

Redes de Computadores

Trabalho Prático N°4

Redes Sem Fios (802.11)

Alexandra Candeias, Pedro Araújo, and Tiago Ribeiro

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a89521,a70699,a76420}@alunos.uminho.pt

1 Introdução

A elaboração do presente relatório tem o intuito de responder às questões colocadas ao longo do guião do *Trabalho Prático 4 (TP4)*, cujo o foco é o estudo do protocolo *IEEE 802.11*, também conhecido como *Wi-Fi*. As questões realizadas têm como objectivo primordial a consolidação de conhecimentos sobre o formato que as tramas apresentam no protocolo, assim como o endereçamento envolvido na comunicação sem fios, os tipos de tramas mais comuns e finalmente como opera o protocolo como um todo. Assim sendo, na secção 2 são expostas as questões presentes no TP4 e apresentadas respostas às mesmas. Na secção 3, são realizadas as devidas conclusões.

2 Questões e Respostas

Esta secção tem o intuito de responder às questões colocadas no guião do TP4.

2.1 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 371, foram obtidos os seguintes resultados para as questões colocadas.

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

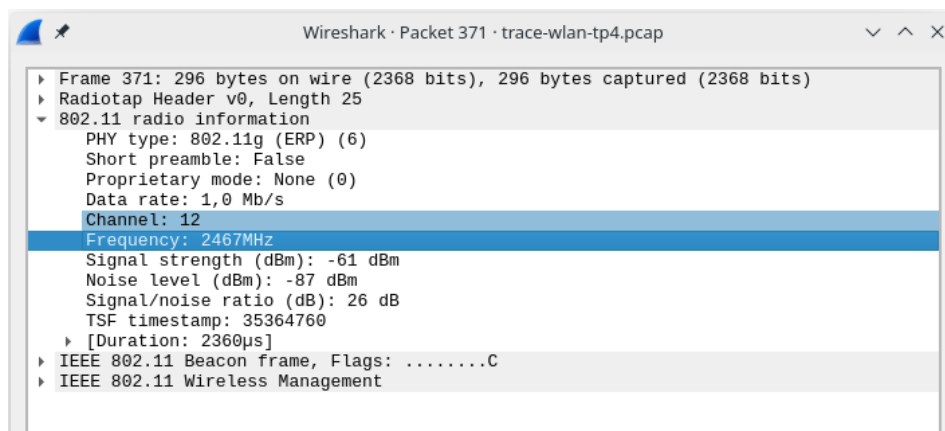


Fig. 1. Frequência e Canal

R: Como é observável na Figura 1, a rede sem fios está a operar na frequência 2467 MHz e esta corresponde ao Canal 12.

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

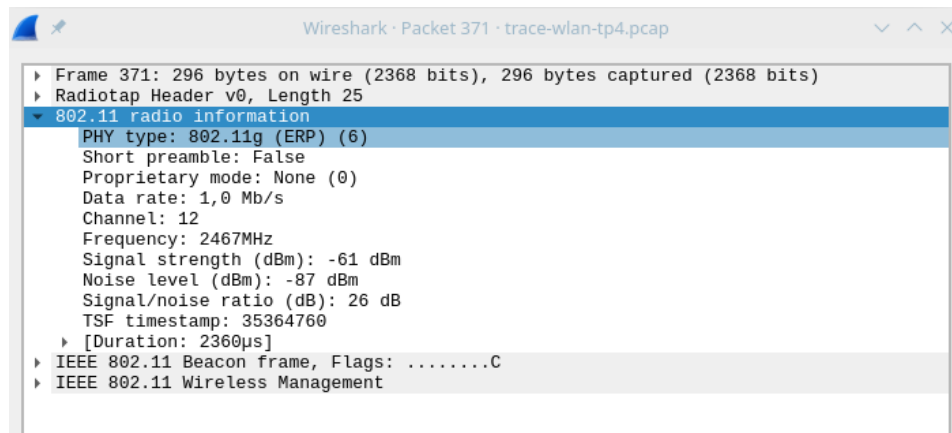


Fig. 2. Versão do protocolo *IEEE 802.11*

R: Recorrendo à Figura 2, a versão que está a ser usada do protocolo em questão corresponde à 802.11g.

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.

