Trabalho Prático Nº4 - Redes sem Fios (Wi-Fi)

Simão Cunha[a93262], Duarte Leitão[a100550], and Diogo Barros[a100600]

Universidade do Minho - Campus de Gualtar, R. da Universidade, 4710-057 Braga Portugal

Redes de Computadores (2022/2023) - PL10 - Grupo 7

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

A trama escolhida pelo nosso grupo foi a 107ª (PL10, Grupo 7)

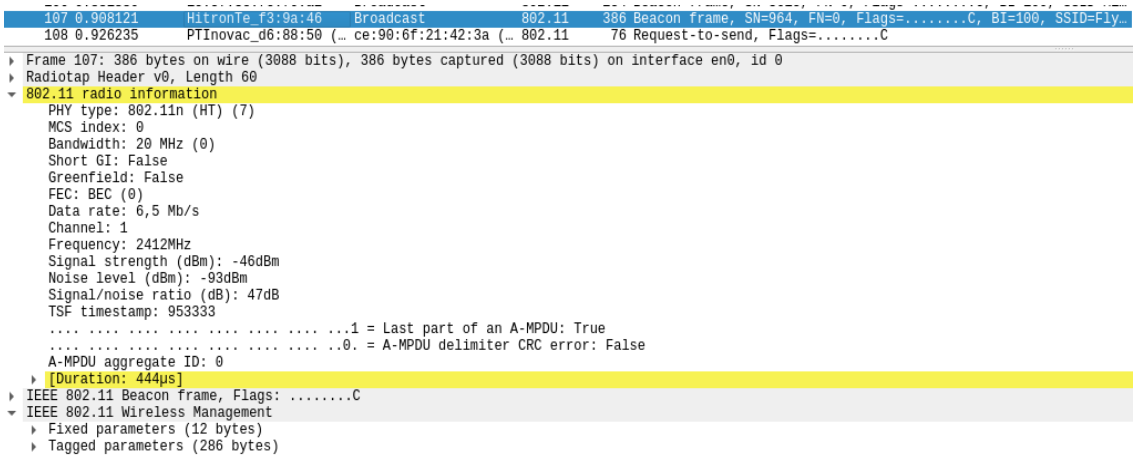


Figura 1: Informação do Wireshark

Analisando a figura da captura, percebemos que a rede sem fios está a operar na canal 1 a 2412 MHz.

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

Recorrendo novamente à figura da captura do exercício anterior, notamos que está ser usada a norma 802.11n. Tal pode ser confirmado no campo `PHY type` do Wireshark.

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

No campo Data rate, presente na figura 1, podemos ver que esta trama está a ser enviada a um débito de 6.5 Mb/s. O valor do débito máximo da versão 802.11n da norma IEEE é 600 Mb/s (figura 2). Concluímos, então, que o débito a que foi enviada a trama não corresponde ao valor máximo a que a interface Wi-Fi pode operar. A figura abaixo comprova esta conclusão.

802.11n (WiFi 4)	2009	600 Mbps	70m	2.4, 5 GHz

Figura 2: Excerto dos slides das aulas teóricas

4 Verifique qual a força do sinal (Signal strength) e a qualidade expectável de receção da trama

Analisando mais uma vez a figura 1, verificamos que o parâmetro Signal Strength tem valor -46 dBm. Olhando para a figura abaixo concluímos que a qualidade de receção da trama será considerada como "excelente", visto estar no intervalo [-55dBm, -30dBm].

Signal strength	Expected Quality
-90dBm	Chances of connecting are very low at this level
-80dBm	Unreliable signal strength
-67dBm	Reliable signal strength– the edge of what Cisco considers to be adequate to support Voice over WLAN
-55dBm	Anything down to this level can be considered excellent signal strength.
-30dBm	Maximum signal strength, you are probably standing right next to the access point.

Figura 3: Qualidade expectável de receção da trama

5 Selecione uma trama beacon cuja ordem (ou terminação) corresponda a XX. Esta trama pertence a que tipo de tramas 802.11? Identifique o valor dos identificadores de tipo e de subtipo da trama. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?

Continuaremos a considerar a trama 107 da figura 1 visto que esta é uma trama beacon.

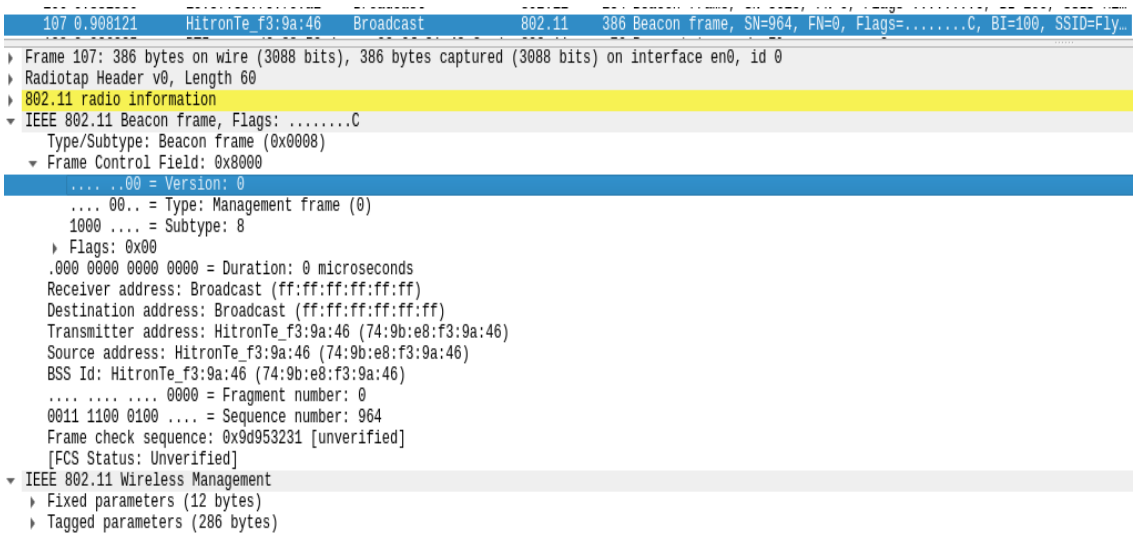


Figura 4: Informação da trama 107

Analisando a secção do cabeçalho `Frame Control Field` na figura acima, sobre a trama 107, percebemos que esta é do tipo 0 (Management frame) e do subtipo 8 (Beacon).

