

UNIVERSIDADE DO MINHO
DEPARTAMENTO DE INFORMÁTICA

TP4: Redes sem Fios (802.11)
Grupo N^o 51

Bruno Carvalho (A89476)

João Correia (A84414)

Rúben Cerqueira (A89593)

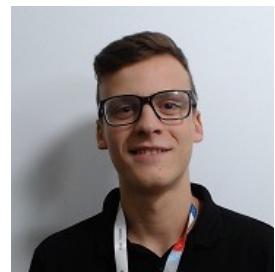
31 de dezembro de 2020



Bruno



João



Rúben

Conteúdo

1	Questões e respostas	3
1.1	4. Acesso Rádio	3
1.1.1	Exercício 1	3
1.1.2	Exercício 2	3
1.1.3	Exercício 3	4
1.2	5. Scanning Passivo e Scanning Ativo	4
1.2.1	Exercício 4	4
1.2.2	Exercício 5	5
1.2.3	Exercício 6	5
1.2.4	Exercício 7	6
1.2.5	Exercício 8	7
1.2.6	Exercício 9	8
1.2.7	Exercício 10	9
1.2.8	Exercício 11	10
1.3	6. Processo de Associação	11
1.3.1	Exercício 12	11
1.3.2	Exercício 13	11
1.4	7. Transferência de Dados	12
1.4.1	Exercício 14	12
1.4.2	Exercício 15	13
1.4.3	Exercício 16	13
1.4.4	Exercício 17	14
1.4.5	Exercício 18	14
2	Conclusão	15

Capítulo 1

Questões e respostas

1.1 4. Acesso Rádio

1.1.1 Exercício 1

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

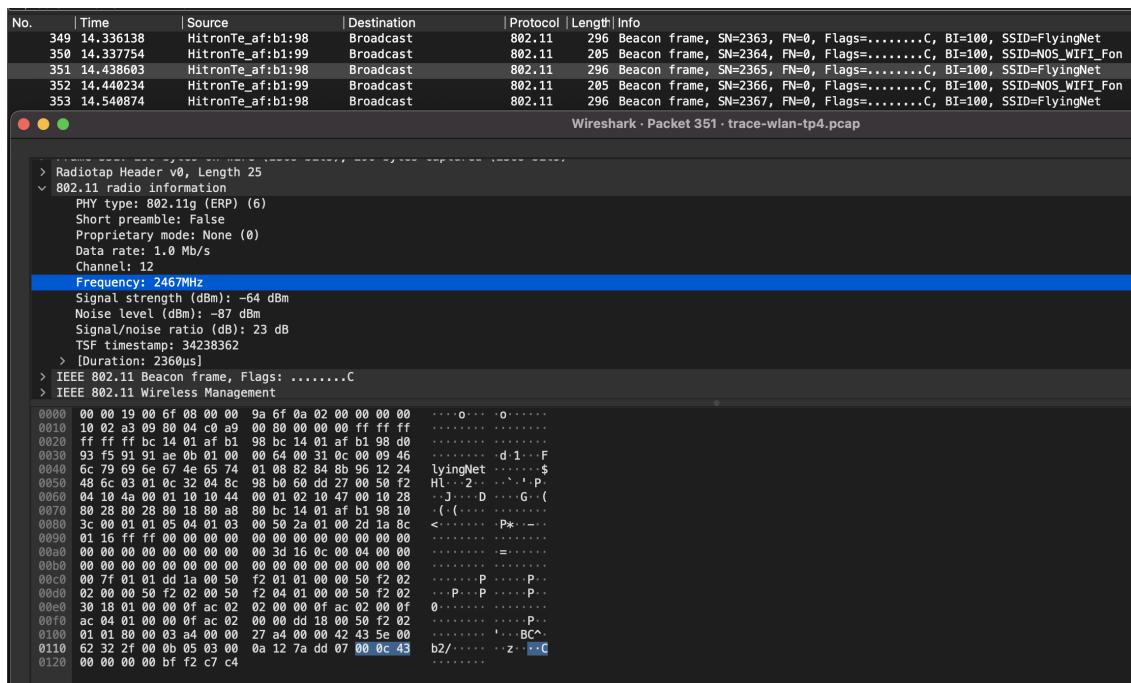


Figura 1.1: trama 351

Como indicado na figura 1.1, a frequência do espetro é 2467MHz.

1.1.2 Exercício 2

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

Verificando, novamente, a figura 1.1, observamos que o campo **PHY type** tem o valor **802.11g**, assumindo ser essa a norma IEEE 802.11g em uso.

1.1.3 Exercício 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.

Observando a figura 1.1, o campo **Data rate** tem o valor **1.0 Mb/s**, sendo esse o débito de envio da trama escolhida.

Este não corresponde ao débito máximo permitido pela norma IEE 802.11g, que tem o valor **54.0 Mb/s**

Tendo uma trama beacon como propósito anunciar a sua presença e transmitir informações tais como a data e hora, é importante garantir que todos os host no range do AP a deteta, razão pela qual se opta por rates o mais baixos possível.

