

Universidade do Minho
Departamento de Informática
2020/2021

TP4: Redes Sem Fios (802.11)

Redes de Computadores

6 de Janeiro de 2021

Grupo 77



Rita Gomes, A87960



Mário Real, A72620

Mestrado Integrado em Engenharia Informática
Universidade do Minho

1. Questões e Respostas

1.1. Acesso Rádio

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

Resposta:

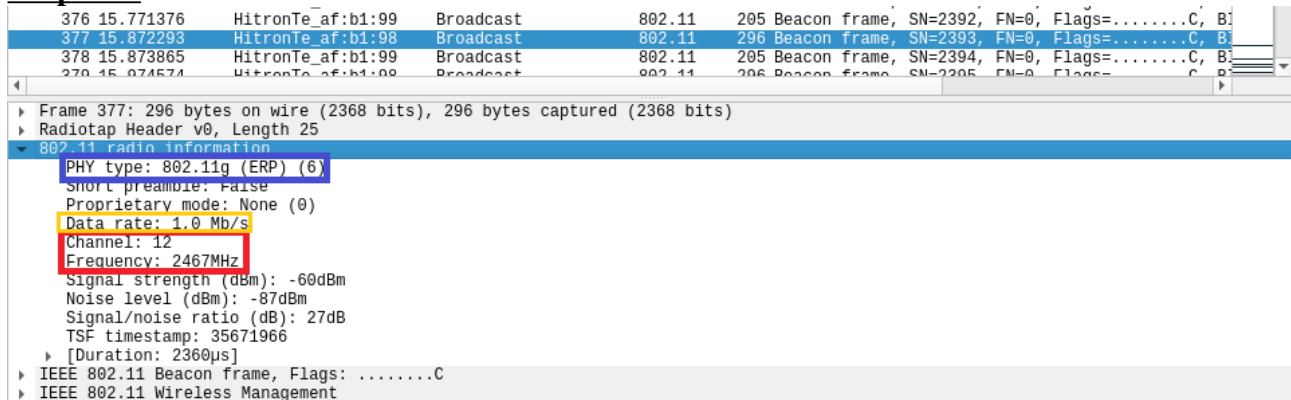


Figura 1: Captura da trama 377.

Como podemos observar na figura acima destacado a vermelho, o espectro está a operar na frequência 2467 MHz e o respetivo canal é o 12.

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

Resposta:

A azul, na figura 1, podemos ver que a versão da norma IEEE 802.11 que está a ser usada é 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.

Resposta:

A trama 377 foi enviada a um débito de 1,0 MB/s, como podemos confirmar na imagem 1 pelo campo destacado a amarelo. O débito máximo de transmissão no 802.11g é de 54 MB/s. Assim sendo, o débito a que foi enviada a trama escolhida não corresponde ao débito máximo a que a interface WiFi pode operar.

1.2. Scanning Passivo e Scanning Ativo

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)?

Resposta:

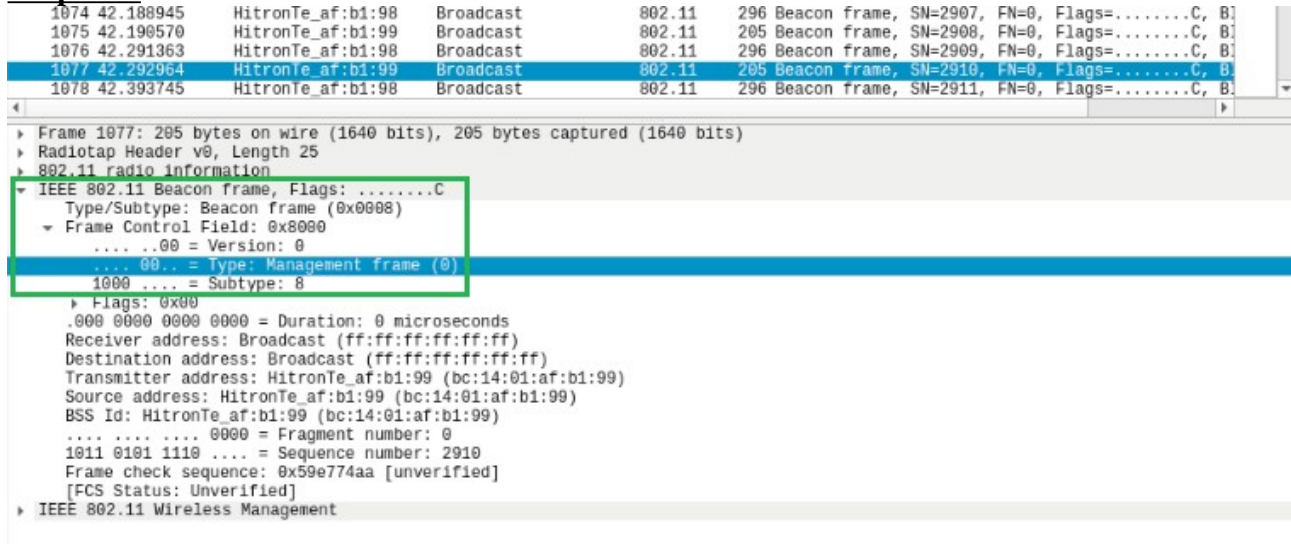


Figura 2: Captura da trama 1077.

O tipo da trama beacon 1077 é 'Management frame', cujo identificador de tipo é 0 (00), e o subtipo é 8 (1000), correspondente a 'Beacon Frame'. Estando especificados no vigésimo quinto byte do cabeçalho da trama com o valor 0x0008.