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

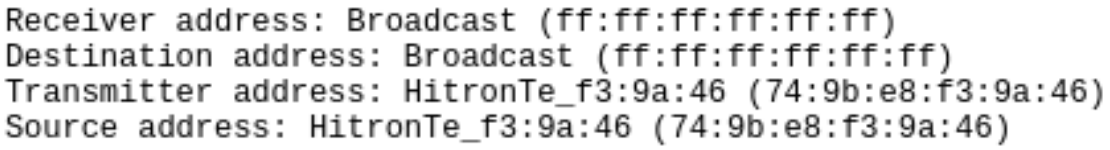


Figura 5: Endereços MAC da trama 107

Na figura 5 vemos que os endereços em uso são ff:ff:ff:ff:ff:ff; ff:ff:ff:ff:ff:ff; 74:9b:e8:f3:9a:46 e 74:9b:e8:f3:9a:46. Através dos endereços identificados podemos concluir que a origem da trama é o Access Point mais perto localizado do host que fez a captura e que a trama será enviada para todos os dispositivos ao alcance desse mesmo Access Point.

7 Verifique se está a ser usado o método de deteção de erros (CRC). Justifique. Justifique o porquê de ser necessário usar deteção de erros em redes sem fios.

Neste exercício, iremos consultar o valor do campo `Frame Check Sequence`.

Na figura abaixo, podemos observar que este campo na trama 107 está *unverified*, e verificamos que o método CRC tem a flag *Unverified*, levando a querer que não é usado.

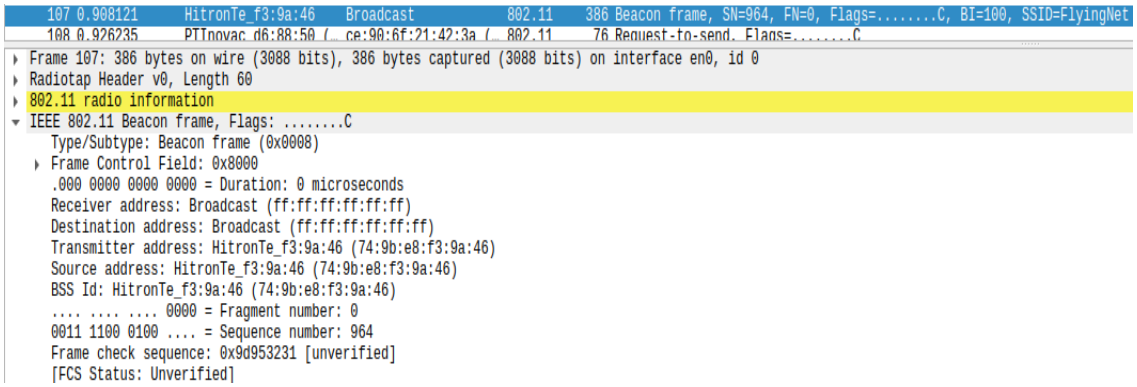


Figura 6: Endereços MAC da trama 107

A utilização destes métodos de deteção de erros em ambientes de redes sem fios permite um melhor tratamento de colisões, uma vez que a probabilidade de estas ocorrerem é superior quando comparada, por exemplo, com a probabilidade de ocorrência em meios de nível 1 da pilha protocolar.

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

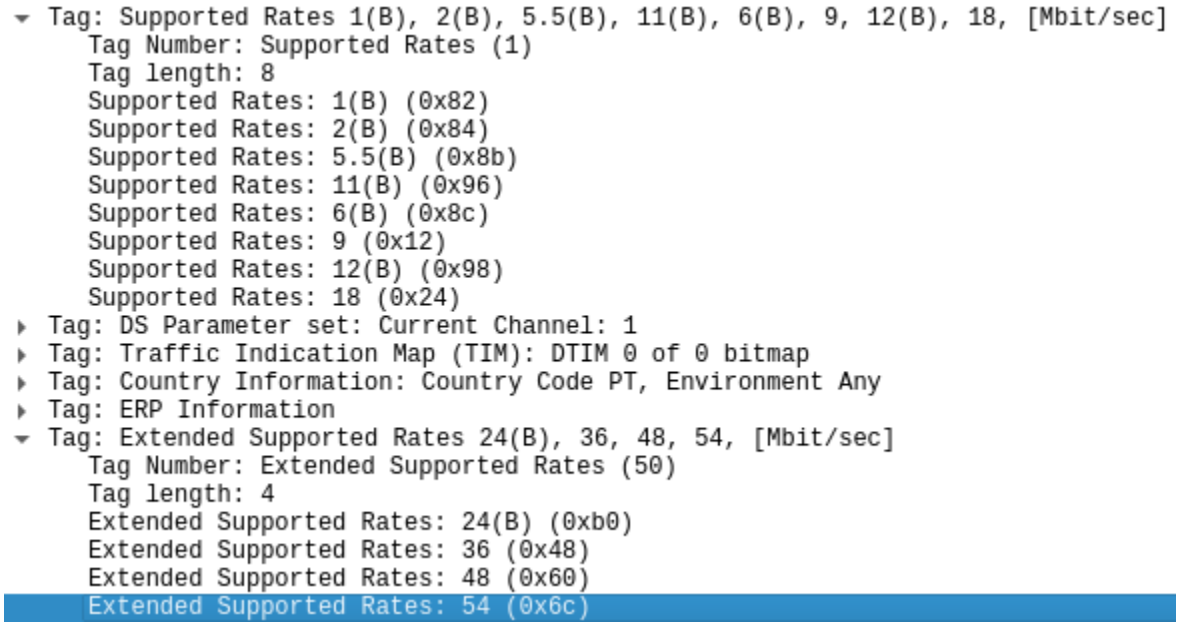


Figura 7: : Identificação dos débitos

Na figura acima vemos que os débitos suportados são os seguintes: 1, 2, 5.5, 6, 9,12 e 18 (todos em Mb/s). Já os débitos adicionais são: 24, 36, 48 e 54 (todos em Mb/s).

9 Qual o intervalo de tempo previsto entre tramas beacon consecutivas (este valor é anunciado na própria trama beacon)? Na prática, a periodicidade de tramas beacon provenientes do mesmo AP é verificada com precisão? Justifique.

