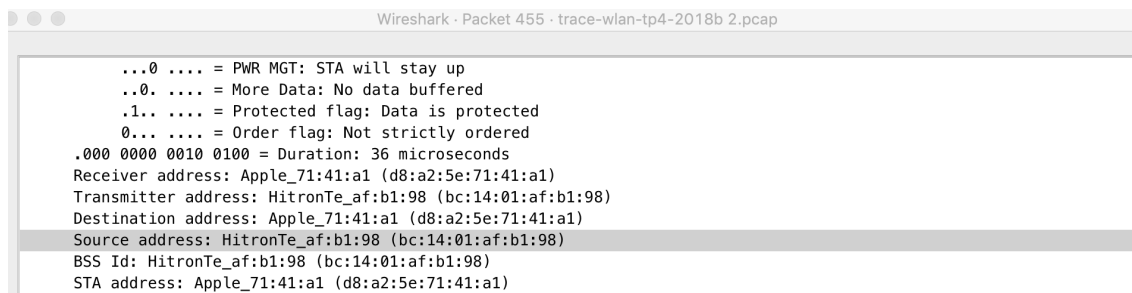


Figure 18: Endereços MAC da trama de dados 455

16. Como interpreta a trama n^o457 face à sua direcionalidade e endereçamento MAC?

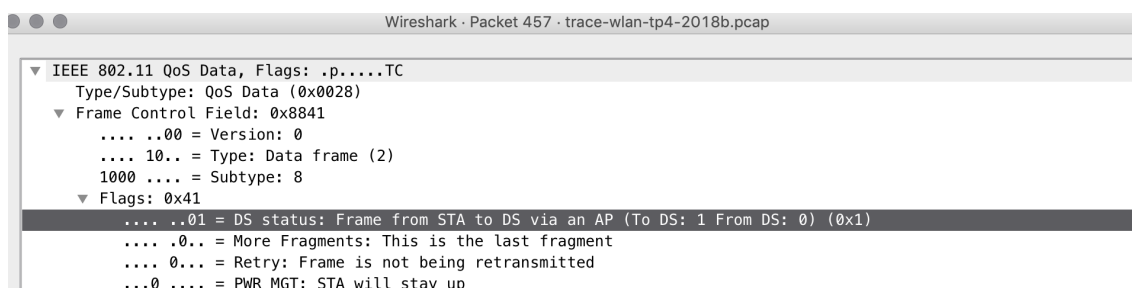


Figure 19: Flags da trama de dados 457

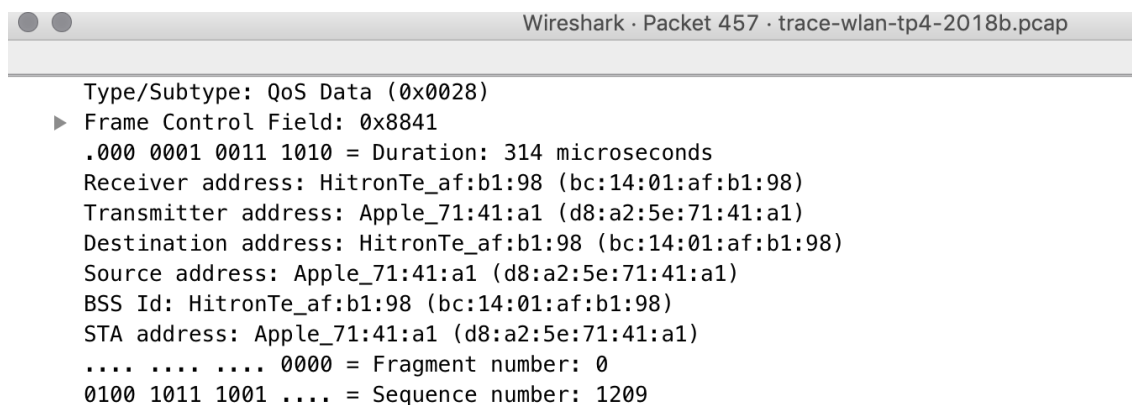


Figure 20: Mac Adresses da trama de dados 457

A trama 457 tem a flag To Ds a 1 e a flag From Ds a 0. Estes valores significam que a trama está a ser transmitida para fora da rede local. Os endereços são iguais todavia, estão em posições diferentes da trama. O endereço da STA fica no address 2, o AP no address 1 e o route no address 3.