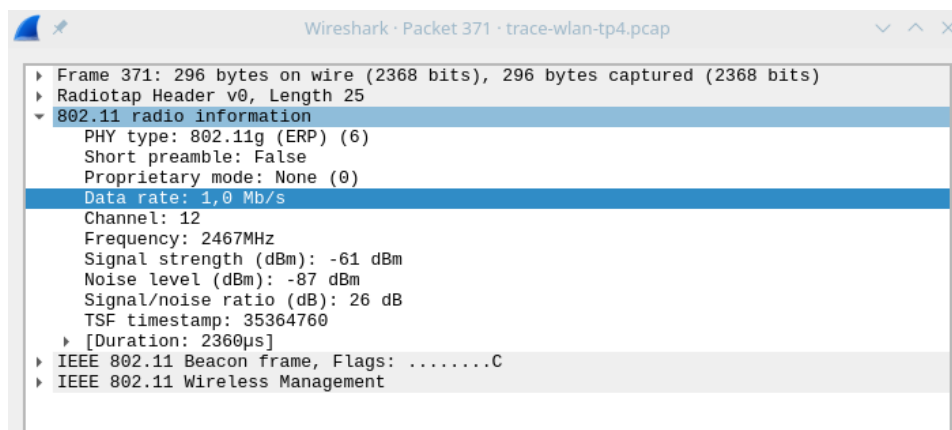


Fig. 3. Débito da trama 371

R: Como se encontra acima representado pela Figura 3, o débito é igual a 1.0 Mb/s. Este débito não corresponde ao débito máximo a que a interface *Wi-Fi* pode operar pois como se trata de uma trama pequena este débito por sua vez também irá ser pequeno. No caso de se transmitir tramas maiores, como é o exemplo das tramas de dados, este débito irá ser maior. O débito máximo atingido pela versão 802.11g é de 58Mbps.

2.2 Scanning Passivo e Scanning Ativo

As tramas beacon permitem efetuar scanning passivo em redes IEEE 802.11 (WiFi). Para responder às seguintes questões foi usada a trama 1071.

4. Selecione uma trama beacon (e.g., trama 10XX). 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)?

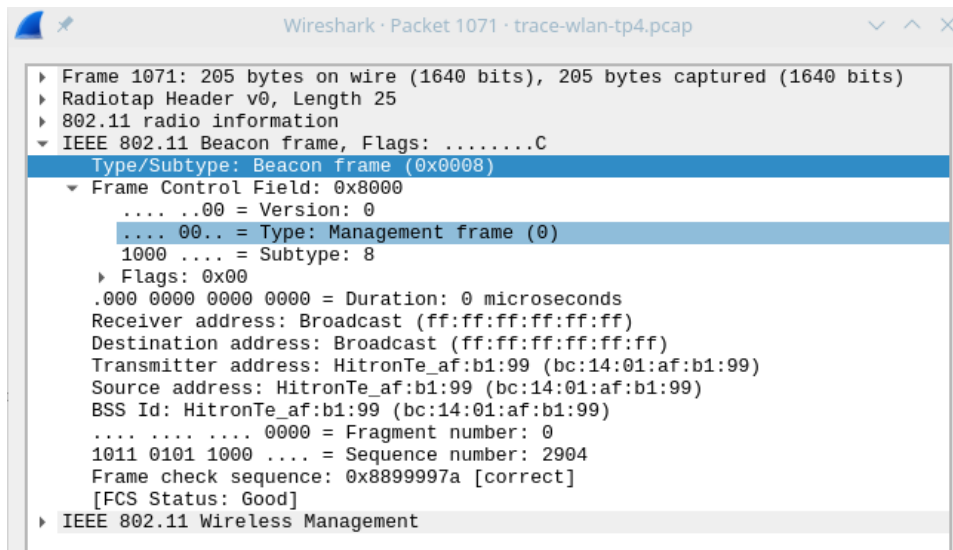


Fig. 4. Beacon

R: Como observável na Figura 4, esta trama é do tipo *Management Frame* sendo a mesma uma Trama de Anúncio, *Beacon*. O valor do identificador do tipo é 0, já o de subtipo é 8. (Visto na imagem acima). Esta parte encontra-se especificada no campo *Frame Control* da trama.