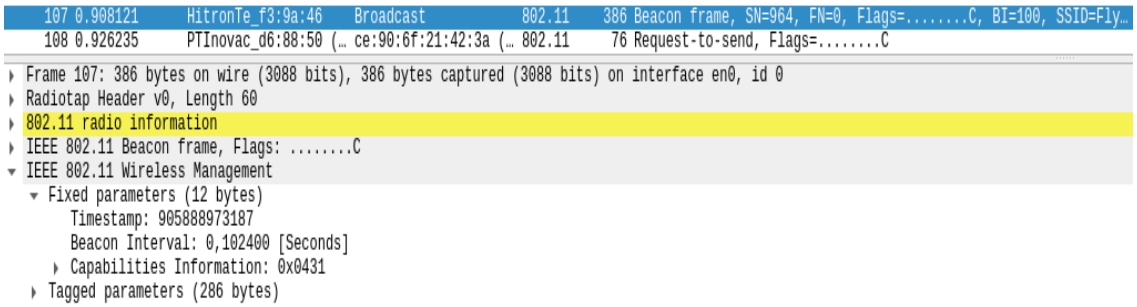
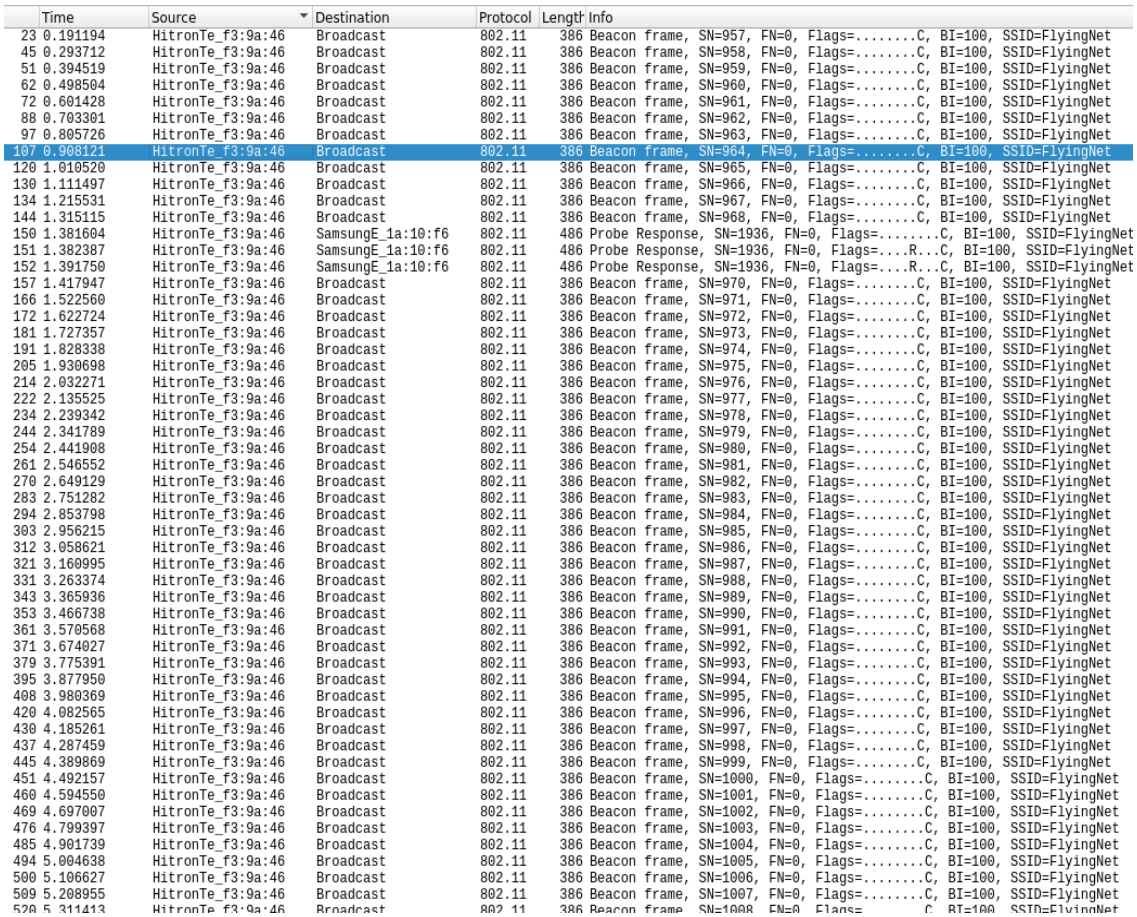


Figura 8: Tempo previsto entre tramas consecutivas

Através da figura, pode-se observar que intervalo de tempo previsto é de 0.102400 segundos. Na prática, este valor acaba por ser mais uma aproximação do que um valor exato porque o Access Point pode estar ocupado no momento exato em que devia enviar a trama beacon levando a um ligeiro atraso no envio da mesma.

10 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).