1.2 5. Scanning Passivo e Scanning Ativo

1.2.1 Exercício 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)?

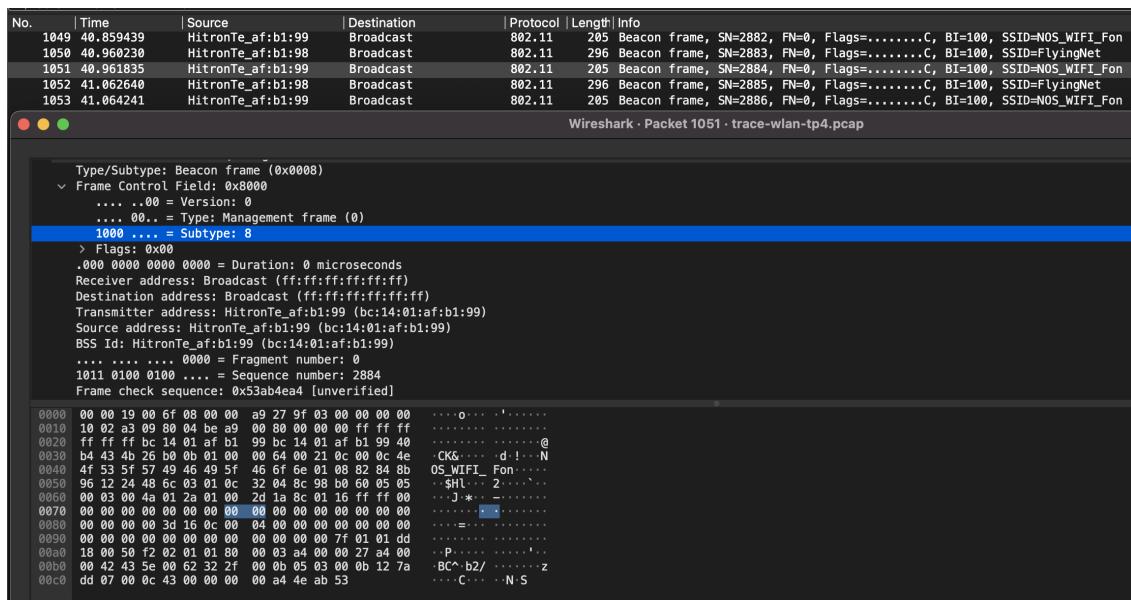


Figura 1.2: Trama 1051

Observando os campos **Type** e **Subtype**, na figura 1.2, estes têm o valor **0** e **8**. Recorrendo à tabela do enunciado, os valores indicados coincidem com a entrada correspondente a uma trama de tipo Management e subtipo Beacon. Esta informação está especificada no campo Frame Control Field, de onde se extraíram os valores relativos ao tipo e subtipo mencionados inicialmente.

00	Management	1000	Beacon
----	------------	------	--------

Figura 1.3: Entrada na tabela

1.2.2 Exercício 5

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

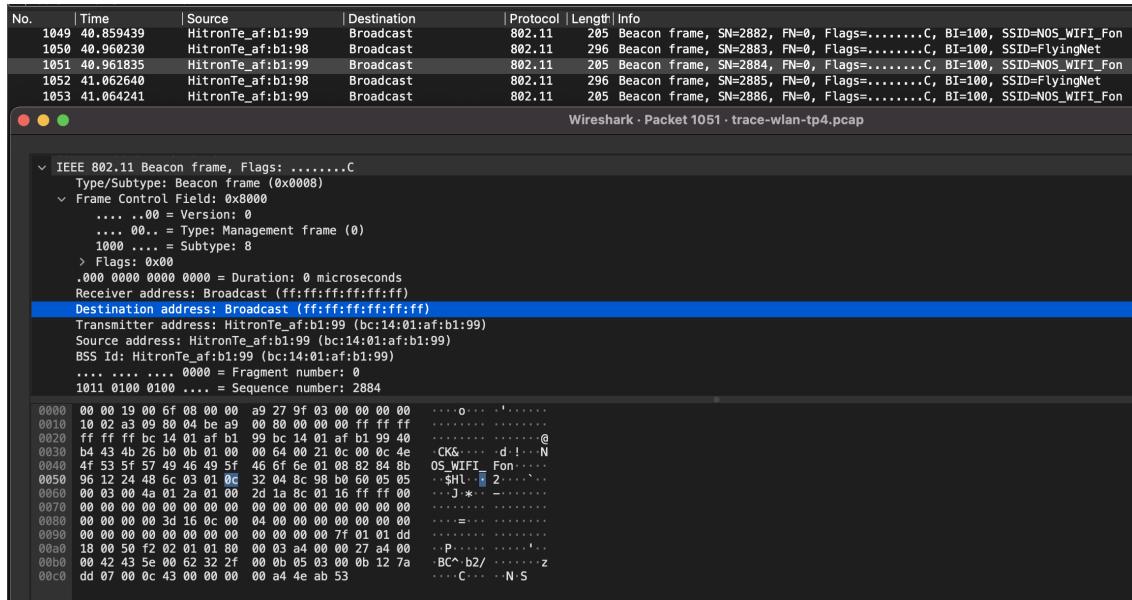


Figura 1.4: Endereços MAC em uso

Como indicado na figura 1.4, os endereços MAC em uso são o **bc:14:01:af:b1:99** e o **ff:ff:ff:ff:ff:ff**. Estes são, respectivamente, os endereços MAC da origem e destino.

Visto o propósito de uma trama do tipo Beacon ser transmitir informações a todos os hosts (STAs), faz sentido que o endereço MAC de destino utilizado seja o indicado, que corresponde ao endereço de *Broadcast*, ou seja, a trama é endereçada a todos os hosts.