5. Para a trama acima, identifique todos os endereços MAC em uso. Que conclui quanto à sua origem e destino?

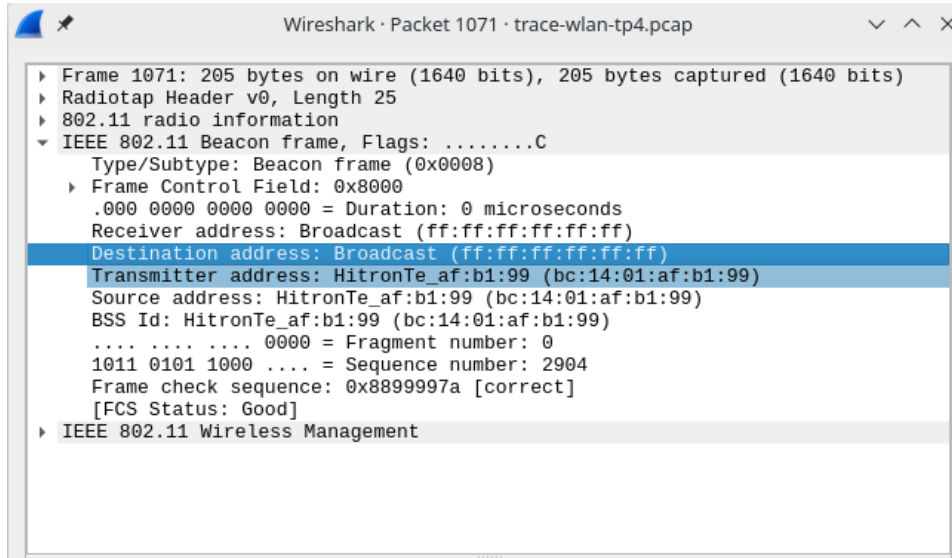


Fig. 5. Endereços MAC da trama 1071

R: Como é possível visualizar na Figura 5, os endereços MAC são:

Endereço Máquina: *bc:14:01:af:b1:99*, sendo este o endereço de origem;

Broadcast: *ff:ff:ff:ff:ff:ff*, sendo este por sua vez o endereço destino.

Conclui-se que sendo esta trama um *Beacon*, esta é enviada com o endereço destino em Broadcast e, claro, o endereço origem.

6. Uma trama beacon anuncia que o AP pode suportar vários débitos de base, assim como vários débitos adicionais (extended supported rates). Indique quais são esses débitos?

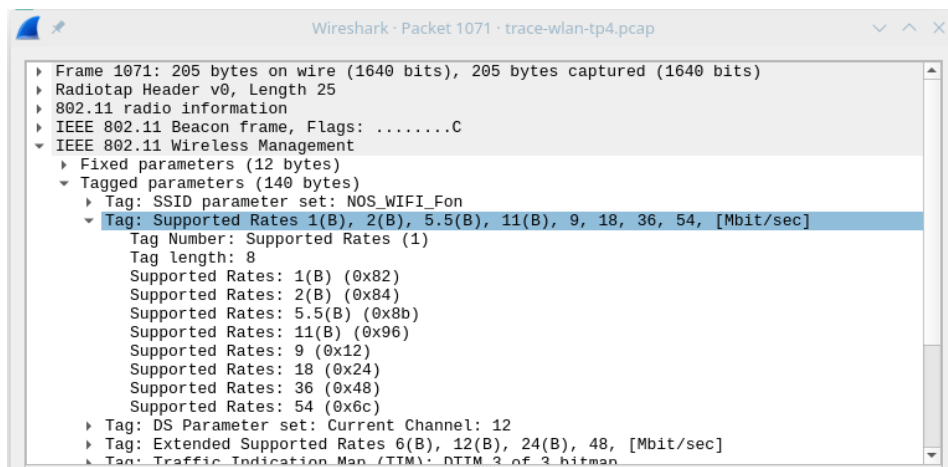


Fig. 6.

R: Como se verifica na Figura 6, os débitos de base são: *1(B), 2(B), 5.5(B), 11(B), 9, 18, 36 e 54 [Mbit/sec]*. Sendo o (B) as Basic Rates, isto é, débitos de versões mais antigas e os débitos adicionais serão: *6(B), 12(B), 24(B) e 48 Mbit/sec*.

7. Qual 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 provenientes do mesmo AP é verificada? Tente explicar porquê.