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

Resposta:

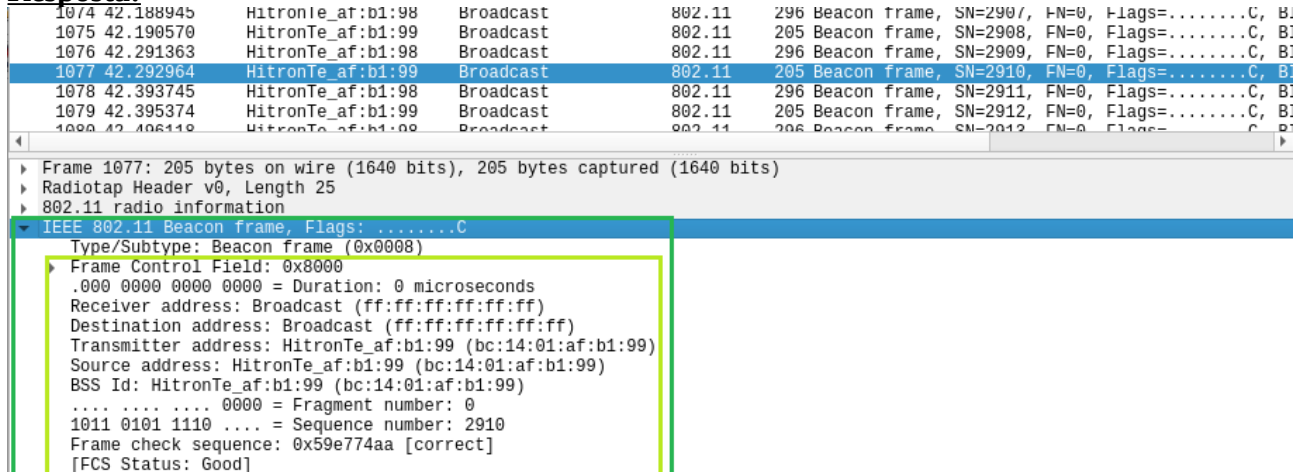


Figura 3: Captura da trama 1077.

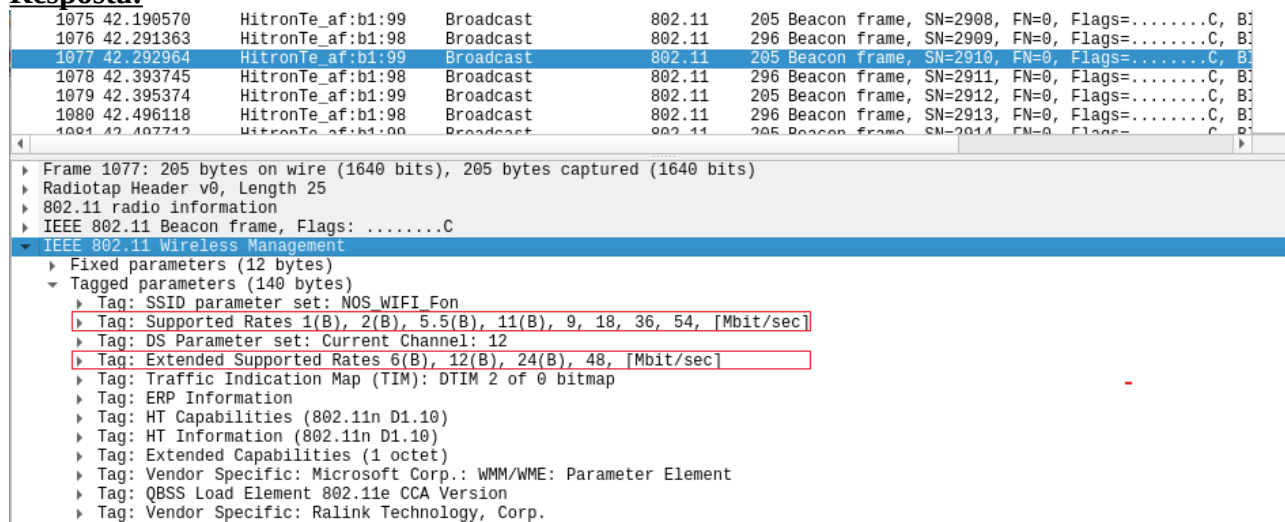
Para os campos 'Receiver address' e 'Destination Address' dos dois SSIDs existentes (FlyingNet e NOS_WIFI_FON) o endereço MAC é sempre o endereço ff:ff:ff:ff:ff:ff (Broadcast).

Para o SSID NOS_WIFI_FON, o 'Transmitter address' é bc:14:01:af:b1:99 (assim como o 'Source Address') e para o SSID FlyingNet é bc:14:01:af:b1:98 (assim como o respetivo 'Source Address').

Conclui-se assim que o ‘Receiver address’ corresponde ao endereço MAC do sistema que recebe a trama, o ‘Destination address’ corresponde ao endereço MAC (broadcast) para poder processar todas as tramas enviadas e o ‘Transmitter address’ e ‘Source address’ correspondem ao endereço MAC do AP que transmite a trama.

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?

Resposta:



No.	Time	Source	Destination	Protocol	Length	Info
1075	42.190570	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2908, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1076	42.291363	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2909, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1077	42.292964	HitronTe_af:b1:99	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	296	Beacon frame, SN=2911, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1079	42.395374	HitronTe_af:b1:99	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	296	Beacon frame, SN=2913, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1081	42.497712	HitronTe_af:b1:99	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	296	Beacon frame, SN=2915, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1083	42.600114	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2916, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

Frame 1077: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits) on interface 0

Ethernet II, Src: HitronTe_af:b1:99, Dst: Broadcast

IEEE 802.11 Beacon frame, Flags:C

IEEE 802.11 Wireless Management

Fixed parameters (12 bytes)

Tagged parameters (140 bytes)

Tag: SSID parameter set: NOS_WIFI_Fon

Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]

Tag: DS Parameter set: Current Channel: 12

Tag: Extended Supported Rates 6(B), 12(B), 24(B), 48, [Mbit/sec]

Tag: Traffic Indication Map (TIM): DTIM 2 of 0 bitmap

Tag: ERP Information

Tag: HT Capabilities (802.11n D1.10)

Tag: HT Information (802.11n D1.10)

Tag: Extended Capabilities (1 octet)

Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

Tag: QBSS Load Element 802.11e CCA Version

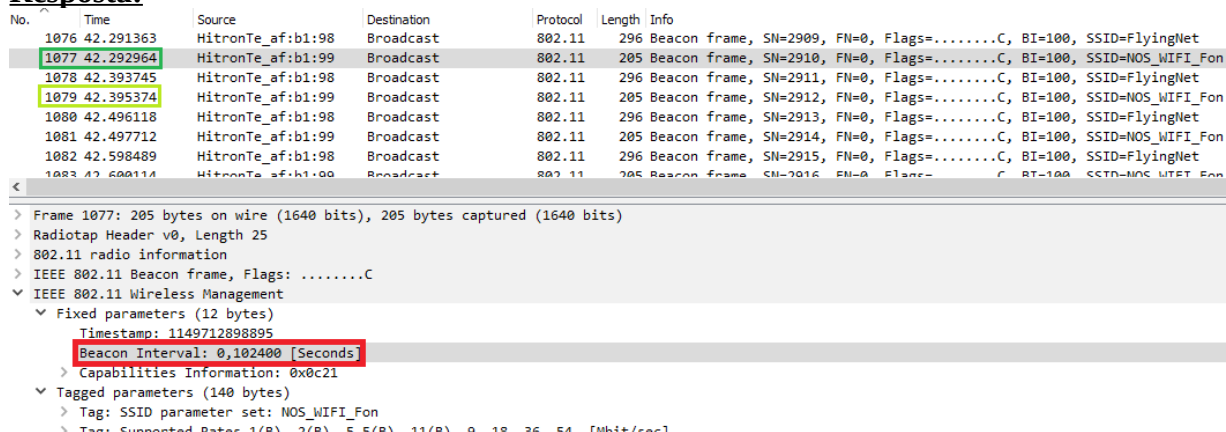
Tag: Vendor Specific: Ralink Technology, Corp.

Figura 4: Débitos bases e débitos adicionais da trama beacon 1077.

Os débitos de base são aqueles que todos os dispositivos devem suportar. Todas as tramas de gestão e tramas enviadas em broadcast são transmitidas usando estes débitos de base. Os débitos de base que um AP pode suportar são 1 Mb/s, 2 Mb/s, 5.5 Mb/s e 11 Mb/s. Os ‘extended support rates’ especificam débitos, que não estão presentes nos supported rates, quando estes têm mais do que 8. Estes débitos são 6 Mb/s, 12 Mb/s, 24 Mb/s e 48 Mb/s.

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.

Resposta:



No.	Time	Source	Destination	Protocol	Length	Info
1076	42.291363	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2909, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1077	42.292964	HitronTe_af:b1:99	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	296	Beacon frame, SN=2911, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1079	42.395374	HitronTe_af:b1:99	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	296	Beacon frame, SN=2913, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1081	42.497712	HitronTe_af:b1:99	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	296	Beacon frame, SN=2915, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1083	42.600114	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2916, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

Frame 1077: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits) on interface 0

Ethernet II, Src: HitronTe_af:b1:99, Dst: Broadcast

IEEE 802.11 Beacon frame, Flags:C

IEEE 802.11 Wireless Management

Fixed parameters (12 bytes)

Timestamp: 1149712898895

Beacon Interval: 0.102400 [Seconds]

Capabilities Information: 0x0c21

Tagged parameters (140 bytes)

Tag: SSID parameter set: NOS_WIFI_Fon

Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]

Figura 5: Tramas beacon analisadas.

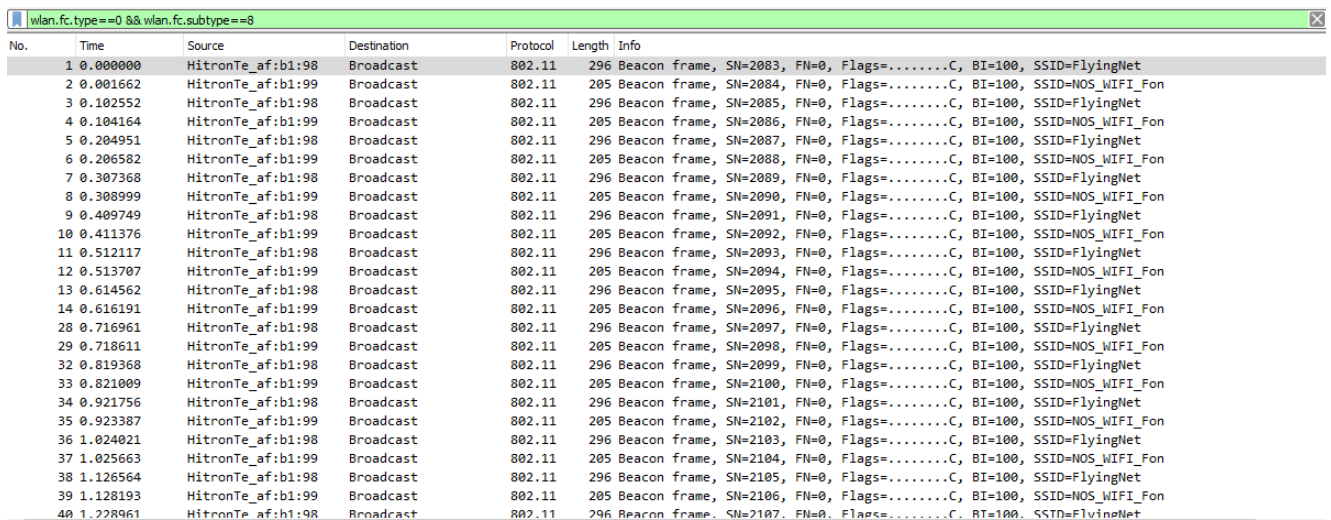
Como podemos observar na figura 5, o intervalo de tempo previsto entre tramas beacon consecutivas é de 0,1024 segundos. Na prática, depois de calcular as durações entre várias tramas consecutivas provenientes dos mesmos APs, identificamos que o valor previsto não ocorre com total

exatidão. Podemos ver no exemplo acima analisado, que as tramas beacon consecutivas, identificadas a verde, provenientes da rede ‘NOS_WIFI_Fon’ tem um tempo entre elas de $42,395374 - 42,292964 = 0,10241$.