	Time	Source	Destination	Protocol	Length	Info
23	0.191194	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=957, FN=0, Flags=........C, BI=100, SSID=FlyingNet
45	0.293712	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=958, FN=0, Flags=........C, BI=100, SSID=FlyingNet
51	0.394519	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=959, FN=0, Flags=........C, BI=100, SSID=FlyingNet
62	0.498504	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=960, FN=0, Flags=........C, BI=100, SSID=FlyingNet
72	0.601428	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=961, FN=0, Flags=........C, BI=100, SSID=FlyingNet
88	0.703301	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=962, FN=0, Flags=........C, BI=100, SSID=FlyingNet
97	0.805726	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=963, FN=0, Flags=........C, BI=100, SSID=FlyingNet
107	0.908121	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=964, FN=0, Flags=........C, BI=100, SSID=FlyingNet
120	1.010520	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=965, FN=0, Flags=........C, BI=100, SSID=FlyingNet
130	1.111497	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=966, FN=0, Flags=........C, BI=100, SSID=FlyingNet
134	1.215531	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=967, FN=0, Flags=........C, BI=100, SSID=FlyingNet
144	1.315115	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=968, FN=0, Flags=........C, BI=100, SSID=FlyingNet
150	1.381604	HitronTe_f3:9a:46	SamsungE_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=........C, BI=100, SSID=FlyingNet
151	1.382387	HitronTe_f3:9a:46	SamsungE_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=....R...C, BI=100, SSID=FlyingNet
152	1.391750	HitronTe_f3:9a:46	SamsungE_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=....R...C, BI=100, SSID=FlyingNet
157	1.417947	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=970, FN=0, Flags=........C, BI=100, SSID=FlyingNet
166	1.522560	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=971, FN=0, Flags=........C, BI=100, SSID=FlyingNet
172	1.622724	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=972, FN=0, Flags=........C, BI=100, SSID=FlyingNet
181	1.727357	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=973, FN=0, Flags=........C, BI=100, SSID=FlyingNet
191	1.828338	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=974, FN=0, Flags=........C, BI=100, SSID=FlyingNet
205	1.930698	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=975, FN=0, Flags=........C, BI=100, SSID=FlyingNet
214	2.032271	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=976, FN=0, Flags=........C, BI=100, SSID=FlyingNet
222	2.135525	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=977, FN=0, Flags=........C, BI=100, SSID=FlyingNet
234	2.239342	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=978, FN=0, Flags=........C, BI=100, SSID=FlyingNet
244	2.341789	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=979, FN=0, Flags=........C, BI=100, SSID=FlyingNet
254	2.441908	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=980, FN=0, Flags=........C, BI=100, SSID=FlyingNet
261	2.546552	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=981, FN=0, Flags=........C, BI=100, SSID=FlyingNet
270	2.649129	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=982, FN=0, Flags=........C, BI=100, SSID=FlyingNet
283	2.751282	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=983, FN=0, Flags=........C, BI=100, SSID=FlyingNet
294	2.853798	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=984, FN=0, Flags=........C, BI=100, SSID=FlyingNet
303	2.956215	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=985, FN=0, Flags=........C, BI=100, SSID=FlyingNet
312	3.058621	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=986, FN=0, Flags=........C, BI=100, SSID=FlyingNet
321	3.160995	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=987, FN=0, Flags=........C, BI=100, SSID=FlyingNet
331	3.263374	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=988, FN=0, Flags=........C, BI=100, SSID=FlyingNet
343	3.365936	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=989, FN=0, Flags=........C, BI=100, SSID=FlyingNet
353	3.466738	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=990, FN=0, Flags=........C, BI=100, SSID=FlyingNet
361	3.570568	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=991, FN=0, Flags=........C, BI=100, SSID=FlyingNet
371	3.674027	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=992, FN=0, Flags=........C, BI=100, SSID=FlyingNet
379	3.775391	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=993, FN=0, Flags=........C, BI=100, SSID=FlyingNet
395	3.877950	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=994, FN=0, Flags=........C, BI=100, SSID=FlyingNet
408	3.980369	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=995, FN=0, Flags=........C, BI=100, SSID=FlyingNet
420	4.082565	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=996, FN=0, Flags=........C, BI=100, SSID=FlyingNet
430	4.185261	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=997, FN=0, Flags=........C, BI=100, SSID=FlyingNet
437	4.287459	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=998, FN=0, Flags=........C, BI=100, SSID=FlyingNet
445	4.389869	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=999, FN=0, Flags=........C, BI=100, SSID=FlyingNet
451	4.492157	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=1000, FN=0, Flags=........C, BI=100, SSID=FlyingNet
460	4.594550	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=1001, FN=0, Flags=........C, BI=100, SSID=FlyingNet
469	4.697007	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=1002, FN=0, Flags=........C, BI=100, SSID=FlyingNet
476	4.799397	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=1003, FN=0, Flags=........C, BI=100, SSID=FlyingNet
485	4.901739	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=1004, FN=0, Flags=........C, BI=100, SSID=FlyingNet
494	5.004638	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=1005, FN=0, Flags=........C, BI=100, SSID=FlyingNet
500	5.106627	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=1006, FN=0, Flags=........C, BI=100, SSID=FlyingNet
509	5.208955	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=1007, FN=0, Flags=........C, BI=100, SSID=FlyingNet
520	5.311413	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=1008, FN=0, Flags=........C, BI=100, SSID=FlyingNet

Figura 9: Lista dos SSIDS e dos APs

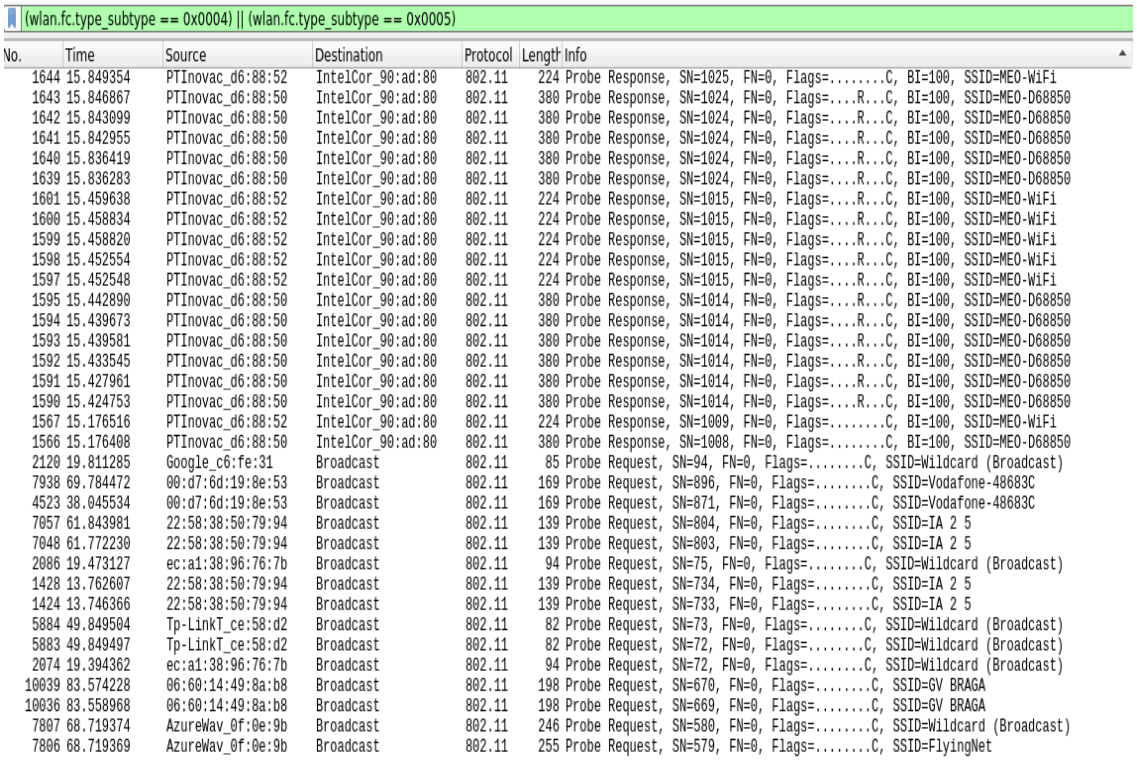
De acordo com a figura, o único SSID a operar na vizinhança é o FlyingNet. Para obter esta informação foi aplicado o filtro `wlan.ssid` no Wireshark.