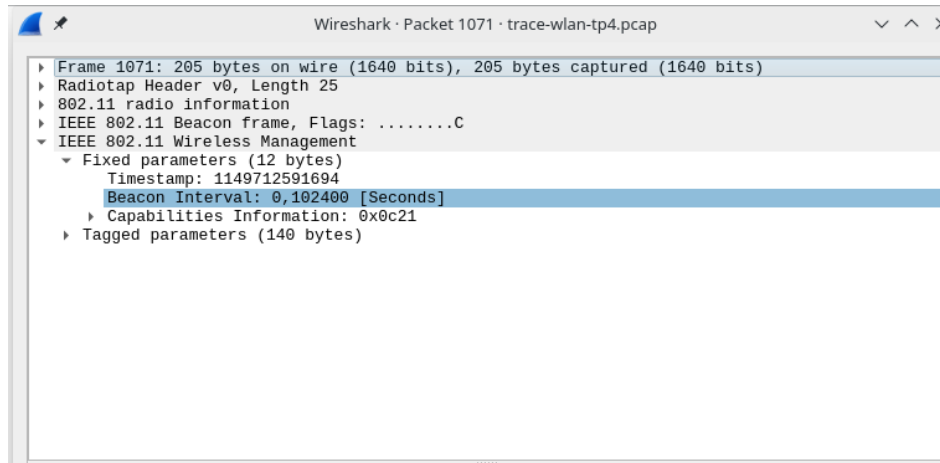


Fig. 7. Intervalo de tempo entre tramas *Beacon*

R: Como é visível na Figura 7, o intervalo previsto entre as tramas *Beacon* é de 0.102400 segundos. Na prática, a periodicidade de tramas *Beacon* não é exactamente igual ao valor teórico uma vez que podem surgir diversos problemas e/ou interferências na transmissão das tramas, em consequência estas podem demorar mais ou menos tempo a chegar.

8. Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura? Explícite o modo como obteve essa informação (por exemplo, se usou algum filtro para o efeito).

wlan.ssid						
No.	Time	Source	Destination	Protocol	Length	Info
1059	41.371522	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2892, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1060	41.472290	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2893, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1061	41.473937	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2894, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1062	41.574567	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2895, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1063	41.576212	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2896, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1064	41.676997	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2897, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1065	41.678627	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2898, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1066	41.779491	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2899, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1067	41.781141	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2900, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1068	41.881896	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2901, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1069	41.883475	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2902, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1070	41.984295	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2903, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1071	41.985944	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2904, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1072	42.086575	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2905, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1073	42.088191	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2906, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1074	42.188945	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2907, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1075	42.190570	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2908, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1076	42.291363	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2909, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1077	42.292964	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2910, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1078	42.393745	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2911, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1079	42.395374	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2912, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1080	42.496118	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2913, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1081	42.497712	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2914, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1082	42.598489	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2915, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1083	42.600114	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2916, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1084	42.709978	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2917, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1085	42.702599	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2918, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1086	42.803447	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2919, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1087	42.805076	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2920, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1088	42.905709	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2921, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1089	42.907340	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2922, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1090	43.008297	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2923, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1091	43.009902	HitronTe_af:b1:98	Broadcast	802.11	205	Beacon frame, SN=2924, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

Fig. 8. SSID identificados

R: Os *SSID* dos APs que estão a operar na vizinhança são o *NOS_WIFI_Fon* e o *FlyingNet*, como é possível visualizar na Figura 8. Podemos verificar isto analisando o tráfego das tramas, concluindo assim que está ser enviadas tramas *Beacon* para estes dois APs.

9. Verifique se está a ser usado o método de detecção de erros (CRC). Justifique. Que conclui? Justifique o porquê de usar detecção de erros em redes sem fios. No trace disponibilizado foi também registado scanning ativo (envolvendo tramas probe request e probe response), comum nas redes Wi-Fi como alternativa ao scanning passivo.

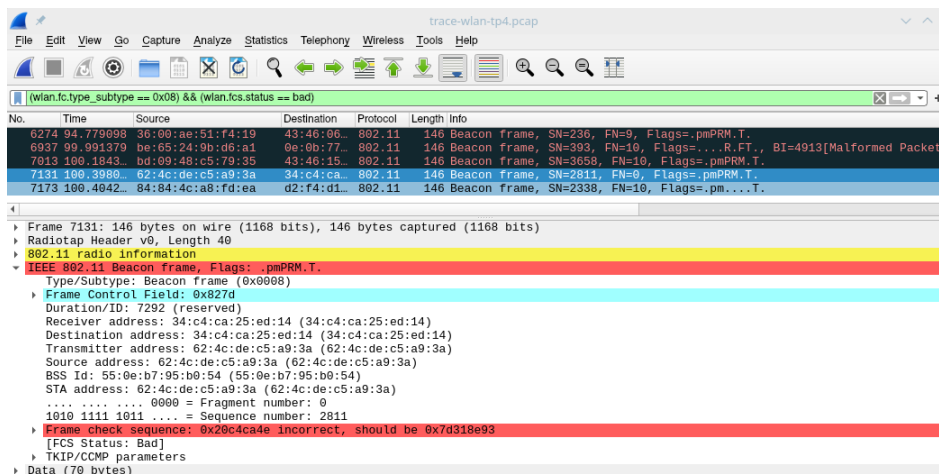


Fig. 9. Erros detectados nas tramas

R: No enunciado é sugerido que se faça uso do filtro (*wlan.fc.type_subtype == 0x08*)&&(wlan.fcs.status == bad), como representado na Figura 9. Conclui-se assim que foram detectadas algumas tramas com erros.