1.2.3 Exercício 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?

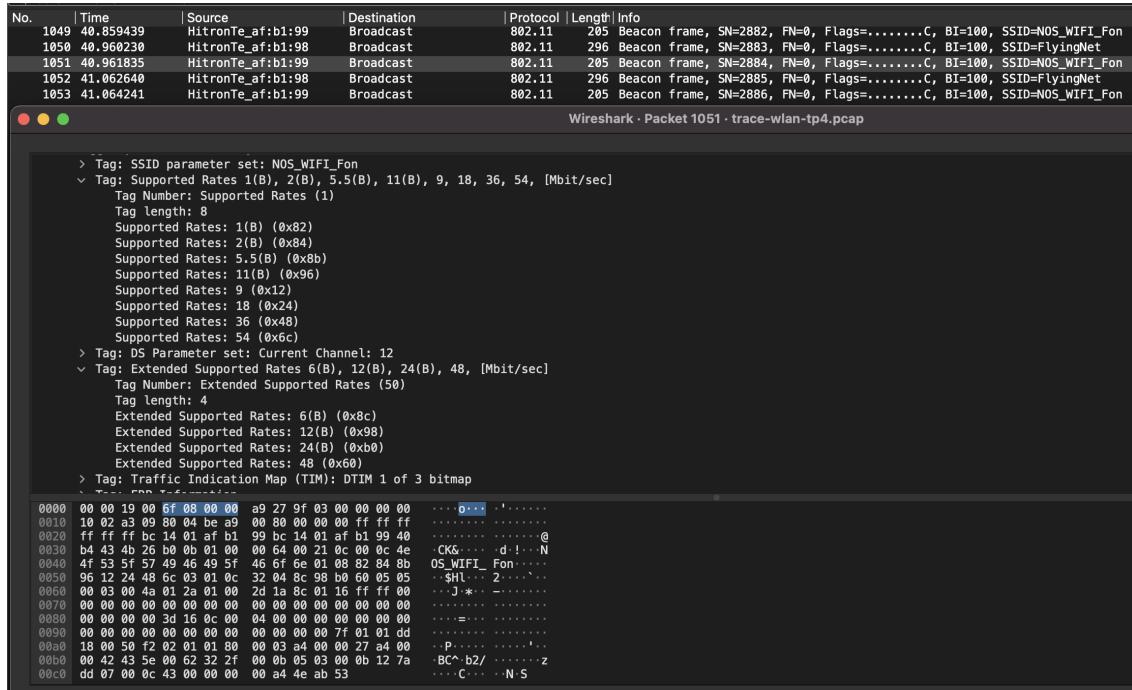


Figura 1.5: Débitos suportados

Como indicado na figura 1.5, os débitos de base suportados são **1,2,5.5,11,9,18,36 e 54 Mbit/sec**. Os débitos adicionais são **6,12,24 e 48 Mbit/sec**.

1.2.4 Exercício 7

Qual o intervalo de tempo previsto entre tramas beacon consecutivas? (nota: este valor é anunciado na própria tramebeacon). Na prática, a periodicidade de tramas beacon provenientes do mesmo AP é verificada? Tente explicar porquê

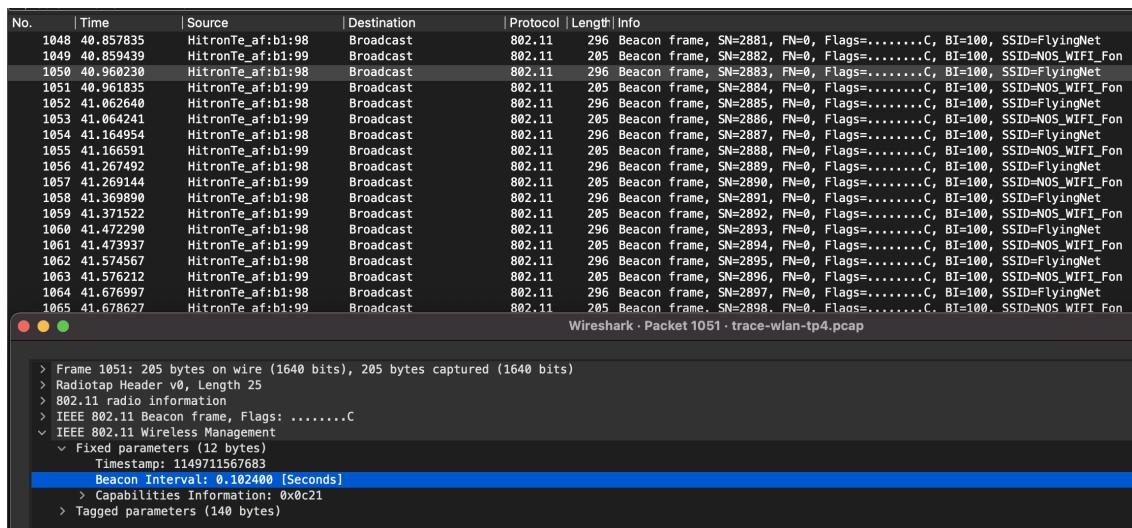


Figura 1.6: Intervalo teórico

O intervalo de tempo previsto entre tramas beacon encontra-se indicado no campo **Beacon**

Interval. Como indicado na figura 1.6, o intervalo teórico seria de **0.102400** segundos.

Como observado na figura 1.7, o intervalo temporal é minimamente superior. Isto deve-se ao congestionamento da rede assim como às próprias propriedades e condições físicas do meio de transmissão, que têm um impacto no tempo de travessia.