Assim, concluímos que a periodicidade de tramas beacon não é verificada, existindo pequenas discrepâncias. Isto acontece pela possibilidade da existência de outros sistemas a ocupar o meio utilizado para comunicar, assim sendo, cada AP espera que o meio esteja disponível para poder então enviar a trama pretendida, não respeitando absolutamente o intervalo de tempo previsto, mas evitando colisões.

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).

Resposta:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2083, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2	0.001662	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2084, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
3	0.102552	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2085, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
4	0.104164	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2086, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
5	0.204951	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2087, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
6	0.206582	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2088, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
7	0.307368	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2089, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
8	0.308999	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2090, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
9	0.409749	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2091, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
10	0.411376	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2092, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
11	0.512117	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2093, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
12	0.513707	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2094, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
13	0.614562	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2095, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
14	0.616191	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2096, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
28	0.716961	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2097, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
29	0.718611	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2098, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
32	0.819368	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2099, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
33	0.821009	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2100, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
34	0.921756	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2101, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
35	0.923387	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2102, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
36	1.024021	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2103, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
37	1.025663	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2104, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
38	1.126564	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2105, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
39	1.128193	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2106, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
40	1.228961	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2107, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Figura 6: Filtro de visualização utilizado.

Os SSIDs dos Aps que estão a operar na vizinhança da STA de captura são ‘FlyingNet’ e ‘NOS_WIFI_FON’.

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.

Resposta:

Primeiramente, para termos acesso ao campo ‘Frame check sequence’ tivemos de modificar a coluna ‘value’ de ‘False’ para ‘True’, como podemos ver na figura abaixo.

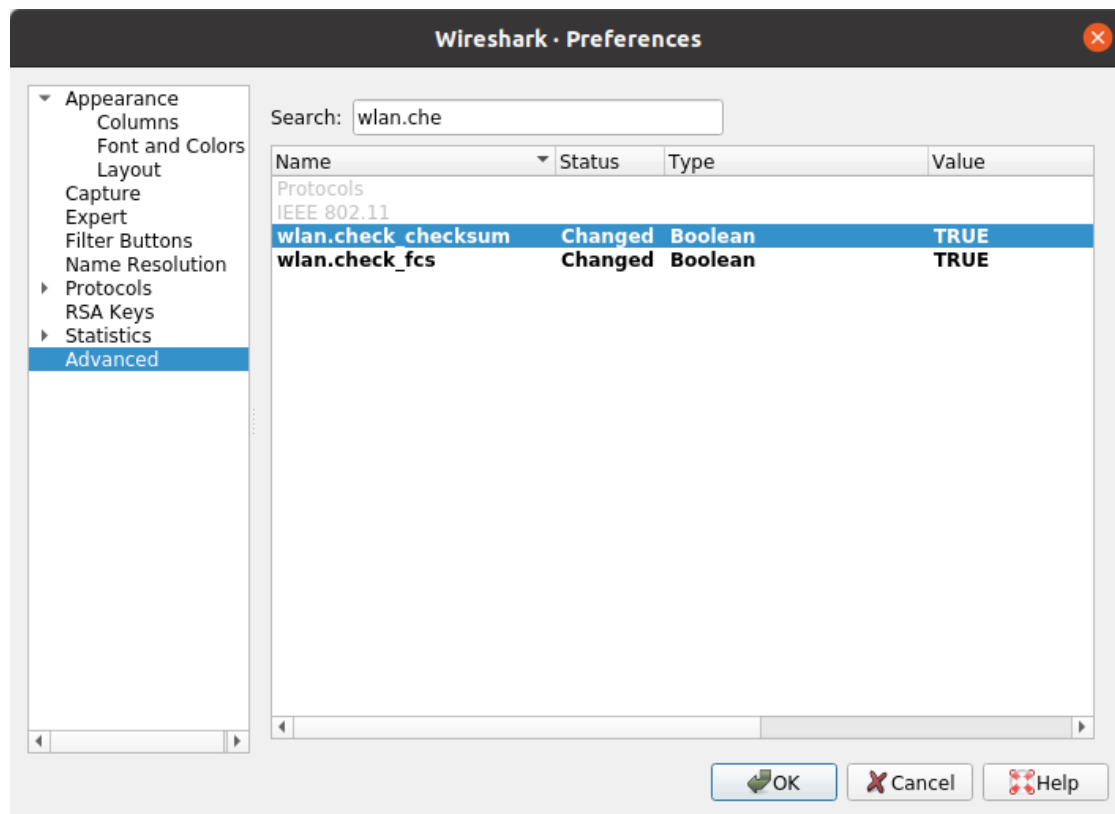


Figura 7: Modificação do campo 'Value' para 'true'.

wlan.fc.type_subtype==0x08 && wlan.fcs.status==bad						
No.	Time	Source	Destination	Protocol	Length	Info
6274	94.779098	36:00:ae:51:f4:19	43:46:06:ca:97:53	802.11	146	Beacon frame, SN=236, FN=9, Flags=.pmPRM.T.
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.FI., BI=4913
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.
7131	100.398018	62:4c:de:c5:a9:3a	34:c4:ca:25:ed:14	802.11	146	Beacon frame, SN=2811, FN=0, Flags=.pmPRM.T.
7173	100.404266	84:84:4c:a8:fd:ea	d2:f4:d1:ff:e5:79	802.11	146	Beacon frame, SN=2338, FN=10, Flags=.pm...T.