O uso de detecção em redes sem fios deve-se ao facto de estas ser muito susceptíveis a erros, devido à liberdade que os diversos dispositivos têm em transmitir informação, para além disso existem vários parâmetros a medir, como por exemplo, a distância da máquina ao AP, quantos utilizadores existem em volta deste do mesmo, entre outros. Face a estas questões é então necessário recorrer ao uso de FCS de modo a identificar os eventuais problemas que possam vir a existir.

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

No.	Time	Source	Destination	Protocol	Length	Info
1389	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:d9:7a	Broadcast	802.11	167	Probe Request, SN=2540, FN=0, Flags=.....C, SSID=DWIRE-PT-431
2468	70.149099	ea:a4:64:7b:d9:7a	Broadcast	802.11	155	Probe Request, SN=2541, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2469	70.149702	HitronTe_af:b1:98	ea:a4:64:7b:d9:7a	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:d9:7a	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:d9:7a	802.11	411	Probe Response, SN=2334, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2475	70.151709	HitronTe_af:b1:98	ea:a4:64:7b:d9:7a	802.11	201	Probe Response, SN=2335, FN=0, Flags=.....C, BI=100, SSID=N05_WIFI_Fon
2477	70.152099	HitronTe_af:b1:98	ea:a4:64:7b:d9:7a	802.11	201	Probe Response, SN=2336, FN=0, Flags=.....C, BI=100, SSID=N05_WIFI_Fon
2479	70.152570	HitronTe_af:b1:98	ea:a4:64:7b:d9:7a	802.11	201	Probe Response, SN=2337, FN=0, Flags=.....C, BI=100, SSID=N05_WIFI_Fon
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	72.570208	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	82.726816	7c:ea:6d:ff:a2:cc	Broadcast	802.11	71	Probe Request, SN=64, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
4494	82.728646	7c:ea:6d:ff:a2:cc	Broadcast	802.11	210	Probe Request, SN=65, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
6193	94.190880	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=.....C, SSID=FlyingNet
6194	94.192095	HitronTe_af:b1:98	Apple_28:b8:0c	802.11	411	Probe Response, SN=2474, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
6195	94.192751	HitronTe_af:b1:98	Apple_28:b8:0c	802.11	411	Probe Response, SN=2475, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Fig. 10. Filtro de identificação de *Probing Request* ou *Probing Responses*

R: Como é visível na Figura 10, o filtro usado na identificação de *Probing Request* ou *Probing Responses* foi o `wlan.fc.type_subtype == 4 or wlan.fc.type_subtype == 5`.

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?

No.	Time	Source	Destination	Protocol	Length	Info
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

Fig. 11. *Probe Request* e respectiva *Probe Responses*

R: Pela Figura 11 é possível de observar que foi efectuado um *Probe Request* na trama n° 2616 e que o respectivo *Probe Response* se encontra na trama n°2621.

É possível de observar que o *Probing Request* é emitido pelo STA `Apple_10:6a:f5`, sendo transmitida para todos os equipamentos da rede; por sua vez a *Probing Response* é dada pelo AP `HitronTe_af:b1:98`.

O propósito deste mecanismo tem o intuito de permitir ao STA determinar quais os APs que estão dentro do seu alcance rádio - *active scanning* - e aquando de uma resposta, este saber com qual AP pode comunicar.

2.3 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 nas redes IEEE 802.11 é executada enviando a

trama association request do host para o AP e a trama association response enviada pelo AP para o host, em resposta ao pedido de associação recebido. Este processo é antecedido por uma fase de autenticação.