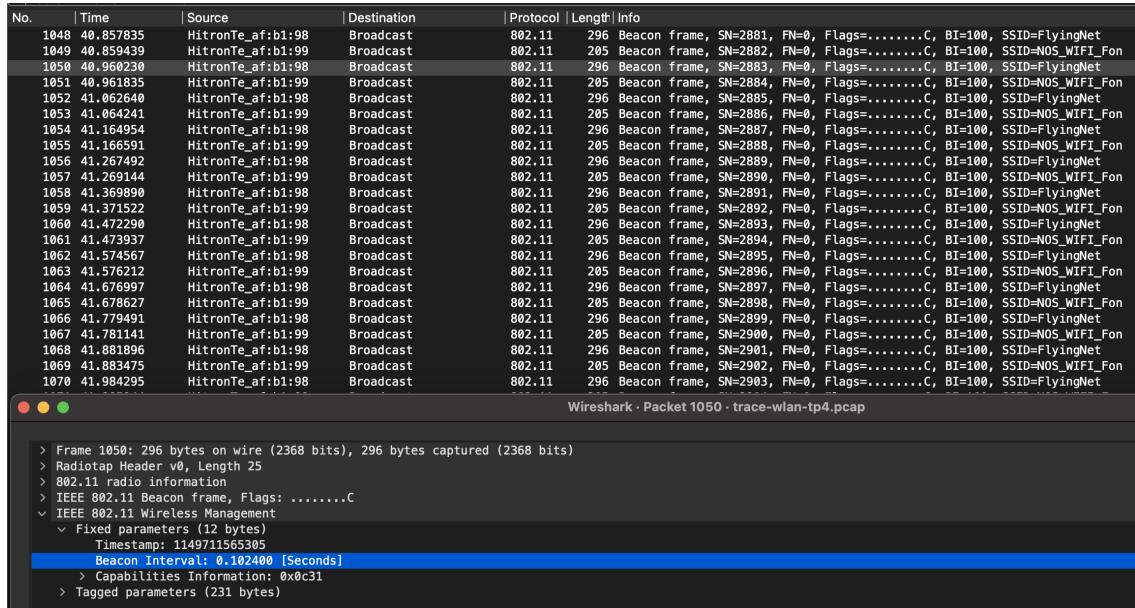


Figura 1.7: Intervalo real

1.2.5 Exercício 8

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

No.	Time	Source	Destination	Protocol	Length	Info
1030	40.347510	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2871, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1039	40.347510	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2872, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1040	40.448146	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2873, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1041	40.449791	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2874, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1042	40.550556	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2875, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1043	40.552179	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2876, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1044	40.652952	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2877, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1045	40.654576	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2878, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1046	40.755337	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2879, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1047	40.756986	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2880, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1048	40.857835	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2881, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1049	40.859439	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2882, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1050	40.960230	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2883, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1051	40.961835	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2884, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1052	41.062640	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2885, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1053	41.064241	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2886, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1054	41.164954	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2887, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1055	41.166591	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2888, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1056	41.267492	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2889, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1057	41.269144	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2890, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1058	41.369890	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2891, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1059	41.371522	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2892, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1060	41.472290	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2893, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1061	41.473937	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2894, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1062	41.574567	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2895, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1063	41.576212	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2896, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1064	41.676997	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2897, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1065	41.678627	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2898, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1066	41.779491	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2899, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1067	41.781141	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2900, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1068	41.881896	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2901, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1069	41.883475	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2902, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1070	41.984295	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2903, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1071	41.985944	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2904, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1072	42.086575	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2905, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1073	42.088191	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2906, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1074	42.188945	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2907, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1075	42.190570	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2908, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1076	42.291363	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2909, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1077	42.292964	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2910, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1078	42.393745	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2911, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1079	42.395374	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2912, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1080	42.496118	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon frame, SN=2913, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1081	42.497712	HitronTe_af:b1:99	Broadcast	802.11	295	Beacon frame, SN=2914, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

Figura 1.8: Listagem de SSIDs

Observando a coluna "Info" da figura 1.8, são observáveis dois APs diferentes que operam na vizinhança da STA de captura, estes têm os SSIDs **"FlyingNet"** e **"NOS_WIFI_Fon"**.

1.2.6 Exercício 9

Verifique se está a ser usado o método de deteção de erros (CRC). Justifique. Use o filtro:(wlan.fc.type_subtype == 0x08) && (wlan.fcs.status == bad) Que conclui? Justifique o porquê de usar deteção de erros em redes sem fios.