Noise level (dBm): -87dBm
Signal/noise ratio (dB): 13dB
TSF timestamp: 119792167
[Duration: 52µs]
IEEE 802.11 Beacon frame, Flags: ...R.FI.
Type/Subtype: Beacon frame (0x0008)
Frame Control Field: 0x830b
....11 = Version: 3
....00.. = Type: Management frame (0)
1000.... = Subtype: 8
Flags: 0x0b
.010 1100 0100 1001 = Duration: 11337 microseconds
Receiver address: 0e:0b:77:ea:c1:bc (0e:0b:77:ea:c1:bc)
Destination address: 0e:0b:77:ea:c1:bc (0e:0b:77:ea:c1:bc)
Transmitter address: be:65:24:9b:d6:a1 (be:65:24:9b:d6:a1)
Source address: be:65:24:9b:d6:a1 (be:65:24:9b:d6:a1)
BSS Id: 8c:3f:e6:82:e5:c9 (8c:3f:e6:82:e5:c9)
....1010 = Fragment number: 10
0001 1000 1001 = Sequence number: 393
Frame check sequence: 0xdf7afa53 incorrect, should be 0x619125e8
[FCS Status: Bad]

Figura 8: Captura da trama 6937.

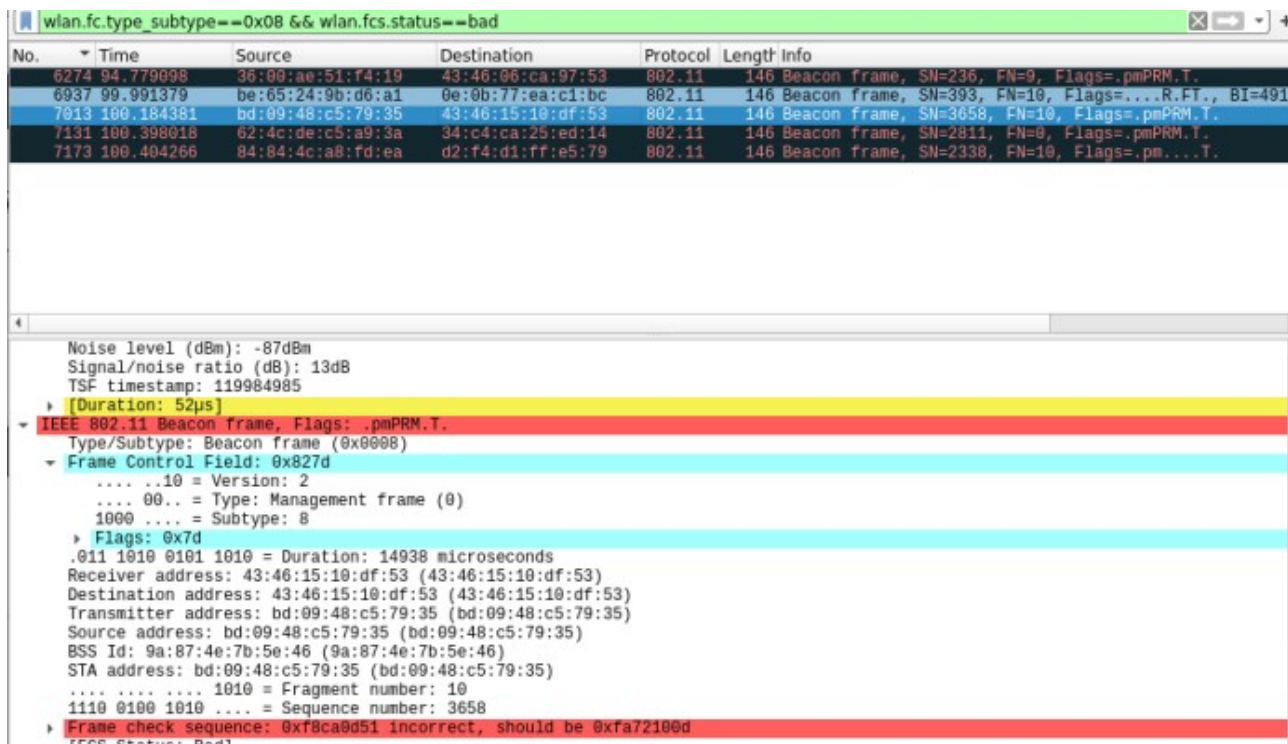


Figura 9: Captura da trama 7013.

Após termos verificado o campo ‘Frame check sequence’ para uma trama de cada SSID apercebemo-nos que o método de detecção de erros está a ser usado. No entanto, nenhuma das tramas é recebida corretamente (sem erros), pois o campo FCS em todas tramas aparece como incorreto, indicando posteriormente qual devia ser o valor deste campo. Ao contrário das redes cabeladas, as redes sem fios têm maior probabilidade de haver colisões e erros nas tramas daí a necessidade de detecção de erros.

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

Resposta:

Para visualizar apenas as tramas ‘probing request’ (subtipo 4) e ‘probing response’ (subtipo 5) é necessário o seguinte filtro: `wlan.fc.type_subtype == 0x0004 || wlan.fc.type_subtype == 0x0005`.

wlan.fc.type_subtype == 0x0004 wlan.fc.type_subtype == 0x0005					
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:b1:98	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:b1:98	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:b1:98	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	72.180590	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)
4494	82.728646	7c:ea:6d:ff:a2:cc	Broadcast	802.11	218 Probe Request, SN=65, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
6193	94.190800	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., 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=....., 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=....., SSID=FlyingNet
6204	94.224724	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6205	94.237944	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6206	94.248503	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6207	94.261777	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6208	94.272579	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6209	94.285744	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6210	94.296433	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6222	94.358606	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6223	94.369617	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6224	94.382988	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6225	94.394120	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6226	94.407423	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6227	94.418665	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6228	94.431968	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6229	94.443153	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6230	94.456432	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6231	94.467671	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6244	94.530299	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6245	94.541478	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6246	94.553920	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
6247	94.564967	Apple_28:b8:0c	Broadcast	802.11	152 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
▼ Frame 1300: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits)					
0000	00 00 19 00 0f 08 00 00 23 3e 62 04 00 00 00 00 #>b			
0010	10 02 a3 09 08 04 b9 a9 00 40 00 00 00 ff ff ff @			
0020	ff ff ff ff 64 9a be 10 6a f5 ff ff ff ff ff ff j @			
0030	9d 00 00 00 04 02 04 0b 16 32 00 9c 12 18 24 30 2 \$0			
0040	48 00 00 03 01 00 2d 1a 21 40 17 ff 00 00 00 00	H'1 !@			
0050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00			
0060	00 00 7f 08 04 00 08 84 00 00 00 40 6b 07 0f ff @k			

Figura 10: Tramas probing request ou probing response.