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

wlan.fc.type_subtype == 0x0 wlan.fc.type_subtype == 0x1 wlan.fc.type_subtype == 0xb wlan.fc.type_subtype == 0xa wlan.fc.type_subtype == 0xc						
No.	Time	Source	Destination	Protocol	Length	Info
2376	66.349591	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	55	Disassociate, SN=2536, FN=0, Flags=.....C
2380	66.350483	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	55	Deauthentication, SN=2537, FN=0, Flags=.....C
2384	66.351544	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	55	Deauthentication, SN=2538, FN=0, Flags=.....C
2387	66.352413	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	55	Deauthentication, SN=2538, FN=0, Flags=....R...C
2389	66.353393	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	55	Deauthentication, SN=2539, FN=0, Flags=.....C
2486	70.361782	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	70	Authentication, SN=2542, FN=0, Flags=.....C
2488	70.381869	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59	Authentication, SN=2338, FN=0, 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
2492	70.389339	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	225	Association Response, SN=2339, FN=0, Flags=.....C
4660	83.505612	7c:ea:6d:ff:a2:cc	HitronTe_af:b1:98	802.11	55	Deauthentication, SN=66, FN=0, Flags=.....C
4692	83.663250	7c:ea:6d:ff:a2:cc	HitronTe_af:b1:98	802.11	59	Authentication, SN=67, FN=0, Flags=.....C
4694	83.663681	HitronTe_af:b1:98	7c:ea:6d:ff:a2:cc	802.11	59	Authentication, SN=2439, FN=0, Flags=.....C
4696	83.665976	7c:ea:6d:ff:a2:cc	HitronTe_af:b1:98	802.11	153	Association Request, SN=68, FN=0, Flags=.....C, SSID=FlyingNet
4698	83.678873	HitronTe_af:b1:98	7c:ea:6d:ff:a2:cc	802.11	225	Association Response, SN=2440, FN=0, Flags=.....C
4699	83.680045	HitronTe_af:b1:98	7c:ea:6d:ff:a2:cc	802.11	225	Association Response, SN=2440, FN=0, Flags=....R...C

Fig. 12. Associação Completa

R: Na Figura 12, é observável que da trama n° 2486 à trama n° 2492 existe uma sequência completa de associação incluindo a fase de autenticação.

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

R:

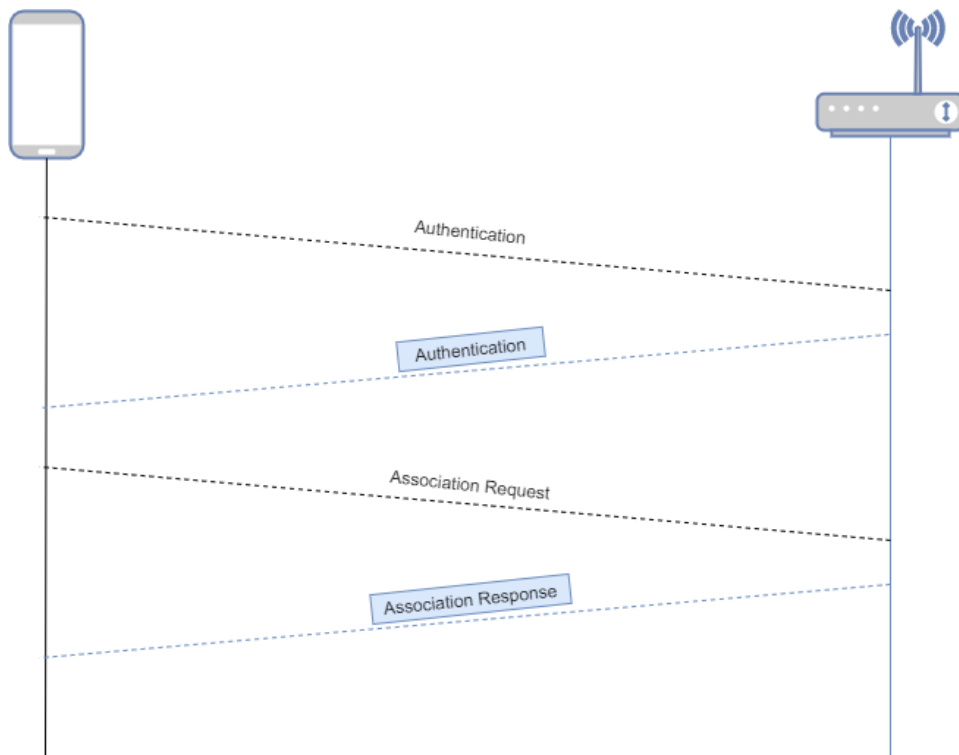


Fig. 13. Diagrama

2.4 Transferência de Dados

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

14. Considere a trama de dados no 455. Sabendo que o campo Frame Control contido no cabeçalho das tramas 802.11 permite especificar a direccionalidade das tramas, o que pode concluir face à direccionalidade dessa trama, será local à WLAN?