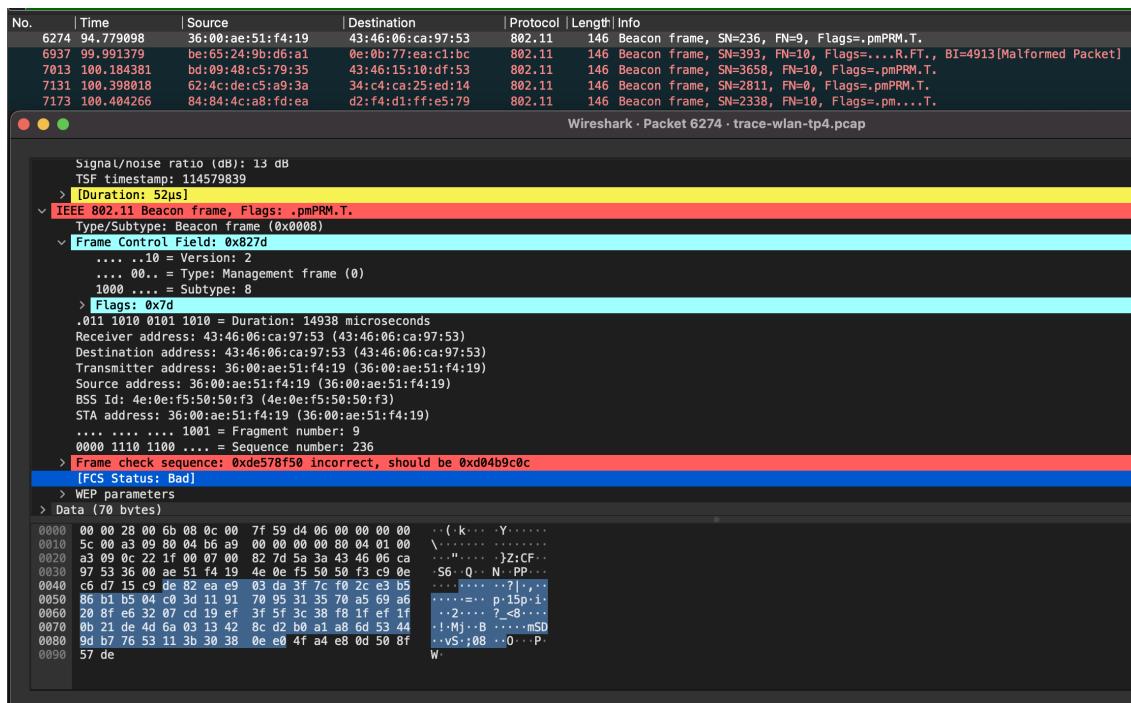


Figura 1.9: Lista de tramas Beacon com erros

Usando o comando proveniente no enunciado obteve-se o resultado constante na figura 1.9. Observa-se que o campo frame check sequence está incorreto, portanto pode-se concluir que o método de correção de erros está a ser usado. Este mecanismo de deteção de erros é importante para conseguir identificar tramas corrompidas e tentar recuperar a informação perdida no envio da mesma.

1.2.7 Exercício 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
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=2334, 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=NOS_WIFI_Fon
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_Fon
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_Fon
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_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	72.180596	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	7:ce:a6:ff:a2:cc	Broadcast	802.11	71	Probe Request, SN=62, FN=0, Flags=....., C, SSID=Wildcard (Broadcast)
4493	82.726818	7:ce:a6:ff:a2:cc	Broadcast	802.11	71	Probe Request, SN=62, FN=0, Flags=....., C, SSID=Wildcard (Broadcast)
4494	82.728646	7:ce:a6:ff:a2:cc	Broadcast	802.11	218	Probe Request, SN=65, FN=0, Flags=....., C, SSID=Wildcard (Broadcast)
6193	94.190088	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
6196	94.193504	HitronTe_af:b1:98	Apple_28:b8:0c	802.11	411	Probe Response, SN=2476, FN=0, Flags=....., C, BI=100, SSID=FlyingNet
6197	94.200286	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., C, SSID=FlyingNet
6198	94.202330	HitronTe_af:b1:98	Apple_28:b8:0c	802.11	411	Probe Response, SN=2477, FN=0, Flags=....., C, BI=100, SSID=FlyingNet
6199	94.202930	HitronTe_af:b1:98	Apple_28:b8:0c	802.11	411	Probe Response, SN=2478, FN=0, Flags=....., C, BI=100, SSID=FlyingNet
6200	94.203665	HitronTe_af:b1:98	Apple_28:b8:0c	802.11	411	Probe Response, SN=2479, FN=0, Flags=....., C, BI=100, SSID=FlyingNet
6203	94.213697	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., C, SSID=FlyingNet
6204	94.224724	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., C, SSID=FlyingNet
6205	94.237944	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., C, SSID=FlyingNet
6206	94.248503	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., C, SSID=FlyingNet
6207	94.261777	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., C, SSID=FlyingNet
6208	94.272579	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., C, SSID=FlyingNet
6209	94.285744	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., C, SSID=FlyingNet
6210	94.296433	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., C, SSID=FlyingNet
6222	94.358606	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., C, SSID=FlyingNet
6223	94.369617	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., C, SSID=FlyingNet
6224	94.382988	Apple_28:b8:0c	Broadcast	802.11	152	Probe Request, SN=0, FN=0, Flags=....., C, SSID=FlyingNet

Figura 1.10: Lista de tramas Pobing Request ou Probing Response

Com a utilização do filtro `wlan.fcsubtype == 5 ou wlan.fcsubtype == 4` é possível obter uma lista com todos os Probing Request e Probing Response obtidos.