17. Que subtipo de tramas de controlo são transmitidas ao longo da transferência de dados acima mencionada? Tente explicar porque razão têm de existir (contrariamente ao que acontece numa rede Ethernet).

455	18.536644	HitronTe_af:b1:98	Apple_71:41:a1	802.11	226	QoS Data, SN=276, FN=0, Flags=p....F.C
456	18.536653	HitronTe_af:b1:98	HitronTe_af:b1:98	802.11	39	Acknowledgement, Flags=.....C
457	18.539762	Apple_71:41:a1	HitronTe_af:b1:98	802.11	178	QoS Data, SN=1209, FN=0, Flags=p.....TC
458	18.540043	HitronTe_af:b1:98	Apple_71:41:a1	802.11	39	Acknowledgement, Flags=.....C

Figure 21: Pacotes de QoS

A figura 21 mostra o envio de duas tramas QoS. Como podemos ver, entre as duas tramas transmitidas temos uma terceira trama no meio que é de Acknowledgement. As redes wi-fi são propícias a ter colisões visto que, os dispositivos podem transferir informação quando quiserem. O envio desta trama de controlo após a transferência de dados permite saber se o houve ou não erro na envio da primeira trama. Assim, sempre que há um erro, o dispositivo consegue saber pela resposta da trama acknowledgment se deve ou não reenviar o pacote.

18. O uso de tramas *Request To Send* e *Clear To Send*, apesar de opcional, é comum para efetuar "pré-reserva" do acesso ao meio quando se pretende enviar tramas de dados, com o intuito de reduzir o número de colisões resultante maioritariamente de STAs escondidas. Para o exemplo acima, verifique se está a ser usada a opção RTS/CTS na troca de dados entre a STA e o AP/Router da WLAN, identificando a direcionalidade das tramas e os sistemas envolvidos.

162	6.653376	Apple_10:6a:f5 (64...	HitronTe_af:b1:98	802.11	45	Request-to-send, Flags=.....C
163	6.653389	HitronTe_af:b1:98	Apple_10:6a:f5 (64...	802.11	39	Clear-to-send, Flags=.....C

Figure 22: Tramas RTS e CTS

Wireshark - Packet 162 - trace-wlan-tp4-2018b.pcap	
▼ Frame Control Field: 0xb400	
.... 00 = Version: 0	
.... 01.. = Type: Control frame (1)	
1011 = Subtype: 11	
▼ Flags: 0x00	
.... 00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)	
.... 0... = More Fragments: This is the last fragment	

Figure 23: Flags

Os sistemas envolvidos são apenas HitronTe_af:b1:98 e Apple_71:41:a1. Na figura 23 temos presente o valor das flags. Como tanto o To DS e o From DS estão a 0 significa que as redes estão a operar localmente. Neste caso o STA (Apple_71:41:a1) envia um RTS para o AP da WLAN(HitronTe_af:b1:98) e posteriormente o AP envia um CTS para o STA.

Conclusão

Neste trabalho prático realizado foi-nos possível aprofundar o conhecimento acerca de Redes sem fios.

Para realização deste guião usamos a ferramenta Wireshark e uma captura fornecida na plataforma E-Learning.

Com a ferramenta foi-nos possível analisar algum do processo de conexões entre STA e AP's assim como os comportamentos destes, como por exemplo o envio de Beacons, probing requests, probing responses, e ainda Request To Send e Clear To Send.

Pudemos também analisar melhor as tramas de dados dos vários pacotes e poder recolher informação importante no funcionamento e gestão de toda a rede.

Desta forma pudemos consolidar conceitos, protocolos e comportamento dos dados transmitidos via redes sem fios.