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

management frames	wlan.fc.type == 0	all management frames
	wlan.fc.type_subtype == 0	association requests
	wlan.fc.type_subtype == 1	association response
	wlan.fc.type_subtype == 2	re-association request
	wlan.fc.type_subtype == 3	re-association response
	wlan.fc.type_subtype == 4	probe requests
	wlan.fc.type_subtype == 5	probe responses
	wlan.fc.type_subtype == 8	beacons
	wlan.fc.type_subtype == 9	atims
	wlan.fc.type_subtype == 10	disassosiations
	wlan.fc.type_subtype == 11	authentications
	wlan.fc.type_subtype == 12	deauthentications
	wlan.fc.type_subtype == 13	actions

Figura 10: Filtros do Wireshark para visualizar tramas

O filtro a aplicar para visualizar todas as tramas probing request e probing response simultaneamente será: `wlan.fc.type_subtype == 0x0004 || wlan.fc.type_subtype == 0x0005`. A imagem acima foi retirada do seguinte website: `https://www.wifi-professionals.com/2019/03/wireshark-display-filters`.



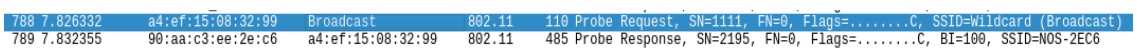
(wlan.fc.type_subtype == 0x0004) || (wlan.fc.type_subtype == 0x0005)

No.	Time	Source	Destination	Protocol	Length	Info
1644	15.849354	PTInovac_d6:88:52	IntelCor_90:ad:80	802.11	224	Probe Response, SN=1025, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi
1643	15.846867	PTInovac_d6:88:50	IntelCor_90:ad:80	802.11	380	Probe Response, SN=1024, FN=0, Flags=....R...C, BI=100, SSID=MEO-D68850
1642	15.843099	PTInovac_d6:88:50	IntelCor_90:ad:80	802.11	380	Probe Response, SN=1024, FN=0, Flags=....R...C, BI=100, SSID=MEO-D68850
1641	15.842955	PTInovac_d6:88:50	IntelCor_90:ad:80	802.11	380	Probe Response, SN=1024, FN=0, Flags=....R...C, BI=100, SSID=MEO-D68850
1640	15.836419	PTInovac_d6:88:50	IntelCor_90:ad:80	802.11	380	Probe Response, SN=1024, FN=0, Flags=....R...C, BI=100, SSID=MEO-D68850
1639	15.836283	PTInovac_d6:88:50	IntelCor_90:ad:80	802.11	380	Probe Response, SN=1024, FN=0, Flags=....R...C, BI=100, SSID=MEO-D68850
1601	15.459638	PTInovac_d6:88:52	IntelCor_90:ad:80	802.11	224	Probe Response, SN=1015, FN=0, Flags=....R...C, BI=100, SSID=MEO-WiFi
1600	15.458834	PTInovac_d6:88:52	IntelCor_90:ad:80	802.11	224	Probe Response, SN=1015, FN=0, Flags=....R...C, BI=100, SSID=MEO-WiFi
1599	15.458820	PTInovac_d6:88:52	IntelCor_90:ad:80	802.11	224	Probe Response, SN=1015, FN=0, Flags=....R...C, BI=100, SSID=MEO-WiFi
1598	15.452554	PTInovac_d6:88:52	IntelCor_90:ad:80	802.11	224	Probe Response, SN=1015, FN=0, Flags=....R...C, BI=100, SSID=MEO-WiFi
1597	15.452548	PTInovac_d6:88:52	IntelCor_90:ad:80	802.11	224	Probe Response, SN=1015, FN=0, Flags=....R...C, BI=100, SSID=MEO-WiFi
1595	15.442890	PTInovac_d6:88:50	IntelCor_90:ad:80	802.11	380	Probe Response, SN=1014, FN=0, Flags=....R...C, BI=100, SSID=MEO-D68850
1594	15.439673	PTInovac_d6:88:50	IntelCor_90:ad:80	802.11	380	Probe Response, SN=1014, FN=0, Flags=....R...C, BI=100, SSID=MEO-D68850
1593	15.439581	PTInovac_d6:88:50	IntelCor_90:ad:80	802.11	380	Probe Response, SN=1014, FN=0, Flags=....R...C, BI=100, SSID=MEO-D68850
1592	15.433545	PTInovac_d6:88:50	IntelCor_90:ad:80	802.11	380	Probe Response, SN=1014, FN=0, Flags=....R...C, BI=100, SSID=MEO-D68850
1591	15.427961	PTInovac_d6:88:50	IntelCor_90:ad:80	802.11	380	Probe Response, SN=1014, FN=0, Flags=....R...C, BI=100, SSID=MEO-D68850
1590	15.424753	PTInovac_d6:88:50	IntelCor_90:ad:80	802.11	380	Probe Response, SN=1014, FN=0, Flags=....R...C, BI=100, SSID=MEO-D68850
1567	15.176516	PTInovac_d6:88:52	IntelCor_90:ad:80	802.11	224	Probe Response, SN=1009, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi
1566	15.176408	PTInovac_d6:88:50	IntelCor_90:ad:80	802.11	380	Probe Response, SN=1008, FN=0, Flags=.....C, BI=100, SSID=MEO-D68850
2120	19.811285	Google_c6:fe:31	Broadcast	802.11	85	Probe Request, SN=94, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
7938	69.784472	00:d7:6d:19:8e:53	Broadcast	802.11	169	Probe Request, SN=896, FN=0, Flags=.....C, SSID=Vodafone-48683C
4523	38.045534	00:d7:6d:19:8e:53	Broadcast	802.11	169	Probe Request, SN=871, FN=0, Flags=.....C, SSID=Vodafone-48683C
7057	61.843981	22:58:38:50:79:94	Broadcast	802.11	139	Probe Request, SN=804, FN=0, Flags=.....C, SSID=IA 2 5
7048	61.772230	22:58:38:50:79:94	Broadcast	802.11	139	Probe Request, SN=803, FN=0, Flags=.....C, SSID=IA 2 5
2086	19.473127	ec:a1:38:96:76:7b	Broadcast	802.11	94	Probe Request, SN=75, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
1428	13.762607	22:58:38:50:79:94	Broadcast	802.11	139	Probe Request, SN=734, FN=0, Flags=.....C, SSID=IA 2 5
1424	13.746366	22:58:38:50:79:94	Broadcast	802.11	139	Probe Request, SN=733, FN=0, Flags=.....C, SSID=IA 2 5
5884	49.849504	Tp-LinkT_ce:58:d2	Broadcast	802.11	82	Probe Request, SN=73, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
5883	49.849497	Tp-LinkT_ce:58:d2	Broadcast	802.11	82	Probe Request, SN=72, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2074	19.394362	ec:a1:38:96:76:7b	Broadcast	802.11	94	Probe Request, SN=72, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
10039	83.574228	06:60:14:49:8a:b8	Broadcast	802.11	198	Probe Request, SN=670, FN=0, Flags=.....C, SSID=GV BRAGA
10036	83.558968	06:60:14:49:8a:b8	Broadcast	802.11	198	Probe Request, SN=669, FN=0, Flags=.....C, SSID=GV BRAGA
7807	68.719374	AzureWav_0f:0e:9b	Broadcast	802.11	246	Probe Request, SN=580, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
7806	68.719369	AzureWav_0f:0e:9b	Broadcast	802.11	255	Probe Request, SN=579, FN=0, Flags=.....C, SSID=FlyingNet