1.2.8 Exercício 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?

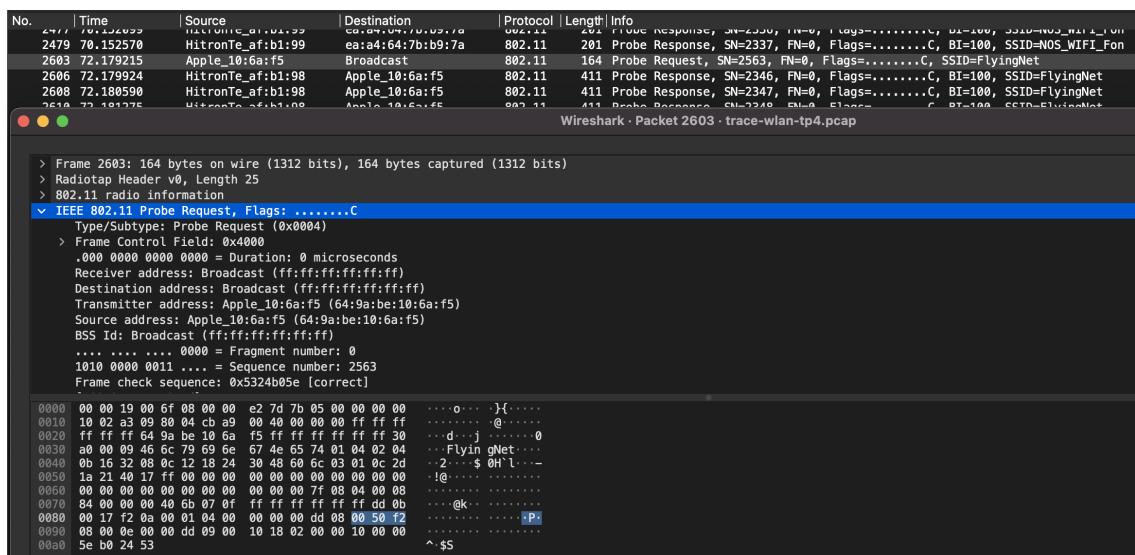


Figura 1.11: Trama Probing Request

O propósito de um Probing Request será para obter informações acerca de outras AP. Como tanto o Destination Address como Receiver Address são o broadcast address, esta trama pretenderá obter informações de todos os AP em alcance da STA que enviou a dada trama.

1.3 6. Processo de Associação

1.3.1 Exercício 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.

No.	Time	Source	Destination	Protocol	Length	Info
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
4692	83.663250	7:ea:6d:ffa:2:cc	HitronTe_af:b1:98	802.11	59	Authentication, SN=67, FN=0, Flags=.....C
4694	83.663681	HitronTe_af:b1:98	7:ea:6d:ff:a2:cc	802.11	59	Authentication, SN=2439, FN=0, Flags=.....C
4696	83.665976	7:ea:6d:ffa:2: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	7:ea:6d:ff:a2:cc	802.11	225	Association Response, SN=2440, FN=0, Flags=.....C
4699	83.680045	HitronTe_af:b1:98	7:ea:6d:ff:a2:cc	802.11	225	Association Response, SN=2440, FN=0, Flags=.....R...C
6915	99.967142	a8:05:ea:f5:cf:a8	e1:37:40:44:46:23	802.11	146	Authentication, SN=434, FN=1, Flags=op.P.M...
7043	100.196334	dd:88:93:0f:ec:e9	af:40:cd:40:5f:82	802.11	146	Authentication, SN=2467, FN=4, Flags=p.P.M...
7065	100.208375	d7:19:51:08:62:f9	6d:1b:44:1a:cc:11	802.11	146	Association Request, SN=2586, FN=7, Flags=pmPRM.T
7163	100.403689	0a:57:13:28:40:84	79:5c:58:10:7a:cc	802.11	146	Association Response, SN=3497, FN=5, Flags=o.MP.F.. [Malformed Packet]
13218	107.753005	20:b4:c4:ad:d7:19	d5:a5:29:9b:fe:00	802.11	1183	Authentication, SN=79, FN=13, Flags=o..PR.F.. [Malformed Packet]
16451	115.725544	fd:31:55:63:20:86	6a:8f:cd:88:f4:55	802.11	146	Authentication, SN=1054, FN=10, Flags=...P..... [Malformed Packet]

Figura 1.12: Tramas presentes no processo de associação completo

Através do filtro presente na figura 1.12 obtemos várias tramas que correspondem ao processo de associação completo. Este processo consiste no envio de quatro tramas: duas tramas de autenticação, uma *Association Request* e uma *Association Response*.