No.	Time	Source	Destination	Protocol	Length	Info
453	18.536461	HitronTe_af:b1:98	(.. Apple_71:41:a1	802.11	49	802.11 Block Ack Req, Flags=.....C
454	18.536469	Apple_71:41:a1	(d8:.. HitronTe_af:b1	802.11	57	802.11 Block Ack, Flags=.....C
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	802.11	39	Acknowledgement, Flags=.....C
457	18.539762	Apple_71:41:a1	HitronTe_af:b1	802.11	178	QoS Data, SN=1209, FN=0, Flags=.p.....TC

▶	Frame 455: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)
▶	Radiotap Header v0, Length 25
▶	802.11 radio information
▼	IEEE 802.11 QoS Data, Flags: .p....F.C
	Type/Subtype: QoS Data (0x0028)
▼	Frame Control Field: 0x8842
00 = Version: 0
 10.. = Type: Data frame (2)
	1000 = Subtype: 8
▶	Flags: 0x42
	.000 0000 0010 0100 = Duration: 36 microseconds
	Receiver address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
	Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
	Destination address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
	Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
	BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
	STA address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
 0000 = Fragment number: 0
	0001 0001 0100 = Sequence number: 276
	Frame check sequence: 0xca46bf48 [correct]
	[FCS Status: Good]
▶	Qos Control: 0x0000
▶	CCMP parameters
▶	Data (163 bytes)

Fig. 14. Trama de dados nº 455

R: A trama tem como receptor da trama o STA local - *Apple_71:41:a1* -, o transmissor é o AP - *HiTronTe_af:b1:98*-, o destino é de novo o STA local e a fonte é o AP. Por isso poderá se afirmar que esta trama é local à WLAN.

15. Para a trama de dados no 455, 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?

R: Pela Figura 14 poderá se observar que o endereço MAC do host sem fios (STA) - *Apple_71:41:a1* - é *d8:a2:53:71:41:a1* e do AP - *HiTronTe_af:b1:98* - é *bc:14:01:af:b1:98*. Este último será também o router de acesso ao sistema de distribuição.

16. Como interpreta a trama no 457 face à sua direccionalidade e endereçamento MAC?

No.	Time	Source	Destination	Protocol	Length	Info
454	18.536460	Apple_71:41:a1 (d8:..	HitronTe_af:b1:98 (-	802.11	57	802.11 Block Ack, Flags=.....C
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 (-	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	Apple_71:41:a1 (d8:..	802.11	39	Acknowledgement, Flags=.....C	
459	18.636990	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2447, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
460	18.638620	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2448, FN=0, Flags=.....C, BI=100, SSID=N05_MIFI_Fon
461	18.739398	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2449, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
462	18.741029	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2450, FN=0, Flags=.....C, BI=100, SSID=N05_MIFI_Fon
463	18.780906	Apple_71:41:a1	HitronTe_af:b1:98	802.11	68	Null function (No data), SN=1751, FN=0, Flags=...P...TC

> Frame 457: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits)

> Radiotap Header v0, Length 25

> 802.11 radio information

IEEE 802.11 QoS Data, Flags: .p.....TC

Type/Subtype: QoS Data (0x0028)

> Frame Control Field: 0x8841

.000 0001 0011 1010 = Duration: 314 microseconds

Receiver address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)

Transmitter address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)

Destination address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)

Source address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)

BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)

STA address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)

.... 0000 = Fragment number: 0

0100 1011 1001 = Sequence number: 1209

Frame check sequence: 0x88cbfe48 [correct]

[FCS Status: Good]

> QoS Control: 0x0000

> CCMP parameters

> Data (115 bytes)

0010 14 02 a3 09 80 04 bd a9 00 88 41 3a 01 bc 14 01--A:--..

0020 af b1 98 d8 a2 5e 71 41 a1 bc 14 01 af b1 98 90

0030 4b 00 00 bc 24 00 20 02 00 00 00 f7 94 63 84 51 K...\$.....c Q

Receiving Station Hardware Address (vlan.ra), 6 bytes

Packets: 17536 · Displayed: 17536 (100.0%)

Fig. 15. Endereços MAC da trama nº 457

R: Analisando os endereços MAC presentes na Figura 15, é possível concluir que a trama é local à WLAN uma vez que esta tem como destino, e receptor, o AP, e como transmissor e fonte, o STA. Isto é, as tramas são internas à BSS - modo *adhoc*.

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.)

R: O subtipo das tramas de controlo é QoS Data. É necessário existir numa rede 802.11 devido ao facto de não ser possível dois STAs transmitir ao mesmo tempo, é necessário estabelecer uma prioridade entre os STAs que estejam a transmitir tramas cujo a informação é de serviços em tempo real, isto é, chat de voz/vídeo, jogos multi-jogador online, entre outros.