Figura 11: Filtro aplicado

A figura acima mostra o resultado da aplicação do filtro no Wireshark.

12 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?



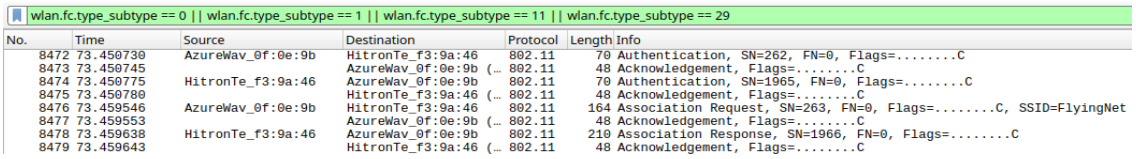
788	7.826332	a4:ef:15:08:32:99	Broadcast	802.11	110	Probe Request, SN=1111, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
789	7.832355	90:aa:c3:ee:2e:c6	a4:ef:15:08:32:99	802.11	485	Probe Response, SN=2195, FN=0, Flags=.....C, BI=100, SSID=NOS-2EC6

Figura 12: Probing Request e Probing Response

Temos, assim, exemplos de probing request e probing response nas tramas 788 e 789, respetivamente. A STA a4:ef:15:08:32:99 envia um probe request em broadcast, ou seja, a todos os access points no seu alcance que são capazes de receber esse request. O AP 90:aa:c3:ee:2e:c6 envia um probe response para a STA emissora. O propósito destas tramas é verificar quais os access points que funcionam numa dada zona e devolvem informação sobre si.

13 Identifique uma sequência de tramas que corresponda a um processo de associação realizado com sucesso entre a STA e o AP, incluindo a fase de autenticação.

Para identificar uma sequência de tramas que corresponda ao pedido no enunciado, utilizamos o filtro `(wlan.fc.type subtype == 0) || (wlan.fc.type subtype == 1) || (wlan.fc.type subtype == 11) ||(wlan.fc.type subtype == 29)` .



wlan.fc.type_subtype == 0 || wlan.fc.type_subtype == 1 || wlan.fc.type_subtype == 11 || wlan.fc.type_subtype == 29

No.	Time	Source	Destination	Protocol	Length	Info
8472	73.450730	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	70	Authentication, SN=262, FN=0, Flags=........C
8473	73.450745		AzureWav_0f:0e:9b (…	802.11	48	Acknowledgement, Flags=........C
8474	73.450775	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	70	Authentication, SN=1965, FN=0, Flags=........C
8475	73.450780		HitronTe_f3:9a:46 (…	802.11	48	Acknowledgement, Flags=........C
8476	73.459546	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	164	Association Request, SN=263, FN=0, Flags=........C, SSID=FlyingNet
8477	73.459553		AzureWav_0f:0e:9b (…	802.11	48	Acknowledgement, Flags=........C
8478	73.459638	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	210	Association Response, SN=1966, FN=0, Flags=........C
8479	73.459643		HitronTe_f3:9a:46 (…	802.11	48	Acknowledgement, Flags=........C