1.3.2 Exercício 13

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

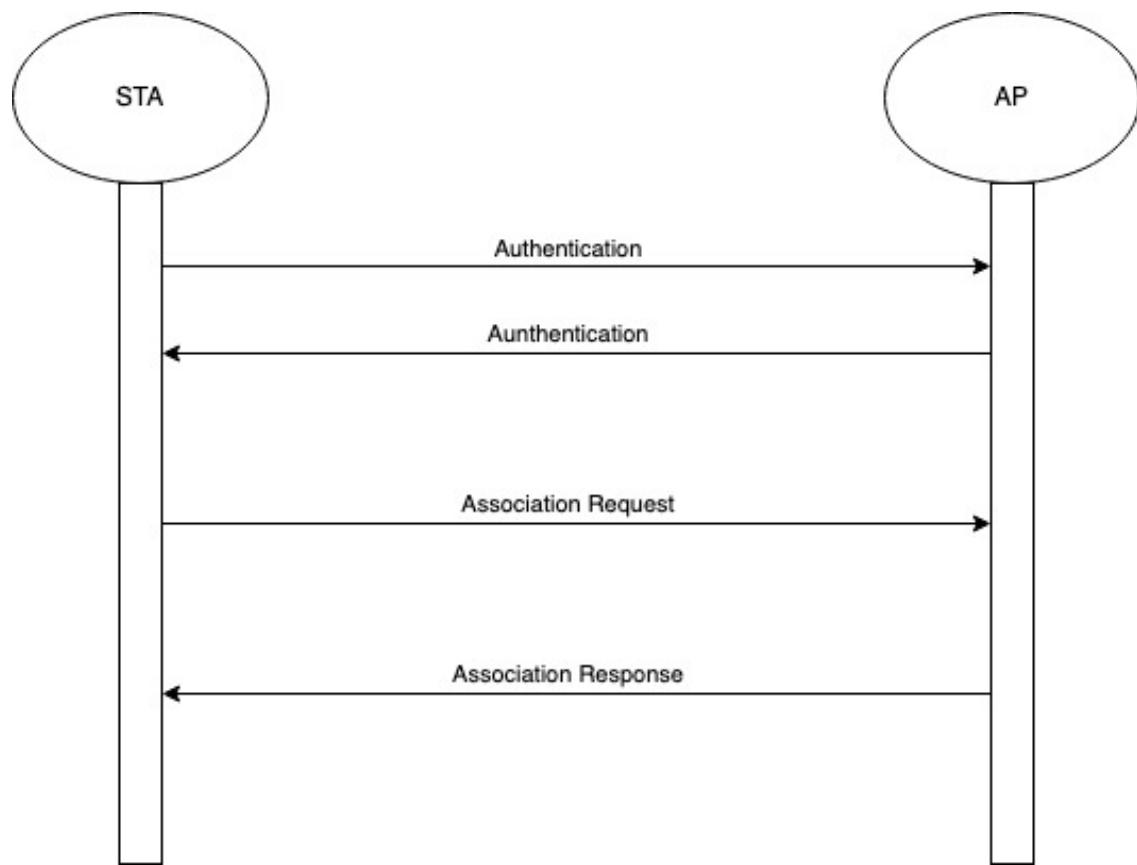


Figura 1.13: Diagrama da sequência de tramas trocadas

1.4 7. Transferência de Dados

1.4.1 Exercício 14

Considere a trama de dados nº455. 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?

Através do campo Frame Control, na flag *DS status*, observa-se que esta se encontra com o valor 10, o que quer dizer que o pacote de dados está a vir do Sistema de Distribuição, fora da rede local, logo, conclui-se que a a trama não será local à WLAN.

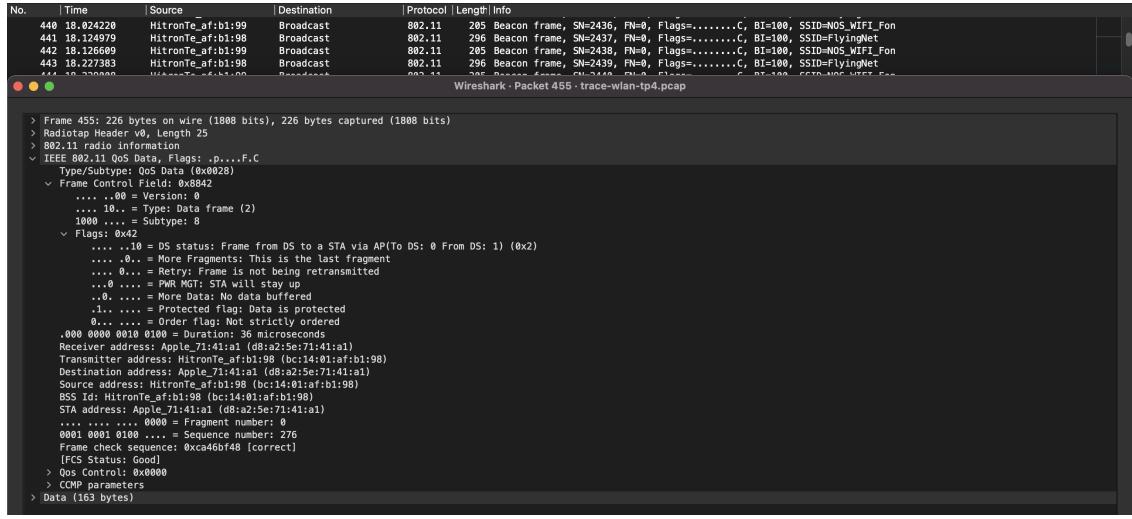


Figura 1.14: Trama número 455

1.4.2 Exercício 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?

Ao observar a figura 1.14 os endereçamentos MAC do STA, AP e do router de acesso ao sistema de distribuição serão, respetivamente, d8:a2:5e:71:41:a1, d8:a2:5e:71:41:a1 e bc:14:01:af:b1:98..

1.4.3 Exercício 16

Como interpreta a trama nº457 face à sua direccionalidade e endereçamento MAC?