18. O uso de tramas Request To Send e Clear To Send, apesar de opcional, é comum para efectuar "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 direccionalidade das tramas e os sistemas envolvidos.

No.	Time	Source	Destination	Protocol	Length	Info
1365	56.422688	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=3185, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1366	56.424317	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=3186, FN=0, Flags=.....C, BI=100, SSID=WDS_WIFI_Fon
1367	56.525992	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=3187, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1368	56.526803	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=3188, FN=0, Flags=.....C, BI=100, SSID=WDS_WIFI_Fon
1369	56.627522	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=3189, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1370	56.629019	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=3190, FN=0, Flags=.....C, BI=100, SSID=WDS_WIFI_Fon
1371	56.660959	Apple_10:6a:f5 (64:..	HitronTe_af:b1:98 (..	802.11	45	Request-to-send, Flags=.....C
1372	56.660973	Apple_10:6a:f5 (64:..	Apple_10:6a:f5 (64:..	802.11	39	Clear-to-send, Flags=.....C
1373	56.660979	Apple_10:6a:f5	IPv4mcast_fb	802.11	335	QoS Data, SN=3687, FN=0, Flags=.p....TC
1374	56.661014	HitronTe_af:b1:98 (-	Apple_10:6a:f5 (64:..	802.11	57	802.11 Block Ack, Flags=.....C
1375	56.661104	HitronTe_af:b1:98 (-	Apple_10:6a:f5 (64:..	802.11	49	802.11 Block Ack Req, Flags=.....C
1376	56.661207	Apple_10:6a:f5 (64:..	HitronTe_af:b1:98 (-	802.11	57	802.11 Block Ack, Flags=.....C
1377	56.661305	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	53	Null function (No data), SN=2520, FN=0, Flags=.....TC
1378	56.661362	Apple_10:6a:f5 (64:..	Apple_10:6a:f5 (64:..	802.11	39	Acknowledgement, Flags=.....C
1379	56.661544	HitronTe_af:b1:98 (-	Apple_10:6a:f5 (64:..	802.11	49	802.11 Block Ack Req, Flags=.....C

> Frame 1371: 45 bytes on wire (360 bits), 45 bytes captured (360 bits)	
> Radiotap Header v0, Length 25	
> 802.11 radio information	
IEEE 802.11 Request-to-send, Flags:C	
Type/Subtype: Request-to-send (0x001b)	
Frame Control Field: 0xb400	
.... 00 = Version: 0	
.... 01.. = Type: Control frame (1)	
1011 = Subtype: 11	
Flags: 0x00	
.000 0000 1011 0010 = Duration: 178 microseconds	
Receiver address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)	
Transmitter address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)	
Frame check sequence: 0x9a56c6e9 [correct]	
[FCS Status: Good]	

0000	00 00 19 00 ef 08 00 00	75 b0 0e 04 00 00 00u.....
0010	12 30 a3 09 00 04 c7 a9	00 00 b2 00 bc 14 01V.....
0020	af b1 98 64 9a be 10 6a	f5 e9 c6 56 9aj.....

Frame subtype (vlan.fc.subtype), 1 byte

Packets: 17536 - Displayed: 17536 (100.0%)

Fig. 16. Tramas *Request To Send* e *Clear To Send*

R: Como podemos observar na Figura 16, estão a ser usadas tramas RTS e CTS. As tramas são intrínsecas à BSS - modo *adhoc* - e os sistemas envolvidos são o STA: 64:91:be:10:6a:f5 e o AP: bc:14:01:af:b1:98.

3 Conclusões

Este trabalho prático permitiu um aprofundamento dos conhecimentos obtidos durante as aulas teóricas sobre Redes Sem Fios. De modo a responder às questões colocadas recorreu-se ao uso da ferramenta *WireShark* e à captura fornecida pela equipa docente. Procedeu-se, deste modo, à análise dos processos de conexão entre STA's e AP's, onde se observou os diferentes comportamentos entre estes. Alguns dos comportamentos analisados foram o envio de *Beacons*; *Probing Requests*, *Probing Responses* assim como *Request To Send* e *Clear To Send*. Foi ainda possível aprofundar os conhecimentos previamente adquiridos nos trabalhos práticos anteriores, no que toca à análise de tramas de dados e informação de vários pacotes. Deste modo, a elaboração deste trabalho prático permitiu a aquisição de conhecimentos no que toca a Redes Sem Fios, enquanto fomentou uma maior compreensão sobre gestão de redes e comportamentos dos diversos protocolos discutidos ao longo deste semestre na Unidade Curricular.