Figura 13: Sequência de tramas

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

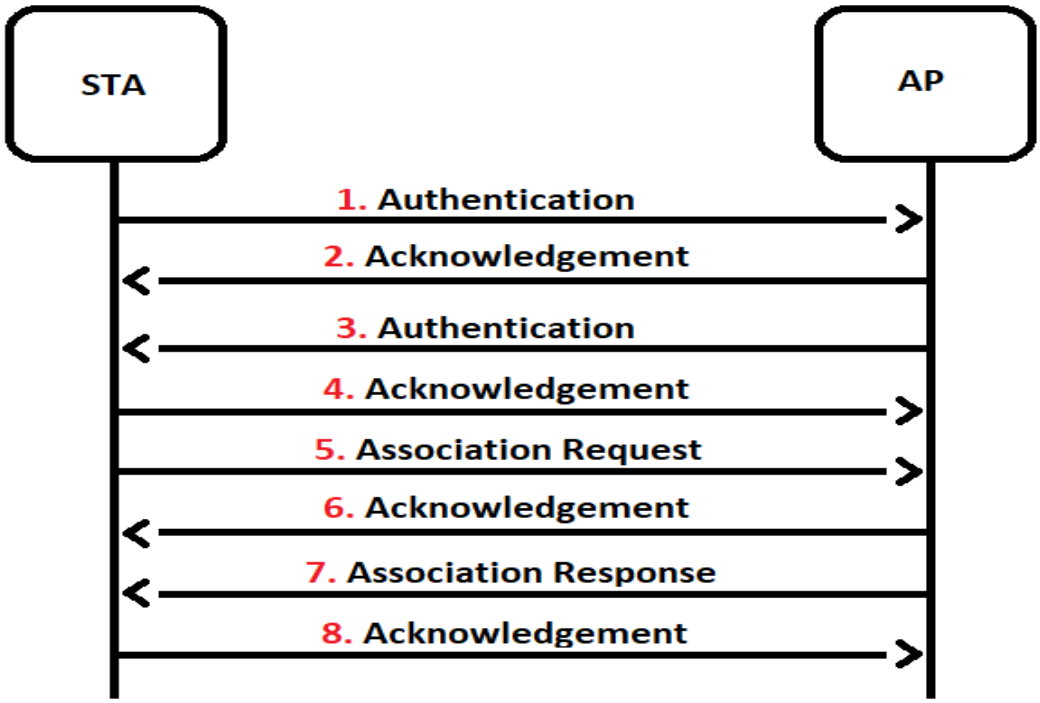


Figura 14: Pseudo-diagrama de sequência a ilustrar a sequência de tramas trocadas

15 Considere a trama de dados nº8503. 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?

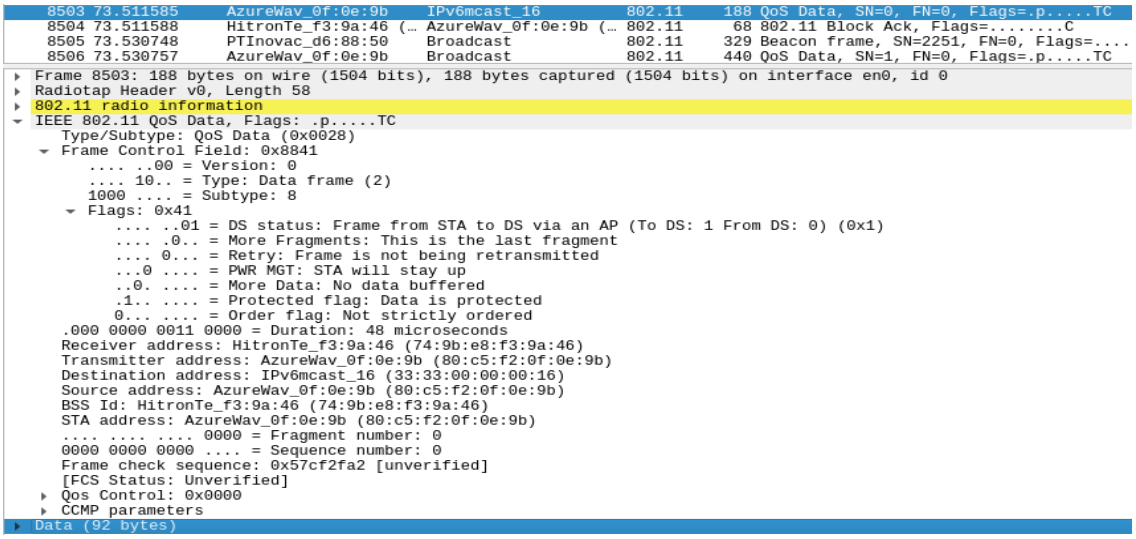


Figura 15: Trama nº8503

A direcionalidade da trama pode ser identificada nos campos To DS e From DS, tendo estes os valores 1 e 0 respetivamente. Para a trama ser local à WLAN, ambos os campos deveriam apresentar o valor 0. Podemos então concluir que a trama vem do STA para o DS.

16 Para a trama de dados nº8503, transcreva os endereços MAC em uso, identificando quais os endereços correspondentes à estação sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição (DS)?

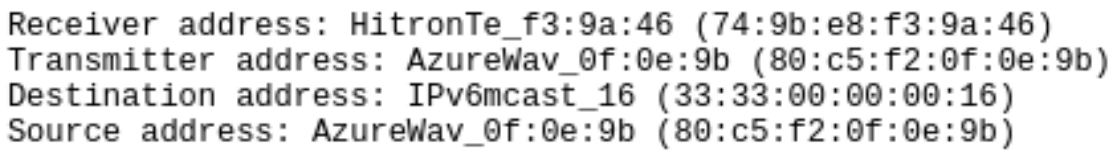


Figura 16: Endereços MAC na trama nº3503

Como é possível verificar, o AP e o router de acesso tem o mesmo MAC address, sendo portanto o mesmo equipamento.

17 Como interpreta a trama nº8521 face à sua direccionalidade e endereçamento MAC?

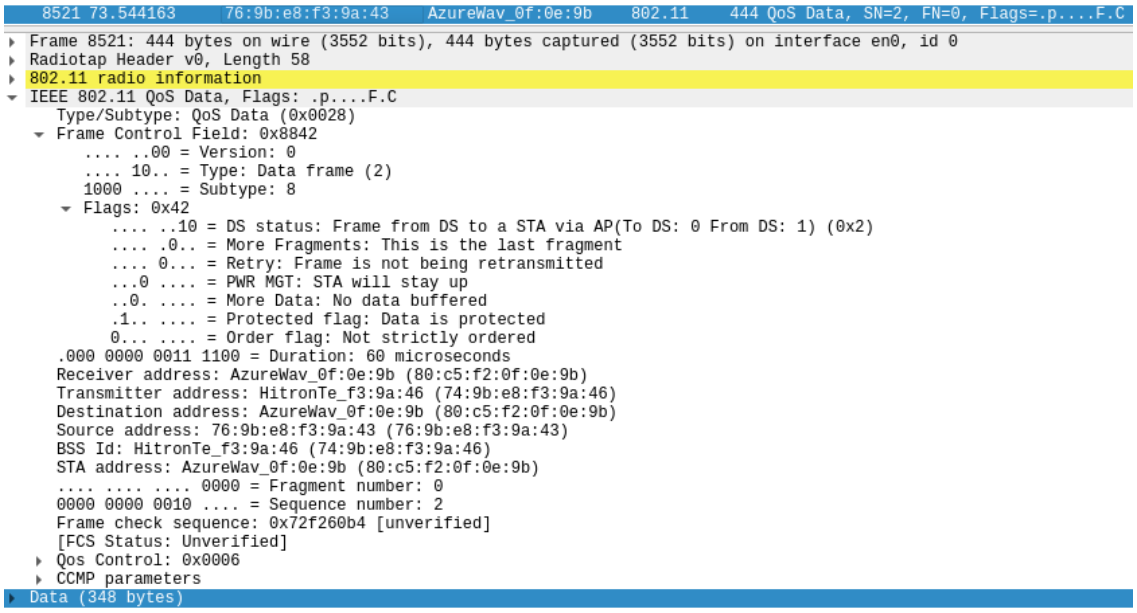


Figura 17: Trama nº8521

A direcionalidade da trama pode ser identificada nos campos To DS e From DS, tendo os valores 0 e 1, respetivamente. Para a trama ser local à WLAN, ambos os campos deveriam apresentar o valor 0. Assim, podemos concluir que a trama vem do DS para o STA.