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?

Resposta:

Quando uma estação (STA) necessita de conhecer quais os APs a que se pode associar, esta envia um ‘probe request’ em broadcast. Após isso, os APs que estão dentro da sua área de cobertura, recebem esta trama de requisito, respondendo com tramas ‘probe response’ à estação (STA) que as requiere.

Para podermos observar este processo, identificamos a trama ‘probing request’ 2616, tratando-se de uma STA (Apple_10:6a:f5) e uma correspondente trama ‘probing response’ 2617, o AP (HitronTe_af:b1:98). Assim, inicialmente, o nosso ‘probing request’ na trama 2616 está a ser enviado em broadcast para todos os equipamentos da rede em questão, procurando possíveis APs. Após isso, na trama 2617 observamos que a partir de um AP está a ser enviado, ao STA em questão, uma ‘probing response’, nas quais também estão incluídas informações úteis sobre as taxas de dados suportadas.

[wlan.fc.type.subtype == 0x0004 wlan.fc.type.subtype == 0x0005						
No.	Time	Source	Destination	Protocol	Length	Info
1390	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	70.148098	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:b1:98	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:b1:98	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:b1:98	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2337, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2693	72.179215	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2563, FN=0, Flags=.....C, SSID=FlyingNet
2696	72.179924	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2347, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2698	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
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
Frame 2610: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface 0 Radiotap Header v0, Length 25 IEEE 802.11 radio information IEEE 802.11 Probe Request, Flags=.....C Type/Subtype: Probe Request (0x0004) Frame Control Field: 0x000000 = Version: 000 = Type: Management frame (0) 0100 = Subtype: 4 Flags: 0x00 000 0000 0000 = Duration: 0 microseconds Receiver address: Broadcast (ff:ff:ff:ff:ff:ff) Destination address: Broadcast Transmitter address: Apple_10:6a:f5 (64:9a:bb:10:6a:f5) Source address: Apple_10:6a:f5 (64:9a:bb:10:6a:f5) BSS ID: Broadcast (ff:ff:ff:ff:ff:ff)0000 = Fragment number: 0 1010 0000 0101 = Sequence number: 2505 Frame check sequence: 0x620b9a9e [correct] [FCS Status: Good] IEEE 802.11 Wireless Management						

Figura 11: Trama ‘probing request’.

[wlan.fc.type.subtype == 0x0004 wlan.fc.type.subtype == 0x0005						
No.	Time	Source	Destination	Protocol	Length	Info
1390	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	70.148098	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:b1:98	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:b1:98	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:b1:98	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2337, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2693	72.179215	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2563, FN=0, Flags=.....C, SSID=FlyingNet
2696	72.179924	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2347, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2698	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
Frame 2617: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits) on interface 0 Radiotap Header v0, Length 25 IEEE 802.11 radio information IEEE 802.11 Probe Response, Flags=.....C Type/Subtype: Probe Response (0x0005) Frame Control Field: 0x000000 = Version: 000 = Type: Management frame (0) 0101 = Subtype: 5 Flags: 0x00 000 0000 0011 0010 = Duration: 50 microseconds Receiver address: Apple_10:6a:f5 (64:9a:bb:10:6a:f5) Destination address: Apple_10:6a:f5 (64:9a:bb:10:6a:f5) 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 0010 1110 = Sequence number: 2350 Frame check sequence: 0xad8c0359 [correct] [FCS Status: Good] IEEE 802.11 Wireless Management						

Figura 12: Trama ‘probing response’.

1.3. Processo de Associação

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.

Resposta:

[(wlan.fc.type==0 && (wlan.fc.subtype==0 wlan.fc.subtype==1 wlan.fc.subtype==0xb)) (wlan.fc.type==1 && wlan.fc.subtype==0xd)						
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
2487	70.362050		Apple_10:6a:f5 (64:9a:bb:10:6a:f5)	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 (bc:14:01: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 (64:9a:bb:10:6a:f5)	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 (bc:14:01:af:b1:98)	802.11	39	Acknowledgement, Flags=.....C

Figura 13: Captura da sequência de tramas.

A figura 13 corresponde ao resultado obtido após ter sido aplicado o filtro ‘(wlan.fc.type==0 && (wlan.fc.subtype==0 || wlan.fc.subtype==1 || wlan.fc.subtype==0xb)) || (wlan.fc.type==1 && wlan.fc.subtype==0xd)’ para encontrar as tramas ‘Association Request’ e ‘Association Response’. A trama 2490 corresponde a um pedido de associação e a trama 2492 corresponde a uma resposta de associação. O processo começa com a STA a enviar um pedido ‘Authentication’ para o AP, no entanto antes dessa trama ser enviada será enviada uma trama do tipo ‘Acknowledgement’ para a STA ser identificada. De seguida o AP passará pelo mesmo processo anterior. Isto será seguido de

um envio de uma trama 'Association Request' da STA para o AP e será enviada no sentido inverso uma trama 'Association Response'.