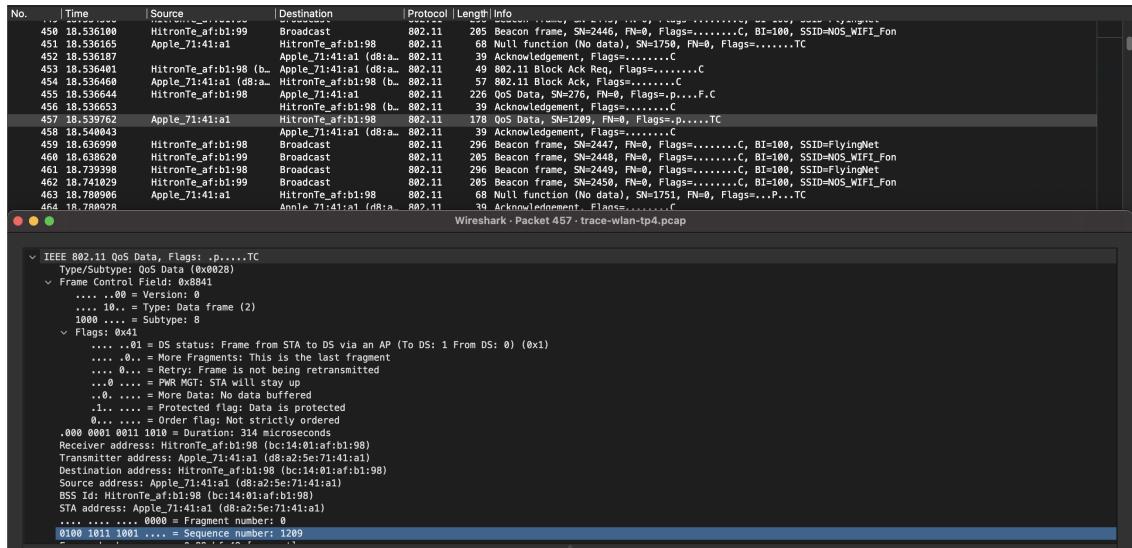


Figura 1.15: Trama número 457

Através da consulta do campo *Frame Control* da figura 1.15 pode-se concluir que, quanto à direccionalidade da trama, esta tem como destino o Sistema de Distribuição devido à flag DS status

estar 01. O endereço MAC de origem e do transmissor é o mesmo, sendo este d8:a2:5e:71:41:a1. O endereço MAC de destino e do receptor também é o mesmo sendo bc:14:01:af:b1:98. Com esta informação verifica-se que a trama em questão vai deixar a rede local, sem haver qualquer tipo de intermediação no envio deste pacote.

1.4.4 Exercício 17

Que subtípico 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.)

No.	Time	Source	Destination	Protocol	Length	Info
15	0.631114	Apple_10:6a:f5 (64:9..	HiproTe_af:b1:98 (b..	802.11	45	Request-to-send, Flags=.....C
16	0.631128	Apple_10:6a:f5 (64:9..	802.11	39	Clear-to-send, Flags=.....C	
21	0.631595	Apple_10:6a:f5 (64:9..	802.11	39	Acknowledgement, Flags=.....C	

Figura 1.16: Tramas de controlo

Ao longo da transferência de dados são transmitidas 3 subtípicos de tramas de controlo, sendo estas Request To Send (RTS), Clear To Send (CTS) e Acknowledgement (ACK). Estas são necessárias para evitar colisões de tramas de dados em APs.

1.4.5 Exercício 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 direccionalidade das tramas e os sistemas envolvidos.

No.	Time	Source	Destination	Protocol	Length	Info
15	0.631114	Apple_10:6a:f5 (64:9..	HiproTe_af:b1:98 (b..	802.11	45	Request-to-send, Flags=.....C
16	0.631128	Apple_10:6a:f5 (64:9..	802.11	39	Clear-to-send, Flags=.....C	
21	0.631595	Apple_10:6a:f5 (64:9..	802.11	39	Acknowledgement, Flags=.....C	

Frame 15: 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
0 = Version: 0
0.. = Type: Control frame (1)
 1011 ..0 = Subtype: 11
 ^ Flags: 0x00
00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (8x0)
0.. = More Fragments: This is the last fragment
 0... = Retry: Frame is not being retransmitted
 0 .. = PWR MGT: STA will stay up
 0.... = More Data: No data buffered
 0.... = Protected flag: Data is not protected
 0.... = Order flag: Not strictly ordered
 .000 0000 1101 0010 .. Duration: 210 microseconds
 Receiver address: Apple_10:6a:f5 (64:9..af:b1:98)
 Transmitter address: Apple_10:6a:f5 (64:9..af:b1:98)
 Frame check sequence: 0x168049c0 (correct)
 [FCS Status: Good]

Figura 1.17: Trama RTS com identificador 15

Através da figura 1.16 verificamos a existência de tramas das tramas de controlo referidas. Observando o conteúdo da trama 15, representada na figura 1.17, deduz-se que as tramas envolvidas nesse processo não irão sair do seu sistema de distribuição ou estarão no modo ad hoc. Neste processo de troca de informação, a STA envia a trama RTS para o AP correspondente, sendo respondida por uma trama CTS enviada pelo AP. Os hosts da rede vão receber também a informação que o AP vai estar "ocupado" durante um período de tempo, para que a STA que enviou a trama RTS consiga enviar o pacote de dados sem correr o risco de colisões no AP, sendo, no fim da receção da trama de dados, respondida por uma trama ACK por parte do AP.

Capítulo 2

Conclusão

Com a realização deste TP foi possível consolidar conhecimentos adquiridos nas aulas teóricas dos temas **Acesso Rádio**, **Scanning Passivo e Ativo**, **Processo de Associação** e **Transferência de Dados**.

Tal como nos restantes TPs, recorremos à ferramenta WireShark que ajudou no processo de captação e análise de tramas. Neste TP o análise das tramas inferiu, especialmente, nas tramas 802.11.

Concluindo, foi possível obter um aproveitamento desejado nos temas abordados neste trabalho prático sendo assim capazes de analisar tramas 802.11, perceber que tipos e subtipos em que se dividem e que funções é que desempenham de forma a garantir uma boa comunicação entre hosts numa rede Wi-Fi.