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

O subtipo de tramas de controlo transmitidas ao longo da transferência de dados mencionada anteriormente designa-se pela abreviatura ACK, representante da expressão *Acknowledgement*. Esta metodologia deve-se ao facto de o meio em uso se tratar de um ambiente wireless, ou seja, um meio de transferência não fiável, o que implica a inexistência da garantia de chegada da trama ao destino. Desta forma, o recetor da mensagem confirma sempre a receção da mensagem enviada.

19 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. Dê um exemplo de uma transferência de dados em que é usada a opção RTC/CTS e um outro em que não é usada.

Para obtermos exemplos de transferência de dados em que é usada a opção RTC/CTS e em que não é usada, utilizados o filtro no wireshark `wlan.fc.type_subtype == 0x1b || wlan.fc.type_subtype == 0x1c` - para obtermos situações em que não é usada, simplesmente negamos a expressão lógica.

1532	14.933362	PTInovac_45:be:32	ea:54:54:89:2b:72	802.11	224	Probe Response, SN=2652, FN=0, Flags=....R...C, BI=100, SSID=MEO-WiFi
1533	14.935586	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=1102, FN=0, Flags=........C, BI=100, SSID=FlyingNet
1534	14.935592	PTInovac_45:be:32	ea:52:54:89:2b:72	802.11	224	Probe Response, SN=2652, FN=0, Flags=....R...C, BI=100, SSID=MEO-WiFi
1535	14.938856	PTInovac_45:be:32	ea:52:54:89:2b:72	802.11	224	Probe Response, SN=2652, FN=0, Flags=....R...C, BI=100, SSID=MEO-WiFi
1536	14.940899	PTInovac_45:be:32	ea:52:54:89:2b:72	802.11	224	Probe Response, SN=2652, FN=0, Flags=....R...C, BI=100, SSID=MEO-WiFi
1537	14.958058	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=1002, FN=0, Flags=........C, BI=100, SSID=MEO-D68850
1538	14.958179	PTInovac_d6:88:52	Broadcast	802.11	254	Beacon frame, SN=1003, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
1539	14.979507	PTInovac_9e:9b:b0	Broadcast	802.11	329	Beacon frame, SN=2710, FN=0, Flags=........C, BI=100, SSID=MEO-9E9BB0
1540	14.986267	92:aa:c3:ee:2e:c3	IPv4mcast_7f:ff:fa	802.11	576	Data, SN=102, FN=0, Flags=.p....F.C
1541	14.992497	92:aa:c3:ee:2e:c3	IPv4mcast_7f:ff:fa	802.11	639	Data, SN=103, FN=0, Flags=.p....F.C
1542	14.996790	92:aa:c3:ee:2e:c3	IPv4mcast_7f:ff:fa	802.11	631	Data, SN=104, FN=0, Flags=.p....F.C
1543	15.005502	92:aa:c3:ee:2e:c3	IPv4mcast_7f:ff:fa	802.11	576	Data, SN=105, FN=0, Flags=.p....F.C
1544	15.022217	92:aa:c3:ee:2e:c3	IPv4mcast_7f:ff:fa	802.11	576	Data, SN=108, FN=0, Flags=.p....F.C
1545	15.028332	92:aa:c3:ee:2e:c3	IPv4mcast_7f:ff:fa	802.11	635	Data, SN=109, FN=0, Flags=.p....F.C
1546	15.031452	92:aa:c3:ee:2e:c3	IPv4mcast_7f:ff:fa	802.11	629	Data, SN=110, FN=0, Flags=.p....F.C
1547	15.039464	HitronTe_f3:9a:46	Broadcast	802.11	386	Beacon frame, SN=1103, FN=0, Flags=........C, BI=100, SSID=FlyingNet
1548	15.060429	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=1004, FN=0, Flags=........C, BI=100, SSID=MEO-D68850

Figura 18: Exemplo em que não é usada a opção RTC/CTS

1774	16.915761		ce:90:6f:21:42:3a (…	802.11	72	Clear-to-send, Flags=........C
1775	16.923228	PTInovac_d6:88:50 (…	ce:90:6f:21:42:3a (…	802.11	76	Request-to-send, Flags=........C
1776	16.923235		ce:90:6f:21:42:3a (…	802.11	72	Clear-to-send, Flags=........C
1777	16.923238	PTInovac_d6:88:50 (…	ce:90:6f:21:42:3a (…	802.11	76	Request-to-send, Flags=........C
1778	16.923245	PTInovac_d6:88:50 (…	ce:90:6f:21:42:3a (…	802.11	76	Request-to-send, Flags=........C
1779	16.923248	PTInovac_d6:88:50 (…	ce:90:6f:21:42:3a (…	802.11	76	Request-to-send, Flags=........C
1780	16.937914		ce:90:6f:21:42:3a (…	802.11	72	Clear-to-send, Flags=........C

Figura 19: Exemplo em que é usada a opção RTC/CTS

Conclusões

Este 4º trabalho prático permitiu-nos que entendêssemos melhor acerca das redes Wi-Fi. Isto deveu-se através da análise no Wireshark de um ficheiro fornecido pela equipa docente sobre uma captura efetuada numa casa, o que trouxe algumas nuances na resposta a algumas questões neste relatório. Além disso, as diversas questões incidiram em tópicos como acesso rádio, scanning ativo e passivo, associação e transferência de dados. Assim, podemos afirmar que este trabalho prático permitiu-nos ter uma conhecimento mais abrangente sobre esta matéria, que poderá ser útil na nossa vida académica.