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

Resposta:

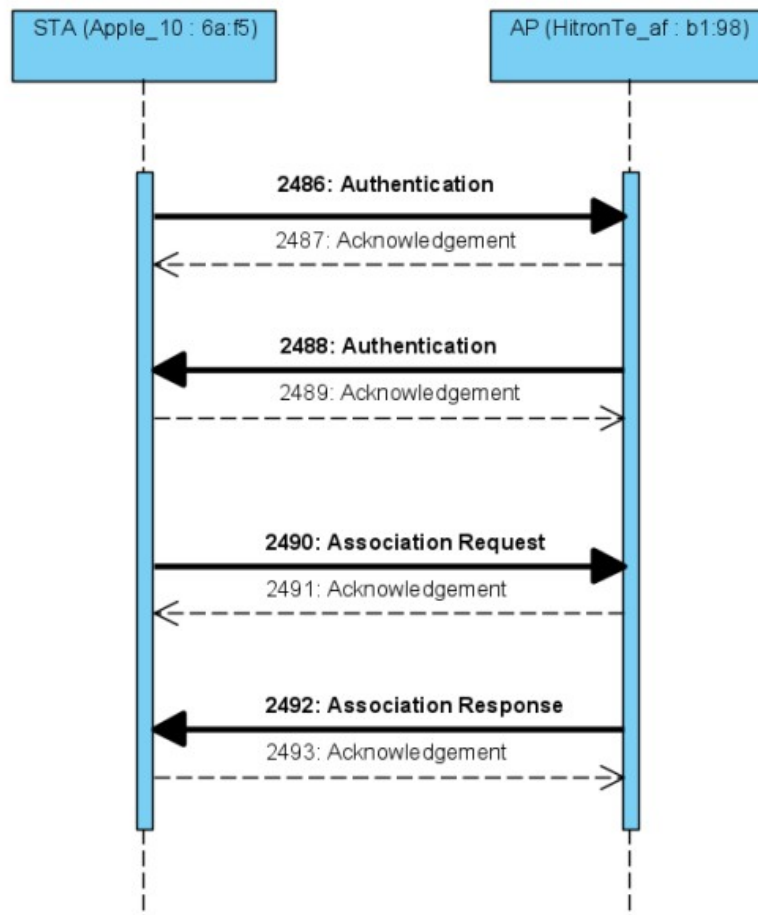


Figura 14: Diagrama ilustrativo da sequência das tramas.

1.4. Transferência de Dados

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?

Resposta:

No.	Time	Source	Destination	Protocol	Length	Info
450	18.536100	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2446, FN=0, Flags=...
451	18.536165	Apple_71:41:a1	HitronTe_af:b1:98	802.11	68	Null function (No data), SN=1750, FN=...
452	18.536187		Apple_71:41:a1 (d8:...)	802.11	39	Acknowledgement, Flags=.....C
453	18.536401	HitronTe_af:b1:98 (...)	Apple_71:41:a1 (d8:...)	802.11	49	802.11 Block Ack Req, Flags=.....C
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....
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....

▶ 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
.... 10 = DS status: Frame from DS to a STA via AP (To DS: 0 From DS: 1) (0x2)
.... 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
.1.. = Protected flag: Data is protected
0... = Order flag: Not strictly ordered
.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)

0010 16 30 a3 09 80 04 bf a9 00 88 42 24 00 d8 a2 5e 00 B\$...^
0020 71 41 a1 bc 14 01 af b1 98 bc 14 01 af b1 98 40 qA.....@
0030 11 00 00 13 11 00 20 02 00 00 00 eb 0f 24 4b 5c \$K\

Figura 14: Captura da trama 455.

Como se pode verificar na figura acima, a direcionalidade da trama 455 é do sistema de distribuição (DS) para o STA via AP, sendo que o tipo é 2 e o subtipo é 8, logo ‘from DS’ vale 1 e o ‘to DS’ vale 0. Assim sendo, a direcionalidade é 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?

Resposta:

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....
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....

.... 0... = Retry: Frame is not being retransmitted
...0 = PWR MGT: STA will stay up
..0. = More Data: No data buffered
.1.. = Protected flag: Data is protected
0... = Order flag: Not strictly ordered
.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)

0010 16 30 a3 09 80 04 bf a9 00 88 42 24 00 d8 a2 5e 00 B\$...^
0020 71 41 a1 bc 14 01 af b1 98 bc 14 01 af b1 98 40 qA.....@
0030 11 00 00 13 11 00 20 02 00 00 00 eb 0f 24 4b 5c \$K\

Figura 15: Endereços da trama 455.

Como se vê na figura 15, têm-se os seguintes endereços:

ROUTER - Source address: bc:14:01:af:b1:98

AP - BSS Id: bc:14:01:af:b1:98

STA - STA address: d8:a2:5e:71:41:a1

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

Resposta:

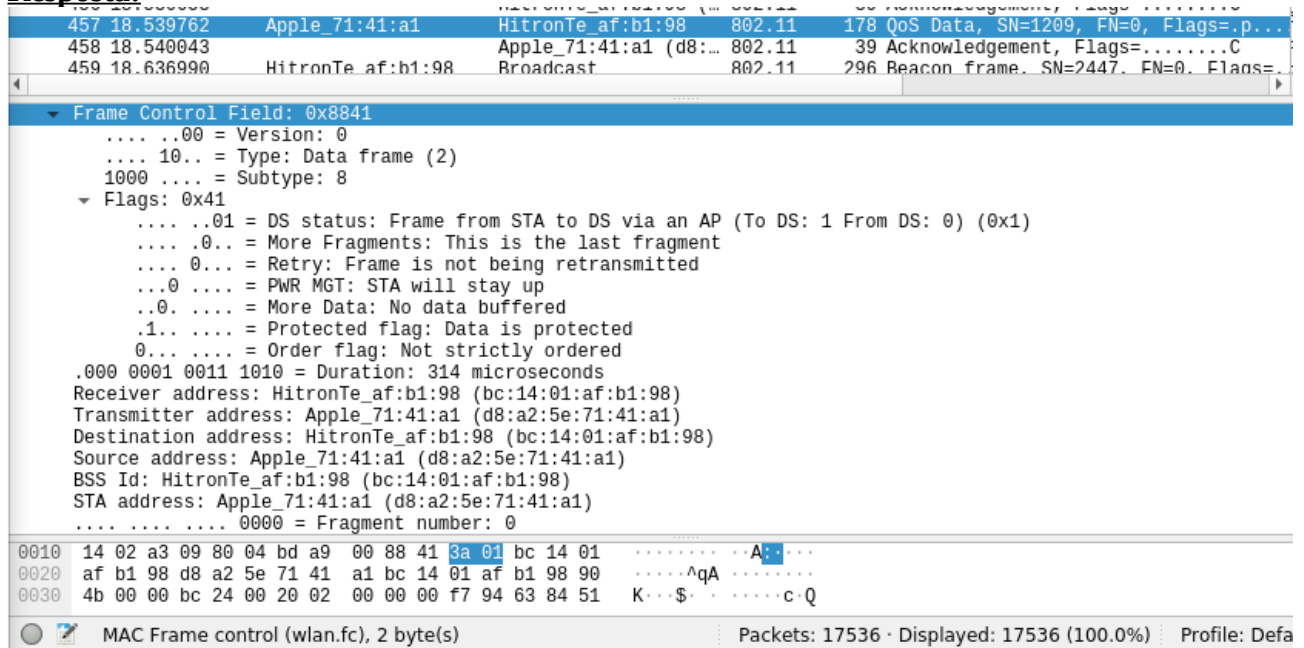


Figura 16: Captura da trama 457.

Tendo em conta que, como se vê na figura 16, a flag 'DS Status' possui o valor 01, o endereço de destino ser o bc:14:01:af:b1:96 e o de fonte ser o d8:a2:5e:71:41:a1, a direccionalidade da trama é da STA para o DS.

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.)

Resposta:

452	18.536187		Apple_71:41:a1 (d8:...	802.11	39	Acknowledgement, Flags=.....C
453	18.536401	HitronTe_af:b1:98 (...	Apple_71:41:a1 (d8:...	802.11	49	802.11 Block Ack Req, Flags=.....C
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
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...
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=...

▶ 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
.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 = Subtype: 8
▼ Flags: 0x41
.... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
.... ..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
..1.. = Protected flag: Data is protected
0... = Order flag: Not strictly ordered
..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)

Figura 17: Subtipo da trama 457.

Como podemos ver na figura 17, o subtipo da trama 457 é 'QoS Data' e é responsável por garantir uma qualidade de serviço na transmissão dos pacotes, através de priorização de tráfego e alocação adicional de recursos, visto que em redes wireless a probabilidade de ocorrerem colisões é muito maior do que em redes Ethernet.

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.

Resposta:

2340	65.461984	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (TA)	HitronTe_af:b1:98 (...	802.11	45	Request-to-send, Flags=.....C
2341	65.461994		Apple_10:6a:f5 (64:...	802.11	39	Clear-to-send, Flags=.....C
2342	65.462049	Apple_10:6a:f5	IPv4mcast_fb	802.11	440	QoS Data, SN=3816, FN=0, Flags=.p....TC
2343	65.462077	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (TA)	Apple_10:6a:f5 (64:...	802.11	57	802.11 Block Ack, Flags=.....C
2344	65.462151	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	53	Null function (No data), SN=2534, FN=0, Flags=.....TC
2345	65.462216		Apple_10:6a:f5 (64:...	802.11	39	Acknowledgement, Flags=.....C
2346	65.462273	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (TA)	HitronTe_af:b1:98 (...	802.11	45	Request-to-send, Flags=.....C
2347	65.462355		Apple_10:6a:f5 (64:...	802.11	39	Clear-to-send, Flags=.....C
2348	65.462437	Apple_10:6a:f5	IPv6mcast_fb	802.11	460	QoS Data, SN=3817, FN=0, Flags=.p....TC
2349	65.462539	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (TA)	Apple_10:6a:f5 (64:...	802.11	57	802.11 Block Ack, Flags=.....C
2350	65.462684	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (TA)	Apple_10:6a:f5 (64:...	802.11	49	802.11 Block Ack Req, Flags=.....C

Figura 18: Pacotes RTS e CTS.

As opções 'Request To Send' (RTS) e 'Clear To Send' (CTS) estão a ser usadas na troca de dados entre a STA e o AP/Router da WLAN, como podemos verificar a destacado na figura acima.

Neste caso específico, primeiramente a STA (Apple_10:6a:f5) envia um RTS ao AP (HitronTe_af:b1:98). Em resposta a este requerimento, a STA recebe um CTS com a indicação se pode fazer a transmissão de dados, indicando se pode ou não fazer a transmissão de dados.

2. Conclusões

O desenvolvimento deste trabalho permitiu um aumento no conhecimento relativamente a redes sem fio IEEE 802.11, tendo abordado aspetos como o formato/tipo de tramas, endereçamento dos componentes envolvidos na comunicação sem fios e o funcionamento do protocolo.

Na secção 1.1. verificámos que a sequência de bytes capturada inclui, para além da trama, uma camada com informação sobre o nível físico, como a frequência do sinal, o canal e o débito que a rede wireless está a operar.

De seguida, vimos o funcionamento do scanning passivo e ativo. As tramas do ‘beacon’ permitem efectuar scanning passivo em redes IEEE 802.11, permitindo desta forma descobrir as APs existentes, enquanto que no scanning activo é usado o ‘probe request’ e o ‘probe response’ para o mesmo efeito.

Posteriormente, analisamos o processo que antecede a autenticação e a consequente associação dos equipamentos que irão trocar informação. Verificamos que para ser possível o envio de dados, a associação de um host a um ponto de acesso é realizada através de um pedido de associação, ao qual se obtém a resposta de um ‘Access Point’.

Por último, abordámos a forma como ocorre a transferência de dados com base na análise da informação obtida na trama de dados e de controlo da transferência. Aqui verificou-se que as redes wireless, contêm controlo de erros (CRC, com FCS), visto que a probabilidade de ocorrência de colisões é muito maior. No entanto, existem mecanismos para evitar as colisões denominados ‘RTS’ e ‘CTS’, que aquando da necessidade de envio de um pacote “questionam” o Access Point (AP) dessa possibilidade, e este responde com um pacote ‘CTS’.

Em suma, este projeto permitiu solidificar a matéria lecionada até ao momento.